

SOPHOS

Sophos Computer Security Scan startup guide

Product version: 1.0

Document date: February 2010



Contents

| | |
|-------------------------------|---|
| 1 About the software..... | 3 |
| 2 What do I need to do?..... | 3 |
| 3 Prepare for scanning..... | 3 |
| 4 Install the software..... | 4 |
| 5 Scan your computers..... | 5 |
| 6 View reports..... | 5 |
| 7 Uninstall the software..... | 6 |
| 8 Further help..... | 6 |
| 9 Copyright..... | 6 |

1 About the software

Sophos Computer Security Scan is a tool that scans computers for the same threats as our full anti-malware product:

- Malware and rootkits.
- Suspicious files.
- Potentially Unwanted Applications.
- Controlled applications. These are legitimate applications (such as games, instant messaging, file sharing) that you might want to block, depending on their impact on business productivity, data loss and IT resources.
- Controlled devices. These are storage or networking devices that you might want to block, depending on whether they pose a risk of malware infection or data loss.

Note: Scanning may affect the performance of your endpoint computers. This is especially true if you scan the computers for rootkits.

If you need advice on the scan results or on cleaning up security risks, contact Sophos or a Sophos partner.

If you also want to check that your computers have an up-to-date operating system and run anti-virus and firewall software, download the Sophos Endpoint Assessment Tool.

2 What do I need to do?

To scan an individual computer or network, you need to:

- Prepare for scanning.
- Install the software on a central computer.
- Use the software to install and run a scanner on computers on your network.

The sections that follow describe these steps.

3 Prepare for scanning

This section tells you how to ensure that you are prepared for scanning.

Note: You do not need to uninstall or disable any other security software you are already running.

3.1 Check your accounts and internet access

Ensure that you have the following:

- Your Sophos account. Sophos emails the account details to you when you download Sophos Computer Security Scan.
- An administrator account that can install software on networked computers.
- An internet connection on the central computer where you run Sophos Computer Security Scan.
- Details of the proxy server you use to access the internet (if you use a proxy server).

3.2 Prepare your computers

Ensure that the computers you want to scan (an individual computer or computers that are on a network) meet these conditions:

- Simple file sharing is disabled.
- The firewall (if there is one) leaves the selected port open. The port can be configured in the wizard. This is so that results can be sent to the central computer.
- The computer can access a shared folder on the central computer.
- The Remote Registry Service is started and its startup type is set to "Automatic" (Windows Vista and later).

You may also need to:

- Turn off User Account Control on any Windows Vista or later computers. This is necessary if you do not have Active Directory available (or do not intend to let Sophos Computer Security Scan use it) and you are signed on as a local administrator.

4 Install the software

To install the software, do as follows.

1. Go to the central computer you want to use to distribute the scanner to other computers.
2. If you have not already downloaded Sophos Computer Security Scan, do so now.
3. Double-click the downloaded package.

An installer is launched. Follow the instructions.

The installer places shortcuts to Sophos Computer Security Scan on your desktop and in the **Start** menu.

5 Scan your computers

To scan computers, do as follows.

Note: You can include no more than 200 computers in each scan, but you can carry out as many scans as you want.

1. Double-click the Sophos Computer Security Scan icon on your desktop.
A wizard is launched.
2. In the wizard, follow the instructions to install and run the scanning software.
 - If you have Active Directory, we recommend that you select it when the wizard prompts you. The wizard will install the scanning software on computers automatically.
 - If you do not have Active Directory, the wizard will tell you how to do the installation manually.

Sophos Computer Security Scan scans your computers and displays live results.

3. Wait for the scans to finish before you close the wizard.
If you close the wizard too soon, the scans will not finish and security risks might not be detected.

If you accept the default settings, Sophos Computer Security Scan displays a report.

Note: The report shows the aggregate results of this scan and any previous scans.

6 View reports

If you accept the default settings, a report on computer security is displayed after each scan.

If you want to see reports again, do as follows.

1. In the Program Files directory, go to Sophos\Computer Security Scan\Reports\Published.
2. Double-click the HTML report you want to view.

If you want to share a report with other users, you can attach the HTML file to an email and send it.

7 Uninstall the software

Sophos Computer Security Scan places software on your server and on the endpoint computers you scan.

- The software on the endpoint computers automatically uninstalls itself when the scan is complete.
- You can use Add/Remove Programs to uninstall Sophos Computer Security Scan from the server.

8 Further help

If you need further help with Sophos Computer Security Scan, see the frequently asked questions in Sophos knowledgebase article 65034

(<http://www.sophos.com/support/knowledgebase/article/65034.html>)

9 Copyright

Copyright © 2010 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.