Sophos Anti-Virus

Quick Start Guide

Windows NT (networked)

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 across a Windows NT network*.

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.

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

*** There is a separate Quick Start Guide for single PC installation.**

See the main user manual for full product details.

Installing Sophos Anti-Virus

Placing the installation files on a server means that workstations can be updated automatically when a new version is placed on the server.

You install Sophos Anti-Virus throughout your network as follows:

Step 1: Central installation.
Places the installation files on the file server.

Step 2: NT workstation installation.
Makes a working installation of Sophos Anti-Virus on a Windows NT workstation, providing on-demand and on-access scanning.

If you want to protect non-Windows NT workstations on your network, there are two more steps:

Step 3: NT InterCheck server installation.
Provides server based on-access scanning of files on client workstations.

Step 4: Non-NT workstation installation.
Enables non-NT workstations to use the on-access scanning provided by the NT InterCheck server.

What you will need for the installation

You can find all the latest documentation, including this guide, on the Sophos Anti-Virus CD.

You will need:

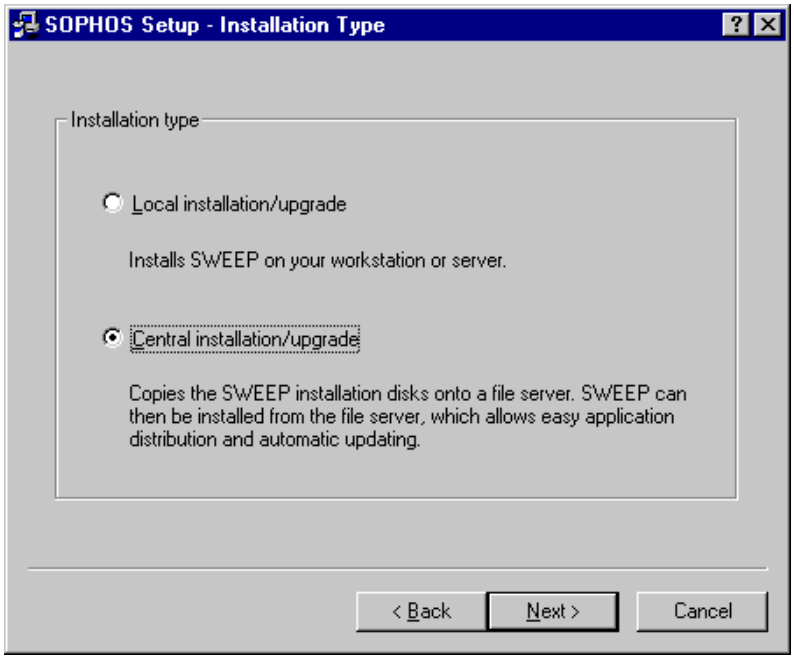
- An Intel 386 or Alpha AXP based computer.
- Microsoft Windows NT 3.51 or later.
- 4 Mb hard disk space for a central installation.
- 10 Mb hard disk space for a working installation.
- The current Sophos Anti-Virus CD.

Step 1: Central installation

If auto-start is not enabled, or under Windows NT 3.51, run D:\LaunchCD where D: is your 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 Windows NT 4.0.

At the **Sophos Anti-Virus** screen, choose **Quick installation**.



At the **Installation Type** setup screen, select:

- **Central installation** to place the installation files on the file server.

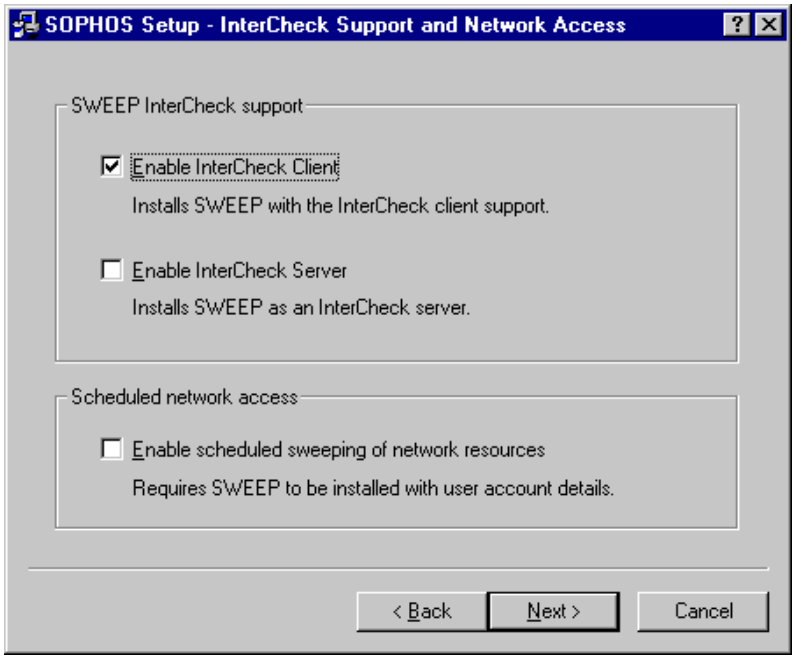
At the **Folder Selection** screen:

- Leave the **SWEEP source folder** unchanged.
- Choose a **SWEEP destination folder** where the installation files will be placed. This folder must be visible to other users on the network.

At the rest of the screens, you do not have to make any choices, as these set defaults that you can confirm or change when you make working installations later.

Step 2: NT workstation installation

Log on to the workstation as a local Administrator and run `Setup` from the central installation directory.



At the **InterCheck Support** screen, select:

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

At the **SWEEP Installation Options** screen, select:

- **Auto-upgrade** for this installation to be updated when the central installation is updated. You will be asked to enter a username and password.
- **Prevent removal** to prevent unauthorised removal.

At the **Auto-upgrade mode screen**, you can specify how auto-upgradng takes place.

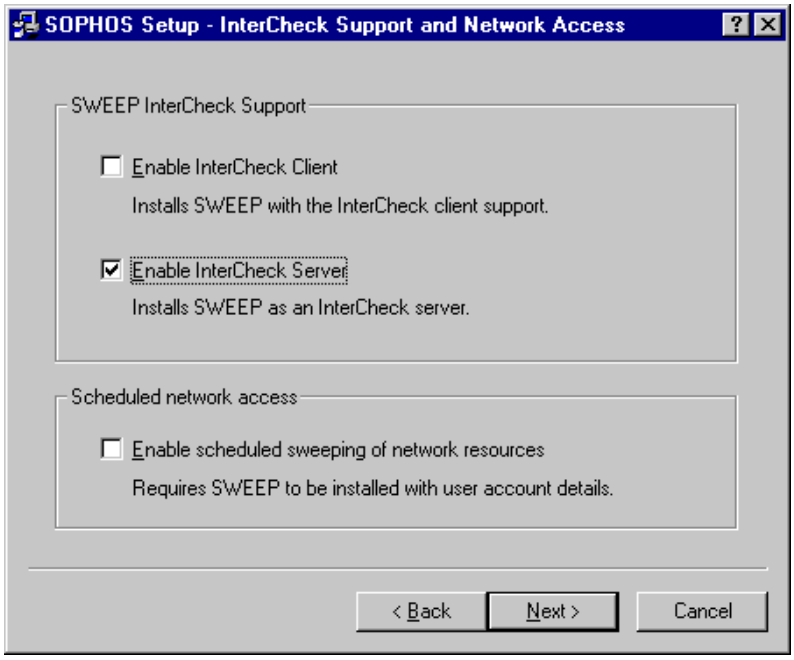
InterCheck is run automatically. At the final setup screen, select **Run SWEEP** if you also want to start SWEEP immediately.

At the Auto-upgrade mode screen, you can allow users to postpone auto-upgrading. This may be useful for those on remote dial-up modems.

Step 3: NT InterCheck server installation

You need to install an NT InterCheck server if you want to provide **server based** on-access scanning of non-Windows NT workstations.

Log on to the server as a local Administrator and run `Setup` from the Sophos Anti-Virus central installation.



At the **InterCheck Support** screen, you should select:

- **Enable InterCheck Server** to enable SWEEP to provide on-access scanning for **non-NT** client workstations.

You can also select:

- **Enable scheduled sweeping of network resources** to enable SWEEP to scan other machines on the network at set times. You will be asked to enter a username and password.

You can perform *immediate* scanning of other machines, and scheduled scanning of the local machine, without choosing this option.

Step 4: Non-NT workstation installation

You can use Sophos Anti-Virus to protect **non-NT** workstations. There are two ways to do this:

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

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 that are not always on the network.

In the case of Windows for Workgroups or Macintosh workstations, consult the special instructions in the main *Sophos Anti-Virus for Windows NT* manual.

See below for instructions for installing either on DOS/Windows 3.x or Windows 95/98 workstations.

To install a networked InterCheck client

Before you install a networked InterCheck client, you must have the InterCheck server enabled (see 'Step 3: NT InterCheck server installation').

DOS/Windows 3.x and Windows 95/98

You can install a networked InterCheck client from your file server. Locate the user's login batch file (see the Windows NT documentation) and include:

```
NET USE I: \\ServerName\INTERCHK
I:\ICLOGIN -U
NET DELETE
```

where `I:` is an unused drive and *`ServerName`* is the name of the server on which you installed Sophos Anti-Virus.

When the workstation logs on, it will run the InterCheck login batch file, giving the workstation server based on-access protection.

To install a stand-alone InterCheck client

DOS/Windows 3.x

Make sure that the central installation directory is mapped to a DOS drive. On the workstation, at a DOS prompt, change to that drive and enter

```
ICINSTAL
```

If you have more than one hard disk, select the desired drive from the **Where** menu. To start the installation, select **Onto hard disk** from the **Install** menu and follow the instructions.

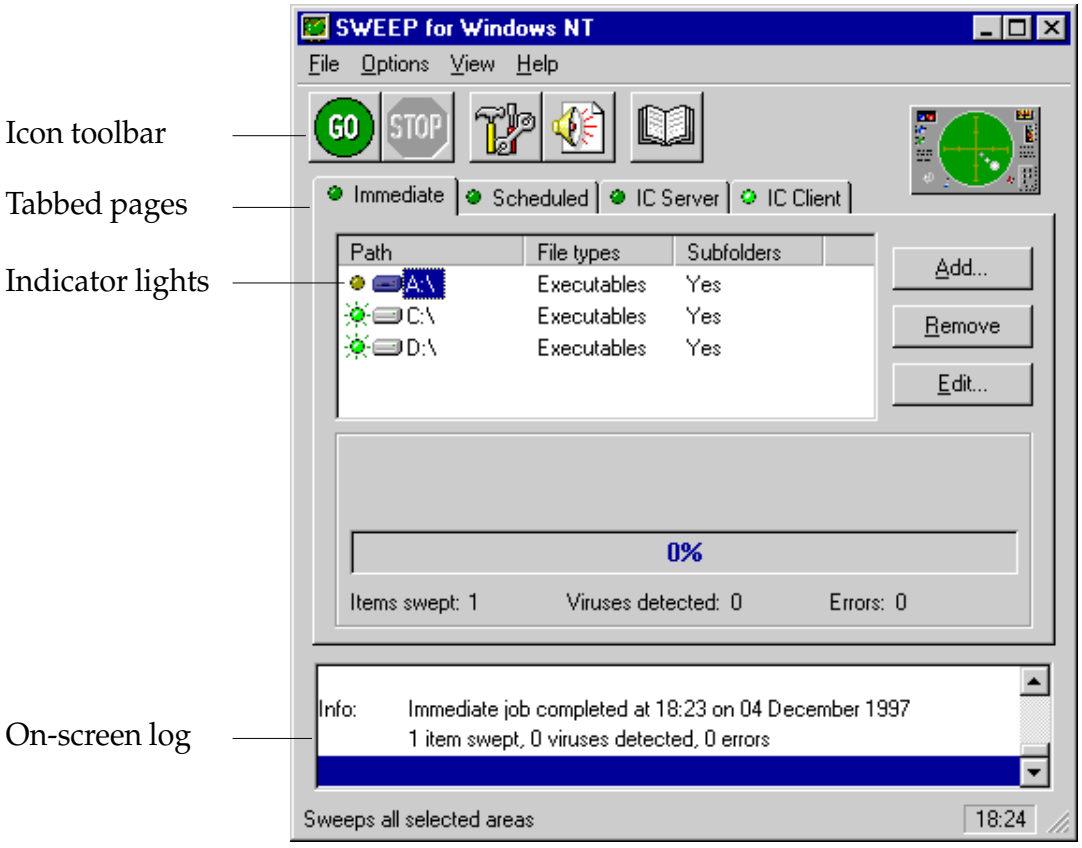
Windows 95/98

Install Sophos Anti-Virus for Windows 95/98 and select the **InterCheck for Windows 95** option at the 'Installation Type' setup screen. See also the *Sophos Anti-Virus for Windows 95* Quick Start Guide.

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

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

There are four 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.

IC Server Lets you configure the InterCheck server and shows the last items checked.

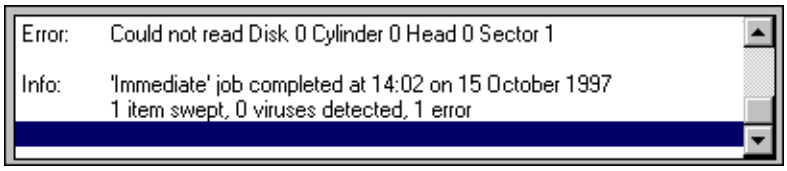
If you did not select the InterCheck client or InterCheck server at setup, these tabs will not appear.

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.

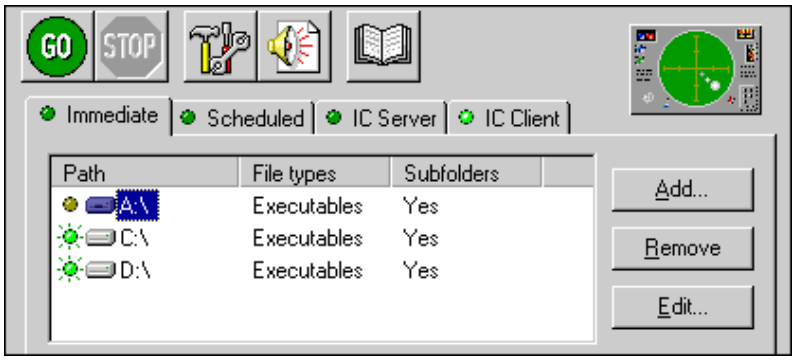
The log can be seen on both server and workstations. The server log details all scans on workstations.

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.

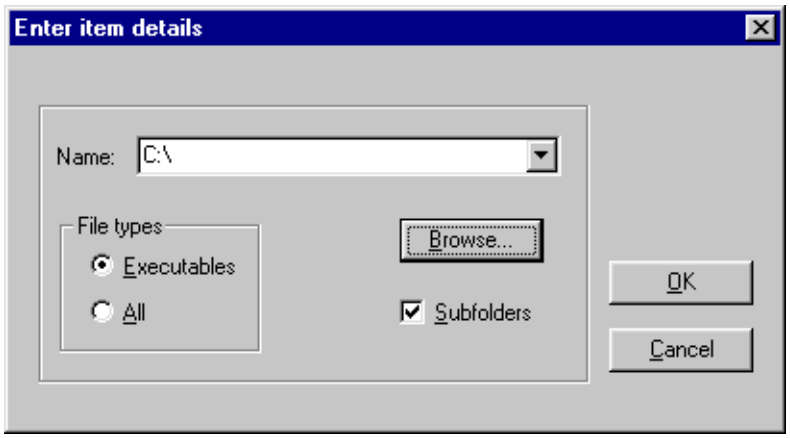
Click on the **GO** icon in the icon toolbar.

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.

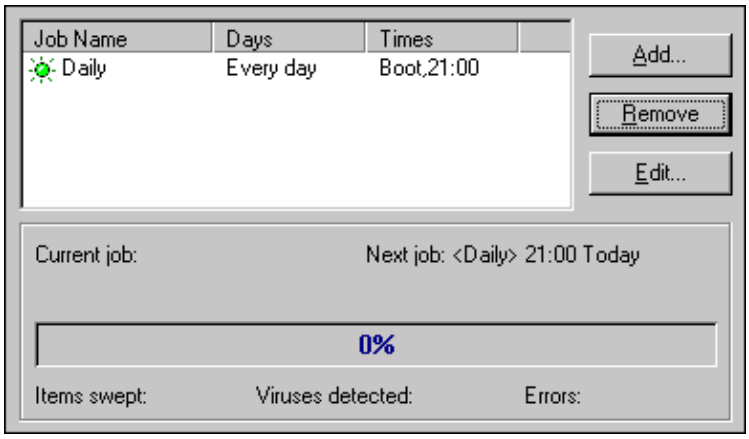
Click on **Remove**.

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, 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.

Administrators can start, stop and configure the InterCheck client or InterCheck server at the **IC Client** or **IC Server** tabbed pages.

Using the InterCheck monitor

When the **InterCheck client** is installed on a **Windows NT workstation**, the InterCheck monitor appears at the bottom of the screen.

To save screen space, click on the monitor with the right mouse button and select No title. Or click on X to minimise it completely. In both cases InterCheck remains active.

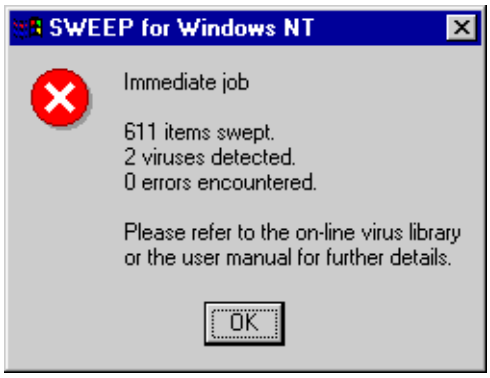
To see this in future, click on the (lightning icon) at the bottom right of the screen. The monitor shows, for the workstation's current session:

- 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. Only Administrators can configure messaging options.

A virus incident anywhere on the network can be automatically reported to a central administrator or specified individuals, according to the messaging 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.

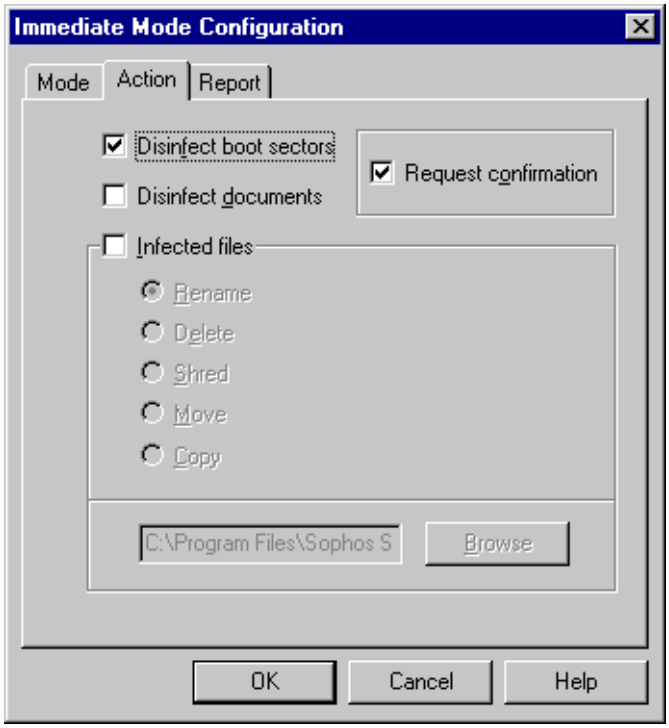
At the server (for non-NT workstations), or at the NT workstation, go to the main SWEEP screen. At the **Immediate**, **IC Client** or **IC Server** page, or at the **Scheduled*** page with the required job selected, click on the configuration icon. At each page, you can specify:

- Disinfection of boot sector viruses (not available for the InterCheck Server).
- Disinfection of macro viruses (not available for the InterCheck Server).
- Removal of program files by a number of different means (not available for the InterCheck client).

This is the configuration icon.

*** Note that non-administrators have no access to the Scheduled page.**

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



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.

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