Sophos Anti-Virus

User Manual

OpenVMS

SOPHOS

Sophos Anti-Virus

for OpenVMS

User Manual
November 1997

This manual documents Sophos Anti-Virus
for OpenVMS, which incorporates
VSWEEP and InterCheck.

Sophos Plc • The Pentagon • Abingdon • OX14 3YP • England

Email enquiries@sophos.com • http://www.sophos.com/

Tel +44 1235 559933 • Fax +44 1235 559935

9 8 7 6 5 4 3 2 1

Part # masvez0p/971022

This document is also available in electronic form from Sophos.

Technical support hotline:
Email technical@sophos.com, Tel +44 1235 559933

Contents

About VSWEEP

This chapter introduces VSWEEP, describes VSWEEP's main features, and helps users identify the chapters most relevant for their needs.

What is VSWEEP?

VSWEEP offers on-demand and (with InterCheck) on-access virus checking, along with automatic reporting and action against viruses.

Virus checking for OpenVMS

At the time of writing, there are no OpenVMS specific viruses. It would be difficult to write a virus that could breach the OpenVMS security features and become widespread.

However, the Digital product PATHWORKS allows VAX and Alpha AXP computers to provide powerful network drive facilities for PC workstations. Thus, an OpenVMS system can contain PC executable files, which can be infected by PC viruses. VSWEEP can check for these and provide protection by denying access to infected files.

VSWEEP and SWEEP for DOS

VSWEEP for OpenVMS is a combined product, including VSWEEP_VAX.EXE and VSWEEP_AXP.EXE, executable programs for OpenVMS VAX and OpenVMS AXP respectively.

VSWEEP customers also receive the corresponding DOS and Windows 95 versions of SWEEP for use on PC workstations.

VSWEEP can be run from DCL for scanning DOS files held on an OpenVMS system under PATHWORKS File Services, including those in FAT container files or Disk Services. The DOS program SWEEP can also scan workstation disks.

Features of VSWEEP

VSWEEP:

- Checks VMS file servers for the presence of all viruses known to Sophos at the time of SWEEP's release.
- Can run as an InterCheck server to provide automatic on-line virus detection for connected workstations.
- Is updated twelve times a year, and urgent updates can be distributed by fax or email, or downloaded from the Sophos Web site.
- Easily detects polymorphic viruses using Sophos' advanced Virus Description Language (VDL) and a built-in code emulator.
- Detects and disinfects Microsoft Word and Excel macro viruses.
- Offers two levels of security, allowing a 'quick sweep' which looks for viruses in parts of files likely to contain a virus, and a 'full sweep' which looks for viruses or virus fragments in every part of every file.
- Is not susceptible to the stealth techniques used by an increasing number of DOS viruses.
- Offers OpenVMS managers centralised control of virus detection and can send them VMSmail to inform them of the discovery of a virus.

- Can be scheduled to sweep as a normal OpenVMS job, and configured to run continuously.
- Imposes no load on the network, and does not tie up a workstation.

How to use this manual

This manual is intended for OpenVMS System Managers, especially those with responsibility for security and/or PATHWORKS installations, and assumes familiarity with DCL concepts and commands as well as with PATHWORKS. It is organised into the following chapters:

- ‘About SWEEP’, this chapter.
- ‘About InterCheck’ presents an overview of Sophos’ InterCheck technology.
- ‘Installing VSWEEP’ describes how to install VSWEEP, how to install the InterCheck server facilities, and how to upgrade VSWEEP.
- ‘Using VSWEEP’ describes how to run VSWEEP from DCL, how to specify the items that will be swept, and how to run VSWEEP from a command procedure. It also describes the VSWEEP command line qualifiers.
- ‘Using the InterCheck server’ describes how to start and configure the InterCheck server function.
- ‘Installing InterCheck clients’ describes how to install and run InterCheck clients.
- ‘Configuring InterCheck clients’ describes the configuration of InterCheck clients running under DOS, Windows 3.x, Windows 95 and Windows for Workgroups.
- ‘Treating viral infection’ gives advice on how to deal with a virus once it has been discovered by VSWEEP.

- ‘Troubleshooting’ provides answers to some common problems which can be encountered when using VSWEEP.

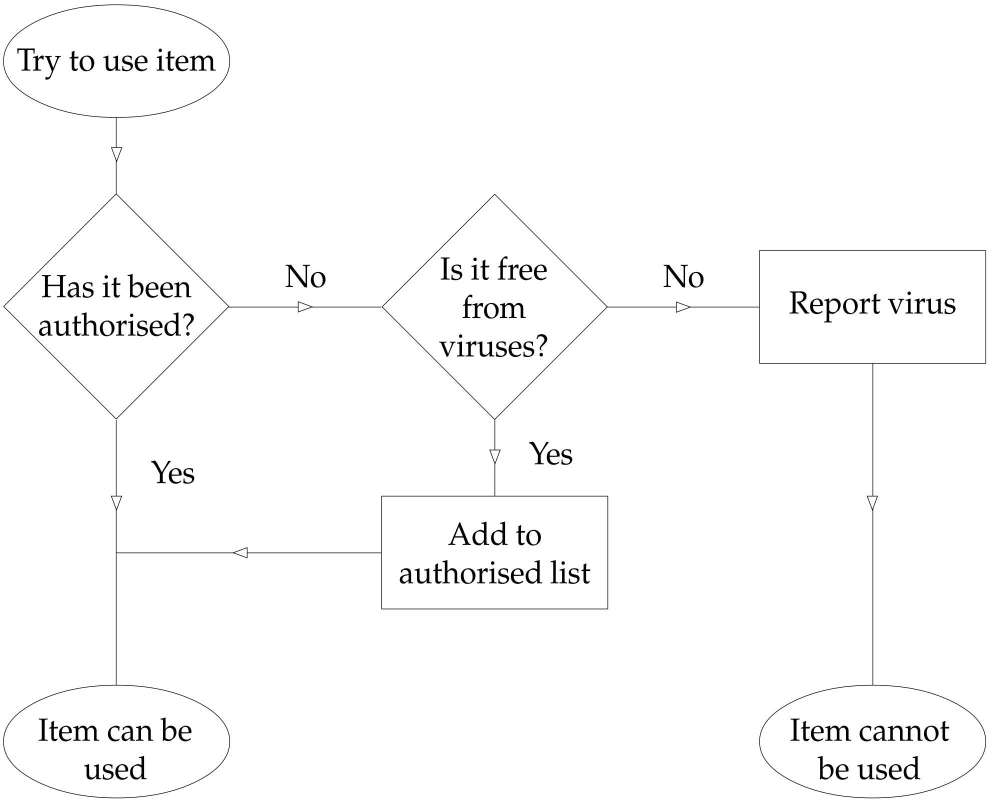
In addition, the ‘Glossary’ contains explanations of some technical terms used in this guide.

About InterCheck

This chapter presents an overview of Sophos' InterCheck technology.

What is InterCheck?

InterCheck ensures that unknown files (e.g. programs, documents, email attachments or Internet downloads) and disks cannot be used until checked for viruses.



The InterCheck principle

How are InterCheck and SWEEP related?

Used alone, SWEEP offers on-demand virus checking; combined with InterCheck technology it also offers on-access checking.

InterCheck splits the task of virus detection between a client and a server. The **InterCheck client** determines whether items on the client workstation should be checked for viruses, while the **InterCheck server** (or a local installation of SWEEP) performs the actual virus checks where necessary.

What types of InterCheck client are there?

There are two main types of InterCheck client: networked and stand-alone.

A **networked InterCheck client** exists on a separate machine from the InterCheck server, and communicates with it over the network.

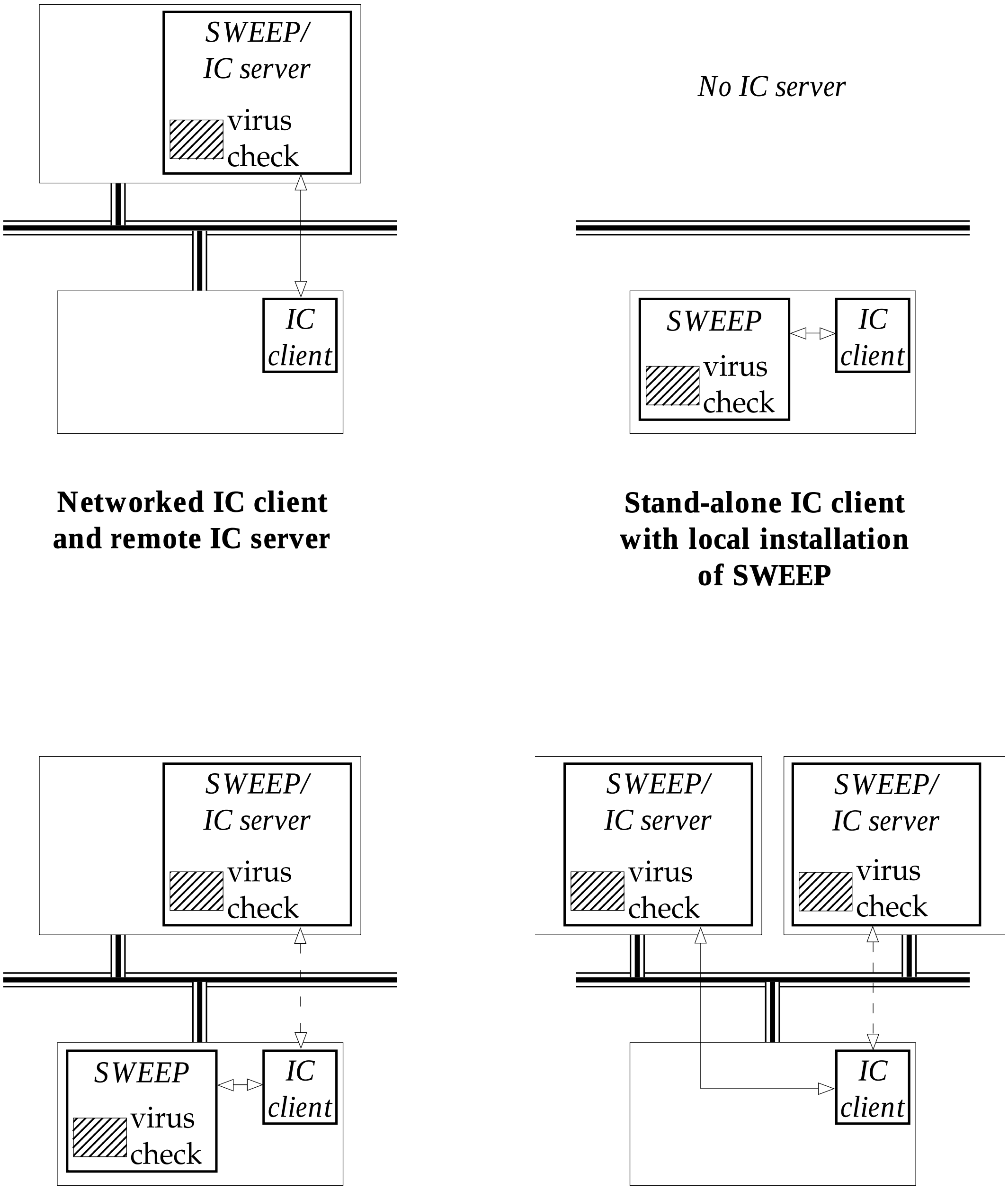
A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

A networked InterCheck client is easier to administer and uses fewer system resources on the client workstations. A stand-alone InterCheck client generally offers faster initial authorisation of files, and can also be used on machines not always connected to the network.

Either way, InterCheck is the most efficient way of protecting users from viruses: each item is checked for viruses only once, unless it is modified, in which case it is rechecked.

How does InterCheck work?

The InterCheck client software monitors all file and disk accesses. Whenever an item is accessed, it is



Networked IC client and remote IC server

Stand-alone IC client with local installation of SWEEP

Stand-alone IC client with local SWEEP and optional IC server

Networked IC client with remote IC server and backup IC server

Different InterCheck client and server configurations compared with a list of authorised items. If a match is found, the access is permitted. If a match is not found, the networked InterCheck client sends a copy of the item to the InterCheck server for checking, while the stand-alone InterCheck client checks with a local installation of SWEEP.

If the item is found to be clean, it is added to the list of authorised items and the access is allowed to continue. Any further accesses of this item are then completed without the need for further authorisation, unless it is modified, in which case authorisation is again automatically requested.

However, if a virus is found, InterCheck prevents access to the item, so the workstation cannot be infected.

Checksum files

The list of authorised items is called a checksum file.

A **local checksum file** is stored on every workstation, whether it is a stand-alone or networked InterCheck client.

A **central checksum file**, where supported, is stored by the InterCheck server. A networked InterCheck client, when configured to use the central checksum file, will check it for items that are not in its local checksum file. This means that when one InterCheck client has had an item checked, all other InterCheck clients can access that item without further checking.

Features

Complete cover Of the network: InterCheck provides complete virus-protection for the entire network with minimal performance and memory overheads, and supports the widest range of client and server platforms.

Of the workstation: InterCheck monitors access to all programs, boot sectors, documents, email attachments, Internet downloads and CD-ROMs.

Performance Once an item has been authorised, further virus checking is not needed unless it changes or SWEEP is updated. The process of checking that an item has been authorised is much faster than performing a full virus check.

Automatic reporting Many virus incidents are more serious than they need to be because users fail to report viruses to their managers. If an InterCheck client is connected to the network and a virus is found, a report can be sent to the network supervisor automatically.

Easy administration InterCheck clients can be centrally controlled, configured and updated. Networked InterCheck clients can in many cases be installed automatically over the network.

Portable PCs Stand-alone InterCheck clients can continue to provide the same levels of protection even when a PC is not connected to the network, and can be automatically upgraded when the PC is reconnected to the network.

Overview of InterCheck installation and configuration

Native InterCheck server functionality is currently included in SWEEP for NetWare, Windows NT (Intel and Alpha), OpenVMS (VAX and Alpha), DOS, OS/2 and Banyan VINES. SWEEP for DOS can also be used to provide InterCheck server functionality for other operating systems.

Networked InterCheck clients require a separate InterCheck server. This involves installing SWEEP and the InterCheck software on the file server, and running SWEEP in InterCheck server mode. Networked InterCheck clients are currently available for DOS, Windows, Windows 95 and Macintosh workstations.

Stand-alone InterCheck clients do not require an InterCheck server. In the case of Windows 95 and Windows NT, the stand-alone InterCheck clients are installed as part of the SWEEP installation process. Stand-alone InterCheck clients are currently available for DOS/Windows 3.x, Windows for Workgroups, Windows 95 and Windows NT (Intel and Alpha) workstations.

InterCheck server installation and configuration

Windows NT, NetWare, OpenVMS, DOS, OS/2 and Banyan VINES

See the SWEEP for Windows NT, NetWare, OpenVMS, DOS, OS/2 and Banyan VINES user manuals (i.e. the InterCheck server's SWEEP user manual) respectively.

Networked InterCheck client installation and configuration

Installation

DOS, Windows, Windows 95 and Macintosh

See the 'Installing InterCheck clients' chapter of the InterCheck server's SWEEP user manual.

Configuration

DOS, Windows and Windows 95

See the 'Configuring InterCheck clients' chapter of the InterCheck server's SWEEP user manual.

Stand-alone InterCheck client installation and configuration

Installation

DOS/Windows 3.x and Windows for Workgroups

See the ‘Installing InterCheck clients’ chapter of the InterCheck server’s SWEEP user manual.

Windows 95 and Windows NT

See the ‘Installing SWEEP’ chapters of the SWEEP for Windows 95 and SWEEP for Windows NT user manuals respectively.

Configuration

DOS/Windows 3.x, Windows for Workgroups and Windows 95

See the ‘Configuring InterCheck clients’ chapter in the InterCheck server’s SWEEP user manual, and also in the SWEEP for Windows 95 user manual.

Windows NT

See the ‘Configuring SWEEP’ chapter of the SWEEP for Windows NT user manual.

Installing VSWEEP

This chapter describes how to install VSWEEP, how to install the InterCheck server facilities, and how to upgrade VSWEEP.

The VSWEEP software

VSWEEP is supplied on tape cartridge as a BACKUP save set. This includes the following files:

- VSWEEP_VAX.EXE
  This is the VSWEEP program for VAX computers running VAX/VMS or OpenVMS.
- VSWEEP_AXP.EXE
  This is the VSWEEP program for Alpha AXP computers running OpenVMS AXP.
- VIRPATS.LST
  This is a text file describing the viruses.
- IC_INSTALL.COM
  This is a DCL procedure for installing VSWEEP as an InterCheck server.
- RELNOTES.TXT
  This file contains the release notes.

Installation procedure

To install VSWEEP, follow these steps. Firstly, delete any existing copies of VSWEEP from the directory into which it will be installed, e.g.

```
$ DELETE [MYAREA.MYEXES]VSWEEP*.EXE;*
$ DELETE [MYAREA.MYEXES]VIRPATS.LST;*
$ DELETE [MYAREA.MYEXES]IC_INSTALL.COM;*
$ DELETE [MYAREA.MYEXES]RELNOTES.TXT;*
```

Then allocate a physical tape device using

```
$ ALLOCATE MK TAPE:
```

where MK refers to a suitable tape device. If the exact device name is known, use it. Load the tape cartridge into the allocated device. Mount the tape as a foreign volume using

```
$ MOUNT/FOREIGN TAPE:
```

and then retrieve the VSWEEP files using the command

```
$ BACKUP/VERIFY/LIST TAPE:*/REWIND []
```

which will place the VSWEEP files in the current directory. To place VSWEEP somewhere other than the current directory, replace [] with the appropriate directory specification, e.g. [MYAREA.MYEXES]. Finally, dismount the tape, remove the cartridge and free the drive using

```
$ DISMOUNT TAPE:
$ DEALLOCATE TAPE:
$ DEASSIGN TAPE:
```

Making VSWEEP a DCL command

If this has not yet been done, make ‘VSWEEP’ a DCL foreign command using a statement such as

```
$ VSWEEP:==$D0:[MYEXES]VSWEEP_VAX.EXE
```

or

```
$ VSWEEP:==$D0:[MYEXES]VSWEEP_AXP.EXE
```

where the device name (here D0) is preceded by a $.

This definition of ‘VSWEEP’ should normally be placed in the LOGIN.COM file.

Important! Take care to invoke the VAX executable if it is to run under OpenVMS VAX, or the AXP executable if it is to run under OpenVMS AXP. A VAX executable inadvertently run under OpenVMS AXP normally results in a graceful OpenVMS error message. An AXP executable run under VAX/VMS or OpenVMS VAX may lead to unspecified system behaviour.

Access rights for VSWEEP

VSWEEP requires read access to all files and directories in the area being swept. No other access modes or privileges are required.

Installing VSWEEP as an InterCheck server

Having logged in to the OpenVMS server as SYSTEM, run the IC_INSTALL procedure supplied with VSWEEP, e.g.:

```
$ @[dirspec]IC_INSTALL
```

where `[`*`dirspec`*`]` specifies the directory into which the VSWEEP executables have been installed.

IC_INSTALL creates a Pathworks File Service called INTERCHK, together with the required subdirectories, and sets all the protections needed. If the default settings are not appropriate, it is possible to specify where the file service should be rooted.

Important! **On a PATHWORKS Version 5 server**, IC_INSTALL creates a LAN Manager user group called ICUSERS of which all InterCheck client PCs will need to be made members.

IC_INSTALL also generates the following DCL procedures:

- IC_START.COM
  This starts VSWEEP in InterCheck server mode.

After this procedure has been run, workstations attached to the network will be able to benefit from InterCheck. This procedure should normally be called from the server's startup file, so that it always runs when the system is rebooted.

- IC_STOP.COM
  This procedure should be called if the InterCheck server process is to be stopped; it lets VSWEEP perform a graceful shutdown.

Installing InterCheck client software (PATHWORKS Version 4 servers)

From a clean-booted workstation, attach to the INTERCHK file service as user SYSTEM, e.g.

```
C:>USE Q: \\ServerName\INTERCHK%SYSTEM password
```

Insert the InterCheck master disk into the A: drive and copy all the files to the root directory of the INTERCHK file service:

```
C:>COPY A:*.* Q:\
```

Then insert the SWEEP master disk into the A: drive and again copy all files to the root directory of the INTERCHK file service.

```
C:>COPY A:*.* Q:\
```

Next, set the protections so that all users can read but not write these files, and then reset the two subdirectory protections:

```
C:>NET ATTRIB Q:\*.* /PROT=(G:RE,W:RE)
C:>NET ATTRIB Q:\COMMS. /PROT=(G:RWE,W:RWE)
C:>NET ATTRIB Q:\LISTS. /PROT=(G:RWE,W:RWE)
```

Alternatively, if the NET ATTRIB command is not available, the protections can be set by logging in to the server as SYSTEM, setting the default directory to the root directory of the INTERCHK file service, and then using

```
$ SET PROT=(G:RE,W:RE) *.*
$ SET PROT=(G:RWE,W:RWE) COMMS.DIR
$ SET PROT=(G:RWE,W:RWE) LISTS.DIR
```

Finally, disconnect from the INTERCHK service:

```
C:>USE Q: /D
```

The server is now fully set up for workstations to be able to run InterCheck.

Installing InterCheck client software (PATHWORKS Version 5 servers)

From a clean-booted workstation, login to the network as an Administrator and attach to the INTERCHK file service, e.g.

```
C:>NET USE Q: \\ServerName\INTERCHK
```

Insert the InterCheck master disk into the A: drive and copy all the files to the root directory of the INTERCHK file service:

```
C:>COPY A:*.* Q:\
```

Then insert the SWEEP master disk into the A: drive and again copy all files to the root directory of the INTERCHK file service.

```
C:>COPY A:*.* Q:\
```

Finally, disconnect from the INTERCHK service:

```
C:>NET USE Q: /D
```

Each client wishing to use InterCheck must be made a member of the LAN Manager group ICUSERS.

The server is now fully set up for workstations to be able to run InterCheck.

Installing InterCheck clients

For workstations to use the InterCheck server, an InterCheck client must now be installed on each workstation. See the ‘Installing InterCheck clients’ chapter.

Updating VSWEEP

Registered users of VSWEEP are sent updated copies of VSWEEP in the first week of every month, or can download updated versions from the Sophos Web site.

VSWEEP can be updated by installing the new executables from tape, as described in the ‘Installation procedure’ section above.

Updating VSWEEP’s InterCheck components

When VSWEEP is used as an InterCheck server, the only items that need to be updated are the VSWEEP executable on the server and the copy of SWEEP for DOS stored in the root directory of the INTERCHK file service. The networked InterCheck clients are normally updated automatically.

To update VSWEEP, first install the new executables from tape as normal, into the same directory as before.

Then run IC_STOP.COM, to shut down the InterCheck server, and wait a few seconds for the server process to shut down.

Next, run IC_START.COM. This will restart the InterCheck server process, this time using the new VSWEEP executable. If the error ‘duplicate process name’ is encountered, wait a few seconds longer and run IC_START.COM again.

Check that the new VSWEEP version is running successfully, by displaying the logical name INTERCHECK_ACTIVE and verifying the version number:

```
$ SHOW LOGICAL/SYSTEM INTERCHECK_ACTIVE
```

The old versions of the VSWEEP software may be purged, to prevent them accumulating.

Updating DOS SWEEP (PATHWORKS Version 4 servers)

From a clean-booted workstation, attach to the INTERCHK file service as user SYSTEM, e.g.

```
C:>USE Q: \\ServerName\INTERCHK%SYSTEM password
```

Insert the SWEEP master disk into the A: drive and copy all files to the root directory of the INTERCHK file service.

```
C:>COPY A:*.* Q:\
```

Set the protections so that all users can read but not write these files, and then reset the two subdirectory protections:

```
C:>NET ATTRIB Q:\*.* /PROT=(G:RE,W:RE)
C:>NET ATTRIB Q:\COMMS. /PROT=(G:RWE,W:RWE)
C:>NET ATTRIB Q:\LISTS. /PROT=(G:RWE,W:RWE)
```

Alternatively, if the NET ATTRIB command is not available, the protections can be set by logging in to the server as SYSTEM, setting the default directory to the root directory of the INTERCHK file service, and then using

```
$ SET PROT=(G:RE,W:RE) *.*
$ SET PROT=(G:RWE,W:RWE) COMMS.DIR
$ SET PROT=(G:RWE,W:RWE) LISTS.DIR
```

Finally, disconnect from the INTERCHK service:

```
C:>USE Q: /D
```

Updating DOS SWEEP (PATHWORKS Version 5 servers)

From a clean-booted workstation, login to the network as an Administrator and attach to the INTERCHK file service, e.g.

```
C:>NET USE Q: \\ServerName\INTERCHK
```

Insert the SWEEP master disk into the A: drive and copy all files to the root directory of the INTERCHK file service.

```
  C:>COPY A:*.* Q:\
```

Finally, disconnect from the INTERCHK service:

```
  C:>NET USE Q: /D
```

Remember that each client wishing to use InterCheck must be a member of the LAN Manager group ICUSERS.

Urgent updates

VSWEEP is updated each month. However, users can add new ‘virus identities’, which VSWEEP uses for virus detection, at any time.

Sophos can supply new virus identities as IDE (identity) files. These consist entirely of printable ASCII characters, and can be faxed, emailed or downloaded from Sophos’ Web site (http://www.sophos.com/).

The IDE files should be placed in files with an .IDE extension in the current default directory. VSWEEP will then load the new virus identities when restarted.

SWEEP IDE files should be removed once they are no longer needed.

Using VSWEEP

This chapter describes how to run VSWEEP from DCL, how to specify the items that will be swept, and how to run VSWEEP from a command procedure. It also describes the VSWEEP command line qualifiers.

Running VSWEEP from DCL

Having made ‘VSWEEP’ a command as described in the ‘Installation procedure’ section of the ‘Installing VSWEEP’ chapter, VSWEEP can be run from the DCL prompt as

```
$ VSWEEP filespec[,...]
```

Specifying which files are swept

The command parameter ‘filespec’ specifies to VSWEEP, in part or in full, the OpenVMS file or files to be searched for viruses.

A single command line can include more than one file specification, separated by commas (,). The filespec defaults to `*.*;*` with the result that

```
$ VSWEEP []
```

is the same as

```
$ VSWEEP []*.*;*
```

A typical invocation of VSWEEP will often specify more than one file to be swept, e.g.

```
$ VSWEEP MYDEV:[PCSAV40...]*.EXE,*.DLL
```

Normal DCL defaulting rules apply, so that here the search of *.EXE and *.DLL would all be on MYDEV in the specified directories.

Sweeping subdirectories

It is important to direct VSWEEP to examine the subdirectories as well as the main directory. In the above example, the ellipsis '`...`' at the end of the directory specification tells VSWEEP to search all subdirectories as well. Remember that:

Under PATHWORKS File Services the DOS directory tree is emulated by an equivalent VMS directory tree, from the File Services directory downwards. See the 'Checking subdirectory levels' section of this chapter.

Under PATHWORKS Disk Services there may be many DOS files and directories within a single VMS container file. See the description of the /DS qualifier in 'Command line qualifiers' below.

Note: The system logical names used by VSWEEP in InterCheck server mode have no effect when running VSWEEP from DCL as described in this chapter. VSWEEP can likewise be run from DCL without affecting operation of the InterCheck server process.

VSWEEP's File Service and Disk Service modes

When run from the DCL prompt or in a batch file, VSWEEP has two modes of operation: File Service mode and Disk Service mode, corresponding to the two main types of service offered by PATHWORKS.

In File Service mode (the default mode) VSWEEP treats VMS files as images of DOS files.

In Disk Service mode (selected using the /DS qualifier described below) VMS files are treated as images of entire DOS disks. Files of this sort are generally referred to as ‘virtual disks’ or ‘FAT container files’.

A single command line can specify searches in File Service and Disk Service modes.

Command line qualifiers

There are two kinds of command line qualifiers:

Global qualifiers, such as /OUTPUT and /VF, have the same effect wherever they appear in the command line. They affect the entire VSWEEP run.

Positional qualifiers, such as /DS, apply only to the preceding file specification. All qualifiers are positional unless stated otherwise. If a positional qualifier appears before any of the file specifications, it applies to all of them as if it were a global qualifier. All VSWEEP’s positional qualifiers can be negated by prefixing NO. For example, the negative of /DS is /NODS. This can be useful for countermanding an effect temporarily:

```
$ VSWEEP /DS *.EXE/NODS, *.DSK, [.TEST]
```

Here VSWEEP will search []*.DSK and [.TEST]*.DSK in Disk Service mode, but will search []*.EXE in File Service mode.

/AD Autodefault mode

This global qualifier will make VSWEEP run in autodefault mode. In this mode, provided primarily for compatibility with earlier versions of VSWEEP, any filename, extension or version in the file specification will be ignored. VSWEEP will instead take the specified device and directory (which may include the ellipsis `[...]` to specify subdirectories), and search there for files matching *.COM, *.DOC, *DOT, *.EXE, *.OV%, *.SYS and *.XL% (in File Service mode) or *.DSK (in Disk Service mode).

See also the /AL and /DA qualifiers.

/AL Check files with any extension

The /AL qualifier is permitted only in autodefault mode (see the /AD qualifier). It directs VSWEEP to check all OpenVMS files, regardless of their extension, instead of the usual subset .COM, .DOC, .DOT, .EXE, .OV%, .SYS, and .XL% (in File Service mode) or .DSK (in Disk Service mode). Use of the /AL qualifier is normally unnecessary, but it can be useful if, following a virus attack, infected files have been renamed to prevent inadvertent execution.

/CC Generate central checksum list

The /CC qualifier causes VSWEEP to generate a central checksum list for use with InterCheck.

This qualifier is not essential for the use of central checksumming. As long as central checksumming is enabled on the InterCheck server, a central checksum file will be created and items will be added to this as they are accessed by users. The /CC qualifier is used only to build a full checksum list in advance, so that files on the server can be accessed by users without further sweeping.

Important! The /CC qualifier works only if VSWEEP has been installed as an InterCheck server.

/DA Search all files in Disk Service

The /DA qualifier is applicable only to Disk Service mode, and then only in default mode. It directs VSWEEP to check all DOS files within the virtual disk, rather than the usual subset .COM, .DOC, .DOT .EXE, .OV%, .SYS and .XL%. As with the /AL qualifier, this is not normally necessary.

/DI Disinfect files containing macro viruses

The /DI qualifier enables VSWEEP to disinfect files containing macro viruses automatically.

/DL List searched files in Disk Service

The /DL qualifier is applicable only in Disk Service mode. It lists all DOS files being checked within the virtual disk. /DL does an implicit /NS (see below).

/DS[=(f1,f2...)] Disk Service mode

By default, VSWEEP treats OpenVMS files as normal File Services. The qualifier /DS directs VSWEEP to treat them as Disk Services, i.e. as FAT container file images of entire DOS disks.

In Disk Service mode VSWEEP searches not only the files contained within the virtual disk, but also its boot sector. /DS can optionally be invoked with a list of DOS file specifications f1, f2, etc. enclosed in brackets. If f1 consists of just filename and extension, with no path, then the file or files will be swept regardless of the directory in which they appear within the virtual disk. If f1 includes a path specification, only the files in the specified directory will be swept. A path specification must start with a backslash (\). DOS drive letters may not be used. DOS wildcards (* and ?) may be used in the filename or extension, but not in the path.

For example,

```
$ VSWEEP /DS=(MYFILE.*,\PROGS\*.EXE) *.DSK
```

would search for viruses in DOS files matching MYFILE.* (anywhere in the DOS directory structure) and \PROGS*.EXE, within each of the *.DSK container files in the OpenVMS default directory.

Using just /DS is the same as using /DS=(*.*), i.e. all files will be searched in all directories in the virtual disk.

/FF Include ‘FIX’ format files

The normal record format for OpenVMS files created by PATHWORKS File Services is ‘Stream’. In File

Service mode VSWEEP by default treats files with any other record format as being unexpected. However, PATHWORKS does have an option allowing the files to be created in 'Sequential' format, with fixed-length records. In File Service mode the /FF qualifier can be used to include fixed-length record files in VSWEEP's concept of 'expected' formats. The /FF qualifier thus interacts with both the /FI and /FO qualifiers.

The /FF qualifier is not applicable in Disk Service mode, as the only expected record format for virtual disks is currently fixed-length sequential.

/FI Ignore record format

This directs VSWEEP not to output informational messages when it encounters files with record formats not expected under PATHWORKS. Likewise, it prevents VSWEEP from returning INFO status as a result of encountering such files. /FI applies both in Disk Service and in File Service mode. It is useful when sweeping directories containing mixed DOS and OpenVMS files. See also the /FF and /FO qualifiers.

When used in conjunction with the /RW qualifier, for example in order to sweep mounted read/write Disk Services, /FI also suppresses messages resulting from apparent corruption or incompleteness.

/FO Standard format files only

This directs VSWEEP to avoid sweeping files with record formats not expected under PATHWORKS.

In File Service mode /FO used without /FF therefore makes VSWEEP search only those files with the normal 'Stream' format used by PATHWORKS File Services. Using /FO and /FF makes VSWEEP search sequential files with fixed-length records as well. Note that this will include normal VMS program files as well, if they are present in the directories being swept. The /FO qualifier is useful when sweeping directories containing mixed DOS and OpenVMS files. See also the /FF and /FI qualifiers.

In Disk Service mode the /FO qualifier directs VSWEEP to search only those files with fixed-length sequential record format.

/IL Ignore locked files

If VSWEEP tries to open a file locked by another process and that file does not become unlocked within 10 seconds, VSWEEP normally returns a warning. The /IL qualifier can be used to direct VSWEEP to ignore any locked files it encounters. In this case no 'locked file' errors are signalled, and VSWEEP proceeds straight to the next file.

/NC Non-concealed device names

The qualifier /NC directs VSWEEP to list OpenVMS files using their physical device names rather than any concealed or logical device name which might have been used in the command line. This can be useful if there is any confusion over the physical location of an infected file.

/NS Non-silent mode

The qualifier /NS directs VSWEEP to list all OpenVMS filenames as the files are checked. Otherwise (i.e. by default) the names are suppressed. See also the /DL qualifier, which lists the names of DOS files within a virtual disk.

/OUTPUT=filename Send output to file

By default, VSWEEP sends its output to SYS$OUTPUT. The /OUTPUT qualifier can be used to send the output to a different destination. /NOOUTPUT can be used to suppress all VSWEEP output except for totals of viruses found, and certain error messages. /OUTPUT and /NOOUTPUT are global qualifiers.

/QU Quick Sweep

By default, VSWEEP sweeps in ‘full mode’, i.e. it searches files intelligently for viruses, and then makes a byte-by-byte search for virus fragments. The /QU qualifier can be used to select the ‘quick mode’. This increases VSWEEP’s speed by restricting it to searching for viruses (virus identities) only. This will still find all normal infections, but in the case of multiple infections of a single file it will report only the ‘outermost’ virus.

Note: When VSWEEP is acting as an InterCheck server, the default is ‘quick mode’.

/RW Read files already opened for writing

VSWEEP normally tries to search only files to which it can gain clean read-only access. This includes non-mounted virtual disks and those which have been mounted as read-only services, but excludes mounted read/write services. If the /RW qualifier is used, virtual disks which have been mounted as read/write services can be searched as well.

Note that a read/write mounted disk service may be in an incomplete state due to unflushed buffers or unfinished writing. Normally, VSWEEP will give up sweeping a disk which it finds incomplete. The /RW qualifier causes VSWEEP to make a best attempt to read such a virtual disk.

Warnings resulting from problems encountered while searching mounted read/write services can be suppressed using the /FI qualifier.

Files which have been opened for exclusive use by another process will not normally be readable, even using /RW.

/SC Search inside compressed files

This qualifier allows VSWEEP to search inside files compressed with the LZEXE, PKLITE and DIET compression software.

/SINCE=time Sweep files revised since specified time

The /SINCE qualifier can be used to select files to be swept based on each file's revision date. The specified value may be VMS date/time string or the keywords YESTERDAY, TODAY, e.g.

```
  $ VSWEEP */SINCE=28-AUG-1997:10:30:00
```

or

```
  $ VSWEEP */SINCE=28-AUG-1997
```

(which is equivalent to 28-AUG-1997 00:00:00)

or

```
  $ VSWEEP */SINCE=TODAY
```

If no time is specified, the default is TODAY.

It is also possible to use delta times, i.e. to specify sweeping of all files modified within a particular period of time. Thus

```
  $ VSWEEP */SINCE=-1-00
```

sweeps files with revision dates less than one day old.

/VF[=filename] Write filenames to file

When a virus is detected, it is useful to be able to take action on the infected files. This could include renaming them, deleting them, moving them, dismounting them or changing their protection. To help automate this, without restricting the choice of possible action, the global qualifier /VF=filename lets VSWEEP create a file containing just the names of the infected OpenVMS files, one name per line. A suitable

DCL command procedure can then read the filenames one by one from this file, and take appropriate action.

If the qualifier is used just as /VF, without specifying a filename, the file will be called SWEEP.VIR, in the current OpenVMS default directory. If the /NC qualifier is used, any concealed or logical device names will be replaced with physical device names.

Details of the infected file's owner and the name of the virus can also be written to the SWEEP.VIR file. See the /VREPORT qualifier.

/VREPORT Write filenames, virus names, owner names to file

This qualifier allows VSWEEP to create a file containing not only the names of infected files (see the /VF qualifier above) but also details of the owners of infected files and the names of the viruses discovered.

The default name of the report file is SWEEP.VIR, but it can be specified using /VF .

/VREPORT takes one or more keywords, which specify what should appear in any line of SWEEP.VIR. When a virus is found, a new line will be added containing the information specified, in the same order as the keywords were given, formatted to the number of characters specified (or the default width for that keyword if no width is specified).

Keyword	**Meaning**
FILENAME	Full name of the VMS file in which the virus was found
DOSFILENAME	(if applicable) name of the DOS file within the FAT Container file
VIRUSNAME	Name of the virus reported by VSWEEP
UIC	Owner of FILENAME in format [123,456]

GROUPNAME	Groupname, if it exists
USERNAME	‘Username’ field from UAF record for UIC
OWNER	‘Owner’ field from UAF record for UIC
ACCOUNT	‘Account’ field from UAF record for UIC

The order and width of each field can be specified, and keywords can be abbreviated, e.g.

```
VSWEEP * /VREP=(OWNER=20,VIRUS,FILE=50)
VSWEEP * /VR=(FILE=50,VIRUS=20,OWNER=20)
VSWEEP * /VREPORT=(OWNER,VIRUS,FILE,ACC)/VF=VIR.TXT
```

VSWEEP status and return codes

VSWEEP’s results can be tested either through its normal process return code, or through a DCL string symbol. These values can be tested by a DCL command procedure, which can take appropriate action such as broadcasting a warning, alerting the security manager, isolating the infected files, etc.

Process return code

The process return code for VSWEEP takes the form %X18008yyz, where yyz are three hexadecimal digits:

yy

00	no viruses found
01	virus(es) found

z

0	completed with warning(s)
1	completed OK
2	error(s) encountered
3	completed with informational message(s)
4	did not complete

Testing the process return code is the recommended method of ascertaining VSWEEP’s results.

DCL string symbol

VSWEEP also creates a local DCL symbol called SWEEP$_STATUS, in which it returns one of the following string values (in order of increasing precedence):

"SWEEP$_CLEAN"	Search OK, no virus found
"SWEEP$_INFO"	Informational message(s) reported
"SWEEP$_WARNING"	Warning(s) reported
"SWEEP$_ERROR"	Error(s) reported
"SWEEP$_VIRUS"	Virus(es) found

Running VSWEEP from a command procedure

There are extensive facilities under VMS for running sequences of DCL commands, either from a terminal or as a batch job. Through its command line qualifiers, its process return code and the return value in SWEEP$_STATUS, VSWEEP lends itself well to integration into such procedures.

Example 1: send mail on finding a virus

A typical requirement is for VSWEEP to run repeatedly in the background and raise the alarm if a problem is found. Here is a simple command procedure to achieve this, using SWEEP$_STATUS to test VSWEEP’s results:

```
$ GOTO DO_IT
$ DO_IT_AGAIN:
$ WAIT 02:00
$ DO_IT:
$ VSWEEP filespec/FO/OUTPUT=VS.LIS
$ PURGE VS.LIS
$ IF SWEEP$_STATUS .NES. "SWEEP$_VIRUS" -
THEN GOTO DO_IT_AGAIN
$ MAIL/SUBJ="VSWEEP alert" VS.LIS SYSTEM
$ EXIT
```

where ‘filespec’ should be replaced by the appropriate specification.

This batch job will go round and round the loop, creating a file called VS.LIS each time it runs VSWEEP, containing VSWEEP’s output. If VSWEEP has reported a virus, it sends the output file as a mail message to SYSTEM and then stops. If VSWEEP reports informational messages or warnings, it simply waits two hours and then starts again. However, if VSWEEP reports errors, this batch job will abort as there is no appropriate handling of the VSWEEP process return code. This could be achieved with a statement of the form ON ERROR THEN ... to take appropriate action.

Note: The mail message includes the virus alert string ‘>>>’, which can cause problems for some users. This string can be changed (see the ‘VIRUS_ALERT_STRING’ system logical name in the ‘Using the InterCheck server’ chapter).

Example 2: delete infected files

The following DCL command procedure uses the /VF qualifier to write the names of the infected VMS files to SWEEP.VIR, so that it can then delete them, and tests the VSWEEP process return code:

```
$ VSWEEP filespec /VF
$ IF ($STATUS .AND. %X10) .EQ. 0 -THEN EXIT
$ OPEN/READ INFILE SWEEP.VIR
$ START_LOOP:
$ READ/END_OF_FILE=END_LOOP INFILE RECORD
$ DELETE/ERASE ‘RECORD’
$ GOTO START_LOOP
$ END_LOOP:
$ CLOSE INFILE
$ EXIT
```

Starting a background command procedure

The DCL command SUBMIT can be used to set a command procedure going as a background process. It can be stopped using the DELETE/ENTRY command. The priority of the task can be controlled using the SUBMIT/PRIORITY command option. The simple example files given here can be tailored and expanded to do much more, such as sweeping several different areas within one job or handling the error conditions more comprehensively. Further information can be found in Digital's OpenVMS documentation, in the section entitled 'Guide to Using Command Procedures'.

Checking subdirectory levels

One general problem with PATHWORKS File Services when viewed from VMS is that of legal file specifications. A VMS file specification can only include eight explicit directory levels, including the root directory, e.g.

```
[000000.L1.L2.L3.L4.L5.L6.L7]MYFILE.EXT
```

A DOS file specification (as seen from a workstation) can however include a greater number of levels, e.g.

```
D:\L1\L2\L3\L4\L5\L6\L7\L8\L9\MYFILE.EXT
```

Since PATHWORKS File Services emulate the DOS directory structure using VMS files and directories, DOS files in directories at the ends of long chains may not be instantly reachable under VMS. This can have implications both for virus detection and for backup purposes.

The following solution is recommended. To test whether any unreachable directories exist, begin by defining a suitable concealed logical name for the PATHWORKS File Services area, e.g.

```
$ DEFINE/TRANS=CONC TEMP $DISK1:[PCSAV40.]
```

and then see whether this has any unreachable directories, i.e.

```
$ DIR TEMP:[000000.*.*.*.*.*.*.*]*.DIR
```

If this returns ‘File not Found’ ($STATUS = ‘%X10018290’), or ‘No such Directory’ ($STATUS = ‘%X1001C04A’) then no unreachable directories exist. Otherwise, create one or more suitable concealed logical names for each of the problem areas in turn and repeat the process, e.g.

```
$ DEF/TRAN=CONC TEMP1 TEMP:[L1.L2.L3.L4.]
$ DIR TEMP1:[000000.*.*.*.*.*.*.*]*.DIR
```

If a search for directories results in ‘File not Found’, that area can safely be swept using

```
$ VSWEEP TEMP1:[000000...]
```

Note that the same considerations apply to the use of BACKUP, which may likewise miss certain files.

Using the InterCheck server

This chapter decribes how to start and configure the InterCheck server.

Note: Installation of the InterCheck server and networked InterCheck client software is described in the 'Installing VSWEEP' chapter.

Starting VSWEEP in InterCheck server mode

To start VSWEEP in InterCheck server mode, run IC_START.COM (the procedure generated by the installation stage):

```
  $ @[dirspec]IC_START
```

This starts VSWEEP as a detached process called INTERCHECK.

After running this procedure, the list of system processes should include INTERCHECK.

Starting the InterCheck clients on workstations

For information on installing and running the InterCheck clients, see the 'Installing InterCheck clients' and 'Configuring InterCheck clients' chapters.

InterCheck reporting

The InterCheck server can report events (e.g. startup, shutdown, virus discovery, errors and file authorisations) in three ways, which are separately controlled:

- To a log file.
- To the terminals of VMS security operators.
- Through VMS Mail. This is particularly useful when reports need to go to a user at a remote host.

These reporting methods, described in outline here, are all controlled by executive-mode system logical names. The logical names are described in detail in the 'Configuring the InterCheck server' section of this chapter.

Log file

If the system logical name INTERCHECK_OUTFILE exists, VSWEEP will assume that it specifies a log file for recording reports from the InterCheck server. The level of reporting is controlled by the logical name INTERCHECK_OUTF_LEVEL.

Security operator

Designated VMS security operators can receive OPCOM messages from the InterCheck server. To receive OPCOM security operator messages, type

```
$ REPLY/ENABLE=SECURITY
```

at the DCL prompt, or put the above line in your LOGIN.COM file. The level of reporting is controlled by the logical name INTERCHECK_OPMSG_LEVEL.

VMS Mail

If the logical name INTERCHECK_MAIL_PROC exists, VSWEEP will assume that it specifies a DCL command file to be run whenever the InterCheck server process generates an event report.

VSWEEP also provides a text file containing information about the report. It puts this file in the directory specified by the system logical name INTERCHECK_MAIL_DIR. The name of the file is passed to the DCL procedure as the first parameter. The extension of the filename is '.INF'. Therefore, to mail that file to user SYSTEM on node VAX1, create a DCL command file containing:

```
$ MAIL INTERCHECK_MAIL_DIR:'P1'.INF
  -VAX1::SYSTEM/SUBJ="InterCheck Message"
$ EXIT
```

Simply create the command file and directory, and ensure that INTERCHECK_MAIL_PROC and INTERCHECK_MAIL_DIR are defined to point to them, using full pathnames. The level of reporting is set by INTERCHECK_MAIL_LEVEL.

Note that the .INF file is erased after the command file completes its execution. To keep a copy of all the .INF files generated, include in the INTERCHECK_MAIL_PROC file a line such as the following:

```
$ COPY 'P1'.INF archive_directory
```

where `archive_directory` specifies a directory in which to store the files.

Make sure that access to the DCL command file is allowed only to those who really need it. There are a number of extended features, described in the 'Configuring the InterCheck server' section.

Configuring the InterCheck server

When VSWEEP runs as an InterCheck server, a number of executive-mode system logical names can be used to control and configure it. These names can be created and deleted using the DCL commands 'DEFINE' and 'DEASSIGN' respectively. For example:

```
$ DEF/SYS/EXEC INTERCHECK_SWEEP_MODE QUICK
$ DEASSIGN/SYS/EXEC INTERCHECK_SWEEP_MODE
```

Creation and deletion of these names requires SYSNAM privilege. The current server settings can be viewed with the command

```
$ SHOW LOGICAL/SYSTEM INTERCHECK_*
```

The names can be modified while the InterCheck server is running, and the new value will be used within a few seconds. This allows on-line tuning and control of the process without any interruption of the service to users.

Note: Two names should **not** normally be changed. These are INTERCHECK_ACTIVE and INTERCHECK_COMMS_DIR. For information, see the entries in the 'Logical names for configuring the InterCheck server' section.

Logical names for configuring the InterCheck server

The system logical names used by VSWEEP in InterCheck mode are as follows.

INTERCHECK_ACTIVE

This is created by VSWEEP when it starts in InterCheck server mode. Its equivalence name is the version number of the currently active copy of VSWEEP. It is thus easy to see which version of the server software is running. Viewing this name or testing its value does not cause a problem.

Do not create or delete this name using DCL commands, unless the InterCheck server process has incorrectly been aborted using the DCL command STOP. In this case it will be necessary to deassign the INTERCHECK_ACTIVE name manually before VSWEEP can be restarted as the InterCheck server.

INTERCHECK_CCFH
INTERCHECK_GENCS

Centralised checksumming is not enabled by default. To enable it, define the logical system names below with the value 1 and add them to the IC_START.COM batch file:

```
$ DEF/SYS/EXEC INTERCHECK_CCFH 1
$ DEF/SYS/EXEC INTERCHECK_GENCS 1
```

Then stop the InterCheck server with IC_STOP and restart it with IC_START. A sub-process INTERCHECK_CCFH will be created after a short delay.

INTERCHECK_COMMS_DIR

This is a required name, without which VSWEEP will not run in InterCheck server mode. It is set by the IC_START.COM procedure generated during installation, and must equate to the [.COMMS] subdirectory of the INTERCHK file service. **It is strongly recommended that this name is not modified unless there is a specific need to do so**.

INTERCHECK_INFECTED_DIR

If INTERCHECK_INFECTED_DIR exists, VSWEEP will use it as a directory specification for ‘capturing’ copies of infected objects, such as program files and boot sectors, which have been found on workstations by the InterCheck client software.

Infected files are given their original name and the extension .VIRUS. For example, an infected copy of C:\DOS\ATTRIB.EXE would be captured to INTERCHECK_INFECTED_DIR:ATTRIB.VIRUS. Infected boot sectors are captured to a file, INTERCHECK_INFECTED_DIR:BOOT.VIRUS. The number of copies kept of identical filenames will depend on the version limit setting for the directory.

INTERCHECK_INFECTED_DIR must be on the same physical disk as the communications directory specified by INTERCHECK_COMMS_DIR. In most cases it is desirable for INTERCHECK_INFECTED_DIR to be in a protected area not accessible to Pathworks File Services, to minimise the chance of users gaining access to the infected objects.

INTERCHECK_MAIL_ADVANCED

If this system logical name exists, an advanced version of the .INF file will be generated when an event report occurs.

This contains, in the first twenty lines, individual pieces of information which can be used selectively in the INTERCHECK_MAIL_PROC DCL procedure. This feature allows creation of more complex procedures which perform different actions according to the type of event report generated. The meaning of each line is as follows:

Line	Value Name	Value Description
1	EVENT_SOURCE	The application generating the report. Will be either InterCheck or SWEEP for DOS.
2	EVENT_LEVEL	A number corresponding to the severity of the report. See INTERCHECK_MAIL_LEVEL for the list of severity levels.
3	EVENT_TYPE	A text description of the message severity, e.g. Fatal, Virus, Error etc.
4	VIRUS_ALERT	The string '>>>'.
5	VIRUS_DESC	The name of the virus discovered.

6	COMPRESSED	Contains ‘Compressed file’ if the file being swept was compressed.
7	FILE_NAME	The name of the file to which the message relates. With virus reports this will be the name of the infected file, or ‘Boot Sector’.
8	TIME	The time and date at which the event occurred.
9	USER_NAME	The login name of the user whose session generated the report.
10	USER_NODE	The client node from which the report originated.
11	COPY_REPORT	A report of any action taken to copy an infected file.
12	SEARCH_TYPE	QUICK or FULL.
13 - 20	RESERVED	Reserved for future use. These lines must be read and the values discarded in order to access the final lines correctly.
21 +	MESSAGE_TEXT	The remainder of the .INF file contains a preformatted message, identical to the one which would have been generated if INTERCHECK_MAIL_ADVANCED had not been defined.

Note: If the virus alert string ‘>>>’ causes problems, it can be changed. See the VIRUS_ALERT_STRING system logical name.

INTERCHECK_MAIL_DIR

INTERCHECK_MAIL_DIR is used to specify the working directory for Mail operations, if the Mail interface is to be used. It is recommended that a directory is dedicated to this purpose. It is essential that the InterCheck server has full access rights to this directory. The definition of this name should preferably include the full path, with node and device names.

INTERCHECK_MAIL_LEVEL

This allows the user to set the level of event report for which InterCheck will run the user procedure specified by INTERCHECK_MAIL_PROC. The higher the level set, the more mail is likely to be sent. The available levels are 0 to 5: if INTERCHECK_MAIL_LEVEL is set to 5, the user procedure will be run for all event reports.

0	No messages
1	Fatal errors
2	Virus reports [DEFAULT]
3	Errors
4	Warnings
5	Info messages

These levels correspond to the settings of INTERCHECK_OPMSG_LEVEL and INTERCHECK_OUTF_LEVEL.

INTERCHECK_MAIL_OUT

This system logical name can be used to specify the location of a file to which SYS$OUTPUT and SYS$ERROR are redirected for the user's DCL procedure.

This feature is useful for debugging the DCL command file INTERCHECK_MAIL_PROC, since usually there will be no other way of telling why a faulty command file is going wrong.

INTERCHECK_MAIL_PROC

This name specifies the DCL command file to be run by the InterCheck server when Mail should be sent. Normally it will be a simple command file invoking VMS Mail to send the .INF file specified by its parameter ‘P1’, e.g.

```
$ MAIL INTERCHECK_MAIL_DIR:'P1'.INF SYSTEM
$ EXIT
```

However, more complex command procedures can be written if desired. The definition of the logical name INTERCHECK_MAIL_PROC should preferably include its full path, with node and device names.

INTERCHECK_MAX_POLL

This name sets the upper limit, in milliseconds, for the time the InterCheck server waits between successive searches of the communications directory. Its default value is 1000. Increasing this upper limit will tend to reduce server load slightly, but will increase delays experienced by the InterCheck client software on workstations.

It is recommended that this name is only used if performance problems are encountered. VSWEEP will ignore settings it considers outside bounds. See also INTERCHECK_MIN_POLL.

INTERCHECK_MIN_POLL

This name sets the lower limit, in milliseconds, for the time the InterCheck server waits between successive searches of the communications directory. Its default value is 100. Increasing this lower limit will tend to reduce server load slightly, but will increase delays experienced by the InterCheck client software on workstations.

It is recommended that this name is only used if performance problems are encountered. VSWEEP will ignore settings it considers outside bounds. See also INTERCHECK_MAX_POLL.

INTERCHECK_OPMSG_LEVEL

This controls the level at which messages are sent to designated VMS security operators. The higher the level set, the more messages are likely to be received. The available levels are 0 through to 5:

0 No messages
1 Fatal errors
2 Virus reports [DEFAULT]
3 Errors
4 Warnings
5 Info messages

To disable all messages, for example:

```
  $ DEF/SYS/EXEC INTERCHECK_OPMSG_LEVEL 0
```

The default for INTERCHECK_OPMSG_LEVEL is 2, i.e. security operators receive InterCheck reports only on viruses and fatal errors. At level 5, a message is sent for each object swept and found to be clean as well as for warnings, errors, virus reports and fatal errors.

INTERCHECK_OUTF_LEVEL

This controls the level at which events are logged to INTERCHECK_OUTFILE, if that logical name exists. The higher the level set, the more messages will be sent. The available levels are 0 through to 5:

0 No messages
1 Fatal errors
2 Virus reports
3 Errors
4 Warnings [DEFAULT]
5 Info messages

To log all activities, for example, including all objects swept:

```
$ DEF/SYS/EXEC INTERCHECK_OUTF_LEVEL 5
```

The default setting for INTERCHECK_OUTF_LEVEL is 4, i.e. the file will log warnings, errors, virus reports and fatal errors.

INTERCHECK_OUTFILE

If the name INTERCHECK_OUTFILE exists, VSWEEP will use it as the name of a file to which to send reports on its operations. Except when actually open for writing, the file can be viewed, copied and so on as required, without halting the InterCheck server. New messages are appended to the file. The level of reporting is controlled by the name INTERCHECK_OUTF_LEVEL.

INTERCHECK_SC

This allows the InterCheck server to scan inside files compressed using the LZEXE, PKLITE or DIET compression software. To enable this feature, define this logical name with the value 1, thus:

```
$ DEF/SYS/EXEC INTERCHECK_SC 1
```

INTERCHECK_SHUTDOWN

Defining the name INTERCHECK_SHUTDOWN gives VSWEEP the signal to perform a graceful shutdown as InterCheck server. As part of the shutdown process, VSWEEP then also deassigns the shutdown name. VSWEEP tests only for the existence of the INTERCHECK_SHUTDOWN name, not for the value of its equivalence name.

The setting of this name is most easily performed by running the IC_STOP.COM procedure generated during the installation process.

INTERCHECK_SWEEP_MODE

When acting as an InterCheck server, VSWEEP can search for viruses in quick mode (the default), or in full mode. For details of these modes, see the /QU qualifier in the 'Command line qualifiers' section of the 'Using VSWEEP' chapter.

If Full mode is selected, with this command line,

```
$ DEF/SYS/EXEC INTERCHECK_SWEEP_MODE FULL
```

the InterCheck clients will experience a slower response, and the server load will be increased. This will be particularly evident on checking very large Windows executables. Since there is little practical security benefit in using full mode for the InterCheck server, it is strongly recommended that the default setting of quick mode be used.

VSWEEP_ALERT_STRING

The virus alert string '>>>' at the beginning of mail messages can cause problems for some users. VSWEEP_ALERT_STRING allows the user to change the string. For example

```
$ DEF/SYS/EXEC VSWEEP_ALERT_STRING ***
```

For the new string to take effect, the InterCheck server must be stopped and restarted.

See also the 'INTERCHECK_MAIL_ADVANCED' logical name above.

Installing InterCheck clients

This chapter describes how to install and run InterCheck clients.

Note: For information on installing the stand-alone Windows 95 and Windows NT InterCheck clients, see the ‘Installing SWEEP’ chapter of the SWEEP for Windows 95 or SWEEP for Windows NT manual.

Which kind of InterCheck client?

There are two kinds of InterCheck clients: networked and stand-alone (see the ‘About InterCheck’ chapter).

Networked InterCheck clients

Networked InterCheck clients require a remote InterCheck server, and communicate with it over the network. They can be easier to install and administer, and use less disk space and fewer system resources, than stand-alone InterCheck clients.

This option is available for DOS, Windows, and Windows 95 and Macintosh workstations. See ‘Installing networked InterCheck clients’ below.

Stand-alone InterCheck clients

Stand-alone InterCheck clients do not require a remote InterCheck server, and use a local installation of SWEEP for virus checking. They offer faster initial authorisation of files, create less network traffic, and can also be used on stand-alone workstations or workstations not always connected to the network.

This option is available for Windows NT, Windows 95, DOS/Windows 3.x, and Windows for Workgroups workstations. See the 'Installing stand-alone InterCheck clients' section below.

Installing networked InterCheck clients

Before installing networked InterCheck clients:

1. **Install SWEEP and InterCheck on the file server.**

   This installs the InterCheck server and makes the InterCheck files available for installation.

2. **Decide whether to run InterCheck with a login script or without.**

   If the client workstation has a login script, this can be used to run the InterCheck executable from the SWEEP directory on the file server. This is the easiest way to install and run a networked InterCheck client. See the 'With a login script' subsection for the relevant operating system.

   If the workstation does not have a login script, or if the user wants to start InterCheck at any time after it has logged in to the network, the InterCheck executable can be run without a login script. See the 'Without a login script' subsection for the relevant operating system.

3. **Inform users that InterCheck is being installed.**

   When the users next log in to the network after the InterCheck client has been installed, SWEEP will be run to check the programs on their workstation. This may take a few minutes, but it only happens once and reduces subsequent levels of client-server communication. Note that InterCheck can be configured to achieve a balance between 'start-up' and 'run-time' sweep times (see the 'Configuring InterCheck clients' chapter).

Now consult the following instructions for the relevant operating system.

Networked InterCheck clients for DOS and Windows

With a login script

Networked InterCheck clients can be installed and run via a login script only with a PATHWORKS Version 5 server (**not** with a Version 4 server).

Locate the users' login batch file (see the OpenVMS PATHWORKS documentation) and include the lines

```
NET USE I:\\ServerName\INTERCHK
I:\ICLOGIN
```

where I is an unused drive letter, and `ServerName` is the name of the server on which VSWEEP is installed.

InterCheck will start on the client workstation when it logs in to the network.

Without a login script

Ensure that the directory on the file server that contains the InterCheck files is permanently mapped to a DOS drive, e.g.

```
C:>USE I:\\ServerName\INTERCHK
```

and execute the DOS InterCheck executable (INTERCHK.EXE), e.g. with the line

```
C:>I:\INTERCHK
```

If the system has a shared AUTOEXEC-style .BAT routine that workstations must always run after connecting to the server, this is an ideal place for these two statements. In this case, there is no need to visit each PC.

Otherwise, the best place to put these statements is in the AUTOEXEC.BAT for each workstation, immediately after running STARTNET.

Networked InterCheck clients for Windows 95

With a login script

See the instructions in the 'With a login script' subsection of the 'Networked InterCheck clients for DOS and Windows' section above.

Without a login script

Execute the Windows 95 InterCheck executable (ICWIN95.EXE) after the workstation has made a connection to the network.

InterCheck cannot be started with AUTOEXEC.BAT under Windows 95, but it can be placed in the Startup folder to make it start automatically every time Windows 95 is started.

To do this, select *Settings* and then *Taskbar* from the Windows 95 Start menu. Click the *Start Menu Programs* tab and then the *Add* button.

Enter the location of the network copy of the ICWIN95.EXE program into the dialog box, and click *Next*. You will then have to select a folder to place the new shortcut in. Select *StartUp* and then *Next*. Finally, select *Finish* to add ICWIN95.

Networked InterCheck clients for Macintosh

The Macintosh InterCheck client is currently only supported by SWEEP for NetWare and SWEEP for Windows NT.

Installing stand-alone InterCheck clients

To install stand-alone InterCheck clients, follow the instructions for the relevant operating system.

Stand-alone InterCheck clients for Windows NT and Windows 95

These are installed as part of the SWEEP installation process. See the 'Installing SWEEP' chapter of the SWEEP for Windows NT and SWEEP for Windows 95 manuals respectively.

Stand-alone InterCheck clients for DOS/Windows

It is important to ensure that InterCheck is still run from the server whenever the workstation is connected to the network, as described in the 'Installing networked InterCheck clients' section. This ensures that the local copy of InterCheck is updated automatically if the central version on the server is updated.

Starting ICINSTAL

Clients with network access

Ensure that the directory on the file server that contains the InterCheck files is mapped to a DOS drive. At a DOS prompt on the workstation, change to that drive and enter

```
ICINSTAL
```

Clients with no network access

Insert the 'InterCheck' disk into the floppy disk drive, and enter

```
A:ICINSTAL
```

at a DOS prompt, if the 'InterCheck' disk is in drive A:.

Using ICINSTAL

If you have more than one hard disk, select the desired drive from the *Where* menu.

To use non-standard installation options, select the *Options* menu. These options correspond to those described in the ‘Configuring InterCheck clients’ chapter.

To start the installation, select *Onto hard disk* from the *Install* menu and follow the instructions.

Please note that when InterCheck first installs, the whole disk is swept for viruses. This may take several minutes depending on the size of the disk drive.

Starting InterCheck when not connected to the network

ICINSTAL installs a local copy of InterCheck on the workstation and modifies the AUTOEXEC.BAT to load INTERCHK.EXE on startup.

Stand-alone InterCheck clients for Windows for Workgroups

For Windows for Workgroups (WFWG) workstations which log in to the network after starting Windows, follow the installation procedure below.

For WFWG workstations that log in to the network **before** starting Windows, see the ‘Networked InterCheck clients for DOS and Windows’ subsection of the ‘Installing networked InterCheck clients’ section.

For WFWG workstations that are not connected to a network, see the ‘Starting ICINSTAL’ subsection of the ‘Stand-alone InterCheck clients for DOS/Windows’ section.

Before installing the InterCheck client

Before installing the InterCheck client on WFWG workstations which log in to the network after starting Windows, there are three issues to consider:

Configuring the InterCheck client

If changes are to be made to the way the InterCheck client is configured, they must be entered in the InterCheck configuration file (INTERCHK.CFG) before installation. Otherwise, InterCheck will be installed with the default configuration. See the 'Configuring InterCheck clients' chapter for more information.

Automatic or manual installation?

There are two ways to run the installation program:

1. Automatically from a login script. This can be used to install the InterCheck client without having to visit each individual workstation. See the 'Installing automatically from a login script' section below.
2. Manually from each client. This approach is generally used when no login script is available. See the 'Installing manually from the client' section below.

Interactive or non-interactive installation?

Both methods of installation can be used interactively, as described in the 'Interactive installation' section below. This might be necessary if an individual client configuration is non-standard, or if the users require more control over the installation and update process. See the 'Interactive installation' section below.

Installing automatically from a login script

This can be done only with PATHWORKS version 5 systems.

Run ICLOGIN with the -A option from the workstation's login script

```
NET USE I: \\ServerName\Directory
I:\ICLOGIN -A
```

where *`ServerName`* and *`Directory`* are the names of the server and directory containing the InterCheck files.

The next time that the workstation logs in to the network, the login program will instruct Windows for Workgroups to run the InterCheck installation program. The installation program will install InterCheck to the local machine, and then automatically start the InterCheck client.

Alternatively, if a permanent mapping to a drive is not required or not possible, use ICLOGIN with the -U command line qualifier and then remove the connection to the drive. The -U option makes ICLOGIN translate all the drive specifications to UNC (Universal Naming Convention) format, removing any dependency on the initial drive mapping. Enter the lines

```
NET USE I: \\ServerName\Directory
I:\ICLOGIN -A -U
NET USE I: /DELETE
```

Installing manually from the client

On the client workstation, select *Run* from the Windows for Workgroups *File* menu and enter

```
I:\ICSETUPW.EXE
```

if the DOS drive I: is mapped to the directory on the server that contains the InterCheck files. This must be a **permanent** drive mapping.

Alternatively, if a permanent connection to a DOS drive is not available or not desired, enter in the Run dialog box

```
\\ServerName\Directory\ICSETUPW.EXE
```

where *`Servername`* and *`Directory`* are the names of the server and the directory containing the InterCheck files.

The installation program will copy all the InterCheck client files to a directory called C:\INTERCHK on the client workstation. After a successful installation, it will restart the workstation and then start the InterCheck client.

Interactive installation

There are two ways of running ICSETUPW interactively:

1. Include the lines

   ```
   [InstallOptions]
   InteractiveInstall=1
   ```

   in the InterCheck configuration file (INTERCHK.CFG) and run ICSETUPW. This is the only way of achieving interactive installation when a login script is used.

2. Run ICSETUPW.EXE with the -I command line qualifier. For example, if installing manually from the client, select *Run* from the *File* menu and enter

   ```
   ICSETUPW -I
   ```

When the installation program is run from a login script in interactive mode, the next time that the workstation logs in to the network the installation program will be presented to the user. The user is given the option of postponing the installation.

When the installation program is run either from a login script or manually from the client, the user is given the option to abort the process at all stages. The installation program will step through the configuration options available. No modifications will be made on the workstation until the user clicks *Finish* on the last page. The installation program will then copy all the InterCheck client files to the specified directory on the client workstation. It will then restart the workstation and start the InterCheck client.

Testing InterCheck functioning

It is often useful to test the communication link between a client and the server. This can be done very simply by creating a file called TEMP.SYS and entering some random text. Use a text editor such as EDIT under DOS, or Notepad under Windows and Windows 95. InterCheck will interpret this as the creation of an executable type file and will send the file to the server for checking.

Configuring InterCheck clients

This chapter describes the configuration of InterCheck clients running under Windows 95, Windows for Workgroups, Windows 3.x, and DOS.

Note: For information on configuring the Windows NT InterCheck client, see the ‘Configuring SWEEP’ chapter of the SWEEP for Windows NT user manual.

Is it necessary to configure the InterCheck client?

The InterCheck client can be installed and run without making any changes to the default configuration. However, users may wish, for example, to:

- Specify the types of files to be checked.
- Achieve a balance between initial checking of files and subsequent requests for checking.
- Configure InterCheck differently for a specific workstation or workstations on the network.

How is the InterCheck client configured?

Configuring the InterCheck client involves editing the configuration file. This is a text file called INTERCHK.CFG stored in the directory from which InterCheck is started. The directory can either be on the server for networked InterCheck clients (central configuration file), or on the workstation for stand-alone InterCheck clients (local configuration file).

Important! If the central configuration file is modified, InterCheck clients may be updated. This may mean that local configuration files are over-written by the central configuration file (see the 'Updating local InterCheck configuration files' section below).

Configuration option section headers

The configuration options can be placed under the following 'global' or 'workstation' section headers, depending on which group of workstations or individual workstation(s) these options will apply to.

[InterCheckGlobal]
All workstations.

[InterCheckW95Global]
All Windows 95 workstations.

[InterCheckDOSGlobal]
All DOS/Windows workstations.

[InterCheckWorkStation]
All specified workstations.

[InterCheckW95WorkStation]
Specified Windows 95 workstations.

[InterCheckDOSWorkStation]
Specified DOS/Windows workstations.

[InstallOptions]
Options for the Windows for Workgroups stand-alone InterCheck client installation program. See the 'Configuring the WFWG InterCheck client installation program' section below.

Workstation and global options

The options in the workstation sections override the global options. This means that individual InterCheck workstations can be configured as required (see the

‘Configuring individual InterCheck workstations’ section below).

Where conflicting options are encountered, the sections are assigned the following order of precedence (with the highest priority listed first):

1. [InterCheckW95WorkStation] or [InterCheckDOSWorkStation].
2. [InterCheckWorkStation].
3. [InterCheckW95Global] or [InterCheckDOSGlobal].
4. [InterCheckGlobal].

Configuring individual InterCheck workstations

If different settings are made for individual workstations, these must be specified by including one or more address options in the [InterCheckWorkStation], [InterCheck95WorkStation], or [InterCheckDOSWorkStation] section.

For example, the following file defines a new virus alert message for all PCs and disables InterCheck on the PC at network address Oldfield.

```
[InterCheckGlobal]
PopUpErrorText=Ring Tim on Ext 2534

[InterCheckWorkStation]
Address=Oldfield
DisableTSR=YES
```

For details of network addresses, see the ‘Using network addresses’ section below.

Note: Comments can be added to the configuration file after a semi-colon.

Using network addresses

Each client workstation should have a unique network address, which InterCheck uses to:

- Identify the target of any workstation specific configuration options in INTERCHK.CFG.
- Identify the workstation in reports such as virus alerts.
- Construct a unique name for the checksum file on diskless workstations.

On NetBIOS compatible networks, such as Microsoft networks, Digital's Pathworks, and Novell NetWare networks, InterCheck is usually able to determine the workstation address automatically.

On a NetBIOS network, the machine name is used to represent the workstation address. This can be determined in a number of ways. For example, to find the computer name on a Windows 95 machine, double-click on the *Networks* icon on the Control Panel and click the Identification tab.

On a NetWare network, the address is automatically set to the physical address of the workstation (i.e. the Ethernet address). This can be determined by using the NETADR program supplied with InterCheck, which will display the network address for the workstation.

Where a NetBIOS and a NetWare type network are both active, InterCheck will use the NetBIOS machine name as the workstation address by default because it is generally more meaningful to the user than a NetWare address. The -NETWORK command line qualifier can be used to override this.

On other networks, the user must specify the address manually, using the -ADDRESS command line qualifier.

For further information, see the Address configuration option, along with the -ADDRESS and -NETWORK command line qualifiers.

What InterCheck checks

There are two main ways in which InterCheck uses SWEEP to look for viruses.

- **At start-up**, InterCheck passes control to SWEEP and the check is performed on the workstation. See the 'Virus checking at InterCheck start-up' section below.
- **At run-time**, items that have to be checked are passed to the server for networked InterCheck clients and a local copy of SWEEP for stand-alone InterCheck clients. See the 'Virus checking at InterCheck run-time' section below.

The levels of checking at both stages are fully configurable, allowing a trade-off between the initial sweeps and the subsequent authorisation requests.

Virus checking at InterCheck start-up

There are three different times when InterCheck will use SWEEP to check the workstation at start-up:

- **Initial InterCheck start-up**
  (i.e. after InterCheck is first installed). This is to check the system is initially virus-free and to create the initial authorised items list. The checking level can be set with the InstallCheckLevel option (see the 'Initial InterCheck start-up' subsection below).
- **Normal InterCheck start-up**
  This is to detect any memory-resident stealth viruses which, if active when InterCheck loads, may be able to subvert the operation of InterCheck.

The checking level can be set with the LoadCheckLevel option (see the ‘Normal InterCheck start-up’ subsection below).

- **InterCheck start-up after a SWEEP update**
  This is to find any new viruses not found by previous versions of SWEEP.
  The checking level can be set with the UpdateCheckLevel and/or PurgeChecksumsOnUpdate options (see the ‘InterCheck start-up after a SWEEP update’ subsection below).

Checking levels

The checking level can be set to NONE, SYSTEM, QUICK, FULL or USER:

NONE No sweep is performed.

SYSTEM Memory, boot sectors, COMMAND.COM, and hidden system files are swept. If a SystemDirectory option has been defined, SWEEP will also check all programs in the specified directory. If the MemoryCheck option has been set to NO then the memory will not be checked.

QUICK Memory, boot sectors, and the executables (including COMMAND.COM and hidden system files) on all fixed disks are swept in quick mode. If the MemoryCheck option has been set to NO then the memory will not be checked.

FULL As QUICK mode, except that the items are swept in full mode.

USER SWEEP is executed with the command line qualifiers specified by InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions. If the relevant

SWEEP option is not given, SWEEP will execute without any qualifiers. The command line qualifiers are listed in the ‘Configuring SWEEP’ chapter of the SWEEP for DOS user manual.

Initial InterCheck start-up

The InstallCheckLevel option defines what is swept and authorised the first time InterCheck is activated on a PC. In the default setting (QUICK) this includes all fixed disk boot sectors and memory. However, the files which are checked depend on whether the PC is stand-alone or networked.

On a **stand-alone PC** when InterCheck cannot detect a network, all files on all fixed disks are swept.

On a **networked PC** only executables are swept, but the scan is extended to include all the executables in the directories defined by the Path environment variable if the ScanNetPath option is set to YES.

The default executables are files with extensions COM, DLL, DOT, DRV, EXE, OV?, SYS and XL?. This can be changed with the ProgramExtensions option.

The number of files scanned can be modified to increase security or reduce the time taken for the initial installation. Sweeping fewer files reduces installation time, but increases the number of subsequent requests for authorisation.

Normal InterCheck start-up

The LoadCheckLevel option defines what is checked on a normal day-to-day start-up. In the default setting (SYSTEM) this includes all fixed disk boot sectors, COMMAND.COM, executables in the root directory, and memory.

InterCheck start-up after a SWEEP update

The PurgeChecksumsOnUpdate and/or UpdateCheckLevel options determine what will be swept after an update.

The PurgeChecksumsOnUpdate option can be used to ensure that the checksum file is completely rebuilt each time SWEEP and/or InterCheck are updated. The default setting is ON if central checksumming is enabled, but OFF if it is not, in order to reduce start-up time for users. For details of checksumming see the ‘Checksumming options’ section below.

If **PurgeChecksumsOnUpdate is ON**, the items defined by the InstallCheckLevel option will be swept. In other words, InterCheck will carry out the same checks, at start-up and run-time, as it did at initial start-up (see the ‘Initial InterCheck start-up’ section).

If **PurgeChecksumsOnUpdate is OFF**, the UpdateCheckLevel option will define what is swept when SWEEP is updated. By default, all executables on all fixed disks are scanned as well as memory and the boot sectors.

Virus checking at InterCheck run-time

The CheckOn option can be set to any combination of EXEC (check all programs executed irrespective of their extension), ACCESS (check the files defined as executables if they are accessed), and FLOPPY (check all floppy disk boot sectors). The default setting includes all three areas.

The ProgramExtensions option specifies the list of file extensions to be treated by InterCheck as executable files. If the CheckOn configuration option has been set to ACCESS, any file whose extension matches an entry in the list will be considered by InterCheck to be a program and will be checked whenever it is opened, closed (if changes have been made) or renamed.

The Exclude, NoDefaultExcludes, FileTypeDetection, CheckNetwork and UseNetList configuration options can also have a bearing on the normal operation of InterCheck.

Checksumming options

When SWEEP is used to check an item, and access to that item is granted, that item does not need to be checked again unless it is changed. InterCheck notes which items have been verified in its checksum file. This is normally stored in the root directory of the client workstation, although the CheckFile configuration option can be used to change its location.

Centralised checksumming

SWEEP for NetWare, SWEEP for Windows NT and VSWEEP for OpenVMS also support centralised checksumming. This means that a checksum file is stored on the server in addition to the checksum file on each client. The central checksum file can be accessed by all networked InterCheck clients, and is checked if an unverified item is not listed in the local checksum file. Therefore, when one client accesses an item, and access to that item is granted, any other client that tries accessing that item will not need to send it to the server for checking.

By default, centralised checksumming is enabled for InterCheck clients if has been enabled on the InterCheck server. The UseNetList option can be used to disable this feature.

Critical program support

InterCheck holds the checksums for a number of ‘critical programs’ in memory, so that they can always be accessed. This is especially important on diskless workstations where the LOGIN program must be executable after one user has logged out and the next user wishes to log in. This removes the need to exclude such files from checking. By default, the following programs are considered critical:

- COMMAND.COM.
- LOGIN.EXE (if the workstation is networked).
- The boot sector of the disk in drive A: (if the workstation has been booted from the floppy disk).

The CriticalProgram and NoStandardCriticalPrograms configuration options allow the use of the critical program checksums to be customised.

Configuring stand-alone InterCheck clients

If a stand-alone InterCheck client has been installed, then InterCheck will continue to protect the workstation from viruses even when it is not connected to the network. In the Windows and Windows 95 environments, a Windows Virtual Device Driver (VxD) is used to authorise files.

The SWEEP VxD shares many of the configuration options used by networked InterCheck clients, and also uses the following options: SweepVxDLoad, SweepVxDMode, SweepVxDScanCompressed, SweepVxDLogFile, SweepVxDLogLevel. See the ‘Configuration options’ section below for more information.

Updating local InterCheck configuration files

If the InterCheck client has been installed locally on a client workstation, the local configuration file can be updated automatically when the workstation logs in to the server. The UpdateLocalCFG option, which allows this, is set to NO by default.

Important! The stand-alone Windows 95 InterCheck client, and the Windows for Workgroups client installed with the automatic installation program, always update local configuration files.

Configuring the WFWG InterCheck client installation program

The Windows for Workgroups stand-alone InterCheck client installation program can be configured by placing the following options under the [InstallOptions] header in the configuration file: AutoInstallExclude[1...n], CommsDirectory, DestinationDirectory, InteractiveInstall, and SourceDirectory. See the 'Configuration options' section below for more information.

Configuration options

Address=<text>

The address option must be included at some point in an [InterCheckWorkStation], [InterCheckW95WorkStation] or [InterCheckDOSWorkStation] section. Multiple address options can be included in one section. The address option defines the workstation(s) to which the options in the section will be applied.

See also the 'Using network addresses' section and the -ADDRESS command line qualifier.

AllowDisable=YES|NO

InterCheck can be disabled if this option is set to YES. For security reasons, disabling is not allowed by default.

See also the -DISABLE command line qualifier.

This option is not currently supported by the Windows 95 client.

AllowUnload=YES | NO

InterCheck can be unloaded from memory if this option is set to YES. For security reasons, unloading is not allowed by default.

See also the -UNLOAD command line qualifier.

AltCommsDir=<directory>

This option can be used to define up to 4 alternative COMMS directories. For example:

```
AltCommsDir=\\BackupServer1\INTERCHK\COMMS
AltCommsDir=\\BackupServer2\INTERCHK\COMMS
```

This will be used if the primary server is unavailable. When using multiple alternative directories, the order in which they are defined in the configuration file determines the search order when attempting to detect an active server.

This option is not currently supported by the Windows 95 client.

AutoInstallExclude[1...n]=<computer1>,<computer2>...

This option excludes named computers from ICSETUPW installations started by ICLOGIN. For example

```
  AutoInstallExclude=Onion, Cheese, Marco
  AutoInstallExclude1=Mini Marco, Derek
```

will exclude the computers with network names Onion, Cheese, Marco, Mini Marco and Derek. Computer names are not case sensitive.

This option is only relevant to the automatic InterCheck client installation program.

AutoUpdate=ON | OFF

This option can be used to disable the automatic updating of local copies of InterCheck from the network. It is ON by default.

This option is not relevant to the Windows 95 client.

CheckFile=<filename>

Checksums are stored in the file C:\INTERCHK.CHK on the client workstation by default. A different filename can be specified by using this option, e.g.

```
CheckFile=D:\MYCHECKS.CHK
```

CheckNetwork=YES | NO

The CheckNetwork configuration option provides the ability to disable the checking of any program files on networked drives. This reduces file validation delay if the file is on the network and can be assumed to be clean. In order to disable checking of files on networked drives use

```
CheckNetwork=NO
```

CheckOn=[EXEC],[ACCESS],[FLOPPY]

The CheckOn option defines which functions InterCheck will intercept. The following options are available:

EXEC	Check all programs executed.
ACCESS	Check all program files accessed, i.e. opened, closed (if changes have been made), or renamed.
FLOPPY	Check all floppy disk boot sectors.

Any combination may be specified, separated by commas. The default is equivalent to:

```
CheckOn=EXEC,ACCESS,FLOPPY
```

See also the ‘What InterCheck checks’ section.

CommsDirectory=<path>

The default location for the InterCheck communications directory is COMMS in the InterCheck server directory. Use the CommsDirectory option to specify a different InterCheck communications directory. For example

```
CommsDirectory=I:\SWEEP\COMMS
```

CriticalProgram=<files>

Defines the critical program(s) whose checksum will be held in memory. Up to 16 critical programs can be defined. See the ‘Critical program support’ section.

To include a boot sector, specify the drive letter, e.g. ‘D:’.

All critical programs are displayed when InterCheck loads if the StartUpDisplay=VERBOSE configuration option is selected.

This option is not relevant to the Windows 95 client.

DestinationDirectory=<path>

The default destination for the local Windows for Workgroups InterCheck installation is C:\INTERCHK. Use the DestinationDirectory option to specify a different location. For example

```
DestinationDirectory=C:\INTERCHK\COMMS
```

This option is only relevant to the automatic InterCheck client installation program.

DisableTSR=YES|NO

The DisableTSR option can be used to prevent InterCheck loading. Once the option has been set to YES, any attempt to run InterCheck results in the message “InterCheck has been disabled”.

The DisableTSR option can also disable the Windows 95 SWEEP VxD.

Exclude=<file>

The Exclude option is used to exempt a file from being checked. The file name must not include a path component. Up to 32 exclusions may be specified and the '?' character can be used as a wildcard. For example

```
Exclude=PROG?.EXE
Exclude=P2.SYS
```

would suppress the checking of PROGA.EXE, PROGB.EXE and P2.SYS.

There are a number of default excludes: 386SPART.PAR, CONFIG.SYS, WIN386.SWP and ~$??????.DOT. The latter is included to suppress the checking of temporary template files used by Microsoft Word for Windows. The inclusion of the default exclusions can be disabled using the configuration option NoDefaultExcludes=YES.

The Exclude configuration option can also be used to disable all checking of a specified drive. For example

```
Exclude=E:
```

would prevent InterCheck from checking anything on the E: drive, including its boot sector.

Note that directories cannot be excluded.

FileTypeDetection=OFF|WINDOWS_EXE|WORD_MACRO|ALL

InterCheck can examine the contents and structure of a file to determine its type and therefore whether it has to be checked for viruses. InterCheck is currently able to determine if a file is either a Windows Program or a Microsoft Word template containing macros. This option is useful for ensuring that all

Word documents are checked for viruses, even if they do not have the extension DOT.

OFF	Disables this feature.
WINDOWS_EXE	Detects Windows programs only.
WORD_MACRO	Detects Word macros only.
ALL	Enables all detection methods.

By default, ALL FileTypeDetection options are enabled.

This feature is only available with Windows and Windows 95 InterCheck clients, and is not supported in a DOS environment.

HaltOnError=YES | NO
HaltOnVirus=YES | NO

These two configuration options provide the system Administrator with the ability to halt a PC if InterCheck detects a virus or encounters an error while loading. For example:

```
HaltOnVirus=YES
HaltOnError=NO
```

Both options are disabled by default.

Neither option is currently supported by the Windows 95 client.

InstallCheckLevel=NONE | SYSTEM | QUICK | FULL | USER

The InstallCheckLevel option defines which files will be swept for viruses when InterCheck is first executed (i.e. installed and then run) on a workstation. The default is QUICK.

This option also defines what is swept when InterCheck is run for the first time after a SWEEP update and purge of checksum file.

See the ‘What InterCheck checks’ section for more information.

InstallSweepOptions=<qualifiers>

The InstallSweepOptions statement defines the command line qualifiers used to run SWEEP when InterCheck is first executed on a workstation. For example, to generate a report from each workstation as InterCheck is installed, use the option:

```
InstallSweepOptions= -P=C:\INSTALL.REP
```

If the InstallCheckLevel option is set to NONE, InstallSweepOptions will have no effect. If InstallCheckLevel is set to SYSTEM, QUICK or FULL, the checking options specified by InstallSweepOptions will take priority.

InteractiveInstall=1|0

If InteractiveInstall is set to 1, ICSETUPW will always run in interactive mode. If set to 0, ICSETUPW will not run in interactive mode, even if it started with the -I command line qualifier.

This option is only relevant to the automatic InterCheck client installation program.

LoadCheckLevel=NONE|SYSTEM|QUICK|FULL|USER

The LoadCheckLevel option defines which files will be swept for viruses when InterCheck is run on a workstation. The default is SYSTEM.

See the ‘What InterCheck checks’ section for more information.

LoadLow=YES|NO

The LoadLow option is used to force InterCheck to load into low memory. By default InterCheck will be loaded into the upper memory area.

This is not relevant to the Windows 95 client.

LoadSweepOptions=<qualifiers>

The LoadSweepOptions statement defines the command line qualifiers used to run SWEEP when InterCheck is loaded on the workstation. For example, to generate a report from each workstation as InterCheck is loaded, use the option:

```
LoadSweepOptions= -P=C:\ICLOAD.REP
```

If the LoadCheckLevel option is set to NONE, LoadSweepOptions will have no effect. If LoadCheckLevel is set to SYSTEM, QUICK or FULL, the checking options specified by LoadSweepOptions will take priority.

MaxAddressLength=<length>
MaxPathLength=<length>

These configuration options can be used to instruct InterCheck to reserve additional memory ready for subsequent configuration changes. Under normal circumstances these options are not required. However, if InterCheck reports any of the following error messages

```
WARNING: Could not update the program directory.
WARNING: Could not update the communication directory.
WARNING: Could not update the workstation address.
```

you may need to use one or both of these options. For example:

```
MaxPathLength=255
MaxAddressLength=64
```

The MaxPathLength option defines the maximum length of the program and communication directory names that will be supported by InterCheck. The MaxAddressLength parameter defines the maximum length of the workstation address. The defaults are defined by the directories and address in use when InterCheck is first loaded. The maximum values for the MaxPathLength and MaxAddressLength parameters are 255 and 64 bytes respectively.

Neither option is relevant to the Windows 95 client.

MemoryCheck=YES | NO

The MemoryCheck option enables and disables checking for viruses in memory when InterCheck loads. Memory checking is enabled by default. The memory check is an integral part of the protection provided by InterCheck and should not normally be disabled.

MonoMonitor=YES | NO

This option overrides the automatic detection of a mono monitor.

This is not relevant to the Windows 95 client.

NoDefaultExcludes=YES | NO

If this option is set to YES, the default file exclusions will be disabled. See also the Exclude configuration option.

NoStandardCriticalPrograms

InterCheck will normally adopt the default critical programs list (see the ‘Critical programs support’ section). If this parameter is used, the default programs are not used.

This is not relevant to the Windows 95 client.

PopUpDisplay=OFF | ERROR | ALL

The PopUpDisplay option determines how much information is presented to the user in the pop-up message boxes:

OFF	No messages are displayed.

ERROR	Only alert messages are displayed (e.g. detecting a virus).
ALL	Status messages are displayed while InterCheck is working.

The default is ALL.

PopUpErrorText=<text>

The PopUpErrorText option defines a text string which is displayed in the virus alert message box. The default is 'Please contact the network Administrator immediately'.

The maximum length of the text is 52 characters. Note that word wrapping may be applied to text in the virus alert message box, which may result in fewer than 52 characters being available for use.

ProgramExtensions=<extensions>

Any file whose extension matches an entry in the list of ProgramExtensions will be considered by InterCheck to be a program and will be checked whenever it is accessed.

If no ProgramExtensions are given, the default extension list will be used, which is equivalent to:

```
ProgramExtensions=COM,DLL,DOT,DRV,EXE,OV?,SYS,XL?
```

The '?' character can be used as a wild card and '.' can be used to represent no extension.

For example

```
ProgramExtensions=COM,DLL,DOT,DRV,EXE,OV?,SYS
```

would remove XL? files (normally Microsoft Excel spreadsheet files) from the list of default executable extensions.

The ProgramExtensions option does not affect checking of files when they are executed, in which case all files are checked irrespective of their extension.

See also the 'What InterCheck checks' section.

PurgeChecksumsOnUpdate=YES | NO | DEFAULT

If this option is set to YES, the checksum file will be deleted whenever InterCheck and/or SWEEP are updated. InterCheck will then run SWEEP in the level defined for use during installation. This can be used to increase security, but is not enabled by default. The DEFAULT option purges checksums on a SWEEP/InterCheck update only if the InterCheck client is using the SWEEP VxD and/or a central checksum list.

Note: Enabling this option will introduce an overhead on the server whenever InterCheck and/or SWEEP are updated.

ReportEvents=[LOAD],[UPDATE],[INSTALL],[ALL],[NONE]

InterCheck can record usage information in the server's SWEEP log file. The type of information that is recorded is determined with the ReportEvents configuration option.

LOAD	Records an entry every time InterCheck loads.
UPDATE	Records an entry every time InterCheck or SWEEP is updated.
INSTALL	Records an entry when InterCheck is first installed on a workstation.
ALL	Records all of the above.
NONE	Records nothing.

If InterCheck reports an event it will also record the current user, the network address of the workstation, and the time and date the event occurs.

Any combination of events can be specified, separated by commas. For example

```
ReportEvents=LOAD,UPDATE
```

will record an entry every time InterCheck loads and every time InterCheck or SWEEP is updated.

By default no events are reported to the server.

ScanNetPath=YES | NO

This option controls the scanning of program files when InterCheck is first installed and run on a client workstation.

If set to YES, InterCheck will search any remote directories specified in the PATH environment variable, and any program files it discovers will be swept for viruses.

The default setting for ScanNetPath depends on whether InterCheck can detect a central checksum file on the server. The ScanNetPath option is disabled when centralised checksumming is active.

ServerTimeout=<time>

The ServerTimeout option defines the time, in seconds, which InterCheck will wait for a reply from the server before reporting that the server is unavailable. The default is 60 seconds.

SourceDirectory=<path>

The default location of Windows for Workgroups InterCheck source files is the directory from which ICSETUPW is run. If for some reason the source files are stored elsewhere, use the SourceDirectory option. For example

```
SourceDirectory=I:\INTERCHK\WFWG
```

This option is only relevant to the automatic InterCheck client installation program.

StartUpDisplay=NONE|NORMAL|VERBOSE

The StartUpDisplay option determines how much information is displayed as InterCheck loads. The default is NORMAL which only displays the program name and version information. Selecting NONE suppresses all output unless an error is detected, whereas the VERBOSE option displays additional information about which InterCheck options have been selected.

Swap=YES|NO

When the InterCheck loader program runs SWEEP, it is swapped out of memory by default in order to minimise the memory requirement. If this causes problems, the swapping can be disabled:

```
Swap=NO
```

This is not relevant to the Windows 95 client.

SwapFlags=ANY,EMS,XMS,EXT,DISK

When the InterCheck loader program runs SWEEP, it is swapped out. By using this option you can specify where the swapping should take place. EMS means EMS memory, XMS means XMS memory, EXT means extended memory, DISK means disk and ANY means any of these. Swapping to disk is always used as the last option. ANY is used by default. For example:

```
SwapFlags=EXT,DISK
```

This is not relevant to the Windows 95 client.

SweepVxDLoad=YES|NO

The SweepVxDLoad option controls whether or not to use the SWEEP VxD. The default is NO. However, the VxD is required for stand-alone InterCheck clients, so the installation program (as described in the 'Installing InterCheck clients' chapter) automatically adds the option SweepVxDLoad=YES when installing locally.

SweepVxDMode=FULL | QUICK

The SweepVxDMode option controls the sweeping level used by the VxD to sweep for viruses. The default is QUICK.

SweepVxDScanCompressed=YES | NO

The SweepVxDScanCompressed option can be used to suppress sweeping inside compressed files.

SweepVxDLogFile=<filename>

The SweepVxDLogFile option defines the name of the SWEEP VxD log file. Unless a filename has been defined using this option no information will be logged.

SweepVxDLogLevel=0..5

The SweepVxDLogLevel controls the amount of information included in the SWEEP VxD log file.

0	No messages
1	Fatal errors
2	Virus alerts
3	Errors
4	Warnings [Default]
5	Information messages

SystemDirectory=<directory>

The SystemDirectory option specifies which directory contains the system files. InterCheck will sweep any programs in this directory when any of the three check levels (InstallCheckLevel, LoadCheckLevel or UpdateCheckLevel) have been set to SYSTEM. By default no directory is specified.

UpdateCheckLevel=NONE|SYSTEM|QUICK|FULL|USER

The UpdateCheckLevel option defines which files will be swept for viruses when InterCheck detects a new version of SWEEP. The default is QUICK.

See the ‘What InterCheck checks’ section for more information.

Note: If PurgeChecksumsOnUpdate is set to YES, or if the default is to purge checksums, the InstallCheckLevel will be used instead of the UpdateCheckLevel option.

UpdateLocalCFG=YES|NO

If the InterCheck client has been installed locally on the client workstation, the local InterCheck configuration file can be updated automatically whenever the workstation logs into the server and runs InterCheck from there. If the configuration option

```
UpdateLocalCFG=YES
```

is present in the server based configuration file, the local configuration file will be replaced by the one held on the server as part of InterCheck’s auto-update procedure. By default, the UpdateLocalCFG option is NO.

Windows 95 InterCheck clients and clients installed with the automated installation program always update local configuration files.

UpdateSweepOptions=<qualifiers>

The UpdateSweepOptions statement defines the command line qualifiers used to run SWEEP when InterCheck detects a new version of SWEEP. For example, to generate a report, use the option:

```
UpdateSweepOptions= -P=C:\ICUPDATE.REP
```

If the UpdateCheckLevel option is set to NONE, UpdateSweepOptions will have no effect. If UpdateCheckLevel is set to SYSTEM, QUICK or FULL, the checking options specified by UpdateSweepOptions will take priority.

UseNetList=YES | NO

The InterCheck client utilises checksum lists generated by the InterCheck server (if supported by the server). Any program that has been swept by the server can be automatically authorised for use on all clients. To disable the use of this feature use

```
UseNetList=NO
```

UseNetSyntax=YES | NO

The UseNetSyntax option removes from InterCheck any dependence on the currently selected DOS drive mappings. The initial drive mapping, from which InterCheck was started, is no longer required to maintain communication with the server. The workstation must, however, remained logged in or attached to the server providing the InterCheck service. To enable support for this feature, use

```
UseNetSyntax=YES
```

The option should not be used with Windows 3.1 if the name of the server running the InterCheck service is longer than 11 characters. When a long server name is encountered, Windows is unable to load the support programs required by InterCheck. This problem does not occur with Windows for Workgroups.

WarnCriticalProgramMissing

If InterCheck cannot find a critical program (as defined with the CriticalProgram option), it will not display any error messages. If this parameter is used, an error message will be displayed.

This is not relevant to the Windows 95 client.

INTERCHK and ICWIN95 command line qualifiers

This section describes the command line qualifiers that can be used with INTERCHK.EXE to start the DOS/Windows 3.x InterCheck client, and with ICWIN95.EXE to start the networked Windows 95 InterCheck client.

-ADDRESS=<address>

The command line qualifier

```
-ADDRESS=<address>
```

allows the workstation address to be specified on networks where InterCheck cannot determine the workstation address automatically.

Note: If the network address contains a space, the -ADDRESS command line qualifier should be enclosed in double quotation marks, for example:

```
ICWIN95 "-ADDRESS=PC 10"
```

See also the ‘Using network addresses’ section and the -NETWORK command line qualifier.

-DISABLE

This command line qualifier stops all the checking performed by InterCheck, although the TSR remains loaded in memory. Checking can be restarted using the -ENABLE command line qualifier. For security reasons, this is not available by default. In order to use it, the line ‘AllowDisable=YES’ must be included in the InterCheck configuration file.

For example:

```
INTERCHK -DISABLE
```

This is not currently supported by the Windows 95 client.

-ENABLE

This command line qualifier restarts InterCheck after it has been disabled. For example:

```
INTERCHK -ENABLE
```

This is not currently supported by the Windows 95 client.

-HELP or -?

Displays a list of available command line qualifiers.

-NETWORK=NETBIOS | NETWARE

This command line qualifier is only required when multiple network types are in use. It selects the preferred network type for InterCheck, and only affects how InterCheck obtains the workstation address. If NetWare and NetBIOS type networks are both active, InterCheck will use the NetBIOS machine name by default.

See also the ‘Using network addresses’ section and the -ADDRESS command line qualifier.

This is not currently supported by the Windows 95 client.

-SILENT

If this command line qualifier is used, screen output will be suppressed. For example:

```
INTERCHK -SILENT
```

-STATUS

This command line qualifier displays information about the status of the InterCheck TSR. It can be used to determine if InterCheck is currently active by examining the returned DOS errorlevel:

0 Success (InterCheck active)
1 Parameter error
2 Other error (InterCheck not loaded)

For example, if TEST.BAT contains:

```
INTERCHK -STATUS -SILENT
IF ERRORLEVEL 1 GOTO NOTACTIVE
ECHO InterCheck active
GOTO END
:NOTACTIVE
ECHO InterCheck not active
:END
```

running it will display 'InterCheck active' if InterCheck is loaded and active.

The normal report only indicates whether or not InterCheck is active. If combined with the -VERBOSE command line qualifier, additional information concerning the configuration of the memory-resident part of InterCheck can be obtained.

-UNLOAD

This command line qualifier removes InterCheck from memory. For security reasons, the unload option is not available by default. In order to use the unload option the line 'AllowUnload=YES' must be included in the InterCheck configuration file.

For example:

```
INTERCHK -UNLOAD
```

Note that it may not be possible to unload InterCheck if other TSR programs have been loaded since InterCheck was first started.

-VERBOSE

This command line qualifier causes additional information to be displayed when InterCheck is run.

ICLOGIN command line qualifiers

This section describes the command line qualifiers that can be used with ICLOGIN to start the InterCheck client from a login script. The -A and -U options are described in more detail in the 'Installing InterCheck clients' chapter.

-? Help

Displays the version number.

-A Automatic Windows installation

Initiates the automatic Windows installation.

-U Use UNC

Uses UNC (Universal Naming Convention) when running or installing InterCheck.

Treating viral infection

This chapter gives advice on how to deal with a virus once it has been discovered by VSWEEP.

Dealing with viruses

The method used to deal with a virus depends on where that virus is found.

Viruses on the OpenVMS server

If VSWEEP or the InterCheck server find a virus on the OpenVMS server, see ‘Eliminating viruses on the OpenVMS server’ below.

Viruses on a workstation

If the InterCheck server finds a virus on an InterCheck client, it should be dealt with on the client workstation. Use the version of SWEEP specific to the workstation’s operating system, or SWEEP for DOS. See the ‘Treating viral infection’ chapter of the relevant SWEEP manual.

Eliminating viruses on the OpenVMS server

If VSWEEP reports a virus, first prevent further use of the infected item, and then disinfect or replace it. The /VF qualifier can be used to list the names of infected files, and these can then be automatically dismounted, moved, renamed or deleted by VSWEEP, if desired. See the ‘Running VSWEEP from a command procedure' and 'Command line qualifiers' sections of the 'Using VSWEEP' chapter.

The action taken against viruses on the file server depends on which kind of item is infected:

Files with macro viruses

Files infected with macro viruses can usually be disinfected by running VSWEEP from DCL using the command line qualifier /DI.

Infected executables

It is generally inadvisable to attempt to disinfect infected executables. This is because it is difficult to ensure that the executable has been properly restored after disinfection; it may be unstable which may put valuable data at risk. The infected executables should be deleted, preferably using the DCL command DELETE/ERASE, and restored from the originals or from sound backups.

Infected disks

On OpenVMS servers, hard disks cannot currently be infected, and floppy disks are generally not used.

Troubleshooting

This chapter provides answers to some common problems which can be encountered when using VSWEEP.

InterCheck responds slowly and/or REQ files accumulate

When a request from an InterCheck client is serviced, temporary files with the extension .REQ are created in the communications directory. These are normally deleted after a few seconds. However, if open-file cacheing is enabled on the PATHWORKS server, this may occasionally fail to happen, leading to a slow build-up of such files.

Open-file cacheing also slows down the InterCheck process as temporary files briefly become locked and inaccessible. It is recommended that open-file cacheing is disabled on the PATHWORKS server serving the communications directory.

Virus fragment reported

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. VSWEEP is able to take advantage of such similarities in its search for virus fragments. See the 'New viruses' section below.

Corrupted virus

Many viruses contain bugs in their replication routines so that they sometimes 'infect' target files incorrectly. A portion of the virus body (possibly a substantial part) may appear within the host file, but in such a way that it will never be actuated. In this case, VSWEEP will report 'Virus fragment' rather than 'Virus'. A corrupted virus cannot normally spread.

If a file contains a corrupted virus, remove the infected file and replace it with a clean copy.

False positive

This may happen for various reasons. Swap files, for example, may contain fragments of real viral code on a computer on which infected files were recently used. See 'False positives' below.

False positives

VSWEEP may very occasionally report a virus in a file that is not infected. This may be because polymorphic viruses (which change their appearance on every infection) are deliberately written to look like normal programs.

If you are ever in doubt, contact Sophos' technical support for advice.

New viruses

Any virus-specific software will discover only those viruses known to the manufacturer at the time of software release. VSWEEP is updated each month, but it may very occasionally encounter a new virus, which it will fail to report.

If a virus unknown to VSWEEP is suspected, please send Sophos a sample and a description as soon as possible. If it is a virus, VSWEEP must be updated as soon as possible. When the virus has been analysed (which may take from 10 minutes to a few days), we will fax or email the IDE file which can be used to update VSWEEP. The latest IDE files can also be downloaded from the Sophos Web site.

Further help needed

On the Web site at http://www.sophos.com/

Frequently asked questions (and their answers), virus analyses, the latest IDE files, product downloads and technical reports are available on the Sophos Web site.

By email to support@sophos.com

Questions can be sent to Sophos by email. Please include as much information as possible, including VSWEEP and InterCheck version.

By telephone on +44 1235 559933

Sophos offers 24-hour, 365-day telephone technical support.

Glossary

ASCII: American Standard Code for Information Interchange; the standard system for representing letters and symbols. Each letter or symbol is assigned a unique number between 0 and 127.

Backup: A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

BAT: The extension given to ‘batch’ file names in MS-DOS. A batch file contains a series of MS-DOS commands, which can be executed by using the name of the file as a command. AUTOEXEC.BAT is a special batch file which is executed whenever a PC is switched on, and can be used to configure the PC to a user’s requirements.

Boot Protection: Method used to prevent bypassing security measures installed on a hard disk by booting a microcomputer from a floppy disk.

Boot Sector Virus: A type of computer virus which subverts the initial stages of the booting-up process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Booting-up: A process carried out when a computer is first switched on or reset, where the operating system software is loaded from disk.

Boot Sector: Part of the operating system which is first read into memory from disk when a PC is switched on (booted). The program stored in the boot sector is then executed, which in turn loads the rest of the operating system into memory from the system files on disk.

Checksum: A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered. Usually 32 or 64 bits long.

COM: The extension given to a type of executable file in MS-DOS. A COM file is similar to an EXE file, but can only contain up to 64K of code and data. In operating systems other than DOS, the extension COM can have a different significance.

Companion Virus: A virus which 'infects' EXE files by creating a COM file with the same name which contains the virus code. It exploits the DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.

DOS: Disk Operating System. See MS-DOS.

DOS Boot Sector: The boot sector which loads the BIOS and DOS into PC RAM and starts their execution. Common point of attack by boot sector viruses.

EXE: The extension given to executable files in MS-DOS. These are similar to COM files, but can contain more than 64K of code and data.

FAT: File Allocation Table; a mnemonic term used by the MS-DOS operating system (and others) to describe the part of a disk which contains information describing the physical location on the disk of the chains of clusters forming the files stored on that disk.

IDE: The extension given to a file containing a virus identity encoded with Sophos' Virus Description Language (VDL). It will appear as a string of ASCII characters.

InterCheck: Proprietary Sophos technology which enables a server-based virus scanner to be used for scanning workstations connected to the network.

LAN: Local Area Network; a data communications network covering a limited area (up to several kilometres in radius) with moderate to high data transmission speeds.

Link Virus: A virus which subverts directory entries to point to the virus code.

Macro Virus: A virus which uses macros in a data file to become active in memory and attach itself to other data files.

Unlike conventional viruses, macro viruses can be written relatively easily with little specialist knowledge, and can also attain a degree of platform independence.

Master Boot Sector: The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the PC is booted. It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition. Common point of attack by boot sector viruses.

Memory-resident Virus: A virus which stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only while an infected application is running.

MS-DOS: The Disk Operating System (DOS) sold by Microsoft. It is the most common microcomputer operating system in the world, and it operates on the IBM Personal Computer.

Multipartite Virus: A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

Multi-tasking: The ability of a computer to divide its processing time amongst several different tasks. Although most computers contain only one CPU, they can switch between operations so quickly that several processes appear to run simultaneously.

Operating System: The computer program which performs basic housekeeping functions such as maintaining lists of files, running programs etc. PC operating systems include MS-DOS and OS/2, while minicomputer and mainframe operating systems include UNIX, VMS and MVS.

OS/2: An operating system for 80286+ based IBM compatibles. It allows true multi-tasking.

OVL: The extension commonly given to overlay files in MS-DOS. Overlay files are used with large programs which cannot fit into RAM: parts of the program are loaded as and when needed. Overlay files can have any extension, not just OVL.

Parasitic Virus: A computer virus which attaches itself to another computer program, and is activated when that program is executed. A parasitic virus can attach itself to either the beginning or the end of a program, or it can overwrite part of the program.

Polymorphic Virus: Self-modifying encrypting virus.

Stealth Virus: A virus which hides its presence from the PC user and anti-virus programs, usually by trapping interrupt services.

SYS: The extension given to system file names in MS-DOS. An example is the file CONFIG.SYS which sets up various configuration parameters for the operating system on power-up.

Trojan Horse: A computer program whose execution would result in undesired side-effects, generally unanticipated by the user. The Trojan horse program may otherwise give the appearance of providing normal functionality.

TSR: Terminate and Stay Resident; a term used to describe an MS-DOS program which remains in memory after being executed. A TSR can be re-activated either by a specific sequence of keystrokes, or at some specific time, or by some specific signal from an I/O port.

UNC: Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.

VDL: Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically. It has extensive facilities to cope with polymorphic viruses.

Virus: Sometimes explicitly referred to as a computer virus, a program which makes copies of itself in such a way as to ‘infect’ parts of the operating system and/or application programs. See Boot Sector Virus and Parasitic Virus.

Virus Identity: An algorithm describing various characteristics of a virus and used for virus recognition. Sophos describe viruses using the proprietary Virus Description Language (VDL).

Index

User comment form

We welcome your comments and suggestions on our software and documentation. They help us to provide you with better products. Please fax this form to +44 1235 559935. Comments about this manual can also be emailed to <publications@sophos.com>.

Product: ________________________________ Version: ❐.❐❐

Documentation:	Excellent	Good	Fair	Poor
Accuracy	❐	❐	❐	❐
Completeness	❐	❐	❐	❐
Clarity	❐	❐	❐	❐
Page layout	❐	❐	❐	❐

Software:	Excellent	Good	Fair	Poor
Ease of use:	❐	❐	❐	❐
Ease of installation:	❐	❐	❐	❐
Overall assessment:	❐	❐	❐	❐

Please indicate any errors found in this software or documentation:

____

____

____

Please give any suggestions for improving the software or documentation:

____

____

____

Name: ____

Position: ____

Organisation: ____

Address: ____

____

Telephone: ______________________ Fax: ______________________

Signed: ______________________ Date: ______________________

Australia:

Doctor Disk
Level 7
418A Elizabeth Street
Surry Hills NSW 2010
Australia
Email sales@drdisk.com.au
http://www.drdisk.com.au/
Tel 02 9281 2099 · Fax 02 9281 9740 · Code +61

Bahrain:

International Information Systems
PO Box 3086
Flat 31, Building 123 Block 320
Exhibition Road
Manama
Bahrain
Tel 293821, 292040 · Fax 293408 · Code +973

Belgium:

Software Marketing Group
rue E. Van Ophemstraat 40
B-1180 Brussels
Belgium
Email pbuysse@netdirect.be
Tel 02 376 57 42 · Fax 02 376 09 85 · Code +32

Brazil:

Datasafe Produtos de Informática e Serviços Ltda
Rua Santa Justina, 336 Gr. 108
Itaim
04545-041 Sao Paolo SP
Brazil
Email datasafe@originet.com.br
Tel 011 822 1129 · Fax 011 822 1129 · Code +55

Channel Islands:

Softek Services Ltd
20 Peter Street
St Helier
Jersey
JE2 4SP
Email sales@softek.co.uk
http://www.softek.co.uk/
Tel 01534 811182 · Fax 01534 811183 · Code +44

Croatia:

Qubis d.o.o.
Nova Cesta 1
10000 Zagreb
Croatia
Email qubis@zg.tel.hr
Tel 01 391461 · Fax 01 391294 · Code +385

Denmark:

Lamb Soft & Hardware
Lille Strandstraede 14
1254 Copenhagen K
Denmark
Email info@lamb-soft.dk
Tel 3393 4793 · Fax 3393 4793 · Code +45

Finland:

Oy Protect Data Ab
P.O. Box 48
00931 Helsinki
Finland
Email antti.laaja@dlc.fi
Tel 09 752 521 · Fax 09 7525 2210 · Code +358

France:

Racal-Datacom S.A.
18 Rue Jules Saulnier
93206 Saint-Denis Cedex
France
Email plemounier@racal-datacom.fr
Tel (1) 49 33 58 00 · Fax (1) 49 33 58 33 · Code +33

Germany:

NoVIR DATA
Hochofenstrasse 19-21
23569 Lübeck
Germany
Email 100141.2044@compuserve.com
Tel 0451 306 066 · Fax 0451 309 600 · Code +49

Hong Kong:

Racal-Datacom Limited
Sun House
181 Des Voeux Road
Central Hong Kong
Email w_chu@racal.com.hk
Tel 28158633 · Fax 28158141 · Code +852

Ireland:

Renaissance Contingency Services Ltd.
The Mews
15 Adelaide Street
Dun Laoghaire
Co Dublin
Ireland
Tel 01 280 9410 · Fax 01 280 8302 · Code +353

Italy:

Telvox s.a.s.
Via F.lli Cairoli 4-6
40121 Bologna
Italy
Email telvox.teleinf@bologna.nettuno.it
http://www.nettuno.it/fiera/telvox/telvox.htm
Tel 051 252 784 · Fax 051 252 748 · Code +39

Japan:

Computer Systems Engineering Co. Ltd.
23-2 Maruyamacho
Aletsusa Bldg.
Shibuya-ku
Tokyo 150
Japan
Email pws@cseltd.co.jp
http://www.cseltd.co.jp/sweep/
Tel 03 3463 5633 · Fax 03 3496 7477 · Code +81

Malta:

Shireburn Co. Ltd.
Carolina Court
Guze Cali Street
Ta'Xbiex, Msd 14
Malta
Email info@shireburn.com
http://www.shireburn.com/
Tel 319977 · Fax 319528 · Code +356

Netherlands:

CRYPSYS Data Security
P.O. Box 542
4200 AM Gorinchem
The Netherlands
Email crypsys@pi.net
http://www.pi.net/~crypsys/
Tel 0183 62 44 44 · Fax 0183 62 28 48 · Code +31

Forum Data Security
WG Plein 202
1054 SE Amsterdam
The Netherlands
Email forum_data_security@pi.net
Tel 20 685 3486 · Fax 20 612 9702 · Code +31

New Zealand:

Wang New Zealand Ltd
P O Box 6648
Wellington
New Zealand
Email sophos@wang.co.nz
Tel 04 382 0100 · Fax 04 385 6067 · Code +64

Norway:

Protect Data Norge AS
Brobekkveien 80
0583 Oslo
Norway
Email protect_data@oslonett.no
Tel 022 65 64 50 · Fax 022 65 64 58 · Code +47

Poland:

Safe Computing Ltd.
ul. Targowa 34
03-733 Warszawa
Poland
Email info@safecomp.com
http://www.safecomp.com/
Tel 022 6198956 · Fax 022 6700756 · Code +48

Portugal:

Década Informática s.a.
Apt. 7558
Estr. Lisboa/Sintra, Km 2,2
2720 Alfragide
Portugal
Email amandio.sousa@decada.mailpac.pt
Tel 01 471 2045 · Fax 01 471 2191 · Code +351

Singapore:

Racal Electronics (S) Pte. Ltd.
26 Ayer Rajah Crescent #04-06/07
Singapore 139944
Email sales@racal.com.sg
http://www.racal.com.sg/
Tel 779 2200 · Fax 778 5400 · Code +65

Slovakia:

Protect Data Slovakia
Kukolova 1
831 07 Bratislava
Slovak Republic
Email protectd@ba.sanet.sk
Tel 07 541 1527 · Fax 07 541 2210 · Code +421

Slovenia:

Sophos d.o.o.
Zwittrova 20
8000 Novo mesto
Slovenia
Email slovenia@sophos.com
Tel 068 322977 · Fax 068 322975 · Code +386

Spain:

Sinutec Data Security Consulting S.L.
Traversera de Gracia 54-56 Entlo. 3 y 4
08006 Barcelona
NIF B-60062502
Spain
Email sinutec@ysi.es
http://www.sinutec.com/
Tel 93 490 70 52 · Fax 93 490 76 04 · Code +34

Sweden:

Protect Datasäkerhet AB
Humlegardsgatan 20, 2tr
Box 5376
102 49 Stockholm
Sweden
Email info@protect-data.se
http://www.protect-data.se/
Tel 08 459 54 00 · Fax 08 459 54 10 · Code +46

Switzerland:

Performance System Software SA
Rue Jean-Pelletier 6
1225 Chene-Bourg
Geneva
Switzerland
Email jlt@pss.ch
http://www.pss.ch/
Tel 022 860 1030 · Fax 022 349 4775 · Code +41

Turkey:

Logic Bilgisayer Ltd
Esentepe Cad. Techno Centre 10/2
Mecidiyekoy
Istanbul
Turkey
Tel 0212 212 3664 · Fax 0212 212 3669 · Code +90

United States of America:

ACT
7908 Cin-Day Rd, Suite W
West Chester
Ohio 45069
USA
Email farrell@altcomp.com
http://www.altcomp.com/
Tel 513 755 1957 · Fax 513 755 1958 · Code +1

Uruguay:

Datasec
Patria 716
Montevideo 11300
Uruguay
Tel 02 715878 · Fax 02 715894 · Code +598

Sophos Plc • The Pentagon • Abingdon Science Park • Abingdon • OX14 3YP • England • Tel 01235 559933 • Fax 01235 559935
Sophos Inc • 18 Commerce Way • Woburn • MA 01801 • USA • Tel 781 932 0222 • Fax 781 932 0251
Sophos GmbH • Am Hahnenbusch 21 • D-55268 Nieder-Olm • Germany • Tel 06136 91193 • Fax 06136 911940

Email sales@sophos.com • http://www.sophos.com/