

McAfee®
VirusScan USB

User Guide

Contents

McAfee VirusScan USB	3
Features	4
Installing and updating VirusScan USB	5
Install VirusScan USB	6
Update VirusScan USB	8
Setting scan options	9
Set scanned file types	10
Set the locations to scan	11
Disable real-time monitoring	12
Start a scan on insertion	13
Disable antivirus software detection	13
Show informational messages	14
Working with alerts	15
About alerts	15
Scanning your USB device	17
Scan your USB device	18
Pause scanning	18
Resume scanning	19
Cancel scanning	19
Working with scan results	21
View the results of a scan	22
Delete an infected file	23
View the last scan summary	23
View the VirusScan USB program summary	24
Protecting your computer	25
Download antivirus software for your computer	25
Renewing your VirusScan USB subscription	27
Renew your VirusScan USB subscription	27
Frequently Asked Questions	29
A threat has been detected. What should I do?	29

Do I need to be connected to the Internet to scan?.....	29
Does VirusScan USB scan zipped files?.....	30
How do I get more help from McAfee?	30
Glossary	31
<hr/>	
About McAfee	33
Copyright.....	34
Index	35

CHAPTER 1

McAfee VirusScan USB

VirusScan USB offers comprehensive, reliable, and up-to-date virus protection for your USB device. Powered by award-winning McAfee scanning technology, VirusScan USB protects the contents of your USB device against viruses and Trojan horses.

In this chapter

Features4

Features

VirusScan USB provides the following features.

Real-time monitoring

When enabled, the VirusScan USB real-time monitor constantly monitors your USB device for file changes (for example, a new file added to the device or a modification made to a file already on the device). If the real-time monitor detects a file change, VirusScan USB scans the affected file for virus activity. If a virus or Trojan is detected, VirusScan USB tries to clean it; if it cannot be cleaned, VirusScan USB tries to rename it. By default, real-time monitoring is enabled.

On-demand scanning

On-demand scanning lets you scan your USB device for viruses and Trojans at any time. For example, if you just added a program or file to your USB device, you can scan the device to ensure that the program or file is not infected. If a virus or Trojan is detected, VirusScan USB tries to clean it; if it cannot be cleaned, VirusScan USB tries to rename it.

CHAPTER 2

Installing and updating VirusScan USB

Install VirusScan USB on your USB device the same way that you install most other U3 USB programs, with the exception that you must register with McAfee. Registering allows you to receive VirusScan USB program and virus definition file updates when they become available. If you are registering with McAfee for the first time, you must provide your name, a valid e-mail address, and a password. If you have already registered with McAfee, you can log in using the e-mail address and password that you provided during the previous registration.

After installing and registering VirusScan USB, you can update it with the latest virus protection files (DATs) at any time. Updates run in the background--you can even run a scan or close the program while an update is in progress. If real-time monitoring is enabled, VirusScan USB launches an automatic update every four hours. For more information about real-time monitoring, see Setting scan options (page 9).

Note: If your USB device comes with an antivirus program already installed, McAfee recommends that you remove that program before installing VirusScan USB.

In this chapter

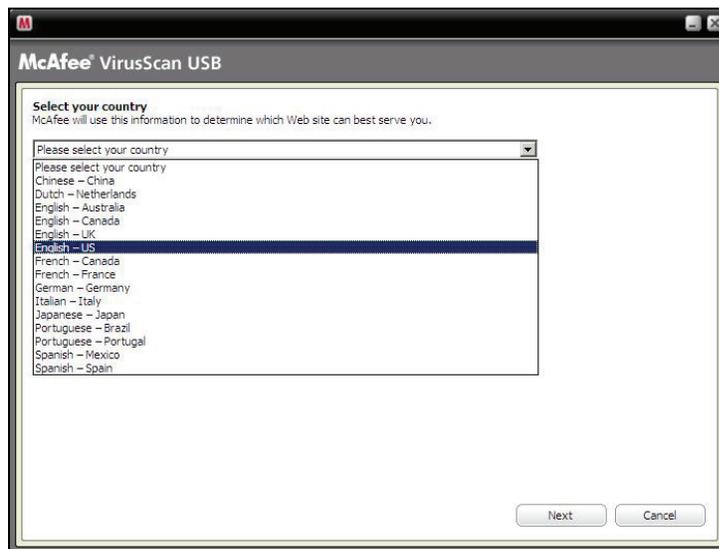
Install VirusScan USB	6
Update VirusScan USB	8

Install VirusScan USB

Install VirusScan USB on your USB device the same way that you install most other U3 USB programs, with the exception that you must register with McAfee. Registering allows you to receive VirusScan USB program and virus definition file updates when they become available.

To install VirusScan USB:

- 1 Insert your USB device in your computer.
- 2 On the U3 Launchpad, click **Add Programs**, and then click **Install from my computer**.
- 3 In the Open dialog box, navigate to the folder where the installation file is stored, select the file, and then click **Open**.
- 4 In the Add Program Wizard, click **Next**.
- 5 In the Select your country dialog box, click the country and language combination that best represents your current location, and then click **Next**.



- 6 In the Program Setup dialog box, review the privacy policy, and then click **Next**.
- 7 In the McAfee User License Agreement dialog box, select a country, review the user license agreement, and then click **Accept**.
- 8 Do one of the following:
 - If you are registering for the first time, type your first name, last name, e-mail address, password, and password confirmation in the appropriate boxes, and then click **Submit**.

- If you have previously registered a program with McAfee, click **Log In**, type the e-mail address and password associated with your McAfee account, and then click **Log In**.



The image shows a screenshot of the McAfee VirusScan USB registration dialog box. The window title is "McAfee VirusScan USB". It contains two main sections: "Current McAfee User" and "Create New McAfee Account".

Current McAfee User
If you already have a McAfee account, please log in.

Create New McAfee Account

First Name:
Last Name:
E-mail Address:
Password:
Re-enter Password:

At the bottom of the dialog box, there are three buttons: , , and .

- 9 In the Program Setup Completed dialog box, record your registration information, and then click **Finish**.

Note: You can also run the VirusScan USB installation file directly from a Web site. On the Web site, start the download and click **Yes** on any security warnings that appear asking if you want to download the file. Then run the installation file and follow the instructions provided in the installation wizard.

Update VirusScan USB

After you install VirusScan USB on your USB device, an update is launched automatically each time that you plug the device into your computer. You can also manually update VirusScan USB with the latest program and virus definition file updates at any time. Updates run in the background--you can even run a scan or close the program while an update is in progress.

To update VirusScan USB:

- 1 On the main VirusScan USB pane, click **Update**.



- 2 Click **OK**.

Note: In order to update VirusScan USB successfully, you must be connected to the Internet.

CHAPTER 3

Setting scan options

You can customize the behavior of VirusScan USB by setting scan options. For example, you can specify which types of files are scanned (archives, subfolders, and computer memory) and the locations to scan. You can also enable or disable real-time monitoring. When enabled, the VirusScan USB real-time monitor constantly monitors your USB device for file changes (for example, a new file added to the device or a modification made to a file already on the device). If the real-time monitor detects a file change, VirusScan USB scans the affected file for virus activity. If a virus or Trojan is detected, VirusScan USB tries to clean it; if it cannot be cleaned, VirusScan USB tries to rename it. By default, real-time monitoring is enabled and McAfee does not recommend that you disable it. When real-time monitoring is enabled, all file types are monitored; when you run an on-demand scan, VirusScan USB scans the file types and locations specified in your scan options. For more information about running an on-demand scan, see *Scanning your USB device* (page 17).

When you install VirusScan USB, it is automatically added to the program list on your U3 Launchpad and configured to start on insertion. This means that a VirusScan USB on-demand scan starts each time that you insert your USB device into your computer. If you disable the start on insertion option on your U3 Launchpad, a VirusScan USB on-demand scan starts the first time you insert your USB device into your computer only. You can then configure VirusScan USB to start scanning on insertion or not. If you configure VirusScan USB not to start scanning on insertion, VirusScan USB does not start until real-time monitoring detects an infection or you start it manually. McAfee does not recommend disabling the start scanning on insertion option in VirusScan USB.

VirusScan USB detects viruses and Trojans on your USB device and in your computer's memory, and it also detects whether you have up-to-date antivirus software installed on your computer. If you do not have up-to-date antivirus software installed on your computer, you are prompted to download a trial or full version of McAfee VirusScan to ensure that your computer is protected. When setting scan options, you can disable antivirus software detection, which prevents VirusScan USB from detecting whether up-to-date antivirus software is installed on your computer. Also, if you have hidden some alerts or other information dialog boxes, you can show them again.



In this chapter

Set scanned file types.....	10
Set the locations to scan	11
Disable real-time monitoring.....	12
Start a scan on insertion	13
Disable antivirus software detection	13
Show informational messages	14

Set scanned file types

You can specify which types of files on your USB device are scanned for viruses or Trojans during an on-demand scan. For example, you can determine whether subfolders and archives are scanned. You can also determine whether you want VirusScan USB to scan your computer's memory.

To set scanned file types:

- 1 In the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
- 2 In the Scan Options pane, under **Options**, select or clear the following check boxes:
 - **Scan subfolders:** Subfolders (folders contained within other folders) are scanned.
 - **Scan .zip and other archive files:** Archived files including .zip files are scanned.

- **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 memory:** Your computer's memory is scanned.
- 3 Click **OK**.

Set the locations to scan

You can specify the locations (USB drives) to scan during an on-demand scan. Because VirusScan USB only scans drives that are associated with your USB device, disk drives that are not associated with your device do not appear in the **Drives to scan on this USB device** list; these include removable drives on your computer and drives that are associated with other USB devices.

To set the locations to scan:

- 1 In the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
- 2 In the Scan Options pane, under **Drives to scan on this USB device**, select or clear the following check boxes:
 - **U3 System:** The CD-ROM partition on the device is scanned. This is the location where the U3 system files are stored.
 - **My U3 Drive:** The data partition on the device is scanned. This is the drive letter assigned to the USB drive.
- 3 Click **OK**.

Disable real-time monitoring

When enabled, the VirusScan USB real-time monitor constantly monitors your USB device for file changes (for example, a new file added to the device or a modification made to a file already on the device). If the real-time monitor detects a file change, VirusScan USB scans the file for virus activity. If a virus or Trojan is detected, VirusScan USB tries to clean it; if it cannot be cleaned, VirusScan USB tries to rename it. Real-time monitoring monitors all file types (regardless of your on-demand scan settings). McAfee does not recommend disabling real-time monitoring.

To disable real-time monitoring:

- 1 In the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
- 2 In the Scan Options pane, under **Real-time monitoring**, clear the **Enable real-time monitoring of USB device** check box.
- 3 Click **OK**.

Note: If real-time monitoring is enabled, it might detect an infected file while an on-demand scan is in progress. To ensure that the infection is reported at least once, real-time monitoring displays an alert as usual.

Start a scan on insertion

When you install VirusScan USB, it is automatically added to the program list on your U3 Launchpad and configured to start on insertion. This means that a VirusScan USB on-demand scan starts each time that you insert your USB device into your computer. If you disable the start on insertion option on your U3 Launchpad, a VirusScan USB on-demand scan starts the first time you insert your USB device into your computer. You can then configure VirusScan USB to start scanning on insertion or not. If you configure VirusScan not to start scanning on insertion, VirusScan USB does not start until real-time monitoring detects an infection or you start it manually. McAfee does not recommend disabling the start scanning on insertion option in VirusScan USB.

To start a scan on insertion:

- 1 In the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
- 2 In the Scan Options pane, under **Options**, ensure that the **Start scanning on insertion** check box is selected.
- 3 Click **OK**.

Tip: You can also select the **Start scanning on insertion** check box on the Scan Progress pane when a scan completes, is paused, or is canceled.

Disable antivirus software detection

By default, VirusScan USB detects whether you have up-to-date antivirus software on your computer; however, you can disable this detection.

To disable antivirus software detection:

- 1 In the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
- 2 In the Scan Options pane, under **Options**, clear the **Detect antivirus software on the host computer** check box.
- 3 Click **OK**.

Show informational messages

If you decide that you want to show some VirusScan USB alerts and dialog boxes that you chose to hide, you can do so.

To show informational messages:

- 1** In the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
- 2** In the Scan Options pane, under **Options**, select the **Show informational messages** check box.
- 3** Click **OK**.

CHAPTER 4

Working with alerts

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, based on the recommendations in the alerts.

In this chapter

About alerts..... 15

About alerts

VirusScan USB real-time monitoring has three basic alert types: red, yellow, and green.

Red alert

Red alerts indicate that an infected file was detected but could not be cleaned or renamed. These alerts allow you to remove the infected file from your USB device or ignore the infection.

Yellow alert

Yellow alerts indicate that an infected file was detected and could not be cleaned, but was renamed with the .vir extension. These alerts allow you to remove the infected file from your USB device or ignore the infection.

Green alert

Green alerts indicate that an infected file was detected and cleaned. Because these alerts are primarily informational, you can choose not to display them again.

CHAPTER 5

Scanning your USB device

When you install VirusScan USB, it is automatically added to the program list on your U3 Launchpad and configured to start on insertion. This means that a VirusScan USB on-demand scan starts each time that you insert your USB device into your computer. If you disable the start on insertion option on your U3 Launchpad, a VirusScan USB on-demand scan starts the first time you insert your USB device into your computer only. You can then configure VirusScan USB to start scanning on insertion or not. If you configure VirusScan not to start scanning on insertion, VirusScan USB does not start until real-time monitoring detects an infection or you can run an on-demand scan. When you run an on-demand scan, VirusScan USB scans the file types and locations specified in your scan options. For more information about setting on-demand scan options, see [Setting scan options](#) (page 9).

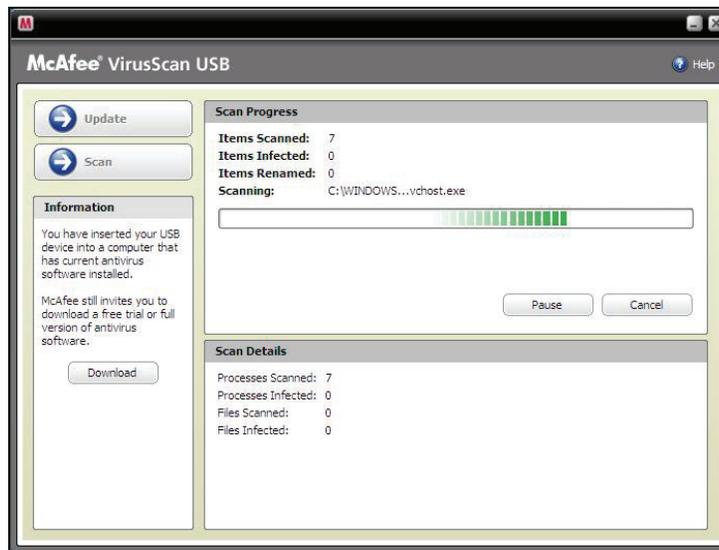
Note: McAfee does not recommend disabling the start scanning on insertion option in VirusScan USB.

When VirusScan USB detects a virus or Trojan in one of the files on your USB device, it performs one of the following operations:

- Clean: The virus or Trojan is removed from the file.
- Rename: The file is renamed with a .vir extension (if the clean operation fails).

If both the clean and rename operations fail, you can delete the infected file. For more information, see [Delete an infected file](#) (page 23).

After you start scanning your USB device, you can pause the scan, and then resume it from that point at a more appropriate time. For example, if you are performing a resource-intensive task when VirusScan USB is scanning, you can pause the scan, and then resume it when the other task is complete. You can also cancel a scan at any time.



In this chapter

Scan your USB device	18
Pause scanning.....	18
Resume scanning	19
Cancel scanning	19

Scan your USB device

You can scan your USB device at any time. For example, if you just installed VirusScan USB, you can perform a scan to ensure that your USB device does not have viruses or other threats.

To manually scan your USB device:

- In the VirusScan USB left pane, click **Scan**.

Pause scanning

You can pause a scan that is in progress. Pausing stops the scan at a specific point and allows you to resume the scan from that point when you are ready.

To pause scanning:

- In the Scan Progress pane, under **Scan Progress**, click **Pause**.

Tip: To resume scanning from the point where you paused it, click the **Resume** button.

Resume scanning

When you pause a scan, it is temporarily stopped. You can resume the scan from the point where it was paused. For more information about pausing a scan, see [Pause scanning](#) (page 18).

To resume scanning:

- In the Scan Progress pane, under **Scan Progress**, click **Resume**.

Cancel scanning

You can cancel (terminate) a scan at any time. Unlike pausing, you cannot resume a canceled scan.

To stop scanning:

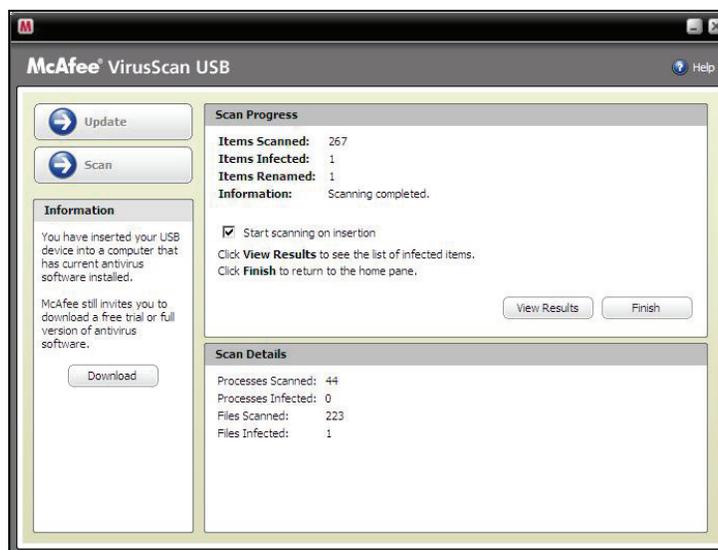
- In the Scan Progress pane, under **Scan Progress**, click **Cancel**, and then click **Finish**.

CHAPTER 6

Working with scan results

While a scan is running, VirusScan USB displays the number of items scanned, infected, and renamed above the scan progress bar. When an infection is detected and the scan completes, you can view a summary of your results, which include the path and name of each infected file, and the operation that was performed on that file (for example, cleaned or renamed). You can also view detailed information about each infected file, including the object type, name, status, and file name.

If VirusScan USB detects a virus or Trojan in one of the files on your USB device, it tries to clean the infected file. If the clean operation fails, VirusScan USB tries to rename the file. If both the clean and rename operations fail, you can delete the file from your USB device.



VirusScan USB also displays a summary of the last scan on the home pane so that you can review the processes scanned, processes infected, files scanned, files infected, and the date of the last scan.

In this chapter

View the results of a scan.....	22
Delete an infected file	23
View the last scan summary	23
View the VirusScan USB program summary	24

View the results of a scan

When a scan completes, you can view the results to see a list of infected items.

To view the results of a scan:

- 1 In the Scan Progress pane, under **Scan Progress**, click **View Results**.
- 2 In the Scan Results pane, click an infected file name.
- 3 Under **Details**, view more specific information about the infected file.
- 4 Click **Finish**.

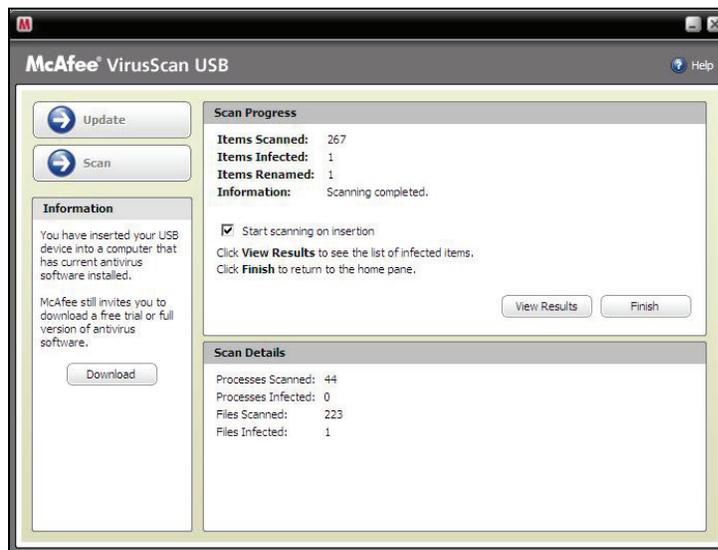
Note: The **View Results** button only appears when infected files have been detected.

Delete an infected file

If VirusScan USB detects a virus or Trojan in one of the files on your USB device, it tries to clean the infected file. If the clean operation fails, VirusScan USB tries to rename the file. If both the clean and rename operations fail, you can delete the file from your USB device.

To delete an infected file:

- 1 In the Scan Progress pane, under **Scan Progress**, click **View Results**.
- 2 In the Scan Results pane, click an infected file name.



- 3 Under **I want to**, click **Delete**.
- 4 Click **Finish**.

View the last scan summary

For your convenience, VirusScan USB displays a summary of the last scan on the home pane.

To view the last scan summary:

- In the VirusScan USB home pane, under **Last Scan Summary**, view the details.

View the VirusScan USB program summary

VirusScan USB displays the date when the last update check occurred and the current version of your virus definition files (DATs) on the home pane.

To view the VirusScan USB program summary:

- On the VirusScan USB home pane, under **Program Summary**, view the details.

CHAPTER 7

Protecting your computer

VirusScan USB does not monitor or scan the files stored on your computer. This protection is provided by McAfee VirusScan. You can download a full or trial version of McAfee VirusScan from the McAfee download site.

In this chapter

Download antivirus software for your computer25

Download antivirus software for your computer

If VirusScan USB is configured to detect whether up-to-date antivirus software is installed on your computer, and it detects that none exists, you are prompted to download a full or trial version of McAfee VirusScan.

To download antivirus software for your computer:

- 1 Under **Warning** or **Information** in the left pane, click **Download**.
- 2 Follow the on-screen instructions to download McAfee VirusScan.

Tip: You can also download VirusScan by clicking the link under **Drives to scan on this USB device** in the Scan Options pane.

CHAPTER 8

Renewing your VirusScan USB subscription

When your VirusScan USB subscription expires, VirusScan USB no longer functions and you cannot receive updates to the program or virus definition files (DATs). However, you can still access the main VirusScan USB home pane, which prompts you to renew your subscription.

Tip: If you renew a subscription before it expires, the remaining time is added to the new subscription period.

In this chapter

Renew your VirusScan USB subscription.....27

Renew your VirusScan USB subscription

When your VirusScan USB subscription expires, you are prompted to purchase a subscription each time the USB device is plugged in or each time you try to run the program. Although VirusScan USB does not scan your USB device or receive updates after your subscription expires, it allows you to renew your subscription.

To renew your VirusScan USB subscription:

- In the VirusScan USB home pane, under **Program Summary**, click **Renew**.

CHAPTER 9

Frequently Asked Questions

This chapter provides answers to the most frequently asked questions.

In this chapter

A threat has been detected. What should I do?.....	29
Do I need to be connected to the Internet to scan? ..	29
Does VirusScan USB scan zipped files?	30
How do I get more help from McAfee?	30

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, based on the recommendations in the alerts.

Do I need to be connected to the Internet to 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 USB scan zipped files?

VirusScan USB scans .zip files and other archived files.

How do I get more help from McAfee?

For additional help and answers to common questions, visit the McAfee Customer Service and Technical Support home page at: <http://www.mcafeehelp.com> (<http://www.mcafeehelp.com>).

Glossary

D

DATs

Virus definition files. These files contain the virus definitions that are used when detecting viruses and Trojans on your computer or USB device.

L

launchpad

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

O

on-demand scan

A scan that is launched on-demand (that is, when you click the **Scan** button). Unlike real-time scanning or real-time monitoring, on-demand scans do not launch automatically.

R

real-time monitoring

Files and folders are constantly monitored for changes (for example, a new file added to a folder or a modification made to a file). If the real-time monitor detects a file change, the affected file is scanned for virus activity. If a virus or Trojan is detected, it is cleaned; if it cannot be cleaned, it is renamed.

S

smart drive

See USB device.

T

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.

U

U3

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

USB

(Universal Serial Bus) A standardized serial computer interface that allows you to attach peripheral devices.

USB device

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

V

virus

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

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

Copyright © 2006 McAfee, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc. McAfee and other trademarks contained herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks and copyrighted material herein are the sole property of their respective owners.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (AND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SITEADVISOR, SITEADVISOR, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS.

Index

A

- A threat has been detected. What should I do?29
- About alerts15
- About McAfee33

C

- Cancel scanning19
- Copyright34

D

- DATs31
- Delete an infected file..... 17, 23
- Disable antivirus software detection.....13
- Disable real-time monitoring12
- Do I need to be connected to the Internet to scan?.....29
- Does VirusScan USB scan zipped files?..30
- Download antivirus software for your computer25

F

- Features4
- Frequently Asked Questions29

H

- How do I get more help from McAfee?...30

I

- Install VirusScan USB.....6
- Installing and updating VirusScan USB...5

L

- launchpad31

M

- McAfee VirusScan USB.....3

O

- on-demand scan.....31

P

- Pause scanning 18, 19
- Protecting your computer.....25

R

- real-time monitoring31
- Renew your VirusScan USB subscription27
- Renewing your VirusScan USB subscription27
- Resume scanning 19

S

- Scan your USB device 18
- Scanning your USB device..... 9, 17
- Set scanned file types..... 10
- Set the locations to scan 11
- Setting scan options 5, 9, 17
- Show informational messages..... 14
- smart drive31
- Start a scan on insertion 13

T

- Trojan..... 31

U

- U3 31
- Update VirusScan USB8
- USB..... 32
- USB device 32

V

- View the last scan summary23
- View the results of a scan.....22
- View the VirusScan USB program summary.....24
- virus32

W

- Working with alerts 15
- Working with scan results.....21