

SUPERAntiSpyware Product Documentation

Table of Contents

03	Introduction
03	About
04	Further Help
04	Threats to Computer
07	Key features of Spyware
07	Scan this computer
09	System Tools
10	Real-Time Protection
11	Automatic Updates
12	Help and Registration
13	Operating System Requirements
14	Web browser Compatibility

Introduction

SUPERAntiSpyware identifies and eliminates the most dangerous spyware, adware, malware, dialer, worm, and keylogger components. To keep our definitions and rules up to date every day, we have a specialized Threat Research Team that examines thousands of system diagnostics and spyware samples.

Please contact our support staff so that we can examine your system and try to identify the issue if you believe SUPERAntiSpyware is not detecting your spyware.

About

The SUPERAntiSpyware focuses on spyware, adware, worms, trojan horses, rootkits, and crimeware. This concentration enables us to respond fast to the constantly expanding groups of malicious software we address, with new definitions issued many times per day, and concentrate on the technology that targets the most prevalent threats in the wild. SUPERAntiSpyware will remove any items that are frequently referred to as viruses (such as several trojans, worms, and so on), but it won't remove any actual viruses or boot-sector viruses.

Several well-known antiviruses and antispymware programs, including McAfee, Symantec Norton, Kaspersky, Bitdefender, ESET NOD32, Spybot Search & Destroy, Hitman Pro, Ad-Aware, AVG, Avast, Panda, Webroot, Malwarebytes, Avira, and others, are compatible with SUPERAntiSpyware.

Further help

The SUPERAntiSpyware Quarantine is a safe "holding pen" for objects that have been identified as threats and eliminated from your hard drive and/or registry. The objects on your Quarantine list have been taken out of your body and are dormant there. Items under quarantine won't operate and can't damage your system.

When a scan is finished, the quarantine procedure takes the threat objects from your hard drive and/or registry to the quarantine and then removes them. This is shown in the quarantine as "Adding:" and "Removing;" respectively.

By using the Restore... button, you can put objects that were quarantined back onto the disc or registry location(s) where they were first discovered. Restore... can be used to un-quarantine objects that SUPERAntiSpyware mistakenly identified as malicious software. Remember that the majority of users won't ever require the Restore... capability. You can be putting your system in danger if a valid malware threat is not quarantined.

You can permanently remove objects from the Quarantine by using the Remove... button. Any thing that has been taken out of quarantine will no longer be present on your computer.

Threats to Computer

Malware (short for malicious software) is the term used to refer to viruses, spyware, rootkits, and all other types of malicious software collectively.

What is a virus?

A computer virus is a piece of software, typically malicious in intent, designed to spread other programs like it from one computer to another. The presence of viruses itself can harm a system and result in the loss of important data, or they can be exploited to infect a system with spyware, rootkits, or other malware.

The installation of the most recent security updates for the computer operating system and the installation of an up-to-date antivirus program on every machine in a network are important steps in preventing infection. Users should also confirm that the software they are obtaining from the internet is from a reliable source because many malware varieties are installed with other software that appears to be trustworthy.

What is spyware?

Spyware is computer software that has been installed and is intended to gather data about computer users, frequently without their knowledge or agreement. This data may lead to so-called identity theft, theft of priceless information (like bank or credit card numbers), or theft of confidential corporate information.







Nowadays, rather than being created by opportunistic lone individuals, most spyware is created by organized crime rings and installed by a virus or another type of malware.


SUPERAntiSpyware


SUPERAntiSpyware Professional X Trial (13 Days Remaining)



SUPERAntiSpyware

 Scan This Computer	 System Tools Explore and Repair this PC	 Help & Registration Product Info and Support
 Real-Time Protection Enabled	 Scheduled Scanning Enabled	 Automatic Updates Enabled

 **SUPERAntiSpyware Version 10.0.1246**
Professional X Trial
[Click here to upgrade](#)




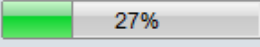
 **Database 17040**
Updated 213 days ago
[Click here to check for updates](#)

SUPERAntiSpyware Main Screen

SUPERAntiSpyware

Malware Database Update

Please wait while we download and update your database.

 Authenticating Connection	Complete
 Checking for Definition Updates	Complete
 Downloading Updates (Mirror 1)	 27%

Database update screen

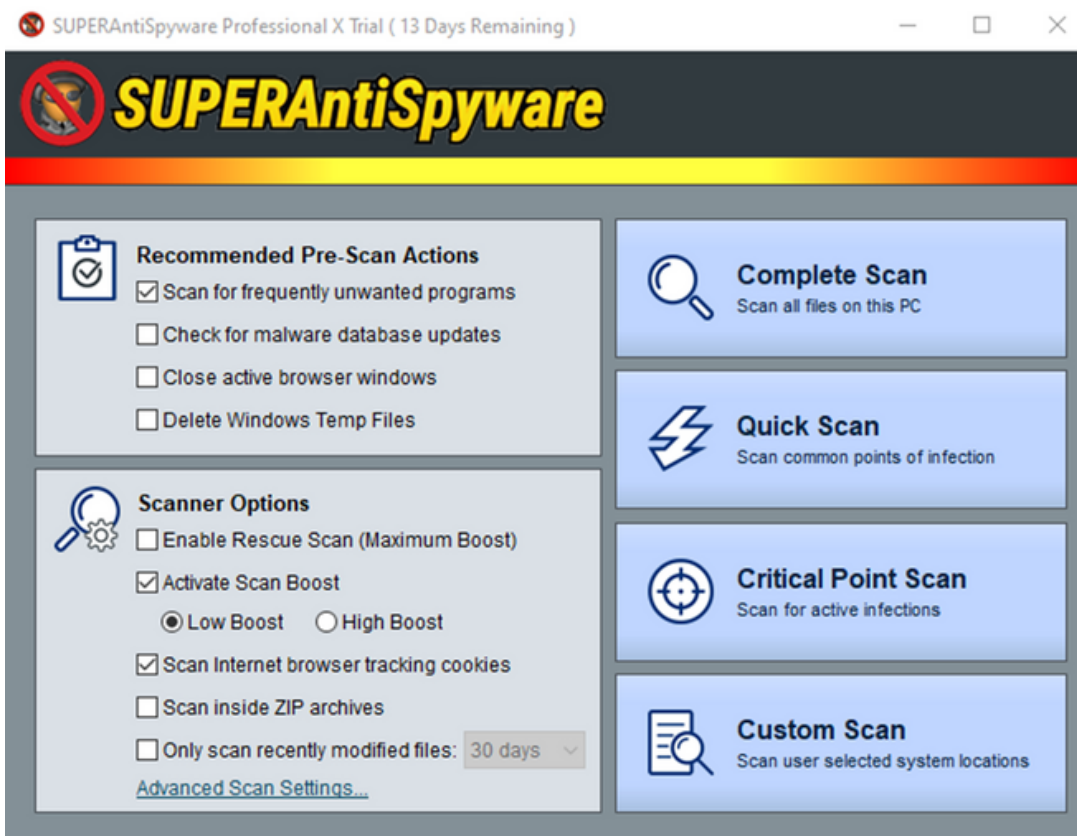
Key features of spyware

Scan this Computer

We advise running a thorough check on your computer at least once a week and a fast scan whenever you notice a problem with its performance.

Sluggish performance, pop-up adverts that occur when browsing or even when you are not browsing, icons that appear out of nowhere on your desktop, and/or changes to your browser's home page or other settings are all possible symptoms of spyware infection.

Users of SUPERAntiSpyware Professional can take advantage of Real-Time Protection to stop spyware from being installed and automated scheduled scans to make sure your computer is always secure and free of malware.



"Scan this Computer" Screen

To add folder exclusion:

- ·Open SUPERAntiSpyware
- ·Click on System Tools
- ·Click on Advanced Scan Settings
- ·Click the Modify Excluded File Locations button
- ·Click the "+" button

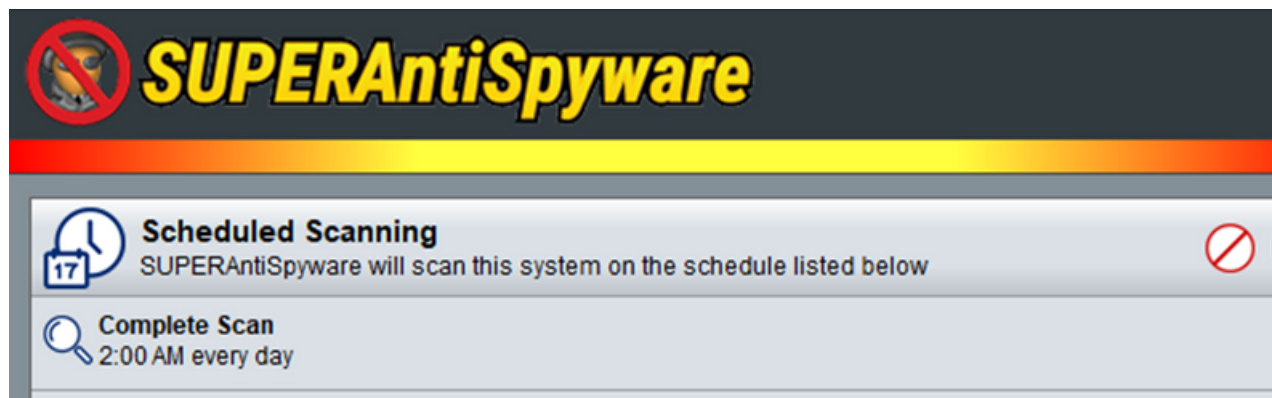
From the list of folders, you will need to find and select the folder containing any files you wish to exclude. Once the folder is selected and added to your exclusions, click "Done".

Critical Point Scan & Quick Scan

The Critical Point Scan is the quicker of the two and quickly scans for malware in the most frequent locations. A Quick Scan takes longer since it is more thorough. For routine scans, a Quick Scan would be advised, and as frequently as possible, a Complete Scan.

Reuse Scan

Only when malware is using up so many system resources that you are unable to conduct a scan should a rescue scan be enabled. Rescue scan makes an effort to take some of those resources back. Do not enable this option if you can conduct a scan normally. Apart from the regular scan, this software also allows for a scheduled scan.



"Scheduled Scan" Screen

System Tools

Only perform repairs if the problem mentioned in the repair description exists. Run the fix even if you don't have that problem or are unsure whether you do.

SUPERAntiSpyware will detect tracking cookies as "Adware. Tracking Cookies" and you can choose to remove them or leave them on your system. You may turn off this feature in the Preferences -> Scanning Control tab of SUPERAntiSpyware should you not wish cookies to be scanned, detected, and removed.



Options inside System Tools Menu

Real-Time Protection

Before a file executes on your computer, REAL-TIME protection from SUPERAntiSpyware examines it to make sure spyware is not present. The file is blocked from running if an infection is found in it. In order to make sure spyware has not "hooked" itself into your operating system or browser, Real-Time Protection will additionally scan important areas of your registry.

Additionally, SUPERAntiSpyware features our own First Chance Prevention technology, which checks your registry and common and uncommon starting sites for spyware that is configured to run when you restart your computer.

When your computer shuts down or logs off, the First Chance system checks these files to check for spyware that changes itself on shutdown and to eliminate it before it has a chance to run.

To enable Real-Time Protection:

- ·Open SUPERAntiSpyware and click on "Real-Time Protection"
- ·Check the "Enable real-time protection" option
- ·Click on the "Done" button to save

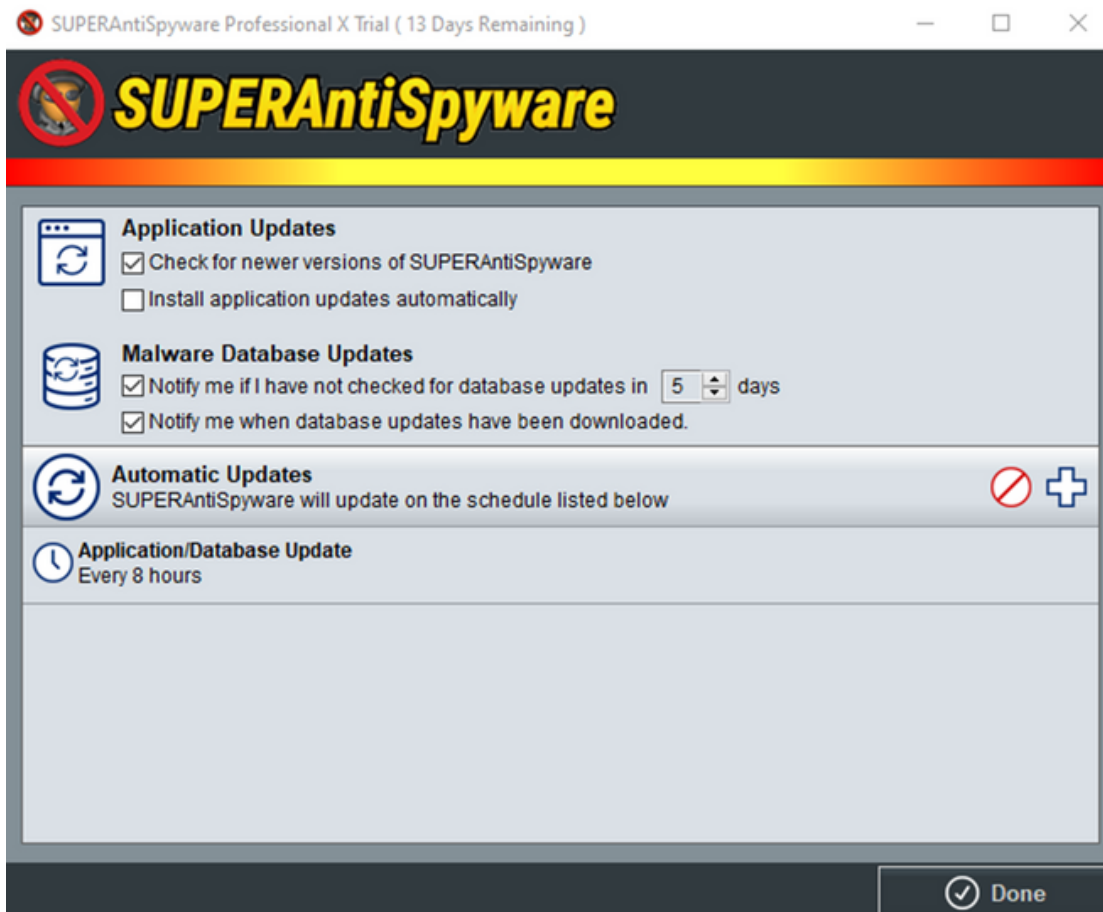


Options inside Real Time Protection Menu

Automatic Updates

Check for program and definition updates at least once a week to ensure optimal efficacy. Right-click the SUPERAntiSpyware icon (the yellow/brown insect) in the system tray (near the Windows system clock) and choose "Check for Updates" to check for software and definition updates. To finish the update procedure, adhere to the instructions.

Using SUPERAntiSpyware Professional, your computer may automatically check for updates. Click the "Automatic Updates" option to gain access to SUPERAntiSpyware Professional's automatic update features. On startup and every eight hours, SUPERAntiSpyware Professional can be configured to check for programme and definition updates.





Options inside Automatic Updates Menu

Please be aware that SUPERAntiSpyware typically does not check for definition updates when it starts up. Both the "Install application updates automatically" and the "Check for newer versions of SUPERAntiSpyware" settings must be selected.

To better fit your schedule and general computer usage, you can modify your Automatic Updates. When you have finished setting all of your choices, click "Done" to store them.

SuperAntiSpyware has a free version and PRO x version. Their differences are stated below.

Features	 SUPERAntiSpyware FREE	 SUPERAntiSpyware PRO X
AI-Powered Detection Engine fueled by machine-learning that constantly updates the database and blocks 1 billion+ malicious threats. Boost Microsoft Defender .		●
Multiple Scan Options schedule either quick, complete, or critical scans to fit your lifestyle.		●
Real-Time Threat Blocking stops malicious files from running as soon as they are detected.	*must run scans to block threats	●
Automatic Updates ensure the program is running with the latest database definitions.	*must update database manually	●
Email Notifications get emails with scan results so you can monitor PCs remotely.		●
Detect & Remove Malicious Threats from Malware, Spyware, Adware, Trojans, Dialers, Worms, Ransomware, Hijackers, Parasites, Rootkits, KeyLoggers, and many more.	●	●
Multi-Dimensional Scanning a next-generation scanning system that goes beyond the typical rules-based methods.	●	●
Process Interrogation Technology detects hard-to-find threats usually missed by standard anti-spyware applications.	●	●

Help and Registration

You don't need to download or reinstall the software if you already have SUPERAntiSpyware Professional installed on your computer or are using the SUPERAntiSpyware Free Edition.



Simply choose Register/Activate from the menu by right-clicking the SUPERAntiSpyware icon (the tiny brown "bug" next to the system clock). To finish the registration procedure, enter your registration code and follow the wizard's instructions.

Start the SUPERAntiSpyware programme on your computer if the "bug" icon isn't already there beside the system clock. Choose Help & Information from the Home screen, then input the code in the box next to "Professional Registration Code." Click the "OK" button after entering the code.

Please use our automatic registration code retrieval system* by clicking here if you do not have your registration code.

Make sure that the registration code e-mail is not trapped in your spam or junk e-mail folder.

You can also email us at superantispyware@support.com or fill out a customer service ticket here.

Operating System requirements

With Windows operating systems, all SUPERAntiSpyware solutions are compatible. The operating systems Windows 7, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, and Windows 11 are all compatible with SUPERAntiSpyware Professional X Edition. Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows Server 2012, Windows 10, and Windows 11 are all compatible with SUPERAntiSpyware Free Edition and SUPERAntiSpyware Technicians Edition.

The SUPERAntiSpyware installer will detect whether you have a 32-bit or 64-bit operating system and will then automatically install the appropriate version. Currently, SUPERAntiSpyware is not supported by Mac, Apple, iOS, or Android operating systems.

Web browser compatibility

SUPERAntiSpyware is compatible with all web browsers. The realtime protection feature and the on-demand scanner work to keep your system secure, regardless of what web browser you use.

SUPERAntiSpyware will detect and remove tracking cookies in Internet Explorer, Firefox, Chrome, and Edge. Currently, the SUPERAntiSpyware Hi-Jack Protection features work with Internet Explorer only.

Disclaimer: This has been created as part of the IIM Skills - Technical Writing Master Course's assignment. The pictures and the data have been captured from real spyware. This has been created solely for educational purposes and not for commercial purposes.