NETOP™

ProtectOn™ PRO

Endpoint Protection Software

Moving from Netop ProtectOn 2 to Netop ProtectOn Pro

If you are an existing ProtectOn 2 user who is considering upgrading to ProtectOn Pro, this document is for you!

The present document assumes that you are familiar with ProtectOn 2 and that you want to know how you can manage the hard disk protection you are used to in ProtectOn Pro instead. The document will give you an overview of the major differences between the two products and explain how to set up hard disk protection and how to turn it on and off.

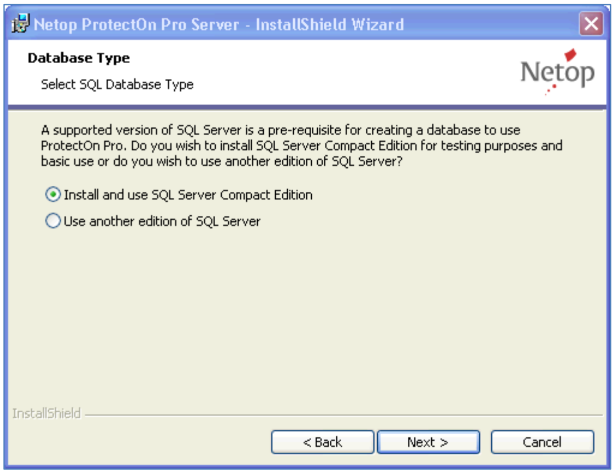
In ProtectOn Pro hard disk protection is only one of the four major feature areas; ProtectOn Pro also offers options to manage Internet access, to manage use of different applications, and to manage devices like USB drives. ProtectOn Pro also includes options to manage a computer remotely, for example to wake up a computer, open a command line interface, and to view change history. If you want to learn about these options, we recommend that you refer to the ProtectOn Pro Help or to the ProtectOn Pro User's Guide.

How ProtectOn Pro works

ProtectOn 2 and ProtectOn Pro share the same basic functionality and purpose: computer hard disk protection across a network. Both products save and restore computers to their last saved configuration, removing any viruses, unwanted files, or unauthorized computer programs. ProtectOn Pro consists of three modules: a Server module, a Console module and an Agent module.
The **Console** module corresponds to the ProtectOn 2 Administrator module and is the administrator's tool for managing hard disk protection.
The **Agent** module corresponds to the ProtectOn 2 Client module and is installed on all the computers that are to have hard disk protection.

The **Server** module is the communication focal point between the Console and Agents and handles access to the database.

Where ProtectOn 2 is file-based, ProtectOn Pro relies on an SQL database. For basic use and testing purposes, Microsoft SQL Server Compact edition is included with the Server component and can be installed automatically. If you plan to use a different edition of SQL Server, it must be acquired and installed prior to installing the ProtectOn Pro Server module.



Database Type

Select SQL Database Type

A supported version of SQL Server is a pre-requisite for creating a database to use ProtectOn Pro. Do you wish to install SQL Server Compact Edition for testing purposes and basic use or do you wish to use another edition of SQL Server?

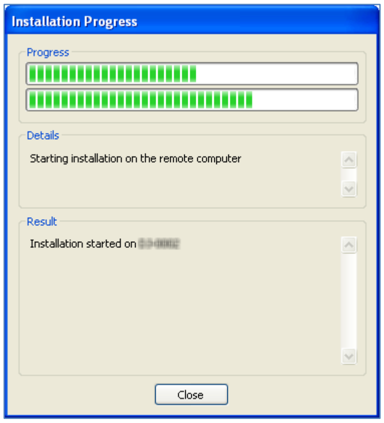
● Install and use SQL Server Compact Edition

○ Use another edition of SQL Server

Also, Microsoft .NET Framework version 2.0 must be available on the Console computer and on the Server computer. Because .Net Framework is required by many different programs today the component is typically already available on computers; if the component is not already installed, the redistributable package can be downloaded from the Microsoft .NET home page (http://www.microsoft.com/net/).

When the Server and the Console modules have been installed, the Agent module can be installed remotely from the Console interface.

The Agent module also has a separate .msi that can be distributed using the process you normally use to deploy programs to be installed on several users' computers.



Starting installation on the remote computer

Installation started on [redacted]

Whereas ProtectOn 2 relies on matching access keys on Administrator and Clients, ProtectOn Pro relies on Windows security: access to deploy and to create hard disk protection on Agent computers requires that the user logged on to the computer running the Console module has admin rights to the Agent computers; typically the access profile that a system or network administrator has.

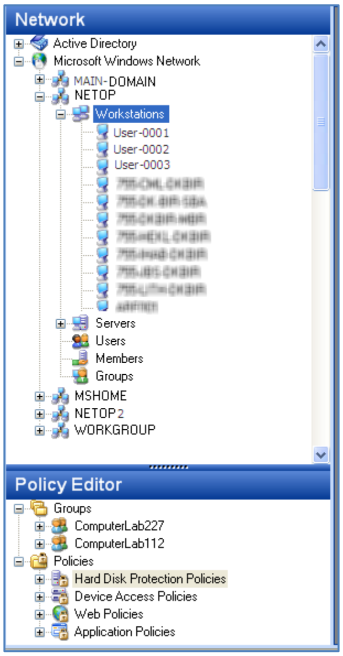
Create hard disk protection

Creating hard disk protection in ProtectOn Pro is done in three steps that are similar to the required steps in ProtectOn 2:

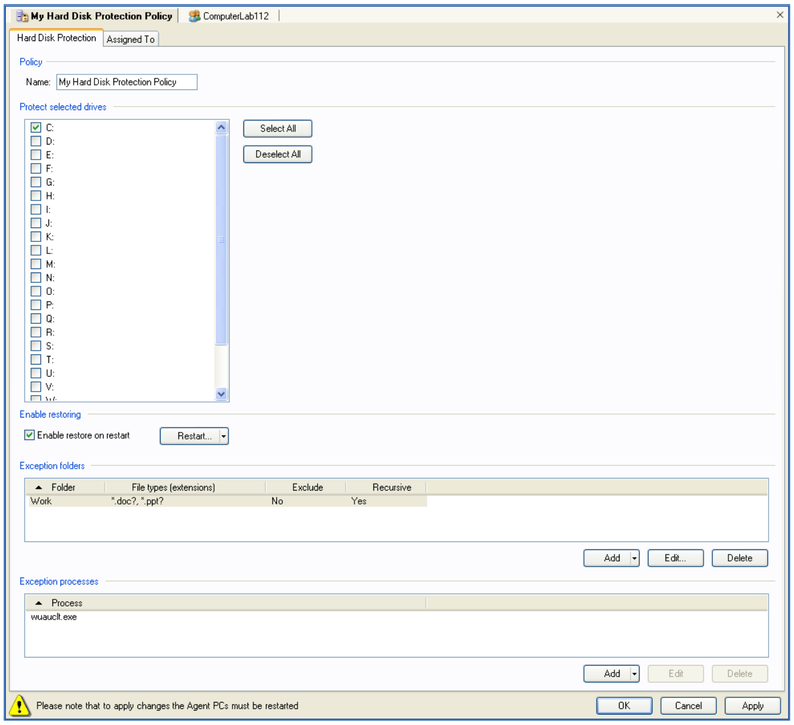
1. Identify the computers that the hard disk protection should be valid for and include them in a group that you create and name.

In ProtectOn Pro this is done by browsing a Microsoft Windows Network tree of your computer network and using a drag-and-drop operation to include the relevant computers in a group.

The network tree is generated automatically in the Console user interface.



2. Choose which drives to protect.



Name: My Hard Disk Protection Policy

☑ C: ☐ D: ☐ E: ☐ F: ☐ G: ☐ H: ☐ I: ☐ J: ☐ K: ☐ L: ☐ M: ☐ N: ☐ O: ☐ P: ☐ Q: ☐ R: ☐ S: ☐ T: ☐ U: ☐ V:

☑ Enable restore on restart

Folder	File types (extensions)	Exclude	Recursive
Work	*.doc?, *.ppt?	No	Yes

Process
wuauclt.exe

Please note that to apply changes the Agent PCs must be restarted

In ProtectOn Pro this is done by creating and naming a hard disk protection policy.

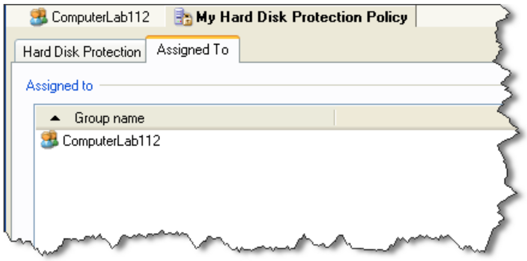
As part of the policy properties you define:

- The drives to protect.
- Any folders and subfolders which should be excluded from the hard disk protection and the restore. For example, this could be a designated Work folder where students and other users are supposed to save their assignments.
- Any processes that should be excluded from the hard disk protection restore. For example, this could be the Windows update process since service packs and other operating system

fixes should not be rolled back.

3. Assign the hard disk policy to an existing group of computers.

   In ProtectOn Pro this is done from a tab page on the hard disk protection policy definition where the group is added by the click of a button or by using drag-and-drop from the existing groups.



The screen shots above illustrate the creation of a hard disk protection policy that protects drive C but excludes a folder called “Work” from the protection and allows users to save files of type doc? and ppt? in the folder. Also, the Windows update process is excluded from any restore.

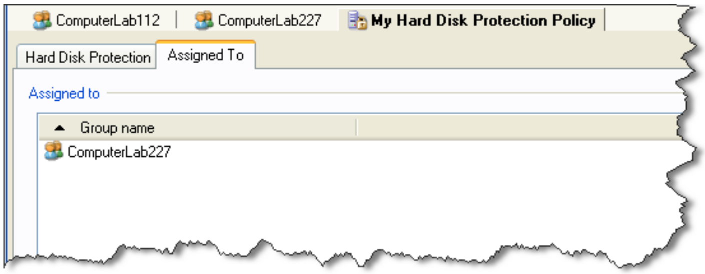
Turn hard disk protection on

To turn on hard disk protection in ProtectOn Pro, the Agent computers need to be restarted. This is done by clicking the **Restart** button on the hard disk protection policy tab page.

As mentioned above, admin rights are required to restart Agent computers and apply a hard disk protection policy.

Turn hard disk protection off

When a hard disk protection policy has been created and turned on as described above, it remains in effect as is until its properties are changed or until the group is deleted.



ComputerLab227

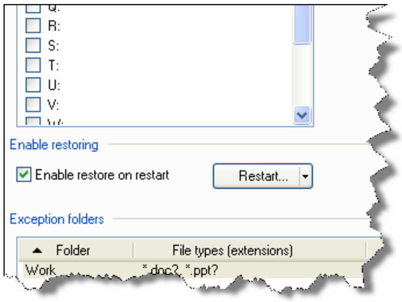
To turn off hard disk protection from computers, remove or replace the group on the **Assigned To** tab page.

To ensure that processes like operating system updates or computer virus protection software updates are allowed to run and not rolled back on restore, exception processes can be used. Hard disk protection can be scheduled to be active only during certain time intervals, for example during normal school hours. This leaves time for the system administrator to maintain student computers, for example to install new software or updates to existing software, outside of school hours.

Restore computers

Agent computers with hard disk protection are automatically restored when they are restarted.

This is defined as part of the hard disk protection policy by ensuring that the **Enable restore on reboot** check box has been selected.

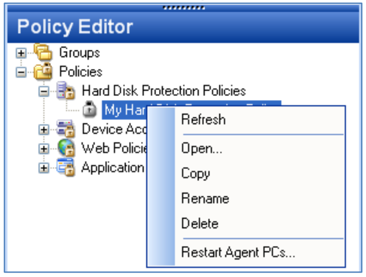


□ R:
□ S:
□ T:
□ U:
□ V:

☑ Enable restore on restart

Folder	File types (extensions)
Work	*.doc?, *.ppt?

Restore of the computers with hard disk protection can also be forced by right-clicking the policy and then clicking **Restart Agent PCs**.



Netop develops and sells software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers over the Internet. For more information, see www.netop.com.