Sophos Anti-Virus

Quick Start Guide

Novell NetWare

SOPHOS

Introducing Sophos Anti-Virus

Sophos Anti-Virus provides complete protection against all viruses known to Sophos, for individual PCs and entire networks.

This guide introduces its key features and shows how to install and use it across a Novell NetWare 4 network. Notes are provided for NetWare 3 users*.

How the software works

Sophos Anti-Virus includes two systems:

- **SWEEP** provides immediate and scheduled scanning of all server volumes, and
- **InterCheck** checks each item as you try to access it, and grants access only if it is virus-free.

InterCheck splits on-access scanning between an **InterCheck client**, which identifies items that have not yet been scanned, and an **InterCheck server** (using SWEEP), which scans them. Thus items are scanned only once, minimising overhead.

Sophos Anti-Virus on a network

If using Sophos Anti-Virus on a network, you can:

Automatically update workstations.

Set up **central reporting** of virus incidents.

Install InterCheck in the way that makes best use of network resources. On workstations, use networked InterCheck clients (which send files to the file server for scanning) to minimise workstation overhead, or stand-alone InterCheck clients (which scan files on the workstation itself) to achieve quicker scanning and save network resources.

*** See the main *Sophos Anti-Virus for NetWare* manual for a complete description of product features.**

Starting off with Sophos Anti-Virus

What you will need for installation

To install Sophos Anti-Virus for NetWare, you will need:

- NetWare 3.11 or later.
- At least 4 Mb of available RAM.
- At least 10 Mb of free hard disk space.

The server should be patched to the baseline recommended by Novell.

The two main steps

This guide shows you how to install Sophos Anti-Virus in two steps:

1. **Install and run SWEEP on the server.**

   In this step, you load and run SWEEP on your server. You can then scan server volumes on demand, test SWEEP, and set up virus reporting and disinfection. Pages 3-10 describe this.

2. **Install InterCheck on-access scanning for connected workstations.**

   In this step, you install the InterCheck client software, either on the server or on the workstations. This enables workstations to use on-access scanning. Pages 11-15 describe this.

You can install Sophos Anti-Virus for NetWare throughout the network (on both server and workstations) from a single workstation.

Installing SWEEP on the server

You install SWEEP on your NetWare server **from a workstation**.

Before installing SWEEP

For more information about ‘clean booting’ and about creating a clean system disk, see the main *Sophos Anti-Virus for NetWare* manual.

Before you begin, you **must** boot the workstation from a virus-free system disk. This is to ensure that there are no viruses in memory that could infect the file server while you are installing SWEEP.

Switch the workstation off.

Insert a clean, write-protected system disk. This should also contain the appropriate NetWare client software and LOGIN programs.

Switch the workstation on and wait for a prompt.

Installing SWEEP

At the workstation, log in as a user with administrator privileges and insert the Sophos Anti-Virus CD into the CD drive.

Copy SWEEP.NLM from the CD drive (e.g. D:) into the system directory of the server, normally F:\SYSTEM, as follows:

```
COPY D:\NETWARE\SWEEP.NLM F:\SYSTEM
```

At the server console, or using RCONSOLE from a workstation, enter:

```
LOAD SWEEP -DS
```

NetWare 3.x users do not need to use -DS, which enables support for NetWare Directory Services.

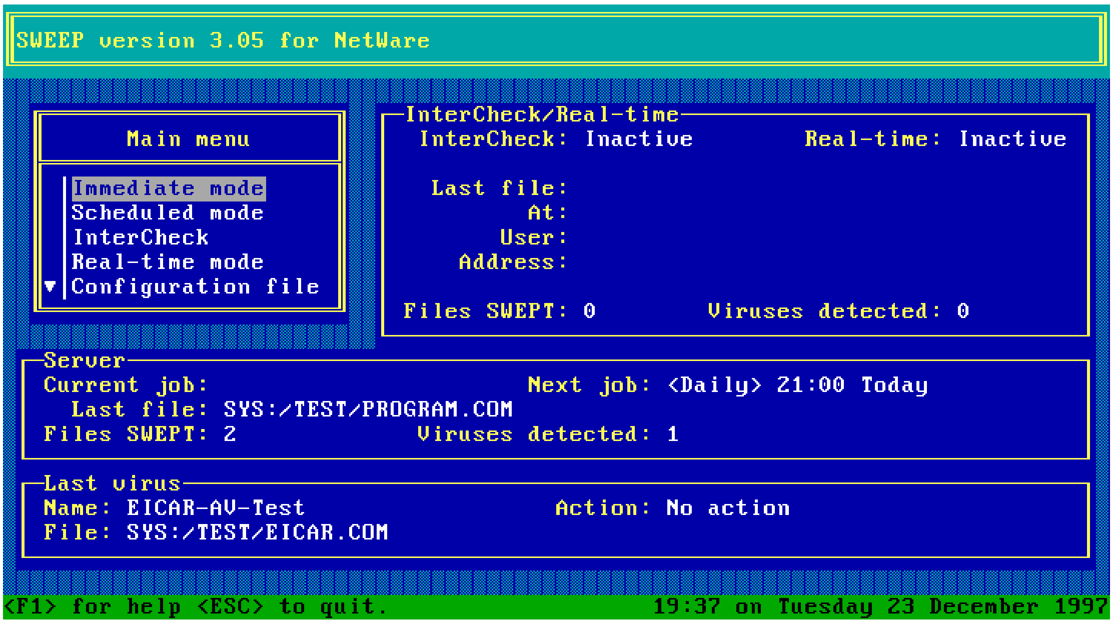
SWEEP will load and run. This may take a few seconds. Then the main SWEEP screen will appear (see next section).

Scanning the server

When you load SWEEP on to the server, the main screen is displayed. You can now run immediate or scheduled scans of the server.

Starting an immediate scan

To scan the server now:



```
SWEEP version 3.05 for NetWare

     Main menu            InterCheck/Real-time
                           InterCheck: Inactive        Real-time: Inactive
  Immediate mode
  Scheduled mode            Last file:
  InterCheck                       At:
  Real-time mode                 User:
 ▼Configuration file           Address:

                          Files SWEPT: 0        Viruses detected: 0
Server
Current job:                         Next job: <Daily> 21:00 Today
  Last file: SYS:/TEST/PROGRAM.COM
Files SWEPT: 2               Viruses detected: 1
Last virus
Name: EICAR-AV-Test                    Action: No action
File: SYS:/TEST/EICAR.COM
<F1> for help <ESC> to quit.              19:37 on Tuesday 23 December 1997
```

Select **Immediate mode** from the **Main menu** and press **Enter**. Then select **Start** and press **Enter**.

Stop the scan by selecting Stop | Enter.

As SWEEP runs, the screen displays information about scanning activity in two windows:

Server

This shows the current job, the next scheduled job, and details of the last file scanned.

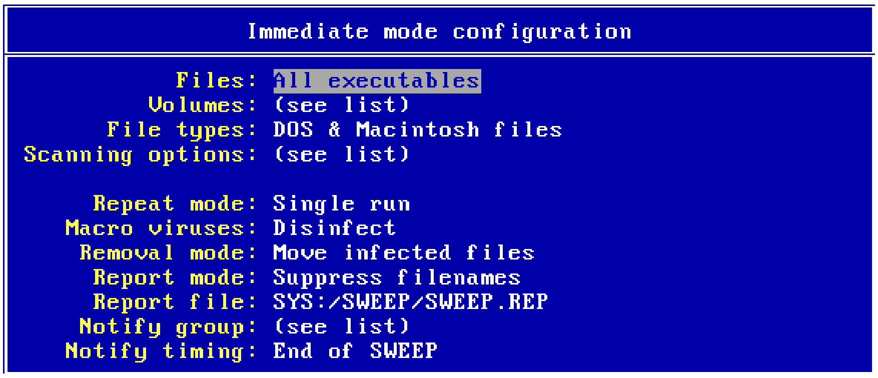
Last virus

This shows the name and location of the last virus discovered, along with the action taken.

Changing the immediate scanning options

You can specify which files SWEEP scans and also configure virus notification and disinfection activity.

To do this, select **Immediate mode** on the **Main menu**, then **Configuration** and press **Enter**. The **Immediate mode configuration** menu is displayed:



```
                Immediate mode configuration

         Files: All executables
       Volumes: (see list)
    File types: DOS & Macintosh files
Scanning options: (see list)

    Repeat mode: Single run
  Macro viruses: Disinfect
   Removal mode: Move infected files
    Report mode: Suppress filenames
    Report file: SYS:/SWEEP/SWEEP.REP
   Notify group: (see list)
  Notify timing: End of SWEEP
```

Here are some options you are likely to use. Full details are in the main *Sophos Anti-Virus for NetWare* manual.

To see which files are defined as executables, select Administration | View/Modify from the Main menu.

Files Choose to scan all executables, all files or specified files only.

Volumes Choose which volumes to scan.

Scanning options Choose a quick scan (checking areas of a file where a virus is likely to be) or full scan.

If you disinfect macro viruses, remember that the original file, although now virus-free, may nevertheless be corrupted.

Macro viruses Choose whether to disinfect macro viruses.

Removal mode Choose to rename, move, delete or purge infected files.

Notify group The name of the user group to whom virus messages should be broadcast.

Scheduled scanning of the server

By default, SWEEP for NetWare carries out a virus check at 21:00 every day.

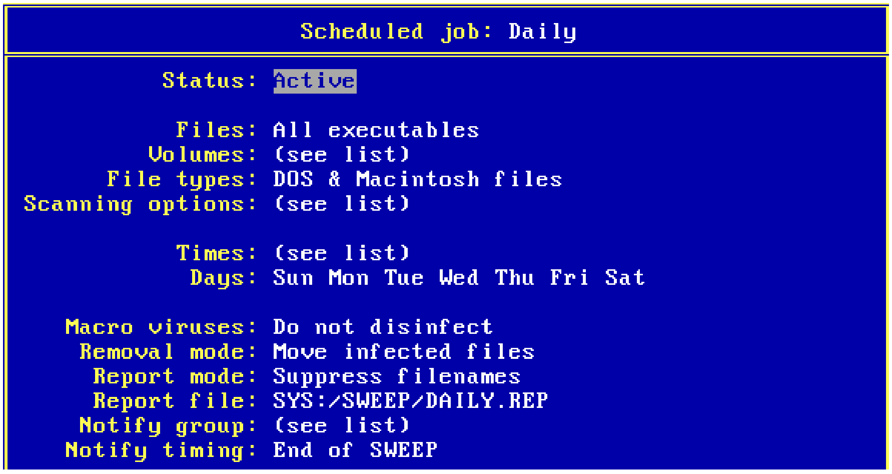
You can add further scheduled scans as described below.

Changing the scheduled scanning options

To view or change the Scheduled mode options, select **Scheduled mode** on the **Main menu** and press **Enter**.

Stop the scan by selecting Immediate mode | Stop | Enter.

To add a new job, press **Insert** and type in the name of the job. To add configuration options for this job or to amend options for existing jobs, select the job name and press **Enter**. The **Scheduled job** menu appears:



```
                 Scheduled job: Daily

          Status: Active

           Files: All executables
         Volumes: (see list)
      File types: DOS & Macintosh files
Scanning options: (see list)

           Times: (see list)
            Days: Sun Mon Tue Wed Thu Fri Sat

   Macro viruses: Do not disinfect
    Removal mode: Move infected files
     Report mode: Suppress filenames
     Report file: SYS:/SWEEP/DAILY.REP
    Notify group: (see list)
   Notify timing: End of SWEEP
```

The options available are similar to those for Immediate mode, but with three extra parameters:

Status Whether the job is Active (if it is not, it will be in the list of scheduled jobs but will not be run).

Times The time(s) you want the job to run.

Days The day(s) you want the job to run.

What happens if SWEEP finds a virus?

This section shows you how SWEEP reports viruses and how to test SWEEP's virus checking.

When SWEEP finds a virus it generates reports in:

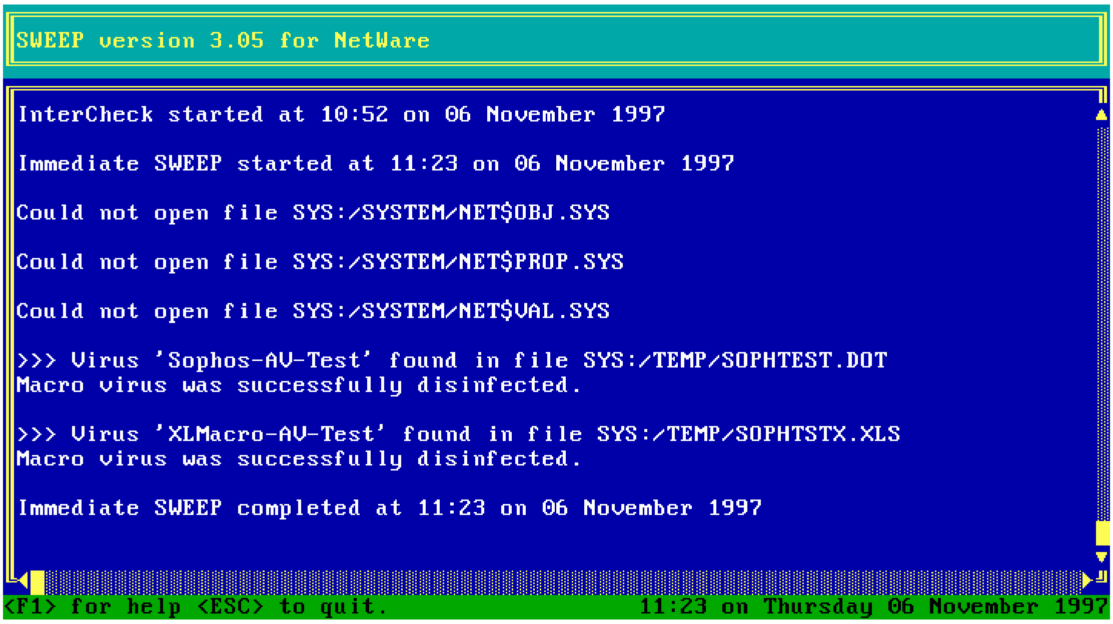
The report file

SWEEP generates separate report files for immediate scans and scheduled scans. Each file is replaced when SWEEP runs the job again. By default, the file for immediate scans is called SWEEP.REP. The file for scheduled scans is given the name of the scheduled job, with a .REP extension. You can view the report from a workstation with any text editor.

To change the maximum size of the log file, select Administration | Log file | Maximum size.

The log file

This holds a complete history of virus incidents, along with details of every scan run:



```
SWEEP version 3.05 for NetWare

InterCheck started at 10:52 on 06 November 1997

Immediate SWEEP started at 11:23 on 06 November 1997

Could not open file SYS:/SYSTEM/NET$OBJ.SYS

Could not open file SYS:/SYSTEM/NET$PROP.SYS

Could not open file SYS:/SYSTEM/NET$VAL.SYS

>>> Virus 'Sophos-AV-Test' found in file SYS:/TEMP/SOPHTEST.DOT
Macro virus was successfully disinfected.

>>> Virus 'XLMacro-AV-Test' found in file SYS:/TEMP/SOPHTSTX.XLS
Macro virus was successfully disinfected.

Immediate SWEEP completed at 11:23 on 06 November 1997

<F1> for help <ESC> to quit.                  11:23 on Thursday 06 November 1997
```

To view the log file, at the main menu select **Administration**, then **Log file** and then **View**.

Testing SWEEP

You may want to test SWEEP's virus checking.

At a workstation, use a text editor, such as EDIT, to create a new file containing the test string:

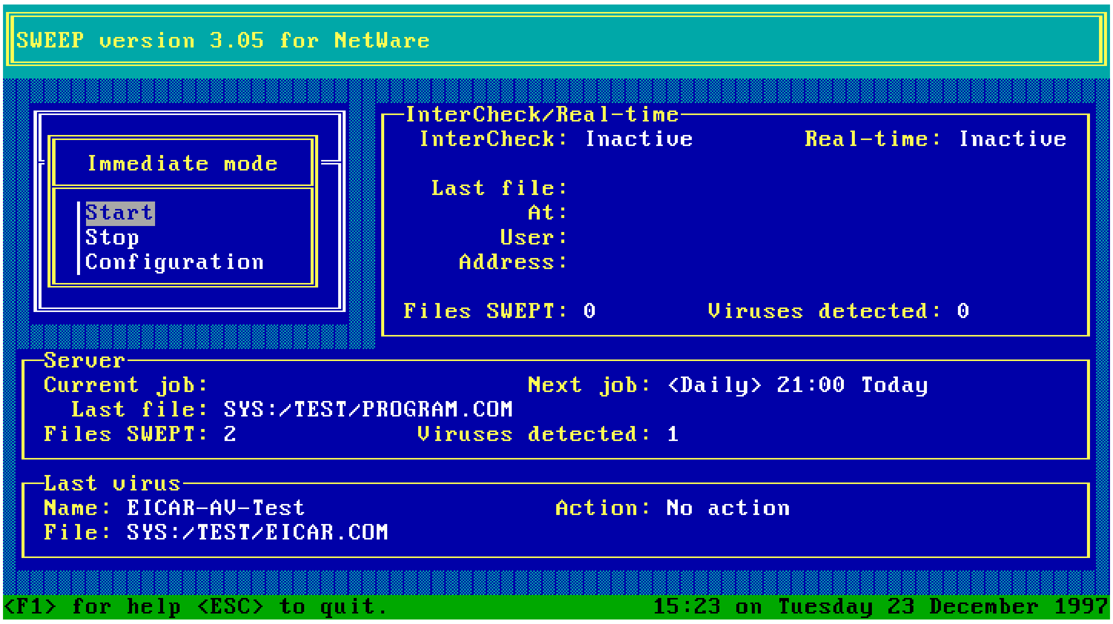
```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

When typing in the test string, ensure that you use a capital O after X5, not a zero.

and save the file as EICAR.COM. Then copy it to a server volume.

Now run an immediate scan on the server. To save time, go to the **Immediate mode configuration** menu, select **Files** and specify the directory in which you have placed EICAR.COM, or even just EICAR.COM.

SWEEP should report a virus found, as below:



```
SWEEP version 3.05 for NetWare

                           InterCheck/Real-time
  Immediate mode            InterCheck: Inactive        Real-time: Inactive

  Start                      Last file:
  Stop                              At:
  Configuration                   User:
                               Address:

                           Files SWEPT: 0          Viruses detected: 0
 Server
 Current job:                          Next job: <Daily> 21:00 Today
   Last file: SYS:/TEST/PROGRAM.COM
 Files SWEPT: 2               Viruses detected: 1
 Last virus
 Name: EICAR-AV-Test                     Action: No action
 File: SYS:/TEST/EICAR.COM
<F1> for help <ESC> to quit.                  15:23 on Tuesday 23 December 1997
```

Setting up messaging

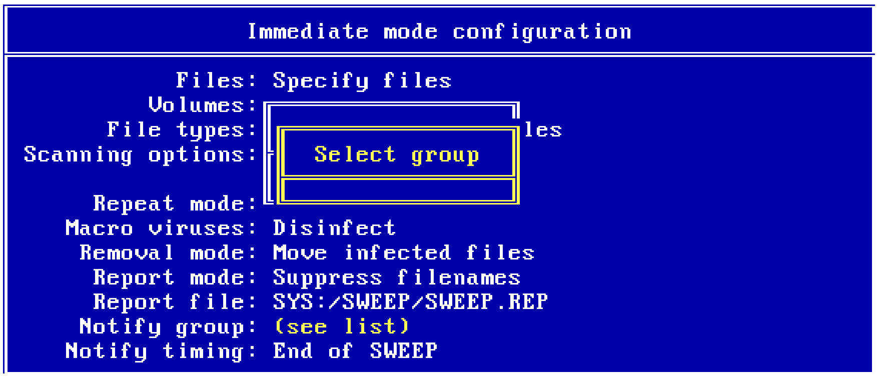
You can configure SWEEP to notify user groups (e.g. CN=VIRALERT.O=SOPHOS) if any virus is detected. Use the Notify Group option to specify the group(s) for each of the following:

You can specify up to 16 notification groups for each option.

- Immediate scan.
- Each separate scheduled scan.
- InterCheck.
- Real-time.

For example, to specify the group that will receive a message if an immediate scan finds a virus, go to the main menu. Select **Immediate mode**, then **Configuration** and then **Notify Group**.

A list of Active groups is displayed. To add a further group, press **Insert** and select the group from the displayed list.



```
                 Immediate mode configuration

             Files: Specify files
           Volumes:
        File types:                  les
  Scanning options:    Select group

       Repeat mode:
     Macro viruses: Disinfect
      Removal mode: Move infected files
       Report mode: Suppress filenames
       Report file: SYS:/SWEEP/SWEEP.REP
      Notify group: (see list)
     Notify timing: End of SWEEP
```

Using SWEEP's virus library

SWEEP for NetWare contains a library of the names of all viruses known to SWEEP.

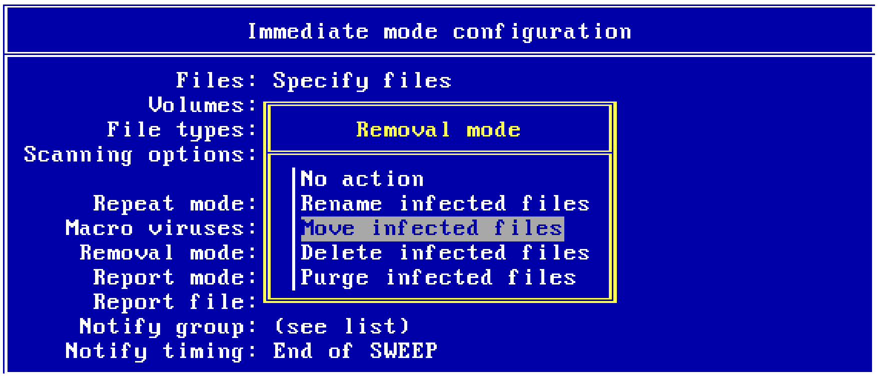
To view the library, at the Main menu select **Administration** and then **Virus library**. Then use keystrokes to scroll through the alphabetical list of virus names.

Specifying virus recovery actions

You can specify separate actions to be taken if a virus is found during immediate, scheduled, InterCheck and Real-time scans.

For example, to specify action after an immediate scan has detected a virus, on the main screen select **Immediate mode** and then **Configuration**.

To specify what action to take, select **Removal mode**.

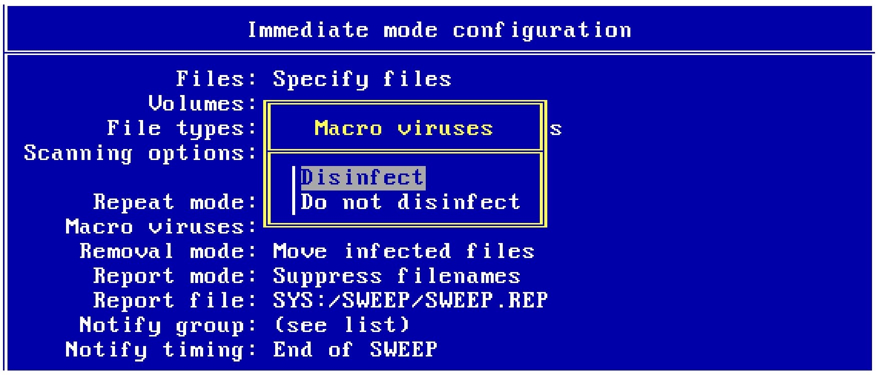


```
                  Immediate mode configuration

             Files: Specify files
           Volumes:
        File types:   Removal mode
  Scanning options:
                     No action
       Repeat mode:  Rename infected files
    Macro viruses:   Move infected files
     Removal mode:   Delete infected files
      Report mode:   Purge infected files
      Report file:
     Notify group: (see list)
    Notify timing: End of SWEEP
```

By default, infected files are moved to the server SWEEP\INFECTED subdirectory.

For files infected with **Macro viruses**, you can specify disinfection instead of removal. Select **Macro viruses**.



```
                  Immediate mode configuration

             Files: Specify files
           Volumes:
        File types:   Macro viruses    s
  Scanning options:
                     Disinfect
       Repeat mode:  Do not disinfect
    Macro viruses:
     Removal mode: Move infected files
      Report mode: Suppress filenames
      Report file: SYS:/SWEEP/SWEEP.REP
     Notify group: (see list)
    Notify timing: End of SWEEP
```

If **Disinfect** is selected, and if disinfection is successful, these files are not removed. Otherwise, the removal mode is applied to these files.

Installing InterCheck for workstations

You can also install InterCheck on-access scanning for workstations on the network, as described below.

This actively prevents viruses from infecting your system by denying users access to any infected file.

If there are any workstations on your network not protected by InterCheck, you should consider using SWEEP's Real-time mode. See page 15.

An overview of InterCheck installation

There are two ways to give workstations access to on-access scanning:

Install a networked InterCheck client.
This sends files over the network to an InterCheck server (running on your server) for scanning. It is easy to install on large networks and suitable for workstations with limited system resources.

For installation instructions, read 'Before installing InterCheck clients' and then 'Installing networked InterCheck clients'.

Install a stand-alone InterCheck client.
This sends files to a local copy of SWEEP for checking. It reduces network traffic, offers faster initial authorisation of files, and is suitable for workstations not always connected to the network.

For installation instructions, read 'Before installing InterCheck clients' and then 'Installing stand-alone InterCheck clients'.

Before installing InterCheck clients

Before installing InterCheck clients, you must run the ICINSTAL program, which sets up the InterCheck client software on your server.

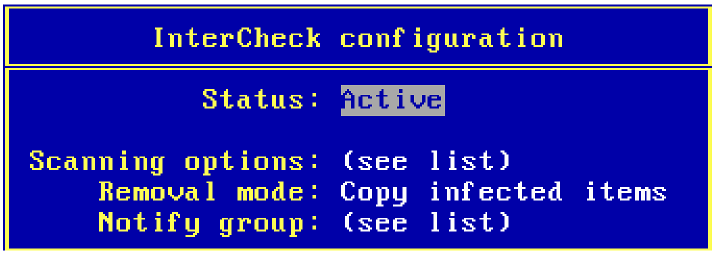
At a workstation, log in as a user with Adminstrator status. Insert the Sophos Anti-Virus CD and type:

```
D:INTERCHK\ICINSTAL
```

if D: is the drive containing the CD. At the setup screen, select **Onto file server** from the **Install** menu and follow the instructions.

At the server console, or using RCONSOLE from a workstation, switch to the SWEEP screen.

At SWEEP's main menu, select **InterCheck**, press **Enter** to display the InterCheck configuration menu, and set **Status** to **Active**:



```
              InterCheck configuration

                 Status: Active

 Scanning options: (see list)
      Removal mode: Copy infected items
      Notify group: (see list)
```

Installing networked InterCheck clients

First, ensure that you have followed the steps in 'Before installing InterCheck clients'.

If using Windows for Workgroups or Macintosh workstations, consult the special instructions in the main *Sophos Anti-Virus for NetWare* manual.

If you are installing InterCheck clients on a large network, it is a good idea to create a group of users who will run InterCheck and to add new members gradually. This makes troubleshooting and dealing with users' queries easier. These instructions assume that you create a group called INTERCHECK.

Installing networked InterCheck clients (continued)

DOS, Windows 3.x and Windows 95 workstations

At a workstation, edit the login script of the appropriate Organisation or Organisational Unit (or the system login script for NetWare 3.x) to include:

NetWare 3.x users do not need the NOSWAP line.

```
MAP INS S1:=SYS:\SWEEP
IF MEMBER OF "INTERCHECK" THEN BEGIN
NOSWAP
#ICLOGIN
END
```

InterCheck will now run on workstations as they log in to the network. This takes a few minutes the first time but only a few seconds on future logins.

Testing InterCheck functioning

Now check that InterCheck is sending files to the server for checking as it should.

Use a text editor, e.g. EDIT under DOS or Notepad under Windows, to create a file with a .SYS extension. Enter a few characters and exit, saving the file.

InterCheck will interpret this as a newly-created executable file and send it to the server for checking. An InterCheck box appears to show this happening.

Monitoring InterCheck activity

The InterCheck/Real-time window on the main SWEEP for NetWare screen shows:

- Whether InterCheck is active.
- The last item scanned.
- The number of viruses detected.

Installing stand-alone InterCheck clients

The workstation must be connected to the network during installation of a stand-alone client.

First, ensure that you have followed the steps in ‘Before installing InterCheck clients’.

If using stand-alone DOS clients, ensure that workstations log in to the network when possible. This will ensure that the local copy of InterCheck is updated when the central version is updated.

DOS/Windows 3.x workstations

Ensure that the directory on the server where you placed the InterCheck client software is mapped to a DOS drive. At a DOS prompt on the workstation, change to that drive and enter

```
ICINSTAL
```

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

If using Windows for Workgroups workstations, consult the main *Sophos Anti-Virus for NetWare* manual.

Windows 95 and Windows NT workstations

On these workstations, an InterCheck client can be installed during SWEEP installation.

For Windows 95, select **InterCheck for Windows 95** at the **Installation type** setup screen.

For Windows NT, select **Enable InterCheck Client** at the **InterCheck Support and Network Access** screen.

Testing and monitoring InterCheck

To test InterCheck, **at a workstation**, use a text editor, such as NOTEPAD, to create a new file, enter the EICAR test string, as described in ‘Testing SWEEP’, and save the file as EICAR.COM. This will be intercepted by InterCheck and reported as a virus.

The InterCheck/Real-time window gives a summary of InterCheck activity (see previous page).

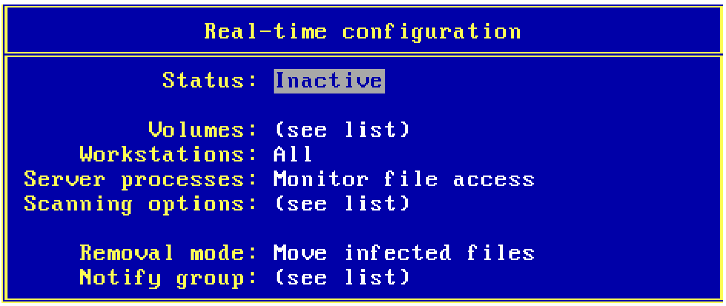
Using Real-time mode

You do not need to use SWEEP's Real-time mode unless there are workstations on your network not protected by InterCheck.

Real-time mode ensures that only virus-free files are written to the server, even if there are unprotected workstations on the network. It will check all files that are sent to the server. Thus, if a workstation without InterCheck accesses an infected file, it cannot transmit the infection across the network.

To activate Real-time mode, select **Active** from the **Real-time** menu on the InterCheck/Real-time window.

Real-time mode can also be configured from the **Real-time configuration** window:



```
                 Real-time configuration

            Status: Inactive

           Volumes: (see list)
      Workstations: All
  Server processes: Monitor file access
  Scanning options: (see list)

      Removal mode: Move infected files
      Notify group: (see list)
```

You can opt to use Real-time mode for specific workstations only, e.g. only for those workstations that are not protected with InterCheck.

Additional information

Workstations supported by Sophos Anti-Virus

Sophos Anti-Virus can protect the following workstations:

- Windows 3.x
- Windows for Workgroups
- Windows 95
- Windows NT (Intel and Alpha AXP)
- Macintosh
- DOS

In a networked environment, InterCheck can provide centrally controlled on-access scanning for workstations. This is available for the server platforms listed below.

Servers supported by Sophos Anti-Virus

- DOS/Windows 3.x
- Windows NT (Intel and Alpha AXP)
- Novell NetWare and IntranetWare
- OpenVMS (VAX and Alpha AXP)
- OS/2
- Banyan VINES

The DOS version can also be used to support various UNIX platforms.

SOPHOS

www.sophos.com

Sophos Plc • The Pentagon • Abingdon Science Park • Abingdon • OX14 3YP • England • Tel 01235 559933 • Fax 01235 559935
Sophos Plc • 2, Place de la Défense • BP 240 • 92053 Paris la Défense • France • Tel 01 46 92 24 42 • Fax 01 46 92 24 00
Sophos GmbH • Am Hahnenbusch 21 • D-55268 Nieder-Olm • Germany • Tel 06136 91193 • Fax 06136 911940
Sophos Inc • 18 Commerce Way • Woburn • MA 01801 • USA • Tel 781 932 0222 • Fax 781 932 0251