McAfee® VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

User Guide

Contents

CHAPTER 1

Introduction

McAfee VirusScan Plus offers proactive PC security to prevent malicious attacks, so you can protect what you value as well as surf, search, and download files online with confidence. McAfee SiteAdvisor's Web safety ratings, help you avoid unsafe Web sites. This service also provides security against multi-pronged attacks by combining anti-virus, anti-spyware and firewall technologies. McAfee's security service continuously delivers the latest software so your protection is never out-of-date. You can now easily add and manage security for multiple PCs in your home. Moreover, improved performance allows it to protect, without disturbing you.

In this chapter

CHAPTER 2

McAfee SecurityCenter

McAfee SecurityCenter allows you to monitor your computer's security status, know instantly whether your computer's virus, spyware, e-mail, and firewall protection services are up-to-date, and act on potential security vulnerabilities. It provides the navigational tools and controls you need to coordinate and manage all areas of your computer's protection.

Before you begin configuring and managing your computer's protection, review the SecurityCenter interface and make sure that you understand the difference between protection status, protection categories, and protection services. Then, update SecurityCenter to ensure that you have the latest protection available from McAfee.

After your initial configuration tasks are complete, you use SecurityCenter to monitor your computer's protection status. If SecurityCenter detects a protection problem, it alerts you so that you can either fix or ignore the problem (depending on its severity). You can also review SecurityCenter events, such as virus scanning configuration changes, in an event log.

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

SecurityCenter features

SecurityCenter provides the following features:

Simplified protection status

Easily review your computer's protection status, check for updates, and fix potential protection problems.

Automated updates and upgrades

Automatically download and install updates for your registered programs. When a new version of a registered McAfee program is available, you get it at no charge while your subscription is valid, 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 options to remove, neutralize, or learn more about the threat.

CHAPTER 3

Using SecurityCenter

Before you begin using SecurityCenter, review the components and configuration areas you will use to manage your computer's protection status. For more information about the terminology used in this image, see Understanding protection status (page 8) and Understanding protection categories (page 9). Then, you can review your McAfee account information and verifying the validity of your subscription.

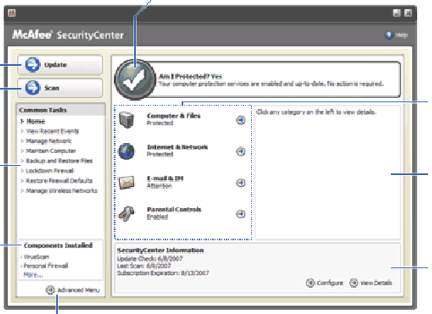
Protection Status Area
Monitor your computer's overall protection status (red, yellow, or green) and automatically fix protection problems.

Update Button
Check for and install SecurityCenter updates.

Scan Button
Scan your computer for viruses, Trojans, and other security threats (if VirusScan is installed).

Common Tasks
Return to the Home pane, view recent events, and perform other popular tasks.

Components Installed Area
See which McAfee security programs are protecting your computer.



Am I Protected? Yes
Your computer protection services are enabled and up-to-date. No action is required.

Click any category on the left to view details.

SecurityCenter Information
Update Check: 6/8/2007
Last Scan: 6/8/2007
Subscription Expiration: 8/13/2007

Protection Categories
Monitor each category's protection status (Protected, Attention, Action Required).

Protection Category Information Area
View a category's protection services and protection problems.

SecurityCenter Information Area
See when the last update of your computer occurred, when the last scan occurred (if VirusScan is installed), and when your subscription expires.

Advanced Menu
Switch to a more advanced menu of configuration options.

In this chapter

Understanding protection status

Your computer's protection status is shown in the protection status area on the SecurityCenter Home pane. It indicates whether your computer is fully protected against the latest security threats and can be influenced by things like external security attacks, other security programs, and programs that access the Internet.

Your computer's protection status can be red, yellow, or green.

Protection Status	Description
Red	Your computer is not protected. The protection status area on the SecurityCenter Home pane is red and states that you are not protected. SecurityCenter reports at least one critical security problem. To achieve full protection, you must fix all critical security problems in each protection category (the problem category's status is set to **Action Required**, also in red). For information about how to fix protection problems, see Fixing protection problems (page 18).
Yellow	Your computer is partially protected. The protection status area on the SecurityCenter Home pane is yellow and states that you are not protected. SecurityCenter reports at least one non-critical security problem. To achieve full protection, you must fix or ignore the non-critical security problems associated with each protection category. For information about how to fix or ignore protection problems, see Fixing or ignoring protection problems (page 17).
Green	Your computer is fully protected. The protection status area on the SecurityCenter Home pane is green and states that you are protected. SecurityCenter does not report any critical or non-critical security problems. Each protection category lists the services that are protecting your computer.

Understanding protection categories

SecurityCenter's protection services are divided into four categories: Computer & Files, Internet & Network, E-mail & IM, and Parental Controls. These categories help you to browse and configure the security services protecting your computer.

You click a category name to configure its protection services and view any security problems detected for those services. If your computer's protection status is red or yellow, one or more categories display an *Action Required* or *Attention* message, indicating that SecurityCenter has detected a problem within the category. For more information about protection status, see Understanding protection status (page 8).

Protection Category	Description
Computer & Files	The Computer & Files category lets you configure the following protection services: ▪ Virus Protection ▪ PUP Protection ▪ System Monitors ▪ Windows Protection
Internet & Network	The Internet & Network category lets you configure the following protection services: ▪ Firewall Protection ▪ Identity Protection
E-mail & IM	The E-mail & IM category lets you configure the following protection services: ▪ E-mail Protection ▪ Spam Protection
Parental Controls	The Parental Controls category lets you configure the following protection services: ▪ Content Blocking

Understanding protection services

Protection services are the core SecurityCenter components that you configure to protect your computer. Protection services directly correspond to McAfee programs. For example, when you install VirusScan, the following protection services become available: Virus Protection, PUP Protection, System Monitors, and Windows Protection. For detailed information about these particular protection services, see the VirusScan help.

By default, all protection services associated with a program are enabled when you install the program; however you can disable a protection service at any time. For example, if you install Privacy Service, Content Blocking and Identity Protection are both enabled. If you do not intend to use the Content Blocking protection service, you can disable it entirely. You can also temporarily disable a protection service while performing setup or maintenance tasks.

Managing your McAfee account

Manage your McAfee account from within SecurityCenter by easily accessing and reviewing your account information and verifying your current subscription status.

Note: If you installed your McAfee programs from a CD, you must register them on the McAfee Web site to set up or update your McAfee account. Only then are you entitled to regular, automatic program updates.

Manage your McAfee account

You can easily access your McAfee account information (My Account) from SecurityCenter.

1. Under **Common Tasks**, click **My Account**.
2. Log in to your McAfee account.

Verify your subscription

You verify your subscription to ensure that it has not yet expired.

- Right-click the SecurityCenter icon in the notification area at the far right of your taskbar, and then click **Verify Subscription**.

CHAPTER 4

Updating SecurityCenter

SecurityCenter ensures that your registered McAfee programs are current by checking for and installing online updates every four hours. Depending on the programs you have installed and registered, online updates may include the latest virus definitions and hacker, spam, spyware, or privacy protection upgrades. If you want to check for updates within the default four hour period, you can do so at any time. While SecurityCenter is checking for updates, you can continue to perform other tasks.

Although it is not recommended, you can change the way SecurityCenter checks for and installs updates. For example, you can configure SecurityCenter to download but not install updates or to notify you before downloading or installing updates. You can also disable automatic updating.

Note: If you installed your McAfee programs from a CD, you cannot receive regular, automatic updates for those programs unless you register them on the McAfee Web site.

In this chapter

Check for updates

By default, SecurityCenter automatically checks for updates every four hours when your computer is connected to the Internet; however, if you want to check for updates within the four hour period, you can do so. If you have disabled automatic updates, it is your responsibility to check for updates regularly.

- On the SecurityCenter Home pane, click **Update**.

Tip: You can check for updates without launching SecurityCenter by right-clicking the SecurityCenter icon M in the notification area at the far right of your taskbar, and then clicking **Updates**.

Configure automatic updates

By default, SecurityCenter automatically checks for and installs updates every four hours when your computer is connected to the Internet. If you want to change this default behavior, you can configure SecurityCenter to automatically download updates and then notify you when the updates are ready to be installed or to notify you before downloading the updates.

Note: SecurityCenter notifies you when updates are ready to be downloaded or installed using alerts. From the alerts, you can either download or install the updates, or postpone the updates. When you update your programs from an alert, you may be prompted to verify your subscription before downloading and installing. For more information, see Working with alerts (page 21).

1 Open the SecurityCenter Configuration pane.

   How?

   1. Under **Common Tasks**, click **Home**.
   2. On the right pane, under **SecurityCenter Information**, click **Configure**.

2 On the SecurityCenter Configuration pane, under **Automatic updates are disabled**, click **On**, and then click **Advanced**.

3 Click one of the following buttons:

   - **Install the updates automatically and notify me when my services are updated (recommended)**
   - **Download the updates automatically and notify me when they are ready to be installed**
   - **Notify me before downloading any updates**

4 Click **OK**.

Disable automatic updates

If you disable automatic updates, it is your responsibility to check for updates regularly; otherwise, your computer will not have the latest security protection. For information about checking for updates manually, see Check for updates (page 13).

1 Open the SecurityCenter Configuration pane.

   How?

1. Under **Common Tasks**, click **Home**.
2. On the right pane, under **SecurityCenter Information**, click **Configure**.

2 On the SecurityCenter Configuration pane, under **Automatic updates are enabled**, click **Off**.

Tip: You enable automatic updates by clicking the **On** button or by clearing **Disable automatic updating and let me manually check for updates** on the Update Options pane.

CHAPTER 5

Fixing or ignoring protection problems

SecurityCenter reports critical and non-critical protection problems as soon as it detects them. Critical protection problems require immediate action and compromise your protection status (changing the color to red). Non-critical protection problems do not require immediate action and may or may not compromise your protection status (depending on the type of problem). To achieve a green protection status, you must fix all critical problems and either fix or ignore all non-critical problems. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician. For more information about McAfee Virtual Technician, see the McAfee Virtual Technician help.

In this chapter

Fixing protection problems

Most security problems can be fixed automatically; however, some problems may require you to take action. For example, if Firewall Protection is disabled, SecurityCenter can enable it automatically; however, if Firewall Protection is not installed, you must install it. The following table describes some other actions that you might take when fixing protection problems manually:

Problem	Action
A full scan of your computer has not been performed in the last 30 days.	Scan your computer manually. For more information, see the VirusScan help.
Your detection signature files (DATs) are out-of-date.	Update your protection manually. For more information, see the VirusScan help.
A program is not installed.	Install the program from the McAfee Web site or CD.
A program is missing components.	Reinstall the program from the McAfee Web site or CD.
A program is not registered, and cannot receive full protection.	Register the program on the McAfee Web site.
A program has expired.	Check your account status on the McAfee Web site.

Note: Often, a single protection problem affects more than one protection category. In this case, fixing the problem in one category clears it from all other protection categories.

Fix protection problems automatically

SecurityCenter can fix most protection problems automatically. The configuration changes that SecurityCenter makes when automatically fixing protection problems are not recorded in the event log. For more information about events, see Viewing events (page 27).

1 Under **Common Tasks**, click **Home**.

2 On the SecurityCenter Home pane, in the protection status area, click **Fix**.

Fix protection problems manually

If one or more protection problems persist after you try to fix them automatically, you can fix the problems manually.

1 Under **Common Tasks**, click **Home**.

2 On the SecurityCenter Home pane, click the protection category in which SecurityCenter reports the problem.

3 Click the link following the description of the problem.

Ignoring protection problems

If SecurityCenter detects a non-critical problem, you can either fix or ignore it. Other non-critical problems (for example, if Anti-Spam or Privacy Service are not installed) are automatically ignored. Ignored problems are not shown in the protection category information area on the SecurityCenter Home pane, unless your computer's protection status is green. If you ignore a problem, but later decide that you want it to appear in the protection category information area even when your computer's protection status is not green, you can show the ignored problem.

Ignore a protection problem

If SecurityCenter detects a non-critical problem that you do not intend to fix, you can ignore it. Ignoring it removes the problem from the protection category information area in SecurityCenter.

1 Under **Common Tasks**, click **Home**.

2 On the SecurityCenter Home pane, click the protection category in which the problem is reported.

3 Click the **Ignore** link beside the protection problem.

Show or hide ignored problems

Depending on its severity, you can show or hide an ignored protection problem.

1 Open the Alert Options pane.

   How?

   1. Under **Common Tasks**, click **Home**.
   2. On the right pane, under **SecurityCenter Information**, click **Configure**.
   3. Under **Alerts**, click **Advanced**.

2 On the SecurityCenter Configuration pane, click **Ignored Problems**.

3 On the Ignored Problems pane, do the following:

   - To ignore a problem, select its check box.
   - To report a problem in the protection category information area, clear its check box.

4 Click **OK**.

Tip: You can also ignore a problem by clicking the **Ignore** link beside the reported problem in the protection category information area.

CHAPTER 6

Working with alerts

Alerts are small pop-up dialog boxes that appear in the bottom-right corner of your screen when certain SecurityCenter events occur. An alert provides detailed information about an event as well as recommendations and options for resolving problems that may be associated with the event. Some alerts also contain links to additional information about the event. These links let you launch McAfee's global Web site or send information to McAfee for troubleshooting.

There are three types of alerts: red, yellow, and green.

Alert Type	Description
Red	A red alert is a critical notification that requires a response from you. Red alerts occur when SecurityCenter cannot determine how to fix a protection problem automatically.
Yellow	A yellow alert is a non-critical notification that usually requires a response from you.
Green	A green alert is a non-critical notification that does not require a response from you. Green alerts provide basic information about an event.

Because alerts play such an important role in monitoring and managing your protection status, you cannot disable them. However, you can control whether certain types of informational alerts appear and configure some other alert options (such as whether SecurityCenter plays a sound with an alert or displays the McAfee splash screen on startup).

In this chapter

Showing and hiding informational alerts

Informational alerts notify you when events occur that do not pose threats to your computer's security. For example, if you have set up Firewall Protection, an informational alert appears by default whenever a program on your computer is granted access to the Internet. If you do not want a specific type of informational alert to appear, you can hide it. If you do not want any informational alerts to appear, you can hide them all. You can also hide all informational alerts when you play a game in full-screen mode on your computer. When you finish playing the game and exit full-screen mode, SecurityCenter starts displaying informational alerts again.

If you mistakenly hide an informational alert, you can show it again at any time. By default, SecurityCenter shows all informational alerts.

Show or hide informational alerts

You can configure SecurityCenter to show some informational alerts and hide others, or to hide all informational alerts.

1 Open the Alert Options pane.

   How?

   1. Under **Common Tasks**, click **Home**.
   2. On the right pane, under **SecurityCenter Information**, click **Configure**.
   3. Under **Alerts**, click **Advanced**.

2 On the SecurityCenter Configuration pane, click **Informational Alerts**.

3 On the Informational Alerts pane, do the following:

   - To show an informational alert, clear its check box.
   - To hide an informational alert, select its check box.
   - To hide all informational alerts, select the **Do not show informational alerts** check box.

4 Click **OK**.

Tip: You can also hide an informational alert by selecting the **Do not show this alert again** check box in the alert itself. If you do so, you can show the informational alert again by clearing the appropriate check box on the Informational Alerts pane.

Show or hide informational alerts when gaming

You can hide informational alerts when you are playing a game in full-screen mode on your computer. When you finish the game and exit full-screen mode, SecurityCenter starts displaying informational alerts again.

1 Open the Alert Options pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the right pane, under **SecurityCenter Information**, click **Configure**.
3. Under **Alerts**, click **Advanced**.

2 On the Alert Options pane, select or clear the **Show informational alerts when gaming mode is detected** check box.

3 Click **OK**.

Configuring alert options

The appearance and frequency of alerts is configured by SecurityCenter; however, you can adjust some basic alert options. For example, you can play a sound with alerts or hide the splash screen alert from displaying when Windows starts. You can also hide alerts that notify you about virus outbreaks and other security threats in the online community.

Play a sound with alerts

If you want to receive an audible indication that an alert has occurred, you can configure SecurityCenter to play a sound with each alert.

1 Open the Alert Options pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the right pane, under **SecurityCenter Information**, click **Configure**.
3. Under **Alerts**, click **Advanced**.

2 On the Alert Options pane, under **Sound**, select the **Play a sound when an alert occurs** check box.

Hide the splash screen at startup

By default, the McAfee splash screen appears briefly when Windows starts, notifying you that SecurityCenter is protecting your computer. However, you can hide the splash screen if you do not want it to appear.

1 Open the Alert Options pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the right pane, under **SecurityCenter Information**, click **Configure**.
3. Under **Alerts**, click **Advanced**.

2 On the Alert Options pane, under **Splash Screen**, clear the **Show the McAfee splash screen when Windows starts** check box.

Tip: You can show the splash screen again at any time by selecting the **Show the McAfee splash screen when Windows starts** check box.

Hide virus outbreak alerts

You can hide alerts that notify you about virus outbreaks and other security threats in the online community.

1 Open the Alert Options pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the right pane, under **SecurityCenter Information**, click **Configure**.
3. Under **Alerts**, click **Advanced**.

2 On the Alert Options pane, clear the **Alert me when a virus or security threat occurs** check box.

Tip: You can show virus outbreak alerts at any time by selecting the **Alert me when a virus or security threat occurs** check box.

CHAPTER 7

Viewing events

An event is an action or configuration change that occurs within a protection category and its related protection services. Different protection services record different types of events. For example, SecurityCenter records an event if a protection service is enabled or disabled; Virus Protection records an event each time a virus is detected and removed; and Firewall Protection records an event each time an Internet connection attempt is blocked. For more information about protection categories, see Understanding protection categories (page 9).

You can view events when troubleshooting configuration issues and reviewing operations performed by other users. Many parents use the event log to monitor their children's behavior on the Internet. You view recent events if you want to examine only the last 30 events that occurred. You view all events if you want to examine a comprehensive list of all events that occurred. When you view all events, SecurityCenter launches the event log, which sorts events according to the protection category in which they occurred.

In this chapter

View recent events

You view recent events if you want to examine only the last 30 events that occurred.

- Under **Common Tasks,** click **View Recent Events**.

View all events

You view all events if you want to examine a comprehensive list of all events that occurred.

1 Under **Common Tasks,** click **View Recent Events**.

2 On the Recent Events pane, click **View Log**.

3 On the event log's left pane, click the type of events you want to view.

CHAPTER 8

McAfee VirusScan

VirusScan's advanced detection and protection services defend you and your computer from the latest security threats, including viruses, Trojans, tracking cookies, spyware, adware, and other potentially unwanted programs. Protection extends beyond the files and folders on your desktop, targeting threats from different points of entry—including e-mail, instant messages, and the Web.

With VirusScan, your computer's protection is immediate and constant (no tedious administration required). While you work, play, browse the Web, or check your e-mail, it runs in the background, monitoring, scanning, and detecting potential harm in real time. Comprehensive scans run on schedule, periodically checking your computer using a more sophisticated set of options. VirusScan offers you the flexibility to customize this behavior if you want to; but if you don't, your computer remains protected.

With normal computer use, viruses, worms, and other potential threats may infiltrate your computer. If this occurs, VirusScan notifies you about the threat, but usually handles it for you, cleaning or quarantining infected items before any damage occurs. Although rare, further action may sometimes be required. In these cases, VirusScan lets you decide what to do (rescan the next time you start your computer, keep the detected item, or remove the detected item).

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

VirusScan features

VirusScan provides the following features.

Comprehensive virus protection

VirusScan's advanced detection and protection services defend you and your computer from the latest security threats, including viruses, Trojans, tracking cookies, spyware, adware, and other potentially unwanted programs. Protection extends beyond the files and folders and on your desktop, targeting threats from different points of entry—including e-mail, instant messages, and the Web. No tedious administration required.

Resource-aware scanning options

If you experience slow scan speeds, then you can disable the option to use minimal computer resources, but keep in mind that highter priority will be given to virus protection than to other tasks. VirusScan offers you the flexibility to customize real-time and manual scanning options if you want to; but if you don't, your computer remains protected.

Automatic repairs

If VirusScan detects a security threat while running a real-time or manual scan, it tries to handle the threat automatically according to the threat type. This way, most threats can be detected and neutralized without your interaction. Although rare, VirusScan may not be able to neutralize a threat on its own. In these cases, VirusScan lets you decide what to do (rescan the next time you start your computer, keep the detected item, or remove the detected item).

Pausing tasks in full-screen mode

When enjoying things like watching movies, playing games on your computer, or any activity that occupies your entire computer screen, VirusScan pauses a number of tasks, such as manual scans.

Starting real-time virus protection

VirusScan provides two types of virus protection: real-time and manual. Real-time virus protection constantly monitors your computer for virus activity, scanning files each time you or your computer access them. Manual virus protection lets you scan files on demand. To make sure that your computer stays protected against the latest security threats, leave real-time virus protection on and set up a schedule for regular, more comprehensive, manual scans. By default, VirusScan performs a scheduled scan once a week. For more information about real-time and manual scanning, see Scanning your computer (page 53).

Although rare, there may be times when you want to temporarily stop real-time scanning (for example, to change some scanning options or troubleshoot a performance issue). When real-time virus protection is disabled, your computer is not protected and your SecurityCenter protection status is red. For more information about protection status, see "Understanding protection status" in the SecurityCenter help.

Start real-time virus protection

By default, real-time virus protection is turned on and protecting your computer against viruses, Trojans, and other security threats. If you turn off real-time virus protection, you must turn it on again to stay protected.

1 Open the Computer & Files Configuration pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the Configure pane, click **Computer & Files**.

2 Under **Virus protection**, click **On**.

Stop real-time virus protection

You can turn off real-time virus protection temporarily, and then specify when it resumes. You can automatically resume protection after 15, 30, 45, or 60 minutes, when your computer restarts, or never.

1 Open the Computer & Files Configuration pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the Configure pane, click **Computer & Files**.

2 Under **Virus protection**, click **Off**.

3 In the dialog box, select when to resume real-time scanning.

4 Click **OK**.

CHAPTER 9

Starting additional protection

In addition to real-time virus protection, VirusScan provides advanced protection against scripts, spyware, and potentially harmful e-mail and instant message attachments. By default, script scanning, spyware, e-mail, and instant messaging protection are turned on and protecting your computer.

Script scanning protection

Script scanning protection detects potentially harmful scripts and prevents them from running on your computer. It monitors your computer for suspect script activity, such as a script that creates, copies, or deletes files, or opens your Windows registry, and alerts you before any damage occurs.

Spyware protection

Spyware protection detects spyware, adware, and other potentially unwanted programs. Spyware is software that can be secretly installed on your computer to monitor your behavior, collect personal information, and even interfere with your control of the computer by installing additional software or redirecting browser activity.

E-mail protection

E-mail protection detects suspect activity in the e-mail and attachments you send.

Instant messaging protection

Instant messaging protection detects potential security threats from instant message attachments that you receive. It also prevents instant messaging programs from sharing personal information.

In this chapter

Start script scanning protection

Turn on script scanning protection to detect potentially harmful scripts and prevent them from running on your computer. Script scanning protection alerts you when a script tries to create, copy, or delete files on your computer, or make changes to your Windows registry.

1 Open the Computer & Files Configuration pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the Configure pane, click **Computer & Files**.

2 Under **Script scanning protection**, click **On**.

Note: Although you can turn off script scanning protection at any time, doing so leaves your computer vulnerable to harmful scripts.

Start spyware protection

Turn on spyware protection to detect and remove spyware, adware, and other potentially unwanted programs that gather and transmit information without your knowledge or permission.

1 Open the Computer & Files Configuration pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the Configure pane, click **Computer & Files**.

2 Under **Script scanning protection**, click **On**.

Note: Although you can turn off spyware protection at any time, doing so leaves your computer vulnerable to potentially unwanted programs.

Start e-mail protection

Turn on e-mail protection to detect worms as well as potential threats in inbound (POP3) e-mail messages and attachments.

1 Open the E-mail & IM Configuration pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the Configure pane, click **E-mail & IM**.

2 Under **E-mail protection**, click **On**.

Note: Although you can turn off e-mail protection at any time, doing so leaves your computer vulnerable to e-mail threats.

Start instant messaging protection

Turn on instant messaging protection to detect security threats that can be included in inbound instant message attachments.

1 Open the E-mail & IM Configuration pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the Configure pane, click **E-mail & IM**.

2 Under **Instant Messaging protection**, click **On**.

Note: Although you can turn off instant messaging protection at any time, doing so leaves your computer vulnerable to harmful instant message attachments.

CHAPTER 10

Setting up virus protection

VirusScan provides two types of virus protection: real-time and manual. Real-time virus protection scans files each time you or your computer access them. Manual virus protection lets you scan files on demand. You can set different options for each type of protection. For example, because real-time protection continuously monitors your computer, you might select a certain set of basic scanning options, reserving a more comprehensive set of scanning options for manual, on-demand protection.

In this chapter

Setting real-time scan options

When you start real-time virus protection, VirusScan uses a default set of options to scan files; however, you can change the default options to suit your needs.

To change real-time scanning options, you must make decisions about what VirusScan checks for during a scan, as well as the locations and file types it scans. For example, you can determine whether VirusScan checks for unknown viruses or cookies that Web sites can use to track your behavior, and whether it scans network drives that are mapped to your computer or just local drives. You can also determine what types of files are scanned (all files, or just program files and documents, since that is where most viruses are detected).

When changing real-time scanning options, you must also determine whether it's important for your computer to have buffer overflow protection. A buffer is a portion of memory used to temporarily hold computer information. Buffer overflows can occur when the amount of information suspect programs or processes store in a buffer exceeds the buffer's capacity. When this occurs, your computer becomes more vulnerable to security attacks.

Set real-time scan options

You set real-time scan options to customize what VirusScan looks for during a real-time scan, as well as the locations and file types it scans. Options include scanning for unknown viruses and tracking cookies as well as providing buffer overflow protection. You can also configure real-time scanning to check network drives that are mapped to your computer.

1 Open the Real-Time Scanning pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the SecurityCenter Home pane, click **Computer & Files**.
3. In the Computer & Files information area, click **Configure**.
4. On the Computer & Files Configuration pane, ensure that virus protection is enabled, and then click **Advanced**.

2 Specify your real-time scanning options, and then click **OK**.

To...	Do this...
Detect unknown viruses and new variants of known viruses	Select the **Scan for unknown viruses using heuristics** check box.

To...	Do this...
Detect cookies	Select the **Scan and remove tracking cookies** check box.
Detect viruses and other potential threats on drives that are connected to your network	Select the **Scan network drives** check box.
Protect your computer from buffer overflows	Select the **Enable buffer overflow protection** check box.
Specify which types of files to scan	Click either **All files (recommended)** or **Program files and documents only**.

Setting manual scan options

Manual virus protection lets you scan files on demand. When you start a manual scan, VirusScan checks your computer for viruses and other potentially harmful items using a more comprehensive set of scanning options. To change manual scanning options, you must make decisions about what VirusScan checks for during a scan. For example, you can determine whether VirusScan looks for unknown viruses, potentially unwanted programs, such as spyware or adware, stealth programs, such as rootkits which can grant unauthorized access to your computer, and cookies that Web sites can use to track your behavior. You must also make decisions about the types of files that are checked. For example, you can determine whether VirusScan checks all files or just program files and documents (since that is where most viruses are detected). You can also determine whether archive files (for example, .zip files) are included in the scan.

By default, VirusScan checks all the drives and folders on your computer each time it runs a manual scan; however, you can change the default locations to suit your needs. For example, you can scan only critical system files, items on your desktop, or items in your Program Files folder. Unless you want to be responsible for initiating each manual scan yourself, you can set up a regular schedule for scans. Scheduled scans always check your entire computer using the default scan options. By default, VirusScan performs a scheduled scan once a week.

If you find that you are experiencing slow scan speeds, consider disabling the option to use minimal computer resources, but keep in mind that higher priority will be given to virus protection than to other tasks.

Note: When enjoying things like watching movies, playing games on your computer, or any activity that occupies your entire computer screen, VirusScan pauses a number of tasks, including automatic updates and manual scans.

Set manual scan options

You set manual scan options to customize what VirusScan looks for during a manual scan as well as the locations and file types it scans. Options include scanning for unknown viruses, file archives, spyware and potentially unwanted programs, tracking cookies, rootkits, and stealth programs.

1 Open the Manual Scan pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the SecurityCenter Home pane, click **Computer & Files**.
3. In the Computer & Files information area, click **Configure**.
4. On the Computer & Files Configuration pane, ensure that virus protection is enabled, and click **Advanced**.
5. Click **Manual Scan** in the Virus Protection pane.

2 Specify your manual scanning options, and then click **OK**.

To...	Do this...
Detect unknown viruses and new variants of known viruses	Select the **Scan for unknown viruses using heuristics** check box.
Detect and remove viruses in .zip and other archive files	Select the **Scan .zip and other archive files** check box.
Detect spyware, adware, and other potentially unwanted programs	Select the **Scan for spyware and potentially unwanted programs** check box.
Detect cookies	Select the **Scan and remove tracking cookies** check box.
Detect rootkits and stealth programs that can alter and exploit existing Windows system files	Select the **Scan for rootkits and other stealth programs** check box.
Use less processor power for scans while giving higher priority to other tasks (such as Web browsing or opening documents)	Select the **Scan using minimal computer resources** check box.
Specify which types of files to scan	Click either **All files (recommended)** or **Program files and documents only**.

Set manual scan location

You set the manual scan location to determine where VirusScan looks for viruses and other harmful items during a manual scan. You can scan all files, folders, and drives on your computer or you can restrict scanning to specific folders and drives.

1 Open the Manual Scan pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the SecurityCenter Home pane, click **Computer & Files**.
3. In the Computer & Files information area, click **Configure**.
4. On the Computer & Files Configuration pane, ensure that virus protection is enabled, and click **Advanced**.
5. Click **Manual Scan** in the Virus Protection pane.

2 Click **Default Location to Scan**.

3 Specify your manual scanning location, and then click **OK**.

To...	Do this...
Scan all the files and folders on your computer	Select the **(My) Computer** check box.
Scan specific files, folders, and drives on your computer	Clear the **(My) Computer** check box, and select one or more folders or drives.
Scan critical system files	Clear the **(My) Computer** check box, and then select the **Critical System Files** check box.

Schedule a scan

Schedule scans to thoroughly check your computer for viruses and other threats any day and time of the week. Scheduled scans always check your entire computer using the default scan options. By default, VirusScan performs a scheduled scan once a week. If you find that you are experiencing slow scan speeds, consider disabling the option to use minimal computer resources, but keep in mind that higher priority will be given to virus protection than to other tasks.

1 Open the Scheduled Scan pane.

How?

1. Under **Common Tasks**, click **Home**.
2. On the SecurityCenter Home pane, click **Computer & Files**.
3. In the Computer & Files information area, click **Configure**.
4. On the Computer & Files Configuration pane, ensure that virus protection is enabled, and click **Advanced**.
5. Click **Scheduled Scan** in the Virus Protection pane.

2 Select **Enable scheduled scanning**.

3 To reduce the amount of processor power normally used for scanning, select **Scan using minimal computer resources**.

4 Select one or more days.

5 Specify a start time.

6 Click **OK**.

Tip: You can restore the default schedule by clicking **Reset**.

Using SystemGuards options

SystemGuards monitor, log, report, and manage potentially unauthorized changes made to the Windows registry or critical system files on your computer. Unauthorized registry and file changes can harm your computer, compromise its security, and damage valuable system files.

Registry and files changes are common and occur regularly on your computer. Because many are harmless, SystemGuards' default settings are configured to provide reliable, intelligent, and real-world protection against unauthorized changes that pose significant potential for harm. For example, when SystemGuards detect changes that are uncommon and present a potentially significant threat, the activity is immediately reported and logged. Changes that are more common, but still pose some potential for damage, are logged only. However, monitoring for standard and low-risk changes is, by default, disabled. SystemGuards technology can be configured to extend its protection to any environment you like.

There are three types of SystemGuards: Program SystemGuards, Windows SystemGuards, and Browser SystemGuards.

Program SystemGuards

Program SystemGuards detect potentially unauthorized changes to your computer's registry and other critical files that are essential to Windows. These important registry items and files include ActiveX installations, startup items, Windows shell execute hooks, and shell service object delay loads. By monitoring these, Program SystemGuards technology stops suspect ActiveX programs (downloaded from the Internet) in addition to spyware and potentially unwanted programs that can automatically launch when Windows starts.

Windows SystemGuards

Windows SystemGuards also detect potentially unauthorized changes to your computer's registry and other critical files that are essential to Windows. These important registry items and files include context menu handlers, appInit DLLs, and the Windows hosts file. By monitoring these, Windows SystemGuards technology helps prevent your computer from sending and receiving unauthorized or personal information over the Internet. It also helps stop suspect programs that can bring unwanted changes to the appearance and behavior of the programs that are important to you and your family.

Browser SystemGuards

Like Program and Windows SystemGuards, Browser SystemGuards detect potentially unauthorized changes to your computer's registry and other critical files that are essential to Windows. Browser SystemGuards, however, monitor changes to important registry items and files like Internet Explorer add-ons, Internet Explorer URLs, and Internet Explorer security zones. By monitoring these, Browser SystemGuards technology helps prevent unauthorized browser activity such as redirection to suspect Web sites, changes to browser settings and options without your knowledge, and unwanted trusting of suspect Web sites.

Enable SystemGuards protection

Enable SystemGuards protection to detect and alert you to potentially unauthorized Windows registry and file changes on your computer. Unauthorized registry and file changes can harm your computer, compromise its security, and damage valuable system files.

1 Open the Computer & Files Configuration pane.

   How?

   1. On the left pane, click **Advanced Menu**.
   2. Click **Configure**.
   3. On the Configure pane, click **Computer & Files**.

2 Under **SystemGuard protection**, click **On**.

Note: You can disable SystemGuard protection, by clicking **Off**.

Configure SystemGuards options

Use the SystemGuards pane to configure protection, logging, and alerting options against unauthorized registry and file changes associated with Windows files, programs, and Internet Explorer. Unauthorized registry and file changes can harm your computer, compromise its security, and damage valuable system files.

1 Open the SystemGuards pane.

   1. Under **Common Tasks**, click **Home**.
   2. On the SecurityCenter Home pane, click **Computer & Files**.
   3. In the Computer & Files information area, click **Configure**.
   4. On the Computer & Files Configuration pane, ensure that SystemGuard protection is enabled, and click **Advanced**.

2 Select a SystemGuard type from the list.

   - **Program SystemGuards**
   - **Windows SystemGuards**

- **Browser SystemGuards**

3 Under **I want to**, do one of the following:

- To detect, log, and report unauthorized registry and file changes associated with Program, Windows, and Browsers SystemGuards, click **Show alerts.**
- To detect and log unauthorized registry and file changes associated with Program, Windows, and Browsers Systemguards, click **Only log changes.**
- To disable detection of unauthorized registry and file changes associated with Program, Windows, and Browser Systemguards, click **Disable the SystemGuard.**

Note: For more information about SystemGuards types, see About SystemGuards types (page 46).

About SystemGuards types

SystemGuards detect potentially unauthorized changes to your computer's registry and other critical files that are essential to Windows. There are three types of SystemGuards: Program SystemGuards, Windows SystemGuards, and Browser SystemGuards

Program SystemGuards

Program SystemGuards technology stops suspect ActiveX programs (downloaded from the Internet) in addition to spyware and potentially unwanted programs that can automatically launch when Windows starts.

SystemGuard	Detects...
ActiveX Installations	Unauthorized registry changes to ActiveX installations that can harm your computer, compromise its security, and damage valuable system files.
Startup Items	Spyware, adware, and other potentially unwanted programs that can install file changes to startup items, allowing suspect programs to run when you start your computer.
Windows Shell Execute Hooks	Spyware, adware, and other potentially unwanted programs that can install Windows shell execute hooks to prevent security programs from running properly.
Shell Service Object Delay Load	Spyware, adware, and other potentially unwanted programs that can make registry changes to the shell service object delay load, allowing harmful files to run when you start your computer.

Windows SystemGuards

Windows SystemGuards technology helps prevent your computer from sending and receiving unauthorized or personal information over the Internet. It also helps stop suspect programs that can bring unwanted changes to the appearance and behavior of the programs that are important to you and your family.

SystemGuard	Detects...
Context Menu Handlers	Unauthorized registry changes to Windows context menu handlers that can affect the appearance and behavior of Windows menus. Context menus allow you to perform actions on your computer, such as right-clicking files.
AppInit DLLs	Unauthorized registry changes to Windows appInit DLLs that can allow potentially harmful files to run when you start your computer.
Windows Hosts File	Spyware, adware, and potentially unwanted programs that can make unauthorized changes in your Windows hosts file, allowing your browser to be redirected to suspect Web sites and to block software updates.
Winlogon Shell	Spyware, adware, and other potentially unwanted programs that can make registry changes to the Winlogon shell, allowing other programs to replace Windows Explorer.
Winlogon User Init	Spyware, adware, and other potentially unwanted programs that can make registry changes to Winlogon user init, allowing suspect programs to run when you log on to Windows.
Windows Protocols	Spyware, adware, and other potentially unwanted programs that can make registry changes to Windows protocols, affecting how your computer sends and receives information on the Internet.
Winsock Layered Service Providers	Spyware, adware, and other potentially unwanted programs that can install registry changes to Winsock Layered Service Providers (LSPs) to intercept and change information you send and receive on the Internet.
Windows Shell Open Commands	Unauthorized changes to Windows shell open commands that can allow worms and other harmful programs to run on your computer.
Shared Task Scheduler	Spyware, adware, and other potentially unwanted programs that can make registry and file changes to the shared task scheduler, allowing potentially harmful files to run when you start your computer.

SystemGuard	Detects...
Windows Messenger Service	Spyware, adware, and other potentially unwanted programs that can make registry changes to the Windows messenger service, allowing unsolicited ads and remotely run programs on your computer.
Windows Win.ini File	Spyware, adware, and other potentially unwanted programs that can make changes to the Win.ini file, allowing suspect programs to run when you start your computer.

Browser SystemGuards

Browser SystemGuards technology helps prevent unauthorized browser activity such as redirection to suspect Web sites, changes to browser settings and options without your knowledge, and unwanted trusting of suspect Web sites.

SystemGuard	Detects...
Browser Helper Objects	Spyware, adware, and other potentially unwanted programs that can use browser helper objects to track Web browsing and show unsolicited ads.
Internet Explorer Bars	Unauthorized registry changes to Internet Explorer Bar programs, such as Search and Favorites, that can affect the appearance and behavior of Internet Explorer.
Internet Explorer Add-ons	Spyware, adware, and other potentially unwanted programs that can install Internet Explorer add-ons to track Web browsing and show unsolicited ads.
Internet Explorer ShellBrowser	Unauthorized registry changes to the Internet Explorer shell browser that can affect the appearance and behavior of your Web browser.
Internet Explorer WebBrowser	Unauthorized registry changes to the Internet Explorer Web browser that can affect the appearance and behavior of your browser.
Internet Explorer URL Search Hooks	Spyware, adware, and other potentially unwanted programs that can make registry changes to Internet Explorer URL search hooks, allowing your browser to be redirected to suspect Web sites when searching the Web.
Internet Explorer URLs	Spyware, adware, and other potentially unwanted programs that can make registry changes to Internet Explorer URLs, affecting browser settings.

SystemGuard	Detects...
Internet Explorer Restrictions	Spyware, adware, and other potentially unwanted programs that can make registry changes to Internet Explorer restrictions, affecting browser settings and options.
Internet Explorer Security Zones	Spyware, adware, and other potentially unwanted programs that can make registry changes to Internet Explorer security zones, allowing potentially harmful files to run when you start your computer.
Internet Explorer Trusted Sites	Spyware, adware, and other potentially unwanted programs that can make registry changes to Internet Explorer trusted sites, allowing your browser to trust suspect Web sites.
Internet Explorer Policy	Spyware, adware, and other potentially unwanted programs that can make registry changes to Internet Explorer policies, affecting the appearance and behavior of your browser.

Using trusted lists

If VirusScan detects a file or registry change (SystemGuard), program, or buffer overflow, it prompts you to trust or remove it. If you trust the item and indicate that you do not want to receive future notification about its activity, the item is added to a trusted list and VirusScan no longer detects it or notifies you about its activity. If an item has been added to a trusted list, but you decide you want to block its activity, you can do so. Blocking prevents the item from running or making any changes to your computer without notifying you each time an attempt is made. You can also remove an item from a trusted list. Removing allows VirusScan to detect the item's activity again.

Manage trusted lists

Use the Trusted Lists pane to trust or block items that have been previously detected and trusted. You can also remove an item from a trusted list so that VirusScan detects it again.

1. Open the Trusted Lists pane.
    1. Under **Common Tasks**, click **Home**.
    2. On the SecurityCenter Home pane, click **Computer & Files**.
    3. In the Computer & Files information area, click **Configure**.
    4. On the Computer & Files Configuration pane, ensure that virus protection is enabled, and click **Advanced**.
    5. Click **Trusted Lists** in the Virus Protection pane.
2. Select one of the following trusted list types:
    - **Program SystemGuards**
    - **Windows SystemGuards**
    - **Browser SystemGuards**
    - **Trusted Programs**
    - **Trusted Buffer Overflows**
3. Under **I want to**, do one of the following:
    - To allow the detected item to make changes to the Windows registry or critical system files on your computer without notifying you, click **Trust**.
    - To block the detected item from making changes to the Windows registry or critical system files on your computer without notifying you, click **Block**.
    - To remove the detected item from the trusted lists, click **Remove**.

4 Click **OK**.

Note: For more information about trusted list types, see About trusted lists types (page 51).

About trusted lists types

SystemGuards on the Trusted Lists pane represent previously unauthorized registry and file changes that VirusScan has detected but that you have chosen to allow from an alert of from the Scan results pane. There are five types of trusted list types that you can manage on the Trusted Lists pane: Program SystemGuards, Windows SystemGuards, Browser SystemGuards, Trusted Programs, and Trusted Buffer Overflows.

Option	Description
Program SystemGuards	Program SystemGuards on the Trusted Lists pane represent previously unauthorized registry and file changes that VirusScan has detected, but that you have chosen to allow from an alert or from the Scan Results pane. Program SystemGuards detect unauthorized registry and file changes associated with ActiveX installations, startup items, Windows shell execute hooks, and shell service object delay load activity. These types of unauthorized registry and file changes can harm your computer, compromise its security, and damage valuable system files.
Windows SystemGuards	Windows SystemGuards on the Trusted Lists pane represent previously unauthorized registry and file changes that VirusScan has detected, but that you have chosen to allow from an alert or from the Scan Results pane. Windows SystemGuards detect unauthorized registry and file changes associated with context menu handlers, appInit DLLs, the Windows hosts file, the Winlogon shell, Winsock Layered Service Providers (LSPs), and so on. These types of unauthorized registry and file changes can affect how your computer sends and receives information over the Internet, change the appearance and behavior of programs, and allow suspect programs to run on your computer.

Option	Description
Browser SystemGuards	Browser SystemGuards on the Trusted Lists pane represent previously unauthorized registry and file changes that VirusScan has detected, but that you have chosen to allow from an alert or from the Scan Results pane. Browser SystemGuards detect unauthorized registry changes and other unwanted behavior associated with Browser helper objects, Internet Explorer add-ons, Internet Explorer URLs, Internet Explorer security zones, and so on. These types of unauthorized registry changes can result in unwanted browser activity such as redirection to suspect Web sites, changes to browser settings and options, and trusting of suspect Web sites.
Trusted Programs	Trusted programs are potentially unwanted programs that VirusScan has previously detected, but which you have chosen to trust from an alert or from the Scan Results pane.
Trusted Buffer Overflows	Trusted buffer overflows represent previously unwanted activity that VirusScan has detected, but which you have chosen to to trust from an alert or from the Scan Results pane. Buffer overflows can harm your computer and damage files. Buffer overflows occur when the amount of information suspect programs or processes store in a buffer exceeds the buffer's capacity.

CHAPTER 11

Scanning your computer

When you start SecurityCenter for the first time, VirusScan's real-time virus protection starts protecting your computer from potentially harmful viruses, Trojans, and other security threats. Unless you disable real-time virus protection, VirusScan constantly monitors your computer for virus activity, scanning files each time you or your computer access them, using the real-time scanning options that you set. To make sure that your computer stays protected against the latest security threats, leave real-time virus protection on and set up a schedule for regular, more comprehensive manual scans. For more information about setting real-time and manual scan options, see Setting up virus protection (page 37).

VirusScan provides a more detailed set of scanning options for manual virus protection, allowing you to periodically run more extensive scans. You can run manual scans from SecurityCenter, targeting specific locations according to a set schedule. However, you can also run manual scans directly in Windows Explorer while you work. Scanning in SecurityCenter offers the advantage of changing scanning options on-the-fly. However, scanning from Windows Explorer offers a convenient approach to computer security.

Whether you run a manual scan from SecurityCenter or Windows Explorer, you can view the scan results when it finishes. You view the results of a scan to determine whether VirusScan has detected, repaired, or quarantined viruses, trojans, spyware, adware, cookies, and other potentially unwanted programs. The results of a scan can be displayed in different ways. For example, you can view a basic summary of scan results or detailed information, such as the infection status and type. You can also view general scan and detection statistics.

In this chapter

Scan your computer

You can run a manual scan from either the Advanced or Basic menu in SecurityCenter. If you run a scan from the Advanced menu, you can confirm your manual scan options before scanning. If you run a scan from the Basic menu, VirusScan starts scanning immediately, using the existing scanning options. You can also run a scan in Windows Explorer using the existing scanning options.

- Do one of the following:

  Scan in SecurityCenter

To...	Do this...
Scan using existing settings	Click **Scan** on the Basic menu.
Scan using changed settings	Click **Scan** on the Advanced menu, select the locations to scan, select scan options, and then cliick **Scan Now**.

Scan in Windows Explorer

1. Open Windows Explorer.
2. Right-click a file, folder, or drive, and then click **Scan**.

Note: The scan results appear in the Scan completed alert. Results include the number of items scanned, detected, repaired, quarantined, and removed. Click **View scan details** to learn more about the scan results or work with infected items.

View scan results

When a manual scan finishes, you view the results to determine what the scan found and to analyze the current protection status of your computer. Scan results tell you whether VirusScan detected, repaired, or quarantined viruses, trojans, spyware, adware, cookies, and other potentially unwanted programs.

- On the Basic or Advanced menu, click **Scan** and then do one of the following:

To...	Do this...
View scan results in the alert	View scan results in the Scan completed alert.
View more information about scan results	Click **View scan details** in the Scan completed alert.
View a quick summary of the scan results	Point to the **Scan completed icon** in the notification area on your taskbar.

To...	Do this...
View scan and detection statistics	Double-click the **Scan completed** icon in the notification area on your taskbar.
View details about detected items, infection status, and type.	Double-click the **Scan completed** icon in the notification area on your taskbar, and then click **View Results** on the Scan Progress: Manual Scan pane.

CHAPTER 12

Working with scan results

If VirusScan detects a security threat while running a real-time or manual scan, it tries to handle the threat automatically according to the threat type. For example, If VirusScan detects a virus, Trojan, or tracking cookie on your computer, it tries to clean the infected file. If it cannot clean the file, VirusScan quarantines it.

With some security threats, VirusScan may not be able to clean or quarantine a file successfully. In this case, VirusScan prompts you to handle the threat. You can take different actions depending on the threat type. For example, if a virus is detected in a file, but VirusScan cannot successfully clean or quarantine the file, it denies further access to it. If tracking cookies are detected, but VirusScan cannot successfully clean or quarantine the cookies, you can decide whether to remove or trust the them. If potentially unwanted programs are detected, VirusScan does not take any automatic action; instead, it lets you decide whether to quarantine or trust the program.

When VirusScan quarantines items, it encrypts and then isolates them in a folder to prevent the files, programs, or cookies from harming your computer. You can restore or remove the quarantined items. In most cases, you can delete a quarantined cookie without impacting your system; however, if VirusScan has quarantined a program that you recognize and use, consider restoring it.

In this chapter

Work with viruses and Trojans

If VirusScan detects a virus or Trojan in a file on your computer during a real-time scan or manual scan, it tries to clean the file. If it cannot clean the file, VirusScan tries to quarantine it. If this too fails, access to the file is denied (in real-time scans only).

1 Open the Scan Results pane.

How?

1. Double-click the **Scan completed** icon in the notification area at the far right of your taskbar.
2. On the Scan Progress: Manual Scan pane, click **View Results**.

2 In the scan results list, click **Viruses and Trojans**.

Note: To work with the files that VirusScan has quarantined, see Work with quarantined files (page 58).

Work with potentially unwanted programs

If VirusScan detects a potentially unwanted program on your computer during a real-time or manual scan, you can either remove or trust the program. Removing the potentially unwanted program does not actually delete it from your system. Instead, removing quarantines the program to prevent it from causing damage to your computer or files.

1 Open the Scan Results pane.

How?

1. Double-click the **Scan completed** icon in the notification area at the far right of your taskbar.
2. On the Scan Progress: Manual Scan pane, click **View Results**.

2 In the scan results list, click **Potentially Unwanted Programs.**

3 Select a potentially unwanted program.

4 Under **I want to**, click either **Remove** or **Trust**.

5 Confirm your selected option.

Work with quarantined files

When VirusScan quarantines infected files, it encrypts and then moves them to a folder to prevent the files from harming your computer. You can then restore or remove the quarantined files.

1 Open the Quarantined Files pane.

How?

1. On the left pane, click **Advanced Menu**.
2. Click **Restore**.
3. Click **Files**.

2 Select a quarantined file.

3 Do one of the following:

- To repair the infected file and return it to its original location on your computer, click **Restore**.

- To remove the infected file from your computer, click **Remove**.

4 Click **Yes** to confirm your selected option.

Tip: You can restore or remove multiple files at the same time.

Work with quarantined programs and cookies

When VirusScan quarantines potentially unwanted programs or tracking cookies, it encrypts and then moves them to a protected folder to prevent the programs or cookies from harming your computer. You can then restore or remove the quarantined items. In most cases, you can delete a quarantined without impacting your system.

1 Open the Quarantined Programs and Tracking Cookies pane.

   How?

   1. On the left pane, click **Advanced Menu**.
   2. Click **Restore**.
   3. Click **Programs and Cookies**.

2 Select a quarantined program or cookie.

3 Do one of the following:

   - To repair the infected file and return it to its original location on your computer, click **Restore**.
   - To remove the infected file from your computer, click **Remove**.

4 Click **Yes** to confirm the operation.

Tip: You can restore or remove multiple programs and cookies at the same time.

CHAPTER 13

McAfee Personal Firewall

Personal Firewall offers advanced protection for your computer and your personal data. Personal Firewall establishes a barrier between your computer and the Internet, silently monitoring Internet traffic for suspicious activities.

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

Personal Firewall features

Personal Firewall provides the following features.

Standard and custom protection levels

Guard against intrusion and suspicious activity using Firewall's default or customizable protection settings.

Real-time recommendations

Receive recommendations, dynamically, to help you determine whether programs should be granted Internet access or network traffic should be trusted.

Intelligent access management for programs

Manage Internet access for programs, through alerts and Event Logs, and configure access permissions for specific programs.

Gaming protection

Prevent alerts regarding intrusion attempts and suspicious activities from distracting you during full-screen gameplay.

Computer startup protection

As soon as Windows® starts, Firewall protects your computer from intrusion attempts, unwanted programs and network traffic.

System service port control

Manage open and closed system service ports required by some programs.

Manage computer connections

Allow and block remote connections between other computers and your computer.

HackerWatch information integration

Track global hacking and intrusion patterns through HackerWatch's Web site, which also provides current security information about programs on your computer, as well as global security events and Internet port statistics.

Lockdown Firewall

Instantly block all inbound and outbound traffic between your computer and the Internet.

Restore Firewall

Instantly restore Firewall's original protection settings.

Advanced Trojan detection

Detect and block potentially malicious applications, such as Trojans, from relaying your personal data to the Internet.

Event logging

Track recent inbound, outbound, and intrusion events.

Monitor Internet traffic

Review worldwide maps showing the source of hostile attacks and traffic. In addition, locate detailed owner information and geographical data for originating IP addresses. Also, analyze inbound and outbound traffic, monitor program bandwidth and program activity.

Intrusion prevention

Protect your privacy from possible Internet threats. Using heuristic-like functionality, McAfee provides a tertiary layer of protection by blocking items that display symptoms of attacks or characteristics of hacking attempts.

Sophisticated traffic analysis

Review both inbound and outbound Internet traffic and program connections, including those that are actively listening for open connections. This allows you to see and act upon programs that can be vulnerable to intrusion.

CHAPTER 14

Starting Firewall

As soon as you install Firewall, your computer is protected from intrusion and unwanted network traffic. In addition, you are ready to handle alerts and manage inbound and outbound Internet access for known and unknown programs. Smart Recommendations and Trusting security level (with the option selected to allow programs outbound-only Internet access) are automatically enabled.

Although you can disable Firewall from the Internet & Network Configuration pane, your computer will no longer be protected from intrusion and unwanted network traffic, and you will be unable to effectively manage inbound and outbound Internet connections. If you must disable firewall protection, do so temporarily and only when necessary. You can also enable Firewall from the Internet & Network Configuration panel.

Firewall automatically disables Windows® Firewall and sets itself as your default firewall.

Note: To configure Firewall, open the Internet & Network Configuration pane.

In this chapter

Start firewall protection

You can enable Firewall to protect your computer from intrusion and unwanted network traffic, as well as manage inbound and outbound Internet connections.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, and then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is disabled**, click **On**.

Stop firewall protection

You can disable Firewall if you do not want to protect your computer from intrusion and unwanted network traffic. When Firewall is disabled, you cannot manage inbound or outbound Internet connections.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, and then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Off**.

CHAPTER 15

Working with alerts

Firewall employs an array of alerts to help you manage your security. These alerts can be grouped into three basic types:

- Red alert
- Yellow alert
- Green alert

Alerts can also contain information to help you decide how to handle alerts or get information about programs running on your computer.

In this chapter

About alerts

Firewall has three basic alert types. As well, some alerts include information to help you learn or get information about programs running on your computer.

Red alert

A red alert appears when Firewall detects, then blocks, a Trojan on your computer, and recommends that you scan for additional threats. A Trojan appears to be a legitimate program, but can disrupt, damage, and provide unauthorized access to your computer. This alert occurs in every security level, except Open.

Yellow alert

The most common type of alert is a yellow alert, which informs you about a program activity or network event detected by Firewall. When this occurs, the alert describes the program activity or network event, and then provides you with one or more options that require your response. For example, the **New Network Detected** alert appears when a computer with Firewall installed is connected to a new network. You can choose to trust or not trust the network. If the network is trusted, Firewall allows traffic from any other computer on the network and is added to Trusted IP Addresses. If Smart Recommendations is enabled, programs are added to the Program Permissions pane.

Green alert

In most cases, a green alert provides basic information about an event and does not require a response. Green alerts are disabled by default, and usually occur when Standard, Trusting, Tight, and Stealth security levels are set.

User Assistance

Many Firewall alerts contain additional information to help you manage your computer's security, which includes the following:

- **Learn more about this program**: Launch McAfee's global security Web site to get information about a program that Firewall has detected on your computer.
- **Tell McAfee about this program**: Send information to McAfee about an unknown file that Firewall has detected on your computer.
- **McAfee recommends**: Advice about handling alerts. For example, an alert can recommend that you allow access for a program.

CHAPTER 16

Managing informational alerts

Firewall allows you to display or hide informational alerts when it detects intrusion attempts or suspicious activity during certain events, for example, during full-screen gameplay.

In this chapter

Display alerts while gaming

You can allow Firewall informational alerts to be displayed when it detects intrusion attempts or suspicious activity during full-screen gameplay.

1. On the McAfee SecurityCenter pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, under **Alerts**, click **Advanced**.
4. On the Alert Options pane, select **Show informational alerts when gaming mode is detected**.
5. Click **OK**.

Hide informational alerts

You can prevent Firewall informational alerts from being displayed when it detects intrusion attempts or suspicious activity.

1. On the McAfee SecurityCenter pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, under **Alerts**, click **Advanced**.
4. On the SecurityCenter Configuration pane, click **Informational Alerts**.
5. On the Informational Alerts pane, do one of the following:
   - Select **Do not show informational alerts** to hide all informational alerts.
   - Clear an alert to hide.
6. Click **OK**.

CHAPTER 17

Configuring Firewall protection

Firewall offers a number of methods to manage your security and to tailor the way you want to respond to security events and alerts.

After you install Firewall for the first time, your computer's protection security level is set to Trusting and your programs are allowed outbound-only Internet access. However, Firewall provides other levels, ranging from highly restrictive to highly permissive.

Firewall also offers you the opportunity to receive recommendations on alerts and Internet access for programs.

In this chapter

Managing Firewall security levels

Firewall's security levels control the degree to which you want to manage and respond to alerts. These alerts appear when it detects unwanted network traffic and inbound and outbound Internet connections. By default, Firewall's security level is set to Trusting, with outbound-only access.

When Trusting security level is set and Smart Recommendations is enabled, yellow alerts provide the option to either allow or block access for unknown programs that require inbound access. When known programs are detected, green informational alerts appear, and access is automatically allowed. Allowing access lets a program create outbound connections and listen for unsolicited incoming connections.

Generally, the more restrictive a security level (Stealth and Tight), the greater the number of options and alerts that are displayed and which, in turn, must be handled by you.

The following table describes Firewall's six security levels, starting from the most restrictive to the least:

Level	Description
Lockdown	Blocks all inbound and outbound network connections, including access to Web sites, e-mail, and security updates. This security level has the same result as removing your connection to the Internet. You can use this setting to block ports you set to open on the System Services pane.
Stealth	Blocks all inbound Internet connections, except open ports, hiding your computer's presence on the Internet. The firewall alerts you when new programs attempt outbound Internet connections or receive inbound connection requests. Blocked and added programs appear on the Program Permissions pane.
Tight	Alerts you when new programs attempt outbound Internet connections or receive inbound connection requests. Blocked and added programs appear on the Program Permissions pane. When the security level is set to Tight, a program only requests the type of access it requires at that time, for example outbound-only access, which you can either allow or block. Later, if the program requires both an inbound and an outbound connection, you can allow full access for the program from the Program Permissions pane.
Standard	Monitors inbound and outbound connections and alerts you when new programs attempt Internet access. Blocked and added programs appear on the Program Permissions pane.

Level	Description
Trusting	Allows programs to have either inbound and outbound (full) or outbound-only Internet access. The default security level is Trusting with the option selected to allow programs outbound-only access. If a program is allowed full access, then Firewall automatically trusts it and adds it to the list of allowed programs on the Program Permissions pane. If a program is allowed outbound-only access, then Firewall automatically trusts it when making an outbound Internet connection only. An inbound connection is not automatically trusted.
Open	Allows all inbound and outbound Internet connections.

Firewall also allows you to immediately reset your security level to Trusting (and allow outbound-only access) from the Restore Firewall Protection Defaults pane.

Set security level to Lockdown

You can set Firewall's security level to Lockdown to block all inbound and outbound network connections.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, move the slider so that **Lockdown** displays as the current level.
4. Click **OK**.

Set security level to Stealth

You can set the Firewall security level to Stealth to block all inbound network connections, except open ports, to hide your computer's presence on the Internet.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, move the slider so that **Stealth** displays as the current level.
4. Click **OK**.

Note: In Stealth mode, Firewall alerts you when new programs request outbound Internet connection or receive inbound connection requests.

Set security level to Tight

You can set the Firewall security level to Tight to receive alerts when new programs attempt outbound Internet connections or receive inbound connection requests.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, move the slider so that **Tight** displays as the current level.
4. Click **OK**.

Note: In Tight mode, a program only requests the type of access it requires at that time, for example, outbound-only access, which you can allow or block. If the program later requires both an inbound and an outbound connection, you can allow full access for the program from the Program Permissions pane.

Set security level to Standard

You can set the security level to Standard to monitor inbound and outbound connections and alert you when new programs attempt Internet access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, move the slider so that **Standard** displays as the current level.
4. Click **OK**.

Set security level to Trusting

You can set Firewall's security level to Trusting to allow either full access or outbound-only network access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, move the slider so that **Trusting** displays as the current level.
4. Do one of the following:
   - To allow full inbound and outbound network access, select **Allow Full Access**.
   - To allow outbound-only network access, select **Allow Outbound-Only Access**.

5 Click **OK**.

Note: The **Allow Outbound-Only Access** is the default option.

Set security level to Open

You can set Firewall's security level to Open to allow all inbound and outbound network connections.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Security Level pane, move the slider so that **Open** displays as the current level.

4 Click **OK**.

Configuring Smart Recommendations for alerts

You can configure Firewall to include, exclude, or display recommendations in alerts when any programs attempt Internet access. Enabling Smart Recommendations helps you decide how to handle alerts.

When Smart Recommendations is enabled (and the security level is set to Trusting with outbound-only access enabled), Firewall automatically allows or blocks known programs, and displays in the alert a recommendation when it detects potentially dangerous programs.

When Smart Recommendations is disabled, Firewall neither allows or blocks Internet access, nor recommends an action plan in the alert.

When Smart Recommendations is set to Display Only, an alert prompts you to allow or block access, but recommends an action plan in the alert.

Enable Smart Recommendations

You can enable Smart Recommendations for Firewall to automatically allow or block programs, and alert you about unrecognized and potentially dangerous programs.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, under **Smart Recommendations**, select **Enable Smart Recommendations**.
4. Click **OK**.

Disable Smart Recommendations

You can disable Smart Recommendations for Firewall to allow or block programs, and alert you about unrecognized and potentially dangerous programs. However, the alerts exclude any recommendations about handling access for programs. If Firewall detects a new program that is suspicious or is known to be a possible threat, it automatically blocks the program from accessing the Internet.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, under **Smart Recommendations**, select **Disable Smart Recommendations**.
4. Click **OK**.

Display Smart Recommendations only

You can display Smart Recommendations for the alerts to provide action plan recommendations only so that you decide whether to allow or block unrecognized and potentially dangerous programs.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, under **Smart Recommendations**, select **Display Only**.
4. Click **OK**.

Optimizing Firewall security

There are many ways the security of your computer can be compromised. For example, some programs can attempt to connect to the Internet before Windows® starts. In addition, sophisticated computer users can trace (or ping) your computer to determine whether it is connected to a network. Firewall allows you to defend against both types of intrusion by allowing you to enable startup protection and to block ping requests. The first setting blocks programs from accessing the Internet as Windows starts up and the second blocks ping requests that help other users detect your computer on a network.

Standard installation settings include automatic detection for the most common intrusion attempts, such as Denial of Service attacks or exploits. Using the standard installation settings ensures that you are protected against these attacks and scans; however, you can disable automatic detection for one or more attacks or scans on the Intrusion Detection pane.

Protect your computer during startup

You can protect your computer as Windows starts up to block new programs that did not have, and now need, Internet access during startup. Firewall displays relevant alerts for programs that had requested Internet access, which you can allow or block. To use this option, your security level must not be set to Open or Lockdown.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Security Level pane, under **Security Settings**, select **Enable startup protection**.
4. Click **OK**.

Note: Blocked connections and intrusions are not logged while startup protection is enabled.

Configure ping request settings

You can allow or prevent detection of your computer on the network by other computer users.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Security Level pane, under **Security Settings**, do one of the following:

- Select **Allow ICMP ping requests** to allow detection of your computer on the network using ping requests.
- Clear **Allow ICMP ping requests** to prevent detection of your computer on the network using ping requests.

4 Click **OK**.

Configure intrusion detection

You can detect intrusion attempts to protect your computer from attacks and unauthorized scans. The standard Firewall setting includes automatic detection for the most common intrusion attempts, such as Denial of Service attacks or exploits; however, you can disable automatic detection for one or more attacks or scans.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **Intrusion Detection**.

4 Under **Detect Intrusion Attempts**, do one of the following:

- Select a name to automatically detect the attack or scan.
- Clear a name to disable automatic detection of the attack or scan.

5 Click **OK.**

Configure Firewall Protection Status settings

You can configure Firewall to ignore that specific problems on your computer are not reported to the SecurityCenter.

1 On the McAfee SecurityCenter pane, under **SecurityCenter Information**, click **Configure**.

2 On the SecurityCenter Configuration pane, under **Protection Status**, click **Advanced**.

3 On the Ignored Problems pane, select one or more of the following options:

- **Firewall protection is disabled.**

- **Firewall is set to Open security level.**
- **Firewall service is not running.**
- **Firewall Protection is not installed on your computer.**
- **Your Windows Firewall is disabled.**
- **Outbound firewall is not installed on your computer.**

4 Click **OK**.

Locking and restoring Firewall

Lockdown instantly blocks all inbound and outbound network traffic to help you isolate and troubleshoot a problem on your computer.

Lock Firewall instantly

You can lock Firewall to instantly block all network traffic between your computer and the Internet.

1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Lockdown Firewall**.
2. On the Lockdown Firewall pane, click **Lockdown**.
3. Click **Yes** to confirm.

> **Tip:** You can also lock Firewall by right-clicking the SecurityCenter icon M in the notification area at the far right of your taskbar, then click **Quick Links**, and then click **Lockdown Firewall**.

Unlock Firewall instantly

You can unlock Firewall to instantly allow all network traffic between your computer and the Internet.

1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Lockdown Firewall**.
2. On the Lockdown Enabled pane, click **Unlock**.
3. Click **Yes** to confirm.

Restore Firewall settings

You can quickly restore Firewall to its original protection settings. This restore resets your security level to Trusting and allows outbound-only network access, enables Smart Recommendations, restores the list of default programs and their permissions in the Program Permissions pane, removes trusted and banned IP addresses, and restores system services, event log settings, and intrusion detection.

1. On the McAfee SecurityCenter pane, click **Restore Firewall Defaults**.
2. On the Restore Firewall Protection Defaults pane, click **Restore Defaults**.
3. Click **Yes** to confirm.

Tip: You can also restore Firewall's default settings by right-clicking the SecurityCenter icon M in the notification area at the far right of your taskbar, then click **Quick Links**, and then click **Restore Firewall Defaults**.

CHAPTER 18

Managing programs and permissions

Firewall allows you to manage and create access permissions for existing and new programs that require inbound and outbound Internet access. Firewall lets you control full or outbound-only access for programs. You can also block access for programs.

In this chapter

Allowing Internet access for programs

Some programs, like Internet browsers, need to access the Internet to function properly.

Firewall allows you use the Program Permissions page to:

- Allow access for programs
- Allow outbound-only access for programs
- Block access for programs

You can also allow a program to have full and outbound-only Internet access from the Outbound Events and Recent Events log.

Allow full access for a program

You can allow an existing blocked program on your computer to have full inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Program Permissions**.
4. Under **Program Permissions**, select a program with **Blocked** or **Outbound-Only Access**.
5. Under **Action**, click **Allow Access**.
6. Click **OK**.

Allow full access for a new program

You can allow a new program on your computer to have full inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Program Permissions**.
4. Under **Program Permissions**, click **Add Allowed Program**.
5. In the **Add Program** dialog box, browse for and select the program that you want to add, then click **Open**.

Note: You can change the permissions of a newly added program as you would an existing program by selecting the program, and then clicking **Allow Outbound-Only Access** or **Block Access** under **Action**.

Allow full access from the Recent Events log

You can allow an existing blocked program that appears in the Recent Events log to have full inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Advanced Menu**.
2. Click **Reports & Logs**.
3. Under **Recent Events**, select the event description, and then click **Allow Access**.
4. In the Program Permissions dialog, click **Yes** to confirm.

Related topics

- View outbound events (page 107)

Allow full access from the Outbound Events log

You can allow an existing blocked program that appears in the Outbound Events log to have full inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Advanced Menu**.
2. Click **Reports & Logs**.
3. Under **Recent Events**, click **View Log**.
4. Click **Internet & Network**, and then click **Outbound Events**.
5. Select a program, and under **I want to**, click **Allow Access**.
6. In the Program Permissions dialog, click **Yes** to confirm.

Allowing outbound-only access for programs

Some programs on your computer require outbound Internet access. Firewall lets you configure program permissions to allow outbound-only Internet access.

Allow outbound-only access for a program

You can allow a program to have outbound-only Internet access.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **Program Permissions**.

4 Under **Program Permissions**, select a program with **Blocked** or **Full Access**.

5 Under **Action**, click **Allow Outbound-Only Access**.

6 Click **OK**.

Allow outbound-only access from the Recent Events log

You can allow an existing blocked program that appears in the Recent Events log to have outbound-only Internet access.

1 On the McAfee SecurityCenter pane, click **Advanced Menu**.

2 Click **Reports & Logs**.

3 Under **Recent Events**, select the event description, and then click **Allow Outbound-Only Access**.

4 In the Program Permissions dialog, click **Yes** to confirm.

Allow outbound-only access from the Outbound Events log

You can allow an existing blocked program that appears in the Outbound Events log to have outbound-only Internet access.

1 On the McAfee SecurityCenter pane, click **Advanced Menu**.

2 Click **Reports & Logs**.

3 Under **Recent Events**, click **View Log**.

4 Click **Internet & Network**, and then click **Outbound Events**.

5 Select a program, and under **I want to**, click **Allow Outbound-Only Access**.

6 In the Program Permissions dialog, click **Yes** to confirm.

Blocking Internet access for programs

Firewall allows you to block programs from accessing the Internet. Ensure that blocking a program will not interrupt with your network connection or another program that requires access to the Internet to function properly.

Block access for a program

You can block a program from having inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Program Permissions**.
4. Under **Program Permissions**, select a program with **Full Access** or **Outbound-Only Access**.
5. Under **Action**, click **Block Access**.
6. Click **OK**.

Block access for a new program

You can block a new program from having inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Program Permissions**.
4. Under **Program Permissions**, click **Add Blocked Program**.
5. On the Add Program dialog, browse for an select the program that you want to add, and then click **Open**.

Note: You can change the permissions of a newly added program by selecting the program and then clicking **Allow Outbound-Only Access** or **Allow Access** under **Action**.

Block access from the Recent Events log

You can block a program that appears in the Recent Events log from having inbound and outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Advanced Menu**.
2. Click **Reports & Logs**.
3. Under **Recent Events**, select the event description, and then click **Block Access**.
4. In the Program Permissions dialog, click **Yes** to confirm.

Removing access permissions for programs

Before removing a program permission, ensure that its absence does not affect your computer's functionality or your network connection.

Remove a program permission

You can remove a program from having any inbound or outbound Internet access.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Program Permissions**.
4. Under **Program Permissions**, select a program.
5. Under **Action**, click **Remove Program Permission**.
6. Click **OK**.

Note: Firewall prevents you from modifying some programs by dimming and disabling certain actions.

Learning about programs

If you are unsure which program permission to apply, you can get information about the program on McAfee's HackerWatch Web site.

Get program information

You can get program information from McAfee's HackerWatch Web site to decide whether to allow or block inbound and outbound Internet access.

Note: Ensure that you are connected to the Internet so that your browser launches McAfee's HackerWatch Web site, which provides up-to-date information about programs, Internet access requirements, and security threats.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Program Permissions**.
4. Under **Program Permissions**, select a program.
5. Under **Action**, click **Learn More**.

Get program information from the Outbound Events log

From the Outbound Events log, you can get program information from McAfee's HackerWatch Web site to decide which programs to allow or block inbound and outbound Internet access.

Note: Ensure that you are connected to the Internet so that your browser launches McAfee's HackerWatch Web site, which provides up-to-date information about programs, Internet access requirements, and security threats.

1. On the McAfee SecurityCenter pane, click **Advanced Menu**.
2. Click **Reports & Logs**.
3. Under Recent Events, select an event, and then click **View Log**.
4. Click **Internet & Network**, and then click **Outbound Events**.
5. Select an IP address, and then click **Learn more**.

CHAPTER 19

Managing system services

To work properly, certain programs (including Web servers and file-sharing server programs) must accept unsolicited connections from other computers through designated system service ports. Typically, Firewall closes these system service ports because they represent the most likely source of insecurities in your system. To accept connections from remote computers, however, the system service ports must be open.

In this chapter

Configuring system service ports

System service ports can be configured to allow or block remote network access to a service on your computer.

The list below shows the common system services and their associated ports:

- File Transfer Protocol (FTP) Ports 20-21
- Mail Server (IMAP) Port 143
- Mail Server (POP3) Port 110
- Mail Server (SMTP) Port 25
- Microsoft Directory Server (MSFT DS) Port 445
- Microsoft SQL Server (MSFT SQL) Port 1433
- Network Time Protocol Port 123
- Remote Desktop / Remote Assistance / Terminal Server (RDP) Port 3389
- Remote Procedure Calls (RPC) Port 135
- Secure Web Server (HTTPS) Port 443
- Universal Plug and Play (UPNP) Port 5000
- Web Server (HTTP) Port 80
- Windows File Sharing (NETBIOS) Ports 137-139

System service ports can also be configured to allow a computer to share its Internet connection with other computers connected to it through the same network. This connection, known as Internet Connection Sharing (ICS), allows the computer that is sharing the connection to act as a gateway to the Internet for the other networked computer.

Note: If your computer has an application that accepts either Web or FTP server connections, the computer sharing the connection may need to open the associated system service port and allow forwarding of incoming connections for those ports.

Allow access to an existing system service port

You can open an existing port to allow remote access to a network service on your computer.

Note: An open system service port can make your computer vulnerable to Internet security threats; therefore, only open a port if necessary.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **System Services**.
4. Under **Open System Service Port**, select a system service to open its port.
5. Click **OK**.

Block access to an existing system service port

You can close an existing port to block remote network access to a service on your computer.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **System Services**.
4. Under **Open System Service Port**, clear a system service to close its port.
5. Click **OK**.

Configure a new system service port

You can configure a new network service port on your computer that you can open or close to allow or block remote access on your computer.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **System Services**.
4. Click **Add**.
5. In the System Services pane, under **Ports and System Services**, enter the following:
   - Program name
   - Inbound TCP/IP ports

- Outbound TCP/IP ports
- Inbound UDP ports
- Outbound UDP ports

6 If you want to send this port's activity information to another networked Windows computer that shares your Internet connection, select **Forward network activity on this port to network users who use Internet Connection Sharing**.

7 Optionally describe the new configuration.

8 Click **OK**.

Note: If your computer has a program that accepts either Web or FTP server connections, the computer sharing the connection may need to open the associated system service port and allow forwarding of incoming connections for those ports. If you are using Internet Connection Sharing (ICS), you also need to add a trusted computer connection on the Trusted IP Addresses list. For more information, see Add a trusted computer connection.

Modify a system service port

You can modify inbound and outbound network access information about an existing system service port.

Note: If port information is entered incorrectly, the system service fails.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **System Services**.

4 Select a system service, and then click **Edit**.

5 In the System Services pane, under **Ports and System Services**, enter the following:

- Program name
- Inbound TCP/IP ports
- Outbound TCP/IP ports
- Inbound UDP ports
- Outbound UDP ports

6 If you want to send this port's activity information to another networked Windows computer that shares your Internet connection, select **Forward network activity on this port to network users who use Internet Connection Sharing**.

7 Optionally describe the modified configuration.

8 Click **OK**.

Remove a system service port

You can remove an existing system service port from your computer. After removal, remote computers can no longer access the network service on your computer.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **System Services**.

4 Select a system service, and then click **Remove**.

5 At the prompt, click **Yes** to confirm.

CHAPTER 20

Managing computer connections

You can configure Firewall to manage specific remote connections to your computer by creating rules, based on Internet Protocol addresses (IPs), that are associated with remote computers. Computers that are associated with trusted IP addresses can be trusted to connect to your computer and those IPs that are unknown, suspicious, or distrusted, can be banned from connecting to your computer.

When allowing a connection, ensure that the computer that you trust is safe. If a computer that you trust is infected through a worm or other mechanism, your computer can be vulnerable to infection. In addition, McAfee recommends that the computer(s) you trust are protected by a firewall and an up-to-date antivirus program also. Firewall does not log traffic or generate event alerts from IP addresses in the Trusted IP Addresses list.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

In this chapter

Trusting computer connections

You can add, edit, and remove trusted IP addresses on the Trusted and Banned IPs pane, under **Trusted IP Addresses**.

The **Trusted IP Addresses** list on the Trusted and Banned IPs pane allows all traffic from a specific computer to reach your computer. Firewall does not log traffic or generate event alerts from IP addresses that appear in the **Trusted IP Addresses** list.

Firewall trusts any checked IP addresses on the list, and always allows traffic from a trusted IP through the firewall on any port. Activity between the computer associated with a trusted IP address and your computer is not filtered or analyzed by Firewall. By default, Trusted IP Addresses lists the first private network that Firewall finds.

When allowing a connection, ensure that the computer that you trust is safe. If a computer that you trust is infected through a worm or other mechanism, your computer can be vulnerable to infection. In addition, McAfee recommends that the computer(s) you trust are protected by a firewall and an up-to-date antivirus program also.

Add a trusted computer connection

You can add a trusted computer connection and its associated IP address.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Trusted and Banned IPs**.
4. On the Trusted and Banned IPs pane, select **Trusted IP Addresses**, and then click **Add**.
5. Under **Add Trusted IP Address Rule**, do one of the following:
   - Select **Single IP Address**, and then enter the IP address.
   - Select **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** boxes.

6 If a system service uses Internet Connection Sharing (ICS), you can add the following IP address range: 192.168.0.1 to 192.168.0.255.

7 Optionally, select **Rule expires in**, and enter the number of days to enforce the rule.

8 Optionally, type a description for the rule.

9 Click **OK**.

10 On the **Trusted and Banned IPs** dialog, click **Yes** to confirm.

Note: For more information about Internet Connection Sharing (ICS), see Configure a new system service.

Add a trusted computer from the Inbound Events log

You can add a trusted computer connection and its associated IP address from the Inbound Events log.

1 On the McAfee SecurityCenter pane, on the Common Tasks pane, click **Advanced Menu**.

2 Click **Reports & Logs**.

3 Under **Recent Events**, click **View Log**.

4 Click **Internet & Network**, and then click **Inbound Events**.

5 Select a source IP address, and under **I want to**, click **Trust This Address**.

6 Click **Yes** to confirm.

Edit a trusted computer connection

You can edit a trusted computer connection and its associated IP address.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **Trusted and Banned IPs**.

4 On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.

5 Select an IP address, and then click **Edit**.

6 Under **Edit Trusted IP Address**, do one of the following:

- Select **Single IP Address**, and then enter the IP address.
- Select **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** boxes.

7 Optionally, check **Rule expires in**, and enter the number of days to enforce the rule.

8 Optionally, type a description for the rule.

9 Click **OK**.

Note: You cannot edit the default(s) computer connection(s) that Firewall automatically added from a trusting private network.

Remove a trusted computer connection

You can remove a trusted computer connection and its associated IP address.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **Trusted and Banned IPs**.

4 On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.

5 Select an IP address, and then click **Remove**.

6 In the **Trusted and Banned IPs** dialog, click **Yes** to confirm.

Banning computer connections

You can add, edit, and remove banned IP addresses in the Trusted and Banned IPs pane, under **Banned IP Addresses**.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

Add a banned computer connection

You can add a banned computer connection and its associated IP address.

Note: Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers.

1 On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.

2 On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.

3 On the Firewall pane, click **Trusted and Banned IPs**.

4 On the Trusted and Banned IPs pane, select **Banned IP Addresses**, and then click **Add**.

5 Under **Add Banned IP Address Rule**, do one of the following:

- Select **Single IP Address**, and then enter the IP address.
- Select **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** boxes.

6 Optionally, select **Rule expires in**, and enter the number of days to enforce the rule.

7 Optionally, type a description for the rule.

8 Click **OK**.

9 On the **Trusted and Banned IPs** dialog, click **Yes** to confirm.

Edit a banned computer connection

You can edit a banned computer connection and its associated IP address.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Trusted and Banned IPs**.
4. On the Trusted and Banned IPs pane, select **Banned IP Addresses**, and then click **Edit**.
5. Under **Edit Banned IP Address**, do one of the following:
   - Select **Single IP Address**, and then enter the IP address.
   - Select **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** boxes.
6. Optionally, select **Rule expires in**, and enter the number of days to enforce the rule.
7. Optionally, type a description for the rule.
8. Click **OK**.

Remove a banned computer connection

You can remove a banned computer connection and its associated IP address.

1. On the McAfee SecurityCenter pane, click **Internet & Network**, then click **Configure**.
2. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
3. On the Firewall pane, click **Trusted and Banned IPs**.
4. On the Trusted and Banned IPs pane, select **Banned IP Addresses**.
5. Select an IP address, and then click **Remove**.
6. In the **Trusted and Banned IPs** dialog, click **Yes** to confirm.

Ban a computer from the Inbound Events log

You can ban a computer connection and its associated IP address from the Inbound Events log.

IP addresses which appear in the Inbound Events log are blocked. Therefore, banning an address adds no additional protection unless your computer either uses ports that are deliberately opened or includes a program that has been allowed access to the Internet.

Add an IP address to your **Banned IP Addresses** list only if you have one or more ports that are deliberately open and if you have reason to believe that you must block that address from accessing open ports.

You can use the Inbound Events page, which lists the IP addresses of all inbound Internet traffic, to ban an IP address that you suspect is the source of suspicious or undesirable Internet activity.

1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Advanced Menu**.
2. Click **Reports & Logs**.
3. Under **Recent Events**, click **View Log**.
4. Click **Internet & Network**, and then click **Inbound Events**.
5. Select a source IP address, and under **I want to**, click **Ban This Address**.
6. On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm.

Ban a computer from the Intrusion Detection Events log

You can ban a computer connection and its associated IP address from the Intrusion Detection Events log.

1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Advanced Menu**.
2. Click **Reports & Logs**.
3. Under **Recent Events**, click **View Log**.
4. Click **Internet & Network**, and then click **Intrusion Detection Events**.
5. Select a source IP address, and under **I want to**, click **Ban This Address**.
6. On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm.

CHAPTER 21

Logging, monitoring, and analysis

Firewall provides extensive and easy-to-read logging, monitoring, and analysis for Internet events and traffic. Understanding Internet traffic and events helps you manage your Internet connections.

In this chapter

Event Logging

Firewall allows you to enable or disable event logging and, when enabled, which event types to log. Event logging allows you to view recent inbound, outbound events and intrusion events.

Configure event log settings

You can specify and configure the types of Firewall events to log. By default, event logging is enabled for all events and activities.

1. On the Internet & Network Configuration pane, under **Firewall protection is enabled**, click **Advanced**.
2. On the Firewall pane, click **Event Log Settings**.
3. If it is not already selected, select **Enable Event Logging**.
4. Under **Enable Event Logging**, select or clear the event types that you want or do not want to log. Event types include the following:
   - Blocked Programs
   - ICMP Pings
   - Traffic from Banned IP Addresses
   - Events on System Service Ports
   - Events on Unknown Ports
   - Intrusion Detection (IDS) events
5. To prevent logging on specific ports, select **Do not log events on the following port(s)**, and then enter single port numbers separated by commas, or port ranges with dashes. For example, `137-139, 445, 400-5000`.
6. Click **OK**.

View recent events

If logging is enabled, you can view recent events. The Recent Events pane shows the date and description of the event. It displays activity for programs that have been explicitly blocked from accessing the Internet.

- On the **Advanced Menu**, under the Common Tasks pane, click **Reports & Logs** or **View Recent Events**. Alternatively, click **View Recent Events** under the Common Tasks pane from the Basic Menu.

View inbound events

If logging is enabled, you can view inbound events. Inbound Events include the date and time, source IP address, host name, and information and event type.

1 Ensure the Advanced menu is enabled. On the Common Tasks pane, click **Reports & Logs**.

2 Under **Recent Events**, click **View Log**.

3 Click **Internet & Network**, and then click **Inbound Events**.

Note: You can trust, ban, and trace an IP address from the Inbound Event log.

View outbound events

If logging is enabled, you can view outbound events. Outbound Events include the name of the program attempting outbound access, the date and time of the event, and the location of the program on your computer.

1 On the Common Tasks pane, click **Reports & Logs**.

2 Under **Recent Events**, click **View Log**.

3 Click **Internet & Network**, and then click **Outbound Events**.

Note: You can allow full and outbound-only access for a program from the Outbound Events log. You can also locate additional information about the program.

View intrusion detection events

If logging is enabled, you can view inbound intrusion events. Intrusion Detection events display the date and time, the source IP, the host name of the event, and the type of event.

1 On the Common Tasks pane, click **Reports & Logs**.

2 Under **Recent Events**, click **View Log**.

3 Click **Internet & Network**, and then click **Intrusion Detection Events**.

Note: You can ban and trace an IP address from the Intrusion Detection Events log.

Working with Statistics

Firewall leverages McAfee's HackerWatch security Web site to provide you with statistics about global Internet security events and port activity.

View global security event statistics

HackerWatch tracks worldwide Internet security events, which you can view from SecurityCenter. Information tracked lists incidents reported to HackerWatch in the last 24 hours, 7 days, and 30 days.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **HackerWatch**.
3. Under Event Tracking, view security event statistics.

View global Internet port activity

HackerWatch tracks worldwide Internet security events, which you can view from SecurityCenter. Information displayed includes the top event ports reported to HackerWatch during the past seven days. Typically, HTTP, TCP, and UDP port information is displayed.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **HackerWatch**.
3. View the top event port events under **Recent Port Activity**.

Tracing Internet traffic

Firewall offers a number of options for tracing Internet traffic. These options let you geographically trace a network computer, obtain domain and network information, and trace computers from the Inbound Events and Intrusion Detection Events logs.

Geographically trace a network computer

You can use Visual Tracer to geographically locate a computer that is connecting or attempting to connect to your computer, using its name or IP address. You can also access network and registration information using Visual Tracer. Running Visual Tracer displays a world map which displays the most probable route of data taken from the source computer to yours.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Visual Tracer**.
3. Type the computer's IP address, and click **Trace**.
4. Under **Visual Tracer**, select **Map View**.

Note: You cannot trace looped, private, or invalid IP address events.

Obtain computer registration information

You can obtain a computer's registration information from SecurityCenter using Visual Trace. Information includes the domain name, the registrant's name and address, and the administrative contact.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Visual Tracer**.
3. Type the computer's IP address, and then click **Trace**.
4. Under **Visual Tracer**, select **Registrant View**.

Obtain computer network information

You can obtain a computer's network information from SecurityCenter using Visual Trace. Network information includes details about the network on which the domain resides.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Visual Tracer**.
3. Type the computer's IP address, and then click **Trace**.
4. Under **Visual Tracer**, select **Network View**.

Trace a computer from the Inbound Events log

From the Inbound Events pane, you can trace an IP address that appears in the Inbound Events log.

1. Ensure the Advanced menu is enabled. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then click **Inbound Events**.
4. On the Inbound Events pane, select a source IP address, and then click **Trace this address**.
5. On the Visual Tracer pane, click one of the following:
   - **Map View**: Geographically locate a computer using the selected IP address.
   - **Registrant View**: Locate domain information using the selected IP address.
   - **Network View**: Locate network information using the selected IP address.
6. Click **Done**.

Trace a computer from the Intrusion Detection Events log

From the Intrusion Detection Events pane, you can trace an IP address that appears in the Intrusion Detection Events log.

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then click **Intrusion Detection Events**. On the Intrusion Detection Events pane, select a source IP address, and then click **Trace this address**.
4. On the Visual Tracer pane, click one of the following:
   - **Map View**: Geographically locate a computer using the selected IP address.
   - **Registrant View**: Locate domain information using the selected IP address.
   - **Network View**: Locate network information using the selected IP address.
5. Click **Done**.

Trace a monitored IP address

You can trace a monitored IP address to obtain a geographical view which shows the most probable route of data taken from the source computer to yours. In addition, you can obtain registration and network information about the IP address.

1 Ensure that the Advanced Menu is enabled and click **Tools**.

2 On the Tools pane, click **Traffic Monitor**.

3 Under **Traffic Monitor**, click **Active Programs**.

4 Select a program and then the IP address that appears below the program name.

5 Under **Program Activity**, click **Trace This IP**.

6 Under **Visual Tracer**, you can view a map which shows the most probable route of data taken from the source computer to yours. In addition, you can obtain registration and network information about the IP address.

Note: To view the most up-to-date statistics, click **Refresh** under **Visual Tracer**.

Monitoring Internet traffic

Firewall provides a number of methods to monitor your Internet traffic, including the following:

- **Traffic Analysis graph**: Displays recent inbound and outbound Internet traffic.
- **Traffic Usage graph**: Displays the percentage of bandwidth used by the most active programs during the past 24 hour period.
- **Active Programs**: Displays those programs that currently use the most network connections on your computer and the IP addresses the programs access.

About the Traffic Analysis graph

The Traffic Analysis graph is a numerical and graphical representation of inbound and outbound Internet traffic. In addition, the Traffic Monitor displays programs using the greatest number of network connections on your computer and the IP addresses that the programs access.

From the Traffic Analysis pane, you can view recent inbound and outbound Internet traffic, current, average, and maximum transfer rates. You can also view traffic volume, including the amount of traffic since you started Firewall, and the total traffic for the current and previous months.

The Traffic Analysis pane displays real-time Internet activity on your computer, including the volume and rate of recent inbound and outbound Internet traffic on your computer, connection speed, and total bytes transferred across the Internet.

The solid green line represents the current rate of transfer for incoming traffic. The dotted green line represents the average rate of transfer for incoming traffic. If the current rate of transfer and the average rate of transfer are the same, the dotted line does not appear on the graph. The solid line represents both the average and current rates of transfer.

The solid red line represents the current rate of transfer for outgoing traffic. The red dotted line represents the average rate of transfer for outgoing traffic. If the current rate of transfer and the average rate of transfer are the same, the dotted line does not appear on the graph. The solid line represents both the average and current rates of transfer.

Analyze inbound and outbound traffic

The Traffic Analysis graph is a numerical and graphical representation of inbound and outbound Internet traffic. In addition, the Traffic Monitor displays programs using the greatest number of network connections on your computer and the IP addresses that the programs access.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Traffic Analysis**.

Tip: To view the most up-to-date statistics, click **Refresh** under **Traffic Analysis**.

Monitor program bandwidth

You can view the pie chart, which displays the approximate percentage of bandwidth used by the most active programs on your computer during the past twenty-four hour period. The pie chart provides visual representation of the relative amounts of bandwidth used by the programs.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Traffic Usage**.

Tip: To view the most up-to-date statistics, click **Refresh** under **Traffic Usage**.

Monitor program activity

You can view inbound and outbound program activity, which displays remote computer connections and ports.

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Active Programs**.
4. You can view the following information:
   - Program Activity graph: Select a program to display a graph of its activity.
   - Listening connection: Select a Listening item under the program name.
   - Computer connection: Select an IP address under the program name, system process, or service.

Note: To view the most up-to-date statistics, click **Refresh** under **Active Programs**.

CHAPTER 22

Learning about Internet security

Firewall leverages McAfee's security Web site, HackerWatch, to provide up-to-date information about programs and global Internet activity. HackerWatch also provides an HTML tutorial about Firewall.

In this chapter

Launch the HackerWatch tutorial

To learn about Firewall, you can access the HackerWatch tutorial from SecurityCenter.

1 Ensure that the Advanced Menu is enabled, and then click **Tools**.

2 On the Tools pane, click **HackerWatch**.

3 Under **HackerWatch Resources**, click **View Tutorial**.

CHAPTER 23

McAfee QuickClean

QuickClean improves your computer's performance by deleting files that can create clutter on your computer. It empties your Recycle Bin and deletes temporary files, shortcuts, lost file fragments, registry files, cached files, cookies, browser history files, sent and deleted e-mail, recently used files, Active-X files, and system restore point files. QuickClean also protects your privacy by using the McAfee Shredder component to securely and permanently delete items that may contain sensitive, personal information, such as your name and address. For information about shredding files, see McAfee Shredder.

Disk Defragmenter arranges files and folders on your computer to ensure that they do not become scattered (that is, fragmented) when saved on your computer's hard drive. By defragmenting your hard drive periodically, you ensure that these fragmented files and folders are consolidated for quick retrieval later.

If you do not want to maintain your computer manually, you can schedule both QuickClean and Disk Defragmenter to run automatically, as independent tasks, at any frequency.

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

QuickClean features

QuickClean provides various cleaners that delete unnecessary files safely and efficiently. By deleting these files, you increase the space on your computer's hard drive and improve its performance.

Cleaning your computer

QuickClean deletes files that can create clutter on your computer. It empties your Recycle Bin and deletes temporary files, shortcuts, lost file fragments, registry files, cached files, cookies, browser history files, sent and deleted e-mail, recently-used files, Active-X files, and system restore point files. QuickClean deletes these items without affecting other essential information.

You can use any of QuickClean's cleaners to delete unnecessary files from your computer. The following table describes the QuickClean cleaners:

Name	Function
Recycle Bin Cleaner	Deletes files in the Recycle Bin.
Temporary Files Cleaner	Deletes files stored in temporary folders.
Shortcut Cleaner	Deletes broken shortcuts and shortcuts that do not have a program associated with them.
Lost File Fragment Cleaner	Deletes lost file fragments on your computer.
Registry Cleaner	Deletes Windows® registry information for programs that no longer exist on your computer. The registry is a database in which Windows stores its configuration information. The registry contains profiles for each computer user and information about system hardware, installed programs, and property settings. Windows continually references this information during its operation.
Cache Cleaner	Deletes cached files that accumulate as you browse Web pages. These files are usually stored as temporary files in a cache folder. A cache folder is a temporary storage area on your computer. To increase Web browsing speed and efficiency, your browser can retrieve a Web page from its cache (rather than from a remote server) the next time you want to view it.

Name	Function
Cookie Cleaner	Deletes cookies. These files are usually stored as temporary files. A cookie is a small file containing information, usually including a user name and the current date and time, stored on the computer of a person browsing the Web. Cookies are primarily used by Web sites to identify users who have previously registered on or visited the site; however, they can also be a source of information for hackers.
Browser History Cleaner	Deletes your Web browser history.
Outlook Express and Outlook E-mail Cleaner (sent and deleted items)	Deletes sent and deleted e-mail from Outlook® and Outlook Express.
Recently Used Cleaner	Deletes recently used files that have been created with any of these programs: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX Cleaner	Deletes ActiveX controls. ActiveX is a software component used by programs or Web pages to add functionality that blends in and appears as a normal part of the program or Web page. Most ActiveX controls are harmless; however, some may capture information from your computer.
System Restore Point Cleaner	Deletes old system restore points (except the most recent one) from your computer. System restore points are created by Windows to mark any changes made to your computer so that you can revert to a previous state if any problems occur.

Clean your computer

You can use any of QuickClean's cleaners to delete unnecessary files from your computer. When finished, under **QuickClean Summary**, you can view the amount of disk space reclaimed after cleanup, the number of files that were deleted, and the date and time when the last QuickClean operation ran on your computer.

1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Maintain Computer**.
2. Under **McAfee QuickClean**, click **Start**.
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.** If you select the Recently Used Cleaner, you can click **Properties** to select or clear the files that have been recently created with the programs in the list, and then click **OK**.
   - Click **Restore Defaults** to restore the default cleaners, and then click **Next.**
4. After the analysis is performed, click **Next**.
5. Click **Next** to confirm the file deletion.
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**, specify the number of passes, up to 10, and then click **Next**. Shredding files can be a lengthy process if there is a large amount of information being erased.
7. If any files or items were locked during cleanup, you may be prompted to restart your computer. Click **OK** to close the prompt.
8. Click **Finish**.

Note: Files deleted with Shredder cannot be recovered. For information about shredding files, see McAfee Shredder.

Defragmenting your computer

Disk Defragmenter arranges files and folders on your computer so that they do not become scattered (that is, fragmented) when saved on your computer's hard drive. By defragmenting your hard drive periodically, you ensure that these fragmented files and folders are consolidated for quick retrieval later.

Defragment your computer

You can defragment your computer to improve file and folder access and retrieval.

1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Maintain Computer**.
2. Under **Disk Defragmenter**, click **Analyze**.
3. Follow the on-screen instructions.

Note: For more information about Disk Defragmenter, see the Windows Help.

Scheduling a task

Task Scheduler automates the frequency with which QuickClean or Disk Defragmenter runs on your computer. For example, you can schedule a QuickClean task to empty your Recycle Bin every Sunday at 9:00 P.M. or a Disk Defragmenter task to defragment your computer's hard drive on the last day of every month. You can create, modify, or delete a task at any time. You must be logged in to your computer for a scheduled task to run. If a task does not run for any reason, it will be rescheduled five minutes after you log in again.

Schedule a QuickClean task

You can schedule a QuickClean task to automatically clean your computer using one or more cleaners. When finished, under **QuickClean Summary**, you can view the date and time when your task is scheduled to run again.

1 Open the Task Scheduler pane.

  How?

  1. On the McAfee SecurityCenter, under **Common Tasks**, click **Maintain Computer**.
  2. Under **Task Scheduler**, click **Start**.

2 In the **Select operation to schedule** list, click **McAfee QuickClean**.

3 Type a name for your task in the **Task name** box, and then click **Create.**

4 Do one of the following:

- Click **Next** to accept the cleaners in the list.
- Select or clear the appropriate cleaners, and then click **Next**. If you select the Recently Used Cleaner, you can click **Properties** to select or clear the files that have been recently created with the programs in the list, and then click **OK**.
- Click **Restore Defaults** to restore the default cleaners, and then click **Next**.

5 Do one of the following:

- Click **Schedule** 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**, specify the number of passes, up to 10, and then click **Schedule**.

6 In the **Schedule** dialog box, select the frequency with which you want the task to run, and then click **OK**.

7 If you made changes to the Recently Used Cleaner properties, you may be prompted to restart your computer. Click **OK** to close the prompt.

8 Click **Finish**.

Note: Files deleted with Shredder cannot be recovered. For information about shredding files, see McAfee Shredder.

Modify a QuickClean task

You can modify a scheduled QuickClean task to change the cleaners it uses or the frequency with which it automatically runs on your computer. When finished, under **QuickClean Summary**, you can view the date and time when your task is scheduled to run again.

1 Open the Task Scheduler pane.

   How?

   1. On the McAfee SecurityCenter, under **Common Tasks**, click **Maintain Computer**.
   2. Under **Task Scheduler**, click **Start**.

2 In the **Select operation to schedule** list, click **McAfee QuickClean**.

3 Select the task in the **Select an existing task** list, and then click **Modify**.

4 Do one of the following:

   - Click **Next** to accept the cleaners selected for the task.
   - Select or clear the appropriate cleaners, and then click **Next**. If you select the Recently Used Cleaner, you can click **Properties** to select or clear the files that have been recently created with the programs in the list, and then click **OK**.
   - Click **Restore Defaults** to restore the default cleaners, and then click **Next.**

5 Do one of the following:

   - Click **Schedule** 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, up to 10, and then click **Schedule**.

6 In the **Schedule** dialog box, select the frequency with which you want the task to run, and then click **OK**.

7 If you made changes to the Recently Used Cleaner properties, you may be prompted to restart your computer. Click **OK** to close the prompt.

8 Click **Finish**.

Note: Files deleted with Shredder cannot be recovered. For information about shredding files, see McAfee Shredder.

Delete a QuickClean task

You can delete a scheduled QuickClean task if you no longer want it to run automatically.

1 Open the Task Scheduler pane.

How?

1. On the McAfee SecurityCenter, under **Common Tasks**, click **Maintain Computer**.
2. Under **Task Scheduler**, click **Start**.

2 In the **Select operation to schedule** list, click **McAfee QuickClean**.

3 Select the task in the **Select an existing task** list.

4 Click **Delete**, and then click **Yes** to confirm the deletion.

5 Click **Finish**.

Schedule a Disk Defragmenter task

You can schedule a Disk Defragmenter task to schedule the frequency with which your computer's hard drive is automatically defragmented. When finished, under **Disk Defragmenter**, you can view the date and time when your task is scheduled to run again.

1 Open the Task Scheduler pane.

How?

1. On the McAfee SecurityCenter, under **Common Tasks**, click **Maintain Computer**.
2. Under **Task Scheduler**, click **Start**.

2 In the **Select operation to schedule** list, click **Disk Defragmenter**.

3 Type a name for your task in the **Task name** box, and then click **Create**.

4 Do one of the following:

- Click **Schedule** to accept the default **Perform defragmentation even if the free space is low** option.
- Clear the **Perform defragmentation even if the free space is low** option, and then click **Schedule.**

5 In the **Schedule** dialog box, select the frequency with which you want the task to run, and then click **OK**.

6 Click **Finish**.

Modify a Disk Defragmenter task

You can modify a scheduled Disk Defragmenter task to change the frequency with which it automatically runs on your computer. When finished, under **Disk Defragmenter**, you can view the date and time when your task is scheduled to run again.

1 Open the Task Scheduler pane.

How?

1. On the McAfee SecurityCenter, under **Common Tasks**, click **Maintain Computer**.
2. Under **Task Scheduler**, click **Start**.

2 In the **Select operation to schedule** list, click **Disk Defragmenter**.

3 Select the task in the **Select an existing task** list, and then click **Modify**.

4 Do one of the following:

- Click **Schedule** to accept the default **Perform defragmentation even if the free space is low** option.
- Clear the **Perform defragmentation even if the free space is low** option, and then click **Schedule.**

5 In the **Schedule** dialog box, select the frequency with which you want the task to run, and then click **OK**.

6 Click **Finish**.

Delete a Disk Defragmenter task

You can delete a scheduled Disk Defragmenter task if you no longer want it to run automatically.

1 Open the Task Scheduler pane.

How?

1. On the McAfee SecurityCenter, under **Common Tasks**, click **Maintain Computer**.
2. Under **Task Scheduler**, click **Start**.

2 In the **Select operation to schedule** list, click **Disk Defragmenter**.

3 Select the task in the **Select an existing task** list.

4 Click **Delete**, and then click **Yes** to confirm the deletion.

5 Click **Finish**.

CHAPTER 24

McAfee Shredder

McAfee Shredder deletes (or shreds) items permanently from your computer's hard drive. Even when you manually delete files and folders, empty your Recycle Bin, or delete your Temporary Internet Files folder, you can still recover this information using computer forensic tools. As well, a deleted file can be recovered because some programs make temporary, hidden copies of open files. Shredder protects your privacy by safely and permanently deleting these unwanted files. It's important to remember that shredded files cannot be restored.

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

Shredder features

Shredder deletes items from your computer's hard drive so that their associated information cannot be recovered. It protects your privacy by safely and permanently deleting files and folders, items in your Recycle Bin and Temporary Internet Files folder, and the entire contents of computer disks, such as rewriteable CDs, external hard drives, and floppy disks.

Shredding files, folders, and disks

Shredder ensures that the information contained in deleted files and folders in your Recycle Bin and in your Temporary Internet Files folder cannot be recovered, even with special tools. With Shredder, you can specify how many times (up to 10) you want an item to be shredded. A higher number of shredding passes increases your level of secure file deletion.

Shred files and folders

You can shred files and folders from your computer's hard drive, including items in your Recycle Bin and in your Temporary Internet Files folder.

1 Open **Shredder**.

   How?

   1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Advanced Menu**.
   2. On the left pane, click **Tools**.
   3. Click **Shredder**.

2 On the Shred files and folders pane, under **I want to**, click **Erase files and folders**.

3 Under **Shredding Level**, click one of the following shredding levels:

   - **Quick**: Shreds the selected item(s) once.
   - **Comprehensive**: Shreds the selected item(s) 7 times.
   - **Custom**: Shreds the selected item(s) up to 10 times.

4 Click **Next**.

5 Do one of the following:

   - In the **Select file(s) to shred** list, click either **Recycle Bin contents** or **Temporary Internet files**.
   - Click **Browse**, navigate to the file that you want to shred, select it, and then click **Open**.

6 Click **Next**.

7 Click **Start**.

8 When Shredder finishes, click **Done**.

Note: Do not work with any files until Shredder has completed the task.

Shred an entire disk

You can shred the entire contents of a disk at once. Only removable drives, such as external hard drives, writeable CDs, and floppy disks can be shredded.

1 Open **Shredder**.

   How?

   1. On the McAfee SecurityCenter pane, under **Common Tasks**, click **Advanced Menu**.
   2. On the left pane, click **Tools**.
   3. Click **Shredder**.

2 On the Shred files and folders pane, under **I want to**, click **Erase an entire disk**.

3 Under **Shredding Level**, click one of the following shredding levels:

   - **Quick**: Shreds the selected drive once.
   - **Comprehensive**: Shreds the selected drive 7 times.
   - **Custom**: Shreds the selected drive up to 10 times.

4 Click **Next**.

5 In the **Select the disk** list, click the drive that you want to shred.

6 Click **Next**, and then click **Yes** to confirm.

7 Click **Start**.

8 When Shredder finishes, click **Done**.

Note: Do not work with any files until Shredder has completed the task.

CHAPTER 25

McAfee Network Manager

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 remotely fix reported security vulnerabilities on those computers.

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

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

Network Manager features

Network Manager provides the following features.

Graphical network map

Network Manager's network map provides a graphical overview of the protection status of the computers and components that make up your home network. When you make changes to your network (for example, you add 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 for any of the components on the network map.

Remote management

Use Network Manager’s network map to manage the protection 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
M	Represents an online, managed computer
M	Represents an offline, managed computer
M	Represents an unmanaged computer that has SecurityCenter installed
M	Represents an offline, unmanaged computer
?	Represents an online computer that does not have SecurityCenter installed, or an unknown network device
?	Represents an offline computer that does not have SecurityCenter installed, or an offline, unknown network device
✓	Signifies that the corresponding item is protected and connected
!	Signifies that the corresponding item may require your attention
✗	Signifies that the corresponding item requires your immediate attention
	Represents a wireless home router
	Represents a standard home router
	Represents the Internet, when connected
	Represents the Internet, when disconnected

CHAPTER 26

Setting up a managed network

To set up a managed network, work with the items on your network map and add members (computers) to the network. Before a computer can be remotely managed, or 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 administrative permissions.

You can view the details associated with any of the components that appear on the network map, even after you make changes to your network (for example, you add a computer).

In this chapter

Working with the network map

When you connect a computer to the network, Network Manager analyzes the network to determine if there are any managed or unmanaged members, what the router attributes are, 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 makes the computer a managed member with administrative permissions. By default, the name of the network includes the workgroup or domain name of the first computer that connects to the network and has SecurityCenter installed; however, you can rename the network at any time.

When you make changes to your network (for example, you add 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 that appear on the network map.

Access the network map

The network map provides a graphical representation of the computers and components that make up your home network.

- On the Basic or Advanced Menu, click **Manage Network**.

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

Refresh the network map

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

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

Note: The **Refresh the network map** link is only available if there are no items selected on the network map. To clear 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 and has SecurityCenter installed. If you prefer to use a different name, you can change it.

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

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

Show or hide an item on the network map

By default, all the computers and components in your home network appear on the network map. However, if you have hidden items, you can show them again at any time. Only unmanaged 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 details for an item

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

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 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 administrative permissions. To ensure that only trusted computers join the network, users at 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 that want to access other network features (for example, send files or share printers).

Note: After you join, if you have other McAfee networking programs installed (for example, 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 accept it or reject it. 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 a computer's virus protection services are up-to-date).

1. In the Managed Network dialog box, ensure that the **Allow every computer on this network to monitor security settings** check box is selected.
2. Click **Join**.
   When you accept the invitation, two playing cards appear.
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 **OK**.

Note: If the computer that invited you to join the managed network does not display the same playing cards that appear in the security confirmation dialog box, there has been a security breach on the managed network. Joining the network can place your computer at risk; therefore, click **Cancel** in the Managed Network 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 administrative permissions on the network can invite other computers to join. When you send the invitation, you also specify the permission level you want to assign to the joining computer.

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 the managed network dialog box, do one of the following:
   - Click **Allow guest access to managed network programs** to allow the computer access to the network (you can use this option for temporary users in your home).
   - Click **Allow full access to managed network programs** to allow the computer access to the network.
   - Click **Allow administrative access to managed network programs** to allow the computer access to the network with administrative permissions. It also allows the computer to grant access to other computers that want to join the managed network.

4 Click **OK**.
An invitation to join the managed network is sent to the computer. When the computer accepts the invitation, two playing cards appear.

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 you invited to join the managed network does not display the same playing cards that appear in the security confirmation dialog box, there has been a security breach on the managed network. Allowing the computer to join the network can place other computers at risk; therefore, click **Reject Access** in the security confirmation dialog box.

Stop trusting computers on the network

If you trusted other computers on the network by mistake, you can stop trusting them.

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

Note: The **Stop trusting computers on this network** link is not available if you have administrative permissions and there are other managed computers on the network.

CHAPTER 27

Managing the network remotely

After you set up your managed network, you can 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 most security vulnerabilities remotely.

In this chapter

Monitoring status and permissions

A managed network has managed 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 that want to access other network features (for example, send files or share printers). 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 administrative, full, or guest permissions. Administrative permissions allow the managed computer to manage the protection status of all other managed computers on the network and 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.

Since a managed network can also have devices (for example, routers), you can use Network Manager to manage them. 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 (the computer is not a member, or is an unmanaged member), you can request to monitor it.

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 network; however, the computer then becomes unmanaged and you cannot monitor its protection status remotely.

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 change a managed computer's permissions at any time. This allows you to modify which computers can monitor the protection status of other computers on the network.

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 Network Manager.

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.

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 **Standard Router** if it is not a wireless router, or **Wireless Router** if it is wireless.
5. Click **OK**.

Fixing security vulnerabilities

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

When you fix security vulnerabilities remotely, Network Manager repairs most reported issues. However, some security vulnerabilities may require manual intervention on the local computer. In this case, Network Manager fixes the 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 resolution is to install the latest version of SecurityCenter on the remote computer or computers on your network.

Fix security vulnerabilities

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

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 open 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 using the latest version of SecurityCenter, their protection status cannot be monitored remotely. If you want to monitor these computers remotely, you must go to each computer, and install the latest version of SecurityCenter.

1. On the computer that you want to install your security software, open SecurityCenter.
2. Under **Common Tasks,** click **My Account**.
3. Log in using the e-mail address and password that you used to register your security software the first time you installed it.
4. Select the appropriate product, click the **Download/Install** icon, and then follow the on-screen instructions.

CHAPTER 28

McAfee EasyNetwork

EasyNetwork allows you to share files securely, simplify file transfers, and share printers among the computers in your home network. However, the computers in your network must have EasyNetwork installed to access its features.

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

Note: SecurityCenter reports critical and non-critical protection problems as soon as it detects them. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician.

In this chapter

EasyNetwork features

EasyNetwork provides the following features.

File sharing

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

File transfer

You can send files to other computers that have full or administrative access to your managed network (members). When you receive a file, it appears in your EasyNetwork inbox. The inbox is a temporary storage location for all the files other computers on the network send to you.

Automated printer sharing

After you join a managed network, you can share any local printers attached to your computer with other members, 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 29

Setting up EasyNetwork

Before you can use EasyNetwork, you must open it and join a managed network. After you join a managed network, you can share, search for, and send files to other computers on the network. You can also share printers. If you decide to leave the network, you can do so at any time.

In this chapter

Open EasyNetwork

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

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

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

Joining a managed network

If no computers on the network you are connected to have SecurityCenter, you are 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, it sends a join request to the other computers 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 that joins the network; for example, guest (file transfer only) or full/administrative (file transfer and file sharing). In EasyNetwork, computers with administrative access can grant access to other computers and manage permissions (promote or demote computers); computers with full access cannot perform these administrative tasks.

Note: After you join, if you have other McAfee networking programs installed (for example, Network Manager), the computer is also recognized as a managed computer in those programs. The permission level that is assigned to a computer in EasyNetwork 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 appears asking whether to join the managed network. If the computer agrees to join, a request is sent to all the 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. The first computer on the network is automatically granted administrative permissions.

1. In the Shared Files window, click **Join this network**.
   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 **OK**; otherwise, click **Cancel**.
3. Confirm that the granting computer displays the playing cards that appear in the security confirmation dialog box, and then click **OK**.

Note: If the computer that invited you to join the managed network does not display the same playing cards that appear in the security confirmation dialog box, there has been a security breach on the managed network. Joining the network can place your computer at risk; therefore, click **Cancel** 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 that have administrative access. The first computer that responds becomes the grantor. As the grantor, you are responsible for deciding which type of access to grant the computer: guest, full, or administrative.

1. In the alert, click the appropriate access level.
2. In the Invite a computer to join the managed network dialog box, do one of the following:
   - Click **Allow guest access to managed network programs** to allow the computer access to the network (you can use this option for temporary users in your home).
   - Click **Allow full access to managed network programs** to allow the computer access to the network.

- Click **Allow administrative access to managed network programs** to allow the computer access to the network with administrative permissions. It also allows the computer to grant access to other computers that want to join the managed network.

3 Click **OK**.

4 Confirm that the computer is displaying the playing cards that appear in the security confirmation dialog box, and then click **Grant Access**.

Note: If the computer does not display the same playing cards that appear in the security confirmation dialog box, there has been a security breach on the managed network. Granting this computer access to the network can place your computer at risk; therefore, click **Reject Access** in the security confirmation dialog box.

Rename the network

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

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 but then decide that you do not want to be a member, you can leave the network. After you leave the managed network, you can always rejoin; however, you must be granted permission again. For more information about joining, see Joining a managed network (page 154).

Leave a managed network

You can leave a managed network that you previously joined.

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 30

Sharing and sending files

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

Note: If you are sharing a large number of files, your computer resources may be affected.

In this chapter

Sharing files

Only computers that are members of the managed network (full or administrative access) can share 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 removed from the Shared Files window. You can stop sharing a file at any time.

To access a shared file, open the file directly from EasyNetwork or copy it to your computer, and then open it from there. If your list of shared files is large and it's difficult to see where the file is, you can search for it.

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

Share a file

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

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 if you click **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 it, 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 cannot access it.

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 **OK**.

Copy a shared file

You copy a shared file so that you still have it when it's not shared any more. You can copy a shared file from any computer on your managed network.

- 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 if you select the file in EasyNetwork, and then click **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 displays the corresponding results in the Shared Files window.

1. In the Shared Files window, click **Search**.
2. Click the appropriate option (page 161) in the **Contains** list.
3. Type part or all of the file name or path in the **File or Path Name** list.
4. Click the appropriate file type (page 161) in the **Type** list.
5. In the **From** and **To** lists, click the dates that represent the range of dates when the file was created.

Search criteria

The following tables describe the search criteria you can specify when searching for shared files.

Name of the file or path

Contains	Description
Contains all of the words	Search for a file or path name that contains all the words you specify in the **File or Path Name** list, in any order.
Contains any of the words	Search for a file or path name that contains any words you specify in the **File or Path Name** list.
Contains the exact string	Search for a file or path name that contains the exact phrase you specify in the **File or Path Name** list.

Type of file

Type	Description
Any	Search all shared file types.
Document	Search all shared documents.
Image	Search all shared image files.
Video	Search all shared video files.
Audio	Search all shared audio files.
Compressed	Search all compressed files (for example, .zip files).

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 the files that other computers on the network send you. 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 at the far right of your taskbar. If you do not want to receive notification messages (for example, they are interrupting what you're doing), you can turn this feature 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 (copy them to your computer).

Send a file to another computer

You can send a file 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 163).

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: To send multiple files to a computer, press CTRL when selecting the files. You can also send files if you click **Send** on the **Tools** menu, select the files, and then click **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 on your computer. If EasyNetwork is not running when a file is sent to your computer, you receive a notification message in the notification area at the far right of your taskbar. Click the notification message to open EasyNetwork and access the file.

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

Tip: You can also receive a file from another computer if you select the file in your EasyNetwork inbox, and then click **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 a notification message when another computer on the managed network sends you a file. If EasyNetwork is not running, the notification message appears in the notification area at the far right of your taskbar.

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

CHAPTER 31

Sharing printers

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

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 shares it on the network. You can also stop sharing a printer at any time.

In this chapter

Working with shared printers

EasyNetwork detects the printers that are shared by the computers on the network. If EasyNetwork detects a remote printer that is not connected to your computer, the **Available network printers** link appears in the Shared Files window when you open EasyNetwork for the first time. You can then install available printers or uninstall printers that are already connected to your computer. You can also refresh the list of printers to ensure that you are viewing up-to-date information.

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

Stop sharing a printer

When you stop sharing a printer, members cannot use it.

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

If you are a member of the managed network, you can access the printers that are shared; however, you must install the printer driver used by the printer. If the owner of the printer stops sharing their printer, you cannot use it.

1. On the **Tools** menu, click **Printers**.
2. In the Available Network Printers dialog box, click a printer name.
3. Click **Install**.

Reference

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

Glossary

8

802.11

A set of IEEE standards for transmitting data across a wireless network. 802.11 is commonly known as Wi-Fi.

802.11a

An extension to 802.11 that transmits 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 transmits data at up to 11 Mbps in the 2.4 GHz band. Although the transmission speed is slower than 802.11a, the distance covered is larger.

802.1x

An IEEE standard for authentication on wired and wireless networks. 802.1x is commonly used with 802.11 wireless networking.

A

Access Point

A network device (commonly called a wireless router) that plugs into an Ethernet hub or switch to extend the physical range of service for a wireless user. When wireless users roam with their mobile devices, transmission passes from one Access Point (AP) to another to maintain connectivity.

ActiveX control

A software component used by programs or Web pages to add functionality that appears as a normal part of the program or Web page. Most ActiveX controls are harmless; however, some may capture information from your computer.

archive

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

authentication

The process of identifying an individual, usually by a unique name and password.

B

back up

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

bandwidth

The amount of data that can be transmitted in a fixed amount of time.

blacklist

In anti-phishing, a list of Web sites that are considered fraudulent.

browser

A program used to view Web pages on the Internet. Popular Web browsers include Microsoft Internet Explorer and Mozilla Firefox.

brute-force attack

A method of decoding encrypted data, such as passwords, through exhaustive effort (brute force) rather than intellectual strategy. Brute force is considered an infallible, although time-consuming, attack method. Brute-force attacking is also called brute-force cracking.

buffer overflow

A condition that occurs when suspicious programs or processes try to store more data in a buffer (temporary storage area) on your computer than it can hold. Buffer overflows corrupt or overwrite data in adjacent buffers.

C

cache

A temporary storage area on your computer. For example, to increase Web browsing speed and efficiency, your browser can retrieve a Web page from its cache (rather than from a remote server) the next time you want to view it.

cipher text

Encrypted text. Cipher text is unreadable until it has been converted into plain text (that is, decrypted).

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 lets you send and receive e-mail.

compression

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

content-rating group

In Parental Controls, an age group to which a user belongs. Content is made available or blocked based on the content rating group to which a user belongs. Content rating groups include: Young Child, Child, Younger Teenager, Older Teenager, and Adult.

cookie

A small file containing information, usually including a user name and the current date and time, stored on the computer of a person browsing the Web. Cookies are primarily used by Web sites to identify users who have previously registered on or visited the site; however, they can also be a source of information for hackers.

D

DAT

(Data signature files) Files containing the definitions that are used when detecting viruses, Trojans, spyware, adware, and other potentially unwanted programs on your computer or USB drive.

deep watch location

A folder 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

A type of attack that slows or halts traffic on a network. A denial of service attack (DoS attack) occurs when a network is flooded with so many additional requests that regular traffic is slowed or completely interrupted. It does not usually result in the theft of information or other security vulnerabilities.

dialer

Software that helps you to establish an Internet connection. When used maliciously, dialers can redirect your Internet connections to someone other than your default Internet Service Provider (ISP), without informing you of additional cost.

dictionary attack

A type of brute-force attack that uses common words to try to discover a password.

DNS

(Domain Name System) A system that converts host names or domain names to IP addresses. On the Web, DNS is used to convert easily legible Web address (for example, www.myhostname.com) to IP addresses (for example, 111.2.3.44) so that the Web site can be retrieved. Without DNS, you would have to type the IP address itself into your Web browser.

DNS server

(Domain Name System server) A computer that returns the IP address associated with a host or domain name. See also DNS.

domain

A local subnetwork or a descriptor for sites on the Internet.

On a local area network (LAN), a domain is a subnetwork made up of client and server computers controlled by one security database. In this context, domains can improve performance. On the Internet, a domain is part of every Web address (for example, in www.abc.com, abc is the domain).

E

e-mail

(electronic mail) Messages sent and received electronically, across a computer network. See also Webmail.

e-mail client

A program that you run on your computer to send and receive e-mail (for example, Microsoft Outlook).

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. Encrypted data is also known as cipher text.

ESS

(Extended Service Set) A set of two or more networks that form a single subnetwork.

event

An action initiated either by the user, a device, or the computer itself which triggers a response. McAfee records events in its event log.

external hard drive

A hard drive that is stored outside of the computer.

F

file fragments

Remnants of a file scattered throughout a disk. File fragmentation occurs as files are added or deleted, and can slow your computer's performance.

firewall

A system (hardware, software, or both) designed to prevent unauthorized access to or from a private network. 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, which examines each message and blocks those that do not meet the specified security criteria.

full archive

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

H

home network

Two or more computers that are connected in a home so that they can share files and Internet access. See also LAN.

hotspot

A geographic boundary covered by a Wi-Fi (802.11) access point (AP). Users who enter a hotspot with a wireless laptop can connect to the Internet, provided that the hotspot is beaconing (that is, advertising its presence) and authentication is not required. Hotspots are often located in heavily populated areas such as airports.

I

image filtering

A Parental Controls option that blocks potentially inappropriate Web images from appearing.

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 computer network, usually inside an organization, that can only be accessed by authorized users.

IP address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255 (for example, 192.168.1.100).

IP spoofing

To forge 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.

K

key

A series of letters and 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.

L

LAN

(Local Area Network) A computer network that spans a relatively small area (for example, a single building). Computers on a LAN can communicate with each other and share resources such as printers and files.

launchpad

A U3 interface component that acts as a starting point for launching and managing U3 USB programs.

library

An online storage area for files that you have backed up and published. The Data Backup library is a Web site on the Internet, accessible to anyone with Internet access.

M

MAC address

(Media Access Control address) A unique serial number assigned to a physical device accessing the network.

man-in-the-middle attack

A method of intercepting and possibly modifying messages between two parties without either party knowing that their communication link has been breached.

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 protection status; unmanaged members do not.

MAPI

(Messaging Application Programming Interface) A 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.

message authentication code (MAC)

A security code used to encrypt messages that are transmitted between computers. The message is accepted if the computer recognizes the decrypted code as valid.

MSN

(Microsoft Network) A group of Web-based services offered by Microsoft Corporation, including a search engine, e-mail, instant messaging, and portal.

N

network

A collection of Access Points and their associated users, equivalent to an ESS.

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

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.

O

on-demand scan

A scan that is launched on demand (that is, when you launch the operation). Unlike real-time scanning, on-demand scans do not launch automatically.

online backup repository

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

P

Parental Controls

Settings that help regulate what your children can see and do while they browse the Web. To set up Parental Controls, you can enable or disable image filtering, choose a content rating group, and set Web browsing time limits.

password

A code (usually consisting of letters and numbers) you use to gain access to your computer, a program, or 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 an administrator) can access them.

PCI wireless adapter cards

(Peripheral Component Interconnect) A wireless adapter card that plugs into a PCI expansion slot inside the computer.

phishing

An Internet scam designed to obtain valuable information (such as credit card and social security numbers, user IDs, and passwords) from unknowing individuals for fraudulent use.

plain text

Text that is not encrypted. See also encryption.

plug-in

A small software program that works with a larger program to provide added functionality. For example, plug-ins permit a 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).

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.

POP3

(Post Office Protocol 3) An interface between an e-mail client program and the e-mail server. Most home users have a POP3 e-mail account, 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.

potentially unwanted program (PUP)

A program that gathers and transmits personal information without your permission (for example, spyware and adware).

PPPoE

(Point-to-Point Protocol Over Ethernet) A method of using the Point-to-Point Protocol (PPP) dial-up protocol with Ethernet as the transport.

protocol

A format (hardware or software) for transmitting data between two devices. Your computer or device must support the correct protocol if you want to communicate with other computers.

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 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. You can access published files by searching the Data Backup library.

Q

quarantine

To isolate. For example, in VirusScan, suspect files are detected and quarantined so that they cannot cause harm to your computer or files.

quick archive

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

R

RADIUS

(Remote Access Dial-In User Service) A protocol that allows user authentication, usually in the context of remote access. Originally defined for use with dial-in remote access servers, the RADIUS protocol is now used in a variety of authentication environments, including 802.1x authentication of a WLAN user's shared secret.

real-time scanning

To scan files and folders for viruses and other activity when they are accessed by you or your computer.

Recycle Bin

A simulated garbage can for deleted files and folders in Windows.

registry

A database in which Windows stores its configuration information. The registry contains profiles for each computer user and information about system hardware, installed programs, and property settings. Windows continually references this information during its operation.

restore

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

roaming

To move from one Access Point (AP) coverage area to another without interruption in service or loss in connectivity.

rogue access point

An unauthorized Access Point. Rogue access points can be installed on a secure company network to grant network access to unauthorized parties. They can also be created to allow an attacker to conduct a man-in-the-middle attack.

rootkit

A collection of tools (programs) that grant a user administrator-level access to a computer or computer network. Rootkits may include spyware and other potentially unwanted programs that can create additional security or privacy risks to your computer data and personal information.

router

A network device that forwards data packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it based on any combination of source and destination address as well as current traffic conditions (for example, load, line costs, and bad lines). A router is sometimes called an Access Point (AP).

S

script

A list of commands that can be executed automatically (that is, without user interaction). Unlike programs, scripts are typically stored in their plain text form and compiled each time they are run. Macros and batch files are also called scripts.

server

A computer or program that accepts connections from other computers or programs and returns appropriate responses. For example, your e-mail program connects to an e-mail server each time you send or receive e-mail messages.

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

To allow 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

A string or key (usually a password) that has been shared between two communicating parties prior to initiating communication. A shared secret is used to protect sensitive portions of RADIUS messages.

shortcut

A file that contains only the location of another file on your computer.

smart drive

See USB drive.

SMTP

(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) A token (secret key) that identifies a Wi-Fi (802.11) network. The SSID is set up by the network administrator and must be supplied by users who want to join the network.

SSL

(Secure Sockets Layer) A protocol developed by Netscape for transmitting private documents on the Internet. SSL works by using a public key to encrypt data which is transferred over the SSL connection. URLs that require an SSL connection start with https instead of http.

standard e-mail account

See POP3.

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.

system restore point

A snapshot (image) of the contents of the computer's memory or a database. Windows creates restore points periodically and at the time of significant system events (such as when a program or driver is installed). You can also create and name your own restore points at any time.

SystemGuard

McAfee alerts that detect unauthorized changes to your computer and notify you when they occur.

T

temporary file

A file, created in memory or on disk, by the operating system or some other program, to be used during a session and then discarded.

TKIP

(Temporal Key Integrity Protocol) A protocol that addresses the 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'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.

Trojan

A program that appears legitimate but can damage valuable files, disrupt performance, and allow unauthorized access to your computer.

trusted list

Contains items that you trusted and are not being detected. If you trust an item (for example, a potentially unwanted program or a registry change) by mistake, or you want the item to be detected again, you must remove it from this list.

U

U3

(You: Simplified, Smarter, Mobile) A platform for running Windows 2000 or Windows XP programs directly from a USB drive. The U3 initiative was founded in 2004 by M-Systems and SanDisk and allows users to run U3 programs on a Windows computer without installing or storing data or settings on the computer.

URL

(Uniform Resource Locator) The standard format for Internet addresses.

USB

(Universal Serial Bus) A standardized serial computer interface that allows you to attach peripheral devices such as keyboards, joysticks, and printers to your computer.

USB drive

A small memory drive that plugs into a computer's USB port. A USB drive acts like a small disk drive, making it easy to transfer files from one computer to another.

USB wireless adapter card

A wireless adapter card that plugs into a USB slot in the computer.

V

virus

Self-replicating programs that might alter your files or data. They often appear to be from a trusted sender or to contain benign content.

VPN

(Virtual Private Network) A private network configured within a public network so as to take advantage of the management facilities of the public network. VPNs are used by enterprises to create wide area networks (WANs) that span large geographic areas, to provide site-to-site connections to branch offices, or to allow mobile users to dial into their company LANs.

W

wardriver

A person who searches for Wi-Fi (802.11) networks by driving through cities armed with a Wi-Fi computer and some special hardware or software.

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.

Webmail

Messages sent and received electronically, across the Internet. See also e-mail.

WEP

(Wired Equivalent Privacy) An encryption and authentication protocol defined as part of the Wi-Fi (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 users are allowed to access because the Web sites are not considered fraudulent.

Wi-Fi

(Wireless Fidelity) A term used by the Wi-Fi Alliance when referring to any type of 802.11 network.

Wi-Fi Alliance

An organization comprised of leading wireless hardware and software providers. The Wi-Fi Alliance strives to certify all 802.11-based products for interoperability and promote 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 the growth of the industry.

Wi-Fi Certified

To be tested and approved by the Wi-Fi Alliance. Wi-Fi Certified products are deemed interoperable even though they may originate 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.

wireless adapter

A device that adds wireless capability to a computer or PDA. It is attached via a USB port, PC Card (CardBus) slot, memory card slot, or internally into the PCI bus.

WLAN

(Wireless Local Area Network) A local area network (LAN) using a wireless connection. A WLAN uses high-frequency radio waves rather than wires to allow computers to communicate with each other.

worm

A self-replicating virus that resides in active memory and can send copies of itself through e-mail. 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

An update to the WPA security standard, based on the 802.11i IEEE standard.

WPA2-PSK

A special WPA mode that 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 (for example, AES, TKIP) simultaneously, while older devices generally support only a single encryption mode at a time (that is, 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

License

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE, INC. OR THE PLACE OF PURCHASE FOR A FULL REFUND.

CHAPTER 32

Customer and Technical Support

SecurityCenter reports critical and non-critical protection problems as soon as it detects them. Critical protection problems require immediate action and compromise your protection status (changing the color to red). Non-critical protection problems do not require immediate action and may or may not compromise your protection status (depending on the type of problem). To achieve a green protection status, you must fix all critical problems and either fix or ignore all non-critical problems. If you need help diagnosing your protection problems, you can run McAfee Virtual Technician. For more information about McAfee Virtual Technician, see the McAfee Virtual Technician help.

If you purchased your security software from a partner or provider other than McAfee, open a Web browser, and go to www.mcafeehelp.com. Then, under Partner Links, select your partner or provider to access McAfee Virtual Technician.

Note: To install and run Virtual Technician, you must log in to your computer as a Windows Administrator. If you don't, Virtual Technician may not be able to resolve your issues. For information about logging in as a Windows Administrator, see the Windows Help. In Windows Vista™, you are prompted when you run Virtual Technician. When this happens, click **Accept**. The Virtual Technician does not work with Mozilla® Firefox.

In this chapter

Using McAfee Virtual Technician

Like a personal, technical support representative, Virtual Technician collects information about your SecurityCenter programs so that it can help resolve your computer's protection problems. When you run Virtual Technician, it checks to make sure your SecurityCenter programs are working correctly. If it discovers problems, Virtual Technician offers to fix them for you or provides you with more detailed information about them. When finished, Virtual Technician displays the results of its analysis and allows you to seek additional technical support from McAfee, if necessary.

To maintain the security and integrity of your computer and files, Virtual Technician does not collect personal, identifiable information.

Note: For more information about Virtual Technician, click the **Help** icon in Virtual Technician.

Launch Virtual Technician

Virtual Technician collects information about your SecurityCenter programs so that it can help resolve your protection problems. To safeguard your privacy, this information does not include personal, identifiable information.

1 Under **Common Tasks**, click **McAfee Virtual Technician**.

2 Follow the on-screen instructions to download and run Virtual Technician.

Support and Downloads

Consult the following tables for the McAfee Support and Download sites in your country, including User Guides.

Support and Downloads

Country	McAfee Support	McAfee Downloads
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brazil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (English)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (French)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp

China (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
China (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Czechoslovakia	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Denmark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
France	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Germany	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Great Britain	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italy	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexico	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norway	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Poland	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Spain	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Sweden	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turkey	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
United States	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection User Guides

Country	McAfee User Guides
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brazil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (English)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (French)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Czechoslovakia	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Denmark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Germany	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Great Britain	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Italy	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Netherlands	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Norway	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Poland	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf

Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Spain	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Sweden	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turkey	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
United States	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security User Guides

Country	McAfee User Guides
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brazil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (English)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (French)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Czechoslovakia	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Denmark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Germany	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Great Britain	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Italy	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf

Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Netherlands	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Norway	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Poland	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Spain	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Sweden	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turkey	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
United States	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus User Guides

Country	McAfee User Guides
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brazil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (English)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (French)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Czechoslovakia	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Denmark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf

France	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Germany	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Great Britain	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Italy	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Netherlands	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Norway	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Poland	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Spain	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Sweden	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turkey	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
United States	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan User Guides

Country	McAfee User Guides
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brazil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canada (English)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Canada (French)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf

China (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Czechoslovakia	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Denmark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
France	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Germany	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Great Britain	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Italy	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Netherlands	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Norway	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Poland	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Spain	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Sweden	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turkey	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
United States	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consult the following table for the McAfee Threat Center and Virus Information sites in your country.

Country	Security Headquarters	Virus Information
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brazil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (English)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (French)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
China (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Czechoslovakia	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Denmark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
France	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Germany	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Great Britain	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Italy	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexico	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Netherlands	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Norway	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo

Poland	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Spain	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Sweden	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turkey	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
United States	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consult the following table for the HackerWatch sites in your country.

Country	HackerWatch
Australia	www.hackerwatch.org
Brazil	www.hackerwatch.org/?lang=pt-br
Canada (English)	www.hackerwatch.org
Canada (French)	www.hackerwatch.org/?lang=fr-ca
China (chn)	www.hackerwatch.org/?lang=zh-cn
China (tw)	www.hackerwatch.org/?lang=zh-tw
Czechoslovakia	www.hackerwatch.org/?lang=cs
Denmark	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
France	www.hackerwatch.org/?lang=fr
Germany	www.hackerwatch.org/?lang=de
Great Britain	www.hackerwatch.org
Italy	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexico	www.hackerwatch.org/?lang=es-mx
Netherlands	www.hackerwatch.org/?lang=nl
Norway	www.hackerwatch.org/?lang=no
Poland	www.hackerwatch.org/?lang=pl

Portugal	www.hackerwatch.org/?lang=pt-pt
Spain	www.hackerwatch.org/?lang=es
Sweden	www.hackerwatch.org/?lang=sv
Turkey	www.hackerwatch.org/?lang=tr
United States	www.hackerwatch.org

Index