McAfee®

VirusScan USB

User Guide

Contents

CHAPTER 1

McAfee VirusScan USB

VirusScan USB offers comprehensive, reliable, and up-to-date protection for your USB drive. It protects the contents of your USB drive against viruses, Trojans, spyware, adware, and other potentially unwanted programs (PUPs).

In this chapter

Features

VirusScan USB provides the following features.

Real-time scanning

When enabled, VirusScan USB real-time scanning constantly monitors your USB drive for file changes (for example, a new file added to the drive or a modification made to a file already on the drive). If real-time scanning 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. If spyware, adware, and other potentially unwanted programs are detected, you can trust or remove them.

On-demand scanning

On-demand scanning lets you scan your USB drive for viruses, Trojans, spyware, adware, and other potentially unwanted programs at any time.

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 active processes) and the locations to scan. You can also enable or disable real-time scanning.

Automatic scanning

When you install VirusScan USB, it is 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 drive into your computer.

Scan summary

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.

CHAPTER 2

Installing and updating VirusScan USB

Install VirusScan USB on your USB drive 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 scanning is enabled, VirusScan USB launches an automatic update every four hours. For more information about real-time scanning, see Setting scan options (page 9).

Note: If your USB drive comes with a virus protection program already installed, McAfee recommends that you remove that program before installing VirusScan USB.

In this chapter

Install VirusScan USB

Install VirusScan USB on your USB drive 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.

1. Insert your USB drive 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**.
9. In the Program Setup Completed dialog box, record your registration information, and then click **Finish**.

Tip: 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 drive, an update is launched each time that you plug the USB drive 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.

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

2 Click **OK**.

Note: To update VirusScan USB, 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 active processes) and the locations to scan. You can also enable or disable real-time scanning. When enabled, real-time scanning constantly monitors your USB drive for file changes (for example, a new file added to the drive or a modification made to a file already on the drive). If real-time scanning 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. If spyware, adware, and other potentially unwanted programs are detected, you can trust or remove them.

By default, real-time scanning is enabled and McAfee does not recommend that you disable it. When real-time scanning is enabled, all file types are scanned; 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 drive (page 17).

When you install VirusScan USB, it is 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 drive 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 drive 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 scanning detects an infection or you start it manually. McAfee does not recommend disabling the start scanning on insertion option in VirusScan USB.

The following table describes the scan options in VirusScan USB:

Option	Description
Scan all files	All types of files are scanned.
Scan subfolders	Subfolders (folders contained within other folders) 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.

Option	Description
Scan .zip and other archive files	Archived files including .zip files are scanned.
Scan for spyware and potentially unwanted programs	Files are scanned for spyware, adware, and other potentially unwanted programs.
Scan active processes	Programs running on your computer are scanned.
Scan scanning when VirusScan USB opens	Scanning begins when VirusScan USB opens.

In this chapter

Set scanned file types

You can specify which types of files on your USB drive are scanned during an on-demand scan. For example, you can determine whether subfolders and archives are scanned, and whether you want to scan for spyware, adware, and other potentially unwanted programs. You can also determine whether you want VirusScan USB to start scanning when it opens.

1 On the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.

2 On the Scan Options pane, under **Options**, select or clear the appropriate check boxes.

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 drive, disk drives that are not associated with your USB drive do not appear in the **Drives to Scan on this USB Drive.** These include removable drives on your computer and drives that are associated with other USB drives.

1. On the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
2. On the Scan Options pane, under **Drives to Scan on this USB Drive**, select or clear the appropriate check boxes.
3. Click **OK**.

The following table describes the USB drives you can scan:

Drive	Description
U3 System	(The drive name that appears can be different.) The CD-ROM partition on the drive is scanned. This is the location where the U3 system files are stored.
My U3 Drive	(The drive name that appears can be different.) The data partition on the drive is scanned. This is the drive letter assigned to the USB drive.

Disable real-time scanning

When enabled, VirusScan USB real-time scanning constantly monitors your USB drive for file changes (for example, a new file added to the drive or a modification made to a file already on the drive). If real-time scanning 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. If spyware, adware, and other potentially unwanted programs are detected, you can trust or remove them.

Real-time scanning monitors all file types (regardless of your on-demand scan settings). McAfee does not recommend disabling real-time scanning.

1. On the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
2. On the Scan Options pane, under **Real-Time Scanning**, clear the **Enable real-time scanning of USB drive** check box.
3. Click **OK**.

Note: If real-time scanning 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 scanning displays an alert, as usual.

Start a scan on insertion

When you install VirusScan USB, it is 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 drive 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 drive into your computer. 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.

1. On the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
2. On 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 is finished or canceled.

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.

1. On the VirusScan USB home pane, under **Current Scan Options**, click **Configure**.
2. On the Scan Options pane, under **Real-Time Scanning**, 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

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 drive 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 drive 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 drive

When you install VirusScan USB, it is 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 drive 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 drive 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 scanning 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 drive, 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 the clean and rename operations fail, you can delete the infected file. For more information, see Delete an infected file (page 22).

If spyware, adware, and other potentially unwanted programs are detected, you can trust or remove them.

- Trust: The potentially unwanted program is trusted and is not removed, even during future scans.
- Remove: The potentially unwanted program is removed permanently.

After you start scanning your USB drive, 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 drive

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

- On 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.

- On 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).

- On 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.

- On 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 drive, 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 drive.

If spyware, adware, and other potentially unwanted programs are detected, you can trust or remove them. When you trust potentially unwanted programs, they are added to a trusted list so that they are not detected any more. If you trusted a program by mistake, or you want the program to be detected, you must remove it from the trusted list by blocking it again.

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

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

1. On the Scan Progress pane, click **View Results**.
2. On the Scan Results pane, click an infected file name or a potentially unwanted program.
3. Under **Details**, view more specific information about the infected file or potentially unwanted program.
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 drive, 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 drive.

1. On the Scan Progress pane, click **View Results**.
2. On the Scan Results pane, click an infected file name.
3. Under **I want to**, click **Delete**.
4. Click **Finish**.

Remove a potentially unwanted program

After VirusScan USB detects spyware, adware, and other potentially unwanted programs, you can remove them. Removing these programs deletes them from your drive.

1. On the Scan Progress pane, click **View Results**.
2. On the Scan Results pane, click a potentially unwanted program.
3. Under **I want to**, click **Remove**.
4. Click **Finish**.

Trust a potentially unwanted program

After VirusScan USB detects spyware, adware, and other potentially unwanted programs, you can trust them. If you trust these programs but later on you want to block them, see Block a trusted program (page 23).

1. On the Scan Progress pane, click **View Results**.
2. On the Scan Results pane, click a potentially unwanted program.
3. Under **I want to**, click **Trust**.
4. Click **Finish**.

Block a trusted program

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

1. On the VirusScan USB home pane, under **Current Scan Options**, click **Trusted Lists**.
2. In the **Trusted Programs** list, select a program.
3. Under **I want to**, click **Block.**
4. Click **OK**.

View the last scan summary

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

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

View the VirusScan USB program summary

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

- 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 VirusScan from the McAfee download site.

In this chapter

Download virus protection software for your computer

You can download a full or trial version of McAfee VirusScan.

1 Under **Information** on the left pane, click **Download**.

2 Follow the on-screen instructions to download VirusScan.

Tip: You can also download VirusScan by clicking the link under **Drives to Scan on this USB Drive** on 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. For more information about your subscription, including when it expires, see View the VirusScan USB program summary (page 24).

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

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

- On the VirusScan USB home pane, under **Program**

Reference

Summary, click **Renew**.

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

Glossary

D

DAT

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

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 launch the operation). Unlike real-time scanning, on-demand scans do not launch automatically.

P

potentially unwanted program (PUP)

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

R

real-time scanning

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

S

smart drive

See USB drive.

T

Trojan

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

U

U3

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

USB

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

USB drive

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

V

virus

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

About McAfee

McAfee, Inc., headquartered in Santa Clara, California and the global leader in Intrusion Prevention and Security Risk Management, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security.

Copyright

License

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE, INC. OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Index