McAfee®

Wireless Protection 2007

User Guide

Contents

McAfee Network Manager 49

McAfee Wireless Network Security 67

McAfee EasyNetwork 145

CHAPTER 1

McAfee Wireless Protection

McAfee Wireless Protection Suite eliminates networking hassles and wireless security risks. Its trusted protection prevents hackers from attacking your Wi-Fi® network, safeguards your personal information and transactions, and deters others from using your network to access the Internet -- all with a single click. McAfee Wireless Network Security's strong, rotating encryption keys thwart even the most determined wireless intruders. Wireless Protection also includes McAfee EasyNetwork which makes sharing files and printers across your network simple. Additionally, it comes with McAfee Network Manager which monitors computers across your network for security weaknesses, and makes it easy to fix potential security issues.

Wireless Protection includes the following programs:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

CHAPTER 2

McAfee SecurityCenter

McAfee SecurityCenter is an easy-to-use environment where McAfee users can launch, manage, and configure their security subscriptions.

SecurityCenter also acts as a source of information for virus alerts, product information, support, subscription information, and one-click access to tools and news hosted at the McAfee Web site.

In this chapter

Features

McAfee SecurityCenter provides the following new features and benefits:

Redesigned protection status

Easily review your computer's security status, check for updates, and fix potential security issues.

Continual updates and upgrades

Automatically install daily updates. When a new version of McAfee software is available, you get it automatically at no charge during your subscription, ensuring that you always have up-to-date protection.

Real-time alerting

Security alerts notify you of emergency virus outbreaks and security threats, and provide response options to remove, neutralize, or learn more about the threat.

Convenient protection

A variety of renewal options help keep your McAfee protection current.

Performance Tools

Remove unused files, defragment used files, and use system restore to keep your computer running at peak performance.

Real online help

Get support from McAfee's computer security experts, by Internet chat, e-mail and telephone.

Safe surfing protection

If installed, the McAfee SiteAdvisor browser plug-in helps protect you from spyware, spam, viruses, and online scams by rating Web sites you visit or that appear in your Web search results. You can view detailed safety ratings that show how a site tested for e-mail practices, downloads, online affiliations, and annoyances such as pop-ups and third-party tracking cookies.

CHAPTER 3

Using SecurityCenter

You can run SecurityCenter from the McAfee SecurityCenter icon M in the Windows notification area at the far right of the taskbar or from your Windows desktop.

When you open SecurityCenter, the Home pane displays your computer's security status and provides quick access to updating, scanning (if McAfee VirusScan is installed), and other common tasks:

Header

Help

View the program help file.

Left column

Update

Update your product to ensure protection from the latest threats.

Scan

If McAfee VirusScan is installed, you can perform a manual scan of your computer.

Common Tasks

Perform common tasks including returning to the Home pane, viewing recent events, managing your computer network (if on a computer with management capability for this network), and maintaining your computer. If McAfee Data Backup is installed, you can also back up your data.

Components Installed

See which security services are protecting your computer's security.

Main pane

Protection Status

Under **Am I Protected?**, see the overall level of your computer's protection status. Below it, view a status breakdown by protection category and type.

SecurityCenter Information

See when the last update of your computer occurred, when the last scan occurred (if McAfee VirusScan is installed), as well as when your subscription expires.

In this chapter

Understanding SecurityCenter icons

SecurityCenter icons appear in your Windows notification area, at the far right of the taskbar. Use them to see whether your computer is fully protected, view the status of a scan in progress (if McAfee VirusScan is installed), check for updates, view recent events, maintain your computer, and get support from the McAfee Web site.

Open SecurityCenter and use additional features

When SecurityCenter is running, the SecurityCenter M icon M appears in your Windows notification area, at the far right of the taskbar.

To open SecurityCenter or use additional features:

- Right-click the main SecurityCenter icon, and click one of the following:
  - Open SecurityCenter
  - Updates
  - Quick Links

    The submenu contains links to Home, View Recent Events, Manage Network, Maintain Computer, and Data Backup (if installed).
  - Verify Subscription

    (This item appears when at least one product subscription is expired.)
  - Upgrade Center
  - Customer Support

Check your protection status

If your computer is not fully protected, the protection status icon ⊗ appears in your Windows notification area, at the far right of the taskbar. The icon can be red or yellow based on the protection status.

To check your protection status:

- Click the protection status icon to open SecurityCenter and fix any problems.

Check the status of your updates

If you are checking for updates, the updates icon appears in your Windows notification area, at the far right of the taskbar.

To check the status of your updates:

- Point to the updates icon to view the status of your updates in a tool tip.

Understanding the protection status

Your computer's overall security protection status is shown under **Am I Protected?** in SecurityCenter.

The protection status informs you whether your computer is fully protected against the latest security threats, or whether problems require attention and how to resolve them. When one problem affects more than one protection category, fixing the problem can result in multiple categories returning to fully protected status.

Some of the factors that influence your protection status include external security threats, the security products installed on your computer, products that access the Internet, and how these security and Internet products are configured.

By default, if Spam Protection or Content Blocking are not installed, these non-critical protection problems are automatically ignored and not tracked in the overall protection status. However, if a protection problem is followed by an **Ignore** link, you can choose to ignore the problem if you are sure that you do not want to fix it.

Am I Protected?

See the overall level of your computer's protection status under **Am I Protected?** in SecurityCenter:

- **Yes** appears if your computer is fully protected (green).
- **No** appears if your computer is partially protected (yellow) or not protected (red).

To resolve most protection problems automatically, click **Fix** next to the protection status. However, if one or more problems persist and require your response, click the link following the problem to take the suggested action.

Understanding protection categories and types

Under **Am I Protected?** in SecurityCenter, you can view a status breakdown consisting of these protection categories and types:

- Computer and Files
- Internet and Network
- E-mail and IM
- Parental Controls

The protection types shown in SecurityCenter depend on which products are installed. For example, the PC Health protection type appears if McAfee Data Backup software is installed.

If a category does not have any protection problems, its status is Green. If you click a Green category, a list of enabled protection types appears on the right, followed by a list of already ignored problems. If no problems exist, a virus advisory appears in place of any problems. You can also click **Configure** to change your options for that category.

If all of the protection types within a category have a status of Green, then the status of the category is Green. Likewise, if all of the protection categories have a status of Green, then the overall Protection Status is Green.

If any protection categories have a status of Yellow or Red, you can resolve the protection problems by fixing or ignoring them, which changes the status to Green.

Understanding Computer and Files protection

The Computer and Files protection category consists of these protection types:

- **Virus Protection** -- Real-time scanning protection defends your computer against viruses, worms, Trojan horses, suspect scripts, hybrid attacks, and other threats. It automatically scans and attempts to clean files (including .exe compressed files, boot sector, memory, and critical files) when they are accessed by either you or your computer.
- **Spyware Protection** -- Spyware protection quickly detects, blocks, and removes spyware, adware, and other potentially unwanted programs that might gather and transmit your private data without your permission.
- **SystemGuards** -- SystemGuards detect changes to your computer and alert you when they occur. You can then review these changes and decide whether to allow them.
- **Windows Protection** -- Windows protection provides the status of Windows Update on your computer. If McAfee VirusScan is installed, buffer overflow protection is also available.

One of the factors that influence your Computer and Files protection is external virus threats. For example, if a virus outbreak occurs, does your antivirus software protect you? Also, other factors include the configuration of your antivirus software and whether your software is continuously being updated with the latest detection signature files to protect your computer from the latest threats.

Open the Computer and Files configuration pane

When no problems exist under **Computer & Files**, you can open the configuration pane from the information pane.

To open the Computer and Files configuration pane:

1. In the Home pane, click **Computer & Files**.
2. In the right pane, click **Configure**.

Understanding Internet and Network protection

The Internet and Network protection category consists of these protection types:

- **Firewall Protection** -- Firewall protection defends your computer against intrusion and unwanted network traffic. It helps you manage inbound and outbound Internet connections.
- **Wireless Protection** -- Wireless protection defends your home wireless network against intrusion and data interception. However, if you are currently connected to an external wireless network, your protection varies based on the security level of that network.
- **Web Browsing Protection** -- Web browsing protection hides advertisements, pop-ups, and Web bugs on your computer when you browse the Internet.
- **Phishing Protection** -- Phishing protection helps block fraudulent Web sites that solicit personal information through hyperlinks in e-mail and instant messages, pop-ups, and other sources.
- **Personal Information Protection** -- Personal information protection blocks the release of sensitive and confidential information over the Internet.

Open the Internet and Network configuration pane

When no problems exist under **Internet & Network**, you can open the configuration pane from the information pane.

To open the Internet and Network configuration pane:

1. In the Home pane, click **Internet & Network**.
2. In the right pane, click **Configure**.

Understanding E-mail and IM protection

The E-mail and IM protection category consists of these protection types:

- **E-mail Protection** -- E-mail protection automatically scans and attempts to clean viruses, spyware, and potential threats in inbound and outbound e-mail messages and attachments.
- **Spam Protection** -- Spam protection helps block unwanted e-mail messages from entering your Inbox.
- **IM Protection** -- Instant Messaging (IM) protection automatically scans and attempts to clean viruses, spyware, and potential threats in inbound instant message attachments. It also blocks instant messaging clients from exchanging unwanted content or personal information over the Internet.
- **Safe Surfing protection** -- If installed, the McAfee SiteAdvisor browser plug-in helps protect you from spyware, spam, viruses, and online scams by rating Web sites you visit or that appear in your Web search results. You can view detailed safety ratings that show how a site tested for e-mail practices, downloads, online affiliations, and annoyances such as pop-ups and third-party tracking cookies.

Open the E-mail and IM configuration pane

When no problems exist under **E-mail & IM**, you can open the configuration pane from the information pane.

To open the E-mail and IM configuration pane:

1. In the Home pane, click **E-mail & IM**.
2. In the right pane, click **Configure**.

Understanding Parental Controls protection

The Parental Controls protection category consists of this protection type:

- **Parental Controls** -- Content Blocking prevents users from viewing unwanted Internet content by blocking potentially harmful Web sites. Users' Internet activity and usage can also be monitored and limited.

Open the Parental Controls configuration pane

When no problems exist under **Parental Controls**, you can open the configuration pane from the information pane.

To open the Parental Controls configuration pane:

1. In the Home pane, click **Parental Controls**.
2. In the right pane, click **Configure**.

Fixing protection problems

Most protection problems can be resolved automatically. However, if one or more problems persist, you must resolve them.

Fix protection problems automatically

Most protection problems can be resolved automatically.

To fix protection problems automatically:

- Click **Fix** next to the protection status.

Fix protection problems manually

If one or more protection problems are not resolved automatically, click the link following the problem to take the suggested action.

To fix protection problems manually:

- Do any of the following:
  - If a full scan of your computer has not been performed in the last 30 days, click **Scan** to the left of the main protection status to perform a manual scan. (This item appears if McAfee VirusScan is installed.)
  - If your detection signature (DAT) files are out-of-date, click **Update** to the left of the main protection status to update your protection.
  - If a program is not installed, click **Get full protection** to install it.
  - If a program is missing components, reinstall it.
  - If a program must be registered to receive full protection, click **Register now** to register it. (This item appears if one or more programs are expired.)
  - If a program is expired, click **Verify my subscription now** to check your account status. (This item appears if one or more programs are expired.)

Viewing SecurityCenter information

At the bottom of the protection status pane, SecurityCenter Information provides access to SecurityCenter options and shows you last update, last scan (if McAfee VirusScan is installed), and subscription expiration information about your McAfee products.

Open the SecurityCenter configuration pane

For your convenience, you can open the SecurityCenter configuration pane to change your options from the Home pane.

To open the SecurityCenter configuration pane:

- In the Home pane under **SecurityCenter Information,** click **Configure**.

View installed product information

You can view a list of installed products that shows the product version number and when the last update occurred.

To view your McAfee product information:

- In the Home pane under **SecurityCenter Information,** click **View Details** to open the product information window.

Using the Advanced Menu

When you first open SecurityCenter, the Basic Menu appears in the left-hand column. If you are an advanced user, you can click **Advanced Menu** to open a more detailed menu of commands in its place. For your convenience, the last menu you use is shown the next time you open SecurityCenter.

The Advanced Menu consists of the following items:

- Home
- Reports and Logs (includes the Recent Events list and logs by type for the past 30, 60, and 90 days)
- Configure
- Restore
- Tools

CHAPTER 4

Configuring SecurityCenter options

SecurityCenter shows your computer's overall security protection status, lets you create McAfee user accounts, automatically installs the latest product updates, and automatically notifies you with alerts and sounds for public virus outbreaks, security threats, and product updates.

In the SecurityCenter Configuration pane, you can change your SecurityCenter options for these features:

- Protection Status
- Users
- Automatic updates
- Alerts

In this chapter

Configuring the protection status

Your computer's overall security protection status is shown under **Am I Protected?** in SecurityCenter.

The protection status informs you whether your computer is fully protected against the latest security threats, or whether problems require attention and how to resolve them.

By default, if Spam Protection or Content Blocking are not installed, these non-critical protection problems are automatically ignored and not tracked in the overall protection status. However, if a protection problem is followed by an **Ignore** link, you can choose to ignore the problem if you are sure that you do not want to fix it. If you later decide to fix a previously ignored problem, you can include it in the protection status for tracking.

Configure ignored problems

You can include or exclude problems from being tracked as part of your computer's overall protection status. If a protection problem is followed by an **Ignore** link, you can choose to ignore the problem if you are sure that you do not want to fix it. If you later decide to fix a previously ignored problem, you can include it in the protection status for tracking.

To configure ignored problems:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to **Protection Status** to expand its pane, and then click **Advanced**.
3. Do one of the following in the Ignored Problems pane:
   - To include previously ignored problems in the protection status, clear their check boxes.
   - To exclude problems from the protection status, select their check boxes.
4. Click **OK**.

Configuring user options

If you are running McAfee programs that require user permissions, these permissions correspond by default to the Windows user accounts on your computer. To make it easier to manage users for these programs, you can switch to using McAfee user accounts at any time.

If you switch to using McAfee user accounts, any existing user names and permissions from your Parental Controls program are automatically imported. However, the first time you switch you must create an Administrator account. Afterward, you can start creating and configuring other McAfee user accounts.

Switch to McAfee user accounts

By default, you are using Windows user accounts. However, switching to McAfee user accounts makes it unnecessary to create additional Windows user accounts.

To switch to McAfee user accounts:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to **Users** to expand its pane, and then click **Advanced**.
3. To use McAfee user accounts, click **Switch**.

If you are switching to McAfee user accounts for the first time, you must create an Administrator acccount (page 23).

Create an Administrator account

The first time you switch to using McAfee users, you are prompted to create an Administrator account.

To create an Administrator account:

1. Enter a password in the **Password** box, and reenter it in the **Confirm Password** box.
2. Select a password recovery question in the list, and enter the answer to the secret question in the **Answer** box.
3. Click **Apply**.

   When you are finished, the user account type is updated in the pane with existing user names and permissions from your Parental Controls program, if any. If you are configuring user accounts for the first time, the Manage User pane appears.

Configure user options

If you switch to using McAfee user accounts, any existing user names and permissions from your Parental Controls program are automatically imported. However, the first time you switch you must create an Administrator account. Afterward, you can start creating and configuring other McAfee user accounts.

To configure user options:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to **Users** to expand its pane, and then click **Advanced**.
3. Under **User Accounts**, click **Add**.
4. Enter a user name in the **User Name** box.
5. Enter a password in the **Password** box, and reenter it in the **Confirm Password** box.
6. Select the **Startup User** check box if you want this new user to log in automatically when SecurityCenter starts.
7. Under **User Account Type**, select an account type for this user, and then click **Create**.

   Note: After creating the user account, you must configure the settings for a Limited User under Parental Controls.

8. To edit a user's password, automatic login, or account type, select a user name in the list, and click **Edit**.
9. When you are finished, click **Apply**.

Retrieve the Administrator password

If you forget the Administrator password, you can retrieve it.

To retrieve the Administrator password:

1. Right-click the SecurityCenter M icon M, and then click **Switch User**.
2. In the **User Name** list, select **Administrator**, and click **Forgot Password**.
3. Enter the answer to the secret question you selected when you created your Administrator account.
4. Click **Submit**.

   Your forgotten Administrator password appears.

Change the Administrator password

If you are having problems remembering the Administrator password or suspect that it might be compromised, you can change it.

To change the Administrator password:

1 Right-click the SecurityCenter M icon M, and then click **Switch User**.

2 In the **User Name** list, select **Administrator**, and click **Change Password.**

3 Enter your existing password in the **Old Password** box.

4 Enter your new password in the **Password** box, and reenter it in the **Confirm Password** box.

5 Click **OK**.

Configuring update options

SecurityCenter automatically checks for updates for all of your McAfee services every four hours when you are connected to the Internet, and then automatically installs the latest product updates. However, at any time you can manually check for updates using the SecurityCenter icon, in the notification area at the far right of the taskbar.

Check for updates automatically

SecurityCenter automatically checks for updates every four hours when you are connected to the Internet. However, you can configure SecurityCenter to notify you before downloading or installing updates.

To check for updates automatically:

1 Under **SecurityCenter Information**, click **Configure**.

2 Click the arrow next to the **Automatic updates are enabled** status to expand its pane, and then click **Advanced**.

3 Select one of the following in the Update Options pane:

- Install the updates automatically and notify me when the product is updated (recommended) (page 27)
- Download the updates automatically and notify me when they are ready to be installed (page 28)
- Notify me before downloading any updates (page 28)

4 Click **OK**.

Note: For maximum protection, McAfee recommends that you let SecurityCenter automatically check for and install updates. However, if you want to only manually update your security services, you can disable automatic updating (page 29).

Automatically download and install updates

If you select **Install the updates automatically and notify me when my services are updated (recommended)** in the SecurityCenter Update Options, SecurityCenter automatically downloads and installs updates.

Automatically download updates

If you select **Download the updates automatically and notify me when they are ready to be installed** in the Update Options, SecurityCenter automatically downloads updates, then notifies you when one is ready to be installed. You can then choose to install the update or postpone the update (page 29).

To install an automatically downloaded update:

1. Click **Update my products now** on the alert, and then click **OK**.

   If prompted, you must log in to the Web site to verify your subscription before the download can occur.

2. After your subscription is verified, click **Update** on the Updates pane to download and install the update. If your subscription is expired, click **Renew my subscription** on the alert and follow the prompts.

Note: In some cases, you will be prompted to restart your computer to complete the update. Save all of your work and close all programs before restarting.

Notify before downloading updates

If you select **Notify me before downloading any updates** in the Update Options pane, SecurityCenter notifies you before downloading any updates. You can then choose to download and install an update for your security services to remove the threat of an attack.

To download and install an update:

1. Select **Update my products now** on the alert, and then click **OK**.

2. If prompted, log in to the Web site.

   The update downloads automatically.

3. Click **OK** on the alert when the update is finished installing.

Note: In some cases, you will be prompted to restart your computer to complete the update. Save all of your work and close all programs before restarting.

Disable automatic updating

For maximum protection, McAfee recommends that you let SecurityCenter automatically check for and install updates. However, if you want to only manually update your security services, you can disable automatic updating.

Note: You must remember to manually check for updates (page 30) at least once a week. If you do not check for updates, your computer is not protected with the latest security updates.

To disable automatic updating:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to the **Automatic updates are enabled** status to expand its pane.
3. Click **Off**.
4. Click **Yes** to confirm the change.

   The status is updated in the header.

If you do not manually check for updates in seven days, an alert reminds you to check for updates.

Postpone updates

If you are too busy to update your security services when the alert appears, you can choose to be reminded later or ignore the alert.

To postpone an update:

- Do one of the following:
  - Select **Remind me later** on the alert, and click **OK**.
  - Select **Close this alert**, and click **OK** to close the alert without taking any action.

Check for updates manually

SecurityCenter automatically checks for updates every four hours when you are connected to the Internet, and then installs the latest product updates. However, at any time you can manually check for updates using the SecurityCenter icon in the Windows notification area at the far right of the task bar.

Note: For maximum protection, McAfee recommends that you let SecurityCenter automatically check for and install updates. However, if you want to only manually update your security services, you can disable automatic updating (page 29).

To check for updates manually:

1 Ensure that your computer is connected to the Internet.

2 Right-click the SecurityCenter M icon M in your Windows notification area, at the far right of the taskbar, and then click **Updates**.

While SecurityCenter is checking for updates, you can continue to perform other tasks with it.

For your convenience, an animated icon appears in your Windows notification area, at the far right of the taskbar. When SecurityCenter is finished, the icon automatically disappears.

3 If prompted, log in to the Web site to verify your subscription.

Note: In some cases, you will be prompted to restart your computer to complete the update. Save all of your work and close all programs before restarting.

Configuring alert options

SecurityCenter automatically notifies you with alerts and sounds for public virus outbreaks, security threats, and product updates. However, you can configure SecurityCenter to show only alerts that require your immediate attention.

Configure alert options

SecurityCenter automatically notifies you with alerts and sounds for public virus outbreaks, security threats, and product updates. However, you can configure SecurityCenter to show only alerts that require your immediate attention.

To configure alert options:

1 Under **SecurityCenter Information**, click **Configure**.

2 Click the arrow next to **Alerts** to expand its pane, and then click **Advanced**.

3 Select one of the following in the Alert Options pane:

- **Alert me when a public virus outbreak or security threat occurs**
- **Show informational alerts when gaming mode is detected**
- **Play a sound when an alert occurs**
- **Show McAfee splash screen at Windows startup**

4 Click **OK**.

Note: To disable future informational alerts from the alert itself, select the **Do not show this alert again** check box. You can enable them again later in the Informational Alerts pane.

Configure informational alerts

Informational alerts notify you when events occur that do not require your immediate response. If you disable future informational alerts from the alert itself, you can enable them again later in the Informational Alerts pane.

To configure informational alerts:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to **Alerts** to expand its pane, and then click **Advanced**.
3. Under **SecurityCenter Configuration**, click **Informational Alerts**.
4. Clear the **Hide informational alerts** check box, and then clear the check boxes for alerts in the list that you want to show.
5. Click **OK**.

CHAPTER 5

Performing common tasks

You can perform common tasks including returning to the Home pane, viewing recent events, managing your computer network (if on a computer with management capability for this network), and maintaining your computer. If McAfee Data Backup is installed, you can also back up your data.

In this chapter

Perform common tasks

You can perform common tasks including returning to the Home pane, viewing recent events, maintaining your computer, managing your network (if on a computer with management capability for this network), and backing up your data (if McAfee Data Backup is installed).

To perform common tasks:

- Under **Common Tasks** in the Basic Menu, do one of the following:
  - To return to the Home pane, click **Home**.
  - To view recent events detected by your security software, click **Recent Events**.
  - To remove unused files, defragment your data, and restore your computer to previous settings, click **Maintain Computer**.
  - To manage your computer network, click **Manage Network** on a computer with management capability for this network.

    Network Manager monitors computers across your network for security weaknesses, so you can easily identify network security issues.
  - To create backup copies of your files, click **Data Backup** if McAfee Data Backup is installed.

Automated backup saves copies of your most valuable files wherever you want, encrypting and storing your files on a CD/DVD, or a USB, external, or network drive.

Tip: For your convenience, you can perform common tasks from two additional locations (under **Home** in the Advanced Menu, and in the **QuickLinks** menu of the SecurityCenter M icon at the far right of the taskbar). You can also view recent events and comprehensive logs by type under **Reports and Logs** on the Advanced Menu.

View recent events

Recent events are logged when changes to your computer occur. Examples include when a protection type is enabled or disabled, when a threat is removed, or when an Internet connection attempt is blocked. You can view the 20 most recent events and their details.

See the help file of the relevant product for details about its events.

To view recent events:

1. Right-click the main SecurityCenter icon, point to **QuickLinks**, and then click **View Recent Events**.

   Any recent events appear in the list, showing the date and a brief description.

2. Under **Recent Events**, select an event to view additional information in the Details pane.

   Under **I want to**, any available actions appear.

3. To view a more comprehensive list of events, click **View Log**.

Maintain your computer automatically

To free up valuable drive space and optimize the performance of your computer, you can schedule QuickClean or Disk Defragmenter tasks to run at regular intervals. These tasks include deleting, shredding, and defragmenting files and folders.

To maintain your computer automatically:

1. Right-click the main SecurityCenter icon, point to **QuickLinks,** and then click **Maintain Computer**.
2. Under **Task Scheduler**, click **Start.**
3. In the operation list, select **QuickClean** or **Disk Defragmenter**.
4. Do one of the following:
   - To modify an existing task, select it, and then click **Modify**. Follow the on-screen instructions.

- To create a new task, enter the name in the **Task Name** box, and then click **Create**. Follow the on-screen instructions.
- To delete a task, select it, and then click **Delete**.

5 Under **Task Summary**, view when the task was last run, when it will run next, and its status.

Maintain your computer manually

You can perform manual maintenance tasks to remove unused files, defragment your data, or restore your computer to previous settings.

To maintain your computer manually:

- Do one of the following:
  - To use QuickClean, right-click the main SecurityCenter icon, point to **QuickLinks,** click **Maintain Computer**, and then click **Start**.
  - To use Disk Defragmenter, right-click the main SecurityCenter icon, point to **QuickLinks,** click **Maintain Computer**, and then click **Analyze**.
  - To use System Restore, on the Advanced Menu, click **Tools**, click **System Restore**, and then click **Start**.

Remove unused files and folders

Use QuickClean to free up valuable drive space and optimize the performance of your computer.

To remove unused files and folders:

1. Right-click the main SecurityCenter icon, point to **QuickLinks,** and then click **Maintain Computer**.
2. Under **QuickClean**, click **Start**.
3. Follow the on-screen instructions.

Defragment files and folders

File fragmentation occurs as files and folders are deleted and new files are added. This fragmentation slows disk access and degrades the overall performance of your computer, although usually not severely.

Use defragmentation to rewrite parts of a file to contiguous sectors on a hard disk to increase the speed of access and retrieval.

To defragment files and folders:

1. Right-click the main SecurityCenter icon, point to **QuickLinks**, and then click **Maintain Computer**.
2. Under **Disk Defragmenter**, click **Analyze**.
3. Follow the on-screen instructions.

Restore your computer to previous settings

Restore points are snapshots of your computer that Windows saves periodically and when significant events occur (such as when a program or driver is installed). However, you can create and name your own restore points at any time.

Use restore points to undo harmful changes to your computer and return to previous settings.

To restore your computer to previous settings:

1. On the Advanced Menu, click **Tools**, and then click **System Restore**.
2. Under **System Restore**, click **Start**.
3. Follow the on-screen instructions.

Manage your network

If your computer has management capability for your network, you can use Network Manager to monitor computers across your network for security weaknesses, so you can easily identify security issues.

If your computer's protection status is not being monitored on this network, your computer is either not part of this network, or an unmanaged member of this network. See the Network Manager help file for details.

To manage your network:

1. Right-click the main SecurityCenter icon, point to **QuickLinks**, and then click **Manage Network**.
2. Click the icon representing this computer on the network map.
3. Under **I want to**, click **Monitor this computer**.

Learn more about viruses

Use the Virus Information Library and the Virus Map to do the following:

- Learn more about the latest viruses, e-mail virus hoaxes, and other threats.
- Get free virus removal tools to help repair your computer.
- Get a real-time, bird's-eye view of where the latest computers are infecting computers worldwide.

To learn more about viruses:

1. On the Advanced Menu, click **Tools**, and then click **Virus Information**.
2. Do one of the following:
   - Research viruses using the free McAfee Virus Information Library.
   - Research viruses using the World Virus Map at the McAfee Web site.

CHAPTER 6

McAfee QuickClean

Clutter accumulates quickly on your computer when you surf the Internet. Protect your privacy and delete Internet and e-mail clutter you do not need with QuickClean. QuickClean identifies and deletes files that accumulate when surfing, including cookies, e-mail, downloads, and history—data that contains personal information about you. It protects your privacy by offering secure deletion of this sensitive information.

QuickClean also deletes unwanted programs. Specify the files you want to eliminate and wipe away the clutter without deleting essential information.

In this chapter

Understanding QuickClean features

This section describes QuickClean features.

Features

QuickClean provides a set of efficient and easy-to-use tools that safely delete digital debris. You can free valuable drive space and optimize the performance of your computer.

CHAPTER 7

Cleaning your computer

QuickClean lets you securely delete files and folders.

When you browse the Internet, your browser copies each Internet page and its graphics to a cache folder on your disk. The browser can then load the page quickly if you return to it again. Caching files is useful if you repeatedly visit the same Internet pages and their content does not change frequently. Most of the time, however, the cached files are not useful and can be deleted.

You can delete various items with the following cleaners.

- Recycle Bin Cleaner: Cleans your Windows Recycle Bin.
- Temporary Files Cleaner: Deletes files stored in temporary folders.
- Shortcut Cleaner: Deletes broken shortcuts and shortcuts without an associated program.
- Lost File Fragment Cleaner: Deletes lost file fragments from your computer.
- Registry Cleaner: Deletes Windows registry information for programs that no longer exist on your computer.
- Cache Cleaner: Deletes cached files that accumulate as you browse the Internet. Files of this type are usually stored as temporary Internet files.
- Cookie Cleaner: Deletes cookies. Files of this type are usually stored as temporary Internet files.
  Cookies are small files that your Web browser stores on your computer at the request of a Web server. Each time you view a Web page from the Web server, your browser sends the cookie back to the server. These cookies can act like a tag, which let the Web server track the pages you view and how often you return to them.
- Browser History Cleaner: Deletes your browser history.
- Outlook Express and Outlook E-mail Cleaner for deleted and sent items: Deletes mail from your Sent and Deleted Outlook folders.
- Recently Used Cleaner: Deletes recently used items stored on your computer, such as Microsoft Office documents.
- ActiveX and Plug-in Cleaner: Deletes ActiveX controls and Plug-ins.
  ActiveX is a technology used to implement controls in a program. An ActiveX control can add a button to a program's interface. Most of these controls are harmless; however, some people can use ActiveX technology to capture information from your computer.

Plug-ins are small software programs that plug into larger applications to provide added functionality. Plug-ins permit the Web browser to access and execute files embedded in HTML documents that are in formats the browser normally would not recognize (for example, animation, video, and audio files).

- System Restore Point Cleaner: Deletes old system restore points from your computer.

In this chapter

Using QuickClean

This section describes how to use QuickClean.

Clean your computer

You can delete unused files and folders, free up disk space, and enable your computer to run more efficiently.

To clean your computer:

1. On the Advanced Menu, click **Tools**.
2. Click **Maintain Computer**, and then click **Start** under **McAfee QuickClean**.
3. Do one of the following:
   - Click **Next** to accept the default cleaners in the list.
   - Select or clear the appropriate cleaners, and then click **Next.** For the Recently Used Cleaner, you can click **Properties** to clear the programs whose lists you do not want to clean.
   - Click **Restore Defaults** to restore the default cleaners, and then click **Next.**
4. After the analysis is performed, click **Next** to confirm file deletion. You can expand this list to see the files that are going to be cleaned and their location.
5. Click **Next.**
6. Do one of the following:
   - Click **Next** to accept the default **No, I want to delete files using standard Windows deletion**.
   - Click **Yes, I want to securely erase my files using Shredder**, and specify the number of passes. Files deleted with Shredder cannot be recovered.
7. Click **Finish**.
8. Under **QuickClean Summary**, view the number of registry files that were deleted and the amount of disk space reclaimed after disk and Internet cleanup.

CHAPTER 8

McAfee Shredder

Deleted files can be recovered from your computer even after you empty your Recycle Bin. When you delete a file, Windows marks that space on your disk drive as no longer being in use, but the file is still there. Using computer forensic tools, you can recover tax records, job resumes, or other documents that you deleted. Shredder protects your privacy by safely and permanently deleting unwanted files.

To permanently delete a file, you must repeatedly overwrite the existing file with new data. Microsoft® Windows does not securely delete files because every file operation would be very slow. Shredding a document does not always prevent that document from being recovered because some programs make temporary hidden copies of open documents. If you only shred documents that you see in Windows® Explorer, you could still have temporary copies of those documents.

Note: Shredded files are not backed up. You cannot restore files that Shredder has deleted.

In this chapter

Understanding Shredder features

This section describes Shredder features.

Features

Shredder allows you to erase your Recycle Bin contents, temporary Internet files, Web site history, files, folders, and disks.

CHAPTER 9

Erasing unwanted files with Shredder

Shredder protects your privacy by safely and permanently deleting unwanted files such as your Recycle Bin contents, temporary Internet files, and Web site history. You can select files and folders to shred, or browse to them.

In this chapter

Using Shredder

This section describes how to use Shredder.

Shred files, folders, and disks

Files can reside on your computer even after you empty your Recycle Bin. However, when you shred files, your data is permanently deleted and hackers cannot access it.

To shred files, folders, and disks:

1. On the Advanced Menu, click **Tools**, and then click **Shredder**.
2. Do one of the following:
   - Click **Erase files and folders** to shred files and folders.
   - Click **Erase an entire disk** to shred disks**.**
3. Select one of the following shredding levels:
   - **Quick**: Shreds the selected items 1 time.
   - **Comprehensive**: Shreds the selected items 7 times.
   - **Custom**: Shreds the selected items up to 10 times. A higher number of shredding passes increases your level of secure file deletion.
4. Click **Next**.
5. Do one of the following:
   - If you are shredding files, click **Recycle Bin contents**, **Temporary Internet files**, or **Web site history** in the **Select files to shred** list. If you are shredding a disk, click the disk.
   - Click **Browse**, navigate to the files you want to shred, and then select them.
   - Type the path to the files you want to shred in the **Select files to shred** list.
6. Click **Next**.
7. Click **Finish** to complete the operation.
8. Click **Done.**

CHAPTER 10

McAfee Network Manager

McAfee® Network Manager presents a graphical view of the computers and components that make up your home network. You can use Network Manager to remotely monitor the protection status of each managed computer in your network and to remotely fix reported security vulnerabilities on those managed computers.

Before you begin using Network Manager, you can familiarize yourself with some of the most popular features. Details about configuring and using these features are provided throughout the Network Manager help.

In this chapter

Features

Network Manager provides the following features:

Graphical network map

Network Manager's network map provides a graphical overview of the security status of the computers and components that make up your home network. When you make changes to your network (for example, adding a computer), the network map recognizes those changes. You can refresh the network map, rename the network, and show or hide components of the network map to customize your view. You can also view the details associated with any of the components displayed on the network map.

Remote management

Use the Network Manager network map to manage the security status of the computers that make up your home network. You can invite a computer to join the managed network, monitor the managed computer's protection status, and fix known security vulnerabilities from a remote computer on the network.

Understanding Network Manager icons

The following table describes the icons commonly used on the Network Manager network map.

Icon	Description
	Represents an online, managed computer
	Represents an offline, managed computer
	Represents an unmanaged computer that has McAfee 2007 security software installed
	Represents an offline, unmanaged computer
	Represents an online computer that does not have McAfee 2007 security software installed, or an unknown network device
	Represents an offline computer that does not have McAfee 2007 security software installed, or an offline, unknown network device
	Signifies that the corresponding item is protected and connected
	Signifies that the corresponding item requires your attention
	Signifies that the corresponding item requires your attention and is disconnected
	Represents a wireless home router
	Represents a standard home router
	Represents the Internet, when connected
	Represents the Internet, when disconnected

CHAPTER 11

Setting up a managed network

You set up a managed network by working with the items on your network map and adding members (computers) to the network.

In this chapter

Working with the network map

Each time that you connect a computer to the network, Network Manager analyzes the state of the network to determine if there are any members (managed or unmanaged), the router attributes, and the Internet status. If no members are found, Network Manager assumes that the currently connected computer is the first computer on the network and automatically makes the computer a managed member with administration permissions. By default, the name of the network includes the workgroup or domain name of the first computer that connects to the network with McAfee 2007 security software installed; however you can rename the network at any time.

When you make changes to your network (for example, adding a computer), you can customize the network map. For example, you can refresh the network map, rename the network, and show or hide components of the network map to customize your view. You can also view the details associated with any of the components displayed on the network map.

Access the network map

You access a map of your network by launching Network Manager from the SecurityCenter list of common tasks. The network map provides a graphical representation of the computers and components that make up your home network.

To access the network map:

- On the Basic or Advanced Menu, click **Manage Network**. The network map appears in the right pane.

Note: The first time that you access the network map, you are prompted to trust the other computers on the network before the network map appears.

Refresh the network map

You can refresh the network map at any time; for example, after another computer joins the managed network.

To refresh the network map:

1. On the Basic or Advanced Menu, click **Manage Network**. The network map appears in the right pane.
2. Click **Refresh the network map** under **I want to**.

Note: The **Refresh the network map** link is only available when no items are selected on the network map. To deselect an item, click the selected item, or click an area of white space on the network map.

Rename the network

By default, the name of the network includes the workgroup or domain name of the first computer that connects to the network with McAfee 2007 security software installed. If this name is not appropriate, you can change it.

To rename the network:

1. On the Basic or Advanced Menu, click **Manage Network**. The network map appears in the right pane.
2. Click **Rename the network** under **I want to**.
3. Type the name of the network in the **Rename network** box.
4. Click **OK**.

Note: The **Rename network** link is only available when no items are selected on the network map. To deselect an item, click the selected item, or click an area of white space on the network map.

Show or hide items on the network map

By default, all of the computers and components in your home network are shown on the network map. However, if you have hidden items, you can show them again at any time. Only unmangaged items can be hidden; managed computers cannot be hidden.

To...	On the Basic or Advanced Menu, click **Manage Network**, and then do this...
Hide an item on the network map	Click an item on the network map, and then click **Hide this item** under **I want to**. In the confirmation dialog box, click **Yes**.
Show hidden items on the network map	Under **I want to**, click **Show hidden items**.

View item details

You can view detailed information about any component in your network by selecting the component on the network map. This information includes the component name, its protection status, and other information required to manage the component.

To view an item's details:

1. Click an item's icon on the network map.
2. Under **Details**, view the information about the item.

Joining the managed network

Before a computer can be remotely managed or can be granted permission to remotely manage other computers on the network, it must become a trusted member of the network. Network membership is granted to new computers by existing network members (computers) with administration permissions. To ensure that only trusted computers join the network, users at both the granting and joining computers must authenticate each other.

When a computer joins the network, it is prompted to expose its McAfee protection status to other computers on the network. If a computer agrees to expose its protection status, it becomes a *managed* member of the network. If a computer refuses to expose its protection status, it becomes an *unmanaged* member of the network. Unmanaged members of the network are usually guest computers who want to access other network features (for example, file or printer sharing).

Note: After joining, if you have other McAfee networking programs installed (for example, McAfee Wireless Network Security or EasyNetwork), the computer is also recognized as a managed computer in those programs. The permission level that is assigned to a computer in Network Manager applies to all McAfee networking programs. For more information about what guest, full, or administrative permissions mean in other McAfee networking programs, see the documentation provided for that program.

Join a managed network

When you receive an invitation to join a managed network, you can either accept or reject the invitation. You can also determine whether you want this computer and other computers on the network to monitor each other's security settings (for example, whether or not a computer's virus protection services are up-to-date).

To join a managed network:

1. In the invitation dialog box, enable the **Allow this computer and other computers to monitor each other's security settings** check box to allow other computers on the managed network to monitor your computer's security settings.
2. Click **Join**.
   When you accept the invitation, two playing cards are displayed.
3. Confirm that the playing cards are the same as those displayed on the computer that invited you to join the managed network.
4. Click **Confirm**.

Note: If the computer that invited you to join the managed network is not displaying the same playing cards that are displayed in the security confirmation dialog box, there has been a security breach on the managed network. Joining the network could put your computer at risk; therefore, click **Reject** in the security confirmation dialog box.

Invite a computer to join the managed network

If a computer is added to the managed network or another unmanaged computer exists on the network, you can invite that computer to join the managed network. Only computers with administration permissions on the network can invite other computers to join the network. When you send the invitation, you also specify the permission level you want to assign to the joining computer.

To invite a computer to join the managed network:

1. Click an unmanaged computer's icon in the network map.
2. Click **Monitor this computer**, under **I want to.**
3. In the Invite a computer to join this managed network dialog box, click one of the following:
   - **Grant guest access**
     Guest access allows the computer access to the network.

- **Grant full access to all managed network applications**
  Full access (like guest access) allows the computer access to the network.
- **Grant administrative access to all managed network applications**
  Administrative access allows the computer access to the network with administration permissions. It also allows the computer to grant access to other computers who want to join the managed network.

4. Click **Invite**.
   An invitation to join the managed network is sent to the computer. When the computer accepts the invitation, two playing cards are displayed.
5. Confirm that the playing cards are the same as those displayed on the computer that you have invited to join the managed network.
6. Click **Grant Access**.

Note: If the computer that you invited to join the managed network is not displaying the same playing cards that are displayed in the security confirmation dialog box, there has been a security breach on the managed network. Allowing the computer to join the network could put other computers at risk; therefore, click **Reject Access** in the security confirmation dialog box.

Stop trusting computers on the network

If you mistakenly agree to trust the other computers on the network, you can stop trusting them.

To stop trusting computers on the network:

- Click **Stop trusting computers on this network**, under **I want to**.

Note: The **Stop trusting computers on this network** link is only available when no other managed computers have joined the network.

CHAPTER 12

Managing the network remotely

After you set up your managed network, you can use Network Manager to remotely manage the computers and components that make up your network. You can monitor the status and permission levels of the computers and components and fix security vulnerabilities remotely.

In this chapter

Monitoring status and permissions

A managed network has two types of members: managed members and unmanaged members. Managed members allow other computers on the network to monitor their McAfee protection status; unmanaged members do not. Unmanaged members are usually guest computers who want to access other network features (for example, file or printer sharing). An unmanaged computer can be invited to become a managed computer at any time by another managed computer on the network. Similarly, a managed computer can become unmanaged at any time.

Managed computers have either administration, full, or guest permissions associated with them. Administration permissions allow the managed computer to manage the protection status of all other managed computers on the network and to grant other computers membership to the network. Full and guest permissions allow a computer to access the network only. You can modify a computer's permission level at any time.

Because a managed network also consists of devices (for example, routers), you can use Network Manager to manage these as well. You can also configure and modify a device's display properties on the network map.

Monitor a computer's protection status

If a computer's protection status is not being monitored on the network (either because the computer is not a member of the network or the computer is an unmanaged member of the network), you can make a request to monitor it.

To monitor a computer's protection status:

1. Click an unmanaged computer's icon on the network map.
2. Click **Monitor this computer**, under **I want to**.

Stop monitoring a computer's protection status

You can stop monitoring the protection status of a managed computer in your private network. The computer then becomes an unmanaged computer.

To stop monitoring a computer's protection status:

1. Click a managed computer's icon on the network map.
2. Click **Stop monitoring this computer**, under **I want to**.
3. In the confirmation dialog box, click **Yes**.

Modify a managed computer's permissions

You can modify a managed computer's permissions at any time. This allows you to adjust which computers can monitor the protection status (security settings) of other computers on the network.

To modify a managed computer's permissions:

1. Click a managed computer's icon on the network map.
2. Click **Modify permissions for this computer**, under **I want to**.
3. In the modify permissions dialog box, select or clear the check box to determine whether this computer and other computers on the managed network can monitor each other's protection status.
4. Click **OK**.

Manage a device

You can manage a device by accessing its administration Web page from within Network Manager.

To manage a device:

1. Click a device's icon on the network map.
2. Click **Manage this device**, under **I want to**.
   A Web browser opens and displays the device's administration Web page.
3. In your Web browser, provide your login information and configure the device's security settings.

Note: If the device is a Wireless Network Security protected wireless router or access point, you must use Wireless Network Security to configure the device's security settings.

Modify a device's display properties

When you modify a device's display properties, you can change the device's display name on the network map and specify whether the device is a wireless router.

To modify a device's display properties:

1. Click a device's icon on the network map.
2. Click **Modify device properties** under **I want to**.
3. To specify the device's display name, type a name in the **Name** box.
4. To specify the type of device, click one of the following:
   - **Router**
     This represents a standard home router.
   - **Wireless Router**
     This represents a wireless home router.
5. Click **OK**.

Fixing security vulnerabilities

Managed computers with administration permissions can monitor the McAfee protection status of other managed computers on the network and fix any reported security vulnerabilities remotely. For example, if a managed computer's McAfee protection status indicates that VirusScan is disabled, another managed computer with administration permissions can *fix* this security vulnerability by enabling VirusScan remotely.

When you fix security vulnerabilities remotely, Network Manager automatically repairs most reported issues. However, some security vulnerabilities might require manual intervention on the local computer. In this case, Network Manager fixes those issues that can be repaired remotely, and then prompts you to fix the remaining issues by logging in to SecurityCenter on the vulnerable computer and following the recommendations provided. In some cases, the suggested fix is to install McAfee 2007 security software on the remote computer or computers on your network.

Fix security vulnerabilities

You can use Network Manager to automatically fix most security vulnerabilities on remote, managed computers. For example, if VirusScan is disabled on a remote computer, you can use Network Manager to enable it automatically.

To fix security vulnerabilities:

1. Click an item's icon on the network map.
2. View the item's protection status, under **Details**.
3. Click **Fix security vulnerabilities** under **I want to**.
4. When the security issues have been fixed, click **OK**.

Note: Although Network Manager automatically fixes most security vulnerabilities, some repairs may require you to launch SecurityCenter on the vulnerable computer and follow the recommendations provided.

Install McAfee security software on remote computers

If one or more computers on your network are not running McAfee 2007 security software, their security status cannot be monitored remotely. If you want to monitor these computers remotely, you must go to each computer, and install the McAfee 2007 security software.

To install McAfee security software on a remote computer:

1. In a browser on the remote computer, go to http://download.mcafee.com/us/.
2. Follow the on-screen instructions to install McAfee 2007 security software on the computer.

CHAPTER 13

McAfee Wireless Network Security

Wireless Network Security provides industry standard, automatic protection against data theft, unauthorized network access, and broadband "freeloading" through an easy and intuitive one-click interface. Wireless Network Security encrypts your personal and private data as it is sent over Wi-Fi and blocks hackers from accessing your wireless network.

Wireless Network Security blocks hackers from attacking your network your wireless network by:

- Preventing unauthorized connects to the Wi-Fi network
- Preventing capture of data that is transmitted over a Wi-Fi network
- Detecting connection attempts to a Wi-Fi network

Wireless Network Security combines ease-of-use features, such as instant network lockdown and the ability to quickly add legitimate users to the network, with robust security features such as automatic encrypted key generation and scheduled key rotation.

In this chapter

Features

Wireless Network Security offers the following features.

Always-on protection

Wireless Network Security automatically detects and protects any vulnerable wireless network that you connect to.

Intuitive interface

Protect your network without having to make difficult decisions or knowing complex technical terms.

Strong automatic encryption

Only let your friends and family have access to your network and protect your data as it travels back and forth.

Software only solution

Wireless Network Security works with your standard wireless router or access point and security software. You do not need to buy additional hardware.

Automatic key rotation

Even the most determined hackers cannot capture your information because the key is continuously rotating.

Addition of network users

You can easily grant your friends and family access to your network. You can add users wirelessly or by transferring software via a USB drive.

Intuitive connection tool

The wireless connection tool is intuitive and informative, with details about signal strength and security state.

Event logging and alerts

Easy to understand reports and alerts offer advanced users more information on your wireless network.

Suspend mode

Temporarily suspend key rotation so that particular applications can run without interruption.

Compatibility with other equipment

Wireless Network Security automatically updates itself with the latest wireless router or access point modules from the most popular brands including: Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet®, and others.

Starting Wireless Network Security

After installation, Wireless Network Security is automatically enabled; you are not required to start it manually. Optionally, however, you can manually enable and disable wireless protection.

After you install Wireless Network Security, your computer attempts to establish a connection to the wireless router. Once the connection is established, the computer programs the encryption key into the wireless router. If the default password has been changed, you are prompted for the password so that Wireless Network Security can configure the wireless router with the shared encryption key, and a strong security mode. Your computer is also configured with the same shared key and encryption mode, establishing a secure wireless connection.

Start Wireless Network Security

Wireless Network Security is enabled by default; however, you can manually enable and disable wireless protection.

Enabling wireless protection defends your wireless network against intrusion and data interception. However, if you are connected to an external wireless network, your protection varies based on its level of security.

To manually enable wireless protection:

1 On the McAfee SecurityCenter pane, do one of the following:

- Click **Internet & Network**, and then **Configure**.
- Click **Advanced Menu**, then **Configure** on the **Home** pane, and then point to **Internet & Network**.

2 On the **Internet & Network Configuration** pane, under **Wireless protection**, click **On**.

Note: Wireless Network Security is automatically enabled if you have a compatible wireless adapter installed.

Stop Wireless Network Security

Wireless Network Security is enabled by default; however, you can manually enable and disable wireless protection.

Disabling wireless protection leaves your network vulnerable to intrusion and data interception.

To disable wireless protection:

1. On the McAfee SecurityCenter pane, do one of the following:
    - Click **Internet & Network**, and then **Configure**.
    - Click **Advanced Menu**, then **Configure** on the **Home** pane, and then point to **Internet & Network**.
2. On the **Internet & Network Configuration** pane, under **Wireless protection**, click **Off**.

CHAPTER 14

Protecting wireless networks

Wireless Network Security protects your network by implementing wireless encryption (either through WEP, WPA, or WPA2 depending on your equipment). It automatically programs clients and wireless routers with the valid encryption key credentials, so that the wireless router authorizes computers to connect.Wireless networks protected with encryption block unauthorized users from accessing the wireless network and protects data that is sent over a wireless network. Wireless Network Security accomplishes this by:

- Creating and distributing a long, strong, random, and shared encryption key
- Rotating the encryption key on a scheduled basis
- Configuring each wireless device with encryption keys

In this chapter

Setting up protected wireless networks

When Wireless Network Security is installed, it automatically prompts you to protect the insecure wireless network that you are connected to or to join a previously protected wireless network.

If you are not connected a wireless network, Wireless Network Security scans for a McAfee-protected network with a strong signal strength and prompts the user to join the network. If no protected networks are available, Wireless Network Security scans for insecure networks with strong signals and when one is found, prompts you to protect that network.

Unless a wireless network has been protected by McAfee Wireless Network Security, McAfee considers wireless networks as “unprotected” -- even if they use wireless security mechanisms such as WEP and WPA.

Unless a wireless network is protected by Wireless Network Security, McAfee considers the network unprotected, even it it employs wireless security mechanism such as WEP and WPA.

About access types

Any wireless computer with Wireless Network Security installed can create a protected wireless network. The first computer to protect a router and create a protected wireless network is automatically granted administrative access on that network. Computers that join later can be granted administrative, full, or guest access by an existing user with administrative access.

Computers with administrative and full access types can perform the following tasks:

- Protect and remove a router or access point
- Rotate security keys
- Change network security settings
- Repair networks
- Grant computers access to the network
- Revoke access to the protected wireless network
- Change a computer's administration level

Computers with guest access types can perform the following tasks on the network:

- Connect to a network
- Join a network
- Modify settings specific to the guest computer

Note: Computers can have administrative access on one wireless network but guest or full access on another. A computer which has guest or full access on a network can create a new network.

Related topics

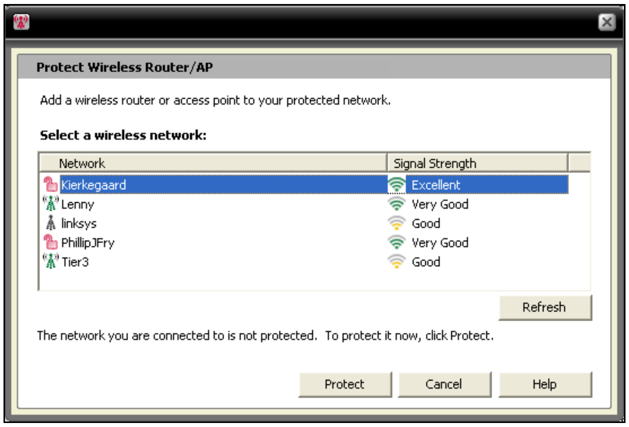
- Join a protected wireless network (page 78)
- Grant computers administrative access (page 82)
- Revoke network access (page 99)

Create protected wireless networks

To create a protected wireless network, you must first add the wireless network's wireless router or access point.

To add a wireless router or access point:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select View Tools.
3. On the Protection Tools pane, under Protect Wireless Router/AP, click Protect.
4. On the Protect Wireless Router/AP pane, select a wireless network to protect, and then click Protect.



Protect Wireless Router/AP

Add a wireless router or access point to your protected network.

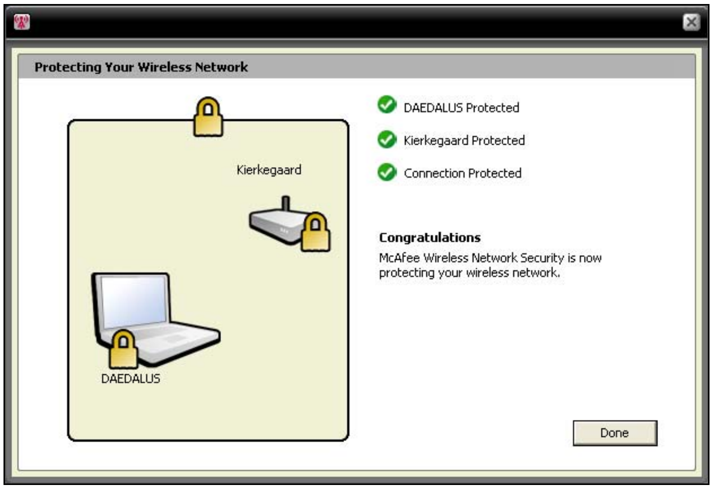
Select a wireless network:

Network	Signal Strength
Kierkegaard	Excellent
Lenny	Very Good
linksys	Good
PhillipJFry	Very Good
Tier3	Good

The network you are connected to is not protected. To protect it now, click Protect.

Protecting Your Wireless Network pane appears as Wireless Network Security attempts to protect your computer, router, and network connection.

Successful protection of all these components results in the total protection of your wireless network.



Protecting Your Wireless Network

✓ DAEDALUS Protected

✓ Kierkegaard Protected

✓ Connection Protected

Congratulations

McAfee Wireless Network Security is now protecting your wireless network.

5 Click Done.

Note: After you protect a network, the Your Next Steps dialog reminds you to install Wireless Network Security on each of your wireless computers to allow them to join the network.

If you had previously manually configured a pre-shared key for your router or access point and you were not connected when you tried to protect the router or access point, you must also enter the key in the WEP Key box, and then click Connect. If you had previously changed your wireless router's administrative user name or password, you are prompted to enter this information prior to protecting a router or access point.

Related topics

- Protect other wireless devices (page 83)
- Add computers to the protected wireless network (page 85)

Join protected wireless networks

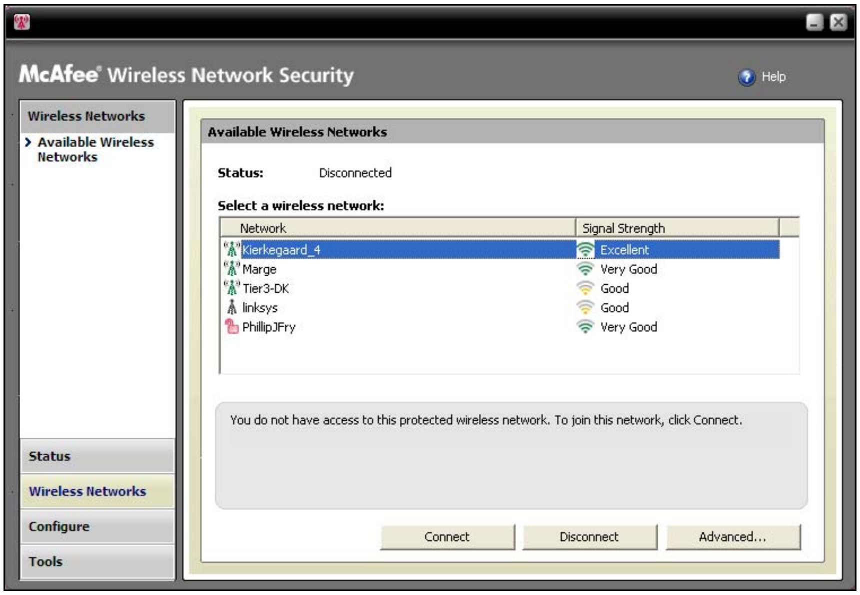
A protected network prevents hackers from intercepting data that is transmitted across the network and from connecting to your network. Before an authorized computer can access a protected wireless network, they must first join it.

When a computer requests to join the managed network, a message is sent to the other computers on the network who have administrative access. As the administrator, you are responsible for deciding which type of access to grant the computer: guest, full, or administrative.

Before you can join a protected network, you must install Wireless Network Security and then connect to the protected wireless network. An existing network user with administrative access on the protected wireless network must allow you to join. After you join the network, it is unnecessary to rejoin it when reconnecting. Both the grantor and the joiner must have an active wireless connection. The grantor must be an administrator computer that is connected to the network.

To join a protected wireless network:

1. On the unprotected computer, right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Wireless Networks**.
3. On the Available Wireless Networks pane, select a network, and then click **Connect**.


McAfee Wireless Network Security
Help
Wireless Networks
Available Wireless Networks
Status
Wireless Networks
Configure
Tools
Available Wireless Networks
Connect
Disconnect
Advanced...

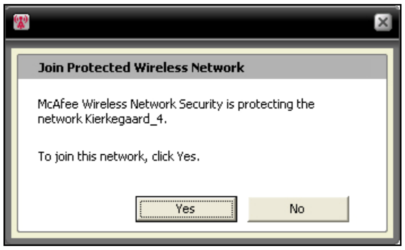
Status: Disconnected

Select a wireless network:

Network	Signal Strength
Kierkegaard_4	Excellent
Marge	Very Good
Tier3-DK	Good
linksys	Good
PhillipJFry	Very Good

You do not have access to this protected wireless network. To join this network, click Connect.

4 On the Join Protected Wireless Network dialog, click **Yes** to join the network.

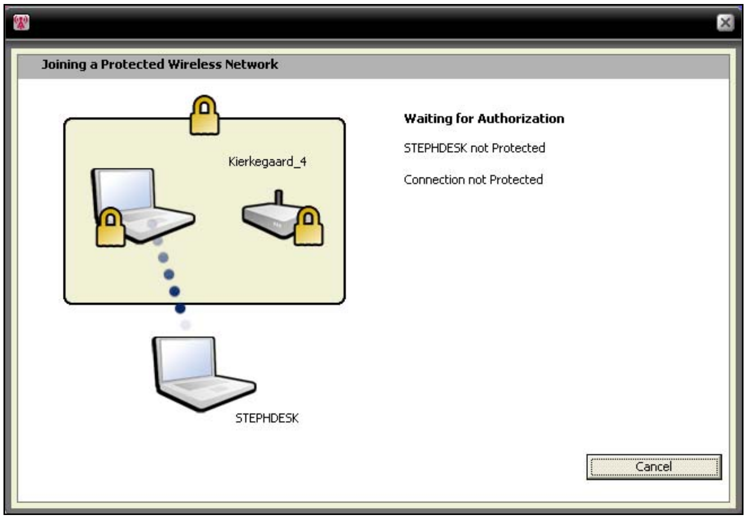


Join Protected Wireless Network

McAfee Wireless Network Security is protecting the network Kierkegaard_4.

To join this network, click Yes.

As Wireless Network Security attempts to request permission to join the network, the Joining a Protected Wireless Network pane appears on the computer attempting to join the network.



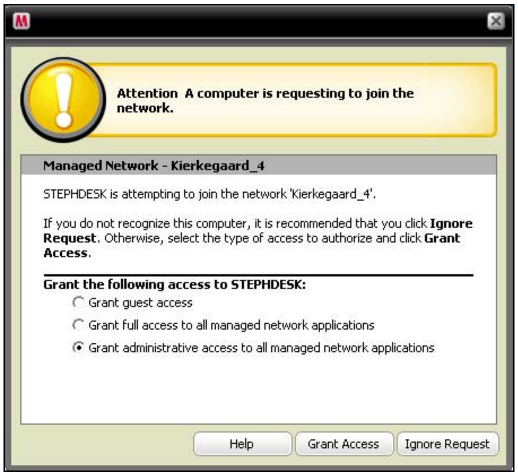
Joining a Protected Wireless Network

Waiting for Authorization

STEPHDESK not Protected

Connection not Protected

5 The Join the Network pane appears on the the administrator computer from which guest, full, or administrative access can be granted.



Attention A computer is requesting to join the network.

Managed Network - Kierkegaard_4

STEPHDESK is attempting to join the network 'Kierkegaard_4'.

If you do not recognize this computer, it is recommended that you click **Ignore Request**. Otherwise, select the type of access to authorize and click **Grant Access**.

Grant the following access to STEPHDESK:

○ Grant guest access

○ Grant full access to all managed network applications

● Grant administrative access to all managed network applications

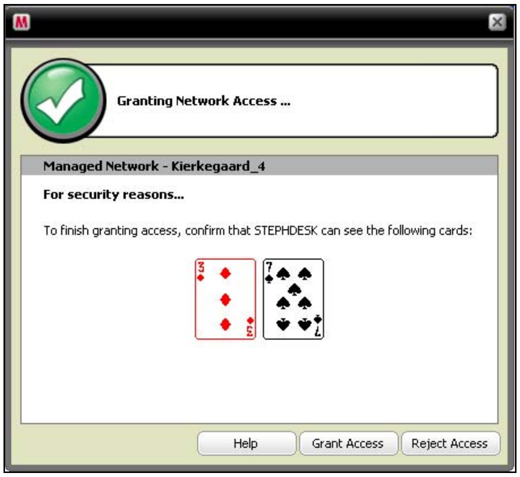
On the Join the Network dialog, select one of the following options:

Grant guest access	Allows the computer to send files to other computers on the wireless network, but not share files with McAfee EasyNetwork.
Grant full access to all managed network applications	Allows the computer to send and share files with McAfee EasyNetwork.
Grant administrative access to all managed network applications:	Allows the computer to send and share files with McAfee EasyNetwork, grant access to other computers, and adjust other computers' access levels on the wireless network.

6 Click **Grant Access**.

7 Confirm that the cards displayed on the Granting Network Access pane match those displayed on the computer attempting to join the wireless network. If the cards match, click **Grant Access**.

If the computers do not display identical playing cards, a potential security breach has occurred. Granting this computer access to the network could put your computer at risk. To prohibit the computer from accessing the wireless network, click **Reject Access**.



Granting Network Access ...

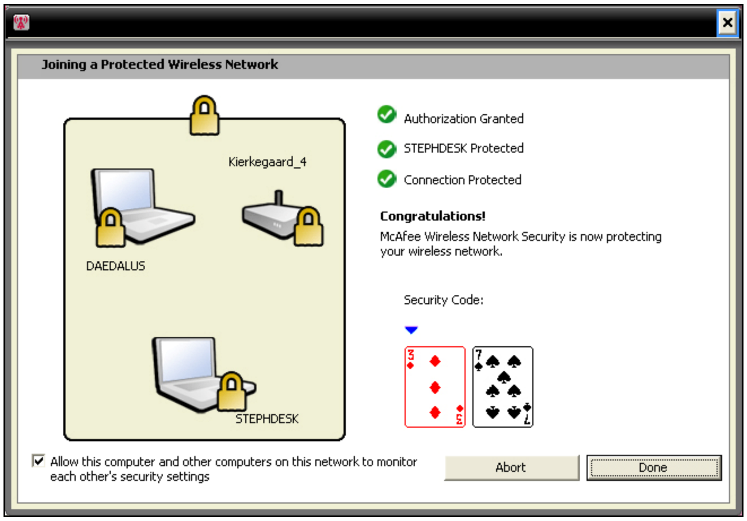
Managed Network - Kierkegaard_4

For security reasons...

To finish granting access, confirm that STEPHDESK can see the following cards:

8 The Granting Network Access pane confirms that the new computer is protected by Wireless Network Security. To monitor the security settings of, and to be monitored by, other computers, select **Allow this computer and other**

computers on this network to monitor each other's security settings.



Joining a Protected Wireless Network

✓ Authorization Granted

✓ STEPHDESK Protected

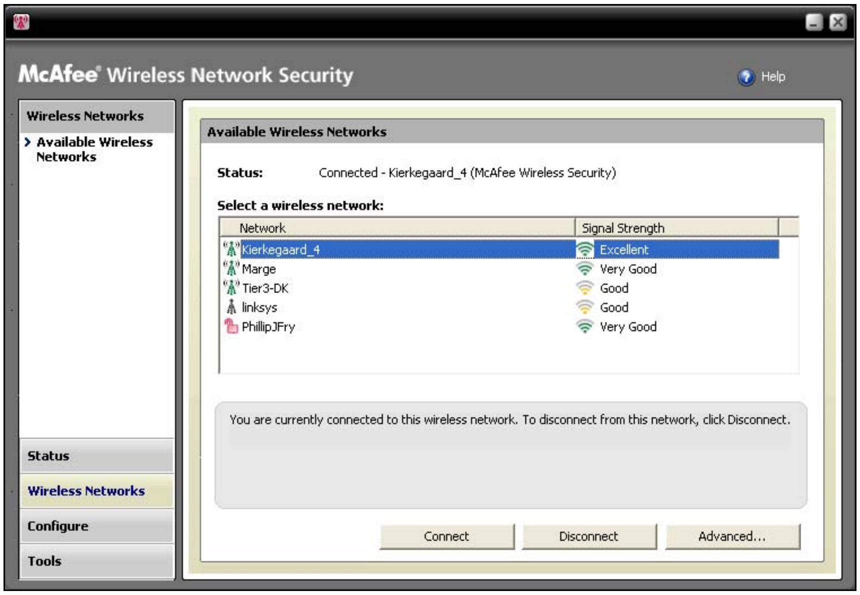
✓ Connection Protected

Congratulations!
McAfee Wireless Network Security is now protecting your wireless network.

☑ Allow this computer and other computers on this network to monitor each other's security settings

9 Click **Done**.

10 The Available Wireless Networks pane shows that you are connected to the protected wireless network.



Available Wireless Networks

Status: Connected - Kierkegaard_4 (McAfee Wireless Security)

Select a wireless network:

Network	Signal Strength
Kierkegaard_4	Excellent
Marge	Very Good
Tier3-DK	Good
linksys	Good
PhillipJFry	Very Good

You are currently connected to this wireless network. To disconnect from this network, click Disconnect.

Related topics

- Add computers to the protected wireless network (page 85)

Connect to protected wireless networks

If you have already joined a protected wireless network, but later disconnected and your access was not revoked, you can reconnect any time without having to rejoin.

To connect to a protected wireless network:

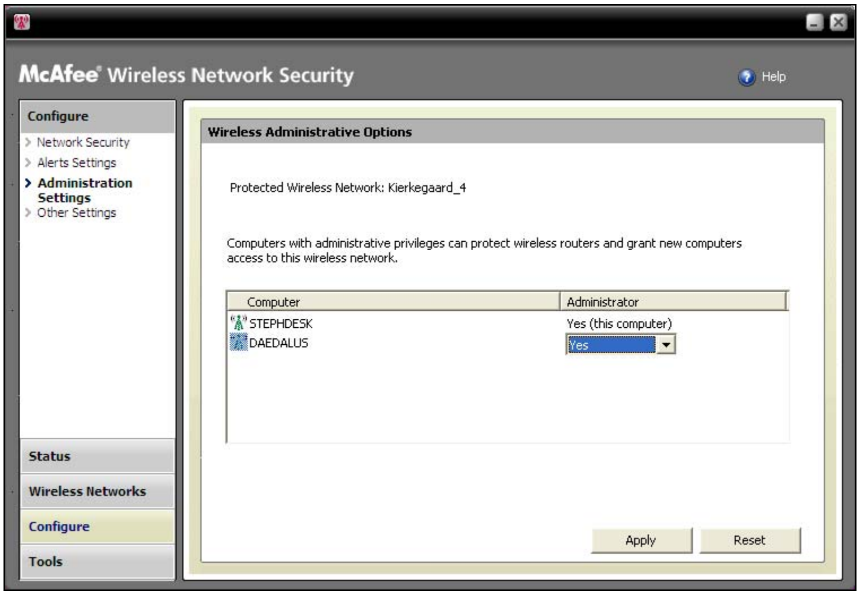
1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Wireless Networks**.
3. On the Available Wireless Networks pane, select a network, and then click **Connect**.

Grant computers administrative access

Computers with administrative privileges can protect wireless routers, change security modes, and grant new computers access to the protected wireless network.

To configure administrative access:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. On the Configure pane, select **Administration Settings**.
4. On the Wireless Administration Options pane, select **Yes** or **No** to allow or disallow administrative access.



Wireless Administrative Options

Protected Wireless Network: Kierkegaard_4

Computers with administrative privileges can protect wireless routers and grant new computers access to this wireless network.

Computer	Administrator
STEPHDESK	Yes (this computer)
DAEDALUS	Yes

5 Click **Apply**.

Related topics

- About access types (page 75)
- Revoke network access (page 99)

Protect other wireless devices

Wireless Network Security allows you to add other wireless devices to the network, including wireless printers, print servers, or game consoles.

To add other wireless devices:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Tools**.

3 On the Protection Tools pane, under **Protect Non-AP Devices**, click **Protect**.

4 On the Protect a Wireless Device pane, select a wireless device, and then click **Protect**.

5 The Non-AP Device Protected alert confirms that the device has been added to the network.

Connect to Broadcast SSID-disabled networks

You can connect to wireless networks that have Broadcast SSID disabled. When routers have Broadcast SSID disabled, they do not appear on the Available Wireless Networks pane.

McAfee recommends that you do not protect wireless routers that have disabled Broadcast SSID with Wireless Network Security.

To connect to a wireless network with Broadcast SSID disabled:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Wireless Networks**.

3 On the Available Wireless Networks pane, click **Advanced**.

4 On the Wireless Networks pane, click **Add**.

5 On the Add Wireless Network pane, specify the following settings, and then click **OK**:

Setting	Description
Network	The name of your network. If you are modifying a network, you cannot change the name.
Security Settings	The security for your unprotected network. Note that if the wireless adapter does not support the mode you select, you cannot connect. Security modes include: Disabled, Open WEP, Shared WEP, Auto WEP, WPA-PSK, WPA2-PSK.
Encryption Mode	The encryption associated with the security mode you selected. Encryption modes include: WEP, TKIP, AES, and TKIP+AES.

Note: McAfee recommends that you do not protect wireless routers that have disabled Broadcast SSID with Wireless Network Security. If you must use this feature, only do so when broadcast SSID is disabled.

Add computers to the protected wireless network

You can add computers to the protected wireless network using a removable device, such as a USB flash drive, writable CD, or Windows Connect Now technology.

Add computers using a removable device

Wireless Network Security allows you add additional computers to the protected wireless network that are not running Wireless Network Security, using a USB flash drive or a writable CD.

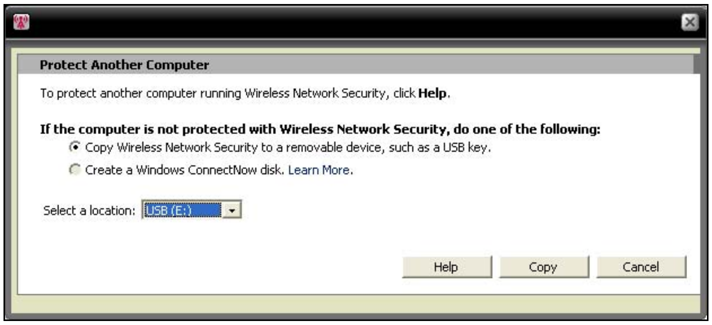
To add a computer:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Tools**.

3 On the Protection Tools pane, under **Protect a Computer**, click **Protect**.

4 On the Protect Another Computer pane, select **Copy Wireless Network Security to a removable device, such as a USB key**.



Protect Another Computer

To protect another computer running Wireless Network Security, click **Help**.

If the computer is not protected with Wireless Network Security, do one of the following:

● Copy Wireless Network Security to a removable device, such as a USB key.

○ Create a Windows ConnectNow disk. Learn More.

Select a location: USB (E:)

5. Select a location of the CD Drive or USB flash drive on which to copy Wireless Network Security.
6. Click **Copy**.
7. After all the files are copied to the CD or USB flash drive, insert the removable device into the computer that you want to protect. If the program does not automatically launch, browse the contents of the removable medium from Windows Explorer, and then click **Install.exe**.
8. Follow the instructions on your screen.

Note: You can also add a computer to the protected wireless network using Windows Connect Now technology.

Related topics

- Add computers using Windows Connect Now technology (page 87)

Add computers using Windows Connect Now technology

Wireless Network Security allows you add additional computers to your network that are not running Wireless Network Security, using Windows Connect Now technology.

To add a computer using Windows Connect Now technology:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Tools**.
3. On the Protection Tools pane, under **Protect a Computer**, click **Protect**.
4. On the Protect Another Computer pane, select **Create a Windows Connect Now disk**
5. Select a location to copy the Windows Connect Now information.
6. Click **Copy**.
7. Insert the Windows Connect Now disk in to the computer you want to protect
8. If the disk does not start automatically, do one of the following:
   - Install Wireless Connect Now technology: Click **Start** from the Windows taskbar, and then click Control Panel. If you're using the Category view of Control Panel, click **Network and Internet Connections**, and then click **Wireless Network Setup Wizard**. If you're using the Classic view of Control Panel, click **Wireless Network Setup Wizard**. Follow the instructions on your screen.
   - Open `setupSNK.exe` on the Windows Connect disk and copy and paste the key into your wireless network selection client.

Note: Suspend key rotation if you use Windows Connect Technology to connect to the wireless network, otherwise your network connection will fail. The connection fails because key rotation creates a new key that differs from the key used by Windows Connect Now Technology.

You can also add computers to the protected wireless network using a removable device, such as a writable CD or USB flash drive.

Related topics

- Add computers using a removable device (page 85)

CHAPTER 15

Administering wireless networks

Wireless Network Security provides a full set of administration tools to help you manage and maintain your wireless network.

In this chapter

Managing wireless networks

When you are connected to a protected wireless network, the information that is sent and received is encrypted. Hackers cannot decrypt the data that is transmitted over the protected network and cannot connect to your network. Wireless Network Security provides a number of tools to help you manage your network to prevent further intrusion.

About Wireless Network Security icons

Wireless Network Security displays icons to represent various network connection types and signal strengths.

Network connection icons

The following table describes the icons commonly used by Wireless Network Security in the Wireless Network Status panes and the Protection Tools and Available Wireless Networks panes. The icons represent various network connection and security states.

Icon	Status panes	Protection Panes
📡	Your computer is connected to the selected protected wireless network.	The device is protected by Wireless Network Security.
📡	Your computer can access the protected wireless network, but is not currently connected.	The device uses WEP or WPA security.
🔓	Your computer is a former member of the protected wireless network, but access was revoked when the computer was disconnected from the network.	The device has Wireless Network Security disabled.

Signal strength icons

The following table describes the icons commonly used by Wireless Network Security to represent various network signal strengths.

Icon	Description
📶	Excellent signal strength
📶	Very good signal strength
📶	Good signal strength
📶	Low signal strength

Related topics

- View the network's signal strength (page 121)
- View currently protected computers (page 127)
- View the network security mode (page 120)

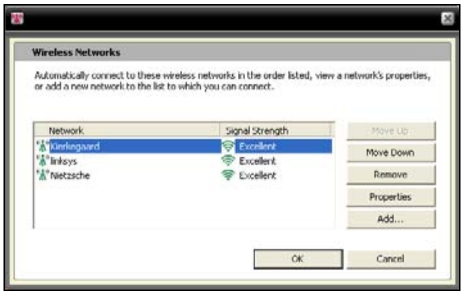
List preferred networks

Wireless Network Security allows you to specify preferred wireless networks. This allows you to specify the order of networks that your computer automatically connects to. Wireless Network Security attempts to connect to the first network that appears on the list.

This features is useful when, for example, you want to automatically connect to your friend's wireless network when you are in his area. You can promote another network to the top of the list.

To list preferred networks:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Wireless Networks**.
3. On the Available Wireless Networks pane, click **Advanced**.
4. Select the network whose order you want to adjust, and click **Move Up** or **Move Down**.



Wireless Networks

Automatically connect to these wireless networks in the order listed, view a network's properties, or add a new network to the list to which you can connect.

Network	Signal Strength
Kierkegaard	Excellent
linksys	Excellent
Nietzsche	Excellent

5. Click **OK**.

Related topics

- Remove preferred wireless networks (page 93)

Remove preferred wireless networks

You can use Wireless Network Security to remove preferred networks.

This is useful when, for example, you would like to remove an obsolete network from the list.

To remove preferred networks:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Wireless Networks**.
3. On the Available Wireless Networks pane, click **Advanced**.
4. On the Wireless Networks pane, select a network, and then click **Remove**.
5. Click **OK**.

Related topics

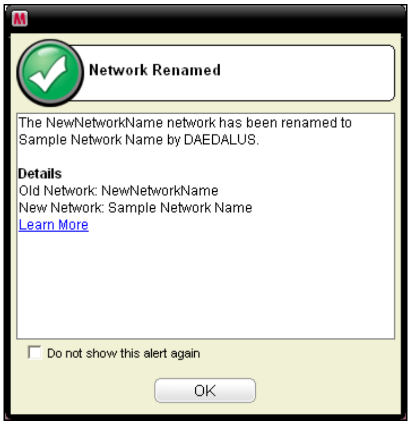
- List preferred networks (page 92)

Rename protected wireless networks

You can use Wireless Network Security to rename your existing protected wireless network.

Renaming the network can be helpful if its name is similar or identical to one used by your neighbor or if you want to create a unique name so that it is easier for you to distinguish.

Computers connected to the protected wireless network may be required to manually reconnect and are notified when the name changes.



Network Renamed

The NewNetworkName network has been renamed to Sample Network Name by DAEDALUS.

Details
Old Network: NewNetworkName
New Network: Sample Network Name
Learn More

After the network has been renamed, the new name appears on the Protected Wireless Router/AP pane.

To modify your protected wireless network name:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Configure**.

3 On the Network Security pane, type the new name in the **Protected Wireless Network Name** box.

4 Click **Apply**.

The Updating Network Security Settings dialog is displayed as Wireless Network Security changes the name of your protected wireless network. Depending on the your computer's settings and signal strength, the name of the network changes in less than one minute.

Note: As a security measure, McAfee recommends that you rename the router's or access point's default SSID. Although Wireless Network Security supports default SSIDs such as "linksys," or "belkin54g" or "NETGEAR," renaming SSIDs protects you against rouge access point threats.

Configure alert settings

Wireless Network Security allows you to configure alert settings to show alerts when certain events occur, such as when a new computer connects to your network.

To configure alert behavior:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Configure**.

3 Click **Alert Settings**.

4 Select or clear one or more of the following events, and then click **Apply**:

Alert Setting	Description
The security key for your protected wireless network is rotated	Displays the Security Key Rotated alert after you manually or automatically rotate the security key. Rotating the key protects your network from hackers attempting to intercept your data or connecting to your network.
Another protected computer connects to or disconnects from the network	Displays the Computer Connected or Computer Disconnected alert after a computer connects to or disconnects from the protected wireless network. Data on connected computers is now protected against intrusion and data interception.
Another computer is granted access to your protected wireless network	Displays the Computer Granted Network Access alert after an administrator computer allows another computer to join the protected wireless network. Granting a computer access to the protected network protects it against hackers attempting to intercept your data.
Key rotation for your protected wireless network is suspended or resumed	Displays either the Key Rotation Suspended or Key Rotation Resumed alert after you manually suspend or resume key rotation. Key rotation protects your network from hackers attempting to intercept your data or connecting to your network.
Access is revoked for all disconnected computers	Displays the Access Revoked alert after access for computers not connected to the network is revoked. Disconnected computers must rejoin the network.
A router is added to or removed from your protected wireless network	Displays the Router/AP Added to Network or the Router/AP Unprotected alert after the wireless router or access point is added to or removed from the protected wireless network.
The logon information for a protected wireless router changes	Displays the Router/AP Logon Changed alert after the Wireless Network Security administrator changes the user name or password for a router or access point.
The name or security setting of your protected wireless network changes	Displays the Network Settings Changed or Network Renamed alert after you rename the protected wireless network or adjust its security setting.
The settings for your protected wireless network are repaired	Displays the Network Repaired alert the security settings on your network's wireless routers or access points are fixed.

Note: To choose or clear all alert settings, click **Select All** or **Clear All**. To reset Wireless Network Security's alert settings, click **Restore Defaults**.

Related topics

- Rotate keys automatically (page 108)
- Join a protected wireless network (page 78)
- Connect to protected wireless networks (page 82)
- Disconnect from protected wireless networks (page 98)
- Suspend automatic key rotation (page 111)
- Revoke network access (page 99)
- Remove wireless routers or access points (page 97)
- Change credentials for wireless devices (page 105)
- Rename protected wireless networks (page 93)
- Repair network security settings (page 106)

Display connection notifications

You can configure Wireless Network Security to notify you when your computer connects to a wireless network.

To display notification when you connect to a wireless network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. Click **Other Settings**.
4. Select **Display notification message when connected to a wireless network**.
5. Click **Apply**.

Related topics

- Connect to protected wireless networks (page 82)

Remove wireless routers or access points

Wireless Network Security allows you to remove one or more routers or access points from your protected network.

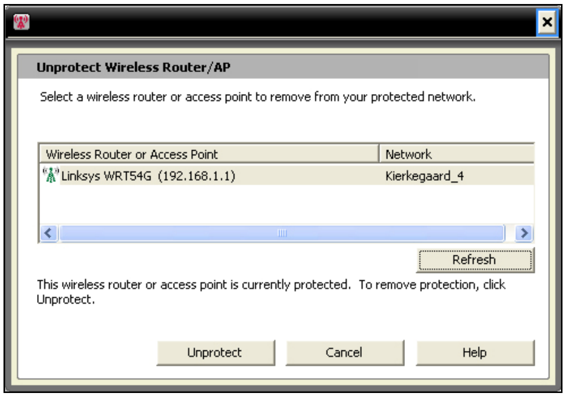
To remove a wireless router or access point:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Tools**.

3 On the Protection Tools pane, under **Unprotect a Device**, click **Unprotect**.

4 On the Unprotect Wireless Router/AP pane, select a wireless router or access point to remove from the protected network, and then click **Unprotect**.



Unprotect Wireless Router/AP

Select a wireless router or access point to remove from your protected network.

Wireless Router or Access Point	Network
Linksys WRT54G (192.168.1.1)	Kierkegaard_4

This wireless router or access point is currently protected. To remove protection, click Unprotect.

5 Click **OK** on the Wireless Router/AP Unprotected dialog to confirm that the wireless router or access point was removed from the network.

Related topics

- Create protected wireless networks (page 76)

Disconnect from protected wireless networks

Wireless Network Security allows you to disconnect your computer from the network.

This task is useful when, for example, your computer has connected to a network using a name that is identical to your network name. You can disconnect from the network, and then reconnect to yours.

This feature is useful, as well, when you accidently connect to the wrong network either because another access point's signal strength is strong or as a result of radio interference.

To disconnect from a protected wireless network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Wireless Networks**.
3. On the Available Wireless Networks pane, select the network, and then click **Disconnect**.

Related topics

- Revoke network access (page 99)
- Leave protected wireless networks (page 100)

Revoke network access

Wireless Network Security allows you to revoke access for computers that are not connected to the network. A new security key rotation schedule is established: computers not connected will lose access to the protected wireless network, but can regain it by rejoining the network. Access for connected computers is preserved.

For example, you can revoke the access of a visitor's computer with Wireless Network Security after it disconnects. In addition, an adult can revoke access of a computer used by a child as a form of parental control to Internet access. Access for a computer that was accidently granted can be revoked also.

To revoke access for all disconnected computers from the protected network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Tools**.
3. On the Tools pane, click Maintenance Tools.
4. On the Maintenance Tools pane, under **Revoke Access**, click **Revoke**.
5. On the Revoke Access pane, click **Revoke**.
6. Click **OK** in the Wireless Network Security dialog.

Related topics

- Disconnect from protected wireless networks (page 98)
- Leave protected wireless networks (page 100)

Leave protected wireless networks

You can use Wireless Network Security to cancel your access rights to a protected network.

To leave a network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. On the Configure pane, click **Other Settings**.
4. On the Other Settings pane, under Protected Network Access, select the network that you want to leave, and then click **Leave Network**.
5. On the Disconnect from the Network pane, click **Yes** to leave the network.

Note: When you leave a network, another user must grant you access to the protected network before rejoining it.

Related topics

- Disconnect from protected wireless networks (page 98)
- Revoke network access (page 99)

CHAPTER 16

Managing wireless network security

Wireless Network Security provides a complete set of tools to help you manage the security features of your wireless network.

In this chapter

Configuring security settings

After you connect to a protected wireless network, Wireless Network Security automatically protects your network; however, you can configure additional security settings at any time.

Configure security modes

You can specify the security mode of your protected wireless network. Security modes define the encryption between your computer and the router or access point.

When you protect your network, WEP is automatically configured. However, McAfee recommends that you change the security mode to WPA2 or WPA-PSK AES. Wireless Network Security uses WEP initially because this mode is supported by all routers and wireless network adapters. Most new routers and wireless network adapters, however, work in WPA mode, which is more secure.

To change the security mode for a protected wireless network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. On the Network Security pane, select the type of security you want to implement from the **Security Mode** box, and then click **Apply**.

The following table describes available security modes:

Strength	Mode	Description
Weakest	WEP	Wired Equivalent Privacy (WEP) is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks. WEP provides a level of security that can prevent unsophisticated snooping, but is generally not as secure as WPA-PSK encryption. Although Wireless Network Security provides a strong (hard to guess and long) key, McAfee recommends that you use a WPA security mode.
Average	WPA-PSK TKIP	Wi-Fi Protected Access (WPA) is an early version of the 802.11i security standard. TKIP is designed for WPA to enhance WEP. TKIP provides message integrity, re-keying mechanism, and per packet key mixing
Strong	WPA-PSK AES	This security mode combines WPA and AES modes. Advanced Encryption Standard (AES) is a block cipher adopted as an encryption standard by the US government.
Stronger	WPA2-PSK AES	This security mode combines WPA2 and AES modes. WPA2 is the next advancement to the ratification of the 802.11i security standard. WPA2 employs Counter Mode CBC MAC Protocol (CCMP), which is a more secure and scalable solution compared than TKIP. This is the strongest security mode available for consumers.
Strongest	WPA2-PSK TKIP+AES	This security mode combines WPA2 and AES, and WPA-PSK TKIP, modes. It allows for greater flexibility so that both old and new wireless adapters can connect.

Note: After the security mode is changed, you may be required to manually reconnect.

Related topics

- Repair network security settings (page 106)
- View the network security mode (page 120)

Configure network security settings

You can modify network properties of networks that are protected by Wireless Network Security. This is useful when, for example, you want to upgrade the security from WEP to WPA.

McAfee recommends that you modify network security settings if an alert suggests that you do so.

To configure unprotected network properties:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Wireless Networks**.
3. On the Available Wireless Networks pane, click **Advanced**.
4. On the Wireless Networks pane, click **Properties**.
5. On the Wireless Network Properties pane, you modify the following settings, and then click **OK**:

Setting	Description
Network	The name of your network. If you are modifying a network, you cannot change the name.
Security Settings	The security for your unprotected network. Note that if the wireless adapter does not support the mode you select, you cannot connect. Security modes include: Disabled, Open WEP, Shared WEP, Auto WEP, WPA-PSK, WPA2-PSK.
Encryption Mode	The encryption associated with the security mode you selected. Encryption modes include: WEP, TKIP, AES, and TKIP+AES.

Change credentials for wireless devices

You can change the user name or password for a device on your protected wireless router or access point. The list of devices appear under **Protected Wireless Network Devices**.

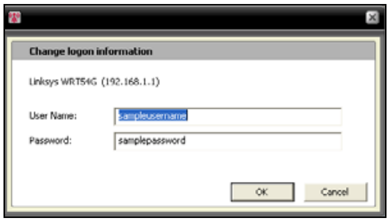
McAfee recommends that you change your credentials because the majority of wireless devices made by a single manufacturer have the same logon credentials. Changing login credentials helps prevent others from accessing your wireless router or access point, and changing its settings.

To change the user name or password for a protected wireless network device:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Configure**.

3 On the Network Security pane, under **Protected Wireless Network Devices**, select a wireless router or access point, and then click **Change User Name or Password**.



Change logon information

Linksys WRT54G (192.168.1.1)

User Name: sampleusername

Password: samplepassword

4 Click **OK** on the Wireless Network Security dialog after entering your logon information.

The new user name and password appear under **Protected Wireless Network Devices**.

Note: Some routers do not support user names and therefore a user name will not appear under **Protected Wireless Network Devices**.

Repair network security settings

If you are experiencing problems with your security settings or configuration, you can use Wireless Network Security to repair your router or access point settings.

To repair your security settings:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Tools**.
3. On the Tools pane, click **Maintenance Tools**.
4. Under **Repair Network Security Settings**, click **Repair**.
5. On the Repair Network Security Settings pane, click **Repair**.

   A Wireless Network Security alert indicates whether the network has or has not been repaired.

Note: If the attempt to repair your network is unsuccessful, connect to the network using a cable, and then retry. If the router or access point password has changed, you must reenter your password to connect.

Administering network keys

Wireless Network Security generates a long, strong, and random encryption keys with a random key generator. With WEP, the key is translated to a 26-digit hexadecimal value (for 104 bits of entropy, or strength, the maximum strength supported by 128 bit WEP), while with WPA, the key is a 63-character ASCII string. Each character has 64 possible values (6 bits), yielding 384 bits of entropy, which exceeds the WAP key strength of 256 bits.

When you manage network keys, you can display keys in plain text or asterisks for non-protected access points, discard saved keys for non-protected access points, enable or disable key rotation, change the key rotation frequency, manually rotate the key, and suspend key rotation.

When keys automatically rotate, hacker's tools cannot capture your information because the key is continuously changing.

However, if you are connecting wireless devices that Wireless Network Security does not support (for example, connecting a wireless handheld computer to your network), you must write down the key, stop key rotation, and then enter it on the device.

View current keys

Wireless Network Security provides quick access to wireless security information, including the current key for a protected wireless network.

To view the current key:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.
3. On the Wireless Network Status pane, under the Protected Wireless Network pane, click **Current Key**.

   The key configured for your network appears in the Key Configuration dialog.

Related topics

- View the number of key rotations (page 124)

Rotate keys automatically

Automatic key rotation is enabled by default, however, if you suspend key rotation, a computer with administrative access can re-enable it later.

You can configure Wireless Network Security to automatically rotate protected wireless network's security key.

Wireless Network Security automatically generates an infinite series of strong keys, which is synchronized across the network. The wireless connection can be briefly interrupted as the wireless router reboots with the new security key configuration, but this is usually undetected by network users.

If no computers are connected to the network, key rotation occurs after the first connects.

To enable automatic key rotation:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Configure**.

3 On the Network Security pane, check **Enable automatic key rotation.**

   You can also resume key rotation from the Wireless Network Status pane.

4 Click **Apply**.

Note: Key rotation automatically occurs every three hours by default, but you can adjust the frequency of key rotation to meet your security requirements.

Related topics

- Adjust the key rotation frequency (page 109)
- Resume key rotation (page 109)
- View the number of key rotations (page 124)

Resume key rotation

Although automatic key rotation is enabled by default, a computer with administrative access can resume key rotation after suspending it.

To resume key rotation:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.
3. On the Wireless Network Status pane, click **Resume Key Rotation**.

   The Key Rotation Started and Security Key Rotated alerts confirms key rotation started and was successful.

Related topics

- Rotate keys automatically (page 108)
- Suspend automatic key rotation (page 111)
- View the number of key rotations (page 124)

Adjust key rotation frequency

If Wireless Network Security is configured to automatically rotate the protected wireless network's security key, you can adjust the period in which key rotation takes place, ranging from every fifteen minutes to fifteen days.

McAfee recommends that the security key be rotated daily.

To adjust automatic key rotation frequency:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. On the Network Security pane, confirm that automatic key rotation is enabled, and then move the **Frequency** slider to one of the following settings:
   - **every 15 minutes**
   - **every 30 minutes**
   - **every 1 hour**
   - **every 3 hours**
   - **every 12 hours**
   - **every 1 day**
   - **every 7 days**
   - **every 15 days**

4 Click **Apply**.

Note: Ensure that automatic key rotation is enabled before setting the key rotation frequency.

Related topics

- Enable automatic key rotation (page 108)
- View the number of key rotations (page 124)

Suspend automatic key rotation

Key rotation can be suspended by any computer connected to the wireless network. You may want to suspend key rotation to do the following:

- Allow a guest to access the network and who does not have Wireless Network Security installed
- Allow a non-Windows system, such as a Macintosh, Linux, or TiVo to gain access. After you stop key rotation, note the key, and enter it on the new device.
- Allow a wireless connection that is uninterrupted by key rotations for certain programs such as online games.
- You should resume automatic key rotation as soon as possible to ensure that your network is fully protected from hackers.

To view the current key:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.
3. On the Wireless Network Status pane, under the Protected Wireless Network pane, click **Current Key**. Note the key that appears on the Key Configuration dialog. Other computers that do not have Wireless Network Security installed can use this key to connect to the protected wireless network.
4. On the Key Configuration dialog, click **Suspend Key Rotation**.
5. On the Key Rotation Suspended dialog, click **OK** to continue working.

Warning: If key rotation is not suspended, unsupported Wireless devices that are manually connected to the network disconnect when the key rotates.

You can create a Windows Connect Now disk and then use the text file to copy and paste the key onto the other computer and device.

Related topics

- Enable automatic key rotation (page 108)
- Add computers using Windows Connect Now technology (page 87)
- Resume key rotation (page 109)
- Rotate keys automatically (page 108)
- View the number of key rotations (page 124)

Manually rotate network keys

Wireless Network Security allows you to manually rotate a network key, even when automatic key rotation is enabled.

To manually rotate a network key:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Tools**.
3. On the Tools pane, click **Maintenance Tools**.
4. On the Maintenance Tools page, under **Manually Rotate Security Key**, click **Rotate**.

   The Key Rotation Started alert appears and confirms that key rotation has begun. After the security key is rotated, the Security Key Rotated alert appears, confirming that the key rotation was successful.

Note: To ease management of your security keys, you can automatically enable key rotation on the Network Security pane.

If no computers are connected to your wireless network, key rotation automatically occurs when the first computer connects.

Related topics

- Enable automatic key rotation (page 108)
- Adjust key rotation frequency (page 109)
- View the number of key rotations (page 124)

Display keys in asterisks

Keys are, by default, displayed as asterisks, but you can configure Wireless Network Security to display keys in plain text on networks that are not protected by Wireless Network Security.

Networks protected by Wireless Network Security display the key in plain text.

To display keys in asterisks:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. Click **Other Settings**.
4. Clear the **Display keys in plain text** box.
5. Click **Apply**.

Related topics

- Display keys in plain text (page 114)

Display keys in plain text

Keys are, by default, displayed as asterisks, but you can configure Wireless Network Security to display keys in plain text on networks that are not protected by Wireless Network Security.

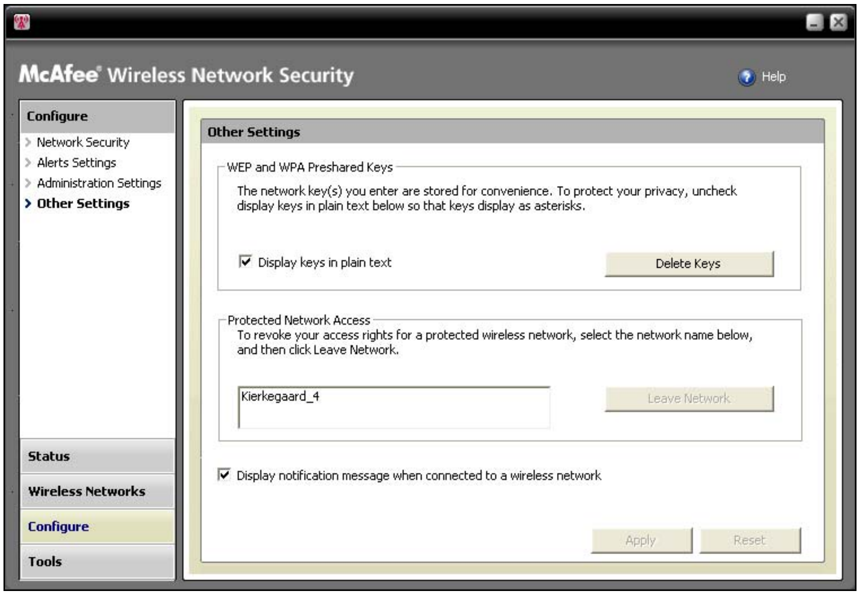
Networks protected by Wireless Network Security display the key in plain text.

To display keys in plain text:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Configure**.

3 Click **Other Settings**.



The network key(s) you enter are stored for convenience. To protect your privacy, uncheck display keys in plain text below so that keys display as asterisks.

☑ Display keys in plain text

To revoke your access rights for a protected wireless network, select the network name below, and then click Leave Network.

Kierkegaard_4

☑ Display notification message when connected to a wireless network

4 Select the **Display keys in plain text** box.

5 Click **Apply**.

Related topics

- Display keys in asterisks (page 113)

Delete network keys

Wireless Network Security automatically saves your WEP and WPA Preshared keys, which you can delete at any time.

To delete all your network key(s):

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Configure**.
3. On the **Configure** pane, click **Other Settings**.
4. On the **Other Settings** pane, under **WEP and WPA Preshared Keys**, click **Delete Keys**.
5. On the Clear Keys dialog, click **Yes** if you are sure you want to delete all stored WEP and WPA Preshared keys.

Warning: Deleting keys permanently removes them from your computer. After you delete your network keys, you must enter the correct key to connect to a WEP and WPA network.

CHAPTER 17

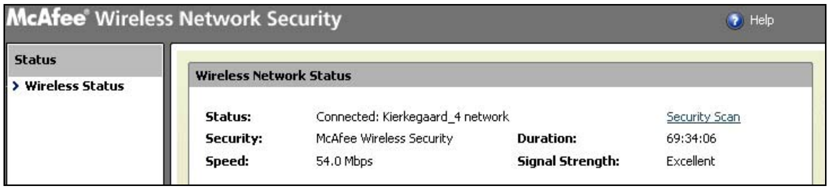
Monitoring wireless networks

Wireless Network Security allows you to monitor the status of your wireless network and protected computers.

In this chapter

Monitoring wireless network connections

You can view the status of your network connection, security mode, speed, duration, signal strength, and a security report on the Wireless Network Status pane.



Wireless Network Status

Status: Connected: Kierkegaard_4 network

Security: McAfee Wireless Security

Duration: 69:34:06

Speed: 54.0 Mbps

Signal Strength: Excellent

The following table describes status indicators for wireless network connections.

Status	Description	Information
Status	Displays whether your computer is connected to a network and which network it is connected to	View the connection status (page 119)
Security	Displays the security mode of the network you are connected to. Wireless Network Security is displayed if you are protected by Wireless Network Security.	View the network security mode (page 120)
Speed	Displays the speed of your computer's connect to the network.	View the network connection speed (page 120)
Duration	Displays the the period of time your computer has been connected to the network.	View the duration of your network connection (page 121)
Signal Strength	Displays the relative signal strength of the network.	View the network's signal strength (page 122)
Security Scan	Clicking **Security Scan** displays security information, such as wireless security vulnerabilities, performance issues, and the status of your wireless network.	View the online security report (page 122)

Related topics

- About Wireless Network Security icons (page 90)

View the connection status

You can use the Wireless Network Status pane to review the status of you network connection, to confirm whether you are connected or disconnected from the network.

To view the wireless connection status:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.

   The computers connected to the protected wireless network and the time and date when each connected is displayed on the Wireless Network Status pane, under **Computers.**

Related topics

- Monitoring wireless network connections (page 118)
- View the network security mode (page 120)
- View the network connection speed (page 120)
- View the duration of your network connection (page 121)
- View the network's signal strength (page 122)
- View the online security report (page 122)

View the network security mode

You can use the Wireless Network Status pane to review the network connection's security mode.

To view the network security mode:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.

   The security mode is displayed on the Wireless Network Status pane in the **Security** box.

   Wireless Network Security is displayed if the wireless network is protected by Wireless Network Security.

Related topics

- Monitoring wireless network connections (page 118)
- View the connection status (page 119)
- View the network connection speed (page 120)
- View the duration of your network connection (page 121)
- View the network's signal strength (page 122)
- View the online security report (page 122)

View the network connection speed

You can use the Wireless Network Status pane to review the speed of your computer's connection to the network.

To view the network connection speed:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.

   The connection speed is displayed on the Wireless Network Status pane in the **Speed** box.

Related topics

- Monitoring wireless network connections (page 118)
- View the connection status (page 119)
- View the network security mode (page 120)
- View the duration of your network connection (page 121)
- View the network's signal strength (page 122)
- View the online security report (page 122)

View the duration of your network connection

You can use the Wireless Network Status pane to review the length of time you have been connected to the network.

To view the duration of your connection to the network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.

   The length of time that your commuter has been connected to the wireless network is displayed in the **Duration** box.

Related topics

- Monitoring wireless network connections (page 118)
- View the connection status (page 119)
- View the network security mode (page 120)
- View the network connection speed (page 120)
- View the network's signal strength (page 122)
- View the online security report (page 122)

View the network's signal strength

You can use the Wireless Network Status pane to review the signal strength of the network.

To view the signal strength:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.

   The quality of your signal is displayed in the **Signal Strength** box.

Related topics

- Monitoring wireless network connections (page 118)
- View the connection status (page 119)
- View the network security mode (page 120)
- View the network connection speed (page 120)
- View the duration of your network connection (page 121)
- View the online security report (page 122)

View the online security report

You can use the Wireless Network Status pane to view a report about the your wireless connection, whether it is safe or insecure.

The McAfee wi-fiscan Web page displays information about your wireless security vulnerabilities, performance issues, information about your wireless connection, a recommended security solution, and indicates whether your connection is secure.

Before you view the security report, ensure that you have an Internet connection.

To view an online security report about your network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.
3. On the Wireless Network Status pane, click **Security Scan**.

   After your browser opens, you must download and install an ActiveX component. Depending on your browser's configuration, the browser may block the control. Allow your browser to download the component and then run it to begin the scan. Depending on your Internet connection speed, the scan can take some time.

Note: See your browser's documentation for information about downloading ActiveX components.

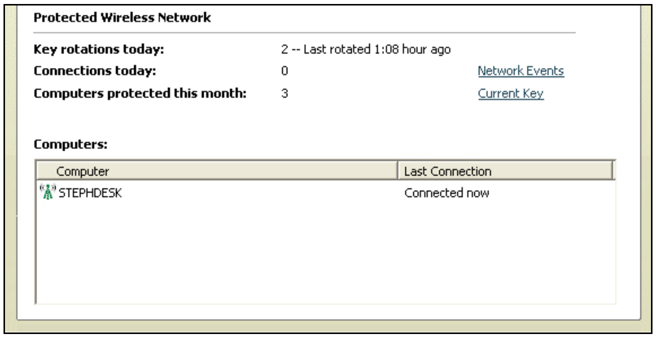
McAfee's wi-fiscan supports Internet Explorer 5.5 and above.

Related topics

- Monitoring wireless network connections (page 118)
- View the connection status (page 119)
- View the network security mode (page 120)
- View the network connection speed (page 120)
- View the duration of your network connection (page 121)
- View the network's signal strength (page 122)

Monitoring protected wireless networks

Wireless Network Security allows you to view the number of connections, key rotations, and protected computers on the Wireless Network Status pane. You can also view network events, current key, and currently protected computers.



Protected Wireless Network

Key rotations today:	2 -- Last rotated 1:08 hour ago	
Connections today:	0	Network Events
Computers protected this month:	3	Current Key

Computers:

Computer	Last Connection
STEPHDESK	Connected now

The following table describes the status indicators for protected wireless network connections.

Status	Description	Information
Key rotations today	Displays the daily number of key rotations on the protected wireless network.	View the number of key rotations (page 124)
Connections today	Displays the daily number of connections to the protected network.	View the number of daily connections (page 125)
Computers protected this month	Displays the number of computers protected for the current month.	View the number of monthly protected computers (page 125)
Network events	Clicking **Network Events** displays network, connection, and key rotation events.	View protected wireless network events (page 125)
Computers	Displays the number of computers connected to the protected wireless network and when each computer connected.	View currently protected computers (page 127)

View the number of key rotations

Wireless Network Security allows you to view the daily number of key rotations that have occurred on your protected network, and when key rotation last took place.

To view the daily number of key rotations:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Status**.

The total number of connections and the most recent key rotation is displayed on the Wireless Network Status pane, under **Protected Wireless Network**, in the **Key rotations today** field.

Related topics

- Monitoring protected wireless networks (page 123)
- View the number of daily connections (page 125)
- View the number of monthly protected computers (page 125)
- View protected wireless network events (page 125)
- View currently protected computers (page 127)
- Administering network keys (page 107)
- Rotate keys automatically (page 108)
- Manually rotate network keys (page 112)

View the number of daily connections

Wireless Network Security allows you to view the daily number of connections to the protected network.

To view the connections of your protected wireless network:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Select **View Status**.

The total number of connections is displayed on the Wireless Network Status pane, under **Protected Wireless Network**, in the **Connections today** box.

Related topics

- Monitoring protected wireless networks (page 123)
- View the number of monthly protected computers (page 125)
- View protected wireless network events (page 125)
- View currently protected computers (page 127)

View the number of monthly protected computers

Wireless Network Security allows you to view the number of computers protected for the current month.

To view the number of computers protected for the current month:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.
3. The number of computers protected during the current month is displayed on the Wireless Network Status pane, under **Protected Wireless Network**, in the **Computers secured this month** box.

Related topics

- Monitoring protected wireless networks (page 123)
- View the number of key rotations (page 124)
- View the number of daily connections (page 125)
- View protected wireless network events (page 125)
- View currently protected computers (page 127)

View protected wireless network events

Wireless Network Security logs events on the wireless network such as when security keys are rotated, when other computers connect to the McAfee-protected network, and when other computers join the McAfee-protected network.

Wireless Network Security allows you to view a report that describes events that have occurred on your network. You can specify the types of events to display and can sort event information based on date, event, or computer.

To view network events:

1 Right-click the Wireless Network Security icon in the Windows Notification area.

2 Do one of the following:

To...	Do this...
View network events from the Wireless Network Status pane	1. Select **View Status**. 2. On the Wireless Network Status pane, under **Protected Wireless Network**, click **Network Events**.
View network events from the Wireless Network Status pane	1. Click **View Tools**. 2. On the Tools pane, click **Maintenance Tools**. 3. On the Maintenance Tools pane, under **View Event Log**, click **View**.

3 Select one or more of the following events to display:

- **Network Events**: Displays information about network activity, such as the protection of a wireless router or access point.
- **Connection Events**: Displays information about network connections, such as the date and time of a computer connected to the network.
- **Key Rotation Events**: Displays information about the dates and times of security key rotations.

4 Click **Close**.

Related topics

- Monitoring protected wireless networks (page 123)
- View the number of key rotations (page 124)
- View the number of daily connections (page 124)
- View the number of daily connections (page 125)
- View currently protected computers (page 127)

View currently protected computers

You can view the number of computers connected to the protected wireless network and when each last connected.

To view computers connected to the protected network:

1. Right-click the Wireless Network Security icon in the Windows Notification area.
2. Select **View Status**.
3. Computers that are connected to the protected wireless network, and the time and date that each most recently connected, are displayed on the Wireless Network Status pane, under **Computers**.

Related topics

- Monitoring protected wireless networks (page 123)
- View the number of key rotations (page 124)
- View the number of daily connections (page 124)
- View the number of monthly protected computers (page 125)
- View protected wireless network events (page 125)

CHAPTER 18

Troubleshooting

You can troubleshoot problems when using Wireless Network Security and third-party equipment, including:

- Difficulties with installation
- Unable to protect or configure your network
- Unable to connect computers to your network
- Unable to connect to a network or the Internet
- Other issues

In this chapter

Installing Wireless Network Security

You can troubleshoot the following installation problems.

- Which computers to install this software on
- Wireless adapter not detected
- Multiple wireless adapters
- Unable to download on wireless computers because the network is already secure

Which computers to install this software on

Install Wireless Network Security on every wireless computer in your network (unlike other McAfee programs, you can install this software on multiple computers). Adhere to the license agreement of your purchased software. In some cases, you may need to purchase additional licenses.

You can (but are not required to) install on computers that do not have wireless adapters, but the software is not active on these computers because they do not need wireless protection.

Wireless Network Security is currently supported on Windows XP or Windows 2000.

Compatible Wireless adapter not detected

If your wireless adapter is not detected when it is installed and enabled, restart your computer. If the adapter is still not detected after restarting your computer, follow these steps.

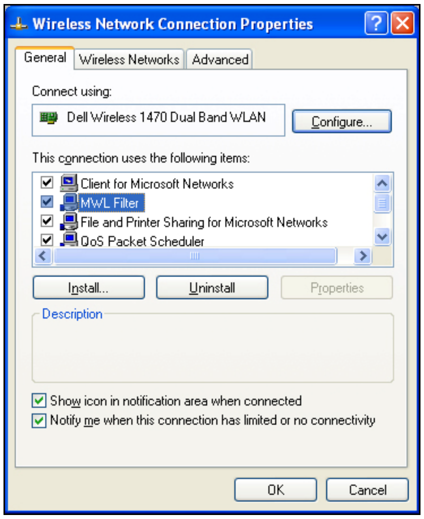
1 Launch Windows' Wireless Network Connection Properties dialog box.

2 Using Windows' Classic Start menu, view, click **Start**, point to **Settings**, and then select **Network Connections**.

3 Click the **Wireless Network Connection** icon.

4 On the Wireless Network Connection Status dialog, click **Properties**.

5 On the Wireless Network Connection Properties pane, clear **MWL Filter** and then re-select it.



Connect using:

Dell Wireless 1470 Dual Band WLAN

This connection uses the following items:

☑ Client for Microsoft Networks
☑ MWL Filter
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

6 Click **OK**.

If this does not solve the problem, verify by running the WiFi Scan. If the wi-fi scan works, then your adapter is supported. If not, then update your adapter's driver (use Windows Update or visit the manufacturer's Web site) or purchase a new device.

Related topics

- View the online security report (page 122)

Multiple wireless adapters

If an error states that you have multiple wireless adapters installed, you must disable or unplug one of them. Wireless Network Security only works with one wireless adapter.

Download fails on secure network

If you have an installation CD, install Wireless Network Security from the CD on all your wireless computers.

If you installed the software on one wireless computer and protected your network before installing the software on all the other wireless computers, you have these options.

- Unprotect your network. Then, download the software and install it on all the wireless computers. Protect your network again.
- View the network key. Then, enter the key on your wireless computer to connect to the network. Download and install the software, and join the network from the wireless computer.
- Download the executable on the computer that is already connected to the network and save it on a USB flash drive or write it to a CD so you can install it on the other computers.
- Run Windows Connect Now technology.

Related topics

- Remove wireless routers or access points (page 97)
- View current keys (page 107)
- Add computers using a removable device (page 85)
- Add computers using Windows Connect Now technology (page 87)

Protecting or configuring your network

You can troubleshoot the following problems when protecting or configuring your network.

- Unsupported router or access point
- Update router or access point firmware
- Duplicate administrator error
- Network appears unsecured
- Unable to repair

Unsupported router or access point

If an error states that your wireless router or access point may not be supported, Wireless Network Security was unable to configure your device because it did not recognize it or find it.

Verify that you have the latest version of Wireless Network Security by requesting an update (McAfee constantly adds support for new routers and access points). If your router or access point appears on the list of supported routers and you still receive this error, you are experiencing communication errors between your computer and the router or access point.

Related topics

- Supported wireless routers http://www.mcafee.com/router

Update router or access point firmware

If an error states that the firmware revision of your wireless router or access point is not supported, your device is supported, but the firmware revision of the device is not. Verify that you have the latest version of Wireless Network Security by requesting an update (McAfee constantly adds support for new firmware revisions).

If you have the latest version of Wireless Network Security, refer to the manufacturer's Web site or support organization for your router or access point and install a firmware version that is listed on the list of supported routers.

Related topics

- Supported wireless routers http://www.mcafee.com/router

Duplicate administrator error

After you configure your router or access point, you must log off the administration interface. In some cases, if you do not log off, the router or access point acts as if another computer is still configuring it and an error message appears.

If you cannot log off, unplug the power from the router or access point and then plug it in again.

Key rotation failed

The key rotation failed because:

- The login information for your router or access point has been changed.
- The firmware version of your router or access point has been changed to a version that is not supported.
- Your router or access point is not available. Ensure that the router or access point is turned on, and that it is connected to your network.
- Duplicate administrator error.
- For some wireless routers, if another computer is manually logged into the wireless router's web interface, the McAfee client may not be able to also access the management interface to rotate the encryption key.

Related topics

- Change credentials for wireless devices (page 105)
- Rotate keys automatically (page 108)

Unable to repair the router or access point

If the repair fails, try the following. Note that each procedure is independent.

- Connect to your network using a cable, then try repairing again.
- Unplug the power from the router or access point, plug it in again, then try connecting.
- Reset the wireless router or access point to its default setting and repair it. Doing so resets the wireless settings to its original settings. Then, reset your Internet connection settings.
- Using the advanced options, leave the network from all the computers and reset the wireless router or access point to its default settings, then protect it. This resets the wireless settings to its original settings. Then, reset your Internet connection settings.

Related topics

- Repair network security settings (page 106)

Network appears unprotected

If your network is showing as unsecured, it is not protected. You must protect the network to secure it. Note that Wireless Network Security only functions with compatible routers and access points.

Related topics

- Create protected wireless networks (page 76)
- Supported wireless routers http://www.mcafee.com/router

Connecting computers to your network

You can troubleshoot the following problems when connecting computers to your network.

- Waiting for authorization
- Granting access to an unknown computer

Waiting for authorization

If you try to join a protected network and your computer remains in waiting for authorization mode, verify the following.

- A wireless computer that already has access to the network is turned on and connected to the network.
- Someone is present to grant access on that computer when it appears.
- The computers are within wireless range of each other.

If **Grant Access** does not appear on the computer that already has access to the network, try granting from another computer.

If other computers are not available, unprotect the network from the computer that already has access, and protect the network from the computer that did not have access. Then, join the network from the computer that originally protected the network.

You can also use the Protect Another Computer feature.

Related topics

- Join a protected wireless network (page 78)
- Leave protected wireless networks (page 100)
- Remove wireless routers or access points (page 97)
- Add computers to the protected wireless network (page 85)

Granting access to an unknown computer

When you receive a request from an unknown computer to grant access, deny it until you can verify its legitimacy. Someone might be trying to illegitimately access your network.

Connecting to the Internet and network

You can troubleshoot the following problems when connecting to a network or the Internet.

- Bad connection to the Internet
- Connection briefly stops
- Devices (not your computer) lose connection
- Prompted to enter the WEP, WPA, or WPA2 key
- Unable to connect
- Update your wireless adapter
- Weak signal level
- Windows cannot configure your wireless connection
- Windows shows no connection

Cannot connect to the the Internet

If you cannot connect, try accessing your network using a cable, and then connect to the Internet. If you still cannot connect, verify the following:

- Your modem is turned on
- Your PPPoE settings are correct
- Your DSL or cable line is active

Connectivity problems such as speed and signal strength can also be caused by wireless interference. Try the following methods to fix the problem:

- Change the channel of your cordless telephone
- Eliminate possible sources of interference
- Change the location of your wireless router, access point, or computer
- Change the router or access point channel. Channels 1, 4, 7, and 11 are recommended for North and South America. Channels 1, 4, 7, 13 are recommended for other countries. Many routers are set to channel 6 by default
- Ensure that your router and wireless adapter (especially a wireless USB adapter) are not against a wall
- Ensure that your USB wireless adapter is not beside a wireless AP/router.
- Position the router away from walls and metal

Connection interrupted

When your connection is briefly interrupted (for example, during an online game), key rotation can be the cause. To prevent this, you can suspend key rotation.

McAfee recommends that you resume key rotation as soon as you can to ensure that your network is fully protected from hackers.

Related topics

- Rotate keys automatically (page 108)
- Resume key rotation (page 109)
- Suspend automatic key rotation (page 111)
- Manually rotate network keys (page 112)

Devices lose connectivity

If some devices are losing their connection when you are using Wireless Network Security, try to fix the problem using the following methods:

- Suspend the key rotation
- Update the driver for the wireless adapter
- Disable the adapter's client manager

Related topics

- Suspend automatic key rotation (page 111)

Prompted to enter the WEP, WPA, or WPA2 key

If you have to enter a WEP, WPA, or WPA2 key to connect to your protected wireless network, you probably did not install the software on your computer.

To function correctly, Wireless Network Security must be installed on every wireless computer in your network.

Related topics

- Starting Wireless Network Security (page 70)
- Add computers to the protected wireless network (page 85)

Unable to connect to wireless network

If you are unable to connect, try the following. Note that each procedure is independent.

- If you are not connecting to a protected network, verify that you have the correct key and enter it again.
- Unplug the wireless adapter and plug it in again, or disable it and re-enable it.
- Turn off the router or access point, and turn it on again, then try connecting.
- Verify that your wireless router or access point is connected, and repair the security settings.
- Restart your computer.
- Update your wireless adapter or buy a new one. For example, your network could be using WPA-PSK TKIP security, and your wireless adapter might not support the network's security mode (the networks show WEP, even though they are set to WPA).
- If you are unable to connect after you upgraded your wireless router or access point, you might have upgraded it to an unsupported version. Verify that the router or access point is supported. If it is not supported, downgrade it to a supported version, or wait until a Wireless Security update is available.

Related topics

- Repair network security settings (page 106)
- Updating your wireless adapter (page 140)

Update your wireless adapter

You may be required to update your wireless adapter so that you can use Wireless Network Security.

To update your adapter:

1 From your desktop, click **Start**, point to **Settings**, and then select **Control Panel**.

2 Double-click the **System** icon. The **System Properties** dialog box appears.

3 Select the **Hardware** tab, and then click **Device Manager**.

4 In Device Manager list, double-click your adapter.

5 Select the **Driver** tab and note the driver you have.

6 Go to the Web site of the adapter's manufacturer to locate an update. Drivers are usually found in the Support or Downloads section. If you are using a miniPCI card, navigate to the computer's, not the card's manufacturer.

7 If a driver update is available, follow the instructions on the Web site to download it.

8 Go back to the **Driver** tab and click **Update Driver**. A Windows wizard appears.

9 To install the driver, follow the instructions on the Web site.

Weak signal level

If your connection drops or is slow, your signal level might not be strong enough. To improve your signal, try the following:

- Ensure that your wireless devices are not blocked by metal objects such as furnaces, ducts, or large appliances. Wireless signals do not travel well through these objects.
- If your signal is going through walls, make sure that it does not have to cross at a shallow angle. The longer the signal travels inside a wall, the weaker it gets.
- If your wireless router or access point has more than one antenna, try moving the two antennas perpendicular to each other (one upright and one horizontal, at a 90 degree angle).
- Some manufacturers have high-gain antennas. Directional antennas provide longer range, while omni-directional antennas offer the most versatility. Consult your manufacturer's installation instructions for installing your antenna.

If these steps are not successful, add an Access Point to your network that is closer to the computer you are trying to connect to. If you configure your second AP with the same network name (SSID) and a different channel, your adapter automatically finds the strongest signal and connects through the appropriate AP.

Related topics

- Signal Strength icons (page 91)
- View the network's signal strength (page 121)

Windows does not support wireless connection

If a Windows error message indicates that it cannot configure your wireless connection, you can ignore it. Use Wireless Network Security to connect to, and configure wireless networks.

In the Windows Wireless Network Connection Properties dialog box, under the Wireless Networks tab, ensure that the **Use Windows to configure my wireless network setting** box is clear.

Wireless Network Security allows:

- Adapters installed on computers running Windows 2000 to connect to WPA networks, even though the card client manager is not supported.
- Adapters on computers running Windows XP to connect to WPA2 networks without having to find and install the Win XP SP2 hotfix
- Adapters under Windows XP SP1 to connect to WPA and WPA2 networks without having to locate and install a hotfix, which is not supported by Windows XP SP1.

Windows shows no connection

If you are connected, but the Windows Network icon is showing an X (no connection), ignore this. You have a good connection.

Other issues

You can troubleshoot the following problems:

- Network name is different when using other programs
- Problem when I configure wireless routers or access points
- Replace computers
- Select another security mode
- Software does not work after upgrading operating systems

Network name differs when using other programs

If the name of the network is different when viewed through other programs (for example, _SafeAaf is part of the name), this is normal.

Wireless Network Security marks networks with a code when they are protected.

Configuring wireless routers or access points

If an error appears when configuring your router or access point or adding multiple routers on the network, verify that all the routers and access points have a distinct IP address.

If the name of your wireless router or access point appears in the Protect Wireless Router or Access Point dialog box, but you get an error when you configure it: Verify that your router or access point is supported.

If your router or access point is configured, but does not seem to be on the correct network (for example, you cannot see other computers attached to the LAN), verify that you configured the appropriate router or access point, and not your neighbor's. Unplug the power from the router or access point, and ensure that the connection drops. If the wrong router or access point was configured, unprotect it and then protect the correct router or access point.

If you are unable to configure or add your router or access point, but it is supported, some changes you performed might be preventing it from being properly configured.

- Follow the manufacturer's directions to configure your wireless router or access point to DHCP, or to configure the correct IP address. In some cases, the manufacturer provides a configuration tool.
- Reset your router or access point to factory defaults and try repairing your network again. You might have changed the administration port on the router or access point, or turned off wireless administration. Ensure that you are using the default configuration, and that wireless configuration is enabled. Another possibility is that the http administration is

disabled. In this case, verify that the http administration is enabled. Ensure you use port 80 for administration.

- If your wireless router or access point does not appear in the list of wireless routers or access points to protect or connect to, enable broadcast SSID and verify that you can see your router or access point in the Wireless Network Security's available wireless networks list.
- If you get disconnected, or cannot establish a connection, MAC filtering might be enabled. Disable MAC filtering.
- If you cannot perform network operations (for example, share files or print to shared printers) across two computers with wireless connection to the network, verify that you have not enabled AP Isolation. AP Isolation prevents wireless computers from being able to connect to each other over the network.
- If you are using a firewall program other than McAfee Personal Firewall, ensure the subnet is trusted.

Related topics

- Supported wireless routers http://www.mcafee.com/router

Replace computers

If the computer that protected the network has been replaced and there are not any computers that have access (you cannot access the network), reset the wireless router or access point to its factory defaults and protect your network again.

Select another security mode

If an error states that you selected a security mode that is not supported by the wireless adapter, you must select a different security mode.

- All adapters support WEP.
- Most adapters that support WPA implement both WPA-PSK TKIP and WPA-PSK AES security modes.
- Adapters that support WPA2 implement WPA security modes and WPA2-PSK TKIP, WPA2-PSK AES, and WPA2-PSK TKIP/AES.

Related topics

- Configuring security settings (page 102)
- View the network security mode (page 120)

Software fails after upgrading operating systems

If Wireless Network Security fails after upgrading operating systems, remove and then reinstall the program.

CHAPTER 19

McAfee EasyNetwork

McAfee® EasyNetwork enables secure file sharing, simplifies file transfers, and automates printer sharing among the computers in your home network.

Before you begin using EasyNetwork, you can familiarize yourself with some of the most popular features. Details about configuring and using these features are provided throughout the EasyNetwork help.

In this chapter

Features

EasyNetwork provides the following features.

File sharing

EasyNetwork makes it easy to share files on your computer with other computers on the network. When you share files, you grant other computers read-only access to those files. Only computers who are members of the managed network (that is, with full or administrative access) can share files or access files shared by other members.

File transfer

You can send files to other computers that are members of the managed network. When you receive a file, it appears in your EasyNetwork inbox. The inbox is a temporary storage location for all the files that are sent to you by other computers on the network.

Automated printer sharing

After you join a managed network, EasyNetwork automatically shares any local printers attached to your computer, using the printer's current name as the shared printer name. It also detects printers shared by other computers on your network and allows you to configure and use those printers.

CHAPTER 20

Setting up EasyNetwork

Before you can use EasyNetwork features, you must launch the program and join the managed network. After you join, you can decide to leave the network at any time.

In this chapter

Launching EasyNetwork

By default, you are prompted to launch EasyNetwork immediately after installation; however you can also launch EasyNetwork later.

Launch EasyNetwork

By default, you are prompted to launch EasyNetwork immediately after installation; however, you can also launch EasyNetwork later.

To launch EasyNetwork:

- On the **Start** menu, point to **Programs**, point to **McAfee**, and then click **McAfee EasyNetwork**.

Tip: If you agreed to create desktop and quick launch icons during the installation, you can also launch EasyNetwork by double-clicking the McAfee EasyNetwork icon on your desktop or by clicking the McAfee EasyNetwork icon in the notification area to the right of your taskbar.

Joining a managed network

After you install SecurityCenter, a network agent is added to your computer and runs in the background. In EasyNetwork, the network agent is responsible for detecting a valid network connection, detecting local printers to share, and monitoring the network status.

If no other computer running the network agent is found on the network to which you are currently connected, you are automatically made a member of the network and are prompted to identify whether the network is trusted. As the first computer to join the network, your computer name is included in the network name; however, you can rename the network at any time.

When a computer connects to the network, a join request is sent to all other computers currently on the network. The request can be granted by any computer with administrative permissions on the network. The grantor can also determine the permission level for the computer currently joining the network; for example, guest (file transfer capability only) or full/administrative (file transfer and file sharing capabilities). In EasyNetwork, computers with administrative access can grant access to other computers and manage permissions (that is, promote or demote computers); computers with full access cannot perform these administrative tasks. Before the computer is allowed to join, a security check is also performed.

Note: After joining, if you have other McAfee networking programs installed (for example, McAfee Wireless Network Security or Network Manager), the computer is also recognized as a managed computer in those programs. The permission level that is assigned to a computer applies to all McAfee networking programs. For more information about what guest, full, or administrative permissions mean in other McAfee networking programs, see the documentation provided for that program.

Join the network

When a computer connects to a trusted network for the first time after installing EasyNetwork, a message prompt appears, asking whether to join the managed network. When the computer agrees to join, a request is sent to all other computers on the network that have administrative access. This request must be granted before the computer can share printers or files, or send and copy files on the network. If the computer is the first computer on the network, it is given administration permissions on the network automatically.

To join the network:

1. In the Shared Files window, click **Yes, join the network now**. When an administrative computer on the network grants your request, a message appears, asking whether to allow this computer and other computers on the network to manage each others' security settings.
2. To allow this computer and other computers on the network to manage each others' security settings, click **Yes**; otherwise, click **No**.
3. Confirm that the granting computer is displaying the playing cards that are currently displayed in the security confirmation dialog box, and then click **Confirm**.

Note: If the granting computer is not displaying the same playing cards that are displayed in the security confirmation dialog box, there has been a security breach on the managed network. Joining the network could put your computer at risk; therefore, click **Reject** in the security confirmation dialog box.

Grant access to the network

When a computer requests to join the managed network, a message is sent to the other computers on the network who have administrative access. The first computer to respond to the message becomes the grantor. As the grantor, you are responsible for deciding which type of access to grant the computer: guest, full, or administrative.

To grant access to the network:

1. In the alert, select one of the following check boxes:
   - **Grant guest access**: Allows the user to send files to other computers, but not share files.
   - **Grant full access to all managed network applications**: Allows the user to send and share files.

- **Grant administrative access to all managed network applications**: Allows the user to send and share files, grant access to other computers, and adjust other computers' permission levels.

2. Click **Grant Access**.
3. Confirm that the computer is displaying the playing cards that are currently displayed in the security confirmation dialog box, and then click **Confirm**.

Note: If the computer is not displaying the same playing cards that are displayed in the security confirmation dialog box, there has been a security breach on the managed network. Granting this computer access to the network could put your computer at risk; therefore, click **Reject** in the security confirmation dialog box.

Rename the network

By default, the network name includes the name of the first computer who joined it; however, you can change the network name at any time. When you rename the network, you change the network description displayed in EasyNetwork.

To rename the network:

1. On the **Options** menu, click **Configure**.
2. In the Configure dialog box, type the name of the network in the **Network Name** box.
3. Click **OK**.

Leaving a managed network

If you join a managed network and then determine that you no longer want to be a member, you can leave the network. After you relinquish your membership, you can rejoin at any time; however, you must be granted permission to join and peform the security check again. For more information, see Joining a managed network (page 149).

Leave a managed network

You can leave a managed network that you previously joined.

To leave a managed network:

1 On the **Tools** menu, click **Leave Network**.

2 In the Leave Network dialog box, select the name of the network that you want to leave.

3 Click **Leave Network**.

CHAPTER 21

Sharing and sending files

EasyNetwork makes it easy to share and send files on your computer among other computers on the network. When you share files, you grant other computers read-only access to those files. Only computers who are members of the managed network (that is, with full or administrative access) can share files or access files shared by other member computers.

In this chapter

Sharing files

EasyNetwork makes it easy to share files on your computer with other computers on the network. When you share files, you grant other computers read-only access to those files. Only computers who are members of the managed network (that is, with full or administrative access) can share files or access files shared by other member computers. If you share a folder, all the files contained in that folder and its subfolders are shared; however, subsequent files added to the folder are not automatically shared. If a shared file or folder is deleted, it is automatically removed from the Shared Files window. You can stop sharing a file at any time.

You access a shared file in two ways: by opening the file directly from EasyNetwork or by copying the file to a location on your computer, and then opening it. If your list of shared files becomes long, you can search for the shared file(s) you want to access.

Note: Files shared using EasyNetwork cannot be accessed from other computers using Windows Explorer. EasyNetwork file sharing is performed over secure connections.

Share a file

When you share a file, it is automatically available to all other members with full or administrative access to the managed network.

To share a file:

1. In Windows Explorer, locate the file you want to share.
2. Drag the file from its location in Windows Explorer to the Shared Files window in EasyNetwork.

Tip: You can also share a file by clicking **Share Files** on the **Tools** menu. In the Share dialog box, navigate to the folder where the file you want to share is stored, select the file, and then click **Share**.

Stop sharing a file

If you share a file on the managed network, you can stop sharing it at any time. When you stop sharing a file, other members of the managed network can no longer access it.

To stop sharing a file:

1. On the **Tools** menu, click **Stop Sharing Files**.
2. In the Stop Sharing Files dialog box, select the file that you no longer want to share.
3. Click **Do Not Share**.

Copy a shared file

You can copy shared files from any computer on the managed network to your computer. Then, if the computer stops sharing the file, you still have a copy.

To copy a file:

- Drag a file from the Shared Files window in EasyNetwork to a location in Windows Explorer or to the Windows Desktop.

Tip: You can also copy a shared file by selecting the file in EasyNetwork, and then clicking **Copy To** on the **Tools** menu. In the Copy to folder dialog box, navigate to the folder where you want to copy the file, select it, and then click **Save**.

Search for a shared file

You can search for a file that has been shared by you or any other network member. As you type your search criteria, EasyNetwork automatically displays the corresponding results in the Shared Files window.

To search for a shared file:

1. In the Shared Files window, click **Search**.
2. Click one of the following options in the **Contains** list:
   - **Contains all of the words**: Searches for file or path names that contain all of the words you specify in the **File or Path Name** list, in any order.
   - **Contains any of the words**: Searches for file or path names that contain any of the words you specify in the **File or Path Name** list.
   - **Contains the exact string**: Searches for file or path names that contain the exact phrase you specify in the **File or Path Name** list.

3. Type part or all of the file name or path in the **File or Path Name** list.
4. Click one of the following file types in the **Type** list:
   - **Any**: Searches all of the shared file types.
   - **Document**: Searches all of the shared documents.
   - **Image**: Searches all of the shared image files.
   - **Video**: Searches all of the shared video files.
   - **Audio**: Searches all of the shared audio files.
5. In the **From** and **To** lists, click dates representing the range of dates on which the file was created.

Sending files to other computers

You can send files to other computers that are members of the managed network. Before sending a file, EasyNetwork confirms that the computer receiving the file has enough disk space available.

When you receive a file, it appears in your EasyNetwork inbox. The inbox is a temporary storage location for all the files that are sent to you by other computers on the network. If you have EasyNetwork open when you receive a file, the file instantly appears in your inbox; otherwise, a message appears in the notification area to the right of the Windows taskbar. If you do not want to receive notification messages, you can turn them off. If a file with the same name already exists in the inbox, the new file is renamed with a numeric suffix. Files remain in your inbox until you accept them (that is, copy them to a location on your computer).

Send a file to another computer

You can send a file directly to another computer on the managed network without sharing it. Before a user on the recipient computer can view the file,it must be saved to a local location. For more information, see Accept a file from another computer (page 160).

To send a file to another computer:

1. In Windows Explorer, locate the file you want to send.
2. Drag the file from its location in Windows Explorer to an active computer icon in EasyNetwork.

Tip: You can send multiple files to a computer by pressing CTRL when selecting the files. You can also send files by click **Send** on the **Tools** menu, selecting the files, and then clicking **Send**.

Accept a file from another computer

If another computer on the managed network sends you a file, you must accept it (by saving it to a folder on your computer). If you do not have EasyNetwork open or in the foreground when a file is sent to your computer, you receive a notification message in the notification area to the right of the taskbar. Click the notification message to open EasyNetwork and access the file.

To receive a file from another computer:

- Click **Received**, and then drag a file from your EasyNetwork inbox to a folder in Windows Explorer.

Tip: You can also receive a file from another computer by selecting the file in your EasyNetwork inbox, and then clicking **Accept** on the **Tools** menu. In the Accept to folder dialog box, navigate to the folder where you want to save the files you are receiving, select it, and then click **Save**.

Receive notification when a file is sent

You can receive notification when another computer on the managed network sends you a file. If EasyNetwork is not currently open or is not in the foreground on your desktop, a notification message appears in the notification area to the right of the Windows taskbar.

To receive notification when a file is sent:

1. On the **Options** menu, click **Configure**.
2. In the Configure dialog box, select the **Notify me when some other computer sends me files** check box.
3. Click **OK**.

CHAPTER 22

Sharing printers

After you join a managed network, EasyNetwork automatically shares any local printers attached to your computer. It also detects printers shared by other computers on your network and allows you to configure and use those printers.

In this chapter

Working with shared printers

After you join a managed network, EasyNetwork automatically shares any local printers attached to your computer, using the printer's current name as the shared printer name. It also detects printers shared by other computers on your network and allows you to configure and use those printers. If you have configured a printer driver to print through a network print server (for example, a wireless USB print server), EasyNetwork considers the printer to be a local printer and automatically shares it on the network. You can also stop sharing a printer at any time.

EasyNetwork also detects printers shared by all of the other computers on the network. If it detects a remote printer that is not already connected to your computer, the **Available network printers** link appears in the Shared Files window when you open EasyNetwork for the first time. This allows you to install available printers or uninstall printers that are already connected to your computer. You can also refresh the list of printers detected on the network.

If you have not yet joined the managed network but are connected to it, you can access the shared printers from the standard Windows printer control panel.

Stop sharing a printer

You can stop sharing a printer at any time. Members who have installed the printer will no longer be able to print to it.

To stop sharing a printer:

1. On the **Tools** menu, click **Printers**.
2. In the Manage Network Printers dialog box, click the name of the printer that you no longer want to share.
3. Click **Do Not Share**.

Install an available network printer

As a member of a managed network, you can access the printers that are shared on the network. To do so, you must install the printer driver used by the printer. If the owner of the printer stops sharing it after you have installed it, you can no longer print to that printer.

To install an available network printer:

1 On the **Tools** menu, click **Printers**.

2 In the Available Network Printers dialog box, click a printer name.

3 Click **Install**.

CHAPTER 23

Reference

The Glossary of Terms lists and defines the most commonly used security terminology found in McAfee products.

About McAfee provides legal information about McAfee Corporation.

Glossary

8

802.11

A set of IEEE standards for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. Several specifications of 802.11 include 802.11a, a standard for up to 54 Mbps networking in the 5Ghz band, 802.11b, a standard for up to 11 Mbps networking in the 2.4 Ghz band, 802.11g, a standard for up to 54 Mbps networking in the 2.4 Ghz band, and 802.11i, a suite of security standards for all wireless Ethernets.

802.11a

An extension to 802.11 that applies to wireless LANs and sends data at up to 54 Mbps in the 5GHz band. Although the transmission speed is faster than 802.11b, the distance covered is much smaller.

802.11b

An extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission in the 2.4 GHz band. 802.11b is currently considered the wireless standard.

802.11g

An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 2.4 GHz band.

802.1x

Not supported by Wireless Home Network Security. An IEEE standard for authentication on wired and wireless networks, but is most notably used in conjunction with 802.11 wireless networking. This standard provides strong, mutual authentication between a client and an authentication server. In addition, 802.1x can provide dynamic per-user, per-session WEP keys, removing the administrative burden and security risks surrounding static WEP keys.

A

Access Point (AP)

A network device that allows 802.11 clients to connect to a local area network (LAN). APs extend the physical range of service for a wireless user. Sometimes referred to as wireless router.

archive

To create a copy of your watch files locally on CD, DVD, USB drive, external hard drive, or network drive.

archive

To create a copy of your watch files locally on CD, DVD, USB drive, external hard drive, or network drive.

authentication

The process of identifying an individual, usually based on a user name and password. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

B

back up

To create a copy of your watch files on a secure, online server.

bandwidth

The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

blacklist

A list of Web sites that are considered malicious. A Web site can be placed on a blacklist because it is a fraudulent operation or because it exploits browser vulnerability to send potentially unwanted programs to the user.

browser

A client program that uses the Hypertext Transfer Protocol (HTTP) to make requests of Web servers throughout the Internet. A Web browser graphically displays content for the browser user.

brute-force attack

Also known as brute force cracking, a trial and error method used by application programs to decode encrypted data such as passwords through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or crack, a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

buffer overflow

Buffer overflows occur when suspect programs or processes try to store more data in a buffer (temporary data storage area) on your computer than its limit, corrupting or overwriting valid data in adjacent buffers.

C

cipher text

Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.

client

An application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

compression

A process by which data (files) are compressed into a form that minimizes the space required to store or transmit it.

content-rating groups

Age groups to which a user belongs. Content is rated (that is, made available or blocked) based on the content rating group to which the user belongs. Content rating groups include: young child, child, younger teenager, older teenager, and adult.

cookie

On the World Wide Web, a block of data that a Web server stores on a client system. When a user returns to the same Web site, the browser sends a copy of the cookie back to the server. Cookies are used to identify users, to instruct the server to send a customized version of the requested Web page, to submit account information for the user, and for other administrative purposes.

Cookies allow the Web site to remember who you are and keep track of how many people visited the Web site, when they visited, and which pages were viewed. Cookies also help a company personalize its Web site for you. Many Web sites require a user name and password to access certain pages, and send a cookie to your computer so you do not have to sign in every time. However, cookies can be used for malicious reasons. Online advertising companies often use cookies to determine which sites you commonly visit, and then post ads on your favorite Web sites. Before you allow cookies from a site, make sure that you trust it.

While cookies are a source of information for legitimate companies, they can also be a source of information for hackers. Many Web sites with online stores put credit card and other personal information in cookies to make it simpler for customers making purchases. Unfortunately, there can be security bugs which allow hackers to access the information from the cookies stored on the customers' computers.

D

deep watch location

A folder (and all subfolders) on your computer that is monitored for changes by Data Backup. If you set up a deep watch location, Data Backup backs up the watch file types within that folder and its subfolders.

Denial of Service

On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.

dictionary attack

These attacks involve trying a host of words from a list to determine someone's password. Attackers don't manually try all combinations but have tools that automatically attempt to identify someone's password.

DNS

Acronym for Domain Name System. The hierarchical system by which hosts on the Internet have both domain name addresses (such as bluestem.prairienet.org) and IP addresses (such as 192.17.3.4). The domain name address is used by human users and is automatically translated into the numerical IP address, which is used by the packet-routing software. DNS names consist of a top-level domain (such as .com, .org, and .net), a second-level domain (the site name of a business, an organization, or an individual), and possibly one or more sub-domain (servers within a second-level domain). See also DNS server and IP address.

DNS server

Short for Domain Name System server. A computer that can answer Domain Name System (DNS) queries. The DNS server keeps a database of host computers and their corresponding IP addresses. Presented with the name apex.com, for example, the DNS server would return the IP address of the hypothetical company Apex. Also called: name server. See also DNS and IP address.

domain

An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, www.whitehouse.gov identifies the Web server at the White House, which is part of the U.S. government.

E

e-mail

Electronic Mail, messages sent via the Internet or within a company LAN or WAN. E-mail attachments in the form of EXE (executable) files or VBS (Visual Basic script) files have become increasingly popular as a means of transmitting viruses and Trojans.

e-mail client

An e-mail account. For example, Microsoft Outlook or Eudora.

encryption

A process by which data is transformed from text to code, obscuring the information to make it unreadable by people who do not know how to decrypt it.

ESS (Extended Service Set)

A set of two or more networks that form a single subnetwork.

event

Events from 0.0.0.0

If you see events from IP address 0.0.0.0, there are two likely causes. The first, and most common, is that for some reason your computer received a badly formed packet. The Internet is not always 100% reliable, and bad packets can occur. Since Firewall sees the packets before TCP/IP can validate them, it might report these packets as an event.

The other situation occurs when the source IP is spoofed, or faked. Spoofed packets may be a sign that someone is scanning around looking for Trojans, and they happened to try your computer. It is important to remember that Firewall blocks the attempt.

Events from 127.0.0.1

Events will sometimes list their source IP as 127.0.0.1. It is important to note that this IP is special, and is referred to as the loopback address.

No matter which computer you are using, 127.0.0.1 always refers to your local computer. This address is also referred to as localhost, as the computer name localhost will always resolve back to the IP address 127.0.0.1. Does this mean that your computer is attempting to hack itself? Is some Trojan or spyware taking over your computer? Not likely. Many legitimate programs use the loopback address for communication between components. For example, many personal mail or Web servers let you configure them via a Web interface that is usually accessible through something like http://localhost/.

However, Firewall allows traffic from these programs, so if you see events from 127.0.0.1, it most likely means that the source IP address is spoofed, or faked. Spoofed packets are usually signs of someone scanning for Trojans. It is important to remember that Firewall blocks this attempt. Obviously, reporting events from 127.0.0.1 will not be helpful, so it is unnecessary to do so.

That said, some programs, most notably Netscape 6.2 and higher, require you to add 127.0.0.1 to the **Trusted IP Addresses** list. These programs' components communicate between each other in such a manner that Firewall cannot determine if the traffic is local.

In the example of Netscape 6.2, if you do not trust 127.0.0.1, then you will not be able to use your buddy list. Therefore, if you see traffic from 127.0.0.1 and all of the programs on your computer work normally, then it is safe to block this traffic. However, if a program (like Netscape) is having problems, add 127.0.0.1 to the **Trusted IP Addresses** list in Firewall, and then find out if the problem is resolved.

If placing 127.0.0.1 in the **Trusted IP Addresses** list fixes the problem, then need to consider your options: if you trust 127.0.0.1, your program will work, but you will be more open to spoofed attacks. If you do not trust the address, then your program will not work, but you will remain protected against such malicious traffic.

Events from computers on your LAN

For most corporate LAN settings, you can trust all the computers on your LAN.

Events from private IP addresses

IP addresses of the format 192.168.xxx.xxx, 10.xxx.xxx.xxx, and 172.16.0.0 - 172.31.255.255 are referred to as non-routable or private IP addresses. These IP addresses should never leave your network, and can be trusted most of the time.

The 192.168 block is used with Microsoft Internet Connection Sharing (ICS). If you are using ICS, and see events from this IP block, you might want to add the IP address 192.168.255.255 to your **Trusted IP Addresses** list. This will trust the entire 192.168.xxx.xxx block.

If you are not on a private network, and see events from these IP ranges, the source IP address may be spoofed, or faked. Spoofed packets are usually a sign that someone is scanning around looking for Trojans. It is important to remember that Firewall blocks this attempt.

Since private IP addresses are separate from IP addresses on the Internet, reporting these events will have no effect.

external hard drive

A hard drive that is stored outside of the computer case.

firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially an intranet. All messages entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

full archive

To archive a complete set of data based on the watch file types and locations that you have set up.

header

A header is information added to the portion of the message throughout its life cycle. The header informs the Internet software how to deliver your message, where message replies should be sent, a unique identifier for your e-mail message, and other administrative information. Examples of header fields are: To, From, CC, Date, Subject, Message ID, and Received.

hotspot

A specific geographic location in which an access point (AP) provides public wireless broadband network services to mobile visitors through a wireless network. Hotspots are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centers, and hotels. Hotspots typically have a short range of access.

image analysis

Blocks potentially inappropriate images from appearing. Images are blocked for all users except members of the adult age group.

integrated gateway

A device that combines the functions of an access point (AP), router, and firewall. Some devices may also include security enhancements and bridging features.

Internet

The Internet consists of a huge number of interconnected networks that use the TCP/IP protocols for the location and transfer of data. The Internet evolved from a linking of university and college computers (in the late 1960s and early 1970s) funded by the U.S. Department of Defense and called the ARPANET. The Internet today is a global network of almost 100,000 independent networks.

intranet

A private network, usually inside an organization, that functions very much like the Internet. It has become common practice to permit access to intranets from standalone computers used by students or employees off-campus or off-site. Firewalls, login procedures, and passwords are designed to provide security.

IP address

The Internet Protocol address or IP address is a unique number consisting of four parts separated by dots (e.g. 63.227.89.66). Every computer on the Internet from the largest server to a laptop communicating through a cell phone has a unique IP number. Not every computer has a domain name but everyone has an IP.

The following lists some unusual IP address types:

- Non-Routable IP Addresses: These are also referred to as Private IP Space. These are IP addresses that cannot be used on the Internet. Private IP blocks are 10.x.x.x, 172.16.x.x - 172.31.x.x, and 192.168.x.x.
- Loop-Back IP Addresses**:** Loop-back addresses are used for testing purposes. Traffic sent to this block of IP addresses comes right back to the device generating the packet. It never leaves the device, and is primarily used for hardware and software testing. The Loop-Back IP block is 127.x.x.x.

Null IP Address: This is an invalid address. When it is seen, it indicates that the traffic had a blank IP address. This is obviously not normal, and frequently it indicates that the sender is deliberately obscuring the origin of the traffic. The sender will not be able to receive any replies to their traffic unless the packet is received by an application that understands the contents of the packet that will include instructions specific to that application. Any address that starts with 0 (0.x.x.x) is a null address. For example, 0.0.0.0 is a null IP address.

IP spoofing

Forging the IP addresses in an IP packet. This is used in many types of attacks including session hijacking. It is also often used to fake the e-mail headers of SPAM so they cannot be properly traced.

key

A series of letters and/or numbers used by two devices to authenticate their communication. Both devices must have the key. See also WEP, WPA, WPA2, WPA-PSK, and WPA2- PSK.

keyword

A word that you can assign to a backed up file to establish a relationship or connection with other files that have the same keyword assigned to them. Assigning keywords to files makes it easier to search for files that you have published to the Internet.

LAN (Local Area Network)

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone and radio waves. A system of LANs connected in this way is called a wide-area network (WAN). Most LANs connect workstations and personal computers generally through simple hubs or switches. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices (e.g., printers) anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, for example, by sending e-mail or engaging in chat sessions.

library

The online storage area for files published by Data Backup users. The library is a Web site on the Internet, accessible to anyone with Internet access.

MAC (Media Access Control or Message Authenticator Code)

For the former, see MAC Address. The latter is a code that is used to identify a given message (e.g., a RADIUS message). The code is generally a cryptographically strong hash of the contents of the message which includes a unique value to insure against replay protection.

MAC Address (Media Access Control Address)

A low-level address assigned to the physical device accessing the network.

man-in-the-middle attack

The attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the messages, or enable the attacker to modify them before transmitting them again. The term is derived from the ball game where a number of people try to throw a ball directly to each other while one person in between attempts to catch it.

managed network

A home network with two types of members: managed members and unmanaged members. Managed members allow other computers on the network to monitor their McAfee protection status; unmanaged members do not.

MAPI account

Acronym for Messaging Application Programming Interface. The Microsoft interface specification that allows different messaging and workgroup applications (including e-mail, voice mail, and fax) to work through a single client, such as the Exchange client. For this reason, MAPI is often used in corporate environments when the company is running Microsoft® Exchange Server. However, many people use Microsoft's Outlook for personal Internet e-mail.

MSN account

Acronym for Microsoft Network. An online service and Internet portal. This is a Web-based account.

network

When you connect two or more computers, you create a network.

network drive

A disk or tape drive that is connected to a server on a network that is shared by multiple users. Network drives are sometimes called remote drives.

network map

In Network Manager, a graphical representation of the computers and components that make up a home network.

NIC (Network Interface Card)

A card that plugs into a laptop or other device and connects the device to the LAN.

node

A single computer connected to a network.

online backup repository

The location on the online server where your watch files are stored after being backed up.

parental controls

Settings that let you configure content ratings, which restrict the Web sites and content that a user can view, as well as Internet time limits, which specify the period and duration of time that a user can access the Internet. Parental controls also let you universally restrict access to specific Web sites, and grant or block access based on age groups and associated keywords.

password

A code (usually alphanumeric) you use to gain access to your computer or to a given program or to a Web site.

Password Vault

A secure storage area for your personal passwords. It allows you to store your passwords with confidence that no other user (even a McAfee Administrator or system administrator) can access them.

PCI wireless adapter cards

Connect a desktop computer to a network. The card plugs into a PCI expansion slot inside the computer.

phishing

Pronounced "fishing," it is a scam to steal valuable information such as credit card and social security numbers, user IDs, and passwords. An official-looking e-mail is sent to potential victims pretending to be from their ISP, bank, or retail establishment. E-mails can be sent to people on selected lists or on any list, expecting that some percentage of recipients will actually have an account with the real organization.

plain text

Any message that is not encrypted.

pop-ups

Small windows that appear on top of other windows on your computer screens. Pop-up windows are often used in Web browsers to display advertisements. McAfee blocks pop-up windows that are automatically loaded when a Web page loads in your browser. Pop-up windows that load when you click a link are not blocked by McAfee.

POP3 account

Acronym for Post Office Protocol 3. Most home users have this type of account. This is the current version of the Post Office Protocol standard in common use on TCP/IP networks. Also known as standard e-mail account.

port

A place where information goes into and/or out of a computer; for example, a conventional analog modem is connected to a serial port. The port numbers in TCP/IP communications are virtual values used to separate traffic into application-specific streams. Ports are assigned to standard protocols like SMTP or HTTP so that programs know what port to try a connection on. The destination port for TCP packets indicates the application or server being looked for.

potentially unwanted program

Potentially unwanted programs include spyware, adware, and other programs that gather and transmit your data without your permission.

PPPoE

Point-to-Point Protocol Over Ethernet. Used by many DSL providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet.

protocol

An agreed-upon format for transmitting data between two devices. From a user's perspective, the only interesting aspect about protocols is that their computer or device must support the right ones if they want to communicate with other computers. The protocol can be implemented either in hardware or in software.

proxy

A computer (or the software that runs on it) that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. By acting as a go-between representing all internal computers, the proxy protects network identities while still providing access to the Internet. See also Proxy Server.

proxy server

A firewall component that manages Internet traffic to and from a local area network (LAN). A proxy server can improve performance by supplying frequently requested data, such as a popular Web page, and can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files.

publish

To make a backed up file available publicly, on the Internet.

quarantine

When suspect files are detected, they are quarantined. You can then take appropriate action.

quick archive

To archive only those watch files that have changed since the last full or quick archive.

RADIUS (Remote Access Dial-In User Service)

A protocol that provides for authentication of users, usually in the context of remote access. Originally defined for use with dial-in remote access servers, the protocol is now used in a variety of authentication environments, including 802.1x authentication of a WLAN user's Shared Secret.

real-time scanning

Files are scanned for viruses and other activity when they are accessed by you or your computer.

restore

To retrieve a copy of a file from the online backup repository or an archive.

roaming

The ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

rogue access points

An access point that a company does not authorize for operation. The trouble is that a rogue access points often don't conform to wireless LAN (WLAN) security policies. A rogue access point enables an open, insecure interface to the corporate network from outside the physically controlled facility.

Within a properly secured WLAN, rogue access points are more damaging than rogue users. Unauthorized users trying to access a WLAN likely will not be successful at reaching valuable corporate resources if effective authentication mechanisms are in place. Major issues arise, however, when an employee or hacker plugs in a rogue access point. The rogue allows just about anyone with an 802.11-equipped device on the corporate network. This puts them very close to mission-critical resources.

router

A network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it. To which interface on the router outgoing packets are sent may be determined by any combination of source and destination address as well as current traffic conditions such as load, line costs, bad lines. Sometimes referred to as access point (AP).

script

Scripts can create, copy, or delete files. They can also open your Windows registry.

server

A computer or software that provides specific services to software running on other computers. The "mail server" at your ISP is software that handles all of the incoming and outgoing mail for all of your ISP's users. A server on a LAN is hardware that constitutes the primary node on the network. It can also have software which provides specific services, data, or other capabilities to all of the client computers attached to it.

shallow watch locations

A folder on your computer that is monitored for changes by Data Backup. If you set up a shallow watch location, Data Backup backs up the watch file types within that folder, but does not include its subfolders.

share

An operation that allows e-mail recipients to access selected backed up files for a limited period of time. When you share a file, you send the backed up copy of the file to the e-mail recipients that you specify. Recipients receive an e-mail message from Data Backup indicating that files have been shared with them. The e-mail also contains a link to the shared files.

shared secret

See also RADIUS. Protects sensitive portions of RADIUS messages. This shared secret is a password that is shared between the authenticator and the authentication server in some secure manner.

SMTP server

Acronym for Simple Mail Transfer Protocol. A TCP/IP protocol for sending messages from one computer to another on a network. This protocol is used on the Internet to route e-mail.

SSID (Service Set Identifier)

Network name for the devices in a wireless LAN subsystem. It is a clear text 32-character string added to the head of every WLAN packet. The SSID differentiates one WLAN from another, so all users of a network must supply the same SSID to access a given AP. An SSID prevents access by any client device that does not have the SSID. By default, however, an access point (AP) broadcasts its SSID in its beacon. Even if SSID broadcasting is turned off, a hacker can detect the SSID through sniffing.

SSL (Secure Sockets Layer)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data which is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer use and support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:

standard e-mail account

Most home users have this type of account. See also POP3 account.

synchronize

To resolve inconsistencies between backed up files and those stored on your local computer. You synchronize files when the version of the file in the online backup repository is newer than the version of the file on the other computers. Synchronizing updates the copy of the file on your computers with the version of the file in the online backup repository.

SystemGuard

SystemGuards detect unauthorized changes to your computer and alert you when they occur.

TKIP (Temporal Key Integrity Protocol)

A quick-fix method to overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP changes temporal keys every 10,000 packets, providing a dynamic distribution method that significantly enhances the security of the network. The TKIP (security) process begins with a 128-bit temporal key shared among clients and access points (APs). TKIP combines the temporal key with the (client machine's) MAC address and then adds a relatively large 16-octet initialization vector to produce the key that encrypts the data. This procedure ensures that each station uses different key streams to encrypt the data. TKIP uses RC4 to perform the encryption. WEP also uses RC4.

Trojan

Trojans are programs that pretend to be benign applications. Trojans are not viruses because they do not replicate, but they can be just as destructive.

URL

Uniform Resource Locator. This is the standard format for Internet addresses.

USB wireless adapter cards

Provide an expandable Plug and Play serial interface. This interface provides a standard, low-cost wireless connection for peripheral devices such as keyboards, mice, joysticks, printers, scanners, storage devices, and video conference cameras.

VPN (Virtual Private Network)

A network constructed by using public wires to reunite nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

wardriver

Interlopers armed with laptops, special software, and some makeshift hardware, who drive through cities, suburbs and business parks in order to intercept wireless LAN traffic.

watch file types

The types of files (for example, .doc, .xls, and so on) that Data Backup backs up or archives within the watch locations.

watch locations

The folders on your computer that Data Backup monitors.

Web bugs

Small graphics files that can embed themselves in your HTML pages and allow an unauthorized source to set cookies on your computer. These cookies can then transmit information to the unauthorized source. Web bugs are also called Web beacons, pixel tags, clear GIFs, or invisible GIFs.

WEP (Wired Equivalent Privacy)

An encryption and authentication protocol defined as part of the 802.11 standard. Initial versions are based on RC4 ciphers and have significant weaknesses. WEP attempts to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

whitelist

A list of Web sites that are allowed to be accessed because they are not considered fraudulent.

Wi-Fi (Wireless Fidelity)

Used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is used by the Wi-Fi Alliance.

Wi-Fi Alliance

An organization made up of leading wireless equipment and software providers with the mission of (1) certifying all 802.11-based products for inter-operability and (2) promoting the term Wi-Fi as the global brand name across all markets for any 802.11-based wireless LAN products. The organization serves as a consortium, testing laboratory, and clearinghouse for vendors who want to promote inter-operability and the growth of the industry.

While all 802.11a/b/g products are called Wi-Fi, only products that have passed the Wi-Fi Alliance testing are allowed to refer to their products as Wi-Fi Certified (a registered trademark). Products that pass are required to carry an identifying seal on their packaging that states Wi-Fi Certified and indicates the radio frequency band used. This group was formerly known as the Wireless Ethernet Compatibility Alliance (WECA) but changed its name in October 2002 to better reflect the Wi-Fi brand it wants to build.

Wi-Fi Certified

Any products tested and approved as Wi-Fi Certified (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a Wi-Fi Certified product can use any brand of access point (AP) with any other brand of client hardware that also is certified. Typically, however, any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 11g, 5GHz for 802.11a) works with any other, even if not Wi-Fi Certified.

wireless adapter

Contains the circuitry to enable a computer or other device to communicate with a wireless router (attach to a wireless network). Wireless adapters can be built into the main circuitry of a hardware device or they can be a separate add-on that can be inserted into a device through the appropriate port.

WLAN (Wireless Local Area Network)

See also LAN. A local area network using a wireless medium for connection. A WLAN uses high-frequency radio waves rather than wires to communicate between nodes.

worm

A worm is a self-replicating virus that resides in active memory and can send copies of itself through e-mail messages. Worms replicate and consume system resources, slowing performance or halting tasks.

WPA (Wi-Fi Protected Access)

A specification standard that strongly increases the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, WPA is derived from, and is compatible with, the IEEE 802.11i standard. When properly installed, it provides wireless LAN users with a high level of assurance that their data remains protected and that only authorized network users can access the network.

WPA-PSK

A special WPA mode designed for home users who do not require strong enterprise-class security and do not have access to authentication servers. In this mode, the home user manually enters the starting password to activate Wi-Fi Protected Access in Pre-Shared Key mode, and should change the pass-phrase on each wireless computer and access point regularly. See also WPA2-PSK and TKIP.

WPA2

See also WPA. WPA2 is an update of the WPA security standard and is based on the 802.11i IEEE standard.

WPA2-PSK

See also WPA-PSK and WPA2. WPA2-PSK is similar to WPA-PSK and is based on the WPA2 standard. A common feature of WPA2-PSK is that devices often support multiple encryption modes (e.g., AES, TKIP) simultaneously, while older devices generally supported only a single encryption mode at a time (i.e., all clients would have to use the same encryption mode).

About McAfee

McAfee, Inc., headquartered in Santa Clara, California and the global leader in Intrusion Prevention and Security Risk Management, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security.

Copyright

TRADEMARK ATTRIBUTIONS

Index