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:

Network Concepts Limited,
PO 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

Unit 802, BlockA, PJ Tower, Amcorp Trade Centre, No 18, Jalan Persiaran Barat, Petaling Jaya, 46050 Selangor, Darul Ehsan, 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.

Minneapolis Headquarters:
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 Facsimile: (+1) 714 641 1543
San Jose: 2001 Gateway Place, Suite 750 West, San Jose, CA 95110
Toll Free: (+1) 800 872 2599 Phone: (+1) 408 573 9592 Facsimile: (+1) 408 573 1514
Washington DC: 2000 Corporate Ridge, 8th Floor, McLean, VA 22102
Toll Free: (+1) 800 872 2599 Phone: (+1) 703 821 8101 Facsimile: (+1) 703 821 2539

Germany: Ontrack Data Recovery GmbH.

Germany: Ontrack Data Recovery GmbH
Hanns-Klemm-Strasse 5, 71034 Boeblingen, Germany
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: 0 800 10 12 13 14 Sales (+44) 0 1372 741999 Tech Support (+44) 0 1372 747414
Facsimile: (+44) 0 1372 741441
Email: WWW: sales@ontrack.com
http://www.ontrack.com

France:

ONTRACK France SARL
Le Dôme - B. P. 10910, 1, rue de la Haye, F-95731 Roissy CDG Cedex France
Toll Free: 00 800 10 12 13 14
Phone +33 (0)1 49 19 22 63
Facsimile: +33 (0)1 49 19 22 37
Email: infofrance@ontrack.de
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.

Year 2000 Conformity for the Vet Range

This document is a response from Cybec Pty Ltd, developer of the Vet Anti-Virus Software Range, to all concerned parties, regarding year 2000 conformity issues, based upon the definition DISC PD2000-1 produced by the British Standards Institute, and upon “SAA/SNZ MP77:1998: A Definition of Year 2000 conformity requirements”. The SAA/SNZ document is almost identical to the BSI document, and “the only variations from the BSI document are the deletion of the list of British contributing organisations from the third paragraph of the Introduction, and the numbering of the clauses.” (quoted from SAA/SNZ MP77:1998)

Introduction

This document describes the degree of conformity of Vet Anti-Virus software sold by Cybec Pty. Ltd. as listed in ***Section C*** of this document, to the BSI document DISC PD2000-1, “A Definition of Year 2000 Conformity Requirements” and to the SAA/SNZ SNZ MP77:1998: A Definition of Year 2000 conformity requirements. It is recommended that the reader refer to the relevant document for details.

Vet Year 2000 Compliance

General Integrity

Vet has been tested to ensure full compliance with the “General Integrity” rule.
This rule requires that all software which conforms to it is able to roll over between all significant time demarcations (eg days, months, years, centuries) correctly. This means that no value for the current date will cause any interruption in operation.

The current date in all Vet products is always displayed as reported by the operating system. The user does not enter or select dates in using Vet (except when using the Vet NT scheduler), which considerably simplifies the issues relating to Year 2000 compliance.

One area where dates are manipulated by the software is reporting to the user that the software is using out-of-date virus information; this is reported typically six months after the software is built. We need not consider any dates more than six months prior to the current date, because dates prior to the build of the software are not used. Neither are we concerned with dates significantly into the future, because no date beyond the current date is used. Leap years are not a consideration, because Vet does no date calculations in which the leap year variation would create any repercussions. Vet will continue to work correctly and recognise both 29th February and the day 366 in the year 2000.

Vet does not store dates in 2-digit format. The native date format for each platform is used. In the case of DOS and Windows 3.1x, the native date format stores the number of days elapsed since 1st January 1980AD in a 16 bit integer. This format has a built-in expiry date, which lies well into the second half of the next century. In the case of Windows 95, Windows 98, and Windows NT, the native date format stores the number of 100 nanosecond intervals elapsed since midnight 1st January 1600AD in a 64 bit integer. This format has a built-in expiry date far beyond the year 3000AD (which in fact is nearer to 30000AD), which should cause no problems.

In reporting dates and times for the start and finish of scans, Vet is using a system library function, which reports the current date as reported by the operating system, so there is minimal likelihood for confusion. This date and time format may be configured by the user to support 4 digit year dates during reporting, using the Windows Control Panel. DOS Vet uses four digit year dates.
Another area where Vet may use dates is when creating reference disks. This date and time format may be configured by the user to support 4 digit year dates during reporting, using the Windows Control Panel. DOS Vet uses four digit year dates.

Date Integrity

Vet has been tested to ensure full compliance with the “Date Integrity” rule.
This rule requires that all Vet products be able to calculate, manipulate and represent dates correctly for all purposes for which they were intended.

Dates used in Vet serve the following purposes:

1) Vet uses dates to inform the user when it is considered “out-of-date”, meaning that it may be too old to detect the latest viruses. This is intended to remind the user that a newer version of Vet is available and should be installed.
2) Vet uses dates during reporting. This includes the reports Vet generates on-screen as well as in log-files. The purpose of the dates is to report the start and finish of each scan performed by the user, purely for reference reasons. In this way, Vet logs allow users to tell when the last scan was made, or when a virus was found.
3) Vet uses dates to program the Vet NT scheduler. Dates are used to prepare a schedule for when Vet should perform a scan automatically, without user intervention. This is perhaps one area where the use of dates in Vet is critical. The scheduler has been extensively tested to ensure full compliance with Year 2000 requirements.
4) Vet uses dates and times to identify when a reference disk was created. This date and time format may be configured by the user to support 4 digit year dates during reporting, using the Windows Control Panel. DOS Vet uses four digit year dates.

Explicit/Implicit Century
Vet has been tested to ensure full compliance with the “Explicit/Implicit Century” rule.

This rule ensures that one of two possible approaches is used in software:
(a) explicit representation of the year in dates: eg by using four digits or by including a century indicator.
(b) the use of inferencing rules: eg two digit years with greater value than 50 imply 19xx, those with a value equal to or less than 50 imply 20xx.
Vet does not use approach (b) in any situation. Explicit representation of 4-digit years is used in most cases (see “General Integrity” rule). In other cases, Vet will use 2 or 4 digits to represent the year, depending on your settings as defined in the Windows (Windows 3.x, Windows 95 or Windows NT) control panel.
Vet Products Conforming to DISC PD2000-1
The products which conform to the DISC PD2000-1 and to the SAA/SNZ MP77 requirements are:

- Vet for DOS
- Vet for Windows 3.x
- Vet for Windows 95
- Vet for Windows NT Workstation
- Vet for Windows NT Server
- Vet Scheduler for Windows NT Server
- Vet for NetWare

The version of each of these products, which conforms to the DISC PD2000-1 and to the SAA/SNZ MP77 requirements is version 9.70 or later.

Legal Statement
Software supplied by Vet is supplied pursuant to the Vet Anti-Virus Software Licence Agreement (“VAVSLA”) which can be found on the Vet master disks. This statement is considered to be part of the documentation supplied from time to time with the Software and is subject to the VAVSLA.

The VAVSLA provides, in part,

“to the fullest extent allowed under law, Cybec excludes all other terms, warranties and conditions, whether express or implied, relating to the performance, quality, or fitness for use of the Software or any disks on which the Software is recorded, including any warranty or condition that the Software will meet the Licensee's requirements or operate without interruption or error.

To the fullest extent allowed under law, and subject only to the express warranty contained in clause 6.2, the liability of Cybec for any breach of any term, condition or warranty, or duty of care, shall be limited, at

the option of Cybec, to any one or more of the following:

(a) the replacement of the Software or the supply of equivalent Software;

(b) the repair of the Software;

(c) the payment of the cost of replacing the Software or acquiring equivalent Software; or

(d) the payment of the cost of having the Software repaired.

The Licensee agrees that in no event will Cybec be liable for damages, including but not limited to, indirect, special, incidental or consequential damages (including loss of profits or anticipated revenue) in connection with or arising out of performance of the Software, even if Cybec or the dealer had been advised of the possibility of such damages."

Accordingly, users should not rely upon this document and make their own enquiries and engage professional assistance in relation to the suitability of the Cybec Software for use in their particular environment beyond the Year 2000.

Further:

- Cybec cannot say and does not state whether or not its software will work in the environment or at the times other than for which the system was expressly designed and tested. In particular, your computer systems may consist of hardware or third party software, which are not year 2000 compliant and which has not been tested by Cybec unless stated expressly otherwise.
- It is your responsibility to ensure that the computer hardware and software that you currently use is year 2000 compliant and although Cybec would be pleased to assist you in this evaluation process in relation to its products, it cannot be held responsible for any consequences which arise as a result of continued use of non compliant technology interfaced with its software or otherwise.

Conclusion

Subject to the Legal Statement, the above information is a true and accurate statement of the conformity as at 26 March 1998.

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, Vet98 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 (Options | Program | Scan Options)

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

Scan compressed archives

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.

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.

Scan compressed archives: If this option is enabled Vet will be able to scan some types of compressed files (ie. .ZIP files). You must also have the file extension listed in the file extension list if you want the files to be scanned.

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.

File Types to Scan (Options | Program | File Types)

This dialog allow you to determine which files types will be scanned for viruses. We recommend that you accept the default and scan “files of these types” as they are the only file types that can carry a virus and selecting “All files” will increase the time it takes to scan a directory or drive.

All files: Causes Vet to check *every* file it encounters for viruses. You can choose either All files or Files of 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 .386, .BIN, .COM, .DLL, .DOC, .DOT, .DRV, .EXE, .MDB, .OVL, .SYS, .XLS, .XLT and .ZIP extensions to be executable. You can choose either All files or Executable only but not both.

Add: 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.

Delete: 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. (.386, .BIN, .COM, .DLL, .DOC, .DOT, .DRV, .EXE, .MDB, .OVL, .SYS, .XLS, .XLT and .ZIP 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.

NOTE: When you are upgrading Vet and chose Next> to continue past this screen Vet will check your current list of file extensions. If you don’t have all of the file extensions that we recommend (as they are susceptible to infection) a dialog will appear and prompt update your extension list.

Infected & Suspect Program Files (Options | Program | Program Viruses)

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

STOP! If you chose for files to be **Cleaned** 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 (Options | Program | Program Viruses)

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 (Options | Program | Macro Viruses)

The following mutually exclusive options are available for dealing with documents, spread sheets or databases that are infected, or suspected, of having a macro virus.

Vet can automatically detect and clean all Word and Excel macro viruses. Vet is also able to detect Access database macro viruses.

Infected Documents

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

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

Rename: Causes Vet to change the first letter of the extension of any document infected with a virus to an underscore '_' (.DOC becomes ._OC). This allows you to keep the file for further examination.

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

NOTE: Use this option with caution, as there is no possibility of recovering documents deleted in this manner.

Suspect Documents:

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

Rename: Causes Vet to change the first letter of the extension of any document suspected of infection with a virus to an underscore '_' (.DOC becomes ._OC). This allows you to keep the file for further examination.

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

Reporting (Options | Program | 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. The log file size can be configured by editing the “limit log file size to” field.

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 (Options | Program | Reporting)

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 (Options | Program | 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 (Options | Program | Memory for Vet95 and Vet98 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 (Options | 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 Vet command line switches.

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

The Configure Progressive Scan button 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, C:\VET\VET98 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

/AllLocalDisks - Include all local hard disk drives in the scan

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

/cancel - Allow cancellation of the scan
/nocancel - Do not allow cancellation of the scan

/compressed - Scan compressed archives, e.g. zip files
/nocompressed - Do not scan compressed archives

/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 /.=)

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

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

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

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

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

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

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

Actions

The Action options will specify one of the following values for how to deal with file viurses: clean, rename, report only, 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 file infections.
/suspect=rename
/suspect=delete
/suspect=reportonly (replaces /O, and /Y)

The Action options will specify one of the following values for how to deal with Macro viurses: clean, rename, report only, delete
/macro= - specify the action to be taken on infected files.
/macro=clean
/macro=rename
/macro=delete
/macro=reportonly

/susmacro= - specify the action to be taken on suspected macro infections.
/susmacro=rename
/susmacro=delete
/susmacro=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

/silent - This switch can ONLY be used during an automatic/master installation. This option removes the progress meters etc so that apart from hard disk activity the user will not know that Vet is being installed/upgraded. Any prompts that you have specified the users to configure will still be displayed.

/waitstart - Specify the number of seconds to wait before starting,

eg: /waitstart15 will wait 15 seconds

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 (Options | Program | Start-Up | Configure Prog. Scan)

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.

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 (Options | Resident Protection | 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

NOTE: Some installation programs recommend that you disable your anti-virus protection before attempting to install their software. Please scan the floppies or CD BEFORE disabling the resident protection as they may be infected with viruses. ‘Shrink wrapped’ software has been found to be infected in the past.

To “Disable your Antivirus software” remove the ticks from each of the Options | Resident protection | Enabling options, then close Vet and save your changes.

NOTE: You MUST open Vet and enable these options once you have finished loading the software as the resident protection is the main component of your anti-virus protection.

Floppy Boot Sector (Options | Resident Protection | 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 (Options | Resident Protection | 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 or Vet98. 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 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 (Options | Resident Protection | 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 (Options | Resident Protection | Macro Virus Actions)

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

The following mutually exclusive options are available for dealing with documents, spread sheets or databases that are infected, or suspected, of having a macro virus.

Vet can automatically detect and clean all Word and Excel macro viruses. Vet is also able to detect Access database macro viruses.

Infected Documents

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

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

Rename: Causes Vet to change the first letter of the extension of any document infected with a virus to an underscore '_' (.DOC becomes ._OC). This allows you to keep the file for further examination.

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

NOTE: Use this option with caution, as there is no possibility of recovering documents deleted in this manner.

Suspect Documents:

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

Rename: Causes Vet to change the first letter of the extension of any document suspected of infection with a virus to an underscore '_' (.DOC becomes ._OC). This allows you to keep the file for further examination.

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

Reporting (Options | Resident Protection | 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 (Options | Alerting | E-Mail)

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 a scan, 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.

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. The email alert can be set to more than one person by placing a semicolon (;) between each of the email addresses that are to be notified.
Ie. SysAdmin@company.com.au; HeadOffice@company.com.au

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 address(es) 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 (Options | Alerting | 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:

Alert administrator via email when a virus is found

By selecting (ticking) this option you can send an Email when a virus is detected after you have opened Vet and started scanning files. In order to successfully send the email alert you must also configure the SMTP Email tab with the details required to send the message.

Resident Protection:

Display message box when virus found

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.

Alert administrator via email when a virus is found

By selecting (ticking) this option you can send an Email when a virus is as you go about your daily work. In order to successfully send the email alert 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 **Finish** 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.

Use of the Condition list

What is the Condition List?

The Condition List is an ordered list of filename patterns and specifications that can be used to ensure certain files and/or directories are never scanned.

How does it differ from the Extension List?

The Extension List (accessed through the on-demand scanner - Options | Program... | File Types) is provided as a method of including only certain file types in on-demand scans, typically to speed up scans by only scanning files that are in danger of being infected by a virus. The Extension List is limited to restricting scans to only certain types of files (those with particular extensions). The Condition List allows individual files/directories or filename patterns (using wildcards) to be always excluded from a scan. The Condition List takes precedence over the Extension List.

What is it used for?

The Condition List provides fine-grained control over the inclusion and exclusion of files and directories. It is harder to use than the Extension List, because of its flexibility, but that is the very reason why a user may choose to take advantage of it.

You could choose to use the Condition List if, for example, you had a read-only directory containing a large number of unchanging complex documents which take considerable time to scan. If users are loading these documents frequently, but not changing them, the time spent scanning them is wasted, so you might choose to exclude them from scanning. There is, naturally, a risk associated with such a decision - should such a document become infected the infection would not be picked up, so you must weigh the decision carefully.

Where is it implemented?

Currently (9.8.0), the Condition List is implemented in:

Vet on-demand scanners for Windows 3.x, Windows 95, Windows 98, and Windows NT.

Vet resident protection for Windows 3.x and Windows NT.

WARNING: If you do not have a specific use for the Condition List then DO NOT experiment. Altering registry settings is a difficult and potentially dangerous operation and SHOULD NOT be undertaken unless you are aware of the dangers involved

Click here for further information about the Condition List

Further information on the Condition List

WARNING: If you do not have a specific use for the Condition List then DO NOT experiment. Altering registry settings is a difficult and potentially dangerous operation and SHOULD NOT be undertaken unless you are aware of the dangers involved

Format

The Condition List consists of an in-order list of 'rules' which explicitly describe which files and/or directories are to be included or excluded while scanning. Each rule is composed of a plus or minus symbol (denoting inclusion or exclusion respectively) followed by a filename pattern (a file or folder specification that may contain wildcard characters - '*' or '?').

Example:

-C:\WINDOWS*.*

This rule specifies that all files in the C:\WINDOWS directory are to be **excluded** from the scan.

-C:\PAGEFILE.SYS

This rule specifies that C:\PAGEFILE.SYS will be **excluded** from the scan, even if '.SYS' **does** appear in the Extension List.

+C:\PAGEFILE.SYS

This rule specifies that C:\PAGEFILE.SYS will be scanned even if '.SYS' **does not** appear in the Extension List.

The order in which rules appear in the Condition List is critical.

The file's name is compared with the pattern in each rule in turn, starting from the top of the list. The comparison stops with the first rule found where the filename matches the pattern. The file is scanned, or not, depending on whether the rule contains a plus or a minus.

Example 1

+C:\WINDOWS\SYSTEM\COMMCTL.DLL

-C:\WINDOWS\SYSTEM*.*

+*.*

Files to be scanned:

C:\WINDOWS\SYSTEM\KRNL386.EXE

- Tested against the first rule '+C:\WINDOWS\SYSTEM\COMMCTL.DLL', does not match, go to second rule.
- Tested against the second rule '-C:\WINDOWS\SYSTEM*.*', a match is made.
- The minus sign means this file is to be excluded.
- C:\WINDOWS\SYSTEM\KRNL386.EXE is ignored.

C:\WINDOWS\SYSTEM\COMMCTL.DLL

- Tested against the first rule '+C:\WINDOWS\SYSTEM\COMMCTL.DLL', a match is made.
- The plus sign means this file is to be included.
- C:\WINDOWS\SYSTEM\COMMCTL.DLL is scanned.

C:\DOS\COMMAND.COM

- Tested against the first rule '+C:\WINDOWS\SYSTEM\COMMCTL.DLL', does not match, go to second rule.
- Tested against the second rule '-C:\WINDOWS\SYSTEM*.*', does not match, go to third rule.
- Tested against '+*.*', a match is made.
- The plus sign means this file is to be included.

- C:\DOS\COMMAND.COM is scanned.

Note the order of the rules. If the first and second rules were to be swapped, COMMCTL.DLL would never be scanned as '-C:\WINDOWS\SYSTEM*.*' would take precedence.

Example 2

You want the files in the 'Temp' directory in the C: drive root directory to be scanned but not the files in any other 'Temp' directories. You also have a large number of files in the directory D:\DATA that you wish to be scanned but they have numeric extensions ranging from .000 to .999 and you don't want to add all of the extensions to the Extension List.

```
+C:\TEMP\*.*
-*\TEMP\*.*
+D:\DATA\*.???
```

Example 3

You do not want any files on your D: drive to be scanned, or the file TEST.EXE wherever it may be. Apart from those, you would like all other files to be scanned regardless of their extension.

```
-D:*
-TEST.EXE
+*.*
```

Creating and editing the Condition List

There is currently no graphical user interface to the Condition List.

Windows 3.x

On-Demand Scanner

The Condition List is stored in VET.INI which is located in the Windows directory.

Resident Protection

The Condition List is stored in VETMON.INI which is located in the Windows directory.

Each of these files can be modified manually to include a Condition List by following these steps:

- Open the file in a text editor (VET.INI for the on-demand scan, VETMON.INI for resident protection)
- Add a section to the end of the file '[Condition List]'
- Add each rule to the section in the format 'Condition*n*=<rule>'

Example:

```
[Condition List]
Condition1=+C:\WINDOWS\SYSTEM\*.*
Condition2=-C:\WINDOWS\*.*
Condition3=+C:\APPS\*.EXE
Condition4=-C:\APPS\*.*
```

- The changes to VET.INI will take effect next time the on-demand scanner is run.
- The changes to VETMON.INI will take effect the next time resident protection is loaded.

Currently (9.8.0), the Condition List is not distributable through a Vet Master Setup for Windows 3.x.

Windows 95 & Windows 98

On-Demand Scanner

The Condition List for the on-demand scanner is stored as a multi-string value 'ConditionList' under the registry key:

HKEY_LOCAL_MACHINE > SOFTWARE > Cybec > VET Antivirus for Win32 > Scanning

The registry editor REGEDIT.EXE that is shipped with Windows 95 and Windows 98 does not allow you to create or edit multi-string registry values. To create a Condition List on a Windows 95/98 workstation, a Master Setup must be performed.

Creating a Condition List using the Master Setup

Run a Master Setup as you normally do for your workstations. Once the Master Setup has been run, a file 'VETAUTO.INF' will have been created in the platform subdirectory of the master installation directory that you specified. This file contains all configuration options that will be set on the workstations during an Automatic Setup. Before an Automatic Setup is performed, you can modify this file manually to distribute a Condition List (for the on-demand scanner) during Automatic Setup by following these steps:

- Open the file in a text editor.
- Add a section to the end of the file '[Condition List]'
- Add each rule to the section in the format 'Rule*n*=<rule>'

Example:

```
[Condition List]
Rule1=+C:\WINDOWS\SYSTEM\*.*
Rule2=-C:\WINDOWS\*.*
Rule3=+C:\APPS\*.EXE
Rule4=-C:\APPS\*.*
```

- When an Automatic Setup is performed, this Condition List will be copied to each workstation.

Windows NT

On-Demand Scanner

The Condition List for the on-demand scanner is stored as a multi-string value 'ConditionList' under the registry key:

HKEY_LOCAL_MACHINE > SOFTWARE > Cybec > VET Antivirus for Win32 > Scanning

Creating the Condition List manually

This registry value can be edited directly by following these steps:

- Run REGEDT32.EXE (usually found in the SYSTEM32 subdirectory of the Windows NT directory)
- In the **HKEY_LOCAL_MACHINE** registry hive, open the key

SOFTWARE > Cybec > VET Antivirus for Win32 > Scanning.

- If the 'ConditionList' value already exists, simply double-click on it to edit.
- If it does not exist, select 'Add Value...' from the Edit menu. Name the value 'ConditionList' (no space) and set the data type to REG_MULTI_SZ.
- A dialog box will appear in which the Condition List can be edited. Enter each rule on a separate line in the correct order. Omitting a plus or minus from the beginning of the rule will default to rule to '+' (inclusion).

Creating a Condition List using the Master Setup

(These instructions are the same as for Windows 95/98)

Run a Master Setup as you normally do for your workstations. Once the Master Setup has been run, a file 'VETAUTO.INF' will have been created in the platform subdirectory of the master installation directory that you specified. This file contains all configuration options that will be set on the workstations during an Automatic Setup. Before an Automatic Setup is performed, you can modify this file manually to distribute a Condition List (for the on-demand scanner) during Automatic Setup by following these steps:

- Open the file in a text editor.
- Add a section to the end of the file '[Condition List]'

- Add each rule to the section in the format 'Rule*n*=<rule>'

Example:

```
[Condition List]
Rule1=+C:\WINDOWS\SYSTEM\*.*
Rule2=-C:\WINDOWS\*.*
Rule3=+C:\APPS\*.EXE
Rule4=-C:\APPS\*.*
```

- When an Automatic Setup is performed, this Condition List will be copied to each workstation.

Resident Protection

The Condition List for the Windows NT resident protection is stored as a multi-string value 'ConditionList' under the registry key:

HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > VETMONNT

This registry value can be edited directly by following these steps:

- Run REGEDT32.EXE (usually found in the SYSTEM32 subdirectory of the Windows NT directory)
- In the **HKEY_LOCAL_MACHINE** registry hive, open the key

SYSTEM > CurrentControlSet > Services > VETMONNT.

- If the 'ConditionList' value already exists, simply double-click on it to edit.
- If it does not exist, select 'Add Value...' from the Edit menu. Name the value 'ConditionList' (no space) and set the data type to REG_MULTI_SZ.
- A dialog box will appear in which the Condition List can be edited. Enter each rule on a separate line in the correct order. If you wish to specify drives in the Condition List for the Windows NT resident protection the drives must not be referenced by drive letter. Rather, they must be specified using the fully qualified path.

  Example:

  ```
  +C:\WINDOWS\*.*
      would normally become
  +\Device\Harddisk0\Partition1\WINDOWS\*.*
  ```

  Determining the fully qualified name of a given drive letter is not always simple. One method is to use the Disk Administrator program. The hard drives are listed by Disk Administrator in order, with the topmost being Hardisk0, the next Hardisk1, and so forth. Within each hard drive, the partitions are listed in order, with the first being Partition1, the next Partition2, and so forth. Note that Harddisk numbers start at zero, while Partition numbers start at one.

  Note also that A: is \Device\Floppy0, and that your first CD-ROM drive (whatever its drive letter) is \Device\CDROM0.

Disabling the Condition List

Windows 3.x

The Condition list for the **on-demand scanner** can be disabled by deleting the section '[Condition List]' in VET.INI (located in the Windows directory). This will take effect the next time the on-demand scanner is run.

The Condition List for the **resident protection** can be disabled by deleting the section '[Condition List]' in VETMON.INI (located in the Windows directory). This will take effect the next time the resident protection is loaded.

Windows 95 & Windows 98

The Condition List for the **on-demand scanner** can be disabled by deleting the registry value

'ConditionList' under the key

HKEY_LOCAL_MACHINE > SOFTWARE > Cybec > VET Antivirus for Win32 > Scanning

This will take effect the next time the on-demand scanner is run.

Windows NT

The Condition List for the **on-demand scanner** can be disabled by deleting the registry value 'ConditionList' under the key

HKEY_LOCAL_MACHINE > SOFTWARE > Cybec > VET Antivirus for Win32 > Scanning

This will take effect the next time the on-demand scanner is run.

The Condition List for the **resident protection** can be disabled by deleting the registry value 'ConditionList' under the key

HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > VETMONNT

This will take effect the next time the machine is booted, or the next time you change any resident file monitor setting using the on-demand scanner.

Tips on using the Condition List effectively

- As a general guide, put more specific rules first and general rules last.
- Remember that the Condition List takes precedence over the Extension List. If a filename is not matched to any rules in the Condition List, it will be passed to the Extension List and the normal rules applied.
- Having '-*.*' or '+*.*' as the last rule in the Condition List will override the Extension List because any filename not previously matched will match this rule and will not be passed to the Extension List.
- Having a rule such as '+C:\WINDOWS\SYSTEM\COMMCTL.DLL', does **not** mean that COMMCTL.DLL will be scanned in **every** scan. It only means that COMMCTL.DLL will be included if it is encountered during an on-demand or on-access scan.
- Wildcard characters can be used anywhere in the path.

  Eg. '-?:\WINDOWS\NET*.EXE'.

  Be careful though, as '-C:\WINDOWS*.DLL' will ensure that C:\WINDOWS\MORICONS.DLL is not scanned, but will also mean that C:\WINDOWS\SYSTEM\COMMCTL.DLL is not scanned either (both 'MORICONS' and 'SYSTEM\COMMCTL' satisfy '*').

  ('?' means zero or one character, '*' means zero or more characters)
- Keep in mind that the Condition List will take effect for all on-demand scans except when individual files are selected explicitly in the on-demand browser. This allows you to force a scan of an otherwise excluded file simply by selecting it in the browser.
- If you wish to specify drives in the Condition List for the Windows NT resident protection the drives must not be referenced by drive letter. Rather, they must be specified using the fully qualified path.

  Example:

  +C:\WINDOWS*.*

  would normally become

  +\Device\Harddisk0\Partition1\WINDOWS*.*

  For more information regarding fully qualified names, refer to the notes in *Creating and editing the Condition List | Windows NT Resident Protection.*

  The drive specification may be omitted, if desired, by specifying

  +*\WINDOWS*.*

VetARRT has been released to help install VetNT across networks.

Until now (due to the security features in Windows NT) it has been necessary for VetNT to be installed, with administrator privileges, to each and every NT workstation and server.

In order to install or update VetNT we need to install/modify registry keys in HKEY_LOCAL_MACHINE\ System\Current Control Set\ Services. This requires administrator privileges on the machine we are installing to. Most System Administrators do not allow their users to log on with administrator privileges.

Solution:

Install to every machine a service that can run under a privileged account to perform the Vet registry key install/update.

Requirements:

You must be running your network on an NT domain server.

VetARRT will only work with VetNT version 9.63 or later.

Workstations must have been configured to be administered by Domain Administrator (this is default for NT workstations attached to an NT domain server).

Where can I get a copy?

Registered Vet users can download a copy from www.vet.com.au or you can call your local Technical Support team to have a floppy disk sent to you.

Do you want VetARRT step-by-step operating instructions?

Do you want more technical information on VetARRT?

Technical Specifications for VetARRT.

Usage

VetARRT (options)

Switches:

/?	Help (display usage text)
/c <filename>	Create a file containing all Windows NT machines registered with the Primary Domain Controller
/u <filename>	Perform the update
/l <filename>	Specify a logfile (the default log file is *VetARRT.log*)
/p <filename>	set a password for the privileged account
/i <filename>	Specify input ini file (the default is *VetARRT.ini*)
/s <filename>	Set the Vet registry keys values
/r <filename>	Specify ini file with the registry keys to update (the default is RegKeys.ini)

Updating Machines

1. Create a domain user account for the VetReg service to be run under. This account must have Log On as a Service rights.
1. Run VetARRT to set up a password for the account created. Eg: **VetARRT /p password**.

   (where "password" is the VetARRT user password, maximum of 14 characters long).

   Note that if the password provided is longer than 14 characters, it will be cut off to 14 chars.
1. Edit *VetARRT.ini* file to specify domain/user details, eg:

   [General]

   0 DomainName = CYBEC

   1 UserAccount = VetARRT

   2 [Users]

   3 Victoria=

   4 Elizabeth=

   5 Tomas=

   6 [SERVICE]

   7 ServiceDisplayName=”VetReg Security Service”

   8 ImagePath=”%SystemRoot%\System32\VetReg.exe”

   VetReg.exe will be copied onto system32 directory by the Vet installation program on all machines.

   Please do not change service name and registry keys.
1. Run VetARRT with /c switch to get the list of the machines in the domain, eg: **VetARRT /c machines.txt**

VetARRT will save the list of all machines in the domain in the *machines.txt* file.

1. Edit *machines.txt* to include only the machines you wish to be updated. The machines file will look as follows:

   ; Domain: CYBEC

   0 ; Primary Domain Controller: \\SERVER

   1 [MachineAccounts]

   2 MELBOURNE=

   3 SYDNEY=

   4 BRISBANE=

   To remove the machine from the list – either delete the line completely or comment it out, eg:;SYDNEY=

1. Run VetARRT with /u and /l switches to update the machines, eg:**VetARRT /u machines.txt /l log.txt**

   VetARRT will attempt to update all machines listed in *machines.txt*. Successfully updated machines will be removed from *machines.txt*. All error messages will be written to *log.txt*

   Note: if you don't specify the log file – all messages will be written to the default *VetARRT.log* file.

Log Messages:

- Service information could not be obtained...
- Failed to connect to the Service Control Manager...
- Failed to stop the service...
- Failed to create the service
  1. The handle to the specified service control manager database does not have SC_MANAGER_CREATE_SERVICE access...
  1. A circular service dependency was specified...
  1. The display name already exists in the service control manager database either as a service name or as another display name…
  1. The handle to the specified service control manager database is invalid....
  2. The specified service name is invalid....
  3. A parameter that was specified is invalid....
  4. The user account name specified does not exist....
  5. The specified service already exists in this database....
  6. Error unknown, number .....
- Failed to add <user_account> to the service access list...
- Failed to add <user_account> to the ACL of the <registry_key>
- Failed to create/open <registry_key>
- Failed to open a file with the list of machines to update...
- Failed to obtain the password for the privileged user account...
- Updated successfully...

- Was not updated successfully...

Example of the log file:

Thu Jan 08 13:38:30 1998

MELBOURNE

Failed to connect to the Service Control Manager...

Was not updated successfully...

BRISBANE

Updated successfully…

The format of the VetARRT.ini file

[General]

DomainName=TEST The name of the domain to update. Only one domain may be updated at a time!

Username=VetARRT The domain user/group account that the service will run under.

[User Access]

irina= Domain user/group accounts that will be granted access to start the service.

[Service]

ServiceDisplayName="VetReg security service" The display name of the service.

ServiceName=VetReg The name of the service.

ImagePath="%SystemRoot%\System32\vetreg.exe" The fully qualified path of the service binary.

[Registry Keys] The keys that the VetReg service will be granted access to.

Hive=HKEY_LOCAL_MACHINE

Key001=SYSTEM\CurrentControlSet\Services\VET-FILT

Key002=SYSTEM\CurrentControlSet\Services\VET-REC

Key003=SYSTEM\CurrentControlSet\Services\VetFDDNT

Key004=SYSTEM\CurrentControlSet\Services\VetMonNT

Key005=SYSTEM\CurrentControlSet\Services\VetMsgNT

Key006=SYSTEM\CurrentControlSet\Services\EventLog\System\VetFDDNT

Key007=SYSTEM\CurrentControlSet\Services\EventLog\System\VetMonNT

Key008=SYSTEM\CurrentControlSet\Control\GroupOrderList

Key009=SYSTEM\CurrentControlSet\Control\ServiceGroupOrder

Setting registry keys on the machines

1. Edit RegKeys.ini file to specify what keys you want VetARRT to update on target machines.
1. Run VetARRT with /c switch to get the list of the machines in the domain, eg: **VetARRT /c machines.txt.** VetARRT will save the list of all machines in the domain in the *machines.txt* file.

1. Edit *machines.txt* to include only the machines you wish to be updated.

The format of the VetARRTKeys.ini file.

Each section in the ini file specifies the key to modify. Each entry in the section defines the value to modify. The entry must have the following format: “ValueName = REG_TYPE ValueData”.

Examples of sections and keys

(HKEY_LOCAL_MACHINE\SYSTEM\C.C.S\Services\VetSrv) Set the key values.

Dword1 = REG_DWORD 0x00000001 Numerical data.

Dword2 = REG_DWORD 0x2

BinaryKey = REG_BINARY KeyValue.bin The value for binary key is the path to the file with the binary data.

String1 = REG_SZ VetARRT String.

String2= REG_EXPAND_SZ %PATH% String containing unexpanded references to environment variables.

String3 = Hello No Type will default to REG_SZ, strings are not to be quote-delimited

MultiString = REG_MULTI_SZ “exe” “dll” “sys” “doc” Multiple strings space delimited

(HKEY_LOCAL_MACHINE\SYSTEM\C.C.S\Services\VetSrv) Create a key with no values.

(-HKEY_LOCAL_MACHINE\SYSTEM\C.C.S\Services\VetSrv) Remove the key *(minus sign means remove)*

(HKEY_LOCAL_MACHINE\SYSTEM\C.C.S\Services\VetSrv) Remove the key value.

-DisplayName =

Link to VetARRT Step by step instructions

VetARRT Step-by-step operating instructions.

1. The System Administrator logs on with Domain Administrator privileges and creates an account in the Domain - i.e. VetAdmin. The Administrator then customises the VetARRT.INI file to suit local conditions. (The VetARRT.INI file also contains information on each of the options that need to be customised).
2. The Administrator runs the Vet Administrator Remote Registry Tool (VetARRT) for the first run. This gathers a list of NT workstations from the domain controller and puts them into a text file. The Administrator edits the list to remove any workstations which you do not wish to install/upgrade Vet to.
1. If all of the computers that need to have VetNT installed/updated are connected when VetARRT is run it will only need to be run once. Unfortunately this may well not be the case. If after running VetARRT there are still some computers that have not been updated then you may need to schedule VetARRT to be run repeatedly (by using the Windows NT 'AT /?' command). When VetARRT is run it will take the first name on the list (.TXT file) to be updated. It will then attempt to attach (won't succeed if the machine is switched off), get the name of the next workstation, and repeat until entire list processed.

If it can attach, VetARRT

- Creates the necessary keys in the registry (these are listed in the .ini file) (File Filter and supporting services)
- Modifies the Access Control List of the registry keys and also the SYSTEM32\DRIVERS directory if on an NTFS partition.
- Registers a new service on that machine called VetReg. (Services run under a user ID - usually system account. VetReg will run under the VetAdmin ID. VetARRT will set up VetAdmin's user rights with the permission to 'logon as a service')
- Gives the local user/or user group permission to run VetReg (by default, only the administrator will be able to run VetReg. The user list and group are all passed from the .ini file)
- If all successful, VetARRT removes the name of the workstation from the list in the .TXT file.
- Repeats until the rest of the list is processed

The System Administrator then:

- Runs Vet for NT setup in /Master mode and configures the automatic installation.
- Modifies the login script to run the setup (/Auto is implied because the VETAUTO.INF file is present).

On next user login, Setup/Auto:

- Writes all registry keys (if it doesn't get access it will write the keys to a text file)

Launches the VetReg service which:

- The local user can run
- Reads the text file
- Logs in to the workstation as a service under the VetAdmin ID (which has permission to modify the Vet registry keys)
- Writes the keys

NT Upgrade Components:

VetARRT.exe:

System Administrator's tool to remotely modify an NT system (once) so that it will accept the installation of VetNT without requiring administrator privileges.

Command Line Switches:

Switch Action

/?	help (display usage text)
/c <list of machines>	create a file containing all Windows NT machines registered with the Primary Domain Controller
/u <list of machines>	perform the update
/l <filename>	specify a logfile (the default log file is VetARlog.txt)
/p <filename>	set a password for the privileged account
/i <filename>	specify input ini file (the default is VetARRT.ini)
/s	allows a single Vet key to be modified

VetReg.exe:

WindowsNT service to write Registry Keys. This will run under the privileged ID and is distributed with the VetNT files (Version 9.63 or later).

Link to VetARRT technical details

‘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.

Once you have decided to ‘‘Yes, always scan local hard disks’’ you will be able to set another option ‘‘Allow cancellation of scan during Setup’’. If you select this option the users will be able to select the STOP button on the Vet interface to cancel out of the scan. We recommend that you DO NOT select this option.

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.

Allow cancellation of dialogs during automatic installation

During a master installation if the system administrator has decided to allow users to configure some (or all) of the dialogs then they are able to select the Cancel button and quit the installation. We recommend that you do NOT allow users to select the Cancel button and quit the installation or upgrade.

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.

Force restart without user interaction (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 automatically 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. This option does not allow the users to save any files that may be open before rebooting their PC so please use with caution.

TIP: If you are updating an NT Server and do not wish to reboot the server to load the latest version of Vet please call Technical Support as it may be possible to update your DAT file(s) without re-booting your server.