

Please click **Topics** to get a list of available help topics.

Security Task Manager

Security Task Manager detects and removes spyware, trojans, keyloggers and adware.


[More information](#)

Please register Security Task Manager. Registration is easy. You can order online via the Internet, by email, by fax, by phone or by ordinary mail.

Thank you for choosing to evaluate Security Task Manager. You were free to use it for the 30 days-trial period. Now it's your turn. Please [register](#) Security Task Manager for only \$29 today!

Security Task Manager

Security Task Manager is not free software. Your 30-day evaluation period has expired. If you wish to continue using Security Task Manager, you should register for \$29 (29 Euro).

For more informationen click [here](#) 

Security Task Manager Trial version

The trial version shows you all running processes.

The full version analyses services and drivers on your computer in additional.

{button How to buy full version,JI(`taskman_en.hlp`,`Bestellen')}


With your registration you obtain additional software SpyProtector for free. Spyprotector eliminates your Internet traces, warns when Autostart key in registry is changed and disables keyboard and mouse surveillance on your computer. All minor updates are free. These are good reasons to buy Security Task Manager today.

Welcome

We thank you for your registration.

Security Task Manager will help you to find and remove unwanted software. All nag screens and shareware limitations were turned off. SpyProtector is unlocked and can now eliminate your Internet traces, warn when registry is changed and disable keyboard and mouse surveillance on your computer.

Please keep your registration key. That key will work with all future upgrades for lifetime.

If you have any questions please contact [us](#) 

Features of Security Task Manager

Security Task Manager provides advanced information about programs and processes running on the computer. For each process it shows in addition in contrast with Windows Task-Manger:

- ▶ file name and directory path
- ▶ security risk rating
- ▶ 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 recognizes also virtual driver software, services, BHO or processes hidden from the Windows task manager.

{button Using Security Task Manager,JI(`taskman_en.hlp`,`Konzept')}

{button ,AL("Info")} [Related Topics](#)

Using Security Task Manager

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

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

{button ,PI(``,`Name`)} Name
{button ,PI(``,`Bewertung`)} Rating
{button ,PI(``,`PID`)} Process ID (PID)
{button ,PI(``,`CPU`)} CPU
{button ,PI(``,`mem`)} Memory
{button ,PI(``,`Aktiv`)} Active runtime
{button ,PI(``,`Datei`)} File
{button ,PI(``,`Typ`)} Type
{button ,PI(``,`Start`)} Start
{button ,PI(``,`Titel`)} Title and Description
{button ,PI(``,`Hersteller`)} Manufacturer and Product

Click a process to obtain more information about this processor to stop it. You can:



see properties




end process



place process in quarantine



Note

- Click  **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.

{button ,AL("Info;Anleitung")} Related Topics

A process can be a program, driver, service or PlugIn - so every executed code which is active in your computers memory.

Shows name of software or name of driver.

Shows an objective and security relevant process Rating. The longer the red Rating bar, the more dangerous functions the process contains. Highly rated programs do not always have to be dangerous: They just have some typical spyware properties.

Click a process to learn more about it. Then you can assess trustworthiness of this software.

Shows the identification number of process. Each process has an unique ID.

Shows CPU (processor) usage. Active program do keep the processor more occupied than inactive processes.

Shows working memory usage.

Shows time active runtime of the process since Windows start.

Shows directory path and name of the file.

Shows file type. The file type can be a program, a system tray icon program, a Browser Helper Object, a driver or a service.

process types distinguished by Security Task Manager

.

Shows when and how did the process start.

Shows Title and file description contained in the file. For a visible window the title corresponds to the text in the windows's title bar.

Shows name of company and product description found in the file.

Process types

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

Software

{button ,PI(``,`Programm')}_Program
{button ,PI(``,`Taskicon')}_Taskbar icon

DLL files

{button ,PI(``,`DLL')}_DLL
{button ,PI(``,`ShellEx')}_SheelExecute

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  **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.

{button ,AL("Prozess")}_ Related Topics

Labels a program with a visible window or a invisible program without a window.

This is a program with an icon in system tray (left beside the watch). Right-mouse click this icon on task bar to open a context menu and to get more information.

A Dynamic Link Library (DLL) executes program code just like a program. A DLL file contains seldom used function outsourced by main program.

This file was started by a Hook using the ShellExecute command in the Windows registry. ShellExecute runs a process (almost a DLL) when any Windows program was started. This process should be examined exactly.

A Browser Helper Object (BHO) is a DLL that allows developers to customize and control Internet Explorer. Alexa, GetRight, Go!Zilla and other download manager uses a BHO. BHO's can monitor all your Internet activities. To deactivate BHO's, click in Internet Explorer on **Extras** menu **Internet Options**. Click **Advanced** tab. Under Browsing, click to clear the **Enable third-party browser extensions** check box.

Driver and Services execute system functions at lower hardware level. (available only in full version)

A service type flag that indicates a Windows NT device driver to control hardware components (e.g. graphic adapter or scanner). Some software modules (e.g. Firewall, AntiVirus) are device driver therewith users cannot close it.

A service type flag that indicates a Windows NT file system driver.

A service type flag that indicates a Win32 service that runs in its own process. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

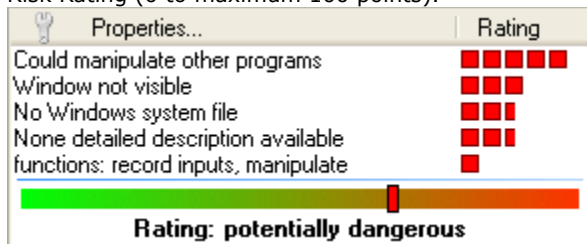
A service type flag that indicates a Win32 service (e.g. Firewall, AntiVirus) that runs in its own process and can interact with the desktop. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

A service type flag that indicates a Win32 service that shares a process with other services. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

A service type flag that indicates a Win32 service that shares a process with other services and can interact with the desktop. A Win32 service starts automatically on Windows start, is always running and doesn't depend on users.

Risk Rating of processes

Security Task Manager judges the safety relevant risk of a process after objective criteria. To this Security Task Manager examines if a process contains critical function calls or suspicious properties. Depending on potential dangerousness of these functions and properties points are allocated. The sum results in the Security Task Manager Risk Rating (0 to maximum 100 points).



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


- {button ,PI(`,` B1') } Able to record keyboard inputs
- {button ,PI(`,` B2a') } Hidden stealth process
- {button ,PI(`,` B2') } File is hidden
- {button ,PI(`,` B3') } Keyboard driver, could record inputs
- {button ,PI(`,` B4') } Could manipulate other programs
- {button ,PI(`,` BHO') } Able to monitor Internet browser
- {button ,PI(`,` ShellEx') } Starts when starting of programs
- {button ,PI(`,` B5') } Listen on port <No.>
- {button ,PI(`,` B6') } Send to <computer name> on port <No.>
- {button ,PI(`,` B7') } unknown program listens or sends
- {button ,PI(`,` B8') } Monitor program starts
- {button ,PI(`,` B9') } Window not visible
- {button ,PI(`,` B10') } Start when Windows starts
- {button ,PI(`,` B11') } None detailed description available
- {button ,PI(`,` B21') } Unknow file in Windows folder
- {button ,PI(`,` B12') } No Windows system file
- {button ,PI(`,` B13') } No description of the program
- {button ,PI(`,` B14') } functions: Internet, monitor, record inputs, hide, manipulate
- {button ,PI(`,` B15') } functions: not determinable
- {button ,PI(`,` B16') } Unknown manufacturer

Trusted properties (reduces risk):

- {button ,PI(`,` B17') } Microsoft signed file
- {button ,PI(`,` B18') } Verisign signed file
- {button ,PI(`,` B20') } Belongs to <software product> from <manufacturer>
- {button ,PI(`,` B19') } Certificated by <registrar> for company <manufacturer>
- {button ,JI(`taskman_en.hlp>Proc1',` Kommentar') } Own comment

Click on an above property to learn more about this.

Note

- Highly rated programs do not always have to be dangerous: They just have some typical spyware properties.
- Click  **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.

{button ,AL("Bewertung")} Related Topics

This property doesn't seem to be critical. To learn more about the process please use the [Internet search](#).

The process monitors each keyboard input. This is realized by a Hook function. Serious programs don't use this Hook function.

To prevent keyboard surveillance

The process hides from the Windows Task Manager by API Hooking. It's not visible in any process viewer. We recommend that you quarantine it.

The file hides from the Windows Explorer. Please not mistake for the harmless file attribute "hidden".

It is a keyboard driver and can read every keyboard input you make.

The process can manipulate any programs or Windows operation system. A Hook is set for this one. A Hook is a Windows internal function that can feign a forged file list for example. This manipulates the dir command. Thus the program (that starts the process) is not visible for other programs like AntiVirus software.

The process can receive information from the Internet. Hackers use such leaks to take control over such computer. You can prevent such attacks with a good firewall.

The process connects to the named computer or IP address and can send any information to this. You can prevent such connections with a good firewall.

A port was opened to receive or send information over network or Internet. Please find out which program it is. You can prevent such connections with a good firewall.

The process monitors when which programs are started or closed.

The program doesn't have any visible window and runs in the background. In the most favorable case, e.g. it is device driver software.

The program is started at every Windows start because it wrote a autostart key in the registry.

Warning when Registry is changed

Some important standard descriptions in the file were not found. Every file contains internally fields for descriptions by default.

The file is not a part of the Windows operating system. The file was copied into the Windows directory, but was not registered correctly. Reason could be a bad programmed software or the file tries to hide in the windows folder.

Please be careful if you cannot assigned the file to any installed software product or hardware driver.

The file is not a part of the Windows operating system. Please be careful if the file is in the Windows directory and it cannot be assigned to any installed software product or hardware driver.

Descriptions were not found in the file. Every file contains internally fields for descriptions by default.

The file contains function calls with the named properties. But this hasn't much influence on the Rating, since there is no evidence if this function comes in action.

No dangerous function calls were found in the file. But these could be integrated hiddenly.

The software manufacturer cannot be found in file description fields. Every file contains internally fields by default to name the software developer.

This file was signed by Microsoft. You can trust this file like you also trust Microsoft.

This file was signed by VeriSign. You can trust this file like you also trust VeriSign.

This file was signed by a registrar. You can trust this file like you also trust this registrar and the software manufacturer.




You can trust the file. It's a part of the mentioned and installed software. When you deinstall that software, the file will be removed too.

Viewing process details


Click on a [process](#) to see more information about this process. Following properties are shown:

{button ,PI(``,`Name`)} [Name](#)
{button ,PI(``,`Bewertung`)} [Rating](#)
{button ,PI(``,`Hersteller`)} [Manufacturer](#)
{button ,PI(``,`Titel`)} [Description](#)
{button ,PI(``,`Typ`)} [Type](#)
{button ,PI(``,`Start`)} [Start](#)
{button ,PI(``,`Datei`)} [File](#)
{button ,JI(`taskman_en.hlp>Proc1`,`Kommentar`)} [Comment](#)

Receive further information or stop the process:


 [Information from the Internet about a process](#)
 [Ending process](#)
 [Putting in quarantine](#)

Note

- Click  **Windows processes** button to see also all Windows internal processes. These processes belong to Windows operation system. Windows system processes are not shown by default.
- Click on **View** menu to chose which properties are shown as column in the main window.

{button ,AL("Prozess")} [Related Topics](#)

Ending a process

- 1 Click on a process you want to close.
- 2 Click the button  **Remove**.
- 3 Then select one of following options:
 {button ,PI(``,`Name`)} [End process](#)
 {button ,PI(``,`Bewertung`)} [Move file to quarantine](#)



Note

- Ending a process can cause system instability, including crashes. Software that needed Adware programs could not work. Please save opened documents.

{button ,AL("Prozess")} [Related Topics](#)


The process will be removed from the memory. If the process wrote a own autostart entry in the Registry (Windows configuration data base), then it is however active again at the next Windows start.

The process will be removed from the memory too. In addition Security Task Manager put the corresponding file into quarantine folder and deletes corresponding Autostart entries in Registry. File and registry entries are saved. Thus you can restore the process at any time.

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 a isolated folder. Corresponding Autostart keys in Windows registry are deleted. Thus the process cannot be started again. Restoring the whole process is possible at any time:


Restoring processes

- 1 Click  **quarantine** button on tool bar.
- 2 In quarantine folder click on process you want to restore.
- 3 Click **Restore** button.

{button ,AL("Beenden")}

[Related Topics](#)

Learning more about a process

- 1 Click on a process you want to examine.
- 2 Click  **Google** button on tool bar.

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



Note

- Your Internet Browser transmits information (e.g. operating system, language setting). Neither the program Security Task Manager nor one of his components make a connection to the Internet.
- Google.com is one of the most used search engines provides you with good results.


{button ,AL("Prozess") } [Related Topics](#)

Exporting process list

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



Note


- Click  **Windows 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 process list from time to time. Thus you can find new processes. A saved process list can serve as exhibit.

{button ,AL("Speichern")} [Related Topics](#)

Printing process list

- 1 On File menu click **Print**.
- 2 Chose a printer and perhaps necessary properties (e.g. duplex print).

Note

- Click  **Windows processes** button to see also all Windows internal processes. Then you be able to print Windows processes too. Windows system processes are not shown by default.

{button ,AL("Speichern")}

[Related Topics](#)

Writing a comment

You can write a own remark to each process. This is 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 appearing context menu.
- 3 Enter you comment and your opinion about the process.

{button ,AL("Shareware")} [Related Topics](#)

Protect your computer with SpyProtector

Buy Security Task Manager today and get the software SpyProtector for free. SpyProtector contains following tools to protect your computer from keylogger, spyware and trojans:



-  Deletes traces of your Internet and computer activity
-  Prevents keyboard input monitoring
-  Prevents mouse activities monitoring
-  Prevents software usage monitoring
-  Warning when registry is changed

{button Buy Security Task Manager Now,JI(`taskman_en.hlp`,`Bestellen')}

{button ,AL("Shareware")} Related Topics

SpyProtector can neutralize mouse monitorings programs for the current Windows session. The surveillance of your mouse movements and clicks by keyloggers is blocked.

SpyProtector can neutralize programs which log starting and ending of any programs for the current Windows session.

Protecting your computer with SpyProtector

To run SpyProtector, click icon in the system tray of your task bar.



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



Delete history

- ✓ Block keyboard monitoring
- ✓ Block other monitoring
- ✓ Warning when registry is changed

{button ,AL("Schutz")} Related Topics

Check this option to block most of keyloggers for the current Windows session. The redirection of all keyboard inputs over an keylogger is blocked. Such a keyboard redirection is realized by programing a Hook function. Even keyboard utilities like macro and autotext programs don't use such dirty Hooks.

Check on of these options to block programs that log following 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. That method often used by macro programs is not usual for keyloggers.

Starting and ending of programs

Program starts and ends are logged. This function is frequently used by tutorial programs (CBT) to the interaction with the software to be learned.


Attention: Some serious programs (e.g. some Macro programs) use these "dirty" Hook functions. If such a program shouldn't work any more, then unselect the corresponding option or restart your computer.

Check this option to eliminate the traces of Internet activities (cookies, cache, history, typed URLs) in InternetExplorer. You can furthermore delete the recent used file list of programs (e.g. Word, ACDSee, PDF, WinZip, Mediaplayer) and the recent used program list of Windows Start menu.

Check this option to get a messagebox if a program tries to write its name on the Windows registry as autostart key. The software is started with such an key secretly at every Windows start. All dangerous programs need such an key to be active at a computer restart!


Changing the language

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

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



Note

- The software can be easily 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](#) .

{button ,AL("Sprache")}

[Related Topics](#)

Adding a language file

You can download additional language files at  www.neuber.com/taskmanager.

- 1 Go to www.neuber.com/taskmanager.
- 2 Here you can see all available languages.
- 3 Copy the latest version in the Security Task Manager directory. for example c:\program files\Security Task Manager
- 4 Change the language and then run Security Task Manager.



Note

- The German and English language files lgs_deutsch.txt and lgs_english.txt are contained by default.

{button ,AL("Sprache")} [Related Topics](#)

Contacting the Security Task Manager Team

Technical Contact:

address: Alexander and Matthias Neuber GbR
PF 11 05 25
D-06019 Halle
Germany
fax: (+49) 0700-11 777 000
Internet:
WWW: www.neuber.com/taskmanager
email: info@neuber.com

The registration is executed by the international registration service ShareIt (Greensburg/U.S.A, Köln/Germany, London/UK, Roissy/France, Upplands Väsby/Sweden).

Eine deutsche Version erhalten Sie unter <http://www.neuber.com/taskmanager>

{button ,AL("Info;Shareware")}[Related Topics](#)

Remarks about the shareware version

Security Task Manager is distributed as shareware. Shareware is a distribution method based on honor, and is not a type of software. You are free to use it for a trial period of up to 30 days. If you find this program useful and would like to continue using Security Task Manager, then you are required to [register](#) for \$29 (29 EUR). You will receive a registration code that you can use to [unlock the shareware](#). The registration code will turn off all nag screens and shareware limitations, and work with future minor updates.

As a registered user, you will get:

- legal license for the software
- your personal key to unlock trial version
- free minor updates
- free software SpyProtector
 - Spyprotector eliminates your Internet traces, warns when Autostart key in registry is changed and disables keyboard and mouse surveillance
- [free technical support \(via email or mail\)](#)

On **Help** menu click **Info...** to see whether your version is registered.

{button ,AL("Team;Shareware")}[Related Topics](#)

Get Security Task Manager now!

Order your own registration code for **\$29** (29 EUR) from our distributor ShareIt today! ShareIt accepts credit cards, bank/wire transfer, checks or cash.

You can order by



Internet:

[Secure Order Form](#)



mail/fax:

[Order Form](#)



phone:

+1-800-903-4152 (orders only)
+1-724-850-8186 (ShareIt customer support)
+49-221-3108820 (ShareIt Germany)
+33-1-491926-54 (ShareIt France)
program ID: 174510



Notes

- If you pay by credit card, you'll receive the registration code immediately. The code unlocks the shareware.
- If you have questions about the program please ask developer.
- If you have questions about ordering please ask: ShareIt! Inc., PO Box 844, Greensburg, PA 15601-0844, U.S.A., phone: 724-850-8186, support@shareit.com (ShareIt has further offices in U.S.A, Germany, UK, France and Sweden)

{button ,AL("Shareware;Team") } [Related Topics](#)

Compra Security Task Manager!

Ordenar hoy su código de registro para **29 EUR!**

You can order by



Internet:

[presione la licencia deseada](#)



mail/fax:

[Formato de Orden](#)



telefónica:

+49-221-3108820 (sólo ordenes)

número: 174510



Notas

- Después de registrarse, Ud. Recibirá por email, fax o correo postal su código de liberación en un lapso de 24 horas. Si Ud. Se registra en línea y paga con tarjeta de crédito, recibirá el registro inmediatamente.
- El código de registro será válido también para todas futuras actualizaciones.

{button ,AL("Shareware;Team")} [Related Topics](#)

Achetez Security Task Manager

Commander votre code d'installation encore aujourd'hui pour **29 EUR!**

Commander simplement par



Internet:

[Commande en ligne](#)



courrier/fax:

[Bon de commande](#)



téléphone:

+33-1-491926-54 (ShareIt France)

+1-800-903-4152 (orders only)

+1-724-850-8186 (ShareIt customer support)

+49-221-3108820 (ShareIt Allemagne)

N° commande: 174510

Vous recevrez votre code d'installation immédiatement (en cas de commande en ligne avec une carte de crédit) ou dans les 24 heures après réception de votre paiement. Vous transformerez votre partiel en produit complet avec votre code d'installation. Le code d'installation est valable pour toutes les versions de Security Task Manager.

Notre vendeur en France:

element 5 AG / ShareIt!
Le Dôme, BP 10910
1, rue de la Hayey
95731 Roissy CDG Cedex
France

Téléphone : +33 (0)1 49 19 26 54
Télécopie : +33 (0)1 49 19 21 00
ventes@element5-france.com

{button ,AL("Shareware;Team")} [Related Topics](#)

Switching the shareware to a registered version

- 1 On **REGISTER** menu click **Unlock the shareware version**.
- 2 Enter the Name and Code in the registration dialog **exactly** as shown in the information sent to you.
- 3 Click **Unlock**.



Notes

- If you have question please ask [us](#).
- You can [order](#) your registration code for \$29 (29 Euro).

{button ,AL("Shareware")}[Related Topics](#)

Uninstalling Security Task Manager


- 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 `uninstal.exe` in the Security Task Manager directory

Enter the code in the registration dialog **exactly** as shown in the information sent to you. Then click Unlock to switch the shareware version to a registered version.

For more information click [here](#) .

