

Network Security Task Manager

User Guide



This software indicates the hazard potential of active processes in the computers on your network.

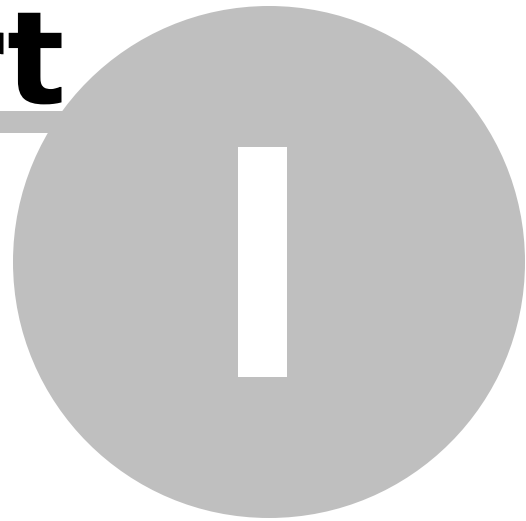
Table of Contents

Part I Welcome	5
Part II Installation	7
System requirements	7
Installation of core components	8
Agent distribution	9
Part III Configuration	11
Managing computers	11
...Adding computers	11
...Grouping computers	12
...Displaying computer properties	13
...Shutting down a computer	14
...Removing computers	14
Scheduling	15
Warning about dangerous processes	17
Hiding harmless processes	18
Reference database of known processes	18
...What is the reference database for?	18
...Adding processes to the reference database	19
...Removing processes from the reference database	20
Part IV Tasks	22
Scanning the active processes on a computer	22
Saving the list of processes	22
Printing the list of processes	22
Displaying process properties	23
Displaying other properties (Google search)	24
Viewing the process log	24
Stopping a process	25
Quarantine folder	25
Part V Basics	27
Risk ranking of processes	27
Process types	29
What is NetTaskTray	30
Admin\$ share	31
Simple File Sharing	32

Scanning a Windows 8/7/Vista pc	33
Microsoft network communication security	34
Files and processes used	35
Uninstalling all of the software	36
Part VI Troubleshooting	38
Resolving connection errors	38
Viewing the error log	40
Scheduling / warning not working	41
Error messages	42
...Finding the cause of the error by using the error message	42
...Connection errors	42
...Multiple SMB connections	44
...No Admin rights	45
Technical support	46
Part VII MSI package software distribution	48
Overview	48
Creating the MST file	49
Creating a shared folder	52
Group policy software distribution	54
Uninstalling an MSI package	67
Index	68

Welcome

Part



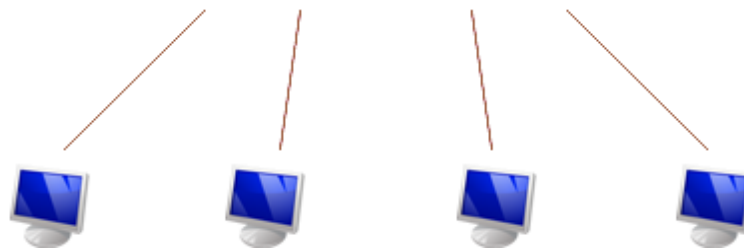
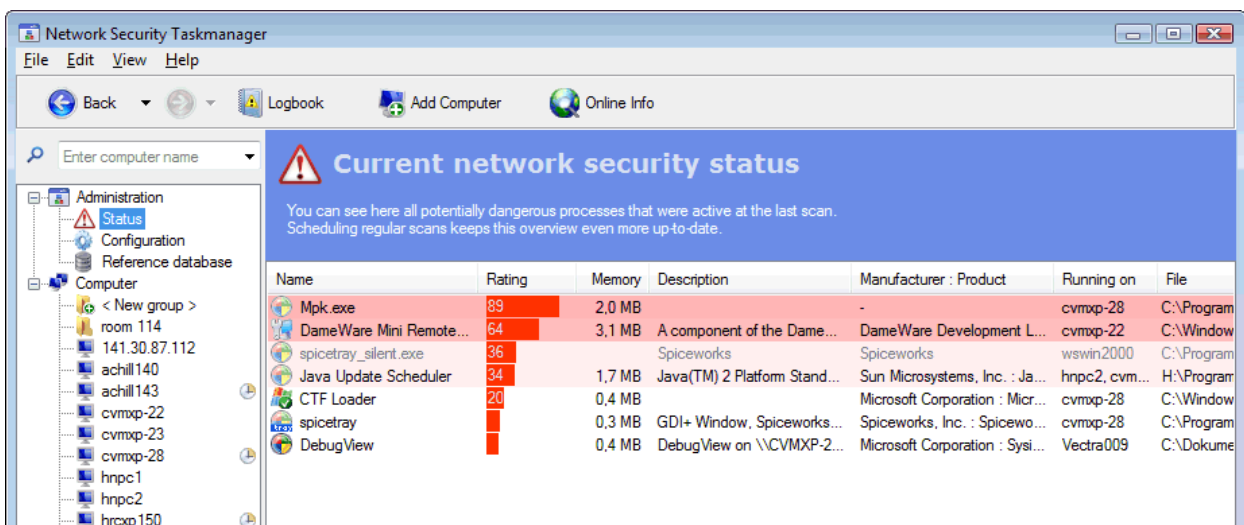
I. Welcome

Network Security Task Manager shows you all active processes on the computers in your network. Based on the [risk rating](#)^[27] you can determine which safety-critical functions are included in the processes.

Network Security Task Manager has two components:

Management Console

The Management Console centrally manages all monitored computers. The administrator can consequently scan computers, make schedules and view reports.

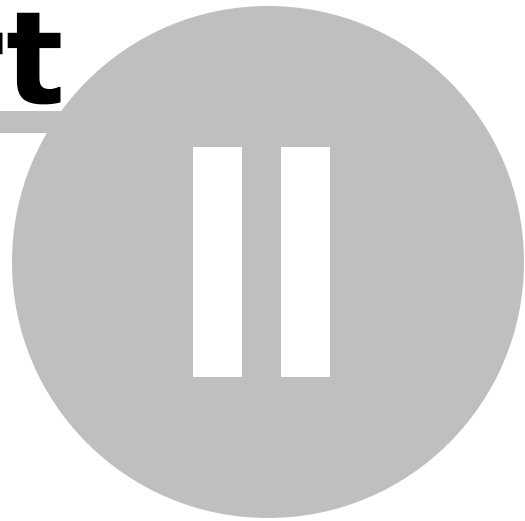


Workstation component

A software agent is started as a service on the computers. Upon being ordered by the management console, the agent analyzes the active processes of the computers.

Installation

Part

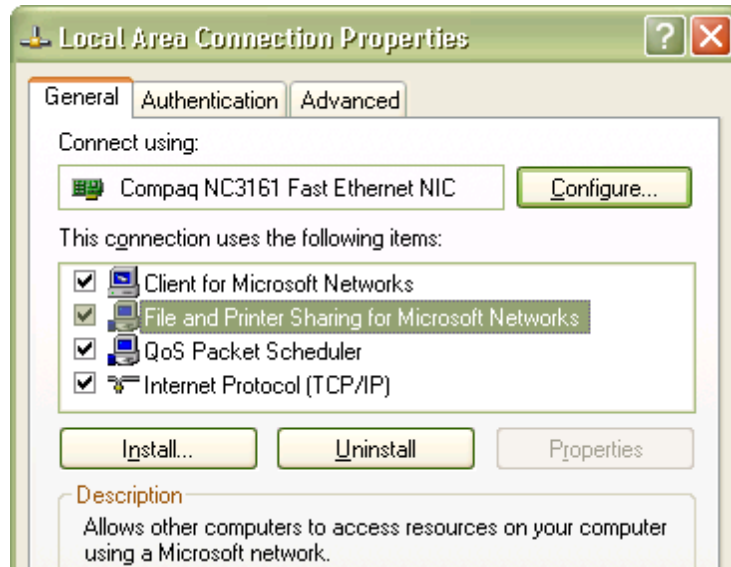


II. Installation

System requirements

General:

- Windows 8, 7, Vista, 2000, XP Professional, Windows Server
- ▼ File and Printer Sharing (enabled by default)
 - Because *Network Security Task Manager* uses the SMB protocol for communication between the management console and workstation components, the following applies to all computers:
 - Activate "File and Printer Sharing for Microsoft Networks"
 - Firewall exception for TCP port 445 (File and Printer Sharing)



Network Security Task Manager operates independently of already existing security software. Firewall or antivirus software from other manufacturers does not need to be uninstalled.

Management console:

- Approx. 4 MB hard disk space
plus 100 KB per monitored workstation

Workstation component:

- less than 1 MB hard disk space
- Admin share [Admin\\$](#)^[31] enabled (enabled by default)
- if the computer does not belong to a domain: [Simple File Sharing](#)^[32] disabled

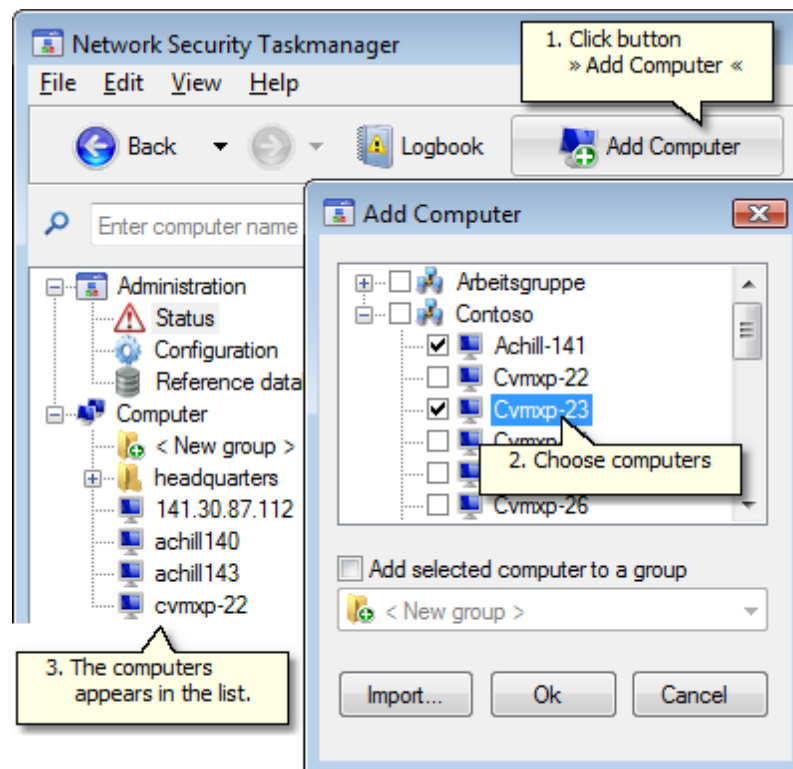
Note: If you can access the computer to be scanned using Windows Explorer as follows, *Network Security Task Manager* will also work.



Installation of core components

The management console can be installed for each user account.

1. Download the latest version from <http://www.neuber.com/network-taskmanager/download.html>
2. Install *Network Security Task Manager*.
3. Then open the management console (Start > All Programs > Network Security Task Manager).
4. Click on **Add Computer**.
The computer names are added to the computer list of the console. Nothing is installed or configured on the computers.



The installation of *Network Security Task Manager* is now complete.

You can now:

- [scan computers](#)^[22],
- [define groups of computers](#)^[12],
- [make schedules](#)^[15],
- [be warned about potentially dangerous processes](#)^[17],
- [include trustworthy programs as known in the reference database](#)^[18].

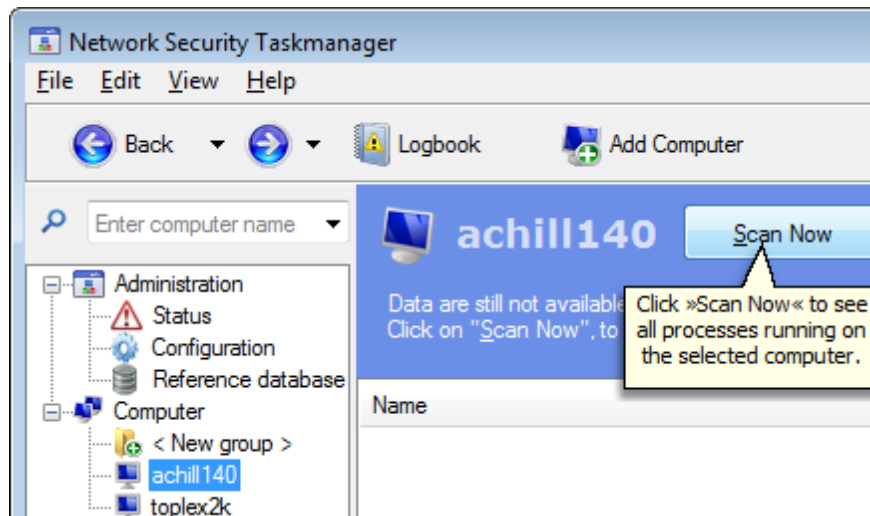
Note

- The management console can additionally be installed on more computers, in order to manually scan any clients. However, no scheduling of the type *At the start of a process* or *After a client boots* can be defined for these clients by another management console.
- If you wish to update the management console, then simply install the latest version on top of your existing installation.

Agent distribution

You do not need to worry about the distribution of the agents in your network:


If you are scanning a computer by using the management console, a remote agent will automatically be installed on this computer. This agent analyzes the active processes and transmits the encrypted data to the management console. After the scan this agent will be removed.








The management console temporarily installs the agent in the network share "ADMIN\$" of the selected computer.

With a [schedule](#)^[15] the computer can be scanned regularly.

Upon using the schedule settings *At the start of a process* and *After a client boots* the agent will be permanently installed. If you deselect this option again, then the agent will be uninstalled.

An advantage of scheduling: In  **Status** you can always see the current security situation of all the computers.

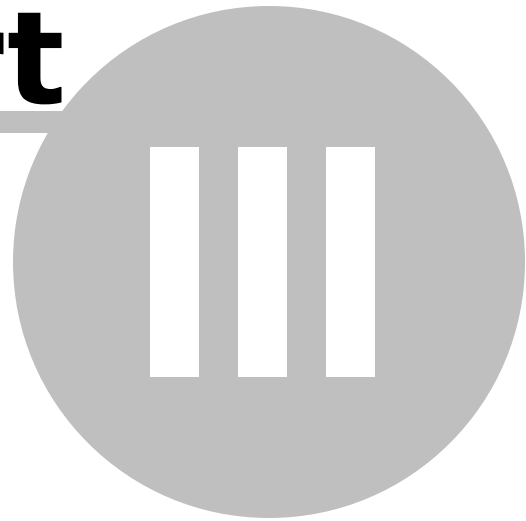
 Current network security status				
You can see here all potentially dangerous processes that were active at the last scan. Scheduling regular scans keeps this overview even more up-to-date.				
Name	Rating	Description	Manufacturer	Running on
 MPK.exe	89	Mini Remote Control	-	vxp-23
 spiceworks.exe	74	A component of ...	spiceworks	vmxp-28
 KGB Monitoring	29	KGB Keylogger	-	vxp-23
 spicetray		GDI+ Window, Spice ...	Spiceworks, Inc.	vmxp-28

Note

- To review, update or remove agents on a computer, click with the right mouse button on the desired computer. Now click on **remote agent** ▶.
- For the distribution of workstation components in large networks, an [MSI-Package](#)^[48] is also available.
- The agent only requires 300 KB on the workstation. A cache of up to 1 MB may also be reserved.

Configuration

Part

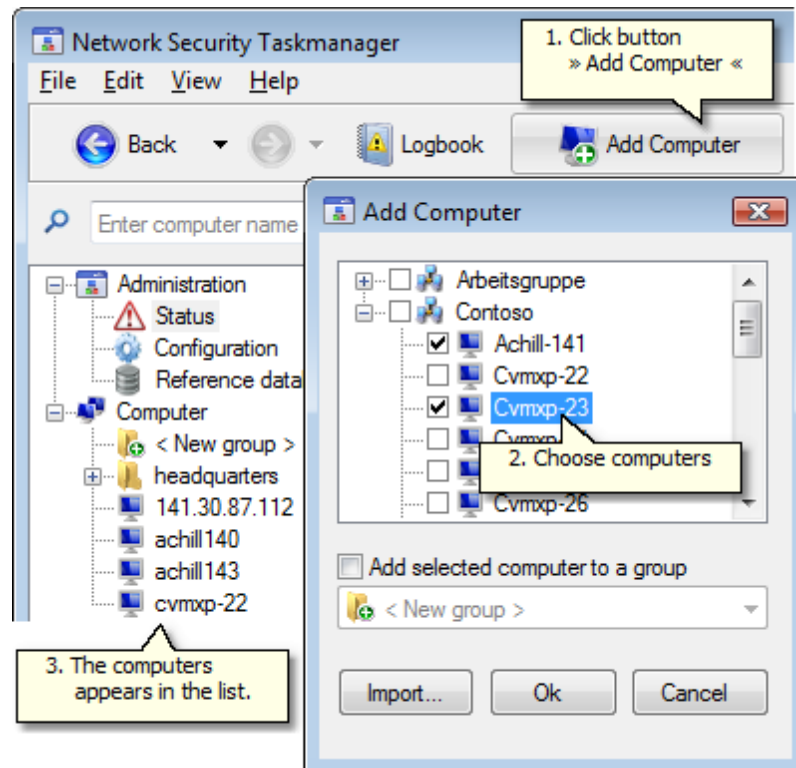


III. Configuration

Managing computers

Adding computers

After the launch of Network Security Task Manager, you can see all the computers that you can scan. To add more computers, click on **Add a computer** in the toolbar.



Alternatively you can type into the field the computer or the computer's IP address.

Nothing is installed on the newly added computer.

You can now scan the newly added computer [manually](#)^[22] or by using a [regular schedule](#)^[15].

Note

- Click on **Import ...** to add computer names from a text file to the computer list. Each line should begin with the name of a computer. After a semicolon, comma or tab character the remaining text is ignored.
- A remote agent will only be installed permanently on computers that have the schedule settings *At the start of a process* or *After a client boots*.
- A computer can be included in different groups simultaneously.

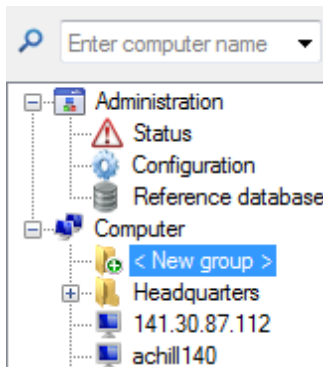
Grouping computers

You can combine multiple computers in a group. The same settings, e.g. same scheduling, will then apply to all the computers in this group.

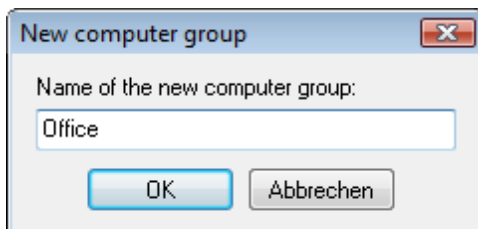
Groups may be formed according to different selection criteria. Like this, you can group together all the computers in the same building, with the same safety requirements or similar to the existing Active Directory structure.

To create a new group

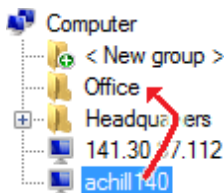
1. Click on **<New Group>**.



2. Enter a distinctive name for the group.



3. Drag the desired computer onto the group.



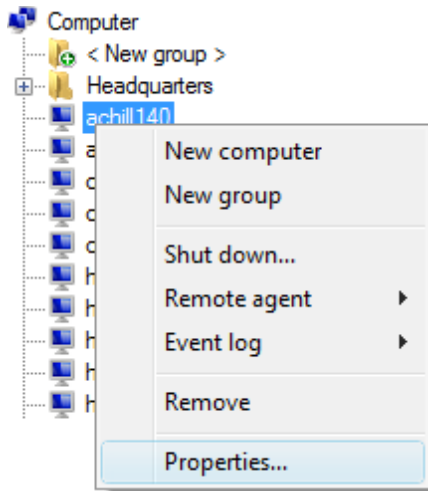
4. To add a computer to a group that is not yet listed in the management console, click on **Add Computer**. Then select the new computer and the desired group.

Note

- To delete a group, click the right mouse button on it. Then click on **Remove**.

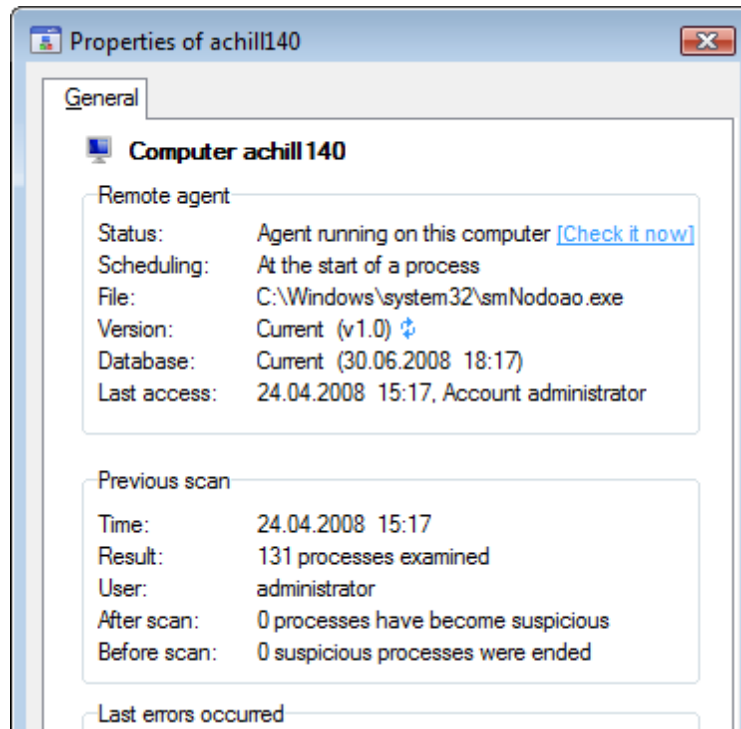
Displaying computer properties

To see all the information about a computer, click on this computer with the right mouse button. Then click on **Properties**.




You can now see for this computer:

- whether the agent is installed permanently,
- whether scheduling is defined
- the date and outcome of the most recent scan

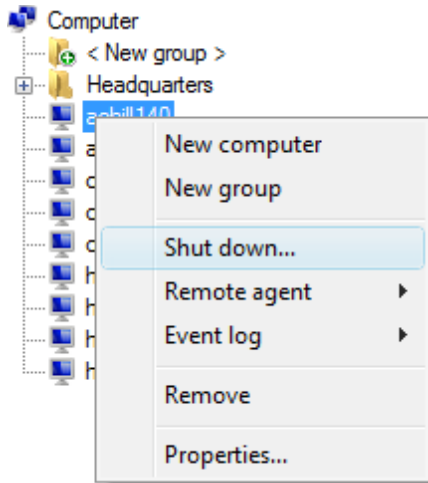


Note

- Upon using the schedule settings *At the start of a process* and *After a client boots* the agent will be permanently installed on a computer. Click on  next to the version information to update the agent file.

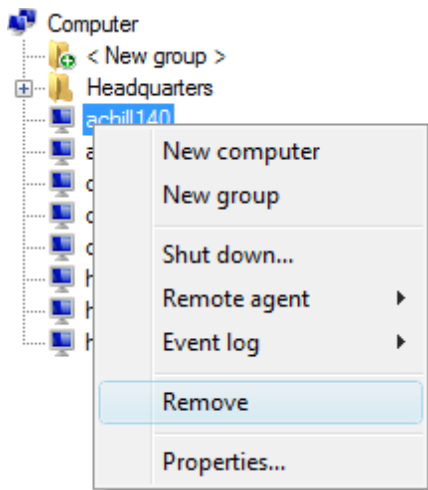
Shutting down a computer

To switch a computer off, click on it with the right mouse button. Then click **off....**



Removing computers

To remove a workstation or a computer group from the list of computers of the management console, click the right mouse button on them. Then click on **Remove**.



If the remote agent is installed on the computer, then it will be automatically stopped and removed. This is the case for computers with the schedule settings *At the start of a process* or *After a client boots*.

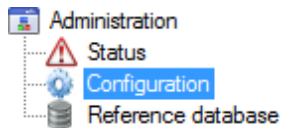
If the remote agent was distributed to the computer by [MSI-Package](#)^[48], un-installation should also be done via MSI. The same applies to your system management software, group policies, etc.

Scheduling

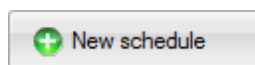
Network Security Task can automatically scan computers or groups of computers at specific times. To do this, you simply create a schedule. Each group or each standalone computer can have one defined schedule.

Creating a schedule

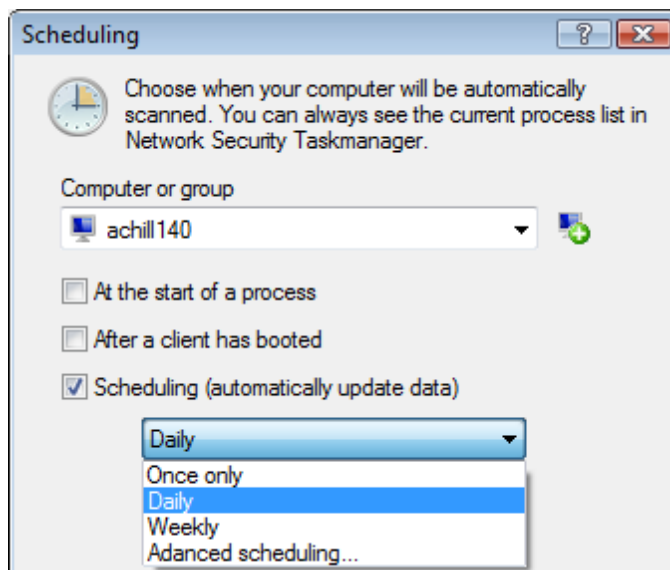
1. Click on **Configuration**.



2. Click on **New Schedule**.



3. Select the desired computer. If you select a computer group, then the schedule will apply for all the computers in this group.



4. Select a schedule type:

- At the start of a process**
 Each new process launched on a workstation is checked (on access). If the process is [potentially dangerous](#)^[17], this is reported to the management console and the administrator is warned.


If you choose this option, Network Security Task Manager then installs a remote agent permanently on the selected computer. The remote agent will only be uninstalled if you choose another option or if you delete the schedule for this computer.

- After a client boots**
 After a computer boots, all the active processes are scanned. In particular you can see new Autostart programs.

If you choose this option, Network Security Task Manager then installs a remote agent permanently on the selected computer. The remote agent will only be uninstalled if you choose another option or if you delete the schedule for this computer.


 Once-only

At the chosen time and date, the computer is scanned by the management console. To do this, a remote agent is temporarily installed on the selected computer. The agent scans the processes that are active at this time and transmits the encrypted results to the management console. The remote agent is then uninstalled again.

 [NetTaskTray](#)^[30] must be active in the system tray of the task bar, so that a computer can be scanned at the predefined time. Otherwise (for example, when the Network Security Task Manager user is not logged in at the scanning time) a query is displayed when the Network Security Task Manager then starts again, as to whether the scan should now take place.


 Daily

The computer is scanned by the management console at the set time every day. To do this, a remote agent is temporarily installed on the selected computer. The agent scans the processes that are active at this time and transmits the encrypted results to the management console. The remote agent is then uninstalled again.

 [NetTaskTray](#)^[30] must be active in the system tray of the task bar, so that a computer can be scanned at the predefined time. Otherwise (for example, when the Network Security Task Manager user is not logged in at the scanning time) a query is displayed when the Network Security Task Manager then starts again, as to whether the scan should now take place.

 Weekly

The computer is scanned by the management console on the set day every week. To do this, a remote agent is temporarily installed on the selected computer. The agent scans the processes that are active at this time and transmits the encrypted results to the management console. The remote agent is then uninstalled again..

 [NetTaskTray](#)^[30] must be active in the system tray of the task bar, so that a computer can be scanned at the predefined time. Otherwise (for example, when the Network Security Task Manager user is not logged in at the scanning time) a query is displayed when the Network Security Task Manager then starts again, as to whether the scan should now take place.


 Advanced scheduling **Note**

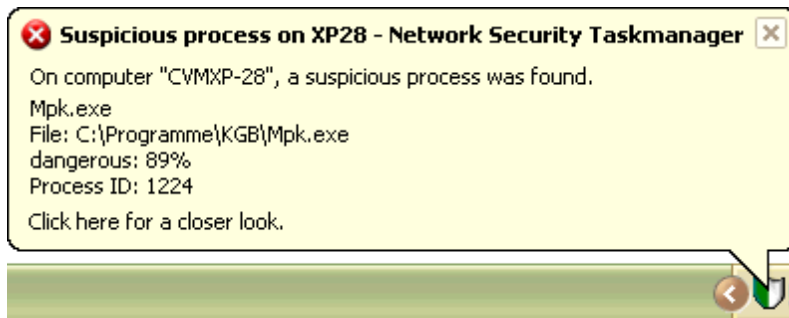
- If you have defined *At the start of a process* or *After a client boots* in the schedule, then file and printer sharing must be enabled on the computer, on which the management console is running. When these two schedules are used, the management console is [informed](#)^[17] if a potentially dangerous process has been found.
- If you have defined Daily/Weekly/One-Off in the scheduling, then [NetTaskTray](#)^[30] must run in a user account that has Admin rights on the computer to be scanned. If not, then the management console must run continuously.

Warning about dangerous processes

If a potentially dangerous process is recognized on a computer in the network, then the administrator is warned in different ways:

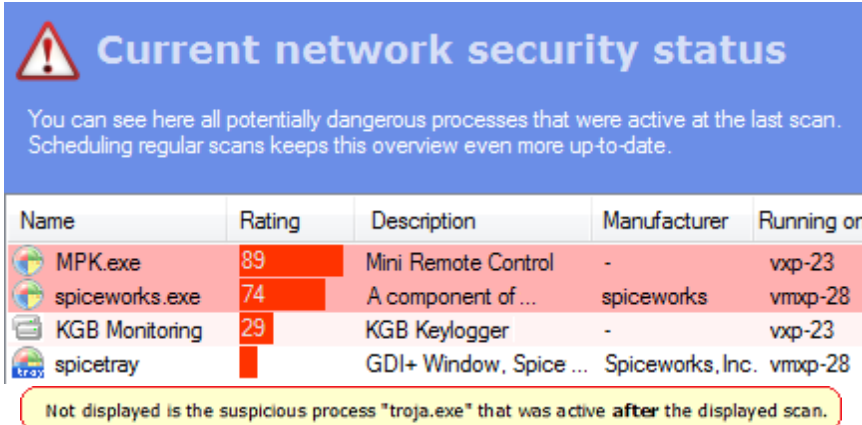
- ☐ Popup window on the Admin PC





 [NetTaskTray](#)^[30] displays a warning as a pop-up window when a potentially dangerous process has been found.



- ☐ "Status" column

The process is listed  in **Status**.



Name	Rating	Description	Manufacturer	Running on
 MPK.exe	89	Mini Remote Control	-	vxp-23
 spiceworks.exe	74	A component of ...	spiceworks	vmxp-28
 KGB Monitoring	29	KGB Keylogger	-	vxp-23
 spicetray		GDI+ Window, Spice ...	Spiceworks, Inc.	vmxp-28

Not displayed is the suspicious process "troja.exe" that was active after the displayed scan.

Reference is made in the yellow line at the end of the process list to potentially dangerous processes which were started after the scan that is being presented. This functionality is only available if the scheduling option [At the start of a process](#)^[15] has been set for the client computer.


- ☐ Process log

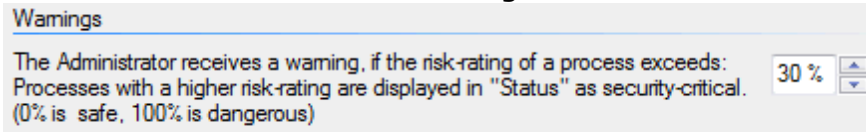
The process is registered in the [process log](#)^[24] (logbook). In this log, you can see all the past alerts that occurred.

- ☐ Local event log of the client computer

The process is registered in the local event log of the computer workstation and is displayed with the Event Viewer [eventvwr.exe](#) or your system management software. The event ID is: 150

Specifying at what level the administrator is warned

1. Click on  **Configuration**.
2. Define a new level of risk in the **Warnings** area.



All processes with a higher risk ranking than this are now considered potentially hazardous..

Note


- You can [classify](#)^[19] a process as harmless. In that case you will no longer be warned in the future in this process .

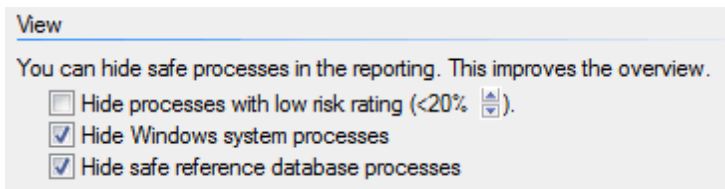
Hiding harmless processes

Having many processes soon makes a process list confusing. Therefore, it is sometimes useful to hide the following processes :

- Processes that belong to the Windows operating system
- Processes that you personally have defined as safe in the [Referencedatabase](#)^[18]

How to determine what processes will not be displayed:

1. Click on  **Configuration**.
2. Decide which processes should not be displayed.




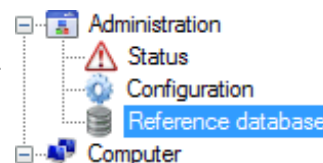
Note


- If you hide operating processes, applications such as explorer.exe are still displayed.


Reference database of known processes

What is the reference database for?

In the  **Reference Database** you save the processes that are known to you. You can attach comments to each process and classify it in one of the following categories of risk:



-  **Dangerous processes**
can be malicious software (spyware, trojans) or unwanted programs (games, adware, filesharing). Potentially dangerous processes will always receive a risk ranking of 100% (maximum risk category). The administrator is thus always warned if such a process is running on a workstation.


-  **Neutral processes**
You have written a comment on these processes. However, these processes were not ranked by you as *potentially dangerous* or *dangerous*.


-  **Harmless processes**

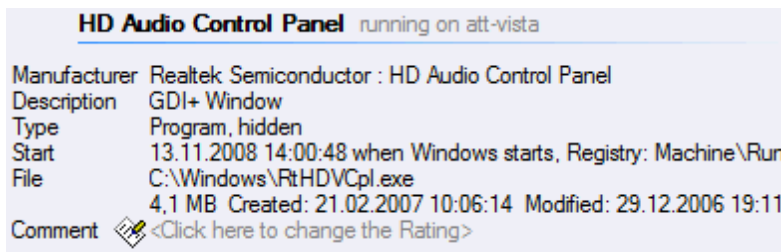
are e.g. Windows system processes, graphics drivers, firewall, antivirus and other trustworthy programs. If you classify a highly ranked process as not dangerous, in the future you will no longer be warned if the process is running on a workstation.

The reference database is therefore an overview of all processes that you have commented or whose risk ranking you have changed. With a revised [risk ranking](#)^[27] you are either *always* or *no longer* warned if the process is scanned.

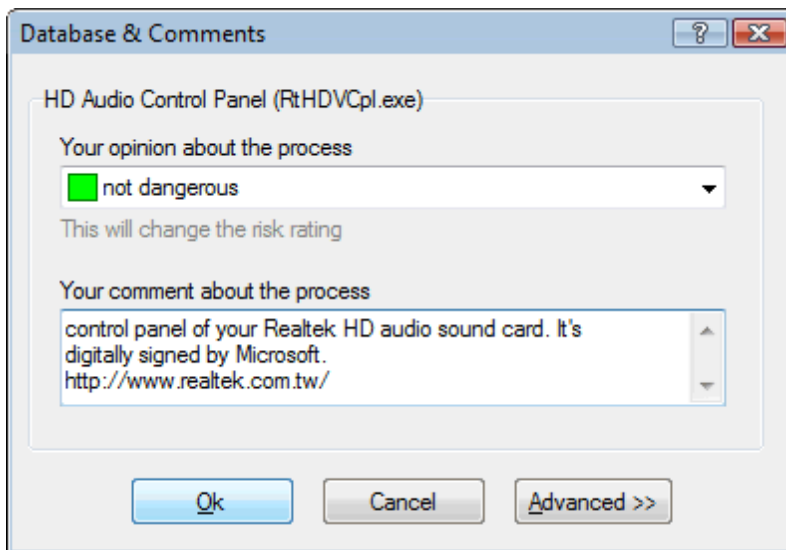
Adding processes to the reference database

You can add any processes, which you see in the process list of a computer or a computer group, to the  **Reference database**.

1. Click on the process, which you want to include in the reference database.
2. Click on the red ranking beams of the process *or* in the lower part of the program window on **Comment** .

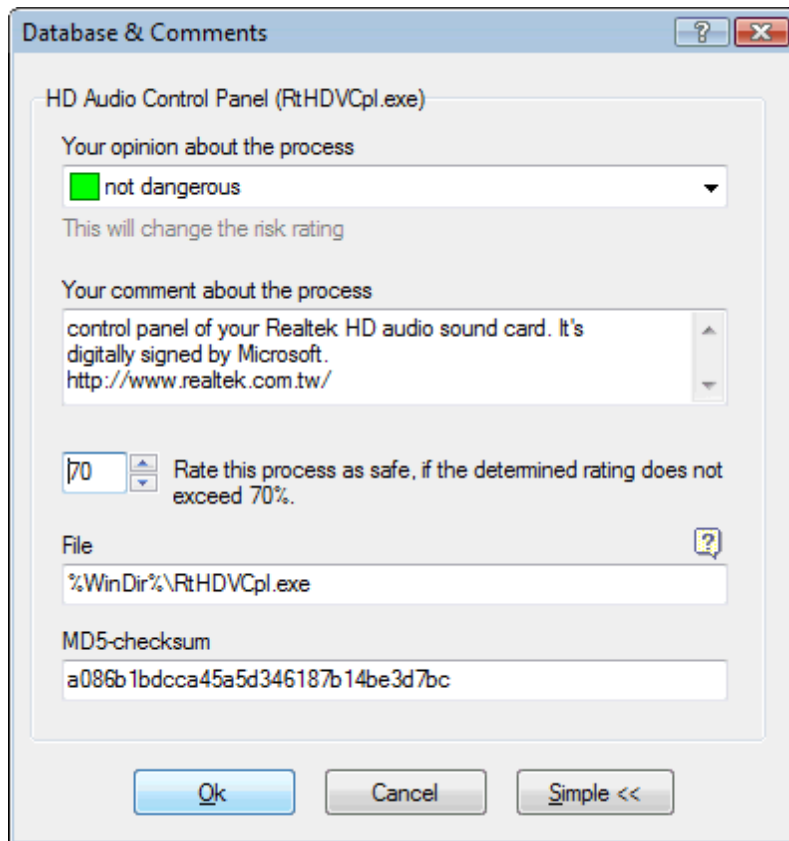


3. Enter a comment (for example, what you know about the process).



4. Optionally, you can rank the process as neutral, [dangerous](#)^[18] or [safe](#)^[18].
5. Click on **Advanced** to make a specific risk ranking (e.g. 70%), at which the administrator should be warned. Dangerous processes always have a 100% risk ranking. You can also use another name, by which the process should be displayed in the future.

Network Security Task Manager identifies the processes by their hash value (unique MD5 checksum). If a process in the reference database that has been ranked as harmless is replaced by a dangerous process, then the Administrator is warned.



Note

- If you always want to be warned when a file, e.g. redgrouse.exe, is executed on a computer, then delete the **MD5** field and in the **file name** field, write only: redgrouse.exe. This is possible because processes are identified by a file name, if the MD5 field is empty.
- Filter order: Dangerous database entries take precedence over safe database entries.
- Sorting order: To change the name of the process or manufacturer displayed, click with Shift on the button marked "Advanced>>".

Removing processes from the reference database

1. Click on the **Reference database** with the right mouse button, on the process that you want to delete.
2. Click on **Remove**.

Note

- If you delete a process in the reference database, you delete "only" your comments and your risk ranking of this process. The actual process will not be affected.

Tasks

Part

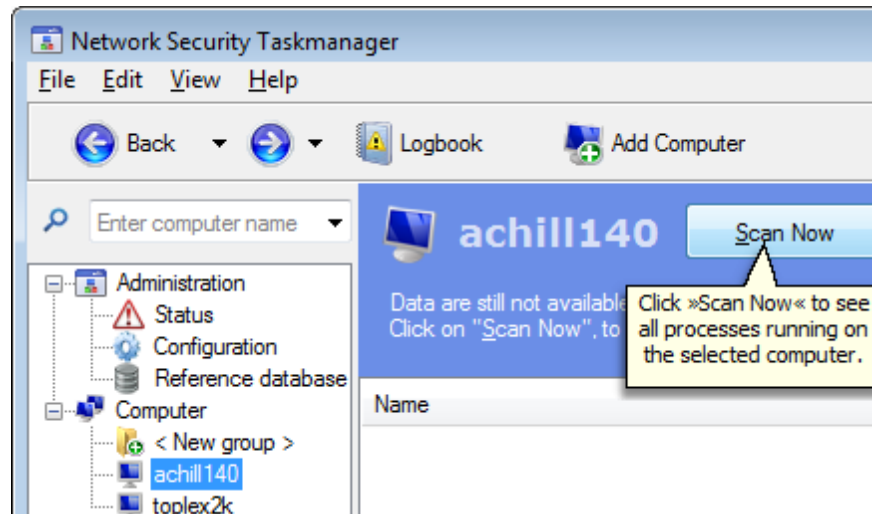


IV

IV. Tasks

Scanning the active processes on a computer

1. Click on the computer or the computer group that you want to scan.
2. Click on **Scan Now**.



Note

- You can scan computers and computer groups automatically by using a [schedule](#) ^[15].
- The first time that you scan a new computer, enter its name or IP address in the field Enter computer name and press the Enter key.

Saving the list of processes

1. Click the **File** menu, click **Save As ...**
2. Choose the type of file:
 - Text file (*.txt)
 - Website (*.html)
 - All details (*.xml)

Note

- Click on **Configuration**, to ensure that no processes are masked. Masked processes, e.g. Windows system processes, will not be saved.
- Save the process list from time to time in order to find new processes. A saved process list can also be useful for subsequent documentation.

Printing the list of processes

1. In the **File** menu, click on **Print...**
2. Choose the printer and any properties to be specified (e.g. double-sided printing).

Note

- Click on **Configuration** to be sure that no processes are masked. Masked processes, e.g. Windows system processes, will not be printed either.



Displaying process properties

Network Security Task Manager shows all active processes on the computers in your network.

In the **View** menu, you can choose which properties will be displayed as columns in the process list:


- ☒ **Name**
Displays the name of the process or of the driver.
- ☒ **Evaluation**
Shows what security-critical functions a process has.
0 % = safe, 100 % = dangerous
[More information](#)^[27]
- ☒ **Clients**
Shows the number of computers in your network, on which the process is running. A process is clearly identified by means of its hash value (MD5 checksum).
- ☒ **Running on the following clients**
Displays the names of the computers in your network, on which the process is running.
- ☒ **Description**
Shows the title and the file description contained in the file. With a visible window the title corresponds to the text in the title bar.
- ☒ **Manufacturer**
Displays the name of the manufacturer (e.g. Microsoft) and the product description stored in the file (e.g. MS Office). You can then see to which installed software product a process belongs.
- ☒ **File**
Shows the full path and name of the file.
- ☒ **Average CPU runtime**
Shows how much the processor is being used. Active programs need more processing power than inactive processes.
- ☒ **Average amount of RAM used on all clients**
Shows the memory consumption of a process.
- ☒ **Average running time on all clients**
Displays the time for which the program has been running since the Windows Start.
- ☒ **Process ID (PID) of the highest-rated process**
Shows the identification number (ID) of the process. Each process has its own unique number. If the process is running on multiple computers, then it has a different PID on each computer. You can see all the PIDs when you double-click on the process.
- ☒ **Type (Program, Driver, Service, Plug-in, ...)**
Shows the nature of the process. Differentiates between different types of process types.
[More information](#)^[28]
- ☒ **Process start information**
Shows when and by whom the process was started.

Note

- Click on the  **Online Info**^[24] button to see information and opinions in this process available on the Internet.
- Double-click on a process to see an overview of all the data for that process.
- Click on  **Configuration**, to hide processes rated as safe. This enlarges the overview. Processes considered safe are e.g. digitally signed operating system processes.

Displaying other properties (Google search)


For each process, you can find an information page, on which you can leave your comment on this software/driver or read comments from other administrators. From this page you can search for more information about this process on Google.com.

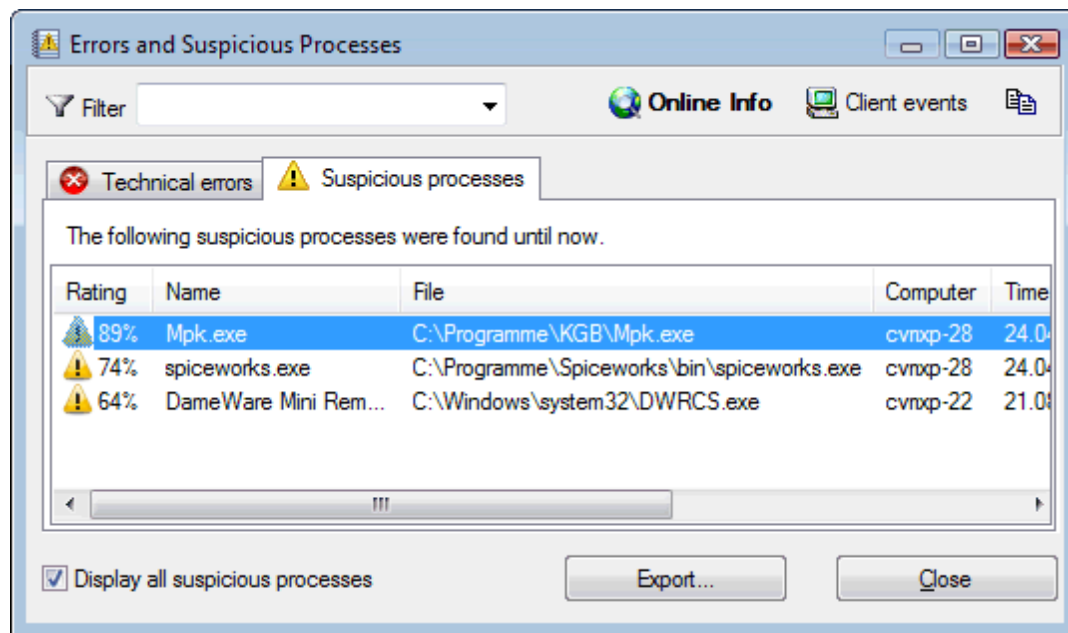
1. Click on the process, about which you want to learn more.
2. Click on the  **Online Info** button.

Viewing the process log



A summary of all processes identified in the past as potentially dangerous can be found in the logbook.




1. In the program toolbar, click on .
2. Click on the tab **Process log**.
3. You can now see all potentially dangerous processes, which were detected in previous scans.




The **Ranking** column shows the [Risk ranking](#)^[27] at the last occurrence of the process. The **Max** column shows the highest ranking since its first occurrence.

-  The process was identified during a complete scan of the computers.
-  The Agent in the computer informed Admin by a [Popup window on the Admin PC](#)^[17]. A complete scan did not take place.

 **Filter** specifies a computer, whose processes are displayed.

 **Online Info** displays detailed online information and opinions on the tagged process.

Stopping a process

1. Click on the process that you want to terminate.
2. In the menu **Edit** click on  **Remove**.
3. Now select one of the following options:
 - ▣ **Terminate process**
The process will be removed from memory. If the process is registered in the registry (Windows configuration database) as Autostart, then it will be activated at the next Windows start.
 - ▣ **Move the file into quarantine**
In this case as well, the process is removed from memory. In addition, the corresponding file is moved into the [Quarantine folder](#)^[25] (Edit | quarantine ...) and the Autostart entries in the registry are deleted. Since file and registry entries are backed up, a restoration of the process is possible.


Note

- Ending a process can lead to instability and data loss. Programs or even Windows can crash. We therefore recommend testing at first by simply terminating the process. If the computer continues stable operation, the process can be moved into quarantine after the next reboot.

Quarantine folder

The quarantine folder works like a wastepaper basket for terminated processes. If you [move a file into the quarantine folder](#)^[25], the file is moved into an isolated folder, and renamed. Autostart entries for this process in the Registry will be deleted. In this way the file is no longer executable. Because Network Security Task Manager saves all its activities, it is possible to restore the process.

Restoring processes

1. In the **Edit** menu, click on  **Quarantine Directory...**
2. In the quarantine folder, click on the desired process.
3. Click on the **Restore** button.

Manual Recovery

The quarantined files are saved in the following folders:

- **C:\ProgramData\Network Security Task Manager** (in Windows 8/7/Vista)
- **C:\Documents and Settings\All Users\Applicationdata\Network Security Task Manager** (in Windows XP)

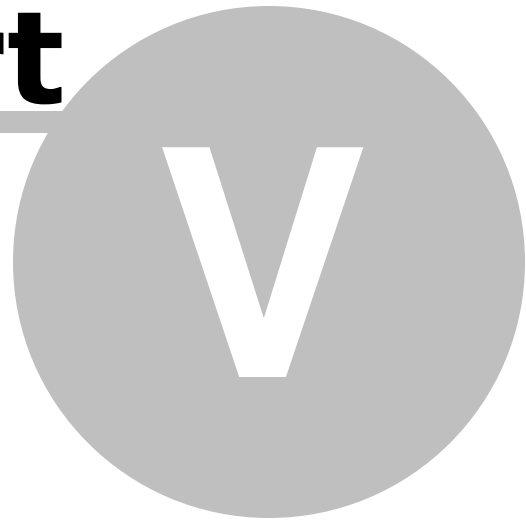
The files are renamed for security as

filename.exe.arbitrarysequence, e.g. *optimizer.exe.q_1182E08_q*

Furthermore, the files are encrypted. In an emergency, you can send [us](#)^[46] the files for decryption.

Basics

Part

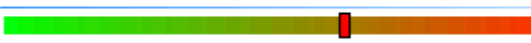


V. Basics

Risk ranking of processes

Network Security Task Manager ranks the security-related risk of a process based on objective criteria. These are used to investigate whether the process contains critical function calls or suspicious features. Depending on the potential dangers, these functions and properties are awarded points. The sum of the points then gives the overall ranking (from 0 to a maximum of 100 points).

Properties	Rating
Sending to CVMXP-22 on port 0, ...	■■■■■
Window not visible	■■■■■
No Windows system file	■■■■■
No detailed description available	■■■■■
Unknown file in Windows folder	■■



Rating: potentially dangerous

Network Security Task Manager investigates the processes according to the following functionalities (Sorted by degree of risk):

- ❑ Can record keyboard input
The process monitors each keystroke. The keystrokes are read by using a Hook. Correctly programmed, professionally written programs do not use this Hook function.
- ❑ Disguised process which is invisible
The process disguises itself by Windows API Hooking. Internal Windows system commands for listing processes are manipulated. Because of this, this process cannot be found in the Windows Task Manager or other process viewers. We recommend that this process be put into quarantine. To do this, click in the **Edit** menu on **Remove**.
- ❑ File is not visible
The file hides itself from Windows Explorer. The file cannot be seen with a file manager. This camouflaging is not the same as the harmless file attribute "hidden".
- ❑ Keyboard driver that could record entries
This concerns a keyboard driver that can read each entry.
- ❑ Can manipulate other programs
The process can link into other programs and then change things. To do this, a hook is used that e.g. can fake a false list of files for all programs (by altering the dir command). The program is then invisible for other programs (AntiVirus).
- ❑ Can monitor Internet browser
Browser Helper Objects (browser plug-ins) link into Internet Explorer. For the most part, this concerns desired download manager or other small tools. However BHO's can also monitor your surfing habits. You can deactivate individual BHOs in the Internet Explorer **Tools** menu under **Manage Add-ons**.
To turn BHOs off in general, click on the Internet Explorer **Tools** menu, click on **Internet Options** and in the **Advanced** tab, disable/deselect the option **Third-party browser extensions enabled**.
- ❑ Starts when you start other programs
The file was started by the ShellExecute command in the Windows system registry (configuration file) by a Hook. ShellExecute starts a process (usually a DLL) as soon as any Windows program is launched. This process should be carefully investigated.
- ❑ Listens on port <Number>
The process can obtain information through this opening. Hackers exploit such vulnerabilities to penetrate unknown computers and to gain control over them. With a good firewall such attacks can be prevented.
- ❑ Sends to <ComputerName> on port <number>
The process has a connection to the specified computer or IP address and can send whatever information it chooses. With a good firewall such connections can be blocked.
- ❑ Unknown program listening or sending
A port was opened to get information from outside or to send it to the outside. Please note which program it is. With a good firewall this connection can be blocked.


- ❑ Monitoring of start/end of programs
The process records which programs are called and terminated, and when this happens.
- ❑ Window not visible
The program has no visible window in Windows and is running in the background. In the best case it is e.g. a device driver.
- ❑ Starts when Windows starts up
The program is called at every Windows start-up. To do that, the program has registered itself in a startup key in the Windows system registry.
- ❑ No detailed description available
Some important standard descriptions in the file are not available. By default, each file contains fields for internal descriptions.
- ❑ Unknown file in the Windows folder
The file does not belong to the Windows operating system. It was copied into the Windows directory. This may be due to poorly programmed software, or because the file is trying to hide itself in the Windows directory.
Caution is advised if you cannot match this file to any installed software product or hardware driver.
- ❑ Not a Windows system file
The file does not belong to the Windows operating system. Increased attention is required if the file is in the Windows directory and cannot be matched to any installed software product or hardware driver.
- ❑ Missing description of the program
There are no descriptions available in the file. By default, each file contains internal fields for descriptions.
- ❑ Internet, monitoring, input-recording, hiding, manipulation functions
The file contains function calls with the specified properties. However, because it cannot be said whether and how these are used, the Network Security Task Manager does not consider this criterion to be strong.
- ❑ Functions not determined
Dangerous function calls have not been found in the file. They could however be contained hidden within the file.
- ❑ Unknown manufacturer
The manufacturer cannot be ascertained. By default, each file has internal fields for information on the software manufacturer.

Trustworthy properties (improve the risk ranking):

- ❑ Microsoft signed file
This file has been signed by Microsoft. You can trust this file to the same level that you trust Microsoft.
- ❑ Verisign signed file
This file was signed by VeriSign. You can trust this file to the same level that you trust VeriSign.
- ❑ Belongs to <Software Product> of <Manufacturer>
This file is classified as trustworthy. It belongs to the named, installed software. If you uninstall the software in the Control Panel, then you will also delete this file.
- ❑ Certified by <Manufacturer>
This file was signed by a CA. You can trust this file to the same level that you trust the certification authority and the software manufacturer.
- ❑ Your own comment
In the reference database you store the processes that are known to you. You can make a comment on each process and classify it as harmless.






[More information](#) 

Note









- Highly ranked processes are not necessarily dangerous. They may possibly just possess typical Malware functions.
Example: System Monitoring by Antivirus-Watchdog/Firewall.
- Click on  **Configuration**, to hide processes classified as safe. Hiding the Windows system processes makes for a wider overview.

Process types

Network Security Task Manager distinguishes between different types of Processes:

Name	Rating	Running on	Description
 Java(TM) 2 Platform St...	67	Hrcxp153	SSVHelper Class
 DameWare Mini Remot...	64	Cvnxp-22, Cvnx...	A component of the Dame...
 FRITZ! Protect	49	Cvnxp-28, Cvnx...	FRITZ!DSL Protect
 Port Reporter	49	Optiplex100	
 aslm75	39	Vectra009	aslm75

In the **View** menu and under **Select columns**, you can set up the display so that the **Type** is also displayed in a column in the table. However, you can also see from the icon which type is concerned:

-  **Process with window**
A normal program with a visible Windows window.
Example: Word
-  **Process without window**
A program that runs in the background. The program has no window or it is in the area that is not visible.
Example: backup process, virus-guard, but also trojans
-  **Process with an icon in the taskbar**
A program whose icon is anchored in the taskbar (on the left next to the clock). Click the right mouse button on the icon in the taskbar to open a contextual menu and to learn more about the program.
Example: Firewall, [NetTaskTray](#)^[30]
-  **Internet Explorer Plug-in**
Browser Helper Objects link in to Internet Explorer. They are mostly desired download manager or other small tools. However BHO's can also monitor your surfing habits. You can deactivate individual BHOs in Internet Explorer "**Tools**" menu by using "**Manage Add-ons**". To turn BHO's off in general, in Internet Explorer click on "**Internet options**" in the "**Tools**" menu, and in the "**Advanced**" tab deactivate the option "**Activate third-party browser extensions**".
Example: Adobe PDF Reader, Java console, but also spyware
-  **DLL files**
A Dynamic Link Library (DLL) contains executable code. In the standard case, rarely used functions are stored in a DLL file, which are only executed when the main program requires them. Thus the main program requires less main memory.
-  **DLL files (via ShellExecute)**
The file is started by a Hook using the ShellExecute command in the Windows system registry (configuration file). ShellExecute starts a process (usually a DLL), as soon as any Windows program is launched. This process should be carefully investigated.
-  **Windows System Process (signed)**
A process digitally signed by Microsoft, which belongs to the Windows operating system. Almost all operating system processes are digitally signed.
Example: explorer.exe, winlogon.exe
-  **Windows System Process**
A process, which belongs to the Windows operating system.
Example: system idle

Drivers and services

Device drivers

Device drivers for the operation of hardware components. They may be drivers for graphics cards and scanners. But also programs that are not destined to be terminated by a user or program (e.g. firewall, antivirus module).

File drivers

Drivers for Windows NT-based file system.

Service (separate process)

A system or hardware-related process to support other programs. The service is executed as a separate process.

Service (separate process with desktop interaction)

A system or hardware-related process to support other programs. The service is executed as a separate process, which can interact with the desktop (e.g. firewall, antivirus module).

Service (shared process)

The service shares a process with other services.

Service (shared process with desktop interaction)

The service shares a process with other services. The process can interact with the desktop.

Notes

- In order to enlarge the overview, you can [hide all Windows system processes](#)^[18].

What is NetTaskTray

NetTaskTray is the name of the tool, which you see in the taskbar next to the clock after the launch of [Network Security Task Manager](#)^[5].



NetTaskTray is responsible for:

Scheduling

NetTaskTray triggers the scheduled verification process on the workstations. The management console does not need to be running in order to regularly and automatically scan computers. NetTaskTray must run under a user account that has administrator rights on the computer to be scanned.

Administrator Exceptions Warning

NetTaskTray displays a small pop-up when a workstation flags a potentially dangerous process. The workstation does not therefore directly contact the management console. NetTaskTray takes charge of the warning message, examines the message and forwards it to the management console.

So that NetTaskTray can receive the messages from the workstations (with the scheduling *At the start of a process* or *After a client boots*), [file and printer sharing](#)^[7] must be enabled on the computer, on which the management console is running.

Note

- If the remote agent detects a potentially dangerous process on the workstation, the administrator will be [warned](#)^[17] in various ways. This ensures that even in the case of network problems, the warning will not be lost.

Admin\$ share

A hidden share is marked by a dollar sign (\$) at the end of the share name. Hidden shares are not listed when you browse the shares on a computer or use the command `net view`.

The system folder `c:\windows` (Variable `%SYSTEMROOT%`) is shared as ADMIN\$. This administrative share allows the administrator remote access to the local Windows folder of the computer on the network.

If you want to scan a Windows 8/7/Vista workgroup computer please consider [following notes](#) [33].

How to check whether Admin\$ is available on the workstation

- On the workstation at the [command prompt](#) (Start> All Programs> Accessories> Command Prompt) run the `net share` command. Admin\$ should be displayed as a share.
- From any computer on the network enter into the Windows Explorer the address: `\target_machine\admin $`
Alternatively, at the command prompt (e.g. `cmd`) `dir \\target_machine\admin$`
You can now see the Windows folder on the desktop.
- These programs show you all the available admin shares on the network: [Microsoft Baseline Security Analyzer](#) (free); [GFI LAN guard - Network Security Scanner](#) (paying); [Hyena](#) (paying).

Creating the administrative share Admin\$

Follow these steps if the Admin\$ share on a computer is not available:

1. Double-click on **Administrative Tools** in the Control Panel, and then click **Computer Management**.
2. Expand the **Shared folder**, click with the right mouse button on **Shares**, and click **New File Shares**.
3. Enter in the field **Folders To Be Shared** the path `%SYSTEMROOT%`.
4. Enter: `Admin$`, and click **Next**.
5. Check the box **Administrators have full control, other users have no access** to restrict access to the release to administrators.
6. Click **Finish**.
7. Click **No**, to go back to the Computer Management console.

Alternatively, you can access the local computer at the command prompt (execute `cmd`) and execute the command `net share admin$`.

Simple File Sharing

If Network Security Task Manager cannot scan a computer in the workgroup, then please deactivate "Simple File Sharing" on this workgroup-computer. If you want to scan a Windows 8/7/Vista workgroup computer please consider [following notes](#)^[33].

To deactivate the **Use simple file sharing** option in Windows XP, run Windows Explorer and click **Folder Options** on **Tools** menu.

According to the settings, this only works on the current folder. Therefore the "save viewing options for each folder" must also be deactivated.

The **security** tab now appears in the Properties dialog for folders and files.

The following registry key is responsible for "Simple File Sharing":

HKEY_LOCAL_MACHINE\ System\CurrentControlSet\Control\LSA

forceguest = **0** - "Simple File Sharing" not used

forceguest = **1** - "Simple File Sharing" used (Standard)

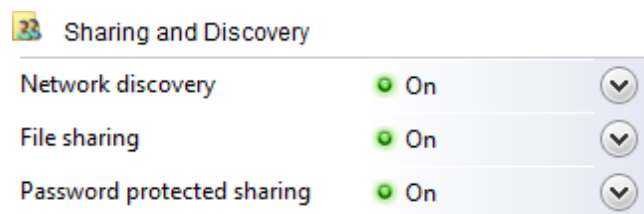
The entry can also be edited via the local security policies (Administrative Tools -> Local Security Policy -> Local Policies

-> Security Options -> Network Access: model for shared use and security model for local accounts).

"Simple File Sharing" is activated by default on Windows XP Professional, when the computer is added to a workgroup at the time of installation of the operating system. If the computer is directly added to a domain at the time of installation of the operating system, then "Simple File Sharing" is disabled by default.

If a computer currently in a workgroup is subsequently upgraded to a domain, then despite this, the setting "Use simple file sharing" still persists and, if unwanted, must be turned off as described above.

By default, simple file sharing is disabled in Windows 8/7/Vista by following settings in *Control Panel\Network and Internet\Network and Sharing Center*:



Scanning a Windows 8/7/Vista pc

Please consider following notes if you want to scan a computer, that runs **Windows 8/7/Vista** and belongs to a **workgroup**.

If the computer to be scanned does not belong to any workgroup, but to a **domain**, then do not consider the following notes, because a domain administrator always have access to admin shares of a computer in a domain.

By default, User Account Control (UAC) in Windows 8/7/Vista prevents local administrator accounts from accessing administrative shares through the network. If you want to scan a Windows 8/7/Vista workgroup computer, *Network Security Taskmanager* shows an error message: **User <UserName> does not have administrator rights on <WorkgroupComputer>**

Solution:

Following fix ([KB947232](#)) is recommended by Microsoft in order to have access to admin\$ share on a Windows 8/7/Vista workgroup computer using a local administrator account. At this the security of the remaining User Account protection (UAC) stays the same. So *Network Security Taskmanager* can scan the Windows 8/7/Vista workgroup computer remotely:

1. Run registry editor (regedit.exe) on the Windows 8/7/Vista workgroup computer to be scanned.
2. Locate and then click the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
4. Type **LocalAccountTokenFilterPolicy** to name the new entry.
5. Right-click LocalAccountTokenFilterPolicy, and then click **Modify**.
6. In the **Value data** box, type **1**, and then click **OK** and close registry editor.

Note

- Alternatively you can install the Agent on the Windows 8/7/Vista workgroup computer **permanently**. Just run the file [NetTaskAgent.msi](#)^[48] (located in the program's folder, e.g. c:\program files\Network Security Taskmanager\) on the Windows 8/7/Vista workgroup computer. So the steps 1 - 6 above are not necessary.

Microsoft network communication security

Microsoft Network Communications (SMB, NetBIOS) can be further secured depending on the structure of the Windows-based network.

NTLMv2, 128-Bit encryption

Further Microsoft Network communication security measures can be activated via the group policy:

1. Open the [command prompt](#) as an administrator (Start > All Programs > Accessories > Command Prompt).
Alternatively: Start > Run: enter "runas /user:Administrator cmd" and execute. Then enter the administrator password.
2. In the new DOS window now enter "gpedit.msc" and press <Enter>.
3. In the left pane change the security options: Computer Configuration -> Windows Settings -> Local Policies -> Security Options

Whichever security measures are involved in your Windows Network topology, please be sure to observe the advice from Microsoft: <http://support.microsoft.com/kb/823659>

Be aware of when and where additional security measures can lead to problems! It is strongly recommended to only use the NTLMv2 authentication method for Windows networks. See also: [How to crack Windows passwords](#)

NetBIOS over TCP / IP (NetBT)

The setting for NetBIOS over TCP / IP networks can be disabled for networks with a DNS server running name resolution, in the case where there is no Windows 9x/ME or Windows NT computer on the network:

1. Start -> Control Panel -> Network Connections
2. Double-click on the desired network connection.
3. Now click on **Properties** in the context menu.
4. Double-click on **Internet protocol TCP / IP**.
5. Click on the **Advanced** button.
6. Click on the **WINS** tab.
7. Select **NetBIOS over TCP / IP off**.
8. Close all network connection windows.

When the NetBIOS over TCP / IP has been deactivated, the access to the network shares (SMB communications) are made directly over TCP port 445.

Blocking NetBIOS over TCP / IP with the firewall

The UDP ports 137, 138 and TCP port 139 are freed when NetBIOS over TCP / IP is shut down. Outside access to these three no longer used ports should be prevented by the firewall:

1. Start -> Control Panel -> Windows Firewall
2. Click the **Exceptions** tab.
3. Double-click on **File and Printer Sharing**.
4. Tick the option for **TCP 445**. Un-tick the options for all other ports.
5. Close all open Windows Firewall windows.

Files and processes used

Network Security Task Manager only needs [Windows Standard installation](#)^[7] on the administrator's computer and on the computers to be scanned. Additional drivers, libraries and services are not needed.

- Are existing system files, libraries, drivers, etc. changed during the installation?
No. The installation of Network Security Task Manager on a computer does not alter the registry or existing files. No files are created or modified outside of the installation directory.


When Network Security Task Manager is started, then the software stores its data here:

- In the registry in the key
`HKEY_CURRENT_USER\Software\Neuber\Network Security Task Manager`
- On the hard disk in the folders
`C:\ProgramData\Network Security Task Manager` (in Windows 8/7/Vista)
`C:\Documents and Settings\All Users\Userdata\Network Security Task Manager` (under Windows XP)

The registry key and the folder will be deleted again when an [uninstall program](#)^[36] is run.

- What processes are active on the administrator computer?
On the computer where the administrator uses Network Security Task Manager, the following processes run:

 **NetTaskConsole.exe** - the [Admin Console](#)^[5], i.e. the main program

 **NetTaskTray.exe**^[30] - controls scheduling and reception of warnings in the taskbar tray

- What processes are active on a workstation?
During the scan of the client computer, the **NetTaskAgent.exe** file is copied into local Admin share [Admin\\$](#)^[31], and started as an agent. After the scan, this remote agent is completely removed again.

Only on computers with scheduling of *At the start of a process* or *After a client boots* will the remote agent be permanently installed.

The remote agent stores cache data on the client computer that is scanned in the following folders:

- `C:\ProgramData\Network Security Task Manager` (in Windows 8/7/Vista)
- `C:\Documents and Settings\All Users\Applicationdata\Network Security Task Manager` (under Windows XP)

This folder will always be erased if the client computer is [removed](#)^[14] from the console.

Note

- Note: For security reasons, the agent file **NetTaskAgent.exe** will be saved on the client under a random name, e.g. as **smPolodo.exe**. Use the command `sc \target_computer qc nettaskagent` to learn the real file name.

Uninstalling all of the software

Uninstalling the remote agent from client computers



The Remote Agent is permanently installed on the computer to be scanned in the case of

- distribution of the remote agent by MSI-package
- scheduling configured as *At the start of a process* or *After a client boots*

You have the following possibilities for removing a remote agent from a computer:

- ❑ Uninstalling via Network Security Task Manager
Delete the scheduling for the desired computer or [remove](#)^[14] the computer from the list.
- ❑ Uninstalling by command
As an administrator you can also completely uninstall the remote agent from a workstation with the command `NetTaskAgent.exe /u` or from a remote computer with the command `sc \target_computer delete nettaskagent`.
- ❑ Uninstalling via login script
You can also save the command `NetTaskAgent.exe /u` in a batch file and then uninstall the remote agent using a **login script** by group policy.
In contrast to the [msi instructions](#)^[62], in step 5 click on "start" in the GPO (Group Policy Object) editor under Computer Configuration > Windows Settings > Scripts (Startup/Shutdown). Then click on "Add" to add the batch file. The batch file is executed in the local system account, which therefore has admin privileges.
- ❑ Uninstalling by distribution software / Group Policy
If you have distributed the remote agent on the computers via an MSI package, then you can uninstall the agent again with your software distribution software or via a [Group Policy uninstall](#)^[67].

Uninstalling the [Console](#)^[5]

1. Open the Windows Control Panel .
2. Click on  **Software** (programs uninstall).
3. Click on *Network Security Task Manager*
4. Click on **Uninstall**.

Note

- Hint: for security reasons, the agent NetTaskAgent.exe file is stored on the client under a random file name, for example as smPolodo.exe. You can find out the real file name with the command `sc \\target_computer qc nettaskagent`.
To uninstall the agent you must use the real file name in the command, e.g. `smPolodo.exe /u`

Troubleshooting

Part



VI

VI. Troubleshooting

Resolving connection errors

Note: If you can use Windows Explorer as follows to access the computer to be scanned, then Network Security Task Manager will also work:



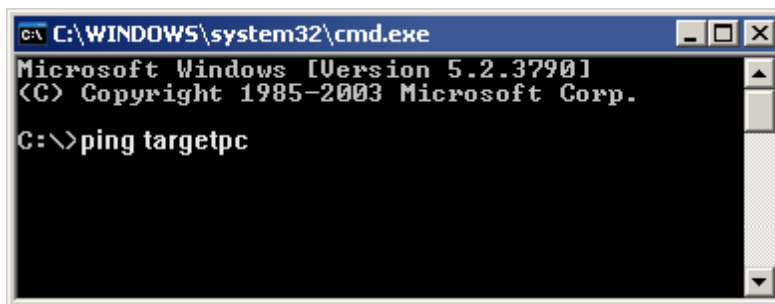
[What to consider before scanning a Windows 8/7/Vista computer](#)^[33]

If Network Security Task Manager cannot scan a computer, then check whether all the conditions are being met:

☐ **Computer is running**

1. Verify that the computer to be scanned is reachable over the network. To do so, type in the [Command prompt](#) (Start > All Programs > Accessories > Command Prompt) the following command:

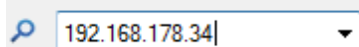
`ping target_machine`



If the computer cannot be pinged, then check whether the computer is powered on and that the computer name is correctly spelled.

Note: A computer can only be pinged if the Windows firewall allows it, under: Advanced > ICMP settings > Allow incoming echo request (default setting). Network Security Task Manager works regardless of this setting.

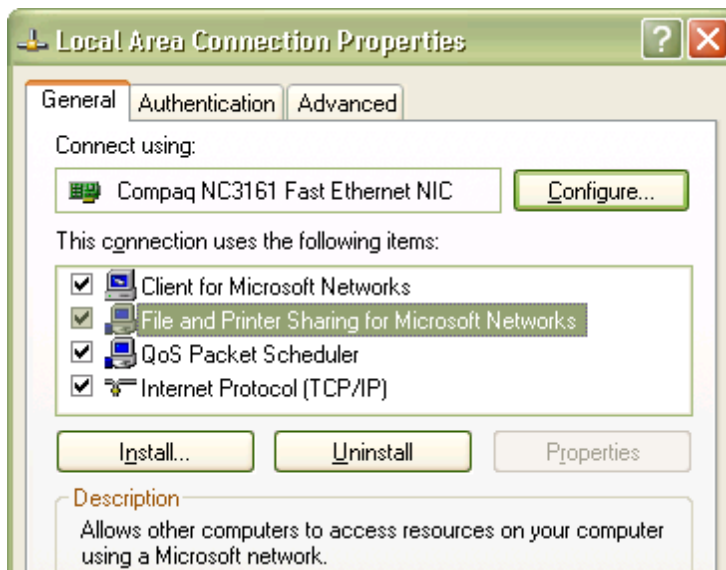
2. If the computer can be pinged, then write down the IP address of the target computer and use it in *Network Security Task Manager* instead of the computer name:



If the scan only works with the IP address, then there is either already a [Connection under a different user name](#)^[44] to the target machine, or the [Name resolution for file and printer sharing](#)^[43] is blocked.

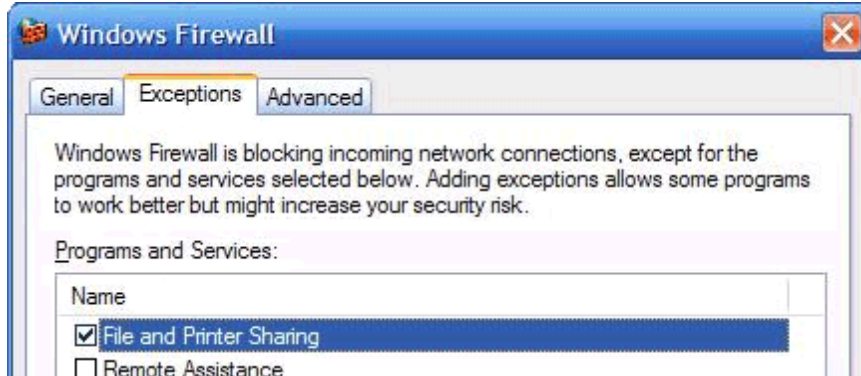
File and Printer Sharing

On the computer to be scanned, turn on the "file and printer sharing for Microsoft Networks" in the Control Panel > Network Connections > Right-click on the desired LAN connection > Properties.



Firewall Exception for File and Printer Sharing

The firewall on the computer to be scanned must not block File and Printer Sharing. That means that TCP port 445 (SMB protocol) must be open.



If your **NetBIOS over TCP/IP** (NetBT) network is active, then TCP port 139 (NetBIOS session service) must be open for [Name resolution](#)^[42].

Please only use "File and Printer Sharing" on the network interface cards/network connections of the internal company network! "File and Printer Sharing" must not be activated for network connections/network cards connected to the outside (to the Internet or to the gateway).

Admin Share Admin\$

To scan a computer, a remote agent is installed temporarily in the local Windows folder (=Admin\$).

To check whether the Admin\$ share exists on the computer to be scanned, use the Command prompt to run the command `net share`. It should display Admin\$ as a share.

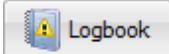
[Other methods to verify the Admin\\$ share](#)^[31]

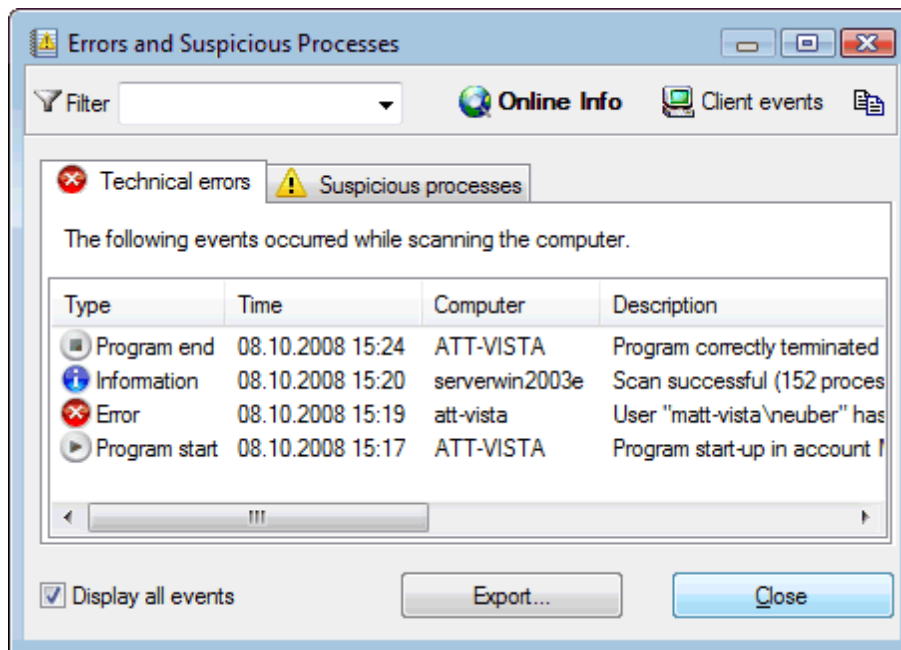
⚠ If the computer to be scanned does not belong to any domain, but to a workgroup, then deactivate [Simple Filesharing](#)^[32] on this computer! If you want to scan a Windows 8/7/Vista workgroup computer please consider [following notes](#)^[33].


If the remote agent has been distributed via an [MSI-Package](#)^[48], or [scheduling](#)^[15] on the basis of *At the start of a process* or *After a client boots* is already in place, then no Admin share is necessary on the computer to be scanned.


Viewing the error log


In the logbook you will find an overview of the technical errors that occur.

1. In the toolbar of the program, click on .
2. You can now see the error that occurred (e.g. connection problems).



 **Filter** applies to one computer. Only the errors that occurred on this computer will be displayed.

 **Online Info** makes it possible to get online help for a specific error.

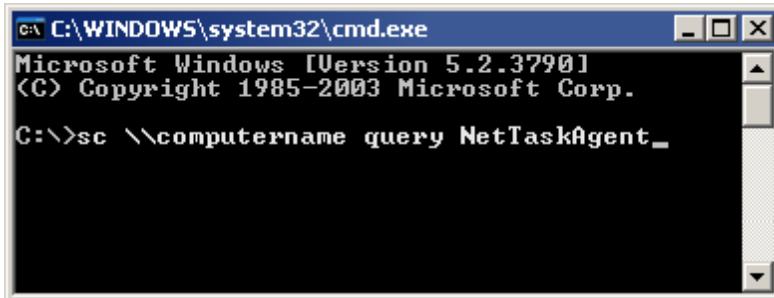
 **Client Events** shows the local event display of the computer that was just selected. For this, the Windows Event display is started. The Remote Registry service on the client must be active and you (i.e. the user that just registered) users) must have Admin rights on the client.


Note

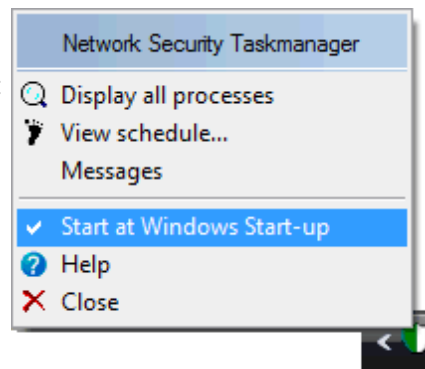
- To view the event log of any client computer, click the right mouse button on the desired computer in the list of computers on the console. Then click on the **event log** ▶

Scheduling / warning not working

To check from the Admin PC, whether the remote agent is running on a client, either click on [Computer properties](#)^[13] and then on [Now test](#) or execute the command `sc \\computername query nettaskagent`. In this instance, *computername* is the name of the computer or the IP address of the workstation on the network.




 [NetTaskTray](#)^[30] controls scheduling and warnings. It must therefore run in system tray of the task bar. To ensure this, you can enable the option **Start at Windows startup**.



Administrator not warned about dangerous processes

If you are using the schedule settings [At the start of a process](#)^[15] or [After a client boots](#)^[15], then the computer on which the management console is running must have File and Printer Sharing enabled. With these two schedules the management console is then informed, if a potentially dangerous process has been found.

Scheduling is not running

When scheduling has been set up,  [NetTaskTray](#)^[30] starts the management console/console if exceptions are detected, or at the appropriate time. The management console then scans the corresponding computer. NetTaskTray must run in a user account that has Administrator rights on the computer that is to be scanned.

Background: A program (in this instance, NetTaskTray) with restricted rights may not start any program with higher rights (such as the management console with admin rights).

Even with the [Advanced scheduling](#)^[15], you must specify an administrator account.

Starting Network Security Task Manager under a different user account

If you start the management console with a different user name (Windows logon name), it may happen that you can no longer scan the computers, on which the remote agent has been installed.

Background: User A defines a schedule for a computer as either [At the start of a process](#)^[15] or [After a client boots](#)^[15]. The remote agent (300 KB) will be permanently installed on this computer. For security reasons, the remote agent can only be contacted and controlled by User A. Later the authorization can be changed again.

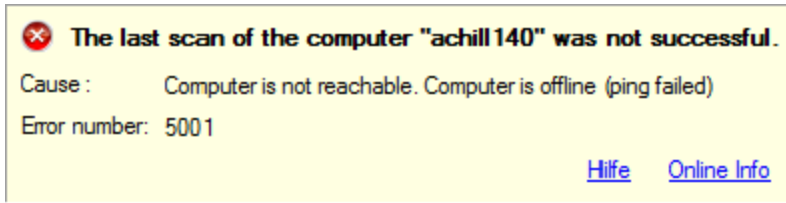
Note

- In the **View** menu, click on [error log](#)^[40] to see an overview of all previously encountered technical errors.

Error messages

Finding the cause of the error by using the error message

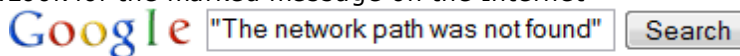
1. If an **error message** appears, then google it.



2. Some error messages:

- [The network path was not found](#)^[42]
- [No access to the services of the computer](#)^[42]
- [The RPC Server is unavailable](#)^[42]
- [The specified network was not accepted by a network service provider](#)^[42]
- [Multiple connections to a server ... are not allowed.](#)^[44]
- [This network folder is currently in use for a connection with another name and password.](#)^[44]
- [User <Username> has no administrator rights on <Clientcomputer>](#)^[45]

3. Look for the marked message on the Internet



Note

- In the **View** menu, click on [Error log...](#)^[40] to see an overview of all previously encountered technical errors.

Connection errors

Error messages:

- **The network path was not found**
- **No access to the services of the computer**
- **The RPC server is unavailable**
- **The specified network was not accepted by any network provider**

Causes & Solutions:

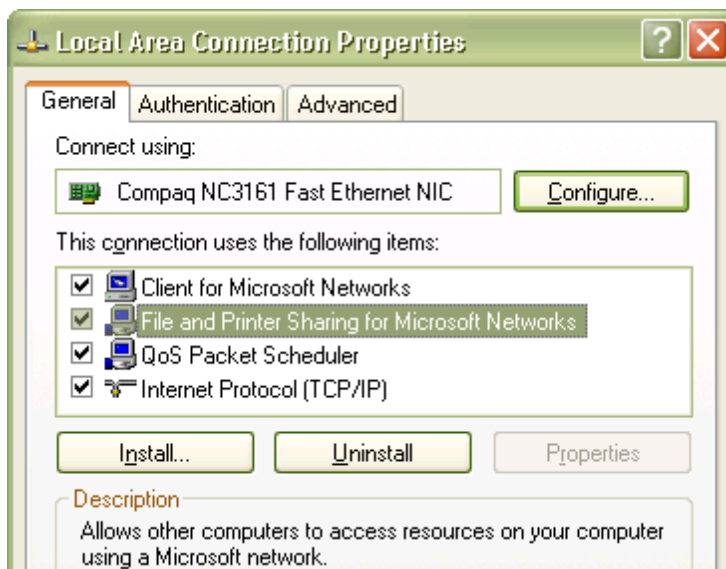
- ☐ Computer not reachable
When you logged on the computer to be scanned, the DNS or NetBIOS name could not be resolved.

Solution:

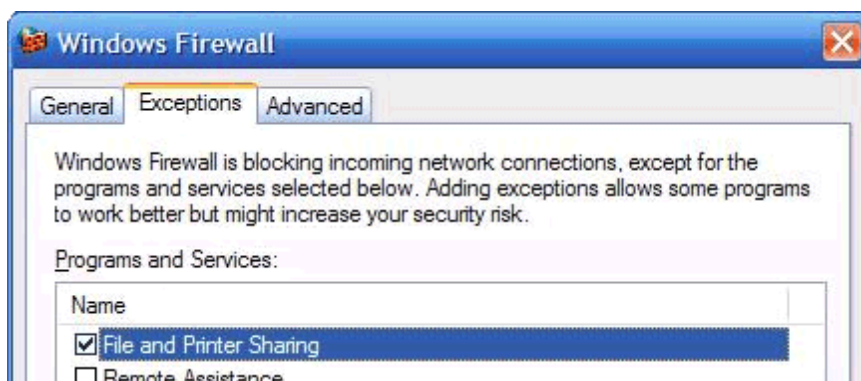
1. Make sure the computer exists (was there a typing error in the computer name?)
 2. Make sure the computer is running.
 3. Verify that the computer is reachable on the network. Enter e.g. in the command prompt (Start > All Programs > Accessories > Command prompt) the command **ping target_computer**.
 4. It may be that *NetBIOS over TCP/IP* is enabled in your network, but that the TCP port 139 on the remote computer is blocked by the firewall. If you open port 139 in the firewall, then name resolution will work again.
If you can ping the target computer, then the connection is working with the IP address instead of the computer name.
- ❑ File and Printer Sharing is not enabled
"File and Printer Sharing for Microsoft Networks" is not enabled on the computer to be scanned, or it is blocked by the firewall.

Solution:

1. Turn on "File and printer sharing for Microsoft Networks" on the computer to be scanned, in the Control Panel > Network Connections > Right-click on the desired LAN connection > Properties



2. The firewall on the computer to be scanned must not block File and Printer Sharing. That means TCP port 445 (SMB protocol) must be open.



Given that the above error messages are generated by a general network problem, you can also find out the cause using the tools that are generally available:

- ☐ via commands in the Command Prompt

1. Open the [Command prompt](#) (Start > All Programs > Accessories > Command prompt).
2. Enter: `ping target_computer`

If you cannot find the target computer by using ping, then please google the error message that you get back from ping. With this you will find suggestions for solutions. Make sure that the computer name is correctly spelled, and that the target computer is running.

3. Enter: `runas /user:administrator cmd`

In this instance `administrator` is an administrator account on the target computer (e.g. admin or domain\administrator). Use this user name as well for logging in to Network Security Task Manager.

3. At the newly launched command prompt, enter: `net view \\target_computer`. By means of the error message you can recognize the cause of the error:

There are no entries in the list or Shared resources on \\target_computer

File and Printer Sharing is enabled.

If the target computer does not belong to any domain, but to a workgroup, then disable [Simple File Sharing](#)^[32]!

System Error 5 has occurred. Access Denied

The user name used in Step 2 is not an administrator account on the target computer.

System Error 53 has occurred or System Error 51 is occurred

"File and Printer Sharing for Microsoft Networks" is not activated, or it is blocked by a firewall.

- ☐ Suggestions for the solution of underlying network problems

1. Open the [Command prompt](#) on the computer to be scanned (Start > All Programs > Accessories > Command prompt).
2. Enter the command `net start rpcss`
Check to see if this resolves the issue. If the problem is still there, go to the next step.
3. Enter the command `ping target_machine`, where the *target_machine* is the computer server, NetBIOS, DNS, or GUID name, whose connection you want to test.
4. If there is a connection problem with one of these computers, then at the command prompt, enter `netdiag` (part of the Microsoft Windows 2000 Resource Kit) in order to determine whether the domain controller is working correctly.
5. If the server name is not properly resolved, check the DNS configuration of the domain controller. If the problem is still there, go to the next step.
6. At the command prompt, enter `netdom` (part of the Microsoft Windows 2000 Resource Kit), to check the network's position of trust and to establish or reset a connection to a server.
7. If the primary domain controller for the domain can not be found, the domain name will not be properly resolved: check the DNS configuration of the domain controller.

✍ Notes

- The RPC server is not remotely controlled by Network Security Task Manager. Thus port 135 can always remain closed for security reasons.
- With the command `netdiag /debug`, network errors can generally be tracked down. Simple problems can be rapidly resolved with `netdiag /fix`. After that you can also continue the search for errors with the `dcdiag` tool.

Multiple SMB connections

Error messages:

- **Multiple connections to a server or shared resource by the same user using multiple user names are not allowed. Disconnect all previous connections to the server or shared resource and try again.**
- **This network folder is currently connected using a different name and password. First disconnect any existing connection to this network share to then connect using a different**

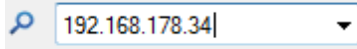
name and password.

Cause:

There is already a network connection (SMB protocol) to the computer to be scanned from another username without administrator rights. Unfortunately Windows does not allow a further connection to be made from another user account.

Solution A:

Use the IP address in the Network Security Task Manager instead of the computer name.



Solution B:

Open Windows Explorer on the computer to be scanned. Click on the **Tools** menu and select **Disconnect Network Drive**. Then disconnect the existing connection

Solution C:

1. Open [Prompt](#) on the computer to be scanned (Start > All Programs > Accessories > Prompt).
2. Then run the `net use` command, to see what connections exist.
3. With `net use /delete <corresponding connection>` terminate the current connection (whether or not the status is shown as "disconnected"). You can also use the command `net use * /delete` to delete all connections.

No Admin rights

Error messages:

- **User <UserName> does not have administrator rights on <Clientcomputer>**

Causes & Solutions:

❑ Windows 8/7/Vista computer to be scanned

On the client computer to be scanned, Windows 8/7/Vista is installed and that client computer belongs to a **workgroup**.

Solution:

If you want to scan a Windows 8/7/Vista workgroup computer please consider [following notes](#)^[33].

❑ The specified user account is not an administrator account

When Network Security Task Manager scans the client computer, you are asked for the user name and password of an administrator account on the computer to be scanned. The login data you have entered however do not belong to any administrator account on the client computer to be scanned.

Solution:

Make sure that you have entered the user name and password correctly, and that this user has admin rights on the client computer to be scanned.

❑ Simple File Sharing is turned on

On the client computer to be scanned, "Simple File Sharing" is enabled and the target computer belongs to a **workgroup**.

Solution:

Turn off [Simple File Sharing](#)^[32] on the client computer.

Technical support

If looking at the [FAQ](#)³⁸⁴ does not resolve your problem, then please write to us:

Address: A. & M. Neuber Software GmbH
PF 11 05 25
D-06019 Halle

Fax: (+49) 0700-11 777 000

email: info@neuber.com

WWW: www.neuber.com/network-taskmanager

MSI package software distribution

Part



VII. MSI package software distribution

Overview

The [distribution of agents](#)^[9] is done automatically by Network Security Task Manager. In large networks however the agent can also be permanently distributed by an MSI package. The MSI package contains the slim agent (only 300 KB in size), which is distributed to computers to be monitored (unattended installation). The MSI package can only be distributed by adjusting the parameters. Without this adjustment, the communication with the management console will not work.

The adjustment of the parameters is done in one of the following ways

☐ With an MST file

Ideal for distribution in larger networks. This document describes how the MST file is created and, together with the msi file, is distributed in the network.

To distribute the remote agent via msi

1. [Create a transform file \(*.mst\)](#)^[49].
2. [Save MSI & MST file in a shared folder](#)^[52].
3. [Distribute the package e.g. via a group policy](#)^[54].

☐ Delivery by parameters

This is useful for testing purposes. The `nettaskagent.exe` filename of the remote agent may however not be changed.

Use the following command to start the installation (for example, at the [command prompt](#) or via a login script):

```
msiexec /i "\\servername\share\NetTaskAgent.msi" INSTALLDIR="c:\myfolder"
SERVER="Servername" USER="Administrator" /qn
```

Parameters

INSTALLDIR specifies the local directory on the target computer, in which the agent `NetTaskAgent.exe` file will be copied. If the parameters are left out, then the agent is installed in the System32 directory of the local Windows folder. This is the default setting.

SERVER is the name of the computer on which `NetTaskTray.exe` runs. In most cases this is also the console. You can see the name of the computer e.g. in the network environment (My Network Places).

USER is the user name (for example: `domain\user`), under which [NetTaskTray.exe](#)^[30] runs. In most cases, the console also runs under this user account. A password does not have to be specified.

/qn specifies no user interface (unattended installation)
If you replace **/qn** by the **/qb** parameter, you see the progress of the installation on the client.

☑ Note

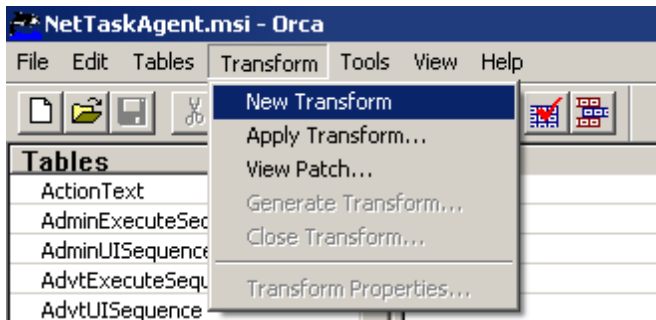
- The MSI package `NetTaskAgent.msi` for the distribution of the agent is located in the program folder (e.g. in `c:\Programme\Network Security Task Manager\`).
- If the agent is installed by MSI package, then these computers will only appear in the program if the agent flags a potentially dangerous process.

Creating the MST file

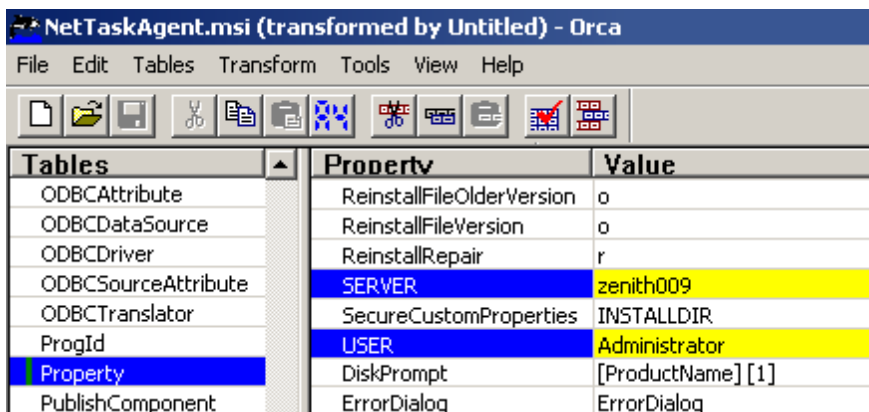
The custom.mst file can be created with the free **ORCA** tool.

Download: <http://www.neuber.com/network-taskmanager/docs/orca.html>

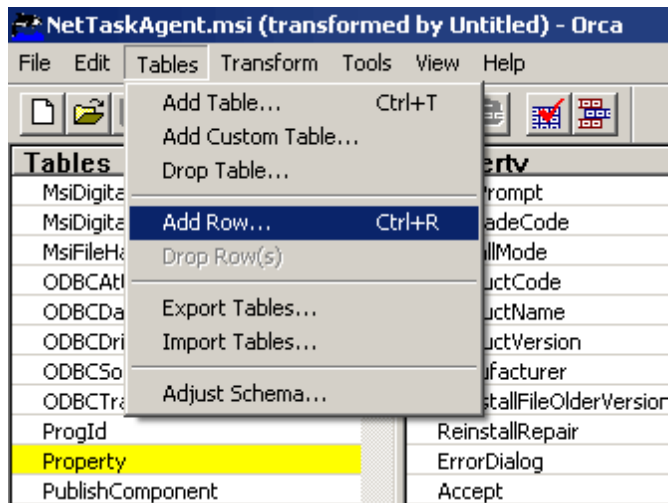
1. Start ORCA and open the **NetTaskAgent.msi** file. The file is located in the program folder of Network Security Task Manager.
2. In the menu **Transform**, click on **New Transform**



3. Click in the table list on **Property**. Enter the computer name and the user account used (e.g.: domain\user) by [NetTaskTray.exe](#)^[30]. In most cases the [Console](#)^[5] also runs under this account.



4. By default, the file is installed in the local Windows\System32 of the workstation. Optionally, an arbitrary folder and file name can be entered for the agent file:



5. Enter **INSTALLDIR** and press the Enter key.

Name	Value
Property	
Value	

Column:
Property - String[72], Required

INSTALLDIR

OK Cancel

6. Enter the local path of the workstation. The NetTaskAgent.exe file will be installed there later. Confirm with OK or Enter.

Name	Value
Property	INSTALLDIR
Value	

Column:
Value - Localizable String[0], Required

c:\myfolder

OK Cancel

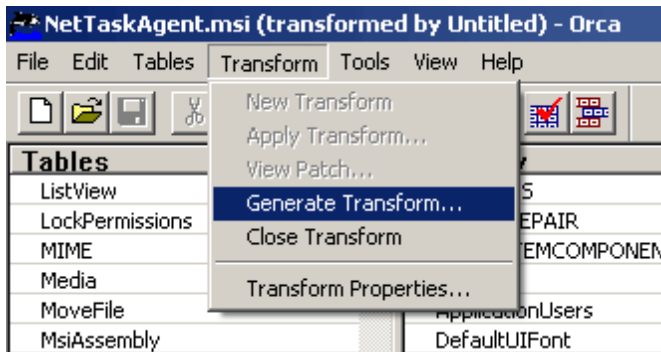
7. Click on the **File** table and enter in the FileName column the name that you want to call the file.

NetTaskAgent.msi (transformed by Untitled) - Orca

File Edit Tables Transform Tools View Help

Tables	File	Component	FileName	FileSize
FeatureCompon...	NetTaskAgent.exe	NetTaskAgent.exe	NewName.exe	29
File				
Font				

- In the **Transform** menu, click on **Generate transform ...**



- Save the file under the name of **custom.mst**.

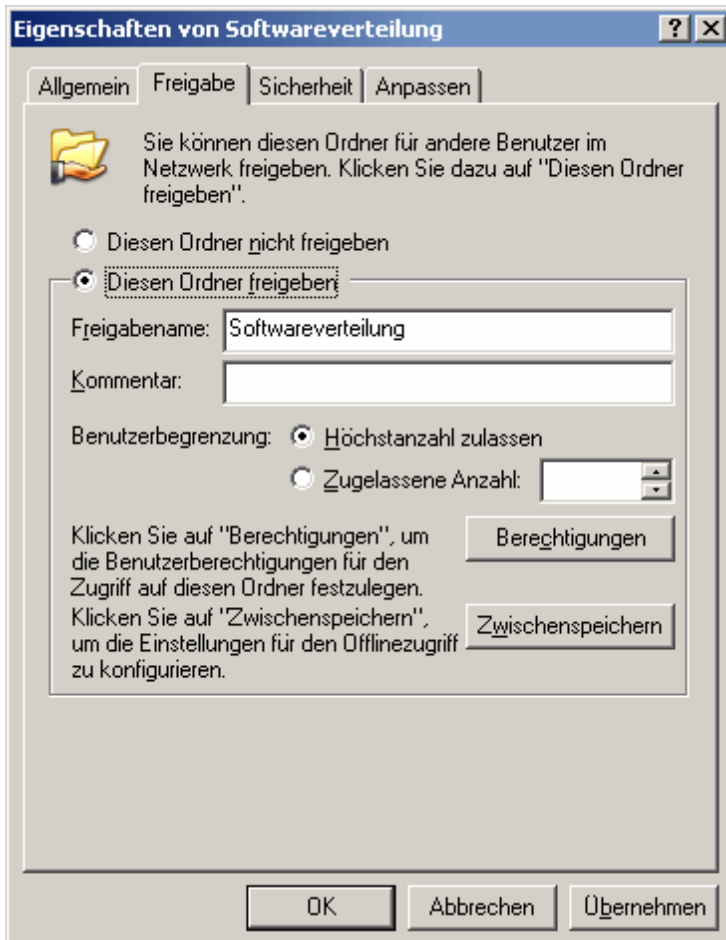
Next step:

[Storing the MSI and MST file in a shared folder](#) ⁵²

Creating a shared folder

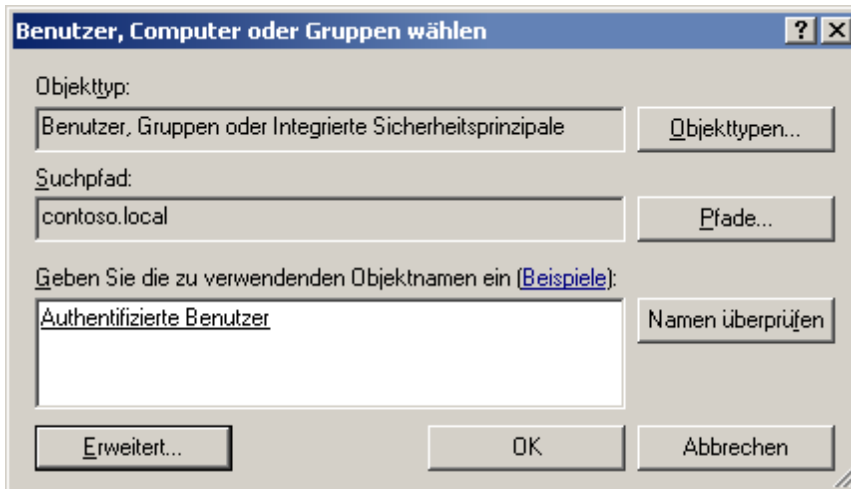
We are sorry that the screenshots aren't in English language.

- Create and share a directory on the file server (domain member) or network drive.

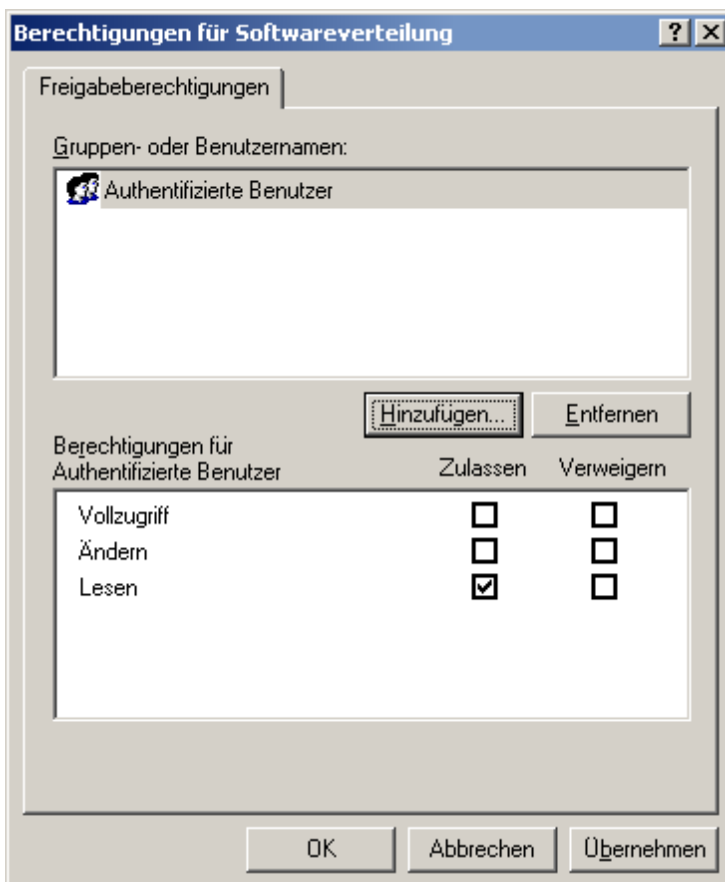


A hidden share can also be used. In this case a dollar sign will be attached to the share name: *softwaredistribution\$*.

2. Click on **Permissions**. By default, read access is set for **All**. Remove this user.
3. Click on **Add** and set the read access for **Authenticated Users** group. Members of this predefined group are all computer and user objects, which have been authenticated for the domain.



4. Click on **Advanced**, then click on **Find Now**. Then select **Authenticated users**. Click **OK**.



5. Click on **OK**.

6. Copy the NetTaskAgent.msi and Custom.mst files into the newly created *softwaredistribution* folder.

Next step:

[The software distribution](#)^[54]

Group policy software distribution

In large networks, the msi and the mst file are distributed via system management and deployment software. The following describes the software distribution by script and by GPMC:

❑ Software distribution by script

The following command (e.g. in the [command prompt](#) or by login script) starts the installation:

```
msiexec /i "\\servername\share\NetTaskAgent.msi" TRANSFORMS="\
\servername\share\custom.mst" /qn
```

❑ Software distribution on Windows 2000 Server

If you are still running a Windows Server 2000, then you can very easily distribute NetTaskAgent.msi by using the following steps. We recommend, however, the instructions via GPMC described below.

1. In the Start menu, click on Control Panel > "Active Directory Users and Computers".
2. With a right click on the desired computer group (OU), open the Properties dialog.
3. Select the **group policy** tab.
4. With New, create a new policy called "NetSTM service installation". Open it with **Edit**.
5. Click on Computer Configuration/software settings. Then right-click on New > package.
6. Open the file \\server name\share\NetTaskAgent.msi.
7. Click on the **Advanced** option.
8. Click on the **changes** tab . Then click on **Add** to add the file custom.mst.
9. Click on the tab **software deployment**. Select the option "*uninstall application if outside the administrative domain*".
10. Confirm your changes by clicking on **OK**.
The next time you restart the client computers in this computer group (OU), the remote agent will be installed before the users log on.

Recommended procedure for distribution by Group Policy

For Windows Server 2003/2008 and all current operating systems, Group Policy Management (in short: GPMC) is recommended. (Download:

<http://www.microsoft.com/downloads/details.aspx?familyid=F39E9D60-7E41-4947-82F5-3330F37ADFE&displaylang=de>)

To be able to use group policy management on a client of an administrator, you need to have previously installed the Administration Tools Pack:

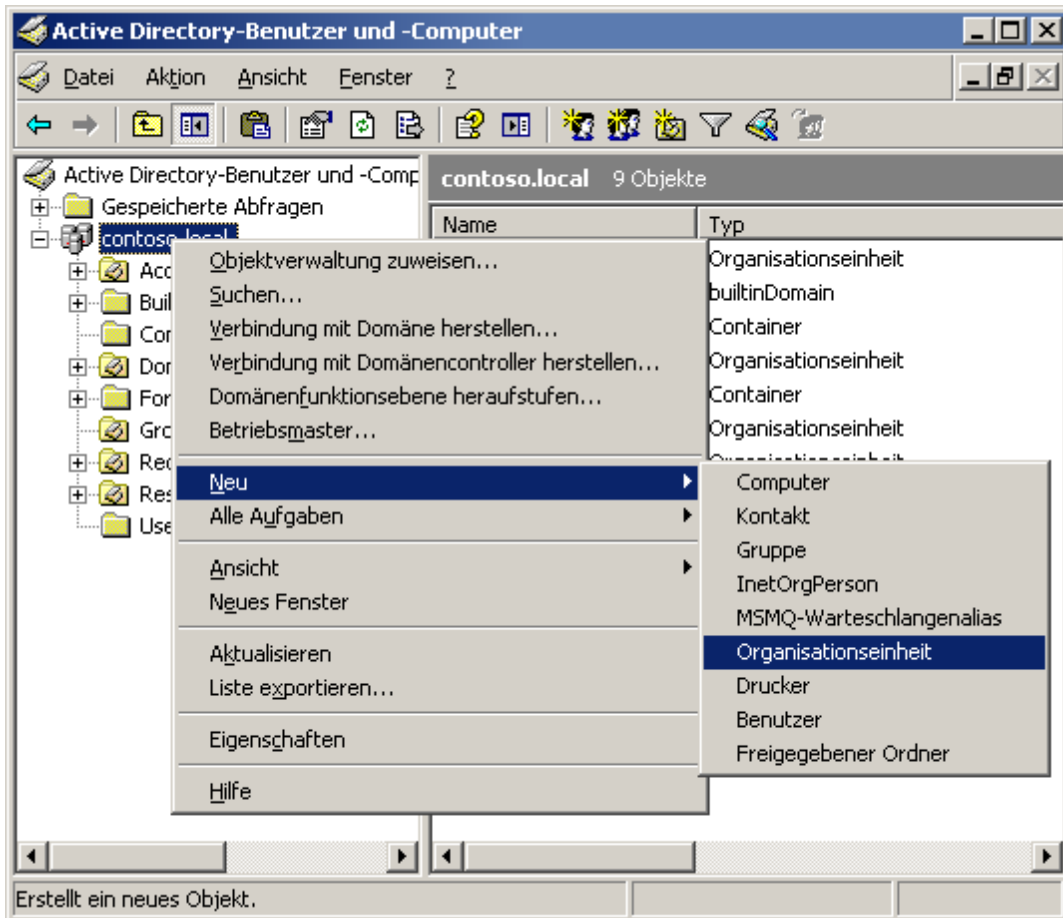
<http://www.google.de/search?hl=de&q=windows+server+Administration+Tools+Pack>

We are sorry that the screenshots aren't in English language.

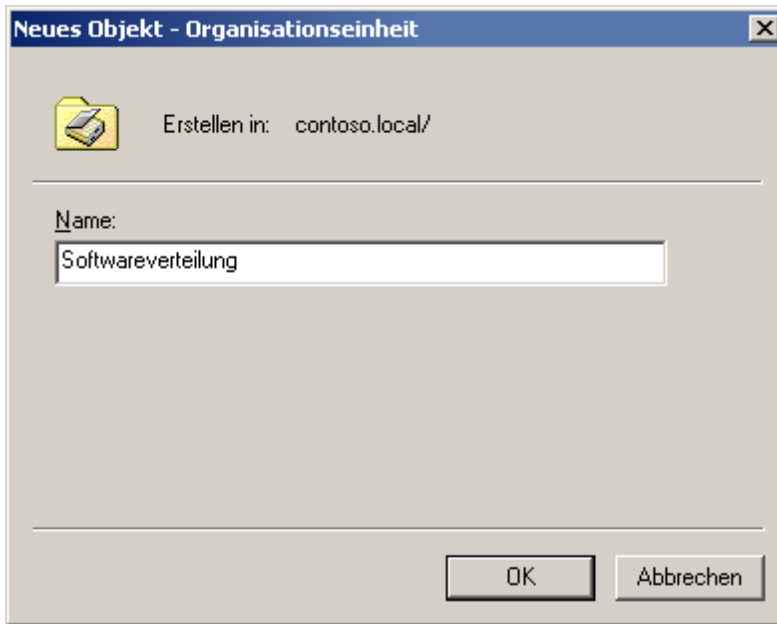
A) Security group set up

The security group includes every computer on which the remote agent is installed.

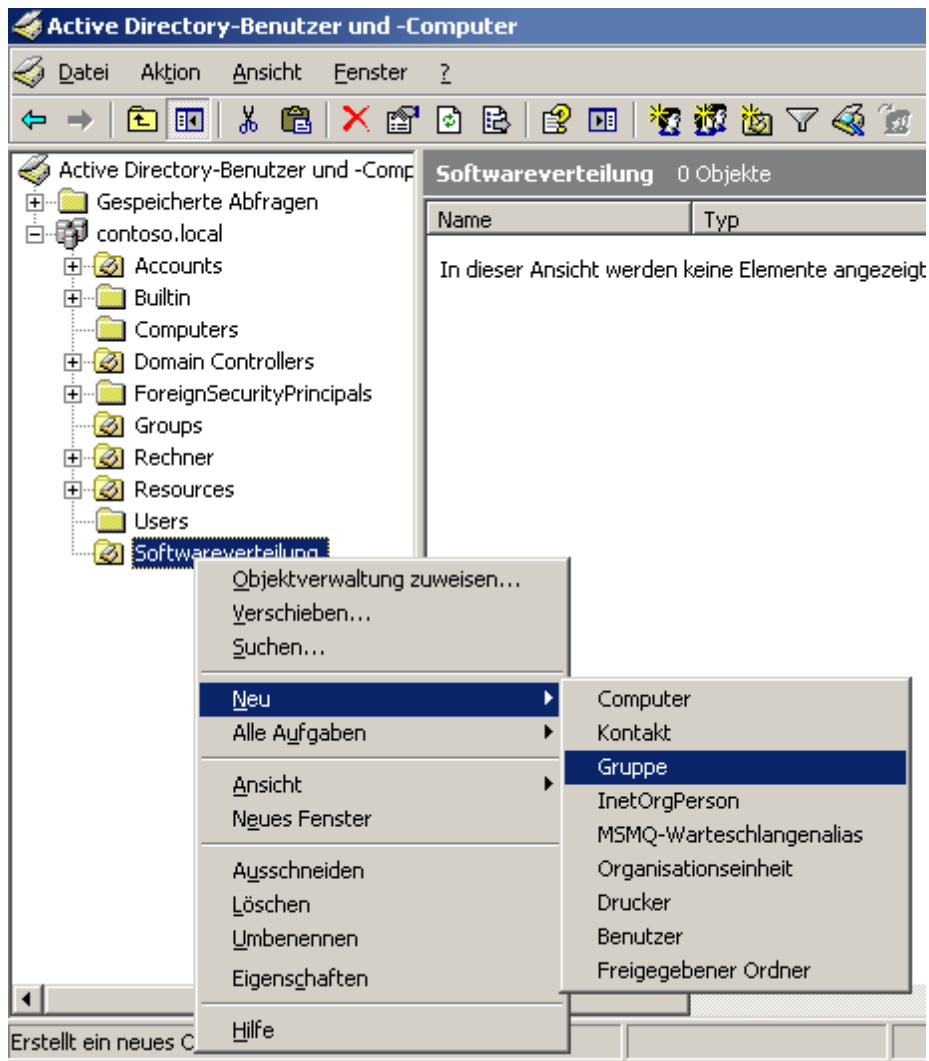
1. Click on the Start menu and then Control Panel > "Active Directory Users and Computers". Now create a new organizational unit (OU).



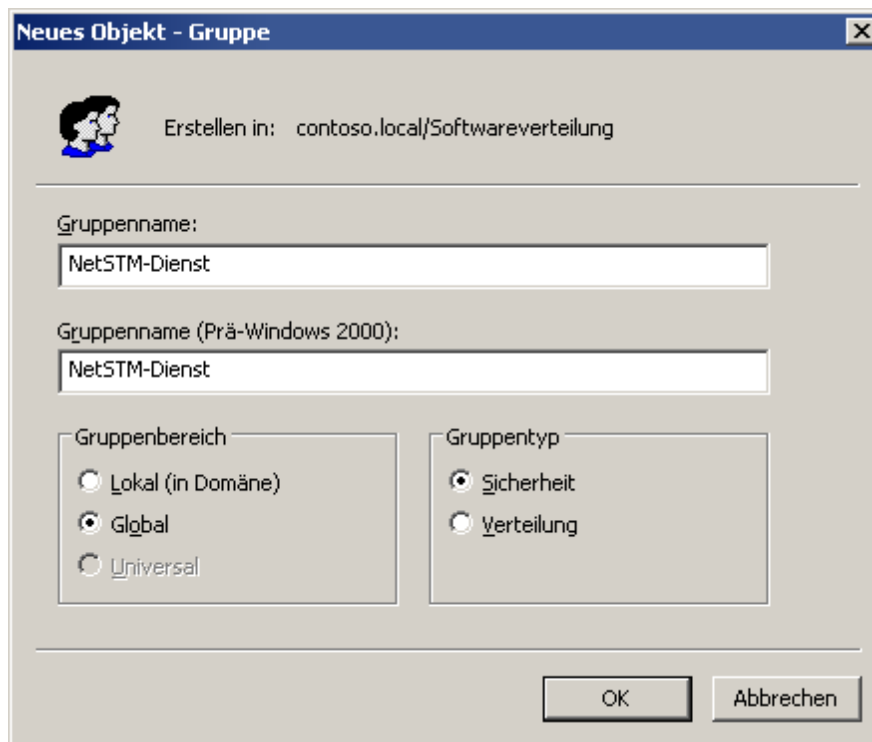
2. Give the OU a name, e.g. "softwaredistribution".



3. Create a new group **NetSTM-service** in the OU "softwaredistribution".

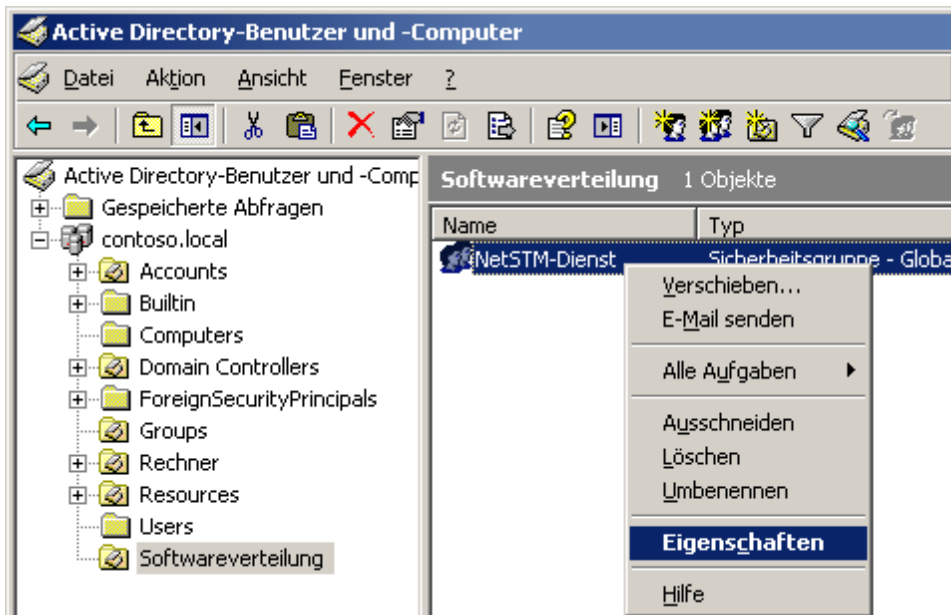


with the following parameters:

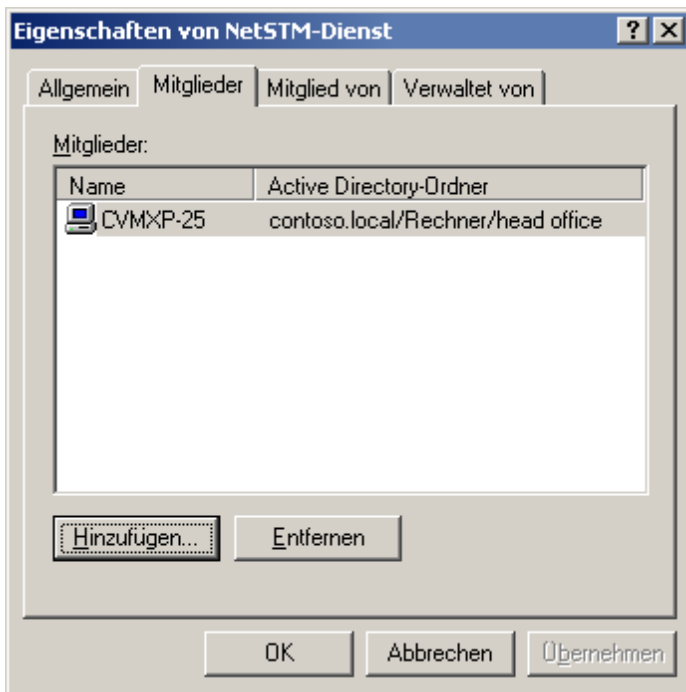


Click on **OK**.

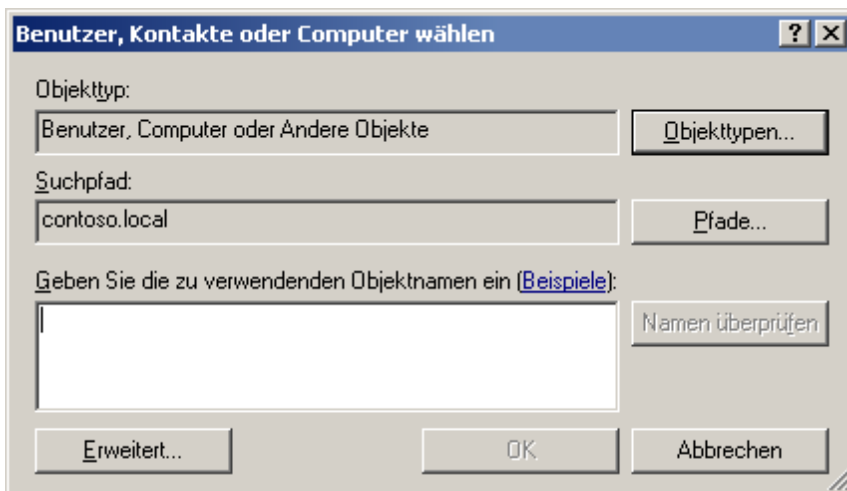
4. Double-click on the newly created group (or right click -> Properties)



5. Click on **Add** to select the computer on which the NetSTM-service NetTaskAgent.msi will later be installed.



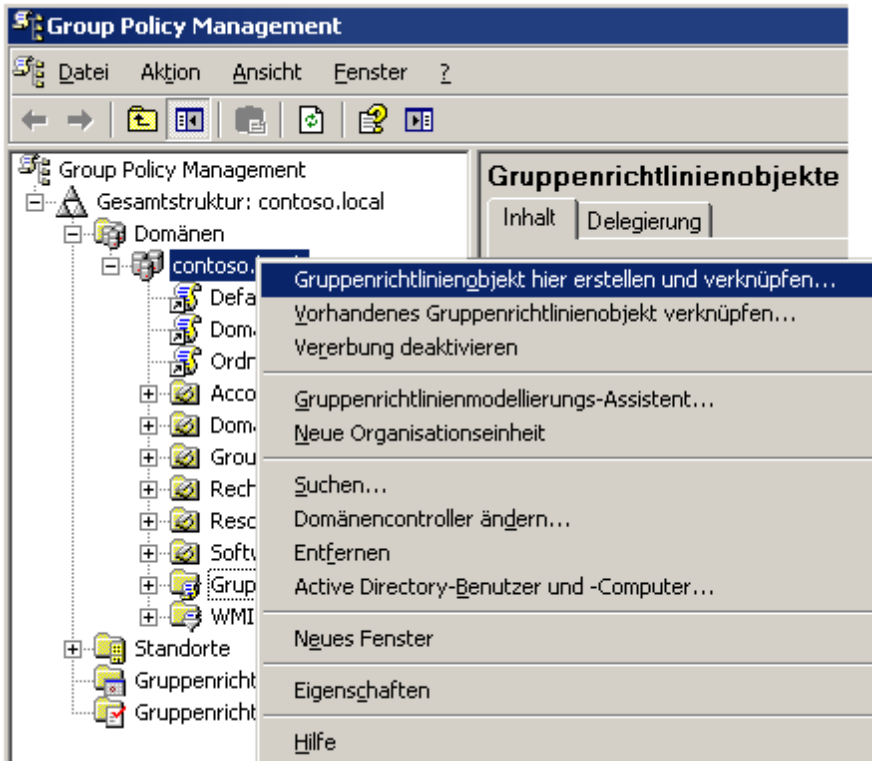
Hint: Click on "**Object types ...**", to verify that Computer is displayed as well. Click on "**Advanced ...**" and then click on "**Find Now**" to see the available clients to see.



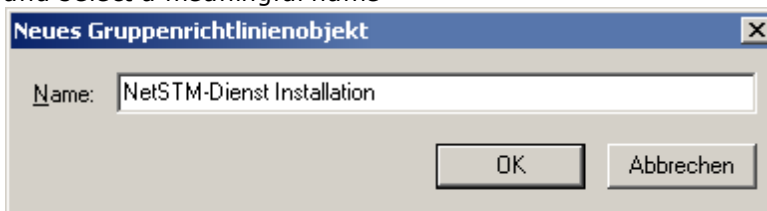
Then finally click **OK** to take over the selected computers.

B) Create the group policy

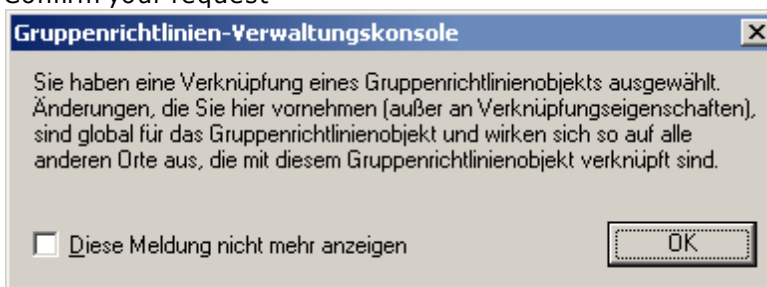
1. Start the Group Policy Management. To do this, execute GPMC.msc or click on the Control Panel or in the Start menu, on Administration > Group Policy Management.
2. Click with the right mouse button on "Create and link group policy object ...".



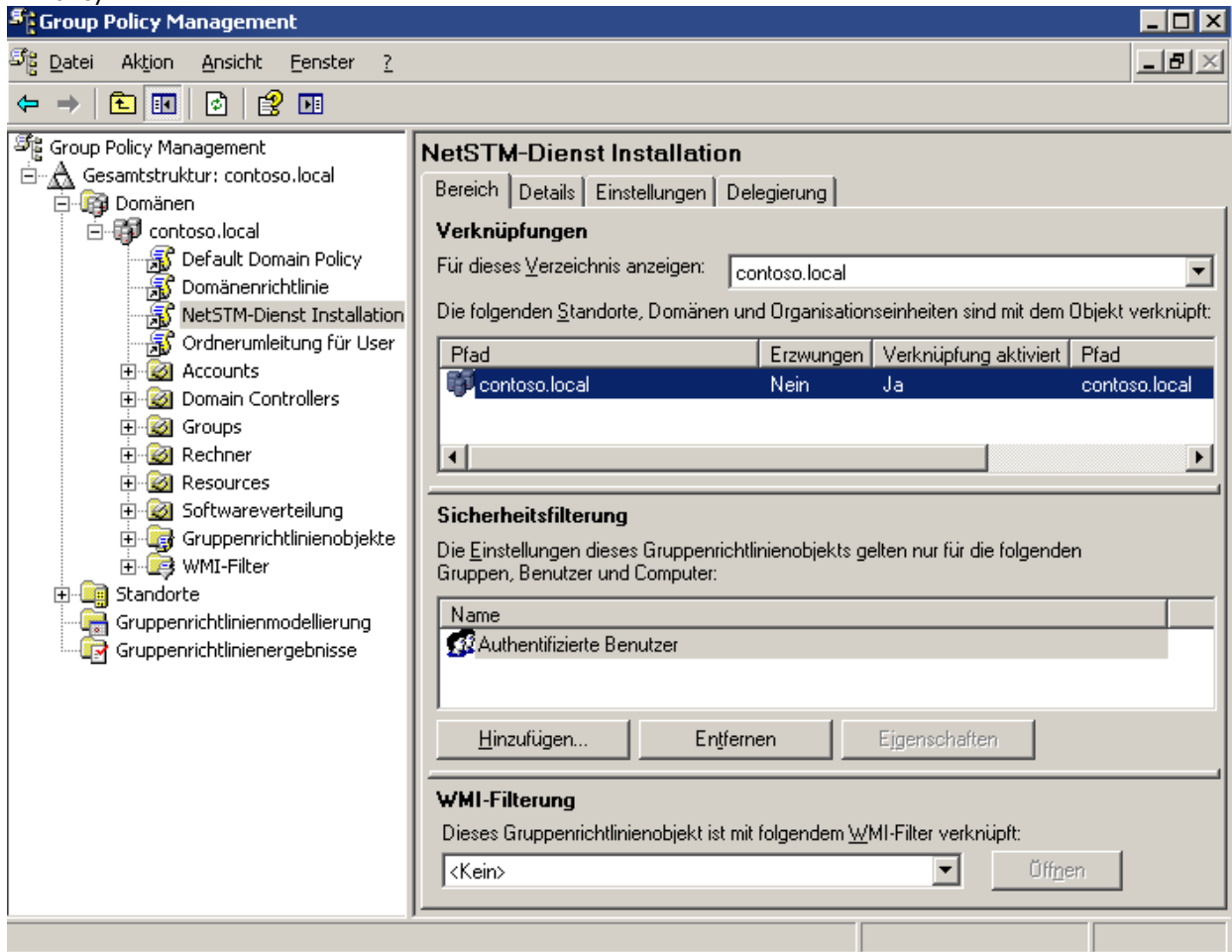
and select a meaningful name



Confirm your request

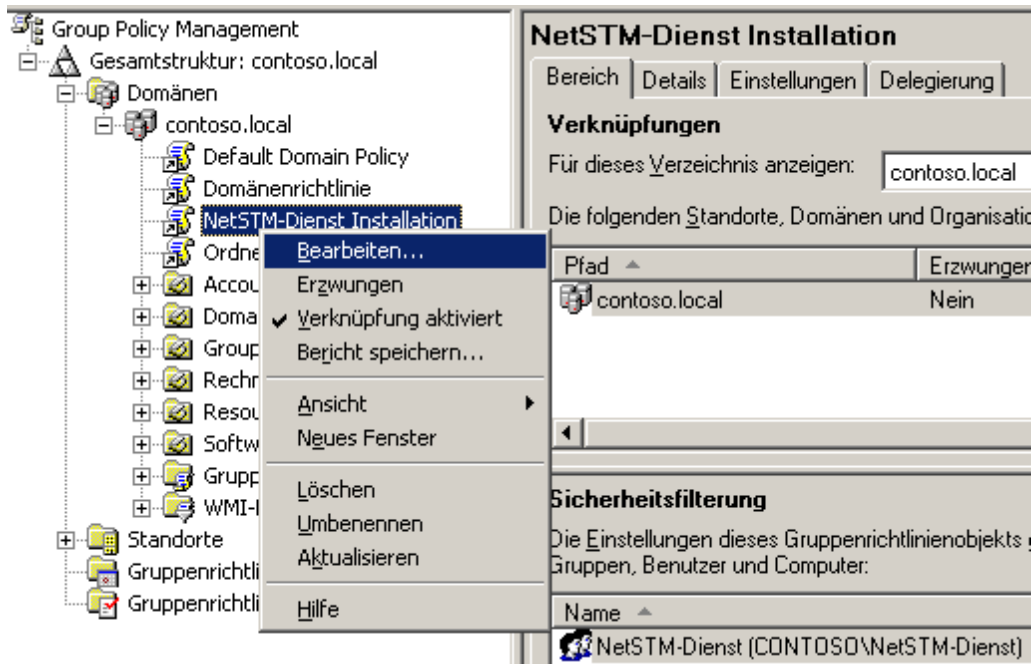


3. Now the group policy just created appears under the domain name and the "Default Domain Policy".

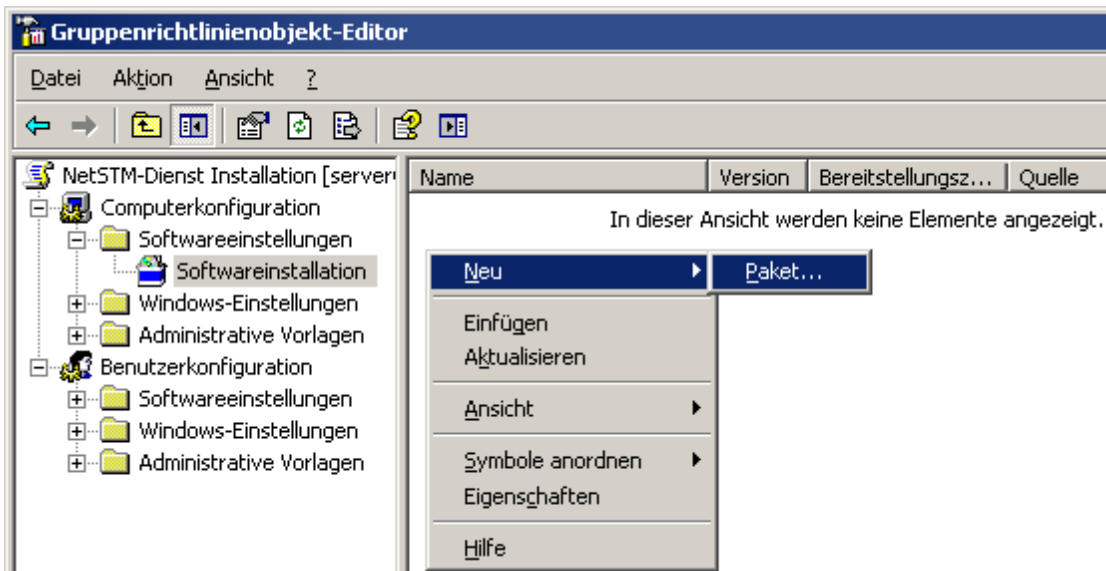


Remove the "Authenticated Users" group and by using **Add**, add the previously created security group "NetSTM-service". By doing this, the scope of this group policy is limited to the security group "NetSTM-service".

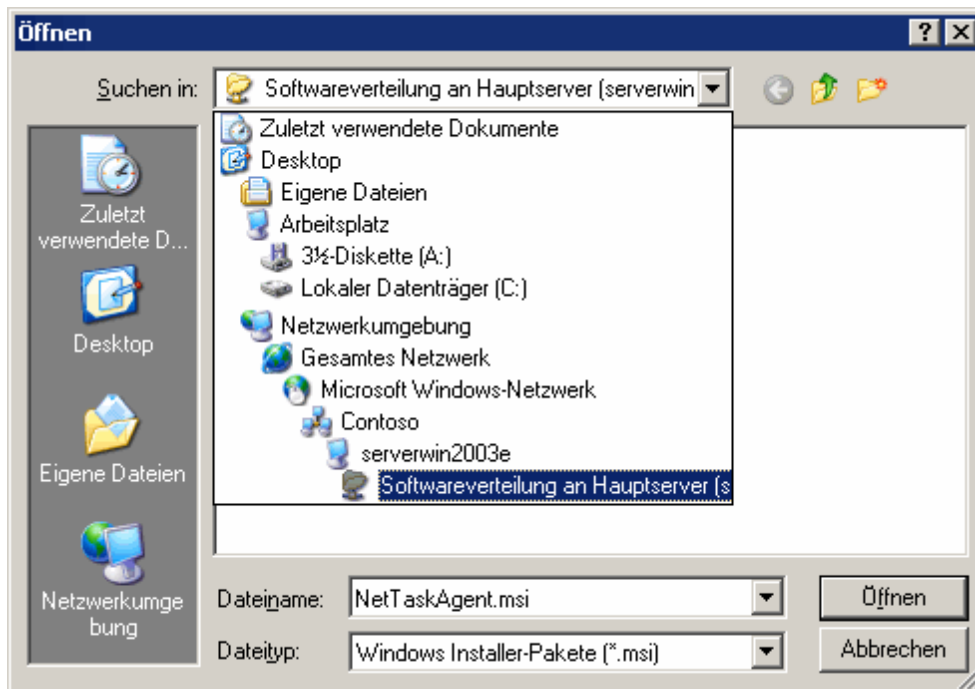
4. Click with the right mouse button on the group policy just created, "NetSTM-service installation". Click on "**Edit ...**".



5. In the Group Policy Object Editor, click on Computer Configuration > Software Settings > Software Installation. Now click with the right mouse button on the white field.



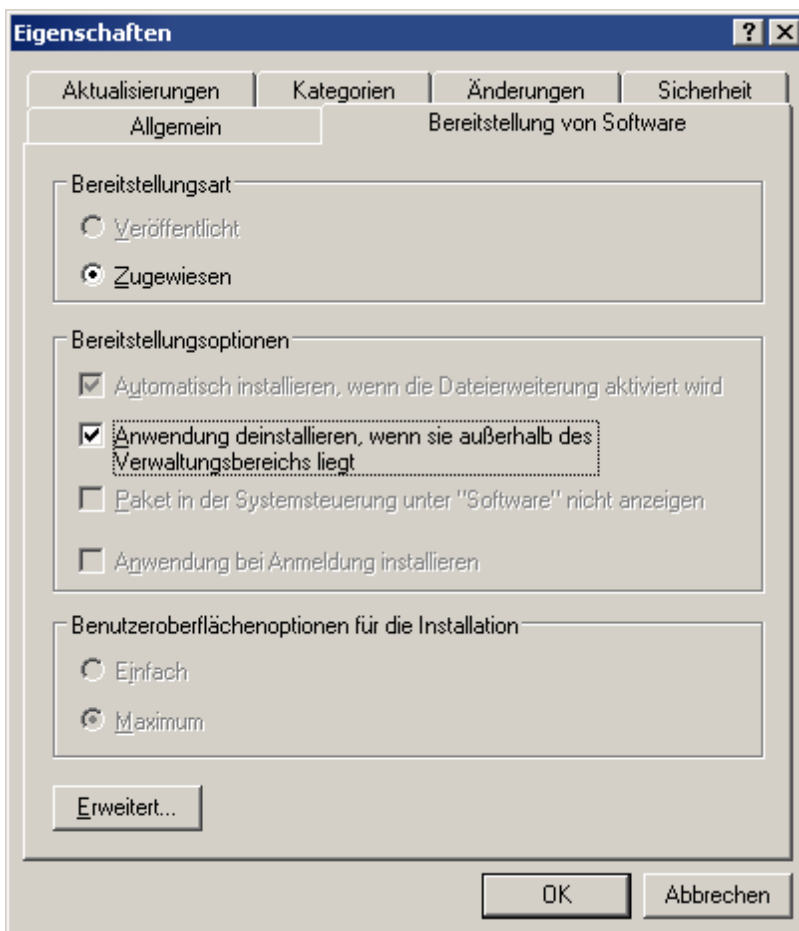
6. Select the MSI package with UNC path, as \\server\softwareverteilung\NetTaskAgent.msi



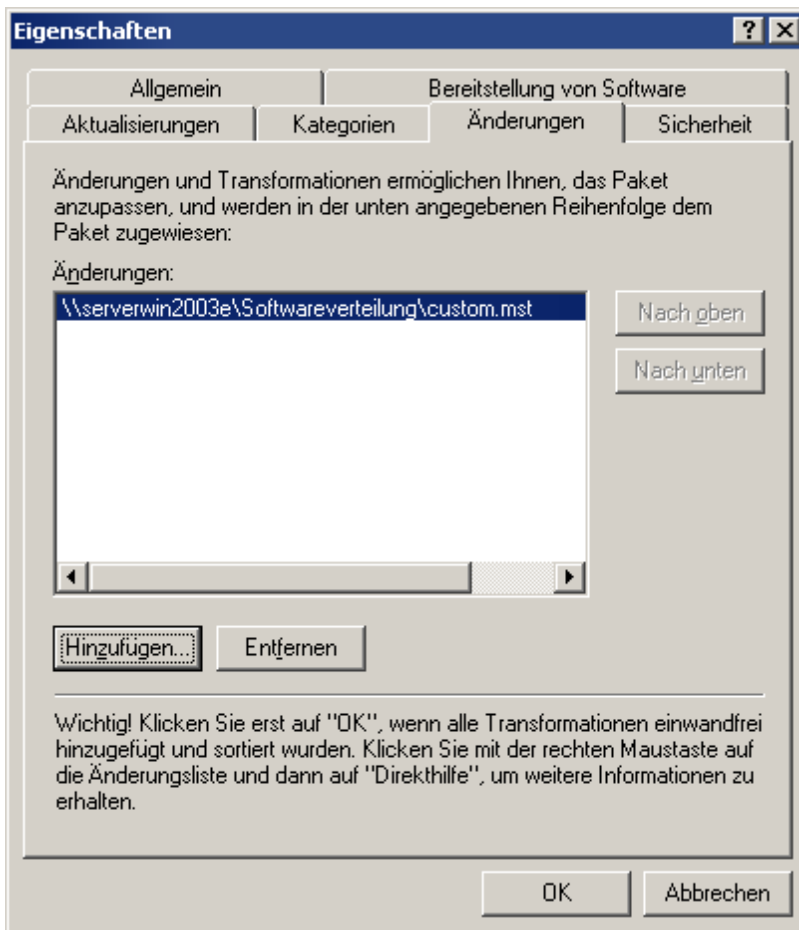
Select the **Advanced** option.



7. Now click the tab for **Software deployment**. Select the option "uninstall application if outside the administrative domain". In this way, the Net-STM-service software is automatically uninstalled from a client, as soon as the client is removed from the "NetSTM-service" security group.



8. Now click on the tab **Changes**. Add the **custom.mst** file that was modified with ORCA.

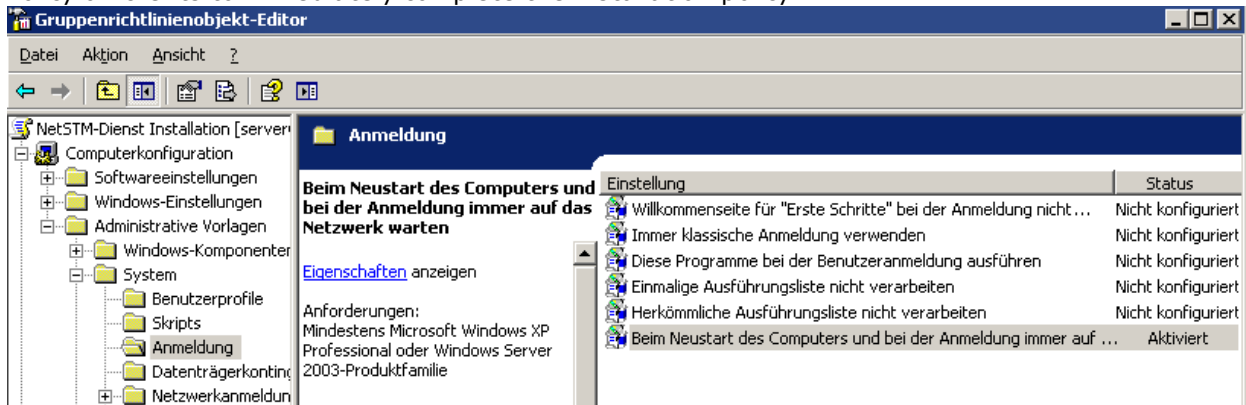


Click on **OK** and close the GPO Editor.

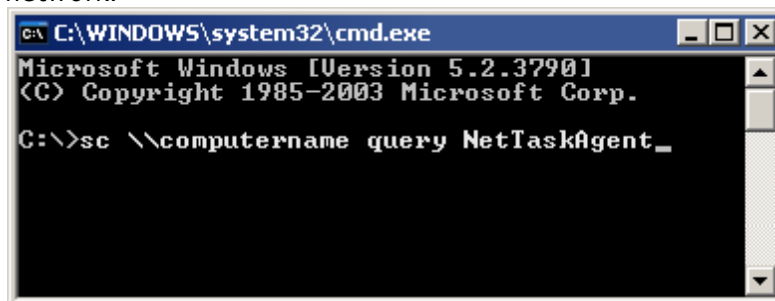
C) Installation of the agent on the workstations.

The selected clients of the security group "NetSTM-service" will now install the agent after one to three restarts.

As administrator, run command "gpupdate /Sync" on the client or change the following Group Policy on clients to immediately complete the installation policy:



Hint: To check from the Admin PC whether NetSTM-service is running on a client either click on [Test now](#) within [Computer properties](#)¹³⁾, or run the command `sc \\clientname query nettaskagent`. In this instance, *clientname* is the computer name of the workstation on the network.



Uninstalling an MSI package

To uninstall the remote agent from a client, you must remove this client from the "NetSTM-service" security group.

In the Start menu, click on Control Panel > "Active Directory Users and Computers". Click with the right mouse button on the security group "NetSTM service". Click on **Properties**.

Then after that click the **Members** tab and remove the desired computer.

Note

- The uninstall of the MSI package can also be started with the following command (for example, at the [command prompt](#) or via a login script):
`msiexec /x{986222E8-C018-4DA2-94BC-9B796A5A75A5} /qb`
- As an administrator, you can also use the command `NetTaskAgent.exe /u` or from a remote computer completely uninstall the remote agent with the command `sc \\target-pc delete nettaskagent`.
- With the command `runas /user:administrator cmd`, you can start the [command prompt](#) with administrator rights (e.g. as user "administrator").

Index

- A -

- Add
 - Comment 19
 - New Computer 11
- Admin\$
 - Admin share 31
 - Connection error 38
 - Windows 8/7/Vista 33
- Agent 9

- C -

- Client Agent 9
- Comments on processes 19
- Computer
 - Add 11
 - Group together 12
 - Properties 13
 - Remove 14
 - Scan 22
 - Set up scheduling 15
- Connection error 38
- Connection errors 41
- Console 8
- Core component 8
- CPU Time 23

- D -

- Database
 - Add processes 19
 - Overview 18
 - Removal of processes 20

- E -

- Error log 40
- Error messages 42
- Event Viewer 17
- Events display of a client 40

Export 22

- F -

- File and Printer sharing 42
 - Admin\$ 31
 - resolve connection problem 38
 - Simple File Sharing 32
- Folder 35

- G -

- Google Search 24
- Group
 - Create 12
- Groups
 - Add new computer 11

- I -

- Import 11
- Install
 - msi Package (Client Agent) 54
 - Network Security Task Manager 8
- Internet
 - Online process database 24
 - Process Type 29
 - Product Homepage 46

- K -

- known process 19

- L -

- Log
 - Dangerous processes 24
 - Technical errors 40

- M -

- Masking harmless processes 18
- MD5 checksum 19
- msi Software distribution 48
- mst file 49

- N -

- NetTaskAgent 9
- NetTaskTray 30
- Network Security Task Manager
 - Display of processes 23
 - Distribution of agents 9
 - Files used 35
 - Install 8
 - Overview 5
 - System requirements 7
 - Technical Support 46
 - Uninstall 36
 - Verwendete Dateien 25

- O -

- Ordner 25

- P -

- Popup Warning message 17
- Print 22
- Process log 24
- Process notices 19
- Processes
 - Comment 19
 - Evaluation 27
 - Mask 18
 - Online Information 24
 - Print 22
 - Properties 23
 - Scan 22
 - Stop 25
 - Type 29
- Properties 24
 - Computer 13
 - Processes 23

- Q -

- Quarantäne 25
- Quarantine 25

- R -

- RAM 23
- Ranking 27
- Reference database 18
- Remove
 - Comment 20
 - Computer 14
- requirements 7
- Risk Rating 27

- S -

- Save
 - Export 22
 - Print 22
- Scan 22
- Scheduling 15
- Share
 - Admin\$ 31
 - Simple File Sharing 32
 - Windows 8/7/Vista 33
- Simple File Sharing 32
- SMB 34, 38
- Software distribution by msi 48
- System requirements 7

- T -

- Tasktray (NetTaskTray) 30
- Terminate
 - NetTaskAgent 36
 - Processes 25
- Troubleshooting 38, 41, 42
- Type 29

- U -

- Uninstall
 - msi-Package (Client Agent) 67
 - Network Security Taskmanager 36
- Updating agents 9

- V -

View 23

- W -

Warning about process exceptions 17

Web Information 24

Windows 8/7/Vista 33

Workstation component 9