nitrobit
device blocker

User's Guide

Content

I. Introduction....4
- Overview....4
- Functions of nitrobit device blocker....4
- System Components....4

II. Installing the system....5
- System requirements....5
- System Setup....5

III. Defining Policies....6
- Devices....7
  - Defining a device definition....7
- Volume Access....8
  - Exceptions....8
  - Path Exceptions....9
  - Device Exceptions....9
  - Define a volume access policy....10
  - Define a volume path exception....10
  - Define a volume device exception....11

IV. Managing Clients....12
- Client Setup....12
  - Manual Installation....12
  - Automated Client Rollout....12
  - Automated Client Rollout with an Administrative Installation....12
  - Automated Client Update....13
- Detecting and Resolving Problems....14
  - Using the Support Data Collection Tool....14
- Client Reference....15
  - Registry Values....15

V. Legal Notice....16
- Contact....16

Document Version: 1.0

I. Introduction

Overview

nitrobit device blocker is a Data Loss Prevention (DLP) product for Microsoft Windows. nitrobit device blocker allows the administrator to configure an access policy to devices which a user could use to export confidential information.

Functions of nitrobit device blocker

With nitrobit device blocker, the following access policies can be defined:

- **Devices**
  Restrict access to COM/LPT ports, Bluetooth and IrDA devices.

- **Volumes**
  Restrict access to fixed disks, removable storage, CD/DVD drives, network drives and plug and play storage devices.

System Components

nitrobit device blocker consists of a system service, a driver as well as an editor. The editor allows the administrator to define various access policies. The system service and the driver are responsible to enforce the policies.

II. Installing the system

System requirements

nitrobit device blocker can be used on workstations with one of the following operating system:

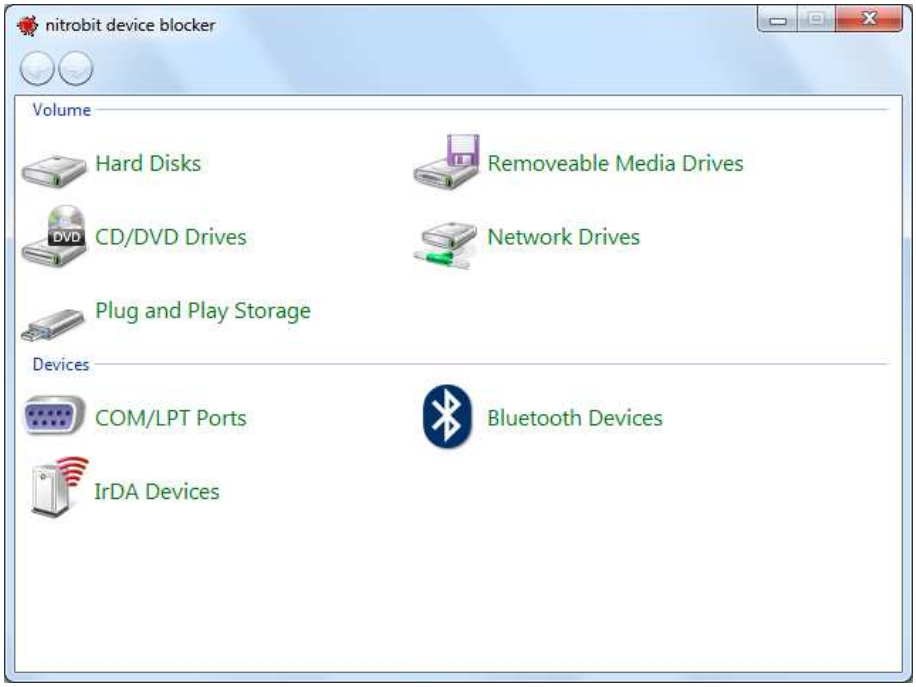
- Microsoft Windows 2000, ServicePack 4
- Windows XP,
- Windows 2003
- Windows Vista

System Setup

To make use of nitrobit device blocker, the software has to be installed on every client computer. A server-side setup or configuration is not necessary.
On administration workstations, you can use the setup to install the editor and client components manually or automatically. For user workstations you can additionally use the group policy based integrated client deployment to install the client component without running a setup program.
Please have a look at chapter IV. Managing Clients on page 12 for further details of the installation.

III. Defining Policies

nitrobit device blocker can define access policies to certain storage media types as well as certain device types. These access policies are managed on a per computer basis and valid for all users on the machine.



Devices

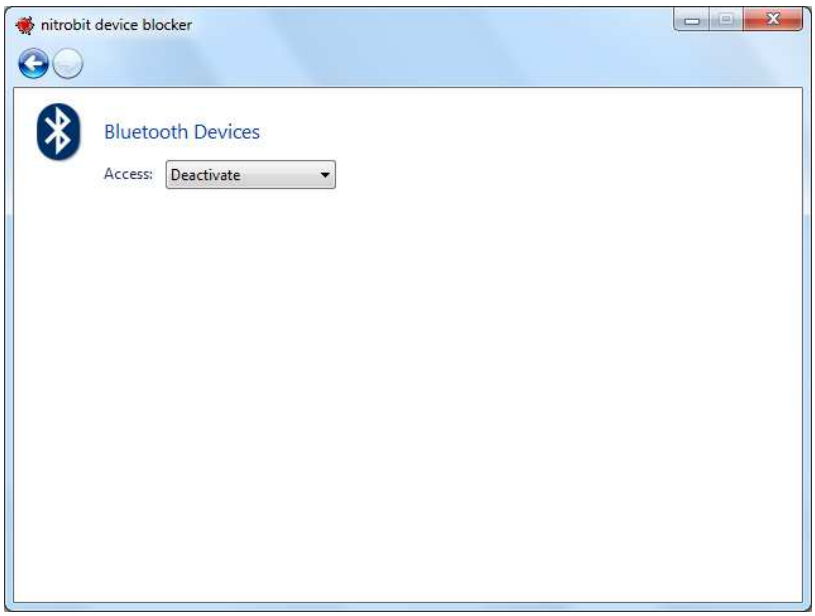
The device management of nitrobit device blocker enables you to activate and deactivate the following device types:

- COM/LPT devices
- Bluetooth devices
- IrDA devices

Defining a device definition

In order to define a device definition, please carry out the following steps:

- Start the nitrobit device blocker editor and open the device type for which you would like to add an access rule by clicking on it.
- On the following screen, you can activate or deactivate the device.



Volume Access

Through volume access policies, nitrobit device blocker helps to control access to external resources on the corporate network. This helps to protect corporate networks from leaking confidential information.

Nitrobit device blocker can distinguish between the following volume types:

- **Hard disks**
  Fixed disks installed on the system. Drives using hot plug busses like USB do not belong to this category, they are categorized as plug and play storage.
- **Removable media drives**
  Drives using Floppies, SD-Cards, ZIP-, and MO-Media. Drives using hot plug busses like USB do not belong to this category, they are categorized as plug and play storage.
- **Plug and play storage**
  All storage devices connected via a Plug and Play Bus. USB-Floppy drives, USB-Hard disks, USB CD/DVD drives and USB Memory Sticks belong to this category, as well as IEEE 1394 Devices.
- **CD/DVD drives**
  All CD and DVD reader/writer drives.
- **Network drives**
  All Network Drives using the Windows/CIFS protocol or WebDAV.

The administrator can control how access to each of these volume types is handled. Additionally the administrator can also define exceptions for each volume type. Nitrobit device blocker can enforce the following access rules:

- **No access**
  The user cannot read or write any data.
- **Read only**
  The user can read files and see directory contents, but cannot write to the volume.
- **Full access**
  The user has full read and write access to the volume.

Please note that additional access control mechanisms may exist, e.g. NTFS-, or share-permissions.

Exceptions

Two different kinds of exceptions are available, depending on the volume's type:

- **Path exceptions**
  Can be defined on all volume types except CD/DVD drives.
- **Device exceptions**
  Can be defined on plug and play storage volumes.

Path Exceptions

Path exceptions allow to define a different access rule for a given path. The access rule consists a path and its access rule. If a file is accessed and its path matches the the access rule, then the access rule is enforced.
The path of an access rule can contain wild cards. If it does not contain any wild card, it will be used as "starts-with" match. Therefore, "`\Temp`" is the same as "`\Temp*`".
Environment variables will be substituted. For example, `%USERNAME%` will be replaced with the username of the current user.
Hard disks and removable media drives can contain a drive letter in the path. If it is left out, the path will match on all hard disks. For example, `C:\Temp` will match on the folder `\Temp` on the first hard disk. `\Temp` will match the Folder `\Temp` on every hard disk.
Plug and play storage devices will get a new drive letter every time they are connected to the computer. Therefore using a drive letter in the path rule for removable storage devices is not supported.
Path rules for network drives are defined by their UNC path even if the network drive is connected through a drive letter. Example: `H:` is a connected network drive that points to `\\server\homes\username`, the corresponding path rule would be `\\server\home\%username%`.
Path exceptions are evaluated in an ordered list. The first exception that matches will be used. Therefore, special cases must be ordered before general cases, e.g. "`C:\Temp\Download`" must be ordered before "`C:\Temp`".

Device Exceptions

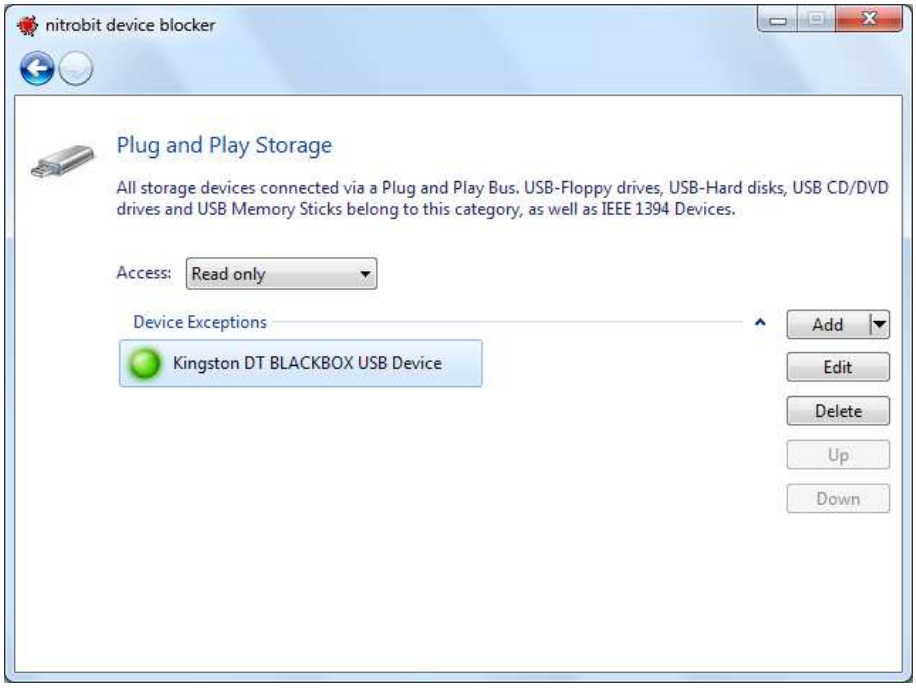
Device exceptions allow to define a different access rule for a specified device. The access rule consists of an access rule, a vendor ID, a product ID and an optional serial number.
Use the product and vendor ID to target specific devices of the same kind. For example a specific USB memory stick product. Additionally, you can specify the serial number to target a specific device by its unique USB ID.

Path and device exceptions can even be combined. If both, a path and a device exception, are matching at the same time, the more restrictive rule will be enforced.

Define a volume access policy

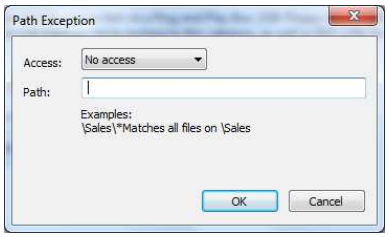
To define a volume access policy, double click the volume type you want to configure. First, define the default access rule, which can be one of the following:

- No Access
- Read only
- Full Access (default)

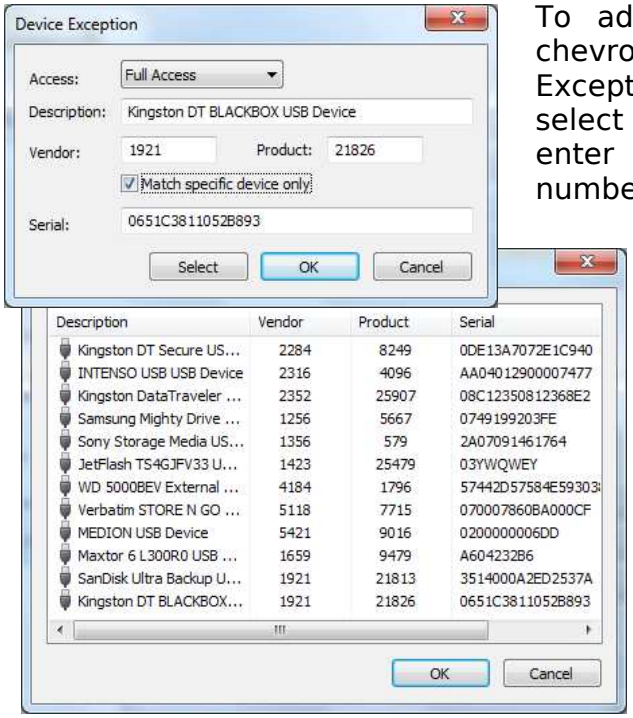


Define a volume path exception

To add a new volume path exception, simply click the “Add” button. On the dialog that pops up, you can select the access rule for this exception and you can enter a path for which the exception is valid.
For a complete description of path exceptions please refer to the chapter “Path Exceptions“ on page 9.



Define a volume device exception



To add a new device exception, click the chevron on the “Add” button and select “Device Exception”. On the dialog that pops up, you can select the access rule for this exception. Next, enter a product and vendor ID. The serial number is optional. If the serial number is omitted the device exception will be valid for the product. If you specify a serial number, the exception is valid only for this unique device.

Instead of entering a product and vendor ID, you can also select a device by clicking the “Select” button. On the following dialog you can choose between all storage devices, that have already been connected to the computer.

Finally, you can enter a description for the exception.

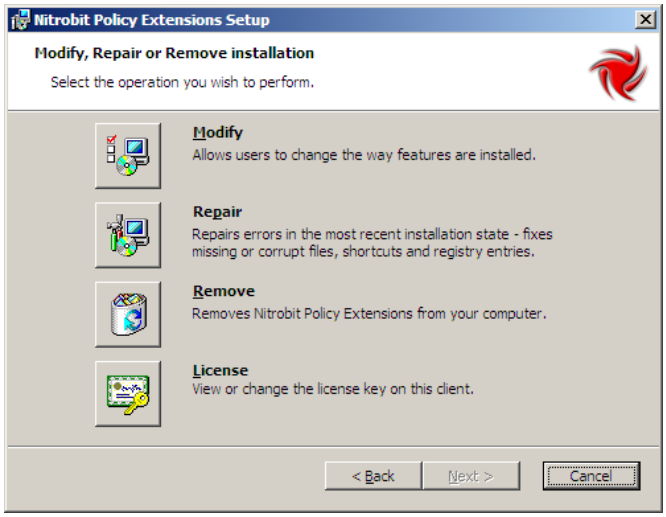
IV. Managing Clients

Client Setup

In order to use nitrobit device blocker, you need to install the client component on every workstation. You can install the nitrobit device blocker Client in different ways. If you plan to install a larger number of clients, you may consider the automated client roll out options described below.

Manual Installation

In order to install the client component manually, you can directly execute the nitrobit device blocker installer file named NitrobitDeviceBlocker.msi. During the installation, you can supply licensing information. If no license is submitted, the software will run in an evaluation mode. You can add a license key later by restarting the setup and choosing the “License” button.



Automated Client Rollout

The client installation can be automated. The property `LICENSEFILE` can be used to configure the client as needed. You can also change the installation directory with the `DIR_NBPROGRAM` property. To submit properties for a silent installation, use the following sample command line:

```
msiexec /i c:\myfolder\NitrobitDeviceBlocker.msi /qn
LICENSEFILE=”c:\myfolder\Nitrobit.lic”
DIR_NBPROGRAM=”c:\Program Files\My folder”
```

Automated Client Rollout with an Administrative Installation

In addition to command line options, you can specify the licensing information during an administrative installation. Use the following command line to start the administrative installation:

```
msiexec /a c:\myfolder\NitrobitDeviceBlocker.msi
```

Now you can use the administrative installation package to install clients manually or automatically without the need to reenter client configuration data.

Automated Client Update

You can also automate the Update Process for your clients. To update your clients with a new version of nitrobit device blocker, use the following sample command line:

```
msiexec /qn /fvoums c:\myfolder\NitrobitDeviceBlocker.msi
```

Your installed license key remains intact.

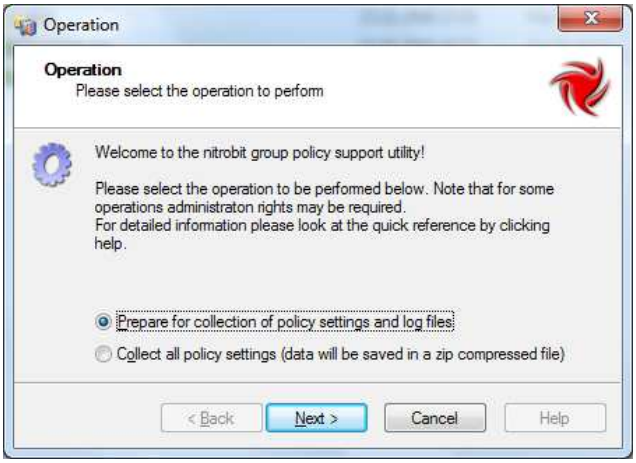
Note that the /qn Option suppresses any dialogs. This includes the reboot confirmation dialog.

Detecting and Resolving Problems

In order to find any problems regarding the nitrobit device blocker client, you should check the event log. The nitrobit device blocker client reports any error condition to the application event log. Moreover, you can get a detailed report of the policy enforcement if you raise the logging level to high logging.

Using the Support Data Collection Tool

If you need to collect data for the nitrobit support team or want to collect data from a machine for your own debugging purposes, you can use the Data Collection Tool that is shipped with nitrobit device blocker. It is located in the Support folder of your installation source and called Support.exe.



You can prepare the Data Collection by raising the nitrobit client Event Log Level to the maximum. Further, Support.exe can collect Data into a Zip-File.

Client Reference

Registry Values

The client component uses the following registry values stored at:

`HKEY_LOCAL_MACHINE\SOFTWARE\Nitrobit\nitrobit device blocker`

`LogLevel`	DWORD-Value defining the logging level for EventLog messages. Values: 0: default; 1: high.
`License`	Client License

V. Legal Notice

Contact

analytiq consulting gmbh
Hermann-Steinhäuser-Straße 43-47
63065 Offenbach
Germany

Tel: +49 (69) 1730 9891 0
Fax: +49 (69) 1730 9891 1
E-Mail: support@nitrobit.com
Web: www.nitrobit.com