Table of Contents

Part I  Features of Security Task Manager  4

Part II  Using Security Task Manager  6

Overview .......................................................................................................................... 6
Viewing process details .................................................................................................... 6
Learning more about a process (Google search) ............................................................. 7
Ending a process ............................................................................................................. 7
Using quarantine folder .................................................................................................. 7
Printing process list ......................................................................................................... 8
Exporting process list ...................................................................................................... 8
Writing a comment ........................................................................................................... 8
Checking Hosts file changes .......................................................................................... 8
Changing the language ..................................................................................................... 9

Part III  Basics  11

Risk Rating of processes ............................................................................................... 11
Process types .................................................................................................................. 12
Uninstalling ..................................................................................................................... 12

Part IV  Protecting your computer with SpyProtector  14

Delete traces of your Internet and computer activity ..................................................... 14
Disable keyboard monitoring ......................................................................................... 14
Disable other monitoring ............................................................................................... 14
Warning when registry is changed ............................................................................... 14

Index  15
Features of Security Task Manager

Part I
I. Features of Security Task Manager

Security Task Manager provides advanced information about programs and processes running on the computer. For each process it shows the following information not shown in Windows Task Manager:

- security risk rating
- virus scan with 40 anti-virus engines
- file name and folder path
- description
- start time
- CPU usage graph
- program icon
- contained hidden functions (keyboard monitoring, Browser supervision, manipulation)
- process type (visible window, systray program, DLL, IE-Plugin, service)

The Security Task Manager also recognizes virtual driver software, services, BHO or processes hidden from the Windows Task Manager.
Using Security Task Manager
II. Using Security Task Manager

Overview

Security Task Manager shows all active processes on your computer. The Rating tells you all relevant security functions a process contains.

The listed processes can be sorted by the following properties. Click on View menu to chose, which properties are shown:

- Name
- Rating
- Process ID (PID)
- CPU and Memory
- Active runtime
- File
- Type
- Start
- Title and Description
- Company and Product

Click a process to obtain more information about the process. You can:

- see properties
- end process
- place process in quarantine

Note

- Click Show system processes button to see all internal Windows operating system processes. Windows system processes are not shown by default.
- When you are logged on to Windows with a standard user account, perhaps you see for some system processes: <taskeng.exe - Services - Access denied>
  Please run Security Task Manager as Administrator in this case: Right-mouse click the Security Task Manager icon. Then click Run as administrator.

Viewing process details

Click on a process to see more information about this process. Following properties are shown:

- Name
- Rating
- Company
- Description
- Type
- Start
- File
- Comment

Receive further information or stop the process:

- Information from the Internet about a process
- Ending process
Putting in quarantine

Learning more about a process (Google search)

1. Click on the process you want to examine.
2. Click the Google button on the toolbar.

An information web page is displayed on www.neuber.com/taskmanager where you can submit your opinion about this software/driver software, or read other user comments. You can also search for further information about this process at Google.com.

Note
- Your Internet browser transmits information (e.g. operating system, language setting). Neither the Security Task Manager program nor any of its components connect to the Internet directly.
- Google.com is one of the most commonly used search engines, and will provide you with relevant results.

Ending a process

1. Click on a process you want to close.
2. Click the button Remove.
3. Then select one of the following options:
   - End process
   - Move file to quarantine
   - Uninstall

Note
- Ending a process can cause system instability, including crashes. Software that needed Adware programs could not work. Please save opened documents.
- You can create a restore point, to can restore your Windows system at any time.
- You need administrator rights for this dialog. To start Security Task Manager with administrator rights, please right-click the Security Task Manager shortcut. Then click Run as...

Using quarantine folder

The quarantine folder works like the Windows Recycle Bin (trash). When you put a file into quarantine folder, the file is renamed and moved to an isolated folder. Corresponding Autostart keys in the Windows registry are deleted so the process cannot be started again. Restoring the whole process is possible at any time:

Restoring processes
1. Click the quarantine button on the toolbar.
2. In the quarantine folder click on process you want to restore.
3. Click Restore button.

Note
- You can create a Windows restore point in the Remove dialog, to restore your Windows system at any time.
Printing process list

1. On File menu click **Print**.
2. Chose a printer and make any necessary settings (e.g. duplex print).

**Note**
- Click **Show system processes** button to see all Windows internal processes. Then you can print Windows processes too. Windows system processes are not shown by default.

Exporting process list

1. On File menu click **Export to**.
2. Chose a file type:
   - Text file (*.txt)
   - Website (*.html)

**Note**
- Click **Show system processes** button to see also all Windows internal processes. Then you be able to save Windows processes too. Windows system processes are not shown by default.
- Please save the process list from time to time. A saved process list can serve as a point of comparison to help you find new processes in the future.

Writing a comment

You can record a remark about each process, which will be visible in the process properties. You can vote the process to change the Security Task Manager Rating.

**To write a comment**

1. Right mouse click a process you want.
2. Click **Comment...** on the appearing context menu.
3. Enter your comment and your opinion about the process.

Checking Hosts file changes

The Windows **hosts** file is located in `c:\Windows\system32\drivers\etc` folder by default. This text file contains the mappings of IP addresses to Internet domain names (e.g. `www.file.net`). If the hosts file was changed without your knowledge, there could be a malware which redirects websites (e.g. from banks, antivirus companies) to fake web pages.

You can edit the hosts file with Windows notepad. To deactivate a redirection, simply delete the line.

**Note**
- The hosts file replaces DNS (Domain Name Service). The lmhosts file in the same folder replaces WINS, which IP addresses to computers in your LAN network.
Changing the language

Security Task Manager recognizes the used language (English, Deutsch, Espanol, ...) automatically. To change the language do the following:

1. On View menu click Language
2. Then click the language you want.

**Note**

- The software can easily be translated to any language. Simply translate the lgs_english.txt text file in the program's folder, and send it to info@neuber.com. You will receive a free registration for your translation.
- Um die deutsch Sprache einzustellen, klicken Sie hier.
Basics

Part III
III. Basics

Risk Rating of processes

Security Task Manager uses objective criteria to judge the safety risk of a process. Security Task Manager examines the process to determine if it contains critical function calls or suspicious properties. Points are allocated depending on the potential danger of these functions and properties. The sum of the points results in the Security Task Manager Risk Rating (0 to 100 points).

<table>
<thead>
<tr>
<th>Properties</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Could manipulate other programs</td>
<td>★★★★</td>
</tr>
<tr>
<td>Window not visible</td>
<td>★★★</td>
</tr>
<tr>
<td>No Windows system file</td>
<td>★★</td>
</tr>
<tr>
<td>None detailed description available</td>
<td>★★</td>
</tr>
<tr>
<td>functions: record inputs, manipulate</td>
<td>★★</td>
</tr>
<tr>
<td>Rating: potentially dangerous</td>
<td></td>
</tr>
</tbody>
</table>

Security Task Manager examines the processes looking for the following functionalities (sorting by dangerousness):

- Able to record keyboard inputs
- Hidden stealth process
- File is hidden
- Keyboard driver, could record inputs
- Could manipulate other programs
- Able to monitor Internet browser
- Starts when starting of programs
- Listen on port
- Send to port
- unknown program listens or sends
- Monitor program starts
- Window not visible
- Start when Windows starts
- No detailed description available
- Unknown file in Windows folder
- No Windows system file
- No description of the program
- functions: Internet, monitor, record inputs, hide, manipulate
- functions: not determinable
- Unknown company

Trusted properties (reduces risk):

- Microsoft signed file
- Verisign signed file
- Belongs to
- Certified by
- Own comment

Click on an above property to learn more about this.

Note

- Highly rated programs are not always dangerous; they may just contain properties typical of
some known spyware programs.

- Click the **Show system processes** button to see all internal Windows operating system processes. Windows system processes are not shown by default.

## Process types

Security Task Manager distinguishes between the following types of processes. Click **Type** on **View** menu, to see or hide the type as column in the main window.

### Software
- Program
- Taskbar icon

### DLL files
- DLL
- ShellExecute

### Internet PlugIns

- **Browser Helpers Objects**

### Driver and Services

- **device driver**
- **file driver**
- **Service (own process)**
- **Service (own process with desktop interaction)**
- **Service (shares process)**
- **Service (shares process with desktop interaction)**

Click on an above type to learn more about this.

**Note**

- Click the **Show system processes** button to see all internal Windows operating system processes. Windows system processes are not shown by default.

## Uninstalling

1. Click Start-Settings-Control panel.
2. Click **Software**.
3. Click the **Remove** button to delete Security Task Manager from your Computer.

**Note**

- You can also run uninstall.exe in the Security Task Manager directory
Protecting your computer with SpyProtector

Part IV
IV. Protecting your computer with SpyProtector

Delete traces of your Internet and computer activity

SpyProtector contains following tools to protect your computer from keylogger, spyware and trojans:

✔ Delete history
  Check this option to eliminate traces of Internet activities (cookies, cache, history, typed URLs) in Internet Explorer. You can also delete the recently used file list of programs (Word, ACDSee, PDF, WinZip, Mediaplayer, etc) and the recently used program list on the Windows Start menu.

✔ Block keyboard monitoring
  Check this option to block the redirection of all keyboard inputs to a keylogger for the current Windows session. Keyboard redirection is realized by programing a Hook function; even keyboard utilities like macro and autotext programs don't use these malicious Hook functions.

✔ Block other monitoring
  Check these options to block programs which log data for the current Windows session:

  Keyboard inputs (indirect):
  This prevents monitoring of internal Windows messages (e.g. keyboard inputs) by other programs.

  Mouse activities:
  This prevents monitoring of mouse movements and mouse clicks

  Macro:
  This prevents recording of user activities. This methode, often used by macro programs, is not typically used by keyloggers.

  Starting and ending of programs:
  Program starts and stops are logged. This function is frequently used by tutorial programs (computer based training) to aid user interaction with the software.

  Attention: Some safe and valid programs (e.g. some Macro programs) do use these Hook functions. If one of your programs stops working after selecting an option above, please deselect the option or restart your computer.

✔ Warn when your registry is changed
  Check this option to see a warning message when any program tries to create an autostart key in the Windows registry. Many dangerous programs use an autostart key in the Registry to activate themselves.
Index

- A -
  active runtime 6

- B -
  BHO 12
  Browser Helpers Objects 12

- C -
  comment 8
  CPU 6

- D -
  DLL 12
  driver 12

- E -
  end process 7
  export to 8

- F -
  file 11
  folder 7

- G -
  Google search 7

- H -
  hosts file 8

- I -
  information about processes 6
  Internet
    delete traces 14
    looking for info about process 7

  process Type 12

- K -
  keyboard 11, 14
  keylogger 14

- L -
  language change 9

- M -
  memory 6
  monitoring 11, 14

- N -
  Note 8

- O -
  Overview 4

- P -
  PID 6
  prevent surveillance 14
  print 8
  process
    comment 8
    end 7
    print 8
    properties 6
    rating 11
    types 12
  Program 12
  properties of processes 6

- Q -
  quarantine 7

- R -
  rating 11
  Registry Warner 14
remark     8
risk of process     11

- S -
save
  export     8
  print     8
Security Task Manager
  Features     4
  How to use     6
  uninstalling     12
service     12
SpyProtector     14
start     6

- T -
task     6
Taskicon     12
title     6
Type     12

- U -
uninstall     12

- W -
web information     7