What's new in InVircible for Windows 95/98/NT, version 7.02

NetZ Computing Ltd. is proud to present this major upgrade of InVircible for Windows, the all-generic Anti Viral Expert System. This version contains additions and improvements to the existing IV tools, as well as totally new features for Windows 3.x, Windows 95/98, and NT.

Among the many new features of the new InVircible package are:

- Support for long path and file names
- Support for Universal Naming Convention (UNC)
- Native Windows user interface
- Significant improvements in speed, especially on Windows NT servers
- Real-time macro virus protection and on-the-fly processing
- On-access protection against PE (Portable Executable) Win 95/98/NT Infectors
- Built-in scheduler, for Windows 95 and NT
- Distribution and management facilities for the network environment

Select one of the following topics to get more specific information:

{button ,JI(`',`IDH_VINFO_GENERAL')} **Primer on viruses and generic AV**

{button ,JI(`',`IDH_IVB_MAIN')} **Audit and Integrity Expert System**

{button ,JI(`',`IDH_IVM_MAIN')} **Macro Sweeper**

{button ,JI(`',`IDH_IVRT_GENERAL')} **Real-time Macro Protection**

{button ,JI(`',`IDH_IVSC_GENERAL')} **Built-in Scheduler**

{button ,JI(`',`IDH_CFG_GENERAL')} **Network Distribution and Management Utilities**

Press this button to add a new item to the **file extensions checklist**.

Press this button to remove the selected item from the **file extensions checklist**.

Press this button to restore the **file extensions checklist** to the program's default**.**

Press this button to add a new item to the list of excluded files & directories.

Press this button to remove currently selected item from the list of excluded files & directories.

Add Extension

Specify a three-character file extension to add to the file extensions checklist. Only files with these extensions will be checked. Note that wildcards are not allowed here.

Press this button to browse for a folder to exclude.

Press this button to browse for a specific file.

Report file name must be specified here.

Press this button to browse for the report file name.

Licensing Agreement

 You, as the purchaser of license rights to the software, are herein referred to as the Licensee.

The installation or use of this software package, or part of, constitutes acceptance and full agreement to the terms and conditions of this warranty and licensing agreement, in so doing the Licensee agrees to be bound by said provisions. This is a legal agreement between the Licensee as the end user -- and NetZ Computing Ltd. who is the owner of all rights to the software. Usage of the InVircible software indicates acceptance of the terms and conditions.

License: InVircible is licensed, it is not sold. The Licensee is obtaining limited rights to use the InVircible software. The Licensee is licensed to use InVircible on a single personal computer. Site licenses are available for individuals or organizations with multiple installation requirements.

Site License Certificate: The Purchaser of a Site License will be issued a License Certificate by NetZ Computing. The holder of the Certificate is entitled to upgrades of IV during the License Term - normally one year from the date of initial purchase -, as well as hot-line support through a NetZ Authorized Agent. The possession of the NetZ License Certificate constitutes the sole proof of a genuine and legally acquired Site License.

Alteration or reverse-engineering of the programs is not authorized, such attempts terminate this license agreement, may result in unpredictable damage and may have irreversible effects on programs and data onto which the tampered software is applied.

Limited Warranty / Limitation of Remedies: The sole remedy available to the Licensee will be limited to the replacement of the defective InVircible software. InVircible is provided "as is". The Licensee assumes all responsibility for the determination of the suitability of this software for Licensee's configuration and the results and performance of this software program package. NetZ Computing, the distributor, and their suppliers do not warrant, guarantee, or make any representations regarding the use of, or the results obtained with, the program in terms of correctness, accuracy, reliability, legality, or otherwise.

Disclaimer: In no event shall NetZ Computing Ltd., nor its Agents, nor anyone else involved in the creation, production, or delivery, of this product be held liable for any damages, loss of profit, consequential, or other damages, that may arise out of the Licensee's use or inability to use the InVircible programs. Some states do not allow excluding or limiting implied warranties or limiting liability for incidental or consequential damages, so the above limitation may not apply to the Licensee. This limited warranty and license agreement is governed by the laws of the State of Israel.

Specifying Multiple Targets to Process

The specification of the start directory from which to start scanning can be used to specify more than a single drive, computer, server, or NT domain, to be processed in a single pass of AI or the Macro Sweeper. The general format for specifying multiple targets to process is:

From Directory: **<PATH1>; <PATH2>; <PATH3>** ...

Items separated by a semicolon from their former will be treated as separate targets to inspect. The specified targets will be processed in queue, in the order they are specified. Mixed syntax is allowed, using any of the following naming conventions:

1. **Domain name** – specify just the domain name, without any slashes or backslashes. Every accessible share of every computer that belongs to the specified domain will be checked.
2. **Computer name** – specify the computer name, prepended with double backslash. Every share of that computer will be checked (please assure that you have sufficient permissions on the specific machine).
3. **Network share name** – UNC names are fully supported, thus \\server\\share\mydirecroty is perfectly legal here.
4. **Simple path** – specify absolute or relative path, with or without the final backslash.

Examples:

\\SERVER1; \\SERVER2	Check all accessible shares of the two servers, SERVER1 and SERVER2
c:\; d:\; e:\;\\SERVER1	Check the three logical drives, C: to E: and \\SERVER1
DOMAIN1; DOMAIN2	Check all computers which belong either to DOMAIN1 or DOMAIN2
C:\Download	Check all files in directory C:\Download, and possibly all sub-directories.

Welcome to InVircible's Audit and Integrity (AI) Expert System

The Audit and Integrity Expert System (IVB32) will secure, authenticate and restore executable programs from virus infection and virus-like modifications. The audit function is used to keep track of changes in program's inventory – like files that were added, removed or modified. Inventory changes are recorded in the audit log, including related data such as the computer name and user identification.

In the 'securing' phase, IVB32 takes a snapshot of critical information from each executable file and stores it in a database (signature) file, on a directory per directory basis. The information is then used during authentication (also called validation) to determine whether a file was modified by a virus. The database is also used to restore files that have been modified by viruses, as well as for auditing. IVB32 uses the same signatures database as its DOS equivalent, IVB, and the two programs are compatible with each other.

Viruses are characterized by unique properties: They replicate into other programs, they modify the host program in typical ways and they normally affect more than one program. All these anomalies are unmistakably detected by IVB32.

Select a topic on which you wish to get more information:

{button ,JI(`',`IDH_VINFO_GENERAL')} **A primer on computer viruses**

{button ,JI(`',`IDH_GEN_PATH')} **Audit and Integrity Expert System (AI) starting path specification.**

{button ,JI(`',`IDH_IVB_OPTIONS')} **AI options**

{button ,JI(`',`IDH_IVB_CMDLINE')} **AI command-line parameters**

Audit and Integrity (AI) Expert System command-line parameters

Most users won't ever need to run AI from the command line, so they may skip this section. Still, command line parameters are useful in corporate and network environment, in batch files, network scripts, or for scheduled operation. The general format of AI's command line is:

IVB32.EXE [*command-line parameters*]

Parameter should be separated by a space, and preceded by a slash (/) or hyphen (-). Parameters are case-insensitive. AI uses two parameter types: Boolean parameters (having just two states: 'true', denoted by the '+' sign and 'untrue', denoted with a minus '-' sign), and String parameters. The general format for Boolean parameters is:

/**ParameterName**[+|-]

When neither a plus nor minus is specified, then the default value assumed is 'true' (plus). The general format for String parameters is:

/ParameterName=*Value*

No spaces are allowed before or after the equal '=' sign. When the string *Value* contains spaces in it, then it should be enclosed in single or double quote marks. Follows a list of all IVB32's command line options:

Parameter	Type	Description
/all	Boolean	Scan all local drives. This parameter is the equivalent of *"All local hard drives"* radio button in AI's main menu.
/append	Boolean	Selects *"append to file"* mode for the report file.
/audit	Boolean	Enable the audit function.
/auditcomma	Boolean	Create a comma-delimited audit report instead of the default 'verbose' one; suitable for importing into databases.
/auditfile	String	Specify the audit report file name. Specifying an audit file name through the command line forces the audit mode and takes precedence over other 'audit' settings in the program's menu. There is no need for the **/audit** switch when **/auditfile** is used.
/autorenew	Boolean	Enable the auto renewing of a signature in the database, when AI determines that the change isn't due to viral causes.
/clean	Boolean	Restore files. Command-line representation of the *"Restore All"* radio button.
/ini	String	Sets the pathname of the .INI file to be used. When used, the directives contained in the designated INI file overrule those of the local machine's registry. Additional options specified in the command line overrule those in the registry or .INI file. **The order of precedence in which options are observed is as follows: Command line options are looked first, then those contained in the specified INI file, and the local machine's registry options are looked last – only if the specific option isn't defined in any of the former sets.**
/nostop	Boolean	Do not stop on errors and exit after the check completes, without pausing. Command line representation of the *"Exit when done"* check box.
/onlyonfinding	Boolean	Do not write anything to the report file unless changes in file(s) were detected.
/prompt	Boolean	Command line representation of the *"Ask on each"* radio button on the general page of the options dialog box.
/quiet	Boolean	Run minimized on the user machine, disable user's ability to intervene. **This is the supervisor mode switch, and together with the /ini option, above, does not have a counterpart in the GUI.**
/rpt2file	Boolean	Report to file. Also see below. Command line representation indicating that either *"append to file"* or *"replace the file"* is selected on the *"report file"* page of the options dialog box.

/rptcomma	Boolean	Create a comma-delimited report instead of the verbose default one.
/rptfile	String	Specify a name for the report file. Command line representation of *"Report file name"* in the *"Report file"* page of the options dialog. This directive overrides the *"No report"* status of the Report options page. No need to use the **/rpt2file** switch with this one, as the latter is inherently implied by this directive.
/scheduled	Boolean	Initiate in "scheduled run" mode. The program will start checking without waiting for the user's "Start" input, and will exit when done, on condition that there are no findings that require the user's decision. For automatic unattended operation, use **/scheduled** with the **/prompt-** and **/nostop+** switches.
/sigfname	String	Specify a **different than the default** filename to use, for the signature files database.
/singledir	Boolean	Command line representation of the *"Check subdirectories"* option. Use when checking of a single directory is needed.
/startdir	String	Start from the specified directory. If none is specified then the AI module will use the last value stored in the local registry. This is command-line representation of the *"From directory"* edit box in the main AI window. If used, this directive negates the *"All local drives"* (no need then to specify **/all-**)

Options dialog box

In this dialog box you can change the way the Audit and Integrity application operates. Select the topic on which you want to know more:

{button ,JI(`',`IDH_IVB_OPT_GENERAL')} **General**

{button ,JI(`',`IDH_IVB_OPT_SIG')} **Signatures**

{button ,JI(`',`IDH_IVB_OPT_AUDIT')} **Auditing**

{button ,JI(`',`IDH_IVB_OPT_REPORT')} **Reports**

{button ,JI(`',`IDH_IVB_OPT_INC_LST')} **Extensions**

{button ,JI(`',`IDH_IVB_OPT_EXC_LST')} **Excluded files & directories**

General options

Action

Choose the action to take when files are found to differ from their previously recorded state:

- **Warn & continue** – Report changes and continue.
- **Ask on Each** – Prompt the user each time a changed file is found.
- **Restore All** – Restore all files to their previous state.

Check Subdirectories

With this option selected, AI will process lower sub-directories, starting at the level of the directory selected.

Exit when done

With this option selected, Audit and Integrity will close as soon as it has completed its check.

Signature files options

Use the 'Signatures' page of the Options dialog box to specify your preferences.

Option	Effect
Auto renew signatures	With this option is selected, AI will automatically renew the signature of files which have changed due to a version upgrade or non-viral activity.
Signatures file attributes	Specify whether you want your signatures files attribute to be hidden, read-only or neither.
Signatures file name	For improved security, chose a different than the default signatures file name.

Audit report options

Use the 'Auditing' page of the Options dialog box to specify the audit mode and report configuration preferences.

Create audit reports

Check this box to enable the ***AI audit*** mode. With audit enabled, the inventory of program files will be audited for deletion, addition, and modification. Findings will be reported in the specified file.

Audit report file format

Two alternative formats of the report file exist:

- **Verbose** (verbal description).
- **Comma-delimited** (best suited for importing reports into databases).

Audit report file name

Denotes the path and file name for the audit report. A new audit report file will be created if one does not exist. Else, new data will be appended to the end of the existing file.

Report options

Use the 'Reports' page of the Options dialog box to specify your preferences for the report file.

Report file format

Two alternative formats of the report file are available:

- **Verbose** (verbal description).
- **Comma-delimited** (best suited for importing reports into databases).

On finding only

With this option selected, AI will only create or append the report file, if there are findings to report that need reporting.

Report file creation mode

The following options exist:

- **Append to file** - If a file with the specified pathname already exists, then append to it, else create a new one.
- **Replace the file** – Create a new file with the specified pathname, overwriting the former one,
- **No Report** – Do not create a report file at all.

Report file name

Designate an existing file to be used for the AI report, or specify a path and name to initialize a new report file.

File extensions checklist

Only files with extensions specified here will be checked by AI. Press **Reset** to revert to the default checklist, containing the following extensions: *386, BIN, COM, EXE, NLM, OVL, OVR, SYS, VLM, VXD*. You can add or remove extensions from the list, to speed up processing. Note that there is no point in adding extensions to the checklist, which do not belong to **binary executable** files. The above default checklist was optimized to cover most environments found in private PCs and networks.

Excluded files & directories

There are binary files that may change for non-viral reasons, like self-modifying executables, configuration files, etc. Such files can be excluded from the AI checklist by adding their names in the 'Exclude' list to avoid repeated and unnecessary reports of changes. The exceptions list accepts everything that complies with the DOS wildcard expansion rules.

Examples:

RANDSEED.BIN	Exclude RANDSEED.BIN from AI checklist
DRV*.BIN	Exclude all files which start with DRV and have extension .BIN
~*.*	Exclude all files having a tilde (~) as first character in their name
C:\Download*.*	Skip all files in the "C:\Download" directory

File restoration

You'll be presented with the following selection, when a modified file – compared to its last recorded signature - is found:

Option	Effect
Restore	Restore the file to its original state using the signatures file.
Secure	Update the signature file and continue. **Warning**: Use this options only when you are absolutely sure that the cause of change is legitimate and benign.
Skip	Do nothing for the moment, skip the file and continue.
Rename	Rename the file. The file's extension is changed to $$$, so that it cannot be accidentally executed, in case the modification was viral after all.
Delete	Delete the offending file.
Accept choice for all files	When this option is checked, no further user intervention will occur and the action selected now will be applied to all offending files.

The InVircible Macro Sweeper

Macro Trojans, bombs and viruses are the most prevalent threats to contemporary computing, especially in the corporate and network environment. InVircible provides both off-line (the Macro Sweeper) and on-line protection (the Macro Interceptor and Watchdogs) against these threats.

Macro Sweeper is and on-demand macro scanner that uses **generic** methods for detecting and deactivating macros in MS Word and Excel files. It thoroughly checks documents and templates for the presence of suspicious or active macros and has the ability to safely disarm them without damaging data contained in them and without compromising security.

For more information, select one of the following topics:

{button ,JI(`',`IDH_VINFO_GENERAL')} **Primer to Computer Viruses and Generic AV**

{button ,JI(`',`IDH_GEN_PATH')} **Macro Sweeper starting path specification.**

{button ,JI(`',`IDH_IVM_OPTIONS')} **Macro Sweeper Options**

{button ,JI(`',`IDH_IVM_CMDLINE')} **Macro Sweeper Command-line Parameters**

Macro Sweeper Command-line Parameters

Most users won't ever need to run Macro Sweeper from the command line, so they may skip this section. Still, command line parameters are useful in corporate and network environment, in batch files, network scripts, or for scheduled operation. The general format of Macro Sweeper's command line is:

IVM32.EXE [*command-line parameters*]

Parameters should be separated by spaces, and preceded by a slash (/) or hyphen (-). Parameter names are case-insensitive. Macro Sweeper uses two parameter types: Boolean parameters (having just two states: 'true', denoted by the '+' sign and 'untrue', denoted with a minus '-' sign), and String parameters. The general format for Boolean parameters is:

/**ParameterName**[+|-]

When neither a plus nor minus is specified, then the default value assumed is 'true' (plus). The general format for String parameters is:

/ParameterName=*Value*

No spaces are allowed before or after the equal '=' sign. When the string *Value* contains spaces in it, then it should be enclosed in single or double quote marks. Follows a list of all Macro Sweeper's command line options:

Parameter	Type	Description
/all	Boolean	Scan all local drives. This parameter is the equivalent of *"All local hard drives"* radio button in Macro Sweeper's main menu.
/append	Boolean	Selects *"Append to file"* mode for the report file.
/clean	Boolean	Deactivate macros. Command line representation of the *"Deactivate all"* radio button.
/daysold	String	Accelerated processing. Macro Sweeper will only check files that were created or modified during the last ***n*** days, where ***n*** is the number of days specified here. Note that specifying **/daysold=0** (zero) disables accelerated processing altogether.
/docs	Boolean	Check only files having extension names contained in the checklist. If negated, then check all files. This directive is the command line representation of the *"Check all files"* checkbox in the options dialog box.
/ini	String	Sets the pathname of the .INI file to be used. When used, the directives contained in the designated INI file overrule those of the local machine's registry. Additional options specified in the command line overrule those in the registry or .INI file. **The order of precedence in which options are observed is as follows: Command line options are looked first, then those contained in the specified INI file, and the local machine's registry options are looked last – only if the specific option isn't defined in any of the former sets.**
/nostop	Boolean	Do not stop on errors and exit after the check completes, without pausing. Command line representation of the *"Exit when done"* check box.
/prompt	Boolean	Command line representation of the *"Ask on each"* radio button on the general page of the options dialog box.
/onlyonfinding	Boolean	Do not write anything to the report file unless changes in file(s) were detected.
/quiet	Boolean	Run minimized on the user machine, disable user's ability to intervene. **This is the supervisor mode switch, and together with the /ini option, above, does not have a counterpart in the GUI.**
/rpt2file	Boolean	Report to file. Also see below. Command line representation indicating that either *"append to file"* or *"replace the file"* is selected on the *"report file"* page of the options dialog box.
/rptcomma	Boolean	Create a comma-delimited report instead of the verbose default one.
/rptfile	String	Specify a name for the report file. Command line representation of *"Report file name"* in the *"Report file"* page of the options dialog. This directive overrides the

		"No report" status of the Report options page. No need to use the **/rpt2file** switch with this one, as the latter is inherently implied by this directive.
/scheduled	Boolean	Initiate in "scheduled run" mode. The program will start checking without waiting for the user's "Start" input, and will exit when done, on condition that there are no findings that require the user's decision. For automatic unattended operation, use **/scheduled** with the **/prompt-** and **/nostop+** switches.
/singledir	Boolean	Command line representation of the *"Check subdirectories"* option. Use when checking of a single directory is needed.
/startdir	String	Start from the specified directory. If none is specified then Macro Sweeper will use the last value stored in the local registry. This is command-line representation of the *"From directory"* edit box in the main window. If used, this directive negates the *"All local drives"* (no need then to specify **/all-**)

Options dialog box

Here you can change the way Macro Sweeper operates. Select one of the following to get help on specific options.

{button ,JI(`',`IDH_IVM_OPT_GENERAL')} **General**

{button ,JI(`',`IDH_IVM_OPT_CRITERIA')} **Select criteria**

{button ,JI(`',`IDH_IVM_OPT_REPORT')} **Report file**

{button ,JI(`',`IDH_IVM_OPT_EXC_LST')} **Excluded files & directories**

General Options

Action

Choose the action to take when active or suspicious macros are found:

- **Warn & continue -** Report findings and continue.
- **Ask on Each** - Prompt the user every time an irregular file is found.
- **Clean All** - Disable or rename all suspicious macros.

Check Subdirectories

With this option selected, Macro Sweeper will process lower sub-directories, starting at the level of the directory selected.

Exit when done

With this option selected, Macro Sweeper will close as soon as it has completed its check.

Select criteria

Check all files

With this box checked, all files will be checked regardless of their extension name, ignoring the **file extensions checklist**.

Accelerated processing

With **Check created/modified** checked, Macro Sweeper will only check files that were created or modified within the last *n* days, where *n* is the number specified in the **within last...** box. The default is 'last 7 days'.

File extensions checklist

Macro Sweeper will check all files regardless of their extension name, when **Check all files** box is checked. Otherwise, only files with extension names contained in the checklist will be checked. The default checklist contains *.DOC and *.DOT.

Report options

Use the 'Reports' page of the Options dialog box to specify your preferences for the report file.

Report file format

Two alternative formats of the report file are available:

- **Verbose** (verbal description).
- **Comma-delimited** (best suited for importing reports into databases).

On finding only

With this option selected, Macro Sweeper will only create or append the report file, if there are findings to report that need reporting.

Report file creation mode

The following options exist:

- **Append to file** - If a file with the specified pathname already exists, then append to it, else create a new one.
- **Replace the file** – Create a new file with the specified pathname, overwriting the former one,
- **No Report** – Do not create a report file at all.

Report file name

Designate an existing file to be used for the Macro Sweeper report, or specify a path and name to initialize a new report file.

Excluded files & directories

Macro Sweeper provides for excluding specific documents and templates from its checklist. This could be necessary for not ruining customized templates, or fancy Word and Excel documents with active macros. You may add to the exceptions list every file specification that complies with the DOS wildcard expansion rules.

Examples:

MY_FORM.DOT	Exclude the My_Form template from Macro Sweeper checklist
***.TMP**	Exclude all files having a TMP extension name
~*.*	Exclude all files having a tilde (~) as first character in their name
C:\HushDocs*.*	Skip all files in the "C:\HushDocs" directory

Custom Worksheet Names

This list contains names of Excel worksheets that are known to contain viral macro code. IV Interceptor and IV Macro Sweeper will detect and clean Excel documents that contain these worksheets.

Deactivating macros in Word or Excel files

Macro Sweeper warns when active macros are found in a Word document, or suspicious macros are present in a Word template, or when specific sheet names are found in an Excel workbook. Macro Sweeper then prompts to chose from the following list of options:

- Disable or rename macros (depending on whether a document, worksheet or template was flagged).
- Do nothing, continue checking.
- Cancel checking.

Press this button to add a new item to the list of suspicious Excel worksheets.

Press this button to remove currently selected item from the list of suspicious Excel worksheets.

Real-time Protection Against Macro Threats

On-demand macro screening does not suffice for countering the threats posed by macro malware. Word documents and Excel worksheets attached to e-mail, or received via internal mail, may contain a payload that executes immediately on opening the file, before even having the chance to scan it. InVircible provides real-time protection against such macro threats.

IV's real-time macro protection are of two sort: The *IV Interceptor* and the *IV Watchdogs* (there are two watchdog types). However resembling, they present different approaches and provide different levels of protection.

The following table shows their use and capabilities:

Feature	IV Interceptor	IV Watchdogs
Runs under Windows 95	✔	
Runs under Windows NT 4.0	✔	✔
Runs under Windows NT 3.xx	✔	✔
Runs under Windows 3.xx	✔	✔
Checks files opened by MS Word	✔	✔
Checks files executed by Association	✔	✔
Checks files opened by **any** program	✔	✔
Deactivates macros on the fly	✔	✔
Process other than doc/dot extensions	✔	

Which one to use and when?

IV's installation provides for installing both the interceptor and the watchdogs on Windows 95/98 and NT 4.xx platforms. Only the watchdogs will be installed on NT 3.xx and Windows 3.xx platforms. In daily usage, the interceptor provides for maximum security and protection. Yet, there are instances in which the deactivation of the IV Interceptor may be necessary. Even then, the Watchdogs will still provide real-time protection against macro malware.

Although they use the same methods and algorithms, the interceptor and the watchdogs are implemented in different ways. The interceptor uses a Virtual Device Driver (VxD) or System Driver (SYS) running in Windows' background, that monitors all attempt to open a Word or Excel files. The Watchdogs, on the other hand, are dormant most of the time and only wake up on specific events – such as an attempt to open a Word or Excel file. IVI and the Watchdogs may seem to perform redundant functions, but they are not. IVI and the Watchdogs act together in a multi-layer protection scheme. There are instances in which the Interceptor could be deactivated, like when processing multiple documents on a server, with marginal network performance. Even then, the Watchdogs will still provide ample of real-time protection against macro malware.

For more details, press a button from those below:

{button ,JI(`',`IDH_IVRT_IVIMAIN')} **IV Interceptor.**

{button ,JI(`',`IDH_IVRT_DOGMAIN')} **IV Watchdog.**

IV Interceptor (IVI) General Information

The IV Interceptor (IVI) is a generic real-time protection tool to protect from Word and Excel macro malware and PE infectors. Portable Executable (PE) are EXE-type files used by Windows 95, 98 and NT. IVI monitors all attempts to open Word or Excel documents and templates as well as PE EXE files. Word document files are verified by IVI for the presence of active macros, while templates are checked for the presence of only suspicious ones. Excel documents are checked for the presence of known infected macro worksheets. PE-EXE files are checked for the presence of Windows EXE viruses (PEI – PE infectors). If any of the above is found, then IVI issues a warning message, or deactivates the offending macros on the fly, depending on the default settings of IVI.

IVI is the most dependable real-time protection against macro malware and Windows EXE viruses. IVI is also the least obtrusive virus protection. IVI generically detects macros, and can remove them while accessing Word files, no matter how they are opened, e.g. like copying DOC files from a floppy to your hard drive. IV Interceptor handles malicious macros of all sorts, not only viruses, like macro Trojans and bombs, as well as PE-EXE viruses, both known and unknown.

If you run Windows 95/98 and need maximum protection, then IV Interceptor is your best choice.

Select one of the buttons below for more detailed information:

{button ,JI(`',`IDH_IVRT_IVIUSE')} **Using IV Interceptor.**

{button ,JI(`',`IDH_IVRT_IVIOPT')} **IVI options.**

Using IV Interceptor

When IV Interceptor is installed on your system, it will automatically load at Windows startup and install an icon on the desktop taskbar, having the following appearance:  . A menu will appears on clicking the IV icon on the taskbar. Select an item from the following list to get help on the menu entry:

- Interceptor Active
- Interceptor Options...
- Help Topics...
- InVircible Web Site...
- **Macro Sweeper...**
- Audit / Integrity...
- Watchdog options...
- IV Scheduler...
- Unload Interceptor

Note: A grayed out item in the above menu indicates that the respective component is not installed.

Select one of the buttons below for more information:

{button ,JI(`',`IDH_IVRT_IVIMAIN')} **IV Interceptor general information.**

{button ,JI(`',`IDH_IVRT_IVIOPT')} **IVI options.**

Switch IV Interceptor into *active* or *standby* mode without unloading from memory. The presence of the check mark and the icon being green indicate IVI is active. When in standby, the check mark disappears and the icon turns red.

Select 'Interceptor Options' to configure IV Interceptor to your preferences.

Select 'Help Topics' to view this help file.

Select 'InVircible Web Site' to open InVircible Web Site URL in your WWW Browser.

Start Macro Sweeper – The generic on-demand macro virus scanner.

Start Audit and Integrity Expert System.

Change the IV Watchdog options.

Start IV Scheduler.

Unload IVI from memory. To restart IVI, select its icon from the InVircible programs group.

IV Interceptor Options

Select "**Options...**" from the pop-up menu to specify your preferences for the configuration of IVI.

General Options

Deactivate macros on the fly

When this box is checked, then all suspicious and active macros will be deactivated **without** prompting the user first. Set this option on only when absolutely sure that there are no 'fancy' documents that could trigger the IV Interceptor alarm.

Don't show IV Interceptor messages

When this box is checked, IVI runs in 'quiet' mode. Access to offending files will be denied and no IVI dialog box will be displayed. The only indication the user will get is an "Access denied...." message from the application that tried to open the offending file.

Check all files

When this box is checked, then all files fill be checked for macros regardless of the extensions specified in the Word file extensions checklist. The *exceptions list* will be taken into account, however.

Load with Windows

When this box is checked, IV Interceptor will load every time Windows is started.

Exclude and Include lists

File extensions checklist

The macro portion of IVI will check all files for macro malware regardless of their extension name, when **Check all files** box is checked. Otherwise, only files with extension names contained in the checklist will be checked. The default checklist contains *.DOC and *.DOT.

Macro Exclude List

IV Interceptor and Macro Sweeper provide for excluding specific documents and templates from their checklist. This could be necessary for not ruining customized templates, or fancy Word documents with active macros. You may add to the exceptions list every file specification that complies with the DOS wildcard expansion rules.

Examples:

MY_FORM.DOT	Exclude the My_Form template from Macro Sweeper checklist
***.TMP**	Exclude all files having a TMP extension name
~*.*	Exclude all files having a tilde (~) as first character in their name
C:\HushDocs*.*	Skip all files in the "C:\HushDocs" directory

Executables Exclude List

This list is similar to Macro Exclude checklist. It contains the names of EXE files that trigger IVI PE Infector alarm, but are not infected.

Custom Worksheet Names

This list contains names of Excel worksheets that are known to contain viral macro code. IV Interceptor and IV Macro Sweeper will detect and clean Excel documents that contain these worksheets. To add a new Excel virus to IVI's list, just find out the name of the offending sheet, and add it to the list.

IV Interceptor Warning Dialog Box

IVI intercepted an attempt to open an offending document or template. The user is now prompted to provide instructions for IV Interceptor:

- **NO** – Do not let the application to open the file. This is the default option.
- **YES** – Deactivate the offending macros in documents, or rename them in templates. Note that the "file open" operation has been already canceled at this stage. If you still wish to open the inert file, then you will have to repeat the request for its opening.

Note that the IVI warning dialog box has a time-out period, to avoid clutter on the Windows desktop. If no action is taken during the time-out period then IVI will silently close the warning box and will not perform any further action on this file.

IV Interceptor Warning Dialog Box

IVI intercepted and denied the opening or execution of an offending EXE file. If you are absolutely sure that this file is not infected by a virus, you can add its name to the IVI PE Infectors exclude list, to prevent further false alerts.

Note that the IVI warning dialog box has a time-out period, to avoid clutter on the Windows desktop. If no action is taken during the time-out period then IVI will silently close the warning box.

IV Interceptor Information Dialog Box

IV has intercepted an attempt to open a file containing offending macros. The offending macros were deactivated, or renamed, if in a template.

Note that the information box has a time-out period. If no action is taken during the time out delay then IVI assumes that the computer is unattended and the box will close, after the time-out delay.

IV Watchdog General Information

IV Watchdog is a generic real-time macro protection tool. The level of protection that the Watchdog provides against macro malware is comparable to that provided by IVI. However, while IVI can only run on Windows 95, the IV Watchdogs run on all Windows platforms. IV Watchdog consists of two modules:

1. The first one intercepts attempts to open .DOC or .DOT files via Windows extension association. This module protects from opening Word files from File Manager / Program Manager / Windows Explorer / Microsoft Internet Explorer / Netscape Navigator / E-mail readers etc. Files with .DOC and .DOT extensions will be first verified and processed by Watchdog and then opened normally.
2. Another watchdog module consists of a special Word template and a DLL. It will check files that are open from within Microsoft Word, with File | Open.

The two watchdogs complement each other, and together they provide effective real-time on-access protection against macro malware.

Click the button below to learn how to use IV Watchdog:

{button ,JI(`',`IDH_IVRT_DOGUSE')} **Using IV Watchdog.**

Using IV Watchdog

Since IV Watchdog isn't constantly present in memory, then you may notice nothing that discloses that it is watching… until macro malware strikes. It may be an e-mail attachment infected with a macro virus, or a suspicious template, or a macro bomb sent by internal mail, etc. In any of these cases you'll see the dialog box informing that an offending file is about to be opened, and asking you to choose what to do next. Your options then are:

- **Don't open file** – Cancel the "open file" operation.
- **Ignore and continue** – Ignore the warning and let Word open the file.

NOTE: Use this option only if absolutely sure that the file is benign and does not contain malicious macro code.

- **Deactivate macros and open** – Deactivate all active macros and then let Word open the file.
- **Add to exceptions list** – Add the file name to the exceptions list (IVX.INI) and let Word open it.

You may chose '**Deactivate macros and open'** file as the watchdogs' default action, i.e. automatically deactivate / rename **all** macros in flagged files without further prompting the user. The default watchdog options can be changed as follows:

- From Word's menu, by selecting **Tools | IV Watchdog Options...**
- From the IVI popup menu, on Windows 95 taskbar, selecting 'Watchdog options',
- or simply executing IV Watchdog by double clicking its icon in Program Manager or Explorer's Start menu.

NOTE: Since the proper operation of IV Watchdog depends on the file extension association to be correctly set, then it is important to re-create the association each time you re-install MS Word or change the .DOC or .DOT associations in any other way. To re-create the IV Watchdog association with Word files, run either the second or the third option, above.

Tip: Windows 95 and NT provide a visual cue that the association to .DOC and .DOT extensions is assigned to the IV Watchdog. The familiar icon for Word files (a sheet with capital W at top left) changes to a sheet with a golden 'IV' at top left, when assigned to IV Watchdog.

IV Scheduler

Computer viruses are easy to combat, on condition that their presence is detected before they have a chance to spread too far. The Scheduler is a powerful addition to InVircible that helps implementing effective virus protection in the single user environment, as well as in the corporate/network environment in particular. IV Scheduler permits running the Macro Sweeper and the Integrity module on a regular and timely basis, without having to start them manually.

IV Scheduler lets you configure the frequency and time at which either, or both Macro Sweeper and AI will execute. Press one of the two ***Schedule*** buttons to set its respective application's agenda.

IV Scheduler is in no way a substitute for the built-in NT scheduler service, *IVSched* is devised to run a single task of either or both AI and Macro Sweeper, under Windows 95 and NT. To run multiple and simultaneous AI and Macro Sweeper tasks (possible only under NT), run IVB32 and IVM32 with command line syntax, from script (batch) files and schedule them as NT's AT tasks. Consult the NT reference manual for "AT" command syntax, or type "AT /?" at the NT command prompt.

For in-depth discussion of IV Scheduler usage and its options, press one of the buttons below:

{button ,JI(`',`IDH_IVSC_BACKGROUND')} Using IV Scheduler on Windows 95 and NT

{button ,JI(`',`IDH_IVSC_OPTIONS')} IV Scheduler options

IV Scheduler options

Both AI and Macro Sweeper have similar scheduling options. However, their scheduling is independent of each other. Therefore, you can configure each the way you like.

The following parameters can be set in each application's agenda:

- Day(s) of execution
- Time of execution
- Mode of execution
- Starting directory

Day(s) of execution

An application may be scheduled to execute every day, or on a particular day once a week. The **Day** combo box lets you specify your preferences. Specifying *Never* disables the respective application schedule altogether.

Time of execution

The following modes are available:

- **Windows startup** – The selected application, AI or the Macro Sweeper will start as part of Windows startup. This mode is recommended for standalone PCs and workstations that are restarted daily.
- **Specific time** – The program will run at a specified time, every day. This mode is recommended for workstations that run continuously.
- **Every ...** – The program will run multiple times a day. For example, setting *Every 4 hours* will run at 00:00, 04:00, 08:00, 12:00, 16:00 and 20:00 hours. This mode is recommended for monitoring network file servers.

Mode of execution

Select between *attended* and *unattended* operation. In unattended mode, the program will not pause for user input. Therefore, you must also supply the default action to be taken in case there are findings. In unattended mode, the program will close when done regardless of whether there were findings or not.

Starting directory

The default for this option is ***check all local drives***. Change it to check a different computer than the local one, like for scheduling a server check from a workstation, or checking another workstation than your own. UNC path, computer or workgroup/domain names are acceptable here, as well as elsewhere in InVircible 32.

Using IV Scheduler

Using IV Scheduler on Windows 95

After you install IV Scheduler during the setup procedure, either manual or automatic, IV Scheduler will be started each time you log into your Windows 95 workstation. It will execute IVB or IVM if any of them are scheduled to be run on Windows startup and this is the first login today, and then it will terminate itself immediately if there's no more scheduled jobs. If there's a job pending, IV Scheduler will remain active and will be terminated after you log out. It means that when IV Scheduler runs, all your network connections are already restored and, thus, you can easily schedule checking of other computers on the network. But, when there's no one logged in, the IV Scheduler is not running and the checking will not be carried out.

Using IV Scheduler on Windows NT

The Windows NT version of IV Scheduler is implemented as an NT service. The IV scheduler service is started every time the computer , NT server or workstation, is started and remains active till system shutdown. Since this service uses very little system resources, it will not noticeably increase the load on your system. When you are only interested in checking files on the local system, then no further steps are required for using IV Scheduler, after being successfully installed.

However, if you wish to verify files located on other computers on the network, when no one is logged in (unattended machine), then the service needs further setting up. Any program that needs network resources must supply a user name and password to access them. To set the IV scheduler user identity, proceed as follows:

1. Be sure you have Administrator privileges.
2. On the local machine, open the Control Panel
3. Open the "Services" applet
4. Select the service named "IV Scheduler"
5. Click on the "Startup..." button
6. Select "This account" radio button
7. Provide a username and password of the account. Be sure that the user given has sufficient privileges to access all network resources that you wish to check with IV Scheduler and its spawns (Macro Sweeper and Audit and Integrity Expert System)
8. Press Ok.

Now, you can use IV Scheduler to check other computers on the network from an unattended NT machine, with no user lodgged in.

Important: Since IV Scheduler is tightly integrated into the core services of the Windows 95 and Windows NT operating systems, it should be installed or uninstalled only by using the IV's native install and uninstall facilities.

A Primer on Viruses and Generic AV

Computer viruses are just computer code, deliberately written to serve a purpose - to replicate, there is absolutely nothing mysterious about them. There exist thousands of them – more than 20,000 in mid 1998, including more than 2,000 macro viruses of Word and Excel, and new viruses add to the list every day.

Computer viruses are passed in many ways; by sharing software, in Word documents and in Excel worksheets, by downloading files from the Internet, in e-mail attachments, with OEM software bundled with computers, and sometimes even on pre-formatted floppies. There exist no way to prevent ever picking a computer virus, except by never using a computer at all, just the same as one cannot avoid ever getting ill.

The threats that should raise most concern are those imposed by MS Word and Excel macros, and the new PE (Portable Executable) infectors, affecting Windows 95/98 and NT programs.

Macro viruses first appeared only in the summer of 1995. Since then, their number increased at the highest rate – 300 new macro viruses or variants per month – compared to the 'traditional' boot and program infectors, the latter 'suffer' from a rapidly decreasing production rate. The reasons are:

- MS Word, as well as Excel, are in common use as means of data interchange in both the private sector and in the corporate environment.
- What's required to write macro malware are just Word, or Excel itself, and minimum knowledge on how to use the Microsoft macro language. If writing virus code was in reach of thousands before, then tens of millions, maybe more, of users can now write macro malware. Corporate internal e-mail, the Internet and the increasing dependence on communication and data sharing makes the distribution of malware extremely easy.

There is a trend in macro malware that should raise even more concern. While conventional viruses found in the wild do not have an immediately destructive payload – as if they had, then their chances to spread would be nil, many macros are found to have a 'short fuse' until they trigger destructive routines. 'MDMA' (clears the entire C:\ root directory on the first of every month) and 'Appder' (kills crucial files in ..\Windows and ..\Windows\System the twentieth time Word is started), are just a couple of such macros. Since the appearance of this new threat, 'known' macro viruses aren't the real problem anymore. The threat are **macro Trojans and bombs that are built in-house**, based on techniques used in macro viruses. The latter techniques are now common knowledge, as result of macro viruses being so widely spread. No virus scanner, even the most up-to-date one, won't protect you from these new threats.

InVircible protects against both know and new macro threats, including macro Trojans and bombs, thanks to the generic methods it uses and its real-time capabilities.

The first PE infector (Boza) appeared shortly after Windows 95 was rolled out, yet PEI didn't constitute a real threat until recently, with the appearance of new PE infectors, some of them even got spread widely in the wild. Version 7.02 of InVircible was improved to generically handle this new class of viruses, both on-access and on-demand.

Click one of the buttons below for more information about computer viruses and how to fight them:

{button ,JI(`',`IDH_VINFO_CATEGORY')} **Categories of Computer Viruses**

{button ,JI(`',`IDH_VINFO_TECH')} **Techniques used by Computer Viruses**

Categories of Computer Viruses

Generally, there exist three virus categories listed below by decreasing order of their prevalence in the wild:

- Macro viruses. They affect MS Word documents and Excel worksheets.
- Viruses that infect through the boot sector or partition sector (MBR), known as 'boot infectors'
- Viruses that infect through executable programs, known as ‘file infectors'.
- Viruses that uniquely infect Windows 95/98 and NT PE (Portable Executable) objects, known as ‘PE infectors’ or PEI.

All DOS viruses fall into one of the last two categories or both. There are also bipartite or multipartite viruses that combine the properties of the two categories (boot and file). Examples of common multipartite infectors are Junkie and Natas.

In late 1991, a new variant of file viruses emerged, known as cluster infectors. These viruses manipulate the file allocation table (FAT) pointers through the directory entries in order to infect. To this date, there are only three cluster infectors known to be in the wild, only two of survive in later than the Dos 5.0 environment.

A last type are the 'companion viruses', these are a variant on the file infector. A companion virus takes advantage of the properties of the operating system by spawning a companion to the victim program.

Below is a quick definition of terms that are used to describe viruses and techniques employed by viruses:

Macro Viruses

Most macro viruses known to be in the wild infect MS Word files, yet there exist macros that infect Excel files, although the latter are far less common than Word macro infectors. Word macro viruses replicate into other documents by first copying themselves into the Word global template (normal.dot). Then, the virus macros copy themselves into other documents, when opened or created with the affected template. In order to assure the virus succession, infected documents are saved as templates, as only the latter can have active macros in them.

Excel macro viruses show a less distinctive pattern, when compared to Word viruses. From the few that exist, they all replicate by creating their own workbook, containing an auto startup macro (auto_open), and place that workbook in the Excel startup directory – normally ..\Excel\XLStart.

InVircible handles Word macros with Macro Sweeper and the IV Watchdogs. Excel macros are taken care of by IVXcel.

PE Infectors

Portable Executable (PE) objects were introduced with Windows 95 and NT. PE EXE files have a more complex structure than ordinary DOS executable files (EXE) and until recently, PE were considered beyond the reach of virus writers. Yet in mid-1998, a number of new PE infectors that were released in the wild became globally wild spread.

PE infectors are taken care of InVircible on several levels, both by the basic DOS modules and in the 32 bit Windows version as well. For screening EXE downloads and new software against PEI, use the InVircible’s Rule Based Scanner – IVZ, contained in the DOS IV package. For maximum protection under Windows 95 and 98, use the on-access IV Interceptor, IVI95. The latter intercepts any attempt to open an infected PE-EXE object.

Boot Viruses

Boot viruses attack the boot sector and the MBR (master boot record, sometimes referred to as the partition sector). When the computer is turned on, it runs a couple of tiny program contained in these special sectors, first the partition bootstrap and then the system bootstrap, to ready itself for work. In case of a boot infection, one of these programs may simply be a virus. Boot viruses will remain active in memory while the computer is on. During this time they will infect write enabled floppies put in the floppy drive.

Boot infectors are taken care of by InVircible during the startup process.

File (Program) Infectors

File infectors attacks executable program files, usually those having a COM or EXE extension name. Sometimes also files having an executable structure are targeted by viruses, regardless of their extension name. File infectors may corrupt non-executable files as well but they cannot spread this way.

Many file viruses are memory resident (TSR). After an infected file is executed, they will remain resident in the computer's memory until the computer is turned off. While in memory they will continue to infect other programs and may interfere with normal operations. If the computer is turned off they will lie dormant in an infected file until the program is executed and then load themselves back into memory again until the next time the computer is turned off.

File infectors are handled by the InVircible integrity monitoring and restoration tools, by IVB when under DOS and by IVB32, under Windows 95 and NT. Both tools share the same signatures database and are compatible with each other.

Multipartite Viruses (boot and file infectors)

Multipartite viruses infect both executable files and boot-partition sectors, sometimes the boot sector on floppies too. Some multipartite become infectious only after rebooting the computer from the infected MBR, like Tequila, others are equally infectious if loaded from file or through the boot process.

Techniques used by Computer Viruses

Stealth

Stealth viruses are so named because they actively seek to hide themselves to prevent detection. Stealth viruses that infect files will subtract their own size (in bytes) from the infected host file at any time that a directory (DIR) command is executed or actually remove themselves from the file, to reinfect it again when the inspection is over.

Stealth file infectors are effectively handled by InVircible for DOS. For more information see in the IV on-line hypertext manual for DOS.

Some boot viruses use stealth (spoofing) techniques too. Stealth boot viruses will deceit disk editing tools, except ResQdisk. Examples of stealth boot viruses are Monkey, AntiEXE and B1-NYB. Natas and Gingerbread Man are multipartite viruses that use boot stealth too.

Stealth boot infectors are effectively handled by the InVircible SeeThru technique, implemented in IV for DOS. For more information see in the IV on-line hypertext manual for DOS.

Encryption

Most of modern viruses use encryption to evade detection by scanners. An encrypted virus has a very short common encryptor (from as few as 3 bytes, to a couple of dozen bytes) and the rest of the virus code is encrypted and differs from copy to copy of the virus. The detection of encrypted viruses cause high false alarm rates due to the ambiguity in the detection of the short common string. The removal of encrypted viruses by scanners is rather difficult, in many instances it may result in the destruction of the program (especially in case of virus misidentification, which is very likely given their large numbers) and in even more instances – is simply impossible.

The InVircible integrity and restoration tools, IVB and IVB32, handle with equal success files which are infected with plain or encrypted viruses, no matter how complex the encryption is. The IV integrity tools can restore programs from no matter what infector, encrypted or not, known or new.

Mutation Engine or Polymorphism

Polymorphic viruses have variable encryption. A polymorphic virus mutates itself so that the encryption varies between each occurrence of an infection. The detection of polymorphic viruses requires more complex than just plain string matching methods, like heuristics, which slows down scanning speed and increases false alarm rate. The detection and recovery from polymorphic viruses by scanner is even more difficult and dubious than with just encrypted viruses.

The InVircible integrity and restoration tools handle equally well polymorphic viruses, just the same as plain file infectors. Actually, InVircible's generic restoration from is the fastest way to fully recover from infections that scanners cannot handle at all.

Companion Viruses

Companion viruses take advantage of the precedence DOS gives to COM over EXE files in the order of execution. If there are two files bearing the same name, one with a COM extension name and the other with an EXE extension, then DOS will execute the COM file first. A companion virus is basically a Trojan that "infects" EXE files by spawning itself into a companion COM file, bearing the same name as the EXE file. Sometimes the companion virus file will have its attribute set to 'hidden', to avoid its detection by the DIR command.

Companion viruses are generically handled by IVB, from the IV DOS package. For more information see in the IV on-line hypertext manual for DOS.

Distribution and Management Utilities for Networks

InVircible contains administration tools to assist system managers to configure, distribute and manage the software throughout the organization. The migration utility, *IVWLOGIN*, automatically installs InVircible from the server to all workstations, without requiring user intervention. The configuration utility, *IVCONFIG*, is used to set the installation profile and control the working parameters of IV on the clients' workstations. The sole requirement is that your network software must support login scripts. All major network systems, like Windows NT and NetWare are supported.

The Configuration Utility - IVConfig

The Configuration Utility sets which components of InVircible are to be installed, as well as the working parameters of each of these components, after having been installed to their destination. Options of the IV applications can be changed, and some restrictions on the use of these programs may be imposed as well. The IV Configuration utility saves the settings data in a file, so that different setups may be created for all users, for groups, or individual users.

The Migration Utility - IVWLogin

The Migration Utility is designed for use in a network login script. When invoked from a script, *IVWLogin* checks for the presence of an up-to-date copy of InVircible on the logging workstation, as well as for its IV parameters settings. Depending on the findings, IVWLogin determines what action to take, such as doing nothing – if IV exists and is properly set, or upgrade the version - in case the version found on the workstation is older than the one on the server, or install from scratch – in case no IV installation can be is found on the workstation.

For more details on a specific topic, select from the following:

{button ,JI(`',`IDH_CFG_SETUP')} Setting Up Distribution in the Network

{button ,JI(`',`IDH_CFG_OPTIONS')} The Configuration Utility

{button ,JI(`',`IDH_CFG_MENU')} Configuration Utility Menu Commands

Setting Up IV Distribution in the Network

Setting the network distribution profile of InVircible involves three steps:

- Installation of InVircible on the server
- Creating a configuration file(s) with the IV Configuration utility
- Making the necessary changes to the network login script

Installing InVircible on the server

Since you are reading this help file, then it's obvious that you have already installed InVircible. In case you have not installed the IV Configuration utility (the latter is not selected by default in the setup program), then simply re-install InVircible. This time, take care checking the "Network Install Tools" box in step 1 of the IV Setup program. The new installation will retain all your custom settings.

Creating a setup configuration file with IVConfig

Run the IV Configuration utility by double clicking the ***IVConfig*** icon in the InVircible program group, and configure future installations the way you prefer. Finally, save these settings in an INI file. See IV Configuration Utility options for further information on how to save INI files.

Modifying the Network Login Script

1. In Windows NT:

To automatically distribute InVircible through a workstation log-in process, insert the following command line into the network login script:

\\SERVER\IVW32-PATH\IVWLOGIN.EXE [/ForceOpt] **\\SERVER\INI-PATH\INI-NAME.INI**

Substitute **\\SERVER** with the actual name of the server from which IV is to be taken, and **IVW32-PATH** and **INI-PATH** with the appropriate sharenames and pathnames of your InVircible installation on the server. Do the same for the setup file and its whereabouts, in **INI-NAME.INI**, above. The optional switch /ForceOut forces IVWLOGIN to set all user options to those specified in the INI file on each login. Please note that this procedure creates significant network traffic and should be avoided when possible. It is advised to store your *.INI files in the InVircible directory on the server, and to create special read-only share pointing to this directory. This way, you can simplify the setup and eliminate the possibility of InVircible files being accidentally modified or erased by an unauthorized user.

2. In Novell NetWare:

First, install InVircible to the server. It is strongly advised to install InVircible into a dedicated directory under the **NetWare default attachment directory** (see below for details). It is also recommended that the installation to the server is done manually, you will need to do it only once. Create the target directory on the server. Next, unarchive the files from the setup program into the newly created directory, with the command: PKUNZIP IVWINST.EXE.

To automatically distribute InVircible through the log-in process, you will need to edit the system login script. In Netware 3.1x, run SYSCON, select 'Supervisor Options', then System Login Script. Under NetWare 4.xx the process is similar, just run NETADMIN (or NWADMIN, if supervising NetWare from a Windows console) in lieu of SYSCON, to access the login script editing menu.

Finally, add the following command to the system login script:

 # NETWARE_PATH\IVW32-PATH\IVWLOGIN.EXE NETWARE_PATH\INI-PATH\INI-NAME.INI

The # (hash) prefix means "execute the following external command", in NetWare syntax. Substitute **NETWARE_PATH** with the NetWare default attachment directory. The specific **NETWARE_PATH** in every system depends on the particular configuration of that system.

To find out the default NetWare login directory in your system proceed as follows:

Start NetWare manually – not with its net-start batch or script – but rather in a step by step fashion. Run single commands, one at a time, for example: LSL, NE2000, IPXODI, and finally NETX or VLM.

At this stage you are attached to the server, but not logged in yet. Note the difference between being "attached"

and "logged in". Do NOT run LOGIN.EXE yet.

After attaching to the server, as explained above, change to F: and note the name of the current directory. It should normally be F:\LOGIN, or just F:\. At this point, you need to establish the full pathname, **from the default NetWare attachment directory, to the InVircible installation directory**. The following example will clarify the issue.

Suppose that the default attachment directory is F:\LOGIN, and that the DIR command shows the presence of a sub-directory named IVWIN, to which InVircible was installed. Therefore, the NETWARE_PATH in this case will be F:IVWIN. Note there is no backslash after F:, as the latter logs you directly into the default NetWare attachment directory. The full command line to be inserted into the system script then is:

 # F:IVWIN\IVWLOGIN.EXE F:IVWIN\INI-NAME.INI

It is advised that you store your *.INI files in the InVircible directory on the server, and assure that the users' permissions in this directory are 'read-only'. This way, you can simplify the setup and eliminate the possibility of the InVircible files from being accidentally modified or affected by an unauthorized user.

The Configuration Utility

The IV Configuration Utility screen is divided into two parts. In the upper one, you can specify the destination path where to install InVircible on the target machines. If the specified directory does not exist, it will be created automatically, even if the destination directory to create is deeper than a single level.

The lower part of the IVConfig screen is sub-divided into setup pages, each handles the installation parameters of the following IV applications and functions:

- Audit & Integrity
- Macro Sweeper
- Real-time protection
- IV Scheduler

Check each of the setup page tick-boxes to install the corresponding component on the target system.

Audit & Integrity; Macro Sweeper

Since the setup pages of the two applications are nearly identical, then the following applies to both:

1. **Permissions:**
   The permissions boxes control whether the user can restore files with IVB32, deactivate macros with IVM32, and change these options on his machine, after IV has been installed.
2. **Exceptions list:**
   With the Allow to change box cleared, the user can not add or delete any item in the exception lists.
   Checking Use remote means that AI or the Macro Sweeper will read the exception lists entries saved in a specified .INI file and add them to the local list. The exceptions list of all workstations can be maintained centrally, by checking 'Use Remote' and updating the appropriate .INI file, only. The workstations' exceptions list will be updated every time the related application is invoked.
3. **Options button:**
   Press this button to change the general options of the related program.

Run-time protection

See IV Interceptor options for details.

IV Scheduler

Press the **Schedule** button to setup its respective application scheduling. See IV Scheduler for details.

Configuration Utility Menu Commands

File | **Open**	– Open an existing .INI file
File | **Save**	– Save the current settings into the currently open .INI file
File | **Save As**	– Save current settings to an .INI file under a different name or path
File | **Exit**	– Exit the Configuration program
Registry | **Get options**	– Read settings from the local registry
Registry | **Set options**	– Save current settings to the local registry
Help | **Help topics**	– Get help
Help | **About**	– View information on current InVircible release