Sophos Anti-Virus

User Manual

Banyan VINES

SOPHOS

Sophos Anti-Virus

for Banyan VINES

User Manual
December 1997

This manual documents Sophos Anti-Virus
for Banyan VINES, which incorporates
SWEEP 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 # masbez08/971112

This document is also available in electronic form from Sophos.

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

Contents

About SWEEP

This chapter introduces SWEEP, describes features specific to SWEEP for Banyan VINES, and helps users identify the most relevant chapters for their needs.

What is SWEEP?

SWEEP offers on-demand, scheduled and (with InterCheck) on-access virus checking, along with automatic reporting and disinfection.

SWEEP for Banyan VINES

SWEEP for Banyan VINES may be installed as a service on a Banyan VINES server to check files held on the server. This has several advantages over checking files on the server by running SWEEP for DOS from a workstation:

- It does not involve DOS in sweeping, which means that it is not susceptible to the stealth techniques used by some viruses.
- It uses the local UNIX file system to access the files being swept, rather than having to use the Banyan Filing System (BFS) service through the network. Thus it is approximately three times faster than SWEEP for DOS run from a workstation, and causes no network traffic.
- It is not subject to BFS access restrictions, and does not need to be given rights to every file in the system.

SWEEP for Banyan VINES also includes a licence to use both the DOS and Windows 95 versions of SWEEP on workstations connected to the server.

Features of SWEEP for Banyan VINES

SWEEP for Banyan VINES:

- Checks Banyan Filing System (BFS) volumes for the presence of all viruses known to Sophos at the time of SWEEP's release.
- Incorporates Sophos' proprietary InterCheck client-server virus detection technology, which allows the use of server based software for checking workstations.
- Is updated twelve times a year, and urgent updates can be distributed by fax or email or downloaded from Sophos' Web site.
- Easily detects polymorphic viruses using Sophos' advanced Virus Description Language (VDL) and a built-in code emulator.
- Scans inside compressed files.
- 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 in every part of every file.
- Is easy to use, and easily integrated into complex virus-checking applications, such as the automated unattended checking of file servers.
- Can be scheduled, so SWEEP can be configured to perform regular checks without any further operator action.
- Allows immediate automatic notification of virus infection.
- Has low network overhead.

How to use this manual

This manual assumes some familiarity with Banyan VINES. It is organised into the following chapters:

- 'About SWEEP', this chapter.
- 'About InterCheck' presents an overview of Sophos' InterCheck technology.
- 'Installing SWEEP' describes how to install SWEEP as a service on a Banyan VINES file server, how to install and start SWEEP as an InterCheck server, and how to update SWEEP.
- 'Using SWEEP' describes how to start, stop, configure, and schedule the SWEEP service, and how to create a new notification list.
- 'Installing InterCheck clients' describes how to install and run InterCheck clients on workstations.
- 'Controlling the InterCheck server' describes how to configure and control SWEEP running as an InterCheck server.
- 'Configuring InterCheck clients' describes the configuration of InterCheck clients running under Windows 95, Windows for Workgroups, Windows 3.x, and DOS.
- 'Treating viral infection' describes how to deal with a virus once it has been discovered.
- 'Troubleshooting' provides help with possible problems.

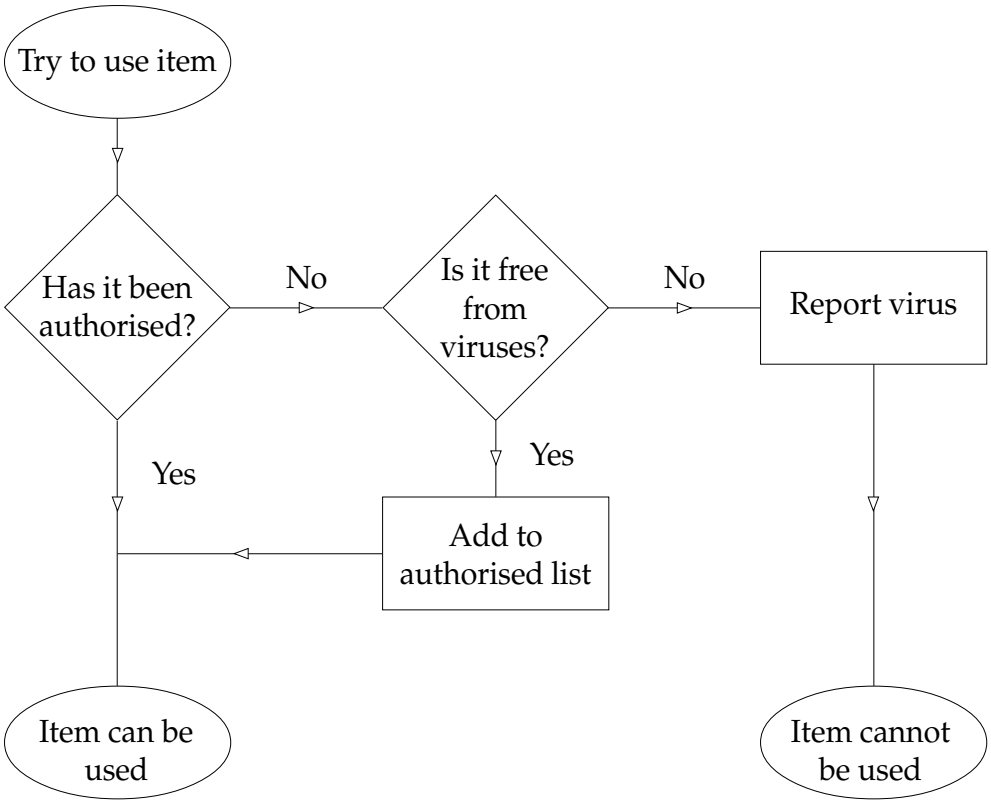
In addition, the 'Glossary' contains explanations of some technical terms used in this guide.

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.

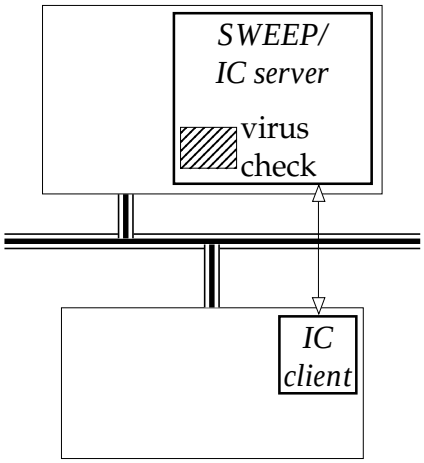
A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

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.

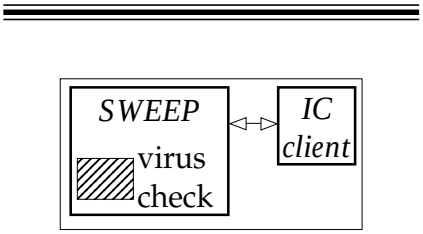
How does InterCheck work?

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

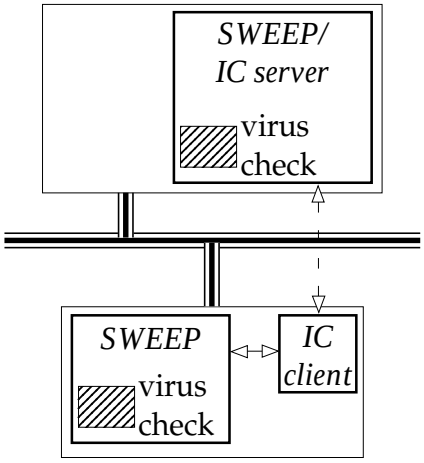


Networked IC client and remote IC server

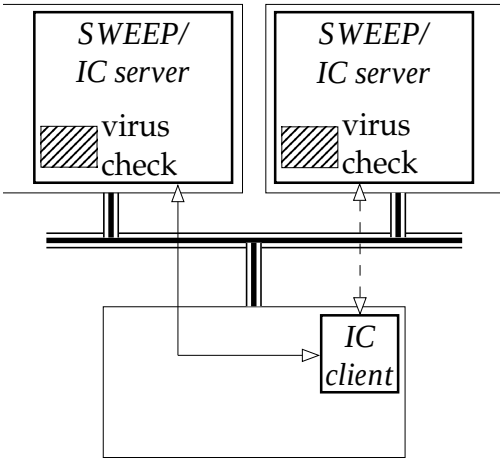
No IC server



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 SWEEP

This chapter describes how to install SWEEP as a service on a Banyan VINES file server, how to install and start SWEEP as an InterCheck server, and how to update SWEEP.

Note: The examples below refer to VINES 6.20(0). Other versions of VINES might differ slightly.

System requirements

The minimum requirements to use SWEEP for Banyan VINES are:

- A PC compatible Banyan VINES server with a 1.44Mb 3.5" floppy disk drive.
- Banyan VINES version 5 or greater, except VINES 6.00(0) and VINES 6.00(10). VINES 6.00(0) must either be upgraded to 6.00(10) with site specific patch V95008, or be upgraded to 6.20(0). VINES 6.00(10) must either have site specific patch V95008 applied, or be upgraded to 6.20(0).
- A minimum of 5Mb free space on the disk1 partition.

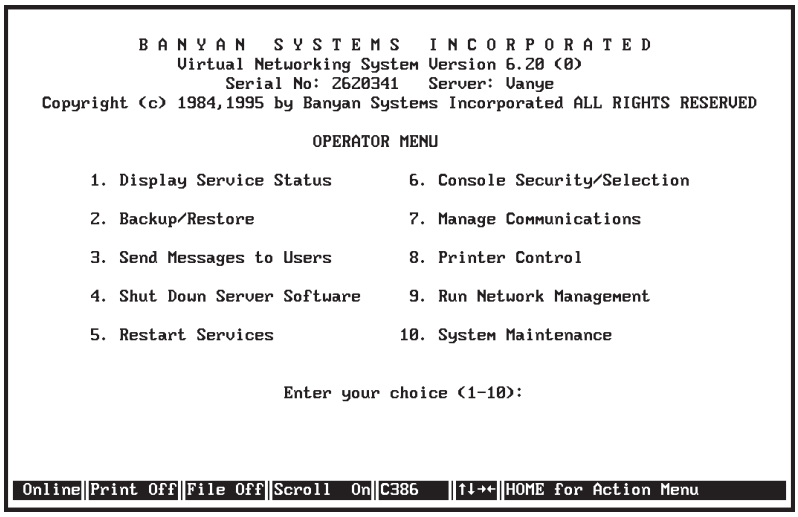
Installing SWEEP as an InterCheck server

When SWEEP for Banyan VINES is active, it should always be capable of serving as an InterCheck server for client workstations.

Installing the SWEEP service

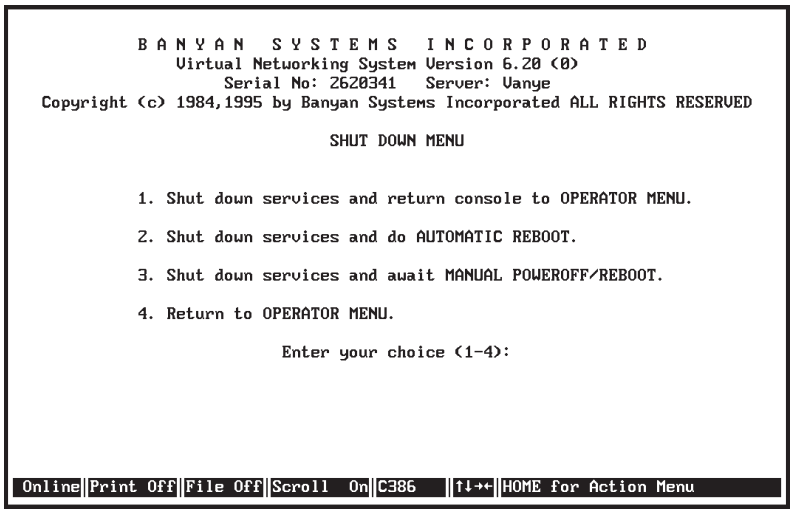
When the server and all the services are running, insert the SWEEP for Banyan VINES disk into the server's disk drive.

On the server console, ensure the main OPERATOR MENU is displayed.



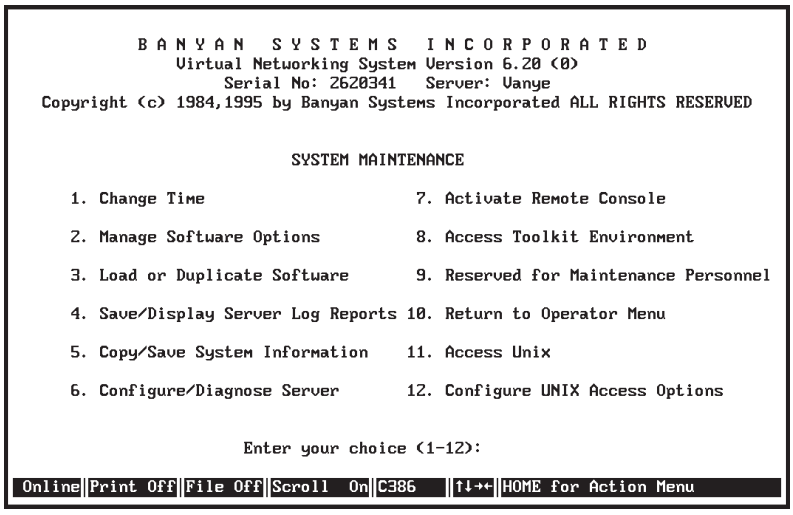
A new service cannot be added while the VINES server service is running, so the server software has to be stopped before the SWEEP service can be installed.

Select the *Shut Down Server Software* option from the OPERATOR MENU. Answer 'y' to 'Do you really want to SHUT DOWN all services?'. The SHUT DOWN MENU appears:

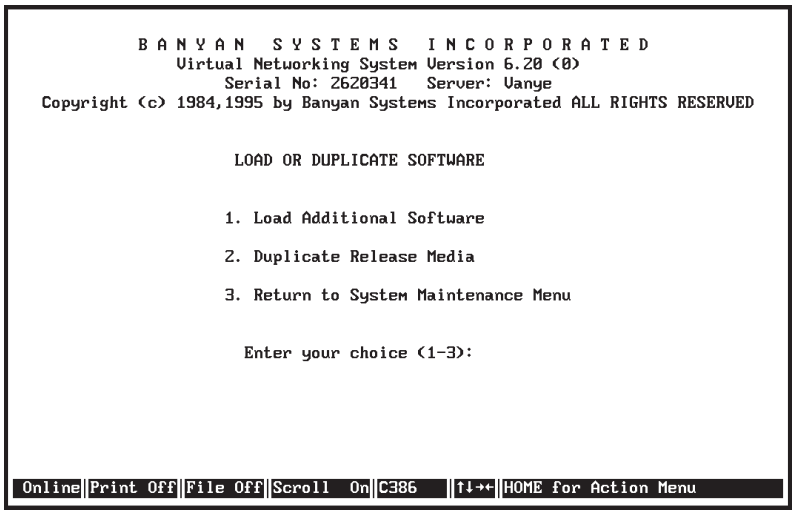


Select *Shut down services and return console to OPERATOR MENU*.

From the OPERATOR MENU, choose *System Maintenance*. Then select *Load or Duplicate Software* from the SYSTEM MAINTENANCE menu:



From the LOAD OR DUPLICATE SOFTWARE menu, select *Load Additional Software*.



Note: Earlier versions of Banyan VINES do not have the *Load or Duplicate Software* option on the SYSTEM MAINTENANCE menu. The option is replaced by *Load Additional Software*. Select this option. The LOAD OR DUPLICATE SOFTWARE menu will not be presented.

The message

```
Load the software diskette. Press [return] when ready, or q [return] to quit :
```

is displayed. Press *Return*. After a short pause, the text

```
One moment please ...
Sophos SWEEP Virus Detection Service Installation ...
```

followed by the names of the files that are copied from the disk is displayed. When all the files have been copied:

```
Sophos SWEEP Virus Detection Service installed successfully.

You must now restart the server's services in order for it to
recognise the existence of SWEEP.

After your services have restarted, create and start the SWEEP
service as described in the SWEEP manual.

Press <RET>
```

Press *Return* to return to the SYSTEM MAINTENANCE menu, and then select *Return to Operator Menu*.

Select *Restart Services* from the OPERATOR MENU to restart the server's services. The server service will now know that a SWEEP service can be created, although the service has not yet been created and started.

Creating the SWEEP directory structure

A directory has to be created for the DOS components of SWEEP. This must be made with a PC that is a client of the server on which the SWEEP for Banyan VINES service has been installed.

On a client PC, log in as a user on the server's AdminList (the list of system administrators). Select a Banyan File Service to install the DOS components onto. This must be on the same server that SWEEP for Banyan VINES is installed on. A new file service can be created for SWEEP and InterCheck if so desired, by following the procedure described in the 'Creating, configuring and starting the SWEEP service' section below.

A file service called InterCheck@Vanye@Servers will be used in the examples below.

Switch to the drive letter which corresponds to that file service. For example, if drive I: is set to the file service 'InterCheck@Vanye@Servers', enter

```
I:
```

at the DOS prompt. On that file service, create the following directory structure using the MKDIR command:

```
MKDIR \SWEEP
MKDIR \SWEEP\COMMS
MKDIR \SWEEP\INFECTED
MKDIR \SWEEP\LISTS
```

Setting the SWEEP access rights

Change to the main SWEEP directory created in the 'Creating the SWEEP directory structure' section, e.g.

```
I:
CD \SWEEP
```

Enter

```
SETARL
```

to start the program used to set the SWEEP Access Rights List (ARL).

SWEEP needs to have sufficient permission on the root directory \ to be able to find and enter the \SWEEP directory. The easiest way to do this is to add the SWEEP service to the Extended ARL for the root directory, to create the following ARL:

```
                    C S R W D  C E R W
EXTENDED LIST: Maximum Rights+ + + + +  + + + +
SWEEP@Vanye@Servers           - + + - -  - - - -
```

\SWEEP should be owned by the SWEEP service, and its ARL should be

```
          Directory  New Files
          C S R W D  C E R W
  Owner + + + + +  + + + +
  Group - + + - -  - + + -
  Other - + + - -  - + + -
```

\SWEEP\COMMS should have the same owner and group as \SWEEP, and its ARL should be

```
          Directory  New Files
          C S R W D  C E R W
  Owner + + + + +  + + + +
  Group - + + + +  - - + +
  Other - + + + +  - - + +
```

\SWEEP\INFECTED should have the same owner and group as \SWEEP, and its ARL should be

```
        Directory  New Files
        C S R W D  C E R W
Owner   + + + + +  + + + +
Group   - - - - -  - - - -
Other   - - - - -  - - - -
```

\SWEEP\LISTS should have the same owner and group as \SWEEP, and its ARL should be

```
        Directory  New Files
        C S R W D  C E R W
Owner   + + + + +  + + + +
Group   - + + + +  + + + +
Other   - + + + +  + + + +
```

Copying the SWEEP and InterCheck files

The contents of the SWEEP for DOS, InterCheck and ICONTROL disks should be copied into the SWEEP directory after the SWEEP access rights have been set. For example, enter

```
COPY A:*.* I:\SWEEP
```

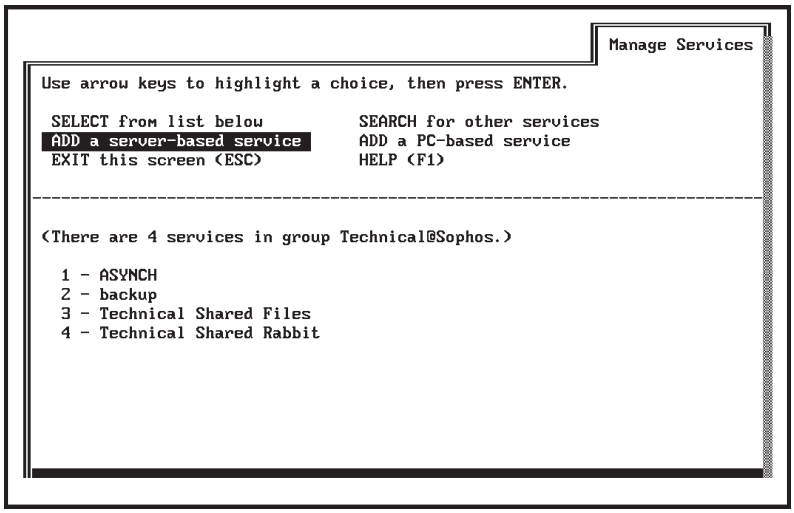
with each disk in drive A: in turn.

Creating, configuring and starting the SWEEP service

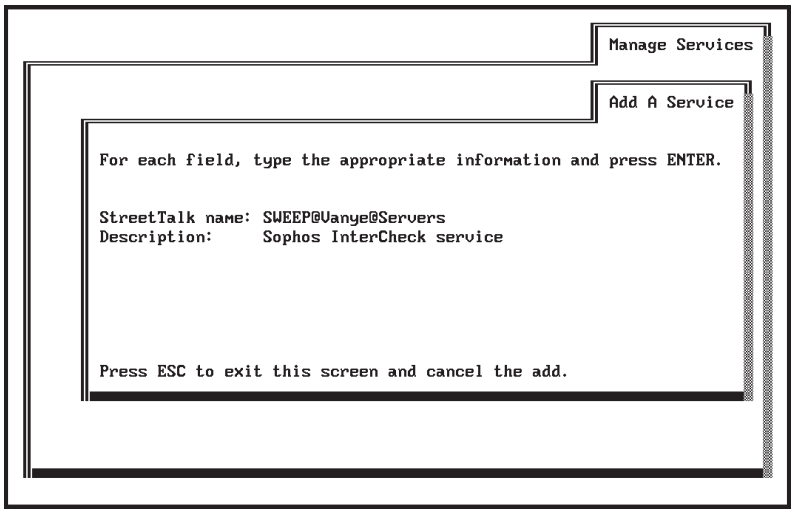
From the DOS prompt, enter

```
MSERVICE
```

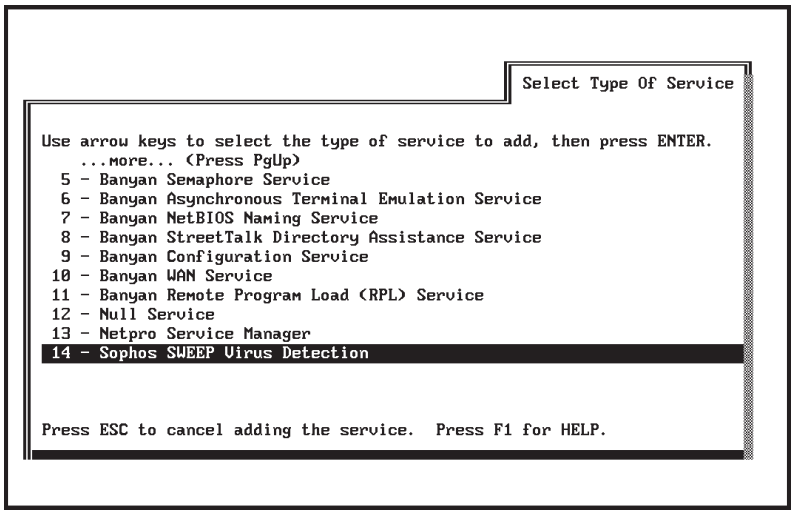
to run the Manage Services program, then select *ADD a server-based service*:



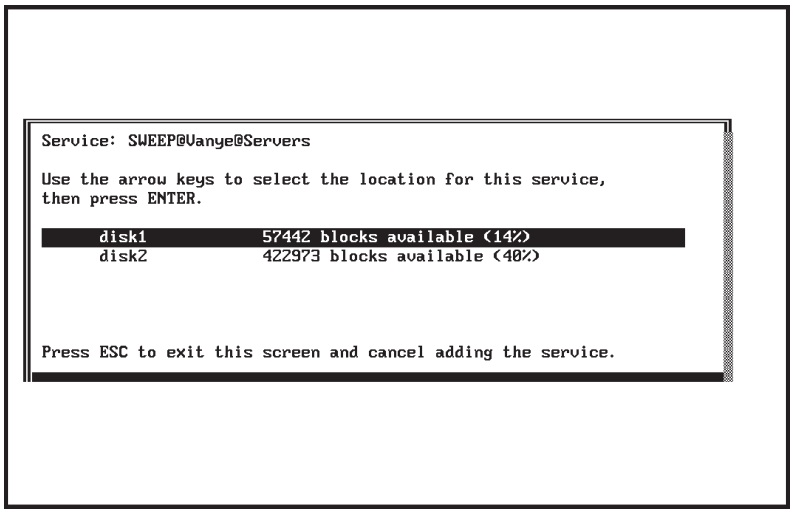
Enter a StreetTalk name for the new service, and a description of it. For example



will name the SWEEP service SWEEP@Vanye@Servers. After pressing *Enter*, the type of service has to be selected:

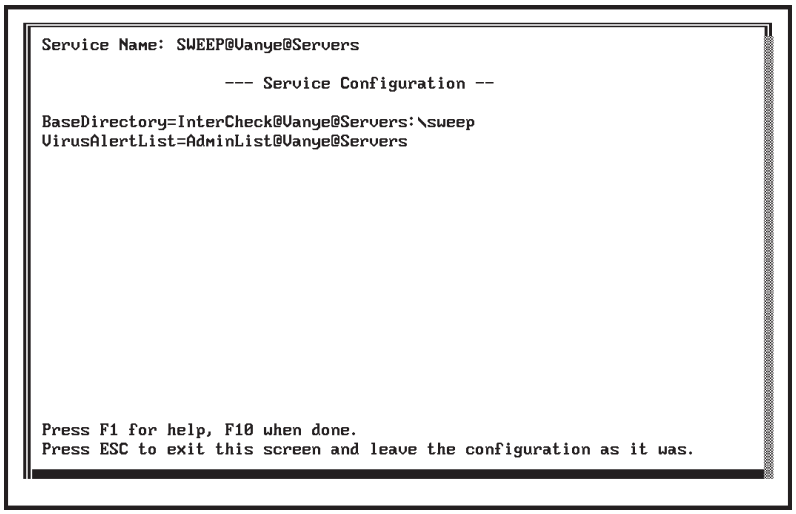


Select *Sophos SWEEP Virus Detection* from the list of service types, then select which disk SWEEP is to use for its log and temporary files:



About 5Mb disk space (10,240 blocks) should be available to SWEEP for this purpose.

After pressing *Enter*, the 'Service Configuration' screen will be presented:



This will initially be blank, but the above example shows entries for BaseDirectory and VirusAlertList. Entries are in the INI-file style, which consists of lines of keyword=value pairs.

BaseDirectory=<fileservice:directory>

This entry **must** be present. SWEEP's BaseDirectory is the directory created in the 'Creating the SWEEP directory structure' section. Within this directory are the SWEEP for DOS and the InterCheck files, along with the InterCheck COMMS, INFECTED and LISTS directories.

The value following this keyword consists of the name of a Banyan File Service and the pathname within that file service, separated by a colon. For example

```
BaseDirectory=InterCheck@Vanye@Servers:\sweep
```

means the directory \sweep within the file service 'InterCheck@Vanye@Servers'.

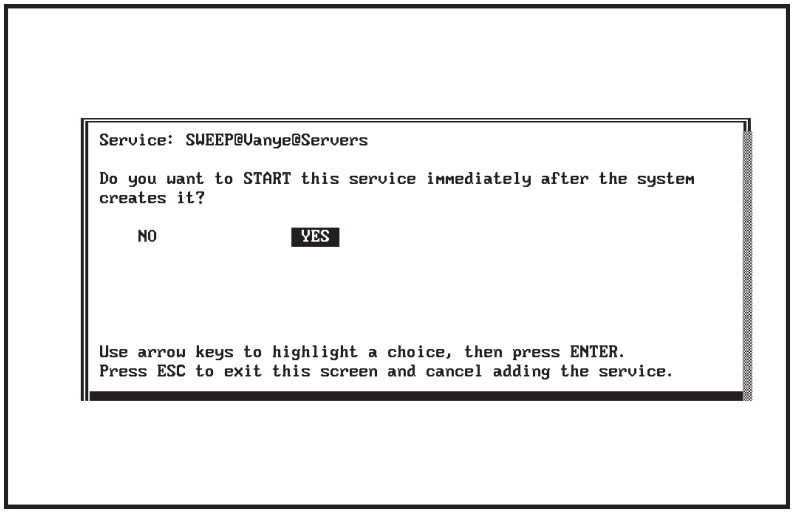
VirusAlertList=<StreetTalkList>

It is advisable to create a list of people to notify if a virus is found.

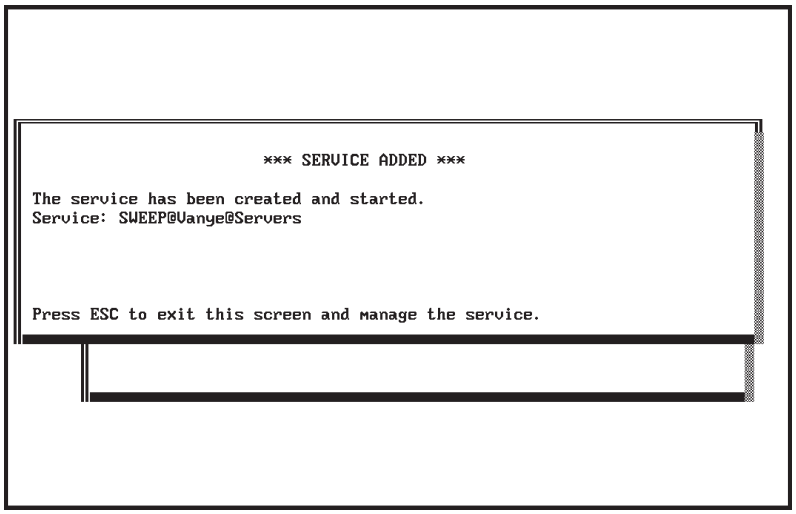
The VirusAlertList is the name of a StreetTalk list containing the StreetTalk names of all the users that will be notified if a virus is discovered. A pre-existing list (e.g. AdminList) can be used or a new list can be created. See the 'Creating a new notification list' section of the 'Using SWEEP' chapter.

Other SWEEP configuration options are described in the 'Configuring SWEEP' section of the 'Using SWEEP' chapter.

Press *F10* to save the configuration. You will then be asked whether you want to start the service immediately on creation:



Select 'YES' to create and start the service. The following screen will appear:



Press *Esc* repeatedly to return to the DOS prompt.

Remotely monitoring and controlling the InterCheck server

This is accomplished with ICONTROL, as described in the 'Controlling the InterCheck server' chapter.

Updating SWEEP

Registered users of SWEEP are sent an updated SWEEP disk in the first week of every month, or can download updated versions from the Sophos Web site. Both SWEEP for Banyan VINES and SWEEP for DOS should be updated.

To update SWEEP for Banyan VINES, stop all SWEEP services, as described in the 'Starting and stopping SWEEP' section of the 'Using SWEEP' chapter. **It is not necessary to shut down the file server or any other services**. Load the additional software, and restart the SWEEP services.

To update the SWEEP for DOS components, copy the contents of the SWEEP for DOS disk into the SWEEP directory as described at the end of the 'Creating the SWEEP directory structure' section. It is not necessary to restart the SWEEP service after doing this.

Urgent SWEEP updates

SWEEP is updated each month. However, users can add new 'virus identities', which SWEEP will use 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 the Sophos Web site (http://www.sophos.com/).

The IDE files should be saved as ASCII files with an IDE extension and placed in the directory configured as the BaseDirectory. SWEEP will then load the new virus identities when restarted.

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

Using SWEEP

This chapter describes how to start, stop, configure, and schedule the SWEEP service, and how to create a new notification list.

Starting and stopping SWEEP

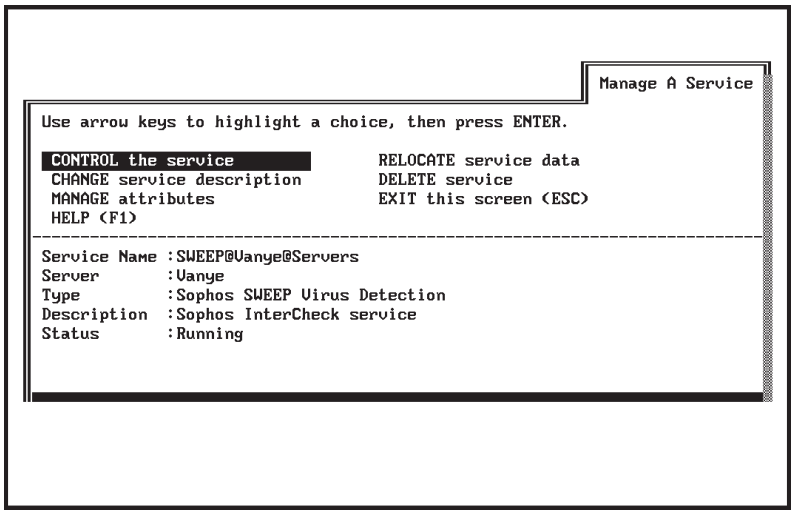
To start or stop the SWEEP for Banyan VINES service, first type the command

```
MSERVICE servicename
```

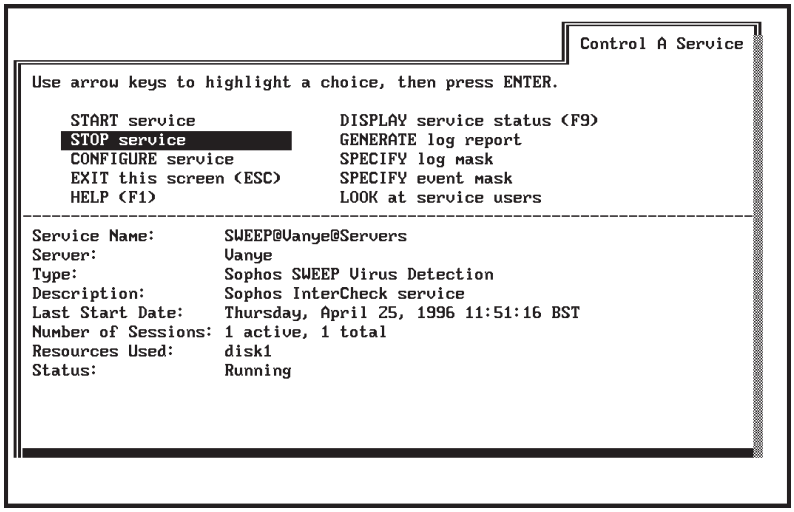
for example

```
MSERVICE SWEEP@Vanye@Servers
```

if the service name is SWEEP@Vanye@Servers, then select *CONTROL the service*.

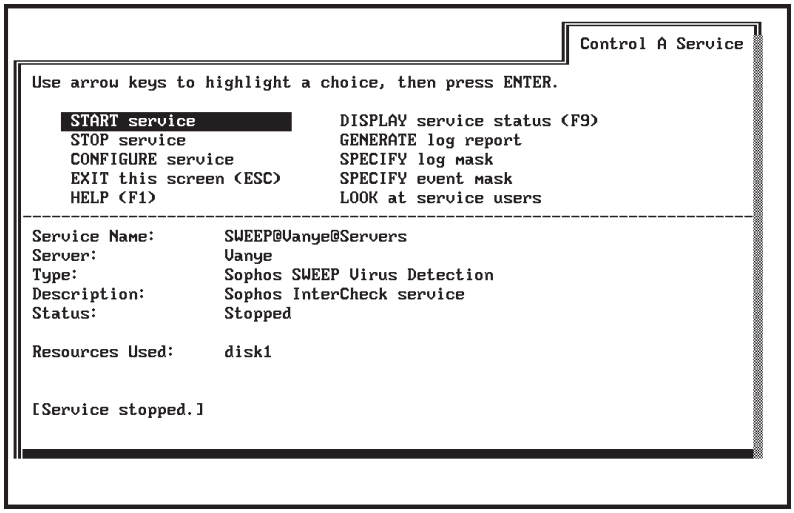


To stop the service, select *STOP service* from the 'Control A Service' screen.



After a few moments the display will show that SWEEP has been halted.

To start the service, select *START service* from the 'Control A Service' screen.



After a few moments the display will show that SWEEP is running.

Configuring SWEEP

The configuration of SWEEP as an InterCheck server, with the exception of some Banyan specific features, is largely handled by the ICONTROL for DOS or ICONTROL for Windows programs. See the 'Controlling the InterCheck server' chapter. All other configuration is defined in the Service Configuration Record for the SWEEP service.

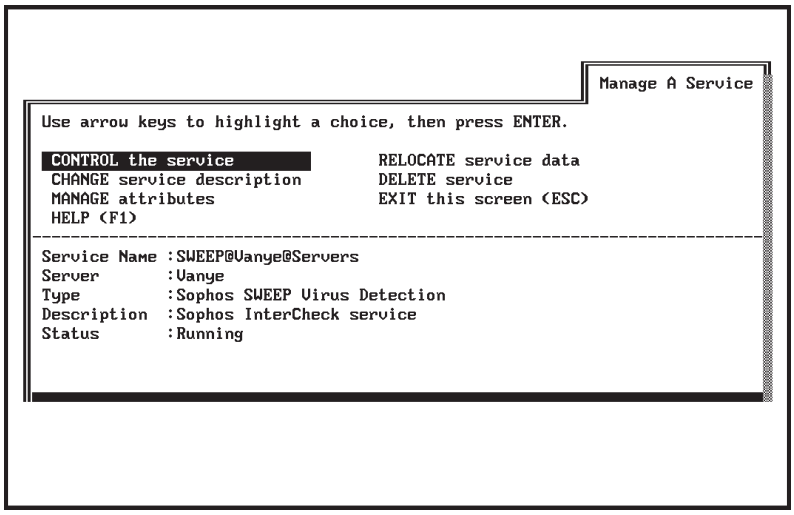
The service must be running in order to edit its Service Configuration Record after it has been installed. To edit it, type the command

```
MSERVICE servicename
```

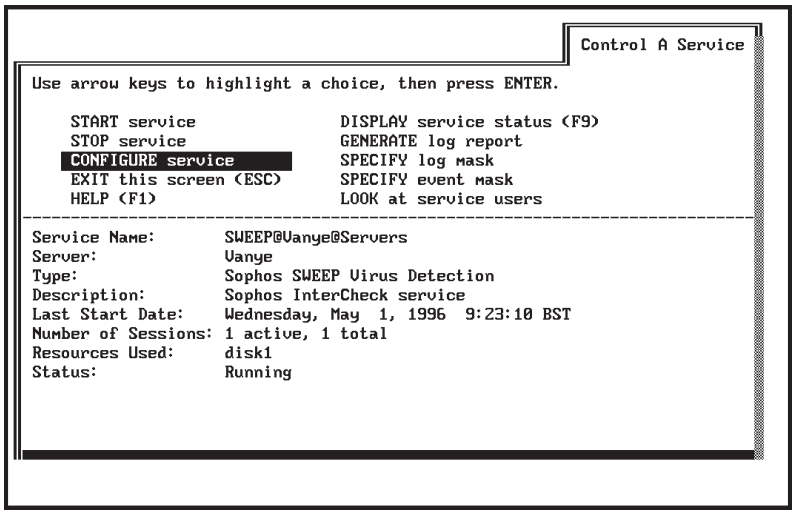
for example

```
MSERVICE SWEEP@Vanye@Servers
```

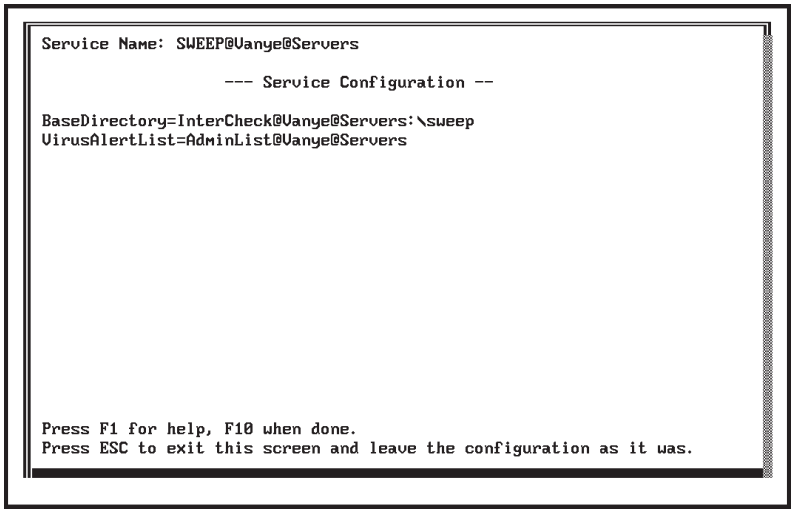
if the service name is SWEEP@Vanye@Servers, then select *CONTROL the service*



and then select *CONFIGURE the service* from the 'Control A Service' screen.



The service configuration record is divided into two by a line consisting of the single word TIMES (case does not matter). Above it are configuration parameters; below it are scheduled job specifiers. If the line consisting of TIMES does not exist, as in the example below, everything is assumed to consist of configuration parameters.



The configuration parameters are:

BaseDirectory=<fileservice:directory>

This specifies the directory on a Banyan File Service volume that contains the COMMS and INFECTED

directories. It is also where SWEEP writes its log files and looks for .IDE virus update files. The directory is specified as the name of the BFS service on which it resides, and the path within that service, separated by a colon.

For example:

```
BaseDirectory=InterCheck@Vanye@Servers:\sweep
```

refers to the directory \sweep on the file service InterCheck@Vanye@Servers.

Important! SWEEP for Banyan VINES cannot function without the BaseDirectory= parameter.

DisinfectDocuments=NO|YES

SWEEP for Banyan VINES can detect and automatically disinfect macro viruses inside OLE files. However, it can only disinfect a document if the SWEEP service has write access to the file, and SWEEP will *not* attempt to change ownership, permissions or attributes to allow itself to do this.

If SWEEP does not have write access to the file it will issue a warning, and SWEEP for DOS should be used to disinfect the file.

The default setting for DisinfectDocuments is NO, because the number of documents that the Banyan SWEEP service has write access to is likely to be limited.

ScheduledNotify=YES|NO

This enables SWEEP to notify the members of the VirusAlertList (see VirusAlertList=<StreetTalkList> parameter below) when a virus or viruses are detected during a scheduled job. Notification takes place once the job is finished.

The default setting for ScheduledNotify is NO.

ScheduledSweepLevel=QUICK|FULL

Specify QUICK or FULL to make either a 'quick sweep' or a 'full sweep' the default for scheduled sweeping. Quick sweep only checks the parts of files likely to contain viruses, while the full sweep examines the complete contents of each file. For normal operation quick sweep is sufficient.

For example:

```
ScheduledSweepLevel=FULL
```

If the ScheduledSweepLevel is not specified, QUICK will be assumed.

VirusAlertList=<StreetTalkList>

This specifies a StreetTalk list whose members are notified by means of 25th line messages (in DOS) or pop-up messages (in Windows) when a virus is detected by InterCheck or a scheduled SWEEP. The user can create a new list for this purpose, or use an existing list such as the AdminList for a relevant server or group.

For example:

```
VirusAlertList=AdminList@Technical@Sophos
```

will cause all members of Technical@Sophos' AdminList to be notified on virus discovery.

Scheduling SWEEP

SWEEP for Banyan VINES can be configured to check areas of local file services at specified times.

Scheduled SWEEP jobs are configured in the Service Configuration Record below a line consisting only of the word 'TIMES'.

Each job definition consists of an *area description* followed by one or more *time descriptions*.

Area description

An area description is enclosed within square brackets ('[' and ']'), and describes the path to be swept. It consists of two components separated by a colon: the file service's StreetTalk name, and the directory and wildcards.

For example:

```
[fs1@technical@sophos:\*.*]
```

specifies that all files and directories under the root (*.*) of the file service fs1@technical@sophos will be swept.

SWEEP will also look at all subdirectories of the specified area.

Time description

Time descriptions refer to the preceding area description. Each time description must appear on a line of its own, and consists of an optional time followed by an optional day or date.

Time is specified in 24-hour format and wildcard characters (?) are allowed.

For example

```
[fs1@technical@sophos:\*.*]
7:00 Mon     ; 7am Monday
12:00 Mon,Tue,Wed,Thu,Fri;12:00weekdays
??:30
  ; 30 mins past each hour
[fs2@technical@sophos:\*.*]
22/4
[fs3@technical@sophos:\*.*]
22/4/96
```

would sweep fs1@technical@sophos:*.* at 7:00 on Mondays, 12:00 on working days and at 30 minutes past each hour. It would also sweep

fs2@technical@sophos:*.* on the 22nd of April and fs3@technical@sophos:*.* on the 22nd of April, 1996.

If a '+' follows a time, it means 'at that time or later'.

For example:

```
[fs1@technical@sophos:\*.*]
19:00+
```

would sweep fs1@technical@sophos:*.* if SWEEP is started at 19:00 or later, or at 19:00 if SWEEP was already running at that time.

Time descriptions can also contain a date, which may contain wildcards.

For example:

```
[fs1@technical@sophos:\*.*]
0:00 1/?/?
```

would sweep fs1@technical@sophos:*.* on the 1st of each month at midnight.

Dates are specified in European style, i.e. day, month, year. Months can be spelled out, e.g. January, but the first three characters must be given.

Example service configuration record

An example of a service configuration record:

```
BaseDirectory=InterCheck@Vanye@Servers:\sweep
VirusAlertList=AdminList@Vanye@Servers
ScheduledSweepLevel=FULL
TIMES
[fs1@technical@sophos:\*.*]
3:00
```

SWEEP log file

SWEEP for Banyan VINES maintains an InterCheck log file (normally called SWEEP.LOG), which is stored in SWEEP's BaseDirectory.

The InterCheck log file contains information about all InterCheck activity since the SWEEP service was installed. Its name, and the level of detail it contains, can be set with ICONTROL for DOS or ICONTROL for Windows (see the 'ICONTROL for DOS options' and 'ICONTROL for Windows options' sections of the 'Controlling the InterCheck server' chapter).

The scheduled scan information is placed in the service log file, which can be accessed using MSERVICE or the StreetTalk Explorer. InterCheck information is also replicated in this log file.

Note: If the service log file is larger than 64Kb, MSERVICE may not be able to display it. However, the log can still be saved to a file and viewed with an external text editor. The service log file should be pruned in the normal way for the user's system.

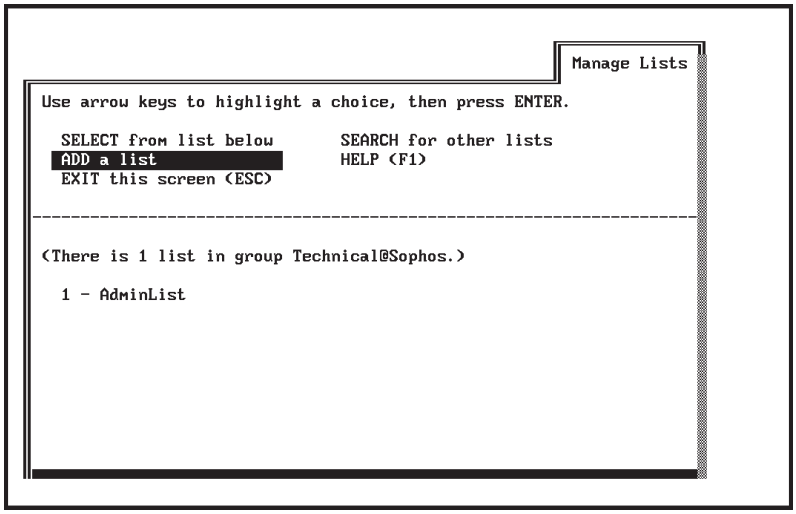
Creating a new notification list

SWEEP can report a virus discovery to all users who are members of a list given to SWEEP and who are logged in at the time the virus is found (see the 'VirusAlertList' parameter in the 'Configuring SWEEP' section above). An existing list, such as the server's AdminList, can be used, or a new list can be created.

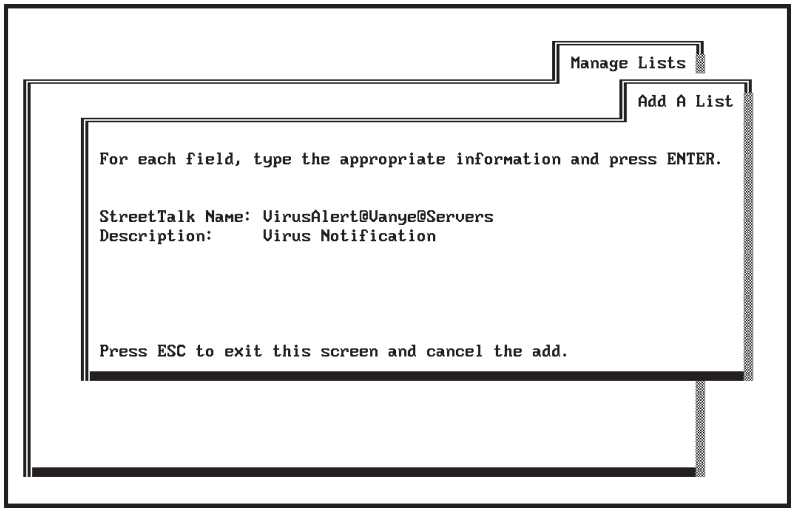
To create a new list, enter

```
MLIST
```

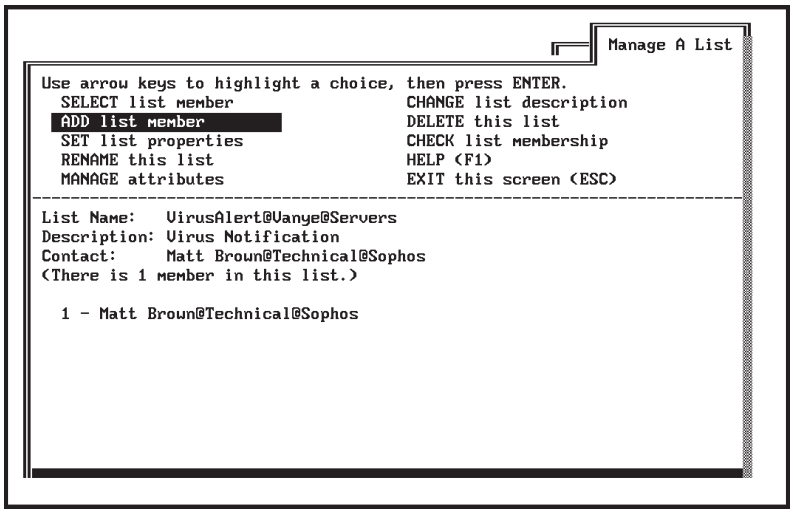
at the DOS prompt. Choose *ADD a list* from the 'Manage Lists' screen:



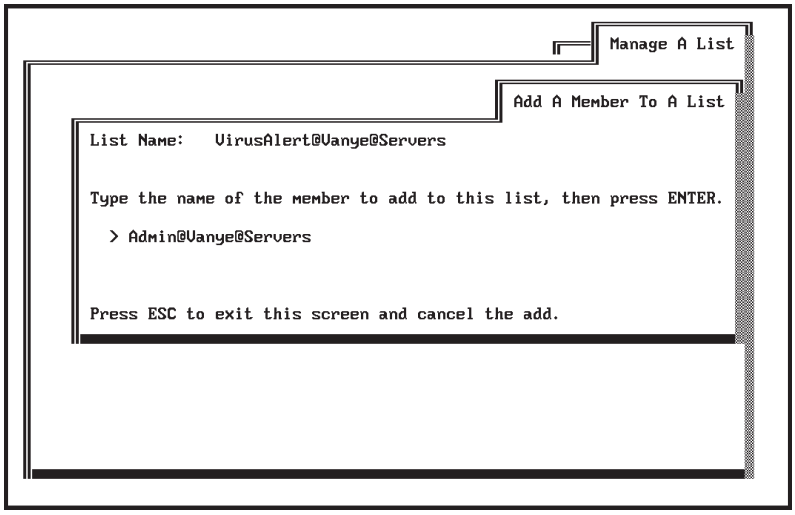
Give this list a name along with a short description of its purpose, for example



Press *Enter*, then on the 'Manage A List' screen select *ADD list member*.



On the 'Add A Member To A List' screen, type the user's name and press *Enter* to confirm the name.



Repeat the process for each individual who is to receive the virus alert message.

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. 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

With a Banyan VINES server, running InterCheck from a login script involves running ICLOGIN from each VINES user profile. Each individual user normally has a profile which includes a sample profile with the USE command. In this case, it is preferable to run ICLOGIN from the sample profile rather than each individual user profile.

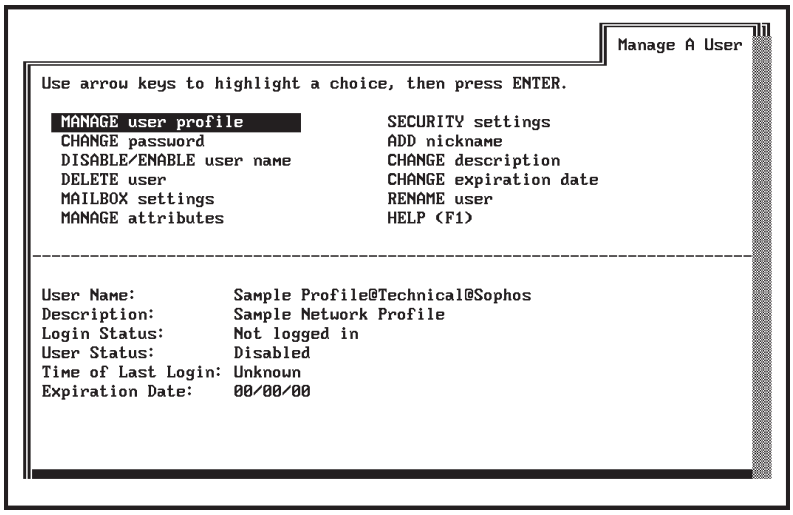
Enter at the DOS prompt

```
MUSER profilename
```

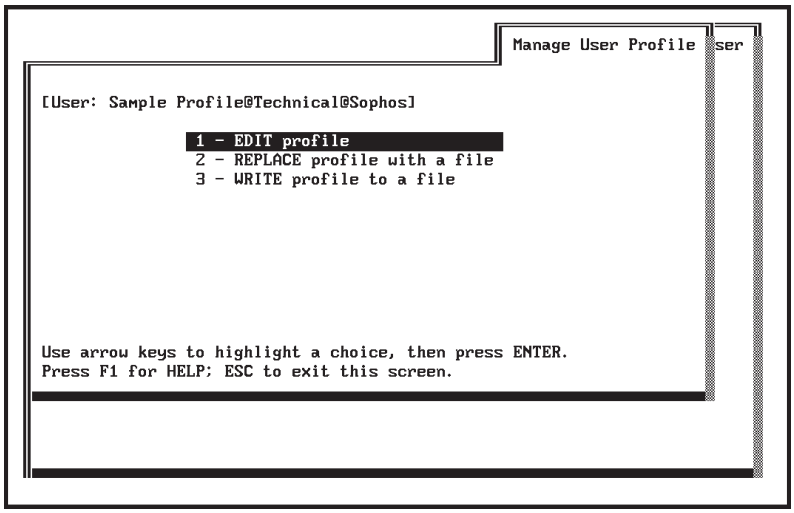
for example

```
MUSER "Sample Profile@Technical@Sophos"
```

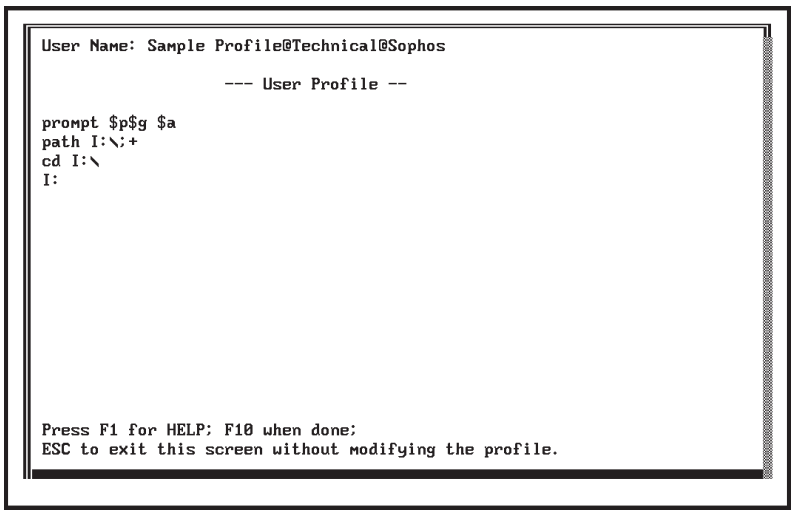
if the profile is 'Sample Profile@Technical@Sophos'. This will display the 'Manage A User' screen for the sample profile. Select *MANAGE user profile*:



Select *EDIT profile* from the 'Manage User Profile' screen:



This will display the sample profile, for example:



Insert a SETDRIVE command to map the InterCheck file service to a DOS drive, if no such mapping already exists. For example, enter

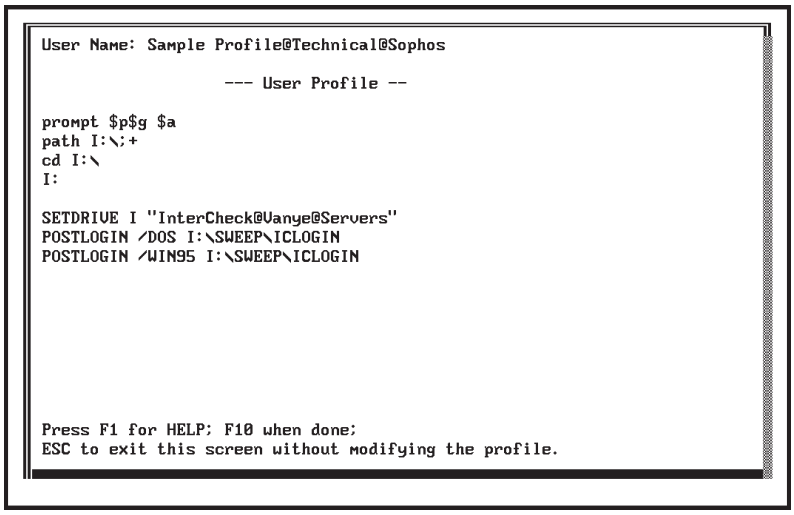
```
SETDRIVE I "InterCheck@Vanye@Servers"
```

to map 'InterCheck@Vanye@Servers' to the DOS drive I:.

After the SETDRIVE command, insert POSTLOGIN commands for both DOS and Windows 95 workstations to run the ICLOGIN program. For example, enter

```
POSTLOGIN /DOS I:\SWEEP\ICLOGIN
POSTLOGIN /WIN95 I:\SWEEP\ICLOGIN
```

if ICLOGIN is to be found in the SWEEP directory on the DOS drive I:



Press *F10* to save the changes, and then press *Esc* until returned to the DOS prompt.

InterCheck will now start on all PCs that use this sample profile when they log in to the network. If there are user profiles which do not use the sample profile, each of them should be updated in the same way as the sample profile.

Without a login script

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

Enter the line

```
SETDRIVE I "InterCheck@Vanye@Server"
```

in the user profile.

Execute the DOS InterCheck executable (INTERCHK.EXE) after the workstation has made a

connection to the network, for example by adding the line

```
I:\SWEEP\INTERCHK
```

to the workstation's AUTOEXEC.BAT file if the InterCheck executables are stored in I:\SWEEP.

Networked InterCheck clients for Windows 95

Windows 95 and Banyan VINES

Windows 95 InterCheck clients cannot use Universal Naming Convention (UNC) drive names if the InterCheck server is running under Banyan VINES. The line

```
UseNetSyntax=No
```

must be added to the InterCheck configuration file for workstations running Windows 95. See the 'Configuring InterCheck clients' chapter.

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*. Then a folder must be selected 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 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 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 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.

Important! A Windows 95 workstation with a stand-alone client may be configured to run InterCheck from the server (for auto-updating purposes) when it is connected to the network. If this is the case, see also 'Windows 95 and Banyan VINES' in the 'Networked InterCheck clients for Windows 95' section above.

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

Run ICLOGIN with the -A option from the user profile. For example

```
SETDRIVE I "InterCheck@Vanye@Servers"
POSTLOGIN /DOS I:\SWEEP\ICLOGIN -A
POSTLOGIN /WIN95 I:\SWEEP\ICLOGIN -A
```

if InterCheck@Vanye@Servers is the file service on the file server that contains 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, the user **may** be able to 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.

Warning! The -U option may not have any effect with a Banyan VINES server because some Banyan VINES clients do not currently support UNC drive names.

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.

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.

Controlling the InterCheck server

This chapter describes how to configure and control SWEEP for DOS, Banyan VINES and OS/2 running as an InterCheck server.

Introduction to ICONTROL

SWEEP running as an InterCheck server provides InterCheck services on any network capable of emulating a logical drive to PCs connected to it.

SWEEP for DOS, Banyan VINES or OS/2 running in InterCheck server mode can be configured and monitored remotely by using ICONTROL for DOS or Windows software. Note that the ICONTROL for DOS program (ICONTROL.EXE) is functionally equivalent to the ICONTROL for Windows program (ICW.EXE).

The ICONTROL programs are copied to the InterCheck server as part of the InterCheck server installation process (see the 'Installing SWEEP as an InterCheck server' section of the 'Installing SWEEP' chapter).

ICONTROL can be run on a remote machine with a drive mapped to the directory on the server containing ICONTROL, or it can be run on the server itself. Write access to the directory ICONTROL is required if any changes to its configuration are to be made.

ICONTROL for DOS

Starting ICONTROL

If the directory D:\SWEEP contains the InterCheck executables, enter at a DOS prompt

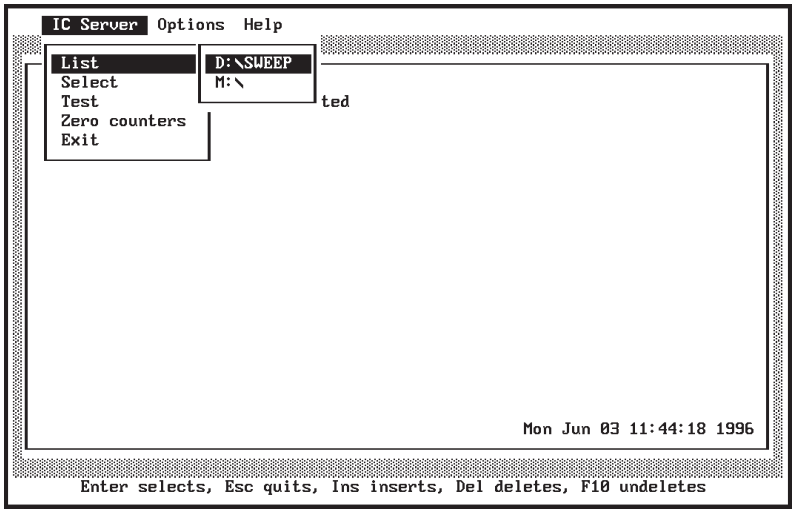
```
D:\SWEEP\ICONTROL
```

to start ICONTROL.

Selecting the InterCheck server

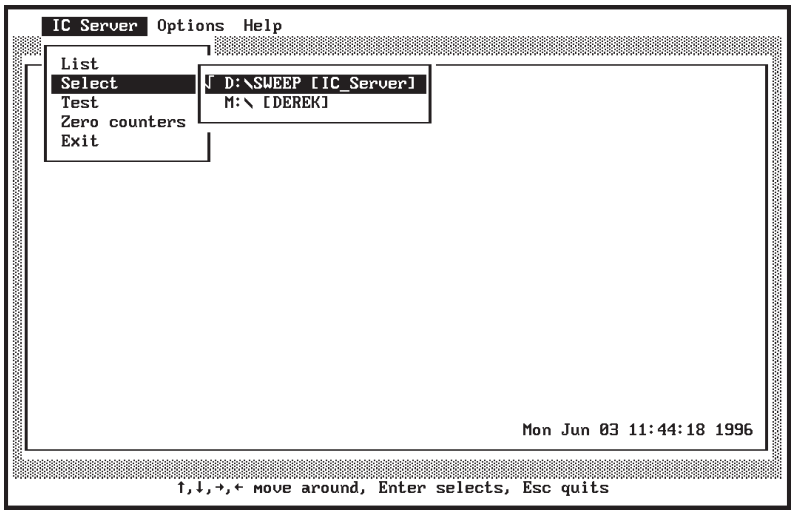
One or more InterCheck server processes can be controlled using ICONTROL under DOS, although only one InterCheck server can be selected and hence monitored at one time.

From the *IC Server* menu select *List* to specify the drive and directory from which SWEEP is running in InterCheck server mode.

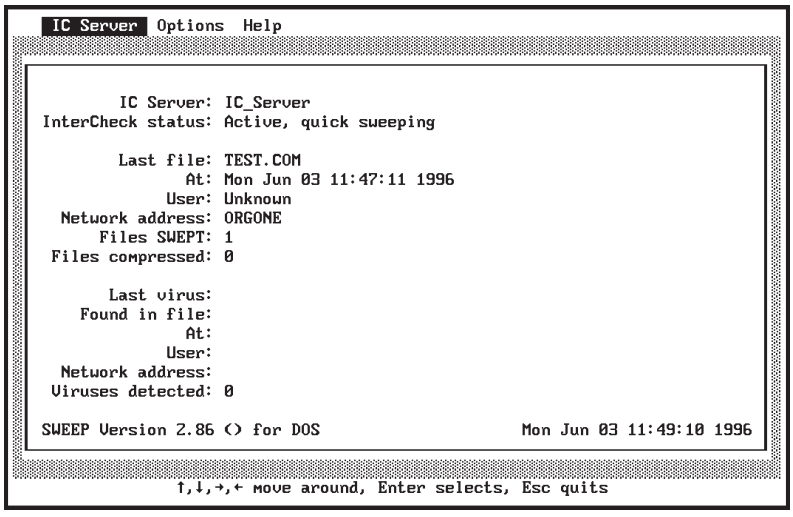


If there is no entry with the correct drive and path, press the *Insert* key and enter the appropriate details, or press *Enter* to edit an existing entry.

The *Select* option from the *IC Server* menu is used to specify the InterCheck server (from the list defined in the *List* option) that is selected for monitoring and controlling.



Assuming that the selected InterCheck server SWEEP is running in InterCheck server mode, and that no menus are 'hanging' off the top bar, ICONTROL will start to monitor SWEEP and update the main ICONTROL display once a server is selected with *Select*.



The main ICONTROL display shows the name of the selected InterCheck server, along with its status (active, inactive or unknown), information about the last file swept, the total number of files swept, the number of compressed files, information about the last virus detected, and the total number of viruses detected.

Testing communications

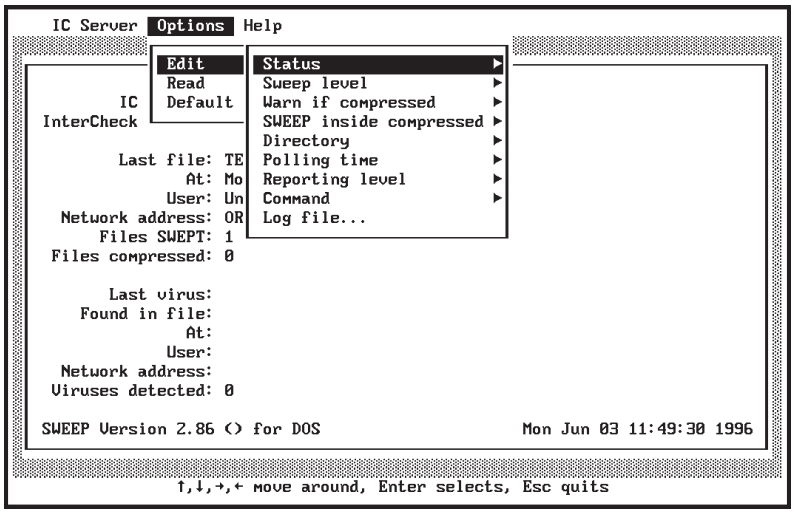
Select *Test* from the *IC Server* menu to test the communication between ICONTROL and the selected InterCheck server. The test server dialog is displayed and updated throughout the process until the outcome is displayed.

The test takes approximately six seconds to complete when the InterCheck server is communicating correctly; otherwise the process will time out after 15 seconds.

Zeroing counters

Select *Zero counters* from the *IC Server* menu to zero the viruses found and files swept counters on the selected InterCheck server.

ICONTROL for DOS options



Edit

Status

The InterCheck server will be able to process requests from InterCheck clients if it is active; otherwise it will not. The server is active by default.

Sweep level

The sweeping level can be set to 'full sweep' or 'quick sweep'. The quick sweep checks only the parts of files likely to contain viruses, while the full sweep examines the full contents of each file. For normal operation quick sweeping is sufficient, and this is the default option.

Warn if compressed

SWEEP does not currently look inside files which have been compressed using static compression utilities such as ARC, ZIP and ZOO. These files will need to be decompressed before sweeping. SWEEP can warn the user if it encounters any of these files, but by default it does not. InterCheck provides automatic protection from viruses in files which have been compressed, because access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been checked for viruses.

SWEEP inside compressed

SWEEP is capable of finding viruses in files which have been compressed using the dynamic compression utilities PKLite, LZEXE and Diet. By default SWEEP will not check inside these compressed files.

Directory

This option allows the location of the INFECTED and COMMS directories on the currently selected InterCheck server to be specified. The COMMS directory is used for communication between InterCheck clients and the server, and the INFECTED directory is used for storing infected items for later analysis.

The locations of these directories are set during the system installation (see 'Installing SWEEP as an InterCheck server' in the 'Installing SWEEP' chapter),

and it is unlikely that they will have to be changed subsequently. Note also that they cannot be changed if a Banyan VINES InterCheck server is being used.

Polling time

The maximum and minimum polling times are the maximum and minimum times the InterCheck server waits between successive searches of the COMMS directory. Increasing the values will tend to reduce server load slightly, but will increase delays experienced by the InterCheck client software. It is recommended that this option is only used if performance problems are encountered.

Reporting level

This controls the level of detail recorded in the continuous SWEEP log file. The options range from None (the least information) to Verbose (the most).

Command

If a DOS or OS/2 InterCheck server is used, a DOS command can be executed when a virus is found, or when the owner of a file has to be determined. Notification can be sent to a user, workstation or group.

The command file may contain other commands at the discretion of the system manager, for example to activate a third party email or paging system to store and forward the notification.

The **'DOS command on virus discovery'** is passed six parameters:

1. Virus name.
2. User name.
3. Time and date of virus discovery.
4. The location of the virus (either a filename or 'Boot_sector').

5. Network Identification Code of the workstation.

6. Name of the server making the report.

Note that all individual parameters have blanks replaced by underscores to allow correct processing by DOS. For example, the 'Dark Avenger' virus would be passed on as 'Dark_Avenger'.

An example of a batch file processing the discovery of a virus might be

```
@ECHO Virus %1 discovered at %3
```

The **'DOS command to get user name'** is passed one parameter in the command line: the full file name.

The appropriate system utility should be used to return the name of the owner of that file, and this name should be written to the file SWEEP.USR in the same directory as the SWEEP InterCheck server.

Note: IBM LAN Server version 3 does not provide a mechanism for obtaining the userid of the file owner.

Log file

This option sets the name and location of the continuous SWEEP log file.

Read

This sets the options to those specified in the InterCheck server configuration file, i.e. it restores them to their last saved values.

Default

This sets the options to their default values.

Command line qualifiers

-BW Display in black and white

Forces display for a black and white monitor.

-CFG=<file> Name of configuration file

The default ICONTROL configuration file is called SWEEPIC.INI and is stored in the same directory as ICONTROL. A different path and name can be specified with the -CFG option.

-CO Colour monitor

Forces display for a colour monitor.

-MO Monochrome monitor

Forces display for a monochrome monitor.

-P.. Path through menus

This qualifier can be used to pre-define the selection of menu options. 0 selects the 1st option, 1 the 2nd option etc. '^' is equivalent to the user pressing *Esc* while '?' allows the user to make a selection. In the example

```
ICONTROL -P120^04
```

1 Selects *Options* menu.

2 Selects *Default*.

0 Enters *OK* on 'Initialise options to default values?' dialog.

^ Escapes to the top menu bar.

0 Selects *IC Server* menu.

4 Selects *Exit* to exit from ICONTROL.

ICONTROL for Windows

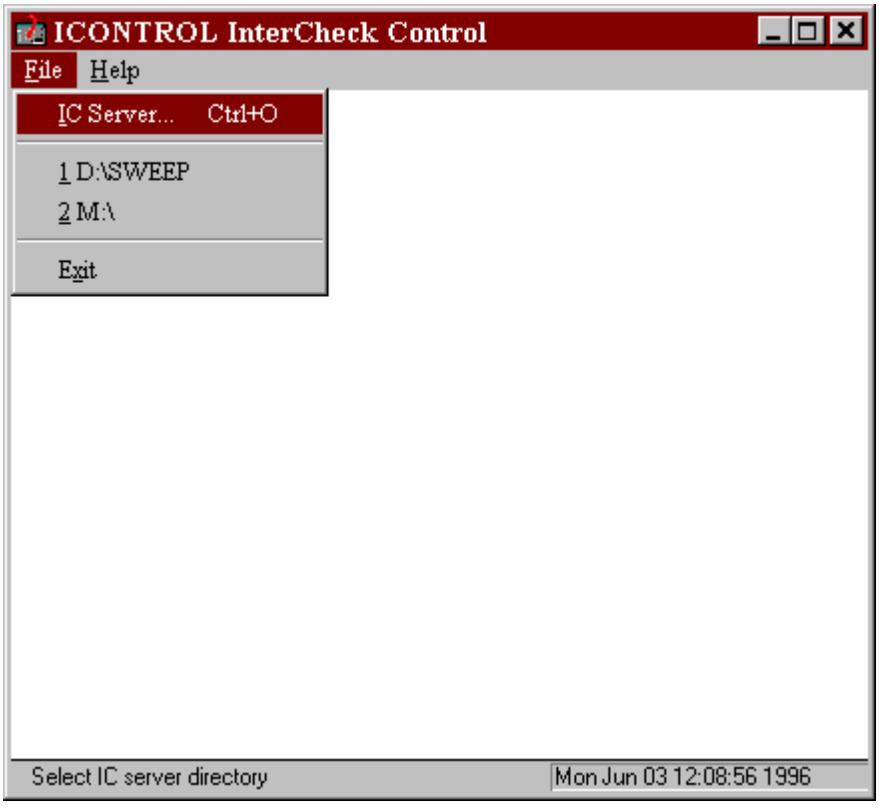
Starting ICONTROL

Use File Manager or Explorer to locate the InterCheck files on the network. Start ICONTROL by double clicking on ICW.EXE.

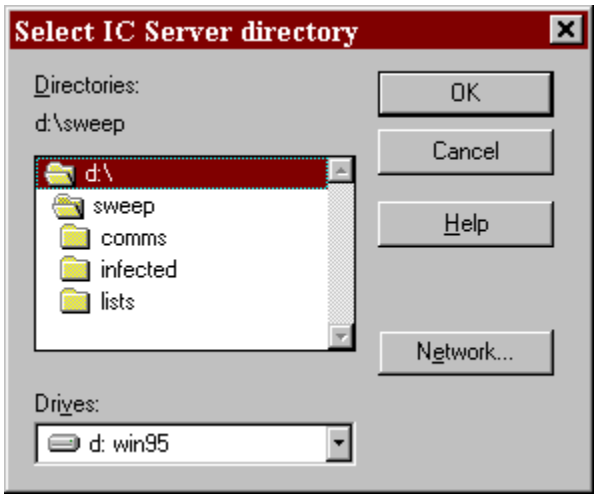
Note that ICW.EXE can be placed in, and launched from, a Windows 3.x Program Group or the Windows 95 Taskbar in the same way as any other Windows executable.

Selecting the InterCheck server

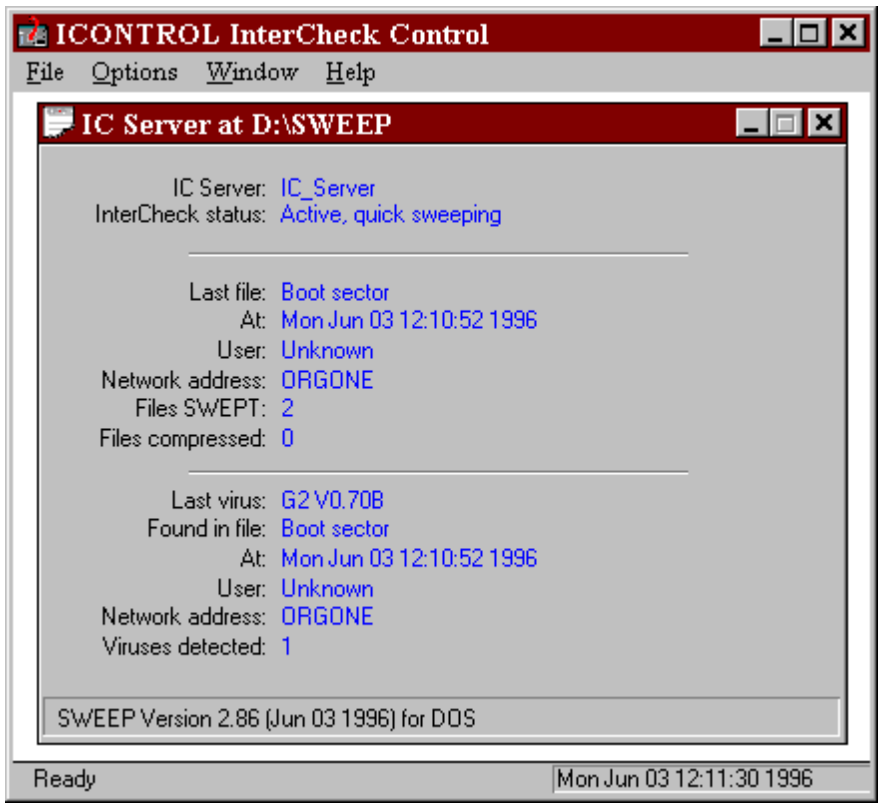
Choose *IC Server* from the *File* menu



and select an InterCheck server working directory



When the directory is specified ICONTROL will display the current status of the InterCheck server that is running at that location, for example:



Other InterCheck servers can be monitored by selecting them via the *File* menu. Unlike ICONTROL

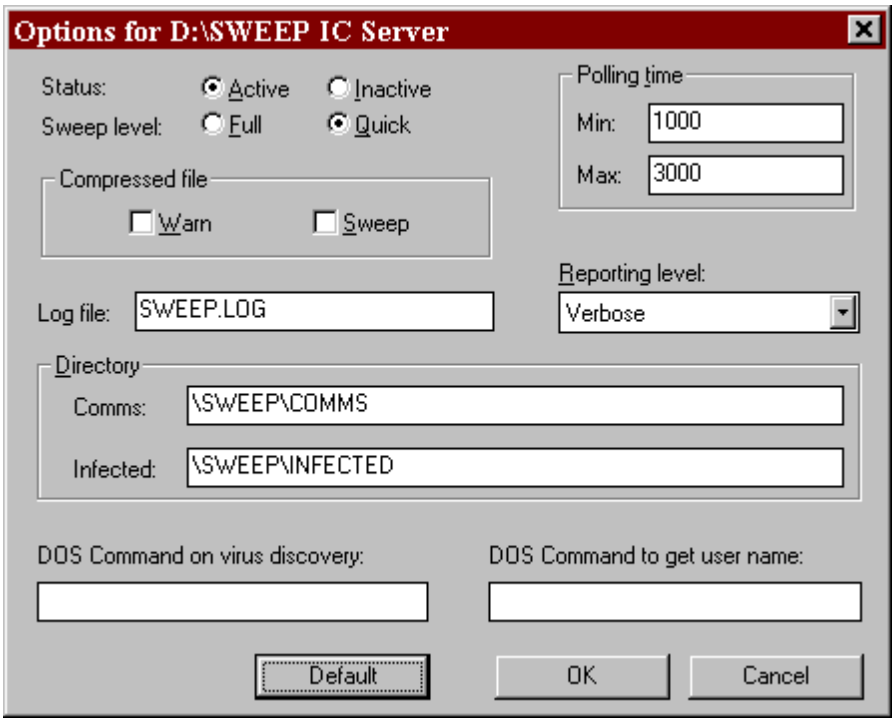
for DOS, ICONTROL for Windows can monitor multiple servers at the same time.

ICONTROL for Windows options

The following options will operate on the InterCheck server whose status window is currently activated/selected.

Edit server settings

You can set parameters such as the minimum and maximum polling times, reporting levels etc. in SWEEP by selecting *Edit server settings* from the *Options* menu:



These parameters are equivalent to those set from the *Options* menu of the DOS ICONTROL (see the 'ICONTROL for DOS options' section above).

Test server

See the 'Testing communications' sub-section of 'ICONTROL for DOS'.

Zero counters

See the 'Zeroing counters' sub-section of 'ICONTROL for DOS'.

Starting a SWEEP InterCheck server automatically

SWEEP can be started as an InterCheck server automatically by ICONTROL for Windows under Windows 3.1, Windows for Workgroups and Windows 95. This is not available in OS/2.

ICONTROL will load SWEEP.EXE as an InterCheck server in hidden mode if the ICW.INI file (stored in the WINDOWS or WIN95 directory) contains an entry such as the following under the [Application Settings] section:

```
ICServer=D:\SWEEP\SWEEP.EXE, -ICS=ServerName, D:\SWEEP
```

All three parameters must be stated. The first parameter specifies the SWEEP executable which will be run in server mode, the second specifies the command line qualifier SWEEP.EXE needs to start in InterCheck server mode, and the third specifies the working InterCheck server path.

The directory from which SWEEP is run in InterCheck server mode must contain a SWEEPIC.INI file and must not contain a file called SWEEPIC.RES. SWEEPIC.INI will ensure that the InterCheck server can be run, while the absence of SWEEPIC.RES means that there are no InterCheck servers already running in that directory.

The InterCheck server loading time is almost the same as the time for which the ICONTROL introductory dialog is displayed. Shortly after this

dialog closes the resident InterCheck server status should be displayed.

Under OS/2 the auto InterCheck server launch will be ignored (even with the ICW.INI ICServer entry supplied).

ICONTROL should not be forced to run a resident InterCheck server with a working directory on a remote workstation, for example:

```
[Application Settings]
ICServer=D:\SWEEP\SWEEP.EXE, -ICS=ServerName, Q:\SWEEP
```

where Q: is a drive on a networked workstation and D: local hard disk. This is because the InterCheck server run on a local machine might have difficulty reading from and writing to its working directory on the remote PC.

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 are checked locally 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 SWEEP.

Dealing with viruses

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

Viruses on the Banyan VINES server

If a virus is found on the file server, see 'Eliminating viruses on the Banyan VINES 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 Banyan VINES server

The names of any infected items will be placed in the system event log.

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

Files with macro viruses

SWEEP can automatically disinfect files infected by macro viruses. To enable this facility, add DisinfectDocuments=YES to the SWEEP Service Configuration Record (see the 'Configuring SWEEP' section of the 'Using SWEEP' chapter).

Note that if SWEEP does not have write access to the file, it will issue a warning, and the file should then be disinfected with SWEEP for DOS (see the SWEEP for DOS user manual).

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 by accessing UNIX via the system console and using the RM commands. Consult your Banyan VINES manual for details. The executables should be restored from the originals or from sound backups.

Infected disks

On Banyan VINES 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 SWEEP for Banyan VINES.

Server instability, crashing, unreliability

This is often a result of the server running out of swap space. Information on ascertaining and increasing swap space usage can be found in the Banyan manual *Monitoring and Optimizing Servers*. SWEEP uses under 3Mb of virtual memory, so adding this amount should be sufficient. It is best to have more swap space than needed to avoid server unreliability.

SWEEP refuses to start, or dies quickly

Check that the BaseDirectory configuration parameter is set correctly. The SWEEP service should be a member of the server's AdminList, and of the Admin List(s) of any StreetTalk group(s) containing file services which are to be swept.

Check also that SWEEP has sufficient rights in the ARLs of its BaseDirectory, all the parent directories of it including the root, and all the subdirectories. Ensure that the service has sufficient rights to create and delete files in the COMMS directory. For details, see 'Setting the SWEEP access rights' in the 'Installing SWEEP as an InterCheck server' section of the 'Installing SWEEP' chapter.

SWEEP appears to hang

Ensure that versions 6.00 or 6.00(10) of Banyan VINES are not running. SWEEP for Banyan VINES cannot function under these revisions due to VINES bugs. Instead use VINES 6.00(10) with site specific patch 95008, or VINES 6.20(0).

InterCheck fails to run from POSTLOGIN

There may not be enough free base memory to run InterCheck in that environment. If INTERCHK.EXE works from a command line but ICLOGIN does not work from POSTLOGIN, the user may wish to run InterCheck from the AUTOEXEC.BAT (for DOS, Windows 3.x, or Windows for Workgroups) or from the Startup folder (for Windows 95). See the 'Installing InterCheck clients' chapter for more information.

SWEEP runs slowly

Full sweep

By default, SWEEP will perform a 'quick sweep' which checks only the parts of files which are likely to contain a virus. However, if a 'full sweep' is set SWEEP will be much slower. The speed difference between full sweep and quick sweep depends on the configuration of your machine, but typically the quick level is 5 to 10 times faster than the full.

Full sweep may be selected for InterCheck using the ICONTROL utility. For scheduled sweeping, it is selected by changing the 'ScheduledSweepLevel=' configuration parameter to FULL instead of QUICK.

Insufficient server memory

VINES implements virtual memory, whereby areas of the disk may be used to extend memory. However, physical memory should be sufficiently large to hold

all frequently used data, with only infrequently used data on disk. If it is not large enough, the server and all services on it, including SWEEP, will experience degraded performance.

The *Monitoring and Optimizing Servers* manual from Banyan describes how to get statistics on server performance. If insufficient server memory is a problem, either fit more memory or relocate some services to another server.

False positives

SWEEP 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 in doubt, contact Sophos' technical support.

To decrease the chance of false positives:

- Only sweep executables.
- Perform a 'quick sweep' rather than a 'full sweep'.

New viruses

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

If a virus unknown to SWEEP is suspected, please send Sophos a sample and a description as soon as possible. If it is a virus, SWEEP 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 SWEEP. 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 SWEEP and InterCheck version, operating system and patch level, and the exact text of any error messages.

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.

BIOS: The Basic Input/Output System of MS-DOS which constitutes the lowest level of software which interfaces directly with the hardware of the microcomputer.

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 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.

Compressed File: See File Compression.

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.

False Negative: An existent event reported as non-existent, e.g. the absence of a virus when the virus is present.

False Positive: A non-existent event reported as existent, e.g. the presence of a virus when no virus is present.

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.

File Compression: The compacting of a file through the process of recoding its bit structure into a shorter form. File compression must be reversible.

Hexadecimal: A system of counting using number base 16. The numbers 10 to 15 are represented by the characters 'A' through 'F' respectively. Hexadecimal is often

	abbreviated to Hex. Each Hex digit is equivalent to four bits (half a byte) of information.
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.
IP Address:	A numeric Internet address; a 32-bit binary number, normally written in dotted-decimal notation; e.g. '194.82.145.1'.
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 sold by Microsoft. It is the most common microcomputer operating system in the world, and operates on the IBM PC.
Multipartite Virus:	A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

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.

Partition Table: A 64-bit table found inside the master boot sector on hard disks which contains information about the starting and ending of up to four partitions on the hard disk. The partition table also contains information on the type of the partition, e.g. DOS partition, UNIX partition etc.

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.

UNIX: UNIX is a multi-user operating system, developed by AT&T. Several versions of UNIX exist, which do not all achieve compatibility with each other.

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

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).

Virus Pattern: A sequence of bytes extracted from a virus and used for virus recognition.

WAN: Wide Area Network; a set of computers that communicate with each other over long distances.

Index

H

I

L

V

W

X

Z

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 7115878 · Fax 02 7115894 · 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/