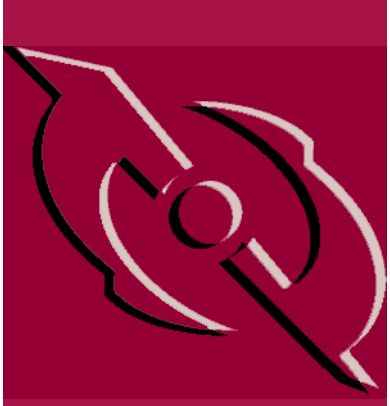


VIREX

Anti-virus software
for Macintosh computers

User's Guide

Version 6.0

Table of Contents

Introducing Virex Anti-Virus Software 1

Congratulations! You have selected the fastest, most complete virus protection available for your Macintosh computer. This *User's Guide* provides all the information you need to install and use Virex* anti-virus software. It also presents information for advanced users about customizing the software.

Be sure to check your Virex Installer disks for the Virex Read Me file, which provides the latest information for Virex software users.

Organization of this Guide

This *User's Guide* is designed as a quick, but complete, reference. Its chapters are:

Chapter 1, "Introducing Virex Anti-Virus Software," gives you an overview of each of the product components.

Chapter 2, "Installing Virex Anti-Virus Software," explains installation procedures.

Chapter 3, "Using the Virex Application," gives procedures and detailed information for using the Virex application.

Chapter 4, "Using the Virex Control Panel," gives procedures and detailed information for using the Virex control panel, the Virex DropScan* utility, and the Control Strip module.

Chapter 5, "Customizing the Virex Application," describes all of the user-definable preferences in the Virex application.

Chapter 6, "Customizing the Virex Control Panel," describes all the user-definable preferences in the Virex control panel.

Chapter 7, **"Scheduling Virex Operations,"** describes how to use the Virex Scheduler to run scheduled scan tasks.

Chapter 8, "Updating Virex," describes how to update your Virus Definition files electronically.

Appendix A, "Troubleshooting," provides helpful information to resolve any problems.

Appendix B, "Repairing Active Files," gives step-by-step instructions for repairing infected active files, such as the Finder.

Appendix C, "Safe Computing Practices," describes techniques to help ensure that your data remains free from virus attacks.

Appendix D, "A Word About Computer Viruses and Trojan Horses," provides information about how viruses and Trojan horses work.

Appendix E, "Understanding Macintosh Viruses and Trojan Horses," describes many viruses and Trojan horses circulating today.

Appendix F, "Before You Call Technical Support," contains crucial instructions that you should follow to ensure you receive fast, efficient technical support.

Appendix G, "Glossary," defines many terms used in this *User's Guide*.

Appendix H, "How to Contact Network Associates," gives contact information for Network Associates, Inc.

Virex program component overview

Virex Installer

The Virex Installer utility first ensures that your Macintosh computer is virus-free, then it installs the Virex application, the Virex control panel, the Virex DropScan utility, the Virex Control Strip module, and the Virex contextual menu plug-in.

Virex application

The Virex application scans your computer for viruses and Trojan horses. You can use it to diagnose and repair a file, a folder or an entire volume, and to see a complete record of the results. The application also allows you to update your Virus Definition file, which gives the Virex software the ability to detect new virus strains. The application's Snapshot function takes a "picture" of your system, then monitors it for changes to that baseline configuration. Sometimes, unexplained or unusual changes to your system configuration could indicate a virus attack.

Virex control panel

The Virex control panel provides you with continuous anti-virus protection. Once you install it, the Control Panel detects and repairs known viruses *before* they do damage. It scans floppy disks when you insert them into your floppy drive and checks files—including e-mail attachments—as you download them from the Internet. The control panel also works with the Virex Administrator application to deliver the most complete virus protection available for Macintosh networks.

Virex Scheduler extension

The Virex Scheduler extension enables the Virex application to run the scan operations and update tasks you set via the Schedule Editor. The extension installs into the Extensions folder by default. In order to have the tasks you schedule automatically, you must have this extension installed and your computer must be on. You do not need to have the Virex application active, however.

Virex contextual menu plug-in

The Virex contextual menu plug-in integrates Virex scanning directly into Mac OS 8.0 and later Finder versions, and in other contextual–menu savvy applications. Scan any file, folder, or volume by control-clicking its icon, then choosing Scan with Virex from the contextual pop-up menu.

Virex DropScan

The Virex DropScan utility puts instant drag-and-drop scanning on your Macintosh desktop. No need to open the Virex control panel or wait for the Virex application to launch—just drag a file, folder, or volume to the Virex DropScan icon.

Virex Control Strip module

The Virex Control Strip module brings the convenience of the Macintosh Control Strip to the Virex control panel. Open the Virex Control Strip Module to use common Virex control panel functions.

Virex Administrator

Virex Administrator lets system and network administrators work from the convenience of their own desktops to install and update Virex, and to diagnose and repair infections anywhere on their networks. This is a separate Network Associates product—contact Network Associates Customer Care for more information. Contact information appears at the end of this guide.

On-line help

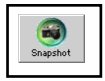
The Virex application and Control Panel provide on-line help, both in their main windows and in their preferences dialog boxes. Click this button in the Virex application, or click Help in the Virex control panel. Balloon Help is also available in the Virex application.

Known Macintosh viruses and Trojan horses

Network Associates continually updates Virex anti-virus software to detect and repair new viruses. For a complete listing and description of system viruses and Trojan horses that the software detects, click this button in the Virex application. Installing a Virex Virus Update also updates this information. See Appendix E, page 87 for an overview. For more detailed information, visit the Dr Solomon website at

http://www.drsolomon.com/vircen/index.cfm

Using Snapshot to detect unknown viruses



In addition to detecting known viruses, the Virex software can detect previously unidentified viruses by creating a baseline record of your files and periodically comparing those files against that baseline. Virex software can detect subtle changes in file sizes, newly introduced bits of code and other changes in files that could indicate possible infection by a new virus.

Detecting new viruses

Network Associates updates Virex anti-virus software regularly when new viruses appear. Refer to the Virex Read Me file on the Virex Installer disks for information on obtaining updates. Network Associates also offers a convenient and affordable support service that automatically provides updates and feature upgrades to you as they are released. Visit the Dr Solomon website at http://www.drsolomon.com/vircen/index.cfm for more information.

Additional products

Network Associates offers a full range of anti-virus solutions for the PC and the network. As Virex software does for the Macintosh platform, the Network Associates family of products for the PC provides powerful and easy-to-use anti-virus protection for IBM and compatible personal computers. Contact Network Associates for details.

Please register now

Network Associates provides the best support in the business to its registered users. Please send in your completed registration card as soon as possible.

Installing Virex Anti-Virus Software 2

Overview

The Virex Installer provides a convenient way to install Virex anti-virus software. It scans your Macintosh computer for viruses and Trojan horses and installs the Virex application and the Virex control panel on your computer.

System requirements

Virex anti-virus software will install and run on any Macintosh computer that meets these requirements:

- It has System 7.55 or Mac OS 8.0 or later installed
- It is a Macintosh II or later computer with a Motorola 68020 processor or later, or a PowerPC 601 processor or later
- It has 4 MB of available random-access memory (RAM), exclusive of other system or application requirements
- It has 9 MB of available hard disk space

Although you can install Virex software with Mac OS extensions turned on, Network Associates recommends that you restart your computer with the extensions disabled so that the Virex extensions will load properly. To do this, restart your computer, then hold the SHIFT key on your keyboard until the Extensions Disabled or Extensions Off message appears.

Preparing for installation

Network Associates distributes Virex software in two ways: as an archived CD-ROM image that you can download from the Network Associates or Dr Solomon websites; and on an actual compact disc. Once you have mounted the Virex CD-ROM image or placed your Virex installation disc in your CD-ROM drive, the installation steps you follow after that are the same for each type of distribution.

NOTE: To make it practical to download, the CD-ROM image stored on the website contains only a subset of the files available on the CD-ROM itself.

Downloading and mounting the Virex CD-ROM image

Network Associates makes Virex software available as a CD-ROM image in BinHex (.hqx) format for you to download from its website or from other electronic services. To download the Virex archive, use your preferred web browser to connect to the website or service, then save the .hqx file to your hard disk. If you do not already have it, be sure also to save the Apple Disk Copy utility stored on the site to your hard disk. You will need this utility to mount the CD-ROM image.

WARNING: If you suspect that your computer has a virus infection, download the .hqx file to a computer that is *not* infected.

Your web browser should convert the .hqx file to a StuffIt compressed file (.sit), then unstuff the file automatically. If it does not, or if you use an FTP client application or another method to download the file, you might need to use DeHQX, BinHex, StuffIt Expander, or a similar utility to convert the file to a usable format. You can download the utilities necessary to perform this conversion from most electronic services.

Once you have converted and unstuffed the CD-ROM image, follow these steps to mount it:

1. Locate and double-click the Disk Copy utility you downloaded to start it, or simply drag the CD-ROM image file onto the Disk Copy program icon.
2. If you double-clicked Disk Copy to start it, drag the CD-ROM image you downloaded to the Disk Copy window. You can also choose Mount Image from Disk Copy's Image menu, then locate the CD-ROM image in the dialog box that appears.

   Disk Copy will verify the integrity of the CD-ROM image, then it will mount the image on your desktop. You can then double-click the mounted image to open it.

See "Using the Virex Installer to scan your computer" on page 13 to continue with your Virex installation.

Using the Virex Installer to scan your computer

Network Associates recommends that you use the Virex Installer to scan your Macintosh computer before you continue with installation.

Follow these steps:

1. If your Virex copy came on CD-ROM, insert the CD-ROM disc into your CD-ROM drive. If you downloaded your Virex copy as a CD-ROM image, first mount the image on your desktop, then double-click it to open the image window. See "Downloading and mounting the Virex CD-ROM image" on page 12 to learn how to mount the CD-ROM image.
2. Double-click the Installer program icon  .

   The Virex Installer window appears (Figure 2-1).

Figure 2-1. Virex Installer window

3. Click Scan.

   The Volumes to Scan dialog box appears (Figure 2-2).

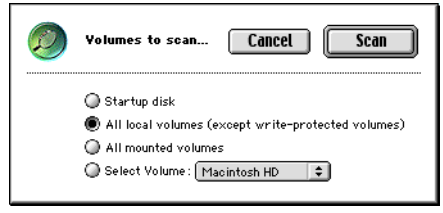


Figure 2-2. Volumes to Scan dialog box

4. Click one of the buttons shown to choose a scan target. You can have the Installer scan these items:

   - **Startup disk.** Choose this option to have the Installer scan only the disk that holds your active System folder.
   - **All local volumes (except write-protected volumes).** Choose this option to have the Installer scan all hard disk volumes on your computer except write-protected volumes—such as CD-ROM discs and locked floppy disks—and server volumes. Network Associates recommends that you choose this option for maximum protection against potential infections.
   - **All mounted volumes.** Choose this option to have the Installer scan all volumes mounted on your computer.
   - **Select Volume.** Choose this option to have the Installer scan the volume you choose from the adjacent pop-up menu.

5. Click Scan.

The Virex Installer will scan the volumes you specified. If the Installer finds no infected files, continue with your installation. If the Installer finds an infection, be sure to repair the infected files or delete them from your system before you continue.

NOTE: The Virex Iinstaller uses the Virus Definition file it comes with to perform the pre-installation scan operation. To protect yourself against viruses that might have appeared since the last full Virex release, you should consider updating the Virus Definition file. To do so, follow the steps outlined below.

Updating the Virus Definition file for installation

To update the Virus Definition file that the installation utility uses to scan your system before installation, follow these steps:

1. If your Virex copy came on CD-ROM, insert the CD-ROM disc into your CD-ROM drive. If you downloaded your copy of Virex as a disk image, first mount the image on your desktop, then double-click it to open the image window. See “Downloading and mounting the Virex CD-ROM image” on page 12 to learn how to mount the disk image.
2. Locate and open the Virex Application folder on the CD-ROM disc or within the mounted disc image.
3. Double-click the Virex application to start it.

The Virex application main window appears. (Figure 2-3).

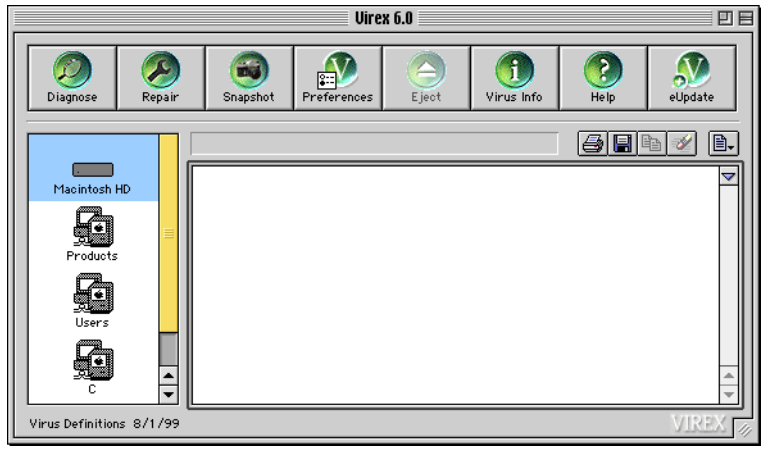


Figure 2-3. Virex application main window

4. Choose Apply Update File from the File menu.

   The Virex application opens a dialog box where you can choose your current Virus Update file. Network Associates recommends that you choose a Virus Update file that you know is virus-free.

5. Choose the volumes you want to scan, then click 

to begin a scan operation. When you have finished, quit the Virex application, then follow the steps outlined in "Installation steps" to continue.

NOTE: Network Associates recommends that you also update the Virex copy that you install on to your hard disk. To do so, follow Steps 2 through 5. In Steps 2 and 3, however, be sure to start the Virex copy installed on your hard disk instead of the one stored on CD-ROM.

Once you install Virex, you can update your Virus Definition files electronically. See Chapter 8, "Updating Virex," for details.

Installation steps

To install Virex software, follow these steps:

IMPORTANT: Be sure that you have scanned your computer for viruses before you continue. If you haven't already, follow the steps outlined in "Using the Virex Installer to scan your computer" on page 13.

1. If your Virex copy came on a compact disc, insert the disc into your CD-ROM drive. If you downloaded your copy of Virex as a CD-ROM image, first mount the image on your desktop, then double-click it to open the image window. See "Downloading and mounting the Virex CD-ROM image" on page 12 to learn how to mount the CD-ROM image.
2. Double-click the Installer program icon .

   The Virex Installer window appears (see Figure 2-1 on page 13).
3. Click Install.

   The Install Virex dialog box appears (Figure 2-4).

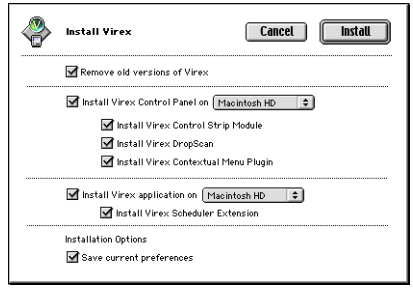


Figure 2-4. Install Virex dialog box

4. Choose your installation options. You can have the Installer:
   - **Remove old versions of Virex**. Select this checkbox to have the Installer remove existing versions of Virex software from the volumes on which you plan to install the Virex application and the Virex control panel. The Installer activates this option by default—clearing the checkbox tells the Installer to ignore any existing Virex versions it finds on your computer.

     NOTE: If you do not select either the **Install Virex Control Panel on** or the **Install Virex Application on** option, a pop-up menu appears adjacent to the **Remove old versions of Virex** checkbox. Here you can choose the hard disk volume from which you want to remove Virex software.

- **Install Virex Control Panel on**. Select this checkbox to install the Virex control panel on the volume you choose from the adjacent pop-up menu. Because the Installer must copy this file to the Control Panels folder in a valid System folder, the menu will list only those volumes that have such a folder. The Installer activates this option by default—clearing the checkbox tells the Installer not to install the Virex control panel. You can choose to install these components along with the Control Panel:
  - **Install Virex Control Strip module**. Select this checkbox to copy the Virex Control Strip module to the same volume you chose for the Control Panel installation. The Installer activates this option by default—clearing the checkbox tells the Installer not to install the Control Strip module.
  - **Install Virex DropScan.** Select this checkbox to copy the Virex DropScan utility to the same volume you chose for the Control Panel installation. A DropScan icon will appear on the desktop when you start your computer with the System folder stored on the volume you've chosen. The Installer activates this option by default—clearing the checkbox tells the Installer not to install the DropScan utility.
  - **Install Virex Contextual Menu Plug-In.** Select this checkbox to copy the Virex Contextual Menu plug-in to the same volume you chose for the Control Panel installation. The Installer activates this option by default—clearing the checkbox tells the Installer not to install the plug-in.
- **Install Virex Application on.** Select this checkbox to copy the Virex application to the top level of the volume you choose from the adjacent pop-up menu. The Installer activates this option by default—clearing the checkbox tells the Installer not to install the Virex application.
- **Install Virex Scheduler Extension.** Select this checkbox to copy the system extension that enables the new Virex Scheduler component. This extension allows the scan tasks and electronic updates that you configure to execute at the time you designate. To learn more how to automate some Virex operations, see Chapter 7, "Scheduling Virex Operations."
- **Save current preferences.** Select this option to tell the Installer to save the preference settings from the existing Virex version installed on your computer. Clearing the checkbox tells the Installer to install Virex with default preference settings.

> **NOTE:** The Installer will retain preference settings only from Virex v5.5 anti-virus software and later.

5. When you have chosen the installation options you want, click Install.
6. When the Installer has finished copying files to your hard disk, it will notify you with a dialog box. Click Quit to quit the Installer. Click Continue to complete your installation and return to the Virex Installer dialog box.
7. Restart your computer to ensure that the Virex control panel and its related modules reload properly into the Mac OS environment.

Pre-configuring Virex preferences

Advanced users and system administrators can pre-configure the preferences for the Virex application and the Virex control panel before they distribute copies to other Macintosh users on the network. You can use either of two methods to do so:

- You can save custom preference files to a location on your administrative computer or a network server, then either have network users download them, or distribute them to other users as e-mail attachments, via floppy disk, or via other methods. To complete the configuration, you or your network users will need to copy the custom files to the Virex Preferences folder. That folder resides inside your Preferences folder in your System folder.
- You can save custom preference files to a location on your administrative computer, then copy all of the Virex installation files and the custom preference files you saved onto a high-capacity floppy disk, such as a Zip, Syquest, or Imation SuperDisk drive. You can then use the high-capacity disk to install Virex on each target computer. To use this method, each Macintosh computer on which you plan to install Virex should have a the same high-capacity removable floppy disk drive. Alternatively, you could save only the custom preference files to a floppy disk, then copy those files to the correct location after you install each Virex copy from the CD-ROM.

Follow these steps to save custom preference files for both program components:

1. Install the Virex software on your administrative computer.
2. Start the Virex application or open the Virex control panel, then set and save the preferences you want to have in all Virex copies that you install on your network. To learn how to set Virex preferences, see Chapter 5, “Customizing the Virex Application” or Chapter 6, “Customizing the Virex Control Panel.”

3. Insert the floppy disk or other medium you want to use to install Virex on other computers on your network.

4. Press and hold the OPTION key on your keyboard, then click the Preferences button  in the Virex application, or click Preferences in the Virex control panel to open a file selection dialog box.

5. Choose the floppy disk you inserted as your destination, or the local hard disk or server disk you want to use for file distribution. Next, click Save. *Be sure to accept the default file name* that the application or control panel gives the file—otherwise, the Virex Installer might not recognize it.

   The Virex software will copy your preferences to the location you chose. If you want to use the preferences file with the Installer, be sure to copy it to the same folder that also contains the Installer application itself.

6. Use your copy of the Virex Installer, whether on high-capacity disk or CD-ROM, to install Virex software to each target computer. See "Installation steps" on page 16 for details. As the Installer works, it will pick up any custom preference files you saved along with it, and copy them to the correct locations.

7. Copy the custom preferences folder to the Virex Preferences folder in each target computer's System folder, if necessary. You'll find the Virex Preferences folder in this path: System folder:Preferences:Virex Preferences Folder.

Installing Virex software over a network

If you are a Macintosh network administrator who wants to install Virex software over a network, you have two options for doing so: the Virex Administrator and the Installer. The Virex Administrator provides complete, centralized control of network virus protection, including installation, diagnosis, repair and updates. To learn more about Virex Administrator, contact Network Associates Customer Care.

To use the Installer to set up Virex software from a file server, you must copy the Virex installation files to the server you want to use for the installation.

Follow these steps:

1. Create a destination folder named Virex Installer on the server.

2. Copy each of the Install Disk folders on the Virex CD-ROM, or on the CD-ROM image you mounted for installation, to the destination folder. Do not, however, copy the System folder from the Virex disc.

Next, move to each computer on which you want to install Virex software, or have individual users continue from this point.

Follow these steps:

1. Mount the server volume that hosts the Virex Installer folder.

   If you are an individual user, consult your network administrator—if necessary—to learn how to mount this file server volume.

2. Open the Virex Installer folder.

3. Follow the installation instructions that begin with Step 2 on page 13 in "Using the Virex Installer to scan your computer."

> **IMPORTANT:** Make sure you have purchased one Virex copy for every computer on which you plan to install the software. You may not install Virex software onto more computers than your license allows. If you have a site with a large number of Macintosh computers, contact Network Associates for affordable site license discounts.

Testing Your Installation

Once you install it, the Virex control panel is ready to scan your system for infected files. You can test whether it has installed correctly and verify that it can properly scan for viruses by implementing a test developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation, follow these steps:

1. Open a standard Macintosh text editor, such as SimpleText, then type:

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

> **NOTE:** The line shown above should appear as *one line* in your text editor window. You can, however, allow your text editor to wrap the line, provided you do not insert a hard return. If you are reading this guide on your computer, you can copy the line directly from the Acrobat file to SimpleText. You must be sure to remove the line break in the text you copy, however, for the file to work correctly.

2. Save the file with the name EICAR.TXT. The file size will be about 1KB. On larger hard disks, the file size might show as 4KB or higher, depending on how you have your hard disk formatted.
3. Activate the Virex control panel or start the Virex application and allow it to scan the disk or folder that contains EICAR.TXT. When Virex software examines this file, it will report that the file EICAR.TXT is an "EICAR Test Virus" test file and is not a real virus.

> **IMPORTANT:** Delete the file when you have finished testing your installation to avoid alarming other users.

Technical information

The Virex control panel includes a utility that can tell you which Virex version you have installed, along with which scan engine version and which Virus Definition file version you have. The utility also provides you with information about your computer and system software. You can use this information to determine whether you need to update your software, or to speak to a Network Associates technical support technician. To see this information, first install the Virex software according to the instructions in the previous sections, then follow these steps:

1. Choose Virex Control Panel from the Apple menu.
2. Click Help.
3. Click Technical Information.

Using the Virex Application 3

Starting the Virex application

The Virex application allows you to scan for viruses and Trojan horses, to repair any infected files you find, to update virus definition files electronically for both the Virex application and the Virex control panel, to create and update snapshots of your system, and to view and print Virex reports and log files.

To start the Virex application, double-click its application icon, which you'll find in the Virex folder on your hard drive. The Virex window will appear (Figure 3-1).

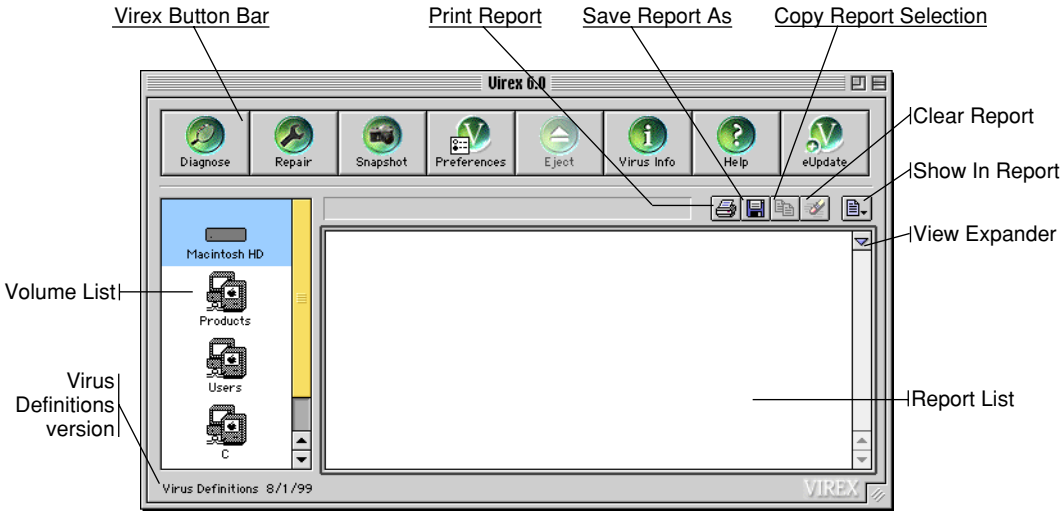


Figure 3-1. Virex window

The Virex window provides buttons, menus and a list of scan targets that you can use to start Virex scan operations and configure Virex options. The Virex window consists of these parts:

- **Virex button bar**. Convenient buttons provide you with control over basic Virex functions. Virex menus provide the same options that are available in the button bar.
- **Virex menus**. Virex menus provide full control over the application. Most menu items also have command-key equivalents, and some have a corresponding button in the button bar.

- **Volume List**. All volumes mounted on your computer—including hard disks, CD-ROM discs, server volumes and floppy disks—appear in this list. Choose which volumes you want to scan here.
- **Report List**. The Virex application tells you about its activities here. You can print this information, copy it to the Clipboard and paste it into another application, or save it to a number of different word processing file formats for later review.
- **Report Shortcut Buttons**. These buttons let you quickly print, save, copy, or clear information shown in the Report List.
- **Show in Report Button**. This button displays a pop-up menu that you can use to specify how much detail you want to appear in the Report List. Choose the items you want to record—those with a check mark beside them will appear in the report.
- **View Expander**. Click here to switch the Virex Report List between an outline view and a fully expanded view.
- **Virus Definitions Version**. This item tells you which version of the virus definition files you have installed. If your virus definition files are more than two months old, the version number appears in red to remind you to update the definitions.

On-line Virex help

The Virex application comes with Balloon Help and with its own on-line help system. Click the Help button  in the Virex button bar, or choose Virex Help from the Help menu to open the window shown in Figure 3-2.

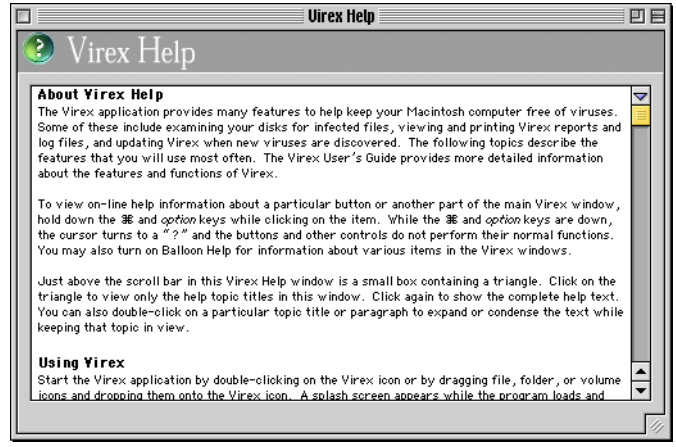


Figure 3-2. Virex on-line help window

To condense the information shown in this window into a list of topics, click  . To expand the topic list again so that it shows complete help information, double-click a topic title, or click  .

To view help information about a particular button or another part of the main Virex window, press ⌘ and OPTION on your keyboard, then click the item. The Virex Help window will open to the corresponding topic.

To see Balloon Help descriptions of buttons and window items, choose Show Balloons from the Help menu. Next, simply move your mouse over the item you want described. To turn Balloon Help off, choose Hide Balloons from the Help menu.

On-line virus descriptions

Click the Virus Info button  in the Virex button bar to open the Virus Info window. This window lists the names of and describes viruses and Trojan horses that appear on the Mac OS platform. Click  above the scroll bar to list only the virus names. Double-click a name, or click  to show complete virus information. To see more detailed information about macro viruses, visit the Dr Solomon website at http://www.drsolomon.com or the Network Associates website at http://www.nai.com.

Scanning for viruses and Trojan horses

Although the Virex control panel provides continuous background protection against virus infection, you should supplement this protection with a full system diagnosis at regular intervals to reduce the possibility of a successful virus attack to an absolute minimum. You can have the Virex application examine volumes, files and folders on your computer and provide detailed reports at any time. The following sections describe different ways to use the Virex application to perform virus and Trojan horse detection.

Scanning entire volumes

To scan the volumes listed in the Virex application window, follow these steps:

1. Choose which volumes you want the Virex application to scan.

   The application chooses an initial set of volumes in the volume list based on its default preferences. You can accept these choices, or click other volumes in the volume list for this scan operation. To learn how to change the initial volume set, see Chapter 5, “Customizing the Virex Application.”

2. Click the Diagnose button 

, or choose Selected Volumes from the Diagnose menu.

   As the application scans the volumes you selected, it displays a progress bar in its main window. Click the Stop button 

at any time to end the scan operation. The application reports its results in the Report List, which you can print or save to a file.

Scanning specific files or folders

To scan particular files or folders within a volume, follow these steps:

1. Choose Folder or File from the Diagnose menu, or press OPTION on your keyboard as you click the **Diagnose** button 

.

   A file selection dialog appears.

2. Choose the file or folder you want to scan.

3. Click Select or Select Item to begin the scan operation.

   As the application scans the item, it displays a progress bar in its main window. Click the Stop button 

at any time to end the scan operation. The application reports its results in the Report List, which you can print or save to a file.

Using drag and drop for diagnosis

The Virex application includes full support for drag-and-drop virus scanning, a convenient way to scan files, folders or volumes.

To use drag-and-drop scanning, follow these steps:

1. Choose Finder from the Application menu in the upper right corner of your screen.

2. Select, then drag a file, folder or volume icon on top of the Virex application icon. If the main Virex window is visible, you can also drag the icon on top of the Virex Diagnose button.

3. Release the mouse button.

The Virex application will start and immediately begin to scan the item you specified. As it works, the application displays a progress bar in its main window. Click the Stop button 

at any time to end the scan operation. The application reports its results in the Report List, which you can print or save to a file.

Repairing viruses and Trojan horses

When the Virex application repairs an infected file, it removes the virus code from the file and restores it to its original state. When the application detects a Trojan horse program, it simply deletes it (see Appendix D, "A Word About Computer Viruses and Trojan Horses," for examples of Trojan horse programs). Network Associates recommends that you replace infected files with uninfected copies of the original files, but if you do not have a virus-free copy, you can use the Virex application to repair nearly any infected file.

Before you use the Virex application to repair infected files:

- Read Appendix D, "A Word About Computer Viruses and Trojan Horses," which lists examples of viruses and Trojan horses and outlines the dangers they pose to your files and data.
- Unlock all disks, and any files locked with security software, that you want to repair. Anti-virus software cannot repair infected files on locked disks.
- Never unlock original application installation disks, including your Virex and Macintosh System installation disks. Unlocking these disks exposes them to possible infection, and robs you of the option to replace infected applications with fresh copies of the originals.

Repairing volumes

To repair infected files and delete Trojan horses on entire volumes, follow these steps:

1. Choose which volumes you want the Virex application to repair.

   The application chooses an initial set of volumes in the volume list based on its default preferences. You can accept these choices, or click other volumes in the volume list for this repair operation. To learn how to change the initial volume set, see Chapter 5, "Customizing the Virex Application."

2. Click the Repair button  , or choose Selected Volumes from the Repair menu.

   The application immediately looks for viruses and Trojan horses in the volumes you chose. Unless you tell it to repair infected files automatically, the application displays a dialog box similar to the one shown in Figure 3-3 on page 28 whenever it finds a virus or a Trojan horse. See "Customizing the Virex Application" on page 45 to learn how to set Virex preferences so that it repairs infected files automatically.

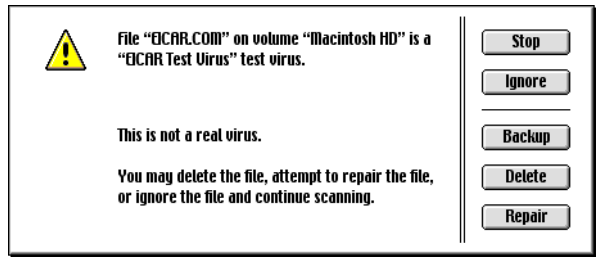


Figure 3-3. Virus Found dialog box

3. Tell the Virex application how you want to respond to the virus or Trojan horse. You can:

   - **Repair the infected file.** Click Repair to have the application remove the infecting virus code from the file.

     NOTE: The Virex application cannot repair Trojan horse files, compressed files, or files that a virus has corrupted beyond salvage. You should choose to delete Trojan horse files. To repair compressed files, on the other hand, first extract them from their archives, then repair them in a separate operation.

   - **Delete the infected file.** Click Delete to have the application remove the file from the volume permanently.

   - **Ignore the infection.** Click Ignore to have the application skip this file and continue its repair operation. Under normal circumstances, you should choose this response only if you know that the file is not infected. The Virex application will not repair files you tell it to ignore.

   - **Stop the repair operation.** Click Stop to halt the repair operation. To restart the operation, follow the previous steps again.

   - **Copy the file to a particular location.** Click Backup to have the application copy the infected file—without repairing it—to a folder or other location that you specify. In the unlikely event that the Virex application cannot repair the infected file, and if you have no original uninfected copy available, you can try to use a disk editing program or other methods to recover data from the backup copy before you delete it.

     NOTE: The Virex application will not back up Trojan horse files—these files contain no useful data and should be deleted.

Repairing specific files or folders

To repair specific files or folders, follow these steps:

1. Choose Folder or File from the Repair menu, or press and hold the OPTION key on your keyboard as you click the Repair button 

.

   A file selection dialog box will appear.

2. Select the file or folder you want to scan.

3. Click Select or Select Item to repair the file or folder you designate.

   The Virex application immediately looks for viruses or Trojan horse programs in the file or folder you selected. Unless you tell it to repair infected files automatically, the application displays a dialog box similar to the one shown in Figure 3-4 when it finds a virus or Trojan horse. See "Customizing the Virex Application" on page 45 to learn how to set Virex preferences so that it repairs infected files automatically.

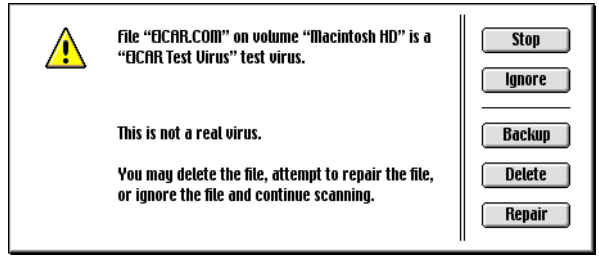


Figure 3-4. Virus Found dialog box

4. Tell the application how you want to respond to the virus or Trojan horse. You can:

   - **Repair the infected file.** Click Repair to have the application remove the infecting virus code from the file.

     NOTE: The Virex application cannot repair Trojan horse files, compressed files, or files that a virus has corrupted beyond salvage. You should choose to delete Trojan horse files. To repair compressed files, on the other hand, first extract them from their archives, then repair them in a separate operation.

   - **Delete the infected file.** Click Delete to have the application remove the file from the volume permanently.

- **Ignore the infection.** Click Ignore to have the application skip this file and continue with its repair operation. Under normal circumstances, you should choose this response only if you know that the file is not infected. The Virex application will not repair files you tell it to ignore.
- **Stop the repair operation.** Click Stop to halt the repair operation. To restart the operation, follow the previous steps again.
- **Copy the file to a particular location.** Click Backup to have the application copy the infected file—without repairing it—to a folder or other location that you specify. In the unlikely event that the Virex application cannot repair the infected file, and if you have no original uninfected copy available, you can try to use a disk editing program or other methods to recover data from the backup copy before you delete it.

> **NOTE:** The Virex application will not back up Trojan horse files—these files contain no useful data and should be deleted.

Using drag-and-drop repair

The Virex application includes full support for drag-and-drop file repair, a convenient way to remove infections from files and folders.

To drag and drop a file for the Virex application to scan, follow these steps:

1. Choose Finder from the Application menu in the upper right corner of your screen.
2. Select, then drag a file, folder or volume icon on top of the Virex Repair button  .
3. Release the mouse button.

The Virex application will start and immediately begin to scan the item you specified. As it works, the application displays a progress bar in its main window. Click the **Stop** button  at any time to end the repair operation. The application reports its results in the Report List, which you can print or save to a file.

Using Snapshots

Although Virex anti-virus software can help to restore your system after a virus attack by repairing infected files and deleting Trojan horses, knowing about potential attacks in advance can save your data and save you time. With its Snapshot feature, you can set the Virex software up as a kind of electronic sentry, so that it alerts you whenever the files on your system change in size or alter any of their other identifying characteristics. Most changes are predictable and harmless, but some unexpected changes might indicate the presence of a virus.

By taking Snapshots periodically, you can use Virex software to detect these changes, often *before* a virus can infect your system or cause damage. Virex Snapshots can also alert you to suspicious changes that could indicate that a new or previously unidentified virus has appeared on your system.

The following sections describe how to take and analyze Virex Snapshots.

Creating a baseline Snapshot

To use the Snapshot feature effectively, you must first take a "picture" of the current state of your system. The Virex software uses this "baseline" Snapshot as the standard against which it compares later Snapshot results. When it finds differences, it tells you about them. That's your signal to run a Virex scan operation to check for infected files.

To create a baseline Snapshot, follow these steps:

1. Select those volumes for which you want to create baseline Snapshots.

   The Virex software chooses an initial set of volumes in the volume list based on its default preferences. You can accept these choices, or click other volumes in the volume list for this Snapshot operation. To learn how to change the initial volume set, see Chapter 5, "Customizing the Virex Application."

2. Click the **Snapshot** button 

.

   An alert message will appear to tell you that Snapshot files for the volume or volumes you've selected do not exist now. The message will ask you whether you want to create a Snapshot file.

3. Click Create to continue.

The Virex software can take several minutes to create a baseline Snapshot for a large volume. When it finishes, the software will store the baseline Snapshot in the System folder of the volume you selected as a file named Virex Snapshot. If the volume does not have a System folder, Virex stores the baseline file on the top level of the volume you selected. If this file later gets deleted, you must create new baseline Snapshot before you can perform a Snapshot comparison.

Comparing volumes against their baseline Snapshots

Once you have created a baseline Snapshot for a volume, you can use the Virex Snapshot feature to detect changes in your files that might indicate a new virus. To do this, you must take a new Snapshot, then compare its results against the results from your baseline Snapshot.

To do so, follow these steps:

1. Select those volumes whose current states you want to compare against their baseline states.
2. Click the Snapshot button 

, or choose Compare Selected Volumes from the Snapshot menu.

   If any of the volumes you selected does not have an existing baseline Snapshot, an alert message will appear to tell you that Snapshot files for the volume or volumes you've selected do not exist now. The message will ask you whether you want to create a Snapshot file. See "Creating a baseline Snapshot" on page 31 for details.

   If each of the volumes you selected already has a baseline Snapshot, the Virex software will take the comparison Snapshot immediately. As it works, the software displays a progress bar in its main window. Click the Stop button 

 at any time to end the comparison. The application reports its results in the Report List, which you can print or save to a file.

Comparing a file or folder against the baseline snapshot

Once you have created a baseline Snapshot for a volume, you can use the Virex Snapshot feature to detect changes in your files that might indicate a new virus. To do this, you need to take a new Snapshot and compare its results against the results from your baseline Snapshot. You can do this on a file-by-file basis, or you can compare entire folders—without needing to compare entire volumes.

Follow these steps:

1. Choose Compare Selected Volumes from the Snapshot menu, or press OPTION on your keyboard as you click the Snapshot button  .
2. Select the file or folder you want to compare with its corresponding baseline Snapshot.
3. Click Select or Select Item to start the comparison.

   As it works, the application displays a progress bar in its main window. Click the Stop button  at any time to end the comparison. The application reports its results in the Report List, which you can print or save to a file.

Using drag-and-drop for baseline comparison

Once you have created a baseline Snapshot for a volume, you can use the Virex Snapshot feature to detect changes in your files that might indicate a new virus. To do this, you need to take a new Snapshot and compare its results against the results from your baseline Snapshot. Virex software includes full support for drag-and-drop Snapshot comparison.

Follow these steps:

1. Choose Finder from the Application menu in the upper right corner of your screen.
2. Select, then drag a file, folder or volume icon on top of the Virex Snapshot button  in the Virex window.
3. Release the mouse button.

The Virex application will start the snapshot comparison immediately. As the application works, it displays a progress bar in its main window. Click the Stop button  at any time to end the comparison. The application reports its results in the Report List, which you can print or save to a file.

Updating a baseline Snapshot for volumes

If a Snapshot comparison notes changes in a volume that you know do not result from a virus infection, you can update the baseline information for that volume so that the Virex software does not report the change each time it takes a new Snapshot.

Follow these steps:

1. Select the volumes whose baseline information you want to update.

   The Virex software chooses an initial set of volumes in the volume list based on its default preferences. You can accept these choices, or click other volumes in the volume list for the updated Snapshot. To learn how to change the initial volume set, see Chapter 5, "Customizing the Virex Application."

2. Choose Update Selected Volumes from the Snapshot menu. The dialog box shown in Figure 3-5 will appear.

Figure 3-5. Update baseline Snapshot dialog box

3. Click Update.

   The Virex software immediately begins to update the baseline Snapshot information for the volumes you selected. As the application works, it displays a progress bar in its main window. Click the Stop button at any time to end the baseline update operation. The application reports its results in the Report List, which you can print or save to a file.

Updating a file or folder in a baseline Snapshot

If a Snapshot comparison notes changes in a volume that you know do not result from a virus infection, you can update the baseline information for those files—without recreating the entire volume baseline—so that the Virex software does not report the change each time it takes a new Snapshot.

To do so, follow these steps:

1. Choose Update Folder or File from the Snapshot menu.
2. Select the file or folder that needs to have its baseline snapshot information updated.
3. Click Select or Select Item to start the baseline update.

   The Virex software asks you to confirm that you want to update your baseline snapshot (Figure 3-6).

Figure 3-6. Update baseline Snapshot dialog box

4. Click Update.

   The software immediately begins to update the baseline Snapshot information for the file or folder you selected. As it works, the application displays a progress bar in its main window. Click the Stop button at any time to end the update operation. The application reports its results in the Report List, which you can print or save to a file.

Deleting a baseline Snapshot

Network Associates recommends that you retain baseline information, updating it as necessary, to help the Virex application detect as-yet unidentified viruses. You can, however, delete the baseline Snapshot for a volume if necessary.

To do so, follow these steps:

1. Select the volumes for which you want to delete the baseline Snapshot.

   The Virex application chooses an initial set of volumes in the volume list based on its default preferences. You can accept these choices, or click other volumes in the volume list for this operation. To learn how to change the initial volume set, see Chapter 5, "Customizing the Virex Application."

2. Choose Remove From Volumes from the Snapshot menu.

   The application asks you to confirm your decision (Figure 3-7).

Figure 3-7. Remove baseline Snapshots dialog box

3. Click Remove.

   To prevent any accidental deletions, the Virex software asks you once again to confirm that you want to delete the baseline information for the volumes you selected.

4. Click Remove again to delete the baseline information.

Interpreting Snapshot comparison reports

Changes to files can result from many causes, not all of which indicate a potential infection. In order to interpret Virex Snapshot comparison reports effectively, you must look for certain patterns of activity that are characteristic of virus attacks. Armed with this information, you can decide when to perform a complete system scan, or whether to suspect that a previously unidentified virus might have infected your system.

Here are some examples of changes that you should consider suspicious:

- **Many files show changes.** Viruses tend to infect many files after they enter your system. If you see changes to a large number of files on your system over a period of time, this could indicate the presence of a virus. Some files, however—such as the Mac OS System file—change frequently as a matter of course because of normal system activity. Changes to this file do not *necessarily* point toward a virus infection.
- **Files change in a consistent manner.** If many of the files that report changes tend to report the same *types* of changes—similar-sized increases in the amount of disk space or RAM these files use, for example, or additions of particular code resources to files—you should suspect that a previously unidentified virus has infected your system.
- **Application files change for no apparent reason.** Ordinarily, most applications remain at a constant size. If an application program grows appreciably or has new code resources added, however, you should suspect that a previously unidentified virus has infected your system.

Use these examples to decide if the changes listed in your Snapshot comparison report are suspicious. If you suspect that a previously unidentified virus might have altered your files, first ensure that you have the latest Virex Virus Update file installed. If you still see the same sorts of changes, however, contact Network Associates. Contact information appears in Appendix H, “How to Contact Network Associates.”

Using the Virex Control Panel 4

Overview

The Virex control panel provides your system with continuous background protection from virus infections. It scans floppy disks and other removable media when you insert them, scans files as you download or open them, and scans your system when you start it and when you shut down. When it detects an infecting virus, the Virex control panel will offer to repair or delete the infected file. A flexible set of configuration options ensures that you can set the control panel to deliver the exact level of protection you need.

The Virex control panel also uses Virex's Snapshot feature to aid your ability to detect potential virus activity before it damages your system, and to alert you to possible threats from as-yet unidentified viruses. To do this, the Virex control panel automatically compares the current state of your system to a baseline state that you record and store for this purpose. It alerts you when it finds discrepancies between your computer's baseline state and its current state. To learn how to make or update the necessary baseline Snapshot, see "Creating a baseline Snapshot" on page 31 or "Updating a baseline Snapshot for volumes" on page 34.

Opening and configuring the Virex control panel

As soon as you install the Virex software and restart your computer, the Virex control panel immediately goes to work, scanning your system in accordance with its default preferences. Unless you later disable the Virex control panel, you do not have to take any other action to activate its background protection. To learn how to reactivate the Virex control panel after you disable it, see "Disabling the Virex control panel" on page 40.

To open the Virex control panel window, choose Control Panels from the Apple Menu , then double-click the Virex control panel icon . the Virex control panel window will appear (see Figure 4-1 on page 40).

Figure 4-1. Control Panel window

In most cases, the Virex control panel's default preferences provide a good balance between anti-virus protection and system performance. You can, however, choose different options that better suit your particular needs. See Chapter 6, "Customizing the Virex Control Panel," for details.

Disabling the Virex control panel

Network Associates recommends that you install and leave the Virex control panel activated so that it constantly monitors your system. If you need to disable it, however, you can:

- Choose Control Panels from the Apple Menu, then double-click the Virex control panel icon. Next, click the switch in the upper right corner of the Virex control panel window to turn it to the OFF position.

  To reactivate the Virex control panel, click the switch again to turn it to the ON position.

- Click the Virex Control Strip module, then choose Off from the menu that appears (Figure 4-2). To reactivate the Virex control panel, choose On from this same menu.

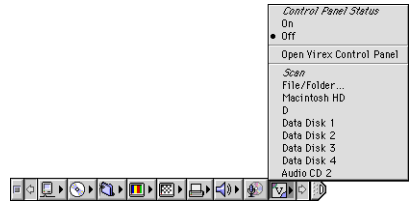


Figure 4-2. The Virex Control Strip module and menu

NOTE: You do *not* need to disable the Virex control panel in order to install software.

Using the control panel to scan floppy disks

By default, the Virex control panel will scan floppy disks as soon as you insert them into your drive (Figure 4-3). To learn how to change this preference, see "Customizing the Virex Control Panel" on page 51.

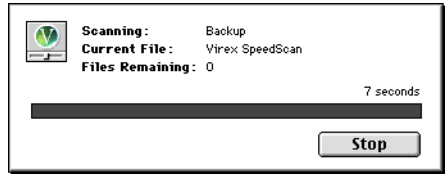


Figure 4-3. Scanning a floppy disk

As the Virex control panel scans floppy disks, it looks for viruses and Trojan horses. If it doesn't find any, the scan operation finishes and the floppy disk mounts normally on your desktop. If the Virex control panel finds a virus or Trojan horse, however, it will alert you and offer you the options shown in Figure 4-4.

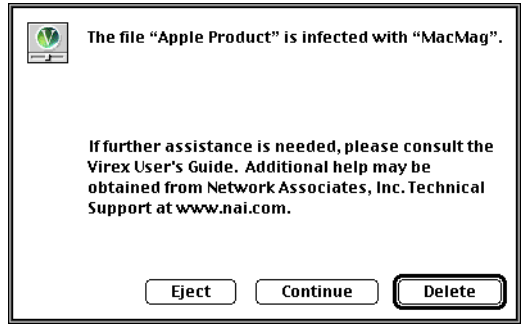


Figure 4-4. Virus Found dialog box

Click one of the buttons shown to tell the control panel how to respond. You can:

- **Tell the Virex control panel to repair the file.** Click Repair to have the Virex control panel remove all known virus code from the infected file.

> **NOTE:** The Virex control panel displays this option only if it has the capability to repair the file. In the example shown, this option does not exist.

- **Delete the file from the disk.** Click Delete to have the Virex control panel delete the infected file permanently.

  NOTE: The Virex control panel displays this option only if it *cannot* repair the file at all.

- **Allow the floppy disk to mount.** Click Continue to stop the scan operation and allow the floppy disk to appear on your desktop.

  WARNING: If you choose this option, you risk infecting your computer. Network Associates recommends that you do so only if you know that the file that the Virex control panel flagged is not infected.

- **Eject the floppy disk.** Click Eject to have the Virex control panel eject the infected floppy disk immediately.

Using the Control Panel to scan files and folders

Although the Virex control panel normally scans your entire system in the background, you can direct its attention to particular files and folders. This lets you scan particular items without starting the Virex application.

Follow these steps:

1. Choose Control Panels from the Apple Menu, then double-click the Virex control panel icon to open the Virex control panel window (see Figure 4-1 on page 40).

2. Click Scan to open a file selection dialog box (Figure 4-5).

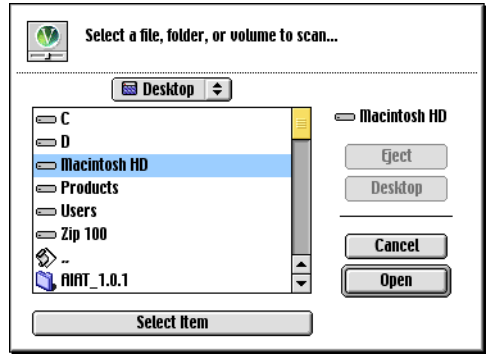


Figure 4-5. Choosing an item to scan

3. Select a file or folder in the list shown, then click Select Item.

   The Virex control panel looks for viruses and Trojan horses in the item you selected.

Using Virex contextual menus

Virex contextual menus integrate Virex scanning directly into the Macintosh Finder and into other applications that support contextual menus. If your computer runs Mac OS 8.0 or later, and you have the Contextual Menu Manager extension enabled, a contextual menu appears whenever you hold the Control key on your keyboard as you click an icon in the Finder.

The menu that appears offers you a set of commands appropriate for the icon you selected (Figure 4-6). To display Virex scan options, you must have the Virex Contextual Menu plug-in installed.

Figure 4-6. Virex contextual menu

Choose Scan with Virex to have Virex look for viruses or Trojan horses in the item you selected. You can select a file, folder, hard disk volume, or other item.

Using the Virex DropScan utility

The Virex DropScan utility provides instant drag-and-drop scanning on your Macintosh desktop. Simply select an item while you are in the Finder, drag it on top of the DropScan icon, then release your mouse button to have the utility scan that item immediately (Figure 4-7).

Figure 4-7. Dragging a hard disk volume to Virex DropScan

NOTE: The Virex DropScan utility can serve as a quick alternative if you do not have Virex contextual menus enabled. To use the DropScan utility, you must have the Virex control panel installed.

Using the Virex Control Strip module

The Virex Control Strip module gives you convenient access to the Virex control panel from the Macintosh Control Strip. To use the module, click the Virex icon on the Control Strip, then choose any of the commands you need from the menu that appears (Figure 4-8).

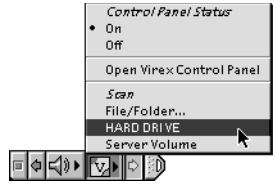


Figure 4-8. Virex Control Strip menu

You can check the working status of the Virex control panel from this menu, open it, or turn it off or on. The Virex Control Strip also dynamically updates the items available under its Scan heading in the menu, which makes scanning any mounted volume quick and easy. To scan individual files or folders, choose File/Folder to open a file selection dialog box.

To use the Virex Control Strip module, you must install both it and the Virex control panel.

Customizing the Virex Application 5

Overview

Although the default preferences that come with the Virex application provide good protection for your system, you can choose different preferences to suit your needs and work habits. To choose your preferences, start the Virex application, then click the Preferences button 

, or choose Preferences from the Edit menu.

The Preferences dialog box organizes the options available for the Virex application into five groups: Diagnose, Repair, Startup, Report, and EUpdate. To choose Virex options, click the icon that corresponds to the group of preferences you want to set—the window will shift to display the available options for that group. The next sections describe the options available in each preference group, with the exception of the EUpdate preferences. See Chapter 8, "Updating Virex," for a complete discussion of the configuration options for this group.

Virex application Diagnose preferences

The Virex application's Diagnose preferences govern how it conducts scan operations, how it alerts you when it finds a virus, and what information it reports as it works (Figure 5-1). Use these options to determine how much protection against viruses and Trojan horses you want the Virex application to give your system, and how much information you want to see during a scan operation.

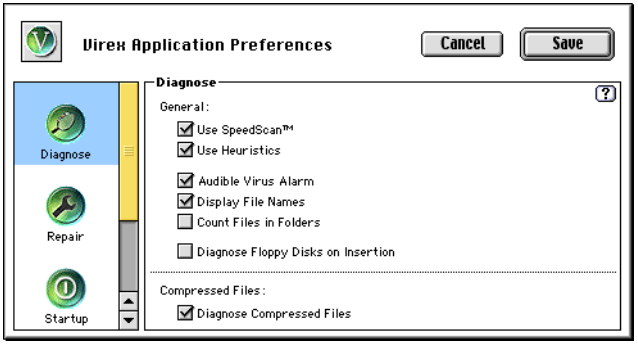


Figure 5-1. Diagnose preferences panel

Your options are:

- **Use SpeedScan.** Select this option to have the Virex application use its proprietary SpeedScan technology to scan files and volumes. This option is active by default—clearing the checkbox causes the Virex application to scan more slowly.
- **Use Heuristics.** Select this option to have the Virex application use proprietary heuristic scanning technology to detect previously unidentified viruses. This option is active by default—clearing the checkbox might cause the Virex application to miss some as-yet unidentified viruses.
- **Audible Virus Alarm.** Select this option to have the Virex application beep when it finds a virus. The Virex application will use the system alert sound you've chosen for other applications on your computer. This option is active by default—clearing the checkbox tells the application to give you only the visual alert messages it ordinarily uses when it finds a virus.
- **Display File Names.** Select this option to have the Virex application display the name of each file that it examines during a scan operation. This option is active by default—clearing the checkbox tells the application not to display file names, which can cause it to scan faster.
- **Count Files in Folders.** Select this option to have the Virex application count the number of files in each folder it scans. This option is not active by default—selecting it provides you with additional information, but can slow down scan operations.
- **Diagnose Floppy Disks on Insertion.** Select this option to have the Virex application examine each floppy disk as you insert it into your floppy drive. The application will examine, then eject each disk in turn. This option is not active by default—selecting it lets you scan a number of floppy disks at once.
- **Diagnose Compressed Files.** Select this option to have the Virex application look for viruses inside StuffIt, Compact Pro, and Zip archives. This option is active by default—clearing the checkbox tells the Virex application not to scan inside compressed files. This can cause the application to miss some viruses, but the program will also scan faster.

> **NOTE:** The Virex control panel scans inside only those Zip archives created by "imploding" or "deflating" files.

Virex application Repair preferences

The Virex application's Repair preferences govern how it responds automatically when it finds a virus or a Trojan horse program (Figure 5-2). Use these options to have the Virex application remove virus code from infected files or delete harmful programs without your intervention.

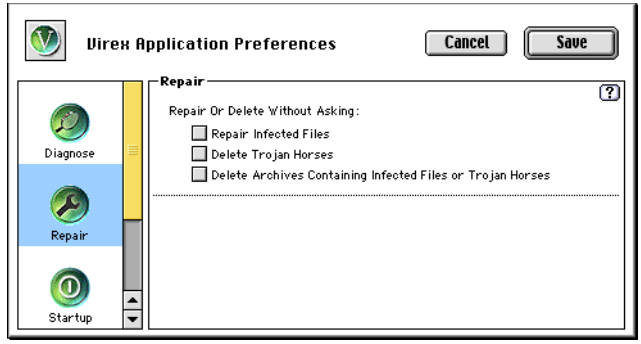


Figure 5-2. Repair preferences panel

Your options are:

- **Repair Infected Files.** Select this option to have the Virex application repair virus-infected files without asking you to respond. This option is not active by default—instead, the Virex application asks you each time it finds an infected file whether it should repair it.
- **Delete Trojan Horses.** Select this option to have the Virex application delete Trojan horse programs as soon as it detects them, without asking you to respond. This option is not active by default—instead, the application asks you each time it finds a Trojan horse whether it should delete it.
- **Delete Archives Containing Infected Files or Trojan Horses.** Select this option to have the Virex application delete infected files or Trojan horse programs saved in StuffIt, Compact Pro, or Zip archives without asking you for a response. This option is not active by default—instead, the application asks you each time it finds a Trojan horse or an infected file in a compressed archive whether it should delete the archive.

Virex application Startup preferences

The Virex application's Startup preferences tell it which volumes, files, or other items it should scan as soon as it starts (see Figure 5-3 on page 48). Set these preferences if you have a series of items that you want the application to scan consistently, without your needing to tell it to do so. The Virex application lists the items you choose here as its initial selection in its volume list when you first start it. You can choose different items for each scan operation, or you can use these selections as default options.

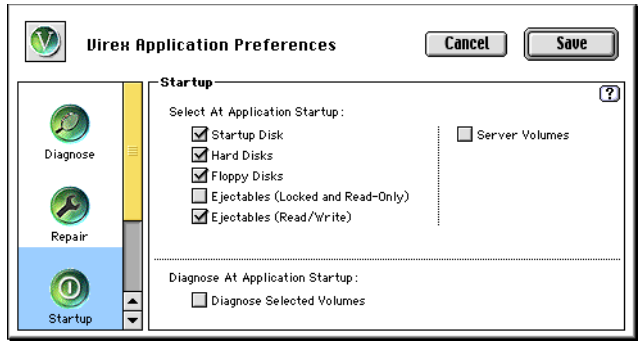


Figure 5-3. Startup preferences panel

Your options are:

- **Startup Disk.** Select this option to have the Virex application select the startup disk in the volume list. This option is active by default.
- **Hard Disks.** Select this option to have the Virex application select the local hard disks on your computer in the volume list. This option is active by default.
- **Floppy Disks.** Select this option to have the Virex application select any floppy disks you have in your floppy drive as you start the program. This option is active by default.
- **Ejectables (Locked and Read-Only).** Select this option to have the Virex application select locked and read-only ejectable disks or other items in the volume list. Examples of these items include CD-ROM discs, locked cartridge drives and read-only optical drives. This option is not active by default—unless a virus infected them before they were locked or manufactured, such disks cannot get infected.
- **Ejectables (Read/Write).** Select this option to have the Virex application select ejectable disks or other items to which you can save files. Examples include cartridge drives, Zip or Syquest drives, and optical drives. This option is active by default.

- **Server Volumes.** Select this option to have the Virex application select server volumes that you have mounted on your computer. This option is not active by default.
- **Diagnose Selected Volumes.** Select this option to have the Virex application scan the volumes you've designated elsewhere in this panel as soon as you start it, instead of waiting for you to click 

or 

. This option is not active by default.

Virex application Report preferences

The Virex application's Report preferences tell it how to display information in the Report List, how often to clear the it, whether to save it as a file automatically, and where to save it.

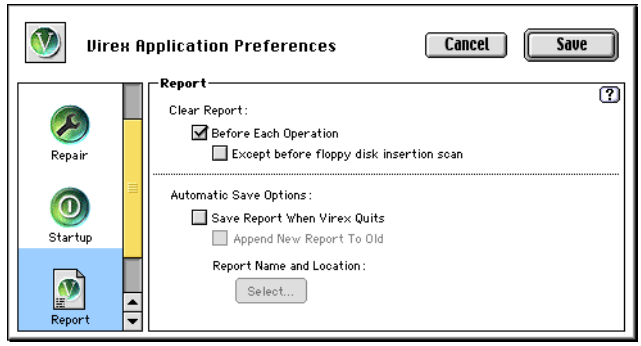


Figure 5-4. Report preferences panel

Your options are:

- **Clear Report Before Each Operation.** Select this option to have the Virex application clear the Report List before it runs a scan operation. This option is active by default; each scan operation produces a fresh report. Clearing the checkbox causes the application to append its scan results to the end of the Report List.
- **Clear Report except before floppy disk insertion scan.** Select this option to have the Virex application add the results from any scan operations it performs on floppy disks to the existing Report List, rather than clearing the Report List each time you insert a disk. You can choose this option only if you have already chosen to clear the Report List before each scan operation. This option is not active by default. You might want to select this option if you plan to scan many floppy disks at a time and want the Virex application to generate a single report that includes all floppy disk scan results.

- **Save Report When Virex Quits.** Select this option to have the Virex application automatically save the Report List as a file in a location you specify. This option is not active by default—because it is not, the application discards its scan results each time it quits unless you select this option.
- **Append New Report To Old.** Select this option to have the Virex application automatically add its scan results to the existing report file as it quits. You can choose this option only if you have already chosen to have the application save the Report List as it quits. This option is not active by default—instead, the Virex application creates a new report file each time it quits if you ask it to save its scan results. If a report file already exists, the application appends a number to the same file name and saves the new file with that name.
- **Report Name and Location.** Click Select to open a file selection dialog box and choose a location for the Virex application to save its report files. By default, the application saves these files on the Macintosh Desktop.

Virex application EUpdate Preferences

The Virex application's EUpdate Preferences govern how and from where the Virex software downloads new Virus Definition files. You can tell the software to download new files from an FTP site on the Internet, or from a particular server on your network. You can also designate which protocol to use —TCP/IP or AppleTalk—to accomplish the update. The preferences you set here provide a framework for the application to use when you initiate or schedule an update operation, but do not start the update itself. See Chapter 8, "Updating Virex," for a complete discussion of all of the issues involved in updating your files.

Customizing the Virex Control Panel 6

Overview

Although the default preferences that come with the Virex control panel provide a good general balance between anti-virus protection and system performance, your particular work requirements might call for a different set of options. The Virex control panel gives you complete control over a range of flexible configuration options that you can use to tailor the program to your needs.

Setting Virex control panel preferences

To set preferences for the Virex control panel, follow these steps:

1. Choose Control Panels from the Apple Menu, then double-click the Virex control panel icon. the control panel window will appear (Figure 6-1).

Figure 6-1. Control Panel Window

2. Click Preferences to open the Virex control panel Preferences dialog box (see Figure 6-2 on page 52).

   The Preferences dialog box for the Virex control panel organizes its available options into six groups: General, File Access, Automatic, Keyboard, Security, and Alerts. Click the icon that corresponds to the group of preferences you want to set, choose the options you want, then click Save at the top of the dialog box to record your changes and close the dialog box. The next sections describe the options available in each preference group.

Virex control panel General preferences

The control panel's General preferences govern how the program loads into the Mac OS environment, how it conducts scan operations, how it alerts you when it finds a virus, and what information it reports as it works (Figure 6-2). Use these options to determine how much protection against viruses and Trojan horses you want the control panel to give your system, and how much information you want to see during a scan operation.

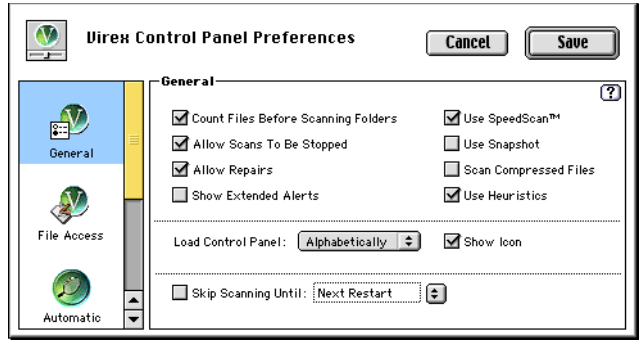


Figure 6-2. General preferences panel

Your options are:

- **Count Files Before Scanning Folders.** Select this option to have the Virex control panel count the files included in folders that it scans. This option is active by default—clearing the checkbox causes the control panel to provide file counts only when it scans volumes. It will scan folders slightly faster, however.
- **Allow Scans To Be Stopped.** Select this option to have the Virex control panel display a Stop button as it runs scan operations. This option is active by default—clearing the checkbox prevents you from stopping a scan operation in progress.
- **Allow Repairs.** Select this option to have the choice to repair infected files as the control panel finds them. This option is active by default—clearing the checkbox removes file repair as a possible response when the control panel finds a virus.
- **Show Extended Alerts.** Select this option to have the Virex control panel display an alert message whenever it cannot scan a file because it does not have adequate access permissions, because of file damage, or because of other access errors. This option is not active by default—leaving the checkbox clear causes the control panel to notify you only when critical errors occur or when it finds a virus.

- **Use SpeedScan.** Select this option to have the Virex control panel use its proprietary SpeedScan technology during scan operations. This option is active by default—clearing the checkbox causes the control panel to scan items more slowly.
- **Use Snapshot.** Select this option to have the Virex control panel compare any existing baseline Snapshots you've made to the current state of your system to try to detect previously unidentified viruses. This option is not active by default—leaving the checkbox clear keeps the control panel from doing Snapshot comparisons. This can cause it to miss potential infections, but your scan operations will run faster.
- **Scan Compressed Files.** Select this option to have the Virex control panel look for viruses and Trojan horse programs inside StuffIt, Compact Pro, Disk Doubler, Auto Doubler, Now Compress and Zip archives.

  NOTE: The control panel scans inside only those Zip archives created by "imploding" or "deflating" files.

  This option is not active by default—leaving the checkbox clear causes the control panel to bypass compressed files during scan operations, which makes the operations run faster. You can still prevent infections from viruses inside compressed files, however. To do so, select the **Scan Files When Opened** option in the Virex control panel File Access preferences. This tells the control panel to scan each file after you have already extracted it and as you first open it. Because infecting viruses will not have a chance to activate before the control panel scans them, you will still have full anti-virus protection.
- **Use Heuristics.** Select this option to have the Virex control panel use proprietary heuristic scanning technology to detect previously unidentified viruses. This option is active by default—clearing the checkbox might cause the control panel to miss some as-yet unidentified viruses.
- **Load Control Panel.** Choose one of the options shown in this pop-up menu to specify where in your computer's startup sequence the Virex control panel will load. Specifying a different load order for the control panel can in some cases prevent other extensions and control panels from conflicting with it.

  Choose First to have the control panel load before all other extensions and control panels. Choose Last to have the control panel load after all other extensions and control panels have loaded. Choose Alphabetically to rearrange the load order for all control panels and extensions so that they load in alphabetical order according to the first character in their names. By default, the control panel loads alphabetically.

- **Show Icon.** Select this option to have the Virex control panel display its icon in the lower portion of your screen as it loads during your startup sequence. This option is active by default—clearing the checkbox causes the control panel to load without displaying an icon.
- **Skip Scanning Until.** Select this option to prevent the Virex control panel from scanning your system for a period that you specify. You can choose to disable scanning for a certain number of minutes—**5**, **10**, **15**, **30**, **45** or **60**—or until you restart your computer. This option is not active by default—selecting the option disables scanning until your next restart unless you choose a different time period.

> **NOTE:** Use this preference in order to disable scanning temporarily and to restore it automatically, without your having to remember to do so.

Virex control panel File Access preferences

The Virex control panel's File Access preferences tell Virex when it should actually perform its scan operations (Figure 6-3). Ordinarily, the control panel examines files for viruses only when you open or download them—scanning all files on your system continuously would needlessly degrade system performance. Because most viruses spread only when their host program starts, scanning for them each time you open a file provides robust anti-virus protection.

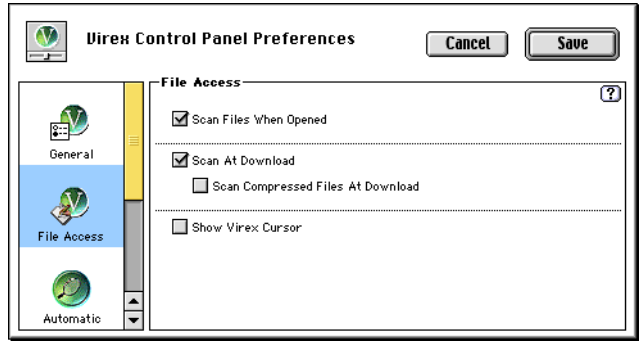


Figure 6-3. File Access preferences panel

Your options are:

- **Scan Files When Opened.** Select this option to have the Virex control panel look for viruses and Trojan horses each time you open a file, whether you do so from inside a running program, or by double-clicking it from the Finder. This option is active by default—clearing the checkbox causes the control panel not to provide this protection. If you disable this option, be sure to use the Virex application to conduct regular scan operations to prevent infections.

  > **NOTE:** The Virex SpeedScan technology works so quickly that you will not usually notice any delays when you open files.

- **Scan At Download.** Select this option to have the Virex control panel look for viruses and Trojan horses as you download or copy files to your computer. This option is active by default, which can help the control panel detect viruses before their host program ever starts. Clearing this checkbox causes the control panel not to provide this protection.

- **Scan Compressed Files At Download.** Select this option to have the Virex control panel look for viruses inside StuffIt, Compact Pro, and Zip archives as you download or copy them to your computer.

  > **NOTE:** The control panel scans inside only those Zip archives created by “imploding” or “deflating” files.

  This option is not active by default. If you have selected the **Scan At Download** option, which scans files as soon as you extract them from an archive, you may not need to choose this option. Because many e-mail applications, communication programs, and web browsers extract files automatically after you download them, the first opportunity the control panel might have to scan these files will come when you open them.

- **Show Virex Cursor.** Select this option to have the Virex control panel change your cursor briefly as it scans those files you open or download. This option is not active by default—leaving the checkbox clear tells the control panel not to change your cursor as it scans.

Virex control panel Automatic preferences

The Virex control panel's Automatic preferences determine which volumes it should scan automatically. You can also tell the control panel to scan specific items each time you start and shut down your computer (Figure 6-4). Use this set of preferences to supplement the options you choose in the File Access preferences panel. Because the control panel scans each volume as it mounts on your desktop, you can catch some infections before you start their host programs.

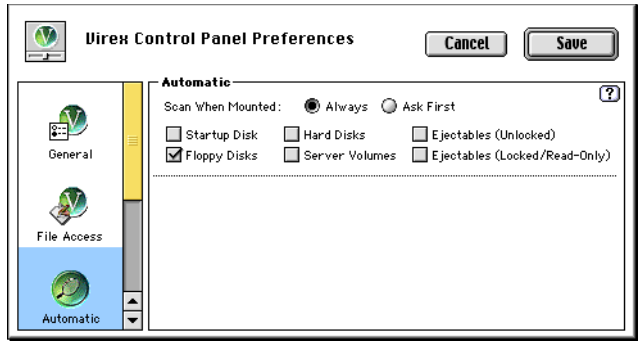


Figure 6-4. Automatic preferences panel

Your options are:

- **Scan When Mounted.** Click one of these buttons to have the Virex control panel scan the items you specify elsewhere in this panel, either as soon as they mount on your desktop, or after you respond to a dialog box that asks you to confirm that you want them scanned. The **Always** option is active by default. To prevent the control panel from scanning any of the items listed in this panel, be sure to clear each checkbox shown.
- **Startup Disk.** Select this option to have the Virex control panel scan your startup disk as it mounts on your desktop. This option is not active by default—selecting it provides your system with excellent protection, but can lengthen the time it takes until you can work with your files.
- **Floppy Disks.** Select this option to have the Virex control panel scan each floppy disk as you insert it. This option is active by default—clearing the checkbox causes the control panel to mount floppy disks on your desktop without scanning them, which can open your system to potential infection.

- **Hard Disks**. Select this option to have the Virex control panel scan all of your hard disks as they mount on your desktop. This option is not active by default—selecting it provides your system with excellent protection, but can lengthen the time it takes until you can work with your files.

> **NOTE:** Some removable disk manufacturers now mount cartridge drives as hard disks, not as ejectable disks. Selecting this option will cause the control panel to scan those types of drives.

- **Server Volumes.** Select this option to have the Virex control panel scan remote server volumes as they mount on your desktop. This option is not active by default—selecting it provides your system with excellent protection, but can lengthen the time it takes until you can work with your files.
- **Ejectables (Unlocked).** Select this option to have the Virex control panel scan ejectable disks, or other items to which you can save files, as they mount on your desktop. Examples of these drives include cartridge drives, Zip or Syquest drives, and optical drives. This option is not active by default—selecting it protects your system against potential infection, but can lengthen the time it takes until you can work with your files.
- **Ejectables (Locked/Read-Only)**. Select this option to have the Virex control panel scan locked and read-only ejectable disks as they mount on your desktop. Examples of these items include CD-ROMs, locked cartridge drives, and read-only optical drives. This option is not active by default—unless a virus infected them before they were locked or manufactured, such disks cannot get infected.

Virex control panel Keyboard preferences

The Virex control panel's Keyboard preference panel lets you specify keyboard combinations and other shortcuts for control panel functions (Figure 6-5).

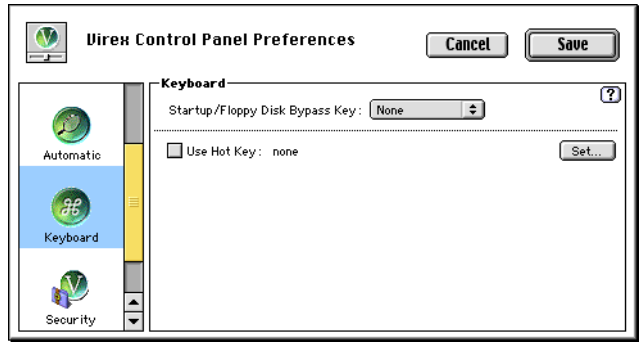


Figure 6-5. Keyboard preference panel

Your options are:

- **Startup/Floppy Disk Bypass Key.** Select this option to designate a key that you can press and hold when you start your computer to prevent the Virex control panel from loading as part of your computer's startup sequence. If you press this same key when you insert a floppy disk, Virex will not scan the disk. By default, no key is active. You can choose CAPS LOCK, CONTROL, OPTION, SHIFT, or ⌘.

  NOTE: Network Associates recommends that you do not disable the control panel in this manner, as you can expose your computer to potential infection.

- **Use Hot Key.** Select this option to have the Virex control panel start a scan operation whenever you press a particular key combination. This option is not active by default—if you leave the checkbox clear, the control panel will not respond to the key combination you choose.

- **Set.** Click this button to open a dialog box where you can specify the key combination you want to use to start a control panel scan operation. Next, press any combination of characters and modifier keys, then click OK to save your preferences and close the dialog box.

Virex control panel Security Preferences

The Virex control panel's Security preference panel lets you set a password to keep the options you choose safe from unauthorized changes, and to prevent your computer from mounting ejectable disks (Figure 6-6). If you are a system administrator, you can use this feature to enforce a strict anti-virus security policy for all Macintosh computer users on your network.

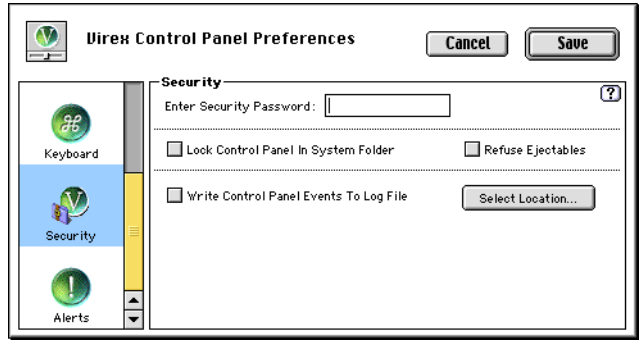


Figure 6-6. Security preferences panel

Your options are:

- **Enter Security Password.** Type a secure password in this text box in order to protect the control panel preferences you choose from unauthorized changes. The control panel will ask you for this password whenever you or anyone else tries to open it. This option is not active by default.
- **Lock Control Panel In System Folder.** Select this option to prevent users from moving, renaming or deleting the Virex control panel. This option is not active by default.
- **Refuse Ejectables**. Select this option to have the Virex control panel immediately eject floppy disks and other removable media when you insert them. This option is not active by default.
- **Write Control Panel Events To Log File**. Select this option to have the Virex control panel keep a record of its activity in a log file you specify. By default, the control panel does not record its activity.

> **NOTE:** If you select this option, you should also delete the log file periodically to prevent it from becoming too large.

- **Select Location.** Click this button to designate a place for the control panel to use to save its log file. The control panel gives the file the default name control panel Log. You can enter a different name if you wish.

Virex control panel Alerts Preferences

The Virex control panel's Alert preference panel lets you designate which response buttons should appear as default choices in the control panel's alert messages (Figure 6-7). These messages appear in an alert dialog box whenever the control panel finds a virus, and during other crucial events. You can also specify alert messages that you want to appear in these dialog boxes, or have the control panel "click" the default button after an interval you choose.

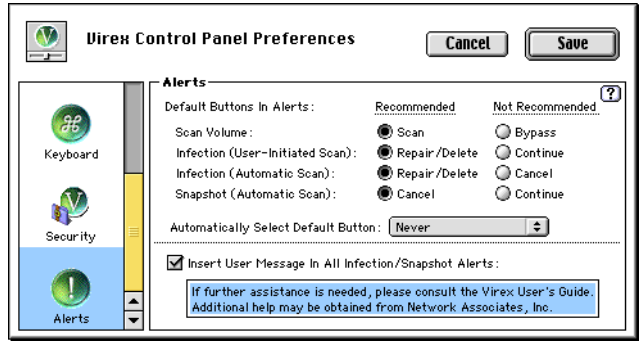


Figure 6-7. Alerts preference panel

Your choices are:

- **Scan Volume.** Click one of these buttons to specify a default button for the alert box that appears if you enable the Ask First option in the Automatic preference panel. The dialog box appears as soon as a designated volume mounts—you can specify Scan or Bypass as the default choice.

  NOTE: Network Associates recommends that you set Scan as the default choice to encourage users to scan volumes as they mount.

- **Infection (User-Initiated Scan).** Click one of these buttons to specify a default button for the alert box that appears when the control panel finds a virus during a scan operation that you started yourself. You can specify Repair/Delete, or Continue.

  NOTE: Network Associates recommends that you set Repair/Delete as the default choice to encourage users to repair all infected files and delete all Trojan horses.

- **Infection (Automatic Scan).** Click one of these buttons to specify a default button for the alert box that appears when the control panel finds a virus during an automatic scan operation. This dialog box will appear if the control panel finds a virus when you either open or download a file. You can specify Repair/Delete, or Continue.

  NOTE: Network Associates recommends that you set Repair/Delete as the default choice to encourage users to repair all infected files and delete all Trojan horses.

- **Snapshot (Automatic Scan).** Click one of these buttons to specify a default button for the alert box that appears when the control panel finds a discrepancy during a Snapshot comparison. You can specify Cancel or Continue.

  NOTE: Network Associates recommends that you set Cancel as the default choice to discourage users from opening files that might harbor new viruses.

- **Automatically Select Default Button.** Choose an interval for the Virex control panel to wait before it "clicks" the default buttons you designate elsewhere in this panel. This causes the control panel to respond to its own alert messages without input from users—you might use this, for example, to proceed with scheduled scan operations on computers left unattended. The control panel does not have this option active by default—to activate it, choose a particular interval. Your choices are: Immediately, 5, 10, 15, 30, 45 and 60 seconds.
- **Insert User Message In All Infection/Snapshot Alerts.** Select this option to have the Virex control panel insert a custom message in each of the alert dialog boxes it displays. Next, enter the message you want users to see in the text box provided. You might want to list contact information for users to locate system administrators and or other people they can turn to for answers to their questions or solutions to their problems.

Scheduling Virex Operations 7

What does Virex Schedule Editor do?

The Virex Schedule Editor runs scan operations and other tasks on the dates and at the times you choose, or at intervals you set. Use the Schedule Editor to run a scan operation in your absence, when it causes the least disruption to your work, as part of a series of automated tasks, or in other ways that suit your needs. You can also use the Schedule Editor in conjunction with the Virex EUpdate feature to download and install new Virus Definition files as they become available.

Why schedule Virex operations?

Although Virex software includes components that look for viruses continuously or that allow you to scan your system whenever you want, you can schedule regular scan operations and other Virex activities to

- **Set a periodic baseline for your system.** If you want to track your system or your network for recurring virus activity, schedule a full scan of your system at regular intervals. The reporting features included in the Virex application can provide you with a complete report on the number, type, size and other characteristics of any viruses it finds.
- **Supplement or replace on-access scanning.** Network Associates recommends that you use the Virex control panel to scan continuously for viruses, but if your environment doesn't permit you to use the control panel or if you have other concerns about system performance, schedule frequent scan operations to prevent infections. Even if you do use the control panel, scheduling periodic full scans of your system reduces the likelihood that infected files remain undetected.
- **Alternate between scan operations.** Scheduled scanning operations give you the flexibility to choose different operations for different purposes or different times. If, for example, you want to use the control panel to scan your own system continuously and scan mounted network drives less frequently, you can schedule a task for this purpose.
- **Update your Virus Definition files regularly.** New viruses emerge frequently, so updating your virus definition files regularly is essential for anti-virus security. With the Virex EUpdate feature, you can designate a location from which to download new definition files. The Schedule Editor will help you to automate this process so that you enjoy maximum protection.

Starting the Virex Schedule Editor

To start the Schedule Editor, follow these steps:

1. Start the Virex application. To learn how to do this, see "Starting the Virex application" on page 23.
2. Choose Edit Schedule from the Schedule menu.
3. The Schedule Editor dialog box will appear (Figure 7-1).

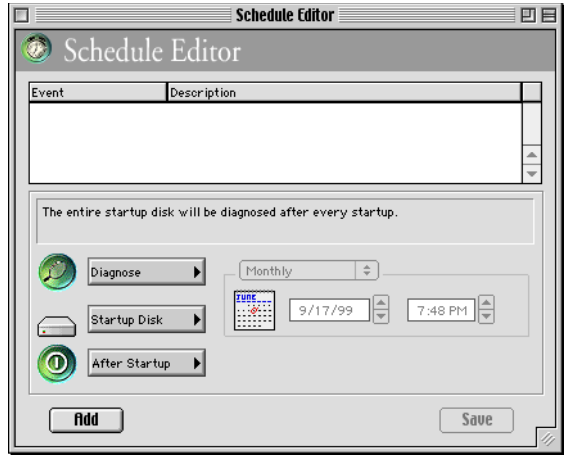


Figure 7-1. Schedule Editor dialog box

Scheduling a scan task

To schedule a diagnosis or repair operation so that it runs automatically and in your absence, you need to specify whether you want to conduct a diagnosis or a repair operation, which disks you want scanned or repaired, and when you want the operation to run. By default, the Schedule Editor does not come with any scan tasks predefined.

NOTE: To run a scheduled task, you must have the Virex Scheduler extension active in your Extensions folder in your System folder.

To schedule a new task, follow these steps:

1. Choose Diagnose or Repair from the top menu in the series of three menus in the Schedule Editor dialog box. To learn more about the distinction between a diagnosis and a repair, see "Scanning for viruses and Trojan horses" on page 25 and "Repairing viruses and Trojan horses" on page 27.

2. Choose your scan targets from the second menu from the top. Your options are:

   - **System Folder.** Choose this option to diagnose or repair only the System folder on your startup disk. This has the advantage of giving you protection in the most frequent target for virus attacks and usually results in a very quick scan operation, but it might miss many viruses that lurk elsewhere on your hard disk. Network Associates recommends that you do not us this option as your sole scan operation. You should consider using it to supplement more thorough scan tasks, perhaps on a daily or more frequent basis.

   - **Startup Disk.** Choose this option to diagnose or repair only the hard disk that contains an active copy of your System folder. This operation is much more thorough than the System folder–only operation, but it can leave you vulnerable to viruses that reside on mounted network disks or removable disks. As with the System folder scan operation, Network Associates recommends that you alternate this type of scan operation with a more thorough scan operation.

   - **Network Disks.** Choose this option to confine your scan operation to mounted network disks. Without a scan operation that targets local hard disks, using only this scan operation can leave your computer vulnerable to infection. Network Associates recommends that you alternate this option with a scan task that examines your local hard disk for viruses, and that you schedule this operation late at night or at a time when network usage is low. The speed of this scan operation depends on the number and size of the disks you have mounted on your desktop.

   - **All Disks.** Choose this option to scan all disks mounted on your desktop, including local hard disks, removable disks, and mounted network disks. This option offers the most comprehensive anti-virus protection for your system, but will take the longest time. Network Associates recommends that you run this operation late at night or at a time when network usage is low.

   You can also select and drag any individual item or group of items that you want to scan from the Macintosh desktop and drop it onto the Event List in Schedule Editor window to designate your scan targets. Be sure to select and drag all of the scan targets that you want to include in a single task to the Event List at the same time. Dragging scan targets to the list individually will create a separate task for each scan target.

3. Choose a time in which to run the operation from the third menu. Your options are:

   - **Never.** Choose this option to deactivate the scheduled task.
   - **After Start Up.** Choose this option to run the operation as soon as you start your computer.
   - **Before Shut Down.** Choose this option to run the operation when you choose Shut Down from the Special menu in the Finder.
   - **At Specific Time.** Choose this option to set up a recurring or non-recurring schedule for running this task. The options to the right of the menu will become active. Choose first from the menu to tell the Virex application how often to run this task—the options beneath the menu will change to reflect your available scheduling choices. Your options are:
     - **Once.** This runs your task exactly once on the date and at the time you specify. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, then enter a time in the list to the right.
     - **Hourly.** This runs your task each hour on a specific date for as long as your computer is on. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin. The application will then run the same operation at intervals of one hour after the initial time you specify.
     - **Daily.** This runs your task once each day at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin.
     - **Weekly.** This runs your task once each week at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin. The scan operation will run every seven days thereafter.
     - **Monthly.** This runs your task once each month at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin. The scan operation will run on the same day of the month for each month thereafter.

- **Week Days.** This runs your task once each weekday at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin.
- **Weekend Days.** This runs your task once each weekend day—that is, Saturday and Sunday—at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin.

4. When you have set all of the options you want for your task, click Add. A summary of the task will appear in the area at the top of the Schedule Editor dialog box (Figure 7-2).

5. To rename this task for your reference, simply click the existing task name to select it, then type the new name in its place.

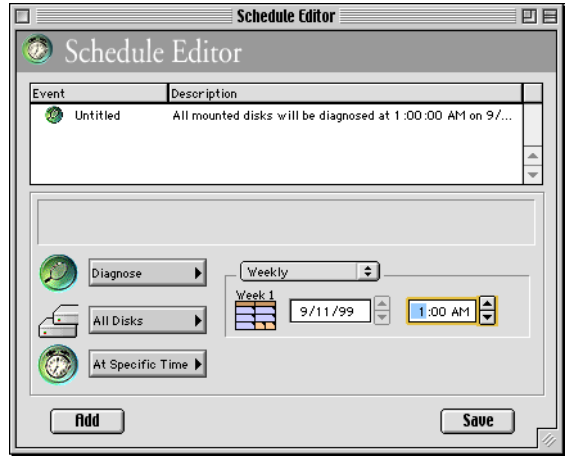


Figure 7-2. Schedule Editor dialog box, with task scheduled

6. To change any of the options for any of the tasks listed in this area, select the task, then follow Step 1 through Step 3 in the preceding list. When you have changed all of the options you want to change, click Save at the bottom of the dialog box.

7. To add another task, deselect any of the tasks listed at the top of the Schedule Editor dialog box, then follow Step 1 through Step 4 in the preceding list.

8. To delete any task listed in the Schedule Editor dialog box, select the task, then drag it to the Trash on the Macintosh desktop, or press DELETE on your keyboard.

9. When you have finished adding new tasks, editing existing tasks, or removing tasks, click Save to save your task settings and close the Schedule Editor dialog box.

Scheduling Virus Definition updates

To function at peak efficiency, the Virex application and the Virex control panel both need regular infusions of new virus definition files. Without updated files, neither the application nor the control panel can detect new virus strains when it encounters them.

Network Associates, through its AVERT Labs division, updates these critical files regularly and frequently, and makes the revised files available on its FTP (File Transfer Protocol) servers each month. You can download and install these files yourself, or you can let the Virex EUpdate utility—in combination with the Virex Schedule Editor—take care of this chore automatically.

NOTE: "Updating" Virex software means downloading and installing new Virus Definition versions; "upgrading" Virex software means downloading and installing product version revisions, application components and, in some cases, Virus Definition files. Network Associates offers free Virus Definition file updates for the life of your product. This does not, however, guarantee that these files will be compatible with product versions to come.

Your right to download free Virex file upgrades depends on the terms of your license or on the terms of the sales contract you agreed to at the time of your purchase. If you have questions about these terms, consult the LICENSE.TXT or README.1ST documents included with your Virex copy, or consult your sales representative. Network Associates makes upgrade files available for you to download freely from its FTP sites and other services for as long as your license permits. You can use the Virex Schedule Editor, in combination with the EUpdate feature, to control when and how often you download new Virex files.

By default, the Schedule Editor does not come with any update tasks predefined. To schedule an update operation, follow these steps:

1. Verify that you have set up your EUpdate preferences to download new Virus Definition files from the correct location. See "Configuring EUpdate preferences" on page 74 to learn how to do so.

1. Choose eUpdate from the top menu in the series of three menus in the Schedule Editor dialog box. Once you do so, the options in the second menu will become unavailable.

2. Choose a time in which to run the operation from the third menu. Your options are:

   - **Never.** Choose this option to deactivate the scheduled task.
   - **After Start Up.** Choose this option to run the operation as soon as you start your computer.
   - **Before Shut Down.** Choose this option to run the operation when you choose Shut Down from the Special menu in the Finder.
   - **At Specific Time.** Choose this option to set up a recurring or non-recurring schedule for running this task. The options to the right of the menu will become active. Choose first from the menu to tell the Virex application how often to run this task—the options beneath the menu will change to reflect your available scheduling choices. Your options are:
     - **Once.** This runs your task exactly once on the date and at the time you specify. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, then enter a time in the list to the right.
     - **Hourly.** This runs your task each hour on a specific date for as long as your computer is on. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin. The application will then run the same operation at intervals of one hour after the initial time you specify.
     - **Daily.** This runs your task once each day at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin.
     - **Weekly.** This runs your task once each week at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin. The scan operation will run every seven days thereafter.
     - **Monthly.** This runs your task once each month at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin. The scan operation will run on the same day of the month for each month thereafter.

- **Week Days.** This runs your task once each weekday at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin.
- **Weekend Days.** This runs your task once each weekend day—that is, Saturday and Sunday—at the time you specify, starting from the date you indicate. Enter the complete date—day, month, and year—in the leftmost text box beneath the menu, the enter the initial time on which you want the cycle to begin.

3. When you have set all of the options you want for your task, click Add. A summary of the task will appear in the area at the top of the Schedule Editor dialog box (Figure 7-3).
4. To rename this task for your reference, simply click the existing task name to select it, then type the new name in its place.

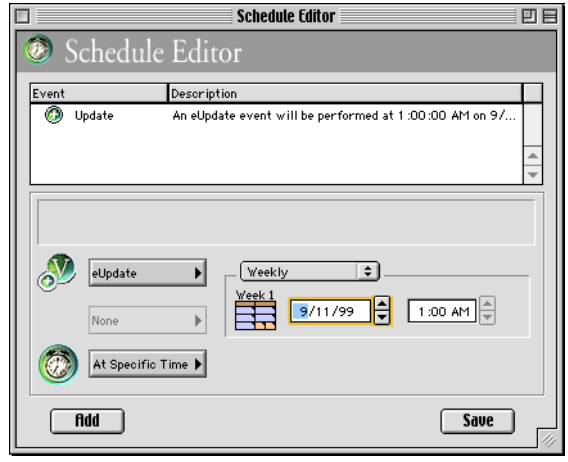


Figure 7-3. Schedule Editor dialog box, with update task scheduled

5. To change any of the options for any of the tasks listed in this area, select the task, then follow Step 1 through Step 3 in the preceding list. When you have changed all of the options you want to change, click Save at the bottom of the dialog box.
6. To add another task, deselect any of the tasks listed at the top of the Schedule Editor dialog box, then follow Step 1 through Step 4 in the preceding list.
7. To delete any task listed in the Schedule Editor dialog box, select the task, then drag it to the Trash on the Macintosh desktop, or press DELETE on your keyboard.

8. When you have finished adding new tasks, editing existing tasks, or removing tasks, click Save to save your task settings and close the Schedule Editor dialog box.

NOTE: To run a scheduled task, you must have the Virex Scheduler extension active in your Extensions folder in your System folder.

Updating Virex 8

Setting an update policy

By default, the EUpdate task included with the Virex software comes configured to download the most recent Virus Definition file updates directly from the Network Associates FTP site. This configuration can make administration simple and straightforward for small networks or individual Virex installations. If you have a large network, however, retaining this configuration can severely tax your external bandwidth if, as will happen if you leave the default configuration enabled, each network node tries to update its Virus Definition files at once.

Instead, Network Associates recommends using EUpdate to download new files to one server on your network, then using that server as a repository from which other computers on your network can download their own updates. By making these updated files available on one or more central servers on your network and configuring your remaining network nodes to download the updated files from those servers, you can

- Schedule network-wide Virus Definition file roll-outs for convenient times and with minimal intervention from either administrators or network users. Use the Virex Schedule Editor dialog box to set individual times when each network node will poll the server for updated files.

  You might, for example, specify one convenient update time when you first deploy Virex software within your network, but then set a schedule that phases in or rotates Virus Definition file updates among different parts of the network. To learn how to schedule an EUpdate task, see "Scheduling Virus Definition updates" on page 68.

- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.

- Reduce the likelihood that you will need to wait to download new Virus Definition files. Traffic on Network Associates servers increases dramatically on regular Virus Update file publishing dates. Avoiding the competition for network bandwidth enables you to deploy your update with minimal interruptions.

Configuring EUpdate preferences

The Virex application's EUpdate preferences panel governs how and from where you download Virus Update files. After you set these preferences, you can update your files immediately, or schedule an update operation for a later time.

To set your EUpdate preferences, follow these steps:

1. Start the Virex application. To learn how to do so, see "Starting the Virex application" on page 23.
2. Click the Preferences button 

in the Virex application toolbar.
3. The Preferences dialog box will appear. Scroll to the bottom of the preferences list, then click the EUpdate icon 

to move to the correct preferences panel (Figure 8-1).

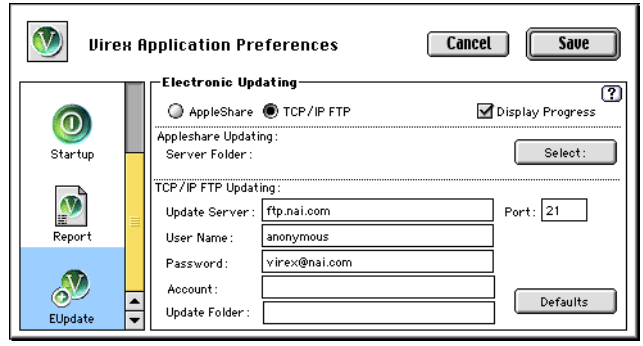


Figure 8-1. EUpdate preferences panel

4. Choose the protocol you want to use to connect to the site that stores the new Virus Definition files. Your choices are:

   - **AppleShare.** Click this button to tell the Virex application to download new files from an AppleShare server on your network. To use this update method, you or a system administrator must download the new Virex files from the Network Associates website to a central server on your network, then make a particular folder on that server available to all Macintosh computers that you want to update. Each computer you want to update must have that central folder mounted on the local system in order to download new files.

     Next, click Select in the AppleShare Updating area to select the central folder you want to use. You must have the central folder mounted on your local computer to select it.

- **TCP/IP FTP.** Click this button to tell the Virex application to download new files from an FTP server on your network, or elsewhere on the Internet. By default, the Virex application will connect to the Network Associates FTP site to download new files. To change the default settings, follow these substeps:

  a. Enter the fully qualified domain address in the Update Server text box in the TCP/IP FTP Updating area. You can enter either a domain name or a TCP/IP address here.

  b. Enter a user name and password that has sufficient rights for FTP access to the server. If your server allows anonymous FTP access, enter `anonymous` in the User Name text box and any combination of characters in the Password text box. If you have an account designation necessary for access to the server, enter that information in the Account text box.

  c. Specify which directory on the server the Virex application should go to in order to find new Virex files. By default, this text box lists a specific directory on the Network Associates FTP site.

  d. If the FTP server from which you want to download new Virex files uses a different port designation for FTP connections, enter that value in the Port text box. By default, the Network Associates FTP site uses port 21.

5. To see the application's progress as it downloads a new Virus Definition file, select the Display Progress checkbox.

6. To save your settings and close the Virex Preferences dialog box, click Save. To close the dialog box without saving your changes, click Cancel. To restore the configuration options for electronic updating to those that came with the product, click Defaults.

7. To update your Virex files immediately, return to the Virex application main window, then click the eUpdate button 

.

   The Virex application will immediately contact the server you specified in the Virex eUpdate Preferences module and download any new files it finds there. If your Virus Definition files are current, the application will tell you so. To stop the download, click 

at any time during the operation.

   Once you connect, the EUpdate utility will download and install your Virus Update files for you. The Virex application and control panel will begin to use the new files immediately.

Installing Virus Update files without EUpdate

Network Associates develops regular Virus Update files to combat new virus threats as they emerge. Each Virus Update file brings new detection and repair capabilities both to the Virex application, and to the Virex control panel. To ensure that you have the most effective protection available, download and install these update files as soon as Network Associates makes them available. You can use your favorite web browser or FTP client software to download new files from this FTP site:

ftp://ftp.nai.com/pub/antivirus/datfiles/virex

Network Associates stores new Virus Definition files on this site as BinHexed archives. If your browser or FTP client software does not automatically decode and unstuff the Virus Definition archives, you must use StuffIt, StuffIt Lite, or another compression utility that can read .hqx files and extract StuffIt archives to do so yourself. You can find the necessary utilities on most electronic services.

Next, locate the file you downloaded and extracted, then double-click it to start the update.

The Virex application will start and will update the Virus Definitions file in your Virex Preferences folder. The Virex application and Virex control panel will immediately begin using the updated virus definitions. Alternatively, you can open the Virex application, then choose Apply Update File from the File menu.

Network Associates recommends that you scan your system immediately to ensure that it does not have any of the new viruses that the update file detects.

NOTE: The latest Virus Update file includes all of the virus definitions available in previous Virus Definitions files.

Troubleshooting A

Virex is optimized for compatibility. However, if you experience problems with your Macintosh as soon as the Virex Control Panel is installed and you have restarted your machine, another extension or control panel installed in your System folder is probably conflicting with the Virex Control Panel. To find the conflicting extension, you should try the steps below, ONE AT A TIME, in order. Each time you try a step, restart your machine and see if the problem is corrected. If one step does not correct the problem, try the next step. Do this until one of the steps corrects the problem.

NOTE: If you have tried ALL of the following steps and the problem still occurs, or if one of the steps you tried corrects the problem, please contact Network Associates technical support and report your findings.

- Make sure your machine has already been scanned and is virus-free.
- Change the **Load Control Panel** option in the Virex Control Panel Preferences. Then try each setting, remembering to restart your machine after each change. Because some programs prefer to load into memory ahead of other programs at startup, the potential for conflict exists. It is a good idea to use as few extensions, control panels, INITs and startup documents as possible.
- Turn OFF **Scan Files When Opened** using the Preferences button in the Virex Control Panel, then restart your machine.
- Turn OFF ALL other extensions, control panels, INITs, or startup documents that are not part of the System software. Leave the Virex Control Panel in your System folder and restart your machine. If the problem goes away, then you know the Virex Control Panel and another program in the System folder were in conflict. The next step is to find out exactly which program is in conflict with the Virex Control Panel.
- Selectively put your other extensions and control panels back into your System folder, one at a time, and restart your machine after each one. This process can be time-consuming, but it is the only way to find out which program is in conflict with the Virex Control Panel.
- Click Preferences in the Virex Control Panel, then select **Automatic**. Clear the **Startup Scan** option, if it is selected, then restart your machine.

  - Turn OFF File Sharing in the Sharing Setup control panel if it is on, then restart your machine.
  - Reinstall a fresh copy of the Virex Control Panel from the Virex Installer disks.
  - If you know which program is in conflict with the Virex Control Panel, replace the problem program with a fresh copy from its master software disk.
  - Reinstall your System software.
  - Rebuild your desktop by pressing the ⌘ and OPTION on your keyboard immediately after you restart your computer. When the dialog appears asking if you are sure you want to rebuild your desktop, release both keys, then click OK.

- If you experience **problems with an application** that you manually launch after the Virex Control Panel is installed and you have restarted your machine, please follow the same steps as above, ONE AT A TIME. For each step you follow, try to repeat the steps you took with your application when the problem first occurred.
- If you experience **problems printing**, there could be a number of causes. If you cannot print, please try the following:
  - Make certain that your startup disk has at least 15K of available disk space
  - Check that your Chooser settings are correct; and
  - Check for loose printer cables.
- If you have recently updated existing software, or installed new software into your System folder, you may be experiencing a conflict. Follow the steps for resolving conflicts with the Virex Control Panel and application as above.
- If Virex **cannot recognize a hard drive**, your hard drives might not be fully compatible with the Macintosh. One way to correct this problem is to contact your dealer or the hard drive manufacturer to obtain a copy of their hard drive utility software.
- If a **repair is unsuccessful**, the infected file may be locked. If the volume on which the file resides is locked, or if the file is locked in the Get Info window or by a security software program, then Virex will not be able to repair that file. Unlock the file or the volume and try the repair again.

- **If Virex exhibits unusual behavior,** other anti-virus programs, especially those installed in the System folder as extensions or control panels, may be interfering with Virex. Remove any such anti-virus programs from the System folder and restart your machine.
- When diagnosing a hard drive, you get an **unexpected Error message**. There are several possible solutions:
  - Try restarting your computer; or
  - Follow the steps for resolving conflicts with the Virex Control Panel and Application as above.
- You get an **Error -50 or Error -108 message** on a few files. You may get error messages when trying to diagnose files that have been encrypted by a data security software program. If you are using software that encrypts files, try decrypting or decompressing those files, and then diagnose them again. The files may also be damaged. Try replacing them with fresh copies from their master disks and then diagnose them again.
- When you use the Option Diagnose feature in the Virex application, you notice **a few new files**, such as Desktop with which you are unfamiliar. These are normal files which are hidden from view in the Finder.
- When installing Virex on your computer the **Virex icon appears as a generic application or document icon** instead of the custom Virex icon. restart your Macintosh and rebuild your desktop by pressing ⌘ and OPTION on your keyboard.

Repairing Active Files B

This Appendix provides procedures for repairing active files, such as the Finder, and discusses the background of why these procedures are necessary. Be sure to review any Read Me files on your Virex CD-ROM for the latest information about Virex before you proceed.

- In order to repair some system files on your hard drive, you must start your Macintosh computer from a different startup disk. Newer Macintosh systems come with system software on a CD-ROM. Follow the directions in your Macintosh User Guide to restart your Macintosh from the CD-ROM. Next, continue with the instructions in "Using the Virex Installer to scan your computer" on page 13.
- If you cannot start from the Virex disk, it might mean that your computer requires special files called "enablers" that are not present on the Installer diskette. Follow the instructions in the following section.

Starting from a Disk Tools Disk

To start your computer from the Disk Tools floppy disk supplied with most Macintosh computers, follow these steps:

1. Start your computer from the locked Disk Tools disk. If your Macintosh did not come with a Disk Tools disk, use your Utilities disk. If you have misplaced it, or if your Macintosh did not come with one, your Macintosh dealer can provide one. When the computer has completed its startup routine, the Disk Tools disk icon will appear above your hard drive icon on the Desktop.
2. Press the ⌘, SHIFT and 1 on your keyboard simultaneously to eject the startup disk.
3. Insert your Virex CD-ROM into your CD-ROM drive.
4. Double-click the Installer icon.
5. Click Scan. The computer will ask you to swap disks again.
6. Repair or delete any viruses or Trojan horses.
7. Quit the Installer and **Restart** your computer. Your computer should now be entirely virus-free.
8. Wait for the computer to finish its startup routine.

Creating a Clean Startup Disk

Network Associates recommends strongly that you create a special startup disk that will allow you to repair future infections in system files without having to perform the procedure listed above. This procedure applies only to users of Macintosh models that will not start from the Virex CD-ROM.

To create a clean startup disk, follow these steps:

1. To ensure your computer is virus-free, follow the installation instructions in Chapter 2, "Installing Virex Anti-Virus Software."
2. Use Apple Disk Copy to make a copy of the Disk Tools disk from the floppy disk images stored on the Virex CD-ROM or the CD-ROM disc image you downloaded from the Network Associates website. If you make your images from a CD-ROM disc image, be sure you do so from an *uninfected* computer. See the documentation for Apple Disk Copy to learn how to create a floppy disk from a disk image.
3. Insert your newly created Disk Tools copy.
4. Open the System folder on your startup disk, then drag the System Enabler(s) from your startup disk to your Disk Tools copy. If there is not enough room on disk, remove other enablers to free up space.
5. Eject your Disk Tools copy and *lock* it.

You have successfully created a new Disk Tools disk, which allows you to start up your computer and repair active infected files. This disk includes the extensions necessary for CD-ROM support. Once you start your computer with it, you can insert your Virex CD-ROM, then use the Virex application to diagnose and repair your system.

Safe Computing Practices C

You can greatly reduce the chance that you will experience problems with a computer virus or Trojan horse by adopting these safe computing practices:

- The most important practice is to use software that is obtained from reputable and reliable sources. In general, commercial software from well known software publishing firms should be virus-free.
- Treat public domain software (freeware and shareware) with caution. If you download public domain software, you should store it on a floppy disk until it has been diagnosed for known viruses. Remember, viruses and Trojan horses do not have an opportunity to replicate themselves or activate until you run the host program in which they reside.
- There have been a number of instances in which commercial software infected with viruses was inadvertently shipped to consumers. While this is an infrequent occurrence, Network Associates recommends that you scan all new commercial software with Virex for possible contamination by computer viruses.
- Be careful with any software that you obtain from other users. Treat such software with the same degree of care that you use with public domain software. Always scan the software for known viruses and before you use it.
- If you start up your Macintosh from a single, familiar, locked System disk, or you make sure you are starting up from a drive that is running the Virex Control Panel, it will be very unlikely that you will become infected.
- Use care before copying any questionable software to your hard drive. Again, scan the software with Virex before you use it.
- Make a backup of your original System disks, fonts, folders, and important data and application files. This will enable you to limit your losses and to restore your hard drive in the event of a hard disk crash or other sudden computer failure.
- Make a backup of your System files after you have customized them with your favorite fonts, extensions and utilities. This precaution will save you hours of work rebuilding your system in the event of a failure.

- Make sure that all original disks are locked and virus-free, back up all newly acquired software, and store them in a safe place. Always launch your application programs from copies and not from the original disks. This will prevent your original software from becoming infected by a virus, and will ensure that a fresh copy is always available if your working copy becomes damaged.
- Systematically backup your important data files to ensure that you do not lose important work.
- Be security conscious and promote security awareness throughout your organization.

These safe computing practices will not only help you to safeguard your system from viruses and Trojan horses, but may help prevent the loss of important data in the event of a catastrophe.

You may wish to consult your dealer to discuss software and hardware backup alternatives.

A Word About Computer Viruses and Trojan Horses

D

What are computer viruses?

Computer viruses are programs that contain the software instructions necessary to make replicas of themselves and insert these instructions into other executable programs. Each time an infected program is run, the virus code is executed, usually resulting in the infection of other programs.

Computer viruses usually replace the first few instructions in the host program, so that the virus can run first. The virus continues to look for uninfected files each time it is run, and may eventually spread to many of your programs.

Computer viruses vary in the degree of harm that they can cause. Some display a humorous or innocuous message, while others are designed to cause catastrophic damage.

Even seemingly innocuous viruses can inadvertently cause problems or unpredictable behavior with your programs, just by being present in the System folder or on the hard drive. For example, if the virus is using memory or disk resources that another program needs, that program could crash.

What are Trojan horses?

As the name implies, a Trojan horse masquerades as a legitimate program, but in reality harbors code that could inflict serious damage to your computer. Trojan horses cannot be repaired and therefore must be deleted. A Trojan horse differs from a virus in that it does not have the ability to replicate. You must obtain a copy of the original software that contains the Trojan horse to be in danger. The most likely place to find a Trojan horse is on a public domain bulletin board (BBS) or on-line service. Although bulletin board administrators are very careful to screen the software that is uploaded to their BBS, you also must take responsibility to protect yourself and do your own screening.

How do viruses and Trojan horses spread?

Viruses and Trojan horses move from machine to machine through the sharing of disks, application programs and by means of computer networks. In our advanced world of on-line computer services, networks, shared computer facilities, and overnight mail services, computer viruses and Trojan horses can spread at an alarming rate.

Many users are unaware that they have been infected with a computer virus and attribute their problems to other causes.

For additional educational and general virus information, visit the Network Associates web site at http://www.nai.com.

Understanding Macintosh Viruses and Trojan Horses

E

Virex combats all of the Macintosh computer viruses and Trojan horses known to Network Associates at the time of manufacture. For a complete list, open the Virex Help window by clicking Help in the Virex application. Then select **Virus Descriptions** in the pop-up menu. Here are details on many of the well-known Mac OS viruses and Trojan horses.

Viruses

- **3 Tunes (HC) HyperCard:** The 3 Tunes HyperCard virus, discovered in Benelux, Belgium in March of 1991, infects all HyperCard stacks and plays three German folk tunes when the infected stack is launched. The virus can also display the messages: “Hey, what are you doing?” and “Don’t panic.” Both messages generate an accompanying sound. The virus has been reported to cause system crashes.
- **ANTI:** The ANTI virus was discovered in France in 1989, and reported to Dr Solomon’s Software by the system manager of a European on-line computer service. Because it adds the text string “ANTI” to infected programs, Dr Solomon’s researchers named the virus ANTI.

  The virus employs an unusual infection technique: it infects programs by modifying existing CODE resources rather than adding a new CODE resource.

  More than one strain of the ANTI virus was written. ANTI-ANGE is a precursor to the ANTI virus and ANTI-0 is an ANTI virus variant with renamed resources. When ANTI infects a file that is already infected by ANTI-ANGE, ANTI will alter the ANTI-ANGE virus to make it harder to detect. The ANTI virus does not spread under MultiFinder.
- **AutoStart 9805:** AutoStart 9805 is a worm that can affect any Power Macintosh system. Non Power Macintosh systems (those with 680x0 processors) are not affected. The worm can be transmitted on almost any Macintosh (HFS) format disk volume, including floppy disks, most removable cartridge drives, hard disks and even disk images.

It normally infects via the QuickTime AutoStart feature that allows a document or application to be launched automatically upon mounting of a disk volume. The risk of the infection can be reduced by disabling the CD-ROM AutoPlay option in the Quicktime Settings Control Panel. This will not help if the system is already infected, or if you boot from a disk containing an infected Extension folder.

- **CDEF:** The CDEF virus, discovered in Ithaca, NY in 1990, is a desktop file infector similar to the WDEF virus, and appears in two strains. It can infect the desktop file of a System 6 drive immediately upon the insertion or mounting of an infected volume, unless the drive is physically write-protected. Although System 7 is immune to the CDEF virus, it is still possible for the virus to exist in a System 7 desktop file, especially if the virus was on the drive before the drive was updated to System 7.

  CDEF infects by adding a CDEF resource to the invisible desktop file and spreads through the sharing of infected floppy disks. It causes system crashes and other anomalous behavior. CDEF can be removed by rebuilding the desktop file on the infected volume either by restarting the drive or inserting (mounting) the infected cartridge or disk, and simultaneously pressing the command and option keys.

  ☐ **NOTE:** If you have chosen the ⌘ or OPTION key as your default bypass key in the Virex Control Panel Preferences, when you rebuild your desktop, the Virex Control Panel will not load into memory while you hold down that key. You must remember to restart your computer, so that the Control Panel will load into memory and continuously monitor your drive.

- **CODE-1:** CODE-1 was discovered at several U.S. sites in 1993. It infects applications and system files, and changes the hard disk name to “Trent Saburo” on October 31 of any year. This virus incorporates “stealth” techniques to evade traditional detection methods. The virus can cause system crashes and other damage, because CODE-1 attempts to alter system files.

- **CODE 252:** The CODE 252 virus was discovered when a Virex customer, using the snapshot feature, noted changes in his files and programs and immediately alerted Dr Solomon’s Software. CODE 252 is passed from application programs to the system file where it infects other applications.

The virus employs a trigger date of June 6 and replicates every time an infected file is launched prior to that date. On or after June 6, the virus stops spreading and displays a message that reads, “You are infected with a virus. Ha Ha Ha Ha Ha Ha Ha. Now Erasing all disks. Ha Ha Ha Ha Ha Ha Ha. (Click to continue).” After clicking to continue, the virus then removes itself from memory and from the infected file. The virus DOES NOT ERASE files, but infected files remain infected until they are launched.

- **Dukakis:** The Dukakis HyperCard virus infects the Home stack when an infected stack is opened. From there, the virus spreads to other HyperCard stacks as they are opened. When triggered, the virus displays the message “Dukakis for President” and then deletes itself. Because of this self destructive characteristic, the Dukakis virus is rarely found.

- **Frankie:** The Frankie virus infects only Macintosh emulators, like Atari, NOT Macintosh computers. When activated, the virus will draw an icon of a bomb and then display the message: “Frankie says: No more piracy!” and then it will cause the system to crash. The Frankie virus is included in Virex for completeness.

- **HC 9507:** The HC 9507 virus infects HyperCard stacks only. It does not infect system files or applications. Once the home stack is infected, the virus spreads to other running HyperCard stacks and other randomly chosen stacks on the startup disk.

  The HC 9507 virus causes unusual system behaviors, depending on the day of the week and the time. While running HyperCard with infected stacks, you may observe the screen fading in and out, the word “pickle” being typed automatically, or suffer a system shutdown or lockup.

- **HC 9603:** HC 9603 is a simple yet effective HyperCard virus. It was discovered by a teacher at Kate Chegwin School in Edmonton, Alberta, Canada. The virus was first noticed on Macintosh computers at the school in January, 1996.

  Like most HyperCard viruses, HC 9603 infects the Home stack when opened. From there, the Home stack infects other stacks as they are opened. The virus does not attempt any malicious behavior and is unlikely to be noticed unless an infected stack script is examined.

  The Home stack can be inoculated against HC 9603 infections by placing a comment with the string “nV” in its stack script. For example:

  – This nV protects the Home stack against infection.

  Since the Home stack must become infected for the virus to spread, this will stop the spread of the virus. This works because the virus will not infect a Home stack script containing that string.

- **INIT 17:** The INIT 17 virus, discovered in Canada, spreads quickly to the System file and applications as they are run. Although INIT 17 appears to be relatively harmless, it contains errors in its virus code that may cause file damage during an infection, making it a dangerous virus. The virus may also cause system crashes on some older Macintosh models, such as the Mac Plus and SE. The only other observable action that INIT 17 exhibits is the display of an innocuous message in a window entitled “From the depths of Cyberspace.” This message is shown the first time an infected machine is restarted after the trigger date of 6:06:06 PM, October 31, 1993.

- **INIT 29:** The INIT 29 virus, discovered toward the end of 1988 in the United States, infects System files by inserting its own INIT 29 code resources. It is different from most Macintosh viruses because it can infect data files as well as executable files. However, the infected data files do not spread the virus. The INIT 29-B variant was discovered in 1994.

  Prior to the appearance of INIT 29, Macintosh viruses could spread only when an infected program was launched. INIT 29 is particularly virulent because it infects unlocked disks the moment they are inserted into an infected machine. If a locked disk is inserted into a machine whose System is infected with the INIT 29 virus, the computer will ask you to unlock the disk saying it “needs minor repairs.” Once the disk is unlocked and reinserted into the infected machine, the virus will then infect it.

  Although INIT 29 does not do intentional damage, it can cause printing problems, system crashes, and other unexplained behavior.

- **INIT 1984:** The INIT 1984 virus, which is programmed to trigger on every Friday the 13th, is a dangerous Macintosh virus that changes the names and attributes of files and folders to random strings and destroys files. This virus affects all types of Apple Macintosh computers running Apple System 6 and System 7 operating systems. The INIT 1984 virus infects only INIT-type system extensions and has been reported at several sites in the United States and Europe. At those sites, it caused significant damage when the infected Macintosh computers were restarted on Friday, March 13, 1992.

- **INIT 9403:** The INIT 9403 virus was discovered in Italy in March of 1994. Also known as “SysX”, it infects the Finder and certain other applications. After infecting a number of other files, INIT 9403 attempts to erase the system disk and other mounted hard disks.

- **INIT-M:** The INIT-M virus, discovered at Dartmouth College, is a malicious virus that spreads quickly to applications, system extensions, documents and preference files. INIT-M causes damage to infected systems that are active on Friday the 13th. On that trigger date, INIT-M renames files and folders with names made up of random strings.

It also changes file creation and modification dates and scrambles file creator type information, which can lead to the inability to open files. In some instances, files are even deleted. When the virus is present on an infected system, it will create a file called FSV Prefs in the Preferences folder. INIT-M can affect all Macintosh computers running Apple operating system 7.0 or greater. The virus does not spread or activate on System 6 machines.

- **Laroux:** Laroux is the first Excel macro virus discovered in the wild. Excel Macro viruses are written in Microsoft's Visual Basic for Applications macro language. This language is supported in Microsoft Excel for the Macintosh 5.0 and later, as well as numerous PC versions of Excel for Windows 3.x, Windows NT, and Windows 95.

  Laroux uses the macros "auto_open" and "check_files" to replicate. It creates a hidden, blank worksheet in infected documents, but it is not intentionally destructive. Laroux does not infect or spread on Macintosh systems, but Macintosh systems can harbor infected files in a multi-platform environment.

- **MBDF A and MBDF B:** The MBDF-A virus, originally discovered in Wales and reported at various sites in the United States, infects the Macintosh system, finder and application files. While MBDF does not cause intentional damage, once infected by the virus, users may experience system crashes and malfunctions with their application programs. Sometimes the system file can be damaged. MBDF is virulent under Apple's System 6 and System 7 and can infect and spread on all Apple Macintosh computers except the Macintosh Plus and SE models. The virus was spread from two games called 10 Tile Puzzle and Obnoxious Tetris, as well as by the Tetricycle Trojan horse masquerading as a game called Tetricycle (see Tetricycle Trojan horse). MBDF B is a strain of the MBDF A virus and was discovered in 1993. According to published reports, the authors of the MBDF virus were undergraduate students at Cornell University. The students were apprehended and charged with second degree computer tampering.

- **MDEF:** The MDEF virus is a family of four viruses all written by a high school student from Ithaca, New York who was identified in October of 1990. He apparently wrote the CDEF virus as well. The four viruses are known as MDEF A or Garfield, MDEF B or Top Cat, MDEF C and MDEF D. These viruses are not malicious in intent, but can cause system crashes and other unexplained behavior. MDEF is the name of a Macintosh resource that is responsible for drawing menus. As a result, it is not uncommon for a program infected with MDEF to have garbled pull-down menus.

- **Merry Xmas:** The Merry Xmas HyperCard virus and its several strains infect HyperCard stacks by appending viral code to the end of the stack script. When an infected stack is run, it first attempts to infect the HyperCard Home stack. Subsequent stacks that are run will receive the infection from the Home stack.

  A "bug" in the most common strains causes the entire host stack script to be appended to the "Home" stack script when it is infected. If the host stack script contains any handler routines, unexpected Home stack behavior may result. One strain replaces the Home stack script and deletes any stack that is run after the Home stack is infected.

  The Merry Xmas virus can cause irreparable damage because it sometimes deletes scripts or carries unrelated script routines from its host stack to the Home stack. For this reason, Network Associates recommends that you replace infected stacks rather than repair them whenever possible.

- **nVIR Family:** The nVIR virus places nVIR resources in the System file and CODE resources in the application software. The CODE resources tell the application to add the nVIR resources to the System folder.

  nVIR can cause applications and System files to crash. If MacinTalk is installed in your System folder, your computer may occasionally say "Don't Panic." Otherwise, it may beep unexpectedly. The source code of the nVIR virus unfortunately has become widely available, enabling individuals to use it as a template to create new viruses.

  Therefore, the nVIR virus is actually a family of viruses with two major strains, nVIR-a and nVIR-b. This virus has been modified a number of times to alter its behavior and to elude detection.

- **AIDS, F***, Hpat, J-nVIR, MEV#, MODM, nCAM, nFLU and prod**: These viruses are derivatives of the nVIR family of viruses, with minor variations that enable them to remain undetected by existing anti-virus software. The viruses replace nVIR code resources with renamed resources. Therefore, they are only renamed variants of a virus whose characteristics are well known. Virex and the Virex INIT have a powerful diagnose and repair capability that handle renamed variations of nVIR automatically.

- **Peace:** The Peace Virus, also called the MacMag virus, was discovered in Montreal in December of 1987. A HyperCard stack called "New Apple Products" was a Trojan horse which generated the Peace virus. The virus infected only system files which, in turn infected other system files. The Peace virus spread from machine to machine, and then displayed a universal message of peace on March 2, 1988. The virus destroyed itself after the message appeared. Consequently, it is rarely reported.

- **Scores:** The Scores virus, discovered in the United States in 1988, was one of the first Macintosh viruses. Scores, also known as Eric or NASA, spreads itself rapidly and efficiently by lying dormant before causing any damage.

  An application infected with Scores has new CODE resources to tell applications to add several invisible files to the System folder. While these files cannot be directly observed, Scores adds a Note Pad and Scrapbook file that have an unusual appearance. They appear as blank, dog-eared icons rather than as normal System icons

Normal Scrapbook file

Scores Scrapbook file

  Scores modifies the System by adding new INIT resources. These new INIT resources cause the virus to spread to uncontaminated applications each time the Macintosh is started. Scores causes system crashes and problems in the normal operation of applications and especially problems with printing.

- **T4:** The T4-A and T4-B virus strains were originally discovered in versions 2.0 and 2.1 of the GoMoku game application, in July of 1992. These games were widely available on the Internet and appeared to have spread extensively. The T4 virus strains are considered to be dangerous, because they can cause significant damage to system files and applications.

  When a file infected with T4 is launched, the virus attempts to alter the System file. This alteration results in changes to the startup code under both Apple's System 6 and System 7 operating systems. The damage caused by this change usually results in INIT files and System extensions not loading and leaves some systems unable to startup.

  The T4 virus also attempts to modify application files on the system disk, by overwriting portions of the files with the viral code. This alteration will, in some instances, damage the applications so severely that users have to replace or reinstall the files.

  T4-C, a strain of the dangerous T4-A and T4-B viruses, was found at the University of Illinois at Urbana-Champaign. Although T4-C does not appear to be as widespread as the T4-A and T4-B strains, it is as dangerous in its attempts to modify application files on the system disk.

- **WDEF:** The WDEF Virus is a type of virus that spreads via the invisible Desktop file under System 6. The WDEF virus will not damage data files, but it can render your computer virtually unusable by causing frequent System crashes. The WDEF virus can infect hard-disks immediately upon the insertion of a WDEF infected floppy. System 7 Desktop files cannot be infected by WDEF.

- **Word Macro Family:** Word Macro viruses are written in the macro language of Microsoft Word. This language is supported in Microsoft Word for the Macintosh 6.0 and later, as well as numerous PC versions of Word including those for Windows 3.x, Windows NT, and Windows 95. The Word Macro viruses each consist of a set of macros contained in a Word template document. All of these viruses take advantage of Word features that allow macros to execute automatically or override menu commands. While an infected document is open, one of its macros will be triggered, allowing the virus to copy itself into Word's global template file. Subsequently, while uninfected documents are open, a virus macro in the global template file may trigger and copy the virus into the document. Other macros may be used to cause damage or interfere with the normal operation of the computer. These viruses spread among all platforms that are capable of running Microsoft Word. Your Macintosh can be infected by transferring Word files to and from DOS, OS/2, Windows, or other non-Macintosh platforms.

  The first Word Macro strain to receive significant attention was Concept, also known as Word Macro 9508. This virus is very common because several thousand infected CD-ROMs were widely distributed before its discovery. New strains are appearing weekly, carrying significantly more destructive capabilities.

  There are well over 1000 macro viruses and new ones are discovered each day. To ensure complete protection, be sure to obtain and install the latest Virex Virus Update file.

- **ZUC:** The ZUC virus was discovered in Italy in 1990 by Don Zucchini, the person who first reported the virus to the public. The three strains of the virus, ZUC A, ZUC B and ZUC C infect applications and display the annoying symptom of controlling the movement of the cursor on your screen. Once the infection reaches the Finder file, the computer becomes virtually unusable.

Trojan Horses

- **ChinaTalk Trojan horse:** The ChinaTalk Trojan horse is an INIT / extension that disguises itself as a "female MacinTalk sound driver." Upon system restart, after ChinaTalk has been installed, the Trojan horse erases the directories of the hard drives and floppies on the infected system.
- **CPro Trojan horse:** The CPro Trojan horse was found in a file named CPro141.sea. To infect, CPro disguises itself as an update to a popular compression program. Once a user launches the CPro application, the Trojan horse will attempt to format mounted hard disks and floppy disks, with internal floppy drives being especially susceptible. CPro is only successful, however, in its attempts at formatting floppy drives.
- **Fontfinder Trojan horse:** The Fontfinder Trojan horse masquerades as a legitimate utility program called Fontfinder, but when launched will destroy the directory of your hard drive and make the files on the drive inaccessible.
- **MacMag Trojan horse:** The MacMag Trojan horse, also known as the Peace Trojan horse, masquerades as a product called New Apple Products. When it is launched, it generates the Peace Virus.
- **Mosaic Trojan horse:** The Mosaic Trojan horse masquerades as a utility program which claims to paint pictures. When launched, it will destroy the directory of your hard drive, making the files inaccessible.
- **Steroid Trojan horse:** The Steroid Trojan horse masquerades as a game, but will destroy the directory of your hard drive when launched.
- **Tetricycle Trojan horse:** The Tetricycle Trojan horse was originally discovered in Wales and masquerades as a game called Tetricycle. When the Tetricycle Trojan horse is launched, it infects System, Finder and application files with the MBDF virus (see MBDF A Virus). Users have reported experiencing long delays after launching the Tetricycle program and even System file damage if the computer is restarted while Tetricycle is running.
- **Virus Info Trojan horse:** The Virus Info Trojan horse masquerades as a utility program which claims to provide virus information, but when launched, will destroy the directory of your hard drive and make the files on the drive inaccessible.

Before You Call Technical Support

F

BEFORE YOU CONTACT Technical Support, locate yourself near your computer with the Virex software installed and have the information listed below available. Much of this information can be obtained by opening the Virex Control Panel, clicking Help, then clicking **Technical Information** button.

- Version of Virex
- Problem using the Virex Control Panel or Virex application
- Have you sent in the registration card?
- Customer number if registered
- Macintosh Model
- Model name of hard disk (internal or external)
- Version of system software
- Amount of memory (RAM)
- Extra cards, boards or monitors
- Name and version of conflicting software
- EXACT error message as on screen:
- What steps were performed prior to receiving error message?
- A complete description of problem:

For contact information, see Appendix H, "How to Contact Network Associates."

Glossary G

- **Active file** - any file that has been launched or otherwise loaded into memory and is currently running. An active application is represented by a small icon in the upper right corner of the menu bar.
- **Application** - a software program written for a specific purpose, such as word processing, database management, graphic design, or telecommunication. Applications normally need to be manually launched.
- **Backup** - Making a copy of the contents of a disk for safe keeping. Backing up your files ensures that you will not lose information if the original files become lost or damaged.
- **Baseline** - the result of an initial Virex snapshot which establishes a reference point for the status of the files on your computer. Virex uses this baseline to detect suspicious changes in files that may be indicative of a new virus.
- **Cartridge drive** - a type of external device that stores information on removable cartridges.
- **CD ROM drive** - a type of device that reads information stored on compact disks.
- **Control Panel** - also known as a cdev, is a program that lets you change various Macintosh features, such as sound, mouse, movement and keyboard options. Control panels are located inside the System folder under System 6. Under System 7, they are located inside the Control Panels folder inside the System folder.
- **Default button** - a button that is highlighted to indicate that it can be selected either by clicking on it with the mouse or by pressing the return or enter key.
- **Desk Accessory** - also called a DA, is a program which can be accessed under the Apple menu in the upper left corner of the menu bar. Under System 7, DAs are stored in the Apple Menu Items folder inside the System folder.
- **Desktop file** - an invisible file created by the Finder to store information about the location of file and folder icons on a disk.
- **Diagnose (scan, examine)** - searching for viruses and Trojan horses on a volume. This is the main function of the Virex application and Control Panel.

- **Diskette** - a 3.5 inch storage medium, also known as a floppy disk, which can be 800 kilobytes or 1.4 megabytes in storage capacity.
- **DropScan** - A Virex utility program that works with the Virex Control Panel to provide instant Drag and Drop scanning on the Macintosh desktop.
- **Ejectables** - any form of storage medium that can be ejected or removed by dragging its icon to the Trash.
- **Executable** - any file that contains code that is executed when the file is launched. Generally this refers to any file that is an application or a system file that loads into memory on startup.
- **Extension** - software programs that expand the capabilities of system software. They include drivers, which make it possible for the computer to use a certain printer or other device, and programs that add features to the Finder or the system software. System extensions, called INITs under System 6, are stored in the Extensions folder inside the System folder under System 7.
- **External drive** - a hard drive or removable cartridge drive that is not housed within the body of a computer. Generally connected to the computer with a SCSI cable.
- **File creator code** - a label which each file has that the system software uses to match documents to the program that created them and to give the file a unique icon.
- **File size** - the space that a file occupies on a storage medium.
- **File type** - a label within each file that the system software uses to match documents to the program that created them and to give the file a unique icon.
- **Floppy disk** - see Diskette.
- **Fonts** - a collection of letters, numbers, punctuation marks, and other typographical symbols having a consistent appearance.
- **Hard drive** - a metal disk coated with a magnetic medium and permanently sealed into a drive or cartridge. A hard drive stores very large amounts of information (20 megabytes-3 gigabytes and operates much faster than a floppy disk.
- **High density diskette** - a floppy disk that can store 1.4 megabytes of information. High-density disks can be used only with the SuperDrive floppy disk drive found on newer Macintosh models.

- **Heuristic Scanning** - analyzes the instructions contained within a program (or macro) for suspicious code, to determine if the file may be a new virus.
- **INIT** - see Extension.
- **Internal drive** - a hard drive or floppy drive that is stored within the body of a computer.
- **Launch** - opening a file by double-clicking on its icon.
- **Load into memory** - before a program can run, its code must load into the computer's memory. This occurs whenever you double-click on a file icon. Whenever you turn on your computer, the system software and any extensions (INITs) and control panels (cdevs) that are stored in the System folder automatically load into memory.
- **Locked disk** - a diskette can be write-protected, so that its contents cannot be modified (or infected), by moving the sliding tab in the right corner of the diskette to the open position (you can see through the hole).
- **Locked file** - a file is locked, so that it cannot be thrown away or its name changed, if the Locked check box is checked in the file's Get Info window. To see the Get Info window, click on and highlight the file's icon and select Get Info from the File menu near the top left corner of the screen.
- **Macro viruses** - viruses written in the macro or scripting languages embedded in application documents such as Microsoft Word or Excel. Unlike most Macintosh system viruses, macro viruses infect documents, not applications or system files. Since these documents are often cross-platform compatible, macro viruses can frequently spread among differing computer platforms such as Macintosh and IBM PC compatible computers.
- **Master disk** - the original Virex floppy disk that came in your retail package or Virex upgrade.
- **Memory (Random Access Memory or RAM)** - computer memory that can be accessed in an arbitrary order. RAM usually means that part of memory available for programs and documents that the computer reads from a disk. The contents of RAM are lost when the computer is turned off.
- **Modification (of file)** - viruses change the structure of a file so that it will propagate the virus. This modification can be detected by Virex. A file can also be modified accidentally if the file is damaged. The System file is modified whenever you add or remove sounds, fonts, desk accessories, or modify the keyboard layout.

- **Mount** - to establish a logical connection between a disk or drive and the computer. When a volume is mounted its icon appears on the desktop, making the volume accessible.
- **Network** - a collection of devices, such as computers, printers, and other computers, that are connected together through special cables. A network is a tool for communication that allows users to store, retrieve and share information, as well as share printers and other devices.
- **Network administrator** - the person who is responsible for overseeing the network and the computers on the network.
- **Original disk** - see master disk.
- **Rebuild Desktop** - to recreate the information about every file and folder on a disk or drive, which is stored in the Desktop file, by pressing command-option while the disk or drive is mounting.
- **Repair (disinfect, remove)** - one of the functions of the Virex application and the Control Panel. Use this to disinfect viruses and remove Trojan horses from your computer.
- **Resource** - a self-contained unit of code within a Macintosh program.
- **Resource length** - the length, in bytes, of a resource.
- **Resource number** - a label used by the system software to identify resources in a unique way.
- **Resource type** - a label used by the system software to classify a resource.
- **Root level** - the top level, or main window of a volume or folder.
- **Scan At Download** - a feature of Virex that immediately checks files for viruses when they are downloaded or copied to your Macintosh.
- **Security software** - programs that are used to restrict access to the data and files on a computer.
- **SpeedScan** - the proprietary technology that enables Virex to scan quickly for viruses.
- **Start up** - the action of turning on a computer.
- **Startup disk** - a disk with all the necessary program files, such as the Finder and System files contained in the System folder, to set the computer into operation.
- **System files** - the files stored in the System folder that are used by the system to start up the computer.

- **10-PAK** - a package of Virex that contains ten manuals, and a copy of the Virex software which may be distributed to ten computers.
- **Trojan Horse** - a program that masquerades as a legitimate program, but was created to maliciously damage computer files.
- **Utility** - programs that perform special operations, such as installing or updating software, checking for damage on a disk, magnifying an image on the screen, and so on.
- **Virus** - a program that contains the software instructions necessary to make replicas of itself and insert these instructions into other executable programs. Each time an infected program is launched, the viral code is executed, usually resulting in the infection of other programs. Viruses vary in the degree of harm that they can cause.
- **Volume** - a general term referring to a storage device or a destination for information. Often used in reference to hard drives, cartridges, CD-ROMs, floppy disks, and file servers. A volume can be an entire disk or only part of a disk.
- **Write-protected** - see locked disk.

How to Contact Network Associates

H

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at (408) 988-3832 or write to the following address:

Network Associates, Inc.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
U.S.A.

Technical support

Network Associates 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 Network Associates software, and for access to Network Associates news and virus information.

World Wide Web	http://support.nai.com

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

Internet	support@nai.com
CompuServe	GO NAI
America Online	keyword MCAFEE

If the automated services do not have the answers you need, contact Network Associates 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) 855-7044
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the Network Associates 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

Network Associates training

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

Comments and feedback

Network Associates appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please address your comments about Network Associates anti-virus product documentation to: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, U.S.A. You can also send faxed comments to (503) 531-7655 or e-mail to tvd_documentation@nai.com.

Reporting new items for anti-virus data file updates

Network Associates anti-virus software offers you the best available detection and removal capabilities, including advanced heuristic scanning that can detect new and unnamed viruses as they emerge. Occasionally, however, an entirely new type of virus that is not a variation on an older type can appear on your system and escape detection.

Because Network Associates researchers are committed to providing you with effective and up-to-date tools you can use to protect your system, please tell them about any new viruses that your software does not now detect. Note that Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your questions or virus samples to:

virus_research@nai.com	Use this address to send questions or virus samples to our North America and South America offices
vsample@nai.com	Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit* software to our offices in the United Kingdom

To report items to our European research office, use these e-mail addresses:

virus_research_europe@nai.com	Use this address to send questions or virus samples to our offices in Western Europe
virus_research_de@nai.com	Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit software to our offices in Germany

To report items to our Asia-Pacific research office, or our office in Japan, use one of these e-mail addresses:

virus_research_japan@nai.com	Use this address to send questions or virus samples to our offices in Japan and East Asia
virus_research_apac@nai.com	Use this address to send questions or virus samples to our offices in Australia and South East Asia

International contact information

To contact Network Associates outside the United States, use the addresses, phone numbers and fax numbers below.

Network Associates Australia

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australia 2065
Phone: 61-2-8425-4200
Fax: 61-2-9439-5166

Network Associates Austria

Pulvermuehlstrasse 17
Linz, Austria
Postal Code A-4040
Phone: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates Belgique

BDC Heyzel Esplanade, boîte 43
1020 Bruxelles
Belgique
Phone: 0032-2 478.10.29
Fax: 0032-2 478.66.21

Network Associates do Brasil

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Phone: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates Canada

139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Phone: (905) 479-4189
Fax: (905) 479-4540

Network Associates People's Republic of China

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
People's Republic of China 100044
Phone: 8610-6849-2650
Fax: 8610-6849-2069

Network Associates Denmark

Lautruphoej 1-3
2750 Ballerup
Danmark
Phone: 45 70 277 277
Fax: 45 44 209 910

NA Network Associates Oy

Sinikalliontie 9, 3rd Floor
02630 Espoo
Finland
Phone: 358 9 5270 70
Fax: 358 9 5270 7100

Network Associates France S.A.
50 Rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

Network Associates Deutschland GmbH
Ohmstraße 1
D-85716 Unterschleißheim
Deutschland
Phone: 49 (0)89/3707-0
Fax: 49 (0)89/3707-1199

Network Associates Hong Kong
19th Floor, Matheson Centre
3 Matheson Way
Causeway Bay
Hong Kong 63225
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates Srl
Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italy
Phone: 39 02 92 65 01
Fax: 39 02 92 14 16 44

Network Associates Japan, Inc.
Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001 Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0780

Network Associates Latin America
1200 S. Pine Island Road, Suite 375
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

Network Associates de Mexico
Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Phone: (525) 282-9180
Fax: (525) 282-9183

Network Associates International B.V.
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates Portugal

Av. da Liberdade, 114
1269-046 Lisboa
Portugal
Phone: 351 1 340 4543
Fax: 351 1 340 4575

Net Tools Network Associates South Africa

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
South Africa 2021
Phone: 27 11 706-1629
Fax: 27 11 706-1569

Network Associates South East Asia

78 Shenton Way
#29-02
Singapore 079120
Phone: 65-222-7555
Fax: 65-220-7255

Network Associates Spain

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid, Spain
Phone: 34 9141 88 500
Fax: 34 9155 61 404

Network Associates Sweden

Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

Network Associates AG

Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland
Phone: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Network Associates Taiwan

Suite 6, 11F, No. 188, Sec. 5
Nan King E. Rd.
Taipei, Taiwan, Republic of China
Phone: 886-2-27-474-8800
Fax: 886-2-27-635-5864

Network Associates International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
United Kingdom
Phone: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

Index

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z