Contact Information

The developers of Vet have always aimed to provide straightforward software that will operate in the background until a virus attempts to infect and damage your PC.

To become a [Registered Vet User](#) talk to our sales department or fill in and return the registration card to your nearest Vet supplier.

AUSTRALIA:

Cybec Pty Ltd,

1601 Malvern Rd, Glen Iris 3146, Victoria, Australia. ACN:007229361

Melbourne Customers Phone Support 9825 5656 (8:30 AM to 6:00 PM)

Non Melbourne Phone Support 1800 807 062 (8:30 AM to 6:00 PM)

Fax (+61) 03 9886 0844   Email support@vet.com.au   Web: http://www.vet.com.au

Phone Sales 1300 364 750   Email info@vet.com.au

U.K. & EUROPE:

Vet Anti-Virus Software Ltd,

342 Glossop Road, Sheffield, S10 2HW, England.

Phone (+44) 0114 275 7501 Fax (+44) 0114 275 7508

Email support@vetavs.co.uk

Web www.vetavs.co.uk

NEW ZEALAND:

Vet Anti-Virus Software Ltd,

Level 4, 10-12 Scotia Place, Auckland, NZ.

P.O. Box 7429, Wellesley Street, Auckland, NZ

Phone(+64) 9 309 3281 Fax (+64) 9 309 3287

Freecall 0800 838 691

Email sales@vetavs.co.nz

BELGIUM, HOLLAND & LUXEMBOURG:

Data Results Nederland BV

Industrieweg 30, NL-4283 GZ   Giessen, The Netherlands

Phone +31 (0)183 449944 (Support: 08:30 to 17:30)

Fax   +31 (0)183 449045

Email support@dataresults.nl

Web www.dataresults.nl

MALAYSIA

Vet Anti-Virus Software Sdn Bhd

21-3A Jalan SS 23/15, Taman SEA, Petaling Jaya, 47400 Selangor, Malaysia.

Phone (+60) 03 705 1103 (8:00 AM to 7:00 PM MST)

Fax (+60) 03 705 1203

Email info-asia@vet.com.au

USA: Ontrack Data International Inc.

6321 Bury Drive, Eden Prairie, MN 55346
Phone: General: (+1) 800 872 2599 Sales: (+1) 612 937 5161 Support: (+1) 612 937 2121
Facsimile: (+1) 612 937 5815
Email: sales@ontrack.com
WWW: http://www.ontrack.com

Ontrack US Offices

Los Angeles: 940 South Coast Drive, Suite 225, Costa Mesa, CA 92626
Toll Free: (+1) 800 872 2599 Phone: (+1) 714 641 0530
San Jose: 2001 Gateway Place, Suite 750 West, San Jose, CA 95110-1013
Toll Free: (+1) 800 872 2599 Phone: (+1) 408 573 9592
Washington DC: 2000 Corporate Ridge, 8th Floor, McLean, VA 22102
Toll Free: (+1) 800 872 2599 Phone: (+1) 703 821 8101

Germany: Ontrack Data Recovery GmbH.

Germany: Ontrack Data Recovery GmbH
Phone: Toll Free: 00 800 10 12 13 14 Sales: +49 (0)7031 644 150
Facsimile: +49 (0)7031 644 100
Email: sales@ontrack.de
WWW: http://www.ontrack.com

London: Ontrack Data Recovery Europe Ltd.

The Pavilions, 1 Weston Rd, Kiln Lane, Epsom, Surrey KT17 1JG England.
Phone: Toll Free France: 0 800 90 72 42 Toll Free Europe: 0 800 24 39 96
Office: (+44) 0 1372 741 999 Tech Support (+44) 0 1372 747 414
Facsimile: (+44) 0 1372 747 074
Email: WWW: sales@ontrack.com http://www.ontrack.com

Why Should You Become a Registered Vet User.

This copy of Vet provides protection against all viruses that are known to be in the wild at the time of production. Unfortunately new viruses and new varieties of existing viruses appear on an almost weekly basis. Registered Vet Customers get a comprehensive solution for protection against viruses.

The services and benefits of becoming a registered Vet customer depend on the country where Vet was purchased. Services that are commonly offered are listed below.

1) A full set of user manuals - comprehensive installation and usage details (manuals are available in some boxes of Vet, from the Web site and are also on Vet CDs)

2) Additional installation options for networks and systems administrators

3) Access to the Vet internet web site and Bulletin board service - used to provide updates and general virus information

4) Free unlimited Email and phone support (See the [Contact](#) page for the support hours)

5) 48 Hour fixes - If you discover a new virus that Vet does not clean we will provide a solution within 48 hours of receiving a copy of the virus

6) Employee Protection - Any company holding a Vet site licence, that is a licence to install Vet on every PC in the work place, may allow all employees to install Vet on their home-use computers, free of charge.

7) On Site Support - Charges normally apply, but we are committed to supporting our registered Vet users

So, please return the registration card with the appropriate fee or talk to your [local Vet sales team.](#)

Command Line Switches

Command line switches can be used by typing in the full path and filename (ie. C:\VET\VET95 or C:\VET\VETNT) and adding any of the command line switches that are listed below.

Long-form command line options

All options are able to be abbreviated providing the abbreviation is unambiguous and three or more characters in length.

Scanning

/display=full - default, display the main GUI.

/display=progress - show a progress meter of the scan.

/display=notify - hide the progress meter unless infection detected.

/display=none - do not show anything.   (replaces /&)

/ext - specify a list of extensions to scan.

Multiple extensions can be delimited like so: /ext="exe,dll,sys" or

/ext=exe,dll,sys;

/ext=* - scan all files

/ext   - scan the default extensions.   (replaces /.=)

/resume - begin scan from where the last scan to use /maxfiles ended.

 /resume now resumes a user-aborted scan also.   (replaces /P)

/maxfiles - specify the number of files to scan. eg.

  /maxfiles=1000   (replaces /M=)

/memoryscan - scan memory.

/nomemoryscan - do not scan memory.

/bootscan - scan the boot sector(s).

/nobootscan - do not scan the boot sector(s).   (replaces /!S)

/renamed - scan renamed files (*._??).

/norenamed - do not scan renamed files.   (replaces /!V)

/fast - scans entry point of each file.

/full - scans every byte of each file.   (replaces /F and /!F)

/sub - includes subdirectories in the scan.

/nosub - does not include subdirectories.   (replaces /R)

/progressive - triggers the progressive scan (options defined within the program).

/autoscan - equivalent to /progressive (redundant as of 9.60)

Actions
The Action options will specify one of the following values...
 clean, rename, reportonly, delete
/infected= - specify the action to be taken on infected files.

/infected=clean
/infected=rename
/infected=delete
/infected=reportonly   (replaces /!C, /U, and /Z)

/suspect= - specify the action to be taken on suspected infections.
/suspect=rename
/suspect=delete
/suspect=reportonly   (replaces /O, and /Y)
/macro= - specify the action to be taken on infected documents.
/macro=clean
/macro=reportonly

Reporting
/report= - specifies how much information is to be output.
Current available values are:
/report=infected   - report only infected files.

/report=all   - report all files scanned show all files scanned.   (replaces /E)

/logfile - use the default log filename.
/logfile="filename" - specify a log filename.
/nologfile - do not write to a log.   (replaces /L and /L=)

Miscellaneous
/exit - VET is to exit on completion of the scan.   (replaces /X)

/help - print the command line help. The current /? switch will be kept as it is a fairly standard option.

/cancel - default, allow cancelling of the scan.

/nocancel - disable cancelling of the scan

Any path or logfile name specified on the command line that contains any of the following characters
MUST be enclosed in quotes =   ;   -   /   (and white space)

Password

The password can be invoked by either selecting **Options** | **Password protect options**, or **Tools** | **Emergency.**

Options | Password protect options:

This feature is in Vet95 and VetNT because many system administrators asked that we provide password protection to stop unauthorised alterations to the Vet configuration. The password protection can be enabled by selecting Options | Password Protect Options and entering a password. This option can also be set while configuring a network installation so that the password will be the same on every workstation that is updated from the server.

The password protection of the Options menu can be disabled by selecting Options | Password Protect Options and entering the correct password. (The password protection for the Tools | Emergency menu is not affected by disabling the Options menu password).

Tools | Emergency:

The re-installation of an old template could cause files to be lost if the drive structure was changed after the template was made. For this reason the ability to re-install templates is protected with a password.

The Emergency Password dialog will appear when the **Tools | Emergency** functions menu is selected. It prompts for a password to allow access to the emergency options, and will continue to prompt until the correct password is entered.

NOTE: If no password was set when Vet was installed the default password **VET** will be used. Enter the password then select OK

The password entered is case dependant, so an "a" is not the same as an "A".

Scan Type

Full Scan: Causes Vet to examine every byte of a file when checking it for viruses.   This will increase the time Vet takes to check your files and disks and is only recommended when you have had (or suspect you may have) a virus. You can choose either Full Scan or Fast Scan but not both.

Fast Scan: Causes Vet to examine the entry point and selected areas of a file when checking it for viruses.   This is the preferred mode for routine checking of your files and disks as it is both an extremely fast and extremely accurate check for viruses. You can choose either Full Scan or Fast Scan but not both.

[Include subfolders](#)

[Skip renamed files](#)

[Show network drives](#)

Include Subfolders/Skip renamed files/ Show network drives

Include subfolders: Causes Vet to check the subdirectories or subfolders of the current directory or folder.

Skip renamed files: Causes Vet not to check those files which have been renamed by Vet during previous scans. Renaming will occur if the default in **Options** | **Program | Actions** is set to Rename and a suspect file is found. The file extension will be changed so that the first letter will be an underscore. So .exe will become ._xe.

Show network drives: If your PC is attached to a network and this option is enabled the network drives will be displayed (and can be scanned) in the Browser.

Enabling this option will also cause files that are stored on network drives to be scanned by the resident protection before they are used by the PC.

File Types to Scan

All files: Causes Vet to check *every* file it encounters for viruses. You can choose either All files or Files <u>o</u>f these types, but not both.

Files of these types: Causes Vet to check files that it considers to be executable (or 'runable'). By default Vet considers files with
the .XLS, .XLT, .BIN, .COM, .DLL, .DRV, .EXE, .OVL, .DOC, .DOT and .SYS extensions to be executable. You can choose either A<u>l</u>l files or E<u>x</u>ecutable only but not both.

<u>A</u>dd: Allows you to add to the list of file extensions Vet will consider executable. With the advent of Macro language viruses, it is now possible for a file with any extension to contain a virus that can infect your PC.   Selecting this button causes an input window to appear.   You then have the opportunity to enter the new file name extension in the type-in box.

<u>D</u>elete: If you select a file extension from the displayed list and press this button, the file extension will be removed from the list that Vet considers executable.

Default: Restores the default list of file extensions Vet considers executable.
(.XLS, .XLT, .BIN, .COM, .DLL, .DRV, .EXE, .OVL, .DOC, .DOT and .SYS extensions)

Add Vet to 'right-click' menus for these file types: If this option is selected and you are using MS explorer (or other navigation tool) you can select a file, directory or drive, right click the mouse button, and Vet will scan your selection.

Infected & Suspect Program Files:

The following mutually exclusive options are available for actions dealing with infected files.

STOP!   If you chose for files to be **Clean**ed and a file has been infected with an [overwriting virus](), Vet will offer to ignore, rename or delete the file, as no disinfection is possible.   By default Vet will offer to delete the file.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Clean: Causes Vet to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, Vet will **Delete** the file, as no disinfection is possible

Rename: Causes Vet to change the first letter of the extension of any file infected with a virus to an underscore '_' (.EXE becomes ._XE).   This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irreversibly any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

> **STOP!**   Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Rename: Causes Vet to change the first letter of the extension of any file suspected of infection with a virus to an underscore '_' (.EXE becomes ._XE).   This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

> **STOP!**   Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Overwriting Viruses

Most viruses are careful not to destroy the infected file, but overwriting viruses overwrite part of the infected file, so that it will no longer operate.   However, this makes these viruses extremely obvious, so they are unlikely to spread far.

The Zeroto-0, or Australian 403 virus, is of this type.   When an infected file is run, the virus searches for an uninfected .COM file and replaces it with a 403 byte file which only contains the virus.   The original file is destroyed, so infected files appear to run, but do nothing.

Suspect Program Files:

The following mutually exclusive options are available for dealing with files suspected to contain a virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Rename: Causes Vet to change the first letter of the extension of any file suspected of infection with a virus to an underscore '_' (.EXE becomes ._XE).   This allows you to keep the file for further examination, without the risk of accidentally running it.

Delete: Delete causes Vet to delete irrevocably any file that it finds has been infected with a virus. The file is first overwritten with 'D's and then set to zero length, so no recovery of the deleted files is possible.

> **STOP!**   Use this option with caution, as there is no possibility of recovering files deleted in this manner.

Infected Document Files:

The following mutually exclusive options are available for dealing with documents or spread sheets that contain a macro virus.

Windows97 has a different file structure to the documents and spreadsheets created by earlier versions of Word and Excel. This new structure (VBA5) requires a different method for detecting and cleaning the viruses.

The good news is that all of this is now transparent to you the user!

Vet95 and VetNT can automatically detect and clean all Word97 macro viruses as well as the Laroux Excel macro virus.

Report only: Causes Vet to report, but not attempt to clean, infected files.

Clean: The file will be cleaned, and if possible, returned to working order.

Reporting

This dialog controls what will be displayed in the Report window and written to the log file.

All files scanned: Causes Vet to display on a separate line the name of each file it tests (which in turn causes the name of every file tested to be written to the log file, regardless of whether it had a virus or not). This is useful in explicitly identifying which files are *not* infected (Vet uses a separate line for each infected file).

Infected or suspect: Causes Vet to report on a separate line the name of each file it finds to be suspected or infected.

The *All files scanned* and *Infected or suspect* options tell Vet which file names are to be listed in the Report window. These two options are mutually exclusive.

Write log: The name of the log file to which all scan results are written is displayed in the type-in box. The location of the log file can be changed using the Browse button to select an existing file or allow the entry a new file name.

Cumulative report: If this option is enabled the results of each scan will be stored cumulatively in the log file. If it is NOT enabled the log file will be cleaned and overwritten each time a scan is performed.

Limit log size to: Once you perform a scan and the file becomes larger than (the default) 32Kb it will automatically be truncated by removing the oldest information first.

Suppress 'Out-of-date' warning

NOTE: As the log file has to be able to be edited in DOS the name MUST NOT contain: spaces, unprintable characters or contain sub-directory names longer than eight characters.

Display 'Out-of-date' Warning

Around four months after you have installed the latest copy of Vet it will display a message to let you know that it is now out of date and to remind you to load the next upgrade. If you are not able to load the next upgrade this option allows you to disable the message.

This option can be enabled/disabled by opening Vet and selecting Options | Program | Reporting and modifying the 'Suppress Out-Of-Date option'.

Boot Sectors

This dialog sets up the defaults for the treatment of boot sectors.

Scan boot sectors Allows Vet to scan boot sectors.   Turning this option off causes all the other options in this dialog box to become inactive.

Consider a boot sector bad if it contains: The following options tell Vet how to define a bad boot sector; The first option gives adequate protection, whilst the last gives an extremely high level of protection. The three levels of protection are mutually exclusive. i.e. only one can be chosen.

> **Known viruses only** Causes Vet to consider a boot sector bad only if it contains a known virus.

> **Invalid boot sector or known virus** Causes Vet to consider a boot sector bad if it contains an invalid boot sector or a known virus.

> **Unknown or invalid boot sector, or known virus**

STOP! Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the Vet support line if you have any questions. Causes Vet to consider a boot sector bad if it contains an unknown or invalid boot sector or a known virus.

Replace bad boot sector Causes Vet to replace bad boot sectors.   Vet will always warn you before replacing a boot sector.

Check for large IDE driver To determine if a large drive is present Vet uses direct port I/O to read the Extended Boot sector. This will not work on all PCs. The **Check for large IDE driver** allows users to disable this test if it causes problems on their system. This option is not available in VetNT.

Memory (for Vet 95 Only)

Enable Memory Scanning

This dialog enables Vet to monitor resident memory for viruses.

If another anti-viral program is running it may cause false alarms as virus templates may be detected from the other program.

Start-Up

This option allows you to configure how Vet will perform the scans that are performed when you start or reboot your computer.

Run Vet automatically when Windows starts up

This option will enable or disable the Start-up scan option.

Start-up Command

Perform progressive scan (recommended)

> This will enable a progressive test which will begin the next test where the last one finished, thus, over a period of days/weeks the entire hard drive will be checked.

Customised Start-up command

> This option allows you to configure your own scan using the <u>Vet command line switches</u>.

A summary of the option that you have selected will be displayed at the bottom of the dialog.

The <u>Configure Progressive Scan button</u> allows you to modify the way the progressive scan is performed.

Command Line Switches

Command line switches can be used by selecting **Start | Run…**, typing in the full path and filename (ie. C:\VET\VET95 or C:\VET\VETNT) and adding any of the command line switches that are listed below.

The following switches are available:

Long-form command line options

All options are able to be abbreviated providing the abbreviation is unambiguous and three or more characters in length.

Scanning

/display=full - default, display the main GUI.
/display=progress - show a progress meter of the scan.
/display=notify - hide the progress meter unless infection detected.
/display=none - do not show anything.   (replaces /&)

/ext - specify a list of extensions to scan.
Multiple extensions can be delimited like so: /ext="exe,dll,sys" or
/ext=exe,dll,sys;
/ext=* - scan all files
/ext   - scan the default extensions.   (replaces /.=)

/resume - begin scan from where the last scan to use /maxfiles ended.
 /resume now resumes a user-aborted scan also.   (replaces /P)

/maxfiles - specify the number of files to scan. eg.
  /maxfiles=1000   (replaces /M=)

/memoryscan - scan memory.
/nomemoryscan - do not scan memory.

/bootscan - scan the boot sector(s).
/nobootscan - do not scan the boot sector(s).   (replaces /!S)

/renamed - scan renamed files (*._??).
/norenamed - do not scan renamed files.   (replaces /!V)

/fast - scans entry point of each file.
/full - scans every byte of each file.   (replaces /F and /!F)

/sub - includes subdirectories in the scan.
/nosub - does not include subdirectories.   (replaces /R)

/progressive - triggers the progressive scan (options defined within the program).
/autoscan - equivalent to /progressive (redundant as of 9.60)

Actions

The Action options will specify one of the following values...
 clean, rename, reportonly, delete

/infected= - specify the action to be taken on infected files.
/infected=clean
/infected=rename
/infected=delete
/infected=reportonly   (replaces /!C, /U, and /Z)

/suspect= - specify the action to be taken on suspected infections.
/suspect=rename
/suspect=delete
/suspect=reportonly   (replaces /O, and /Y)
/macro= - specify the action to be taken on infected documents.
/macro=clean
/macro=reportonly

Reporting
/report= - specifies how much information is to be output.
Current available values are:
/report=infected   - report only infected files.
/report=all   - report all files scanned show all files scanned.   (replaces /E)

/logfile - use the default log filename.
/logfile="filename" - specify a log filename.
/nologfile - do not write to a log.   (replaces /L and /L=)

Miscellaneous
/exit - VET is to exit on completion of the scan.   (replaces /X)

/help - print the command line help. The current /? switch will be kept as it is a fairly standard
option.

/cancel - default, allow cancelling of the scan.
/nocancel - disable cancelling of the scan

Any path or logfile name specified on the command line that contains any of the following characters
MUST be enclosed in quotes =   ;   -   /   (and white space)

Progressive Scan Properties

This dialog allows you to configure how the start-up scan will be performed and what will be reported.

Display

Progress of the scan: This will display Vet and show you the details as the scan is performed.

Nothing unless infected: Vet will not appear unless it has found a problem with a file.

Number of Files to Scan

First boot: This is the number of files that will be scanned when you first start your PC for the day.

Reboots: This is the number of files that will be scanned if you re-boot your PC throughout the day.

Log File

Write log file: By selecting this option you can either select the browse button to specify the name of the log file, or you can type in the path and file name that you wish to call the log file.

Allow Cancellation of Progressive

If this option is NOT selected (NOT ticked) you will not be able to stop the scan until it is finished.

Options | Resident Protection

The Vet suite includes memory resident programs to automatically check files and floppy disks for viruses. Settings for these programs are controlled by this dialog.

The Resident Protection Options dialog is initiated by selecting **Options** | **Resident Protection** from the menu. Each of the dialogs can be entered by selecting the appropriate tab at the top of the dialogs.

Enabling

[More information](#)

Floppy boot sectors

[More information](#)

File Monitoring

[More information](#)

File virus action

[More information](#)

Macro virus action

[More information](#)

Reporting

[More information](#)

Enabling

Enable resident floppy disk boot sector protection

You can configure the floppy disk protection by selecting Options | Resident protection | Floppy Boot Sectors. [Resident floppy protection settings](#)

Enable resident file monitor (file & macro protection)

This will allow Vet to automatically check files, documents and spreadsheets for viruses as they are accesses by Windows.

> [File monitoring](#)
>
> [File virus actions](#)
>
> [Macro virus actions](#)

Floppy Boot Sector

This dialog controls the checking of floppy boot sectors for viruses.   You may choose the level of protection required from the three (mutually exclusive) options.   The first option gives adequate protection, whilst the last gives an extremely high level of protection. These options will also contain a message to note if this option is currently loaded.

A known virus   Causes Vet to consider a boot sector bad only if it contains a known virus. This is the default level of protection.

An invalid boot, sector or known virus   Causes Vet to consider a boot sector bad if it contains an invalid boot sector or a known virus.

An unknown or invalid boot sector, or known virus   This option causes Vet to consider a boot sector bad if it contains an unknown or invalid boot sector or contains a known virus.

    STOP!   Replacing unknown boot sectors may cause problems with some backup programs and copy-protected software. You should only use this setting if you are aware of the potential problems. Please call the Vet support line if you have any questions.

Replace any boot sector considered bad   Causes Vet to replace bad boot sectors.   Vet will always warn you before replacing a boot sector.

File Monitoring

This dialog controls which events will trigger Vet's automatic file monitors to scan files.   There are three events where files may be monitored for viruses.   You may enable as many of these options as you wish as they are not mutually exclusive.

An infected file may trigger more than one of the following options. A warning will be issued from each of the options that is activated, so it is possible for a single infected file to create multiple warnings.

Monitor Activation

If the file is infected with a virus it may activate as soon as the file is opened (macro viruses normally infect normal.dot when the infected file is opened). For this reason Opening will automatically be enabled when you select either Executing or Closing if you are using Vet95. VetNT can be fully configured and will allow any configuration to be set by the user.

Executing programs   If a virus is found when a Windows application is run the resident protection will prevent the file from running.   If the resident protection only suspects a virus is present you will be given the choice of whether or not to run the file.

Opening files   Files with extensions specified in the *File types to scan* box of the Options | Program | File types menu are checked for viruses on opening. If a virus is found, you have the option of proceeding.

Closing files Files with extensions specified in the *File types to scan* box of the Options | Program | File Types menu are scanned for viruses on closing.   If a virus is found the filename and the name of the virus will appear in the Report window and the log file if it is enabled.

Scan Type

Fast Scan: Causes Vet to examine the entry point and selected areas of a file when checking it for viruses.   This is the preferred mode for routine checking of your files and disks as it is both an extremely fast and extremely accurate check for viruses. You can choose either Full Scan or Fast Scan but not both.

Full Scan: Causes Vet to examine every byte of a file when checking it for viruses.   This will increase the time the resident protection takes to check your files and disks and is only recommended when you have had (or suspect you may have) a virus.

Scan Network Files

The resident protection can be configured to scan all files that are passed to, or are copied from, the network drive by enabling the Options | Resident Protection | File Monitoring | Scan Network Files. Once this is set every file that is moved to or from the network drive, as you go about your daily business, will be checked for viruses.

File Virus Actions

Action - Infected Files

Report only: Causes Vet to report, but not attempt to clean, infected files.

Report & deny access: Causes Vet to report when an infected file is detected and to lock the file so that it may not be used by other programs.

Clean file: Causes Vet to attempt to disinfect virus-infected files, returning the files to working order. If the file has been infected by an overwriting virus, Vet will delete the file, as no disinfection is possible

Action - Suspected Files

Report only: Causes Vet to report, but not attempt to clean, infected files.

Report & Deny access: Causes Vet to report when an infected file is detected and to lock the file so that it may not be used by other programs.

If this option is viewed form the Vet program is will also have a note to indicate if the option is currently loaded and active.

Macro Virus Actions

By default Vet macro monitoring will check documents and spreadsheets for macro viruses.

A message is included on the bottom of the dialog to let you know if the macro resident protection is currently loaded.

Action - Infected Documents

Select on of the following options to determine what the macro resident protection will do when it detects a Word or Spreadsheet document that is infected with a virus.

Report Only

> Causes the macro resident protection to report when a virus is detected but not attempt to clean the file. Vet will still allow the document to be used so it is likely that the virus will infect your PC. We recommend you do not use this option.

Report and Deny Access

> When an infected document or spreadsheet is detected Vet will report that a virus has been found and not allow you to access the file.

Clean Document

> When an infected document or spreadsheet is detected Vet will remove the virus, return the file to working order and allow access to the file.

Reporting

Write log file

Selecting this option will cause a log file to be written when suspect or infected files are detected by the resident file protection. The log file will record the filename and path of any infected files, and results of Vet's attempt to clean the files.

SMTP E-Mail Alerting

This dialog allows you to configure the details of the SMTP email message that will be sent when a virus is detected.   At the end of the report that is produced during an on-demand scan (when you open Vet and start scanning files), there is a summary of the results. If a virus has been found this summary will be copied into the body of a mail message and sent to the address in the TO: field below.

If all of the fields are grey Email alerting has not been enabled on the Alerting.

Mail Configuration:

> **Mail Server:** This is the Name or TCP/IP address of your mailserver. Please call your Network Administrator if you are unsure what to enter.
>
> **From:** Enter your email address. This is so that when the email is sent it is easy to work out which PC it has come from.
>
> **To:** Enter the email address of your computer support person that you want the message sent to.

Subject:

> This is the Subject line in the email message that will be sent.

Test (send e-mail):

> This will send a test message to the person specified in the TO: field. This button is designed to allow you to test that the details you have entered will work when a virus is detected.

Alerting

This dialog allows to enable/disable the sending of an Email message when a virus is detected. (Currently email messages can only be sent via SMTP mail protocol)

On-demand scanner:

By selecting (ticking) the "Alert administrator via e-mail when virus found" option you can send an Email when a virus is detected after you have opened Vet and started scanning files. You must also configure the [SMTP Email tab](#) with the details required to send the message.

Resident Protection: (Only available in Vet for Windows NT version 9.5x)

By selecting (ticking) the "Display message box when virus found" option you will be notified if a virus is detected by the resident protection as you go about your daily tasks.

You must also configure the [SMTP Email tab](#) with the details required to send the message.

Confirm Configuration Selections

This dialog will display a list with all of the options that the installation intends to install Vet with. If you wish to change the settings; select the <Back button until you see the dialog with the option that you wish to change, modify the option and then select Next> until the Confirm Configuration Sections dialog is once again displayed. Select the Next> button to accept the configuration and complete the installation.

Online Registration For New Customers

If you are installing Vet for the first time and are not yet a registered Vet user you can select "Yes, please register me now" and, provided you have a modem and Internet access, you will be connected to the registration section of the Vet web page. Once you have filled in all the details, select the submit button to send the information to us. Your Vet Customer Number will be displayed. Copy down this number as you will need it to get access to the download area. You can record it by selecting Options | Options Wizard and filling in the Customer Details dialog. Once you have entered your details here you can view them at any time by selecting Help | About...

If you wish to register at a later date then select "No, do not register now" and select Run | Programs | Vet Anti-Virus for Windows | Web Update & Tech Support, then select Online Registration and enter your details when you are ready to register.   NOTE: It is not necessary to enter your customer number to successfully complete the Vet installation. It is possible to enter your customer number at a later date by opening Vet and selecting Options | Options Wizard and running through all of the screens till you find the customer details dialog.

Once you have entered your customer number and other details it will be displayed in the About box (Open Vet and select Help | About...).

You will need to know these details if you call the Vet Technical Support department.

'Read-me' Help File

Setup can display a 'Read-me' help file, which will include late-breaking information that has not made it into the manual. The 'Read Me' help file will also give a summary of all the changes that have been made since the last version of Vet.

By selecting the *Yes please display the 'Read Me' file* the Readme help file will be displayed during the installation of Vet.

User Identification

Please enter your name, the name of your company or organisation and you customer number. Customer numbers are issued to registered customers, so if you have only just purchased Vet and sent in your registration card you may not have this number yet.

You can enter these details at a later stage by opening Vet and selecting Options | Options Wizard and moving through until the User Identification dialog is displayed.

Once you have entered your details here they will be displayed if you open Vet and select Help | About. This will make it easier to find your customer number if you call us for technical support.

Future versions of Vet will be able to use the information that you enter into this dialog to connect to the Vet web site and automatically download an upgrade.

Vet Program Directory

This is the directory that Vet will be installed into. By default Vet is installed into C:\VET, if Vet has already been installed onto your PC the directory that it has already been installed to will be displayed instead of C:\VET.
If you wish to install Vet to a different directory select the Browse button and chose another directory.

Vet Desktop Options

By accepting the defaults a Vet short-cut will be added to the Tray area (bottom left of your screen, next to the clock if you have one). Once the icon is installed to the Tray you can easily determine in the resident protection is loaded and active by moving the cursor over the icon (and a summary of which components of resident protection are loaded will popup)

It is possible to remove the Vet icon from the tray by opening Vet and selecting Options | Options Wizard… and changing the defaults on the Desktop Options Dialog.

Enabling Vet NT Server Scheduler

This option will enable the scheduler if you are installing Vet NT Server. If you wish to enable the scheduler so that you can configure it to run periodic scans across you network please select "Yes, enable Vet scheduler".
Any other command line application can also be run by this scheduler.

AUTOEXEC Clean Up (Master Installation Only)

The Autoexec.bat file is used to store information on what files to load when you turn on your PC, in the past Vet has modified this file so that the DOS resident protection was automatically started when you turned on your PC. These changes are no longer necessary as they have been superseded with newer functionality.
We recommend you accept the default (**Yes, allow Vet to modify AUTOEXEC.BAT**) and select Next> to continue.

DOS Vet Clean Up

References to DOS Vet commands are no longer required in DOSSTART.BAT, as the requirement for this has been superseded by newer functionality. We recommend that you accept the default (**Yes, allow Vet to modify DOSSTART.BAT**) and select Next> to continue.

'Read-Me' Help File

Setup can display a 'Read-me' help file, which will include late-breaking information that has not made it into the manual. The 'Read Me' help file will also give a summary of all the changes that have been made since the last version of Vet.

Most site administrators have asked for Vet to be installed as unobtrusively as possible, for this reason the default is **No, never display the 'Read Me' file**. The other options available will allow the user to decided if they wish to read the Read Me file, or for the Read Me File to be displayed to every user during installation. Select an option and then select Next> to proceed.

Boot Sector Templates

Setup will offer to record a template (or copy) of the local hard drive boot sectors. These are used to check if the boot sector has been changed. Select the drive(s) that you wish to make templates for. We recommend templates are made for all local drives. (It is not appropriate to make templates for network or CD-ROM drives)

Reference Disk

The wizard will offer to make a reference disk which will hold a template for each of the local drives. We recommend creating a reference disk; you will need a formatted, write enabled system disk with at least 600k of free space. Select Next> to proceed.

If you choose to make a reference disk, the "Make a reference disk" dialog will be displayed. Enter a line of text so that you can uniquely identify your PC, insert a freshly formatted floppy, and select OK. When Vet has finish creating the reference disk, label it with a "Reference Disk" sticker (that comes in the Vet box if you have purchased a boxed set of Vet).

If you do not wish to create a reference disk select Next> to proceed.

Scan Hard Disk

By enabling this option the users PC will be scanned once Vet has finished loading. This is recommended as each version of Vet can only detect those viruses that where known about when that version was made. By scanning with a later version you may detect recent viruses that have not been detected in the past.

Information Dialogs (Master Installation Only)

These options allow you to configure what will be displayed to the users during the installation of Vet from a master copy. Select what you will need to keep the user informed

Splash Screen

>This will display the Vet splash screen before beginning the installation. It is the best way to let the users know exactly what is being loaded onto their machine and will only be displayed until they select the Next> button.

Welcome Screen

>The welcome screen also reminds users that they should not have other programs running when they install Vet, and especially warns against loading more than one anti-virus scanner at a time.

Licence Agreement

>By creating a master copy of Vet for installation across a site/network you are accepting responsibility to enforce the licence agreement. If you wish to make individual users to accept the licence agreement then enable this option.

Installation confirmation

>This option will display a dialog to the users to confirm that the installation has completed and been successful.

Configuration confirmation

>This option will display to the users a summary of the default options, and those options that the user has selected during the installation and asks them to confirm that they wish to complete the installation. This option is useful if you are installing Vet across a site/network where you have a number of users that have a high IT knowledge. Because these people may have non-standard configurations they may need to examine the options that will be installed with this version of Vet.

Most System Administrators do not want the users to know that the latest version is being loaded so by default these options are not enabled.

Enable Scheduler (Vet NT Server Installation Only)

This dialog allows you to enable or disable the scheduler facility on NT Scheduler. By enabling the scheduler you will be able to configure Vet NT Server to run regular scans over your NT Server.

Automatic Setup Completion

This dialog allows you to determine what you want to be displayed to the users after they have had Vet installed/upgraded.

Most System Administrators do not want the users to know that the latest version is being loaded so the Complete silently option is the default.

Complete silently (no message or prompt)

By selecting this option nothing will be displayed to the user once the installation/upgrade is completed and the computer will not be rebooted. It is recommended that you restart Windows as restarting Windows will allow the latest version of the resident protection to be loaded.

Display a completion message only

By selecting this option a message will be display to let the user know that their version of Vet had been updated.

Prompt the user to restart Windows

This option will display a message prompting the users to restart Windows. It is recommended that Windows be restarted as restarting Windows will allow the latest version of the resident protection to be loaded. The latest version of the resident protection will be able to detect all of the viruses that have been discovered since the last version of Vet was released.

Always restart Windows (after displaying completion message)

This option will display a message to inform the user that the installation/upgrade has completed successfully and that Windows will be restarted to allow the latest version of the resident protection to be loaded. The latest version of the resident protection will be able to detect all of the viruses that have been discovered since the last version of Vet was released.