McAfee®

PC Protection Plus 2007

VirusScan Plus, Backup & Restore

User Guide

Contents

CHAPTER 1

Introduction

McAfee PC Protection Plus Suite protects your computer from viruses, spyware, and hackers. You can surf the Web and download files safely and confidently, knowing McAfee is always on, always updating, and always protecting you. McAfee's trusted computer protection also offers automated backup with a one-click way to restore your photos, music, videos and other important files. McAfee makes it easy to view your security status, scan for viruses and spyware, and ensure your products are up-to-date using the redesigned McAfee SecurityCenter. Plus, you will receive the latest McAfee software and updates with your subscription automatically.

PC Protection Plus includes the following programs:

- SecurityCenter
- VirusScan
- Personal Firewall
- Data Backup
- Network Manager
- EasyNetwork (3-user license only)
- SiteAdvisor

CHAPTER 2

McAfee SecurityCenter

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

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

In this chapter

Features

McAfee SecurityCenter provides the following new features and benefits:

Redesigned protection status

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

Continual updates and upgrades

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

Real-time alerting

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

Convenient protection

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

Performance Tools

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

Real online help

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

Safe surfing protection

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

CHAPTER 3

Using SecurityCenter

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

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

Header

Help

View the program help file.

Left column

Update

Update your product to ensure protection from the latest threats.

Scan

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

Common Tasks

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

Components Installed

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

Main pane

Protection Status

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

SecurityCenter Information

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

In this chapter

Understanding SecurityCenter icons

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

Open SecurityCenter and use additional features

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

To open SecurityCenter or use additional features:

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

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

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

Check your protection status

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

To check your protection status:

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

Check the status of your updates

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

To check the status of your updates:

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

Understanding the protection status

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

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

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

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

Am I Protected?

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

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

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

Understanding protection categories and types

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

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

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

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

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

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

Understanding Computer and Files protection

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

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

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

Open the Computer and Files configuration pane

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

To open the Computer and Files configuration pane:

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

Understanding Internet and Network protection

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

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

Open the Internet and Network configuration pane

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

To open the Internet and Network configuration pane:

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

Understanding E-mail and IM protection

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

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

Open the E-mail and IM configuration pane

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

To open the E-mail and IM configuration pane:

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

Understanding Parental Controls protection

The Parental Controls protection category consists of this protection type:

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

Open the Parental Controls configuration pane

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

To open the Parental Controls configuration pane:

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

Fixing protection problems

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

Fix protection problems automatically

Most protection problems can be resolved automatically.

To fix protection problems automatically:

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

Fix protection problems manually

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

To fix protection problems manually:

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

Viewing SecurityCenter information

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

Open the SecurityCenter configuration pane

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

To open the SecurityCenter configuration pane:

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

View installed product information

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

To view your McAfee product information:

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

Using the Advanced Menu

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

The Advanced Menu consists of the following items:

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

CHAPTER 4

Configuring SecurityCenter options

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

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

- Protection Status
- Users
- Automatic updates
- Alerts

In this chapter

Configuring the protection status

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

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

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

Configure ignored problems

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

To configure ignored problems:

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

Configuring user options

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

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

Switch to McAfee user accounts

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

To switch to McAfee user accounts:

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

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

Create an Administrator account

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

To create an Administrator account:

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

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

Configure user options

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

To configure user options:

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

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

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

Retrieve the Administrator password

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

To retrieve the Administrator password:

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

   Your forgotten Administrator password appears.

Change the Administrator password

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

To change the Administrator password:

1. Right-click the SecurityCenter M icon, and then click **Switch User**.
2. In the **User Name** list, select **Administrator**, and click **Change Password.**
3. Enter your existing password in the **Old Password** box.
4. Enter your new password in the **Password** box, and reenter it in the **Confirm Password** box.
5. Click **OK**.

Configuring update options

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

Check for updates automatically

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

To check for updates automatically:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to the **Automatic updates are enabled** status to expand its pane, and then click **Advanced**.
3. Select one of the following in the Update Options pane:
   - Install the updates automatically and notify me when the product is updated (recommended) (page 27)
   - Download the updates automatically and notify me when they are ready to be installed (page 28)
   - Notify me before downloading any updates (page 28)
4. Click **OK**.

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

Automatically download and install updates

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

Automatically download updates

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

To install an automatically downloaded update:

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

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

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

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

Notify before downloading updates

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

To download and install an update:

1. Select **Update my products now** on the alert, and then click **OK**.
2. If prompted, log in to the Web site.

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

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

Disable automatic updating

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

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

To disable automatic updating:

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

   The status is updated in the header.

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

Postpone updates

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

To postpone an update:

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

Check for updates manually

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

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

To check for updates manually:

1. Ensure that your computer is connected to the Internet.
2. Right-click the SecurityCenter M icon in your Windows notification area, at the far right of the taskbar, and then click **Updates**.

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

   For your convenience, an animated icon appears in your Windows notification area, at the far right of the taskbar. When SecurityCenter is finished, the icon automatically disappears.
3. If prompted, log in to the Web site to verify your subscription.

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

Configuring alert options

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

Configure alert options

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

To configure alert options:

1. Under **SecurityCenter Information**, click **Configure**.
2. Click the arrow next to **Alerts** to expand its pane, and then click **Advanced**.
3. Select one of the following in the Alert Options pane:
   - **Alert me when a public virus outbreak or security threat occurs**
   - **Show informational alerts when gaming mode is detected**
   - **Play a sound when an alert occurs**
   - **Show McAfee splash screen at Windows startup**
4. Click **OK**.

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

Configure informational alerts

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

To configure informational alerts:

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

CHAPTER 5

Performing common tasks

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

In this chapter

Perform common tasks

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

To perform common tasks:

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

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

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

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

View recent events

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

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

To view recent events:

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

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

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

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

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

Maintain your computer automatically

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

To maintain your computer automatically:

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

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

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

Maintain your computer manually

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

To maintain your computer manually:

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

Remove unused files and folders

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

To remove unused files and folders:

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

Defragment files and folders

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

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

To defragment files and folders:

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

Restore your computer to previous settings

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

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

To restore your computer to previous settings:

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

Manage your network

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

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

To manage your network:

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

Learn more about viruses

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

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

To learn more about viruses:

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

CHAPTER 6

McAfee QuickClean

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

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

In this chapter

Understanding QuickClean features

This section describes QuickClean features.

Features

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

CHAPTER 7

Cleaning your computer

QuickClean lets you securely delete files and folders.

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

You can delete various items with the following cleaners.

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

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

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

In this chapter

Using QuickClean

This section describes how to use QuickClean.

Clean your computer

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

To clean your computer:

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

CHAPTER 8

McAfee Shredder

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

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

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

In this chapter

Understanding Shredder features

This section describes Shredder features.

Features

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

CHAPTER 9

Erasing unwanted files with Shredder

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

In this chapter

Using Shredder

This section describes how to use Shredder.

Shred files, folders, and disks

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

To shred files, folders, and disks:

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

CHAPTER 10

McAfee Network Manager

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

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

In this chapter

Features

Network Manager provides the following features:

Graphical network map

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

Remote management

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

Understanding Network Manager icons

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

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

CHAPTER 11

Setting up a managed network

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

In this chapter

Working with the network map

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

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

Access the network map

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

To access the network map:

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

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

Refresh the network map

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

To refresh the network map:

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

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

Rename the network

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

To rename the network:

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

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

Show or hide items on the network map

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

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

View item details

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

To view an item's details:

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

Joining the managed network

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

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

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

Join a managed network

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

To join a managed network:

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

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

Invite a computer to join the managed network

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

To invite a computer to join the managed network:

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

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

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

5 Confirm that the playing cards are the same as those displayed on the computer that you have invited to join the managed network.

6 Click **Grant Access**.

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

Stop trusting computers on the network

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

To stop trusting computers on the network:

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

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

CHAPTER 12

Managing the network remotely

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

In this chapter

Monitoring status and permissions

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

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

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

Monitor a computer's protection status

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

To monitor a computer's protection status:

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

Stop monitoring a computer's protection status

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

To stop monitoring a computer's protection status:

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

Modify a managed computer's permissions

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

To modify a managed computer's permissions:

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

Manage a device

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

To manage a device:

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

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

Modify a device's display properties

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

To modify a device's display properties:

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

Fixing security vulnerabilities

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

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

Fix security vulnerabilities

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

To fix security vulnerabilities:

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

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

Install McAfee security software on remote computers

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

To install McAfee security software on a remote computer:

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

CHAPTER 13

McAfee VirusScan

VirusScan offers comprehensive, reliable, and up-to-date virus and spyware protection. Powered by award-winning McAfee scanning technology, VirusScan protects against viruses, worms, Trojan horses, suspect scripts, rootkits, buffer overflows, hybrid attacks, spyware, potentially unwanted programs, and other threats.

In this chapter

Features

This version of VirusScan offers the following features.

Virus protection

Real-time scanning scans files when they are accessed by you or your computer.

Scan

Search for viruses and other threats in hard drives, floppy disks, and individual files and folders. You can also right-click an item to scan it.

Spyware and adware detection

VirusScan identifies and removes spyware, adware, and other programs that can jeopardize your privacy and slow down your computer's performance.

Automatic updates

Automatic updates protect against the latest identified and unidentified computer threats.

Fast background scanning

Fast, unobtrusive scans identify and destroy viruses, Trojans, worms, spyware, adware, dialers, and other threats without interrupting your work.

Real-time security alerting

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

Detection and cleaning at multiple entry points

VirusScan monitors and cleans at your computer’s key entry points: e-mail, instant message attachments, and Internet downloads.

E-mail monitoring for worm-like activity

WormStopper™ blocks Trojans from e-mailing worms to other computers, and prompts you before unknown e-mail programs send e-mail messages to other computers.

Script monitoring for worm-like activity

ScriptStopper™ blocks known, harmful scripts from running on your computer.

McAfee X-ray for Windows

McAfee X-ray detects and kills rootkits and other programs that hide from Windows.

Buffer overflow protection

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

McAfee SystemGuards

SystemGuards examine your computer for specific behaviors that can signal virus, spyware, or hacker activity.

CHAPTER 14

Managing Virus Protection

You can manage real-time virus, spyware, SystemGuards, and script protection. For example, you can disable scanning, or specify what to scan.

Only users with Administrator rights can modify advanced options.

In this chapter

Using virus protection

When virus protection (real-time scanning) is started, it constantly monitors your computer for virus activity. Real-time scanning scans files each time you or your computer access them. When virus protection detects an infected file, it tries to clean or remove the infection. If a file cannot be cleaned or removed, an alert prompts you to take further action.

Related topics

- Understanding security alerts (page 101)

Disable virus protection

If you disable virus protection, your computer is not continuously monitored for virus activity. If you must stop virus protection, ensure that you are not connected to the Internet.

Note: Disabling virus protection also disables real-time spyware, e-mail, and instant messaging protection.

To disable virus protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **Off**.
4. In the confirmation dialog box, do one of the following:
   - To restart virus protection after a specified time, select the **Re-enable real-time scanning after** check box, and select a time from the menu.
   - To stop virus protection from restarting after a specified time, clear the **Re-enable virus protection after** check box.
5. Click **OK**.

If real-time protection is configured to start when Windows starts, your computer is protected when you restart your computer.

Related topics

- Configure real-time protection (page 74)

Enable virus protection

Virus protection continuously monitors your computer for virus activity.

To enable virus protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **On**.

Configuring real-time protection

You can modify real-time virus protection. For example, you can only scan program files and documents, or disable real-time scanning when Windows starts (not recommended).

Configure real-time protection

You can modify real-time virus protection. For example, you can only scan program files and documents, or disable real-time scanning when Windows starts (not recommended).

To configure real-time protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **Advanced**.
4. Select or clear the following check boxes:
   - **Scan for unknown viruses using heuristics**: Files are matched to signatures of known viruses in order to detect signs of unidentified viruses. This option provides the most thorough scan, but is generally slower than a normal scan.
   - **Scan floppy drive on shutdown**: When you shutdown your computer, your floppy drive is scanned.
   - **Scan for spyware and potentially unwanted programs**: Spyware, adware, and other programs that potentially gather and transmit data without your permission are detected and removed.
   - **Scan and remove tracking cookies**: Cookies that potentially gather and transmit data without your permission are detected and removed. A cookie identifies users when they visit a Web page.
   - **Scan network drives**: Drives connected to your network are scanned.
   - **Enable buffer overflow protection**: If buffer overflow activity is detected, it is blocked and you are alerted.
   - **Start real-time scanning when Windows starts (recommended)**: Real-time protection is enabled every time you start your computer, even if you turn it off for a session.
5. Click one of the following buttons:
   - **All files (recommended)**: Every file type that your computer uses is scanned. Use this option to get the most thorough scan.
   - **Program files and documents only**: Only program files and documents are scanned.

6 Click **OK**.

Using spyware protection

Spyware protection removes spyware, adware, and other potentially unwanted programs that gather and transmit data without your permission.

Disable spyware protection

If you disable spyware protection, potentially unwanted programs that gather and transmit data without your permission are not detected.

To disable spyware protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Spyware protection**, click **Off**.

Enable spyware protection

Spyware protection removes spyware, adware, and other potentially unwanted programs that gather and transmit data without your permission.

To enable spyware protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Spyware protection**, click **On**.

Using SystemGuards

SystemGuards detect potentially unauthorized changes to your computer and alert you when they occur. You can then review those changes and decide whether to allow them.

SystemGuards are categorized as follows.

Program

Program SystemGuards detect changes to your startup files, extensions, and configuration files.

Windows

Windows SystemGuards detect changes to your Internet Explorer settings, including browser attributes and security settings.

Browser

Browser SystemGuards detect changes to Windows® services, certificates, and configuration files.

Disable SystemGuards

If you disable SystemGuards, potentially unauthorized changes to your computer are not detected.

To disable all SystemGuards:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **SystemGuard protection**, click **Off**.

Enable SystemGuards

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

To enable SystemGuards:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **SystemGuard protection**, click **On**.

Configuring SystemGuards

You can modify SystemGuards. For each change that is detected, you can decide whether to be alerted and log the event, only log the event, or disable the SystemGuard.

Configure SystemGuards

You can modify SystemGuards. For each change that is detected, you can decide whether to be alerted and log the event, only log the event, or disable the SystemGuard.

To configure SystemGuards:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **SystemGuard protection**, click **Advanced**.
4. In the SystemGuards list, click a category to view a list of associated SystemGuards and their status.
5. Click the name of a SystemGuard.
6. Under **Details**, view information about the SystemGuard.
7. Under **I want to**, do one of the following:
   - Click **Show alerts** if you want to be alerted when a change occurs, and the event is logged.
   - Click **Only log changes** if you do not want an action to be taken when a change is detected. The change is only logged.
   - Click **Disable this SystemGuard** to turn off the SystemGuard. You are not alerted when a change occurs, and the event is not logged.
8. Click **OK**.

Understanding SystemGuards

SystemGuards detect potentially unauthorized changes to your computer and alert you when they occur. You can then review those changes and decide whether to allow them.

SystemGuards are categorized as follows.

Program

Program SystemGuards detect changes to your startup files, extensions, and configuration files.

Windows

Windows SystemGuards detect changes to your Internet Explorer settings, including browser attributes and security settings.

Browser

Browser SystemGuards detect changes to Windows® services, certificates, and configuration files.

About Program SystemGuards

Program SystemGuards detect the following items.

ActiveX Installations

Detect ActiveX programs downloaded through Internet Explorer. ActiveX programs are downloaded from Web sites and stored on your computer in C:\Windows\Downloaded Program Files or C:\Windows\Temp\Temporary Internet Files. They are also referenced in the registry by their CLSID (the long string of numbers between curly braces).

Internet Explorer uses many legitimate ActiveX programs. If you are unsure of an ActiveX program, you can delete it without harming your computer. If you need this program later, Internet Explorer downloads it the next time you return to a Web site that requires it.

Startup Items

Monitor changes made to your startup registry keys and folders. Startup registry keys in the Windows registry and startup folders in the Start menu store paths to programs on your computer. Programs listed in these locations are loaded when Windows starts. Spyware or other potentially unwanted programs often try to load when Windows starts.

Windows Shell Execute Hooks

Monitor changes made to the list of programs that load in explorer.exe. A shell execute hook is a program that loads into the explorer.exe Windows shell. A shell execute hook program receives all execute commands that run on a computer. Any program that is loaded in the explorer.exe shell can perform an additional task before another program is actually launched. Spyware or other potentially unwanted programs can use shell execute hooks to prevent security programs from running.

Shell Service Object Delay Load

Monitor changes to files listed in the Shell Service Object Delay Load. These files are loaded by explorer.exe when your computer starts. Because explore.exe is the shell for your computer, it always starts, loading the files under this key. These files are loaded early in the startup process before any human intervention occurs.

About Windows SystemGuards

Windows SystemGuards detect the following items.

Context Menu Handlers

Prevent unauthorized changes to Windows context menus. These menus allow you to right-click a file, and perform specific actions relevant to that file.

AppInit DLLs

Prevent unauthorized changes or additions to Windows AppInit.DLLs. The AppInit_DLLs registry value contains a list of files that are loaded when user32.dll is loaded. Files in the AppInit_DLLs value are loaded early in the Windows startup routine, allowing a potentially harmful .DLL hide itself before any human intervention occurs.

Windows Hosts File

Monitor changes to your computer Hosts file. your Hosts file is used to redirect certain domain names to specific IP addresses. For example, when you visit www.example.com, your browser checks the Hosts file, sees an entry for example.com, and points to the IP address for that domain. Some spyware programs try to change your Hosts file to redirect your browser to another site or to prevent your software from updating properly.

Winlogon Shell

Monitor the Winlogon Shell. This shell is loaded when a user logs on to Windows. The shell is the main User Interface (UI) used to manage Windows, and is usually Windows Explorer (explore.exe). However, the Windows shell can be easily changed to point to another program. If this occurs, a program other than the Windows shell is launched every time a user logs on.

Winlogon User Init

Monitor changes to your Windows logon user settings. The key HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit specifies what program is launched after a user logs on to Windows. The default program restores your profile, fonts, colors, and other settings for your user name. Spyware and other potentially unwanted programs can try to launch by adding themselves to this key.

Windows Protocols

Monitor changes to your network protocols. Some spyware or other potentially unwanted programs take control of certain ways that your computer sends and receives information. This is accomplished through the Windows protocol filters and handlers.

Winsock Layered Service Providers

Monitor Layered Service Providers (LSPs), which can intercept your data over the network and change or redirect it. Legitimate LSPs include parental controls software, firewalls, and other security programs. Spyware can use LSPs to monitor your Internet activity and modify your data. To avoid reinstallation of the operating system, use McAfee programs to automatically remove spyware and compromised LSPs.

Windows Shell Open Commands

Prevent changes to your Windows Shell (explorer.exe) Open Commands. Shell Open Commands allow a specific program to run every time a certain type of file is run. For example, a worm can attempt to run every time an .exe application runs.

Shared Task Scheduler

Monitor the SharedTaskScheduler registry key, which contains a list of programs that run when Windows starts. Some spyware or other potentially unwanted programs modify this key, and add themselves to the list without your permission.

Windows Messenger Service

Monitor Windows Messenger Service, an undocumented feature of Windows Messenger that allows users to send pop-up messages. Some spyware or other potentially unwanted programs attempt to enable the service and send unsolicited advertisements. The service can also be exploited using a known vulnerability to remotely run code.

Windows Win.ini File

The win.ini file is a text-based file that provides a list of programs to run when Windows starts. The syntax to load these programs exists in the file used to support older versions of Windows. Most programs do not use the sin.ini file to load programs: however, some spyware or other potentially unwanted programs are designed to take advantage of this syntax and load themselves during Windows startup.

About Browser SystemGuards

Browser SystemGuards detect the following items.

Browser Helper Objects

Monitor additions to your Browser Helper Objects (BHOs). BHOs are programs that act as Internet Explorer plug-ins. Spyware and browser hijackers often use BHOs to show ads or track your browsing habits. BHOs are also used by many legitimate programs such as common search toolbars.

Internet Explorer Bars

Monitor changes made to your list of Internet Explorer bar programs. An explorer bar is a pane like the Search, Favorites, or History panes that you see in Internet Explorer (IE) or Windows Explorer.

Internet Explorer Plug-ins

Prevent spyware from installing Internet Explorer plug-ins. Internet Explorer plug-ins are software add-ons that are loaded when Internet Explorer starts. Spyware often uses Internet Explorer plug-ins to show ads or track your browsing habits. Legitimate plug-ins add functionality to Internet Explorer.

Internet Explorer ShellBrowser

Monitor changes made to your Internet Explorer ShellBrowser instance. The Internet Explorer ShellBrowser contains information and settings about an instance of Internet Explorer. If these settings are changed, or a new ShellBrowser is added, this ShellBrowser can take full control of Internet Explorer, adding features such as toolbars, menus, and buttons.

Internet Explorer WebBrowser

Monitor changes made to your Internet Explorer WebBrowser instance. The Internet Explorer WebBrowser contains information and settings about an instance of Internet Explorer. If these settings are changed, or a new WebBrowser is added, this WebBrowser can take full control of Internet Explorer, adding features such as toolbars, menus, and buttons.

Internet Explorer URL Search Hooks

Monitor changes made to your Internet Explorer URL Search Hook. A URL Search Hook is used when you type an address in the location field of the browser without a protocol such as http:// or ftp:// in the address. When you enter such an address, the browser can use the UrlSearchHook to search the Internet to find the location you entered.

Internet Explorer URLs

Monitor changes to your Internet Explorer preset URLs. This prevents spyware or other potentially unwanted programs from changing your browser settings without your permission.

Internet Explorer Restrictions

Monitor Internet Explorer restrictions, which allow a computer administrator to prevent a user from changing the home page or other options in Internet Explorer. These options only appear if your administrator intentionally set them.

Internet Explorer Security Zones

Monitor Internet Explorer security zones. Internet Explorer has four predefined security zones: Internet, Local intranet, Trusted sites, and Restricted sites. Each security zone has its own security setting which is predefined or customized. Security zones are a target of some spyware or other potentially unwanted programs because lowering the security level allows these programs to bypass security alerts and act undetected.

Internet Explorer Trusted Sites

Monitor Internet Explorer trusted sites. The trusted site list is a directory of the Web sites you trusted. Some spyware or other potentially unwanted programs target this list because it provides a method to trust suspect sites without your permission.

Internet Explorer Policy

Monitor Internet Explorer policies. These settings are usually changed by system administrators but can be exploited by spyware. Changes can prevent you from setting a different Home page or can hide tabs from your view in the Internet Options dialog box of the Tools menu.

Using script scanning

A script can create, copy, or delete files. It can also open your Windows registry.

Script scanning automatically blocks known harmful scripts from running on your computer.

Disable script scanning

If you disable script scanning, suspicious script executions are not detected.

To disable script scanning:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Script scanning protection**, click **Off**.

Enable script scanning

Script scanning alerts you if a script execution results in the creation, copying, or deletion of files, or the opening of your Windows registry.

To enable script scanning:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Script scanning protection**, click **On**.

Using e-mail protection

E-mail protection detects and blocks threats in inbound (POP3) and outbound (SMTP) e-mail messages and attachments, which include viruses, Trojans, worms, spyware, adware, and other threats.

Disable e-mail protection

If you disable e-mail protection, potential threats in inbound (POP3) and outbound (SMTP) e-mail messages and attachments are not detected.

To disable e-mail protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **E-mail & IM**.
3. Under **E-mail protection**, click **Off**.

Enable e-mail protection

E-mail protection detects threats in inbound (POP3) and outbound (SMTP) e-mail messages and attachments.

To enable e-mail protection:

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

Configuring e-mail protection

E-mail message protection options allow you to scan inbound e-mail messages, outbound e-mail messages, and worms. Worms replicate and consume system resources, slowing performance or halting tasks. Worms can send copies of themselves through e-mail messages. For example, they can attempt to forward e-mail messages to people in your address book.

Configure e-mail protection

E-mail message protection options allow you to scan inbound e-mail messages, outbound e-mail messages, and worms.

To configure e-mail protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **E-mail & IM**.
3. Under **E-mail protection**, click **Advanced**.
4. Select or clear the following check boxes:
   - **Scan inbound e-mail messages**: Inbound (POP3) messages are scanned for potential threats.
   - **Scan outbound e-mail messages**: Outbound (SMTP) messages are scanned for potential threats.
   - **Enable WormStopper**: WormStopper blocks worms in e-mail messages.
5. Click **OK**.

Using instant messaging protection

Instant messaging protection detects threats in inbound instant message attachments.

Disable instant messaging protection

If you disable instant messaging protection, threats in inbound instant message attachments are not detected.

To disable instant messaging protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **E-mail & IM**.
3. Under **Instant Messaging protection**, click **Off**.

Enable instant messaging protection

Instant messaging protection detects threats in inbound instant message attachments.

To enable instant messaging protection:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **E-mail & IM**.
3. Under **Instant Messaging protection**, click **On**.

CHAPTER 15

Manually Scanning Your Computer

You can search for viruses and other threats on hard drives, floppy disks, and individual files and folders. When VirusScan finds a suspicious file, it tries to clean it, unless it is a potentially unwanted program. If VirusScan cannot clean the file, you can quarantine or delete it.

In this chapter

Manually scanning

You can manually scan at any time. For example, if you just installed VirusScan, you can perform a scan to ensure that your computer does not have any viruses or other threats. Or, if you disabled real-time scanning, you can perform a scan to ensure that your computer is still secure.

Scan using your manual scan settings

This type of scan uses the manual scan settings you specify. VirusScan scans inside compressed files (.zip, .cab, etc.), but counts a compressed file as one file. Also, the number of files scanned can vary if you have deleted your temporary Internet files since your last scan.

To scan using your manual scan settings:

1. On the Basic Menu, click **Scan**. When the scan is completed, a summary shows the number of items scanned and detected, the number of items cleaned, and when your last scan occurred.
2. Click **Finish**.

Related topics

- Configuring manual scans (page 92)

Scan without using your manual scan settings

This type of scan does not use the manual scan settings you specify. VirusScan scans inside compressed files (.zip, .cab, etc.), but counts a compressed file as one file. Also, the number of files scanned can vary if you have deleted your temporary Internet files since your last scan.

To scan without using your manual scan settings:

1. On the Advanced Menu, click **Home**.
2. On the Home pane, click **Scan**.
3. Under **Locations to Scan**, select the check boxes beside the files, folders, and drives you want to scan.
4. Under **Options**, select the check boxes beside the type of files you want to scan.
5. Click **Scan Now**. When the scan is completed, a summary shows the number of items scanned and detected, the number of items cleaned, and when your last scan occurred.
6. Click **Finish**.

Note: These options are not saved.

Scan in Windows Explorer

You can scan for viruses and other threats in selected files, folders, or drives within Windows Explorer.

To scan files in Windows Explorer:

1. Open Windows Explorer.
2. Right-click the file, folder, or drive that you want to scan, and then click **Scan**. All the default scan options are selected to provide a thorough scan.

Configuring manual scans

When performing a manual or scheduled scan, you can specify the type of files to scan, the locations to scan, and when to run a scan.

Configure the type of files to scan

You can configure the type of files to scan.

To configure the type of files to scan:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **Advanced**.
4. On the Virus Protection pane, click **Manual Scan**.
5. Select or clear the following check boxes:
   - **Scan for unknown viruses using heuristics**: Files are matched to signatures of known viruses in order to detect signs of unidentified viruses. This option provides the most thorough scan, but is generally slower than a normal scan.
   - **Scan .zip and other archive files**: Detects and removes viruses in .zip and other archive files. Sometimes virus authors plant viruses in a .zip file, and then insert that .zip file it into another .zip file in an effort to bypass anti-virus scanners.
   - **Scan for spyware and potentially unwanted programs**: Spyware, adware, and other programs that potentially gather and transmit data without your permission are detected and removed.
   - **Scan and remove tracking cookies**: Cookies that potentially gather and transmit data without your permission are detected and removed. A cookie identifies users when they visit a Web page.
   - **Scan for rootkits and other stealth programs**: Detect and remove any rootkit or other program that hides from Windows.
6. Click one of the following buttons:
   - **All files (recommended)**: Every file type that your computer uses is scanned. Use this option to get the most thorough scan.
   - **Program files and documents only**: Only program files and documents are scanned.
7. Click **OK**.

Configure the locations to scan

You can configure the locations to scan for manual or scheduled scans.

To configure where to scan:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **Advanced**.
4. On the Virus Protection pane, click **Manual Scan**.
5. Under **Default Location to Scan**, select the files, folders, and drives that you want to scan.

   To get the most thorough scan possible, ensure that **Critical files** is selected.
6. Click **OK**.

Schedule scans

You can schedule scans to thoroughly check your computer for viruses and other threats at specified intervals.

To schedule a scan:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **Advanced**.
4. On the Virus Protection pane, click **Scheduled Scan**.
5. Ensure that **Enable scheduled scanning** is selected.
6. Select the check box beside the day of the week on which to perform the scan.
7. Click values in the start time lists to specify a start time.
8. Click **OK**.

Tip: To use the default schedule, Click **Reset.**

CHAPTER 16

Administering VirusScan

You can remove items from trusted lists, manage quarantined programs, cookies, and files, view events and logs, and report suspicious activity to McAfee.

In this chapter

Managing trusted lists

When you trust a SystemGuard, program, buffer overflow, or e-mail program, the item is added to a trusted list so that it is not detected any more.

If you trust a program by mistake, or you want the program to be detected, you must remove it from this list.

Manage trusted lists

When you trust a SystemGuard, program, buffer overflow, or e-mail program, the item is added to a trusted list so that it is not detected any more.

If you trust a program by mistake, or you want the program to be detected, you must remove it from this list.

To remove items from the trusted lists:

1. On the Advanced Menu, click **Configure**.
2. On the Configure pane, click **Computer & Files**.
3. Under **Virus protection**, click **Advanced**.
4. On the Virus Protection pane, click **Trusted Lists**.
5. In the list, select a trusted SystemGuard, program, buffer overflow, or e-mail program to view its items and their trusted status.
6. Under **Details**, view information about the item.
7. Under **I want to**, click an action.
8. Click **OK**.

Managing quarantined programs, cookies, and files

Quarantined programs, cookies, and files, can be restored, deleted, or sent to McAfee for analysis.

Restore quarantined programs, cookies, and files

If required, you can restore programs, cookies, and files that are quarantined.

To restore quarantined programs, cookies, and files:

1. On the Advanced Menu, click **Restore**.
2. On the Restore pane, click **Programs and Cookies** or **Files**, as appropriate.
3. Select the quarantined programs, cookies, or files you want to restore.
4. For more information about the virus that is quarantined, click its detection name under **Details**. The Virus Information Library appears with the virus description.
5. Under **I want to**, click **Restore**.

Remove quarantined programs, cookies, and files

You can remove programs, cookies, and files that are quarantined.

To remove quarantined programs, cookies, and files:

1. On the Advanced Menu, click **Restore**.
2. On the Restore pane, click **Programs and Cookies** or **Files**, as appropriate.
3. Select the quarantined programs, cookies, or files you want to restore.
4. For more information about the virus that is quarantined, click its detection name under **Details**. The Virus Information Library appears with the virus description.
5. Under **I want to**, click **Remove**.

Send quarantined programs, cookies, and files, to McAfee

You can send quarantined programs, cookies, and files, to McAfee for analysis.

Note: If the quarantined file you are sending exceeds a maximum size, the file can be rejected. In most instances, this does not occur.

To send quarantined programs or files to McAfee:

1. On the Advanced Menu, click **Restore**.
2. On the Restore pane, click **Programs and Cookies** or **Files**, as appropriate.
3. Select the quarantined programs, cookies, or files you want to send to McAfee.
4. For more information about the virus that is quarantined, click its detection name under **Details**. The Virus Information Library appears with the virus description.
5. Under **I want to**, click **Send to McAfee**.

Viewing recent events and logs

Recent events and logs display events from all installed McAfee products.

Under Recent Events you can see the last 30 significant events that occurred on your computer. You can restore blocked programs, re-enable real-time scanning, and trust buffer overflows.

You can also view logs, which record every event that occurred over the last 30 days.

View events

Under Recent Events you can see the last 30 significant events that occurred on your computer. You can restore blocked programs, re-enable real-time scanning, and trust buffer overflows.

To view events:

1. On the Advanced Menu, click **Reports & Logs**.
2. On the Reports & Logs pane, click **Recent Events**.
3. Select the event you want to view.
4. Under **Details**, view information about the event.
5. Under **I want to**, click an action.

View logs

Logs record every event that occurred over the last 30 days.

To view logs:

1. On the Advanced Menu, click **Reports & Logs**.
2. On the Reports & Logs pane, click **Recent Events**.
3. On the Recent Events pane, click **View Log**.
4. Select the type of log you want to view, and then select a log.
5. Under **Details**, view information about the log.

Automatically reporting anonymous information

You can anonymously send virus, potentially unwanted program, and hacker tracking information to McAfee. This option is only available during installation.

No personal identifiable information is collected.

Report to McAfee

You can send virus, potentially unwanted program, and hacker tracking information to McAfee. This option is only available during installation.

To automatically report anonymous information:

1. During VirusScan installation, accept the default **Submit anonymous information**.
2. Click **Next**.

Understanding security alerts

If real-time scanning detects a threat, an alert appears. For most viruses, Trojans, scripts, and worms, real-time scanning automatically tries to clean the file, and alerts you. For potentially unwanted programs and SystemGuards, real-time scanning detects the file or change, and alerts you. For buffer overflow, tracking cookies, and script activity, real-time scanning automatically blocks the activity, and alerts you.

These alerts can be grouped into three basic types.

- Red alert
- Yellow alert
- Green alert

You can then choose how to manage detected files, detected e-mail, suspect scripts, potential worms, potentially unwanted programs, SystemGuards, or buffer overflows.

Manage alerts

McAfee 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

Red alert

A red alert requires a response from you. In some cases, McAfee cannot determine how to respond automatically to a particular activity. In these cases, the red alert describes the activity in question and gives you one or more options to select.

Yellow alert

A yellow alert is a non-critical notification that usually requires a response from you. The yellow alert describes the activity in question and gives you one or more options to select.

Green alert

In most cases, a green alert provides basic information about an event and does not require a response.

Configuring alert options

If you choose not to show an alert again and later on you change your mind, you can go back and configure that alert to appear again. For more information about configuring alert options, see your SecurityCenter documentation.

CHAPTER 17

Additional Help

This chapter describes frequently asked questions and troubleshooting scenarios.

In this chapter

Frequently Asked Questions

This section provides answers to the most frequently asked questions.

A threat has been detected, what should I do?

McAfee uses alerts to help you manage your security. These alerts can be grouped into three basic types.

- Red alert
- Yellow alert
- Green alert

You can then choose how to manage detected files, detected e-mail, suspect scripts, potential worms, potentially unwanted programs, SystemGuards, or buffer overflows.

For more information about managing particular threats, consult the Virus Information Library at: http://us.mcafee.com/virusInfo/default.asp?affid=.

Related topics

- Understanding security alerts (page 101)

Can I use VirusScan with Netscape, Firefox, and Opera browsers?

You can use Netscape, Firefox, and Opera as your default Internet browser, but you must have Microsoft® Internet Explorer 6.0 or later installed on your computer.

Do I need to be connected to the Internet to perform a scan?

You do not have to be connected to the Internet to run a scan, but you should connect at least once a week in order to receive McAfee updates.

Does VirusScan scan e-mail attachments?

If you have real-time scanning and e-mail protection enabled, any attachment is scanned as the e-mail message arrives.

Does VirusScan scan zipped files?

VirusScan scans .zip files and other archived files.

Why do outbound e-mail scanning errors occur?

When scanning outbound e-mail messages, these types of errors can occur:

- Protocol error. The e-mail server has rejected an e-mail message.
  If a protocol error or system error occurs, the remaining e-mail messages for that session are processed and sent to the server.
- Connection error. A connection to the e-mail server has been dropped.
  If a connection error occurs, ensure that your computer is connected to the Internet, and then retry sending the message from the **Sent** items list in your e-mail program.
- System error. A file handling failure or other system error has occurred.
- Encrypted SMTP connection error. An encrypted SMTP connection from your e-mail program has been detected.
  If an encrypted SMTP connection occurs, you turn off the encrypted SMTP connection in your e-mail program to ensure that your e-mail messages are scanned.

If timeouts occur while sending e-mail messages, disable outbound e-mail scanning or turn off encrypted SMTP connection in your e-mail program.

Related topics

- Configure e-mail protection (page 87)

Troubleshooting

This section provides help for general problems you can experience.

A virus cannot be cleaned or deleted

For some viruses, you must manually clean your computer. Try restarting your computer and then scanning again.

If your computer cannot clean or delete a virus, consult the Virus Information Library at: http://us.mcafee.com/virusInfo/default.asp?affid=.

If you need additional help, consult McAfee Customer Support at the McAfee Web site.

Note: Viruses cannot be cleaned from CD-ROMs, DVDs, and write-protected floppy disks.

After restarting, an item still cannot be removed

After scanning and removing items, some situations require that you restart your computer.

If the item is not removed after restarting your computer, submit the file to McAfee.

Note: Viruses cannot be cleaned from CD-ROMs, DVDs, and write-protected floppy disks.

Related topics

- Managing quarantined programs, cookies, and files (page 97)

Components are missing or corrupt

Some situations can cause VirusScan to install incorrectly:

- Your computer does not have enough disk space or memory. Verify that your computer meets the system requirements to run this software.
- Your Internet browser is incorrectly configured.
- You have a faulty Internet connection. Check your connection; otherwise, try to connect again later.
- Files are missing or the installation failed.

The best solution is to resolve these potential issues, and then reinstall VirusScan.

CHAPTER 18

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.

In this chapter

Features

Personal Firewall provides complete inbound and outbound firewall protection and automatically trusts known good programs and helps blocks spyware, Trojans, and key loggers. Firewall allows you to defend against hacker probes and attacks, monitors Internet and network activity, alerts you to hostile or suspicious events, provides detailed information about Internet traffic, and complements antivirus defenses.

Standard and custom protection levels

Guard against intrusion and suspicious activity using Firewall's default protection settings or customize Firewall to your own security needs.

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, or configure access permissions for specific programs from Firewall's Program Permissions pane.

Gaming protection

Prevent alerts regarding intrusion attempts and suspicious activities from distracting you during full-screen gameplay and configure Firewall to display alerts following completion of the computer game.

Computer startup protection

Before Windows opens, Firewall protects your computer from intrusion attempts and unwanted programs and network traffic.

System service port control

System Service ports can provide a backdoor to your computer. Firewall allows you to create and manage open and closed system service ports required by some programs.

Manage computer connections

Trust and ban remote connections and IP addresses that can connect to your computer.

HackerWatch information integration

HackerWatch is a security information hub that tracks global hacking and intrusion patterns as well as providing the most up-to-date information about programs on your computer. You can view global security event and Internet port statistics.

Lockdown Firewall

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

Restore Firewall

Instantly restore the original protection settings for Firewall. If Personal Firewall exhibits undesirable behavior that you cannot correct, you can restore Firewall to its default settings.

Advanced Trojan detection

Combines program connection management with an enhanced database to detect and block potentially malicious applications, such as Trojans, from accessing the Internet and relaying your personal data.

Event logging

Specify whether you want to enable or disable logging and, when enabled, which event types to log. Event logging allows you to view recent inbound and outbound events. You can also view intrusion detected events.

Monitor Internet traffic

Review easy-to-read graphical maps showing the source of hostile attacks and traffic worldwide. 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 by providing intrusion prevention of 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.

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 Standard security level 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.

Start firewall protection

Enabling firewall protection defends your computer from intrusion and unwanted network traffic and helps you manage inbound and outbound Internet connections.

To enable firewall protection:

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

Stop firewall protection

Disabling firewall protection leaves your computer vulnerable to intrusion and unwanted network traffic. Without firewall protection enabled, you cannot manage inbound and outbound Internet connections.

To disable firewall protection:

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

Working with alerts

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

- Trojan Blocked alert
- Red alert
- Yellow alert
- Green alert

Alerts can also contain information to help the user decide how to handle alerts or get information about programs running on their computer.

About alerts

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

Trojan Blocked alert

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

Red alert

The most common type of alert is the red alert, which generally requires a response from you. Because Firewall is, in some cases, unable to automatically determine a particular course of action for a program activity or network event, the alert first describes the program activity or network event in question followed by one or more options to which you must respond. If Smart Recommendations is enabled, programs are added to the Program Permissions pane.

The following alert descriptions are the most commonly encountered:

- **Program requests Internet access**: Firewall detects a program attempting to access the Internet.
- **Program has been modified**: Firewall detects a program that has changed in some way, perhaps as a result of an online update.
- **Program Blocked**: Firewall blocks a program because it is listed on the Program Permissions pane.

Depending on your settings and program activity or network event, the following options are the most commonly encountered:

- **Grant access**: Allow a program on your computer access to the Internet. The rule is added to the Program Permissions page.
- **Grant access once**: Allow a program on your computer to temporarily access the Internet. For example, the installation of a new program may require access once only.
- **Block access**: Prevent a program's access to the Internet.

- **Grant outbound-only access**: Allow an outbound connection to the Internet only. This alert typically appears when Tight and Stealth security levels are set.
- **Trust this network**: Allow inbound and outbound traffic from a network. The network is added to the Trusted IP Addresses section.
- **Do not trust this network at this time**: Block inbound and outbound traffic from a network.

Yellow alert

The yellow alert is a non-critical notification which informs you about a network event detected by Firewall. For example, the **New Network Detected** alert appears when Firewall is run for the first time or 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.

Green alert

In most cases, a green alert provides basic information about an event and does not require a response. Green alerts usually occur when Standard, Tight, Stealth, and Lockdown security levels are set. Green alert descriptions are as follows:

- **Program has been Modified**: Informs you that a program that you previously allowed access to the Internet has been modified. You can opt to block the program, but if you do not respond, the alert disappears from your desktop and the program continues to have access.
- **Program Granted Internet Access**: Notifies you that a program has been granted Internet access. You can opt to block the program, but if you do not respond, the alert disappears and the program continues to access the Internet.

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 grant access for a program.

Managing informational alerts

Firewall allows you to display or hide informational alerts during certain events.

Display alerts while gaming

By default, Firewall prevents informational alerts from appearing during full-screen gameplay. However, you can configure Firewall to show informational alerts during gameplay when Firewall detects intrusion attempts or suspicious activity.

To show alerts during gameplay:

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

Hide informational alerts

Informational alerts notify you about events that do not require your immediate attention.

To hide informational alerts:

1. On the Common Tasks pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, click **Alerts**.
4. Click **Advanced**.
5. On the **SecurityCenter Configuration** pane, click **Informational Alerts**.
6. On the **Informational Alerts** pane, do one of the following:
   - Select an alert type to hide.
   - Select **Hide informational alerts** to hide all informational alerts.
7. Click **OK**.

CHAPTER 19

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 level of protection is set to Standard security. For most, this setting meets all their security needs. 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

You can configure security levels to control the degree to which you want to manage and respond to alerts when Firewall detects unwanted network traffic and inbound and outbound Internet connections. By default, Standard security level is enabled.

When Standard security level is set and Smart Recommendations is enabled, red alerts provide the options to grant or block access for unknown or modified programs. When known programs are detected, green informational alerts appear, and access is automatically granted. Granting access allows a program to create outbound connections and to 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.

Firewall employs six security levels. Starting from the most restrictive to the least, these levels include the following:

- **Lockdown**: Blocks all Internet connections.
- **Stealth**: Blocks all inbound Internet connections.
- **Tight**: Alerts require your response to every inbound and outbound Internet connection request.
- **Standard**: Alerts notify you when unknown or new programs require Internet access.
- **Trusting**: Grants all inbound and outbound Internet connections and automatically adds them to the Program Permissions pane.
- **Open**: Grants all inbound and outbound Internet connections.

Firewall also allows you to immediately reset your security level to standard from the Restore Firewall Protection Defaults pane.

Set security level to Lockdown

Setting the firewall's security level to 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. During Lockdown, alerts can continue to prompt you to block programs.

To set the firewall's security level to Lockdown:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Lockdown** displays as the current level.
3. Click **OK**.

Set security level to Stealth

Setting the firewall's security level to Stealth blocks all inbound network connections, except open ports. This setting completely hides your computer's presence on the Internet. When the security level is set to Stealth, 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.

To set the firewall's security level to Stealth:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Stealth** displays as the current level.
3. Click **OK**.

Set security level to Tight

When you set the security level to Tight, Firewall informs 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 grant or block. Later, if the program requires both an inbound and an outbound connection, you can grant full access for the program from the Program Permissions pane.

To set the firewall's security level to Tight:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Tight** displays as the current level.
3. Click **OK**.

Set security level to Standard

Standard is the default and recommended security level.

When you set the firewall's security level to Standard, Firewall monitors inbound and outbound connections and alerts when new programs attempt Internet access. Blocked and added programs appear on the Program Permissions pane.

To set the firewall's security level to Standard:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Standard** displays as the current level.
3. Click **OK**.

Set security level to Trusting

Setting the firewall's security level to Trusting allows all inbound and outbound connections. In Trusting security, the firewall automatically grants access for all programs, and adds them to the list of allowed programs on the Program Permissions pane.

To set the firewall's security level to Trusting

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Trusting** displays as the current level.
3. Click **OK**.

Configuring Smart Recommendations for alerts

You can configure Firewall to include, exclude, or display recommendations in alerts regarding programs which attempt to access the Internet.

Enabling Smart Recommendations helps you decide how to handle alerts. When Smart Recommendations is enabled (and the security level is Standard), the Firewall automatically grants or blocks known programs, and alerts you and recommends a course of action when it detects unknown and potentially dangerous programs.

When Smart Recommendations is disabled, the Firewall neither grants or blocks Internet access automatically nor recommends a course of action.

When Firewall is configured to display Smart Recommendations only, an alert prompts you to grant or block access, but suggests a course of action.

Enable Smart Recommendations

Enabling Smart Recommendations helps you decide how to handle alerts. When Smart Recommendations is enabled, the Firewall automatically grants or blocks programs, and alerts you about unrecognized and potentially dangerous programs.

To enable Smart Recommendations:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Smart Recommendations**, select **Enable Smart Recommendations**.
3. Click **OK**.

Disable Smart Recommendations

When you disable Smart Recommendations, alerts exclude assistance about handling alerts and managing access for programs. If Smart Recommendations is disabled, the firewall continues to grant and block programs, and alerts you about unrecognized and potentially dangerous programs. And, if it detects a new program that is suspicious or is known to be a possible threat, Firewall automatically blocks the program from accessing the Internet.

To disable Smart Recommendations:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Smart Recommendations**, select **Disable Smart Recommendations**.
3. Click **OK**.

Display Smart Recommendations only

Displaying Smart Recommendations helps you decide how to handle alerts regarding unrecognized and potentially dangerous programs. When Smart Recommendations is set to **Display Only**, information about handling alerts is shown, but unlike the **Enable Smart Recommendations** option, the recommendations displayed are not automatically applied and programs' access are not automatically granted or blocked. Instead, alerts provide recommendations to help you decide to grant or block programs.

To display Smart Recommendations only:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Smart Recommendations**, select **Display Only**.
3. 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 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 boot time protection and to block ICMP ping requests. The first setting blocks programs from accessing the Internet as Windows starts 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

Firewall can protect your computer as Windows starts up. Boot time protection blocks all new programs that have not been previously granted and require access to the Internet. After Firewall is launched, it displays relevant alerts for programs that had requested Internet access during startup, which you can grant or block. To use this option, your security level must not be set to Open or Lockdown.

To protect your computer during startup:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under Security Settings, select **Enable boot time protection**.
3. Click **OK**.

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

Configure ping request settings

Computer users can use a ping tool, which sends and receives ICMP Echo Request messages, to determine whether a given computer is connected to the network. You can configure Firewall to prevent or allow computer users to ping your computer.

To configure your ICMP ping requests setting:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. 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.
3. Click **OK**.

Configure intrusion detection

Intrusion detection (IDS) monitors data packets for suspicious data transfers or transfer methods. IDS analyzes traffic and data packets for specific traffic patterns used by attackers. For example, when Firewall detects ICMP packets, it analyzes these for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns. Firewall compares packets to a signature database and, if suspicious or harmful, drops the packets from the offending computer, and then optionally logs the event.

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.

To configure intrusion detection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Intrusion Detection**.
3. 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.
4. Click **OK.**

Configure Firewall Protection Status settings

SecurityCenter tracks problems that are part of your overall computer Protection Status. However, you can configure Firewall to ignore specific problems on your computer which can affect your Protection Status. You can configure SecurityCenter to ignore when Firewall is set to Open security level, when the Firewall service is not running, and when an outbound-only firewall is not installed on your computer.

To configure Firewall Protection Status settings:

1. On the Common Tasks pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, click **Alerts**.
4. Click **Advanced**.
5. On the Common Tasks pane, click **Advanced Menu**.
6. Click **Configure**.
7. On the SecurityCenter Configuration pane, click **Protection Status**.
8. Click Advanced.
9. In the Ignored Problems pane, select one or more of the following options:
   - **Firewall is set to Open security level.**
   - **Firewall service is not running.**
   - **Outbound firewall is not installed on your computer.**
10. Click **OK**.

Locking and restoring Firewall

Lockdown is helpful when handling computer-related emergencies, for users who need to block all traffic to isolate and troubleshoot a problem on their computer, or for those who are uncertain, and need to determine, how to manage a program's access to the Internet.

Lock Firewall instantly

Locking down Firewall instantly blocks all inbound and outbound network traffic between your computer and the Internet. It stops all remote connections from accessing your computer and blocks all programs on your computer from accessing the Internet.

To instantly lock Firewall and block all network traffic:

1. On the Home or Common Tasks panes with the **Basic** or **Advanced Menu** enabled, click **Lockdown Firewall**.
2. On the Lockdown Firewall pane, click **Lockdown**.
3. On the dialog, click **Yes** to confirm that you want to instantly block all inbound and outbound traffic.

Unlock Firewall instantly

Locking down Firewall instantly blocks all inbound and outbound network traffic between your computer and the Internet. It stops all remote connections from accessing your computer and blocks all programs on your computer from accessing the Internet. After you Lockdown Firewall, you can unlock it to allow network traffic.

To instantly unlock Firewall and allow network traffic:

1. On the Home or Common Tasks panes with the **Basic** or **Advanced Menu** enabled, click **Lockdown Firewall**.
2. On the Lockdown Enabled pane, click **Unlock**.
3. On the dialog, click **Yes** to confirm that you want to unlock Firewall and allow network traffic.

Restore Firewall settings

You can quickly restore Firewall to its original protection settings. This sets your security level to standard, enables Smart Recommendations, resets trusted and banned IP addresses, and removes all programs from the Program Permissions pane.

To restore Firewall to its original settings:

1. On the Home or Common Tasks panes with the **Basic** or **Advanced Menu** enabled, click **Restore Firewall Defaults**.
2. On the Restore Firewall Protection Defaults pane, click **Restore Defaults**.
3. On the Restore Firewall Protection Defaults dialog, click **Yes** to confirm that you want to restore the firewall configuration to its default settings.

Set security level to Open

Setting the firewall's security level to Open allows the firewall to grant access to all inbound and outbound network connections. To grant access for previously blocked programs, use the Program Permissions pane.

To set the firewall's security level to Open:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Open** displays as the current level.
3. Click **OK**.

Note: Previously blocked programs continue to be blocked when the firewall security level is set to **Open**. To prevent this, you can change the program's rule to **Full Access**.

CHAPTER 20

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 allows you to grant full or outbound-only access for programs. You can also block access for programs.

In this chapter

Granting 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:

- Grant access for programs
- Grant outbound-only access for programs
- Block access for programs

You can also grant full and outbound-only access from the Outbound Events and Recent Events log.

Grant full access for a program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can modify these permissions.

To grant a program full Internet access:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program with **Blocked** or **Outbound-Only Access**.
4. Under **Action**, click **Grant Full Access**.
5. Click **OK**.

Grant full access for a new program

Many programs on your computer require inbound and outbound access to the Internet. Firewall includes a list of programs that are automatically allowed full access, but you can add a new program and change its permissions.

To grant a new program full Internet access:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the **Firewall** pane, click **Program Permissions**.
3. Under **Program Permissions**, click **Add Allowed Program**.
4. On the **Add Program** dialog browse for and select the program you want to add.
5. Click **Open**.
6. Click **OK**.

   The newly added program appears under **Program Permissions**.

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

Grant full access from the Recent Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Recent Events log and grant it full Internet access.

To grant a program full access from the Recent Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, select the event description, and then click **Grant Full Access**.
3. In the Program Permissions dialog, click **Yes** to confirm that you want to grant the program full access.

Related topics

- View outbound events (page 160)

Grant full access from the Outbound Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Outbound Events log and grant it full access to the Internet.

To grant a program full Internet access from the Outbound Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.
4. In the Outbound Events pane, select a source IP address, and then click **Grant access**.
5. On the Program Permissions dialog, click **Yes** to confirm that you want to grant the program full Internet access.

Related topics

- View outbound events (page 160)

Granting outbound-only access for programs

Some programs on your computer only require outbound access to the Internet. Firewall allows you to grant programs outbound-only access to the Internet.

Grant outbound-only access for a program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can modify these permissions.

To grant a program outbound-only access:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program with **Blocked** or **Full Access**.
4. Under **Action**, click **Grant Outbound-Only Access**.
5. Click **OK**.

Grant outbound-only access from the Recent Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Recent Events log and grant it outbound-only Internet access.

To grant a program outbound-only access from the Recent Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, select the event description, and then click **Grant Outbound-Only Access**.
3. In the Program Permissions dialog, click **Yes** to confirm that you want to grant the program outbound-only access.

Related topics

- View outbound events (page 160)

Grant outbound-only access from the Outbound Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Outbound Events log and grant it outbound-only Internet access.

To grant a program outbound-only access from the Outbound Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.
4. In the Outbound Events pane, select a source IP address, and then click **Grant outbound-Only Access**.
5. In the Program Permissions dialog, click **Yes** to confirm that you want to grant the program outbound-only access.

Related topics

- View outbound events (page 160)

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

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can block these permissions.

To block Internet access for a program:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program with **Full Access** or **Outbound-Only Access**.
4. Under **Action**, click **Block Access.**
5. Click **OK**.

Block access for a new program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can add a new program and then block its access to the Internet.

To block Internet access for a new program:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. Under the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, click **Add Blocked Program**.
4. On the **Add Program** dialog browse for and select the program you want to add.
5. Click **Open**.
6. Click **OK**.

   The newly added program appears under **Program Permissions**.

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

Block access from the Recent Events log

Many programs on your computer require inbound and outbound access to the Internet. However, you can also opt to block programs from accessing the Internet from the Recent Events log.

To block access for a program from the Recent Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, select the event description, and then click **Block Access**.
3. In the Program Permissions dialog, click **Yes** to confirm that you want to block the program.

Related topics

- View outbound events (page 160)

Removing access permissions for programs

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

Remove a program permission

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can remove programs that have been automatically and manually added.

To remove a program permission for a new program:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program.
4. Under **Action**, click **Delete Program Permission**.
5. Click **OK**.

   The program is removed from the Program Permissions pane.

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

Learning about programs

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

Get program information

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can modify these permissions.

Firewall can help you decide to grant or block Internet access for a program. Ensure that you are connected to the Internet so that your browser successfully launches McAfee's HackerWatch Web site, which provides up-to-date information about programs, Internet access requirements, and security threats.

To get program information:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program.
4. Under **Action**, click **Learn More**.

Get program information from the Outbound Events log

Personal Firewall allows you to get information about programs that appear in the Outbound Events log.

Before getting information about a program, ensure that you have an Internet connection and an Internet browser.

To get program information from the Outbound Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.
4. On the Outbound Events pane, select a source IP address, and then click **Learn more**.

   You can view information about the program on the HackerWatch Web site. HackerWatch provides up-to-date information about programs, Internet access requirements, and security threats.

Related topics

- View outbound events (page 160)

CHAPTER 21

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.

This list shows the standard ports for common services.

- 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
- 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

In this chapter

Configuring system service ports

To allow remote access to a service on your computer you must specify the service and associated port to open. Only select a service and port if you are certain it must be open. Rarely is it necessary to open a port.

Allow access to an existing system service port

From the System Services pane, you can open or close an existing port to allow or deny remote access to a network service on your computer. An open system service port can make your computer vulnerable to Internet security threats; therefore only open a port, if necessary.

To allow access to a system service port:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **System Services**.
3. Under **Open System Service Port**, select a system service to open a port.
4. Click **OK**.

Block access to an existing system service port

From the System Services pane, you can open or close an existing port to allow or deny remote access to a network service on your computer. An open system service port can make your computer vulnerable to Internet security threats; therefore only open a port, if necessary.

To block access to a system service port:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. Under the Firewall pane, click **System Services**.
3. Under **Open System Service Port**, clear a system service to close a port.
4. Click **OK**.

Configure a new system service port

From the System Services pane, you can add a new system service port which, in turn, you can open or close to allow or deny remote access to a network service on your computer. An open system service port can make your computer vulnerable to Internet security threats, therefore only open a port when necessary.

To create and configure a new system service port:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **System Services**.
3. Click **Add**.
4. Under **Add Port Configuration**, specify the following:
   - Program name
   - Inbound TCP/IP ports
   - Outbound TCP/IP ports
   - Inbound UDP ports
   - Outbound UDP ports
5. Optionally describe the new configuration.
6. Click **OK**.

   The newly configured system service port appears under **Open System Service Port**.

Modify a system service port

An open and closed port allows and denies access to a network service on your computer. From the System Services pane, you can modify inbound and outbound information for an existing port. If port information is entered incorrectly, the system service fails.

To modify a system service port:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **System Services**.
3. Select a system service, and click **Edit**.
4. Under **Add Port Configuration**, specify the following:
   - Program name
   - Inbound TCP/IP ports
   - Outbound TCP/IP ports
   - Inbound UDP ports

- Outbound UDP ports

5 Optionally describe the modified configuration.

6 Click **OK**.

The modified configure system service port appears under **Open System Service**.

Remove a system service port

An open or closed port allows or denies access to a network service on your computer. From the System Services pane, you can remove an existing port and associated system service. After a port and system service is removed from the System Services pane, remote computers are no longer able to access the network service on your computer.

To remove a system service port:

1 On the Internet & Network Configuration pane, click **Advanced**.

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

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

4 On the **System Services** dialog, click **Yes** to confirm that you want to delete the system service.

The system service port no longer appears in the System Services pane.

CHAPTER 22

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 in the Trusted and Banned IPs pane, under **Trusted IP Addresses**.

The **Trusted IP Addresses** list on the Trusted and Banned IPs pane lets you allow 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. Firewall does not log any events from trusted IP addresses. Activity between the computer associated with a trusted IP address and your computer is not filtered or analyzed by Firewall.

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 use Firewall to add a trusted computer connection and its associated IP address.

The **Trusted IP Addresses** list on the Trusted and Banned IPs pane lets you allow 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.

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To add a trusted computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.
4. Click **Add**.
5. Under **Add Trusted IP Address Rule**, do one of the following:
   - Select a **Single IP Address**, and then enter the IP address.

- Select an **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 In the Add Trusted IP Address Rule dialog, click **Yes** to confirm that you want to add the trusted computer connection.

The newly added IP address appears under **Trusted IP Addresses**.

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.

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To add a trusted computer connection from 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 **Inbound Events**.

4 On the Inbound Events pane, select a source IP address, and then click **Trust this address**.

5 In the Add Trusted IP Address Rule dialog, click **Yes** to confirm that you want to trust the IP address.

The newly added IP address appears under **Trusted IP Addresses**.

Related topics

- Event Logging (page 158)

Edit a trusted computer connection

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

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To edit a trusted computer connection:

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

   The modified IP address appears under **Trusted IP Addresses**.

Remove a trusted computer connection

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

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To remove a trusted computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.
4. Select an IP address, and then click **Remove**.
5. In the **Trusted and Banned IPs** dialog, click **Yes** to confirm that you want to remove the trusted IP address under **Trusted IP Addresses**.

Banning computer connections

You can add, edit, and remove trusted 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 use Firewall to add a banned computer connection and its associated IP address.

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.

To add a banned computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Banned IP Addresses**.
4. Click **Add**.
5. Under Add Banned IP Address Rule, do one of the following:
   - Select a **Single IP Address**, and then enter the IP address.
   - Select an **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** fields.

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

7 Optionally, type a description of the rule.

8 Click **OK**.

9 On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm that you want to add the banned computer connection.

The newly added IP address appears under **Banned IP Addresses**.

Edit a banned computer connection

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

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.

To edit a banned computer connection:

1 From the Internet & Network Configuration pane, click **Advanced**.

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

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

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

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

- Select a **Single IP Address**, and then type the IP address.
- Select an **IP Address Range**, then type the starting and ending IP addresses in the **From IP Address** and **To IP Address** fields.

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

7 Optionally, type a description of the rule.

Click **OK**. The modified IP address appears under **Banned IP Addresses**.

Remove a banned computer connection

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

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.

To remove a banned computer connection:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Banned IP Addresses**.
4. Select an IP address, and click **Remove**.
5. On the **Trusted and Banned IPs** dialog, click **Yes** to confirm that you want to remove the IP address from **Banned IP Addresses**.

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 use ports that are deliberately opened or unless your computer includes a program that has been granted 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.

To ban a trusted computer connection from 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 **Inbound Events**.
4. In the Inbound Events pane, select a source IP address, and then click **Ban this address**.
5. On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm that you want to ban the IP address.

   The newly added IP address appears under **Banned IP Addresses**.

Related topics

- Event Logging (page 158)

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.

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.

To ban a computer connection from 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**.
4. In the Intrusion Detection Events pane, select a source IP address, and then click **Ban this address**.
5. On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm that you want to ban the IP address.

   The newly added IP address appears under **Banned IP Addresses**.

Related topics

- Event Logging (page 158)

CHAPTER 23

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 specify whether you want to enable or disable logging and, when enabled, which event types to log. Event logging allows you to view recent inbound and outbound events. You can also view intrusion detected events.

Configure event log settings

To track firewall events and activity, you can specify and configure the types of events to view.

To configure event logging:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Event Log Settings**.
3. On the Event Log Settings pane, do one of the following:
   - Select **Log the event** to enable event logging.
   - Select **Do not log the event** to disable event logging.
4. Under **Event Log Settings**, specify which events types to log. Event types include the following:
   - 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. The Recent Events pane only displays activity for programs that have been explicitly blocked from accessing the Internet.

To view Firewall's recent events:

- 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 and sort inbound events.

The Inbound Events log includes the following logging categories:

- Date and time
- Source IP address
- Host name
- Information and event type

To view your firewall's inbound events:

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 **Inbound Events**.

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

Related topics

- Add a trusted computer from the Inbound Events log (page 149)
- Ban a computer from the Inbound Events log (page 155)
- Trace a computer from the Inbound Events log (page 163)

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.

To view your firewall's outbound events:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.

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

Related topics

- Grant full access from the Outbound Events log (page 134)
- Grant outbound-only access from the Outbound Events log (page 136)
- Get program information from the Outbound Events log (page 141)

View intrusion detection events

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

To view your intrusion detection events:

1. Under 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.

Related topics

- Ban a computer from the Intrusion Detection Events log (page 156)
- Trace a computer from the Intrusion Detection Events log (page 164)

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.

To view global security statistics:

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

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.

To view worldwide port activity:

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.

To geographically locate a computer:

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.

To obtain a computer's domain information:

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.

To obtain a computer's network information:

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.

To trace a computer's IP address from 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 **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**.

Related topics

- Tracing Internet traffic (page 162)
- View inbound events (page 159)

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.

To trace a computer's IP address from 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**. In 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**.

Related topics

- Tracing Internet traffic (page 162)
- Logging, monitoring, and analysis (page 157)

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.

To monitor program bandwidth use:

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**.

Related topics

- Monitoring Internet traffic (page 166)

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.

Related topics

- Analyze inbound and outbound traffic (page 167)

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.

To analyze inbound and outbound traffic:

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**.

Related topics

- About the Traffic Analysis graph (page 166)

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.

To monitor program bandwidth use:

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.

To monitor program bandwidth use:

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 24

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.

To launch the HackerWatch tutorial:

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 25

McAfee Data Backup

Use Data Backup to avoid accidental loss of your data by archiving your files to CD, DVD, USB drive, external hard drive, or network drive. Local archiving allows you to archive (back up) your personal data to CD, DVD, USB drive, external hard drive, or network drive. This provides you with a local copy of your records, documents, and other materials of personal interest in case of accidental loss.

Before you begin using Data Backup, you can familiarize yourself with some of the most popular features. Details about configuring and using these features are provided throughout the Data Backup help. After browsing the program's features, you must ensure that you have adequate archive media available to perform local archives.

In this chapter

Features

Data Backup provides the following features to save and restore your photos, music, and other important files.

Local scheduled archiving

Protect your data by archiving files and folders to CD, DVD, USB drive, external hard drive, or network drive. After you initiate the first archive, incremental archives occur automatically for you.

One-click restore

If files and folders are mistakenly deleted or become corrupt on your computer, you can restore the most recently archived versions from the archive media used.

Compression and encryption

By default, your archived files are compressed, which saves space on your archive media. As an additional security measure, your archives are encrypted by default.

CHAPTER 26

Archiving files

You can use McAfee Data Backup to archive a copy of the files on your computer to CD, DVD, USB drive, external hard drive, or network drive. Archiving your files in this way makes it easy for you to retrieve information in case of accidental data loss or damage.

Before you start archiving files, you must choose your default archive location (CD, DVD, USB drive, external hard drive, or network drive). McAfee has preset some other settings; for example, the folders and file types that you want to archive, but you can modify those settings.

After you set the local archive options, you can modify the default settings for how often Data Backup runs full or quick archives. You can run manual archives at any time.

In this chapter

Setting archive options

Before you start archiving your data, you must set some local archive options. For example, you must set up the watch locations and watch file types. Watch locations are the folders on your computer that Data Backup monitors for new files or file changes. Watch file types are the types of files (for example, .doc, .xls, and so on) that Data Backup archives within the watch locations. By default, Data Backup watches all file types stored in your watch locations.

You can set up two types of watch locations: deep watch locations and shallow watch locations. If you set up a deep watch location, Data Backup archives the watch file types within that folder and its subfolders. If you set up a shallow watch location, Data Backup archives the watch file types within that folder only (not its subfolders).You can also identify locations that you want to exclude from the local archive. By default, the Windows Desktop and My Documents locations are set up as deep watch locations.

After you set up your watch file types and locations, you must set up the archive location (that is, the CD, DVD, USB drive, external hard drive, or network drive where archived data will be stored). You can change the archive location at any time.

For security reasons or size issues, encryption or compression are enabled by default for your archived files. The content of encrypted files is transformed from text to code, obscuring the information to make it unreadable by people who do not know how to decrypt it. Compressed files are compressed into a form that minimizes the space required to store or transmit it. Although McAfee does not recommend doing so, you can disable encryption or compression at any time.

Include a location in the archive

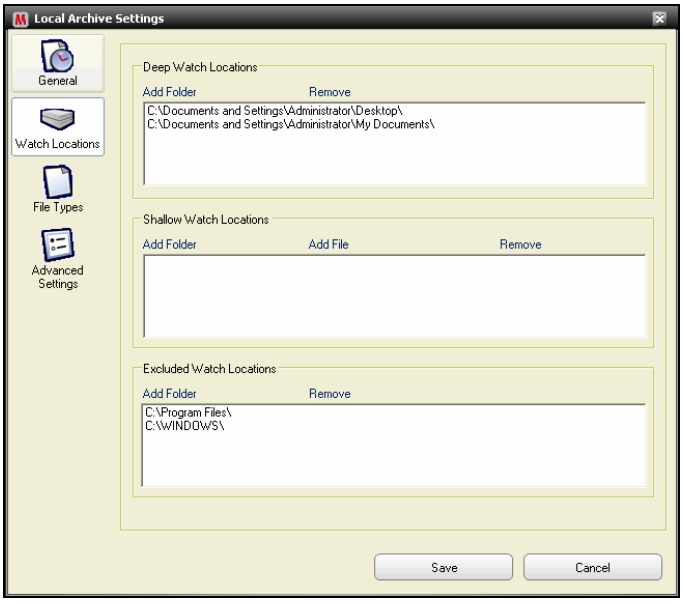
You can set two types of watch locations for archiving: deep and shallow. If you set a deep watch location, Data Backup monitors the contents of the folder and its subfolders for changes. If you set a shallow watch location, Data Backup monitors the contents of folder only (not its subfolders).

To include a location in the archive:

1 Click the **Local Archive** tab.

2 In the left pane, click **Settings**.

3 In the Local Archive Settings dialog box, click **Watch Locations**.



4 Do one of the following:

- To archive the contents of a folder, including the contents of its subfolders, click **Add Folder** under **Deep Watch Locations**.
- To archive the contents of a folder, but not the contents of its subfolders, click **Add Folder** under **Shallow Watch Locations**.

5 In the Browse For Folder dialog box, navigate to the folder that you want to watch, and then click **OK**.

6 Click **Save**.

Tip: If you want Data Backup to watch a folder that you have not yet created, you can click **Make New Folder** in the Browse For Folder dialog box to add a folder and set it as a watch location at the same time.

Set archive file types

You can specify which types of files are archived within your deep or shallow watch locations. You can choose from an existing list of file types or add a new type to the list.

To set archive file types:

1. Click the **Local Archive** tab.
2. In the left pane, click **Settings**.
3. In the Local Archive Settings dialog box, click **File Types**.
4. Expand the file types lists, and select the check boxes beside the file types that you want to archive.
5. Click **Save**.

Tip: To add a new file type to the **Selected File Types** list, type the file extension in the **Add Custom File Type to 'Other'** box, and then click **Add**. The new file type automatically becomes a watch file type.

Exclude a location from the archive

You exclude a location from the archive if you want to prevent that location (folder) and its contents from being archived.

To exclude a location from the archive:

1. Click the **Local Archive** tab.
2. In the left pane, click **Settings**.
3. In the Local Archive Settings dialog box, click **Watch Folders**.
4. Click **Add Folder** under **Excluded Watch Locations**.
5. In the Browse For Folder dialog box, navigate to the folder that you want to exclude, select it, and then click **OK**.
6. Click **Save**.

Tip: If you want Data Backup to exclude a folder that you have not yet created, you can click **Make New Folder** in the Browse For Folder dialog box to add a folder and exclude it at the same time.

Change the archive location

When you change the archive location, files previously archived in a different location are listed as *Never Archived*.

To change the archive location:

1. Click the **Local Archive** tab.
2. In the left pane, click **Settings**.
3. Click **Change Archive Location**.
4. In the Archive Location dialog box, do one of the following:
   - Click **Select CD/DVD Writer**, click your computer's CD or DVD drive in the **Writer** list, and then click **Save**.
   - Click **Select Drive Location**, navigate to a USB drive, local drive, or external hard drive, select it, and then click **OK**.
   - Click **Select Network Location**, navigate to a network folder, select it, and then click **OK**.
5. Verify the new archive location under **Selected Archive Location**, and then click **OK**.
6. In the confirmation dialog box, click **OK**.
7. Click **Save**.

Disable archive encryption and compression

Encrypting archived files protects the confidentiality of your data by obscuring the content of the files so that they are unreadable. Compressing archived files helps to minimize the size of the files. By default, both encryption and compression are enabled; however, you can disable these options at any time.

To disable archive encryption and compression:

1. Click the **Local Archive** tab.
2. In the left pane, click **Settings**.
3. In the Local Archive Settings dialog box, click **Advanced Settings**.
4. Clear the **Enable encryption to increase security** check box.
5. Clear the **Enable compression to reduce storage** check box.
6. Click **Save**.

Note: McAfee recommends that you do not disable encryption and compression when archiving your files.

Running full and quick archives

You can run two types of archive: full or quick. When you run a full archive, you archive a complete set of data based on the watch file types and locations that you have set up. When you run a quick archive, you archive only those watched files that have changed since the last full or quick archive.

By default, Data Backup is scheduled to run a full archive of the watch file types in your watch locations every Monday at 9:00 a.m and a quick archive every 48 hours after the last full or quick archive. This schedule ensures that a current archive of your files is maintained at all times. However, if you do not want to archive every 48 hours, you can adjust the schedule to suit your needs.

If you want to archive the contents of your watch locations on demand, you can do so at any time. For example, if you modify a file and want to archive it, but Data Backup is not scheduled to run a full or quick archive for another few hours, you can archive the files manually. When you archive files manually, the interval that you set for automatic archives is reset.

You can also interrupt an automatic or manual archive if it occurs at an inappropriate time. For example, if you are performing a resource-intensive task and an automatic archive starts, you can stop it. When you stop an automatic archive, the interval that you set for automatic archives is reset.

Schedule automatic archives

You can set the frequency of full and quick archives to ensure that your data is always protected.

To schedule automatic archives:

1. Click the **Local Archive** tab.
2. In the left pane, click **Settings**.
3. In the Local Archive Settings dialog box, click **General**.
4. To run a full archive each day, week, or month, click one of the following under **Full archive every**:
   - **Day**
   - **Week**
   - **Month**

5 Select the check box beside the day on which you want to run the full archive.

6 Click a value in the **At** list to specify the time at which you want to run the full archive.

7 To run a quick archive on a daily or hourly basis, click one of the following under **Quick Archive**:

- **Hours**
- **Days**

8 Type a number representing the frequency in the **Quick archive every** box.

9 Click **Save**.

Interrupt an automatic archive

Data Backup automatically archives the files in your watch locations according to the schedule that you define. However, if an automatic archive is in progress and you want to interrupt it, you can do so at any time.

To interrupt an automatic archive:

1 In the left pane, click **Stop Archiving**.

2 In the confirmation dialog box, click **Yes**.

Note: The **Stop Archiving** link only appears when an archive is in progress.

Run archives manually

Although automatic archives run according to a predefined schedule, you can run a quick or full archive manually at any time. A quick archive archives only those files that have changed since the last full or quick archive. A full archive archives the watch file types in all watch locations.

To run a quick or full archive manually:

1 Click the **Local Archive** tab.

2 To run a quick archive, click **Quick Archive** in the left pane.

3 To run a full archive, click **Full Archive** in the left pane.

4 In the Ready to start archival dialog box, verify your storage space and settings, and then click **Continue**.

CHAPTER 27

Working with archived files

After you archive some files, you can use Data Backup to work with them. Your archived files are presented to you in a traditional explorer view which allows you to locate them easily. As your archive grows, you might want to sort the files or search for them. You can also open files directly in the explorer view to examine the content without having to retrieve the files.

You retrieve files from an archive if your local copy of the file is out of date, is missing, or becomes corrupt. Data Backup also provides you with the information you need to manage your local archives and storage media.

In this chapter

Using the local archive explorer

The local archive explorer allows you to view and manipulate the files that you have archived locally. You can view each file's name, type, location, size, state (archived, not archived, or archive in progress), and the date on which each file was last archived. You can also sort the files by any of these criteria.

If you have a large archive, you can find a file quickly by searching for it. You can search for all or part of a file's name or path and can then narrow your search by specifying the approximate file size and the date on which it was last archived.

After you locate a file, you can open it directly in the local archive explorer. Data Backup opens the file in its native program, allowing you to make changes without leaving the local archive explorer. The file is saved to the original watch location on your computer and is archived automatically according to the archive schedule you have defined.

Sort archived files

You can sort your archived files and folders by the following criteria: name, file type, size, state (that is, archived, not archived, or archive in progress), the date on which the files were last archived, or the location of the files on your computer (path).

To sort archived files:

1. Click the **Local Archive** tab.
2. In the right pane, click a column name.

Search for an archived file

If you have a large repository of archived files, you can find a file quickly by searching for it. You can look for all or part of a file's name or path and can then narrow your search by specifying the approximate file size and the date on which it was last archived.

To search for an archived file:

1. Type all or part of the file name in the **Search** box at the top of the screen, and then press ENTER.
2. Type all or part of the path in the **All or part of the path** box.
3. Specify the approximate size of the file that you are searching for by doing one of the following:
   - Click **<100 KB**, **<1 MB**, or **>1 MB**.
   - Click **Size in KB**, and then specify the appropriate size values in the boxes.

4 Specify the approximate date of the file's last online backup by doing one of the following:
   - Click **This Week**, **This Month**, or **This Year**.
   - Click **Specify Dates**, click **Archived** in the list, and then click the appropriate date values from the date lists.
5 Click **Search**.

Note: If you do not know the approximate size or date of the last archive, click **Unknown**.

Open an archived file

You can examine the content of an archived file by opening it directly in the local archive explorer.

To open archived files:

1 Click the **Local Archive** tab.
2 In the right pane, click a file name, and then click **Open**.

Tip: You can also open an archived file by double-clicking the file name.

Restoring archived files

If a watch file becomes corrupt, is missing, or is mistakenly deleted, you can restore a copy of it from a local archive. For this reason, it is important to ensure that you archive your files regularly. You can also restore older versions of files from a local archive. For example, if you regularly archive a file, but want to revert to a previous version of a file, you can do so by locating the file in the archive location. If the archive location is a local drive or network drive, you can browse for the file. If the archive location is an external hard drive or USB drive, you must connect the drive to the computer, and then browse for the file. If the archive location is a CD or DVD, you must insert the CD or DVD in the computer, and then browse for the file.

You can also restore files that you have archived on one computer from a different computer. For example, if you archive a set of files to an external hard drive on computer A, you can restore those files on computer B. To do so, you must install McAfee Data Backup on computer B and connect the external hard drive. Then, in Data Backup, you browse for the files and they are added to the **Missing Files** list for restoration.

For more information about archiving files, see Archiving files. If you delete a watch file from your archive intentionally, you can also delete the entry from the **Missing Files** list.

Restore missing files from a local archive

Data Backup's local archive allows you to recover data that is missing from a watch folder on your local computer. For example, if a file is moved out of a watch folder or deleted, and has already been archived, you can restore it from the local archive.

To retrieve a missing file from a local archive:

1. Click the **Local Archive** tab.
2. On the **Missing Files** tab at the bottom of the screen, select the check box beside the name of the file that you want to restore.
3. Click **Restore**.

Tip: You can restore all the files in the **Missing Files** list by clicking **Restore All**.

Restore an older version of a file from a local archive

If you want to restore an older version of an archived file, you can locate it and add it to the **Missing Files** list. Then, you can restore the file, as you would any other file in the **Missing Files** list.

To restore an older version of a file from a local archive:

1. Click the **Local Archive** tab.
2. On the **Missing Files** tab at the bottom of the screen, click **Browse**, and then navigate to the location where the archive is stored.

   Archived folder names have the following format: `cre ddmmyy_hh-mm-ss_***`, where `ddmmyy` is the date on which the files were archived, `hh-mm-ss` is the time on which the files were archived, and `***` is either `Full` or `Inc`, depending on whether a full or quick archive was performed.
3. Select the location, and then click **OK**.

   Files contained in the selected location appear in the **Missing Files** list, ready to be restored. For more information, see Restore missing files from a local archive.

Remove files from the missing files list

When an archived file is moved out of a watch folder or deleted, it automatically appears in the **Missing Files** list. This alerts you to the fact that there is an inconsistency between the files archived and the files contained in the watch folders. If the file was moved out of the watched folder or deleted intentionally, you can delete the file from the **Missing Files** list.

To remove a file from the Missing Files list:

1. Click the **Local Archive** tab.
2. On the **Missing Files** tab at the bottom of the screen, select the check box beside the name of the file that you want to remove.
3. Click **Delete**.

Tip: You can remove all the files in the **Missing Files** list by clicking **Delete All**.

Managing archives

You can view a summary of information about your full and quick archives at any time. For example, you can view information about the amount of data currently being watched, the amount of data that has been archived, and the amount of data that is currently being watched but has not yet been archived. You can also view information about your archive schedule, such as the date on which the last and next archives occur.

View a summary of your archive activity

You can view information about your archive activity at any time. For example, you can view the percentage of files that have been archived, the size of the data being watched, the size of the data that has been archived, and the size of the data that is being watched but has not yet been archived. You can also view the dates on which the last and next archives occur.

To view a summary of your backup activity:

1. Click the **Local Archive** tab.
2. At the top of the screen, click **Account Summary**.

CHAPTER 28

McAfee EasyNetwork

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

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

In this chapter

Features

EasyNetwork provides the following features.

File sharing

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

File transfer

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

Automated printer sharing

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

CHAPTER 29

Setting up EasyNetwork

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

In this chapter

Launching EasyNetwork

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

Launch EasyNetwork

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

To launch EasyNetwork:

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

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

Joining a managed network

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

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

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

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

Join the network

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

To join the network:

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

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

Grant access to the network

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

To grant access to the network:

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

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

2 Click **Grant Access**.

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

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

Rename the network

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

To rename the network:

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

Leaving a managed network

If you join a managed network and then determine that you no longer want to be a member, you can leave the network. After you relinquish your membership, you can rejoin at any time; however, you must be granted permission to join and peform the security check again. For more information, see Joining a managed network (page 191).

Leave a managed network

You can leave a managed network that you previously joined.

To leave a managed network:

1. On the **Tools** menu, click **Leave Network**.
2. In the Leave Network dialog box, select the name of the network that you want to leave.
3. Click **Leave Network**.

CHAPTER 30

Sharing and sending files

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

In this chapter

Sharing files

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

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

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

Share a file

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

To share a file:

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

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

Stop sharing a file

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

To stop sharing a file:

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

Copy a shared file

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

To copy a file:

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

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

Search for a shared file

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

To search for a shared file:

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

3 Type part or all of the file name or path in the **File or Path Name** list.

4 Click one of the following file types in the **Type** list:

- **Any**: Searches all of the shared file types.
- **Document**: Searches all of the shared documents.
- **Image**: Searches all of the shared image files.
- **Video**: Searches all of the shared video files.
- **Audio**: Searches all of the shared audio files.

5 In the **From** and **To** lists, click dates representing the range of dates on which the file was created.

Sending files to other computers

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

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

Send a file to another computer

You can send a file directly to another computer on the managed network without sharing it. Before a user on the recipient computer can view the file,it must be saved to a local location. For more information, see Accept a file from another computer (page 202).

To send a file to another computer:

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

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

Accept a file from another computer

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

To receive a file from another computer:

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

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

Receive notification when a file is sent

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

To receive notification when a file is sent:

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

CHAPTER 31

Sharing printers

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

In this chapter

Working with shared printers

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

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

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

Stop sharing a printer

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

To stop sharing a printer:

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

Install an available network printer

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

To install an available network printer:

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

CHAPTER 32

Reference

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

About McAfee provides legal information about McAfee Corporation.

Glossary

8

802.11

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

802.11a

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

802.11b

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

802.11g

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

802.1x

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

A

Access Point (AP)

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

archive

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

archive

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

authentication

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

B

back up

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

bandwidth

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

blacklist

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

browser

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

brute-force attack

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

buffer overflow

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

C

cipher text

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

client

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

compression

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

content-rating groups

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

cookie

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

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

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

D

deep watch location

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

Denial of Service

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

dictionary attack

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

DNS

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

DNS server

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

domain

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

E

e-mail

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

e-mail client

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

encryption

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

ESS (Extended Service Set)

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

event

Events from 0.0.0.0

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

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

Events from 127.0.0.1

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

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

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

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

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

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

Events from computers on your LAN

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

Events from private IP addresses

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

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

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

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

external hard drive

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

firewall

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

full archive

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

header

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

hotspot

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

image analysis

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

integrated gateway

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

Internet

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

intranet

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

IP address

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

The following lists some unusual IP address types:

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

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

IP spoofing

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

key

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

keyword

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

LAN (Local Area Network)

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

library

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

MAC (Media Access Control or Message Authenticator Code)

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

MAC Address (Media Access Control Address)

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

man-in-the-middle attack

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

managed network

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

MAPI account

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

MSN account

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

network

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

network drive

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

network map

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

NIC (Network Interface Card)

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

node

A single computer connected to a network.

online backup repository

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

parental controls

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

password

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

Password Vault

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

PCI wireless adapter cards

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

phishing

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

plain text

Any message that is not encrypted.

pop-ups

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

POP3 account

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

port

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

potentially unwanted program

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

PPPoE

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

protocol

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

proxy

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

proxy server

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

publish

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

quarantine

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

quick archive

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

RADIUS (Remote Access Dial-In User Service)

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

real-time scanning

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

restore

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

roaming

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

rogue access points

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

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

router

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

script

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

server

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

shallow watch locations

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

share

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

shared secret

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

SMTP server

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

SSID (Service Set Identifier)

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

SSL (Secure Sockets Layer)

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

standard e-mail account

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

synchronize

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

SystemGuard

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

TKIP (Temporal Key Integrity Protocol)

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

Trojan

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

URL

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

USB wireless adapter cards

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

VPN (Virtual Private Network)

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

wardriver

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

watch file types

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

watch locations

The folders on your computer that Data Backup monitors.

Web bugs

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

WEP (Wired Equivalent Privacy)

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

whitelist

A list of Web sites that are allowed to be accessed because they are not considered fraudulent.

Wi-Fi (Wireless Fidelity)

Used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is used by the Wi-Fi Alliance.

Wi-Fi Alliance

An organization made up of leading wireless equipment and software providers with the mission of (1) certifying all 802.11-based products for inter-operability and (2) promoting the term Wi-Fi as the global brand name across all markets for any 802.11-based wireless LAN products. The organization serves as a consortium, testing laboratory, and clearinghouse for vendors who want to promote inter-operability and the growth of the industry.

While all 802.11a/b/g products are called Wi-Fi, only products that have passed the Wi-Fi Alliance testing are allowed to refer to their products as Wi-Fi Certified (a registered trademark). Products that pass are required to carry an identifying seal on their packaging that states Wi-Fi Certified and indicates the radio frequency band used. This group was formerly known as the Wireless Ethernet Compatibility Alliance (WECA) but changed its name in October 2002 to better reflect the Wi-Fi brand it wants to build.

Wi-Fi Certified

Any products tested and approved as Wi-Fi Certified (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a Wi-Fi Certified product can use any brand of access point (AP) with any other brand of client hardware that also is certified. Typically, however, any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 11g, 5GHz for 802.11a) works with any other, even if not Wi-Fi Certified.

wireless adapter

Contains the circuitry to enable a computer or other device to communicate with a wireless router (attach to a wireless network). Wireless adapters can be built into the main circuitry of a hardware device or they can be a separate add-on that can be inserted into a device through the appropriate port.

WLAN (Wireless Local Area Network)

See also LAN. A local area network using a wireless medium for connection. A WLAN uses high-frequency radio waves rather than wires to communicate between nodes.

worm

A worm is a self-replicating virus that resides in active memory and can send copies of itself through e-mail messages. Worms replicate and consume system resources, slowing performance or halting tasks.

WPA (Wi-Fi Protected Access)

A specification standard that strongly increases the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, WPA is derived from, and is compatible with, the IEEE 802.11i standard. When properly installed, it provides wireless LAN users with a high level of assurance that their data remains protected and that only authorized network users can access the network.

WPA-PSK

A special WPA mode designed for home users who do not require strong enterprise-class security and do not have access to authentication servers. In this mode, the home user manually enters the starting password to activate Wi-Fi Protected Access in Pre-Shared Key mode, and should change the pass-phrase on each wireless computer and access point regularly. See also WPA2-PSK and TKIP.

WPA2

See also WPA. WPA2 is an update of the WPA security standard and is based on the 802.11i IEEE standard.

WPA2-PSK

See also WPA-PSK and WPA2. WPA2-PSK is similar to WPA-PSK and is based on the WPA2 standard. A common feature of WPA2-PSK is that devices often support multiple encryption modes (e.g., AES, TKIP) simultaneously, while older devices generally supported only a single encryption mode at a time (i.e., all clients would have to use the same encryption mode).

About McAfee

McAfee, Inc., headquartered in Santa Clara, California and the global leader in Intrusion Prevention and Security Risk Management, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security.

Copyright

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W