McAfee®

Wireless Protection 2007

Manual do Utilizador

Índice

McAfee Wireless Protection 5

McAfee SecurityCenter 7

Funcionalidades ... 8
Utilizar o SecurityCenter ... 9
Cabeçalho ... 9
Coluna da esquerda ... 9
Painel principal ... 10
Noções sobre os ícones do SecurityCenter ... 11
Noções sobre o estado de protecção ... 13
Resolução de problemas relacionados com protecção ... 19
Ver informações sobre o SecurityCenter ... 20
Utilizar o Menu Avançado ... 20
Configurar as opções do SecurityCenter ... 21
Configurar o estado de protecção ... 22
Configurar opções de utilizador ... 23
Configurar opções de actualização ... 26
Configurar opções de alerta ... 31
Efectuar tarefas comuns ... 33
Efectuar tarefas comuns ... 33
Ver eventos recentes ... 34
Manutenção automática do computador ... 35
Manutenção manual do computador ... 36
Gerir a sua rede ... 38
Obter mais informações sobre vírus ... 38

McAfee QuickClean 39

Noções básicas sobre as funcionalidades do QuickClean ... 40
Funcionalidades ... 40
Limpar o computador ... 41
Utilizar o QuickClean ... 43

McAfee Shredder 45

Noções básicas das funcionalidades do Shredder ... 46
Funcionalidades ... 46
Apagar ficheiros indesejados com o Shredder ... 47
Utilizar o Shredder ... 48

McAfee Network Manager 49

Funcionalidades 50
Noções básicas sobre os ícones do Network Manager 51
Configurar uma rede gerida 53
Utilizar o mapeamento de rede 54
Aderir à rede gerida 57
Gerir a rede de forma remota 61
Monitorizar o estado e as permissões 62
Corrigir vulnerabilidades de segurança 65

McAfee Wireless Network Security 67

Funcionalidades 68
Iniciar o Wireless Network Security 70
Iniciar o Wireless Network Security 70
Parar o Wireless Network Security 71
Proteger redes sem fios 73
Configurar redes sem fios protegidas 74
Adicionar computadores à rede sem fios protegida 86
Administrar redes sem fios 91
Gerir redes sem fios 92
Gerir segurança da rede sem fios 103
Configurar definições de segurança 104
Administrar chaves de rede 109
Monitorizar redes sem fios 119
Monitorizar ligações de rede sem fios 120
Monitorizar redes sem fios protegidas 125
Resolução de problemas 131

McAfee EasyNetwork 147

Funcionalidades 148
Configurar o EasyNetwork 149
Iniciar o EasyNetwork 150
Aderir a uma rede gerida 151
Abandonar uma rede gerida 155
Partilhar e enviar ficheiros 157
Partilhar ficheiros 158
Enviar ficheiros para outros computadores 161
Partilhar impressoras 163
Trabalhar com impressoras partilhadas 164

Referência 167

Glossário 168

Acerca da McAfee 187

Copyright 188

Índice remissivo 189

CAPÍTULO 1

McAfee Wireless Protection

O McAfee Wireless Protection Suite elimina os problemas de trabalho em rede e os riscos de segurança em ambientes de rede sem fios. A respectiva protecção de confiança evita ataques de hackers à sua rede Wi-Fi®, protege as suas informações e transacções pessoais e impede que outras pessoas utilizem a sua rede para aceder à Internet – tudo com apenas um clique. As chaves de encriptação fortes e de rotação do McAfee Wireless Network Security frustram até mesmo os intrusos mais determinados. O Wireless Protection inclui também o McAfee EasyNetwork, que simplifica a partilha de ficheiros e impressoras através da rede. Além disso, é fornecido em conjunto com o McAfee Network Manager, que procura a existência de vulnerabilidades de segurança nos computadores da rede e permite corrigir facilmente potenciais problemas de segurança.

O Wireless Protection inclui os seguintes programas:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter é um ambiente fácil de utilizar onde os utilizadores da McAfee podem criar, gerir e configurar as respectivas subscrições de segurança.

O SecurityCenter funciona também como uma fonte de informação de alertas contra vírus, informações sobre produtos, suporte, informações de subscrição e acesso de um clique a ferramentas e notícias incluídas no Web site da McAfee.

Neste capítulo

Funcionalidades 8
Utilizar o SecurityCenter 9
Configurar as opções do SecurityCenter 21
Efectuar tarefas comuns 33

Funcionalidades

O McAfee SecurityCenter oferece as seguintes funcionalidades e benefícios novos:

Estado de protecção optimizado

Analisa facilmente o estado de segurança do computador, procura actualizações e corrige potenciais problemas de segurança.

Actualizações contínuas

Instala actualizações diárias automaticamente. Quando existe uma nova versão do software da McAfee disponível, esta pode ser obtida automaticamente e de forma gratuita durante a subscrição, garantindo sempre uma protecção actualizada.

Alerta em tempo real

Os alertas de segurança informam-no de surtos de vírus e ameaças de segurança, fornecendo opções de resposta para remover, neutralizar ou obter mais informações sobre a ameaça.

Protecção adequada

Existe uma grande variedade de opções de renovação que ajudam a manter a protecção da McAfee actualizada.

Ferramentas de desempenho

Removem ficheiros não utilizados, desfragmentam ficheiros utilizados e utilizam processos de restauro do sistema que maximizam o desempenho do computador.

Ajuda real online

Pode obter suporte de peritos na segurança do seu computador da McAfee através de chat, correio electrónico ou telefone.

Protecção de navegação segura

Se instalada, a extensão do browser McAfee SiteAdvisor protege-o contra spyware, correio publicitário não solicitado, vírus e fraudes online, classificando os Web sites que visita ou que aparecem nos resultados de procura na Web. Pode ver classificações de segurança detalhadas que reflectem os testes efectuados aos sites em termos de práticas de correio electrónico, transferências, filiações online e perturbações, tais como janelas de contexto e cookies de registo de terceiros.

CAPÍTULO 3

Utilizar o SecurityCenter

Pode executar o SecurityCenter a partir do ícone McAfee SecurityCenter na área de notificação do Windows na parte mais à direita da barra de tarefas ou no ambiente de trabalho do Windows.

Ao abrir o SecurityCenter, o painel Página Inicial apresenta o estado de segurança do computador e permite um acesso rápido a actualizações e pesquisas (se o McAfee VirusScan estiver instalado), bem como a outras tarefas comuns:

Cabeçalho

Ajuda

Veja o ficheiro de ajuda dos programas.

Coluna da esquerda

Actualizar

Actualize o seu produto para garantir protecção contra as mais recentes ameaças.

Analisar

Se o McAfee VirusScan estiver instalado, pode efectuar uma pesquisa manual do computador.

Tarefas comuns

Efectue tarefas comuns, que incluem voltar ao painel Página Inicial, ver eventos recentes, gerir a rede do computador (se trabalhar num computador com capacidade de gestão para este tipo de rede) e efectuar a manutenção do computador. Se o McAfee Data Backup estiver instalado, pode também criar uma cópia de segurança dos dados.

Componentes instalados

Veja quais são os serviços de segurança que estão a proteger a segurança do seu computador.

Painel principal

Estado de protecção

Em **Estou protegido?**, veja o nível geral do estado de protecção do seu computador. Abaixo desta opção, veja uma perturbação de estado por categoria e tipo de protecção.

Informações sobre o SecurityCenter

Pode ver quando ocorreu a última actualização do computador, a última pesquisa (caso o McAfee VirusScan esteja instalado), assim como a data de expiração da subscrição.

Neste capítulo

Noções sobre os ícones do SecurityCenter 11
Noções sobre o estado de protecção 13
Resolução de problemas relacionados com protecção 19
Ver informações sobre o SecurityCenter 20
Utilizar o Menu Avançado 20

Noções sobre os ícones do SecurityCenter

Os ícones do SecurityCenter são apresentados na área de notificação do Windows, na parte mais à direita da barra de tarefas. Utilize os ícones para ver se o computador está totalmente protegido, ver o estado de uma pesquisa em curso (caso o McAfee VirusScan esteja instalado), verificar se existem actualizações, ver eventos recentes, efectuar a manutenção do computador e obter suporte do Web site da McAfee.

Abrir o SecurityCenter e utilizar funções adicionais

Quando o SecurityCenter estiver a funcionar, é apresentado o ícone M do SecurityCenter na área de notificação do Windows, na parte mais à direita da barra de tarefas.

Para abrir o SecurityCenter ou utilizar funções adicionais:

- Clique com o botão direito do rato no ícone do SecurityCenter e clique numa das seguintes opções:
  - Abrir o SecurityCenter
  - Actualizações
  - Ligações rápidas

    O submenu contém ligações a Página Inicial, Ver Eventos Recentes, Gerir Rede, Manter Computador e Cópia de Segurança de Dados (caso esteja instalada).
  - Verificar Subscrição

    (Esta opção é apresentada quando expira, pelo menos, uma subscrição de produtos.)
  - Centro de Actualizações
  - Suporte ao Cliente

Verificar o estado de protecção

Se o computador não estiver totalmente protegido, é apresentado o ícone de estado de protecção na área de notificação do Windows na parte mais à direita da barra de tarefas. O ícone pode aparecer a vermelho ou a amarelo, conforme o estado de protecção.

Para verificar o estado de protecção:

- Clique no ícone de estado de protecção para abrir o SecurityCenter e corrigir quaisquer problemas.

Verificar o estado das actualizações

Se estiver a verificar actualizações, é apresentado o ícone de actualizações na área de notificação do Windows, na parte mais à direita da barra de tarefas.

Para verificar o estado das actualizações:

- Clique no ícone de actualizações para ver o estado das actualizações numa sugestão.

Noções sobre o estado de protecção

O estado de protecção de segurança geral do computador é indicado em **Estou protegido?** no SecurityCenter.

O estado de protecção informa-o se o computador está totalmente protegido contra as mais recentes ameaças de segurança ou se os problemas requerem atenção e mostra-lhe como resolver esses problemas. Se um problema afectar mais de uma categoria de protecção, a resolução desse problema pode resultar na reposição de várias categorias para o estado de protecção total.

Alguns dos factores que influenciam o estado de protecção incluem ameaças de segurança externas, produtos de segurança instalados no computador, produtos que acedem à Internet e o tipo de configuração destes produtos de segurança e Internet.

Por predefinição, se as opções Protecção contra Correio Publicitário Não Solicitado ou Bloqueio de Conteúdos não estiverem instaladas, estes problemas de protecção não críticos serão automaticamente ignorados, não sendo registados no estado de protecção geral. No entanto, se for apresentada uma ligação **Ignorar** junto a um problema de protecção, pode ignorar o problema, caso tenha a certeza de que não quer resolvê-lo.

Estou protegido?

Verifique o nível geral do estado de protecção do computador em **Estou protegido?** no SecurityCenter:

- É apresentado **Sim** se o computador estiver totalmente protegido (verde).
- É apresentado **Não** se o computador estiver parcialmente protegido (amarelo) ou não protegido (vermelho).

Para resolver a maioria dos problemas de protecção automaticamente, clique em **Corrigir** junto do estado de protecção. No entanto, se continuarem a aparecer um ou mais problemas que exijam a sua resposta, clique na ligação junto do problema para realizar a acção sugerida.

Noções sobre tipos e categorias de protecção

Em **Estou protegido?** no SecurityCenter, pode ver uma perturbação de estado que inclui estes tipos e categorias de protecção:

- Computador e ficheiros
- Internet e rede
- Correio electrónico e mensagens instantâneas
- Limitações de acesso

Os tipos de protecção apresentados no SecurityCenter dependem dos produtos instalados. Por exemplo, é apresentado o tipo de protecção Monitorização do Estado do Sistema se o software Cópia de Segurança de Dados McAfee estiver instalado.

Se uma categoria não tiver quaisquer problemas de protecção, o estado é Verde. Se clicar numa categoria Verde, é apresentada no lado direito uma lista dos tipos de protecção activados, assim como uma lista dos problemas já ignorados. Se não houver nenhum problema, é apresentado um aviso de vírus em vez de quaisquer problemas. Pode também clicar em **Configurar** para alterar as opções dessa categoria.

Se todos os tipos de protecção de uma categoria tiverem o estado Verde, o estado dessa categoria é Verde. Do mesmo modo, se todas as categorias de protecção tiverem o estado Verde, o estado de protecção geral é Verde.

Se alguma das categorias de protecção tiver o estado Amarelo ou Vermelho, pode resolver os problemas de protecção corrigindo-os ou ignorando-os, mudando o estado para Verde.

Noções sobre protecção de computadores e ficheiros

A categoria de protecção Computador e Ficheiros inclui os seguintes tipos de protecção:

- **Protecção Antivírus** -- A protecção de pesquisa em tempo real protege o computador de vírus, worms, cavalos de Tróia, scripts suspeitos, ataques híbridos e outras ameaças. Efectua uma pesquisa automática e tenta limpar os ficheiros (incluindo ficheiros comprimidos .exe, sector de arranque, memória e ficheiros críticos) quando são utilizados pelo utilizador ou pelo computador.
- **Protecção Anti-Spyware** -- A protecção anti-spyware detecta, bloqueia e remove spyware, adware e outros programas potencialmente indesejados que possam recolher e transmitir dados privados sem a sua autorização.
- **Protecções do Sistema** -- As Protecções do Sistema detectam alterações no computador e avisam-no quando ocorrem. Pode, em seguida, analisar estas alterações e decidir se pretende autorizá-las.
- **Protecção do Windows** -- A protecção do Windows mostra o estado do Windows Update no computador. Se o McAfee VirusScan estiver instalado, a protecção contra sobrecargas da memória intermédia está também disponível.

Um dos factores que influenciam a protecção Computador e Ficheiros são as ameaças de vírus externos. Por exemplo, se ocorrer um surto de vírus, será que o software antivírus instalado pode protegê-lo? Além disso, outros factores incluem a configuração do software antivírus e se o software está a ser constantemente actualizado com os mais recentes ficheiros de assinatura de detecção que protegem o computador das mais recentes ameaças.

Abra o painel de configuração Computador e Ficheiros

Se não existirem problemas em **Computador e & Ficheiros**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Computador e Ficheiros:

1. No painel Página Inicial, clique em **Computador e & Ficheiros**.
2. No painel da direita, clique em **Configurar**.

Noções sobre protecção da Internet e da rede

A categoria de protecção Internet e Rede inclui os seguintes tipos de protecção:

- **Protecção por Firewall** -- A protecção por firewall protege o computador de intrusões e tráfego de rede indesejado. Ajuda-o a gerir as ligações de entrada e saída da Internet.
- **Wireless Protection** -- A protecção sem fios protege a rede doméstica sem fios de intrusões e intercepção de dados. Contudo, se tiver uma ligação a uma rede sem fios externa, a protecção varia consoante o nível de segurança dessa rede.
- **Protecção da Navegação na Web** -- A protecção de navegação na Web oculta anúncios, janelas de contexto e bugs da Web no computador quando se navega na Internet.
- **Protecção contra Phishing** -- A protecção contra Phishing permite bloquear Web sites fraudulentos que solicitam informações pessoais através de hiperligações em mensagens instantâneas e de correio electrónico, janelas de contexto e outros meios.
- **Protecção de Informações Pessoais** -- A protecção de informações pessoais impede a divulgação de informações sensíveis e confidenciais na Internet.

Abra o painel de configuração Internet e Rede

Se não existirem problemas em **Internet e & Rede**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Internet e Rede:

1. No painel Página Inicial, clique em **Internet e & Rede**.
2. No painel da direita, clique em **Configurar**.

Noções sobre protecção de correio electrónico e mensagens instantâneas

A categoria de protecção Correio Electrónico e Mensagens Instantâneas inclui os seguintes tipos de protecção:

- **Protecção do Correio Electrónico** -- A protecção do correio electrónico efectua pesquisas automáticas e tenta limpar vírus, spyware e ameaças potenciais em mensagens de correio electrónico e anexos enviados e recebidos.
- **Protecção contra Correio Publicitário Não Solicitado** -- A protecção contra correio publicitário não solicitado ajuda a impedir a entrada de mensagens de correio electrónico na caixa de correio.
- **Protecção do IM** -- A protecção de mensagens instantâneas (IM) efectua pesquisas automáticas e tenta limpar vírus, spyware e potenciais ameaças nos anexos de mensagens instantâneas recebidas. Além disso, impede que clientes de mensagens instantâneas troquem conteúdo ou informações pessoais indesejadas através da Internet.
- **Protecção de Navegação Segura** -- Se estiver instalado, o plug-in do browser McAfee SiteAdvisor ajuda a protegê-lo de spyware, correio electrónico não solicitado, vírus e fraudes online, classificando os Web sites visitados ou que são apresentados nos resultados de procura da Web. Pode ver classificações de segurança pormenorizadas que indicam o resultado do teste de um site no que respeita a práticas de correio electrónico, transferências, afiliações online e aspectos incómodos, como janelas de contexto e cookies de registo de terceiros.

Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas

Se não existirem problemas em **Correio Electrónico e& Mensagens Instantâneas**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Correio Electrónico e Mensagens Instantâneas:

1. No painel Página Inicial, clique em **Correio Electrónico e& Mensagens Instantâneas**.
2. No painel da direita, clique em **Configurar**.

Noções sobre a protecção de limitação de acesso

A categoria de protecção Limitação de Acesso inclui o seguinte tipo de protecção:

- **Limitações de acesso** -- As limitações de acesso impedem que os utilizadores vejam conteúdo indesejado da Internet, bloqueando o acesso a Web sites potencialmente nocivos. É possível monitorizar e limitar a actividade e utilização da Internet.

Abra o painel de configuração Limitações de Acesso

Se não existirem problemas em **Limitações de Acesso**, pode abrir o painel de configuração no painel de informações.

Para abrir o painel de configuração Limitações de Acesso:

1. No painel Página Inicial, clique em **Limitações de Acesso**.
2. No painel da direita, clique em **Configurar**.

Resolução de problemas relacionados com protecção

A maioria dos problemas de protecção pode ser resolvida automaticamente. No entanto, se persistirem um ou mais problemas, deve resolvê-los manualmente.

Resolução automática de problemas de protecção

A maioria dos problemas de protecção pode ser resolvida automaticamente.

Para uma resolução automática de problemas de protecção:

- Clique em **Corrigir** junto ao estado de protecção.

Resolução manual de problemas de protecção

Se um ou mais problemas de protecção não forem resolvidos automaticamente, clique na ligação junto do problema para realizar a acção sugerida.

Para uma resolução manual de problemas de protecção:

- Efectue uma das seguintes acções:
  - Se não tiver efectuado uma pesquisa total do computador nos últimos 30 dias, clique em **Analisar** no lado esquerdo do estado de protecção principal para realizar uma pesquisa manual. (Esta opção é apresentada se o McAfee VirusScan estiver instalado.)
  - Se os ficheiros de assinatura de detecção (DAT) estiverem desactualizados, clique em **Actualizar** no lado esquerdo do estado de protecção geral para actualizar a protecção.
  - Se um programa não estiver instalado, clique em **Obter protecção total** para instalá-lo.
  - Se faltarem componentes no programa, reinstale-o.
  - Se for necessário registar um programa para receber protecção total, clique em **Registar agora** para o registar. (Esta opção é apresentada se um ou mais programas tiverem expirado.)
  - Se um programa tiver expirado, clique em **Verificar a minha subscrição agora** para ver o estado da conta. (Esta opção é apresentada se um ou mais programas tiverem expirado.)

Ver informações sobre o SecurityCenter

A opção Informações sobre o SecurityCenter, localizada na parte inferior do painel do estado de protecção, permite acesso a opções do SecurityCenter e mostra as mais recentes informações sobre actualizações, pesquisas (caso o McAfee VirusScan esteja instalado) e data de expiração da subscrição dos produtos McAfee.

Abra o painel de configuração SecurityCenter

Para sua comodidade, pode abrir o painel de configuração SecurityCenter para alterar as opções no painel Página Inicial.

Para abrir o painel de configuração SecurityCenter:

- No painel Página Inicial em **Informações sobre o SecurityCenter**, clique em **Configurar**.

Ver informações sobre os produtos instalados

Pode ver uma lista dos produtos instalados, onde é indicado o número da versão do produto e a data da última actualização.

Para ver as informações sobre o produto McAfee:

- No painel Página Inicial em **Informações sobre o SecurityCenter**, clique em **Ver Detalhes** para abrir a janela de informações sobre o produto.

Utilizar o Menu Avançado

Quando abre o SecurityCenter pela primeira vez, é apresentado o Menu Básico na coluna da esquerda. Se for um utilizador avançado, pode clicar em **Menu Avançado** para abrir um menu de comandos mais pormenorizado. Para sua comodidade, é apresentado o último menu que utilizou quando abrir novamente o SecurityCenter.

O Menu Avançado inclui as seguintes opções:

- Página inicial
- Relatórios e Registos (inclui a lista Eventos Recentes e registos por tipo relativos aos últimos 30, 60 e 90 dias)
- Configurar
- Restaurar
- Ferramentas

CAPÍTULO 4

Configurar as opções do SecurityCenter

O SecurityCenter mostra o estado geral de protecção do computador, permite-lhe criar contas de utilizador McAfee, instala automaticamente as mais recentes actualizações de produtos e notifica automaticamente o utilizador através de alertas e avisos sonoros de surtos de vírus públicos, ameaças de segurança e actualizações de produto.

No painel Configuração do SecurityCenter, pode alterar as opções do SecurityCenter para estas funções:

- Estado de protecção
- Utilizadores
- Actualizações automáticas
- Alertas

Neste capítulo

Configurar o estado de protecção 22
Configurar opções de utilizador 23
Configurar opções de actualização 26
Configurar opções de alerta 31

Configurar o estado de protecção

O estado de protecção de segurança geral do computador é indicado em **Estou protegido?** no SecurityCenter.

O estado de protecção informa-o se o computador está totalmente protegido contra as mais recentes ameaças de segurança ou se os problemas requerem atenção e mostra-lhe como resolver esses problemas.

Por predefinição, se as opções Protecção contra Correio Publicitário Não Solicitado ou Bloqueio de Conteúdos não estiverem instaladas, estes problemas de protecção não críticos serão automaticamente ignorados, não sendo registados no estado de protecção geral. No entanto, se for apresentada uma ligação **Ignorar** junto a um problema de protecção, pode ignorar o problema, caso tenha a certeza de que não quer resolvê-lo. Se decidir corrigir mais tarde um problema ignorado anteriormente, pode incluí-lo no estado de protecção para registo.

Configurar problemas ignorados

Pode incluir ou excluir o registo de problemas como parte do estado de protecção geral do computador. Se for apresentada uma ligação **Ignorar** junto a um problema de protecção, pode ignorar o problema, caso tenha a certeza de que não quer resolvê-lo. Se decidir corrigir mais tarde um problema ignorado anteriormente, pode incluí-lo no estado de protecção para registo.

Para configurar problemas ignorados:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Estado da Protecção** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Seleccione uma das seguintes opções no painel Problemas Ignorados:
   - Para incluir problemas ignorados anteriormente no estado da protecção, desmarque as respectivas caixas de verificação.
   - Para excluir problemas do estado da protecção, seleccione as respectivas caixas de verificação.
4. Clique em **OK**.

Configurar opções de utilizador

Se utilizar programas McAfee que requerem autorizações de utilizador, estas autorizações correspondem, por predefinição, às contas de utilizador do Windows no computador. Para facilitar a gestão destes programas pelos utilizadores, pode optar por utilizar as contas de utilizador McAfee em qualquer altura.

Se optar por utilizar contas de utilizador McAfee, quaisquer nomes de utilizador e autorizações existentes do programa Limitações de Acesso serão importados automaticamente. No entanto, quando mudar pela primeira vez, deve criar uma conta de administrador. Em seguida, pode criar e configurar outras contas de utilizador McAfee.

Mudar para contas de utilizador McAfee

Por predefinição, está a utilizar contas de utilizador do Windows. No entanto, se mudar para contas de utilizador da McAfee, já não é necessário criar contas adicionais do Windows.

Para mudar para contas de utilizador McAfee:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Utilizadores** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Para utilizar contas de utilizador McAfee, clique em **Mudar**.

Se mudar para contas de utilizador McAfee pela primeira vez, deve **criar uma conta de administrador** (página 23).

Criar uma conta de administrador

Quando muda pela primeira vez para utilizar utilizadores McAfee, é-lhe solicitado que crie uma conta de administrador.

Para criar uma conta de administrador:

1. Introduza uma palavra-passe na caixa **Palavra-passe** e introduza-a novamente na caixa **Confirmar Palavra-passe**.
2. Seleccione uma pergunta de recuperação de palavra-passe na lista e introduza a resposta à pergunta secreta na caixa **Resposta**.
3. Clique em **Aplicar**.

   Quando terminar, o tipo de conta de utilizador é actualizado no painel com os nomes de utilizador e autorizações existentes no programa Limitações de Acesso, caso existam. Quando configurar as contas de utilizador pela primeira vez, é apresentado o painel Gerir Utilizador.

Configurar opções de utilizador

Se optar por utilizar contas de utilizador McAfee, quaisquer nomes de utilizador e autorizações existentes do programa Limitações de Acesso são importados automaticamente. No entanto, quando mudar pela primeira vez, deve criar uma conta de administrador. Em seguida, pode criar e configurar outras contas de utilizador McAfee.

Para configurar opções de utilizador:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Utilizadores** para expandir o respectivo painel e, em seguida, clique em **Avançadas**.
3. Em **Contas de Utilizador**, clique em **Adicionar**.
4. Introduza um nome de utilizador na caixa **Nome de Utilizador**.
5. Introduza uma palavra-passe na caixa **Palavra-passe** e introduza-a novamente na caixa **Confirmar Palavra-passe**.
6. Seleccione a caixa de verificação **Utilizador de Arranque** se quiser que este novo utilizador inicie sessão automaticamente quando o SecurityCenter for iniciado.
7. Em **Tipo de Conta do Utilizador**, seleccione um tipo de conta para este utilizador e, em seguida, clique em **Criar**.

   Nota: Depois de criar a conta de utilizador, deve configurar as definições para um Utilizador Limitado em Limitações de Acesso.

8. Para editar a palavra-passe de um utilizador, início de sessão automático ou tipo de conta, seleccione um nome de utilizador na lista e clique em **Editar**.
9. Quando terminar, clique em **Aplicar**.

Obter a palavra-passe de administrador

Quando se esquecer da palavra-passe de administrador, pode obtê-la.

Para obter a palavra-passe de administrador:

1. Clique com o botão direito do rato no ícone M do SecurityCenter e depois clique em **Mudar de Utilizador**.
2. Na lista **Nome de Utilizador**, seleccione **Administrador** e clique em **Palavra-passe Esquecida**.
3. Introduza a resposta da pergunta secreta que seleccionou ao criar a conta de administrador.
4. Clique em **Submeter**.

   É apresentada a sua palavra-passe de administrador.

Alterar a palavra-passe de administrador

Se não se lembrar da palavra-passe de administrador ou se suspeitar que pode não ser seguro utilizá-la, pode alterá-la.

Para alterar a palavra-passe de administrador:

1. Clique com o botão direito do rato no ícone M do SecurityCenter e depois clique em **Mudar de Utilizador**.
2. Na lista **Nome de Utilizador**, seleccione **Administrador** e clique em **Alterar Palavra-passe**.
3. Introduza a palavra-passe existente na caixa **Palavra-passe Antiga**.
4. Introduza a nova palavra-passe na caixa **Palavra-passe** e introduza-a novamente na caixa **Confirmar Palavra-passe**.
5. Clique em **OK**.

Configurar opções de actualização

O SecurityCenter verifica automaticamente actualizações para todos os serviços McAfee de quatro em quatro horas quando se está ligado à Internet e depois instala automaticamente as mais recentes actualizações de produtos. No entanto, pode verificar manualmente em qualquer altura se existem actualizações, carregando no ícone do SecurityCenter na área de notificação, localizada na parte mais à direita da barra de tarefas.

Verificar actualizações automaticamente

O SecurityCenter verifica automaticamente se existem actualizações de quatro em quatro horas quando existe uma ligação à Internet. Contudo, pode configurar o SecurityCenter para notificá-lo antes de transferir ou instalar actualizações.

Para verificar actualizações automaticamente:

1. Em **Informações do SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto do estado **As actualizações automáticas estão activadas** para expandir o respectivo painel e, em seguida, clique em **Avançadas**.
3. Seleccione uma das seguintes opções no painel Opções de Actualização:
   - **Instalar as actualizações automaticamente e notificar quando o produto for actualizado (recomendado)** (página 27)
   - **Transferir as actualizações automaticamente e notificar quando estiverem prontas para serem instaladas** (página 28)
   - **Notificar antes de transferir quaisquer actualizações** (página 28)
4. Clique em **OK**.

Nota: Para uma máxima protecção, a McAfee recomenda que permita ao SecurityCenter procurar e instalar automaticamente as actualizações. No entanto, se pretende actualizar apenas manualmente os serviços de segurança, pode **desactivar a actualização automática** (página 29).

Transferir e instalar actualizações automaticamente

Se seleccionar **Instalar as actualizações automaticamente e notificar quando o produto for actualizado (recomendado)** nas Opções de Actualização do SecurityCenter, este transfere e instala automaticamente as actualizações.

Transferência automática de actualizações

Se seleccionar **Transferir as actualizações automaticamente e notificar quando estiverem prontas para serem instaladas** nas Opções de Actualização, o SecurityCenter transfere actualizações automaticamente e depois notifica-o quando estão prontas a instalar. Em seguida, pode instalar a actualização ou **adiá-la** (página 29).

Para instalar uma actualização transferida automaticamente:

1. Clique em **Actualizar os meus produtos agora** no alerta e depois clique em **OK**.

   Se solicitado, deve iniciar sessão no Web site para verificar a subscrição antes de efectuar a transferência.

2. Depois de verificar a subscrição, clique em **Actualizar** no painel Actualizações para transferir e instalar a actualização. Se a subscrição tiver expirado, clique em **Renovar a minha subscrição** no alerta e siga as indicações.

Nota: Nalguns casos, ser-lhe-á solicitado para reiniciar o computador de modo a concluir a actualização. Guarde o trabalho que estiver a fazer e feche todos os programas antes de reiniciar o computador.

Notificar antes de transferir actualizações

Se seleccionar **Notificar antes de transferir quaisquer actualizações** no painel Opções de Actualização, o SecurityCenter notifica-o antes de transferir quaisquer actualizações. Em seguida, pode transferir e instalar uma actualização para que os serviços de segurança possam eliminar a ameaça de ataque.

Para transferir e instalar uma actualização:

1. Seleccione **Actualizar os meus produtos agora** no alerta e depois clique em **OK**.

2. Se solicitado, inicie sessão no Web site.

   A actualização é transferida automaticamente.

3. Clique em **OK** no alerta quando a instalação da actualização estiver concluída.

Nota: Nalguns casos, ser-lhe-á solicitado para reiniciar o computador de modo a concluir a actualização. Guarde o trabalho que estiver a fazer e feche todos os programas antes de reiniciar o computador.

Desactivar a actualização automática

Para uma máxima protecção, a McAfee recomenda que permita o SecurityCenter procurar e instalar automaticamente as actualizações. No entanto, se pretende actualizar apenas manualmente os serviços de segurança, pode desactivar a actualização automática.

Nota: Deve **verificar manualmente as actualizações** (página 30) pelo menos uma vez por semana. Se não verificar as actualizações, isso significa que o computador não está protegido com as mais recentes actualizações de segurança.

Para desactivar a actualização automática:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto do estado **As actualizações automáticas estão activadas** para aumentar o painel.
3. Clique em **Desligado**.
4. Clique em **Sim** para confirmar a alteração.

   O estado é actualizado no cabeçalho.

Se não verificar manualmente as actualizações durante sete dias, é apresentado um alerta a indicar-lhe para verificá-las.

Adiar actualizações

Se estiver demasiado ocupado para actualizar os serviços de segurança quando aparecer o alerta, pode ser avisado mais tarde ou pode ignorar o alerta.

Para adiar uma actualização:

- Efectue uma das seguintes acções:
  - Seleccione **Lembrar-me mais tarde** no alerta e clique em **OK**.
  - Seleccione **Fechar este alerta** e clique em **OK** para fechar o alerta sem efectuar qualquer acção.

Verificar actualizações manualmente

O SecurityCenter verifica automaticamente actualizações de quatro em quatro horas quando se está ligado à Internet e depois instala as mais recentes actualizações de produtos. No entanto, pode verificar manualmente em qualquer altura se existem actualizações, utilizando o ícone do SecurityCenter na área de notificação do Windows na parte mais à direita da barra de tarefas.

Nota: Para uma máxima protecção, a McAfee recomenda que permita ao SecurityCenter procurar e instalar automaticamente as actualizações. No entanto, se pretende actualizar apenas manualmente os serviços de segurança, pode **desactivar a actualização automática** (página 29).

Para verificar actualizações manualmente:

1. Certifique-se de que o computador está ligado à Internet.
2. Clique com o botão direito do rato no ícone M do SecurityCenter na área de notificação do Windows, na parte mais à direita da barra de tarefas e, em seguida, clique em **Actualizações**.

   Embora o SecurityCenter verifique as actualizações, pode continuar a executar outras tarefas com a referida aplicação.

   Para sua comodidade, é apresentado um ícone animado na área de notificação do Windows, na parte mais à direita da barra de tarefas. Quando o SecurityCenter terminar, o ícone desaparece automaticamente.
3. Se solicitado, inicie sessão no Web site para verificar a subscrição.

Nota: Em alguns casos, ser-lhe-á solicitado que reinicie o computador de modo a concluir a actualização. Guarde o trabalho e feche todos os programas antes de reiniciar o computador.

Configurar opções de alerta

O SecurityCenter notifica-o automaticamente através de alertas e avisos sonoros para obter informações sobre surtos de vírus públicos, ameaças de segurança e actualizações de produtos. No entanto, pode configurar o SecurityCenter para apresentar apenas alertas que exijam a sua atenção imediata.

Configurar opções de alerta

O SecurityCenter notifica-o automaticamente através de alertas e avisos sonoros para obter informações sobre surtos de vírus públicos, ameaças de segurança e actualizações de produtos. No entanto, pode configurar o SecurityCenter para apresentar apenas alertas que exijam a sua atenção imediata.

Para configurar opções de alerta:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Alertas** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Seleccione uma das seguintes opções no painel Opções de Alerta:
   - **Alertar-me se ocorrer um surto de vírus público ou ameaças de segurança**
   - **Mostrar alertas informativos se for detectado um modo de jogo**
   - **Reproduzir um aviso sonoro se ocorrer um alerta**
   - **Mostrar o ecrã splash da McAfee no arranque do Windows**
4. Clique em **OK**.

Nota: Para desactivar futuros alertas informativos do respectivo alerta, seleccione a caixa de verificação **Não voltar a mostrar este alerta**. Pode activá-los de novo posteriormente no painel Alertas Informativos.

Configurar alertas informativos

Os alertas informativos notificam-no quando ocorrem eventos que não requerem a sua resposta imediata. Se desactivar futuros alertas informativos do próprio alerta, pode activá-los de novo posteriormente no painel Alertas Informativos.

Para configurar alertas informativos:

1. Em **Informações sobre o SecurityCenter**, clique em **Configurar**.
2. Clique na seta junto de **Alertas** para aumentar o respectivo painel e depois clique em **Avançadas**.
3. Em **Configuração do SecurityCenter**, clique em **Alertas Informativos**.
4. Desmarque a caixa de verificação **Ocultar alertas informativos** e depois desmarque as caixas de verificação dos alertas na lista que pretende mostrar.
5. Clique em **OK**.

CAPÍTULO 5

Efectuar tarefas comuns

Pode efectuar tarefas comuns, que incluem voltar ao painel Página inicial, ver eventos recentes, gerir a rede do computador (se estiver a trabalhar com um computador com capacidade de gestão para este tipo de rede) e efectuar a manutenção do computador. Se a opção Cópia de Segurança de Dados McAfee estiver instalada, pode também criar uma cópia de segurança dos dados.

Neste capítulo

Efectuar tarefas comuns 33
Ver eventos recentes 34
Manutenção automática do computador 35
Manutenção manual do computador 36
Gerir a sua rede 38
Obter mais informações sobre vírus.....38

Efectuar tarefas comuns

Pode efectuar tarefas comuns, que incluem voltar ao painel Página Inicial, ver eventos recentes, efectuar a manutenção do computador, gerir a rede do computador (se estiver ligada a um computador com capacidade de gestão para este tipo de rede) e criar cópias de segurança dos dados (se o software Cópia de Segurança de Dados McAfee estiver instalado).

Para efectuar tarefas comuns:

- Em **Tarefas Comuns** no Menu Básico, efectue uma das seguintes opções:
  - Para voltar ao painel Página Inicial, clique em **Página Inicial**.
  - Para ver eventos recentes detectados pelo software de segurança, clique em **Eventos Recentes**.
  - Para remover ficheiros não utilizados, desfragmente os dados e restaure o computador para as definições anteriores, clique em **Fazer Manutenção do Computador**.
  - Para efectuar a gestão da rede do computador, clique em **Gerir Rede** num computador com capacidade de gestão para esta rede.

    A opção Gestor de Rede monitoriza os computadores na rede no que respeita a falhas de segurança, para que possa facilmente identificar problemas de segurança na rede.

- Para criar cópias de segurança dos ficheiros, clique em **Cópia de Segurança de Dados** se o software Cópia de Segurança de Dados McAfee estiver instalado.

  A cópia de segurança automática guarda cópias dos ficheiros mais importantes num local à sua escolha, encriptando e armazenando os ficheiros num CD/DVD ou numa unidade USB, externa ou de rede.

Sugestão: Para sua comodidade, pode executar tarefas comuns a partir de dois locais adicionais (em **Página Inicial** no Menu Avançado e no menu **QuickLinks** do ícone M do SecurityCenter na parte mais à direita da barra de tarefas). Pode ver também eventos recentes e registos por tipo abrangentes em **Relatórios e Registos** no Menu Avançado.

Ver eventos recentes

Os eventos recentes são registados quando ocorrem alterações no computador. Isto verifica-se quando, por exemplo, um tipo de protecção é activado ou desactivado, quando uma ameaça é removida ou quando uma tentativa de ligação à Internet é bloqueada. Pode ver os 20 eventos mais recentes e os respectivos pormenores.

Consulte o ficheiro de ajuda do respectivo produto para obter informações detalhadas sobre os eventos.

Para ver eventos recentes:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Ver Eventos Recentes**.

   São apresentados na lista quaisquer eventos recentes, mostrando a data e uma descrição resumida.

2. Em **Eventos Recentes**, seleccione um evento para ver as informações adicionais no painel Detalhes.

   Em **Pretendo**, são apresentadas as acções disponíveis.

3. Para ver uma lista mais abrangente de eventos, clique em **Ver Registo**.

Manutenção automática do computador

Para libertar espaço em disco importante e optimizar o desempenho do computador, pode agendar as tarefas QuickClean ou Desfragmentador de Disco para intervalos regulares. Estas tarefas incluem eliminar, apagar e desfragmentar ficheiros e pastas.

Para efectuar uma manutenção automática do computador:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Fazer Manutenção do Computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.
3. Na lista de operações, seleccione **QuickClean** ou **Desfragmentador de Disco**.
4. Efectue uma das seguintes acções:
   - Para modificar uma tarefa existente, seleccione-a e depois clique em **Modificar**. Siga as instruções indicadas no ecrã.
   - Para criar uma nova tarefa, introduza o nome na caixa **Nome da Tarefa** e depois clique em **Criar**. Siga as instruções indicadas no ecrã.
   - Para eliminar uma tarefa, seleccione-a e depois clique em **Eliminar**.
5. Em **Resumo de Tarefas**, veja a data em que a tarefa foi executada pela última vez, a data da próxima execução e o respectivo estado.

Manutenção manual do computador

Pode efectuar tarefas de manutenção manual para remover ficheiros não utilizados, desfragmentar dados ou repor o computador para as definições anteriores.

Para efectuar uma manutenção manual do computador:

- Efectue uma das seguintes acções:
  - Para utilizar a opção QuickClean, clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks**, clique em **Fazer Manutenção do Computador** e depois clique em **Iniciar**.
  - Para utilizar a opção Desfragmentador de Disco, clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks**, clique em **Fazer Manutenção do Computador** e depois clique em **Analisar**.
  - Para utilizar a opção Restauro do Sistema, no Menu Avançado clique em **Ferramentas**, clique em **Restauro do Sistema** e depois clique em **Iniciar**.

Remover ficheiros e pastas não utilizados

Utilize a opção QuickClean para disponibilizar espaço em disco importante e optimizar o desempenho do computador.

Para remover ficheiros e pastas não utilizados:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e, em seguida, clique em **Fazer Manutenção do Computador**.
2. Em **QuickClean**, clique em **Iniciar**.
3. Siga as instruções indicadas no ecrã.

Desfragmentar ficheiros e pastas

A fragmentação de ficheiros ocorre quando os ficheiros e pastas são eliminados e são adicionados novos ficheiros. Esta fragmentação reduz o acesso ao disco e resulta numa deterioração geral do desempenho do computador, embora não seja normalmente grave.

Utilize a desfragmentação para gravar novamente partes de um ficheiro em sectores contíguos num disco rígido, de modo a aumentar a velocidade de acesso e obtenção.

Para desfragmentar ficheiros e pastas:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Fazer Manutenção do Computador**.
2. Em **Desfragmentador de Disco**, clique em **Analisar**.
3. Siga as instruções indicadas no ecrã.

Restaurar o computador para as definições anteriores

Os pontos de restauro são instantâneos do computador guardados periodicamente pelo Windows e quando ocorrem eventos significativos (por exemplo, durante a instalação de um programa ou controlador). No entanto, pode criar e atribuir um nome aos seus pontos de restauro em qualquer altura.

Utilize os pontos de restauro para resolver alterações nocivas no computador e voltar às definições anteriores.

Para restaurar o computador para as definições anteriores:

1. No Menu Avançado, clique em **Ferramentas** e depois clique em **Restauro do Sistema**.
2. Em **Restauro do Sistema**, clique em **Iniciar**.
3. Siga as instruções indicadas no ecrã.

Gerir a sua rede

Se o computador dispuser de capacidade de gestão de rede, pode utilizar o Gestor de Rede para monitorizar computadores na rede no que respeita a falhas de segurança, para que possa identificar facilmente problemas de segurança.

Se o estado de protecção do computador não estiver a ser monitorizado nesta rede, isso significa que o computador não faz parte desta rede ou não está a ser gerido nesta rede. Para obter informações detalhadas, consulte o ficheiro de ajuda do Gestor de Rede.

Para gerir a sua rede:

1. Clique com o botão direito do rato no ícone principal do SecurityCenter, vá para **QuickLinks** e depois clique em **Gerir Rede**.
2. Clique no ícone que representa este computador no mapa de rede.
3. Em **Pretendo**, clique em **Monitorizar este computador**.

Obter mais informações sobre vírus

Utilize a Virus Information Library e o Virus Map para:

- Obter mais informações sobre os mais recentes vírus, logros de vírus por correio electrónico e outras ameaças.
- Obter ferramentas gratuitas de remoção de vírus para ajudar a reparar o computador.
- Obter uma visão de conjunto, em tempo real, do local onde os computadores mais recentes estão a infectar computadores a nível mundial.

Para obter mais informações sobre vírus:

1. No Menu Avançado, clique em **Ferramentas** e depois em **Informações sobre Vírus**.
2. Efectue uma das seguintes acções:
   - Efectue uma procura de vírus com o Virus Information Library gratuito da MacAfee.
   - Efectue uma procura de vírus com o World Virus Map no Web site da McAfee.

CAPÍTULO 6

McAfee QuickClean

Quando se navega na Internet, acumula-se rapidamente muito lixo no computador. Proteja a sua privacidade e elimine o correio electrónico indesejado, bem como os ficheiros da Internet de que já não precisa através do QuickClean. O QuickClean identifica e elimina os ficheiros que se acumulam enquanto utiliza a Internet, incluindo cookies, correio electrónico, conteúdos transferidos, ficheiros de histórico (dados que contêm informações pessoais). Protege a sua privacidade, proporcionando uma eliminação segura desta informação confidencial.

O QuickClean elimina também programas indesejados. Poderá especificar os ficheiros que pretende eliminar e destruir os ficheiros indesejados sem eliminar informações essenciais.

Neste capítulo

Noções básicas sobre as funcionalidades do QuickClean 40
Limpar o computador.....41

Noções básicas sobre as funcionalidades do QuickClean

Esta secção descreve as funcionalidades do QuickClean.

Funcionalidades

O QuickClean disponibiliza um conjunto de ferramentas eficientes e de fácil utilização para eliminar o lixo digital de uma forma segura. Pode libertar espaço em disco valioso e optimizar o desempenho do computador.

CAPÍTULO 7

Limpar o computador

O QuickClean permite-lhe eliminar ficheiros e pastas com segurança.

Quando navega na Internet, o browser copia cada página da Internet e respectivos gráficos para uma pasta de cache no disco. O browser pode assim carregar rapidamente a página se voltar novamente a essa página. Os ficheiros de cache são úteis se visitar constantemente as mesmas páginas da Internet e o seu conteúdo não mudar com frequência. Na maior parte dos casos, no entanto, os ficheiros de cache não são úteis e podem ser eliminados.

É possível eliminar vários itens com as seguintes funções de limpeza.

- Limpeza da Reciclagem: Limpa a reciclagem do Windows.
- Limpeza de Ficheiros Temporários: Elimina os ficheiros armazenados em pastas temporárias.
- Limpeza de Atalhos: Elimina atalhos quebrados e atalhos sem um programa associado.
- Limpeza de Fragmentos Perdidos de Ficheiros: Elimina fragmentos perdidos de ficheiros do computador.
- Limpeza do Registo: Elimina informações de registo do Windows relativas a programas que já não existem no computador.
- Limpeza da Cache: Elimina ficheiros de cache que se vão acumulando quando navega na Internet. Os ficheiros deste tipo são normalmente guardados como ficheiros temporários da Internet.
- Limpeza de Cookies: Elimina cookies. Os ficheiros deste tipo são normalmente guardados como ficheiros temporários da Internet.
  Os cookies são pequenos ficheiros que o Web browser guarda no computador a pedido de um servidor Web. Sempre que consulta uma página Web a partir do servidor Web, o browser envia o cookie para o servidor. Estes cookies podem funcionar como um código, que permite ao servidor Web registar as páginas que visita e a frequência com que as visita.
- Limpeza do Histórico do Browser: Elimina o histórico do browser.
- Limpeza de mensagens das pastas 'Itens enviados' e 'Itens eliminados' do Correio Electrónico do Outlook Express e do Outlook: Elimina as mensagens de correio electrónico das pastas 'Itens enviados' e 'Itens eliminados' do Outlook.

- Limpeza de Ficheiros Utilizados Recentemente: Elimina os itens recentemente utilizados que se encontram guardados no computador, como os documentos do Microsoft Office.
- Limpeza de ActiveX e Plug-in: Elimina controlos e extensões ActiveX.
  ActiveX é uma tecnologia utilizada para implementar controlos num programa. Um controlo ActiveX permite adicionar um botão à interface de um programa. A maioria destes controlos são inofensivos; no entanto, algumas pessoas podem utilizar a tecnologia ActiveX para capturar informações do computador.
  Extensões são pequenos programas de software que estabelecem ligação com aplicações mais abrangentes, com vista a proporcionar uma maior funcionalidade. As extensões permitem que o Web browser aceda a e execute ficheiros incorporados em documentos HTML em formatos que o browser normalmente não reconheceria (por exemplo, ficheiros de animação, vídeo e áudio).
- Limpeza de Pontos de Restauro do Sistema: Elimina do computador pontos de restauro do sistema antigos.

Neste capítulo

Utilizar o QuickClean 43

Utilizar o QuickClean

Esta secção descreve como utilizar o QuickClean.

Limpar o computador

Pode eliminar ficheiros e pastas não utilizados, libertar espaço em disco e tornar o computador mais eficiente.

Para limpar o computador:

1. No menu Avançado, clique em **Ferramentas**.
2. Clique em **Fazer Manutenção do Computador** e, em seguida, seleccione **Iniciar** em **McAfee QuickClean**.
3. Efectue um dos seguintes procedimentos:
   - Clique em **Seguinte** para aceitar as limpezas predefinidas na lista.
   - Seleccione ou desmarque as limpezas que considerar adequadas e, em seguida, clique em **Seguinte.** Para a Limpeza de Ficheiros Utilizados Recentemente, pode clicar em **Propriedades** para desmarcar os programas cujas listas não deseja limpar.
   - Clique em **Restaurar Predefinições** para repor as limpezas predefinidas e, em seguida, clique em **Seguinte.**
4. Depois de efectuada a análise, clique em **Seguinte** para confirmar a eliminação dos ficheiros. Pode expandir esta lista para ver os ficheiros que serão limpos e a sua localização.
5. Clique em **Seguinte**.
6. Efectue um dos seguintes procedimentos:
   - Clique em **Seguinte** para aceitar a opção predefinida **Não, quero eliminar os ficheiros utilizando o método padrão de eliminação do Windows**.
   - Clique em **Sim, pretendo apagar os ficheiros com segurança utilizando o Shredder** e especifique o número de passagens. Os ficheiros eliminados com o Shredder não podem ser recuperados.
7. Clique em **Concluir**.
8. Em **Resumo do QuickClean**, visualize o número de ficheiros de registo que foram eliminados e a quantidade de espaço em disco recuperada após a limpeza do disco e da Internet.

CAPÍTULO 8

McAfee Shredder

Os ficheiros eliminados podem ser recuperados a partir do computador mesmo depois de esvaziar a Reciclagem. Quando elimina um ficheiro, o Windows marca esse espaço na unidade de disco para indicar que já não está a ser utilizado, mas o ficheiro continua presente. Com ferramentas de peritagem informática, pode recuperar registos de impostos, currículos ou outros documentos que tenha eliminado. O Shredder protege a sua privacidade eliminando os ficheiros indesejados de forma segura e permanente.

Para eliminar um ficheiro de forma permanente, é necessário substituir várias vezes o ficheiro existente por novos dados. O Microsoft® Windows não elimina ficheiros com segurança, porque cada operação de ficheiro seria muito lenta. A destruição de um documento nem sempre impede que o documento seja recuperado, pois alguns programas fazem cópias ocultas temporárias de documentos abertos. Se destruir apenas os documentos apresentados no Explorador do Windows®, é possível que ainda tenha cópias temporárias desses documentos.

Nota: Não é efectuada cópia de segurança dos ficheiros destruídos. Não é possível recuperar ficheiros eliminados pelo Shredder.

Neste capítulo

Noções básicas das funcionalidades do Shredder....46
Apagar ficheiros indesejados com o Shredder.....47

Noções básicas das funcionalidades do Shredder

Esta secção descreve as funcionalidades do Shredder.

Funcionalidades

O Shredder permite apagar o conteúdo da Reciclagem, os ficheiros temporários da Internet, o histórico dos Web sites, ficheiros, pastas e discos.

CAPÍTULO 9

Apagar ficheiros indesejados com o Shredder

O Shredder protege a sua privacidade, eliminando, de forma segura e permanente, ficheiros indesejados, tais como o conteúdo da Reciclagem, os ficheiros temporários da Internet e o histórico dos Web sites. Pode seleccionar ou procurar os ficheiros e as pastas que pretende destruir.

Neste capítulo

Utilizar o Shredder 48

Utilizar o Shredder

Esta secção descreve como utilizar o Shredder.

Destruir ficheiros, pastas e discos

Os ficheiros podem permanecer no computador, mesmo depois de esvaziar a Reciclagem. No entanto, quando destrói ficheiros, os dados são eliminados de forma permanente e os hackers não conseguem aceder aos mesmos.

Para destruir ficheiros, pastas e discos:

1. No menu Avançado, clique em **Ferramentas** e, em seguida, clique em **Shredder**.
2. Efectue um dos seguintes procedimentos:
   - Clique em **Apagar ficheiros e pastas** para destruir ficheiros e pastas.
   - Clique em **Apagar um disco inteiro** para destruir discos**.**
3. Seleccione um dos seguintes níveis de destruição:
   - **Rápido**: Destrói os itens seleccionados uma vez.
   - **Abrangente**: Destrói os itens seleccionados 7 vezes.
   - **Personalizar**: Destrói os itens seleccionados até 10 vezes. Um número maior de passagens de destruição aumenta o nível de eliminação segura dos ficheiros.
4. Clique em **Seguinte**.
5. Efectue um dos seguintes procedimentos:
   - Para destruir ficheiros, clique em **Conteúdo da Reciclagem**, **Ficheiros temporários da Internet** ou **Histórico dos Web sites** na lista **Seleccionar os ficheiros a destruir**. Para destruir um disco, clique no disco.
   - Clique em **Procurar**, procure os ficheiros que pretende destruir e seleccione-os.
   - Escreva o caminho para os ficheiros que pretende destruir na lista **Seleccionar os ficheiros a destruir**.
6. Clique em **Seguinte**.
7. Clique em **Terminar** para concluir a operação.
8. Clique em **Concluído**.

CAPÍTULO 10

McAfee Network Manager

O McAfee® Network Manager apresenta uma vista gráfica dos computadores e componentes que compõem a sua rede doméstica. Pode utilizar o Network Manager para monitorizar, de forma remota, o estado de protecção de cada computador gerido na sua rede e corrigir remotamente vulnerabilidades de segurança comunicadas nesses computadores geridos.

Antes de começar a utilizar o Network Manager, pode familiarizar-se com algumas das funcionalidades mais populares. A ajuda do Network Manager inclui detalhes sobre configuração e utilização destas funcionalidades.

Neste capítulo

Funcionalidades 50
Noções básicas sobre os ícones do Network Manager 51
Configurar uma rede gerida 53
Gerir a rede de forma remota 61

Funcionalidades

O Network Manager oferece as seguintes funcionalidades:

Mapeamento de rede gráfico

O mapeamento de rede do Network Manager proporciona uma visão gráfica global do estado de segurança dos computadores e componentes que compõem a sua rede doméstica. Quando altera a rede (por exemplo, adicionando um computador), o mapeamento de rede reconhece essas alterações. Pode actualizar o mapeamento de rede, mudar o nome da rede e mostrar ou ocultar componentes do mapeamento de rede, para personalizar a visualização. Pode também ver as informações associadas aos componentes apresentados no mapeamento de rede.

Gestão remota

Utilize o mapeamento de rede do Network Manager para gerir o estado de segurança dos computadores que fazem parte da sua rede doméstica. Pode convidar um computador a aderir à rede gerida, monitorizar o estado de protecção do computador gerido e resolver problemas de vulnerabilidade de segurança detectados a partir de um computador remoto da rede.

Noções básicas sobre os ícones do Network Manager

A tabela seguinte descreve os ícones normalmente utilizados no mapeamento de rede do Network Manager.

Ícone	Descrição
	Representa um computador gerido e online
	Representa um computador gerido e offline
	Representa um computador não gerido com o software de segurança McAfee 2007 instalado
	Representa um computador não gerido e offline
	Representa um computador online que não tem o software de segurança McAfee 2007 instalado nem um dispositivo de rede desconhecido
	Representa um computador offline que não tem o software de segurança McAfee 2007 instalado nem um dispositivo de rede desconhecido offline
	Significa que o item correspondente está protegido e ligado
	Significa que o item correspondente requer a sua atenção
	Significa que o item correspondente requer a sua atenção e está desligado
	Representa um router de raiz sem fios
	Representa um router de raiz padrão
	Representa a Internet, quando está ligada
	Representa a Internet, quando está desligada

CAPÍTULO 11

Configurar uma rede gerida

Configurou uma rede gerida, utilizando os itens no mapeamento de rede e adicionando membros (computadores) à rede.

Neste capítulo

Utilizar o mapeamento de rede 54
Aderir à rede gerida.....57

Utilizar o mapeamento de rede

Sempre que liga um computador à rede, o Network Manager analisa o estado da rede para determinar se existem membros (geridos ou não geridos), atributos de router e o estado da Internet. Se não forem encontrados membros, o Network Manager presume que o computador actualmente ligado é o primeiro computador na rede e torna-o automaticamente um membro gerido com permissões de administração. Por predefinição, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador que é ligado à rede com o software de segurança McAfee 2007 instalado; no entanto, é possível mudar o nome da rede a qualquer momento.

Se efectuar alterações na rede (por exemplo, adicionar um computador), pode personalizar o mapeamento de rede. Por exemplo, pode actualizar o mapeamento de rede, mudar o nome da rede, bem como mostrar ou ocultar componentes do mapeamento de rede para personalizar a sua vista. Pode também ver as informações associadas aos componentes apresentados no mapeamento de rede.

Aceder ao mapeamento de rede

Pode aceder ao mapa da sua rede, iniciando o Network Manager a partir da lista de tarefas comuns do SecurityCenter. O mapeamento de rede mostra uma representação gráfica dos computadores e componentes que compõem a sua rede doméstica.

Para aceder ao mapeamento de rede:

- No menu Básico ou Avançado, clique em **Gerir Rede**.
  O mapeamento de rede é apresentado no painel da direita.

Nota: A primeira vez que acede ao mapeamento de rede, é-lhe solicitado que confie nos outros computadores da rede antes de o mapeamento de rede ser apresentado.

Actualizar o mapeamento de rede

Pode actualizar o mapeamento de rede em qualquer altura; por exemplo, depois de adicionar outro computador à rede gerida.

Para actualizar o mapeamento de rede:

1. No menu Básico ou Avançado, clique em **Gerir Rede**.
   O mapeamento de rede é apresentado no painel da direita.
2. Clique em **Actualizar o mapeamento de rede** em **Quero**.

Nota: A lista **Actualizar o mapeamento de rede** só está disponível se não estiverem seleccionados itens no mapeamento de rede. Para desmarcar um item, clique no item seleccionado ou numa área em branco no mapeamento de rede.

Mudar o nome da rede

Por predefinição, o nome da rede inclui o nome do grupo de trabalho ou do domínio do primeiro computador que é ligado à rede com o software de segurança McAfee 2007 instalado. Se o nome não for adequado, pode alterá-lo.

Para mudar o nome da rede:

1. No menu Básico ou Avançado, clique em **Gerir Rede**.
   O mapeamento de rede é apresentado no painel da direita.
2. Clique em **Mudar o nome da rede** em **Quero**.
3. Introduza o nome da rede na caixa **Mudar o nome da rede**.
4. Clique em **OK**.

Nota: A ligação **Mudar o nome da rede** só está disponível se não estiverem seleccionados itens no mapeamento de rede. Para desmarcar um item, clique no item seleccionado ou numa área em branco no mapeamento de rede.

Mostrar ou ocultar itens no mapeamento de rede

Por predefinição, todos os computadores e componentes na sua rede doméstica são apresentados no mapeamento de rede. No entanto, se tiver itens ocultos, pode mostrá-los novamente em qualquer altura. Só é possível ocultar os itens não geridos; os computadores geridos não podem ser ocultos.

Para...	No menu Básico ou Avançado, clique em **Gerir Rede** e efectue o seguinte...
Ocultar um item no mapeamento de rede	Clique num item no mapeamento de rede e, em seguida, clique em **Ocultar este item** em **Quero**. Na caixa de diálogo de confirmação, clique em **Sim**.
Mostrar itens ocultos no mapeamento de rede	Em **Quero**, clique em **Mostrar itens ocultos**.

Ver detalhes do item

Pode ver informações detalhadas sobre qualquer componente na sua rede, seleccionando o componente no mapeamento de rede. Estas informações incluem o nome do componente, o respectivo estado de protecção e outras informações necessárias para gerir o componente.

Para ver os detalhes de um item:

1. Clique no ícone de um item no mapeamento de rede.
2. Em **Detalhes**, visualize a informação sobre o item.

Aderir à rede gerida

Antes de um computador poder ser gerido remotamente ou ser-lhe concedida permissão para gerir, de forma remota, outros computadores na rede, deve tornar-se um membro de confiança da rede. A confirmação de membro da rede é concedida a novos computadores através de membros de rede existentes (computadores) com permissões de administração. Para garantir que aderem apenas computadores de confiança à rede, os utilizadores dos computadores de concessão e adesão devem autenticar-se entre si.

Se um computador aderir à rede, ser-lhe-á solicitado para expor o respectivo estado de protecção McAfee a outros computadores na rede. Se um computador aceitar expor o respectivo estado de protecção, torna-se um membro *gerido* da rede. Se um computador recusar expor o respectivo estado de protecção, torna-se um membro *não gerido* da rede. Os membros não geridos da rede são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, partilha de ficheiros ou impressoras).

Nota: Depois de aderir, se tiver outros programas de rede da McAfee instalados (por exemplo, o McAfee Wireless Network Security ou o EasyNetwork), o computador é igualmente reconhecido como um computador gerido nesses programas. O nível de permissão atribuído a um computador no Network Manager aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o significado das permissões de convidado, de acesso total ou administrativo noutros programas de rede da McAfee, consulte a documentação fornecida com o respectivo programa.

Aderir a uma rede gerida

Se receber um convite para aderir a uma rede gerida, pode aceitá-lo ou recusá-lo. Pode também determinar se pretende que este computador e outros computadores na rede monitorizem as definições de segurança de cada um (por exemplo, se os serviços de protecção antivírus de um computador estão actualizados).

Para aderir a uma rede gerida:

1. Na caixa de diálogo de convite, active a caixa de verificação **Permitir que este e outros computadores da rede monitorizem as definições de segurança de cada um** para permitir que outros computadores na rede gerida monitorizem as definições de segurança do seu computador.
2. Clique em **Aderir**.
   Se aceitar o convite, são apresentadas duas cartas de jogar.
3. Confirme se essas cartas de jogar são iguais às apresentadas no computador que o convidou para aderir à rede gerida.
4. Clique em **Confirmar**.

Nota: Se o computador que o convidou para aderir à rede gerida não apresentar as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. A adesão à rede pode colocar o computador em perigo; por conseguinte, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Convidar um computador para aderir à rede gerida

Se um computador for adicionado à rede gerida ou existir outro computador não gerido na rede, pode convidar esse computador para aderir à rede gerida. Apenas os computadores com permissões de administração na rede podem convidar outros computadores para aderir à rede. Se enviar o convite, pode também especificar o nível de permissão que pretende atribuir ao computador aderente.

Para convidar um computador para aderir à rede gerida:

1. Clique no ícone de um computador não gerido no mapeamento de rede.
2. Clique em **Monitorizar este computador** em **Quero**.
3. Na caixa de diálogo Convidar um computador a aderir a esta rede gerida, clique numa das seguintes opções:
   - **Conceder acesso de convidado**
     O acesso de convidado permite ao computador ter acesso à rede.

- **Conceder acesso total a todas as aplicações de rede geridas**
  Acesso total (tal como o acesso de convidado) permite o acesso do computador à rede.
- **Conceder acesso administrativo a todas as aplicações de rede geridas**
  O acesso administrativo permite ao computador aceder à rede com permissões de administração. Permite também ao computador conceder acesso a outros computadores que pretendam aderir à rede gerida.

4 Clique em **Convidar**.
É enviado ao computador um convite para aderir à rede gerida. Se o computador aceitar o convite, são apresentadas duas cartas de jogar.

5 Confirme se essas cartas de jogar são iguais às apresentadas no computador que convidou para aderir à rede gerida.

6 Clique em **Conceder Acesso**.

Nota: Se o computador que convidou para aderir à rede gerida não apresentar as mesmas cartas de jogar apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. Permitir a adesão de um computador à rede pode colocar outros computadores em risco; por conseguinte, clique em **Rejeitar Acesso** na caixa de diálogo de confirmação de segurança.

Parar de confiar nos computadores da rede

Se, por engano, concordar em confiar noutros computadores na rede, pode parar essa acção.

Para parar de confiar em computadores na rede:

- Clique em **Parar de confiar em computadores nesta rede** em **Quero**.

Nota: A ligação **Parar de confiar em computadores nesta rede** só está disponível se outros computadores geridos não tiverem aderido à rede.

CAPÍTULO 12

Gerir a rede de forma remota

Depois de configurar a rede gerida, pode utilizar o Network Manager para gerir remotamente os computadores e componentes que compõem a sua rede. Pode monitorizar o estado e os níveis de permissão dos computadores e componentes e corrigir vulnerabilidades de segurança de forma remota.

Neste capítulo

Monitorizar o estado e as permissões 62
Corrigir vulnerabilidades de segurança.....65

Monitorizar o estado e as permissões

Uma rede gerida dispõe de dois tipos de membros: membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede monitorizem o respectivo estado de protecção McAfee; os membros não geridos não o permitem. Os membros não geridos são normalmente computadores convidados que pretendem aceder a outras funções de rede (por exemplo, partilha de ficheiros ou impressoras). Como computador não gerido, pode ser convidado a tornar-se um computador gerido em qualquer altura por outro computador gerido na rede. Do mesmo modo, um computador gerido pode tornar-se não gerido em qualquer altura.

Os computadores geridos têm permissões de administração, total ou de convidado associadas aos mesmos. As permissões de administração permitem ao computador gerido administrar o estado de protecção de todos os outros computadores geridos na rede e conceder aos computadores inscritos acesso à rede. As permissões de convidado e acesso total permitem que um computador aceda apenas à rede. Pode modificar o nível de permissão de um computador em qualquer altura.

Uma vez que a rede gerida é composta igualmente por dispositivos (por exemplo, routers), pode utilizar o Network Manager para geri-los também. Pode também configurar e modificar as propriedades de visualização de um dispositivo no mapeamento de rede.

Monitorizar o estado de protecção de um computador

Se o estado de protecção de um computador não estiver a ser monitorizado na rede (quer seja pelo facto do computador não ser um membro da rede ou pelo facto do computador ser um membro não gerido da rede), pode efectuar um pedido para monitorizá-lo.

Para monitorizar o estado de protecção de um computador:

1. Clique no ícone de um computador não gerido no mapeamento de rede.
2. Clique em **Monitorizar este computador** em **Quero**.

Parar de monitorizar o estado de protecção de um computador

Pode parar de monitorizar o estado de protecção de um computador gerido na sua rede privada. Em seguida, o computador torna-se um computador não gerido.

Para parar de monitorizar o estado de protecção de um computador:

1. Clique no ícone de um computador gerido no mapeamento de rede.
2. Clique em **Parar de monitorizar este computador** em **Quero**.
3. Na caixa de diálogo de confirmação, clique em **Sim**.

Modificar as permissões de um computador gerido

Pode modificar as permissões de um computador gerido em qualquer altura. Isto permite-lhe ajustar os computadores que podem monitorizar o estado de protecção (definições de segurança) de outros computadores na rede.

Para modificar as permissões de um computador gerido:

1. Clique no ícone de um computador gerido no mapeamento de rede.
2. Clique em **Modificar as permissões deste computador** em **Quero**.
3. Na caixa de diálogo para modificar as permissões, seleccione ou desmarque a caixa de verificação para determinar se este e outros computadores na rede gerida podem monitorizar o estado de protecção de cada um.
4. Clique em **OK**.

Gerir um dispositivo

Pode gerir um dispositivo, acedendo à respectiva página Web de administração a partir do Network Manager.

Para gerir um dispositivo:

1. Clique no ícone de um dispositivo no mapeamento de rede.
2. Clique em **Gerir este dispositivo** em **Quero**.
   É aberto um Web browser e aparece a página Web de administração do dispositivo.
3. No Web browser, introduza as informações de início de sessão e configure as definições de segurança do dispositivo.

Nota: Se o dispositivo for um router ou um ponto de acesso sem fios protegido pelo Wireless Network Security, deve utilizar o Wireless Network Security para configurar as definições de segurança do dispositivo.

Modificar as propriedades de visualização de um dispositivo

Se modificar as propriedades de visualização de um dispositivo, pode também alterar o nome de visualização do dispositivo no mapeamento de rede e especificar se o dispositivo é um router sem fios.

Para modificar as propriedades de visualização de um dispositivo:

1. Clique no ícone de um dispositivo no mapeamento de rede.
2. Clique em **Modificar as propriedades do dispositivo** em **Quero**.
3. Para especificar o nome de visualização do dispositivo, introduza um nome na caixa **Nome**.
4. Para especificar o tipo de dispositivo, clique numa das seguintes opções:
   - **Router**
     Isto representa um router de raiz padrão.
   - **Router sem fios**
     Isto representa um router de raiz sem fios.
5. Clique em **OK**.

Corrigir vulnerabilidades de segurança

Os computadores geridos com permissões de administração podem monitorizar o estado de protecção McAfee de outros computadores geridos na rede e corrigir remotamente quaisquer vulnerabilidades de segurança. Por exemplo, se o estado de protecção McAfee de um computador gerido indicar que o VirusScan está desactivado, outro computador gerido com permissões de administração pode *corrigir* esta vulnerabilidade de segurança, activando o VirusScan remotamente.

Se corrigir vulnerabilidades de segurança remotamente, o Network Manager repara automaticamente a maioria dos problemas comunicados. No entanto, algumas vulnerabilidades de segurança podem requerer intervenção manual no computador local. Neste caso, o Network Manager corrige esses problemas que podem ser reparados remotamente e depois pede-lhe para corrigir os problemas restantes, iniciando sessão no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Nalguns casos, a correcção sugerida é instalar o software de segurança McAfee 2007 no(s) computador(es) remoto(s) na sua rede.

Corrigir vulnerabilidades de segurança

Pode utilizar o Network Manager para corrigir automaticamente a maior parte das vulnerabilidades de segurança de computadores remotos geridos. Por exemplo, se o VirusScan estiver desactivado num computador remoto, pode utilizar o Network Manager para activá-lo automaticamente.

Para corrigir vulnerabilidades de segurança:

1. Clique no ícone de um item no mapeamento de rede.
2. Veja o estado de protecção do item em **Detalhes**.
3. Clique em **Corrigir vulnerabilidades de segurança** em **Quero**.
4. Quando os problemas tiverem sido corrigidos, clique em **OK**.

Nota: Embora o Network Manager corrija automaticamente a maioria das vulnerabilidades de segurança, algumas correcções podem exigir que inicie o SecurityCenter no computador vulnerável e siga as recomendações fornecidas.

Instalar o software de segurança McAfee em computadores remotos

Se um ou mais computadores na sua rede não utilizarem o software de segurança McAfee 2007, o estado de segurança não pode ser monitorizado remotamente. Se pretender monitorizar estes computadores remotamente, deve aceder a cada computador e instalar o software de segurança McAfee 2007.

Para instalar o software de segurança McAfee num computador remoto:

1. Num browser do computador remoto, vá para http://download.mcafee.com/us/.
2. Siga as instruções no ecrã para instalar o software de segurança McAfee 2007 no computador.

CAPÍTULO 13

McAfee Wireless Network Security

O Wireless Network Security proporciona uma protecção padrão e automática contra furto de dados, acesso não autorizado à rede e utilização não autorizada da largura de banda através de uma interface simples, intuitiva e de fácil utilização. O Wireless Network Security encripta os dados pessoais e privados à medida que são enviados na rede Wi-Fi e impede que os hackers acedam à rede sem fios.

O Wireless Network Security bloqueia ataques de hackers à rede sem fios:

- Evitando ligações não autorizadas à rede Wi-Fi
- Evitando a captura de dados transmitidos através de uma rede Wi-Fi
- Detectando tentativas de ligação a uma rede Wi-Fi

O Wireless Network Security combina funcionalidades fáceis de utilizar, tais como o bloqueio instantâneo da rede e a capacidade para adicionar rapidamente utilizadores legítimos à rede, com funcionalidades de segurança robustas como, por exemplo, geração automática de chaves encriptadas e rotação de chaves agendada.

Neste capítulo

Funcionalidades 68
Iniciar o Wireless Network Security 70
Proteger redes sem fios 73
Administrar redes sem fios 91
Gerir segurança da rede sem fios 103
Monitorizar redes sem fios 119

Funcionalidades

O Wireless Network Security oferece as seguintes funcionalidades:

Protecção contínua

O Wireless Network Security detecta e protege automaticamente qualquer rede sem fios vulnerável com a qual estabeleça ligação.

Interface intuitiva

Protege a sua rede sem ter de tomar decisões difíceis nem ter de conhecer termos técnicos complicados.

Encriptação automática forte

Permite que apenas os seus amigos e familiares tenham acesso à rede, protegendo os seus dados durante as transmissões.

Solução baseada apenas em software

O Wireless Network Security trabalha com o seu router ou ponto de acesso sem fios e com o seu software de segurança padrão. Não necessita de adquirir hardware adicional.

Rotação automática da chave

Até mesmo os hackers mais determinados não conseguem capturar as suas informações, porque a chave está em rotação constante.

Adição de utilizadores à rede

Pode facilmente conceder acesso à rede a familiares e amigos. Pode adicionar utilizadores através de um sistema sem fios ou transferindo software através de uma unidade USB.

Ferramenta de ligação intuitiva

A ferramenta de ligação sem fios é intuitiva e informativa, fornecendo detalhes sobre a potência do sinal e o estado da segurança.

Registo de eventos e alertas

Os relatórios e alertas de fácil compreensão proporcionam aos utilizadores avançados mais informações sobre a rede sem fios.

Modo de suspensão

Suspende temporariamente a rotação da chave, para permitir que aplicações específicas funcionem sem interrupções.

Compatibilidade com outros equipamentos

O Wireless Network Security actualiza-se automaticamente com os mais recentes módulos de routers ou pontos de acesso sem fios das marcas mais populares, incluindo: Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet® e outras.

Iniciar o Wireless Network Security

Após a instalação, o Wireless Network Security é automaticamente activado; não é necessário iniciá-lo manualmente. No entanto, pode também activar e desactivar manualmente a protecção sem fios.

Depois de instalar o Wireless Network Security, o computador tenta estabelecer ligação ao router sem fios. Quando a ligação for estabelecida, o computador programa a chave de encriptação no router sem fios. Se a palavra-passe predefinida tiver sido alterada, será solicitada a palavra-passe para que o Wireless Network Security possa configurar o router sem fios com a chave de encriptação partilhada e um modo de segurança forte. O computador também é configurado com a mesma chave partilhada e modo de encriptação, estabelecendo uma ligação sem fios segura.

Iniciar o Wireless Network Security

O Wireless Network Security está activado por predefinição; no entanto, é possível activar e desactivar a protecção sem fios manualmente.

A activação da protecção sem fios protege a rede sem fios contra intrusos e intercepção de dados. No entanto, se estiver ligado a uma rede sem fios externa, a protecção varia em função do respectivo nível de segurança.

Para activar manualmente a protecção sem fios:

1. No painel McAfee SecurityCenter, efectue uma das seguintes acções:
   - Clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
   - Clique em **Menu Avançado**, **Configurar** no painel **Página Inicial** e, em seguida, aponte para **Internet e Rede**.
2. No painel **Configuração de Internet eRede**, em **Protecção sem fios**, clique em **Ligado**.

Nota: O Wireless Network Security é activado automaticamente se tiver uma placa sem fios compatível instalada.

Parar o Wireless Network Security

O Wireless Network Security está activado por predefinição; no entanto, é possível activar e desactivar a protecção sem fios manualmente.

A desactivação da protecção sem fios deixa a rede vulnerável a intrusos e intercepção de dados.

Para desactivar a protecção sem fios:

1. No painel McAfee SecurityCenter, efectue uma das seguintes acções:
   - Clique em **Internet e Rede** e, em seguida, clique em **Configurar**.
   - Clique em **Menu Avançado**, **Configurar** no painel **Página Inicial** e, em seguida, aponte para **Internet e Rede**.
2. No painel **Configuração de Internet eRede**, em **Protecção sem fios**, clique em **Desligado**.

CAPÍTULO 14

Proteger redes sem fios

O Wireless Network Security protege a rede implementando encriptação sem fios (através de WEP, WPA ou WPA2, consoante o equipamento). Programa automaticamente clientes e routers sem fios com as credenciais da chave de encriptação válida, de forma a que o router sem fios autorize os computadores a estabelecer ligação. As redes sem fios protegidas por encriptação impedem que os utilizadores não autorizados acedam à rede sem fios e protegem os dados enviados através de uma rede sem fios. O Wireless Network Security consegue isto:

- Criando e distribuindo uma chave de encriptação longa, forte, aleatória e partilhada
- Efectuando a rotação da chave de encriptação de forma agendada
- Configurando cada dispositivo sem fios com chaves de encriptação

Neste capítulo

Configurar redes sem fios protegidas 74
Adicionar computadores à rede sem fios protegida .86

Configurar redes sem fios protegidas

Quando o Wireless Network Security estiver instalado, solicitará automaticamente ao utilizador que proteja a rede sem fios não segura à qual está ligado ou adira a uma rede sem fios anteriormente protegida.

Se não estiver ligado a uma rede sem fios, o Wireless Network Security procura uma rede protegida da McAfee com uma potência de sinal forte e solicita ao utilizador que adira à rede. Se não estiverem disponíveis redes protegidas, o Wireless Network Security procura redes não seguras com sinais fortes e quando for encontrada uma, solicita ao utilizador que proteja essa rede.

A não ser que uma rede sem fios tenha sido protegida pelo McAfee Wireless Network Security, a McAfee considera as redes sem fios “não protegidas”, mesmo se utilizarem mecanismos de segurança sem fios, como, por exemplo, WEP e WPA.

A menos que uma rede sem fios esteja protegida pelo Wireless Network Security, a McAfee considera a rede não protegida, mesmo que utilize mecanismos de segurança sem fios, tais como WEP e WPA.

Acerca de tipos de acesso

Qualquer computador sem fios com o Wireless Network Security instalado pode criar uma rede sem fios protegida. É concedido automaticamente ao primeiro computador a proteger um router e a criar uma rede sem fios protegida acesso administrativo a essa rede. Um utilizador existente com acesso administrativo pode conceder acesso administrativo, total ou de convidado aos computadores que aderirem posteriormente.

Os computadores com tipos de acesso administrativo e total podem efectuar as seguintes tarefas:

- Proteger e remover um router ou ponto de acesso
- Rodar as chaves de segurança
- Alterar as definições de segurança da rede
- Reparar redes
- Conceder aos computadores acesso à rede
- Revogar o acesso à rede sem fios protegida
- Alterar o nível de administração de um computador

Os computadores com tipos de acesso de convidado podem efectuar as seguintes tarefas na rede:

- Estabelecer ligação a uma rede
- Aderir a uma rede
- Modificar definições específicas do computador convidado

Nota: Os computadores podem ter acesso administrativo numa rede sem fios, mas acesso de convidado ou total noutra. Um computador com acesso de convidado ou total numa rede pode criar uma nova rede.

Tópicos relacionados

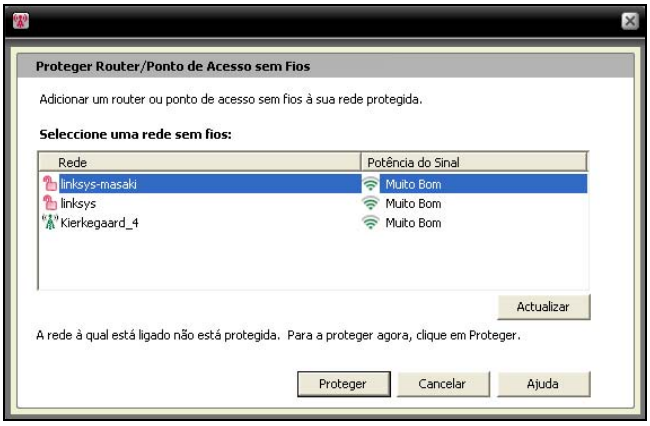
- **Aderir a uma rede sem fios protegida** (página 78)
- **Conceder acesso administrativo a computadores** (página 82)
- **Revogar o acesso à rede** (página 101)

Criar redes sem fios protegidas

Para criar uma rede sem fios protegida, é necessário adicionar primeiro o router ou ponto de acesso sem fios da rede sem fios.

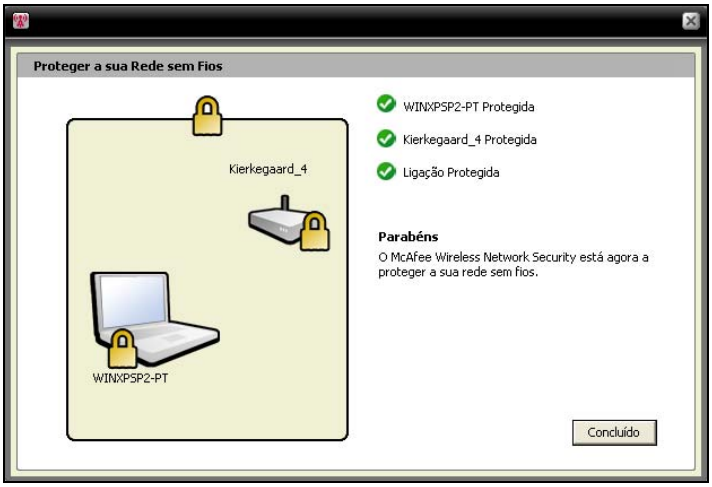
Para adicionar um router ou ponto de acesso sem fios:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas de Protecção, em **Proteger Router/Ponto de Acesso Sem Fios**, clique em **Proteger**.
4. No painel Proteger Router/Ponto de Acesso Sem Fios, seleccione uma rede sem fios a proteger e, em seguida, clique em **Proteger**.



O painel Proteger a sua Rede Sem Fios é apresentado quando o Wireless Network Security tentar proteger o computador, router e ligação à rede.

A protecção com êxito de todos estes componentes resulta na protecção total da rede sem fios.



5 Clique em **Concluído**.

Nota: Depois de proteger uma rede, a caixa de diálogo Passo Seguinte indica que deverá instalar o Wireless Network Security em cada computador sem fios para permitir que adiram à rede.

Se configurou anteriormente uma chave pré-partilhada manualmente para o router ou ponto de acesso e não esteve ligado quando tentou proteger o router ou ponto de acesso, também terá de introduzir a chave na caixa Chave WEP e, em seguida, clicar em Ligar. Se tiver alterado anteriormente o nome de utilizador ou palavra-passe administrativa do router sem fios, será solicitado que introduza estas informações antes de proteger um router ou ponto de acesso.

Tópicos relacionados

- **Proteger outros dispositivos sem fios** (página 84)
- **Adicionar computadores à rede sem fios protegida** (página 86)

Aderir a redes sem fios protegidas

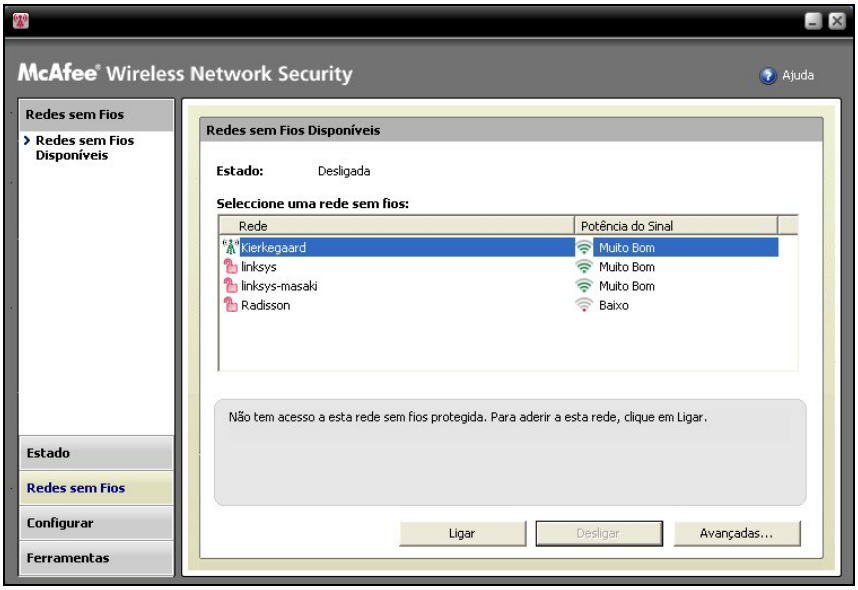
Uma rede protegida evita que os hackers interceptem os dados transmitidos através da rede e estabelecem ligação à rede. Antes de um computador autorizado poder aceder a uma rede sem fios protegida, tem de aderir primeiro à mesma.

Quando um computador pede para aderir à rede gerida, é enviada uma mensagem aos outros computadores da rede que têm acesso administrativo. Como administrador, é responsável por determinar o tipo de acesso a conceder ao computador: convidado, total ou administrativo.

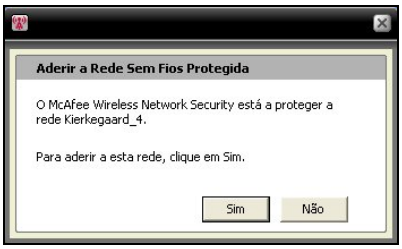
Antes de poder aderir a uma rede protegida, é necessário instalar o Wireless Network Security e, em seguida, estabelecer ligação à rede sem fios protegida. Um utilizador existente da rede com acesso administrativo na rede sem fios protegida tem de permitir a adesão. Depois de aderir à rede, não é necessário aderir novamente quando restabelecer ligação. É necessário que o concessor e o computador que adere tenham uma ligação sem fios activa. O concessor tem de ser um computador administrador ligado à rede.

Para aderir a uma rede sem fios protegida:

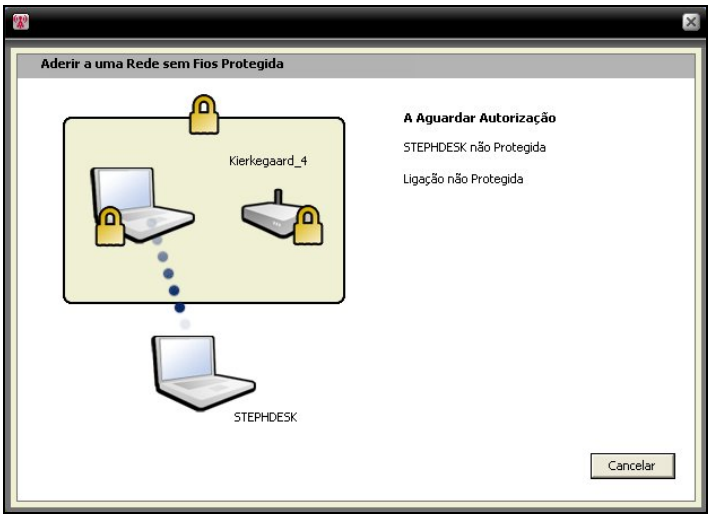
1. No computador não protegido, clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Redes Sem Fios**.
3. No painel Redes Sem Fios Disponíveis, seleccione uma rede e, em seguida, clique em **Ligar**.



4 Na caixa de diálogo Aderir a Rede Sem Fios Protegida, clique em **Sim** para aderir à rede.



Quando o Wireless Network Security tentar solicitar permissão para aderir à rede, é apresentado o painel Aderir a uma Rede Sem Fios Protegida no computador que está a tentar aderir à rede.



5 O painel Aderir à Rede é apresentado no computador administrador a partir do qual é possível conceder acesso de convidado, total ou administrativo.

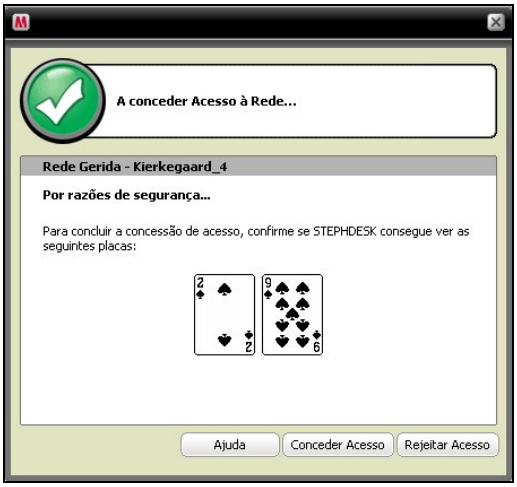
Na caixa de diálogo Aderir à Rede, seleccione uma das seguintes opções:

Conceder acesso de convidado	Permite ao computador enviar ficheiros para outros computadores na rede sem fios, mas não partilhar ficheiros com o McAfee EasyNetwork.
Conceder acesso total a todas as aplicações da rede gerida	Permite ao computador enviar e partilhar ficheiros com o McAfee EasyNetwork.
Conceder acesso administrativo a todas as aplicações da rede gerida:	Permite ao computador enviar e partilhar ficheiros com o McAfee EasyNetwork, conceder acesso a outros computadores e ajustar os níveis de acesso de outros computadores na rede sem fios.

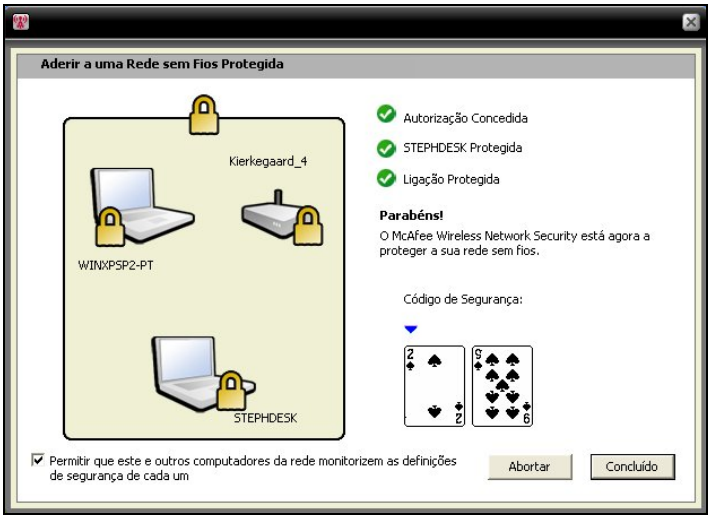
6 Clique em **Conceder Acesso**.

7 Confirme se as cartas de jogar apresentadas no painel Conceder Acesso à Rede correspondem às apresentadas no computador que está a tentar aderir à rede sem fios. Se as cartas de jogar corresponderem, clique em **Conceder Acesso**.

Se os computadores não apresentarem cartas de jogar idênticas, ocorreu uma potencial falha de segurança. Conceder acesso à rede a este computador poderá colocar o computador em risco. Para proibir o computador de aceder à rede sem fios, clique em **Rejeitar Acesso**.

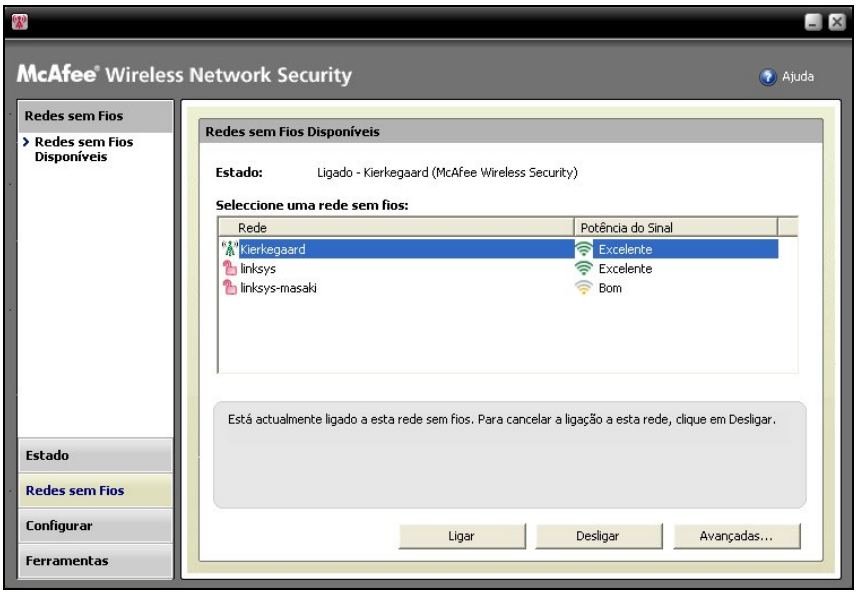


8 O painel Conceder Acesso à Rede confirma se o novo computador está protegido pelo Wireless Network Security. Para monitorizar as definições de segurança e ser monitorizado por outros computadores, seleccione **Permitir que este e outros computadores da rede monitorizem as definições de segurança de cada um**.



9 Clique em **Concluído**.

10 O painel Redes Sem Fios Disponíveis indica se está ligado à rede sem fios protegida.



Tópicos relacionados

- **Adicionar computadores à rede sem fios protegida** (página 86)

Ligar a redes sem fios protegidas

Se já tiver aderido a uma rede sem fios protegida, mas tiver terminado posteriormente a ligação e o acesso não foi revogado, poderá restabelecer a ligação a qualquer altura sem ter de aderir novamente.

Para ligar a uma rede sem fios protegida:

1 Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.

2 Seleccione **Ver Redes Sem Fios**.

3 No painel Redes Sem Fios Disponíveis, seleccione uma rede e, em seguida, clique em **Ligar**.

Conceder acesso administrativo a computadores

Os computadores com privilégios administrativos podem proteger routers sem fios, alterar modos de segurança e conceder a novos computadores acesso à rede sem fios protegida.

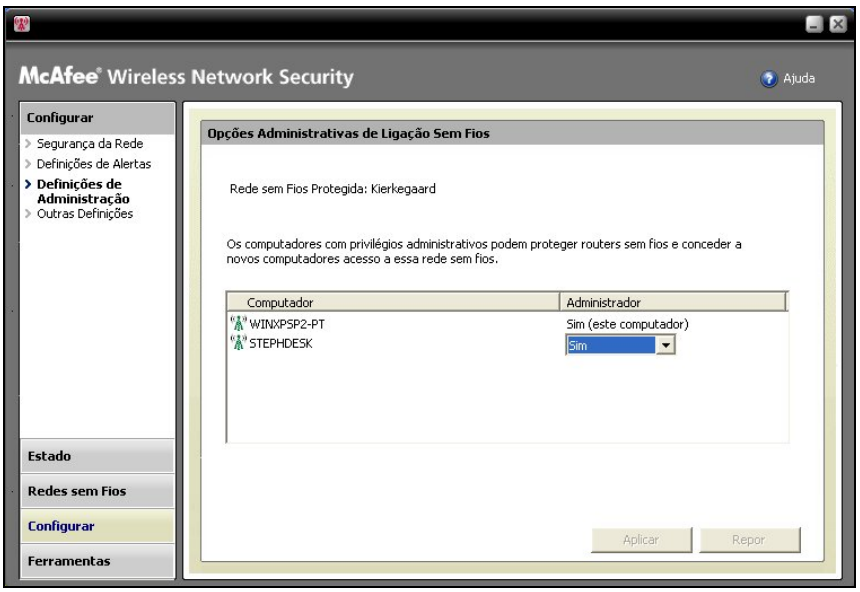
Para configurar o acesso administrativo:

1 Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.

2 Seleccione **Configurar Vista**.

3 No painel Configurar, seleccione **Definições de Administração**.

4 No painel Opções de Administração de Ligação Sem Fios, seleccione **Sim** ou **Não** para permitir ou impedir o acesso administrativo.



5 Clique em **Aplicar**.

Tópicos relacionados

- **Acerca de tipos de acesso** (página 75)
- **Revogar o acesso à rede** (página 101)

Proteger outros dispositivos sem fios

O Wireless Network Security permite adicionar uma ou várias impressoras, servidores de impressão ou consolas de jogos sem fios à rede.

Para adicionar uma impressora, um servidor de impressão ou uma consola de jogos sem fios:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas de Protecção, em **Proteger Dispositivos Que Não São Pontos de Acesso**, clique em **Proteger**.
4. No painel Proteger um Dispositivo Sem Fios, seleccione um dispositivo sem fios e, em seguida, clique em **Proteger**.
5. O alerta Dispositivo Que Não É um Ponto de Acesso Protegido confirma que o dispositivo foi adicionado à rede.

Ligar a redes com Difusão do SSID desactivada

É possível ligar a redes sem fios que tenham a Difusão do SSID desactivada. Quando os routers têm a Difusão do SSID desactivada, não são apresentados no painel Redes Sem Fios Disponíveis.

A McAfee recomenda que não proteja routers sem fios que tenham desactivado a Difusão do SSID no Wireless Network Security.

Para ligar a uma rede sem fios com a Difusão do SSID desactivada:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Redes Sem Fios**.
3. No painel Redes Sem Fios Disponíveis, clique em **Avançadas**.
4. No painel Redes Sem Fios, clique em **Adicionar**.
5. No painel Adicionar Rede Sem Fios, especifique as seguintes definições e, em seguida, clique em **OK**:

Definição	Descrição
Rede	O nome da rede. Se estiver a modificar uma rede, não poderá alterar o nome.
Definições de Segurança	A segurança da rede não protegida. Tenha em atenção que, se a placa sem fios não suportar o modo seleccionado, não será possível estabelecer ligação. Os modos de segurança incluem: Desactivado, WEP Aberta, WEP Partilhada, WEP Automática, WPA-PSK e WPA2-PSK.
Modo de Encriptação	A encriptação associada ao modo de segurança seleccionado. Os modos de encriptação incluem: WEP, TKIP, AES e TKIP+AES.

Nota: A McAfee recomenda que não proteja routers sem fios que tenham desactivado a Difusão do SSID no Wireless Network Security. Se tiver de utilizar esta funcionalidade, faça-o apenas quando a difusão do SSID estiver desactivada.

Adicionar computadores à rede sem fios protegida

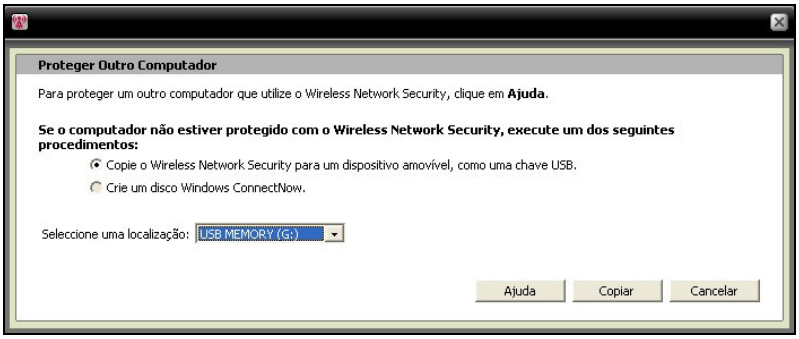
É possível adicionar computadores à rede sem fios protegida utilizando um dispositivo amovível, como, por exemplo, uma unidade flash USB, CD gravável ou tecnologia Windows Connect Now.

Adicionar computadores utilizando um dispositivo amovível

O Wireless Network Security permite adicionar computadores à rede sem fios protegida que não tenham o Wireless Network Security instalado, utilizando uma unidade flash USB ou um CD gravável.

Para adicionar um computador:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas de Protecção, em **Proteger Computador**, clique em **Proteger**.
4. No painel Proteger Outro Computador, seleccione **Copiar o Wireless Network Security para um dispositivo amovível, como uma chave USB**.



5 Seleccione a localização da Unidade de CD ou unidade flash USB para a qual pretende copiar o Wireless Network Security.

6 Clique em **Copiar**.

7 Depois de todos os ficheiros serem copiados para o CD ou unidade flash USB, insira o dispositivo amovível no computador que pretende proteger. Se o programa não for iniciado automaticamente, navegue para o conteúdo do suporte amovível a partir do Explorador do Windows e, em seguida, clique em **Install.exe**.

8 Siga as instruções apresentadas no ecrã.

Nota: Também poderá adicionar um computador à rede sem fios protegida utilizando a tecnologia Windows Connect Now.

Tópicos relacionados

- **Adicionar computadores utilizando a tecnologia Windows Connect Now** (página 88)

Adicionar computadores utilizando a tecnologia Windows Connect Now

O Wireless Network Security permite adicionar computadores à rede que não tenham o Wireless Network Security instalado, utilizando a tecnologia Windows Connect Now.

Para adicionar um computador utilizando a tecnologia Windows Connect Now:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas de Protecção, em **Proteger Computador**, clique em **Proteger**.
4. No painel Proteger Outro Computador, seleccione **Criar um disco do Windows Connect Now**
5. Seleccione a localização para a qual pretende copiar as informações do Windows Connect Now.
6. Clique em **Copiar**.
7. Insira o disco do Windows Connect Now no computador que pretende proteger.
8. Se o disco não for iniciado automaticamente, efectue um dos seguintes procedimentos:
   - Instale a tecnologia Wireless Connect Now: Clique em **Iniciar** na barra de tarefas do Windows e, em seguida, clique em Painel de Controlo. Se estiver a utilizar a vista Categoria do Painel de Controlo, clique em **Ligações de Rede e de Internet** e, em seguida, clique em **Assistente de Configuração de Rede Sem Fios**. Se estiver a utilizar a vista Clássica do Painel de Controlo, clique em **Assistente de Configuração de Rede Sem Fios**. Siga as instruções apresentadas no ecrã.
   - Abra o ficheiro `setupSNK.exe` no disco do Windows Connect e copie e cole a chave no cliente de selecção de rede sem fios.

Nota: Suspenda a rotação da chave se utilizar a tecnologia Windows Connect para ligar à rede sem fios, caso contrário a ligação à rede falhará. A ligação falhará, porque a rotação da chave cria uma nova chave que difere da utilizada pela tecnologia Windows Connect Now.

Também poderá adicionar computadores à rede sem fios protegida utilizando um dispositivo amovível, como, por exemplo, um CD gravável ou uma unidade flash USB.

Tópicos relacionados

- **Adicionar computadores utilizando um dispositivo amovível** (página 86)

CAPÍTULO 15

Administrar redes sem fios

O Wireless Network Security fornece um conjunto completo de ferramentas de administração para ajudar a gerir e efectuar a manutenção da rede sem fios.

Neste capítulo

Gerir redes sem fios.....92

Gerir redes sem fios

Quando está ligado a uma rede sem fios protegida, as informações enviadas e recebidas são encriptadas. Os hackers não conseguem desencriptar os dados transmitidos na rede protegida e não conseguem aceder à rede. O Wireless Network Security fornece várias ferramentas para ajudar a gerir a rede de forma a evitar intrusões adicionais.

Acerca dos ícones do Wireless Network Security

O Wireless Network Security apresenta ícones para representar vários tipos de ligação à rede e potências de sinal.

Ícones de ligação à rede

A tabela seguinte descreve os ícones mais utilizados pelo Wireless Network Security nos painéis Estado da Rede Sem Fios, Ferramentas de Protecção e Redes Sem Fios Disponíveis. Os ícones representam vários estados de segurança e ligação à rede.

Ícone	Painéis de estado	Painéis de protecção
	O computador está ligado à rede sem fios protegida seleccionada.	O dispositivo está protegido pelo Wireless Network Security.
	O computador pode aceder à rede sem fios protegida, mas não está actualmente ligado.	O dispositivo utiliza o modo de segurança WEP ou WPA.
	O computador foi anteriormente membro da rede sem fios protegida, mas o acesso foi revogado quando o computador foi desligado da rede.	O dispositivo tem o Wireless Network Security desactivado.

Ícones de potência de sinal

A tabela seguinte descreve os ícones mais utilizados pelo Wireless Network Security para representar as várias potências de sinal da rede.

Ícone	Descrição
	Potência de sinal excelente
	Potência de sinal muito boa
	Potência de sinal boa
	Potência de sinal baixa

Tópicos relacionados

- **Ver a potência de sinal da rede** (página 123)
- **Ver computadores actualmente protegidos** (página 129)
- **Ver o modo de segurança da rede** (página 122)

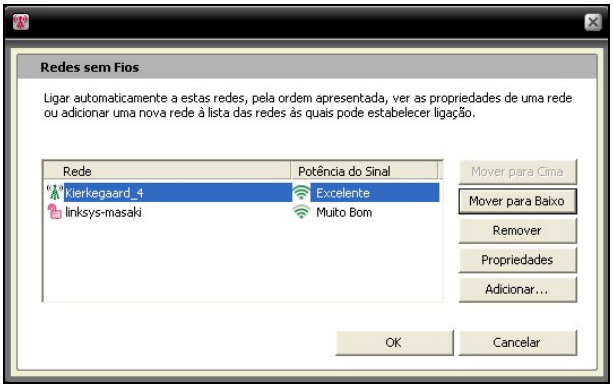
Listar redes preferenciais

O Wireless Network Security permite especificar redes sem fios preferenciais. Isto permite especificar a ordem das redes às quais o computador estabelece ligação automaticamente. O Wireless Network Security tenta ligar à primeira rede apresentada na lista.

Esta funcionalidade é útil quando pretender, por exemplo, ligar automaticamente à rede sem fios de um amigo quando estiver na respectiva área. Poderá promover outra rede para o topo da lista.

Para listar redes preferenciais:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Redes Sem Fios**.
3. No painel Redes Sem Fios Disponíveis, clique em **Avançadas**.
4. Seleccione a rede cuja ordem pretende ajustar e clique em **Mover para Cima** ou **Mover para Baixo**.



5. Clique em **OK**.

Tópicos relacionados

- **Remover redes sem fios preferenciais** (página 95)

Remover redes sem fios preferenciais

É possível utilizar o Wireless Network Security para remover redes preferenciais.

Isto é útil quando pretender, por exemplo, remover uma rede obsoleta da lista.

Para remover redes preferenciais:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Redes Sem Fios**.
3. No painel Redes Sem Fios Disponíveis, clique em **Avançadas**.
4. No painel Redes Sem Fios, seleccione uma rede e, em seguida, clique em **Remover**.
5. Clique em **OK**.

Tópicos relacionados

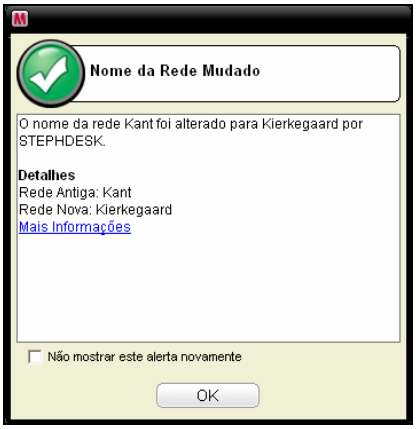
- **Listar redes preferenciais** (página 94)

Mudar o nome de redes sem fios protegidas

É possível utilizar o Wireless Network Security para mudar o nome da rede sem fios protegida existente.

Mudar o nome da rede pode ser útil se o respectivo nome for semelhante ou idêntico ao utilizado pelo seu vizinho ou se pretender criar um nome exclusivo que seja mais fácil de distinguir.

Poderá ser necessário restabelecer manualmente a ligação dos computadores ligados à rede sem fios protegida e será recebida uma notificação quando o nome for alterado.



Após a alteração do nome da rede, o novo nome é apresentado no painel Router/Ponto de Acesso Sem Fios Protegido.

Para modificar o nome da rede sem fios protegida:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel Segurança da Rede, escreva o novo nome na caixa **Nome da Rede Sem Fios Protegida**.
4. Clique em **Aplicar**.

   A caixa de diálogo Actualizar Definições de Segurança de Rede é apresentada quando o Wireless Network Security alterar o nome da rede sem fios protegida. Dependendo das definições e da potência de sinal do computador, o nome da rede é alterado em menos de um minuto.

Nota: Como medida de segurança, a McAfee recomenda que mude o nome do SSID predefinido do router ou ponto de acesso. Apesar de o Wireless Network Security suportar SSIDs predefinidos, tais como "linksys", "belkin54g" ou "NETGEAR", mudar o nome de SSIDs protege-o contra ameaças de pontos de acesso rogue.

Configurar definições de alerta

O Wireless Network Security permite configurar definições de alerta de forma a mostrar alertas quando ocorrerem determinados eventos, como, por exemplo, quando é ligado um novo computador à rede.

Para configurar o comportamento dos alertas:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. Clique em **Definições de Alerta**.
4. Seleccione ou desmarque um ou vários dos seguintes eventos e, em seguida, clique em **Aplicar**:

Definição de Alerta	Descrição
A chave de segurança da rede sem fios protegida foi rodada	Apresenta o alerta Chave de Segurança Rodada depois de efectuar a rotação manual ou automática da chave de segurança. A rotação da chave protege a rede contra a tentativa dos hackers de interceptar os dados ou aceder à rede.
Um outro computador protegido iniciou ou terminou a ligação à rede.	Apresenta o alerta Computador Ligado ou Computador Desligado depois de um computador iniciar ou terminar a ligação à rede sem fios protegida. Os dados existentes nos computadores ligados estão, agora, protegidos contra intrusos e intercepção de dados.
Foi concedido acesso à sua rede sem fios protegida a outro computador.	Apresenta o alerta Acesso à Rede Concedido ao Computador depois de um computador administrador permitir a adesão de outro computador à rede sem fios protegida. Conceder a um computador o acesso à rede protegida protege-o contra a tentativa dos hackers de interceptar os dados.
A rotação da chave da sua rede sem fios protegida foi suspensa ou retomada.	Apresenta o alerta Rotação da Chave Suspensa ou Rotação da Chave Retomada depois de suspender ou retomar manualmente a rotação da chave. A rotação da chave protege a rede contra a tentativa dos hackers de interceptar os dados ou aceder à rede.
Foi revogado o acesso a todos os computadores desligados	Apresenta o alerta Acesso Revogado depois de o acesso dos computadores não ligados à rede ter sido revogado. Os computadores desligados têm de voltar a aderir à rede.
Foi adicionado ou removido um router da sua rede sem fios protegida	Apresenta o alerta Router/Ponto de Acesso Adicionado à Rede ou Router/Ponto de Acesso Não Protegido depois de o router ou ponto de acesso sem fios ser adicionado ou removido da rede sem fios protegida.
As informações de início de sessão de um router sem fios protegido mudaram	Apresenta o alerta Início de Sessão do Router/Ponto de Acesso Alterado depois de o administrador do Wireless Network Security alterar o nome de utilizador ou palavra-passe de um router ou ponto de acesso.

O nome ou as definições de segurança da sua rede sem fios protegida foram alterados	Apresenta o alerta Definições de Rede Alteradas ou Nome da Rede Mudado depois de mudar o nome da rede sem fios protegida ou ajustar a respectiva definição de segurança.
As definições da sua rede sem fios protegida estão a ser reparadas	Apresenta o alerta Rede Reparada; as definições de segurança dos routers ou pontos de acesso sem fios da rede são fixas.

Nota: Para escolher ou limpar todas as definições de alerta, clique em **Seleccionar Tudo** ou **Limpar Tudo**. Para repor as definições de alerta do Wireless Network Security, clique em **Restaurar Predefinições**.

Tópicos relacionados

- **Rodar chaves automaticamente** (página 110)
- **Aderir a uma rede sem fios protegida** (página 78)
- **Ligar a redes sem fios protegidas** (página 82)
- **Terminar ligação de redes sem fios protegidas** (página 100)
- **Suspender rotação automática da chave** (página 113)
- **Revogar o acesso à rede** (página 101)
- **Remover routers ou pontos de acesso sem fios** (página 99)
- **Alterar credenciais de dispositivos sem fios** (página 107)
- **Mudar o nome de redes sem fios protegidas** (página 95)
- **Reparar definições de segurança da rede** (página 108)

Apresentar notificações de ligação

É possível configurar o Wireless Network Security para notificá-lo quando o computador estabelecer ligação a uma rede sem fios.

Para apresentar uma notificação quando estabelecer ligação a uma rede sem fios:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. Clique em **Outras Definições**.
4. Seleccione **Apresentar uma mensagem de notificação quando estiver ligado a uma rede sem fios**.
5. Clique em **Aplicar**.

Tópicos relacionados

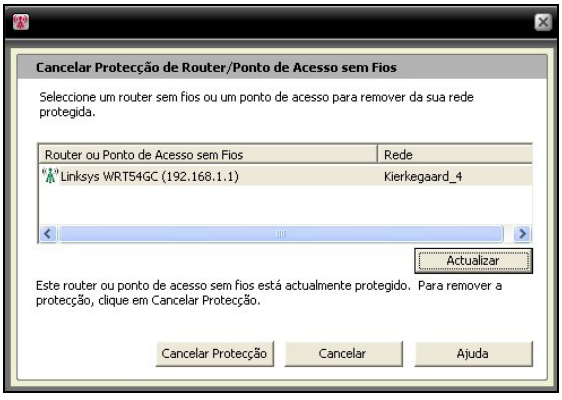
- **Ligar a redes sem fios protegidas** (página 82)

Remover routers ou pontos de acesso sem fios

O Wireless Network Security permite remover um ou vários routers ou pontos de acesso da rede protegida.

Para remover um router ou ponto de acesso sem fios:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas de Protecção, em **Desproteger um Dispositivo**, clique em **Cancelar Protecção**.
4. No painel Cancelar Protecção de Router/Ponto de Acesso Sem Fios, seleccione um router ou ponto de acesso sem fios a remover da rede protegida e, em seguida, clique em **Cancelar Protecção**.



5 Clique em **OK** na caixa de diálogo Router/Ponto de Acesso Sem Fios Não Protegido para confirmar se o router ou ponto de acesso sem fios foi removido da rede.

Tópicos relacionados

- **Criar redes sem fios protegidas** (página 76)

Terminar ligação de redes sem fios protegidas

O Wireless Network Security permite desligar o computador da rede.

Esta tarefa é útil quando, por exemplo, o computador tiver estabelecido ligação à rede utilizando um nome idêntico ao nome da rede. É possível terminar a ligação da rede e, em seguida, ligar novamente.

Esta funcionalidade também é útil quando ligar inadvertidamente à rede errada devido à potência de sinal de outro ponto de acesso ser forte ou como resultado de interferência de rádio.

Para terminar a ligação de uma rede sem fios protegida:

1 Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.

2 Seleccione **Ver Redes Sem Fios**.

3 No painel Redes Sem Fios Disponíveis, seleccione a rede e, em seguida, clique em **Desligar**.

Tópicos relacionados

- **Revogar o acesso à rede** (página 101)
- **Sair de redes sem fios protegidas** (página 102)

Revogar o acesso à rede

O Wireless Network Security permite revogar o acesso de computadores que não estejam ligados à rede. É estabelecido um novo agendamento de rotação da chave de segurança: os computadores não ligados perderão o acesso à rede sem fios protegida, mas poderão recuperá-lo aderindo novamente à rede. Os computadores ligados continuam a ter acesso.

Por exemplo, pode revogar o acesso do computador de um visitante com o Wireless Network Security depois de se desligar. Além disso, um adulto pode revogar o acesso de um computador utilizado por uma criança como forma de controlo de acesso à Internet. Também é possível revogar o acesso de um computador ao qual foi concedido inadvertidamente.

Para revogar o acesso de todos os computadores desligados da rede protegida:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas, clique em Ferramentas de Manutenção.
4. No painel Ferramentas de Manutenção, em **Revogar Acesso**, clique em **Revogar**.
5. No painel Revogar Acesso, clique em **Revogar**.
6. Clique em **OK** na caixa de diálogo Wireless Network Security.

Tópicos relacionados

- **Terminar ligação de redes sem fios protegidas** (página 100)
- **Sair de redes sem fios protegidas** (página 102)

Sair de redes sem fios protegidas

É possível utilizar o Wireless Network Security para cancelar os direitos de acesso a uma rede protegida.

Para sair de uma rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel Configurar, seleccione **Outras Definições**.
4. No painel Outras Definições, em Acesso a Rede Protegida, seleccione a rede da qual pretende sair e, em seguida, clique em **Abandonar Rede**.
5. No painel Terminar ligação da rede, clique em **Sim** para sair da rede.

Nota: Quando sair de uma rede, outro utilizador terá de conceder-lhe acesso à rede protegida antes de poder aderir novamente.

Tópicos relacionados

- **Terminar ligação de redes sem fios protegidas** (página 100)
- **Revogar o acesso à rede** (página 101)

CAPÍTULO 16

Gerir segurança da rede sem fios

O Wireless Network Security fornece um conjunto completo de ferramentas para ajudar a gerir as funcionalidades de segurança da rede sem fios.

Neste capítulo

Configurar definições de segurança 104
Administrar chaves de rede 109

Configurar definições de segurança

Depois de ligar a uma rede sem fios protegida, o Wireless Network Security protege automaticamente a rede; no entanto, poderá configurar definições de segurança adicionais a qualquer altura.

Configurar modos de segurança

É possível especificar o modo de segurança da rede sem fios protegida. Os modos de segurança definem a encriptação entre o computador e o router ou ponto de acesso.

Quando proteger a rede, o modo WEP é configurado automaticamente. No entanto, a McAfee recomenda a alteração do modo de segurança para WPA2 ou WPA-PSK AES. O Wireless Network Security utiliza inicialmente o modo WEP, uma vez que é suportado por todos os routers e placas de rede sem fios. Contudo, a maioria dos novos routers e placas de rede sem fios utilizam o modo WPA, o qual é mais seguro.

Para alterar o modo de segurança de uma rede sem fios protegida:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel Segurança da Rede, seleccione o tipo de segurança que pretende implementar a partir da caixa **Modo de Segurança** e, em seguida, clique em **Aplicar**.

A tabela seguinte descreve os modos de segurança disponíveis:

Potência	Modo	Descrição
Mais fraca	WEP	O protocolo WEP (Wired Equivalent Privacy) faz parte da norma de rede sem fios IEEE 802.11 para proteger redes sem fios IEEE 802.11. O modo WEP proporciona um nível de segurança que consegue impedir monitorizações não sofisticadas, mas, normalmente, não é tão seguro como a encriptação WPA-PSK. Apesar de o Wireless Network Security fornecer uma chave forte (difícil de adivinhar e longa), a McAfee recomenda a utilização de um modo de segurança WPA.
Média	WPA-PSK TKIP	O WPA (Wi-Fi Protected Access) é uma versão antiga da norma de segurança 802.11i. O TKIP destina-se ao WPA para melhorar o modo WEP. O TKIP proporciona integridade de mensagens, mecanismo de recriação de chaves e mistura de chaves por pacote.
Forte	WPA-PSK AES	Este modo de segurança combina os modos WPA e AES. O protocolo AES (Advanced Encryption Standard) é uma cifra em bloco adoptada como norma de encriptação pelo Governo dos Estados Unidos.
Mais forte	WPA2-PSK AES	Este modo de segurança combina os modos WPA2 e AES. O WPA2 é o próximo avanço da ratificação da norma de segurança 802.11i. O WPA2 utiliza o protocolo CCMP (Counter Mode CBC MAC Protocol), o qual constitui uma solução mais segura e escalável em comparação com o TKIP. Trata-se do modo de segurança mais forte disponível para os consumidores.
Máxima	WPA2-PSK TKIP+AES	Este modo de segurança combina os modos WPA2, AES e WPA-PSK TKIP. Permite obter uma maior flexibilidade de forma a que as placas sem fios antigas e novas possam estabelecer ligação.

Nota: Após a alteração do modo de segurança, poderá ser necessário restabelecer a ligação manualmente.

Tópicos relacionados

- **Reparar definições de segurança da rede** (página 108)
- **Ver o modo de segurança da rede** (página 122)

Configurar as definições de segurança da rede

É possível modificar as propriedades das redes protegidas pelo Wireless Network Security. Isto é útil quando pretender, por exemplo, actualizar a segurança de WEP para WPA.

A McAfee recomenda a modificação das definições de segurança da rede se um alerta sugerir que o faça.

Para configurar propriedades de redes não protegidas:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Redes Sem Fios**.
3. No painel Redes Sem Fios Disponíveis, clique em **Avançadas**.
4. No painel Redes Sem Fios, clique em **Propriedades**.
5. No painel Propriedades da Rede Sem Fios, modifique as seguintes definições e, em seguida, clique em **OK**:

Definição	Descrição
Rede	O nome da rede. Se estiver a modificar uma rede, não poderá alterar o nome.
Definições de Segurança	A segurança da rede não protegida. Tenha em atenção que, se a placa sem fios não suportar o modo seleccionado, não será possível estabelecer ligação. Os modos de segurança incluem: Desactivado, WEP Aberta, WEP Partilhada, WEP Automática, WPA-PSK e WPA2-PSK.
Modo de Encriptação	A encriptação associada ao modo de segurança seleccionado. Os modos de encriptação incluem: WEP, TKIP, AES e TKIP+AES.

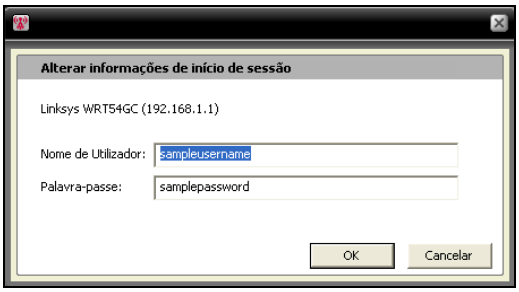
Alterar credenciais de dispositivos sem fios

É possível alterar o nome de utilizador ou a palavra-passe de um dispositivo no router ou ponto de acesso sem fios protegido. A lista de dispositivos é apresentada em **Dispositivos de Rede Sem Fios Protegida**.

A McAfee recomenda a alteração das credenciais, porque a maioria dos dispositivos sem fios de um único fabricante possuem as mesmas credenciais de início de sessão. A alteração das credenciais de início de sessão evita que outros utilizadores acedam ao router ou ponto de acesso sem fios e alterem as respectivas definições.

Para alterar o nome de utilizador ou palavra-passe de um dispositivo de rede sem fios protegida:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel Segurança da Rede, em **Dispositivos de Rede Sem Fios Protegida**, seleccione um router ou ponto de acesso sem fios e, em seguida, clique em **Alterar Nome de Utilizador ou Palavra-passe**.



4. Clique em **OK** na caixa de diálogo Wireless Network Security depois de introduzir as informações de início de sessão.

   O novo nome de utilizador e palavra-passe são apresentados em **Dispositivos de Rede Sem Fios Protegida**.

Nota: Alguns routers não suportam nomes de utilizador e, por isso, não será apresentado nenhum nome de utilizador em **Dispositivos de Rede Sem Fios Protegida**.

Reparar definições de segurança da rede

Se tiver problemas com a configuração ou as definições de segurança, poderá utilizar o Wireless Network Security para reparar as definições do router ou ponto de acesso.

Para reparar as definições de segurança:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas, clique em **Ferramentas de Manutenção**.
4. Em **Reparar Definições de Segurança de Rede**, clique em **Reparar**.
5. No painel Reparar Definições de Segurança de Rede, clique em **Reparar**.

   Um alerta do Wireless Network Security indica se a rede foi ou não reparada.

Nota: Se a tentativa de reparação da rede não for efectuada com êxito, estabeleça ligação à rede utilizando um cabo e, em seguida, tente novamente. Se a palavra-passe do router ou ponto de acesso tiver sido alterada, será necessário reintroduzi-la para estabelecer ligação.

Administrar chaves de rede

O Wireless Network Security gera chaves de encriptação longas, fortes e aleatórias através de um gerador de chaves aleatórias. Através do modo WEP, a chave é convertida num valor hexadecimal de 26 dígitos (para 104 bits de entropia, ou força, a força máxima suportada por WEP de 128 bits), enquanto que com o WPA, a chave é uma cadeia ASCII de 63 caracteres. Cada carácter possui 64 valores possíveis (6 bits), proporcionando 384 bits de entropia, a qual excede a força da chave WAP de 256 bits.

Quando gere chaves de rede, poderá apresentar chaves em texto simples ou asteriscos para pontos de acesso não protegidos, ignorar chaves guardadas para pontos de acesso não protegidos, activar ou desactivar a rotação da chave, alterar a frequência de rotação da chave, efectuar a rotação da chave manualmente e suspender a rotação da chave.

Quando a rotação das chaves é efectuada automaticamente, as ferramentas dos hackers não conseguem capturar as informações devido à alteração contínua da chave.

No entanto, se estiver a ligar dispositivos sem fios não suportados pelo Wireless Network Security (por exemplo, ligar um PDA sem fios à rede), deverá anotar a chave, parar a rotação da chave e, em seguida, introduzi-la no dispositivo.

Ver chaves actuais

O Wireless Network Security permite um acesso rápido às informações de segurança sem fios, incluindo a chave actual para uma rede sem fios protegida.

Para ver a chave actual:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.
3. No painel Estado da Rede Sem Fios, no painel Rede Sem Fios Protegida, clique em **Chave Actual**.

   A chave configurada para a rede é apresentada na caixa de diálogo Configuração da Chave.

Tópicos relacionados

- **Ver o número de rotações da chave** (página 126)

Rodar chaves automaticamente

A rotação automática da chave está activada por predefinição. No entanto, se suspender a rotação da chave, um computador com acesso administrativo poderá reactivá-la posteriormente.

É possível configurar o Wireless Network Security para efectuar automaticamente a rotação da chave de segurança da rede sem fios protegida.

O Wireless Network Security gera automaticamente um conjunto infinito de chaves fortes, o qual é sincronizado na rede. A ligação sem fios pode ser interrompida por breves instantes quando o router sem fios for reiniciado com a nova configuração de chave de segurança, mas normalmente esta acção não é detectada pelos utilizadores da rede.

Se não estiverem ligados computadores à rede, a rotação da chave ocorre depois de o primeiro estabelecer ligação.

Para activar a rotação automática da chave:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel Segurança da Rede, seleccione a opção **Activar rotação automática da chave.**

   Também poderá retomar a rotação da chave a partir do painel Estado da Rede Sem Fios.
4. Clique em **Aplicar**.

Nota: Por predefinição, a rotação da chave ocorre automaticamente de três em três horas, mas pode ajustar a respectiva frequência de forma a cumprir os seus requisitos de segurança.

Tópicos relacionados

- **Ajustar a frequência de rotação da chave** (página 111)
- **Retomar a rotação da chave** (página 111)
- **Ver o número de rotações da chave** (página 126)

Retomar a rotação da chave

Apesar da rotação automática da chave estar activada por predefinição, um computador com acesso administrativo pode retomar a rotação após a respectiva suspensão.

Para retomar a rotação da chave:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.
3. No painel Estado da Rede Sem Fios, clique em **Retomar Rotação da Chave**.

   Os alertas Começou a Rotação da Chave e Chave de Segurança Rodada confirmam que a rotação da chave foi iniciada e efectuada com êxito.

Tópicos relacionados

- **Rodar chaves automaticamente** (página 110)
- **Suspender rotação automática da chave** (página 113)
- **Ver o número de rotações da chave** (página 126)

Ajustar a frequência de rotação da chave

Se o Wireless Network Security estiver configurado para efectuar automaticamente a rotação da chave de segurança da rede sem fios protegida, poderá ajustar o período em que ocorrerá a rotação, variando entre quinze minutos e quinze dias.

A McAfee recomenda que a rotação da chave de segurança seja efectuada diariamente.

Para ajustar a frequência de rotação da chave automática:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel Segurança da Rede, confirme se a rotação automática da chave está activada e, em seguida, mova a barra de deslocamento **Frequência** para uma das seguintes definições:
   - **a cada 15 minutos**
   - **a cada 30 minutos**
   - **a cada 1 hora**
   - **a cada 3 horas**
   - **a cada 12 horas**

- **a cada 1 dia**
- **a cada 7 dias**
- **a cada 15 dias**

4 Clique em **Aplicar**.

Nota: Certifique-se de que a rotação automática da chave está activada antes de definir a frequência de rotação da chave.

Tópicos relacionados

- **Activar rotação automática da chave** (página 110)
- **Ver o número de rotações da chave** (página 126)

Suspender rotação automática da chave

A rotação da chave pode ser suspendida por qualquer computador ligado à rede sem fios. Poderá suspender a rotação da chave para efectuar as seguintes acções:

- Permitir o acesso à rede a um convidado e a qualquer utilizador que não tenha o Wireless Network Security instalado
- Permitir o acesso a um sistema não Windows, como, por exemplo, Macintosh, Linux ou TiVo. Depois de parar a rotação da chave, anote a chave e introduza-a no novo dispositivo.
- Permitir uma ligação sem fios que não seja interrompida por rotações de chaves para determinados programas, tais como jogos online.
- Deverá retomar a rotação automática da chave o mais rapidamente possível para assegurar que a rede está totalmente protegida contra hackers.

Para ver a chave actual:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.
3. No painel Estado da Rede Sem Fios, no painel Rede Sem Fios Protegida, clique em **Chave Actual**. Anote a chave apresentada na caixa de diálogo Configuração da Chave. Outros computadores que não tenham o Wireless Network Security instalado poderão utilizar esta chave para ligar à rede sem fios protegida.
4. Na caixa de diálogo Configuração da Chave, clique em **Suspender Rotação da Chave**.
5. Na caixa de diálogo Rotação da Chave Suspensa, clique em **OK** para continuar a trabalhar.

Aviso: Se a rotação da chave não for suspensa, os dispositivos sem fios não suportados que forem ligados manualmente à rede serão desligados quando for efectuada a rotação da chave.

Poderá criar um disco do Windows Connect Now e, em seguida, utilizar o ficheiro de texto para copiar e colar a chave no outro computador e dispositivo.

Tópicos relacionados

- **Activar rotação automática da chave** (página 110)
- **Adicionar computadores utilizando a tecnologia Windows Connect Now** (página 88)

- **Retomar a rotação da chave** (página 111)
- **Rodar chaves automaticamente** (página 110)
- **Ver o número de rotações da chave** (página 126)

Rodar chaves de rede manualmente

O Wireless Network Security permite rodar uma chave de rede manualmente, mesmo quando a rotação automática da chave estiver activada.

Para rodar uma chave de rede manualmente:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Ferramentas**.
3. No painel Ferramentas, clique em **Ferramentas de Manutenção**.
4. Na página Ferramentas de Manutenção, em **Rodar Chave de Segurança Manualmente**, clique em **Rodar**.

   O alerta Começou a Rotação da Chave é apresentado e confirma que a rotação da chave foi iniciada. Após a rotação da chave de segurança, o alerta Chave de Segurança Rodada é apresentado, confirmando que a rotação da chave foi efectuada com êxito.

Nota: Para facilitar a gestão das chaves de segurança, é possível activar automaticamente a rotação da chave no painel Segurança da Rede.

Se não estiverem ligados computadores à rede sem fios, a rotação da chave ocorre automaticamente quando o primeiro computador estabelecer ligação.

Tópicos relacionados

- **Activar rotação automática da chave** (página 110)
- **Ajustar a frequência de rotação da chave** (página 111)
- **Ver o número de rotações da chave** (página 126)

Apresentar chaves como asteriscos

Por predefinição, as chaves são apresentadas como asteriscos, mas pode configurar o Wireless Network Security para apresentar as chaves em texto simples em redes que não estejam protegidas pelo Wireless Network Security.

As redes protegidas pelo Wireless Network Security são apresentadas em texto simples.

Para apresentar chaves como asteriscos:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. Clique em **Outras Definições**.
4. Desmarque a caixa **Apresentar as chaves em texto simples**.
5. Clique em **Aplicar**.

Tópicos relacionados

- **Apresentar as chaves em texto simples** (página 116)

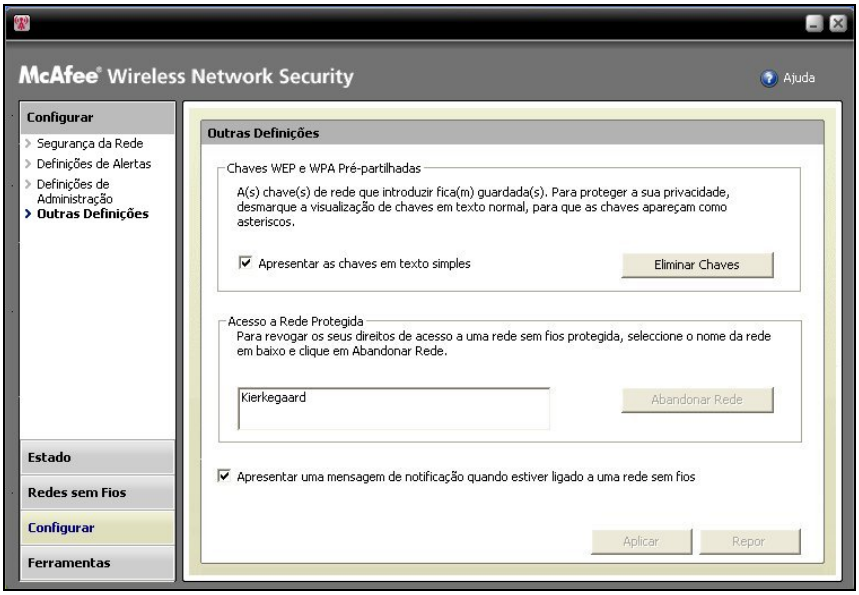
Apresentar as chaves em texto simples

Por predefinição, as chaves são apresentadas como asteriscos, mas pode configurar o Wireless Network Security para apresentar as chaves em texto simples em redes que não estejam protegidas pelo Wireless Network Security.

As redes protegidas pelo Wireless Network Security são apresentadas em texto simples.

Para apresentar as chaves em texto simples:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. Clique em **Outras Definições**.



4. Seleccione a caixa **Apresentar as chaves em texto simples**.
5. Clique em **Aplicar**.

Tópicos relacionados

- **Apresentar chaves como asteriscos** (página 115)

Eliminar chaves de rede

O Wireless Network Security guarda automaticamente as chaves WEP e WPA pré-partilhadas, as quais podem ser eliminadas em qualquer altura.

Para eliminar todas as chaves de rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Configurar Vista**.
3. No painel **Configurar**, clique em **Outras Definições**.
4. No painel **Outras Definições**, em **Chaves WEP e WPA Pré-partilhadas**, clique em **Eliminar Chaves**.
5. Na caixa de diálogo Limpar Chaves, clique em **Sim** se tiver a certeza de que pretende eliminar todas as chaves WEP e WPA pré-partilhadas guardadas.

Aviso: A eliminação das chaves remove-as permanentemente do computador. Depois de eliminar as chaves de rede, será necessário introduzir a chave correcta para ligar a uma rede WEP e WPA.

CAPÍTULO 17

Monitorizar redes sem fios

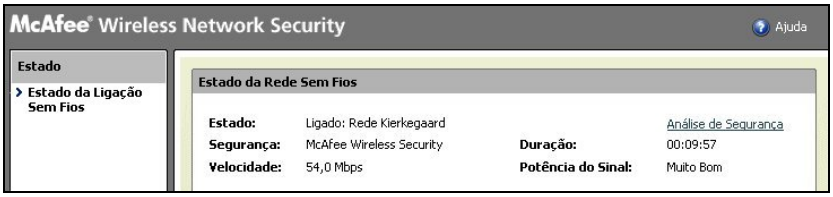
O Wireless Network Security permite monitorizar o estado da rede sem fios e dos computadores protegidos.

Neste capítulo

Monitorizar ligações de rede sem fios 120
Monitorizar redes sem fios protegidas 125
Resolução de problemas..... 131

Monitorizar ligações de rede sem fios

É possível ver o estado da ligação de rede, modo de segurança, velocidade, duração, potência do sinal e um relatório de segurança no painel Estado da Rede Sem Fios.



A tabela seguinte descreve os indicadores de estado para ligações de rede sem fios.

Estado	Descrição	Informações
Estado	Indica se o computador está ligado a uma rede e qual a rede a que está ligado.	**Ver o estado da ligação** (página 121)
Segurança	Apresenta o modo de segurança da rede à qual está ligado. O Wireless Network Security será apresentado se estiver protegido pelo Wireless Network Security.	**Ver o modo de segurança da rede** (página 122)
Velocidade	Indica a velocidade da ligação do computador à rede.	**Ver a velocidade da ligação à rede** (página 122)
Duração	Indica o período de tempo da ligação do computador à rede.	**Ver a duração da ligação à rede** (página 123)
Potência do Sinal	Apresenta a potência de sinal relativa da rede.	**Ver a potência de sinal da rede** (página 124)

Análise de Segurança	Se clicar em **Análise de Segurança**, serão apresentadas informações de segurança, tais como vulnerabilidades de segurança da rede sem fios, problemas de desempenho e o estado da rede sem fios.	**Ver o relatório de segurança online** (página 124)

Tópicos relacionados

- **Acerca dos ícones do Wireless Network Security** (página 92)

Ver o estado da ligação

É possível utilizar o painel Estado da Rede Sem Fios para consultar o estado da ligação à rede, para confirmar se está ligado ou desligado da rede.

Para ver o estado da ligação sem fios:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   Os computadores ligados à rede sem fios protegida e a hora e a data de ligação de cada um são apresentados no painel Estado da Rede Sem Fios, em **Computadores**.

Tópicos relacionados

- **Monitorizar ligações de rede sem fios** (página 120)
- **Ver o modo de segurança da rede** (página 122)
- **Ver a velocidade da ligação à rede** (página 122)
- **Ver a duração da ligação à rede** (página 123)
- **Ver a potência de sinal da rede** (página 124)
- **Ver o relatório de segurança online** (página 124)

Ver o modo de segurança da rede

É possível utilizar o painel Estado da Rede Sem Fios para consultar o modo de segurança da ligação à rede.

Para ver o modo de segurança da rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   O modo de segurança é apresentado no painel Estado da Rede Sem Fios, na caixa **Segurança**.

   O Wireless Network Security será apresentado se a rede sem fios estiver protegida pelo Wireless Network Security.

Tópicos relacionados

- **Monitorizar ligações de rede sem fios** (página 120)
- **Ver o estado da ligação** (página 121)
- **Ver a velocidade da ligação à rede** (página 122)
- **Ver a duração da ligação à rede** (página 123)
- **Ver a potência de sinal da rede** (página 124)
- **Ver o relatório de segurança online** (página 124)

Ver a velocidade da ligação à rede

É possível utilizar o painel Estado da Rede Sem Fios para consultar a velocidade da ligação do computador à rede.

Para ver a velocidade da ligação à rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   A velocidade de ligação é apresentada no painel Estado da Rede Sem Fios, na caixa **Velocidade**.

Tópicos relacionados

- **Monitorizar ligações de rede sem fios** (página 120)
- **Ver o estado da ligação** (página 121)
- **Ver o modo de segurança da rede** (página 122)
- **Ver a duração da ligação à rede** (página 123)
- **Ver a potência de sinal da rede** (página 124)
- **Ver o relatório de segurança online** (página 124)

Ver a duração da ligação à rede

É possível utilizar o painel Estado da Rede Sem Fios para consultar o tempo de ligação à rede.

Para ver a duração da ligação à rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   O tempo de ligação do computador à rede sem fios é apresentado na caixa **Duração**.

Tópicos relacionados

- **Monitorizar ligações de rede sem fios** (página 120)
- **Ver o estado da ligação** (página 121)
- **Ver o modo de segurança da rede** (página 122)
- **Ver a velocidade da ligação à rede** (página 122)
- **Ver a potência de sinal da rede** (página 124)
- **Ver o relatório de segurança online** (página 124)

Ver a potência de sinal da rede

É possível utilizar o painel Estado da Rede Sem Fios para consultar a potência de sinal da rede.

Para ver a potência de sinal:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   A qualidade do sinal é apresentada na caixa **Potência do Sinal**.

Tópicos relacionados

- **Monitorizar ligações de rede sem fios** (página 120)
- **Ver o estado da ligação** (página 121)
- **Ver o modo de segurança da rede** (página 122)
- **Ver a velocidade da ligação à rede** (página 122)
- **Ver a duração da ligação à rede** (página 123)
- **Ver o relatório de segurança online** (página 124)

Ver o relatório de segurança online

É possível utilizar o painel Estado da Rede Sem Fios para ver um relatório sobre a ligação sem fios, quer seja segura ou não segura.

A página Web do McAfee Wi-FiScan apresenta informações sobre as vulnerabilidades de segurança da rede sem fios, problemas de desempenho, informações sobre a ligação sem fios, uma solução de segurança recomendada e indica se a ligação é segura.

Antes de ver o relatório de segurança, certifique-se de que tem uma ligação à Internet.

Para ver um relatório de segurança online sobre a rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.
3. No painel Estado da Rede Sem Fios, clique em **Análise de Segurança**.

   Depois de o browser ser aberto, terá de transferir e instalar um componente ActiveX. Consoante a configuração do browser, este poderá bloquear o controlo. Permita que o browser transfira o componente e, em seguida, execute-o para iniciar a análise. Dependendo da velocidade da ligação à Internet, a análise poderá demorar algum tempo.

Nota: Consulte a documentação do browser para obter informações sobre a transferência de componentes ActiveX.

O Wi-FiScan da McAfee suporta o Internet Explorer 5.5 e versões posteriores.

Tópicos relacionados

- **Monitorizar ligações de rede sem fios** (página 120)
- **Ver o estado da ligação** (página 121)
- **Ver o modo de segurança da rede** (página 122)
- **Ver a velocidade da ligação à rede** (página 122)
- **Ver a duração da ligação à rede** (página 123)
- **Ver a potência de sinal da rede** (página 124)

Monitorizar redes sem fios protegidas

O Wireless Network Security permite ver o número de ligações, rotações de chaves e computadores protegidos no painel Estado da Rede Sem Fios. Também poderá ver os eventos da rede, chave actual e computadores actualmente protegidos.

A tabela seguinte descreve os indicadores de estado para ligações de rede sem fios protegida.

Estado	Descrição	Informações
Rotações da chave hoje	Indica o número diário de rotações da chave na rede sem fios protegida.	**Ver o número de rotações da chave** (página 127)
Ligações hoje	Indica o número diário de ligações à rede protegida.	**Ver o número de ligações diárias** (página 127)
Computadores protegidos este mês	Indica o número de computadores protegidos referente ao mês actual.	**Ver o número de computadores protegidos mensalmente** (página 127)
Eventos da Rede	Se clicar em **Eventos da Rede**, serão apresentados os eventos da rede, ligação e rotação da chave.	**Ver eventos da rede sem fios protegida** (página 128)
Computadores	Indica o número de computadores ligados à rede sem fios protegida e quando foi ligado cada computador.	**Ver computadores actualmente protegidos** (página 129)

Ver o número de rotações da chave

O Wireless Network Security permite ver o número diário de rotações da chave ocorridas na rede protegida e quando foi efectuada a última rotação da chave.

Para ver o número diário de rotações da chave:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   O número total de ligações e a rotação da chave mais recente são apresentados no painel Estado da Rede Sem Fios, em **Rede Sem Fios Protegida**, no campo **Rotações da chave hoje**.

Tópicos relacionados

- **Monitorizar redes sem fios protegidas** (página 125)
- **Ver o número de ligações diárias** (página 127)
- **Ver o número de computadores protegidos mensalmente** (página 127)
- **Ver eventos da rede sem fios protegida** (página 128)
- **Ver computadores actualmente protegidos** (página 129)
- **Administrar chaves de rede** (página 109)
- **Rodar chaves automaticamente** (página 110)
- **Rodar chaves de rede manualmente** (página 114)

Ver o número de ligações diárias

O Wireless Network Security permite ver o número diário de ligações à rede protegida.

Para ver as ligações à rede sem fios protegida:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.

   O número total de ligações é apresentado no painel Estado da Rede Sem Fios, em **Rede Sem Fios Protegida**, na caixa **Ligações hoje**.

Tópicos relacionados

- **Monitorizar redes sem fios protegidas** (página 125)
- **Ver o número de computadores protegidos mensalmente** (página 127)
- **Ver eventos da rede sem fios protegida** (página 128)
- **Ver computadores actualmente protegidos** (página 129)

Ver o número de computadores protegidos mensalmente

O Wireless Network Security permite ver o número de computadores protegidos referente ao mês actual.

Para ver o número de computadores protegidos referente ao mês actual:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Seleccione **Ver Estado**.
3. O número de computadores protegidos durante o mês actual é apresentado no painel Estado da Rede Sem Fios, em **Rede Sem Fios Protegida**, na caixa **Computadores protegidos este mês**.

Tópicos relacionados

- **Monitorizar redes sem fios protegidas** (página 125)
- **Ver o número de rotações da chave** (página 127)
- **Ver o número de ligações diárias** (página 127)
- **Ver eventos da rede sem fios protegida** (página 128)
- **Ver computadores actualmente protegidos** (página 129)

Ver eventos da rede sem fios protegida

O Wireless Network Security regista os eventos na rede sem fios, como, por exemplo, quando é efectuada a rotação das chaves de segurança, quando outros computadores estabelecem ligação e aderem à rede protegida da McAfee.

O Wireless Network Security permite ver um relatório que descreve os eventos ocorridos na rede. Poderá especificar os tipos de eventos a apresentar e ordenar as respectivas informações com base na data, evento ou computador.

Para ver eventos da rede:

1. Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.
2. Efectue um dos seguintes procedimentos:

Para...	Efectue o seguinte...
Ver eventos da rede a partir do painel Estado da Rede Sem Fios	1. Seleccione **Ver Estado**. 2. No painel Estado da Rede Sem Fios, em **Rede Sem Fios Protegida**, clique em **Eventos da Rede**.
Ver eventos da rede a partir do painel Estado da Rede Sem Fios	1. Clique em **Ver Ferramentas**. 2. No painel Ferramentas, clique em **Ferramentas de Manutenção**. 3. No painel Ferramentas de Manutenção, em **Ver o Registo de Eventos**, clique em **Ver**.

3. Seleccione um ou vários dos seguintes eventos para serem apresentados:
   - **Eventos da Rede**: Apresenta informações sobre a actividade da rede, como, por exemplo, a protecção de um router ou ponto de acesso sem fios.
   - **Eventos de Ligação**: Apresenta informações sobre as ligações à rede, tais como a data e a hora de ligação de um computador à rede.
   - **Eventos de Rotação da Chave**: Apresenta informações sobre as datas e horas das rotações da chave de segurança.

4 Clique em **Fechar**.

Tópicos relacionados

- **Monitorizar redes sem fios protegidas** (página 125)
- **Ver o número de rotações da chave** (página 127)
- **Ver o número de ligações diárias** (página 127)
- **Ver o número de ligações diárias** (página 127)
- **Ver computadores actualmente protegidos** (página 129)

Ver computadores actualmente protegidos

É possível ver o número de computadores ligados à rede sem fios protegida e quando foi ligado cada computador pela última vez.

Para ver os computadores ligados à rede protegida:

1 Clique com o botão direito do rato no ícone do Wireless Network Security na área de Notificação do Windows.

2 Seleccione **Ver Estado**.

3 Os computadores ligados à rede sem fios protegida, e a hora e a data de ligação mais recente de cada um, são apresentados no painel Estado da Rede Sem Fios, em **Computadores**.

Tópicos relacionados

- **Monitorizar redes sem fios protegidas** (página 125)
- **Ver o número de rotações da chave** (página 127)
- **Ver o número de ligações diárias** (página 127)
- **Ver o número de computadores protegidos mensalmente** (página 127)
- **Ver eventos da rede sem fios protegida** (página 128)

CAPÍTULO 18

Resolução de problemas

É possível resolver problemas quando utilizar o Wireless Security e equipamento de terceiros, incluindo:

- Dificuldades de instalação
- Não é possível proteger ou configurar a rede
- Não é possível ligar computadores à rede
- Não é possível ligar a uma rede ou à Internet
- Outros problemas

Neste capítulo

Instalar o Wireless Network Security 132
Proteger ou configurar a rede 134
Ligar computadores à rede 137
Estabelecer ligação à Internet e à rede 139
Outros problemas 143

Instalar o Wireless Network Security

É possível resolver os problemas de instalação que se seguem.

- Computadores nos quais o software deve ser instalado
- Placa sem fios não detectada
- Várias placas sem fios
- Não é possível efectuar transferências em computadores sem fios porque a rede já está protegida

Computadores nos quais o software deve ser instalado

Instale o Wireless Network Security em todos os computadores sem fios existentes na rede (contrariamente aos outros programas da McAfee, este software pode ser instalado em vários computadores). Cumpra o contrato de licença do software adquirido. Em alguns casos, poderá ser necessário adquirir licenças adicionais.

Pode (mas não necessita de) instalar o software nos computadores que não estão equipados com placas sem fios, mas o software não estará activo nesses computadores porque eles não necessitam de protecção sem fios.

O Wireless Network Security é suportado actualmente pelo Windows XP ou Windows 2000.

Placa sem fios compatível não detectada

Se a placa sem fios não for detectada após ter sido instalada e activada, reinicie o computador. Se a placa continuar a não ser detectada após reiniciar o computador, siga estes passos.

1. Inicie a caixa de diálogo Propriedades de Ligação de Rede Sem Fios do Windows.
2. Através da vista clássica do menu Iniciar do Windows, clique em **Iniciar**, aponte para **Definições** e, em seguida, seleccione **Ligações de Rede**.
3. Clique no ícone **Ligação de Rede Sem Fios**.
4. Na caixa de diálogo Estado da Ligação de Rede Sem Fios, clique em **Propriedades**.
5. No painel Propriedades de Ligação de Rede Sem Fios, desmarque a opção **Filtro MWL** e, em seguida, seleccione-a novamente.

6. Clique em **OK**.

   Se este procedimento não resolver o problema, verifique executando o WiFiScan. Se o WiFiScan funcionar, a placa é suportada. Caso contrário, actualize o controlador da placa (utilize o Windows Update ou visite o Web site do fabricante) ou adquira um novo dispositivo.

Tópicos relacionados

- **Ver o relatório de segurança online** (página 124)

Várias placas sem fios

Se um erro indicar que tem várias placas de rede instaladas, terá de desactivar ou desligar uma delas. O Wireless Home Network Security só funciona com uma placa de rede.

Falha ao transferir na rede segura

Se tiver um CD de instalação, instale o Wireless Network Security a partir desse CD em todos os computadores sem fios.

Se tiver instalado o software num computador sem fios e tiver protegido a rede antes de instalar o software em todos os outros computadores sem fios, tem as seguintes opções.

- Cancele a protecção da rede. Em seguida, transfira o software e instale-o em todos os computadores sem fios. Proteja novamente a rede.
- Veja a chave de rede. Em seguida, introduza a chave no computador sem fios para estabelecer ligação à rede. Transfira e instale o software e, em seguida, adira à rede a partir do computador sem fios.
- Transfira o ficheiro executável para o computador que já está ligado à rede e guarde-o numa unidade flash USB ou grave-o num CD para o poder instalar nos outros computadores.
- Execute a tecnologia Windows Connect Now.

Tópicos relacionados

- **Remover routers ou pontos de acesso sem fios** (página 99)
- **Ver chaves actuais** (página 109)
- **Adicionar computadores utilizando um dispositivo amovível** (página 86)
- **Adicionar computadores utilizando a tecnologia Windows Connect Now** (página 88)

Proteger ou configurar a rede

É possível resolver os seguintes problemas quando proteger ou configurar a rede.

- Router ou ponto de acesso não suportado
- Actualizar o firmware do router ou ponto de acesso
- Erro de administrador duplicado
- A rede aparece como não protegida
- Não é possível reparar

Router ou ponto de acesso não suportado

Se um erro indicar que é possível que o router ou ponto de acesso sem fios não seja suportado, o Wireless Network Security não conseguiu configurar o dispositivo porque não o reconheceu ou não o localizou.

Verifique se tem a versão mais recente do Wireless Network Security solicitando uma actualização (a McAfee adiciona constantemente suporte para novos routers e pontos de acesso). Se o router ou ponto de acesso constar da lista de routers suportados e, mesmo assim, receber este erro, o problema está relacionado com erros de comunicação entre o computador e o router ou ponto de acesso.

Tópicos relacionados

- **Routers sem fios suportados**
  http://www.mcafee.com/router

Actualizar o firmware do router ou ponto de acesso

Se um erro indicar que a revisão de firmware do seu router ou ponto de acesso sem fios não é suportada, isso significa que o dispositivo é suportado mas a versão do respectivo firmware não é suportada. Verifique se tem a versão mais recente do Wireless Network Security solicitando uma actualização (a McAfee adiciona constantemente suporte para novas revisões de firmware).

Se tiver a versão mais recente do Wireless Network Security, visite o Web site do fabricante do router ou ponto de acesso, ou contacte a respectiva organização de suporte, e instale uma versão que seja apresentada na lista de routers suportados.

Tópicos relacionados

- **Routers sem fios suportados**
  http://www.mcafee.com/router

Erro de administrador duplicado

Depois de configurar o router ou ponto de acesso, tem de terminar sessão na interface de administração. Em alguns casos, caso não termine a sessão, o router ou ponto de acesso age como se ainda estivesse a ser configurado por outro computador e é apresentada uma mensagem de erro.

Se não conseguir terminar a sessão, desligue a alimentação do router ou ponto de acesso e, em seguida, ligue-a novamente.

Ocorreu uma falha na rotação da chave

A rotação da chave falhou porque:

- As informações de início de sessão do router ou ponto de acesso foram alteradas.
- A versão de firmware do router ou ponto de acesso foi alterada para uma versão que não é suportada.
- O router ou ponto de acesso não está disponível. Certifique-se de que o router ou ponto de acesso está ligado e de que está ligado à rede.
- Erro de administrador duplicado.
- Para alguns routers sem fios, se a sessão de outro computador for iniciada manualmente na interface Web do router sem fios, o cliente McAfee poderá não conseguir aceder à interface de gestão para efectuar a rotação da chave de encriptação.

Tópicos relacionados

- **Alterar credenciais de dispositivos sem fios** (página 107)
- **Rodar chaves automaticamente** (página 110)

Não é possível reparar o router ou ponto de acesso

Se a reparação falhar, tente os seguintes procedimentos. Repare que cada procedimento é independente.

- Estabeleça ligação à rede utilizando um cabo e, em seguida, tente efectuar a reparação novamente.
- Desligue a alimentação do router ou ponto de acesso, ligue-a novamente e, em seguida, tente estabelecer ligação.
- Reponha as predefinições do router ou ponto de acesso sem fios e efectue a reparação. Ao efectuar este procedimento, irá repor as definições da ligação sem fios para as definições originais. Em seguida, reponha as definições de ligação à Internet.
- Utilizando as opções avançadas, isole a rede de todos os computadores, reponha as predefinições do router ou ponto de acesso sem fios e, em seguida, proteja a rede. Este procedimento repõe as definições da ligação sem fios para as definições originais. Em seguida, reponha as definições de ligação à Internet.

Tópicos relacionados

- **Reparar definições de segurança da rede** (página 108)

As redes aparecem desprotegidas

Se a rede é apresentada como não protegida, é porque está vulnerável. Tem de proteger a rede para garantir a respectiva segurança. Tenha em atenção que o Wireless Network Security só funciona com routers e pontos de acesso compatíveis.

Tópicos relacionados

- **Criar redes sem fios protegidas** (página 76)
- **Routers sem fios suportados**
  http://www.mcafee.com/router

Ligar computadores à rede

É possível resolver os seguintes problemas quando ligar computadores à rede.

- A aguardar autorização
- Conceder acesso a um computador desconhecido

A aguardar autorização

Se tentar aderir a uma rede protegida e o seu computador permanecer a aguardar autorização, verifique o seguinte.

- Um computador que já tem acesso à rede está ligado e possui uma ligação activa à rede.
- Está alguém a utilizar esse computador quando o pedido de autorização é apresentado.
- Os computadores encontram-se dentro do alcance da rede sem fios.

Se **Conceder Acesso** não for apresentado no computador que já tem acesso à rede, tente conceder o acesso a partir de outro computador.

Se não existirem outros computadores disponíveis, cancele a protecção da rede a partir do computador que já tem acesso e proteja a rede a partir do computador que não obteve acesso. Em seguida, adira à rede a partir do computador que protegia originalmente a rede.

Também poderá utilizar a funcionalidade Proteger Outro Computador.

Tópicos relacionados

- **Aderir a uma rede sem fios protegida** (página 78)
- **Sair de redes sem fios protegidas** (página 102)
- **Remover routers ou pontos de acesso sem fios** (página 99)
- **Adicionar computadores à rede sem fios protegida** (página 86)

Conceder acesso a um computador desconhecido

Quando receber um pedido de acesso proveniente de um computador desconhecido, recuse-o até conseguir confirmar a respectiva legitimidade. É possível que alguém esteja a tentar aceder ilegitimamente à sua rede.

Estabelecer ligação à Internet e à rede

É possível resolver os seguintes problemas quando estabelecer ligação a uma rede ou à Internet.

- Má ligação à Internet
- A ligação pára por breves instantes
- Os dispositivos (que não o seu computador) perdem a ligação
- Pedido de introdução da chave WEP, WPA ou WPA2
- Não é possível estabelecer ligação
- Actualizar a placa sem fios
- Nível de sinal fraco
- O Windows não consegue configurar a ligação sem fios
- O Windows não indica a ligação

Não é possível estabelecer ligação à Internet

Se não conseguir estabelecer ligação, tente aceder à rede utilizando um cabo e, em seguida, aceda à Internet. Se mesmo assim não conseguir estabelecer ligação, verifique se:

- O modem está ligado
- As definições de PPPoE estão correctas
- A linha de DSL ou cabo está activa

Alguns problemas de conectividade, tais como os problemas de velocidade e potência do sinal, também podem ser causados por interferências. Experimente os seguintes métodos para corrigir o problema:

- Altere o canal do telefone sem fios
- Elimine as possíveis origens de interferência
- Altere a localização do router sem fios, ponto de acesso ou computador.
- Altere o canal do router ou ponto de acesso. Os canais 1, 4, 7 e 11 são recomendados para a América do Norte e do Sul. Os canais 1, 4, 7 e 13 são recomendados para outros países. Por predefinição, muitos routers estão definidos para o canal 6.
- Certifique-se de que o router e a placa sem fios (sobretudo uma placa USB sem fios) não estão virados em direcção a uma parede
- Assegure-se de que a placa USB sem fios não está junto a um ponto de acesso/router sem fios.
- Posicione o router de forma a ficar afastado de paredes e metal

Ligação interrompida

Quando a ligação for interrompida durante breves instantes (por exemplo, durante um jogo online), a causa poderá ser a rotação da chave. Para evitar esta situação, poderá suspender a rotação da chave.

A McAfee recomenda que retome a rotação da chave o mais rapidamente possível, para garantir que a sua rede está totalmente protegida dos hackers.

Tópicos relacionados

- **Rodar chaves automaticamente** (página 110)
- **Retomar a rotação da chave** (página 111)
- **Suspender rotação automática da chave** (página 113)
- **Rodar chaves de rede manualmente** (página 114)

Os dispositivos perdem a conectividade

Se alguns dispositivos perderem a ligação quando utilizar o Wireless Network Security, tente corrigir o problema utilizando os seguintes métodos:

- Suspenda a rotação da chave
- Actualize o controlador da placa sem fios
- Desactive o gestor cliente da placa

Tópicos relacionados

- **Suspender rotação automática da chave** (página 113)

Pedido de introdução da chave WEP, WPA ou WPA2

Se tiver de introduzir uma chave WEP, WPA ou WPA2 para estabelecer ligação à rede sem fios protegida, é provável que não tenha instalado o software no computador.

Para funcionar correctamente, o Wireless Network Security tem de estar instalado em todos os computadores sem fios existentes na rede.

Tópicos relacionados

- **Iniciar o Wireless Network Security** (página 70)
- **Adicionar computadores à rede sem fios protegida** (página 86)

Não é possível estabelecer ligação à rede sem fios

Se não conseguir estabelecer ligação, tente os seguintes procedimentos. Repare que cada procedimento é independente.

- Se não estiver ligado a uma rede protegida, verifique se tem a chave correcta e introduza-a novamente.
- Desligue a placa sem fios e ligue-a novamente, ou desactive-a e reactive-a.
- Desligue o router ou ponto de acesso, ligue-o novamente e, em seguida, tente estabelecer ligação.
- Verifique se o router ou ponto de acesso sem fios está ligado e repare as definições de segurança.
- Reinicie o computador.
- Actualize a placa sem fios ou compre uma nova. Por exemplo, a sua rede pode estar a utilizar a segurança WPA-PSK TKIP e a placa sem fios pode não suportar esse modo de segurança (as redes indicam WEP, apesar de estarem configuradas para WPA).
- Se não conseguir estabelecer ligação depois de ter actualizado o router ou ponto de acesso sem fios, é possível que o tenha actualizado para uma versão não suportada. Verifique se o router ou ponto de acesso é suportado. Se não for suportado, reponha uma versão anterior suportada ou aguarde até que esteja disponível uma actualização do Wireless Network Security.

Tópicos relacionados

- **Reparar definições de segurança da rede** (página 108)
- **Actualizar a placa sem fios** (página 141)

Actualizar a placa sem fios

Poderá ser necessário actualizar a placa sem fios para que seja possível utilizar o Wireless Network Security.

Para actualizar a placa:

1. No ambiente de trabalho, clique em **Iniciar**, aponte para **Definições** e, em seguida, seleccione **Painel de Controlo**.
2. Faça duplo clique no ícone **Sistema**. É apresentada a caixa de diálogo **Propriedades do Sistema**.
3. Seleccione o separador **Hardware** e, em seguida, clique em **Gestor de Dispositivos**.
4. Na lista do Gestor de Dispositivos, faça duplo clique na placa.
5. Seleccione o separador **Controlador** e anote a versão do controlador que está instalada.
6. Aceda ao Web site do fabricante da placa para localizar uma actualização. Os controladores encontram-se normalmente

nas secções Support (Suporte) ou Downloads (Transferências). Se estiver a utilizar uma placa miniPCI, aceda ao Web site do fabricante do computador e não da placa.

7 Se existir uma actualização, siga as instruções existentes no Web site para a transferir.

8 Regresse ao separador **Controlador** e clique em **Actualizar Controlador**. É apresentado um assistente do Windows.

9 Para instalar o controlador, siga as instruções apresentadas no Web site.

Nível de sinal fraco

Se a ligação for interrompida ou estiver lenta, é possível que o nível de sinal não seja suficientemente forte. Para melhorar o sinal, tente os seguintes procedimentos:

- Certifique-se de que os dispositivos sem fios não estão bloqueados por objectos de metal, tais como fornos, condutas ou electrodomésticos de grandes dimensões. Os sinais sem fios não viajam bem através destes objectos.
- Se o sinal tiver de passar através de paredes, certifique-se de que não atravessa as paredes num ângulo demasiado aberto. Quanto maior for a distância percorrida pelo sinal no interior da parede, mais fraco fica.
- Se o router ou ponto de acesso sem fios tiver mais de uma antena, tente orientar as duas antenas perpendicularmente entre si (uma na vertical e outra na horizontal, com um ângulo de 90 graus).
- Alguns fabricantes dispõem de antenas de alto ganho. As antenas direccionais proporcionam maior alcance, enquanto que as antenas omnidireccionais proporcionam maior versatilidade. Consulte as instruções do fabricante para instalar a antena.

Se estes passos não tiverem êxito, adicione um Ponto de Acesso que esteja mais perto do computador a que está a tentar aceder. Se configurar o segundo ponto de acesso com o mesmo nome de rede (SSID) e um canal diferente, o adaptador irá localizar automaticamente o sinal mais forte e aceder através do ponto de acesso adequado.

Tópicos relacionados

- **Ícones de potência de sinal** (página 93)
- **Ver a potência de sinal da rede** (página 123)

O Windows não suporta a ligação sem fios

Se uma mensagem de erro do Windows indicar que não é possível configurar a ligação sem fios, poderá ignorá-la. Utilize o Wireless Network Security para estabelecer ligação e configurar redes sem fios.

Na caixa de diálogo Propriedades de Ligação de Rede Sem Fios do Windows, no separador Redes Sem Fios, certifique-se de que a caixa de verificação **Utilizar o Windows para configurar as definições de rede sem fios** está desmarcada.

O Wireless Network Security permite ter:

- Placas instaladas em computadores com o Windows 2000 para ligar a redes WPA, apesar de o gestor cliente da placa não ser suportado.
- Placas em computadores com o Windows XP para ligar a redes WPA2 sem ser necessário localizar e instalar a correcção Win XP SP2
- Placas no Windows XP SP1 para ligar a redes WPA e WPA2 sem ser necessário localizar e instalar uma correcção, a qual não é suportada pelo Windows XP SP1.

O Windows não indica a ligação

Se tiver uma ligação estabelecida e o ícone de Rede do Windows apresentar um X (sem ligação), ignore-o. A ligação está estabelecida.

Outros problemas

É possível resolver os problemas que se seguem.

- O nome da rede é diferente quando são utilizados outros programas
- Ocorre um problema ao configurar routers ou pontos de acesso sem fios
- Substituir computadores
- Seleccionar outro modo de segurança
- O software não funciona após a actualização do sistema operativo

O nome da rede é diferente quando são utilizados outros programas

É normal que o nome da rede seja diferente quando visualizado através de outros programas (por exemplo, _SafeAaf faz parte do nome da rede).

O Wireless Network Security marca as redes protegidas com um código.

Configurar routers ou pontos de acesso sem fios

Se for apresentado um erro quando configura o router ou ponto de acesso ou quando adiciona vários routers à rede, verifique se todos os routers e pontos de acesso têm um endereço IP diferente.

Se o nome do router ou ponto de acesso sem fios for apresentado na caixa de diálogo Proteger Router ou Ponto de Acesso Sem Fios mas obtiver um erro durante a respectiva configuração: Verifique se o router ou ponto de acesso é suportado.

Se o router ou ponto de acesso estiver configurado mas parecer não estar na rede correcta (por exemplo, se não conseguir ver os outros computadores ligados à LAN), verifique se configurou o router ou ponto de acesso adequado e não o do seu vizinho. Desligue a alimentação do router ou ponto de acesso e certifique-se de que a ligação é interrompida. Se tiver configurado o router ou ponto de acesso incorrecto, cancele a protecção e, em seguida, proteja o router ou ponto de acesso correcto.

Se não conseguir configurar ou adicionar o router ou ponto de acesso mas este for suportado, algumas alterações efectuadas poderão estar a impedir a sua correcta configuração.

- Siga as instruções do fabricante para configurar o router ou ponto de acesso sem fios para DHCP ou para configurar o endereço IP correcto. Em alguns casos, o fabricante fornece uma ferramenta de configuração.
- Reponha as definições de fábrica do router ou ponto de acesso e tente reparar a rede novamente. É possível que tenha alterado a porta de administração do router ou ponto de acesso ou que tenha desactivado a administração sem fios. Certifique-se de que está a utilizar a configuração predefinida e de que a configuração sem fios está activada. É ainda possível que a administração HTTP esteja desactivada. Neste caso, verifique se a administração HTTP está activada. Certifique-se de que utiliza a porta 80 para administração.
- Se o router ou ponto de acesso sem fios não for apresentado na lista de routers ou pontos de acesso sem fios que pretende proteger ou estabelecer ligação, active a difusão do SSID e verifique se consegue visualizar o router ou ponto de acesso na lista de redes sem fios disponíveis do Wireless Network Security.
- Se a ligação for interrompida ou não conseguir estabelecer ligação, é possível que a filtragem MAC esteja activada. Desactive a filtragem de endereços MAC.
- Se não conseguir efectuar operações de rede (por exemplo, partilhar ficheiros ou imprimir em impressoras partilhadas) em dois computadores com ligação sem fios à rede, verifique se não activou o Isolamento do Ponto de Acesso. O Isolamento do Ponto de Acesso impede que os computadores consigam interligar-se através da rede.

- Se estiver a utilizar um programa de firewall sem ser o McAfee Personal Firewall, certifique-se de que a sub-rede é fidedigna.

Tópicos relacionados

- **Routers sem fios suportados**
  http://www.mcafee.com/router

Substituir computadores

Se o computador que protegeu a rede tiver sido substituído e nenhum computador tiver acesso (se não conseguir aceder à rede), reponha as predefinições de fábrica do router ou ponto de acesso sem fios e proteja a rede novamente.

Seleccionar outro modo de segurança

Se um erro indicar que seleccionou um modo de segurança não suportado pela placa sem fios, é necessário seleccionar um modo de segurança diferente.

- Todas as placas suportam o modo WEP.
- A maioria das placas que suportam WPA implementam os modos de segurança WPA-PSK TKIP e WPA-PSK AES.
- As placas que suportam WPA2 implementam os modos de segurança WPA, WPA2-PSK TKIP, WPA2-PSK AES e WPA2-PSK TKIP/AES.

Tópicos relacionados

- **Configurar definições de segurança** (página 104)
- **Ver o modo de segurança da rede** (página 122)

O software falha após a actualização do sistema operativo

Se o Wireless Network Security falhar após a actualização do sistema operativo, remova e reinstale o programa.

CAPÍTULO 19

McAfee EasyNetwork

O McAfee® EasyNetwork permite a partilha segura de ficheiros, simplifica as transferências de ficheiros e torna a partilha de impressoras automática entre os computadores da sua rede doméstica.

Antes de começar a utilizar o EasyNetwork, pode familiarizar-se com algumas das funcionalidades mais conhecidas. Na ajuda do EasyNetwork, encontrará informações pormenorizadas sobre como configurar e utilizar essas funcionalidades.

Neste capítulo

Funcionalidades 148
Configurar o EasyNetwork 149
Partilhar e enviar ficheiros 157
Partilhar impressoras 163

Funcionalidades

O EasyNetwork oferece as seguintes funcionalidades.

Partilha de ficheiros

O EasyNetwork facilita a partilha de ficheiros entre o seu computador e outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (isto é, que têm acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros.

Transferência de ficheiros

Pode enviar ficheiros para outros computadores que sejam membros da rede gerida. Quando recebe um ficheiro, este aparece na pasta A receber do EasyNetwork. A pasta A receber é um local de armazenamento temporário para todos os ficheiros que lhe são enviados por outros computadores da rede.

Partilha de impressoras automática

Depois de aderir a uma rede gerida, o EasyNetwork partilha automaticamente todas as impressoras locais ligadas ao seu computador, utilizando o nome actual da impressora como nome de impressora partilhada. Detecta ainda impressoras partilhadas por outros computadores na rede e permite-lhe configurar e utilizar essas impressoras.

CAPÍTULO 20

Configurar o EasyNetwork

Antes de utilizar as funcionalidades do EasyNetwork, tem de iniciar o programa e aderir à rede gerida. Uma vez efectuada a adesão, pode abandonar a rede em qualquer altura.

Neste capítulo

Iniciar o EasyNetwork.....150
Aderir a uma rede gerida 151
Abandonar uma rede gerida.....155

Iniciar o EasyNetwork

Por predefinição, é-lhe solicitado que inicie o EasyNetwork imediatamente após a instalação; no entanto, pode também fazê-lo posteriormente.

Iniciar o EasyNetwork

Por predefinição, é-lhe solicitado que inicie o EasyNetwork imediatamente após a instalação; no entanto, pode também fazê-lo posteriormente.

Para iniciar o EasyNetwork:

- No menu **Iniciar**, seleccione **Programas**, seleccione **McAfee** e, em seguida, clique em **McAfee EasyNetwork**.

Sugestão: Se aceitou criar ícones no ambiente de trabalho e de início rápido durante a instalação, pode igualmente iniciar o EasyNetwork fazendo duplo clique no ícone McAfee EasyNetwork no ambiente de trabalho ou clicando no ícone McAfee EasyNetwork na área de notificação situada à direita da barra de tarefas.

Aderir a uma rede gerida

Depois de instalar o SecurityCenter, é adicionado um agente de rede ao computador que funciona em segundo plano. No EasyNetwork, o agente de rede é responsável por detectar uma ligação de rede válida e impressoras locais para partilhar, bem como por monitorizar o estado da rede.

Se não for encontrado outro computador com o agente de rede na rede à qual está ligado, fica automaticamente membro da rede e é-lhe solicitado que identifique se a rede é fidedigna. Sendo o primeiro computador a aderir à rede, o nome do seu computador é incluído no nome da rede; no entanto, pode alterar o nome da rede em qualquer altura.

Quando um computador acede à rede, é enviado um pedido de adesão a todos os outros computadores actualmente ligados à rede. O pedido pode ser concedido por qualquer computador com permissões administrativas na rede. O concessor pode também determinar o nível de permissão do computador que está a aderir à rede; por exemplo, direitos de convidado (permite apenas a transferências de ficheiros) ou acesso total/administrativo (transferência e partilha de ficheiros). No EasyNetwork, os computadores com acesso administrativo podem conceder acesso a outros computadores e gerir permissões (isto é, promover ou despromover computadores); os computadores com acesso total não podem executar estas tarefas administrativas. Antes de o computador poder efectuar a adesão, é efectuada uma verificação de segurança.

Nota: Depois da adesão, se tiver outros programas de rede da McAfee instalados (por exemplo, McAfee Wireless Network Security ou Network Manager), o computador é reconhecido como um computador gerido nesses programas. O nível de permissão atribuído a um computador aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o significado das permissões de convidado, de acesso total ou administrativo noutros programas de rede da McAfee, consulte a documentação fornecida com o respectivo programa.

Aderir à rede

Quando um computador acede a uma rede fidedigna pela primeira vez depois de instalar o EasyNetwork, é apresentada uma mensagem a perguntar se pretende aderir à rede gerida. Quando o computador aceita aderir, é enviado um pedido a todos os computadores da rede que têm acesso administrativo. Este pedido tem de ser aceite para que o computador possa partilhar impressoras ou ficheiros, enviar e copiar ficheiros da rede. Se o computador for o primeiro computador da rede, adquire automaticamente permissões de administração na rede.

Para aderir à rede:

1. Na janela Ficheiros Partilhados, clique em **Sim, quero aderir à rede agora**.
   Quando um computador com direitos administrativos na rede aceita o pedido, é apresentada uma mensagem a perguntar se este computador e outros computadores da rede estão autorizados a gerir as definições de segurança uns dos outros.
2. Para autorizar este e outros computadores da rede a gerir as definições de segurança uns dos outros, clique em **Sim**; caso contrário, clique em **Não**.
3. Confirme se o computador concessor apresenta as cartas de jogar actualmente apresentadas na caixa de diálogo de confirmação de segurança e, em seguida, clique em **Confirmar**.

Nota: Se o computador concessor não apresentar as mesmas cartas apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. A adesão à rede pode colocar o computador em perigo; por conseguinte, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Conceder acesso à rede

Quando um computador pede para aderir à rede gerida, é enviada uma mensagem aos outros computadores da rede que têm acesso administrativo. O primeiro computador a responder à mensagem passa a ser o concessor. Como concessor, esse computador é responsável por determinar o tipo de acesso a conceder ao computador: convidado, total ou administrativo.

Para conceder acesso à rede:

1. No aviso, seleccione uma das seguintes caixas de verificação:
   - **Conceder acesso de convidado**: Permite que o utilizador envie ficheiros para outros computadores, mas não permite a partilha de ficheiros.

- **Conceder acesso total a todas as aplicações da rede gerida**: Permite que o utilizador envie e partilhe ficheiros.
- **Conceder acesso administrativo a todas as aplicações da rede gerida**: Permite que o utilizador envie e partilhe ficheiros, conceda acesso a outros computadores e ajuste os níveis de permissão de outros computadores.

2 Clique em **Conceder Acesso**.

3 Confirme se o computador apresenta as cartas de jogar actualmente apresentadas na caixa de diálogo de confirmação de segurança e, em seguida, clique em **Confirmar**.

Nota: Se o computador não apresentar as mesmas cartas apresentadas na caixa de diálogo de confirmação de segurança, isso significa que houve uma falha de segurança na rede gerida. Permitir o acesso deste computador à rede pode colocar o seu computador em perigo; por conseguinte, clique em **Rejeitar** na caixa de diálogo de confirmação de segurança.

Mudar o nome da rede

Por predefinição, o nome da rede inclui o nome do primeiro computador que aderiu à rede; no entanto, pode mudar o nome da rede em qualquer altura. Ao mudar o nome da rede, altera a descrição da rede apresentada no EasyNetwork.

Para mudar o nome da rede:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, introduza o nome da rede na caixa **Nome da Rede**.
3. Clique em **OK**.

Abandonar uma rede gerida

Se aderir a uma rede gerida e, posteriormente, decidir que quer deixar de ser membro da rede, pode abandonar a rede. Depois de anular a sua subscrição, pode voltar a aderir à rede em qualquer altura; no entanto, tem novamente de obter permissão para aderir e efectuar a verificação de segurança. Para obter mais informações, consulte **Aderir a uma rede gerida** (página 151).

Abandonar uma rede gerida

Pode abandonar uma rede gerida à qual anteriormente aderiu.

Para abandonar uma rede gerida:

1. No menu **Ferramentas**, clique em **Abandonar Rede**.
2. Na caixa de diálogo Abandonar Rede, seleccione o nome da rede que pretende abandonar.
3. Clique em **Abandonar Rede**.

CAPÍTULO 21

Partilhar e enviar ficheiros

O EasyNetwork permite que ficheiros do seu computador sejam facilmente partilhados e enviados para outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (isto é, que têm acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros.

Neste capítulo

Partilhar ficheiros.....158
Enviar ficheiros para outros computadores.....161

Partilhar ficheiros

O EasyNetwork facilita a partilha de ficheiros entre o seu computador e outros computadores da rede. Ao partilhar ficheiros, está a conceder aos outros computadores acesso apenas de leitura aos ficheiros. Apenas os computadores que são membros da rede gerida (isto é, que têm acesso total ou administrativo) podem partilhar ficheiros ou aceder a ficheiros partilhados por outros membros. Se partilhar uma pasta, todos os ficheiros contidos nessa pasta e respectivas subpastas são partilhados; no entanto, os ficheiros posteriormente adicionados à pasta não são automaticamente partilhados. Se um ficheiro ou uma pasta partilhados forem eliminados, são automaticamente removidos da janela Ficheiros Partilhados. Pode deixar de partilhar um ficheiro em qualquer altura.

Pode aceder a um ficheiro partilhado de duas formas: abrindo o ficheiro directamente a partir do EasyNetwork ou copiando o ficheiro para o seu computador para depois o abrir. Se a sua lista de ficheiros partilhados ficar muito extensa, pode procurar os ficheiros partilhados aos quais pretende aceder.

Nota: Os ficheiros partilhados através do EasyNetwork não podem ser acedidos a partir de outros computadores através do Explorador do Windows. A partilha de ficheiros no EasyNetwork é efectuada com base em ligações seguras.

Partilhar um ficheiro

Quando partilha um ficheiro, este fica automaticamente disponível para todos os outros membros da rede gerida que tenham acesso total ou administrativo.

Para partilhar um ficheiro:

1. No Explorador do Windows, localize o ficheiro que pretende partilhar.
2. Arraste o ficheiro do Explorador do Windows para a janela Ficheiros Partilhados do EasyNetwork.

Sugestão: Pode igualmente partilhar um ficheiro, clicando em **Partilhar Ficheiros** no menu **Ferramentas**. Na caixa de diálogo Partilhar, percorra a pasta onde está guardado o ficheiro que pretende partilhar, seleccione o ficheiro e clique em **Partilhar**.

Interromper a partilha de um ficheiro

Se estiver a partilhar um ficheiro na rede gerida, pode interromper a partilha desse ficheiro em qualquer altura. Quando interrompe a partilha de um ficheiro, os outros membros da rede gerida deixam de ter acesso ao mesmo.

Para interromper a partilha de um ficheiro:

1. No menu **Ferramentas**, seleccione **Parar Partilha de Ficheiros**.
2. Na caixa de diálogo Parar Partilha de Ficheiros, seleccione o ficheiro que já não pretende partilhar.
3. Clique em **Não Partilhar**.

Copiar um ficheiro partilhado

Pode copiar ficheiros partilhados para o seu computador, a partir de qualquer computador da rede gerida. Se o computador interromper a partilha do ficheiro, continua a ter a cópia.

Para copiar um ficheiro:

- Arraste o ficheiro da janela Ficheiros Partilhados do EasyNetwork para uma localização no Explorador do Windows ou para o ambiente de trabalho do Windows.

Sugestão: Pode também copiar um ficheiro partilhado, seleccionando o ficheiro no EasyNetwork e clicando em **Copiar para** no menu **Ferramentas**. Na caixa de diálogo Copiar para a pasta, percorra a pasta até ao local para onde pretende copiar o ficheiro, seleccione-o e clique em **Guardar**.

Procurar um ficheiro partilhado

Pode procurar um ficheiro que tenha sido partilhado por si ou por qualquer outro membro da rede. À medida que digita os seus critérios de procura, o EasyNetwork apresenta automaticamente os resultados correspondentes na janela Ficheiros Partilhados.

Para procurar um ficheiro partilhado:

1. Na janela Ficheiros Partilhados, clique em **Procurar**.
2. Clique numa das seguintes opções da lista **Contém**:
   - **Contém todas as palavras**: Procura nomes de ficheiros ou caminhos que contenham todas as palavras especificadas na lista **Nome do Caminho ou Ficheiro**, por qualquer ordem.

- **Contém qualquer das palavras**: Procura nomes de ficheiros ou caminhos que contenham qualquer uma das palavras especificadas na lista **Nome do Caminho ou Ficheiro**.
- **Contém a cadeia exacta**: Procura nomes de ficheiros ou caminhos que contenham a frase exacta que especificou na lista **Nome do Caminho ou Ficheiro**.

3 Introduza o nome parcial ou completo do ficheiro ou do caminho na lista **Nome do Caminho ou Ficheiro**.

4 Clique num dos seguintes tipos de ficheiro da lista **Tipo**:

- **Qualquer**: Procura todos os tipos de ficheiros partilhados.
- **Documento**: Procura todos os documentos partilhados.
- **Imagem**: Procura todos os ficheiros de imagem partilhados.
- **Vídeo**: Procura todos os ficheiros de vídeo partilhados.
- **Áudio**: Procura todos os ficheiros de som partilhados.

5 Na listas **De** e **Até**, seleccione as datas correspondentes ao intervalo de datas em que o ficheiro foi criado.

Enviar ficheiros para outros computadores

Pode enviar ficheiros para outros computadores que sejam membros da rede gerida. Antes de enviar um ficheiro, o EasyNetwork confirma se o computador de destino tem espaço em disco suficiente.

Quando recebe um ficheiro, este aparece na pasta A receber do EasyNetwork. A pasta A receber é um local de armazenamento temporário para todos os ficheiros que lhe são enviados por outros computadores da rede. Se tiver o EasyNetwork aberto quando receber um ficheiro, o ficheiro aparece de imediato na pasta A receber; caso contrário, aparece uma mensagem na área de notificação situada à direita da barra de tarefas do Windows. Se não quiser receber mensagens de aviso, pode desactivá-las. Se já existir um ficheiro com o mesmo nome na pasta A receber, é acrescentado um sufixo numérico ao nome do novo ficheiro. O ficheiros permanecem na pasta A receber até que os aceite (isto é, até que os copie para uma localização no seu computador).

Enviar um ficheiro para outro computador

Pode enviar um ficheiro directamente para outro computador da rede gerida, sem o partilhar. Para que o utilizador do computador de destino possa ver o ficheiro, tem de o guardar localmente. Para mais informações, consulte **Aceitar um ficheiro de outro computador** (página 162).

Para enviar um ficheiro para outro computador:

1. No Explorador do Windows, localize o ficheiro que pretende enviar.
2. Arraste o ficheiro do Explorador do Windows para o ícone de um computador activo do EasyNetwork.

Sugestão: Pode enviar vários ficheiros para um computador, premindo CTRL quando selecciona os ficheiros. Em alternativa, pode clicar em **Enviar** no menu **Ferramentas**, seleccionar os ficheiros e clicar em **Enviar** para enviar ficheiros.

Aceitar um ficheiro de outro computador

Se outro computador da rede gerida lhe enviar um ficheiro, tem de o aceitar (guardando-o numa pasta do seu computador). Se não tiver o EasyNetwork aberto ou em primeiro plano quando o ficheiro for enviado para o seu computador, receberá uma mensagem de aviso na área de notificação situada à direita da barra de tarefas. Clique na mensagem de aviso para abrir o EasyNetwork e aceder ao ficheiro.

Para receber um ficheiro de outro computador:

- Clique em **Recebidos** e, em seguida, arraste um ficheiro da pasta A receber do EasyNetwork para uma pasta do Explorador do Windows.

Sugestão: Pode também receber um ficheiro de outro computador, seleccionando o ficheiro na pasta A receber do EasyNetwork e clicando em **Aceitar** no menu **Ferramentas**. Na caixa de diálogo Aceitar para a pasta, percorra a pasta até ao local onde pretende guardar os ficheiros recebidos, seleccione-o e clique em **Guardar**.

Receber um aviso de envio de ficheiro

Pode receber um aviso quando outro computador da rede gerida lhe envia um ficheiro. Se o EasyNetwork não estiver aberto nem a funcionar em primeiro plano no ambiente de trabalho, aparece uma mensagem de aviso na área de notificação situada à direita da barra de tarefas do Windows.

Para receber um aviso de envio de ficheiro:

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, seleccione a caixa de verificação **Notificar-me quando outro computador me enviar ficheiros**.
3. Clique em **OK**.

CAPÍTULO 22

Partilhar impressoras

Depois de aderir a uma rede gerida, o EasyNetwork partilha automaticamente todas as impressoras locais ligadas ao seu computador. Detecta ainda impressoras partilhadas por outros computadores na rede e permite-lhe configurar e utilizar essas impressoras.

Neste capítulo

Trabalhar com impressoras partilhadas.....164

Trabalhar com impressoras partilhadas

Depois de aderir a uma rede gerida, o EasyNetwork partilha automaticamente todas as impressoras locais ligadas ao seu computador, utilizando o nome actual da impressora como nome de impressora partilhada. Detecta ainda impressoras partilhadas por outros computadores na rede e permite-lhe configurar e utilizar essas impressoras. Se tiver configurado um controlador de impressão para imprimir através de um servidor de impressão de rede (por exemplo, um servidor de impressão USB sem fios), o EasyNetwork considera a impressora como uma impressora local e partilha-a automaticamente na rede. Pode deixar de partilhar uma impressora em qualquer altura.

O EasyNetwork detecta ainda as impressoras partilhadas por todos os outros computadores da rede. Se for detectada uma impressora remota que ainda não esteja ligada ao seu computador, aparecerá a hiperligação **Impressoras de rede disponíveis** na janela Ficheiros Partilhados, quando abrir o EasyNetwork pela primeira vez. Desta forma, poderá instalar impressoras disponíveis ou desinstalar impressoras que já estejam ligadas ao seu computador. Pode também actualizar a lista de impressoras detectadas na rede.

Se ainda não aderiu à rede gerida, mas estiver ligado a ela, pode aceder às impressoras partilhadas a partir do painel de controlo de impressoras padrão do Windows.

Interromper a partilha de uma impressora

Pode deixar de partilhar uma impressora em qualquer altura. Os membros que instalaram a impressora deixarão de conseguir imprimir através dessa impressora.

Para interromper a partilha de uma impressora:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Gerir Impressoras de Rede, clique no nome da impressora que já não pretende partilhar.
3. Clique em **Não Partilhar**.

Instalar uma impressora de rede disponível

Como membro de uma rede gerida, pode aceder às impressoras partilhadas na rede. Para isso, tem de instalar o controlador de impressora utilizado pela impressora. Se, depois de ter instalado uma impressora, o seu proprietário interromper a partilha, deixa de poder imprimir com essa impressora.

Para instalar uma impressora de rede disponível:

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Impressoras de Rede Disponíveis, clique no nome de uma impressora.
3. Clique em **Instalar**.

CAPÍTULO 23

Referência

O Glossário de Termos apresenta e define a terminologia de segurança mais utilizada que pode encontrar nos produtos da McAfee.

Acerca da McAfee fornece informações jurídicas sobre a McAfee Corporation.

Glossário

8

802.11

Um conjunto de normas da IEEE para a tecnologia de LAN sem fios. A 802.11 especifica uma interface via rádio entre um cliente sem fios e uma estação base ou entre dois clientes sem fios. As várias especificações da 802.11 incluem a 802.11a, uma norma para redes até 54 Mbps na banda de frequências dos 5 Ghz, a 802.11b, uma norma para redes até 11 Mbps na banda de frequências dos 2,4 Ghz, a 802.11g, uma norma para redes até 54 Mbps na banda de frequências dos 2,4 Ghz, e a 802.11i, um conjunto de normas de segurança para todas as Ethernets sem fios.

802.11a

Uma extensão da 802.11 aplicável a LANs sem fios e que envia dados até 54 Mbps na banda de frequências dos 5 GHz. Apesar da velocidade de transmissão ser superior à da 802.11b, a distância abrangida é muito menor.

802.11b

Uma extensão da 802.11 aplicável a LANs sem fios e que permite a transmissão a 11 Mbps na banda de frequências dos 2,4 GHz. A 802.11b é actualmente considerada a norma das redes sem fios.

802.11g

Uma extensão da 802.11 aplicável a LANs sem fios e que permite a transmissão até 54 Mbps na banda de frequências dos 2,4 GHz.

802.1x

Não suportada pelo Wireless Home Network Security. Uma norma da IEEE para autenticação em redes com e sem fios, mas mais frequentemente utilizada em redes sem fios 802.11. Esta norma fornece uma autenticação forte e mútua entre um cliente e um servidor de autenticação. Para além disso, a 802.1x fornece chaves WEP dinâmicas por utilizador e por sessão, diminuindo o trabalho administrativo e os riscos de segurança associados às chaves WEP estáticas.

A

adaptador sem fios

Adaptador que contém os circuitos necessários para permitir que um computador ou outro dispositivo comunique com um router sem fios (ou seja, que aceda a uma rede sem fios). Os adaptadores sem fios podem estar incorporados nos circuitos principais de um dispositivo de hardware ou constituir um periférico separado, que pode ser inserido num dispositivo através da porta adequada.

Adaptadores sem fios PCI

Permitem ligar um computador de secretária a uma rede. A placa é ligada a uma ranhura de expansão PCI existente no interior do computador.

Adaptadores sem fios USB

Fornecem uma interface série Plug and Play expansível. Esta interface fornece uma ligação sem fios padrão, de baixo custo, para dispositivos periféricos tais como teclados, ratos, joysticks, impressoras, digitalizadores, dispositivos de memória e câmaras de videoconferência.

análise de imagens

Bloqueia a apresentação de imagens potencialmente inapropriadas. As imagens são bloqueadas para todos os utilizadores, excepto para os membros do grupo dos adultos.

análise em tempo real

Quando o utilizador ou o computador acede aos ficheiros, estes são analisados para detecção de vírus e outras actividades.

arquivo

Para criar uma cópia dos seus ficheiros de monitorização localmente na unidade de CD, DVD, USB, na unidade de disco externo ou na unidade de rede.

arquivo

Para criar uma cópia dos seus ficheiros de monitorização localmente na unidade de CD, DVD, USB, na unidade de disco externo ou na unidade de rede.

arquivo integral

Para arquivar um conjunto completo de dados baseado nas localizações e nos tipos de ficheiros monitorizados que definiu.

arquivo rápido

Para arquivar apenas os ficheiros monitorizados que foram alterados desde o último arquivo completo ou rápido.

ataque de dicionário

Estes ataques envolvem a utilização de um conjunto de palavras existente numa lista para identificar a palavra-passe de um utilizador. Os atacantes não experimentam manualmente todas as combinações, dispondo de ferramentas que tentam automaticamente identificar a palavra-passe de um utilizador.

ataque de força bruta

Trata-se de um método de tentativa e erro utilizado pelas aplicações para descodificarem dados encriptados, tais como palavras-passe, através do esforço exaustivo (utilizando a força bruta) em vez da utilização de estratégias intelectuais. Tal como um criminoso pode conseguir abrir um cofre tentando as várias combinações possíveis, uma aplicação de ataque de força bruta tenta sequencialmente todas as combinações possíveis de caracteres legais. A força bruta é considerada uma abordagem infalível, se bem que demorada.

ataque de intermediário (man-in-the-middle)

O atacante intercepta as mensagens numa troca de chaves públicas e, em seguida, retransmite-as, substituindo a chave pedida pela sua própria chave pública de modo a que pareça que os dois interlocutores originais continuam a comunicar directamente. O atacante utiliza um programa que aparenta ser o servidor ao cliente e que aparenta ser o cliente ao servidor. O ataque pode ser utilizado apenas para obter acesso às mensagens ou para permitir que o atacante modifique as mensagens antes de as retransmitir. O termo deriva do facto do atacante agir como "intermediário" da comunicação.

autenticação

O processo de identificação de um indivíduo, normalmente baseado num nome de utilizador e palavra-passe. A autenticação assegura que esse indivíduo é realmente quem afirma ser, mas não contém quaisquer informações sobre os direitos de acesso desse indivíduo.

B

biblioteca

Área de armazenamento online para ficheiros publicados por utilizadores do Data Backup. A biblioteca é um Web site da Internet, que está acessível a todos os que tiverem acesso à Internet.

browser

Um programa cliente que utiliza o Hypertext Transfer Protocol (HTTP) para efectuar pedidos de servidores Web na Internet. Um Web browser apresenta o conteúdo graficamente ao utilizador.

C

cabeçalho

Um cabeçalho são informações adicionadas a uma parte da mensagem durante o seu ciclo de vida. O cabeçalho indica ao software da Internet como enviar a mensagem, para onde as respostas da mensagem devem ser enviadas, um identificador exclusivo para a mensagem de correio electrónico e outras informações administrativas. Exemplos de campos de cabeçalho: Para, De, CC, Data, Assunto, ID da Mensagem e Recebido.

Cavalo de Tróia

Os Cavalos de Tróia são programas que aparentam ser aplicações benignas. Os cavalos de Tróia não são considerados vírus porque não se replicam, mas podem ser tão destrutivos como estes.

chave

Uma série de letras e/ou números utilizada por dois dispositivos para autenticação da respectiva comunicação. Ambos os dispositivos têm de possuir a chave. Consulte também WEP, WPA, WPA2, WPA-PSK e WPA2- PSK.

cliente

Uma aplicação, em execução num computador pessoal ou estação de trabalho, que depende de um servidor para efectuar algumas operações. Por exemplo, um cliente de correio electrónico é uma aplicação que lhe permite enviar e receber correio electrónico.

cliente de correio electrónico

Uma conta de correio electrónico. Por exemplo, Microsoft Outlook ou Eudora.

Cofre de Palavras-passe

Área de armazenamento seguro para palavras-passe pessoais. Permite guardar palavras-passe com a certeza de que nenhum outro utilizador (nem mesmo um Administrador da McAfee ou um administrador do sistema) terá acesso às mesmas.

compressão

Processo pelo qual os dados (ficheiros) são comprimidos num formato que reduz o espaço necessário para os armazenar ou transmitir.

conta de correio electrónico padrão

A maioria dos utilizadores domésticos possui este tipo de conta. Consulte também Conta POP3.

Conta MAPI

Acrónimo de Messaging Application Programming Interface, interface de programação de aplicações de mensagens. Especificação de interface Microsoft que permite que diferentes aplicações de mensagens e de grupos de trabalho (incluindo correio electrónico, correio de voz e fax) funcionem através de um único cliente, como o cliente Exchange. Por este motivo, o MAPI é utilizado frequentemente em ambientes empresariais quando a empresa utiliza o Microsoft® Exchange Server. No entanto, muitas pessoas utilizam o Microsoft Outlook para o correio electrónico da Internet pessoal.

conta MSN

Abreviatura de Rede Microsoft. Um serviço online e um portal da Internet. Trata-se de uma conta baseada em ambiente Web.

Conta POP3

Acrónimo de Post Office Protocol 3. A maioria dos utilizadores domésticos possuem este tipo de conta. Trata-se da versão actual do protocolo de postos de correio utilizado na maioria das redes TCP/IP. Também conhecida como conta de correio electrónico padrão.

cookie

Na World Wide Web, um bloco de dados que um servidor Web guarda num sistema cliente. Quando um utilizador regressa ao mesmo Web site, o browser envia uma cópia do cookie para o servidor. Os cookies são utilizados para identificar utilizadores, para dar indicação ao servidor para enviar uma versão personalizada da página Web solicitada, para enviar informações de conta ao utilizador e para outros efeitos administrativos.

Os cookies permitem que o Web site memorize a identificação do utilizador e rastreie o número de pessoas que o visitaram, quando o visitaram e que páginas foram visualizadas. Os cookies também ajudam uma empresa a personalizar o respectivo Web site em função do utilizador. Um grande número de Web sites requer um nome de utilizador e uma palavra-passe para permitir o acesso a determinadas páginas, enviando um cookie ao computador para que não seja necessário iniciar sessão sempre que a página é visitada. No entanto, os cookies podem ser utilizados por motivos maliciosos. As empresas de publicidade online utilizam frequentemente os cookies para determinarem os sites que o utilizador visita com mais frequência, colocando anúncios nos Web site favoritos do utilizador. Antes de aceitar os cookies de um site, verifique se os cookies são fidedignos.

Embora sejam uma fonte de informações para empresas legítimas, os cookies podem também ser uma fonte de informações para hackers. Um grande número de Web sites com lojas online armazenam informações de cartões de crédito e outras informações pessoais em cookies para simplificar o processo de compra. Infelizmente, podem existir erros de segurança que permitem aos hackers aceder às informações dos cookies armazenados nos computadores dos clientes.

cópia de segurança

Para criar uma cópia dos ficheiros de monitorização num servidor online seguro.

correio electrónico

Correio Electrónico, mensagens enviadas através da Internet ou por uma rede local ou alargada empresarial. Os anexos de correio electrónico no formato de ficheiros EXE (executáveis) ou VBS (scripts do Visual Basic) tornaram-se muito populares como forma de transmissão de vírus e Troianos.

D

Denial-of-Service

Na Internet, um ataque Denial-of-Service (DoS) é um incidente no qual um utilizador ou organização fica privado dos serviços de um recurso que normalmente esperaria ter. Normalmente, a perda de serviço é a indisponibilidade de um serviço de rede específico, tal como o correio electrónico, ou a perda temporária de toda a conectividade e serviços de rede. Por exemplo, nos piores casos, um Web site acedido por milhões de pessoas pode ocasionalmente ser forçado a interromper temporariamente o funcionamento. Um ataque Denial-of-Service também poderá destruir a programação e os ficheiros num sistema informático. Apesar de ser normalmente intencional e malicioso, um ataque Denial-of-Service também pode por vezes ocorrer acidentalmente. Um ataque Denial-of-Service é um tipo de falha de segurança de um sistema informático que não resulta normalmente no furto de informações ou na perda de outros serviços. No entanto, estes ataques podem causar à vítima uma grande perda de tempo e dinheiro.

DNS

Sigla de Domain Name System, sistema de nomes de domínios. Sistema hierárquico através do qual os anfitriões na Internet possuem endereços de nome de domínio (como bluestem.prairienet.org) e endereço IP (como 192.17.3.4). O endereço do nome de domínio é utilizado pelas pessoas e é automaticamente convertido no endereço IP numérico, que é utilizado pelo software de encaminhamento de pacotes. Os nomes DNS são constituídos por um domínio de nível superior (como .com, .org e .net), um domínio de nível secundário (o nome do site de uma empresa, de uma organização ou de um indivíduo) e, possivelmente, um ou mais subdomínios (servidores dentro do domínio de nível secundário). Consulte também Servidor DNS e Endereço IP.

domínio

Um endereço de uma ligação de rede que identifica o proprietário desse endereço num formato hierárquico: servidor.organização.tipo. Por exemplo, www.whitehouse.gov identifica o servidor Web da Casa Branca, que faz parte do governo dos E.U.A.

E

encriptação

Processo pelo qual os dados passam de texto a código, ocultando as informações para impedir que sejam lidas por pessoas que não sabem como as desencriptar.

endereço IP

O endereço de protocolo Internet, ou endereço IP, é um número exclusivo composto por quatro partes separadas por pontos (por exemplo, 63.227.89.66). Todos os computadores na Internet, do maior servidor a um computador portátil, que comunicam através de um telemóvel, têm um número IP exclusivo. Nem todos os computadores têm um nome de domínio, mas todos têm um IP.

Lista de alguns tipos de endereços IP pouco frequentes:

- Endereços IP Não Encaminháveis: São igualmente designados por Espaço IP Privado. São endereços IP que não podem ser utilizados 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 Loop-Back**:** Os endereços de loop-back são utilizados para testes. O tráfego enviado para este bloco de endereços IP volta para o dispositivo que gerou o pacote. Nunca sai do dispositivo e é utilizado principalmente para testes de hardware e software. O bloco de endereços IP de Loopback é 127.x.x.x.

Endereço IP Nulo: É um endereço IP inválido. Quando for apresentado, indica que o tráfego tem um endereço IP nulo. Não é normal e geralmente indica que o remetente está deliberadamente a ocultar a origem do tráfego. O remetente não poderá receber nenhuma resposta para o tráfego, a não ser que o pacote seja recebido por uma aplicação que compreenda o respectivo conteúdo, o qual incluirá instruções específicas para essa aplicação. Qualquer endereço que comece por 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Endereço MAC (Endereço de Controlo de Acesso a Suportes de Dados)

Um endereço de baixo nível atribuído a um dispositivo físico que acede à rede.

Erros de Web

Pequenos ficheiros gráficos que podem incorporar-se nas páginas HTML e permitir que uma fonte não autorizada instale cookies no computador. Estes cookies podem depois transmitir informações à fonte não autorizada. Erros de Web são também designados sinalizadores Web, pixel tags, GIFs limpos ou GIFs invisíveis.

ESS (Extended Service Set)

Um conjunto de duas ou mais redes que constituem uma única sub-rede.

evento

Eventos de 0.0.0.0

Se vir eventos com o endereço IP 0.0.0.0, existem duas causas prováveis. A primeira, e mais comum, é que, por algum motivo, o computador recebeu um pacote inválido. A Internet nem sempre é 100% fiável e poderão surgir pacotes danificados. Uma vez que o Firewall vê os pacotes antes de o TCP/IP os poder validar, poderá comunicar estes pacotes como um evento.

A segunda situação ocorre quando o IP de origem é alvo de fraude ou é falso. Os pacotes alvo de fraudes podem ser indícios de que alguém anda à procura de Troianos e tentou procurar no seu computador. É importante lembrar que o Firewall bloqueia a tentativa.

Eventos de 127.0.0.1

Por vezes, os eventos listam o respectivo endereço IP de origem como 127.0.0.1. É importante referir que este IP é especial e é designado como o endereço de loopback.

Independentemente do computador que está a utilizar, 127.0.0.1 designa sempre o seu computador local. Este endereço também é denominado localhost, visto que o localhost do nome do computador será sempre convertido no endereço IP 127.0.0.1. Isto significa que o computador está a tentar atacar-se a si mesmo? Estará algum Troiano ou spyware a tentar controlar o computador? Provavelmente não. Muitos programas legítimos utilizam o endereço de loopback para comunicação entre componentes. Por exemplo, muitos servidores de correio electrónico pessoal ou servidores Web podem ser configurados através de uma interface Web que normalmente é acedida através de um endereço semelhante a http://localhost/.

No entanto, o Firewall permite tráfego desses programas, pelo que, se forem apresentados eventos de 127.0.0.1, isso significa que o endereço IP de origem é fraudulento ou falso. Normalmente, os pacotes falsificados são um sinal de que alguém está a procurar Troianos. É importante lembrar que o Firewall bloqueia esta tentativa. Obviamente que reportar eventos a partir de 127.0.0.1 não tem qualquer utilidade, pelo que é desnecessário fazê-lo.

Assim sendo, alguns programas, nomeadamente o Netscape 6.2 e posterior, requerem que o endereço 127.0.0.1 seja adicionado à lista **Endereços IP de Confiança**. Os componentes destes programas comunicam entre si de um modo que o Firewall não consegue determinar se o tráfego é local ou não.

No exemplo do Netscape 6.2, se não considerar o endereço 127.0.0.1 fidedigno, não poderá utilizar a sua lista de amigos. Desta forma, se receber tráfego de 127.0.0.1 e todos os programas do computador funcionarem normalmente, então é seguro bloquear esse tráfego. No entanto, se um programa (como o Netscape) estiver com problemas, adicione 127.0.0.1 à lista **Endereços IP de Confiança** do Firewall e, em seguida, verifique se o problema ficou resolvido.

Se a introdução de 127.0.0.1 na lista **Endereços IP de Confiança** resolver o problema, será necessário analisar as opções: se considerar o endereço 127.0.0.1 fidedigno, o programa funcionará, mas estará mais vulnerável a ataques fraudulentos. Se não confiar no endereço, o programa não funcionará, mas continuará protegido contra qualquer tráfego malicioso.

Eventos de computadores na rede local

Para a maioria das definições de LAN empresarial, pode confiar em todos os computadores da rede local.

Eventos de endereços IP privados

Os endereços IP no formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são referidos como endereços IP privados ou não encaminháveis. Estes endereços IP nunca devem sair da rede e, na maioria das vezes, podem ser considerados fidedignos.

O bloco 192.168 é usado com o Microsoft Internet Connection Sharing (ICS). Se estiver a utilizar o ICS e vir eventos deste bloco de IPs, poderá pretender adicionar o endereço IP 192.168.255.255 à respectiva lista de **Endereços IP de Confiança**. Isto tornará todo o bloco 192.168.xxx.xxx de confiança.

Se não estiver numa rede privada e receber eventos destes intervalos de endereços IP, é possível que o endereço IP de origem seja fraudulento ou falso. Normalmente, os pacotes falsificados são um sinal de que alguém está a procurar Troianos. É importante lembrar que o Firewall bloqueia esta tentativa.

Uma vez que os endereços IP privados estão separados dos endereços IP na Internet, a comunicação destes eventos não terá qualquer efeito.

Falsificação de IP

Falsificação dos endereços IP existentes num pacote IP. Esta técnica é utilizada em vários tipos de ataques, incluindo a utilização indevida de sessões. Esta técnica é também frequentemente utilizada para falsificar os cabeçalhos de correio publicitário não solicitado, para impedir que estes sejam correctamente rastreados.

firewall

Um sistema concebido para impedir o acesso não autorizado a uma rede privada. As firewalls podem ser implementadas em hardware, software, ou numa combinação dos dois. As firewalls são frequentemente utilizadas para impedir que utilizadores não autorizados acedam a redes privadas ligadas à Internet, especialmente a uma intranet. Todas as mensagens enviadas e recebidas pela intranet passam pela firewall. A firewall examina todas as mensagens e bloqueia as mensagens que não correspondem aos critérios de segurança especificados. As firewalls são consideradas a primeira linha de defesa na protecção das informações privadas. Para maior segurança, os dados podem ser encriptados.

Gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (AP), de um router e de um firewall. Alguns dispositivos também podem incluir melhoramentos de segurança e funcionalidades de bridging.

grupos de classificação de conteúdos

Escalões etários a que um utilizador pertence O conteúdo é classificado (isto é, disponibilizado ou bloqueado), com base no grupo de classificação de conteúdos ao qual o utilizador pertence. Os grupos de classificação de conteúdos incluem: criança pequena, criança, adolescente mais novo, adolescente mais velho e adulto.

hotspot

Uma localização geográfica especifica em que um ponto de acesso (AP) fornece serviços públicos de banda larga aos utilizadores móveis através de uma rede sem fios. Os hotspots encontram-se frequentemente localizados em áreas de grande movimento, tais como aeroportos, estações ferroviárias, bibliotecas, marinas, centros de convenções e hotéis. Os hotspots dispõem normalmente de um alcance reduzido.

Internet

A Internet é composta por um grande número de redes interligadas que utilizam protocolos TCP/IP para localização e transferência de dados. A Internet surgiu a partir de uma rede criada para ligar computadores de universidades e faculdades (no fim da década de 60 e início de 70), fundada pelo Departamento de Defesa dos E.U.A. e era denominada ARPANET. Actualmente, a Internet é uma rede global de aproximadamente 100.000 redes independentes.

intranet

Rede privada, normalmente dentro de uma organização, que funciona da mesma maneira que a Internet. Tornou-se prática comum permitir o acesso a Intranets a partir de computadores autónomos utilizados por alunos ou funcionários remotos. As firewalls, os procedimentos de início de sessão e as palavras-passe são utilizados para proporcionar segurança.

LAN (Rede Local)

Uma rede de computadores que abrange uma área relativamente pequena. A maior parte das LANs estão confinadas a um só edifício ou a um grupo de edifícios. No entanto, uma LAN pode estar ligada a outras LANs através de linhas telefónicas e ondas de rádio. Um sistema de LANs interligado deste modo é chamado uma rede alargada (WAN). A maior parte das LANs interligam estações de trabalho e computadores pessoais através de concentradores ou comutadores simples. Cada nó (computador individual) existente numa LAN tem uma CPU própria com a qual executa programas, mas também pode aceder a dados e dispositivos (por ex.: impressoras) localizados em qualquer ponto da LAN. Isto permite que os utilizadores partilhem dispositivos dispendiosos, tais como impressoras laser, bem como dados. Os utilizadores também podem utilizar a LAN para comunicarem entre si (por exemplo, enviando mensagens de correio electrónico ou participando em sessões de conversação).

largura de banda

A quantidade de dados que pode ser transmitida num período de tempo fixo. Nos dispositivos digitais, a largura de banda é normalmente indicada em bits por segundo (bps) ou em bytes por segundo. Nos dispositivos analógicos, a largura de banda é indicada em ciclos por segundo, ou Hertz (Hz).

limitações de acesso

Definições que permitem configurar classificações de conteúdos que restringem o acesso a Web sites e conteúdos a utilizadores, bem como tempos limite da Internet que especificam o período e a duração do acesso dos utilizadores à Internet. As limitações de acesso também permitem restringir universalmente o acesso a Web sites específicos e conceder e bloquear acesso com base em permissões e palavras-chave por grupos etários.

lista de sites bloqueados

Uma lista de Web sites considerados maliciosos. Um Web site pode ser colocado numa lista negra, por actuação fraudulenta ou por explorar a vulnerabilidade do browser para enviar ao utilizador programas potencialmente indesejados.

lista de sites seguros

Lista de sites Web cujo acesso é permitido por não serem considerados fraudulentos.

localização com monitorização abrangente

Uma pasta (e todas as subpastas) do computador sujeita a monitorização para detecção de alterações pela Cópia de Segurança de Dados. Se tiver definido uma localização de monitorização abrangente, a Cópia de Segurança de Dados efectua a cópia de segurança dos tipos de ficheiros monitorizados dentro da pasta e respectivas subpastas.

localizações com monitorização superficial

Uma pasta do computador sujeita a monitorização para detecção de alterações efectuadas pelo Data Backup. Se tiver definido uma localização para monitorização superficial, o Data Backup efectua a cópia de segurança dos tipos de ficheiros monitorizados dentro da pasta, mas não inclui as respectivas subpastas.

localizações monitorizadas

Pastas do computador monitorizadas pelo Data Backup.

MAC (Controlo de Acesso a Suportes de Dados ou Código de Autenticação da Mensagem)

Para o primeiro, consulte Endereço MAC. O último é um código utilizado para identificar uma mensagem específica (por ex.: uma mensagem RADIUS). O código é, geralmente, um hash criptograficamente forte do conteúdo da mensagem, que inclui um valor exclusivo de protecção contra a reprodução.

mapeamento de rede

No Network Manager, corresponde a uma representação gráfica dos computadores e dos componentes que fazem parte de uma rede doméstica.

nó

Um único computador ligado a uma rede.

palavra-chave

Palavra que pode atribuir a um ficheiro do qual foi efectuada uma cópia de segurança para estabelecer uma relação ou uma ligação com outros ficheiros aos quais foi atribuída a mesma palavra-chave. A atribuição de palavras-chave a ficheiros facilita a procura de ficheiros publicados na Internet.

palavra-passe

Código (normalmente alfanumérico) utilizado para obter acesso ao computador ou a um determinado programa ou Web site.

partilha

Operação que permite que os destinatários do correio electrónico tenham acesso a ficheiros com cópia de segurança durante um período de tempo limitado. Quando partilha um ficheiro, envia uma cópia de segurança do ficheiro para os destinatários do correio electrónico que especificar. Os destinatários recebem a mensagem de correio electrónico a partir do Data Backup, com a indicação de que os ficheiros foram partilhados com os mesmos. A mensagem de correio electrónico inclui ainda uma ligação para os ficheiros partilhados.

phishing

Pronuncia-se como "fishing" e é um esquema fraudulento para obter ilicitamente informações valiosas, tais como números de cartões de crédito e de segurança social, IDs de utilizador e palavras-passe. Uma mensagem de correio electrónico com um aspecto aparentemente oficial é enviada para as potenciais vítimas, alegadamente como sendo proveniente do seu fornecedor de serviços Internet, banco ou revendedor. As mensagens de correio electrónico podem ser enviadas para pessoas constantes em listas seleccionadas ou em qualquer lista, na expectativa de que uma parte dos destinatários tenha realmente uma conta na verdadeira organização.

Placa de Rede

Uma placa que é ligada a um computador portátil ou outro dispositivo, permitindo-lhe aceder à LAN.

Ponto de Acesso (AP)

Um dispositivo de rede que permite que os clientes 802.11 acedam a uma rede local (LAN). Os APs aumentam o alcance físico dos utilizadores sem fios. Por vezes são chamados routers sem fios.

pontos de acesso não autorizados

Um ponto de acesso cujo funcionamento não seja autorizado por uma empresa. O problema é que os pontos de acesso não autorizados não respeitam, de uma maneira geral, as políticas de segurança das LANs sem fios (WLANs). Um ponto de acesso não autorizado constitui uma interface aberta e não protegida para a rede empresarial a partir do exterior das respectivas instalações.

Numa WLAN devidamente protegida, os pontos de acesso não autorizados são mais prejudiciais do que os utilizadores não autorizados. Os utilizadores não autorizados que tentem aceder a uma WLAN terão poucas hipóteses de alcançar recursos empresariais valiosos se os mecanismos de autenticação adequados estiverem activos. No entanto, a ligação de um ponto de acesso não autorizado por um funcionário ou um hacker origina problemas muito mais graves. Estes pontos de acesso não autorizados permitem que praticamente qualquer pessoa com um dispositivo compatível com 802.11 aceda à rede empresarial. Isto coloca qualquer pessoa muito perto dos recursos críticos.

pop-ups

Pequenas janelas que aparecem por cima de outras janelas no ecrã do computador. As janelas de pop-up são frequentemente utilizadas em Web browsers para apresentação de anúncios. A McAfee bloqueia as janelas de pop-up que são automaticamente transferidas quando abre uma página Web no browser. As janelas de pop-up que são transferidas quando clica numa ligação não são bloqueadas pela McAfee.

porta

Local por onde as informações passam para entrar ou sair de um computador; por exemplo, um modem analógico convencional está ligado a uma porta série. Os números de porta em comunicações TCP/IP são valores virtuais utilizados para separar tráfego em fluxos específicos de aplicações. As portas são atribuídas a protocolos padrão como SMTP ou HTTP para que os programas saibam quais as portas a utilizar para tentar estabelecer uma ligação. A porta de destino para pacotes TCP indica a aplicação ou o servidor procurado.

PPPoE

Point-to-Point Protocol Over Ethernet. Utilizado por muitos fornecedores de DSL, o PPPoE suporta as camadas de protocolo e a autenticação utilizadas no PPP, permitindo o estabelecimento de uma ligação ponto-a-ponto na arquitectura multiponto da Ethernet.

programa potencialmente indesejado

Os programas potencialmente indesejados incluem spyware, adware e outros programas que recolhem e transmitem dados do utilizador sem a sua permissão.

Protecções do Sistema

As Protecções do Sistema detectam alterações não autorizadas no computador e alertam-no quando estas ocorrem.

protocolo

Um formato acordado para a transmissão de dados entre dois dispositivos. Do ponto de vista do utilizador, o único aspecto interessante dos protocolos é que o respectivo computador ou dispositivo tem de suportar os protocolos adequados para comunicar com outros computadores. O protocolo pode ser implementado por hardware ou software.

proxy

Computador (ou software executado no mesmo) que funciona como barreira entre uma rede e a Internet, apresentando apenas um endereço de rede para sites externos. Ao agir como intermediário representando todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que fornece acesso à Internet. Consulte também Servidor Proxy.

publicar

Disponibilizar publicamente na Internet um ficheiro do qual foi efectuada uma cópia de segurança.

quarentena

Quando são detectados ficheiros suspeitos, estes são colocados em quarentena. Pode então tomar as medidas apropriadas.

RADIUS (Remote Access Dial-In User Service)

Um protocolo que permite a autenticação de utilizadores, normalmente no contexto do acesso remoto. Originalmente definido para utilização com servidores de acesso telefónico remoto, o protocolo é agora utilizado numa vasta gama de ambientes de autenticação, incluindo a autenticação 802.1x do Segredo Partilhado dos utilizadores de uma WLAN.

rede

Quando liga dois ou mais computadores, cria uma rede.

rede gerida

Uma rede doméstica com dois tipos de membros: membros geridos e membros não geridos. Os membros geridos permitem que outros computadores da rede monitorizem o respectivo estado de protecção McAfee; os membros não geridos não o permitem.

repositório de cópia de segurança online

Localização do servidor online onde os ficheiros monitorizados são guardados depois de ter sido efectuada a cópia de segurança.

restaurar

Para repor uma cópia de um ficheiro a partir de um arquivo ou do repositório de cópias de segurança online.

roaming

A capacidade de passar da área de cobertura de um ponto de acesso para outra sem interrupção do serviço ou perda de conectividade.

router

Um dispositivo de rede que encaminha pacotes entre redes. Com base nas tabelas de encaminhamento internas, os routers lêem cada pacote recebido e decidem como o devem encaminhar. A interface de destino dos pacotes enviados pelo router pode ser determinada por qualquer combinação de endereços de origem e destino, bem como pelas condições actuais de tráfego, tal como a carga, os custos das linhas e a existência de linhas danificadas. Por vezes é referido como ponto de acesso.

script

Os scripts podem criar, copiar ou eliminar ficheiros. Podem também abrir o Registo do Windows.

segredo partilhado

Consulte também RADIUS. Protege partes sensíveis de mensagens RADIUS. Este segredo partilhado é uma palavra-passe que é partilhada entre o autenticador e o servidor de autenticação de modo seguro.

servidor

Computador ou software que fornece serviços específicos ao software em execução noutros computadores. O "servidor de correio" no ISP é um software que processa todas as mensagens enviadas e recebidas dos utilizadores. Um servidor numa rede local é um hardware que constitui o nó principal da rede. Também poderá conter software que forneça serviços específicos, dados ou outros recursos a todos os computadores clientes ligados ao mesmo.

Servidor DNS

Versão abreviada do servidor de sistema de nomes de domínios. Um computador capaz de responder a consultas do sistema de nomes de domínios (DNS). O servidor DNS dispõe de uma base de dados de computadores anfitriões e respectivos endereços IP. Confrontado com o nome apex.com, por exemplo, o servidor DNS devolve o endereço IP da empresa hipotética Apex. Também designado: servidor de nomes. Consulte também DNS e Endereço IP.

servidor proxy

Componente de firewall que gere o tráfego de Internet de e para uma rede local. Um servidor proxy pode melhorar o desempenho ao fornecer dados pedidos com frequência, como, por exemplo, uma página Web popular, e consegue filtrar e ignorar pedidos que o proprietário não considera adequados, como pedidos de acesso não autorizado a ficheiros de propriedade.

Servidor SMTP

Sigla do protocolo de transferência de correio simples, Simple Mail Transfer Protocol. Um protocolo TCP/IP para o envio de mensagens de um computador para outro numa rede. Este protocolo é utilizado na Internet para encaminhamento de correio electrónico.

sincronizar

Permite resolver problemas de inconsistência entre ficheiros com cópia de segurança e ficheiros guardados no computador local. Sincroniza-se ficheiros quando a versão do ficheiro no repositório de cópias de segurança online é mais recente do que a versão do ficheiro existente nos outros computadores. A sincronização actualiza a cópia do ficheiro nos computadores com a versão do ficheiro existente no repositório de cópias de segurança online.

sobrecarga da memória temporária

As sobrecargas da memória temporária ocorrem quando programas ou processos suspeitos tentam armazenar numa memória temporária (área de armazenamento de dados temporário) mais dados do que o limite suportado, danificando ou substituindo dados válidos nas memórias temporárias adjacentes.

SSID (Identificador do Conjunto de Serviços)

Nome da rede para os dispositivos num subsistema de LAN sem fios. Trata-se de uma cadeia de 32 caracteres, em texto limpo, adicionada ao cabeçalho de cada pacote de uma WLAN. O SSID diferencia as WLANs, pelo que todos os utilizadores de uma rede têm de fornecer o mesmo SSID para acederem a um determinado ponto de acesso. Um SSID impede o acesso a qualquer dispositivo cliente que não possua o SSID. No entanto, por predefinição, os pontos de acesso difundem o respectivo SSID no sinalizador. Mesmo que a difusão do SSID esteja desactivada, um hacker poderá detectar o SSID utilizando aplicações de intercepção (sniffing).

SSL (Secure Sockets Layer)

Protocolo desenvolvido pela Netscape para a transmissão de documentos privados através da Internet. O SSL funciona através da utilização de uma chave pública para encriptar os dados que são transferidos através da ligação SSL. O Netscape Navigator e o Internet Explorer utilizam e suportam o SSL e muitos Web sites utilizam o protocolo para obterem informações confidenciais dos utilizadores, tais como números de cartões de crédito. Por convenção, os URLs que requerem uma ligação SSL começam com https: em vez de http:

texto cifrado

Dados que foram encriptados. O texto cifrado não é legível até ser convertido em texto simples (desencriptado) com uma chave.

texto simples

Qualquer mensagem que não está encriptada.

tipos de ficheiros monitorizados

Tipos de ficheiros (por exemplo, .doc, .xls, etc.) que o Data Backup copia ou arquiva nas localizações de monitorização.

TKIP (Temporal Key Integrity Protocol)

Um método de resolução dos pontos fracos inerentes à segurança WEP, especialmente a reutilização de chaves de encriptação. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmica que melhora significativamente a segurança da rede. O processo de segurança do TKIP começa com uma chave temporal de 128 bits que é partilhada entre os clientes e os pontos de acesso. O TKIP combina a chave temporal com o endereço MAC das máquinas clientes e, em seguida, adiciona um vector de inicialização de 16 octetos, relativamente grande, para produzir a chave que encripta os dados. Este procedimento assegura que cada estação utiliza sequências de chaves diferentes para encriptar os dados. O TKIP utiliza o RC4 para a encriptação. O WEP também utiliza o RC4.

unidade de disco rígido externa

Disco instalado fora da caixa do computador.

unidade de rede

Uma unidade de disco ou uma unidade de banda que está ligada a um servidor de uma rede e que é partilhada por vários utilizadores. As unidades de rede são por vezes designadas unidades remotas.

URL

Uniform Resource Locator. É o formato padrão para endereços da Internet.

VPN (Rede Privada Virtual)

Uma rede criada através da utilização de cablagem pública para a interligação de nós. Por exemplo, existem vários sistemas que lhe permitem criar redes utilizando a Internet como meio de transporte dos dados. Estes sistemas utilizam encriptação e outros mecanismos de segurança para garantir que apenas os utilizadores autorizados podem aceder à rede e que os dados não podem ser interceptados.

wardriver

Hackers móveis, equipados com computadores portáteis, software especial e algum hardware alterado, que viajam de automóvel pelas cidades, subúrbios e parques de estacionamento para interceptarem o tráfego de LANs sem fios.

WEP (Wired Equivalent Privacy)

Um protocolo de encriptação e autenticação definido como parte da norma 802.11. As versões iniciais são baseadas em cifras RC4 e têm vários pontos fracos. O WEP tenta proporcionar segurança, encriptando os dados transmitidos através das ondas de rádio, de modo a que estes estejam protegidos enquanto viajam entre dois pontos. No entanto, chegou-se à conclusão que o WEP não é tão seguro como se pensava inicialmente.

Wi-Fi (Wireless Fidelity)

Termo utilizado genericamente para referir qualquer tipo de rede 802.11, quer seja 802.11b, 802.11a, banda dupla, etc. Este termo é utilizado pela Wi-Fi Alliance.

Wi-Fi Alliance

Uma organização composta pelos principais fabricantes de equipamento e software sem fios, tendo em vista (1) certificar a interoperacionalidade de todos os produtos baseados na norma 802.11 e (2) promover o termo Wi-Fi, como marca global, para qualquer produto de LAN sem fios baseado na norma 802.11. Esta organização age como um consórcio, laboratório de testes e ponto de encontro para todos os fabricantes que pretendam promover a interoperacionalidade e o crescimento da indústria.

Apesar de todos os produtos 802.11a/b/g serem denominados Wi-Fi, apenas os produtos que passaram os testes da Wi-Fi Alliance estão autorizados a ser referenciados como Wi-Fi Certified (uma marca registada). As embalagens dos produtos que passaram estes testes têm de apresentar um selo identificativo com a marca Wi-Fi Certified e a banda de frequências de rádio utilizada. Este grupo chamava-se anteriormente Wireless Ethernet Compatibility Alliance (WECA), mas mudou o respectivo nome em Outubro de 2002 para melhor reflectir a marca Wi-Fi que pretende criar.

Wi-Fi Certified

Quaisquer produtos testados e aprovados como Wi-Fi Certified (uma marca registada) pela Wi-Fi Alliance têm a garantia de serem interoperacionais entre si, mesmo que provenham de fabricantes diferentes. Um utilizador com um produto Wi-Fi Certified pode utilizar qualquer marca de ponto de acesso com qualquer outra marca de hardware cliente que também seja certificado. No entanto, normalmente, qualquer produto Wi-Fi que utilize a mesma frequência de rádio (por exemplo: 2,4 GHz para a 802.11b ou 11g, 5 GHz para a 802.11a) funciona com outro produto que utilize a mesma frequência de rádio, mesmo que este não seja Wi-Fi Certified.

WLAN (Rede Local sem Fios)

Consulte também LAN. Uma rede local que utiliza um suporte sem fios como ligação. Uma WLAN utiliza ondas de rádio de alta frequência para comunicar entre os nós, em vez de fios.

worm

Um worm é um vírus de replicação automática que reside na memória activa e que pode enviar cópias de si próprio através de mensagens de correio electrónico. Os worms replicam-se e consomem recursos do sistema, diminuindo o desempenho ou parando tarefas.

WPA (Wi-Fi Protected Access)

Uma norma que aumenta o nível de protecção de dados e controlo de acesso para os sistemas de LAN sem fios actuais e futuros. Concebido para funcionar no hardware existente, sob a forma de uma actualização de software, o WPA deriva e é compatível com a norma IEEE 802.11i. Quando instalado de modo correcto, fornece aos utilizadores da LAN sem fios um elevado grau de confiança em que os respectivos dados permanecem protegidos e que apenas os utilizadores autorizados da rede podem aceder a esta.

WPA-PSK

Um modo especial do WPA concebido para utilizadores domésticos que não requerem segurança de nível empresarial e que não dispõem de acesso a servidores de autenticação. Neste modo, o utilizador doméstico introduz manualmente a palavra-passe inicial para activar o Wi-Fi Protected Access no modo de Chave Pré-Partilhada, devendo alterar a frase-passe em cada computador e ponto de acesso sem fios regularmente. Consulte também WPA2-PSK e TKIP.

WPA2

Consulte também WPA. WPA2 é uma actualização da norma de segurança WPA e baseia-se na norma IEEE 802.11i.

WPA2-PSK

Consulte também WPA-PSK e WPA2. O WPA2-PSK é semelhante ao WPA-PSK e baseia-se na norma WPA2. Uma funcionalidade comum do WPA2-PSK é o facto de os dispositivos normalmente suportarem vários modos de encriptação (ex.: AES, TKIP) em simultâneo, enquanto que os dispositivos mais antigos, geralmente, suportavam apenas um único modo de encriptação de cada vez (isto é, todos os clientes teriam de utilizar o mesmo modo de encriptação).

Acerca da McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia (EUA), é o líder global em Prevenção de Intrusões e Gestão de Riscos de Segurança, fornecendo soluções e serviços preventivos e comprovados destinados a proteger sistemas e redes em todo o mundo. Graças aos seus conhecimentos ímpares na área da segurança e ao compromisso de inovação, a McAfee permite que utilizadores domésticos, empresas, o sector público e fornecedores de serviços possam bloquear ataques, impedir interrupções e controlar e melhorar continuamente a respectiva segurança.

Copyright

Índice remissivo

8

802.11 168
802.11a 168
802.11b 168
802.11g 168
802.1x 168

A

A aguardar autorização 138
Abandonar uma rede gerida 155
Abra o painel de configuração Computador e Ficheiros 15
Abra o painel de configuração Correio Electrónico e Mensagens Instantâneas 17
Abra o painel de configuração Internet e Rede 16
Abra o painel de configuração Limitações de Acesso 18
Abra o painel de configuração SecurityCenter 20
Abrir o SecurityCenter e utilizar funções adicionais 11
Aceder ao mapeamento de rede 54
Aceitar um ficheiro de outro computador .. 161, 162
Acerca da McAfee 187
Acerca de tipos de acesso 75, 83
Acerca dos ícones do Wireless Network Security 92, 121
Actualizar a placa sem fios 141
Actualizar o firmware do router ou ponto de acesso 135
Actualizar o mapeamento de rede 55
adaptador sem fios 168
Adaptadores sem fios PCI 169
Adaptadores sem fios USB 169
Aderir à rede 152
Aderir à rede gerida 57
Aderir a redes sem fios protegidas ... 75, 78, 98, 138
Aderir a uma rede gerida 58, 151, 155
Adiar actualizações 28, 29
Adicionar computadores à rede sem fios protegida 77, 82, 86, 138, 140
Adicionar computadores utilizando a tecnologia Windows Connect Now 87, 88, 113, 134
Adicionar computadores utilizando um dispositivo amovível 86, 89, 134
Administrar chaves de rede 109, 126
Administrar redes sem fios 91
Ajustar a frequência de rotação da chave .. 110, 111, 114
Alterar a palavra-passe de administrador 25
Alterar credenciais de dispositivos sem fios 98, 107, 136
análise de imagens 169
análise em tempo real 169
Apagar ficheiros indesejados com o Shredder 47
Apresentar as chaves em texto simples 115, 116
Apresentar chaves como asteriscos 115, 116
Apresentar notificações de ligação 99
arquivo 169
arquivo integral 169
arquivo rápido 169
As redes aparecem desprotegidas 137
ataque de dicionário 169
ataque de força bruta 169
ataque de intermediário (man-in-the-middle) 170
autenticação 170

B

biblioteca 170
browser 170

C

cabeçalho 170
Cavalo de Tróia 170

Ch

chave 170

C

cliente 170
cliente de correio electrónico 171
Cofre de Palavras-passe 171
compressão 171

Computadores nos quais o software deve ser instalado....132
Conceder acesso à rede....152
Conceder acesso a um computador desconhecido....138
Conceder acesso administrativo a computadores....75, 82
Configurar alertas informativos....32
Configurar as definições de segurança da rede 106
Configurar as opções do SecurityCenter....21
Configurar definições de alerta 96
Configurar definições de segurança 104, 145
Configurar modos de segurança....104
Configurar o EasyNetwork....149
Configurar o estado de protecção....22
Configurar opções de actualização....26
Configurar opções de alerta....31
Configurar opções de utilizador 23, 24
Configurar problemas ignorados....22
Configurar redes sem fios protegidas....74
Configurar routers ou pontos de acesso sem fios 144
Configurar uma rede gerida....53
conta de correio electrónico padrão....171
Conta MAPI 171
conta MSN....171
Conta POP3....171
Convidar um computador para aderir à rede gerida 58
cookie 171
cópia de segurança 172
Copiar um ficheiro partilhado 159
Copyright....188
correio electrónico....172
Corrigir vulnerabilidades de segurança....65
Criar redes sem fios protegidas 76, 100, 137
Criar uma conta de administrador 23

D

Denial-of-Service 172
Desactivar a actualização automática 27, 29, 30
Desfragmentar ficheiros e pastas....37
Destruir ficheiros, pastas e discos 48
DNS....173
domínio....173

E

Efectuar tarefas comuns 33
Eliminar chaves de rede 117
encriptação 173
endereço IP....173
Endereço MAC (Endereço de Controlo de Acesso a Suportes de Dados)....173
Enviar ficheiros para outros computadores 161
Enviar um ficheiro para outro computador. 161
Erro de administrador duplicado 135
Erros de Web 174
ESS (Extended Service Set).... 174
Estabelecer ligação à Internet e à rede.... 139
Estou protegido? 13
evento 174

F

Falha ao transferir na rede segura 134
Falsificação de IP.... 175
firewall.... 176
Funcionalidades 8, 40, 46, 50, 68, 148

G

Gateway integrado 176
Gerir a rede de forma remota.... 61
Gerir a sua rede.... 38
Gerir redes sem fios 92
Gerir segurança da rede sem fios.... 103
Gerir um dispositivo 64
grupos de classificação de conteúdos 176

H

hotspot 176

I

Iniciar o EasyNetwork 150
Iniciar o Wireless Network Security..... 70, 140
Instalar o software de segurança McAfee em computadores remotos 66
Instalar o Wireless Network Security 132
Instalar uma impressora de rede disponível 165
Internet.... 176
Interromper a partilha de um ficheiro.... 159
Interromper a partilha de uma impressora.. 164
intranet 176

L

LAN (Rede Local) 177
largura de banda.... 177
Ligação interrompida.... 140
Ligar a redes com Difusão do SSID desactivada 84
Ligar a redes sem fios protegidas 82, 98, 99
Ligar computadores à rede.... 137
limitações de acesso.... 177
Limpar o computador 41, 43
lista de sites bloqueados 177
lista de sites seguros 177
Listar redes preferenciais.... 94, 95
localização com monitorização abrangente 177
localizações com monitorização superficial 177

localizações monitorizadas.....177

M

MAC (Controlo de Acesso a Suportes de Dados ou Código de Autenticação da Mensagem) 178
Manutenção automática do computador.....35
Manutenção manual do computador 36
mapeamento de rede.....178
McAfee EasyNetwork 147
McAfee Network Manager.....49
McAfee QuickClean.....39
McAfee SecurityCenter.....7
McAfee Shredder 45
McAfee Wireless Network Security.....67
McAfee Wireless Protection 5
Modificar as permissões de um computador gerido 63
Modificar as propriedades de visualização de um dispositivo.....64
Monitorizar ligações de rede sem fios120, 121, 122, 123, 124
Monitorizar o estado de protecção de um computador 62
Monitorizar o estado e as permissões.....62
Monitorizar redes sem fios 119
Monitorizar redes sem fios protegidas125, 126, 127, 129
Mostrar ou ocultar itens no mapeamento de rede 56
Mudar o nome da rede.....55, 154
Mudar o nome de redes sem fios protegidas 95, 98
Mudar para contas de utilizador McAfee 23

N

Não é possível estabelecer ligação à Internet 139
Não é possível estabelecer ligação à rede sem fios 141
Não é possível reparar o router ou ponto de acesso.....136
Nível de sinal fraco.....142
nó.....178
Noções básicas das funcionalidades do Shredder.....46
Noções básicas sobre as funcionalidades do QuickClean 40
Noções básicas sobre os ícones do Network Manager 51
Noções sobre a protecção de limitação de acesso.....18
Noções sobre o estado de protecção.....13
Noções sobre os ícones do SecurityCenter....11
Noções sobre protecção da Internet e da rede16
Noções sobre protecção de computadores e ficheiros..... 15
Noções sobre protecção de correio electrónico e mensagens instantâneas..... 17
Noções sobre tipos e categorias de protecção14
Notificar antes de transferir actualizações... 27, 28

O

O nome da rede é diferente quando são utilizados outros programas 143
O software falha após a actualização do sistema operativo 145
O Windows não indica a ligação 143
O Windows não suporta a ligação sem fios 143
Obter a palavra-passe de administrador..... 24
Obter mais informações sobre vírus 38
Ocorreu uma falha na rotação da chave..... 136
Os dispositivos perdem a conectividade..... 140
Outros problemas..... 143

P

palavra-chave..... 178
palavra-passe 178
Parar de confiar nos computadores da rede .. 60
Parar de monitorizar o estado de protecção de um computador 63
Parar o Wireless Network Security..... 71
partilha..... 178
Partilhar e enviar ficheiros..... 157
Partilhar ficheiros 158
Partilhar impressoras 163
Partilhar um ficheiro..... 158
Pedido de introdução da chave WEP, WPA ou WPA2..... 140
phishing 178
Placa de Rede..... 178
Placa sem fios compatível não detectada.... 133
Ponto de Acesso (AP)..... 179
pontos de acesso não autorizados 179
pop-ups 179
porta..... 179
PPPoE..... 179
Procurar um ficheiro partilhado..... 159
programa potencialmente indesejado 179
Protecções do Sistema 179
Proteger ou configurar a rede 134
Proteger outros dispositivos sem fios 77, 84
Proteger redes sem fios..... 73
protocolo..... 180
proxy..... 180
publicar..... 180

Q

quarentena 180

R

RADIUS (Remote Access Dial-In User Service) 180
Receber um aviso de envio de ficheiro..... 162
rede 180
rede gerida 180
Referência..... 167
Remover ficheiros e pastas não utilizados..... 36
Remover redes sem fios preferenciais..... 94, 95
Remover routers ou pontos de acesso sem fios 98, 99, 134, 138
Reparar definições de segurança da rede..... 98, 106, 108, 136, 141
repositório de cópia de segurança online..... 180
Resolução automática de problemas de protecção..... 19
Resolução de problemas..... 131
Resolução de problemas relacionados com protecção..... 19
Resolução manual de problemas de protecção 19
restaurar..... 180
Restaurar o computador para as definições anteriores..... 37
Retomar a rotação da chave. 110, 111, 114, 140
Revogar o acesso à rede ... 75, 83, 98, 100, 101, 102
roaming..... 180
Rodar chaves automaticamente 98, 110, 111, 112, 113, 114, 126, 136, 140
Rodar chaves de rede manualmente ... 114, 126, 140
router 181
Router ou ponto de acesso não suportado ... 135

S

Sair de redes sem fios protegidas 100, 101, 102, 138
script..... 181
segredo partilhado 181
Seleccionar outro modo de segurança 145
servidor..... 181
Servidor DNS 181
servidor proxy 181
Servidor SMTP..... 181
sincronizar 182
sobrecarga da memória temporária 182
SSID (Identificador do Conjunto de Serviços) 182
SSL (Secure Sockets Layer)..... 182
Substituir computadores 145
Suspender rotação automática da chave 98, 111, 113, 140

T

Terminar ligação de redes sem fios protegidas 98, 100, 101, 102
texto cifrado..... 182
texto simples..... 182
tipos de ficheiros monitorizados..... 182
TKIP (Temporal Key Integrity Protocol) ... 183
Trabalhar com impressoras partilhadas 164
Transferência automática de actualizações.. 27, 28
Transferir e instalar actualizações automaticamente 27

U

unidade de disco rígido externa 183
unidade de rede..... 183
URL 183
Utilizar o mapeamento de rede 54
Utilizar o Menu Avançado..... 20
Utilizar o QuickClean..... 43
Utilizar o SecurityCenter 9
Utilizar o Shredder..... 48

V

Várias placas sem fios 134
Ver a duração da ligação à rede. 120, 121, 122, 123, 124
Ver a potência de sinal da rede 93, 123, 142
Ver a velocidade da ligação à rede 120, 121, 122, 123, 124
Ver chaves actuais 109, 134
Ver computadores actualmente protegidos.. 93, 125, 126, 127, 129
Ver detalhes do item..... 56
Ver eventos da rede sem fios protegida..... 125, 126, 127, 128, 129
Ver eventos recentes..... 34
Ver informações sobre o SecurityCenter..... 20
Ver informações sobre os produtos instalados 20
Ver o estado da ligação 120, 121, 122, 123, 124
Ver o modo de segurança da rede 93, 106, 122, 145
Ver o número de computadores protegidos mensalmente..... 125, 126, 127, 129
Ver o número de ligações diárias 125, 127, 129
Ver o número de rotações da chave... 109, 110, 111, 112, 114, 126
Ver o relatório de segurança online ... 120, 121, 122, 123, 124, 133

Verificar actualizações automaticamente.....27
Verificar actualizações manualmente.....29, 30
Verificar o estado das actualizações.....12
Verificar o estado de protecção.....11
VPN (Rede Privada Virtual).....183

W

wardriver 183
WEP (Wired Equivalent Privacy) 183
Wi-Fi (Wireless Fidelity) 183
Wi-Fi Alliance.....184
Wi-Fi Certified 184
WLAN (Rede Local sem Fios).....184
worm.....184
WPA (Wi-Fi Protected Access) 184
WPA2.....185
WPA2-PSK 185
WPA-PSK 185