NETOP™

ProtectOn™ PRO

Endpoint Protection Software

User's Guide

Version 1.1

Netop

Please send any comments to:
Netop Business Solutions A/S
Bregnerodvej 127
DK-3460 Birkerod
Denmark
Fax: Int +45 45 90 25 26
E-mail: info@netop.com
Internet: www.netop.com

The document is optimized for double-sided printing.

Contents

1 Netop ProtectOn Pro overview

1.1 Introduction to Netop ProtectOn Pro

Netop ProtectOn Pro is a tool for IT administrators who manage networked computers, including networked computers that do not have permanent users. Examples of networks with many different users are computers at schools, Internet cafés, and hotels. IT administrators of computers with many different users typically focus on these tasks:

- Keeping the networked computers free from user-installed software, so that the computer does not run out of disk space.
- Protecting data from accidental or deliberate alterations as well as execution of malicious code.
- Preventing recreational or inappropriate Internet surfing.
- Preventing the use of inappropriate software.
- Ensuring the most efficient use of computer facilities.

Netop ProtectOn Pro features

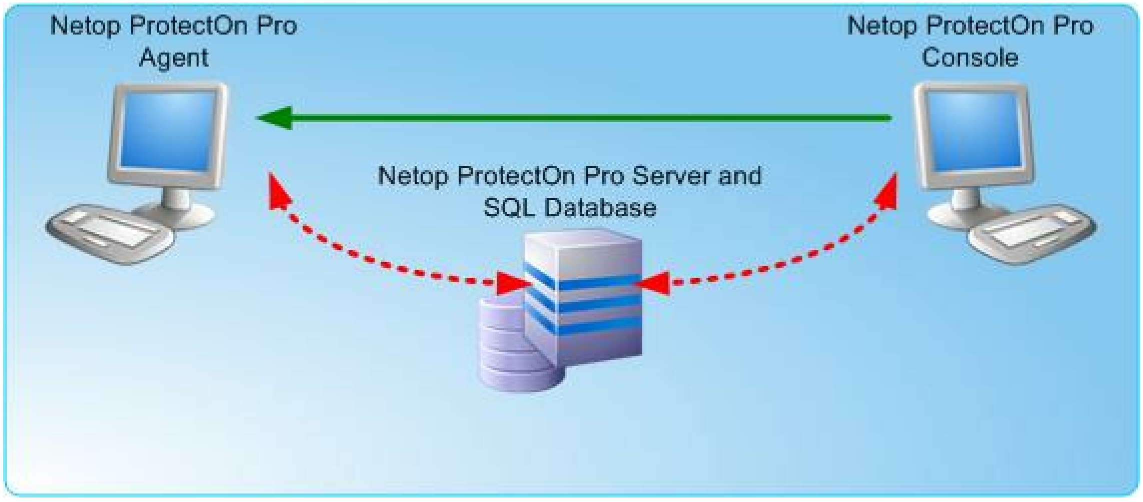
To assist the IT administrator in handling these tasks, Netop ProtectOn Pro includes functionality to:

- Automatically remove all hard disk changes on , and return the hard disk to its initial state. Exceptions can be defined for certain folders where changes are permitted, and certain applications - like for example antivirus software - can be allowed to make permanent changes to hard disks.
- Grant or deny access to system devices like hard disks, DVD/CD and floppy drives, parallel and serial ports, USB and WiFi devices.
- Hide hard disk contents from users or let users view certain folders only.
- Deny access to inappropriate Internet sites.
- Disallow running specific applications.
- Browse Microsoft Windows networks to obtain information about networked computers.
- Manage networked computers remotely.

Netop ProtectOn Pro components

Netop ProtectOn Pro consists of three components:

- Netop ProtectOn Pro Server
- Netop ProtectOn Pro Console
- Netop ProtectOn Pro Agent


Netop ProtectOn Pro Agent
Netop ProtectOn Pro Console
Netop ProtectOn Pro Server and SQL Database

The Server handles access to the SQL database located on the same computer as the Server, or on another computer. The Console is the administrator’s tool for administration of policies and other management functions. The Agent is installed on the computers that the administrator wants to apply policies on or wants to manage via the Console functionality.

1.2 How Netop ProtectOn Pro works

Netop ProtectOn Pro uses the concepts of *groups* and *policies*; policies are assigned to groups.

A group can include the following objects:

- Windows domain objects: Computers (workstations and servers), Windows Network Users, Windows Network Groups.
- Active Directory objects: All Windows domain objects (users, groups, computers), Containers, Organizational units.

There are four types of policies:

Hard disk protection policy	A hard disk protection policy is used to protect hard disk contents from harmful changes. With a hard disk policy the administrator can select drives to be protected, enable restoring of the hard disk drive's initial state on reboot, choose exception folders that are not cleared on reboot and choose applications that are allowed to make permanent changes to hard disks.
Device access policy	A device access policy is used to grant or deny access to system devices, such as floppy and DVD/CD-ROM drives, USB devices, Bluetooth devices, and serial ports. It also allows hiding hard disk contents from users.
Web policy	A Web policy is used to grant or deny access to Internet sites.
Application policy	An application policy is used to define which applications can or cannot be run.

You can create as many policies of the same type as you need.

Each policy is assigned to a group, which can consist of the objects listed above, but at the basic level a policy is applied to either computers or users. Therefore, if a group contains, for example, an Active Directory organizational unit, policies are applied to the users and computers that are included in this unit. If this unit, in turn, contains other units, the policies are applied to their members, too. The same is true for Windows network groups.

When a policy is applied to a user, this means that it is active only for a particular Active Directory or Windows network user. When a policy is applied to a computer, this means that the policy is active for all users that utilize this computer.

A hard disk protection policy can be applied to computers only, whereas device access policies, Web policies and application policies can be applied to both computers and to users. If a hard disk protection policy is assigned to a group that contains both computers and users, the users of the group are ignored and the policy is applied only to the computers.

Within a policy type, policies that are applied to a user have top priority: if there are user-level policies, then the policies at computer level are ignored. For example, when you apply two different policies, one of which denies Computer 1 access to the site www. funniest&coolest_games.com, while the other allows users of Computer 1 access to the site, the user-level policy will have higher priority, and consequently access to the site is allowed. However, a policy option allows you to make a policy a higher-priority one so that it can override other policies of its type.

1.3 Supported operating systems

Netop ProtectOn Pro supports a wide range of operating systems. These features are available with each operating system:

Operating Systems ▶ **▼ Modules or sessions**	**2008/2003/Win7/ Vista/XP[2] (64-bit)[1]**	**2008/2003/Win7/ Vista/XP2)/2000[3]**	**NT4[3]**
Netop ProtectOn Pro Server	x	x	
Netop ProtectOn Pro Console	x	x	
Agent: Hard Disk Protection	x	x	x
Agent: Device Access	x	x	
Agent: Application Access	x	x	x
Agent: Web Access	x	x	x
Remote management	x	x	x
Remote control	x	x	x

1) Windows Server 2008, 2003 Standard, Web Edition, Enterprise edition. Windows 2000 Server and Advanced Server. Windows 2000 Professional, Service Pack 2.

2) Windows XP, Service Pack 2

3) Including the Windows 2000, Service Pack 4, and NT4 server versions, Service Pack 6.

Note

- The Remote control feature depends on whether Netop Remote Control has been installed or not: if Netop Remote Control Guest is available on the Netop ProtectOn Pro Console, Netop ProtectOn Pro activates this program. If Netop Remote Control Guest has NOT been installed, Windows **Remote Desktop Connection** is activated.

2 Configuration and connection settings

2.1 Server settings

When the Server component has been installed, it has default settings and is operational with no further setup. Changes to the default settings, for example for test purposes or if the SQL server or database is changed, can be defined from Netop ProtectOn Pro Server Settings.

The Server settings dialog box is opened from Windows' **Start** menu: **All Programs** > **Netop ProtectOn Pro** > **Server Configuration**.

⊟ **Connection properties tab**

The **Connection properties** tab page defines how the Server component works with the SQL Server database that stores the device policies.

Configuration and connection settings

Option	Description
Server name	To use another SQL Server, type the name of the server and the Netop ProtectOn Pro Server automatically locates the SQL Server on the network.
Use Windows NT Integrated security	Integrated security uses the current Windows identity to access the SQL Server database. You can then map the Windows identity to an SQL Server database and permissions. This is the default setting.
Use a specific user name and password	Select this option if you want to use a user name and password that are different from the Windows user name and password.
Database name	To use another database, type the name of an existing database on the SQL Server. Use the **Test Connection** button after changing the database name. **A note on changing database after installation** We do not recommend that you change the database name unless you are an experienced SQL database manager. The installation program automatically creates and initializes an empty SQL database. If you want to change database after the initial setup, you must create the database manually. When the database has been created, you must run the DB_All.sql script manually. The script was installed with the Netop ProtectOn Pro Server. If you want to use a different database name than the default one, NPP_DB, you can do a find-replace in the script file.
Port number	Port 1973 is the default port. The port number can be changed but should match the port server setting on the Console and on the Agent. For a description of those settings and where to set them, see Console settings and Agent settings.

Note

Once you have configured the Console, return to this tab and test the connection.

The **Test Connection** button checks whether the Server can see the data base and whether the user has sufficient rights to access the database.

Licensing tab

The **Licensing** tab shows the current licenses.

Option	Description
License Name	License file name. Click **Install** to add a new license file, or **Remove** to remove an existing.
Limit	The number of Netop ProtectOn Pro Agents which can be controlled by the Netop ProtectOn Pro Console. **Note** The list can contain several licenses; the numbers listed are simply added up. For example, if you have a 10 user license and a 20 user license, your system can control 30 users.
Expired	The date the license expires.
Type	List of modules included in the Netop ProtectOn Pro installation: • Application Blocker • Web Blocker • Hard Disk Protection • Device Access These are the areas where policies can be defined.
Comments	Textual comments from the license file.

Use the **Reset connections** button to count the number of active Agents. This is useful in situations when the limit for Agent installations has been reached and one or more computers with Agent software installed are taken off the network. Clicking **Reset connections** will then ensure that the computers no longer on the network do not count against the limit.

⊟ Miscellaneous tab

Configuration and connection settings

Option	Description
Network scanning interval	The interval by which the Netop ProtectOn Pro Server must search the network for MAC addresses and USB devices. The recommended setting is 3,600 seconds.
RM Port Number	The port number on the Netop ProtectOn Pro Server to be used for remote management. Port 1972 is the default setting.
Download policy interval	The interval with which the Netop ProtectOn Pro Server downloads new and changed policies to the Agents. The recommended setting is 900 seconds.
Apply policy interval	The interval with which the Netop ProtectOn Pro Server applies new or changed policies on Agents. The recommended setting is 900 seconds.

2.2 Console settings

When the Console component has been installed, it has default settings and is operational with no further setup. The first time you start the Netop ProtectOn Pro Console after installation, the **Settings** dialog box opens for informational purposes. Subsequent changes to the default settings, for example if the Server is re-installed on a different machine, can be set from the **Settings** dialog box.

The Console settings dialog box is opened from within the Netop ProtectOn Pro Console program: **File > Settings**.

Option	Description
Computer name	The name of the computer where the Netop ProtectOn Pro Server is installed.
Port Number (Netop ProtectOn Pro Server)	The port number on the Netop ProtectOn Pro Server used for communication with the Console. The port number can be changed but should match the port server setting on the Netop ProtectOn Pro Server and on the Netop ProtectOn Pro Agent. For a description of those settings and where to set them, see Server settings and Agent settings.
Port Number (Remote management)	The port number on the Console used for remote management of agent computers.

If you log on to an Netop ProtectOn Pro Server where you do not have proper credentials, you will get an "Error Connecting to ProtectOn Pro server" message. If you click **No** to the question about specifying other credentials, you will get view access to Netop ProtectOn Pro Server data, but you will not be able to make any changes.

If you click **Yes** to the question about specifying other credentials, and the new credentials are the administrator ones, you will be able to create new policies and groups as well as modify existing policies and groups.

2.3 Agent settings

When the Agent component has been installed, it has default settings and is operational with no further setup. Changes to the default settings, for example if the Server is re-installed on a different machine or during test when logging requirements might change, can be set from the **Netop ProtectOn Pro Agent Settings** dialog box.

The Agent settings dialog box is opened from Windows' **Start** menu: **All Programs** > **Netop ProtectOn Pro** > **Agent Configuration**.

Note
To prevent unauthorized Agent users from making configuration changes, access to the Agent Settings dialog box can be protected with a password. The password is defined from the Console: On the **File** menu, click **Agent Settings**.

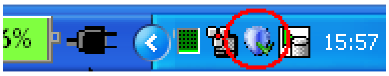
⊟ General tab

Option	Description
Host name	The name of the computer where the Netop ProtectOn Pro Server is installed. To connect to a different server, type another computer name. If you enter a non-existing server name, the server icon in the notification area turns gray.
Port number	The port number used for device control. Port 1973 is the default port.
Service account	Select this option to connect to the Netop ProtectOn Pro Server using Windows authentication.
This account	Select this option to define different access rights. Click the Browse button (...) to select an account.
Port number (Remote management connection)	The port number used for remote management. Port 1972 is the default setting. **Note** The port numbers can be changed but should match the port server setting on the server and on the console. For a description of those settings and where to set them, see Server settings and Console settings.

⊟ Restriction messages tab

Use the options to define whether the Netop ProtectOn Pro Agent should display all, some or no messages informing the user about restrictions that block access to use of devices or programs, or access to sites.

The settings on this tab can also be changed from the Netop ProtectOn Pro Agent dialog box, which is opened by double-clicking the Netop ProtectOn Pro Agent icon in the notification area:



Agent icon has three different looks:

- Normal, as shown above.
- Gray. If the Agent has failed to connect to the Netop ProtectOn Pro Server three consecutive times, the icon turns gray. This is to inform the user that there are connectivity problems. The Agent will continue trying to connect, meanwhile using its old policies. Once connection is established, the icon returns to normal.
- Red **X**. The icon has a red **X** across it if license conditions are violated. For example, the sixth Agent computer that tries to connect to a five license Netop ProtectOn Pro Server will be denied access and have a **X** across the icon. The Agent will not be able to communicate with the Netop ProtectOn Pro Server.

⊟ Logging tab

Use the options on this tab to define the extent of logging: whether repeatable messages are logged and whether log files are limited by size or by time. When a log file is limited, it is re-used cyclically when the size or hour limitation is reached.

2.4 Remotely install the Agent module

For Netop ProtectOn Pro to offer hard disk protection or control access to programs, resources and Internet sites the Agent module needs to be physically located on client computers and run as a service.

As the number of computers can be large, and as they may not be located on the same site, the Console includes features to remotely install and uninstall the Agent module.

However, if you have a large number of client computers that you want to distribute the Agent to, this method might not be practical and you might prefer to use the Agent installation file (NPPAgentSetup.msi) instead.

Note

As with other types of install, remote install requires administrator access to the computer where the Agent module is installed.

⊟ Install the Agent module from the Console

1. Select a computer in the **Network** pane, either in **Active Directory** or in **Microsoft Windows Network**.
2. Right-click the computer and select **Install Agent** on the shortcut menu.

   The progress bar will show the installation progress. When finished, click **Close**.

This will install and start the Agent as a service and the computer can be protected with policies defined from the Console.

If you later need to remove the Agent module from a computer, right-click the computer and then click **Uninstall Agent**.

⊟ Install the Agent module using the Agent installation file

An installation file can be distributed and run in a number of different ways, for example from a logon script or using Group Policy in Active Directory.

The Agent installation file must be run with parameters that specify Netop ProtectOn Pro Server name and Netop ProtectOn Pro Server port. To configure an Agent to connect to ***policyservername*** and to use port ***port*** the command line looks like this:

NPPAgentSetup.msi ACTION=INSTALL POLICYSERVER=***policyservername*** SERVERPORT=***port***

Replace ***policyservername*** and ***port*** with the settings that match your actual environment.

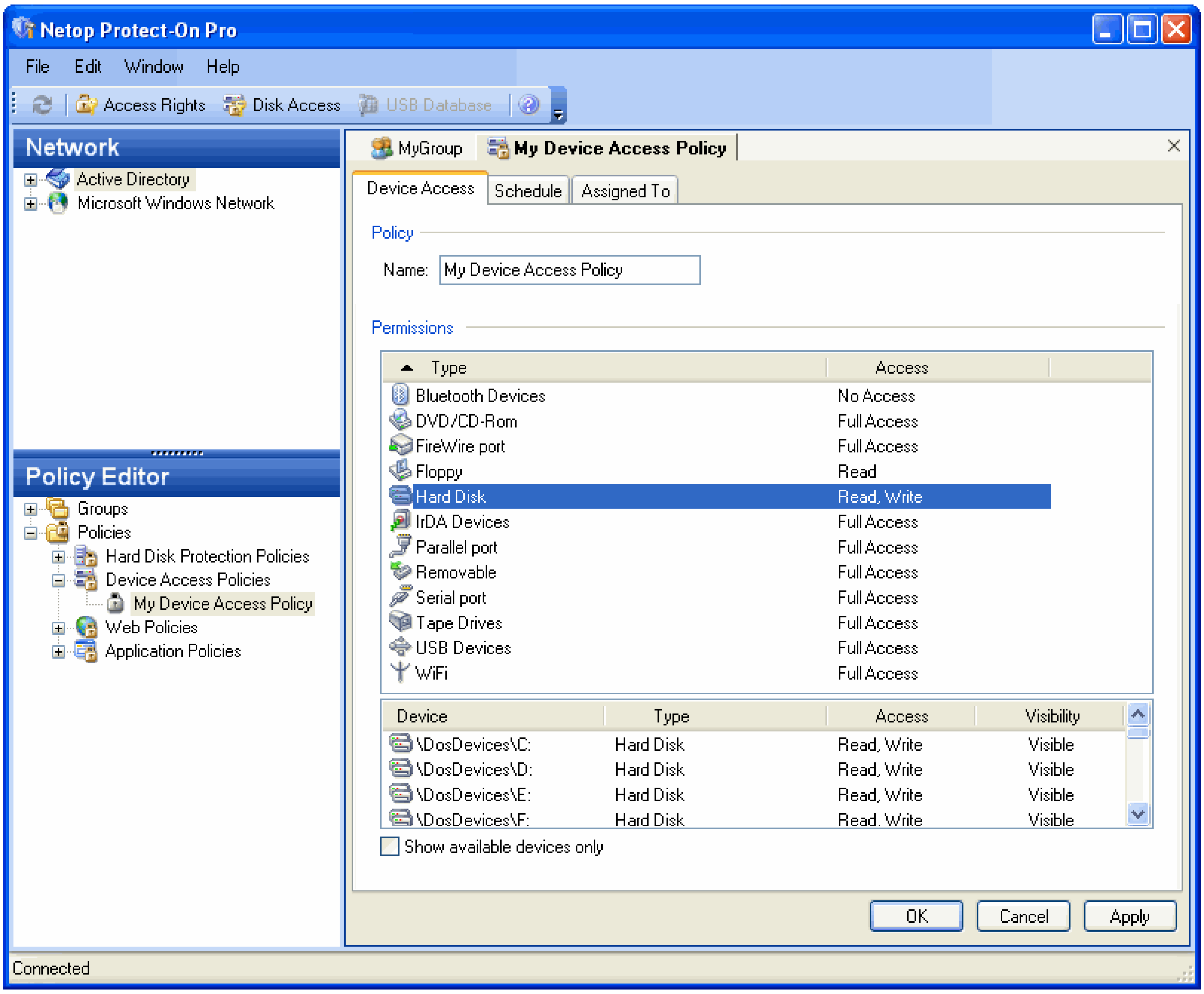
To create a transform file (MST) for the MSI file, you will need to specify the POLICYSERVER and SERVERPORT properties.

3 Netop ProtectOn Pro Console

3.1 Console user interface

The Netop ProtectOn Pro Console user interface consists of these four components:

- Menu bar and toolbar
- Network pane
- Policy Editor pane
- Data panel



Name: My Device Access Policy

Type	Access
Bluetooth Devices	No Access
DVD/CD-Rom	Full Access
FireWire port	Full Access
Floppy	Read
Hard Disk	Read, Write
IrDA Devices	Full Access
Parallel port	Full Access
Removable	Full Access
Serial port	Full Access
Tape Drives	Full Access
USB Devices	Full Access
WiFi	Full Access

Device	Type	Access	Visibility
\DosDevices\C:	Hard Disk	Read, Write	Visible
\DosDevices\D:	Hard Disk	Read, Write	Visible
\DosDevices\E:	Hard Disk	Read, Write	Visible
\DosDevices\F:	Hard Disk	Read, Write	Visible

☐ Show available devices only

Menu bar and toolbar

The menu bar has the **File**, **View**, **Window** and **Help** menus and may have additional menus available depending on the object selected in the **Network** pane, the **Policy Editor** pane or the data panel.

The toolbar beneath the menu bar contains buttons for menu commands. The number and availability of buttons also depend on the object selected in the **Network** pane, the **Policy Editor** pane or the data panel.

Network pane

The **Network** pane allows you to:

- Browse both Active Directory and Microsoft Windows networks to pick up objects to include in groups.
- Manage Active Directory network by means of the standard Active Directory Users and Computers Microsoft Management Console snap-in.
- View tooltip with information about Microsoft Windows Network workstations, which includes domain and user name, IP address, and operating system version.
- Open a session on a networked computer that has an Agent module installed.

Policy Editor pane

The **Policy Editor** pane allows you to:

- Create four types of policies: Hard Disk Protection Policies, Device Access Policies, Web Policies, Application Policies.
- Create groups of objects to assign policies to.
- Assign policies to groups.

If a policy is assigned to at least one group, it is marked with a 🔒 symbol. If a policy is not assigned to any groups, it is marked with a 🔒symbol. If a policy overrides other policies, it is marked with an exclamation mark (🔒).

Data panel

Data panel displays information about an object when you double-click it in the **Network** pane or in the **Policy Editor** pane.

The object can be:

- A network object
- A policy
- A group to assign a policy to

One or more data panels can be opened simultaneously.

By default, the information for different objects is presented in the form of tabs, but you can change the presentation by selecting **Window** > **Cascade**, or **Window** > **Tile** on the menu bar.

3.2 Browse a network tree

To browse the **Active Directory** or the **Microsoft Windows Network** tree, use ⊞ and ⊟ to expand and collapse its branches, respectively.

To display the properties of an object in the data panel, double-click an object in the tree.

When browsing **Active Directory** networks, you can connect to any network domain. The fact that you can connect to another domain is useful because it means that you can reach any computer on the network.

Connect to a domain

1. Right-click **Active Directory** in the **Network** pane and select **Connect to Domain**.
2. In the **Connect to Domain** dialog box type the name of the domain you want to connect to, or click **Browse** to select from the domain list.

Note

After restarting the Netop ProtectOn Pro Console, the default domain will be displayed in the Active Directory node. The default domain is the one the computer is a member of.

3.3 Manage Active Directory networks

From within the **Network** pane you can manage Active Directory networks conveniently using **Active Directory Users and Computers** snap-in for **Microsoft Management Console** (MMC). **Active Directory Users and Computers** allows management of users, groups, organizational units, and all other Active Directory objects.

Note

To manage an **Active Directory** network, you must first install the Microsoft Management Console, unless it is already installed as part of your operating system. MMC is included in the Windows 2000 and later operating systems. **Active Directory Users and Computers** snap-in should also be installed on the administrator's computer. This snap-in is a part of Win2003/Win2008 Admin Pack and ships with Windows 2003/2008. It can also be installed on Windows 2000 and XP. MMC is available from the Microsoft Download Center.

Manage an Active Directory object

1. Select an object in the **Active Directory** tree.
2. Right-click the object and select **Open in MMC** on the shortcut menu.

   The **Microsoft Management Console** opens and displays the selected object.

   You can also use the **Open Properties in MMC** command on the shortcut menu. By choosing this option, you can not only open MMC, but also go directly to the properties of the selected object. This menu item is available only if Windows 2000, XP, 2003 or 2008 has been installed on the computer. The **Open in MMC** and **Open Properties in MMC** options are also available from the **View** menu when an Active directory object is selected in the **Network** pane.
3. Make necessary changes to the object properties in MMC. For information on how to use MMC, refer to the MMC help.

Manage a group policy

You can also manage group policies for Active Directory domains and organizational units. To do so, one of the following software components should be installed on the computer where the Console component is installed:

- **Group Policy Object Editor** (GPOE). This software is a MMC snap-in and part of Win 2003/2008 Admin Pack.
- **Group Policy Management Console** (GPMC). This MMC snap-in is stand-alone software.

1. Right-click the domain or organizational unit in the **Active Directory** tree and select

Open Group Policy in MMC.

2. The **Group Policies** dialog box opens and displays the following:

   - If only GPOE is installed on your computer, the dialog box will contain the list of effective group policies. You can edit a policy by selecting it and clicking **Edit**.
   - If GPMC is installed on you computer, the dialog box has an **Open** button. Click the button to open **Group Policy Management Console**. For information on how to use the Console, refer to the Microsoft Management Console help.

3.4 View details of Microsoft Windows Network computer

While browsing the **Microsoft Windows Network** using the **Network** pane, you can obtain information about a networked computer. To do so, pause on a computer name in the tree to display a tooltip with the following information:

- Name of the domain the computer belongs to
- Computer name
- IP address of the computer
- Version of the operating system installed on the computer
- Type of operating system and other system information presented in the form of acronyms and abbreviations.

⊟ **List of acronyms and abbreviations**

Abbreviation	**Description**
BBS	Server running Backup Browser Service
MBS	Server running Master Browser Service
BDC	Backup Domain Controller
PDC	Primary Domain Controller
NTC	NT Cluster
DFS	Root of a DSF tree
DMBS	Server running Domain Master Browser Service
LOCAL	Servers maintained by Browser Service
MEMB	LAN Manager 2.x Domain Member
NWS	Novell Servers
WNT	Windows NT/2000/XP/2003 (Workstation or Server)
WDE	Microsoft Windows Server 2003, Datacenter Edition
WEE	Microsoft Windows Server 2003, Enterprise Edition

Abbreviation	Description
WSE	Microsoft Windows Server 2003, Standard Edition
WWE	Microsoft Windows Server 2003, Web Edition
WS	Microsoft Windows NT/2000/2003 Server
WAS	Microsoft Windows 2000 Advanced Server
WDS	Microsoft Windows 2000 Datacenter Server
WEES	Microsoft Exchange 2000 Enterprise Server
WES	Microsoft Exchange 2000 Server
WISS	Microsoft Internet Security and Acceleration Server 2000
WSPS	Microsoft SharePoint Portal Server 2001
WSMS	Microsoft Systems Management Server
WMOM	Microsoft Operations Manager 2000
WMAC	Microsoft Application Center 2000
WTPC	Microsoft Windows XP Tablet PC Edition
NTS	Windows NT/2000/2003 non-DC server
PBS	Server that can run the browser service
PDOM	Primary Domain
SPQ	Server sharing print queue
SQL	All servers running SQL Server
TSS	Server running Time Source Service
WIN	All Windows operating systems
16	Windows 16-bit operating systems
32	Windows 32-bit operating systems
64	Windows 64-bit operating systems
WFWS	Server running Windows for Workgroups
WFW	Workstation running Windows for Workgroups
WS	All workstations
WTS	Server running Windows Terminal Services

Abbreviation	Description
CTS	Server running Citrix Terminal Services
MAC	Any MAC workstation
MACS	Any MAC server
LINUX	Any Linux workstation
LINUXS	Any Linux server
SOL	Any Solaris workstation
SOLS	Any Solaris server

3.5 Wake up networked computers

From the **Network** pane you can send a wake up signal to turn on any networked computer. That might be useful if you have to work with remote, physically inaccessible computers that cannot be kept switched on 24x7 and need to be woken up occasionally.

Send a wake up signal

1. Select a computer in the **Network** pane, either in **Active Directory** or in **Microsoft Windows Network**.
2. Right-click the computer and select **Wake Up** on the shortcut menu.

Note

To use this feature, you must ensure that the computer you try to wake up is plugged into an electricity socket, and the switch on its back panel is ON. You should also check if this feature is supported by the remote computer's BIOS and turn it on in Network Adapter settings, if necessary.

Modify Network Adapter settings

1. Click **Start** > **Control Panel**.
2. Open **System** and on the **Hardware** tab click **Device Manager**.
3. Find your network adapter in **Network adapters** and double-click to display its properties.
4. In the properties dialog, click on the **Advanced** tab and select **Wake on Capabilities** in the **Property** list. In the **Value** list, select **Magic Packet**.
5. Click **OK** to save the changes.

Note that the exact steps and the commands to use are operating system dependent.

3.6 Remotely install the Agent module

For Netop ProtectOn Pro to offer hard disk protection or control access to programs, resources and Internet sites the Agent module needs to be physically located on client computers and run as a service.

As the number of computers can be large, and as they may not be located on the same site, the Console includes features to remotely install and uninstall the Agent module.

However, if you have a large number of client computers that you want to distribute the Agent to, this method might not be practical and you might prefer to use the Agent installation file (NPPAgentSetup.msi) instead.

Note

As with other types of install, remote install requires administrator access to the computer where the Agent module is installed.

⊟ **Install the Agent module from the Console**

1. Select a computer in the **Network** pane, either in **Active Directory** or in **Microsoft Windows Network**.
2. Right-click the computer and select **Install Agent** on the shortcut menu.

   The progress bar will show the installation progress. When finished, click **Close**.

This will install and start the Agent as a service and the computer can be protected with policies defined from the Console.

If you later need to remove the Agent module from a computer, right-click the computer and then click **Uninstall Agent**.

⊟ **Install the Agent module using the Agent installation file**

An installation file can be distributed and run in a number of different ways, for example from a logon script or using Group Policy in Active Directory.

The Agent installation file must be run with parameters that specify Netop ProtectOn Pro Server name and Netop ProtectOn Pro Server port. To configure an Agent to connect to ***policyservername*** and to use port ***port*** the command line looks like this:

NPPAgentSetup.msi ACTION=INSTALL POLICYSERVER=***policyservername*** SERVERPORT=***port***

Replace ***policyservername*** and ***port*** with the settings that match your actual environment.

To create a transform file (MST) for the MSI file, you will need to specify the POLICYSERVER and SERVERPORT properties.

3.7 Open a remote session on a networked computer

You can use the Netop ProtectOn Pro Console to open a session on any one of the networked computers.

Note

Opening a session on a networked computer requires administrator access to the remote computer, and the remote computer must have an Netop ProtectOn Pro Agent installed.

Using remote management of Agent computers, these are some of the features you have access to:

- View information about available disk drives and their properties.
- View the Windows events log.

- Access the Task Manager.
- Manage computer services.
- Manage computer shares like drives and folders.
- View an inventory of hardware and software.

Start a remote session

1. Select a computer in the **Network** pane.
2. Right-click the computer and select **Manage** on the shortcut menu.

   The remote management interface will be displayed in the data panel.

Start a remote session with other account's credentials

You can start a session on a networked computer using other credentials.

1. Select a computer in the **Network** pane.
2. Right-click the computer and select **Manage As** on the shortcut menu.
3. Specify credentials in the form of user name and password and click **OK**.

See also

Remote management pane

4 Creating groups

4.1 Create a group

Policies can be assigned to a group only, not to single objects like a user or a computer. This means that to assign a policy to a single object, you have to create a group and include this object in it. However, usually a group contains more than one object that can be of any type, both **Active Directory** and **Microsoft Windows Network**.

Create a group

1. In the **Policy Editor** pane, right-click **Groups** and select **New Policy Group**.

   A new group with a default name is created.

2. Type a suitable name for the group.

   Once you have created a group, you can add members to it.

3. In the **Network** pane, locate an object that you want to include in the group.

4. Move the object from the **Network** pane to the group by using a drag-and-drop operation.

   The object is now part of the group.

You can also add members to a group by moving members from other groups:

- To add a member to a group without deleting it from its original group, press the Ctrl key and drag the member to the target group.
- To move a member of a group to another group, press Shift and drag the member to the target group.

To remove a member from a group, right-click the object you want to remove and select **Remove from Group** on the shortcut menu.

4.2 Rename, copy, or delete a group

Rename a group

1. In the **Policy Editor** pane, right-click the group you want to rename and select **Rename**.
2. Type a suitable name for the group.

Copy a group

Copying groups can be useful when you need to create a group based on an existing one, and save you the effort of adding members to the new group. A copy of the old group contains exactly the same members as the old group did, and needs only renaming as well as making minor changes to its members. However, the copy does not inherit any policies assigned to the initial group; these must be reassigned.

1. In the **Policy Editor** pane, right-click the group you want to copy and select **Copy**.

A new group with a default name is created.

2. Type a suitable name for the group.

Delete a group

If a group is no longer in use, you can delete it. There are no restrictions on deleting a group; a group can be deleted also when effective policies are assigned to the group. Group references to the policies are deleted, while the policies remain intact.

1. In the **Policy Editor** pane, right-click the group you want to delete and select **Delete**.

   A dialog box opens asking you to confirm that you want to delete.

2. Click **Yes** to confirm, and the group is deleted.

5 Defining and applying policies

5.1 About policies

Netop ProtectOn Pro can be used to implement four different types of policies:

- Hard Disk Protection Policies
- Device Access Policies
- Web Policies
- Application Policies

Policies are created in the Policy Editor by right-clicking the node named like the policy type. The properties for a policy are defined on three tab pages that are available in the data panel when the policy has been created. The first tab is policy type-specific and is used for defining name and policy scope. The second tab is used for limiting the time schedule if the policy should not be enforced around the clock. The third tab lists the groups that the policy has been assigned to.

Below are descriptions of the purpose of each policy type as well as general examples of how each type could be defined.

⊟ Hard Disk Protection Policies

The purpose of a hard disk protection policy is to protect selected drives from harmful alterations and to enable restore to the initial state. This means that a computer can be rolled back to a previous state, and after the roll-back the computer will have lost any new programs and settings implemented after the hard disk protection policy was made effective.

Note that to activate this protection, the relevant computer must be re-started. This is to ensure that all changes are captured. After activation, all changes to the computer configuration are captured in a virtual, hidden folder; changes include installation of programs, registry changes and changes to the user interface. During roll-back the content of the virtual folder is deleted.

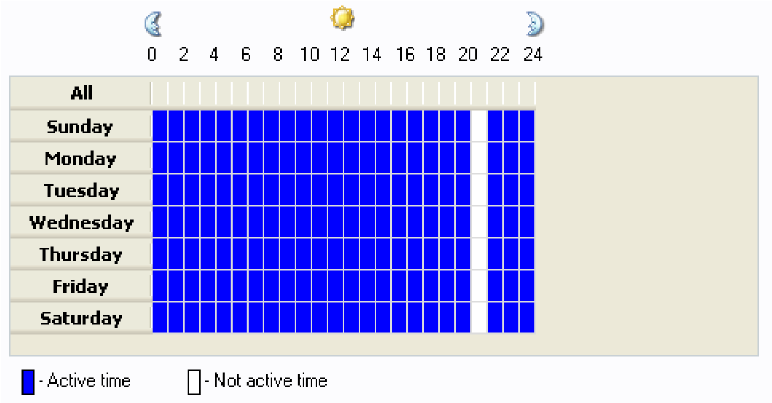
EXAMPLE: Hard Disk Protection Policy

The first tab called **Hard Disk Protection** has a list of drives to protect under the heading **Protect selected drives**. Select the drives to protect. The protection will be effective when the computer has been restarted.

The roll-back functionality can be set independently of when the protection of the drives is set. Select **Enable restore on reboot**, and the next time the computer is restarted the content of the virtual folder will be deleted and the computer restored to the state when the protection was initially enabled.

Certain folders and processes should not be rolled back, for example anti-virus programs or service packs. Folders and processes are excluded from the roll-back by adding them to the exception lists.

To schedule a hard disk restore daily, disable hard disk protection for a specific time slot (for example between 8 and 9 P.M.).



Computers with the hard disk policy enabled will then be restored at 8 P.M. every night

To activate the policy, click **Apply** or click **OK** to activate and close the window.

⊟ Device Access Policies

The purpose of a device access policy is to define access for various types of internal and external devices, for example to protect against malicious programs infesting the company network or to prevent company data from being copied to external devices. The first tab called **Device Access** has a list of the types of devices for which policies can be implemented. Right-click a device type to see the available options:

- For **USB Devices** you can grant full access or set to **No Access** and then define a white list. This gives the IT administrator high flexibility in defining the exact USB policy required by the organization.
- For **Hard Disk** you can grant **Full Access**, **Read**, **Write**, or **Format access** or **No Access**. Additionally, you can define detailed access rights for each individual hard disk as well as details about folders and files to hide.

Access matrix

The table below shows the types of access that can be granted for the various device types.

Possible Access	**Device type**
Full Access/No Access/White list	USB Devices, WiFi
Full Access/No Access, or Read, Write, Format, hide files and folders	Hard Disk
Full Access/No Access, or Read, Write, Eject	DVD/CD-ROM
Full Access/No Access, or Read, Write, Format	Floppy, Removable
Full Access/No Access or Eject	Tape drives
Full Access/No Access	Bluetooth Devices, FireWire port, IrDA Devices, Parallel port, Serial port, USB Devices, WiFi

EXAMPLE: DVD/CD-ROM

On the **Device Access tab**, right-click **DVD/CD-ROM** and select **Access Rights** to enable or disable **Read**, **Write** or **Eject** access. **Full Access** means that all three types of access have been enabled. When all three have been disabled, this corresponds to **No Access**.

To activate the policy, click **Apply** or click **OK** to activate and close the window.

EXAMPLE: USB Devices

Right-click **USB Devices** and make sure that **Full Access** is not selected on the shortcut menu and access is now **No Access**. The USB White list area below now becomes available.

For the USB White list you can choose:

- **Add Classes**: The policy will cover all types of USB devices belonging to the selected class.
- **Add Devices** > **Add devices**: Select USB devices from the database and add to the white list.
- **Add Devices** > **Add local devices**: Select USB devices at the local computer and add to the white list.
- **Add Devices** > **Scan computers**: Scan the computer network for USB devices. Once the scanning is complete, devices can be selected and added to the white list.

Alternatively, click the **USB Database** button to open a window with a list of devices from the USB database and the same functionality as described above.

EXAMPLE: Hard Disk

Use the **Hard Disk** feature to hide files and folders, for example music files like MP3, MP4 or WMA. The below example illustrates how to hide MP3 files.

1. Right-click **Hard Disk** and select **Disk Access**.
2. Select one or more drives to be hidden.

   To hide a drive means that the drive is neither visible to the user nor to the operating system. The next step is to except those drives, so they become visible again, and in the same process you exclude MP3 files from this exception. When MP3 files are not part of the exception they will remain hidden.
3. Click **Add** and select **Add from disk**.
4. In the Folder field, type C:\ or browse to the location.
5. In the File types field, type *.mp3 and select the **Exclude only these file types** option.

   This means that MP3 files are excluded from the exception.
6. Select **Include subfolders** and click **OK**.

The effect of these settings is that the C-drive is visible but all MP3 files are hidden.

To activate the policy, click **Apply** or click **OK** to activate and close the window.

⊟ Web Policies

The purpose of a Web policy is to prevent access to sites that are not appropriate for business or educational use and thus indirectly protect the company or school network, since such a policy can minimize the download of malware.

On the **Internet** tab page, choose the type, **Deny All** or **Allow All**, and then define exceptions to the overall strategy. We recommend that you start by creating a **User Defined** list because this list is generic for all Web policies and can be used when creating the **Except** list for each individual Web policy. The **User Defined** list is created by adding either keywords or complete URLs after clicking **Add** in the lower right corner.

EXAMPLE: Web Policy

1. Select the **Allow all** type and as an exception add the word "XXX". This Web policy will block for all URLs that contain the word XXX.
2. To activate the policy, click **Apply** or click **OK** to activate and close the window.

⊟ **Application Policies**

The purpose of an application policy is to prevent use of applications that are not appropriate for business or educational use and thus indirectly protect the company or school network, since it can minimize the use of not approved and hence potentially dangerous applications.

On the **Application** tab page, choose the type, **Deny All** or **Allow All**, and then define exceptions to the overall strategy. The Applications list has default applications grouped in the folders **Desktop**, **Start Menu** and **Default Programs Dir**; you can also create your own **User Defined** list. These four folders are generic for all application polices created and can be used when creating the **Except** list for each individual application policy.

EXAMPLE: Application Policy

1. Select the **Allow all** type and as an exception add the word "YYY". This application policy will then block for YYY.
2. To activate the policy, click **Apply** or click **OK** to activate and close the window.

5.2 Create a policy

1. In the **Policy Editor** pane, select **Policies**, right-click the type of policy you want to create, for example **Application Policies**, and select **New Policy**.

   A new group with a default name is created.
2. Type a suitable name for the policy.

Once you have created a policy, you define policy settings. For information about defining policies, see Define a hard disk protection policy, Define a device access policy, Define a Web policy, or Define an application policy.

5.3 Define a hard disk protection policy

To define a hard disk protection policy, create the policy first. For instructions, see Create a Policy.

1. Open an existing policy by double-clicking it in the **Hard Disk Protection Policies** tree.

The policy properties are displayed on three tabs in the data panel.

2. Define properties on the **Hard Disk Protection** and on the **Assigned To** tabs.

   For descriptions of the options on the two tabs, see Hard Disk Protection tab, Schedule tab and Assigned To tab.

3. When you have completed the policy definition, click the **Apply** button to apply the changes.

Restart computers when a policy is applied

When a hard disk protection policy has been defined and is applied, the computers where the policy is applied must be restarted to ensure that the computers have a well-defined restore point and to ensure data consistency on the hard disk.

The fact that a restart is necessary is indicated by a yellow note icon at the bottom of the dialog.

- On the **Restart** button drop-down menu, click **Restart and apply policy changes**.

The command is available only if the policy has been assigned to at least one group with actual members.

This option is useful when policies are defined initially and when existing policies are updated. For example, if the initial policy defined that the C-drive was protected, an update might exclude the My Documents folder from protection.

When you send a restart command to agent computers, you can define a message to display on the computers before they restart, for example:

> Your computer will restart in 2 minutes. Please save any unsaved work.

The time interval before the restart takes place can also be set. To set these defaults:

- On the **Restart** button drop-down menu, click **Restart Options**.

If a policy has previously be applied, the restart can also include a rollback to the previous restore point. This means that when the computer restarts, all modifications like programs installed or removed will be undone and the computer is brought back to its original state.

- On the **Restart** button drop-down menu, click **Restart, restore and apply policy changes**.

This option is useful in environments where users typically make many, unwanted changes, for example in school computer labs or where computers are publicly available like hotels or Internet cafés.

5.4 Define a device access policy

To define a device access guard policy, create the policy first. For instructions, see Create a Policy.

1. Open an existing policy by double-clicking it in the **Device Access Policies** tree.

   The policy properties are displayed on three tabs in the data panel.

2. Define properties on the **Application** tab, the **Schedule** tab and on the **Assigned To** tab.

   For descriptions of the options on the tabs, see Device Access tab, Schedule tab and

Assigned To tab.

3. When you have completed the policy definition, click the **Apply** button to apply the changes.

See also

Define access rights at the level of type of devices

Define access rights at the level of single device

Define access rights for USB devices

Hiding contents of hard disks

5.5 Device access policies

5.5.1 Define access rights at the level of type of device

1. In the **Permissions** list section, select a type of devices for which you want to define access rights.

   By default, Full Access is assigned to all types of devices.

2. Right-click the type and select **Access Rights** on the shortcut menu.

3. In the **Access Rights** dialog box, select or clear the relevant check boxes.

   For different types of devices this dialog box provides different options to select from. Basically, the dialog box can include the **Enable** option that should be selected to make the devices available, but other check boxes are also possible:

   - For DVD/CD-ROM and tape drives the **Eject** option is also available to allow or prevent opening the drives and removing disks/tapes from them.
   - For floppy disks, hard disks, DVD/CD, CD/DVD-RW and removable data storage the **Read**, **Write** and **Format** options are also available to allow or prevent reading, writing and formatting operations.

   All these options are also available on the shortcut menu when a type of devices is selected in the top pane.

4. Press OK to save the changes.

Note

When you set permissions for WiFi and Bluetooth adapters in a Device Access policy, connections that have already been established are not interrupted.

See also

Define access rights at the level of single device

Define access rights for a USB device

Hide the contents of a hard disk

5.5.2 Define access rights at the level of single device

1. In the **Permissions** list select the type of devices to which your device belongs.

   The full list of devices of this type will be displayed in the bottom pane.

2. Select the device you want to define access rights for.

To reduce the full list to the list of devices available only on the administrator's computer, select the Show available devices only checkbox.

3. Right-click the device and select **Access Rights** on the shortcut menu.

   The **Access Rights** dialog box for a single device is the same as one for its type of devices.

4. In the **Access Rights** dialog box, select or clear the relevant check boxes.

When you change access rights for a single device, access to its type of devices changes to **Custom** and settings at the level of type will be cleared. Access rights for the other devices of the type will stay the same as they were before the change.

It is important to remember that in the bottom pane of the **Permissions** section, you can see either generic devices or, if the **Show available devices only** check box is selected, devices currently installed on the administrator's computer. To define access rights to other devices of the type that are not installed on the administrator's computer, but present on Agent computers, use the option **Others**.

Note

When you set permissions for WiFi and Bluetooth adapters in a Device Access policy, it does not affect existing connections.

See also

Define access rights at the level of type of devices

Define access rights for a USB device

Hide the contents of a hard disk

5.5.3 Define access rights for a USB device

Note

This is applicable to USB devices only.

Access to USB devices can be granted or denied at the level of the entire type of USB devices. But even if access to the entire type of USB devices is denied, you will still be able to grant access to chosen USB devices or classes of USB devices by means of USB white lists and the USB Database.

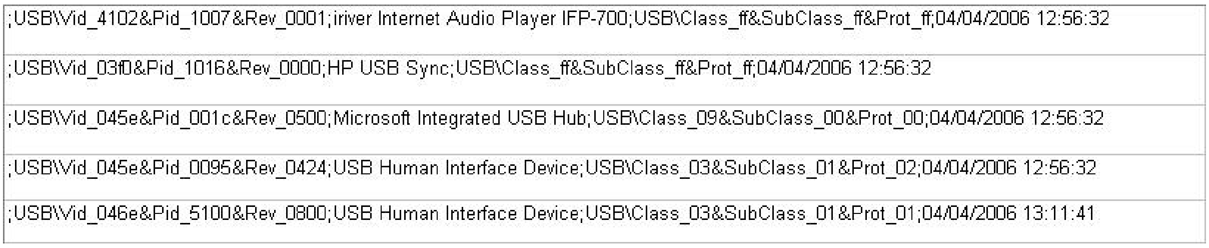
A USB white list is a list of USB devices and classes of USB devices that can be accessed irrespective of the fact that access to the whole type of USB devices is denied by a device access policy. Each device access policy can have its own white list. A white list can be exported to or imported from a .csv file. To populate white lists, you can use data stored in the USB database or other techniques described below.

The USB Database is a database that stores information about USB devices. The purpose of the database is to allow you to easily and conveniently compile white lists by taking records from it. The database can also be exported to or imported from a .csv file. Generally, the database can be populated in the following ways:

- By adding information about USB devices either currently or ever connected to the administrator's computer.
- By scanning any networked computers running Agent to identify devices ever connected to them.

You can also add information to the USB Database manually by editing its .csv file.

Information import from other .csv files is also supported. The format of the data in a .csv file is presented in the figure below:



```
;USB\Vid_4102&Pid_1007&Rev_0001;iriver Internet Audio Player IFP-700;USB\Class_ff&SubClass_ff&Prot_ff;04/04/2006 12:56:32
;USB\Vid_03f0&Pid_1016&Rev_0000;HP USB Sync;USB\Class_ff&SubClass_ff&Prot_ff;04/04/2006 12:56:32
;USB\Vid_045e&Pid_001c&Rev_0500;Microsoft Integrated USB Hub;USB\Class_09&SubClass_00&Prot_00;04/04/2006 12:56:32
;USB\Vid_045e&Pid_0095&Rev_0424;USB Human Interface Device;USB\Class_03&SubClass_01&Prot_02;04/04/2006 12:56:32
;USB\Vid_046e&Pid_5100&Rev_0800;USB Human Interface Device;USB\Class_03&SubClass_01&Prot_01;04/04/2006 13:11:41
```

The data is the following pieces of information separated by ";":

- Device identifier;
- Device description;
- Class the device belongs to;
- Date and time the device was discovered.

Each identifier (for example, USB\Vid_4102&Pid_1007&Rev_0001) contains the following information separated by "\" and "&":

Example	**Description**
USB	Device type, always USB.
Vid_4102	Vendor ID. This is a unique ID assigned to the vendor (manufacturer) of the device by USB Implementers Forum, Inc. (www.usb.org). To obtain vendor ID, contact this organization.
Pid_1007	Product ID. Each product has an identification number assigned by its vendor. To obtain product ID, contact the vendor.
Rev_0001	Revision number of the product. This information can also be obtained from vendor.

By default, when a new device access policy is created, **Full Access** is assigned to the whole USB Devices type and its white list is empty. To deny access to the whole type of USB devices and assign access right at the level of USB classes and single devices instead, do the following:

1. Disable the whole type of USB devices as described in Define access rights at the level of type of devices.
2. Create the white list of USB devices and classes of USB devices that will always be accessible.

To create a USB devices white list, start by selecting **USB Devices** in the **Permissions** section on the **Device Access** tab. The USB white list will be displayed in the bottom pane of the **Device Access** tab. In a newly created policy, this list is empty.

See also

Add a USB device class to white list

Add a USB device to white list

Work with the USB database

5.5.4 Define access rights for a WiFi device

Access to using wireless local area network, or WiFi, can be completely open or completely close. On the **Device Access** tab, **Access** can be set to either "No Access" or to "Full Access":

- Right-click the WiFi device type and click **Full Access**. The command toggles between "No Access" or to "Full Access".

When acces has been set to "No Access", the bottom pane of the **Device Acces** tab displays the white list. Use the white list to grant access to one of more specific wireless networks that users are allowed to connect to.

To add a WiFi device to the white list:

- Click the **Add** button and type the network name of the wireless device, for example "MyCompanyWireless".

5.5.5 Hide the contents of a hard disk

Notes

- This is applicable to hard disk devices only.
- Hiding contents means that users can neither *see* nor *use* programs and files in hidden folders. However, Netop ProtectOn Pro ensures that you cannot hide the drive where the operating system is installed: the folders and files required by the operating system will remain visible and functional.

For hard disks, you can not only define access rights at the levels of type and single devices, but also hide contents of Agent computers' hard disks from their users. Netop ProtectOn Pro allows you either to hide entire disks or define exception folders where the contents can be viewed by users.

For example, if you manage a computer lab where all computers have a C-drive with the operating system and program files and a D-drive with a designated folder called "Work" where students and other users are supposed to save their work, you might write-protect the C-drive and hide the content of the D-drive except for the **Work** folder. This would ensure that students and other users can only save their files in the Work folder.

Hide contents of hard disks installed on an Agent computer from users of this computer

1. In the **Permissions** list, select **Hard Disk**, right-click and select **Disk Access** in the shortcut menu.
2. In the **Disk Access** dialog box, do the following
    - In the **Hide selected drives** list select the drives you want to hide from users.
    - Click the **Add** button and select **Add from Disk** to add folders that should not be hidden from users.

    Users will be able to view only contents of this directory and its subdirectories (if this option is selected). For example, if users are permitted to view educational materials that are stored in `C:\School Materials\Grade 6 Materials\Biology`, add this folder to the list of exception folders, and the users will be able to view the contents of the Biology folder. Still, the contents of the folders `School Materials` and `Grade 6 Materials` will be hidden.

5.5.6 Work with the USB database

1. In the **Permissions** list, select **USB Devices** and click the **USB Database** button.

   The **USB Devices Database** dialog box opens displaying a list of the USB devices database contents.

   To add records to the database, use two available options:

   - Click **Add local devices** to add devices available on the computer.
   - Click **Scan computers** to scan networked computers for devices.

   To delete a device from the USB devices database, select it in the list and click **Delete**.

   To import a USB devices database from a .csv file, click **Load** and select the file with the database.

   To export a USB devices database to a .csv file, click **Save** and type the name of the database file.

2. Click **OK** in the **USB Devices Database** dialog box.
3. Click **Apply** on the **Device Access** tab to save the changes.

See also

Define access rights at the level of type of devices

Define access rights at the level of single device

Hide the contents of a hard disk

5.5.7 Add a USB device class to a white list

1. Click the **Add Classes** button.

   The **Add Classes** and **Add Devices** buttons are unavailable when USB Devices are given full access. In the **Permissions** list, right-click **USB Devices** and make sure that **Full Access** has not been selected.

2. Select one or more classes in the **Choose USB class** dialog box and click **Add**.

   If the white list already contains devices of the class or classes you are trying to add, you will be notified of this by a system message. These individual devices will be removed from the list and the whole class will be allowed instead.

3. Click **Apply** on the **Device Access** tab to save the changes.

See also

Define access rights at the level of type of devices

Define access rights at the level of single device

Hide the contents of a hard disk

5.5.8 Add a USB device to a white list

To add an individual device or devices to the white list, click the **Add Devices** button and select one of the three commands available:

⊟ **Add devices**

- Select the device to add and click the **Add** button.

If the devices you need are not present in the USB Database, you can add them for easy future access. For information on how to add to the USB database, see Work with the USB database.

⊟ Add local devices

The list displays devices currently connected to your computer. You can supplement the list with devices ever connected to the computer by selecting the **Show all local devices** box.

- Select devices to include in the white list and click **OK** to add.

⊟ Scan computers

1. Choose to scan specified computers only, or to scan all computers.
2. Click **Find Now** to start the scanning.

   If you scan the entire network, it will probably be a time-consuming procedure. When the scanning is finished, the list of identified USB devices is displayed in the **Found USB devices** list.
3. In the **Found USB devices** list, select the devices to include and click **Add**.

If the classes of USB devices the selected devices belong to are already present in the white list, you will be notified of this by a system message. The selected devices will not be added to the list, as they are already allowed as part of their classes.

See also

Define access rights at the level of type of devices

Define access rights at the level of single device

Hide the contents of a hard disk

5.6 Define a Web policy

To define a Web policy, create the policy first. For instructions, see Create a policy.

1. Open an existing policy by double-clicking it in the **Web Policies** tree.

   The policy properties are displayed on three tabs in the data panel.
2. Define properties on the **Internet** tab, the **Schedule** tab and on the **Assigned To** tab.

   For descriptions of the options on the tabs, see Internet tab, Schedule tab and Assigned To tab.
3. When you have completed the policy definition, click the **Apply** button to apply the changes.

5.7 Define an application policy

To define an application policy, create the policy first. For instructions see Create a policy
.

1. Open an existing policy by double-clicking it in the **Application Policies** tree.

   The policy properties are displayed on three tabs in the data panel.

2. Define properties on the **Application** tab, the **Schedule** tab and on the **Assigned To** tab.

   For descriptions of the options on the tabs, see Application tab, Schedule tab and Assigned To tab.

3. When you have completed the policy definition, click the **Apply** button to apply the changes.

5.8 View effective policies for a member of a group

You can obtain information about policies that are active for a member of a group:

1. Locate the group member in the **Policy Editor** pane under **Groups**.
2. Right-click the member and select **View Effective Policies** on the shortcut menu.

The data panel displays information about the policies assigned to this group member. The list of effective policies includes a brief description of each policy. If you need more detailed information, double-click a policy to display it in data panel.

5.9 Rename, copy, or delete a policy

Rename a policy

1. In the **Policy Editor** pane, right-click the policy you want to rename and select **Rename**.
2. Type a suitable name for the policy.

Copy a policy

Copying policies can prove useful when you need to create a policy based on an existing one, and save the effort of creating a new policy. A copy of the old policy contains exactly the same settings as the old policy, and needs only renaming.

1. In the **Policy Editor** pane, right-click the policy you want to copy and select **Copy**.

   A new policy with a default name is created.

2. Type a suitable name for the policy.

Delete a policy

If a policy is no longer in use, you can delete it. There are no restrictions on deleting a policy; a policy can be deleted when assigned to a group.

1. In the **Policy Editor** pane, right-click the policy you want to delete and select **Delete**.

   A dialog box opens asking you to confirm that you want to delete.

2. Click **Yes** to confirm, and the policy is deleted.

5.10 Policies tab pages

5.10.1 Hard Disk Protection tab

The **Hard Disk Protection** tab is used to select hard disks to protect, to define exception folders where permanent changes are allowed, and to add processes that are allowed to make permanent changes to the hard disks.

The tab consists of the following sections:

Protect selected drives

Drives to protect. The list of drives contains letters from C to Z. If you select drives that are not hard disks on Agent computers, this setting is ignored.

Enable restoring

Select **Enable restore on reboot** to remove all changes made to the disks selected in the **Protect selected drives** section after restarting the computers.

Note

If you select disks to protect, but do not enable restore on reboot, changes made by users are not rolled back. If you do not enable restoring for a long time, performance might decrease. In this case, use the **Enable restore on reboot** option to clear the changes.

Restart button with these options:

Restart, restore and apply policy changes

Shut down the computers where the policy is applied, restore the hard disk to its most recent restore point and apply the policy.

Restart and apply policy changes

Shut down the computers where the policy is applied and apply the policy.

Restart Options

Define default settings for restarting agent computers:

- Time interval before restart.
- Message to display to users before their computers are restarted.
- Allow users to cancel the restart command.
- Whether the agent computers should also be restored.

The settings are used when you click Restart Agent PCs from the toolbar or by right-clicking a hard disk protection policy in the Policy Editor.

Exception folders

Folders where permanent changes are permitted.

Two commands are available from the **Add** button: use **Add** to enter a folder name manually or **Add from disk** to browse to the folders to be added.

Tip

The folder list in the **Add Exception Folder** dialog box includes a number of default folders such as My Documents, My Pictures, User Profile, My Desktop, Program Files where the contents are frequently changed by users.

Exception processes

Processes that are allowed to make permanent changes to the hard disks. Exception processes can be added using one of the three commands on the **Add** button:

Add - Manually specify path to the executable file of a process.

Note

If you enter an application path manually, make sure to enter the absolute local path on the Agent computer. The path can include environment variables like for example %AppData%, %SystemRoot%, %UserName%, and %UserProfile%.

Add from Processes – Select a process from the list of currently running processes.

Add from Disk – Select an executable file by browsing disk contents. The path must be an absolute local path. If applications on Agent computers are installed to folders different from folders on administrator's computer, identify the actual folder structure and then enter the absolute local path manually.

5.10.2 Device Access tab

The **Device Access** tab is used to define permissions to access various types of devices.

The top pane of the **Permissions** section provides the full list of device types that can be controlled. If a type of devices is selected in the top pane, the bottom pane displays either all devices of this type that are installed on the administrator's computer (if the **Show available devices only** check box has been selected) or all generic devices of this type.

The bottom pane also includes an **<Others>** type. The purpose of the **<Others>** type is to allow controlling devices installed on Agent computers, but not present on the administrator's computer, at the level of single device.

Note

Exceptions are USB devices and WiFi.

For USB devices the bottom pane displays not single devices, but the white list, which is the list of USB devices and classes of USB devices that are available even when the entire USB Devices type is disabled. For more information about the white list, see Define access rights for USB devices.

For WiFi devices the bottom pane displays the white list which is the list of WiFis that are available even cccess has been set to "No Access" for the WiFi device type. For more information about adding a WiFi to the white list, see Define access rights for a WiFi device.

Levels of control

You can control access to devices at the following levels:

Type of devices

This means that the access rule is applied to the whole type and that the policy will cover all devices of this type installed on Agent computers. For information about defining access on types of devices, see Define access rights at the level of type of device.

Single device

This means that the access rule is applied to a single device only. For information about defining access on a single device, see Define access rights at the level of single device.

With USB devices, to control access at the level of single device, you should compile a white list and include devices that are always available in it.

Class of USB devices

This is applicable to USB devices only.

You can allow accessing such classes as USB Human Input Devices (HID), USB printers and Smart Card devices. Controlling access at the level of class is achieved using the USB white list that allows defining USB devices and classes of USB devices that are always available. For information about using a white list, see Define access rights for a USB device.

Devices are recognized both by their user-mode names or letters (such as A:, COM1) and internal names (such as \Device\Floppy0, \Device\Serial0), which allows working even with unnamed devices.

5.10.3 Internet tab

The **Internet** tab is used to define whether the overall Web strategy should be to allow access to all sites or to deny access to all sites, and to define exceptions to the overall strategy.

The **Except** list contains the list of exceptions to the overall policy. For example, if the policy type is **Allow All**, the **Except** list displays the list of locations to which access is blocked. Items can be added to this list either manually or by using a drag-and-drop operation to move items from the **Internet Addresses** list. This list can include both full URLs, for example www.google.com and parts of URLs, for example *google* or *game*.

The **Internet Addresses** list allows you to create a customized list of Internet resources to select from. This list is the same for all policies and can be accessed and extended from any policy. The list can also include both proper URLs and masks. In case only a mask is defined, the policy will allow/deny access to all Internet pages that comply with the mask.

The **Ports to scan** list includes the ports that ProtectOn Pro scans and is capable of blocking access to when a policy related to Internet access is defined. If the port your computer environment uses for Internet access is not on the list, you should add it by clicking the **Edit** button. If your computer environment uses a proxy server for Internet access, make sure that the proxy port is included in the list.

Add an item to the Except list

- Click the **Add** button below the **Except** list, type a URL or part of a URL and press Enter to save the changes.

Add an item to the Internet Addresses list

- Click the **Add** button below the **Internet Addresses** list, type a URL or part of a URL and press Enter to save the changes.

5.10.4 Application tab

The **Application** tab is used to define whether the overall application strategy should be to allow use of all applications or to deny access to all applications, and to define exceptions to the overall strategy.

The **Except** list contains the list of exceptions to the overall policy. For example, if the policy type is **Allow All**, the **Except** list displays the list of applications to which access is blocked. The list of exceptions does not have to contain paths but can be, for example, excel.exe.

The **Applications** list shows applications installed on the administrator's computer. The list is available to save you the effort of re-entering paths to executable files and items from this list can be conveniently added to the list of exceptions to the left. By default, the **Applications** list contains the **Desktop**, **Start Menu** and **Default Programs** folders. When you click the **Rescan** button, Netop ProtectOn Pro scans these folders for executable files. You can add other applications to the **User Defined** folder.

Add an item to the Except list

1. Click the **Add** button below the **Except** list and select **Add from Disk**.
2. Browse to the application you want to add to get the full path added automatically.

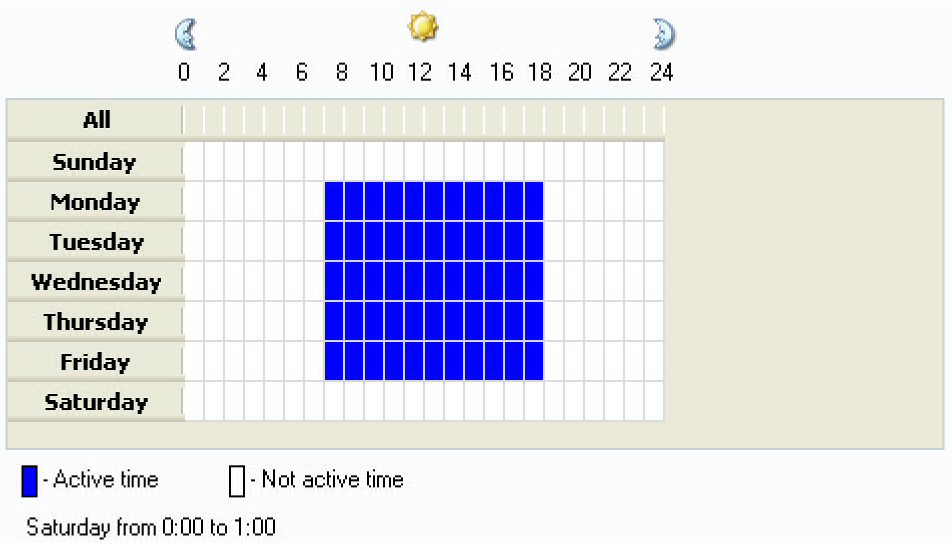
Add an item to the Applications list

1. Click the **Add** button below the **Applications** list and select **Add from Disk**.
2. Browse to the application you want to add to get the full path added automatically.

5.10.5 Schedule tab

All four types of polies can be scheduled

The **Schedule** tab is used to define the periods when the policy is active. The figure below illustrates a policy which is active during working hours.



🟦 - Active time   □ - Not active time

Saturday from 0:00 to 1:00

To change **Active time** to **Not active time**, right-click the cell you want to change.

5.10.6 Assigned To tab

The **Assigned To** tab is used to assign policies to existing groups. For information about creating groups, see Create a group.

Assign a policy to a group

1. Click the **Add** button.

2. In the **Policy Groups** dialog box, select one or more groups and click **Add**.

If you want the policy to have higher priority than other policies of this type, select the **Override other policies** check box. When the flag has been set, this is indicated visually by change of icon in the Policy Editor pane 🔒. If more than one policy has precedence, they are merged like polices without the flag set. For more information about policies and precedence, see Policies merging.

6 Overlapping policies

6.1 Policies merging

When more than one policy of a policy type have been defined, for example three application policies, Netop ProtectOn Pro automatically resolves any inconsistencies and calculates how the sum of the rules defined within each policy will be applied. This means that you do not necessarily have to worry about inconsistencies, but it might be useful to understand how the policies are merged to be able to comprehend the result of applying the policies.

A simple example: The user group called "Marketing" includes all employees from that marketing department. The members of the group are allowed to use all applications that the company has licenses for, except a number of developer tools like .NET Framework. The user Peter is a member of the Marketing group, but since he manages the company Web site, he is also a member of the "Developers" group. As the Developers have general Allow All access to developer tools, the result is that Peter has access to .NET Framework tools, even though the Marketing group as such does not have access.

From a technical point of view, only one policy of each type is effective, and this one policy is automatically created by merging several policies into one. When you have defined groups and assigned policies to these groups, the internal algorithm that Netop ProtectOn Pro applies to define an effective policy of each type consists of these two steps:

1. Identification of policies for each type.
2. Merging of policies within each type.

Identification of policies for each type

Policies of each type are identified for the *computer* that the policies are to be applied to, and for the *user* that the policies are to be applied to. This is the sequence for each of the four policy types:

1. The list of groups that the user belongs to is identified.

   A group is included in the list if the user is a member of the group or if the user is a member of another group or an Organizational unit included in the group. The resulting list of groups is used to identify which policies have been assigned to the user.

   The result set is a list of policies identified by "assigned to user".

2. The list of groups that the computer belongs to is identified.

   A group is included in the list if the computer is a member of the group or the computer is a member of another group or an organizational unit included in the group. The resulting list of groups is used to identify which policies have been assigned to the computer.

   The result set is a list of policies identified by "assigned to computer".

3. The two lists of policies are each divided into two lists: policies with the **Override other policies** option selected on the **Assigned To** tab are included into the first list; the other policies are included into the second list.

   As a result a prioritized list of policies is created:

Overlapping policies

Priority	Override other policies	Assigned to	Description
1	+	user[1]	Policies assigned to users with the override flag set have the highest priority.
2	+	computer	Policies assigned to computers with the override flag set have the next highest priority.
3	-	user[1]	When policies do not have the override flag set, polices assigned to users have the higher priority.
4	-	computer	

[1] Hard Disk Protection policies are applied only per computer, not per user. This means that lists 1 and 3 are always empty for policy type **Hard Disk Protection**.

Merging of policies within each type

On this step the effective policy is defined based on merging policies from the set of policies above defined for the computer and for the user.

If the above lists are empty, a default policy will be applied. Default policy is defined individually for every policy type.

⊟ Default policy

The table below describes how the default policy is defined for every policy type.

Policy type	Default policy description
Hard Disk Protection Policy	There are no protected disks in the default policy.
Device Access Policy	The default policy allows using any devices.
Web Policy	The default policy allows the user access to any addresses.
Application Policy	The default policy allows launching any applications.

The following sections describe the rules of merging two policies of each type. Merging more than two policies is performed as a sequential merging of every next policy with the result of merging the previous ones. For example, there are three effective policies of one type – p1, p2 and p3. Their merging will be performed as ((p1 merge with p2) merge with p3), that is: first the merging of p1 and p2 is calculated, and after that the resulting policy is merged with p3.

6.2 Hard disk protection policies merging

If several Hard Disk Protection policies are assigned to a computer, they are merged. Here is a schematic overview of how the policies are merged.

Policies	**Restore on reboot**	**Protected disks**	**Exceptions folders**	**Exception processes**
Policy 1	Enabled	Drives1	Folders1	Processes1
Policy 2	Disabled	Drives2	Folders2	Processes2
Resulting policy	Enabled	Drives1 ∪ Drives2[1)]	Folders1 ∪ Folders2	Processes1 ∪ Processes2

1) "∪" is the symbol for mathematical union: A or B or both (inclusive union)

Examples

An example of merging is presented in the table below.

A Hard Disk Protection (HDP) policy can only be associated with a single computer or a group of computers, not with users.

Policies	**Restore on reboot**	**Protected disks**	**Exception folders**	**Exception processes**
HDP Policy 1	Enabled	C D E	C:\Folder C1 D:\Folder D1 E:\Folder E1	Process 1 Process 2
HDP Policy 2	Disabled	D E F	D:\Folder D1 E:\Folder E2 F:\Folder F1	Process 3 Process 4

Resulting policy	**Restore on reboot**	**Resulting protected disks**	**Resulting exception folders**	**Resulting exception processes**
HDP Policy	Enabled	C D E F	C:\Folder C1 D:\Folder D1 E:\Folder E1, E2 F:\Folder F1	Process 1 Process 2 Process 3 Process 4

If you define types of files that are allowed to change in the exception folders, these file types must be allowed to change in all folders of the resulting policy. If these types of files are not allowed to change at least in one exception folder of the resulting policy, they will not be allowed to change in all exception folders of the resulting policy.

Note
If you create multiple HDP policies, it might not be easy to understand how exception folders are merged. That is why it is highly recommended to have only one HDP policy that covers all Hard Disks.

6.3 Device access policies merging

If several Device Access policies are assigned to a user, computer or other object, they are merged.

As access rights to a device can be defined at the levels of type and device (class or individual device for USB devices), this is taken into account when merging the policies.

The below table is a compact schematic overview for all types of devices in the Device Access policy.

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	Drives1	Folders1	DevMasks1	DevTypeMasks1	WLMembers1
Policy 2	Drives2	Folders2	DevMasks2	DevTypeMasks2	WLMembers2
Resulting policy	Drives1 ∪ Drives2[1)]	Folders1 ∪ Folders2	DevMasks1 ∪ DevMasks2[2)]	DevTypeMasks1 ∪ DevTypeMasks2[2)]	WLMembers1 ∪ WLMembers2

1) "∪" is the symbol for mathematical union: A or B or both (inclusive union)

2) If both sets (DevMasks1 and DevMasks2) contain masks for one device, these masks are merged. For example, if DevMasks1 contains the mask Read and DevMasks2 contains the mask Write for the same device, the final mask is Read AND Write. The same rule is valid for devices type masks.

Examples

Examples of merging of Device Access policies are presented in the tables below.

The first 3 examples show different scenarios for the merging of DVD/CD-ROM policies. For the following types of devices the merging is performed similarly:

- Floppy
- Removable
- Tape Drives

Note
The most restrictive setting always wins when merging.

In the example tables below, "NA" means "Not applicable".

Example 1 - for DVD/CD:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	Read enabled Write enabled	Type level	NA
Policy 2	NA	NA	Read enabled Write disabled	Type level	NA

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	NA	NA	Read enabled Write enabled	Type level	NA

Note

The policy is applied to all DVD/CD-ROM drives since it is "type level".

Example 2 - for DVD/CD:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	Read enabled Write enabled	Type level	NA
Policy 2	NA	NA	Read enabled Write disabled	Device level (policy is active for \Device\CdRom0)	NA
Policy 3	NA	NA	Read enabled Write disabled	Type level	NA

Overlapping policies

Example 2 - for DVD/CD - interim step, merging Policy 1 and Policy 2:

Policy 1 & 2	NA	NA	Read enabled Write disabled	Device level Policy only valid for \Device\CdRom0	NA
			Read enabled Write enabled	Type level For other devices of the type	
Policy 3	NA	NA	Read enabled Write enabled	Device level (policy is active for \Device\CdRom0)	NA

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	NA	NA	Read enabled Write disabled	Device level Policy only valid for \Device\CdRom0	NA
			Read enabled Write enabled	Type level For other devices of the type	

Example 3 - for DVD/CD:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	Read disabled Write disabled	Type level	NA
Policy 2	NA	NA	Read enabled Write disabled	Device level (policy is active for \Device\CdRom0)	NA
Policy 3	NA	NA	Read enabled Write enabled	Device level (policy is active for \Device\CdRom0)	NA

Example 3 - for DVD/CD - interim step, merging Policy 1 and Policy 2:

Policy 1 & 2	NA	NA	Read disabled Write disabled	Type level (=the policy is applied to all DVD/CD-ROM drives)	NA
Policy 3	NA	NA	Read enabled Write enabled	Device level (policy is active for \Device\CdRom0)	NA

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	NA	NA	Read disabled Write disabled	Type level (=the policy is applied to all DVD/CD-ROM drives)	NA

A Device Access policy can also contain a USB white list. These are the rules if two or more USB Device Access policies are merged:

- If access is allowed but only with white list, the resulting white list will include USB devices from all white lists.
- The strictest policy is “No access”. If this is merged with another USB policy (Full access of “access with white list”) the resulting policy will be “No access”.

Overlapping policies

Example 4 - for USB:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	Full access	Type level	NA
Policy 2	NA	NA	No access - white list only	Type level	HID class[1)]

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Final policy	NA	NA	Only access with white list	Type level	HID class HID devices are accessible on all computers

1) The white list content is HID (Human Interface Device) class like for example mouse and keyboard.

Below examples are for merge of three Device Access policies; UC_A, UC_B and UC_C can each be an individual user or a computer, but can also be a group of users/computers.

Example 5 - for USB:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	No access - white list	Device level (only valid for UC_A)	HID class
Policy 2	NA	NA	No access - white list	Device level (policy covers UC_A, UC_B and UC_C)	Mass storage class
Policy 3	NA	NA	No access	Type level (only valid for UC_C)	NA

Example 5 - for USB - interim step, merging Policy 1 and Policy 2:

Policy 1 & 2	NA	NA	No access - white list	Device level (only valid for UC_A)	HID class
			No access - white list	Device level (policy covers UC_A, UC_B and UC_C)	Mass storage class
Policy 3	NA	NA	No access	Type level (only valid for UC_C)	NA

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	NA	NA	No access - white list	Device level (only valid for UC_A)	HID class
			No access - white list	Device level (only valid for UC_B)	Mass storage class
			No access	Type level (only valid for UC_C)	

Example 6 - for USB:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	No access - white list	Device level (only valid for UC_A)	HID class
Policy 2	NA	NA	No access - white list **Override** other policies	Device level (policy covers UC_A, UC_B and UC_C)	Mass storage class
Policy 3	NA	NA	No access	Type level (only valid for UC_C)	NA

Example 6 - for USB - interim step, merging Policy 1 and Policy 2:

Policy 1 & 2	NA	NA	No access - white list **Override** other policies	Device level (policy covers UC_A, UC_B and UC_C)	*Policy 2 overrides the other policies:* Mass storage class
Policy 3	NA	NA	No access	Type level (only valid for UC_C)	NA

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	NA	NA	No access - white list **Override** other policies	Device level (policy covers UC_A, UC_B and UC_C)	*Policy 2 overrides the other policies:* Mass storage class

A Device Access policy can also be a Hard Disk policy that specifies access to drives, folders or files. Below are examples of the resulting Hard Disk policy when two or more policies are intersecting.

"Hide" means that the drives, folders or files cannot be seen by the user or by the Operating System (OS). To ensure that a Hard Disk policy has no impact on the operating system, Netop ProtectOn Pro has the built-in feature that if a Hard Disk policy is set to "Hide C drive", where Windows normally is installed, then some default folders and files will still be visible in order for the computer to run Windows OS. The default folder names and file names are not listed here, since the names depend on the specific operating system.

Example 7 - for Hard Disk:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	C drive	Default folders	NA	Device level (only valid for UC_A)	NA
Policy 2	NA	NA	NA	Type level (policy covers UC_A and UC_B)	NA

Resulting policy	Hidden drives	Exception folders	Device masks	Device type masks	USB white list members
Policy	C drive	Default folders	NA	Device level (only valid for UC_A)	NA

Other drives - full access

Example 8 - for Hard Disk:

Policies	Hidden drives	Exception folders	Device masks	Device type masks	USB white list members
Policy 1	NA	NA	NA	Type level (only valid for UC_A)	NA
Policy 2	D drive	Default folders	NA	Device level (policy covers UC_A, UC_B and UC_C)	NA
Policy 3	C drive	two folders, based on environment variables and default folders	Exclude=No Recursive=Yes	Device level (only valid for UC_C)	NA

Example 8 - for Hard Disk - interim step, merging Policy 1 and Policy 2:

Policy 1 & 2	D drive	Default folders	NA	Device level (policy covers UC_A, UC_B and UC_C)	NA
Policy 3	C drive	two folders, based on environment variables and default folders	Exclude=No Recursive=Yes	Device level (only valid for UC_C)	NA

Overlapping policies

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	D drive C drive	Default folders two folders, based on environment variables and default folders	Exclude=No Recursive=Yes	Device level (policy covers UC_A, UC_B and UC_C) Device level (only valid for UC_C)	NA

For the remaining Device Access policies – Bluetooth Devices, FireWire port, IrDA Devices, Parallel port, Serial port and WiFi – the policy intersection is simple: The options for altering those devices are either: Full access or no access.

The strictest rule will be the resulting one.

Example 9 - for Infrared:

Policies	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy 1	NA	NA	NA	Infrared - Full access	NA
Policy 2	NA	NA	NA	Infrared - No access	NA

Resulting policy	**Hidden drives**	**Exception folders**	**Device masks**	**Device type masks**	**USB white list members**
Policy	NA	NA	NA	Infrared - No access	NA

6.4 Web policies merging

If several Web policies are assigned to a user, a computer or other object, they are merged.

The below table is a schematic overview of Web policies merging. In the overview "WebSites" can be a number, a letter, a word, part of a URL or a full URL. Note that the shorter the source exception, the more it will block.

Example #	Source policies	Source exceptions	Resulting policy	Resulting exceptions
1	Policy 1 Allow All	WebSites1	Allow All	Except all websites in WebSites1 and WebSites2
	Policy 2 Allow All	WebSites2		
2	Policy 1 Deny All	WebSites1	Deny All	Except websites in WebSites1, if they are not defined in WebSites2
	Policy 2 Allow All	WebSites2		
3	Policy 1 Allow All	WebSites1	Deny All	Except websites in WebSites2, if they are not defined in WebSites1
	Policy 2 Deny All	WebSites2		
4	Policy 1 Deny All	WebSites1	Deny All	Except all websites both in WebSites1 and WebSites2
	Policy 2 Deny All	WebSites2		

Examples of merging are presented in the table below. UC_A, UC_B and UC_C can each be an individual user or a computer, but can also be a group of users or computers.

Example 1:

Source policies	Source exceptions	Resulting policy	Resulting exceptions
Policy 1 Allow All (valid for UC_A and UC_B)	Word1 WebSite1 Word2 WebSite2 Word3	Allow All	For UC_A the exceptions are: Word1 WebSite1 Word2 WebSite2 Word3 For UC_B the exceptions are: Word1 WebSite1 Word2 WebSite2 Word3 WebSite3 Word4 Word5
Policy 2 Allow All (only valid for UC_B)	Word1 WebSite2 Word4 WebSite3 Word5		

Example 2:

Source policies	**Source exceptions**	**Resulting policy**	**Resulting exceptions**
Policy 1 Allow All	Word1 WebSite1 Word2 WebSite2 Word3	Deny All	Word4 WebSite3 Word5
Policy 2 Deny All	Word1 WebSite2 Word4 WebSite3 Word5		

Example 3:

Source policies	**Source exceptions**	**Resulting policy**	**Resulting exceptions**
Policy 1 Deny All	Word1 WebSite1 Word2 WebSite2 Word3	Allow All	Word1 WebSite1 Word2 WebSite2 Word3 Word4 WebSite3 Word5
Policy 2 Deny All	Word1 WebSite2 Word4 WebSite3 Word5		

An example of merging with three policies is presented in the table below.

Example 4:

Source policies	**Source exceptions**	**Resulting policy**	**Resulting exceptions**
Policy 1 Allow All (only valid for UC_A)	None	UC_A: Allow All UC_B: Allow All UC_C: Deny All	For UC_A and UC_B the exceptions are: Word1 WebSite1 Word2 WebSite2 Word3 For UC_C the exceptions are: Word4 WebSite3 Word5
Policy 2 Allow All (valid for UC_A, UC_B and UC_C)	Word1 WebSite1 Word2 WebSite2 Word3		
Policy 3 Deny All (only valid for UC_C)	Word1 WebSite2 Word4 WebSite3 Word5		

6.5 Application policies merging

If several Application Policies are assigned to a user, a computer or other object, they are merged. Below is a schematic overview of how polices are merged.

Example #	Source policies	Source exceptions	Resulting policy	Resulting exceptions
1	Policy 1 Allow All	Apps 1	Allow All	Except all applications in Apps 1 and Apps 2
	Policy 2 Allow All	Apps 2		
2	Policy 1 Deny All	Apps 1	Deny All	Except applications in Apps 1 if they are not defined in Apps 2
	Policy 2 Allow All	Apps 2		
3	Policy 1 Allow All	Apps 1	Deny All	Except applications in Apps 2 if they are not defined in Apps 1
	Policy 2 Deny All	Apps 2		
4	Policy 1 Deny All	Apps 1	Deny All	Except applications both in Apps 1 and Apps 2
	Policy 2 Deny All	Apps 2		

Below examples are for lists of applications.

Example 1:

Source policies	Source exceptions	Resulting policy	Resulting exceptions
Policy 1 Allow All	Application1 Application2 Application3 Application4	Allow All	Application1 Application2 Application3 Application4 Application5 Application6
Policy 2 Allow All	Application1 Application2 Application5 Application6		

Example 2:

Source policies	Source exceptions	Resulting policy	Resulting exceptions
Policy 1 Deny All	Application1 Application2 Application3 Application4	Deny All	Application3 Application4
Policy 2 Allow All	Application1 Application2 Application5 Application6		

Example 3:

Source policies	Source exceptions	Resulting policy	Resulting exceptions
Policy 1 Allow All	Application1 Application2 Application3 Application4	Deny All	Application5 Application6
Policy 2 Deny All	Application1 Application2 Application5 Application6		

Example 4:

Source policies	Source exceptions	Resulting policy	Resulting exceptions
Policy 1 Deny All	Application1 Application2 Application3 Application4	Deny All	Application1 Application2
Policy 2 Deny All	Application1 Application2 Application5 Application6		

7 Remote management

7.1 About remote management

Remote management is activated by using the **Microsoft Windows Network** in the **Network** pane.

- Locate the computer you want to manage, right-click the computer name and select **Manage** on the shortcut menu.

The remote control session opens a new tab in the data panel.

For the remote managed computer you can see the **Disk drives**, **Event Viewer**, **Task Manager**, **Registry**, **Services**, **Shared Folders**, **Inventory**, **Command Console**, **System Control** and **Local Users and Groups**.

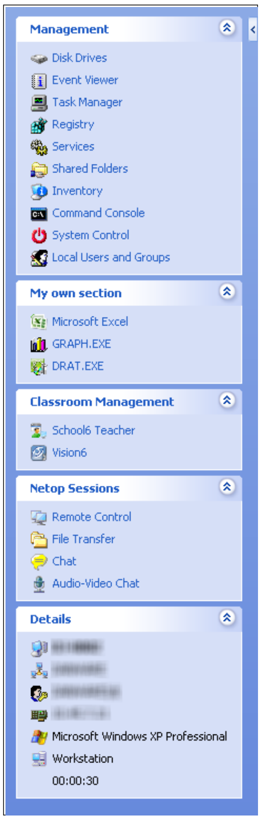
If you have Netop Remote Control installed on the computer where you also have Netop ProtectOn Pro Console installed, the Netop Remote Control program will automatically be included in the window section called **Netop Sessions**.

Other third party programs can be installed in their own window section. On the **File** menu, click **Third Party Program Integration**. The first step is to add your own window section, and the next step is to add shortcuts to relevant programs.

By using **Active Directory** and choosing a user, this user can be managed by right-clicking the user name and selecting **Open in MMC** on the shortcut menu.

7.2 Management pane

When the administrator has started a remote session from the Console, the Console data panel displays the available management tools in three or more sections; the Agent computer display does not change.



Management

The first section provides access to the **Management** tools. The tools are also available from the **Management** menu, which is added to the Netop ProtectOn Pro menu bar when a remote management session is opened.

For details about each tool, see the relevant topic below.

My own section and Classroom Management

The second section is completely user-defined and does not exist initially. This section contains third party applications integrated into Netop ProtectOn Pro. For information on how to add sections and applications, see Integrate third party applications.

The third section in the sample screen shot is also a user defined section and illustrates that both section heading and the integrated applications are completely user defined.

Netop Sessions

The fourth section provides access to **Netop Sessions** commands. For a brief overview of the command, see Netop Sessions

Details

The fifth section is informational only and displays this information:

- The name of the Agent computer which is accessed remotely.
- The name of the network that the Agent computer is on.
- The name of the network and the user opening the remote access session.
- The Agent computer IP address
- The Agent computer operating system
- The Agent computer machine type
- The remote management session duration in this format: HH:MM:SS

7.3 Disk Drives

Click **Disk Drives** in the Management section to display available Agent computer disk drives and their properties.

Use the **Disk Drives** tool to get an overview of the available disk space on a networked computer.

Viewing options are available from the **Disk Drives** menu and from the shortcut menu that opens when you right-click the data panel.

7.4 Event Viewer

Click **Event Viewer** in the **Management** section to display Windows event logs of the Agent computer.

Use the **Event Viewer** tool to

- View and change log properties.
- View the properties of an event record and copy them to the clipboard.
- Clear logs.
- Save a log on the administrator's or Agent computer.
- Open a log saved on the administrator's or Agent computer to view it.

Note

Only Windows NT and later versions (2008, 2003, XP, and 2000) record event logs. Consequently, the Event Viewer command is enabled only if the Host computer runs on a Windows NT or later operating system.

Like the Windows Event Viewer, the Event Viewer tool includes three categories of information: **Application**, **Security** and **System**.

The fourth tab named **File** can display a saved event log.

The following commands are available from the **Event Viewer** menu and from the shortcut menu that opens when you right-click the data panel:

Command	Description
Open	Opens an event log that was previously saved using the **Save** command. Event log files have extension .evt. **Note** Opening a saved event log overwrites any previous **File** tab contents.
Save	Saves an event log as a file in a specified location. The file must have extension .evt.
Clear	Clears the Application, Security, or System event log from Windows. Before the event log is cleared, you can choose to save the information to a log file for later inspection. The log file should be saved with extension . evt.
Refresh	Retrieves new data from the Agent computer to refresh the tab display.
Log Properties	Opens the properties window for the Application, Security or System log file. You can view and change log size and filter properties.
Event Properties	Displays properties for the selected event. Use the up and down arrows to scroll through the list of events. Click the **Copy** button to copy the record properties to the clipboard.

7.5 Task Manager

Click **Task Manager** in the **Management** section to display lists of applications and processes that are running on the Agent computer.

The **Task Manager** tool works like the **Windows Task Manager**, only on a remote controlled computer. The tool can be used to view and control applications and end processes, and to view the computer load and process threads.

7.6 Registry

Click **Registry** in the **Management** section to open the Windows registry on the Agent computer.

The **Registry** tool works like the **Windows Registry Editor**, only on a remote controlled computer.

About Windows registry

The Windows registry stores the configuration of the Windows operating system in a structured database. The registry is created when Windows is installed on the computer and is automatically modified when applications are installed and used and when users create or change personal settings. The registry settings should be modified with caution as erroneous data entries can make the computer malfunction.

Refer to the Windows Registry Editor help for details about entries and how to modify them.

7.7 Services

Click **Services** in the **Management** section to display a list of services that are running on the Agent computer. *Services* are programs that can run in the background, that is not displaying on the desktop, to support operating system or application functionalities.

The **Services** tool enables you to start, stop, pause, resume and restart Agent computer services, to add and remove services and to change the properties of services.

Note
Only Windows NT+ (Windows 2008, 2003, XP, 2000 and NT) can manage services. Consequently, the **Services** command is enabled only if the Agent computer runs on a Windows NT+ operating system.

The following commands are available from the **Services** menu and from the shortcut menu that opens when you right-click the data panel:

Add...	Adds a service on the Agent computer. Follow the instructions in the wizard that opens.
Remove	Deletes a service. When a **Services** record is deleted, the service status and startup type change to **Stopped** and **Disabled**. When the application that uses the service is unloaded, the record is removed.

Note

Deleting a **Services** record and removing the service will affect dependent services. Dependencies are shown on the **Dependencies** tab on the **Properties** dialog box: Right-click and select **Properties** on the shortcut menu.

Restart

Stops and starts the service.

Note

Stopping, pausing or restarting a service may affect dependent services. Dependencies are shown on the **Dependencies** tab on the **Properties** dialog box: Right-click and select **Properties** on the shortcut menu.

Refresh

Retrieve new information from the Agent computer to refresh the displayed information.

Properties

Displays properties for the service on three tab pages.

Note

Do not change service properties unless you know exactly what you are doing. Keep notes of changes to enable restoring properties if changes cause an unexpected behaviour.

⊟ **General tab**

Use the **Startup type** field to change the way the service starts.

Note

If you change **Startup type** to **Disabled**, a service which has already been started or paused does not change its status, but when it is stopped, it can no longer be started.

Use the **Start**, **Stop**, **Pause** and **Resume** buttons to control the service.

The **Start parameters** field is enabled when a service is **Stopped** . Specify any parameters like command line options to be used when the service is started.

Note

Start parameters are not saved. A backslash (\) is interpreted as an ESCAPE character. Specify two backslashes for each backslash in a parameter.

⊟ **Log On tab**

Use the **Log on as** options to specify how to log on to a service using a different account.

- Use **Local System account** to log on as a local system account that has extensive rights on the Agent computer, but no rights on other computers (typically the default selection).

- Use **This account** to log on as a specific user and specify the user credentials in the fields.

  To specify that the selected Agent computer service will use the Local Service account, type `NT AUTHORITY\LocalService`. To specify that it shall use the Network Service account, specify `NT AUTHORITY\NetworkService`. Do not specify a password for these accounts; both of them have built-in passwords.

⊟ **Dependencies tab**

Displays dependencies and dependants. You cannot change dependencies on this tab.

7.8 Shared Folders

Click **Shared Folders** in the **Management** section to view and manage agent computer shared resources and view and disconnect shared resource sessions and shared file connections.

⊟ **Shares tab**

Special shares, typically with $ as the last character in the share name, are created automatically as hidden resources by the operating system for administrative and system use. Typically, you should not delete or change special shares. If you delete or change special shares, they may become restored when the server service is stopped and restarted or when the computer is restarted.

These special shares may appear on the Shares tab:

<Drive letter>$	Enables administrators to connect to the root directory of a drive.
ADMIN$	Enables remote administration of a computer. Its path is always the path of the system root directory.
IPC$	Enables inter program communication by named pipes. IPC$ is used during remote administration of a computer and when viewing a computer's shared resources and cannot be deleted.
NETLOGON	Required on domain controllers. Removing it causes a loss of functionality on domain client computers.
SYSVOL	Required on domain controllers. Removing it causes a loss of functionality on domain client computers.
PRINT$	Used during remote administration of printers.
FAX$	A server folder that is used by clients when

sending a fax. It stores temporary fax files and fax cover pages.

7.9 Inventory

Click **Inventory** in the **Management** section for an overview of the Agent computer inventory of hardware and software.

7.10 Command Console

Click **Command Console** in the **Management** section to open a command prompt window on the Agent computer. This corresponds to clicking **Run** on the Windows **Start** menu and typing `cmd` but have the command prompt window display the *Agent computer*, not the Console.

Before the command prompt window opens, you will be required to enter credentials (user name, password and domain) that are valid on the Agent computer.

7.11 System Control

Click **System Control** in the **Management** section to control the Agent computer status.

The System Control allows you to:

- Lock the computer (Windows NT, 2000, XP only)
- Log off the user
- Restart the computer
- Shut down the computer.

Before any of these actions are performed, you can choose to warn the user by displaying a message, for example:

```
Computer updates need to be implemented and you will be logged
off in a few minutes. Please save your work and close any open
program.
```

Use the **Options** section to specify whether the user is to be warned and to specify the number of seconds between prompting the user and executing the action selected under **Action to Perform**.

Allow user to cancel

Generally, you cannot cancel system control command. However, selecting this option enables the **Abort** button on the pop-up message and the user is allowed to cancel the command.

Close open programs without saving data

Normally data is saved before the selected system control command is executed. Select this option to close any open programs without saving data.

7.12 Local Users and Groups

Click **Local Users and Groups** in the **Management** section to manage users and groups on the Agent computer.

With **Local Users and Groups**, you can:

- Add new users and groups.
- View and edit properties of existing local users and groups.
- Set user passwords.
- Rename or delete users and groups.

Users tab

The **Users** tab contains the list of users of the Agent computer.

The shortcut menu has these commands:

New User

Select this command to add a new user.

In the **New User** dialog box, type the appropriate information and select or clear options related to password and account. Click **Create**, and then click **Close**.

Notes

A user name cannot be identical to any other user or group name on the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A user name cannot consist solely of periods (.) or spaces.

A password can have up to 127 characters. However, if you are using Windows 2000 or Windows XP on a network that also has computers using Windows 95 or Windows 98, consider using passwords no longer than 14 characters. Windows 95 and Windows 98 support passwords of up to 14 characters. If your password is longer, you may not be able to log on to your network from those computers.

Set Password

Select this command to change the selected user's password.

Delete

Select this command to delete the selected user.

Note

When you need to remove a user account, it is a good idea to disable the account first. When you are certain that disabling the account has not caused a problem, you can safely delete it. To disable the account, select **Account is disabled** in the **Properties** dialog box. A deleted user account cannot be recovered. The built-in Administrator and Guest accounts cannot be deleted.

Rename

Select this command to rename the selected user. Type a new name and press Enter to save.

Note

Because it retains its security identifier, a renamed user account retains all its other properties, such as its description, password, group memberships, user environment profile, account information, and any assigned permissions and rights. A user name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A user name cannot consist solely of periods (.) or spaces.

Refresh F5 — Select this command to retrieve new data from the Agent computer and refresh the tab display.

Properties — Select this command to view and change properties for a user account.

When a user has been created with the **New User** command, the user must be added to a group. This is done on the **Member Of** tab in the properties dialog box.

Note

Adding users to the Administrators group will give them unlimited access rights.

⊟ Groups tab

The **Groups** tab contains the list of groups of the Agent computer.

The shortcut menu has these commands:

New Group — Select this command to add a new group.

In the **New Group** dialog box, type the appropriate information and click **Add** to add existing users to the group. Click **Create**, and then click **Close**.

Note

A local group name cannot be identical to any other group or user name on the computer being administered. It can contain up to 256 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A group name cannot consist solely of periods (.) or spaces.

Delete — Select this command to delete the selected group.

Notes

The following built-in groups cannot be deleted: Administrators, Backup Operators, Power Users, Users, Guests, Replicator.

A deleted group cannot be recovered.

Deleting a local group removes only the group; it does not delete the user accounts and global groups that were members of that group.

If you delete a group and then create another group with the same group name, you must set new permissions for the new group; it will not inherit the permissions that were granted to the old group.

Rename — Select this command to rename the selected group. Type a new name and press Enter to save.

Note

Because it retains its security identifier, a renamed group retains all its other properties, such as its description and members. A group name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A group name cannot consist solely of periods (.) or spaces.

Refresh F5 — Select this command to retrieve new data from the Agent computer and refresh the tab display.

Properties — Select this command to add and remove users from the group.

7.13 Integrate third party applications

If there are applications that you use frequently in connection with remote management, you can create your own section in the Management pane and add commands to open any third party application. The user defined section in the Management pane is added beneath the Management section; see illustration and description in Management pane. Within the user defined section, the third party applications can be added beneath user-defined group headings like for example **Utilities** or **Tools**.

Add a third party application

1. On the **File** menu, click **Third Party Program Integration**.
2. Click **Add Section** to create the section and give it a name.

   As an example, the section heading could be **Classroom Management**.

   Note that the section will not appear until one or more programs have been added.
3. Select a section and click **Add Program**.
4. In the **Add Program** dialog box, click the Browse button to locate the executable.

   As an example, the executable could be `C:\Program Files\GenevaLogic\Vision\XL\MeSuAx.exe`.

   This would add teacher module from Vision6. Note that the module requires a command line parameter to start correctly: `/InvokeVerb:OpenDashboard`.

   When this parameter is added to the **Command Line** field, it is automatically used and added to the **File Name** field.

   The **Working Folder** field is updated automatically.
5. Click **OK** to add the program and close the dialog box.

⊟ **Optional parameters**

In addition to specifying the name of the executable, optional parameters can also be specified.

Display Name	Define the program name to be shown in the new section. If this parameter is not set, the name of the executable (for example: excel.exe) is shown.
Tooltip	Define the text to be displayed when the mouse pointer rests on the program name. If this parameter is not set, the name of the executable (for example: excel.exe) is shown.
Command Line	Define the program parameters that should be passed to the program when it is started. The following built-in parameters can be used: %%CN - Host Computer Name %%CD - Host Computer Domain %%LU - Host Logged in User %%LD - Host Logged in Domain %%IA - Host IP Address %%MA - Host MAC Address
Working Folder	Select the folder for the program to store its data. If this parameter is not set, the folder where the executable is located is used.
Run As	Select how the program window will be displayed: Normal Window, Minimized, Maximized, Hidden.

Tip

Any program that is installed on the Netop ProtectOn Pro Console computer and can react to command line executions can be integrated. To view any necessary command line parameters you can open the program properties dialog box: Right-click the program on Windows' Start menu and then click **Properties**.

7.14 Netop Sessions

The **Netop Sessions** section is available only if

- Netop Remote Control Guest has been installed on the computer where the Netop ProtectOn Pro Console is installed.
- Netop Remote Control Host has been installed on the computer where the Netop ProtectOn Pro Agent is installed.

These commands are available in the **Netop Sessions** section:

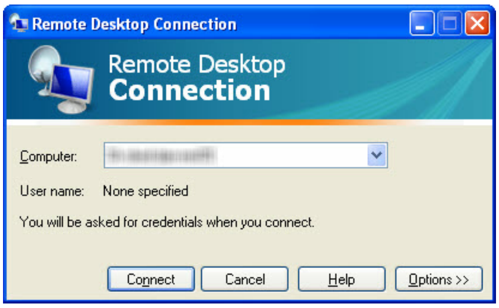
Remote Control	Start/stop a Remote Control session with the connected Host.
File Transfer	Start/stop a File Transfer session with the connected Host.

Chat	Start/stop a Chat session with the connected Host.
Audio Chat	Start/stop an Audio Chat session with the connected Host.

Note

Start **Audio Chat** will be disabled if the Guest and Host computers are not both interactive audio enabled or if the Guest is engaged in another audio session. Host Guest Access Security may deny a Guest starting a session, see Guest Authorization in the Netop Remote Control documentation.

If Netop Remote Control is not available on the computer where the Netop ProtectOn Pro Console is installed, the **Netop Sessions** section is replaced with a **Remote Desktop** section and rely on the operating system's **Remote Desktop Connection**:



Computer: [redacted]

User name: None specified

You will be asked for credentials when you connect.

Index