What is InocuLAN AntiVirus?

InocuLAN AntiVirus is a full-featured Windows 95 application that detects and removes computer viruses. Once it is installed and running, AntiVirus can be set to continuously scan 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 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.

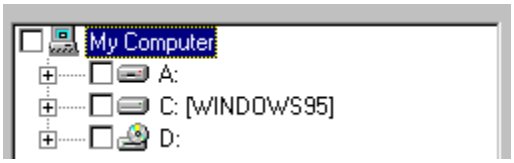
See Also

Getting Started

Scan Screen Overview

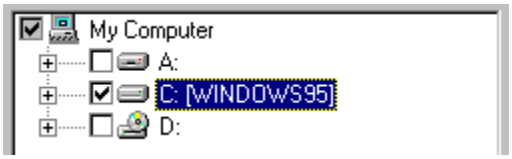
Scan Screen Overview

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



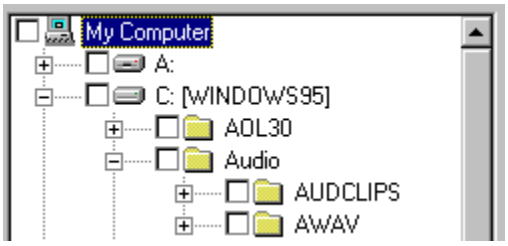
When first opened, the tree directory shows all the drives connected to your system. Directories and folders are not shown but indicated by a plus sign ⊞ next to the drive. In this case there are three drives, drive A: which is a floppy drive, drive C: which is a hard drive, and drive D: which is a CD-ROM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

To set the scanner to scan an entire drive:



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.

To expand the view of a drive so you can mark individual folders for scanning:



Click the plus sign next to the drive and it will 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.

Once drives and/or folders are selected, you can click the **Start Scan** push-button to begin the virus scanning process.

{button ,JI(`CAV.HLP',`Toolbar')} **See Also** - **Toolbar Information**

Getting Started

As part of the installation process, AntiVirus checks your system memory for infection. If no viruses are found, select the **Options** button on the toolbar to display the Preferences dialog box. Use this dialog box to configure InocuLAN AntiVirus to function the way you want it to. Select each tab at the top of the dialog box to view pages containing the various features. Press the F1 key to get help then click on any item you do not understand to display on-screen tips and help.

It is recommended that you scan the entire contents of all hard drives as well as any frequently used floppies after you successfully install AntiVirus.

If the installation process discovers a virus on your system:

You have a virus in your computer's memory. In this case, you need to shut down and reboot your system from a known safe floppy disk. Once you re-boot, run AntiVirus again to check your memory. If no infection is detected, then make a Rescue Disk and scan and clean your hard drive.

The Rescue Disk

This Rescue Disk Wizard guides you through the process of creating a rescue disk.

A rescue disk contains a back-up of critical system files and settings that are required to boot your system. Boot from the rescue disk if a virus is causing boot problems or installing itself in memory during the boot process. Booting with the rescue disk ensures a clean start-up without viruses in memory.

The wizard offers you three options:

Create a new rescue disk

Selecting this option formats the disk in the floppy drive and then backs up the required system files and settings.

Update

Use this option when you already have a rescue disk and only need to update it due to changes to your system. You should update your rescue disk whenever you make hardware or setting changes to your system.

Verify and show information

Lists information about the machine that the disk was created for and the last time that the disk was modified.

It is important to always have a current rescue disk on hand so that you will always be able to boot your computer and maintain critical system data and settings.

Getting Help

You can access help information about the various features of InocuLAN AntiVirus in several ways.

Help Topics

Select the Help Topics option from the Help menu. This displays the Contents panel for the online help system. From here you can browse the help topics or search the index or the entire help file for a word or phrase.

Context-sensitive Help

You can also access context-sensitive information to get help without interrupting your work:

- For an explanation of each toolbar icon, place the cursor over the icon and read a description in the status bar at the bottom of the window.
- For an explanation of a menu option, highlight the option and press the `F1` key.
- For an explanation of a field or control in a dialog box, press the `F1` key.

{button ,JumpHelpOn()} Click here for more detailed information on using the online help system.

See Also

Context Help command

Contacting Cheyenne Software

For further product support, please contact one of the following:

Customer Support:

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

Preventing Infection

InocuLAN AntiVirus should be able to detect and clean up 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.

Precautions

- Your best protection against virus damage is to **MAKE BACKUPS**. Knowing that you have good backups enables you to simply delete an infected file and replace it with a backed up copy. It's 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 catastrophic system failure.
- 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.
- Always **remove any disk in a floppy drive immediately after using it**. Leaving a disk in the drive is the main way people accidentally boot from a floppy. If you, by accident, have left a non-bootable diskette in drive A: when you turn the computer on and get a "Not a system disk" message, turn off the computer 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.
- If you must boot from a floppy diskette, **always use the same diskette**, and keep it write-protected.
- In fact it is a good idea to **keep all diskettes write-protected** unless you need to write to them.
- **Be really 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. But be sure to scan all files of who origins you are unsure. You never know where they have been.
- And even with all these precaution, you should still s**can your entire system on a regular basis**.

Viruses

What is a Computer Virus?

A computer virus is (usually) a small computer program that makes copies of itself on computer disks. Viruses may infect (copy to), and spread from, executable/program files, or programs in disk boot sectors. Some non-executable files that use macros can also be affected. This parasitic nature that virus programs have is neither an accident, nor a computer glitch. People familiar with writing computer programs create viruses.

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 the details of all the 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 online services or bulletin board systems.
- Loading files received via e-mail.
- Exchanging files by swapping diskettes.
- Copying files from a LAN or network to your hard drive.

How do I keep AntiVirus from scanning certain files, directories, and file types?

There may be times when you do not want AntiVirus to scan certain file types (extensions), directories, or files. For example, if you always move infected files to a particular directory, then it would be a good idea to exclude that directory from scanning since you know the files there are infected.

To exclude items from scanning:

1 Select the **Options** button 

on the toolbar.

2 Select the **Exclusion** tab.

3 Select the **Add** push-button for the item you wish to exclude (file type, folder, or specific file).

4 Enter the file extension, or a complete path to the folder or specific file you wish to exclude from scanning.

5 Click **OK**.

6 Repeat the procedure for other exclusions if necessary.

7 Click **OK**.

How Do I Set AntiVirus for the Highest Level of Protection?

1 Select the **Options** button 

on the toolbar.

2 Select the **General** tab.

3 Click the **Set all options for highest level of protection** push-button.

How Do I Tell the Program What to Do When it Finds a Virus

1 Select the **Options** button 

on the toolbar.

2 Select the **Cleaning** tab.

3 Select the radio button in the Actions area to specify the action you want the program to take.

NOTE Selecting the **Prompt** option is recommended.

TIP If you select either Move or Rename, you might want to exclude the new file extension or the directory specified so they will not show up in future virus scans.

How Do I Control What Drives are Displayed in the Main Window

1 Select the **Options** button 

on the toolbar.

2 Select the **Drives** tab.

3 In the list at the top of the dialog box, check the box(es) next to the drive types you wish to display. If you wish certain drives types to always be selected by default, also select them in the list at the bottom of the dialog box.

How Can I Set the Program to Scan Inside Compressed Files?

1 Select the **Options** button 

on the toolbar.

2 Select the **Scanning** tab.

3 Check the **Scan inside compressed files** check box.

How Can I Control the Level of Detail in My Log Files?

1 Select the **Options** button 

on the toolbar.

2 Select the **Logs** tab.

3 Select a radio button in the Level of Detail area.

How Can I Empty My Log Files

1 Select the **Options** button 

on the toolbar.

2 Select the **Logs** tab.

3 Press one of the **Purge** pushbuttons.

TIP You can also set AntiVirus to automatically purge your log file after a set number of days by checking the **Purge Log entries** check box and adjusting the number of days.

How Can I Set AntiVirus to Run Automatically?

You can set AntiVirus to automatically scan any file being executing before it is allowed to run.

1 Select the **Options** button 

on the toolbar.

2 Select the **Real-time Scanning** tab.

3 Select **Initiate background scanning at start-up**.

How Do I Manually Scan a Particular Directory?

1. Make sure the media you want to scan is in an accessible drive.
2. Un-check all drives in the main window.
3. Click the Plus box ⊞ next to the drive to expand the drive contents until you reach the desired folder or file.
4. Check the box ☑ next to the folder to indicate it is to be scanned.
5. Click **Start Scan**.

How Do I Manually Scan a Particular File?

1. Make sure the media you want to scan is in an accessible drive.
2. Un-check all drives in the main window.
3. Select **Scan File(s)** from the File menu. The Select File(s) to scan dialog box opens.
4. Navigate to the folder containing the file(s) you want to scan.
5. Select the file to scan by clicking it with the left mouse button. You can select more than one file in the same folder by clicking while holding down the **Ctrl** or **Shift** key.
6. Click **Open**. The scan is performed and you are notified of the results.

How Do I Get Detailed Information About a Particular Virus?

1 Select the **Virus List** button 

on the toolbar.

2 Type all or part of the virus name in the **Enter a virus name** field, or scroll through the list and select a virus.

3 View the **Virus Properties** list, a checked box indicates that the selected virus has that property.

TIP For an explanation of each property, click the property with the right mouse button.

How Do I Update My Virus Signature File?

AntiVirus stores information about the various viruses for which it scans in a file called a signature file. Since new viruses appear every day, it is important to update your signature file on a regular basis.

To update your signature file, run the Update Wizard by clicking the Update button on the toolbar.

The Update Wizard will connect to Cheyenne Software via the Internet and load a new signature file onto your system. You may need to connect to your Internet service provider prior to starting the Update Wizard.

You can connect directly to Cheyenne Software for an update via the world wide web at:
www.cheyenne.com/desktop/sigpat.html

If you cannot update your signature file online, you can call Cheyenne Software at **1-800-521-8591** to order an update on a floppy disk.

File menu commands

The File menu offers the following commands:

Scan	Starts scanning the selected items
Scan Files	Allows you to select and scan individual files
Scan Bootsector	Allows you to manually start a boot sector scan
Exit	Exit InocuLAN AntiVirus

Scan command (File menu)

Start scanning the selected drives and/or directories.

Shortcut

Keys: CTRL+S

Scan Files command (File menu)

Select this menu option to open a dialog box that allows you to select an individual file for scanning.

Shortcut

Keys: CTRL+F

Scan Bootsectors command (File menu)

Start a scan of your drive's boot sector(s).

Shortcut

Keys: CTRL+B

Exit command (File menu)

End your InocuLAN AntiVirus session.

Shortcuts

Mouse:	click the application's control menu Exit button.
Keys:	ALT+F4

Tools menu commands

The Tools menu offers the following commands:

Online Update	Update the Virus Encyclopedia
Create Rescue Disk	Create a disk to be used to boot your system in case of virus problems.
Scan Scheduler	Starts the Schedule Wizard that allows you to schedule automatic virus scans.
Virus Encyclopedia	View the list of viruses scanned for
History Log	View a list of viruses detected in the past and the correction
Quarantine Viewer	Allows you to see files in the quarantine area
Visit our Web Site	Starts your Web browser and connects to the Cheyenne Software virus information page.
Options	Set operation preference for all aspects of the program.

Online Update command (Tools menu)

Connect to the Cheyenne Software web site and update the contents of the Virus Encyclopedia and virus signature files so that newly discovered viruses can be scanned for.
Shortcuts:

Mouse Click **Update** on the toolbar.

Create Rescue Disk command (Tools menu)

Creates a disk to be used to restore data on your drive that has been damaged by a virus.

Shortcuts:

Mouse	Click **Rescue** on the toolbar

Virus Encyclopedia command (Tools menu)

View the Virus Encyclopedia. The encyclopedia lists all the viruses that are known to the program and provides details as to the nature of each virus.

Shortcuts

Mouse: Click **Virus List** toolbar button.

Scan Scheduler command (Tools menu)

Starts the Schedule Wizard that allows you to schedule automatic virus scans. The Schedule Wizard leads you through the process of setting up one or more scans that run automatically and regularly at a specific day and time.

Shortcuts

Mouse: Click **Schedule** toolbar button.

Quarantine Viewer command (Tools menu)

Lets you view the files that have been moved into your quarantine area.

History Log command (Tools menu)

View a list of all viruses that have been detected in the past and the action taken as a result.

Shortcuts

Mouse: Click **History** toolbar button.

Visit our Web Site command (Tools menu)

Use this command to start your web browser and connect to the Cheyenne Software virus information page. If you do not have a permanent Internet connection, you must connect to the web before using this command.

Shortcuts

Mouse: Click **Internet** toolbar button.

Options command (Tools menu)

View the Options dialog to set or view all preferences and options regarding the program's operation.

Shortcuts

Mouse: Click the **Options** toolbar button.

View Menu commands

The View menu offers the following commands:

Toolbar	Shows or hides the toolbar.
Status Bar	Shows or hides the Status Bar.

Toolbar command (View menu)

Use this command to display and hide the Toolbar. A check mark appears next to the menu item when the Toolbar is displayed.

Toolbar

The toolbar is displayed across the top of the application window, below the menu bar. The toolbar provides quick mouse access to many tools used in InocuLAN AntiVirus.

To hide or display the Toolbar, choose **Toolbar** from the View menu (ALT, V, T).

Click To:

Connect to the world wide web to update your virus signature file

Start the Rescue Disk Wizard to create a clean boot disk

View Preferences and Options

View the Virus Encyclopedia

View the History Log

Start the Schedule Wizard to schedule scans

Start your Web browser and connect to Cheyenne's site

Status Bar command (View menu)

Use this command to display and hide the Status Bar. The Status Bar at the bottom of the application window describes the action to be executed by the selected menu item or depressed toolbar button, and keyboard latch state. A check mark appears next to the menu item when the Status Bar is displayed.

Help menu commands

The Help menu offers the following commands, which provide you assistance with this application:

Help Topics	Offers you an index to topics on which you can get help.
About	Displays the version number and copyright information for this application as well as the signature file information and the remaining number of free updates.

Help Topics command (Help menu)

Use this command to display the Help Contents screen. From the Contents you can jump to step-by-step instructions for using InocuLAN AntiVirus and various types of reference information.

Once you open Help, you can click the Contents button whenever you want to return to the Contents screen.

About command (Help menu)

Use this command to display the copyright notice and version number of your copy of InocuLAN AntiVirus as well as the signature file version number, and number of free updates remaining.

Context Help command

Use the Context Help command to obtain help on some portion of InocuLAN AntiVirus.

When you choose the Toolbar's Context Help button, the mouse pointer changes to an arrow and question mark. Then click somewhere in the window, such as another Toolbar button. The Help topic will be shown for the item you clicked.

Shortcut

Keys: SHIFT+F1

Schedule Wizard

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.

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 Scans dialog box opens with your selections displayed in the description area.
4. If satisfied with these selections, click the **New** pushbutton to start the Schedule Wizard. You can use the **Close** button to return to the Scanner screen to make other selections.

To schedule a scan on drives only:

1. Select the **Schedule** button  on the toolbar. The Schedule Scans dialog box opens.
2. Click the **New** push-button to start the Schedule Wizard where you can select the drive(s) you wish to scan.

Select Drives

Select one or more drives to schedule a scan for by checking the box ⊞ next to each drive in the list. Un-check the box to remove the drive from scanning. Click the **Next** push-button to continue on to the next wizard panel.

Scan When

Select how often you want the scheduled scan to occur by checking one of the radio buttons. If the **Daily** radio button is selected, the **Days** push-button is activated. You can select this push-button to go to a dialog box that allows you to exclude certain days of the week if you wish.

Enter the time at which you want the scheduled scan to start in the **Scan At** field, or accept the current time as the default.

Select the **Next** push-button to advance to the next wizard panel.

Days Dialog Box

Select which days you want the scheduled scan to run by checking the box next to the day of the week.

Scheduled Scan Options

Select one of the radio button to indicate your scanning options choice.

Use normal options but ALWAYS log as action

Selecting this button uses all your normally set scanning options, 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. Note, 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.

Scan Confirmation

This panel lists all the details of the scan you have scheduled. Review the entire contents of the window then click the **Finish** push-button to complete the process and enter the scan in the scheduler, or click the **Back** push-button to go back and make changes.

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.

Cleaning Wizard

The Cleaning Wizard appears when a virus is found during scanning. This first page lists the virus type and location and tells you if the file can be cleaned.

How would you like to handle this infection?

The default action is checked, but you can select the **Display All Options** radio button if you wish to choose another option. The default option that is displayed is determined by the settings 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.

Virus info

Select this push-button to display the Virus Encyclopedia information of the virus detected.

Continue Scanning check box

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.

Do this for all infected files check box

If you wish the selected action to be performed for all infected files found, then check the **Do this for all infected files** check box.

Skip File push-button

No action is taken for the file listed. The scan continues for more infected files.

All possible options

Clean

Attempts to clean the infected file.

Rename

Adds the extension .AVB to the filename.

Move

Moves the file to the quarantine area directory - \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.

Click the **Next** push-button to continue on to the next wizard panel.

All Options

The first panel of the wizard is re-displayed, now listing all available cleaning options. The available options are determined by the settings on the **Cleaning** page of the Options dialog.

Skip File push-button

No action is taken for the file listed. The scan continues for more infected files.

All possible options

Clean

Attempts to clean the infected file.

Rename

Adds the extension .AVB to the filename.

Move

Moves the file to the quarantine directory area - ...\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.

Click the **Next** push-button to continue on to the next wizard panel.

Rename Confirmation

The action you have selected is to rename the infected file. AntiVirus will rename infected files by giving them the extension .AVB. For example, VIRUS.EXE when renamed becomes VIRUS.EXE.AVB.

Do not show this page ever again check box

When checked, this page will not be displayed. If you wish to change an option, such as the quarantine folder, you will have to quit the Cleaning Wizard and make the change from the Options dialog.

Click the **Finish** push-button to complete the wizard operation for this file. The Cleaning Wizard then continues to scan for infected files.

Once the scan is complete, you are shown a list of all infections found and the actions taken.

Log Only Confirmation

The action you have selected is to only log the infected file. No other action is taken at this time.

Do not show this page ever again check box

When checked, this page will not be displayed. If you wish to change an option, such as the quarantine folder, you will have to quit the Cleaning Wizard and make the change from the Options dialog.

Click the **Finish** push-button to complete the wizard operation for this file. The Cleaning Wizard then continues to scan for infected files.

Once the scan is complete, you are shown a list of all infections found and the actions taken.

Move Confirmation

The action you have selected is to move the infected file to the Quarantine folder. AntiVirus will move the infected file to …\VIRUS directory located beneath the folder where you installed AntiVirus.

Do not show this page ever again check box

> When checked, this page will not be displayed. If you wish to change an option, such as the quarantine folder, you will have to quit the Cleaning Wizard and make the change from the Options dialog.

Click the **Finish** push-button to complete the wizard operation for this file. The Cleaning Wizard then continues to scan for infected files.

Once the scan is complete, you are shown a list of all infections found and the actions taken.

Never Scan Confirmation

The action you have selected is to skip the infected file and list it to never be scanned again. It is added to the exclusion list that can be viewed and edited on the **Exclusions** page of the Options dialog.

Do not show this page ever again check box

> When checked, this page will not be displayed. If you wish to change an option, such as the quarantine folder, you will have to quit the Cleaning Wizard and make the change from the Options dialog.

Click the **Finish** push-button to complete the wizard operation for this file. The Cleaning Wizard then continues to scan for infected files.

Once the scan is complete, you are shown a list of all infections found and the actions taken.

Remove from drive Confirmation

The action you have selected is to completely remove the infected file from your drive. This is done in a manner that prevents the activation or spread of the virus.

Do not show this page ever again check box

> When checked, this page will not be displayed. If you wish to change an option, such as the quarantine folder, you will have to quit the Cleaning Wizard and make the change from the Options dialog.

Click the **Finish** push-button to complete the wizard operation for this file. The Cleaning Wizard then continues to scan for infected files.

Once the scan is complete, you are shown a list of all infections found and the actions taken.

Clean Confirmation

The action you have selected is to attempt to clean the infected file. Also, the infected file is copied to your Quarantine folder.

Do not show this page ever again check box

When checked, this page will not be displayed. If you wish to change an option, such as the quarantine folder, you will have to quit the Cleaning Wizard and make the change from the Options dialog.

Click the **Finish** push-button to complete the wizard operation for this file. The Cleaning Wizard then continues to scan for infected files.

Once the scan is complete, you are shown a list of all infections found and the actions taken.

Fix Failed

The attempted fix action failed. Select another action.

Scan Complete

Once the scan is complete, you are shown a list of all infections found and the actions taken.
Select the **Done** push-button to close the wizard.

Add Extension dialog box

Use this dialog box to add another extension to the list of file types that are excluded from scanning.

Dialog Options

Extension

Type the new extension in the field or use the Browse push-button to select a file of the desired type.

File Extensions dialog box

Use this dialog to view and change the file extensions that are considered to be program files or compressed files (depending upon how you accessed this dialog box).

.EXE, .DLL, .COM, .DOC, .DOT, .OBD, .PPT, .WIZ, and .XLS are entered as Program file types by default.

.ARJ, .CAB, .EXE, .LHA, .LHZ, .MIM, .UU, .UUE, .and ZIP are entered as Compressed file types by default.

Dialog Options

Extensions list

List all file extensions that are currently defined as “program files” or “compressed files”, depending upon how you accessed this dialog box.

Close Push-button

Closes the dialog, any changes you have made are maintained.

Add Push-button

Displays the Add dialog box that allows you to add other file extensions to the list.

Remove Push-button

A file extension in the list must be selected to activate this button. Clicking this button removes the file extension from the list.

Cleaning Prompt Options dialog box

Use this dialog box to define the options that are available to you when you set AntiVirus to prompt you when it finds a virus.

Dialog Options

Use Custom Prompt

Check this box to activate the text entry field below it. In this field you can type custom text that will appear as an action available to you.

Available prompt actions

Check each action that you wish to have available to you when AntiVirus detects an infected file.

Curable files

Sets the default action to be taken when an infected file can be cleaned. The actions listed here will vary depending upon which items you have checked in the **Available prompt actions** area. This entry appears on the first screen of the Cleaning Wizard. The other actions are also available to you.

Non-curable files

Sets the default action to be taken when an infected file cannot be cleaned The actions listed here will vary depending upon which items you have checked in the **Available prompt actions** area.. This entry appears on the first screen of the Cleaning Wizard. The other actions are also available to you.

Quarantine Folder dialog box

The Quarantine folder should be excluded from the scan since you know that the files in this folder are infected.

Dialog Options

Disarm files moved to quarantine

When this option is checked, AntiVirus will prevent any file in the quarantine folder from executing and spreading viruses or damaging your system.

Quarantine Viewer dialog box

Use this dialog box to view a list of files that have been moved into the quarantine folder. The dialog shows the filename, virus type, original directory location, and if you have uploaded the virus to Cheyenne Software for further evaluation.

Select a file in the list and right-click on it to view a menu of actions.

Upload Quarantine files Wizard

The Upload Quarantine files Wizard guides you through the process of connecting to Cheyenne Software via the Internet to upload new or unidentified viruses.

If you have dial-up Internet access, you should connect to your service provider before moving to the next Wizard screen.

Quarantine Upload Summary

The file(s) you selected in the Quarantine files Viewer has been successfully uploaded to Cheyenne Software. Click **Finish** to return to the InocuLAN AntiVirus screen.

Add dialog box

Use this dialog box to add file types, folders, or specific files to a list.

Scan Boot Sectors dialog box

Use this dialog box to select one or more drives for a boot sector scan. Click the box next to the drive letter to select it. Click **Scan** to start the boot sector scan.

Scheduled Scans Dialog Box

Use this dialog box to start the Schedule Wizard to create a new scheduled scan, to view all the scheduled scans, to remove unwanted scans, and to modify previously defined scheduled scans.

Click **New** to create a new scheduled scan.

Select an existing scan and click **Modify** to change the settings for a scheduled scan you defined previously.

About InocuLAN AntiVirus dialog box

This dialog box lists the version number of the copy of InocuLAN AntiVirus that you are running. You can also access this dialog to determine the version number and date of your virus signature list.

View Scan Logs Dialog Box

Select either the History Log or Infection Log tab to view the contents of those files.

History Log Tab

The contents of this log depend upon your settings in the Logs tab of the Preferences dialog box. It can contain a list of all files scanned, or only summary information or just infected files found. The contents of this log can be purged using the Options/Logs dialog.

Infection Log Tab

This log list all infected files, the type of infection and the action taken as a result of finding the virus found during this session. The contents of this log can be purged using the Options/Logs dialog.

Last Scan Tab

Lists the results of the most recent scan.

Update Introduction

This is the introduction panel for the Update Wizard. This wizard attempts to dial your Internet service and connect to Cheyenne software. Once connected, it will check your AntiVirus files to make sure you have the latest changes and virus signatures.

You must have Internet access in order to use this wizard. If you do not have access, press the **Update options** push-button for other options for updating your software.

The Update Wizard will attempt to automatically dial your Internet service, but if unsuccessful, you need to manually connect to the Internet as you normally would, then re-start the Wizard.

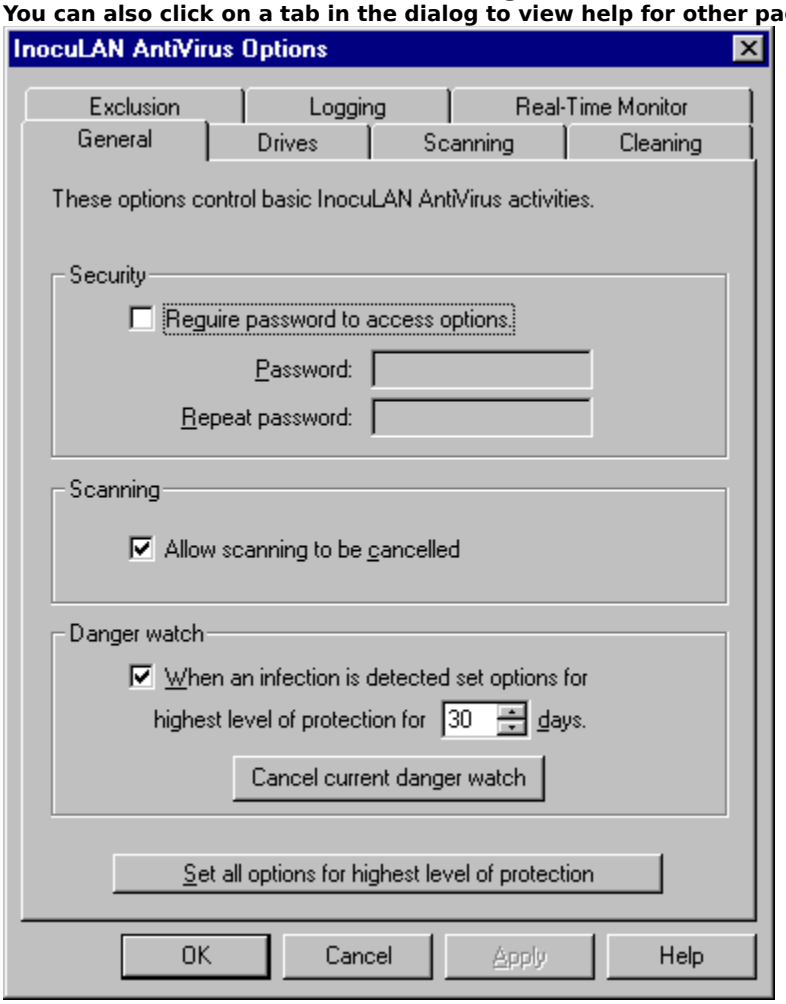
Danger Watch

Danger Watch is a function that automatically reacts once an infection is found on your system to change all AntiVirus settings to their highest level of protection. The Danger Watch will continue for a set number of days or you can manually cancel the watch.

The duration of the Danger watch is set on the General Tab of the options dialog box. You can also cancel the Danger Watch from this location.

General Tab

Click on one of the fields in the dialog below for detailed information.
You can also click on a tab in the dialog to view help for other pages.



Require password checkbox

Allows you to set password protection for your preference settings. To define or change a password, use the fields below.

Password field

Type a password to be used to protect your preference settings in this field. This field is only activated if the **Require Password** check box is checked.

Repeat password

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 canceled check box

Activates the **Stop Scan** push-button located in the bottom of the screen displayed during the scanning process.

When infection detected set to high level for specified number of days

When a virus is detected in your system, InocuLAN AntiVirus will go to its highest level of protection for the number of days specified.

Cancel Current Danger Watch

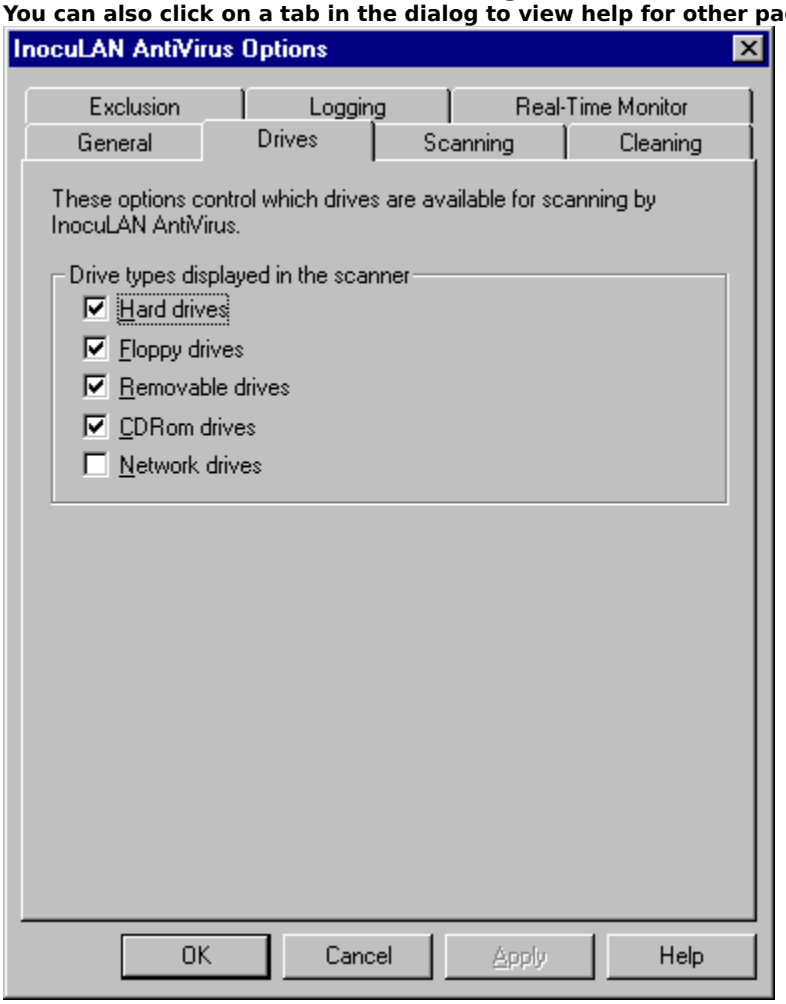
Select this push-button to cancel a danger watch that is currently active. This push-button is only active if there is currently a danger watch.

Set all options to highest level push-button

Immediately set all the preferences to reflect the highest possible level of AntiVirus protection.

Drives Tab

Click on one of the fields in the dialog below for detailed information.
You can also click on a tab in the dialog to view help for other pages.



Hard Drive

Displays all of your system's hard drives so they can be selected in the main scanning window.

Floppy drives

Displays all of your system's floppy drives so they can be selected in the main scanning window.

Removable drives

Displays all of your system's removable drives so they can be selected in the main scanning window. These drives would include Zip drives and SuperDisk.

CD-ROM Drives

Displays all of your system's CD-ROM drives so they can be selected in the main scanning window.

Network Drives

Displays all of the network drives to which you are connected so they can be selected in the main scanning window.

Hard drive

Automatically checks the box for each hard drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all hard drives are always scanned by default. You can always uncheck this box in the scanner screen.

Floppy drive

Automatically checks the box for each floppy drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all floppy drives are always scanned. Depending upon the settings above, floppy drives that do not have a disk inserted may not be displayed in the list.

Removable Drive

Automatically checks the box for each removable drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all removable drives are always scanned by default. Depending upon the settings above, removable drives that do not have media inserted may not be displayed in the list.

CD-ROM Drive

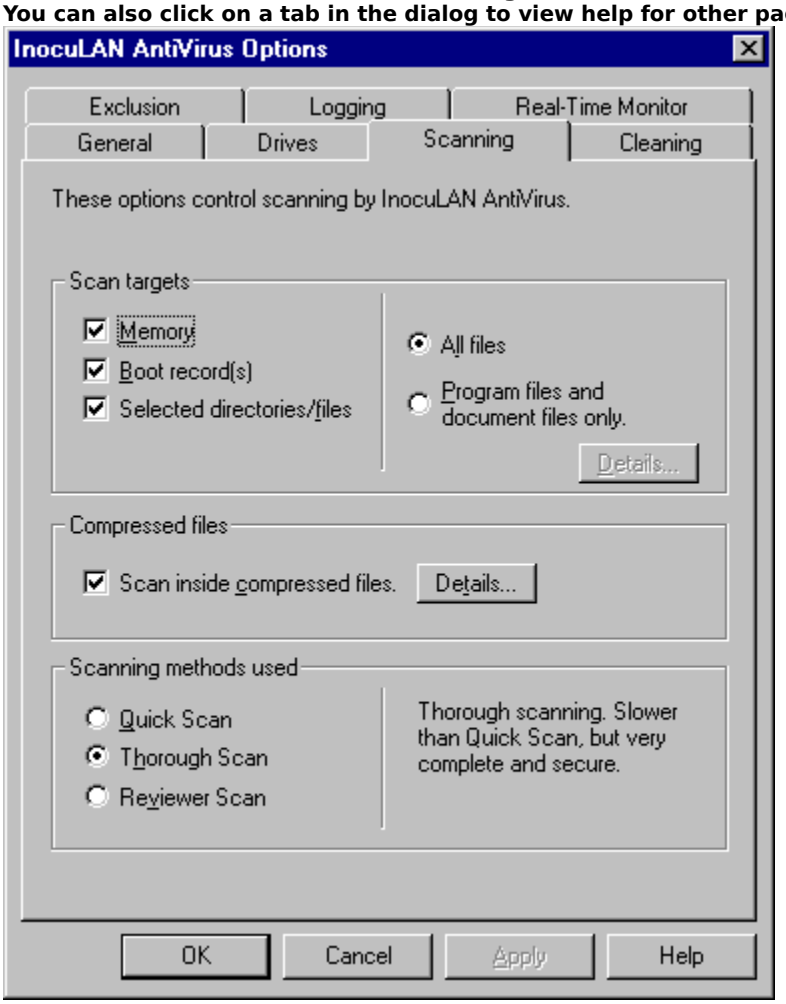
Automatically checks the box for each CD-ROM drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all CD-ROM drives are always scanned. Depending upon the settings above, CD-ROM drives that do not have a disk inserted may not be displayed in the list.

Network Drive

Automatically checks the box for each network drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all network drives are always scanned.

Scanning Tab

Click on one of the fields in the dialog below for detailed information.
You can also click on a tab in the dialog to view help for other pages.



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 Files

Scans the contents of individual directories and files that you checked in the list in the main scanning screen.

Scan All Files

Scans all the files in the targets selected in the Scan Targets list.

Scan Program Files

Scans only program and document files in the targets selected in the Scan targets list. By default, program files are defined as those files with .EXE, .COM, or .DLL extensions. By default, document files are those files with .DOC, .DOT, .OBD, .PPT, .WIZ, and .XLS extensions. Select the **Details** push-button to add other extensions or remove extensions.

Scan Inside Compressed Files

Sets the program to scan inside compressed files (such as .ZIP) for attached viruses.

Quick Scan

Adequate scanning for normal operation. Combines the best performance with reasonable security.

Thorough Scan

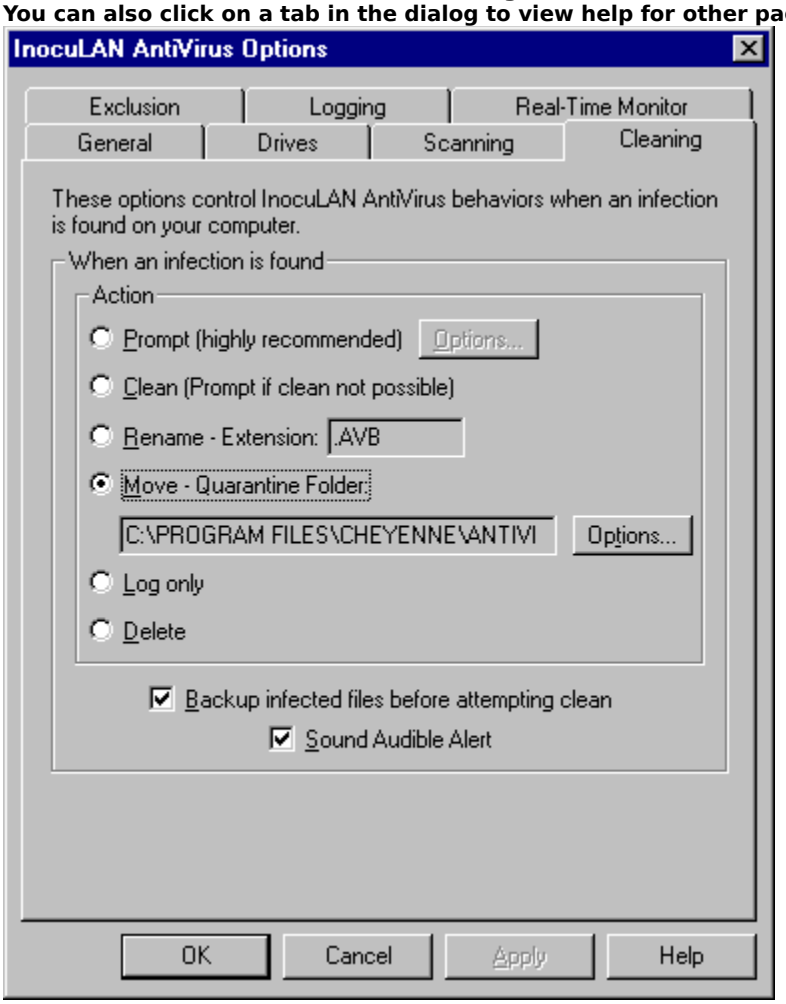
Slower than Quick Scan but performs a complete and secure scan.

Reviewer Scan

This scan method should be used for testing, verification, and review purposes. This method is slower than the Thorough Scan but does not provide any extra protection.

Cleaning Tab

Click on one of the fields in the dialog below for detailed information.
You can also click on a tab in the dialog to view help for other pages.



Prompt Action

When an infection is found on your system, InocuLAN AntiVirus will ask you what action to take.

Prompt Options Button

Lists all available prompt options; Clean, Log, Rename, Delete, Move, Exclude, and Virus Info. Also allows you to create and use a custom prompt.

Clean action

When an infection is found in your system, InocuLAN 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.

Rename Action

When an infection is found in your system, InocuLAN AntiVirus automatically renames the file using the original filename and the extension shown.

Move Action

When an infection is found in your system, InocuLAN AntiVirus automatically moves the file to the specified location. Press the **Options** pushbutton to set the Move options.

Options Pushbutton

Press this button to view the location to where infected files are moved when the Move action is selected. You can also set an option to automatically disarm (prevent from infecting) any file moved into this folder.

Log Only Action

When an infection is found in your system, InocuLAN AntiVirus automatically logs the file but does not perform any other action.

Delete Action

When an infection is found in your system, InocuLAN AntiVirus automatically deletes the file.

Backup Before Clean Check Box

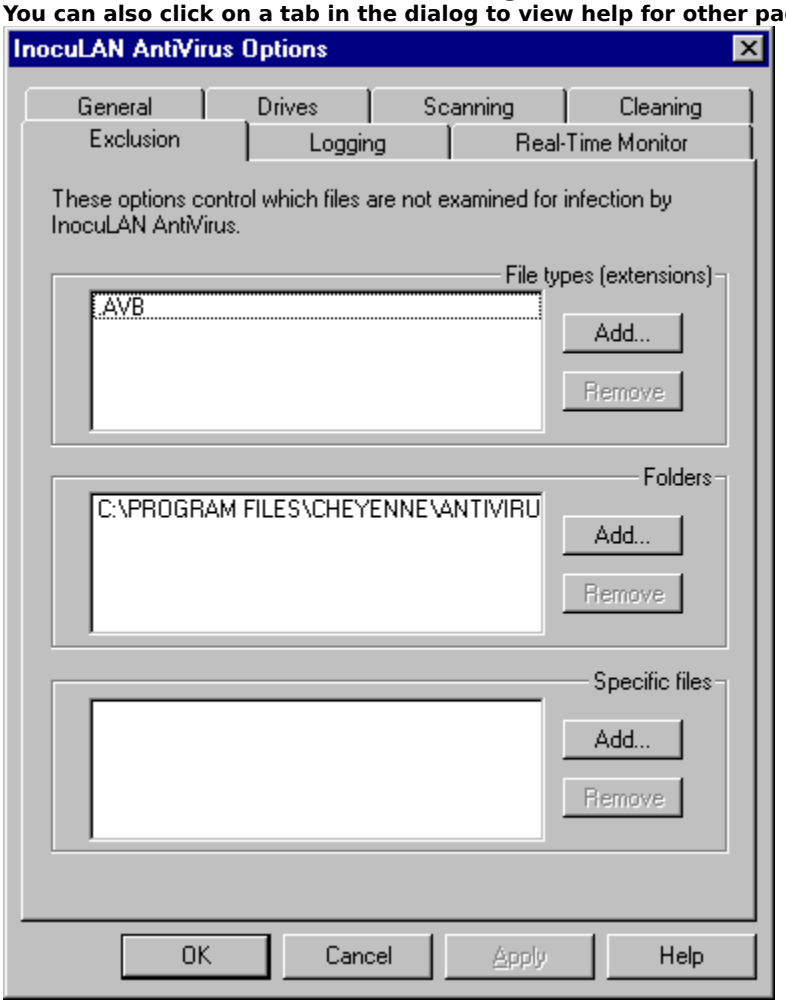
Any infected file is backed up before any file cleaning and restoration is attempted.

Sound Alert

An audible alert is sounded whenever an infection is discovered. Especially helpful if you have **Log Only** as the selected action.

Exclusion Tab

Click on one of the fields in the dialog below for detailed information.
You can also click on a tab in the dialog to view help for other pages.



Exclude File Type

Lists all the specific file extensions that are currently excluded from scanning. When an extension is on this list, any file that ends in that extension (for example .AVB) is never scanned. To add an extension to the list, or remove one from the list, use the push-buttons to the right.

Exclude Folders

Lists all the specific folders (directories) that are currently excluded from scanning. When a folder is on this list, any file that is contained in that folder is never scanned. To add a folder to the list, or remove one from the list, use the push-buttons to the right.

Exclude Specific Files

Lists all the specific files that are currently excluded from scanning. When a file is on this list, it is never scanned. To add a file to the list, or remove one from the list, use the pushbuttons to the right.

Add Push-button

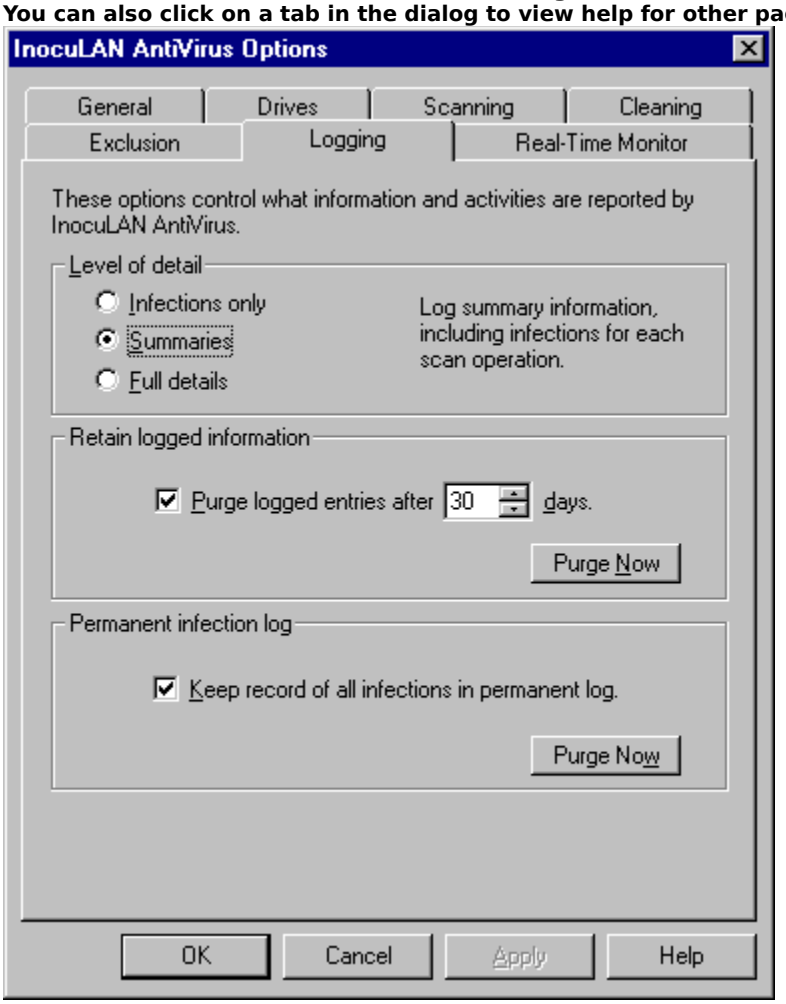
Displays a dialog box that allows you to add an item to the associated list.

Remove Push-button

Removes the selected items from the list. An item in the list must be highlighted to activate this push-button.

Logging Tab

Click on one of the fields in the dialog below for detailed information. You can also click on a tab in the dialog to view help for other pages.



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.

Purge logged entries after number of days

Automatically purges the contents of your log file 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 pushbutton

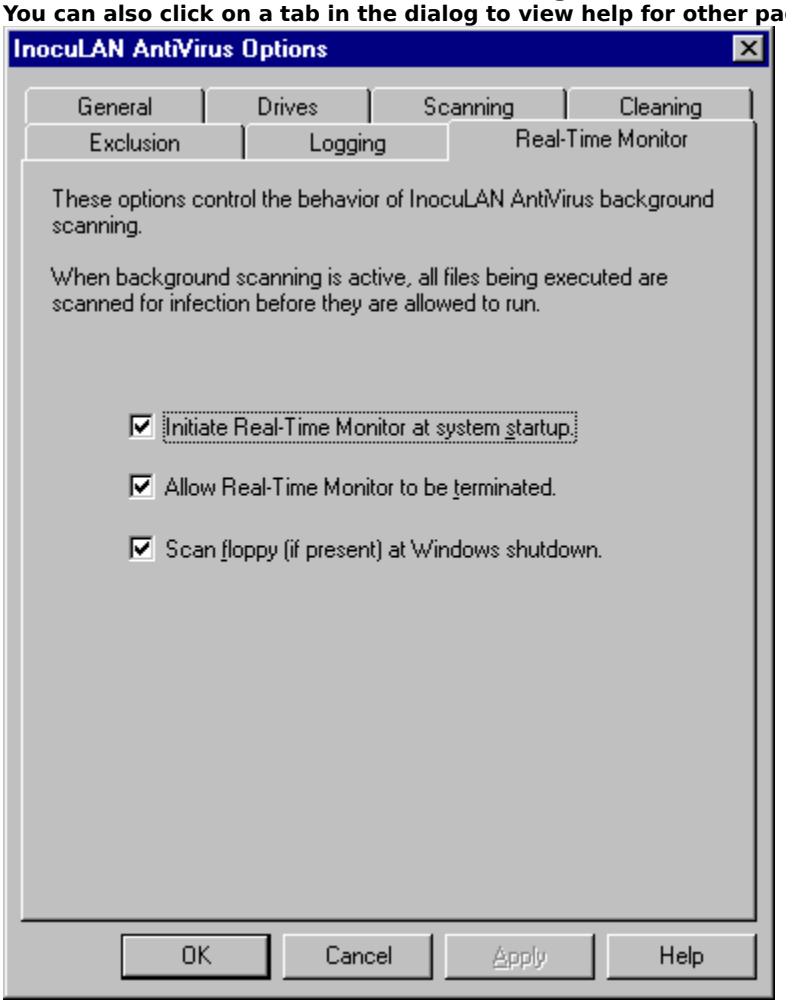
Immediately purges the contents of the log file.

Keep a record of all infections in permanent log.

Writes details of all infections detected by AntiVirus to the permanent History log file.

Real-Time Monitor Tab

Click on one of the fields in the dialog below for detailed information. You can also click on a tab in the dialog to view help for other pages.



Initiate Background Scan at Start-up

Starts InocuLAN AntiVirus when you start your system. Checks all internal memory and scans programs before they are allowed to run.

Allow background scan to be terminated

Allows you to stop background scanning while the scan is running.

Scan Floppy (if present) at Windows Shutdown

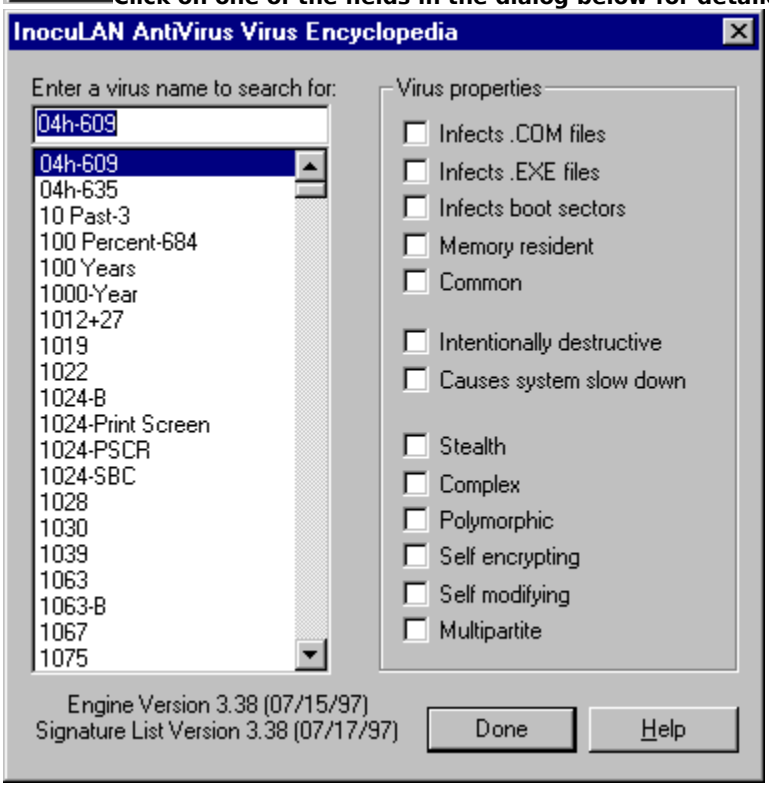
Select this option to set AntiVirus to automatically scan any floppy left in the drive when you shut down Windows. This prevents accidental infection from the floppy if you forget to remove it before you boot the computer next time.

Run Start-up Scan

Sets the program to automatically scan the items selected in the list in the main panel when you start your system.

Virus Encyclopedia Information

Click on one of the fields in the dialog below for detailed information.



Virus Name Field

Enter all or part of a virus name to select the virus in the list and view its properties. Virus properties are indicated by checks in the boxes to the right.

Infects .COM files

The selected virus infects .COM executable files.

Infects .EXE Files

The selected virus infects .EXE executable files.

Infects Boot Sector

The selected virus infects the boot sector on a diskette. The boot sector contains code to load the operating system files. Boot sector viruses can travel from a diskette to your hard drive then to every disk you read or write to.

Memory Resident

When a program containing the selected virus is executed, the virus may stay resident in memory and infect every program run.

Common

The selected virus is very common.

Intentionally Destructive

The selected virus does damage to your data or system by design.

Causes your system to slow down

The selected virus causes your system to slow down, in some cases considerably.

Stealth

The selected virus hides itself, so anti-virus products have a hard time detecting a decrease of memory or the increase in infected file sizes. They can avoid detection redirecting disk reads, and by altering data to hide the additional bytes of the virus. They may also redirect system pointers and information to infect a file without actually changing the infected program.

Complex

Indicates that the selected virus affects more than one area of the host program.

Polymorphic

The selected virus can mutate by changing its internal code so it appears different from one infection to another.

Self Encrypting

The selected virus uses encryption to evade detection. Encryption is a change made to data, code or a file so that it can no longer be read or accessed without processing or unencrypting.

Self Modifying

Software applications that change their executable program on their own. These programs usually change themselves to prevent virus infection, or to stop unauthorized copying. May cause a false detection. If so, add them to the list of excluded files.

Multipartite

The selected virus can infect both files and boot sectors.

Rescue Disk Format dialog

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. Use this options unless you are certain that the disk you are formatting has not been damaged.

About the Rescue Disk

This dialog box lists information about the machine the current Rescue Disk was created for, and the last time that it was modified.

Rescue Disk Wizard Help

This Wizard will guide you through the process of creating a rescue disk.

A rescue disk contains a back-up of critical system files and settings that are required to boot your system. Boot from the rescue disk if a virus is causing boot problems or installing itself in memory during the boot process. Booting with the rescue disk ensures a clean start-up without viruses in memory.

What would you like to do?

Create a new rescue disk

Selecting this option formats the disk in the floppy drive and then backs up the required system files and settings.

Update

Use this option when you already have a rescue disk and only need to update it due to changes to your system. You should update your rescue disk whenever you make hardware or setting changes to your system.

Verify and show information

Lists information about the machine the disk was created for and the last time that the disk was modified.

Press the **Next** push-button to continue.

Scan First?

AntiVirus gives you the option of scanning your system for infection before creating the Rescue Disk, or creating the disk without scanning first. If you have just installed AntiVirus and have not scanned you system, it is recommended that you let AntiVirus scan your system before creating the Rescue Disk.

Click **Next** to scan your system first.

Click **Skip** to create the Rescue Disk without scanning.

Insert Disk to be Formatted

Insert the disk you want to be formatted and made into a Rescue disk into your floppy drive. Make sure that the disk is not write-protected and that you do not have important information on the disk. The disk will be formatted and all data lost.

Insert Disk to be Updated

Insert the Rescue disk you created into the floppy drive. Make sure that the disk is not write-protected.

Insert Rescue Disk

Insert the Rescue disk you created into the floppy drive so AntiVirus can display the disk information.

Outdated Signature File

AntiVirus has determined that your virus signature file is out of date.

AntiVirus stores information about the various viruses for which it scans in a file called a Signature file. Since new viruses appear every day, it is important to update your signature file on a regular basis.

To update your signature file, run the Update Wizard by clicking the Update button on the toolbar.

Select the **Don't warn me again** checkbox to prevent this message from appearing.

Congratulations screen

You have successfully installed AntiVirus on your computer. Use this screen to select other actions you can perform now that AntiVirus is installed.

Select any or all of the check boxes:

Register InocuLAN AntiVirus

Allows you to register your copy of AntiVirus electronically.

Make sure that your signature files are up-to-date

Connects to Cheyenne Software via the Internet to see if virus signature file updates are available for download.

Scan your system and create a Rescue Disk

Starts the Rescue Disk Wizard that guides you through the process of making a Rescue Disk. This disk will contain backups of critical system settings and files and can be used to boot from in case of an emergency.

Options Settings

Select the Options button on the toolbar to display the Options Dialog box. Select one of the tabs along the top of the dialog box to set specific options.

General Tab

Require password checkbox

Allows you to set password protection for your preference settings. To define or change a password, use the fields below.

Password field

Type a password to be used to protect your preference settings in this field. This field is only activated if the **Require Password** check box is checked.

Repeat password

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 canceled check box

Activates the **Stop Scan** push-button located in the bottom of the screen displayed during the scanning process.

When infection detected set to high level for specified number of days

When a virus is detected in your system, InocuLAN AntiVirus will go to its highest level of protection for the number of days specified.

Cancel Current Danger Watch

Select this push-button to cancel a danger watch that is currently active. This push-button is only active if there is currently a danger watch.

Set all options to highest level push-button

Immediately set all the preferences to reflect the highest possible level of AntiVirus protection.

Drives Tab

Hard Drive

Displays all of your system's hard drives so they can be selected in the main scanning window.

Floppy drives

Displays all of your system's floppy drives so they can be selected in the main scanning window.

Removable drives

Displays all of your system's removable drives so they can be selected in the main scanning window. These drives would include Zip drives and tape drives.

CD-ROM Drives

Displays all of your system's CD-ROM drives so they can be selected in the main scanning window.

Network Drives

Displays all of the network drives to which you are connected so they can be selected in the main scanning window.

Hard drive

Automatically checks the box for each hard drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all hard drives are always scanned by default. You can always uncheck this box in the scanner screen.

Floppy drive

Automatically checks the box for each floppy drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all floppy drives are always scanned. Depending upon the settings above, floppy drives that do not have a disk inserted may not be displayed in the list.

Removable Drive

Automatically checks the box for each removable drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all removable drives are always scanned by default.

Depending upon the settings above, removable drives that do not have media inserted may not be displayed in the list.

CD-ROM Drive

Automatically checks the box for each CD-ROM drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all CD-ROM drives are always scanned. Depending upon the settings above, CD-ROM drives that do not have a disk inserted may not be displayed in the list.

Network Drive

Automatically checks the box for each network drive displayed in the list in the main scanning window. This sets the system so that the entire contents of all network drives are always scanned.

Scanning Tab

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 Files

Scans the contents of individual directories and files that you checked in the list in the main scanning screen.

Scan All Files

Scans all the files in the targets selected in the Scan Targets list.

Scan Program Files

Scans only program and document files in the targets selected in the Scan targets list. By default, program files are defined as those files with .EXE, .COM, or .DLL extensions. By default, document files are those files with .DOC, .DOT, .OBD, .PPT, .WIZ, and .XLS extensions. Select the **Details** push-button to add other extensions or remove extensions.

Scan Inside Compressed Files

Sets the program to scan inside compressed files (such as .ZIP) for attached viruses.

Quick Scan

Adequate scanning for normal operation. Combines the best performance with reasonable security.

Thorough Scan

Slower than Quick Scan but performs a complete and secure scan.

Reviewer Scan

This scan method should be used for testing, verification, and review purposes. This method is slower than the Thorough Scan but does not provide any extra protection.

Cleaning Tab

Prompt Action

When an infection is found on your system, InocuLAN AntiVirus will ask you what action to take.

Prompt Options Button

Lists all available prompt options; Clean, Log, Rename, Delete, Move, Exclude, and Virus Info. Also allows you to create and use a custom prompt.

Clean action

When an infection is found in your system, InocuLAN 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.

Rename Action

When an infection is found in your system, InocuLAN AntiVirus automatically renames the file using the original filename and the extension shown.

Move Action

When an infection is found in your system, InocuLAN AntiVirus automatically moves the file to the specified location. Press the **Options** pushbutton to set the Move options.

Options Pushbutton

Press this button to view the location to where infected files are moved when the Move action is selected.

You can also set an option to automatically disarm (prevent from infecting) any file moved into this folder.

Log Only Action

When an infection is found in your system, InocuLAN AntiVirus automatically logs the file but does not perform any other action.

Delete Action

When an infection is found in your system, InocuLAN AntiVirus automatically deletes the file.

Backup Before Clean Check Box

Any infected file is backed up before any file cleaning and restoration is attempted.

Sound Alert

An audible alert is sounded whenever an infection is discovered. Especially helpful if you have **Log Only** as the selected action.

Exclusion Tab

Exclude File Type

Lists all the specific file extensions that are currently excluded from scanning. When an extension is on this list, any file that ends in that extension (for example .AVB) is never scanned. To add an extension to the list, or remove one from the list, use the push-buttons to the right.

Exclude Folders

Lists all the specific folders (directories) that are currently excluded from scanning. When a folder is on this list, any file that is contained in that folder is never scanned. To add a folder to the list, or remove one from the list, use the push-buttons to the right.

Exclude Specific Files

Lists all the specific files that are currently excluded from scanning. When a file is on this list, it is never scanned. To add a file to the list, or remove one from the list, use the pushbuttons to the right.

Add Push-button

Displays a dialog box that allows you to add an item to the associated list.

Remove Push-button

Removes the selected items from the list. An item in the list must be highlighted to activate this push-button.

Logging Tab

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.

Purge logged entries after number of days

Automatically purges the contents of your log file 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 pushbutton

Immediately purges the contents of the log file.

Keep a record of all infections in permanent log.

Writes details of all infections detected by AntiVirus to the permanent History log file.

Real-Time Monitor Tab

Initiate Background Scan at Start-up

Starts InocuLAN AntiVirus when you start your system. Checks all internal memory and scans programs before they are allowed to run.

Allow background scan to be terminated

Allows you to stop background scanning while the scan is running.

Scan Floppy (if present) at Windows Shutdown

Select this option to set AntiVirus to automatically scan any floppy left in the drive when you shut down Windows. This prevents accidental infection from the floppy if you forget to remove it before you boot the computer next time.

Run Start-up Scan

Sets the program to automatically scan the items selected in the list in the main panel when you start your system.