Sophos Anti-Virus

Quick Start Guide

Windows NT (single user)

SOPHOS

Introducing Sophos Anti-Virus

Sophos Anti-Virus detects all viruses known to Sophos and carries out automatic disinfection, providing complete protection for individual PCs and entire networks.

This guide shows how to install and use it on a single Windows NT workstation*.

How the software works

Sophos Anti-Virus includes two systems:

- **SWEEP** provides immediate and scheduled scanning of all disks, files and documents, 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. Therefore 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.

* There is a separate Quick Start Guide for networked installations.

See the main user manual for full product details.

Set up **server based on-access scanning for workstations**, to minimise workstation overhead; or, if you prefer, base scanning on the workstations, which is quicker and saves network resources.

Installing Sophos Anti-Virus

For installation, you will need:

- An Intel 386 or Alpha AXP based computer.

- Microsoft Windows NT 3.51 or later.

- 10 Mb free hard disk space.

- The current Sophos Anti-Virus CD.

Installation on a PC

💡 **If auto-run is not enabled, or under Windows NT 3.51, run D:\LaunchCD, where D: is the CD drive.**

Log on as a local Administrator and put the Sophos Anti-Virus CD in the CD drive. The CD will auto-start under NT 4.0.

At the **Sophos Anti-Virus** screen, choose **Quick installation**.
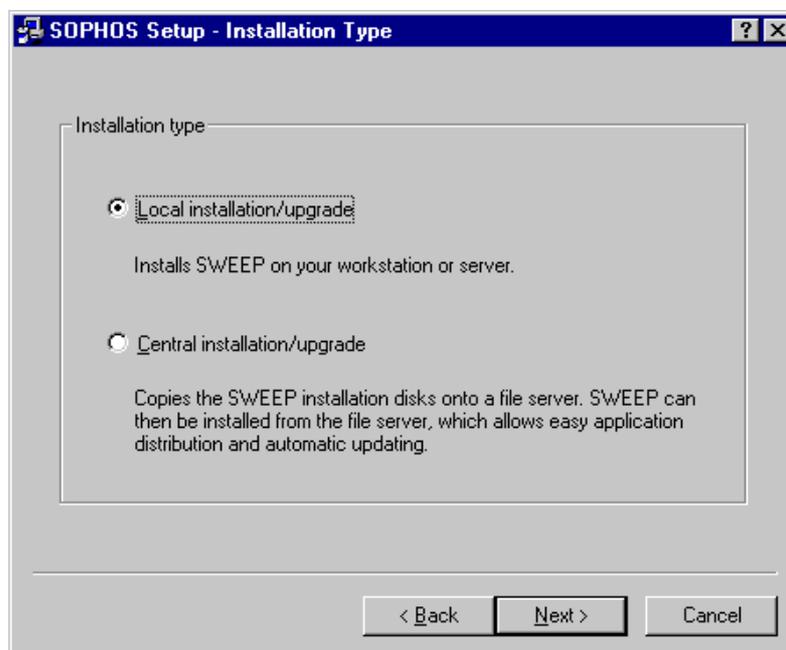
At the **Installation Type** screen, select:

- **Local installation** to install Sophos Anti-Virus on a single PC.

Installation on a PC (continued)

At the **Folder Selection** screen:

- Leave the **SWEEP source folder** unchanged.

- Choose a **SWEEP destination folder** where you want to install Sophos Anti-Virus, or accept the default folder.
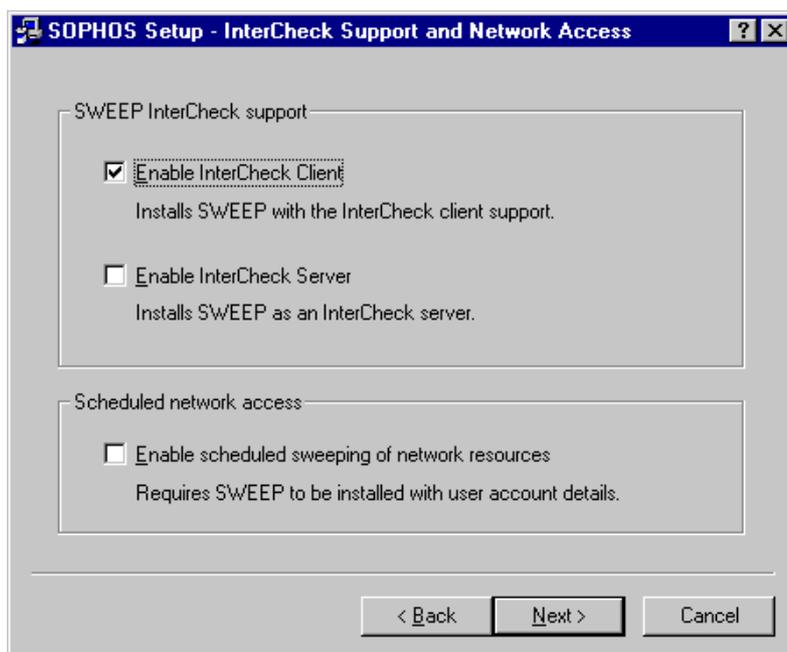
At the **InterCheck Support and Network Access** screen, select:

- **Enable InterCheck Client** for automatic checking of all files accessed on the workstation.

InterCheck is run automatically. At the final setup screen, select **Run SWEEP** if you also want to start SWEEP immediately.

SWEEP overview

To start SWEEP, at the taskbar, select **Start** | **Programs** | **Sophos SWEEP** | **SWEEP for Windows NT**.

The SWEEP screen appears. Here is a quick guide.

Icon toolbar

Tabbed pages

Indicator lights

On-screen log
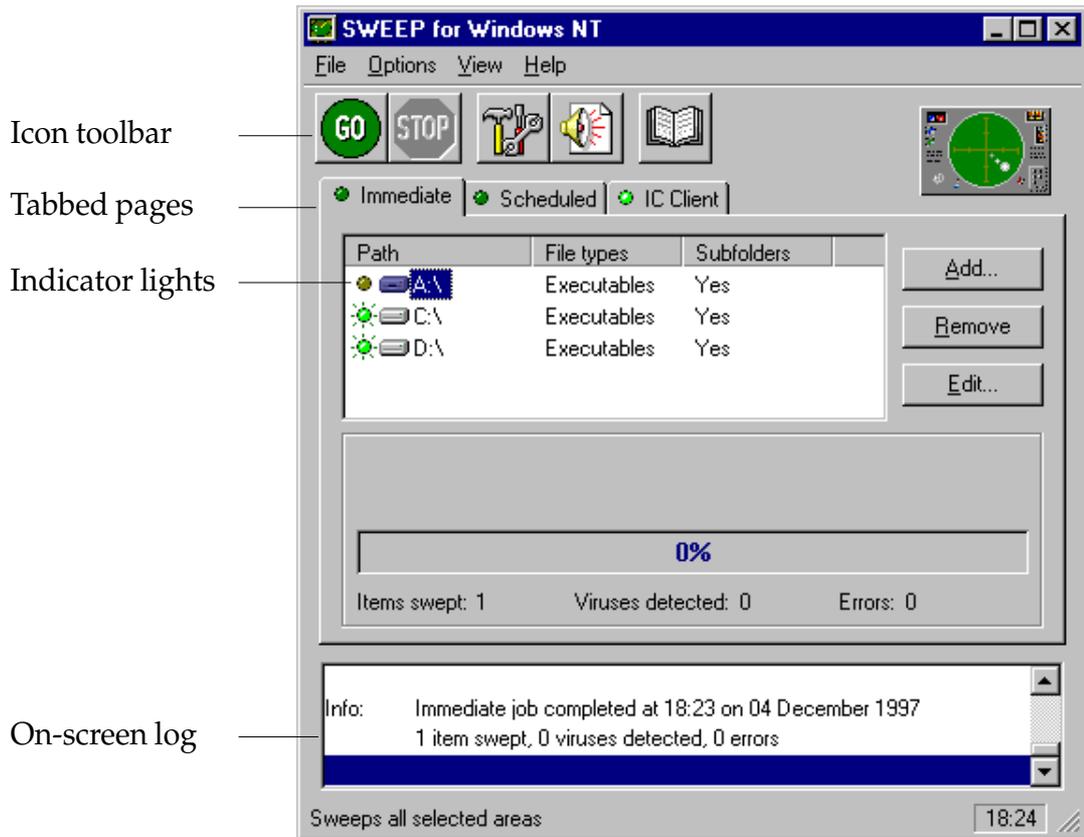
Icon toolbar

GO starts and STOP ends scanning.

Lets you configure the selected page or scheduled job.

Lets you specify virus alert systems, e.g. notification by email.

Displays the virus library.

Tabbed pages

When using Sophos Anti-Virus in stand-alone mode, there are three tabbed pages at which you can specify different scanning functions.

Immediate Lets you scan disks and files on demand.

Scheduled Lets you specify disks to be scanned at set times, even if no-one is logged on.

IC Client Lets you configure the InterCheck client and shows the last items checked.

Indicator lights

When lit these indicate that the item is selected. To select or deselect the item, click on its indicator light.

On-screen log

The on-screen log holds details of actions carried out by SWEEP, viruses detected, action taken and errors. It appears once a job is run.

💡 **Double-click on a virus name to display details of the virus and how to recover from it.**
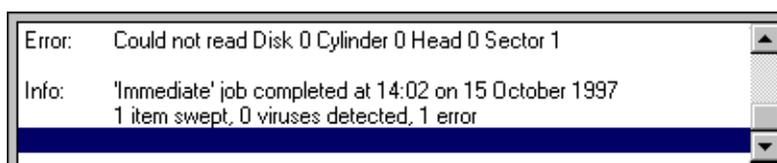
Drag the lower edge of the screen to expand the log, and use the scroll bars to view the complete log.

On-demand scanning

To scan selected drives on demand (i.e. now):

Ensure that the **Immediate** tabbed page is displayed.
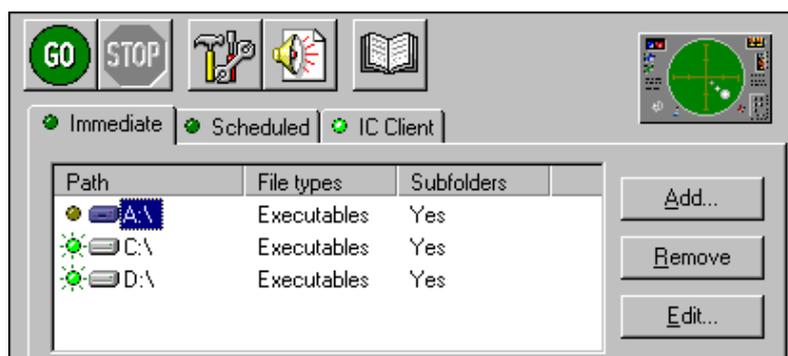
💡 **By default, SWEEP will scan local hard drives, checking executables only.**

Now select the drives that you want to virus check. You do this by illuminating their indicator lights.

Click on the **GO** icon in the icon toolbar.

Scanning begins. You can stop scanning at any time by clicking on the **STOP** icon.

To add new items for on-demand scanning

To add a new drive, folder or file to the **Path** list, click on **Add** on the main screen.

In **Enter item details**, you can specify:

💡 **To see which files are defined as Executables, select Options | Executables on the menu bar.**
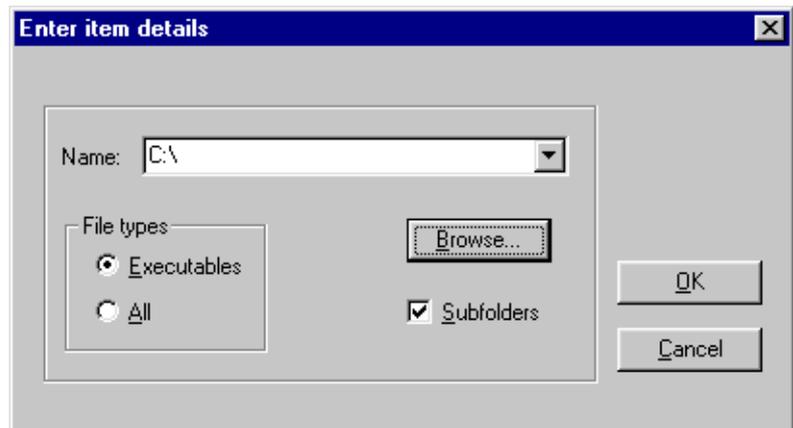
Name	Specify an item or use the drop-down menu to select **Local hard drives**. **Browse** shows available items.
File types	Choose executables only or all files.
Subfolders	Choose whether to include subfolders in the scan.

To change items for on-demand scanning

Highlight the item.

Click on **Edit**, and amend the details in the **Enter item details** dialog (see above).

To remove items for on-demand scanning

Highlight the item to be removed.

Click on **Remove**.

Scheduled scanning

By default, SWEEP carries out a virus check whenever the machine is booted and at 21:00 daily.

To change this, or to add further scheduled sweeps, use the **Scheduled** tabbed page on the main screen.

Setting up a scheduled job

🔆 **You can set up more than one scan per day as part of a single scheduled 'job'.**

To add a scheduled job, click the **Add** button and enter a job name when SWEEP prompts you.

The **Scheduled Job Configuration** pages appear.

Specify the files to be swept at the **File list** page and the sweeping time(s) at the **Time** page.

Changing a scheduled job

To edit a scheduled job, highlight the job in the list on the **Scheduled** tabbed page. Click on **Edit** and use the configuration pages to specify time, files swept etc.

Removing a scheduled job

To remove a scheduled job, highlight the job in the list and click on **Remove**.

On-access scanning

On-access scanning is automatic. It is provided by InterCheck and is enabled during installation.

InterCheck becomes active when the workstation is started.

To check that InterCheck is active, and for details of activity, go to the **IC Client** tabbed page on the main SWEEP screen, or look at the InterCheck monitor.

Using the InterCheck monitor
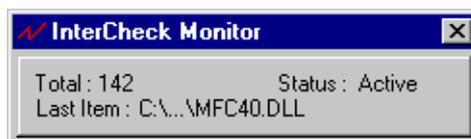
When the workstation is started up, the InterCheck monitor appears at the bottom of the screen.

To see this in future, click on the ⚡ (lightning icon) at the bottom right of the screen. The monitor shows, for the workstation's current session:

• The total number of items filtered (i.e. checked against InterCheck's list of authorised files).

• The last item filtered.

• Whether or not InterCheck is active.

What happens if a virus is found?

💡 **If a background scheduled scan finds a virus, a similar screen appears.**

If SWEEP finds a virus, a message like this appears:

If InterCheck finds a virus, access to the infected item is denied and a warning is displayed.

Any virus find is also added to SWEEP's on-screen log. To find out how to deal with a virus, double-click on the virus name in this on-screen log.

Sophos Anti-Virus can deal with many viruses automatically. See 'Automatic disinfection'.

Notifying other users

🔊 **This is the notification icon.**

If you are on a network, you can automatically notify other users, a central administrator etc. of virus finds, according to options set up at the **Notification configuration** screen. You reach this by clicking on the notification icon on the main SWEEP screen.

You can specify different messaging options depending on whether viruses are found during immediate, scheduled or on-access scanning. See the main user manual for details.

Automatic disinfection

Sophos Anti-Virus can deal with many viruses automatically.

You can specify different anti-virus measures, depending on whether viruses are found during immediate, scheduled or on-access scanning.

This is the configuration icon.

At the **Immediate** or **IC Client** tabbed page, or at the **Scheduled*** tabbed page with the required job selected, click on the configuration icon. At each page, you can specify:

- Disinfection of boot sector viruses.

- Disinfection of macro viruses.

- Removal of program files by a number of different means (not available for the InterCheck client).

Infected program files should be replaced and not disinfected, since disinfection cannot guarantee that the 'cleaned' files are exactly the same as the originals.

Immediate Mode Configuration

Mode | Action | Report

☑ Disinfect boot sectors

☐ Disinfect documents

☑ Request confirmation

☐ Infected files

○ Rename
○ Delete
○ Shred
○ Move
○ Copy

C:\Program Files\Sophos S   Browse

OK   Cancel   Help
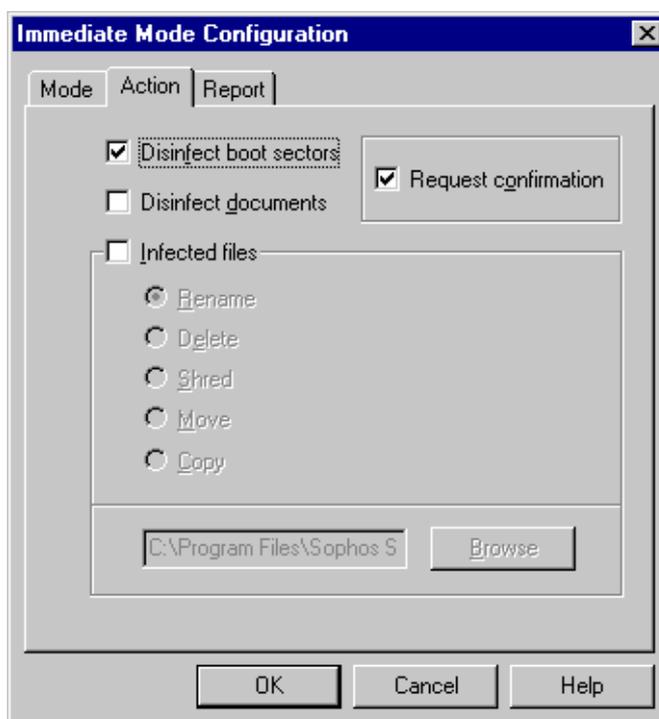
* Non-administrators have no access to the Scheduled tabbed page.

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 98

- 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.

S|O|P|H|O|S

www.sophos.com