

InocuLAN AntiVirus for Windows 95 version 5.0 User Guide

©Copyright 1997 Computer Associates International, Inc. and/or its subsidiaries.
All Rights Reserved.

U.S. GOVERNMENT RESTRICTED RIGHTS

The software and accompanying materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 subdivision (c)(1) and (2), as applicable. Contractor/manufacturer is Computer Associates International, Inc., One Computer Associates Plaza, Islandia, NY 11788-7000 (hereinafter "Computer Associates").

Computer Associates provides this publication "as is" without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. The entire risk as to the use of this information is assumed by the user.

In no event will Computer Associates be liable for any damages, direct, indirect, incidental, special or consequential, resulting from any defect in the information, even if it has been advised of the possibility of such damages.

Further, Computer Associates reserves the right to revise this publication and to make changes to it from time to time without obligation to notify any person or organization of such revision or change.

The use of software accompanying this documentation is subject to the Computer Associates License Agreement delivered with the software.

Trademarks

Cheyenne and InocuLAN are registered trademarks, and InocuLAN AntiVirus is a trademark of Computer Associates International, Inc., or one of its subsidiaries.

Other brand or product names used in this manual, but not listed here, are trademarks or registered trademarks of their respective holders.

Credits

Written by Richard Sheffield

Product Support

If you have any questions about this product, please contact us at one of the following locations:

USA, Canada, Asia, Latin America: 3 Expressway Plaza Roslyn Heights, New York 11577 USA	Main Voice Number: Technical Support: BBS: CompuServe: World-wide Web: FTP Server: InfoFax System:	516-465-4000 516-465-6600 Mon-Fri 8 am-8 pm EST 516-465-3900 GO CHEYENNE http://www.cheyenne.com/ ftp.cheyenne.com 516-465-5979 (Outside of North America you must use a fax machine's telephone.)
European Headquarters: Cheyenne Software S.A.R.L. Bel Air Building 58 rue Pottier 78150 Le Chesnay, France	Southern Europe Tech Support: Tech Support (FAX Hot Line): BBS: Infifax:	+33-1-39-23-18-70 Mon-Fri 09:00 - 17:00 +33-1-39-23-18-69 +33-1-39-23-18-60 +33-1-39-23-47-00
Germany: Cheyenne Software Deutschland Bayerwaldstr. 3 81737 Munich, Germany	Central and Eastern Europe Tech Support: Tech Support FAX: BBS (28800,N,8,1): BBS ISDN 64kB (v110, v120):	+49-89-627241-50 Mon-Fri 09:00 - 17:00 +49-89-627241-41 +49-89-627241-80 +49-89-627241-85
England: Cheyenne Software (UK) LTD Furness House 53 Brighton Road Redhill, Surrey, England RH1 6PZ	Northern Europe Tech Support: Tech Support FAX: BBS:	+44 (0) 990 134216 Mon-Fri 09:00 - 17:00 +44 (0) 990 785783 +44 (0) 990 143012
Japan: Cheyenne Software K.K. Sumitomo Fudosan Sanbancho Bldg. 3F, 6-26, Sanban-cho, Chiyoda-ku Tokyo 102, Japan	Voice: FAX: BBS:	+81-3-3222-3760 +81-3-3222-3762 +81-3-3222-3763
Taiwan: Cheyenne Software, Taiwan Branch Room C, 4th Floor 170 Tun Hua North Road Taipei, Taiwan	Voice: FAX:	886-2-545-5611 Mon-Fri 9 am-5 pm 886-2-545-5616

1

Chapter

ABOUT ANTIVIRUS FOR WINDOWS 95

In this chapter, you will learn:

Page

- | | | |
|-----|---|---------------------------------------|
| 1-2 | ➤ | About AntiVirus |
| 1-3 | ➤ | What a computer virus is |
| 1-4 | ➤ | Hints for preventing infection |
| 1-6 | ➤ | About the key features of AntiVirus |
| 1-7 | ➤ | Style conventions used in this manual |

What is AntiVirus for Windows 95?

InocuLAN AntiVirus is a full-featured Windows 95 application that detects and removes computer viruses. Once it is installed and running, AntiVirus continuously scans your files and memory for stored or active viruses. When a virus is detected, AntiVirus can be set to automatically respond, or to prompt you for action. Actions include attempting to clean, move, or delete the file.

Since new viruses appear all the time, InocuLAN AntiVirus can be easily updated by using the Update function to connect to Cheyenne's web site and download the latest virus signature file. This ensures that your system is protected from the most recently discovered viruses.

If you do not have access to an internet connection, you can request an update on a 3.5 inch disk by calling Cheyenne Software at 1-800-521-8591. You will be charged for shipping and handling costs.

What is a Computer Virus?

1

A computer virus is usually a small computer program which makes copies of itself on disks. Viruses may infect (copy to), or spread from executable/program files, or programs in disk boot sectors. Some non-executable files which use macros are also sometimes affected. The parasitic nature of a virus program is neither accident, nor a computer glitch. Viruses are created by people familiar with writing computer programs.

The effects of a computer virus can be as mild as a "Save the whales" message or as severe as deleting the entire contents of your hard drive.

InocuLAN AntiVirus lists details of all viruses for which it scans in the Virus Encyclopedia.

How Can a Virus Infect My System?

A virus has to "hitch-hike" onto your computer, usually attached to a file. The most common ways of picking up a virus are:

- Downloading software from on-line services or bulletin board systems (BBS).
- Loading files received via e-mail.
- Exchanging files by swapping diskettes.
- Copying files from a LAN or network to your hard drive.

Helpful Hints for Preventing Infection

InocuLAN AntiVirus has the ability to detect and clean most virus infections on your system, still there are a number of precautions you should take to avoid getting a virus in the first place.

These precautions will help prevent a virus from infecting your system or causing severe damage if you are infected:

Make Backups

Your best defense against virus damage is to **MAKE BACKUPS**. Knowing that you have good backups allows you to simply delete an infected file and replace it with a backed up copy. It is always a good idea to keep several backups of everything on your system you do not want to lose. Not only are backups handy to have in case of an infection, but they are also your main protection against system failure.

Never boot from a diskette

If your computer has a hard drive, never boot from a diskette. This is the main way the hard disk can become infected with a boot sector virus.

Remove floppy disks from the drive after use

Always remove any disk in a floppy drive immediately after using it. Leaving a disk in the drive leaves you open to accidentally booting from a diskette. If you have left a non-bootable diskette in drive A: when you turn the system on and get a "Not a system disk" message, turn the system off or press the Reset button. If the disk was infected, simply removing the disk or pressing Ctrl+Alt+Del may not be enough to stop the virus.

Write protect boot floppy disks

If you must boot from a floppy diskette, always use the same diskette, and keep it write-protected.

It is a good idea to keep all diskettes write-protected unless you need to write to them.

Be careful about your software source

Be careful regarding your sources of software. In general, shrink-wrapped commercial software should be "clean", but there have been a few documented cases of infected commercial software.

Public-Domain, Freeware and Shareware products are not necessarily more dangerous - it all depends on the source. If you obtain software from a BBS, check what precautions the SysOp takes against viruses.

Check all new software for infection before you run it for the first time.

Obtain Shareware, Freeware and Public-Domain software from the original author, if at all possible. All files of questionable origin should be scanned. You never know where they have been.

Use AntiVirus to scan often

Even with all these precautions, you should still scan your entire system for infection on a regular basis.



1

Software Preview

AntiVirus for Windows 95 advanced features

- *Complete Scanning* - scans not only files but memory, system files, and boot sectors.
- *Flexible Scanning* - enables scanning of individual files, individual folders and sub-folders, or one or more drives.
- *Real-time Scanning* - when Real-time scanning is running, it constantly scans all executable files that you run, and scans files copied to your system. If an infection is found, you are notified before the file is copied or executed.
- *Scheduled Scans* - a scan can be scheduled to run automatically.
- *Compressed File Scan* - AntiVirus can be set to scan the contents of compressed files for infection.
- *Cleaning Wizard* - when an infection is detected, the Cleaning Wizard guides you step-by-step through the process of either cleaning, moving, or deleting the infected file.
- *Rescue Disk* - a wizard guides you through the process of making a clean boot disk to use in case of an infection of the boot sector of your hard drive.
- *Updated Signatures* - as new infections are detected, they are added to the list of files that are detected by AntiVirus. The latest virus signature file can always be accessed by clicking the “Update” button.

Finding information in this manual

1

Scanning the left column of each page

You'll notice that this manual uses a two-column format. In the left column of each page, you will find three pieces of information:

- Margin headings
- Figure captions
- Note and warning icons

You can scan these items and get a quick summary of the information on each page.

The main headings serve two purposes: they divide the chapter into sections (normal function), and they act as a short summary for the paragraphs they represent.

The figure captions also serve two purposes: they identify a figure and they provide additional information about concepts being discussed.

Notes and warnings each have an associated icon that appears in the left column. You can scan for these items to find information critical to using AntiVirus.

*This is the icon for a note.
Its purpose is to remind you to do something or to emphasize important information.*



*This is the warning icon.
Its purpose is to draw attention to critical information.*



Using the tabs,
Table of Contents,
and Index

In addition to scanning the left column on each page,
you can also use the tabs, Table of Contents, and Index
to search for specific information.



2

Chapter

GETTING STARTED

In this chapter, you will learn:

Page	
2-2 >	About hardware and software requirements
2-3 >	How to install AntiVirus
2-9 >	How to start AntiVirus
2-10 >	How to make a rescue disk

Hardware and software requirements

To install and use AntiVirus, you will need the following hardware and software:

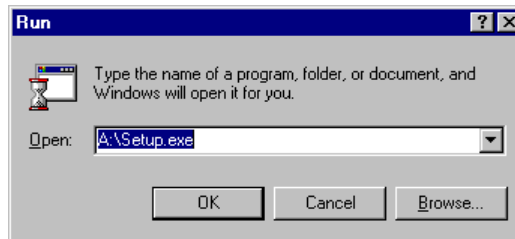
Machine Type	80486 DX 66MHz or higher computer
Operating System	Windows 95
System Memory	8 MB
Disk Space	8 MB

Installing AntiVirus

Follow these instructions to install AntiVirus on a Windows 95 machine:

1. **Start Windows 95.**
2. **Insert the CD-ROM in its drive.**
3. **From the Start menu, select *Run...***

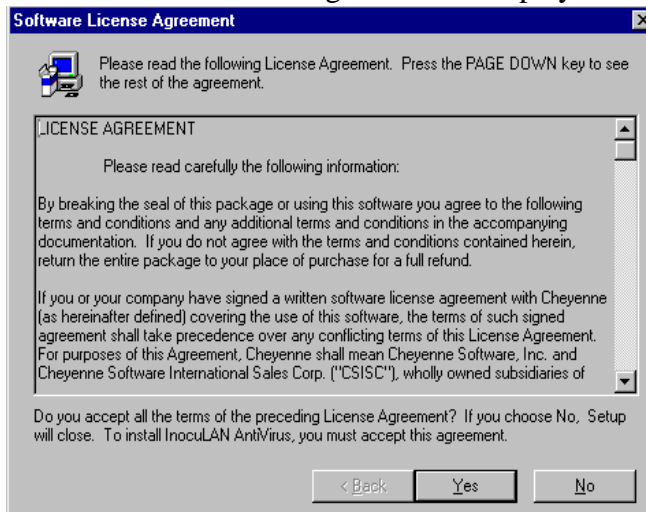
The following dialog box opens.



Run **SETUP.EXE** from the CD-ROM to start the Install Wizard.

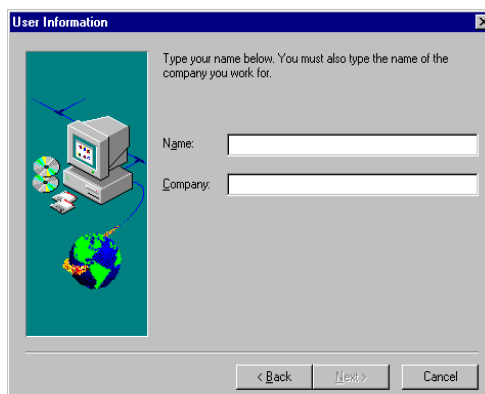
Click Next.

The Software License Agreement is displayed.



4. **Click Yes if you agree to the terms of the agreement.**

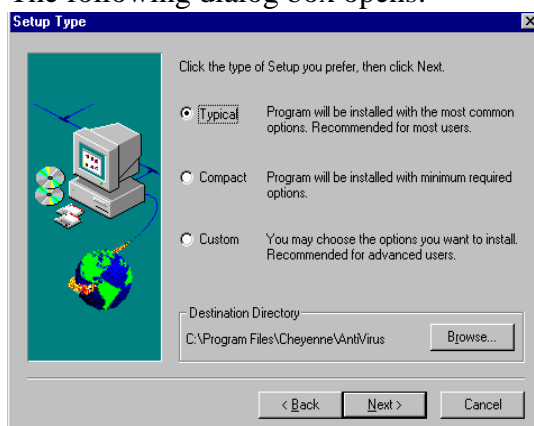
The following dialog box opens:



Enter your user information.

5. Click Next.

The following dialog box opens:

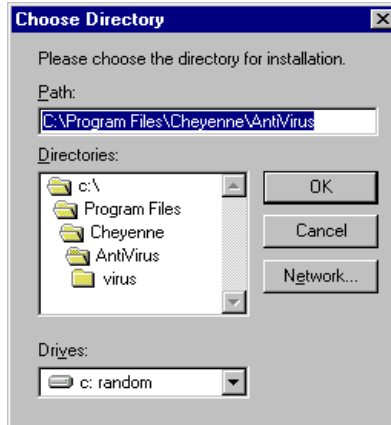


6. Choose the setup you want to perform.

Typical is the recommended setting.

7. Specify the directory where you want to install AntiVirus.

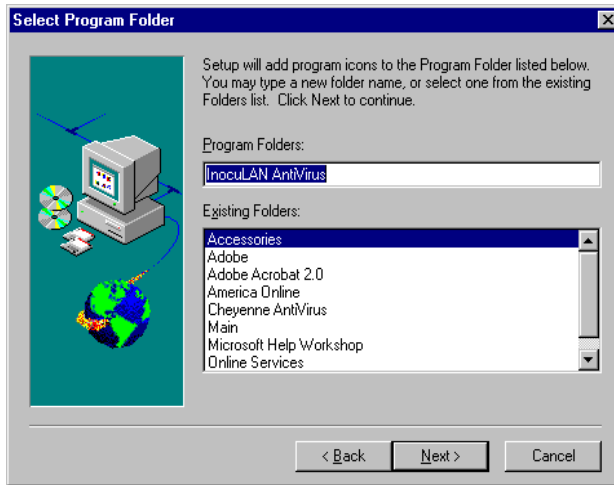
To change the default directory, click the Browse push-button to display the following dialog box:



Click OK to close the Choose Directory dialog box.

8. Click Next.

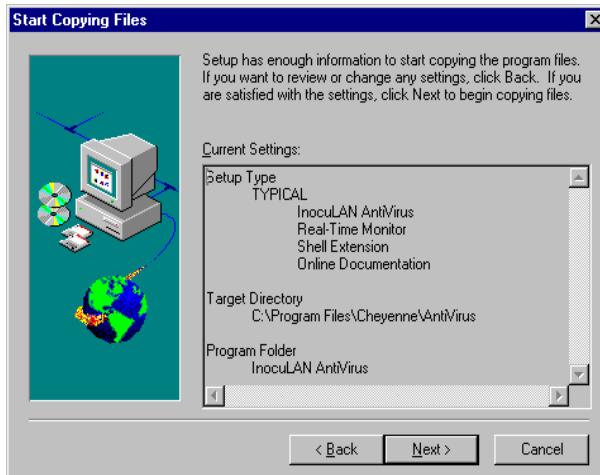
The following dialog box opens:



Accept the default program folder (InocuLAN AntiVirus), select an existing folder, or type in a new folder name in the edit field.

9. Click Next.

The following dialog box opens:

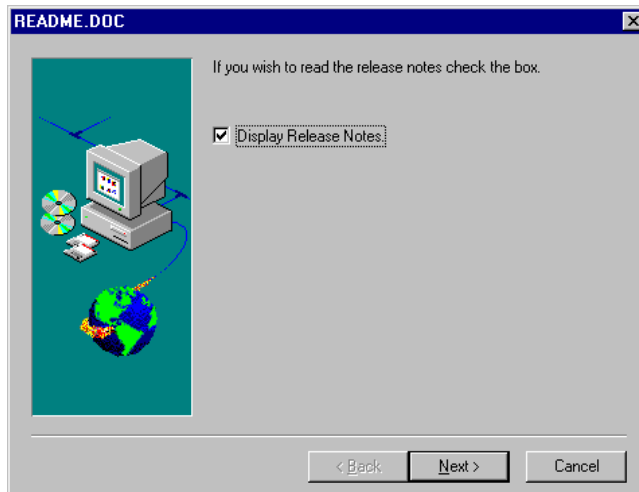


Verify your installation entries. If there is a problem, click Back to go back and correct it.

10. Click Next.

The install wizard starts to copy the AntiVirus files to the specified directory.

Once finished, the following dialog opens:



If you want to read the release notes now, check the box.

11. Click Next.

Select either to re-start your machine now or later. You must re-start your machine before you can use AntiVirus.

12. Click Finish.

AntiVirus is now installed on your machine. If you selected to do so, your system shuts down and re-starts.

Once your system re-starts, AntiVirus starts and the Setup Wizard continues by asking you if you would like to go ahead and scan your hard drive and make a rescue disk.

13. Click Next to go ahead and scan your system.

Otherwise, click Skip to skip to the rescue disk panel.

14. The scanner starts (if you selected to do so).

If an infection is detected, the Cleaning Wizard opens. See Chapter 4, “Dealing with Infections,” for detailed information on using the Cleaning Wizard.

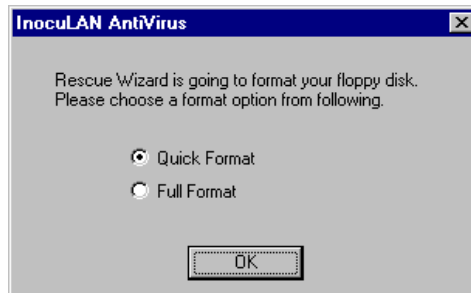
15. Click Done on the Scan Complete dialog box once the scan is finished.

The Rescue Disk Wizard opens.

16. Click Create.

This function allows you to create the Rescue Disk that contains critical system files and settings.

The following dialog box opens:



Choose the type of formatting to use during creation of the rescue disk.

- *Quick Format* - Removes all the files on the disk but does not scan for bad sectors. (This option can only be used on disks that have been previously formatted).
- *Full Format* - Removes all data from the disk and scans and marks bad sectors. (If you are certain that the disk you are using has not been damaged, use the *Quick Format* option).

17. Click OK.

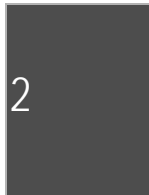
The disk is formatted and system files and settings are copied.

AntiVirus will open and is ready for use. Open the options dialog to customize AntiVirus to your work style and environment.

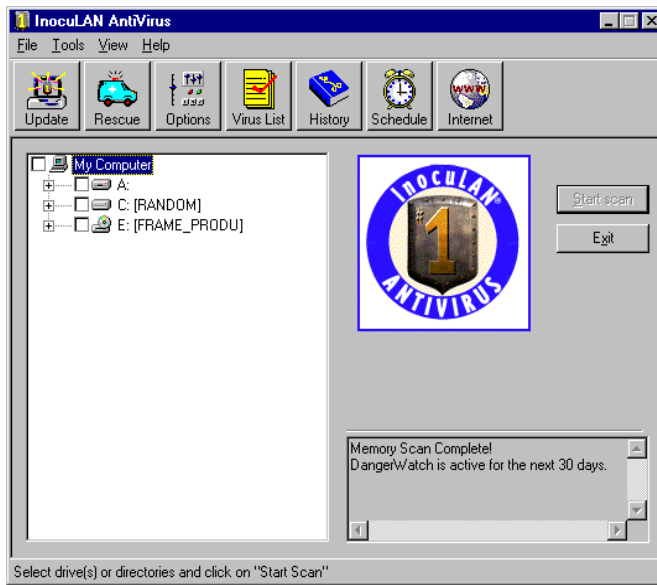
Starting AntiVirus

This section explains how to start AntiVirus.

1. **Click the Windows 95 Start button.**
2. **Click on Programs.**
3. **Click on the Cheyenne folder, then click the InocuLAN AntiVirus program icon.**



The application starts and opens the main scanner window:



The Rescue Disk

One of the first things you should do (if you did not do it during the installation process) after installing AntiVirus is to make a rescue disk. A rescue disk contains a backup of critical system files and settings that are required to boot your system. Boot up from the rescue disk if a virus causes boot problems by attaching itself in memory during the boot process. Booting with the rescue disk ensures a clean start-up without viruses in memory.

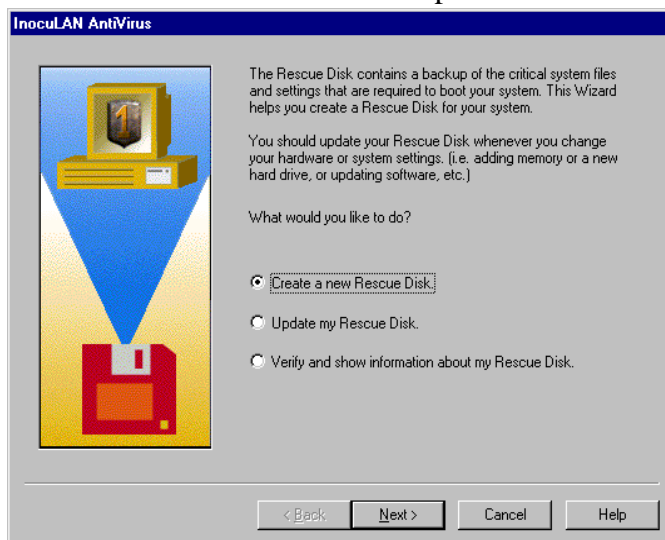
To make a rescue disk you need to run the Rescue Disk Wizard. This wizard guides you through the process of creating a rescue disk

How to run the Rescue Disk Wizard and make a rescue disk:



1. Select the Rescue icon on the toolbar.

The wizard introduction screen opens.



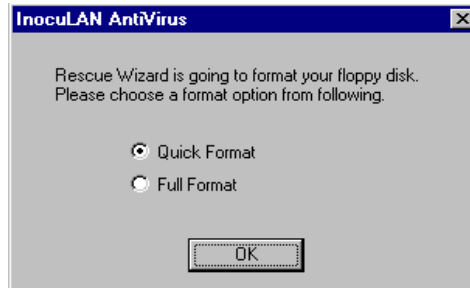
2. Select Create a new Rescue Disk and Click Next.

The following screen opens:



3. Make sure the disk is inserted into the floppy drive, then click Finish.

The following dialog box opens:



Select one of the radio buttons to indicate the type of formatting to use during creation of the rescue disk.

- *Quick Format* - Removes all the files on the disk but does not scan for bad sectors. (This option can only be used on disks that have been previously formatted).

-
- *Full Format* - Removes all data from the disk and scans and marks bad sectors. (If you are certain that the disk you are using has not been damaged, use the *Quick Format* option).

4. Click OK.

The disk is formatted and system files and settings are copied.

Updating a Rescue
Disk

To update an existing Rescue Disk:

1. Select the Rescue icon on the toolbar.

The wizard introduction screen opens.

2. Select Update.

3. Click Next.

The next wizard screen opens.

4. Make sure the disk is inserted into the floppy drive then click Finish.



You should update your rescue disk whenever you add new hardware or change system settings.

Verifying and
viewing Rescue
Disk information

Rescue disk data includes the date of the last update and the CPU that created it. To verify the critical system data copied to your Rescue disk, or to view information regarding the machine it was created for or when it was last updated:

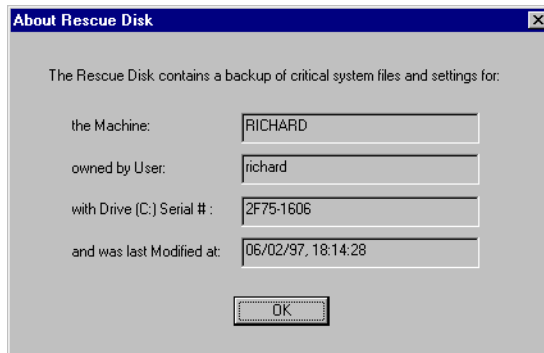
1. Select the Rescue icon on the toolbar.

The wizard introduction screen opens.

2. Select Verify and show information, then click Next.

3. Make sure the Rescue Disk is inserted into the floppy drive, then click Finish.

A report similar to the following opens:



Setting General options

There are a number of options that govern the basic operation of AntiVirus. After installation, review these settings and make changes if needed.

To set the general options:

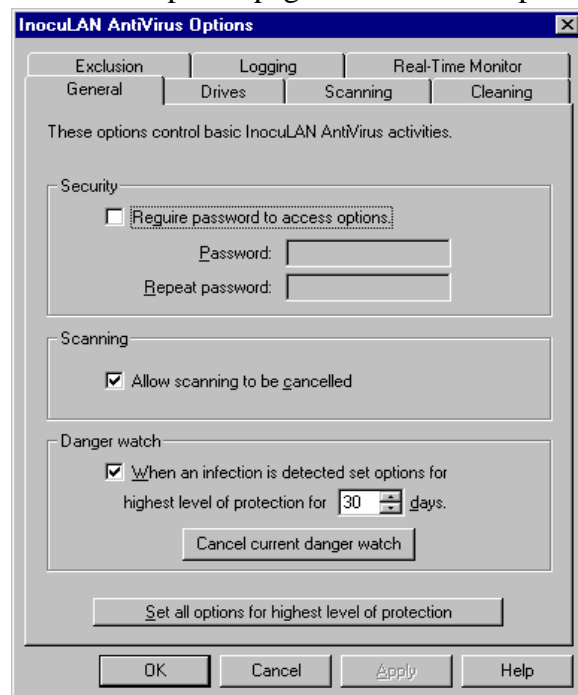


1. **Select the Options button on the toolbar.**

The Options dialog box opens.

2. **Click the General tab (if necessary).**

The Drives options page moves to the top



3. **Make your desired changes to the page.**

- *Require password* - Allows you to set password protection for your options settings. To define or change a password, use the fields below.
- *Password* - Type a password to be used to protect your options settings in this field. This field is only activated if the Require Password check box is checked. Repeat the password you just typed in the field above to double-check its accuracy. This field is only activated if the Require Password check box is checked.
- *Allow scanning to be cancelled* - Activates the Stop Scan push-button located in the bottom of the screen. This button allows you to cancel the scanning process.
- *Danger watch* - When a virus is detected in your system, InocuLAN AntiVirus will go to its highest level of protection for the number of days specified.
- *Set all options to highest level* - Immediately set all the preferences to reflect the highest possible level of AntiVirus protection.

4. Click OK.

3

Chapter


SCANNING FOR INFECTIONS

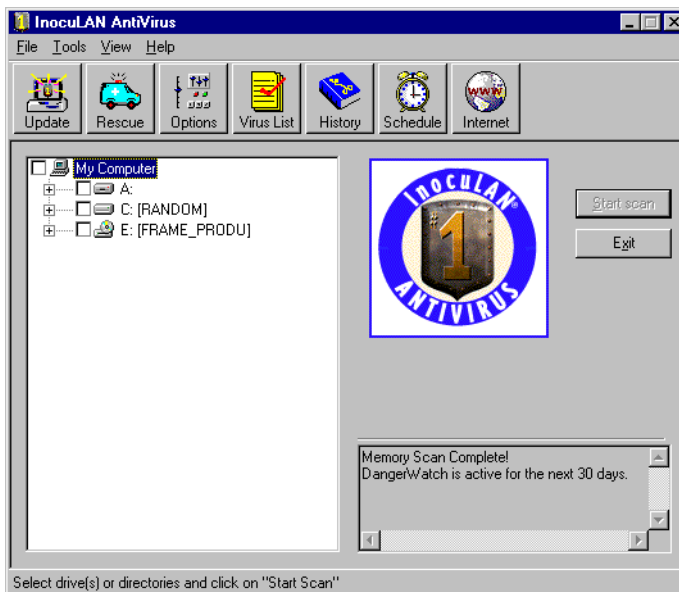
In this chapter, you will learn:

Page	
3-2	➤ About the scanner window
3-3	➤ About scanner display options
3-5	➤ How to scan an entire drive
3-5	➤ How to scan a folder and all its files and sub-folders
3-6	➤ How to scan an individual file
3-11	➤ About real-time scanning
3-13	➤ How to schedule an automatic scan
3-18	➤ About the AntiVirus logs
3-22	➤ How to update AntiVirus

The Scanner window

The Scanner window is the main interface into AntiVirus. The most important part of the Scanner window is the tree directory of drives and folders.

When first opened, the tree directory shows all the drives connected to your system (this can be changed in the Drives tab of the Options dialog box). Directories and folders are not shown but indicated by a plus sign  next to the drive. In this case, there are three drives; drive A: which is a floppy drive, drive C: which is a hard drive, and drive D: which is a CD-ROM drive.



Click on a plus sign to expand the list to view folders and sub-folders.

Scanner display options

A number of settings can be changed that affect what is displayed in the drives tree in the Scanner window.

To change the display:

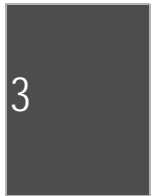
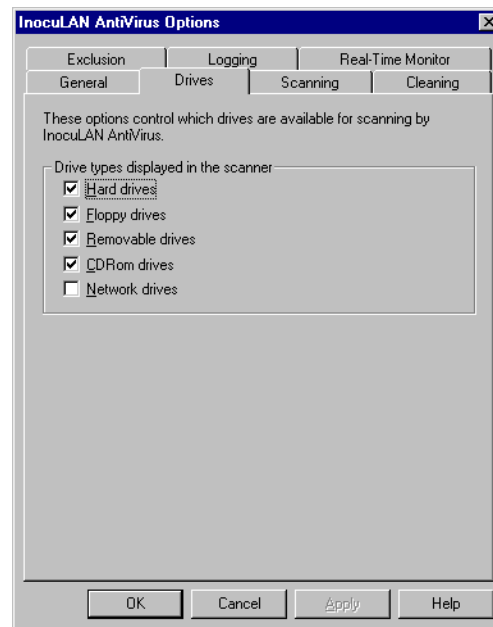


1. **Select the Options button on the toolbar.**

The Options dialog box opens.

2. **Click the Drives tab.**

The Drives options page moves to the top.



These are the default settings for drives.

3. **Make your changes and click OK.**

Drives configuration fields

Drive type displayed
in the scanner

Click the items in this list to tell the scanner what drive types to display in the tree structure.

- Hard Drives
- Floppy drives
- Removable drives
- CD-ROM drives
- Network drives

Scanning

AntiVirus can scan:

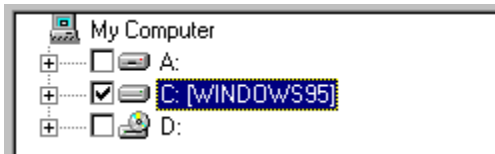
- An entire drive
- An individual folder including all files and sub-folders it contains
- An individual file

Scanning an entire drive

To set the scanner to scan an entire drive:

- 1. Click on the empty box next to the drive, a check mark is placed in the box.**

This indicates that the entire drive is to be scanned.



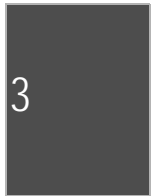
- 2. Click on *Start scan*.**

The scanner starts and scans through all folders and files on the selected drive. If a virus is detected, the Cleaning Wizard is started (see chapter 4, "Dealing with an Infection" for more information on the Cleaning Wizard).

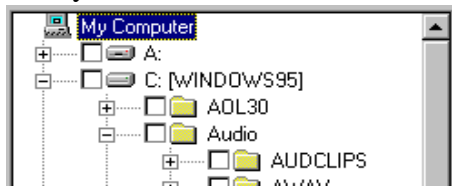
Scanning a folder

To set the scanner to scan only a particular folder:

- 1. Click the plus sign next to a drive to expand to the next level.**



If a folder contains sub-folders, a plus sign appears next to the folder. You can keep expanding the tree until you reach the desired folder.



2. Click in the empty box next to the desired folder.

This marks the folder for scanning.

3. Click *Start Scan*.

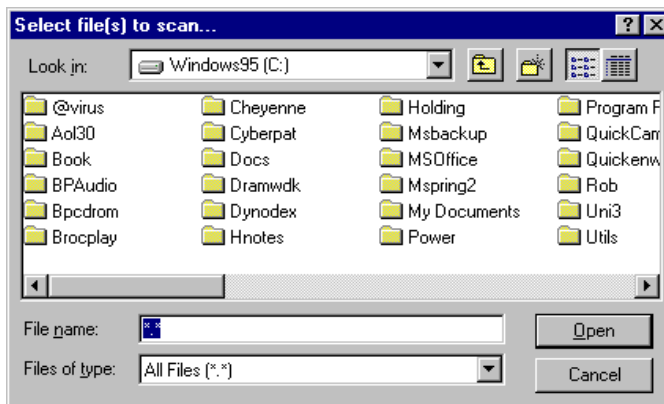
The scanner starts and scans through all files and sub-folders in the selected folder. If a virus is detected, the Cleaning Wizard is started (see chapter 4, “Dealing with an Infection” for more information on the Cleaning Wizard).

Scanning an individual file

To set the scanner to scan an individual file:

1. Choose *Scan files...* from the File menu.

The Select file to scan dialog box opens:



2. Double-click a folder (if necessary) to view its sub-folders.

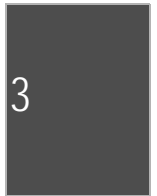
Navigate through the folders until you can see the file you want to scan.

3. Click on the file name to select it and click *Open*.

The scanner starts and scans through the file. If a virus is detected, the Cleaning Wizard is started (see the, “Dealing with an Infection” chapter for more information on the Cleaning Wizard).



You can scan both an entire drive and a particular folder at the same time by placing checkmarks next to each item you want to scan. However, multiple files can be scanned at the same time only if they reside in the same folder.



Scanning with the
Microsoft Windows
Explorer

You can also scan an individual file by right-clicking on it from within the Microsoft Windows Explorer and choosing *Scan for Viruses*.

Setting Scanning options

A number of settings can be changed that affect the scanning process.

To change the scanner settings:

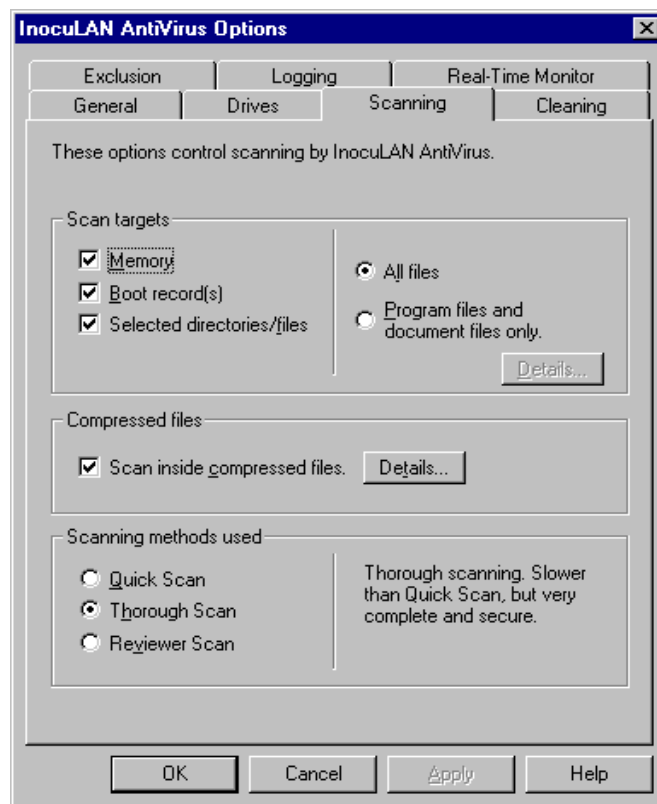


1. **Select the Options button on the toolbar.**

The Options dialog box opens.

2. **Click the Scanning tab.**

The Scanning options page moves to the top.



3. **Make your changes and click *OK*.**

Scanning configuration settings

Scan targets

Check one or more of the following:

- Scan Memory - Scans internal memory as part of each scanning process.
- Scan Boot Record - Scans the boot record portion of your hard drive as part of each scanning operation.
- Scan Selected Directories/Files - Scans the contents of individual directories and files that you checked in the list in the main scanning screen.

Select either:

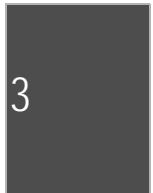
- Scan All Files - Scans all the files in the targets.
- Scan Program Files - Scans only program files in the selected targets list. By default, program files are defined as those files with .EXE, .COM, or .DLL extensions. Select the Details button to add other extensions or remove extensions.

Compressed files

Scan Inside Compressed Files - Sets the program to scan inside compressed files (such as .ZIP) for attached viruses. Select the Details push-button to add or remove file extensions that identify a file as compressed.

Scanning method used

Select one of the following to determine the intensity and speed of the scanning process.



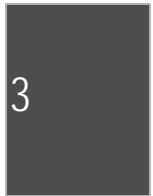
-
- Quick Scan - Adequate scanning for normal operation. Combines the best performance with reasonable security.
 - Thorough Scan - Slower than Fast Scan but performs a complete and secure scan.
 - Reviewer Scan - Should be used by testers and reviewers only. This setting slows scanning without adding additional virus protection.

Real-time Scanning

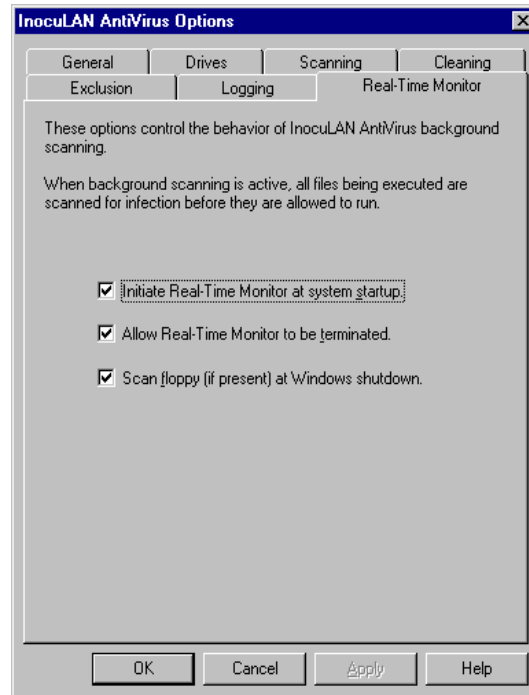
AntiVirus can be set so that it runs all the time, in the background, when your computer is booted. This is referred to as real-time scanning. Real-time scanning scans all executable files before they are allowed to run. It also scans any file that you attempt to copy to your computer. If a virus is detected, the Cleaning Wizard opens. Refer to chapter 4, “Dealing with an Infection” for more information on the Cleaning Wizard.

To activate real-time scanning:


1. **Select the Options button on the toolbar.**
2. **Click the Real-Time Monitor tab.**



The Real-Time Monitor page moves to the top.



3. Select *Initiate Real-time Monitor at start up* and click **OK.**

Whenever Real-time Scanning is activated, the AntiVirus icon  can be seen in the tray area of the windows task bar at the bottom of the screen.

Scheduling an Automatic Scan

The AntiVirus Schedule Wizard is used to set up automatic scans at a determined time and/or frequency.

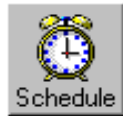
The Schedule Wizard guides you through the process of setting up an automatic scheduled scan. This automatic scan can occur only once (at a time you determine), or you can set it to run hourly, daily, weekly, or monthly.

Scheduled scans can be set to run on one or more folders or on one or more drives.

Schedule a scan for folders only, or folders and drives

To Schedule a scan on folders only, or drives and folders:

1. **Go to the main scanning screen and expand the tree directory to view the folder(s) you wish to scan.**
2. **Check the box next to each folder or drive for which you want to schedule a scan.**



3. **Select the Schedule button on the toolbar.**

The Schedule Wizard opens with your selections displayed in the first panel.

4. **If satisfied with these selections, click Next to advance to the next panel.**

You can clear the selections using the Clear Current Selections button and use the Back button to return to the Scanner screen to make other selections.

(See the section on “Completing the Schedule Wizard” for further instructions)

Schedule a scan for
drive(s) only



To schedule a scan on drives only:

1. **Select the Schedule button on the toolbar. The Schedule Wizard opens.**
2. **Click Next to advance to the next panel where you can select the drive(s) you wish to scan.**
3. **Select one or more drives to schedule a scan for by checking the box next to each drive in the list.**
4. **Click Next to continue on to the next wizard panel.**

Completing the
Schedule Wizard

Once you have selected the drives and/or folders for which you want to schedule a scan, the *When do you want to run the scan* panel opens.

1. **Select how often you want the scheduled scan to occur by checking one of the radio buttons.**

If you choose *Daily*, the *Days* push-button is activated. You can now exclude from scanning certain days of the week if you wish.

2. **Enter the time when you want the scheduled scan to start in the *Scan At* field, or accept the current time as the default.**
3. **Select Next to advance to the Scheduled Scan Options panel.**
4. **Indicate your scanning options:**

➤ *Use normal options but ALWAYS log as action* - Your normally set scanning options are used, BUT if a virus is detected, the only action taken is to log the infection and continue the scan. Using this option insures that the entire

scan is completed. You can view the Infection Log later to see if any infections were found.

- *Use normal options* - Selecting this button uses all your normal scanning options.



If you have your options set to prompt you if an infection is found, the scan will stop until you make a selection in the Prompt dialog box. If you are running this scheduled scan when you are not at the computer, the scan will not be completed until you return.

- *Specify custom options now* - Allows you to set custom options that are used for this scheduled scan only.

5. Click Next.

The Scan Confirmation panel opens. This panel lists all the details of the scan you have scheduled.

6. Review the entire contents of the window then click **Finish** to complete the process and enter the scan in the Scheduler or click **Back** to make changes.

Editing and deleting a scheduled scan

Once the scan is entered in the Scheduler, you can view all scheduled scans by selecting *Scheduled Scans* from the View menu. From here you can view all the scheduled scans, remove unwanted scans and modify previously defined scheduled scans.

Excluding specific files and folders from scanning

There may be times when you want to keep AntiVirus from scanning a particular file type, folder or file. For example, if you always move infected files to a quarantine folder, you should exclude this folder from scanning since you know the files there are infected.

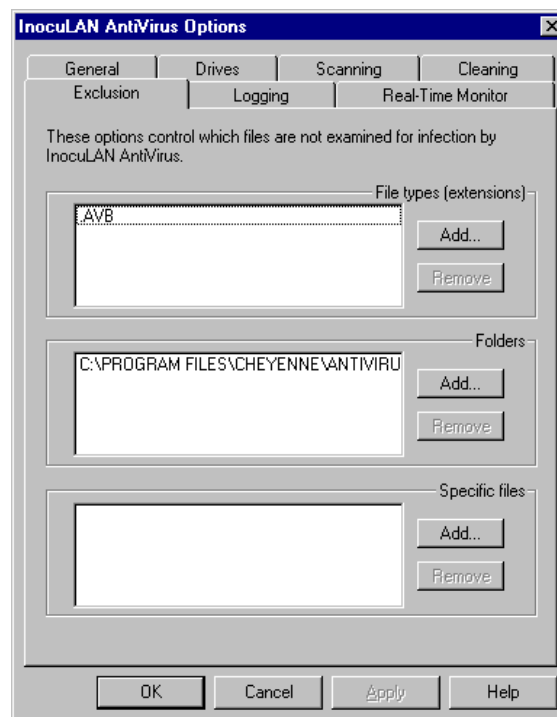
To exclude a file type, folder or file from scanning:



1. **Select the Options button on the toolbar.**

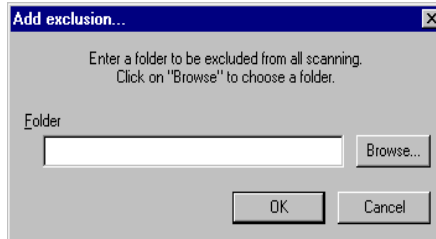
The Options dialog box opens.

2. **Click the Exclusion tab.**



3. **Click Add in the appropriate area to add a new file extension, folder, or file to the exclusion list.**

The following (or similar) dialog box opens:



4. Complete the dialog box.

For a new file extension - enter the new extension in the edit field.

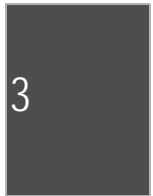
For a new folder - enter the folder name (including the complete path) in the edit field or click the Browse button to select the folder.

For a new file - enter the file name (including the complete path) in the edit field or click the Browse button to select the file.

5. Click OK.

The new item is added to the list in the Exclusion page.

6. Click OK to close the Options dialog box.



AntiVirus Logs

AntiVirus keeps log files of your virus scanning activities. Three different log files are maintained:

- **The History Log** - keeps a list of each scan and records information regarding the number of files scanned and the number of infections found. The contents of this log can be changed in the Logging page of the Options dialog box.
- **The Infection Log** - keeps a list of names and locations of each infected file found, the infection type and what was done as a result of finding it. The contents of this log can be changed in the Logging page of the Options dialog box.
- **Last Scan** - lists the results of the most recent scan during this AntiVirus session.

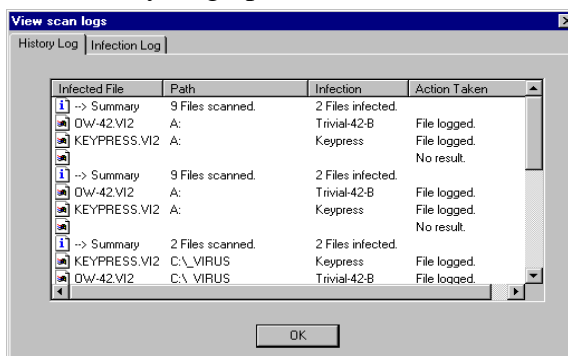
The History Log



To view the History Log:

1. **Select the History button on the toolbar.**
The View Scan Logs dialog box opens.
2. **If not on top, select the History Log tab.**

The History Log opens.



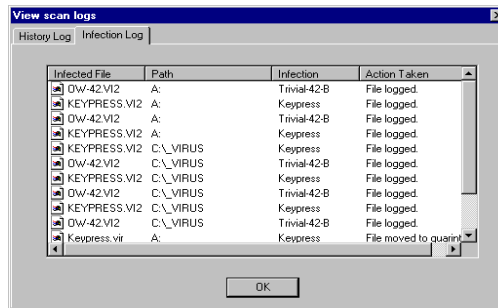
The Infection Log



To view the Infection Log:

1. **Select the History button on the toolbar.**
The View Scan Logs dialog box opens.
2. **If not on top, select the Infection Log tab.**

The Infection Log opens.



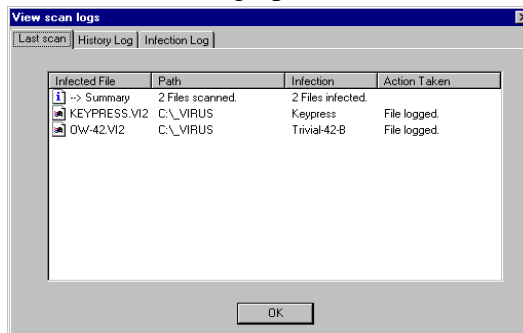
The Last Scan Log



To view the Last Scan Log:

1. **Select the History button on the toolbar.**
The View Scan Logs dialog box opens.
2. **If not on top, select the Last Scan Log tab.**

The Last Scan Log opens.



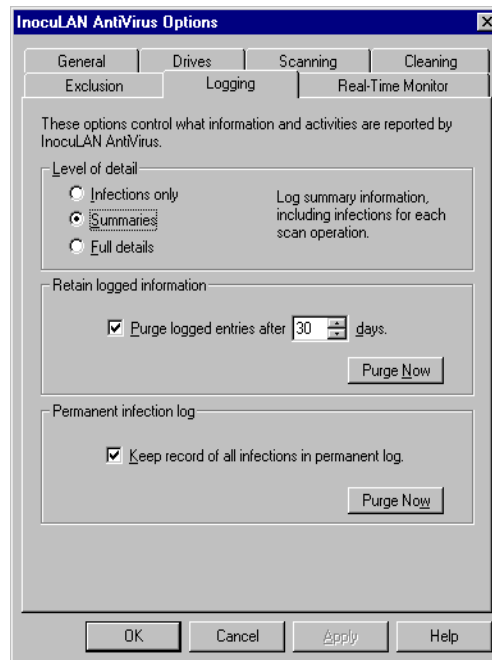
Logging Options

The Logging options control what information gets stored in the logs and how to handle purging old information.

To view the Logging options:



- 1. Select the Options button on the toolbar.**
The Options dialog box opens.
- 2. Click the Logging tab.**



Logging configuration fields

Level of Detail

Click one of the items in this list to control the amount of information logged in the History log.

- **Infections Only** - Only writes information about infected files to the infection log.
- **Summaries** - Writes information about infected files and summary information to the infection log.
- **Full Details** - Writes information about every file scanned to the log file.

Retain Logged Information

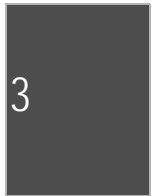
Purge logged entries after number of days - Automatically purges the contents of your log files after the number of days indicated. Adjust the number of days using the up and down arrows or type a new number in the field.

Purge Now - Immediately purges the contents of the log file.

Permanent Infection Log

Keep a record of all infections in permanent log - Writes details of all infections detected by AntiVirus to the permanent History log file.

Purge Now - Immediately purges the contents of the log file.



Updating InocuLAN AntiVirus Files

New viruses appear every day so AntiVirus provides a quick and easy way to update your virus signature files via the Internet. These signature files contain the data that AntiVirus uses to identify known viruses.

If you do not have access to an internet connection, you can request an update on a 3.5 inch disk by calling Cheyenne Software at 1-800-521-8591. You will be charged for shipping and handling costs.

Using the Live Update Wizard

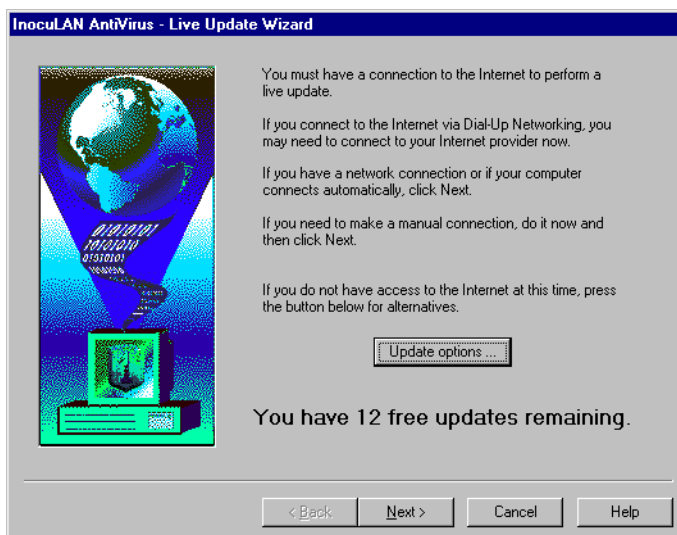
The Live Update Wizard guides you through the process of connecting to Cheyenne Software and downloading a new signature file if necessary.

To use the Update Wizard:



1. Select the Update button on the toolbar.

The Live Update Wizard opens.



- 2. Connect to the Internet if you do not have a permanent Internet connection.**
- 3. Click Next.**

The Wizard connects to Cheyenne Software and guides you through the update process.

When purchased, InocuLAN AntiVirus includes one or more free updates. Follow the directions above to check for monthly update postings. The number of free updates remaining only decreases when you complete a download.

You can also click on *Help, About InocuLAN AntiVirus...* in the main Scanner window for a listing of the number of signature file updates remaining.



3

4

Chapter

DEALING WITH AN INFECTION

In this chapter, you will learn:

Page

- 4-2 ➤ How to set the Cleaning options
- 4-5 ➤ What happens when a virus is found during scanning
- 4-6 ➤ How to use the Cleaning Wizard

Cleaning Options

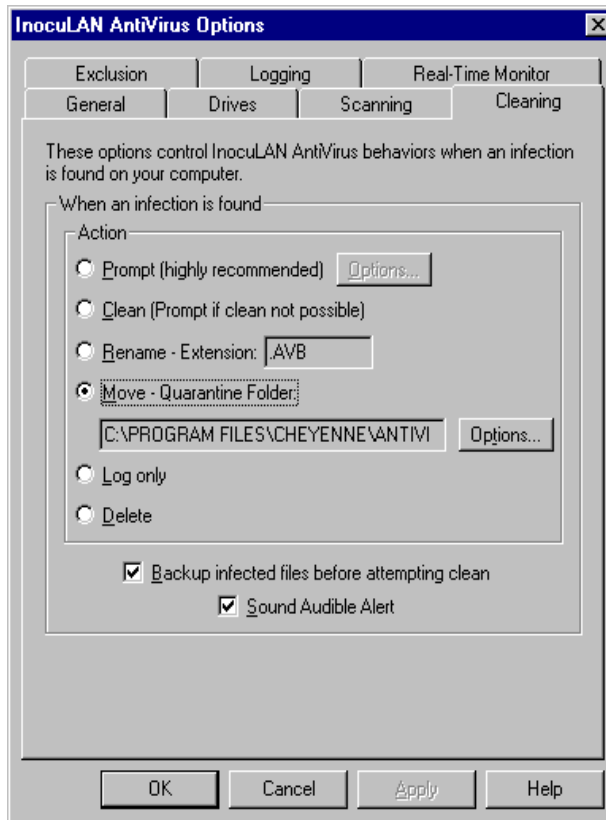
The action taken by AntiVirus when it finds an infected file is determined by the settings on the Cleaning tab of the Options dialog box.

To view the Cleaning options:

1. **Select the Options button on the toolbar.**

The Options dialog box opens.

2. **Click the Cleaning tab.**



Cleaning Configuration fields

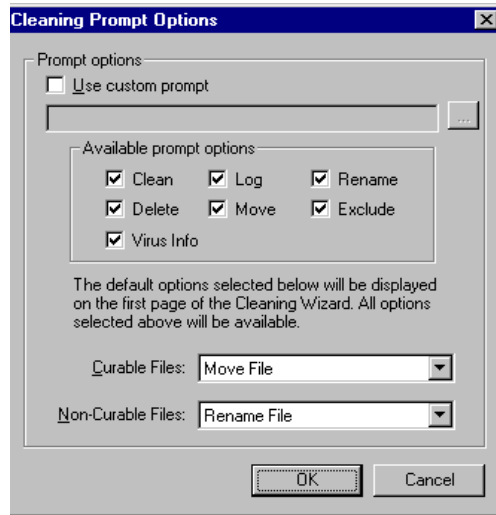
Prompt

When an infection is found on your system, InocuLAN AntiVirus will ask you what action to take. The Cleaning Wizard starts and guides you through the process of dealing with the infection. **(Highly recommended setting)**

Prompt Options

Clean, Log, Rename, Delete, Move, Exclude, and Virus Info. Also, this option allows you to create and use a custom prompt. You can select from this list the options that will be available to you when prompted for action.

This dialog box also allows you to specify default prompt actions for curable files and non-curable files.



Clean

When an infection is found in your system, AntiVirus automatically attempts to clean and restore the file. If this is not possible, you are prompted for further action such as “delete” or “move”.

<i>Rename</i>	When an infection is found in your system, AntiVirus automatically renames the file using the original filename plus the extension shown. To change the extension used, type the new extension in the edit field.
<i>Move</i>	When an infection is found in your system, AntiVirus automatically moves the file to the specified location. Press the Change button to change the location.
<i>Change Location</i>	Press this button to tell the program where to move infected files when the Move action is selected.
<i>Log Only</i>	When an infection is found in your system, AntiVirus automatically logs the file but does not perform any other action.
<i>Delete</i>	When an infection is found in your system, AntiVirus automatically deletes the file.
<i>Backup Before Clean</i>	An infected file is backed up before file cleaning and restoration is attempted.
<i>Sound Alert</i>	An audible alert is sounded whenever an infection is discovered. This is especially helpful if you have Log Only as the selected action.

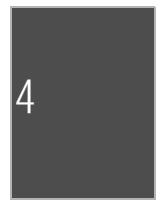
The Cleaning Wizard

If you have your Cleaning options set to *Prompt*, the Cleaning Wizard opens whenever AntiVirus finds an infected file during scanning.

The Cleaning Wizard tells you about the nature of the virus, the infected file, offers advice on dealing with the virus, and then steps you through the process.

The selections available on the first screen of the Cleaning Wizard depend on two conditions:

- whether the infected file is determined to be curable or non-curable and,
- what the default options are for curable and non-curable files.



Using the Cleaning Wizard

The Cleaning Wizard appears when a virus is found during scanning and you have *Prompt* set as the action to take. This first page lists the virus type and location and tells you if the file can be cleaned.

- 1. The Cleaning Wizard opens. An infected file has been found during scanning and you have Prompt set as the action to take.**

The first screen of the Wizard opens.

- 2. Under “How would you like to handle this infection?” select either the default action or the Display All Options radio button.**

The default action is checked, but you can select *Display All Options* if you wish to choose another option. The default option that is displayed is determined by the setting on the Cleaning tab of the Options dialog box. Here you can set a default option for files that can be cleaned and files that cannot be cleaned.

- 3. (Optional) Select *Virus info* to display the Virus Encyclopedia information of the virus detected.**

The Virus Encyclopedia opens for the detected virus.

- 4. (Optional) If the selected action is *Log Only*, then you may check the Continue Scanning check box to keep scanning the archive and logging infected files.**

Otherwise this check box is grayed out.

- 5. If you wish the selected action to be performed for all infected files of the type found, then check *Do this for all infections...* and click *Next*.**

To continue on to the next wizard screen or click *Skip File* so that no action is taken for the file listed. The scan continues for more infected files.

6. If you select *Display All Options* and click Next, the first panel of the wizard is re-appears, now listing all available cleaning options.

The available options are determined by the settings on the Cleaning page of the Options dialog.

All possible options:

- Clean - Attempts to clean the infected file.
- Rename - Adds the specified extension to the filename. This extension is .AVB.
- Move - Moves the file to the directory specified as the quarantine area. This folder is ... \VIRUS beneath the folder where you installed AntiVirus.
- Log - Makes an entry in the History and Infection logs only.
- Never Scan Again - Sets AntiVirus to exclude this file so it is not scanned again.
- Securely Remove - Deletes the infected file in a manner that prevents the activation or spread of the virus.

7. Click Next to continue to the next Wizard panel.

The selected action is described.

8. Click Finish to execute the selected action.

If the action is successful, the scan continues to look for more infected files. If it is not successful, you are prompted for another action.

Once the scan is complete, a report opens listing the infections found and actions taken.