

# User's Manual

---

## VirusScan for UNIX



*Network Security & Management*

2805 Bowers Avenue  
Santa Clara, CA 95051-0963

Phone: (408) 988-3832  
Monday - Friday  
6:00 A.M. - 6:00 P.M.

## **COPYRIGHT**

Copyright © 1997 by McAfee Associates, 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 Associates, Inc.

## **TRADEMARK NOTICES**

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee Associates, Inc. WebScan, WebScan X, SiteExpress, BootShield, ScanPM, ServerStor, ScreenScan, GroupScan, GroupShield, PCCrypto, WebCrypto, Remote Desktop 32, eMail-It, PCFirewall, NetCrypto, WebShield, Hunter, SecureCast, and NetRemote are trademarks of McAfee Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

"SABRE" is a trademark of American Airlines, Inc. and is licensed for use to McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

## **FEEDBACK**

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your comments to: McAfee Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, or send a fax to McAfee Documentation at (408) 970-9727, or send e-mail to [documentation@mcafee.com](mailto:documentation@mcafee.com).

*Issued September 1997/VirusScan v3.0.4*

---

# Table of Contents

<b>Preface .....</b>	<b>v</b>
<b>Chapter 1. Introducing VirusScan.....</b>	<b>9</b>
Welcome .....	9
Why use VirusScan?.....	9
How To Contact Us .....	10
Customer Care.....	10
Technical support.....	10
McAfee training .....	11
International contact information.....	12
Reporting new items for VirusScan updates.....	13
<b>Chapter 2. Installing VirusScan .....</b>	<b>14</b>
Before You Begin .....	14
Installation requirements.....	14
About the distributions .....	14
Performing the Installation .....	15
Testing your installation.....	15
<b>Chapter 3. Using VirusScan .....</b>	<b>16</b>
Overview .....	16
Syntax.....	16
Options.....	16
Sample VirusScan Scenarios .....	20
Setting Scheduled Scans.....	21

---

<b>Appendix A. Preventing Virus Infection .....</b>	<b>22</b>
Keys to a Secure System Environment .....	22
Detecting New and Unknown Viruses.....	23
Why would I need a new data file? .....	23
Updating your data files .....	24
Unpacking the files.....	26
Reporting new items for VirusScan updates.....	26
<b>Appendix B. Testing Your Installation.....</b>	<b>27</b>
<b>Appendix C. McAfee Support Services .....</b>	<b>28</b>
Customer Service Programs.....	28
Free VirusScan support program.....	28
Free subscription maintenance and support program .....	29
Optional support plans .....	30
Professional Services Programs.....	31
Training .....	31
Consulting.....	31
Jump Start program .....	32
Enterprise support.....	32
Optional 7 x 24 enterprise support.....	33
<b>Index.....</b>	<b>34</b>



# Preface

---

## The Bits and the Bytes

Computer viruses, most users know, can have a devastating impact on productivity. What many of those same users don't know is basic information that could help them protect themselves from infection—such as where viruses come from and how they operate.

### In the beginning

The conceptual foundations for viruses have been around much longer than the virus threat itself. Although virus historians disagree on the specific whens and wheres, most do agree that the ideas were born when computers were still huge and expensive—the domain of large corporations and the government, not the public. And while many of the viruses circulating today are malicious, destruction of data was not part of the original premise.

The researchers who created the first viruses sought to create computer programs that could make copies of themselves, or self-replicate, with the idea that such programs might also “evolve.” If, for example, an error occurred in the replication process, the resulting code (the bits of information that make up the program) would be mutant. Just as mutant genetic code can either enhance or diminish the ability of a biological virus to survive and propagate, mutant digital code might dispose a computer virus to be more or less able to survive in the computer environment. Given enough time, the logical extension of the theory goes, a computer virus could evolve into something approaching artificial intelligence. Science fiction suddenly starts to look more like science and less like fiction.



---

## What viruses really are

At its core, a virus is simply a program with one goal: self-replication. Part of achieving that goal is remaining undetected. Users who find viruses will likely delete them, which puts quite a damper on any self-replicating plans. Just like any other program, a virus has to be run to do its work. And since users will not run a virus intentionally, the virus must attach itself to a file that a user will run. That includes executable files and document files with embedded macros, as we will see in a couple of pages. For a virus to infect any other type of file—say, a plain text file—would be counter-productive: Remember, replication is its primary objective.

## Computers with the sniffles?

Consider the similarities between computer and biological viruses. A computer virus infects a host program, just as a biological virus infects a host cell. It writes its own code in among the pieces of code that make up the host program. Then, in much the same way that a biological virus uses resources from its host organism to reproduce, a computer virus runs each time the infected host program runs, and makes copies of itself. Those copies then infect other programs, and the cycle begins again.

Just as biological viruses have detrimental effects, so do their computer counterparts. The first computer viruses were simply experiments by research scientists to test the theory—to see if it could be done. They proved the theory, but they also discovered that viruses had some unfortunate side effects. Viruses got in the way of some of the normal processes of the computer and caused erratic behavior. Many viruses are now specifically programmed to perform some function outside of self-replication. This function, called the payload, can be as innocuous as displaying a message on the computer's monitor or as harmful as destroying data on the system's hard disks. It is delivered when the trigger, an event such as a particular combination of keystrokes, a certain date or a pre-determined number of actions, occurs.



## Who writes viruses?

The reason for this change in the behavior of viruses—from innocent experiment to malicious sneak attack—is a result of a change in the type of people who write them. Virus code is now developed by many people who are less interested in studying the possibility of artificial intelligence than in inflicting harm. Some do it out of spite, some because they aspire to be the underground “mad hacker” romanticized in much of pop culture as a freedom fighter of the digital age. The reasons people write virus code are probably as varied and strange as the reasons people perform other destructive acts.

Some virus writers actually choose to identify themselves, such as the Pakistani brothers who wrote the Brain virus. The brothers included the name, address, and telephone number of their software company in the viral code. When the payload was delivered, this information would be displayed for the user. Apparently, the brothers wrote the virus to show how widespread software pirating was. They put it on diskettes leaving their office with the idea that wherever the virus spread, so had their software. Of course, what they overlooked was the fact that the virus spread by infecting programs other than the one it left their office in.

Other virus writers are disgruntled employees seeking revenge. Still others are schoolkids who write just to see if they can. The famous Stoned virus is said to have been written by such a youngster. Having written it, he feared the consequences of unleashing it, so he destroyed all copies of the virus except one, which he kept at his house. His younger brother and a couple of friends managed to lay their hands on it though, and infected some disks as a joke. But the infection spread quickly and soon was impossible to stop.

Whatever the motivation, the number of people capable of writing a virus is growing right alongside the computer industry. Those who stand to be affected by virus infection—anyone who uses a computer—should be alert and wary.



## Only getting worse

In part, the fact that so many of us must be on the alert today is what makes virus proliferation possible. When the computer world was made up entirely of huge, expensive machines, a virus did not have very far to go once it got started. But with the advent of the personal computer, viruses suddenly had a lot of places to go. The rapid growth of the Internet, the capability to attach files to e-mail messages, and the increasing degree to which the world depends on its computers all make conditions ever-better for the spread of computer viruses.

## New developments

There are other reasons to be especially wary these days. Viruses get increasingly complex and advanced as computers on the whole do the same. Just in the last few years, sophisticated and dangerous new virus families have appeared, such as polymorphic viruses and macro viruses. Polymorphic viruses are especially tricky to detect because they change each time they infect new files. Where once anti-virus software could search for viruses by “signatures” (chunks of code unique to each virus), it now must detect polymorphic viruses that change their signatures each time they infect a file.

Macro viruses infect documents and document templates—new territory for viruses. Documents used to be safe from viral attack because until a few years ago, a document file didn’t have any executable code in it. Now that software applications like Microsoft Word and Microsoft Excel have embedded macro capabilities, viruses can use an application’s own macro language to infect application documents and templates.

All that just in the last few years. And viruses as a serious threat have only been around for about ten years. To imagine what is in store as the computer becomes more complicated and more a part of everyday life is frightening. Luckily, you have purchased the best protection against infection available today. And with McAfee’s outstanding support and worldwide anti-virus research teams, you can make sure your protection keeps up with the ever-changing computer world.



# 1

## Introducing VirusScan

---

### Welcome

Thank you for purchasing VirusScan for UNIX—McAfee's virus detection and removal solution for UNIX-based systems.

VirusScan, the world's best-selling anti-virus software, employs McAfee's Hunter technology to detect known and new boot, file, stealth, multi-partite, mutating, encrypted, macro, and polymorphic viruses. McAfee's worldwide virus research team develops monthly updates to VirusScan's virus definition files, which gives VirusScan the highest possible detection rates.

### Why use VirusScan?

UNIX is a secure environment relatively unaffected by computer viruses. The DOS and Windows world, however, is different. DOS computers have no security and are very susceptible to virus infections. Since DOS viruses don't affect UNIX systems, you might be asking, "Why should I be concerned?"

One reason for concern is that DOS- and Windows-based computers are a rapidly expanding presence on the Internet—and most of these computers use the Internet for file transfer. A UNIX server may still harbor DOS viruses and, while not itself affected, pass them on to numerous DOS- and Windows-based clients. Rather than trying to block viruses at each DOS- or Windows-based computer served by a UNIX system, VirusScan for UNIX is the efficient, comprehensive, centralized solution. In order to protect yourself and your users, it is more important than ever to maintain anti-virus security.

VirusScan provides the best available anti-virus security, but it is only one important element of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness.

## How To Contact Us

### Customer Care

To order products or obtain product information, we invite you to contact our Customer Care department by calling (408) 988-3832 or by writing to the following address:

McAfee Associates, Inc.  
2805 Bowers Avenue  
Santa Clara, CA 95051-0963  
U.S.A.

### Technical support

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information..

World Wide Web	<a href="http://www.mcafee.com">http://www.mcafee.com</a>
----------------	---

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	<a href="mailto:support@McAfee.com">support@McAfee.com</a>
McAfee BBS	(408) 988-4004
	1200 bps to 28,800 bps
	8 bits, no parity, 1 stop bit
	24 hours, 365 days a year
CompuServe	GO MCAFEE

## 1 Introducing VirusScan

### How To Contact Us

---

America Online	keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

If the automated services do not have the answer you need, contact McAfee at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the McAfee technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

## McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

## International contact information

To contact McAfee outside the United States, use the addresses and numbers below.

**McAfee Canada**

139 Main Street  
Unionville, Ontario  
Canada L3R 2G6  
Phone: (905) 479-4189  
Fax: (905) 479-4540

**McAfee Europe B.V.**

Gatwickstraat 25  
1043 GL Amsterdam  
The Netherlands  
Phone: 31 20 586 6100  
Fax: 31 20 586 6101

**McAfee France S.A.**

50 rue de Londres  
75008 Paris  
France  
Phone: 33 1 44 908 737  
Fax: 33 1 45 227 554

**McAfee Deutschland GmbH**

Industriestrasse 1  
D-82110 Germering  
Germany  
Phone: 49 8989 43 5600  
Fax: 49 8989 43 5699

**McAfee (UK) Ltd.**

Hayley House, London  
Road  
Bracknell, Berkshire  
RG12 2TH  
United Kingdom  
Phone: 44 1344 304 730  
Fax: 44 1344 306 902

**McAfee Japan KK**

4F Toranomori Mori, Bldg. 33  
3-8-12 Toranomori  
Minato-Ku, Tokyo, 105  
Japan  
Phone: 81 3 3435 8246  
Fax: 81 3 3435 1349

## Reporting new items for VirusScan updates

McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses that VirusScan does not now detect. Please note that McAfee reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

AVResearch@McAfee.com

Use this address to report new virus strains.

# 2

## Installing VirusScan

---

### Before You Begin

#### Installation requirements

To install and run VirusScan for UNIX, you need:

- 4MB of free disk space
- One of these operating systems:
  - Solaris 2.x for SparcStations
  - HP-UX version 10.x
  - NCR UNIX for the Intel 80x86 platform

#### About the distributions

VirusScan for UNIX comes in three distribution versions, one for each supported operating system. If you install VirusScan from CD-ROM, you'll find each version in its own directory. Each distribution also includes its own install script. The next section discusses installation using the Solaris 2.x for SparcStations distribution as an example. To install any of the other distributions, substitute the path and filename for the distribution you want to install for those given in the example.



## Performing the Installation

To start an install script for VirusScan, follow the steps below. This example installs VirusScan for Solaris 2.x. To install other versions, substitute the correct filename where the example specifies `sparc.solaris2.x`.

Step	Action
1.	Copy the file <code>sparc.solaris2.x.tar.Z</code> to a directory on your system.
2.	Uncompress the file by typing:  <pre>uncompress sparc.solaris2.x.tar.Z</pre> <b>Response:</b> This action creates the file <code>sparc.solaris2.x.tar</code> .
3.	Unarchive the file by typing:  <pre>tar -xf sparc.solaris2.x.tar</pre> <b>Response:</b> This action creates an unarchived copy of the VirusScan for UNIX files.
4.	Execute the installation script by typing:  <pre>install-vscan</pre> <b>Response:</b> This action copies VirusScan files to your hard disk. The <code>install-vscan</code> program notifies you when it has finished the installation.

## Testing your installation

To learn how to test your VirusScan installation with the Eicar Standard AntiVirus Test File, see [Appendix B, "Testing Your Installation."](#)

# 3

## Using VirusScan

### Overview

VirusScan for UNIX is a command line–driven software package designed to offer sophisticated virus scanning without sacrificing flexibility.

### Syntax

The VirusScan command structure is designed for ease of use and should seem familiar. A summary of the command line with its associated options appears below.

```
uvscan [-d | --data-directory directory][-e | --exit-on-error]
[-f | --file file][--ignore-compressed][--ignore-links]
[--one-file-system][-p | --atime-preserve][-r | --recursive]
[-s | --selected][-c | --clean][--delete][-m | --move directory]
[-h | --help][--summary][-v | --verbose][--version]
[--virus-list] {file | directory}
```

To start VirusScan for UNIX, type **uvscan** at the UNIX prompt, followed by any of the options shown in brackets above, and the target file or directory.

### Options

Use VirusScan’s command options to change how the program runs. You can specify how it scans for viruses, how it responds when it finds a virus, where it looks for its data files, and a number of other settings. In the option summary below, short versions of each command appear after a single dash (-). Long versions of each command option, if any, appear after two dashes (--). The | symbol indicates that you may use either version as a valid command option.



Variables, such as filenames or paths, appear in italic within the brackets [ ] that delineate each command option, or in curly brackets { } when not part of a command option. Do not type the brackets or the | symbol when entering command options.

### Setting the location of VirusScan data files

**`[-d | --data-directory directory]`**

This option specifies the location of the three data files VirusScan requires: scan.dat, names.dat, and clean.dat. If you do not specify the location of these files in the command line, VirusScan looks for them in the directory specified by the MCAFEE.SCAN environment variable. If this environment variable does not exist, VirusScan looks for them in /usr/local/lib/mcafee.

### Setting scanning options

These options determine how and where VirusScan looks for infected files. You may use any combination of these options to customize the type of scan VirusScan performs.

**`[-e | --exit-on-error]`**

This tells VirusScan to stop scanning, quit, and display an error message when it encounters an error. The error message indicates the severity of the error.

**`[-f | --file filename]`**

This option tells VirusScan to determine which files to scan by reading a list of filenames. You can create the list as a text file and specify its path in the command line, or you can tell VirusScan to read the list from standard input by substituting "-" for the filename.

**`[--ignore-compressed]`**

This option tells VirusScan to ignore compressed files. By default, VirusScan decompresses files compressed with LHA, LZEXE, PKLITE, PKZIP and WINZIP in memory, then scans their contents. Using this option reduces the time it takes to complete a scan, but it also reduces file security.

#### `[--ignore-links]`

This option tells VirusScan not to resolve any symbolic links it encounters and not to scan the link targets. VirusScan normally resolves links and scans their targets.

#### `[--one-file-system]`

When used in conjunction with the recursion option, this option allows you to scan an entire directory tree without scanning attached file systems.

Normally, VirusScan treats a mount point as a subdirectory and scans that file system. Unless you want to scan attached file systems, you should use this option.

#### `[-p | --atime-preserve]`

This option tells VirusScan to reset the last access time shown for each scanned file to the value it had before VirusScan examined it.

#### `[-r | --recursive]`

This option tells VirusScan to scan target directories recursively. With this option selected, VirusScan scans the target directory and all of its subdirectories.

#### `[-s | --selected]`

This option tells VirusScan to scan only those files most susceptible to virus infection. VirusScan identifies these files by looking for the extensions .exe, .com, .xl?, or .do?. It uses the extensions .do? and .xl? to identify Microsoft Word and Excel's document and template files, which can contain macro viruses. The ? character is a wildcard. Because VirusScan scans a smaller set of files, it can scan a target directory faster.

### Setting response options

These options determine how VirusScan responds to a virus infection. You may choose only one of these three options:

`[-c | --clean]`

This option tells VirusScan to repair infected files by removing viruses from them. If VirusScan cannot clean a file, it displays a warning.

`[--delete]`

This option tells VirusScan to delete any infected files it finds automatically.

`[-m | --move directory]`

This option tells VirusScan to move any infected files it detects to a quarantine directory that you specify. When VirusScan moves an infected file, it replicates the full directory path for the infected file inside the quarantine directory so that you can determine the infected file's original location.

### General Options

These options give you additional information you can use when working with VirusScan.

`[-h | --help]`

This option tells VirusScan to display a short list of help information.

`[--summary]`

This option tells VirusScan to display a summary of scan results at the end of its scanning session.

`[-v | --verbose]`

This option tells VirusScan to report its progress verbosely as it scans.

`[--version]`

This option shows you the VirusScan version number you have installed.

`[--virus-list]`

This option tells VirusScan to display a list of the viruses it detects.

### Specifying a target file or directory

Type the name of the file you want VirusScan to examine, or the directory that contains files you want scanned, after your list of VirusScan options.

### Setting VirusScan to run automatically

To set VirusScan to examine your target files or directories automatically, add the VirusScan command line, along with any options you want to use, to a cron file. See the UNIX man page for `cron` to learn how to set up a cron file.

## Sample VirusScan Scenarios

This section describes a few circumstances in which you might use VirusScan and how to structure the command line to accomplish a task you want completed. The following scenarios assume that you have installed the `uvscan` executable in `usr/local/bin` and the data files (\*.dat) in `usr/local/lib/mcafee`.

### Scenario No. 1

To tell VirusScan to scan and clean all files in the `usr/dos` directory and all of its subdirectories, type:

```
uvscan -d /usr/local/lib/mcafee -c -r /usr/dos
```

VirusScan scans `usr/dos` and its subdirectories automatically, cleaning any infected files it encounters.

#### Scenario No. 2

To tell VirusScan to scan and clean all files in `usr/dos` and its subdirectories, but to ignore any other file systems that are mounted as volumes, type:

```
uvscan -d /usr/local/lib/mcafee -c -r --one-file-system  
/usr/dos
```

VirusScan scans `usr/dos` and its subdirectories automatically without moving across file systems. It cleans any infected files it encounters.

#### Scenario No. 3

To tell VirusScan to scan all files, except compressed files, in `usr/dos` and its subdirectories and to move any infected files to `/usr/local/viruses`, type:

```
uvscan -d /usr/local/lib/mcafee -m /usr/local/viruses -r  
--ignore-compressed --exit-on-error /usr/dos
```

VirusScan scans `usr/dos` and its subdirectories automatically. It ignores any compressed files. It moves any viruses it encounters to `/usr/local/viruses`. If it encounters any errors, it automatically exits.

#### Scenario No. 4

To display a list of all viruses VirusScan detects, type:

```
uvscan --virus-list
```

VirusScan displays a list of the viruses it detects.

## Setting Scheduled Scans

After testing VirusScan and choosing the options you want to use with it, add the VirusScan command line and the options you want to use to a cron file. See the UNIX man page for `cron` to learn how to set up a cron file.

# A

## Preventing Virus Infection

---

### Keys to a Secure System Environment

VirusScan is an effective tool for preventing virus infections, but it is most effective when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.


To create a secure system environment and minimize your chance of infection, McAfee recommends that you

- Install VirusScan and other McAfee anti-virus software
- Schedule regular scanning operations by including the VirusScan command line and all appropriate options in a cron file.
- Make frequent backups of important files. Even with VirusScan available to prevent attacks from viruses, fire, theft, or vandalism can render data unrecoverable without a recent backup.

## Detecting New and Unknown Viruses

The best way for you to deal with new and unknown viruses and harmful applets that might affect your system is to update your VirusScan virus definition (.DAT) files.

To offer the best virus protection possible, McAfee continually updates the definition files VirusScan uses to detect viruses. For maximum protection, you should update these files on a regular basis.

 *The term “update” refers only to the virus definition files; the term “upgrade” refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. We cannot, however, guarantee backward compatibility of the signature files with previous versions’ executable files. By upgrading your software to the latest product version and updating to the latest .DAT files regularly, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

### Why would I need a new data file?

New viruses appear at a rate of more than 200 per month. Often, older data files cannot assist VirusScan in detecting these new variations. The data files that came with your copy of VirusScan, for example, may not detect a virus that was discovered after you bought the product.

McAfee’s virus researchers are working constantly to update these data files with more and better virus definitions. New data files are released monthly.

 *McAfee cannot guarantee that the VirusScan .DAT files included with this release will work with previous VirusScan versions.*

## Updating your data files

You can use any of these methods to update your data files for VirusScan:

- **Connect to McAfee's FTP server.** Open a connection to <ftp.mcafee.com>. Use anonymous as your user name and your e-mail address as your password to gain access. Look for VirusScan .DAT files in the directory `pub/anti-virus`.
- **Connect to the McAfee Web Site.** Start your favorite browser software, then go to <http://www.mcafee.com> to download the latest data files and read up-to-the-minute news.
- **Connect to the McAfee Bulletin Board System (BBS).** Use your preferred communications software to dial (408) 988-4004. Additional instructions for using the BBS appear in the next section.

## Logging on to the McAfee BBS

- The McAfee BBS operates at up to 28,800 bps. Set your communications parameters to 8 data bits, 1 stop bit, and no parity. Set your terminal emulation to ANSI or TTY.
- The BBS is Bell- and ITU- (formerly CCITT) compatible.

After you receive the CONNECT message from your modem, enter your name, geographic location, and password.

To connect as a guest, type the following names at the prompts you see:

**guest**                    (for first name)

**user**                    (for last name)

You may also create your own account by entering your first name, your last name, and a password. Creating your own account on the McAfee BBS gives you a place to retrieve e-mail answers to technical support questions or receive other information in a convenient electronic form. To create an account, enter a user name and a password between 3 and 8 characters long. Note that passwords are case sensitive.




Once you connect successfully, the BBS starts you in the main menu. To use the system, type a letter command at the prompt. Common BBS commands include:

- F** Go to the file transfer area to download McAfee updates
- M** Go to the message area to read and write messages
- G** Log off the system and hang up

To download updates to your VirusScan data files, for example, start at the main menu, then follow these steps:

1. Type F to go to the File transfer area.
2. Type 1 to see a directory of McAfee anti-virus files.
3. Type D to ready the system for a download, then type the name of the file you want to receive. Refer to the directory for the correct filename.
4. Select a file-transfer protocol to use. Use an error-correcting protocol such as ZMODEM, YMODEM or XMODEM, if possible.
5. When you see the message "Awaiting start signal," set your software to receive files.

 *Please note that your access to these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.*

6. Your software should prompt you to specify a file-transfer protocol and a filename. Specify the same protocol and filename you set for the BBS to use.

## Unpacking the files

After you download a new data file, follow these steps to unpack the update and use the new definition files.

1. Change to the directory that contains the files you downloaded, then type:

```
unzip -L DAT-3007.ZIP
```

where dat-3007.zip is the name of the file you downloaded.

**Response:** The Unzip utility decompresses the VirusScan data files.

 *If you do not have the Unzip utility for UNIX, download a copy from the McAfee BBS or the McAfee FTP site.*

2. Move the data files to the usr/local/lib/mcafee directory (or to the directory that contains your current virus definition files) by typing:

```
mv *.dat /usr/local/lib/mcafee
```

**Response:** Your system overwrites the old definition files with the new files. The next time VirusScan for UNIX runs, it uses the new data files to scan for viruses.

## Reporting new items for VirusScan updates

McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses that VirusScan does not now detect. Please note that McAfee reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

AVResearch@McAfee.com

Use this address to report new virus strains.

# B

## Testing Your Installation

---

The Eicar Standard Anti-Virus Test File is the result of a world-wide combined effort by anti-virus vendors to set one standard that customers can use to verify their anti-virus installations. To test your installation, copy the following line into its own file and name it EICAR.COM.


```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-  
TEST-FILE!$H+H*
```

 *The characters in this file must all appear on one line.*

When saved, this file will use 69 or 70 bytes on disk.

Use VirusScan to scan this file. If VirusScan reports finding the EICAR-STANDARD-AV-TEST-FILE virus, your installation is correct.

THE FILE YOU CREATED DOES NOT HAVE A VIRUS! Delete the file when you have finished using it for installation testing so that unsuspecting users are not unnecessarily alarmed.

 *Because the Eicar Standard Anti-Virus Test File is not a true virus infection, you may not clean or repair the “infected” file.*

# C

## McAfee Support Services

---

### Customer Service Programs

McAfee offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you or your business.

#### Free VirusScan support program

All registered owners of single-node (one computer) VirusScan products purchased or downloaded from the McAfee Web Site are entitled to:

- Unlimited free online virus updates (new .DAT files) for the life of your product
- One year of unlimited free online product upgrades (product version revisions) with the newest features
- Free support services listed below


#### Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004

- ❑ World Wide Web site: <http://www.McAfee.com>
  - ❑ CompuServe: GO MCAFEE
  - ❑ Microsoft Network: MCAFEE
  - ❑ America Online: keyword MCAFEE
- 90 days of free technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

## Free subscription maintenance and support program


McAfee offers all registered owners of licensed multiple-node (ten computers or more) subscription products the following free support services and maintenance during the two-year term of the software subscription.

 *You must be a registered owner to receive these services.*

### Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
  - ❑ Automated voice and fax system: (408) 988-3034
  - ❑ McAfee BBS (electronic bulletin board system): (408) 988-4004
  - ❑ World Wide Web site: <http://www.McAfee.com>
  - ❑ CompuServe: GO MCAFEE
  - ❑ The Microsoft Network: MCAFEE
  - ❑ America Online: keyword MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus definition data. If you upgrade your operating system, you can also upgrade your product version to one that runs on your new platform.

## Optional support plans

 *Contact McAfee for current pricing structures.*


### Option 1: One-year personal support plan

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical telephone support, download the latest virus protection updates each month, and periodically download upgrades from any of McAfee's registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product version to one that runs on your new platform.

### Option 2: One-year quarterly disk/CD-ROM maintenance and support programs

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CD-ROMs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus data files without having to download from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through McAfee's Customer Care department at (408) 988-3832.

 *McAfee reserves the right to change part or all of its Customer Service Programs at any time without notice.*



## Professional Services Programs

McAfee Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. McAfee consultants are trained on a variety of operating systems and desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved.

### Training

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of its computing resources. McAfee offers on-site training on all McAfee products, network management seminars, anti-virus seminars, customized curricula for site-specific applications as well as product and personnel certification. McAfee's consultants provide extensive training with a curriculum tailored to your organization's needs.

### Consulting

McAfee Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installing and configuring McAfee products
- Configuring Windows 95
- One-on-one consulting

McAfee Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

## Jump Start program

This fixed-fee consulting program is designed to get clients up and running on McAfee products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

## Enterprise support

McAfee's Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:


- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. central time, Monday through Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Every Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.



## Optional 7 x 24 enterprise support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.

 *McAfee reserves the right to change part or all of its Professional Services Programs at any time without notice.*



# Index

---

## A

access time for files,  
    resetting 18  
automated voice and fax  
    response system 10  
automatic scans, setting up  
    20, 21

## B

backups, use of in security  
    program 22  
brackets, use of in  
    command syntax  
    summary 16  
Bulletin Board System  
    (BBS) 10

## C

cleaning infected files 19  
command syntax  
    variables 17  
command-line syntax  
    sample scenarios 20  
    summary 16  
compressed files, ignoring  
    during scans 17  
cron file, using with  
    VirusScan 20, 21

## Customer Care

    contacting 10  
    programs 28

## D

dashes, use of in command  
    line options 16  
data (.DAT) file, updating  
    23  
data directory, setting 17  
deleting infected files 19

## E

Eicar Standard Anti-Virus  
    Test File, using 27  
electronic services  
    America Online 11  
    CompuServe 10  
    e-mail 10  
    the McAfee BBS 10,  
        24  
    the McAfee FTP site  
        24  
    the McAfee Web Site  
        10, 24  
    the Microsoft Network  
        11  
enterprise support 32  
exit on error, setting for  
    scan operations 17

## F

file extensions, use of to  
    identify susceptible files  
    18  
file systems, ignoring  
    during scans 18

## H

help, displaying 19

## I

infected files  
    cleaning 19  
infected files, deleting 19  
infections, responding to  
    19  
installing VirusScan 14  
    testing 27

## L

links, ignoring during scans  
    18  
long command options 16



## M

### McAfee

- contacting 10
  - automated voice and fax system 10
- BBS 10
- outside the United States 12
- via America Online 11
- via CompuServe 10
- via the Microsoft Network 11
- within the United States 10
- World Wide Web 10

- Customer Care 10
- enterprise support 32
- jump start program 32
- support services 28
- training 11, 31

- moving infected files to a quarantine directory 19

## O

### options

- using in command line 16

## P

- personal support plan 30
- professional services
  - consulting 31
  - enterprise support 32
  - jump start program 32
  - training 31

## Q

- quarantine directory, specifying 19

## R

- recursive scans, performing 18
- reporting new virus strains 13, 26
- response options, setting 19
- running VirusScan automatically 20, 21

## S

- scan results, displaying 19
- scanning options, setting 17
- scanning specific files or directories 20
- scans, running automatically 20, 21
- scenarios for using VirusScan 20, 21
- securing your system environment 22
- selected files, scanning for 18
- short command options 16
- standard input, using to set scan targets 17
- starting VirusScan 16
- structuring command lines for VirusScan use 20, 21
- subscription maintenance program 29
- summary of command-line options 16

- summary of scan results, displaying 19

### Support

- programs 28
- support, technical
  - see technical support 10
- symbolic links, ignoring during scans 18
- syntax 16
  - use of options in command line 16
  - using variables in 17

## T

- target directories for scans, specifying 20
- technical support
  - automated voice and fax system 10
  - e-mail address for 10
  - free support policies 28
  - information needed from user 11
  - online 28
  - programs 28
  - via BBS 10
- testing your installation 27
- training
  - scheduling for McAfee products 11

## U

- update, definition of 23
- updating VirusScan methods 24



updating VirusScan .DAT files 23  
upgrade, definition of 23  
using a file to supply scan targets 17

## V

variables, use of in command line 17  
verbose scan reports, setting 19  
version number, determining 19  
viruses  
    cleaning out of infected files 19  
    preventing infection by 22  
    reporting new strains 13, 26  
    responding to infections 19  
    showing VirusScan detection list 20

## VirusScan

.DAT files, updating 23  
as a part of security program 22  
installing 14  
introducing 9  
options  
    atime preserve 18  
    clean 19  
    data directory 17  
    delete 19  
    exit on error 17  
    file 17  
    help 19  
    ignore compressed 17  
    ignore links 18  
    move 19  
    one file system 18  
    recursive 18  
    selected 18  
    summary 19  
    verbose 19  
    version 19  
    virus list 20  
overview of features 9  
reporting items not detected 13, 26  
scenarios for use 20, 21  
starting 16  
system requirements 14  
testing your installation 27  
updating  
    methods 24  
using 16

## W

what viruses does VirusScan detect? 20  
why use VirusScan? 9  
World Wide Web, McAfee site on 10

## Z

zipped files, ignoring during scans 17