



## **Options...**

Use the Options command to change settings for these categories:

**Scanner**

**Auto-Protect**

**Alerts**

**Activity Log**

**Exclusions List**

**Inoculation**

**Password**

**General**

You must select OK to exit the Options dialog box in order to save any changes made.

## **Categories**

Select a category name to see help for that category's settings.

**Scanner**

**Auto-Protect**

**Alerts**

**Activity Log**

**Exclusions List**

**Inoculation**

**Password**

**General**



## Problems Found/Details of Scan

When Norton AntiVirus finds a virus or inoculation issue, it shows you:

**Name:** Name of the infected or uninoculated file or boot record, or file or boot record whose inoculation data has changed.

**Virus:** Name of the virus.

**Status:** The status of the file or boot record.

If the Problems Found dialog box is displayed, you have the following options:

**Repair:** Repairs the file or boot record.

**Delete:** Deletes the file. Boot records cannot be deleted.

**Inoculate:** Inoculates or reinoculates the file.

**Exclude:** Adds the file to the exclusions list; it is excluded from future checks for known viruses or for inoculation activity.

**Info:** The Virus Information dialog box shows more details about the virus.

You should attempt to repair the infected file. If the infected file is a system file, such as COMMAND.COM, IO.SYS, MSDOS.SYS, IBMBIO.COM, or IBMDOS.COM you must restore it using the DOS SYS command. Refer to your DOS manual for instructions on using the SYS command.

For directions, see Chapter 3, "Taking Corrective Action," in the printed manual.

### See also:

---

[Removing Viruses from Files and Boot Records](#)

[Resolving Inoculation Issues](#)



## Alerts Settings Reference

[Categories](#)   [See Also](#)

Use these settings to configure the way Norton AntiVirus informs you and others of events. For directions, see [Customizing Alerts](#).

**Display Alert Message:** Tells Norton AntiVirus to add your text to its alert messages. You can enter up to 76 characters in the text box.

**Audible Alert:** Tells Norton AntiVirus to sound a tone when it detects a virus.

**Remove Alert Dialog After (X) Seconds:** Specifies the number of seconds (between 1 and 99) that a notification dialog stays on your screen.

### Alert Others

Use these settings to set network-specific options.

**Alert Network Users:** Messages from Norton AntiVirus are sent to other users on your network. Type the names of the users in the text box or select the browse button and select users from the list that appears.

**Network Console:** Messages from Norton AntiVirus are sent to the network server.

**Alert Norton AntiVirus NLM If Present:** Messages from Norton AntiVirus are sent to the Norton AntiVirus NetWare Loadable Module (NLM) if it is present on your network.

**Others... Button:** If you checked an option in the Alert Others group box, select this button. It opens the [Alert Others](#) dialog box, where you select the types of events to inform other network users about.

**NOTE:** You must reload automatic protection before it will recognize any of your new settings.

---

## Customizing Alerts



## Activity Log Settings Reference

[Categories](#)   [See Also](#)

Use these settings to determine what events Norton AntiVirus records in the activity log. For directions, see [Using the Activity Log](#).

### Log Following Events:

**Known Virus Detections:** Records known virus detections.

**Unknown Virus Detections:** Records unknown virus detections.

**Inoculation Activities:** Records detections of uninoculated files and files that have changed since they were inoculated.

**Virus-Like Activities:** Records virus-like activity detections.

**Completion of Scans:** Records end times of scans that you initiate.

**Virus List Changes:** Records deletions and updates that you make to the virus list.

**Limit Size of Log File to (amount) Kilobytes:** Sets size of the activity log file. When the file grows to the size you specify, Norton AntiVirus starts deleting the oldest entries as it adds new ones.

**Activity Log Filename:** Lets you type a path and filename for the activity log file. You can also select the browse button to go to the Log File dialog box to select an existing file or a path for a new file.

**NOTE:** You must reload automatic protection before it will recognize any of your new settings.

---

Using the Activity Log  
Activity Log Filter



## Activity Log Filter

You can filter the activity log to display any combination of the events listed here:

**Known Virus Detections:** Detections of viruses that Norton AntiVirus can identify by name.

**Unknown Virus Detections:** Detections of viruses for which Norton AntiVirus has no virus definition data.

**Inoculation Activities:** Detections of uninoculated files or changes in a file's inoculation data.

**Virus-Like Activities:** Detections of activities that Norton AntiVirus has determined to be the work of a possible unknown virus.

**Completion of Scans:** The dates, times, and durations of scans.

**Virus List Changes:** Any modifications to the virus database, with the date and time the change was made.

**Dated:** Entries for a date or range of dates. Used only in conjunction with one or more event types.

### See also:

---

[Using the Activity Log](#)





## Alert Others

Use these settings to determine what alerts to send to the network users you selected. For directions, see [Customizing Alerts](#).

### Alert others when the following events occur:

**Known Virus Detections:** Norton AntiVirus detects a virus that it can identify by name.

**Unknown Virus Detections:** Norton AntiVirus detects a virus for which it has no virus definition.

**Inoculation Activities:** Norton AntiVirus detects an uninoculated file or a change in a file's inoculation data.

**Virus-Like Activities:** Norton AntiVirus detects an activity that it perceives as the work of a possible unknown virus.

**Completion of Scans:** Informs others when a scan ends.

**Virus List Changes:** Informs others when any modifications are made to the virus list.

**Registration Activities:** Informs others of changes to registered files.

### See also:

---

[Alerts Settings Reference](#)



## Norton AntiVirus Main Window

If you have completed a full install as directed of Norton AntiVirus...

**YOU ARE ALREADY PROTECTED**

Every time you start up your computer, Norton AntiVirus will:

- ◆ Automatically scan the root directory on your hard drive and monitor all programs you run for viruses
- ◆ Inform you immediately if a virus is found

---

**From this main window you can do the following:**

- ◆ Select the **Scan Now** button to scan selected drives immediately. Norton AntiVirus will scan the drives you see selected in the drive list.
- ◆ Select a menu command to change settings or view information.

For more information, choose [QuickHelp](#) or [Contents](#) on the Help Menu.



## Exclusions List Settings Reference

[Categories](#)   [See Also](#)

An exclusion is a condition or activity that would normally be detected during a scan, but you have told Norton AntiVirus not to look for in a particular file.

Use the Exclusions List settings to view and change files you want excluded from selected Norton AntiVirus protection. You use the Add..., Edit..., and Delete buttons to make changes to the list. For more information, see [Modifying the Exclusions List](#).

Select a file in the **Items** group box to see what activities it is excluded from.

**Add...:** Define exclusions for a file, group of files using wildcards, or a directory.

**Edit...:** Change the exclusions for a selected file.

**Delete:** Remove a selected file and its exclusions from the exclusions list.

**NOTE 1:** Excluding files reduces your protection level. Use sparingly. Also be advised that renaming or moving a file invalidates its exclusions.

---

**NOTE 2:** You must reload automatic protection before it will recognize any of your new settings.

---

[Add/Edit Exclusion](#)

[Modifying the Exclusions List](#)

[Responding to Virus-Like Activity Alerts](#)

[Resolving Inoculation Issues](#)



## Add/Edit Exclusion

### Item...

Type the pathname for the file, directory, or group of files (using wildcards) in the text box or use the browse button to select a single file from a list.

**Include Subdirectories:** Also exclude files in the subdirectories of the item. Only applies if the item is a directory.

### Exclude From...

**Known Virus Detection:** Exclude the item from checks for known viruses.

**Unknown Virus Detection:** Exclude the item from checks for unknown viruses.

**Inoculation Detection:** Exclude the item from checks to see if it has been inoculated and for inoculation changes.

**Low-Level Format of Hard Disk:** Exclude the item from checks for attempts to perform a low-level format of your hard disk, which obliterates all information on the disk.

**Write to Hard Disk Boot Records:** Exclude the item from checks for attempts to write to the boot records on your hard disk. This action is performed legitimately by very few programs.

**Write to Floppy Disk Boot Records:** Exclude the item from checks for attempts to write to the boot record on a floppy disk. This action is performed legitimately by few programs.

**Write to Program Files:** Exclude the item from checks for attempts to write to a program file. Some programs save configuration information within themselves rather than in a separate file.

**Read-Only Attribute Change:** Exclude the item from checks for attempts to change a read-only file so that it can be written to.

### See also:

---

[Exclusions List Settings Reference](#)

[Modifying the Exclusions List](#)



## Select Exclude File

Select a file to exclude and select OK.

**File Name:** Type the path and filename if you know it; otherwise select the drive, directory, and file type from the other list boxes, then select the file from the list box.

**Drives:** The drive shown in the window is selected; to select a different drive, use the drop-down list box.

**Directories:** Select a directory.

**List Files of Type:** Select the type of file from the drop-down list box. All files of the selected type will appear in the File Name list box.



## General Settings Reference

[Categories](#)   [See Also](#)

Use these settings to configure general Norton AntiVirus activity.

**Backup File When Repairing:** Norton AntiVirus makes a copy of the infected file before repairing it.

Enter an extension to be used for the backup file (the default is .VIR). If you have more than one backup for the same file, the extension will be modified successively (that is, .VIR, .VI1, .VI2, and so on). You should delete all backup files when you know that the repair operation was successful. Be advised that all files with the backup extension will be added to the exclusions list and will not be checked for known viruses.

**Scan High Memory When Scanning Memory:** Norton AntiVirus scans the High Memory Area when scanning memory. Some viruses can be active in this area of memory.

**NOTE:** You must reload automatic protection before it will recognize any of your new settings.

---

## Customizing Scanner Options





## Password Settings Reference

[Categories](#)   [See Also](#)

Use these settings to define what features you want password-protected, and to set or change the password. For directions, see [Customizing Password Protection](#).

**Password Protect:** Activates the Set Password button so you can open the [Set Password dialog box](#) and set a password. Turning this off removes all password protection.

**Maximum Password Protection:** Sets password protection for all Norton AntiVirus features listed. You will not be able to access any of these features without the password.

**Custom Password Protection:** Sets password protection for the items you select in the list box. You will not be able to access any of these features without the password.

Customizing Password Protection  
Set/Change Password



## Set/Change Password

Before setting or changing your password, make sure you've selected the items you want protected. See [Customizing Password Protection](#) for instructions.

Passwords can be from 1 to 16 characters in length and are not case-sensitive ("a" is the same as "A").

**Old Password:** If this is the first time you've created a password, this text box is dimmed. If you're changing a password, type the old one here.

**New Password:** Type the new password in the text box. As you type, Norton AntiVirus replaces the characters in your password with asterisks (\*) on the screen for security.

**Confirm New Password:** Type the new password again in the text box. The features you selected are password protected the next time you start Norton AntiVirus.

### See also:

---

[Password Settings Reference](#)



## Inoculation Settings Reference

[Categories](#)   [See Also](#)

Use these settings to change inoculation activity. You can inoculate the boot records and system files on your hard disk and any program file. Norton AntiVirus uses the [program file extensions](#) list to determine if a file is a program file. For directions, see [Customizing Inoculation](#). For more information, select the See Also button at the top of this window.

**Inoculate Boot Records and System Files:** Causes Norton AntiVirus to inoculate the master boot record, boot records, and system files on your hard disk during the next scan you perform. This information is checked on every scan.

**Inoculate Program Files:** Causes Norton AntiVirus to inoculate all program files on hard disks and network drives.

**Inoculate Files on Floppies:** Causes Norton AntiVirus to also inoculate all program files on floppy disks.

### How to Respond...

#### When an Item has not been Inoculated:

Select one of these options from the drop-down list box:

**Prompt:** Informs you when it finds an uninoculated program file or boot record and allows you to choose how to respond.

**Inoculate Automatically:** Inoculates each uninoculated program file and boot record as soon as it is detected.

**Notify Only - Don't Inoculate:** Informs you but takes no action when it encounters an uninoculated program file or boot record.

**Deny Access:** Informs you that a program file is not inoculated and prevents you from using that file. This option does not apply to boot records.

#### When an Inoculated Item has Changed:

Select one of these options from the drop-down list box:

**Prompt:** Informs you when it finds a program file or boot record that has changed and allows you to choose how to respond.

**Notify Only - Don't Inoculate:** Informs you but takes no action when it encounters a changed file or boot record.

**Deny Access:** Informs you that a program file has changed and prevents you from using that file. This option does not apply to boot records.

#### Buttons to Display if Prompted:

Select the buttons you want to appear when an inoculation issue is found:

**Repair:** Allows you to repair a file or boot record with an inoculation change.

**Delete:** Allows you to delete a file with an inoculation change. Boot records cannot be deleted.

**Inoculate:** Allows you to inoculate or reinoculate the file or boot record.

**Continue:** Allows you to continue scanning or accessing the file with no change to its inoculation data.

**Stop:** Allows you to stop scanning or accessing the file with no change to its inoculation data.

**Exclude:** Allows you to exclude the file from future inoculation checks.

**Inoculation Path:** Type a directory for the inoculation file.

When you inoculate program files and boot records, an inoculation file is placed in the specified location on each drive you inoculate.

**NOTE:** You must reload automatic protection before it will recognize any of your new settings.

---

Customizing Inoculation  
Inoculating Files  
Monitoring for Unknown Viruses



## Auto-Protect Settings Reference

[Categories](#)   [See Also](#)

Use these settings to automate protection. For directions, see [Customizing Automatic Protection](#) or select the See Also button at the top of this window.

### Scan a File When:

**Run:** Scans a program file each time you run it.

**Opened:** Scans files whenever they are opened, such as when you copy a file.

**Created:** Scans files when they are created on your drive by an installation program, by compressing or uncompressing a file, or by some other means.

### What to Scan:

**All Files:** Scans all files you access. This includes files less likely to contain viruses.

**Program Files Only:** Scans files with the extensions contained in the program file extensions list. These are the files most likely to be infected.

**Program Files button:** Takes you to the [program file extensions](#) list, where you can see, add, or delete file extensions.

### When a Virus is Found:

**Prompt:** Informs you when a known virus is found and allows you to choose how to respond.

**Deny Access:** Prevents you from using a file when a known virus is detected.

**Repair Automatically:** Repairs an infected file or boot record without notifying you. The outcome of the repair is recorded in the activity log.

Note that, by default, Norton AntiVirus makes backup copies of files before they are repaired. See [General Settings](#) for more information.

**Delete Automatically:** Deletes an infected file as soon as a known virus is detected. The name of the deleted file is recorded in the activity log.

**Halt Computer:** Halts your computer when a known virus is detected. You must then restart your computer.

### Buttons to Display if Prompted:

**Repair:** Allows you to repair the file.

**Delete:** Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is dimmed.

**Continue:** Allows you to continue accessing the file. If you select the Continue button when a virus is found, you may activate the virus.

**Stop:** Allows you to stop accessing the file. The virus will not be activated, but the file will still be infected.

**Exclude:** Allows you to exclude the file from being checked for known viruses. (Use sparingly!)

### Other Settings:

**Advanced:** See [Auto-Protect Advanced Settings](#)

**Startup:** See [Auto-Protect Startup Settings](#)

**Sensor:** See [Auto-Protect Virus Sensor Settings](#)

**NOTE:** You must reload automatic protection before it will recognize any of your new settings.

---

[Customizing Automatic Protection](#)

[Monitoring the Files You Use](#)

[Monitoring During Startup](#)

[Monitoring for Virus-Like Activities](#)

[Setting Up Automatic Protection](#)

[Monitoring for Unknown Viruses](#)



## Auto-Protect Advanced Settings

Use these settings to have Norton AntiVirus check for virus-like activities and scan floppy disks for boot viruses before using them. For directions, see [Monitoring for Virus-Like Activities](#) and [Monitoring Floppy Disks](#).

### Virus-Like Activity Monitors

These settings determine what Norton AntiVirus does when it detects each virus-like activity.

For each activity, your choices are:

**Prompt:** Informs you when a program tries to perform the activity and allows you to decide whether the activity should continue, stop, or be excluded for the program. This choice provides you with the best combination of flexibility and protection.

**Allow:** Allows the activity to continue every time without informing you. Selecting Allow offers you no protection against an unknown virus performing that activity.

**Don't Allow:** Prevents the activity from occurring every time it is detected. This selection provides the greatest protection, but can impede your work.

### Virus-Like Activities:

**Low-Level Format of Hard Disk:** A low-level format of your hard disk obliterates all information on the disk, and it cannot be recovered. This type of format is generally performed at the factory only. Detection of this activity almost certainly indicates an unknown virus at work.

**Write to Hard Disk Boot Records:** Your hard disk boot records should be written to only by very few programs. Detection of this activity often indicates an unknown virus at work.

**Write to Floppy Disk Boot Records:** Floppy disk boot records should only be written to by few programs. Detection of this activity can indicate an unknown virus at work.

**Write to Program Files:** Program files are written to by programs that save configuration information within themselves rather than in a separate file. This activity occurs legitimately more often than the preceding activities, although it can also indicate the presence of a virus.

**Read Only Attribute Change:** Many programs change a file's read-only attribute, so this activity is least likely to indicate a virus at work. Some viruses, however, will change this attribute, so they can write their viral code to the file.

### Check Floppies:

Boot viruses are most likely to spread through floppy disks, so it's important to check every floppy disk you use. Use these settings to ensure maximum safety automatically.

**Check Floppies for Boot Viruses Upon Access:** Checks for boot viruses on each floppy disk you access.

**Check Floppies when Rebooting Computer:** Checks a floppy disk in drive A: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del.

**When Rebooting, Check Both Drives (A and B):** Also checks a floppy disk in drive B: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del. Check this option if you have a system that can boot from a disk in your B: drive.

**CAUTION:** These last two options do NOT offer protection when you restart your computer using the power switch or Reset button.

### See also:

---

[Monitoring the Files You Use](#)

[Monitoring During Startup](#)

[Monitoring for Virus-Like Activities](#)

[Setting Up Automatic Protection](#)

[Customizing Auto-Protect Options](#)

[Auto-Protect Settings Reference](#)

[Monitoring for Unknown Viruses](#)







## Auto-Protect Startup Settings

Use these settings to define what automatic protection does when you start up your computer. For directions, see [Monitoring During Startup](#).

**What to Scan Upon Startup** (We recommend that you check all of these items.)

**Memory:** Scans for any viruses resident in your computer's memory. A virus found at this point would indicate an infection in one or more programs run prior to the time that the automatic protection feature is loaded.

**Master Boot Record:** Scans for boot viruses in the master boot record.

**Boot Records:** Scans for boot viruses in the boot records on your hard disk.

### Types of Memory to Use

Specify what types of memory you want automatic protection to run in. If you are not sure what types of memory you have, check all three options. Norton AntiVirus will determine what types you have and what type to use at a given time.

**High Memory Area (HMA)**

**Upper Memory Blocks (UMBs)**

**Expanded Memory (EMS)**

If you have a type of memory that you don't want Norton AntiVirus to use, leave the option unchecked.

### Bypass Keys

This specifies the keystroke combination you want to use to prevent automatic protection for DOS from loading at startup. The options are: **None**, **Both Shift Keys**, **Both Alt Keys**, **Both Ctrl Keys**.

If you do **not** want to allow the automatic protection feature to be bypassed, select None.

**WARNING:** If you are using MS-DOS 6.0, do not select the Both Shift Keys option. It will cause both the CONFIG.SYS and AUTOEXEC.BAT files to be bypassed completely.

---

**TIP:** To bypass the automatic protection feature, press and hold both of the specified keys during the entire boot process.

---

Check **Auto-Protect Can Be Unloaded** to make the automatic protection feature unloadable, for example, if you need to run programs that might conflict with Norton AntiVirus. To be unloaded, the automatic protection TSR (terminate-and-stay-resident program) must be the last TSR loaded. For information on how to unload the TSR, see Chapter 7, "Customizing Automatic Protection," in the printed manual.

Check **Hide Icon In Windows** if you don't want the Norton AntiVirus Auto-Protect icon displayed on your Windows desktop.

### See also:

[Monitoring During Startup](#)

[Auto-Protect Settings Reference](#)



## Scanner Settings Reference

[Categories](#)    [See Also](#)

Use these settings to customize the way Norton AntiVirus scans for viruses when you initiate scans. For directions, see [Customizing Scanner Options](#) or select the See Also button at the top of this window.

**What to Scan...**(We recommend you check all of the first three items: Memory, Master Boot Record, and Boot Records.)

**Memory:** Checks for viruses resident in your computer's memory before any files are scanned. If a virus is in memory while you are scanning, every file scanned can become infected.

**Master Boot Record:** Checks for boot viruses in the master boot record of your hard disk.

**Boot Records:** Checks for boot viruses in the boot records on your hard disk and on any floppy disk that you scan.

**All Files:** Scans all files on your disk. This includes files that are less likely to contain viruses.

**Program Files Only:** Scans files with the extensions contained in the program file extensions list. These are the files most likely to become infected.

**Program Files button:** Takes you to the [program file extensions](#) list, where you can see, add, or delete file extensions.

**Within Compressed Files:** Scans files compressed using the PKZIP utility.

### When a Virus is Found:

**Prompt:** Informs you when a virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.

**Notify Only:** Informs you when a virus is found, but does not allow you to repair or delete the infected file.

**Repair Automatically:** Repairs an infected file or boot record as soon as a virus is detected. You are informed of the results at the end of the scan.

**Delete Automatically:** Deletes an infected file as soon as a virus is detected. You are informed of the deletion at the end of the scan.

**Halt Computer:** Halts your computer when a virus is detected. You must then restart your computer.

### Buttons to Display if Prompted:

If you select the Prompt setting above, you can select from these options in the group box:

**Repair:** Allows you to repair the file or boot record. If the virus infects an item that cannot be repaired, such as a compressed file, the button is dimmed.

**Delete:** Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is dimmed.

**Continue:** Allows you to continue scanning without resolving the problem. (This button only appears if you use the Immediate Notification option.)

**Exclude:** Allows you to exclude the file from being checked for known viruses. (Use sparingly!)

**Advanced... button:** This contains more options, including network scanning, immediate notification when a virus is found, and drive preselection. For additional information see [Scanner Advanced Settings](#).

[Customizing Scanner Options](#)  
[Customizing Automatic Protection](#)  
[Scanning Drives](#)  
[Scanner Advanced Settings](#)  
[Program File Extensions](#)



## Scanner Advanced Settings

Use these settings to further customize the way Norton AntiVirus scans for viruses when you initiate scans. For directions, see [Customizing Scanner Options](#)

### Advanced Settings...

**Allow Network Scanning:** Allows Norton AntiVirus to scan entire network drives. (This can be very time-consuming.)

**Allow Scanning To Be Stopped:** Enables the Stop button in the Scan Progress dialog box, allowing you to stop a scan in progress.

**Immediate Notification:** Displays an alert box whenever a problem is detected while scanning. This allows you to respond immediately, without waiting until the scan is completed.

### Preselect at Start...

**All Floppy Drives:** All floppy drives are automatically selected to be scanned when you start Norton AntiVirus.

**All Hard Drives:** All hard drives are automatically selected to be scanned when you start Norton AntiVirus.

**All Network Drives:** All network drives automatically selected to be scanned when you start Norton AntiVirus. (You must have checked Allow Network Scanning before you can scan network drives. Your network access privileges will affect the drives on which you may repair and delete files.)



## Activity Log

For directions on how to use the Activity Log, see [Using the Activity Log](#).

Use the activity log to view a record of Norton AntiVirus activities. Which activities are recorded is specified in the Options - Activity Log Settings dialog box. These include:

- ◆ A record of known and unknown virus and virus-like activity detections.
- ◆ A list of files that have changed since they were inoculated or have not been inoculated.
- ◆ The end times of scans that you initiate.
- ◆ A record of when you make changes to the virus list.

You can print the entries displayed in the log, filter the entries to display only those of interest, and clear the log to remove all entries.

**Print...:** Outputs the entries to a printer or to a file whose name and path you can specify.

**Filter...:** Allows you to filter the activity log to display specific categories of entries. See [Activity Log Filter](#) for choices.

**Clear...:** Deletes all entries in the activity log.

### See also:

---

[Activity Log Settings Reference](#)



## Clear Activity Log

Select **Yes** to erase everything in the activity log. Otherwise, the log expands indefinitely or until it reaches the maximum size you've set in the Activity Log Settings.

### See also:

---

[Using the Activity Log](#)



## Activity Log File Name

Select an activity log file and select OK.

**File Name:** Type the path and filename if you know it; otherwise select the drive, directory, and file type from the other list boxes, then select the file from the list box.

**Drives:** The drive shown in the window is selected; to select a different drive, use the drop-down list box.

**Directories:** Select a directory.

**List Files of Type:** Select the type of file in the drop-down list box. All files of the selected type will appear in the File Name list box.





## Infection Log

For directions on how to use the infection log, see [Using the Infection Log](#).

Use the infection log to view a record of known and unknown virus detections. You can:

- ◆ See which files were infected.
- ◆ See what action was taken to correct the problem.
- ◆ Print a report to a printer or to a file, or send it to another user via electronic mail.

Select **Filter...** to filter the entries. See [Infection Log Filter](#) for your options.

Select **Print...** to print the log entries.



## Infection Log Filter

The infection log contains the activity log entries for detections of known and unknown viruses. You can filter these entries to display only information about a specific activity or activities detected on certain dates.

You can filter the activity log to display any combination of the events listed here.

**Known Virus Detections:** Detections of viruses that Norton AntiVirus can identify by name.

**Unknown Virus Detections:** Detections of viruses for which Norton AntiVirus has no virus definition data.

**Dated:** Entries for a date or range of dates. This is used only in conjunction with one or more event types.

### **See also:**

---

[Using the Infection Log](#)



## Virus List

Use the virus list to view, print, or delete virus information. For directions, see [Viewing the Virus List](#).

**Display:** Lets you select what viruses to view: all viruses, common viruses, [program viruses](#), [boot viruses](#), [stealth viruses](#), [polymorphic viruses](#), or [multipartite viruses](#).

**Virus list box:** Shows a list of virus names and what kind of files (programs, boot records, or both) the virus infects.

**Info...:** Displays detailed information about a selected virus.

**Print...:** Outputs the virus list to a printer or file.

**Delete:** Allows you to delete a virus and its definition from the virus list.

### See also:

---

[Viewing the Virus List](#)



## Delete Virus Definition

**WARNING:** Do not delete a virus definition unless you are sure you don't need it. Once a virus definition is deleted, files and boot records are no longer protected from that virus.

---

If you delete a selected virus definition, it is marked as deleted in the virus list box. The next time you access the virus list, that virus will not appear.

**NOTE:** You must reload automatic protection before it will recognize changes to the virus list.

---

For directions, see [Viewing the Virus List](#).



## Virus Information

The Virus Information dialog box gives detailed information about the virus you selected in the virus list box. Use the arrow buttons to page forward or back to the next or previous virus in the list box. For directions, see [Viewing the Virus List](#).

**Virus Name and Aliases:** The most common names by which the virus is known.

**Infects:** What files or boot records the virus attacks.

**Likelihood:** Options are: Common and Rare.

**Length:** Length, in bytes, of the virus code.

### Characteristics:

**Memory Resident:** Stays in memory after it activates.

**Size Stealth:** Tries to conceal itself from detection by disguising its size.

**Full Stealth:** Tries to conceal itself from detection by disguising its size and attributes.

**Triggered Event:** Performs some action based on certain criteria (for example a date on the computer's system clock).

**Encrypting:** Encrypts its code to make detection more difficult.

**Polymorphic:** Appears differently in each infected file.

**Comments:** Further description of the selected virus's characteristics.



## Inoculation

Use this dialog box to inoculate or uninoculate specified program files. For directions, see [Inoculating Files](#).

### Settings:

**Inoculate Item:** Designates that any item specified is to be inoculated.

**Uninoculate Item:** Designates that any item specified is to be uninoculated.

**Item:** Specifies what item (drive, directory, group of files, or file) is to be inoculated or uninoculated. You can use a wildcard to specify a group of files. You can also use the browse button to select a single file.

**Include Subdirectories:** Designates that any program files in subdirectories of a directory are also to be inoculated or uninoculated. Applies only if the item is a directory.

### Why inoculate?

Inoculation is a form of prevention against unknown viruses. When a file or boot record has been inoculated, it is checked against its inoculation data each time it is scanned if the Inoculate Program Files option or Inoculate Boot Records and Systems Files option has been selected in the Options - Inoculation Settings dialog box. Changes in inoculation data can indicate the presence of an unknown virus.

### What causes an inoculation change?

An inoculation change could occur for the following reasons:

- ◆ A change to the file for legitimate purposes. For example, you may have installed a new version of the software and forgotten to inoculate the new program file.
- ◆ An unknown virus that is not in the definitions file -- either because Norton AntiVirus doesn't have a definition for it or you don't have the most recent definitions.

### Why uninoculate?

If you are removing a program from your drive or no longer want to use inoculation, you should uninoculate files to remove the inoculation data and free up space on your disk.

### See also:

---

[Inoculating Files](#)

[Customizing Inoculation](#)

[Monitoring for Unknown Viruses.](#)



## Select File to Inoculate

Select a file to inoculate and select OK.

**File Name:** Type the path and filename if you know it; otherwise select the drive, directory, and file type from the other list boxes, then select the file from the list box.

**Drives:** The drive shown in the window is selected; to select a different drive, use the drop-down list box.

**Directories:** Select a directory on the selected drive.

**List Files of Type:** Select the type of file from the drop-down list box. All files in the directory of the selected type will appear in the File Name list box.



## Program File Extensions

Program files are the files most likely to become infected and spread viruses. When you configure Norton AntiVirus to scan program files only, it looks at the program file extensions list and scans only files with extensions in the list.

Use the Program File Extensions dialog box to add new extensions, to delete extensions, and to reset the extensions to the original list installed with Norton AntiVirus. The list contains the most common extensions for executable files. A file must be executable for a virus to spread from it.

**Add...:** Allows you to add an extension (you'll be prompted to type the extension's letters).

**Delete:** Deletes the extension you've selected in the list.

**Default:** Resets the extensions to the original list installed with Norton AntiVirus.

### **See also:**

---

[Add Program File Extension](#)





## **Add Program File Extension**

Type a new extension in the **Extension to Add** text box (up to three characters). You may use wildcards in the extension, but not to represent all three characters.

This new extension is added to the program file extensions list, and Norton AntiVirus will treat any files with this extension as program files when it scans for viruses and inoculates.



## Printing

In most cases Norton AntiVirus can print information to a printer or to a file.

**Print to Printer:** Sends the information to a printer.

**Print to File:** Outputs the information to a text file. Type the pathname for the file or use the browse button to select a path or to overwrite an existing file.

**Mail to User:** (Optional) Allows you to send the information to another person using your electronic mail system. This option only appears if your mail system supports this feature, such as Microsoft Mail or cc:Mail for Windows, version 2.0 or above.



## **Overwrite or Append**

You are about to overwrite an existing file with the file you're printing to disk.

Select **Overwrite** to replace the old file.

Select **Append** to add information to the existing file.

Select **Cancel** to go back and change the filename.



## **Print to File**

### **To locate a specific file:**

- 1** Select a drive in the Drives list box. The Directories and Files list boxes change to reflect your selection.
- 2** Select a directory in the Directories list box. The Files list box changes to reflect your selection.
- 3** Select a file from the Files list box.
- 4** Click OK.  
Or,  
Type the path and filename in the File Name box.



## Virus Found Information

When Norton AntiVirus finds a virus, you can display information about the infection.

**File Name:** The name of the infected file and its path.

**Status:** Whether it is infected, repaired, or deleted.

**Virus Name and Aliases:** The most common names by which the virus is known.

**Infects:** What files or boot records the virus attacks.

**Likelihood:** Options are: Common and Rare.

**Length:** Length, in bytes, of the virus code.

### Characteristics:

**Memory Resident:** Stays in memory after it activates.

**Size Stealth:** Tries to conceal itself from detection by disguising its size.

**Full Stealth:** Tries to conceal itself from detection by disguising its size and attributes.

**Triggered Event:** Performs some action based on certain criteria (for example a date on the computer's system clock).

**Encrypting:** Encrypts its code to make detection more difficult.

**Polymorphic:** Appears differently in each infected file.

**Comments:** Further description of the selected virus's characteristics.

### See also:

---

[Removing Viruses from Memory](#)

[Removing Viruses from Files and Boot Records](#)



## Virus Information

**Virus Name and Aliases:** The most common names by which the virus is known.

**Infects:** What files or boot records the virus attacks.

**Likelihood:** Options are: Common and Rare.

**Length:** Length, in bytes, of the virus code.

### Characteristics:

**Memory Resident:** Stays in memory after it activates.

**Size Stealth:** Tries to conceal itself from detection by disguising its size.

**Full Stealth:** Tries to conceal itself from detection by disguising its size and attributes.

**Triggered Event:** Performs some action based on certain criteria (for example a date on the computer's system clock).

**Encrypting:** Encrypts its code to make detection more difficult.

**Polymorphic:** Appears differently in each infected file.

**Comments:** Further description of the selected virus's characteristics.



## Repair/Delete/Inoculate File

**Repair:** Repairing a file or boot record removes the virus and/or returns the file to its original state. Select **Repair All** to have Norton AntiVirus repair all the infected files found during the scan.

**Delete:** Files deleted by Norton AntiVirus cannot be recovered. After you have deleted the file, you can replace it with an uninfected copy. Select **Delete All** to have Norton AntiVirus delete all the infected files found during the scan.

**Inoculate:** Files will be inoculated or reinoculated depending on the issue. Select **Inoculate All** to have Norton AntiVirus inoculate all the files found to have inoculation activity.

### See also:

---

[Scanning Drives](#)

[Removing Viruses from Files and Boot Records](#)



## Scan Results

The Scan Results dialog box summarizes information about the scan just performed.

**Summary:** Reports if infected files, infected boot records, or inoculation issues were found.

**Items Scanned:** Lists the drives, directories, or files that were scanned.

**File Type:** Lists the types of files that were scanned.

**Inoculation:** Reports whether inoculation was active or disabled.

**Other Settings:** Reports on other settings, such as whether compressed files were included in the scan.

**Scan Time:** Reports the duration of the scan.

### Item:

**Scanned:** Lists whether memory, master boot record, boot records, and/or files were scanned.

**Infected:** Lists what items, if any, were infected.

**Cleaned:** Lists whether infected items were cleaned. (That is, whether the affected file was deleted, repaired, or inoculated.)

Select **Print...** to output this summary to a printer or to a file.

Select **Details...** to see more information. This button is dimmed if no problems were found.

**NOTE:** If you see a Problems Found dialog box or other alert, see Chapter 3, "Taking Corrective Action," in the printed manual.

---





## Scan Directory

Use this dialog box to specify and scan a directory on one of your disks.

Type in the directory path to be scanned, or select it from the list box. Then select the Scan button. If you want subdirectories included in the scan, be sure to check the **Include Subdirectories** option.

### See also:

---

[Scanning a Directory](#)



## Scan File

Use this dialog box to select and scan one file. Type the filename in the text box or select it from the list box, then select the Scan button.

### See also:

---

[Scanning Files](#)



## Open Setup File

Select a setup file from the list box, or type the name of a new one, then select OK. The default setup file name is `_DEFAULT.NNS`.

A setup file contains the settings for installing, updating, and using NAV on a workstation. You can create one setup file for everyone to use, or you can create different setup files for different groups of users.

**TIP:** It's a good idea to create one "master" setup file that you can then modify, using the Save As... command in the File menu to save the modified file under a new name.

---



## **Save Setup File**

Use the Save Setup File command to save your changes. The setup file should reside in the network directory containing the Norton AntiVirus program files.

When you make changes to the Install/update Settings, the Norton AntiVirus files on the workstation are automatically updated the next time the user logs onto the network.



## Auto-Protect Virus Sensor Settings

### Use Virus Sensor Technology

Check this option to use the full power of Norton AntiVirus to detect unknown viruses.

### When an Unknown Virus is Found:

**Prompt:** Informs you when an unknown virus is found and allows you to choose how to respond. Select this option to have the most control over what happens to an infected file.

**Repair Automatically:** Repairs an infected file as soon as an unknown virus is detected. The repair is recorded in the activity log.

**Delete Automatically:** Deletes an infected file without asking you. The deletion is recorded in the activity log.

**Halt Computer:** Halts your computer when an unknown virus is detected. You must then restart your computer.

### Buttons to Display if Prompted:

If you select the Prompt setting above, you can select from these options on the drop-down list:

**Repair:** Allows you to repair the file.

**Delete:** Allows you to delete the file.

**Continue:** Allows you to continue working. The file is still infected and the virus will be activated the next time you access the file.

**Exclude:** Allows you to exclude the file from being checked for unknown viruses. (Use sparingly!)



## Select Network Users

To send messages from Norton AntiVirus to other users on your network, select the server, the type and the names of those available from the lists.



## **Credits**

### **Product Management**

Janet Daly  
Ken Felderstein  
Peter Uhlir  
Germaine Ward  
Richard Yim

### **Development Team**

David Allee  
Reese Anschultz  
Sherralee Buzzell  
Leo Cohen  
Shane Coursen  
Peter Dickinson  
Martin Fallenstedt  
Barry Gerhardt  
Carlton Guc  
Brad Kingsbury  
Chengi Jimmy Kuo  
Steve Kurtz  
Mark Lawler  
Kevin Marcus  
Carey Nachenberg  
Brad Rembielak  
Radoslav Stanev  
Joe Wells  
Naser (Sami) Ziadeh

### **Quality Assurance Team**

George Chlentzos  
Scott Goldstein  
George McMullen  
Diann Milosek  
John M. Moldenhauer  
Therese Padilla  
David Shannon  
Andrew Sharp  
Thomas A. Smith

### **Documentation**

Karen Bergen  
Barbara Duarte  
Karen Goldsmith

### **Online Help**

Elizabeth Anders  
Dorthea Atwater

Ken Baker

Chris Ratner

**Technical Support Team**

Justin Bell

Alex Haddox

Cory Haibloom

Gary King

Kraig Lane

Andrew McGuirk

David Perry

Mike Shkolnik

Todd Sutphen

Mark Taylor

Mike Topacio

Mark Welinder

Bill Whipple

Mike Willison

**Engineering Services Team**

Scott Andrew

Ardeshir Babak

Alex Beyk

Alena Cespivova

John Eusebi

John Fawcett

Brian Foster

Kim Johnston

Camille Kazadi

Bob Kirwin

Patrick Martin

Scott Pasnikowski

Vicki Routs

Vickie VonBergen

Calvin Walker

Laura Weatherford





## **About...**

This command displays information about the product version.



## Verify Password

Type your password to access the feature.



## **Selected Drives**

This command immediately scans the drives selected in the Norton AntiVirus main window. (Selecting the Scan Now button does the same thing.)

### **See also**

---

[Scanning Drives](#)



## Directory...

Use this command to specify and scan a directory on one of your disks.

### See also

---

[Scanning a Directory](#)



## **File...**

Use this command to select and scan one file.

## **See also**

---

[Scanning Files](#)



## **Exit**

Use this command (or select the Exit button in the Norton AntiVirus main window) to leave Norton AntiVirus.



## **Scheduler...**

Use the Scheduler command to set up Norton AntiVirus to scan automatically at the times you specify.



## **Inoculation...**

Use this command to inoculate selected program files to protect them from unauthorized changes and to uninoculate selected program files.

### **See also**

---

[Inoculating Files](#)





## **Virus List...**

Use this command to view, print, or delete virus information.

### **See also**

---

[Viewing the Virus List](#)



## **Activity Log...**

Use this command to view a record of Norton AntiVirus activities in order to:

- ◆ Record known and unknown virus detections.
- ◆ List files that have changed since they were inoculated.
- ◆ Record virus-like activity detections.
- ◆ Record the end times of scans that you initiate (but not automatic scans).
- ◆ Record deletions and updates that you make to the virus list.



## Infection Log...

Use this command following a scan in order to:

- ◆ See which files were infected.
- ◆ View information about the virus found.
- ◆ See what action was taken to correct the problem.
- ◆ Ensure that all viruses were removed.
- ◆ Print a report to a printer or to a file.



## **New Setup File**

Use this command to create a new setup file for the Norton AntiVirus network manager.

For more information, see [Open Setup File](#); [Save Setup File](#); and Chapter 9, "Using the Network Manager" in the Norton AntiVirus manual.

# QuickHelp for Norton AntiVirus



## How do I . . . ?

Check for Viruses

Scan selected drives now.

Protect Against Viruses

Set up automatic protection.

Remove Viruses

Read how to remove viruses.

## Show me the . . .

Top 5 Questions

Review the most frequently-asked questions.

Contents

See the table of contents for Norton AntiVirus online help.

Tech Support Number

See the phone number and information for Norton AntiVirus technical support and customer service.



## Checkup

Ask yourself the following three questions. If you can say "yes" to all three, congratulations! If not, follow these tips.

- 1 Is my computer virus-free?

Conduct a complete scan of all your disks to find out. See [Scanning Drives](#)

- 2 Is my computer protected against viruses?

Make sure you're set up to

Scan floppy disks when you access them. See [Monitoring Floppy Disks](#)

Conduct automatic scans on your computer. See [Setting Up Automatic Protection](#)

- 3 Have I done everything I can?

"The 90s Guide to Safe Computing Practices:"

Keep Norton AntiVirus automatic protection active at all times.

Scan it before you use it -- no matter HOW trustworthy the source!

Write-protect your floppy disks before copying files from them.

Update virus definitions regularly so that you get maximum protection against new viruses. See [Updating the Virus List](#) for information.



## Top Five Questions

**1** What are viruses?

A computer virus is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. Computer viruses infect executable program files, such as word processing programs or spreadsheet programs. Viruses can also infect disks by attacking boot records and master boot records, which contain information your computer uses to start up. For more information see [Viewing the Virus List](#).

**2** What are known and unknown viruses?

A known virus is one that can be detected and identified by name. An unknown virus is a virus for which Norton AntiVirus does not have a definition. Rest assured that Norton AntiVirus can protect your computer from both types of viruses. See [Monitoring for Unknown Viruses](#).

**3** How do viruses spread?

A virus becomes active when you run an infected program or start up your computer from an infected disk. Once active, the virus spreads by making copies of itself and attaching them to other program files or disks. Most viruses stay active in memory until you turn off your computer. Turning off your computer removes the virus from memory, but it does not remove the virus from the infected file or disk.

**4** What do I do if my computer has a virus?

If you think your computer has a virus, scan your disks immediately. If a virus is found, Norton AntiVirus will step you through the process of eliminating it. See [Scanning Drives](#) for more information.

**5** Is my computer protected against viruses?

Norton AntiVirus automatically protects your computer from viruses as soon as you start it, providing constant protection while you work.



## **Contacting Technical Support and Customer Service**

Symantec's Technical Support department offers expanded support options designed for your individual needs no matter where you are located around the world. You are given StandardCare Support by purchasing the product. StandardCare Support provides all registered users of Symantec products the following services at no charge:

- ◆ Unlimited calls for 90 days (from date of first call) for installation assistance, configuration, and general usage questions.
- ◆ Unlimited technical assistance via CompuServe and America Online.
- ◆ Unlimited use of Symantec's Bulletin Board System (BBS). This download BBS is kept updated with sample files and product technical notes for quick and easy electronic access.
- ◆ Unlimited access to company information via the Internet. With an Internet browser program such as Mosaic, Cello, or Netscape, you get the latest company news by entering Symantec's Internet address: <http://www.symantec.com>.

The Web pages include links to our FTP site, where you can download the latest software patches and drivers for Symantec products. You can also FTP directly to the site by entering:

**<ftp.symantec.com>**

- ◆ Unlimited use of Symantec's automated fax retrieval system for instant printouts of technical notes, bulletins, product literature, and general information by fax.

StandardCare Support is available Monday through Friday, 7:00 a.m. to 4:00 p.m. Pacific Time. For your first 90 days of free technical support, use the phone number on the back of the *User's Guide*.

You can also choose from PriorityCare and PremiumCare services to extend your level of support. See the back of the *User's Guide* for complete descriptions of both services.

For more technical support or customer service information, click on one of the following:

[Customer Service, U.S. and Canada](#)

[Customer Service & Technical Support, International](#)

[Symantec BBS/CompuServe/American Online](#)

[Technical Support, U.S. and Canada](#)





## **Customer Service, U.S. and Canada**

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401

(800) 441-7234 United States and Canada only  
(541) 334-7400 fax  
Hours: 7:00 A.M.---4:00 P.M. Pacific Time, Monday--Friday



## Technical Support, U.S. and Canada

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401

If you are a registered user, free technical support is available for 90 days from the date of your first telephone call. The phone number is:

(541) 465-8420

Hours: 7:00 A.M.---4:00 P.M. Pacific Time, Monday through Friday

The number for the Symantec automated fax retrieval system is:

◆ Technical Support: (541) 984-2490

◆ Customer Service: (800) 554-4403

To receive technical application notes and samples of "how tos," please call out Technical Support fax retrieval number, and choose Option 2.

For PriorityCare 900 and 800 Number Service, call the numbers on the back of the *User's Guide*.

Hours for PriorityCare services are 6:00A.M. - 5:00P.M. Pacific Time, Monday through Friday.

For other Technical Support plans (PremiumCare Gold and PremiumCare Platinum), see the Symantec Customer Service Plan in the back of the printed manual.



## **Symantec BBS/CompuServe/America Online**

For 24-hr a day information, including updated virus definitions files, call the Symantec BBS at:

300- through 14,400-baud modems

(541) 984-5366 (24 hrs.)

300- through 28,200-baud modems only

(503) 484-6669 (24 hrs.)

For the Symantec Forums on CompuServe, type:

**GO SYMANTEC** at any ! prompt.

To access the Symantec bulletin boards on America Online, type keyword:

**SYMANTEC**



## Customer Service and Technical Support, International

If your country is not listed in the International Locations section below, please call out Technical Support automated fax retrieval service, located in the United States, at (541) 984-2490, choose Option 2, and request Document 1400.

### *World Headquarters*

Symantec Corporation  
10201 Torre Avenue  
Cupertino, CA 95014  
U.S.A.

Tel. 1 (408) 253-9600

### *European Headquarters*

Symantec Europe  
Kanaalpark 145  
2321 JV Leiden  
The Netherlands  
Tel. (31) (71) 353 111  
Fax Tel. (31) (71) 353 150  
Automated fax retrieval (voice  
menu)  
Tel. (31) (71) 353 255

#### Technical Support:

Dutch	Tel. (31) (71) 353 184
French	Tel. (31) (71) 353 180
German	Tel. (31) (71) 353 181
English	Tel. (31) (71) 353
182	
Fax	Tel. (31) (71) 353 153
BBS	Tel. (31) (71) 353 169

### *Asia/Pacific Rim region*

Symantec Australia Pty. Ltd.  
408 Victoria Road  
Gladesville, NSW 2111  
Australia  
Tel. (61) (2) 879 6577  
Fax Tel. (61) (2) 879 6805

Technical Support	Tel. (61) (2) 879 6577
Fax	Tel. (61) (2) 879 6594
BBS	Tel. (61) (2) 879
6322	
DOS/Win Antivirus	Tel. (61) (2) 879 7362
Mac Antivirus	Tel. (61) (2) 879 6968

### *Mexico*

Ruben Dario No. 36 Piso 2  
Oficina 6  
Col. Rincon del Bosque  
11580 Mexico, D.F.

Technical Support	Tel. (52) (5) 545 1234
Fax	(52) (5) 531 2252

Technical Support

For Technical Support call the automated fax retrieval service, located in the United States, at (541) 984-2490, and request document 1400.



## Keyboard Shortcuts

The following key combinations activate corresponding Norton AntiVirus functions and commands:

### Menu Command Keys

Use these keys to select and execute corresponding menu commands.

<b>Keys</b>	<b>Menu Command</b>
<b>Alt or F10</b>	Selects the first menu on the menu bar.
<b>Alt + underlined letter</b>	Selects the menu whose underlined letter matches the one you press.
<b>Underlined letter</b>	When in a menu, selects the command whose letter matches the one you press.

### Mouse Equivalent Keys

Use these keys to navigate Norton AntiVirus without a mouse.

<b>Keys</b>	<b>Movement</b>
<b>Up Arrow</b>	Moves up one item or line in a list or text box. Or moves among menu items in a selected menu.
<b>Down Arrow</b>	Moves down one item or line in a list or text box. Or moves among menu items in a selected menu.
<b>Left Arrow</b>	Moves left one character in a text box. Or moves left among menus.
<b>Right Arrow</b>	Moves right one character in a text box. Or moves among menu items in a selected menu.
<b>Alt + underlined letter</b>	Moves to the option or group in a dialog box whose underlined letter matches the one you press.
<b>Underlined letter</b>	Executes the command (in an open menu or dialog box) whose underlined letter matches the one you press.
<b>Tab</b>	Moves right one character in a text box. Or moves among menu items in a selected menu. Or moves between dialog box elements.
<b>Shift + Tab</b>	Moves up one item or line in a list or text box. Or moves among menu items in a selected menu. Or moves backwards between dialog box elements.



## Setting Up Automatic Protection

If you completed a full install of Norton AntiVirus as directed:

### **YOU ARE ALREADY PROTECTED**

Every time you start up your computer, Norton AntiVirus will:

- ◆ Automatically scan the root directory on your hard drive and monitor all programs you run for viruses
- ◆ Inform you if a virus is found

**NOTE:** If you performed a full install, automatic protection for DOS is installed in your CONFIG.SYS file as a device driver. You may wish to set up automatic protection as a terminate-and-stay-resident program (TSR) to avoid conflicts with programs that must load before Norton AntiVirus.

---

**If you need to set up automatic protection for the first time or change the way it is currently set up:**

See "Setting Up Automatic Protection" in Chapter 7 in the printed manual.

---

**If you want to customize the automatic protection options to suit your own needs:**

See Chapter 7, "Customizing Automatic Protection," in the printed manual for more information.

---

**See also:**

[Customizing Automatic Protection](#)

---



## Monitoring During Startup

The Auto-Protect Startup options determine such things as which areas of your computer are automatically scanned when you turn it on.

---

### To customize the startup options:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the **Auto-Protect** category on the left side of the Options dialog box. The Options - Auto-Protect Settings dialog box appears.
- 3 Select **Startup...** The Auto-Protect Startup Settings dialog box appears.
- 4 Specify in the **What to Scan Upon Startup** group box the areas to scan each time you start your computer. We recommend you check all of these: Memory - Master Boot Record -Boot Records.
- 5 Specify in the **Types of Memory To Use** group box the type(s) of memory you want automatic protection to run in: High Memory (HMA), Upper Memory (UMB), or Expanded Memory (EMS). If you don't know what types of memory you have, check them all. Norton AntiVirus will determine which types you have and which type to use at a given time.
- 6 Specify in the **Bypass Keys** group box the keystroke combination you want to use to prevent automatic protection for DOS from loading when your computer starts up. Select **None** if you don't want a bypass key combination.

**WARNING:** If you are using MS-DOS 6.0, do not select the **Both Shift Keys** option. Pressing a Shift key while booting with MS-DOS 6.0 causes both your CONFIG.SYS and AUTOEXEC.BAT files to be completely bypassed.

---

- 7 Check **Auto-Protect Can Be Unloaded** to make automatic protection unloadable. You may want to unload automatic protection at times when you are running programs that conflict with Norton AntiVirus.  
In order to unload automatic protection, it must be the last TSR (terminate-and-stay-resident program) loaded into memory. See "Using Automatic Protection as a TSR" in Chapter 7 of the printed manual for more information.
- 8 Check **Hide Icon In Windows** to hide the Norton AntiVirus Auto-Protect icon on the Windows desktop.  
Note that you will not be able to unload automatic protection from within Windows.
- 9 Select OK in the Auto-Protect Startup Settings dialog box.
- 10 Select OK in the Options - Auto-Protect Settings dialog box.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

---



## Monitoring the Files You Use

Norton AntiVirus can check for known and unknown viruses whenever you run a program, copy a file, or write a file to a disk for the first time. For maximum protection and flexibility configure automatic protection as follows:

---

### To monitor the files you use:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the **Auto-Protect** category on the left side of the Options dialog box.  
The Options - Auto-Protect Settings dialog box appears.
- 3 Check all three of the options in the **Scan a File When** group box. Files will be scanned each time they are accessed.
- 4 Select **Program Files Only** in the **What to Scan** group box. Norton AntiVirus will scan every file with an extension contained in the program file extensions list. These are the files most likely to become infected.
- 5 Select **Prompt** in the **When a Virus is Found** drop-down list box. This gives you the most control over what happens to an infected file.
- 6 Check the **Repair**, **Delete**, and **Stop** check boxes in the **Buttons to Display if Prompted** group box and select OK.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

### See also:

---

[Monitoring During Startup](#)

[Setting Up Automatic Protection](#)





## Monitoring Floppy Disks

Floppy disks are the most likely way for boot viruses to spread.

---

### To monitor floppy disks:

- 1 Select **Options...** from the Tools menu.
- 2 Select the **Auto-Protect** category on the left side of the Options dialog box. The Options - Auto-Protect Settings dialog box appears
- 3 Select **Advanced...**  
The Auto-Protect Advanced Settings dialog box appears.
- 4 In the **Check Floppies** group box, specify how you want Norton AntiVirus to check for boot viruses on floppy disks:

**Check Floppies for Boot Viruses Upon Access:** Checks for boot viruses on each floppy disk you access (when you list the directory, copy a file, write to a file, or run a file).

**Check Floppies When Rebooting Computer:** Checks a floppy disk in drive A: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del.

**When Rebooting, Check both drives (A: and B:):** Also checks a floppy disk in Drive B: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del. Select this option if you have a system that can boot from a disk in the B: drive.

**CAUTION:** These options offer no protection when you restart your computer using the power switch or the Reset button.

---

- 5 Select OK in the Auto-Protect Advanced Settings dialog box.
- 6 Select OK in the Options - Auto-Protect Settings dialog box.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

### See also:

[Monitoring the Files You Use](#)

---



## Monitoring for Unknown Viruses

An unknown virus is one for which Norton AntiVirus does not have a definition. The Norton AntiVirus Virus Sensor Technology feature checks the files you access for unknown viruses.

---

### To monitor for unknown viruses:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Auto-Protect category on the left side of Options dialog box. The Options - Auto-Protect Settings dialog box appears.
- 3 Select **Sensor....** The Auto-Protect Virus Sensor Settings dialog box appears.
- 4 Check **Use Virus Sensor Technology** to detect when your programs become infected by an unknown virus.
- 5 Select an option in the **When an Unknown Virus is Found** drop-down list box:
  - Prompt:** Informs you when an unknown virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.
  - Repair Automatically:** Repairs an infected file without notifying you. The outcome of the repair is recorded in the activity log.
  - Delete Automatically:** Deletes an infected file without notifying you. Use caution when selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
  - Halt Computer:** Halts your computer when an unknown virus is detected. You must then restart your computer.
- 6 If you selected Prompt in step 5, specify in the **Buttons to Display If Prompted** group box which options you want Norton AntiVirus to make available when an unknown virus is found:
  - Repair:** Allows you to repair the infected file.
  - Delete:** Allows you to delete the infected file.
  - Continue:** Allows you to continue without taking action on the file. The file remains infected with the unknown virus.
  - Exclude:** Allows you to exclude the file from future checks for unknown viruses. Use caution when allowing this button to appear; it can reduce your protection against unknown viruses.
- 7 Select OK in the Auto-Protect Virus Sensor Settings dialog box.
- 8 Select OK in the Options - Auto-Protect Settings dialog box.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

---



## Inoculating Files

### Why inoculate?

Inoculation is a form of prevention against unknown viruses. When a file or boot record has been inoculated, it is checked against inoculation data each time it is scanned, to see if the file or boot record has changed.

- ◆ Changes in inoculation data can indicate the presence of a virus.
- ◆ Only boot records on your startup drive and program files can be inoculated.
- ◆ Inoculation makes no change to the file itself, nor does it ever repair an infected file.

You can inoculate boot records and program files:

- ◆ using the Inoculation... command in the Tools menu.
- ◆ during a scan. This includes scans performed by automatic protection.

---

### To inoculate files using the Inoculation... command:

- 1 Choose **Inoculation...** from the Tools menu.  
The Inoculation dialog box appears.
- 2 Select **Inoculate Item**.
- 3 Type the pathname for the file, group of files, directory, or drive in the **Item** text box.  
You can use a wildcard to specify a group of files. For example, if you wish to inoculate all .COM files in your DOS directory, you might type C:\DOS\\*.COM.  
Or,  
Select the **Item** browse button to choose a single file from a list, then select OK.
- 4 If the item is a directory, check **Include Subdirectories** if you want to inoculate files in all associated subdirectories.
- 5 Select OK.

**NOTE:** Norton AntiVirus will not check for changes in inoculated files unless you enable the Inoculate Program Files feature. See "To inoculate during a scan" below for more information.

---

**To reinoculate** after you have upgraded files, follow the same steps.

**To uninoculate**, select **Uninoculate Item** and type the pathname for the file, group of files, directory, or drive in the **Item** text box.

---

### To inoculate during a scan:

- 1 See [Customizing Inoculation](#) in online help and set up all options.
- 2 Scan the files, directory, or drives that you want to inoculate.  
The items will be inoculated as you scan.

**NOTE:** To be able to reinoculate during a scan, the Prompt setting must be selected in the When an Inoculated Item Has Changed drop-down list box in the Options - Inoculation Settings dialog box.

---

### See also:

[Customizing Inoculation](#)



## Monitoring for Virus-Like Activities

Norton AntiVirus can monitor your computer for five types of activities that viruses use to damage your files. There are indeed applications that perform these activities for valid reasons, but Norton AntiVirus monitors for them on the chance that an unknown virus is involved.

---

### To monitor for virus-like activities:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the **Auto-Protect** category on the left side of the Options dialog box.  
The Options - Auto-Protect Settings dialog box appears.
- 3 Select **Advanced...**  
The Auto-Protect Advanced Settings dialog box appears.
- 4 Select an option in each drop-down list box to specify what Norton AntiVirus should do when it detects the virus-like activity:
  - Prompt:** Informs you when a program tries to perform the activity and allows you to decide whether the activity should continue, stop, or be excluded for the program. Select Prompt for the best combination of flexibility and protection.
  - Allow:** Allows the activity to continue every time without informing you. Selecting Allow offers you no protection against an unknown virus performing the activity.
  - Don't Allow:** Prevents the activity from occurring every time it is detected. This gives the maximum protection, but can impede your work.
- 5 Select OK in the Auto-Protect Advanced Settings dialog box.
- 6 Select OK in the Options - Auto-Protect Settings Dialog box.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

### See also:

---

[Virus-Like Activities](#)



## Viewing the Exclusions List

Norton AntiVirus uses the entries in the exclusions list in all scans it performs. An exclusion is a condition or activity that would normally be detected during a scan, but you have told Norton AntiVirus not to look for in a particular file.

---

### To view the exclusions list:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Exclusions List category on the left side of the Options dialog box.  
The Options - Exclusions List Settings dialog box appears.
- 3 Select a file or group of files in the **Items** group box.  
The activities excluded for the file or files are displayed in the **Exclusions** group box.
- 4 Select OK.



## Modifying the Exclusions List

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

---

### Adding Exclusions

In most cases, you add an exclusion when you select the Exclude button to resolve a problem that Norton AntiVirus has detected. You can also add exclusions to Norton AntiVirus manually.

---

#### To add exclusions manually:

- 1 Select **Add...** in the Options - Exclusions List Settings dialog box.  
The Add Exclusion dialog box appears.
- 2 Type the pathname for the file or group of files in the **Item** text box.  
Or,  
Select the **Item** browse button to choose a single file from a list, then select OK.  
If you enter a filename with no path, such as NAV.EXE or JUNK.\*, all files fitting that description are excluded.  
If you enter a full pathname, such as C:\NAV\NAV.EXE or C:\JUNK.\*, only files in that directory fitting that description are excluded.  
If you enter a directory, all files in the directory are excluded.
- 3 Check **Include Subdirectories** if you want files in the subdirectories of a directory to be excluded also. Note that this option only applies if the item is a directory.
- 4 Check the activities that you want Norton AntiVirus not to look for in the item specified. For a list, see [Add/Edit Exclusion](#).
- 5 Select OK in the Add Exclusion Settings dialog box.
- 6 Select OK in the Options - Exclusions List Settings dialog box.

### Editing the Exclusions List

You can edit the exclusions list when changes are necessary.

---

#### To edit the exclusions list:

- 1 Select a file or group of files in the **Items** group box in the Options - Exclusions List Settings dialog box.
- 2 Select **Edit...** The Edit Exclusion dialog box appears.
- 3 Change the appropriate settings.
- 4 Select OK in the Edit Exclusion dialog box.
- 5 Select OK in the Options - Exclusions List Settings dialog box.

### Deleting Exclusions

If you no longer want to use an exclusion, you can delete it.

---

#### To delete an exclusion:

- 1 Select a file or group of files in the **Items** group box in the Options - Exclusion List Settings dialog box.
- 2 Select Delete.  
The exclusion is deleted from the list.
- 3 Select OK.

Be sure to reload automatic protection to activate the new settings.



## Virus-Like Activities

Norton AntiVirus can monitor your computer for five types of activities that viruses use to damage your files:

**Low-Level Format of Hard Disk:** All information on the disk is erased and cannot be recovered. This type of format is generally performed at the factory only. If this activity is detected, it almost certainly indicates an unknown virus at work.

**Write to Hard Disk Boot Records:** Only a few programs write to hard disk boot records. If this activity happens on your computer, it could indicate an unknown virus at work.

**Write to Floppy Disk Boot Records:** Only a few programs (such as the DOS FORMAT command) write to floppy disk boot records. If this activity is detected on your computer, it could indicate an unknown virus at work.

**Write to Program Files:** Some programs save configuration information within themselves. Although this activity often happens legitimately, it could indicate an unknown virus at work.

**Read-Only Attribute Change:** Many programs change a files read-only attribute. Although this activity often happens legitimately, it could indicate an unknown virus at work.

### See also:

---

[Monitoring for Virus-Like Activities](#)



## Removing Viruses from Memory

A virus in memory means the virus has been activated, is spreading to other files, and, in the worst cases, is damaging data on your disk. You will know you have a virus in your computer's memory when an alert box appears and your computer is halted.

You will not be able to access help. See, Chapter 3, "Taking Corrective Action," in the printed manual for a procedure to remove the virus from memory.

---

### Overview of what to do when your computer is halted because of a virus in memory:

- 1 Use the power switch to turn off your computer to get the virus out of memory.
- 2 Next, reboot from your rescue disk and perform a scan of all files.

### See also:

---

[Scanning Files](#)





## Removing Viruses from Files and Boot Records

If Norton AntiVirus finds a virus in a file, you should either delete the file and replace it with an uninfected copy or attempt to repair the file. If a virus is found in boot records, you should attempt to repair them. You cannot delete boot records. (The boot record and master boot record are the areas on a disk that contain the information your computer uses to start up.)

---

### To delete an infected file:

- ◆ Select **Delete** in the alert box. After the file is deleted, your computer resumes its previous operation.

Or,

- 1 Select the file you want to delete in the Problems found dialog box.
- 2 Select **Delete**. The Delete File dialog box appears.
- 3 Select **Delete** in the Delete File dialog box.

Or,

Select **Delete All** to delete all the infected files listed in the Problems Found dialog box.

- 4 When all problems have been addressed, select Done in the Problems Found dialog box. After deleting infected files, scan your drives and floppy disks with Norton AntiVirus to make sure there aren't any other files that contain viruses. Then replace the files you deleted with uninfected copies. (Make sure you scan the replacement copies before copying them to your hard disk.)

---

### To repair an infected file or boot record:

- ◆ Select **Repair** in the alert box.

After the file or boot record is repaired, your computer resumes its previous operation. If Norton AntiVirus finds another virus, the alert box appears again.

(If the Repair button is dimmed, the file cannot be repaired or the Repair option has not been enabled in the Options - Scanner Settings or Options - Auto-Protect Settings dialog boxes.)

Or,

- 1 Select the item you want to repair in the **Problems Found** dialog box.
- 2 Select **Repair**.

The **Repair File** dialog box appears. The name of the infected file or drive and the name of the virus are shown.

- 3 Select **Repair** or **Repair All** in the Repair File dialog box.

When the repair procedure is complete, the Status column in the Problems Found dialog box shows Repaired next to the item repaired.

- 4 Select **Done** when you are finished. The **Scan Results** dialog box appears.
- 5 Select **Details** in the Scan Results dialog box if you want to see details about the scan.

Or,

Select Close. The Norton AntiVirus main window appears.

- 6 Scan your drive again to make sure all the viruses have been repaired.

### Unable to Repair a File

If Norton AntiVirus could not repair the infected file, the only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy.

### Unable to Repair a Boot Record

If Norton AntiVirus could not successfully repair a boot record or master boot record on a hard disk, you can use your [rescue disk](#) to restore the boot records to an uninfected state. See Restoring a Hard Disk Using the Rescue Disk in Chapter 3 of the printed manual.

If Norton AntiVirus could not successfully repair a boot record on a floppy disk, the information on the disk is still accessible. You can no longer use the floppy disk to boot your computer from; however, you can use the DOS SYS command to make the disk bootable again. Refer to your DOS manual for information

on how to use the SYS command.

**See also:**

---

[Restoring System Files](#)

[Customizing Automatic Protection](#)

[Customizing Scanner Options](#)

[Repair/Delete/Inoculate File](#)



## **Restoring System Files**

If the infected file is a system file such as COMMAND.COM, IO.SYS, MSDOS.SYS, IBMBIO.COM, or IBMDOS.COM, restore it using the DOS SYS command. Refer to your DOS manual for instructions on using the SYS command.



## Resolving Inoculation Issues

If you have set Norton AntiVirus up to prompt you to inoculate boot records or program files, Norton AntiVirus will bring the issue to your attention in an alert box.

---

### To inoculate boot records and system files:

- ◆ Select **Inoculate**.

If you choose to inoculate, Norton AntiVirus will notify you if the boot records or system files ever change. Changes to these items can indicate the presence of an unknown virus. Inoculation makes no change to the boot records or system files.

Or,

- ◆ Select **Continue** to continue without taking any action.

This does not prevent Norton AntiVirus from notifying you about this again. If you do not want future notifications, you can turn the feature off.

---

### To inoculate files:

Select **Inoculate** to generate inoculation data for the file. If you are inoculating a file in the Problems Found dialog box, select **Inoculate** in the Inoculate File dialog box that appears.

If Norton AntiVirus informs you that a file has an inoculation change, it means the file has changed since you last inoculated it. This information appears in an alert box or in the Problems Found dialog box. The change in the file could be due to one of these situations:

- ◆ The file has changed for legitimate reasons since the last time you inoculated it. For example, you may have installed a new version of the software and forgotten to reinoculate the program file.
- ◆ The file contains a virus that is not in the definitions file (perhaps because you don't have the most recent virus definitions or because it is a new virus that Norton AntiVirus does not yet have a definition for).

The message on your screen indicates whether the inoculation change is in a program file or in the boot records and system files.

---

### To resolve an inoculation change in boot records or system files:

- ◆ If you are certain the boot records or system files have changed for legitimate reasons, select **Inoculate** to reinoculate them.

Or,

- ◆ If you suspect a virus, select **Repair** to return the boot records and system files to the way they were when you last inoculated them.

**NOTE:** Inoculation changes in boot records and system files are likely to indicate the presence of an unknown virus. Boot records and system files change legitimately in very few situations, such as when you have installed a new operating system, repartitioned your hard disk, or changed the volume label.

---

### To resolve an inoculation change in a file:

- ◆ If you are certain the file has changed for legitimate reasons, select **Inoculate** to reinoculate the file.

Or,

- ◆ If you suspect the file has not changed for legitimate reasons, it may contain an unknown virus. Select **Repair** to reconstruct the file to the way it was when you last inoculated it.

Or,

- ◆ Select **Delete** to remove the file, then replace it with an uninfected copy.

Or,

- ◆ Select **Exclude** if you do not want to reinoculate the file or receive future notifications about inoculating this file.

If any of these command buttons is dimmed, Norton AntiVirus is configured not to use it at this time. See [Customizing Inoculation](#).

If you have never inoculated a file, see "Protecting Against Unknown Viruses" in Chapter 4 in the printed manual to find out how to inoculate files, why you should do this, and what your options are.

**See also:**

---

[Inoculating Files](#)



## Responding to Virus-Like Activity Alerts

A virus-like activity alert does not necessarily mean your computer has a virus--it is simply a warning. It's up to you to decide whether the operation is valid in the context in which it occurred.

---

### To respond to the alert:

- ◆ Select **Continue** if the message in the alert box describes an activity that is valid in the context of the application you're running, for example, if you're updating a program and the alert warns you of an attempt to change the program file.

Or,

- ◆ Select **Stop** if the activity detected is not related to what you're trying to do. For example, if you are playing a game and receive an alert stating that there is an attempt to write to the boot records of your hard disk, select Stop to prevent your disk from being written to.

Or,

- ◆ Select **Exclude** if the activity is valid in the context you're working in and you don't want Norton AntiVirus to alert you of this activity (performed by this application) in the future.

**NOTE:** If any of these command buttons is dimmed, you have selected Don't Allow for this activity in the Auto-Protect Advanced Settings dialog box. See [Monitoring for Virus-Like Activities](#) to find out how to change this option.

### See also:

---

[Virus-Like Activities](#)



## Restarting a Halted Computer

If you set up Norton AntiVirus to halt every time a virus is found, you will have to:

Reboot from your [rescue disk](#). See "Removing Viruses from a Halted Computer" in Chapter 3 of the printed manual for more information.

### See also:

---

[Removing Viruses from Files and Boot Records](#)

[Resolving Inoculation Issues](#)



## **Using a Rescue Disk**

### **Using a Rescue Disk**

If you have eliminated viruses and subsequently your computer won't boot, you can use a rescue disk to restore your hard disk.

See "Restoring a Hard Disk Using the Rescue Disk," in Chapter 3 of the printed manual to find out how to use a rescue disk.





## Scanning Drives

If you suspect a virus has infected your computer, you should scan the entire drive or a combination of hard drive, floppy drives and/or network drives to locate all of the infected files.

---

### To scan one or more drives:

- 1 Select the drives you want to scan in the **Drives** list box.  
The selected drives are shown on the Selected Drives information line.
- 2 Select **Scan Now**.  
The Scan Dialog box reports on the progress of the scan.

**If no problems were found**, the **Scan Results** dialog box appears with summary information.

**If a problem was found** (such as a virus), the **Problems Found** dialog box or an alert box appears.

### See also:

---

[Removing Viruses from Files and Boot Records](#)



## Scanning a Directory

There may be times when you want to scan only the files in a particular directory for viruses.

---

### To scan a directory:

- 1 Choose **Directory...** from the Scan menu.  
The Scan Directory dialog box appears.
- 2 If you want to change to another drive, select a drive letter in the **Drives** drop-down list box.  
The directories for the selected drive appear in the Directory list box.
- 3 Select the directory you want to scan in the **Directory** list box.
- 4 Check **Include Subdirectories** to also scan the subdirectories of the selected directory.
- 5 Select **Scan**.  
The Scan dialog box reports on the progress of the scan.

**If no problems were found**, the **Scan Results** dialog box appears with summary information.

**If a problem was found** (such as a virus), the **Problems Found** dialog box or an alert box appears.

### See also:

---

[Removing Viruses from Files and Boot Records](#)

[Resolving Inoculation Issues](#)



## Scanning Files

Before copying a file to your disk, check it for viruses first.

---

### To scan a file:

- 1 Choose **File...** from the Scan menu.  
The Scan File dialog box appears.
- 2 If you want to change to another drive, select a drive letter from the **Drives** drop-down list box.  
The directories for the selected drive appear in the **Directories** list box.
- 3 Select the directory where the file you want to scan is located. Then select the file from the **File Name** list box.
- 4 Select **Scan**.  
The Scan dialog box reports on the progress of the scan.

**If no problems were found**, the **Scan Results** dialog box appears with summary information.

**If a problem was found** (such as a virus), the **Problems Found** dialog box or an alert box appears.

### See also:

---

[Removing Viruses from Files and Boot Records](#)

[Resolving Inoculation Issues](#)



## Scheduling Scans

You can schedule scans to be performed automatically. You specify what to scan and how often you want the scans to occur.

---

### To schedule virus scans:

- 1 Choose **Scheduler...** from the Tools menu.  
The Scheduler dialog box appears.
- 2 Select **Add...**  
The Add Event dialog box appears.
- 3 Check **Enable This Event**. If you uncheck this option, the scan won't run.
- 4 Check **Audible Alarm** if you want to hear a sound when the scan starts.
- 5 Select **Run Program**.
- 6 Type a brief description in the **Description** text box. This text will appear in the events list box in the Scheduler dialog box.
- 7 Type the appropriate command line statement to run Norton AntiVirus in the **Command Line To Run** text box. See Appendix C, "Using Command-Line Switches" for the command line switches you can use.  
For example, if you want to scan your C: drive, type C:\NAV\NAVW C: in the Command Line to Run text box.
- 8 Select how often you want the scan to occur in the **Frequency** drop-down list box.
- 9 Finish scheduling the scan by entering the correct time, day, and date information.

**NOTE:** You can ignore the Startup Directory and Run Style options because they do not apply to scheduling Norton AntiVirus scans. They can be used when scheduling other programs to run at specified times.

---

- 10 Select OK.
- 11 Choose **Load With Windows** from the Scheduler Options menu. A check mark appears next to the command to indicate it is on. The Scheduler must be loaded in order to execute the scans you have scheduled.
- 12 Choose **Minimize...** from the control-menu box.



## Viewing the Virus List

You can view details about viruses, including the type of files they infect, their symptoms, and their aliases.

---

### To view the list of virus names:

- 1 Choose **Virus List...** from the Tools menu.  
The Virus List dialog box appears. The list box displays the name of the virus and what it infects (program files, boot records, or both).
- 2 Select the category of viruses to display in the **Display** drop-down list box.
  - All Viruses:** Displays all of the viruses that Norton AntiVirus can detect.
  - Common Viruses:** Displays the most common viruses.
  - Program Viruses:** Displays viruses that can infect program files that you run.
  - Boot Viruses:** Displays viruses that can infect boot records or master boot records on disks.
  - Stealth Viruses:** Displays viruses that try to conceal themselves from attempts to analyze or remove them.
  - Polymorphic Viruses:** Displays viruses that appear differently in each infected file; making detection more difficult.
  - Multipartite Viruses:** Displays viruses that infect both program files and boot records.
- 3 Select OK.

---

### To search for a virus name:

- 1 Activate the virus list box by pressing Tab or Shift+Tab to highlight it, or by clicking inside the list box.
- 2 Start typing the name of the virus you want to find.  
A text box appears. As you type the consecutive letters in the virus name, the highlight bar moves the corresponding virus name.
- 3 When the virus name you want is highlighted, press Enter.

If the virus name you are looking for is not in the list, it might be because the list is not showing all viruses or you might be looking for an alias rather than a standard name. To display all virus names, select **All Viruses** in the **Display** drop-down list box.

### See also:

---

[Updating the Virus List](#)

---

### To display detailed information about a virus:

- 1 Select the virus name in the **Virus List** dialog box.  
If the virus name you are looking for is not in the list, it might be because the list is not showing all viruses or you might be looking for an alias rather than a standard name. To display all virus names, select **All Viruses** in the **Display** drop-down list box.
- 2 Select **Info...** The Virus Information dialog box appears, displaying detailed information about the virus.
- 3 Select **Print...** if you want to print the detailed virus information to the printer or to a text file.
- 4 To see detailed information about other viruses, select **Next Virus** or **Previous Virus**, as appropriate.
- 5 Select **Close** in the Virus Information dialog box.
- 6 Select OK in the Virus List dialog box.

### See also:

---

[Updating the Virus List](#)



## Updating the Virus List

To ensure that your computer is protected from new viruses, update the virus list as new definitions become available. The Customer Service Plan located in the manual explains how to get current virus definition files. Instructions for updating the virus list are provided with each update you receive.

Occasionally, a virus definition may become out of date. When this happens, you can delete it from the virus list.

---

### To delete a virus definition:

- 1 Choose **Virus List...** from the Tools menu.  
The Virus List dialog box appears.
- 2 Select the virus name that you want to delete.
- 3 Select **Delete...**  
A dialog box appears asking you to verify the deletion.
- 4 Select **Yes** to delete the virus definition.
- 5 Select **OK**.

**NOTE:** After changing the virus list, you must reload automatic protection for the new virus definitions to take effect.

### See also:

---

[Viewing the Virus List](#)



## Using the Activity Log

You can see information about the problems Norton AntiVirus detected and the way they were resolved by viewing the activity log.

---

### To view entries:

- 1 Choose **Activity Log...** from the Reports menu.  
The Activity Log dialog box appears.
- 2 Select **Filter...** in the Activity Log dialog box to specify the events that you are interested in seeing entries for.  
To display entries from specific dates or a range of dates, check **Dated**, then select an option in the Dated drop-down list box.
- 3 Select **Print...** in the Activity Log dialog box if you want to print the entries displayed.
- 4 Select **Clear...** in the Activity Log dialog box to delete all entries. Select Yes to accept changes.
- 5 Select Close to exit the Activity Log dialog box.

### See also:

---

[Using the Infection Log](#)



## Using the Infection Log

To view a report of viruses found and the resolution for each:

- 1 Select **Infection Log...** from the Reports menu.  
The Infection Log dialog box appears.
- 2 Select **Filter...** in the Infection Log dialog box and check events that you are interested in seeing reported.  
To display entries from specific dates or a range of dates, check **Dated**, then select an option in the Dated drop-down list box.
- 3 Select **Print...** to output a report of viruses found and the resolution for each.
- 4 Select Close.

### See also:

---

[Using the Activity Log](#)





## Troubleshooting Networks

If the **Network Drives** option is dimmed, you are not connected to the network, do not have access to the network drives, or Norton AntiVirus is configured not to allow network drive scanning.

If you find an infected file on a particular network drive, you cannot repair or delete it unless you have write access to that file.



## Customizing Scanner Options

The settings for the Scanner category of options define what Norton AntiVirus does when you scan a file, directory, or drive, using the commands in the Scan menu or using the Scan Now command button.

---

### To customize scanning:

- 1 Choose **Options...** from the Tools menu. Select the Scanner category on the left side of the Options dialog box. The Options - Scanner Settings dialog box appears.
- 2 Specify in the **What To Scan** group box the areas Norton AntiVirus scans before it scans files:
  - Memory:** Checks for viruses resident in your computers memory, so they will not spread to all of the files you scan.
  - Master Boot Record:** Checks for boot viruses in the master boot record on your hard disk.
  - Boot Records:** Checks for boot viruses in the boot records on your hard disk and on any floppy disks that you scan.

We recommend that you check all of these options.

- 3 Specify what files you want to scan:
  - All Files:** Scans all files in the specified directory or drive. This includes files less likely to contain viruses.
  - Program Files Only:** Scans files that are most likely to become infected. Only the files with an extension that is specified in the program file extensions list are scanned.  
For information on program file extensions, see *Selecting Which Files to Scan* in Chapter 8 of the printed manual.
- 4 Check **Within Compressed Files** to have Norton AntiVirus scan files compressed using the PKZIP utility.

Scanning time may increase slightly if you have many .ZIP files. If you have no .ZIP files, scanning time is not affected by having this option selected.

- 5 Select an option in the **When a Virus is Found** drop-down list box:
  - Prompt:** Informs you when a virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.
  - Notify Only:** Merely informs you when a virus is detected. You will not be able to repair or delete the infected file.
  - Repair Automatically:** Repairs an infected file or boot record without notifying you. The results of the repair are displayed at the end of the scan. Note that Norton AntiVirus is preset to make backup copies of files before they are repaired.
  - Delete Automatically:** Deletes an infected file without notifying you. The file deletion will be displayed at the end of the scan. Use caution when selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
  - Halt Computer:** Halts your computer when a virus is detected. You must then restart your computer.
- 6 If you selected Prompt in Step 5, specify in the **Buttons to Display if Prompted** group box which options you want Norton AntiVirus to make available when a virus is found:
  - Repair:** Allows you to repair the file. If the virus infects an item that cannot be repaired, such as a compressed file, the button will be dimmed.
  - Delete:** Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button will be dimmed.
  - Continue:** Allows you to continue scanning without resolving the problem. The Continue button applies only when Immediate Notification is turned on. See the next step for details about Immediate Notification.
  - Exclude:** Allows you to exclude this file from future checks for known viruses. Use caution when enabling this button; it can reduce your protection against viruses.

- 7 Select **Advanced...**  
The Scanner Advanced Settings dialog box appears.
- 8 Check the options you want to enable:
  - Allow Network Scanning:** Allows you to scan entire network drives. Scanning network drives is more time-consuming than scanning local drives.
  - Allow Scanning to be Stopped:** Allows you to halt a scan in progress. When this option is checked, the Stop button is available during a scan.
  - Immediate Notification:** Displays an alert box when a problem is detected while scanning. This allows you to respond immediately, instead of waiting until the scan is completed.
- 9 Specify in the **Preselect at Start** group box the drives that you want selected automatically in the Drives list box when you start Norton AntiVirus.
- 10 Select OK in the Scanner Advanced Settings dialog box.
- 11 Select OK in the Options - Scanner Settings dialog box.



## Customizing the Activity Log

You can specify the name and location for the activity log file, the types of events to record, and a maximum size for the file.

---

### To customize the activity log:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Activity Log category on the left side of the Options dialog box. The Options - Activity Log Settings dialog box appears.
- 3 In the **Log Following Events** group box, check each type of event that you want Norton AntiVirus to record:
  - Known Virus Detections:** Records detections of known viruses.
  - Unknown Virus Detections:** Records detections of unknown viruses.
  - Inoculation Activities:** Records detections of uninoculated files and changes in a file's inoculation data.
  - Virus-Like Activities:** Records detections of virus-like activities, such as an attempt to format your hard disk.
  - Completion of Scans:** Records the date and ending time of scans that you initiate.
  - Virus List Changes:** Records changes to the virus list.
- 4 If you want to limit the size of the activity log file, check **Limit Size of Log File To**, then enter the desired size in the **Kilobytes** text box. When the specified file size is reached, each new entry added to the activity log will cause the oldest entry or entries to be deleted.
- 5 Enter the pathname for the activity log file in the **Activity Log Filename** text box.  
Or,  
Use the browse button to select an existing file or a path for a new file.
- 6 Select OK.

**NOTE:** You must reload automatic protection before it will recognize any of your new settings.

---



## Customizing Automatic Protection

The automatic protection feature of Norton AntiVirus is a terminate-and-stay-resident program (TSR) and is loaded when you start up your computer, so you are protected from viruses as soon as you start working.

---

### To customize protection for:

- ◆ The files you use, see [Monitoring the Files You Use](#)
- ◆ Virus-like activities, see [Monitoring for Virus-Like Activities](#)
- ◆ The floppy disks you use, see [Monitoring Floppy Disks](#)
- ◆ What happens when you start up your computer, see [Monitoring During Startup](#)
- ◆ Unknown viruses, see [Monitoring for Unknown Viruses](#)

While performing all of these functions for you, automatic protection is inconspicuous. It does not cause any delays in opening files and programs.



## Customizing Alerts

You can customize how Norton AntiVirus informs you that it has detected a virus or suspicious virus-like activity:

---

### To customize alerts:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the **Alerts** category on the left side of the Options dialog box. The Options - Alerts Settings dialog box appears.
- 3 Check any or all of the following categories:
  - Display Alert Message:** Lets you add a message with instructions or special warnings to all alerts that Norton AntiVirus displays. You can then enter a message of up to 76 characters in the text box.
  - Audible Alert:** Sounds a tone when Norton AntiVirus alerts you of a virus.
  - Remove Alert Dialog:** Removes notification dialog boxes after a specified number of seconds. You can enter a number between 1 and 99 in the **Seconds** text box.
- 4 Use the **Alert Others** group box to specify where you want Norton AntiVirus to send alerts over the network.
  - Alert Network Users:** Messages from Norton AntiVirus are sent to other users on your network. Type the names of the users in the text box or select the browse button and select the users from the list that appears.
  - Alert Network Console:** Messages from Norton AntiVirus are sent to the network server.
  - Alert Norton AntiVirus NLM If Present:** Messages from Norton AntiVirus are sent to the Norton AntiVirus NetWare Loadable Module (NLM) if it is present on your network.
- 5 If you checked an option in step 4, select **Others....** The Alert Others dialog box appears.
- 6 Select the types of alerts you want to broadcast over your network, then select OK.
- 7 Select OK in the Options - Alerts Settings dialog box.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

---



## Customizing Inoculation

The first step to inoculating files and boot records during a scan is to customize the Inoculation options.

---

### To customize inoculation options:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Inoculation category on the left side of the Options dialog box. The Options - Inoculation Settings dialog box appears.
- 3 Check **Inoculate Boot Records and System Files** to check the master boot record, boot record, and system files on your hard disk for inoculation.  
We recommend you check this option, since it is the only means by which Norton AntiVirus can detect unknown viruses in boot records.
- 4 Select an option in the **When An Item Has Not Been Inoculated** drop-down list box:
  - Prompt:** Informs you when a program file or boot record has not been inoculated and lets you choose how to respond.
  - Inoculate Automatically:** Inoculates each uninoculated program file or boot record as soon as it is detected.
  - Notify Only - Don't Inoculate:** Merely informs you that a program file or boot record is not inoculated. It will not inoculate the item.
  - Deny Access:** Informs you that a program file has not been inoculated and does not allow you to use the program. This options does not apply to uninoculated boot records.
- 5 Select an option in the **When An Inoculated File Has Changed** drop-down list box. See descriptions of your choices in step 5:
  - Prompt**
  - Notify Only - Don't Reinoculate**
  - Deny Access**
- 6 If you selected Prompt after either step 5 or 6 or both, specify in the **Buttons to Display If Prompted** group box which options you want Norton AntiVirus to make available when an inoculation issue is found.
  - Repair:** Allows you to repair a program file or boot record with an inoculation change, returning the item to its state when it was last inoculated.
  - Delete:** Allows you to delete a program file with an inoculation change. Boot records cannot be deleted.
  - Inoculate:** Allows you to inoculate a program file or boot record or reinoculate a changed program file or boot record.
  - Continue:** Allows you to continue the current operation (scanning or accessing a program file). No change is made to the inoculation data.
  - Stop:** Allows you to stop the current operation (scanning or accessing a program file). No change is made to the inoculation data.
  - Exclude:** Allows you to exclude the program file from future checks for inoculation changes.
- 7 Type a pathname for the inoculation files in the **Inoculation Path** text box.  
When you inoculate program files and boot records, an inoculation file is placed in the specified location on each drive you inoculate. If you are inoculating files on network drives, you must have read-write access privileges to this directory on the network drive. You do not need read-write access to the files you inoculate.
- 8 Select OK.

**NOTE:** You must reload automatic protection before it will recognize any of the new settings.

### See also:

---

[Monitoring for Unknown Viruses](#)







## Customizing Password Protection

You can add password protection to selected features of Norton AntiVirus to prevent unauthorized access.

---

### To password protect features:

- 1 Choose **Options...** from the Tools menu.
- 2 Select the Password category on the left side of the Options dialog box. The Options - Password Settings dialog box appears.
- 3 Check **Password Protect** to turn on the password protection feature.
- 4 If you want to protect all of the features shown in the list box, select **Maximum Password Protection**.  
Or,  
If you would like to protect only certain features, select **Custom Password Protection**; then select the features you would like to protect in the list box.
- 5 Select **Set Password...** to set a password. The Set Password dialog box appears.
- 6 Type a password in the **New Password** text box, then type it again in the **Confirm New Password** text box.

Passwords can be from 1 to 16 characters in length and are not case-sensitive ("a" is the same as "A"). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (\*) for security.

**TIP:** Write down your password and store it in a secure place.

---

- 7 Select OK in the Set Password dialog box.
- 8 Select OK in the Options - Password Settings dialog box.  
Password protection will activate the next time you start Norton AntiVirus. The password must be entered the first time you use a protected feature.

**NOTE:** Norton AntiVirus will also prompt for the password before allowing changes to the password protection options.

### See also:

[Password Settings Reference](#)

Close

## Glossary

A  
B  
C  
D  
E  
F  
G  
H  
I  
J  
K  
L  
M  
N  
O  
P  
Q  
R  
S  
T  
U  
V  
W  
X  
Y  
Z

-A-

**activity log file**  
**alert box**  
**application**  
**archive file**  
**AUTOEXEC.BAT**

-B-

**back up**  
**batch file**  
**(to) boot**  
**bootable disk**  
**boot partition**  
**boot record**  
**boot record program**  
**boot virus**  
**bulletin board system (BBS)**  
**button bar**

-C-

**CMOS**  
**cold boot**  
**.COM file**  
**command line switch**  
**compressed file**  
**CONFIG.SYS**  
**conventional memory**

-D-

**data file**  
**device driver**  
**dialog box**  
**directory**  
**disk**  
**document file**  
**DOS**  
**double-click**  
**download**  
**drag**  
**drive**  
**drop-down list box**

-E-

**EMS**  
**encryption**  
**exclusion**  
**exclusions list**  
**.EXE file**  
**executable file**  
**expanded memory**  
**extended memory**  
**extension**

-F-

**file allocation table (FAT)**  
**file server**

**floppy disk**

-G-

-H-

**hard disk**  
**hidden files**  
**high memory area**  
**HMA**  
**hotkey**

-I-

**icon**  
**infected file**  
**Infection log**  
**inoculate**  
**inoculation file**  
**Inoculation Technology**

-J-

-K-

**known virus**

-L-

**LAN**  
**launch**  
**list box**  
**load**  
**Local Area Network (LAN)**

-M-

**master boot record (MBR)**  
**master boot record program**  
**memory-resident program**  
**multipartite viruses**

-N-

**network**  
**network server**

-O-

-P-

partition table  
pathname  
polymorphic virus  
program  
program virus

-Q-

-R-

RAM  
random access memory  
read-only  
reboot  
reinoculate  
repair  
rescue disk

-S-

scan  
stealth virus  
subdirectory  
system disk  
system files

-T-

terminate-and-stay-resident program (TSR)  
Trojan horse  
TSR

-U-

UMBs  
uninoculate  
unknown virus  
upper memory blocks (UMBs)

-V-

virus  
virus definition  
virus-like activity

-W-

warm boot

workstation

write-protected disk

-X-

-Y-

-Z-

.ZIP file

**activity log file**

a file in which Norton AntiVirus records each activity it performs, such as scanning disks, finding viruses, and detecting virus-like activities.

**alert box**

a dialog box that appears on your screen to notify you that a virus, inoculation change, or virus-like activity has been detected. Norton AntiVirus may display alert boxes even while you are using another application.



**application**  
see program

**archive file**

a series of files that have been compressed into one file.

**AUTOEXEC.BAT**

a batch file that is automatically executed when the computer is started. See also batch file.

**back up**

the process of making copies of important files (to disks that are put away in a safe place), protecting yourself against loss of data.

**batch file**

a text file that contains a sequence of DOS commands. Batch files are used to save command sequences so that they can be re-executed at any time. Batch files typically have a .BAT extension.

**bootable disk**

a disk that contains the Disk Operating System(DOS) necessary to start, or boot, the computer.

**(to) boot**

to start the computer.

**boot disk**

a disk that contains the Disk Operating System (DOS) necessary to start, or boot, the computer.



**boot partition**

see master boot record.

**boot record**

the first physical sector on a floppy disk or the first logical sector of hard disk partition. It identifies the disks architecture (sector size, cluster size, and so on). It also contains the boot record program.

**boot record program**

the program that is responsible for loading DOS.

**boot virus**

a virus that infects the boot record program on both hard and floppy disks and/or the master boot record program on hard disks. A boot virus loads into memory before DOS, taking control of your computer and infecting any floppy disks that you access. A boot virus may prevent your computer from starting up at all from an infected disk.

**bulletin board system (BBS)**

an on-line service that allows messaging, electronic mail, and file transfer between computer users via modem.

**button bar**

a component of the Norton AntiVirus for Windows screen that contains buttons used for performing certain Norton AntiVirus functions.

**CMOS**

an abbreviation for Complimentary Metal Oxide Semiconductor: a battery-powered chip in 80286 (and more advanced) computers that preserves basic data about the system's hardware.

**cold boot**

to start your computer by switching on the power. A cold boot recycles your computer's random access memory, thus removing any viruses that might be present in memory.



**.COM file**  
see [executable file](#)

**command-line switch**

an option that controls the operation of a program. Switches are used when a program is executed from the DOS prompt or through the RUN... command in Windows.

**compressed file**

a single file or series of files that have been compressed into one file.

**CONFIG.SYS**

a text file containing commands that configure DOS and the system's hardware and that load device drivers. The file is automatically executed by DOS when you start your computer.

**conventional memory**

the first 640K of memory. This is the largest amount of memory that DOS can use without the aid of an extended or expanded memory manager.

**data file**

a file that is created by or associated with an application and contains no executable code. Examples include word processing documents, databases, and spreadsheets.

**device driver**

a type of terminate-and-stay-resident program that is loaded from CONFIG.SYS at each startup and cannot be unloaded. The Norton AntiVirus system monitor can be loaded as a device driver, providing earlier protection than when it is loaded as a normal TSR. See also terminate-and-stay-resident program.

**dialog box**

a box on the screen containing buttons and options that you select to tell Norton AntiVirus how to proceed.



**directory**

a portion of a disk that you designate to store certain files. Applications are typically kept in separate directories. Directories make it easier for you to organize the files on your disk. See also subdirectory.

**disk**

a device that stores information. There are two main types, floppy disks and hard disks.

**document file**  
see data file.

**DOS**

an abbreviation for Disk Operating System. See operating system.

**double-click**

to press the primary mouse button twice in rapid succession.

**download**

to transfer a file from one computer system to another through a modem or network. Most frequently used when referring to the act of transferring a file (through a modem) from a bulletin board service or server on a network.

**drag**

to hold the primary mouse button down while moving the mouse in a given direction. Often used to move an object on the screen.

**drive**

an entire disk or a partition. see also partition.



**drop-down list box**

a special type of list box that reveals a list of choices when you select its prompt button.

**EMS**

an abbreviation for Expanded Memory Specification. see expanded memory.

**encryption**

a way to impose data security on selected files, directories, or disks. Encryption scrambles data (usually by intertwining a key code or set of characters into the data) and seals it with a password. Only those who know the password can access (decrypt and use) the data.

**exclusion**

an action that you have instructed Norton AntiVirus not to look for in a particular file. For example, you may not want Norton AntiVirus to watch for the DOS program FORMAT to try to write to the boot sector of a floppy disk.

**exclusions list**

the list where Norton AntiVirus stores its exclusions.

**.EXE file**  
see executable file.

**executable file**

a file containing a program that can be run by DOS or Windows. Executable files generally have the following extensions: .COM, .EXE, .OVR, .OVL, .DRV, .BIN, or .SYS.

**expanded memory**

memory added to your computer using an expanded-memory board and/or an expanded-memory management program. Although expanded memory leaves more conventional memory available for other programs to use, it can be slower to use than extended memory.



**extended memory**

a memory area, in addition to conventional memory, available in 286 and higher machines. Programs that can use extended memory run faster and more efficiently and leave more conventional memory available for other programs to use.

**extension**

a three-letter suffix of a DOS filename, usually descriptive of the files contents. For example, .EXE is an extension of an executable file; .TXT is often an extension of a text file.

**file allocation table (FAT)**

a table in the system area of a disk that identifies the specific place on the disk where each file is physically stored.

**file extension**  
see extension

**file server**

a central disk storage device (or devices) connected to a network that provides network users access to shared applications and data files.

**floppy disk**

a removable disk used to store information, such as software and data, in files.

**hard disk**

a non-removable disk built into your computer and used to store information, such as software and data, in files.

**hidden files**

files with the file attributes set so that the files do not appear in a directory listing, thus making the files more difficult to delete and copy.



**high memory area**

the first 64K of extended memory. Few programs use this part of extended memory.

**HMA**

abbreviation for High Memory Area. see high memory area.

**hotkey**

a key that can be pressed to open a menu or invoke a menu command, button, or option, in place of using the mouse. Pressing the hotkey works the same as highlighting the item and pressing Enter.

**icon**

a graphic symbol used to represent an application, a document, or a group item.

**infected file**

a file that contains a virus.

**infection log**

a subset of the Activity Log, containing only known and unknown virus detection records.

**inoculate**

to generate information or data about a file that can be used to verify the integrity of the file at a later time.

**inoculation file**

a file containing inoculation data that is used during scans to verify the files integrity. An inoculation file is created for each drive on which you inoculate files.



**Inoculation Technology**

a technique used by Norton AntiVirus to compare the current state of a file with the information in the inoculation file to determine if the file has been changed, possibly by an unknown virus.

**known virus**

any virus that Symantec has analyzed and defined and that Norton AntiVirus can detect and identify by name.

**LAN**

an abbreviation for Local Area Network. See Local Area Network.

**launch**

to start or run an application, with or without a related document.

**list box**

a dialog box component that contains a roster of available choices.

**load**  
see launch.

**Local Area Network (LAN)**

a group of computers linked together with cables that have access to a shared computer. Common programs and data files may reside on the shared computer, known as the server. Also called a network.

**master boot record (MBR)**

the first physical sector on a hard disk. It contains information on how a hard disk is partitioned and the master boot record program. See also [master boot record program](#).



**master boot record (MBR) program**

the program that is responsible for directing the computer to load the boot record program from the bootable hard disk.

**memory-resident program**

(same as terminate-and-stay-resident, or TSR.) A program that loads itself into random-access memory (RAM) the first time it runs, and remains there until it is disabled or restarted, or until the computer is turned off or restarted.

**multipartite virus**

viruses that affect both programs and boot files, and can spread from one type of file to another.

**network**

a series of computers and associated hardware (printers, and so forth) connected together in a work group for the purpose of sharing information and hardware between users.

**network server**

a computer that allows other computers to access its file, and can provide them with centralized and shared services, including programs, storage, and communication.

**partition table**

a table in the master boot record of a hard disk that specifies how the disk is set up, such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.

**pathname**

the route to a file or directory on a disk. For example, if a file named QTR1.DOC is stored in the directory OFFICE on drive C:, the pathname for the file is C:\OFFICE\QTR1.DOC.

**polymorphic virus**

a type of virus that changes its telltale code segments so that it "looks" different from one infected file to another, thus making detection more difficult.



**program**

an executable file or group of files written for a specific purpose such as word processing or creating a spreadsheet.

**program file extension**

an extension for a program filename.

**program virus**

a virus that affect executable program files, which often have one of these file extensions: .COM, .EXE, .OVL, .DRV, .SYS, .BIN. Program viruses can stay in memory even after a program is executed, until you turn off your computer.

**RAM**

see Random-Access Memory

**random access memory**

the computer's working memory that determines the size and number of programs that can be run at the same time, as well as the amount of data that can be processed instantly.

**read-only**

refers to a disk or file containing data that can be read, but cannot be written to or deleted.

**reboot**

to restart your computer. See also warm boot and cold boot

**reinoculate**

to replace a previously inoculated file's inoculation data with data for the file in its current state.



**repair**

to remove a virus from a file and return the file to its original, uninfected state.

**rescue disk**

a floppy disk containing the partition table, boot record, and CMOS values for your hard disk, which can be used to restore this information if it is corrupted by a virus.

**scan**

the systematic search for viruses that is performed by Norton AntiVirus.

**stealth virus**

a virus that actively seeks to conceal itself from discovery or defends itself against attempts to analyze or remove it.

**subdirectory**

a branch of a directory at a lower level of hierarchy than a directory.

**system disk**  
see bootable disk.

**system files**

the files that make up DOS.

**terminate-and-stay-resident program (TSR)**

a program that loads itself into random-access memory (RAM) the first time it runs and remains there until it is disabled or restarted, or until the computer is turned off or restarted. Also called memory resident program.



**Trojan horse**

a program that promises to be something useful or interesting (like a game), but covertly may damage or erase files on your computer while you are running it. Trojan horses are not viruses.

**TSR**

see terminate and stay resident program.

**UMBs**

see upper memory blocks

**uninoculate**

to remove the inoculation data for a file, directory, or drive. See *also* [inoculate](#).

**unknown virus**

a virus for which Norton AntiVirus does not contain a virus definition. See also [virus definition](#).

**upper-memory blocks (UMBs)**

an area of memory normally reserved for running your system's hardware. TSR's can be loaded into this area, leaving more conventional memory available for programs to use.

**virus**

a self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge.

**virus definition**

virus information that allows Norton AntiVirus to recognize and alert you to the presence of a specific virus.



**virus-like activity**

an activity or action caused by other software that Norton AntiVirus perceives as the work of a possible unknown virus.

**warm boot**

to restart your computer by pressing Ctrl+Alt+Del. A warm boot can be detected and emulated by some viruses, so a virus in memory may still be there when the boot is complete.

**workstation**

a computer that is attached to a network and is not the network server.

**write-protected disk**

a disk that cannot be written to. Write-protecting disks prevents viruses from infecting them. To write-protect a 5.25" disk, cover the notch on the side of the disk with an adhesive label (usually included with boxes of disks.) To write-protect a 3.5" disk, slide the lever on the back of the disk to uncover the hole through the disk.

**.ZIP file**

a series of files that have been compressed into one file with a .ZIP extension using the PKZIP utility.



## Norton AntiVirus Help Contents



### **QuickHelp**



**Procedures**



**Commands**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**



# Norton AntiVirus Help Contents

 QuickHelp

 Quickhelp

 Checkup

 Procedures

 Commands

 Dialog Boxes

 Glossary

 Keyboard Shortcuts

 Credits



# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



## **Taking Precautions Against Viruses**



## **Taking Corrective Action**



## **Checking for Viruses**



## **Managing Virus Definitions**



## **Reporting Results**



## **Customizing Norton AntiVirus**



## **Troubleshooting**



## **Commands**



## **Dialog Boxes**



## **Glossary**



## **Keyboard Shortcuts**



## **Credits**





# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



## **Taking Precautions Against Viruses**



### **Setting up Automatic Protection**



### **Monitoring During Startup**



### **Monitoring the Files You Use**



### **Monitoring Floppy Disks**



### **Monitoring for Unknown Viruses**



### **Inoculating Files**



### **Monitoring for Virus-Like Activities**



## **Taking Corrective Action**



### **Checking for Viruses**



### **Managing Virus Definitions**



### **Reporting Results**



### **Customizing Norton AntiVirus**



### **Troubleshooting**



## **Commands**



## **Dialog Boxes**



## **Glossary**



## **Keyboard Shortcuts**



## **Credits**



# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



## **Taking Precautions Against Viruses**



## **Taking Corrective Action**



Removing Viruses from Memory



Removing Viruses from Files and Boot Records



Restoring System Files



Resolving Inoculation Issues



Responding to Virus-Like Activity Alerts



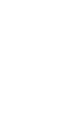
Restarting a Halted Computer



Using a Rescue Disk



Checking for Viruses



Managing Virus Definitions



Reporting Results



Customizing Norton AntiVirus



Troubleshooting



Commands



Dialog Boxes



Glossary



Keyboard Shortcuts



Credits



# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



## **Taking Precautions Against Viruses**



## **Taking Corrective Action**



## **Checking for Viruses**



## **Scanning Drives**



## **Scanning Files**



## **Scanning a Directory**



## **Scheduling Scans**



## **Managing Virus Definitions**



## **Reporting Results**



## **Customizing Norton AntiVirus**



## **Troubleshooting**



## **Commands**



## **Dialog Boxes**



## **Glossary**



## **Keyboard Shortcuts**



## **Credits**



# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



### **Taking Precautions Against Viruses**



### **Taking Corrective Action**



### **Checking for Viruses**



### **Managing Virus Definitions**



### **Reporting Results**



### **Customizing Norton AntiVirus**



### **Customizing Scanner Options**



### **Customizing Automatic Protection**



### **Customizing Alerts**



### **Customizing the Activity Log**



### **Customizing Inoculation**



### **Customizing Password Protection**



### **Modifying the Exclusions List**



### **Viewing the Exclusions List**



## **Troubleshooting**



## **Commands**



## **Dialog Boxes**



## **Glossary**



## **Keyboard Shortcuts**



## **Credits**



# **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Taking Precautions Against Viruses**



**Taking Corrective Action**



**Checking for Viruses**



**Managing Virus Definitions**



**Reporting Results**



**Customizing Norton AntiVirus**



**Troubleshooting**



**Troubleshooting Networks**



**Commands**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**



# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



## **Taking Precautions Against Viruses**



## **Taking Corrective Action**



## **Checking for Viruses**



## **Managing Virus Definitions**



## **Viewing the Virus List**



## **Updating the Virus List**



## **Reporting Results**



## **Customizing Norton AntiVirus**



## **Troubleshooting**



## **Commands**



## **Dialog Boxes**



## **Glossary**



## **Keyboard Shortcuts**



## **Credits**



# **Norton AntiVirus Help Contents**



## **QuickHelp**



## **Procedures**



## **Taking Precautions Against Viruses**



## **Taking Corrective Action**



## **Checking for Viruses**



## **Managing Virus Definitions**



## **Reporting Results**



## **Using the Activity Log**



## **Using the Infection Log**



## **Customizing Norton AntiVirus**



## **Troubleshooting**



## **Commands**



## **Dialog Boxes**



## **Glossary**



## **Keyboard Shortcuts**



## **Credits**



## **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Scan Menu**



**Tools Menu**



**Reports Menu**



**Help Menu**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**





## **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Scan Menu**



**Selected Drives**



**File**



**Directory**



**Exit**



**Tools Menu**



**Reports Menu**



**Help Menu**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**



# **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Scan Menu**



**Tools Menu**



**Options**



**Scheduler**



**Inoculation**



**Virus List**



**Reports Menu**



**Help Menu**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**



# **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Scan Menu**



**Tools Menu**



**Reports Menu**



**Activity Log**



**Infection Log**



**Help Menu**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**



# **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Scan Menu**



**Tools Menu**



**Reports Menu**



**Help Menu**



**Contents**



**Procedures**



**Commands**



**QuickHelp**



**How to Use Help**



**About Help**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Credits**

 **Norton AntiVirus Help Contents** **QuickHelp** **Procedures** **Commands** **Dialog Boxes** **Options Settings** **Activity Log** **Infection Log** **Virus List** **Inoculation** **Scheduler** **Glossary** **Keyboard Shortcuts** **Credits**





Inoculation



Scheduler



Glossary



Keyboard Shortcuts



Credits

 **Norton AntiVirus Help Contents** **QuickHelp** **Procedures** **Commands** **Dialog Boxes** **Options Settings** **Activity Log** **Activity Log** **Clear Activity Log** **Activity Log Filter** **Infection Log** **Virus List** **Inoculation** **Scheduler** **Glossary** **Keyboard Shortcuts** **Credits**





## **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Dialog Boxes**



**Options Settings**



**Activity Log**



**Infection Log**



**Infection Log Settings**



**Infection Log Filter**



**Virus List**



**Inoculation**



**Scheduler**




**Glossary**




**Keyboard Shortcuts**



**Credits**

 **Norton AntiVirus Help Contents** **QuickHelp** **Procedures** **Commands** **Dialog Boxes** **Options Settings** **Activity Log** **Infection Log** **Virus List** **Virus List** **Inoculation** **Scheduler** **Glossary** **Keyboard Shortcuts** **Credits**

 **Norton AntiVirus Help Contents** **QuickHelp** **Procedures** **Commands** **Dialog Boxes** **Options Settings** **Activity Log** **Infection Log** **Virus List** **Inoculation** **Inoculation** **Scheduler** **Glossary** **Keyboard Shortcuts** **Credits**



## **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Dialog Boxes**



**Options Settings**



**Activity Log**



**Infection Log**



**Virus List**



**Inoculation**



**Scheduler**



**Scheduler**



**Glossary**



**Keyboard Shortcuts**



**Credits**

 **Norton AntiVirus Help Contents** **QuickHelp** **Procedures** **Commands** **Dialog Boxes** **Glossary** **Glossary** **Keyboard Shortcuts** **Credits**



## **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Dialog Boxes**



**Glossary**



**Keyboard Shortcuts**



**Keyboard Shortcuts**



**Credits**



## **Norton AntiVirus Help Contents**



**QuickHelp**



**Procedures**



**Commands**



**Dialog Boxes**



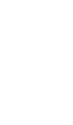
**Glossary**



**Keyboard Shortcuts**



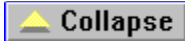
**Credits**



**Credits**



# Norton AntiVirus Help Contents



## QuickHelp

[Quickhelp](#)

[Checkup](#)

## Procedures

### Taking Precautions Against Viruses

[Setting up Automatic Protection](#)

[Monitoring During Startup](#)

[Monitoring the Files You Use](#)

[Monitoring Floppy Disks](#)

[Monitoring for Unknown Viruses](#)

[Inoculating Files](#)

[Monitoring for Virus-Like Activities](#)

### Taking Corrective Action

[Removing Viruses from Memory](#)

[Removing Viruses from Files and Boot Records](#)

[Restoring System Files](#)

[Resolving Inoculation Issues](#)

[Responding to Virus-Like Activity Alerts](#)

[Restarting a Halted Computer](#)

[Using a Rescue Disk](#)

### Checking for Viruses

[Scanning Drives](#)

[Scanning Files](#)

[Scanning a Directory](#)

[Scheduling Scans](#)

### Managing Virus Definitions

[Viewing the Virus List](#)

[Updating the Virus List](#)

### Reporting Results

[Using The Activity Log](#)

[Using The Infection Log](#)

### Customizing Norton AntiVirus

[Customizing Scanner Options](#)

[Customizing Automatic Protection](#)



[Customizing Alerts](#)  
[Customizing the Activity Log](#)  
[Customizing Inoculation](#)  
[Customizing Password Protection](#)  
[Modifying the Exclusions List](#)  
[Viewing the Exclusions List](#)

## **Troubleshooting**

[Troubleshooting Networks](#)

## **Commands**

### **Scan Menu**

[Selected Drives](#)  
[File](#)  
[Directory](#)  
[Exit](#)

### **Tools Menu**

[Options](#)  
[Scheduler](#)  
[Inoculation](#)  
[Virus List](#)

### **Reports Menu**

[Activity Log](#)  
[Infection Log](#)

### **Help Menu**

[Contents](#)  
[Procedures](#)  
[Commands](#)  
[QuickHelp](#)  
[How to Use Help](#)  
[About Help](#)

## **Dialog Boxes**

### **Options Settings**

[Options Dialog Box](#)  
[Scanner Settings Reference](#)  
[Scanner Advanced Settings](#)  
[Auto-Protect Settings Reference](#)  
[Auto-Protect Advanced Settings](#)  
[Auto-Protect Startup Settings](#)

[Auto-Protect Virus Sensor Settings](#)

[Alerts Settings Reference](#)

[Alert Others](#)

[Activity Log Settings Reference](#)

[Exclusions Settings Reference](#)

[Add/Edit Exclusion](#)

[Inoculation Settings Reference](#)

[Password Settings Reference](#)

[Set/Change Password](#)

[General Settings Reference](#)

## **Activity Log**

[Activity Log Settings Reference](#)

[Clear Activity Log](#)

[Activity Log Filter](#)

## **Infection Log**

[Infection Log](#)

[Infection Log Filter](#)

## **Virus List**

[Virus List](#)

## **Inoculation**

[Inoculation Settings Reference](#)

## **Scheduler**

[Scheduler](#)

## **Glossary**

[Glossary](#)

## **Keyboard Shortcuts**

[Keyboard Shortcuts](#)

## **Credits**

[Credits](#)



## **Keyboard Shortcuts**

Keyboard Shortcuts



## Commands

### Scan Menu

[Selected Drives](#)

[File](#)

[Directory](#)

[Exit](#)

### Tools Menu

[Options](#)

[Scheduler](#)

[Inoculation](#)

[Virus List](#)

### Reports Menu

[Activity Log](#)

[Infection Log](#)

### Help Menu

[Contents](#)

[Procedures](#)

[Commands](#)

[QuickHelp](#)

[How to Use Help](#)

[About Help](#)

## Dialog Boxes

### Options Settings

[Options Dialog Box](#)

[Scanner Settings](#)

[Scanner Advanced Settings](#)

[Auto-Protect Settings](#)

[Auto-Protect Advanced Settings](#)

[Auto-Protect Startup Settings](#)

[Auto-Protect Virus Sensor Settings](#)

[Alerts Settings](#)

[Alert Others](#)

[Activity Log Settings](#)

[Exclusions Settings](#)

[Add/Edit Exclusions](#)

[Inoculation Settings](#)

[Password Settings](#)

[Set/Change Password](#)

General Settings

**Activity Log**

Activity Log Settings

Clear Activity Log

Activity Log Filter

**Infection Log**

Infection Log

Infection Log Filter

**Virus List**

Virus List

**Inoculation**

Inoculation

**Scheduler**

Scheduler



## Procedures

### Procedures

#### Taking Precautions Against Viruses

- [Setting up Automatic Protection](#)
- [Monitoring During Startup](#)
- [Monitoring the Files You Use](#)
- [Monitoring Floppy Disks](#)
- [Monitoring for Unknown Viruses](#)
- [Inoculating Files](#)
- [Monitoring for Virus-Like Activities](#)

#### Taking Corrective Action

- [Removing Viruses from Memory](#)
- [Removing Viruses from Files and Boot Records](#)
- [Restoring System Files](#)
- [Resolving Inoculation Issues](#)
- [Responding to Virus-Like Activity Alerts](#)
- [Restarting a Halted Computer](#)
- [Using a Rescue Disk](#)

#### Checking for Viruses

- [Scanning Drives](#)
- [Scanning Files](#)
- [Scanning a Directory](#)
- [Scheduling Scans](#)

#### Managing Virus Definitions

- [Viewing the Virus List](#)
- [Updating the Virus List](#)

#### Reporting Results

- [Using the Activity Log](#)
- [Using the Infection Log](#)

#### Customizing Norton AntiVirus

- [Customizing Scanner Options](#)
- [Customizing Automatic Protection](#)
- [Customizing Alerts](#)
- [Customizing the Activity Log](#)
- [Customizing Inoculation](#)
- [Customizing Password Protection](#)
- [Modifying the Exclusions List](#)

[Viewing the Exclusions List](#)

**Troubleshooting**

[Troubleshooting Networks](#)



## Scan Menu

Selected Drives

Directory...

File...

Exit





## How to Use Help

This command displays information on how to use the Windows help system.

