nitrobit
policy extensions

Administrator's Guide

Content

Document Version: 1.1

I. Introduction

Overview

nitrobit policy extensions are an add-on for the Windows group policy system. The extensions provide new functions within group policy objects. Those functions could so far only be used with the aid of self-scripting or manual customization of the user configuration.

Functions of nitrobit policy extensions

With nitrobit policy extensions, group policies can execute the following functions:

- **Deployed Printers**
  Allows to assign local printers, TCP/IP-printers as well as printers, that are shared through a windows-server to users and computers.

- **Network Drives**
  Configures the connection to network-drives for the user.

- **Device Restrictions**
  Can restrict users to access certain devices.

- **Services**
  Allows the configuration of Services, e.g. starting and stopping a service during the user log-in.

- **Registry**
  Allows the creation of registry keys and values.

- **Volume Restrictions**
  Can restrict access to certain storage media types.

System Components

nitrobit policy extensions are group policy extensions. They consist of a group policy object editor extension as well as a group policy client extension. The extension of the group policy object editor allows editing the nitrobit policy extensions within the Microsoft Management Console (MMC) environment.
The extension of the group policy client is responsible for executing the group policies on the target computers.
Both components can be installed within one setup. Moreover, you can install the group policy client directly from a group policy.

II. Installing the system

System requirements

nitrobit policy extensions can be used on workstations with one of the following operating system:

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

The following server- and domain-models are supported:

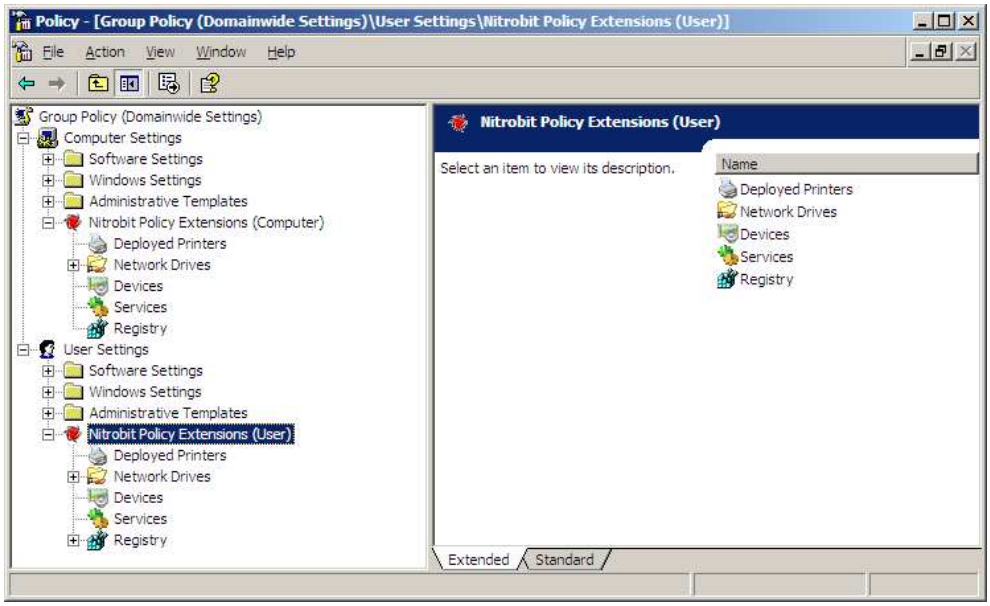
- Windows 2000 Server with Active Directory
- Windows 2003 Server with Active Directory
- Windows NT4 Server with NT-4 domain and nitrobit group policy
- Samba 3.x with Samba Domain and nitrobit group policy
- Samba 4.x with Active Directory Domain
- Samba 4.x with Samba Domain and nitrobit group policy

System Setup

To make use of nitrobit policy extensions, the software has to be installed on every client computer. A server-side setup or configuration is not necessary. The nitrobit policy extensions Client can be installed in different ways.
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 for further details of the installation.

III. Defining Policies

With nitrobit policy extensions computer- as well as user-policies can be defined. Thus, the policy extensions can be found in both configuration trees of a group policy object. Depending on whether you choose to establish guidelines within the computer configuration or the user configuration the functions differ slightly.



Printers

The Printer manager helps you to centrally define printers that are available within the user's environment.

The printer manager of nitrobit policy extensions distinguishes three different printer-types:

- **Network printers** are shared by a Windows print server.
- **TCP/IP-Printers** are being addressed directly through the network or through an LPR-Print server.
- **Local Printers** are attached directly to the local PC.

Network printers can be added either to the user settings or to the computer settings of a group policy.
If a printer has been applied to the user settings, the user will be automatically connected to the printer during the logon-process – no matter which PC the user is working at.
If a printer has been created within the computer settings, every user that logs onto that computer, will be connected to the printer.

Defining a printer within the user settings always makes sense, when a printer should be made available to a certain group of users, e.g. a plotter to the construction department.
Defining a printer within the computer settings is useful when a printer should be available at certain computers, e.g. all computers in a certain room or floor.

Local printers are usually defined within the computer settings. The attached device will be installed on the corresponding computer and can than be used by all users, that log on to that computer.

It is also possible to install a TCP/IP-printer within the user settings of a group policy. The respective printer will be installed on every computer the user logs on and will be deinstalled when the user logs off. This approach can be useful for software solutions, e.g. a fax printer or PDF-printer.

Local or TCP/IP-Printer, which are defined within the user settings, will only be installed when the user logs on interactively at a certain computer. Within terminal server sessions only local and TCP/IP-Printer which are defined within the computer-configuration are installed.

Creating a printer definition

To define a printer definition, please follow the instruction described below:

- Start the group policy object editor and open the group policy you would like to use for creating the printer.
- In the tree view, open the folder “Nitrobit Policy Extensions (Computer)”, if you would like to create the printer within the computer configuration. Open “Nitrobit Policy Extensions (User)”, in case the printer shall be installed within the user settings.
- Select the printer-object.
- In the action menu or in the context menu under “New” select the according

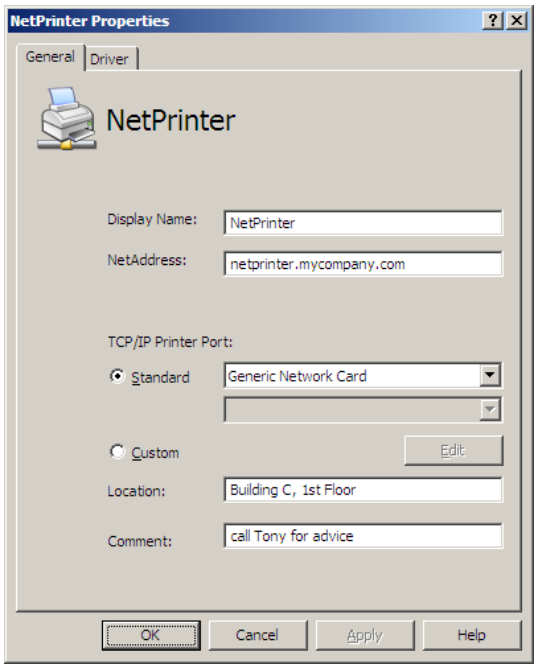
printer type you would like to create.

Configuring Network Printers

For a network printer you only need to specify the server name and the share name of the printer on that server. The computer can then retrieve further configuration parameters directly from the server during the connecting process. Also the printer driver will be downloaded and installed from the print server.

Configuring TCP/IP-Printers

TCP/IP-Printer need the following general information:



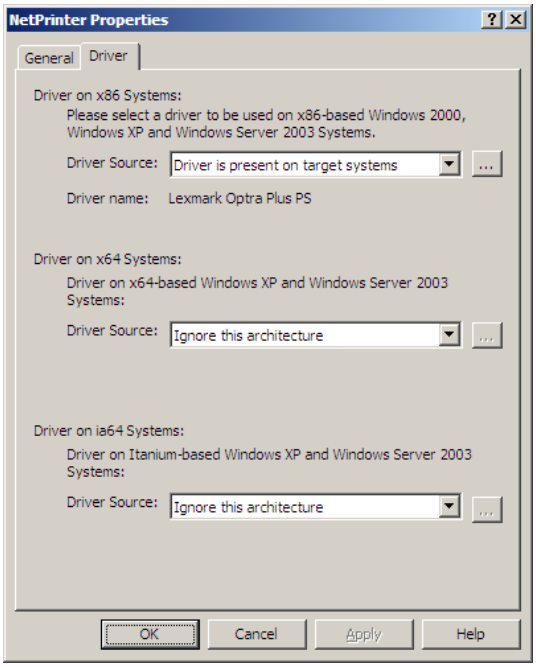
- A **display name**, which will represent the printer within the user's environment.
- A **network address**, at which the printer can be accessed. You can either use a TCP/IP-Address or a DNS-name for that.
- For the **TCP/IP Printer port** you can choose a standard port out of the list.
- If there are no port definitions available for your printer-model, you can create your own **user-defined port**. For this please name the protocol (**Raw** or **LPR**). For the Raw-Protocol you additionally have to enter the **port number**. The standard port is 9100. For the LPR-Protocol please specify the **queue name**. If supported by your printer or print server, you can furthermore enable the SNMP-Protocol.
- Optionally you can enter a **location** and a **comment**. Both entries will later appear within the properties of the created printer and will be indicated to the user.

Beside the general information it is also necessary to choose a printer driver, which should be used by the created printer.
For the following architectures the printer driver can be assigned independently:

- **x86-Systems**
  with the operating systems Windows 2000, Windows XP, Windows Server 2003 and Windows Vista.

- **x64-Systems**
  with the operating systems Windows XP, Windows Server 2003 and Windows Vista.

- **ia64-Systems**
  with the operating systems Windows XP, Windows Server 2003 and Windows Vista.



To choose the adequate driver, please use the browse button.

For every architecture you can choose between the following different installation sources for the printer driver:

- **Existing driver on the target system**
  The selected driver is delivered with the operating system or installed by a softwaredistribution-system.

- **Driver is copied into the group policy**
  The selected driver is copied into the group policy object and gets installed on the computer during the installation process of the printer.

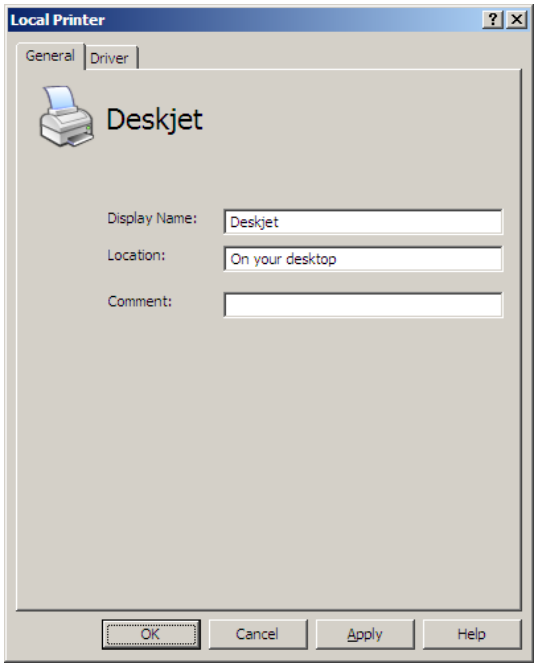
- **Driver is present on a network share**
  The selected driver can be installed directly from a network drive. To do so, please additionally fill in the network path of the driver.

- **Ignore this architecture**
  Please choose that option, if there is no adequate driver available for the respective architecture.

Configuring local printers

The following details are needed for local printers:

- A **display name**, which will represent the printer within the user's environment.
- Optionally you can enter a **location** and a **comment**. Both entries will later appear within the properties of the created printer and will be indicated to the user.



Additionally to that information it is necessary to select a printer driver for the printer. Please have a look at the paragraph on TCP/IP-Printer to find out how to assign a printer driver.

Network Drives

With nitrobit policy extensions you can assign network drives to users as well as computers.

In case you define a network drive within the user settings, the users will be connected to the network drive during log-on. That way you can assign a group drive to a certain department, e.g. the accounting department.
If you use environment variables, you can assign users their home directory.

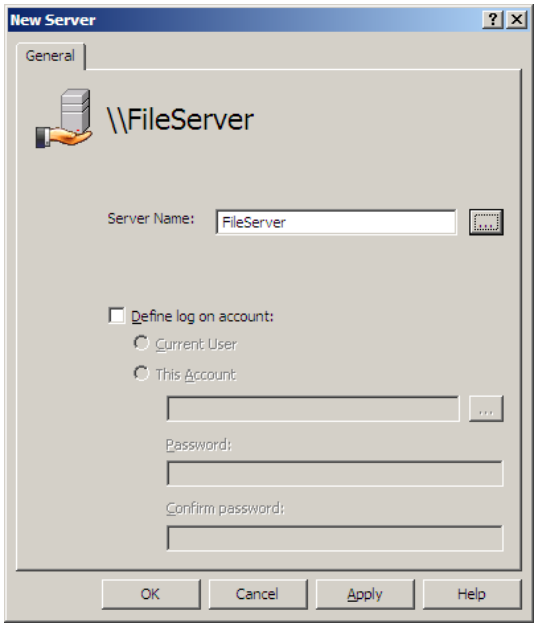
It is also possible to define a network drive within the computer settings. All users that log on to that computer are then connected to that network drive.

That way location related directories can be managed. For example, you can connect notebooks to the server within their current location.

Creating a server definition

In order to create a new server definition, please execute the following steps:

- Start the group policy object editor and open the group policy you would like to use for creating the server.
- In the tree view, open the folder “Nitrobit Policy Extensions (Computer)”, if you would like to create the server within the computer configuration. Open “Nitrobit Policy Extensions (User)”, in case the server shall be created within the user settings.
- Select the network drives object.
- In the action menu or in the context menu under “New” select “New Server”.



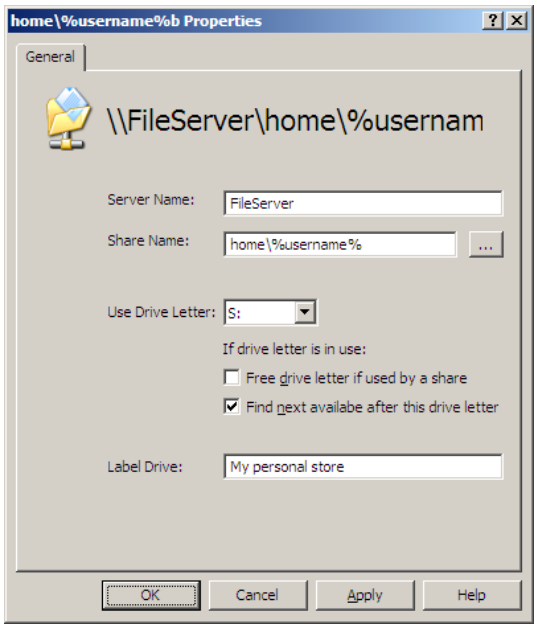
Defining parameters for a server

In order to define a server, you need to specify the network name which can be used to reach the server within the network. You can enter the DNS-Name, the Net-Bios Name or an IP-Address.

Furthermore you can configure a logon account, which will be used to connect network drives on that server. If you do not specify a logon-account, a connection to the server will be established in the context of the logged on user.

Defining parameters for a network drive

The following entries are necessary for a network drive:



- The share name of the network drive. The path may also include environment variables, i.e. %UserName%.
- The drive letter, which will be used to connect the network drive.
- Furthermore, you can determine how to handle situations where the drive letter is already occupied. First of all you can disconnect a network drive, that may occupy the drive letter. Moreover you can search for the next free drive letter that follows the drive letter you initially wanted to use.
- Optionally, you can enter a label for the network drive, which will be displayed in the user's environment.

Devices

The device management of nitrobit policy extensions enables you to activate and deactivate devices.

The devices can be managed through the computer- or the user settings. If you want to activate or deactivate a device at certain computers you have to define a device within the computer settings. Use the user settings to enable or disable devices on a per-user basis. For example, you can deactivate the access to all USB mass storage devices for certain users.

Within the device management you can define three different objects:

- **Devices** are system components, that are using the same device driver, e.g. USB mass storage devices or Intel PRO/100 network adapter. You can optionally specify that your device definitions should be applied to compatible devices, too.

- **Device Classes** are groups of devices, e.g. USB-controllers or network adapters. If a device class gets deactivated, every device belonging to that class are deactivated.

- **Device Categories** are groups of devices, that are fulfilling similar functions, but do not necessarily form a device class. Device categories are for example all removable mass storage devices or all wireless network adapters.

Defining a device definition

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

- Start the group policy object editor and open the group policy you would like to use for creating the device definition.

- In the tree view, open the folder “Nitrobit Policy Extensions (Computer)”, if you would like to create the device within the computer configuration. Open “Nitrobit Policy Extensions (User)”, in case the device shall be created within the user settings.

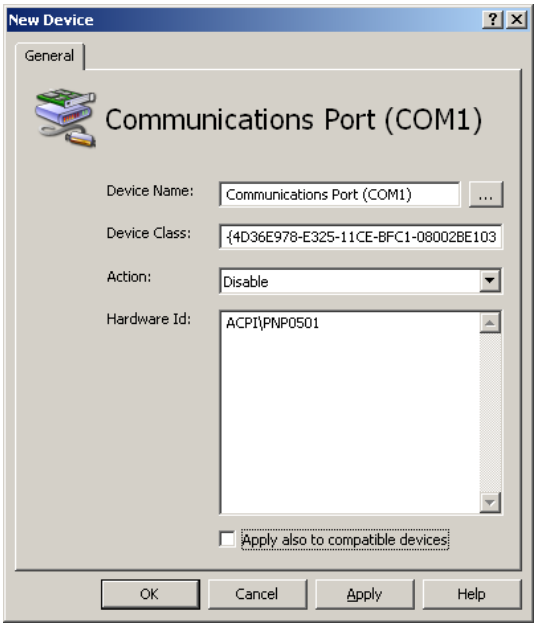
- Select the devices object.

- In the action menu or in the context menu under “New” select “New Device”.

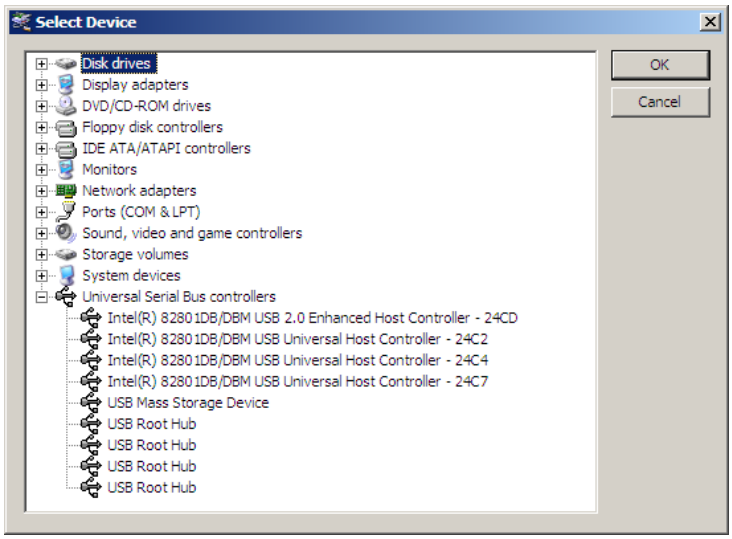
Defining parameters for a device

A device definition consists of the following parameters:

- A **device name**, which only comes to use within the group policy object editor.
- A **Device Class ID** to which the device belongs.
- A **Hardware ID** clearly identifying the device.
- An **action**, that should be executed for the device. You can activate or deactivate the device.
- Optionally, you can apply the definition to compatible devices as well.



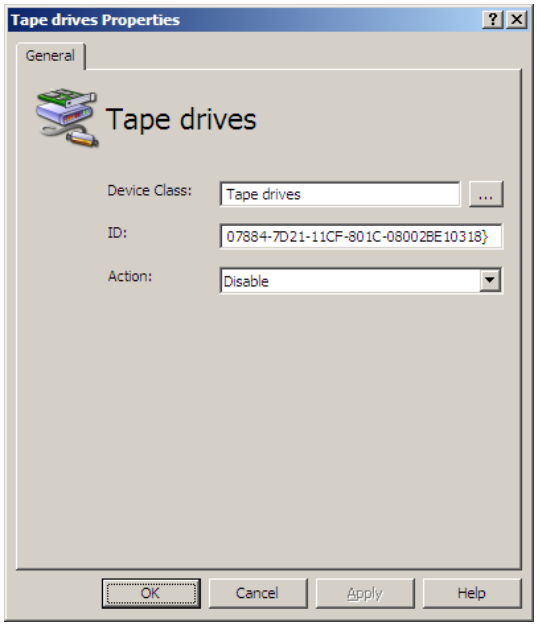
In order to produce a device definition, you can use the search-button to select a locally available device and take over its values. Within the search-dialog you can see all locally available devices, that support deactivation.



Defining parameters for a device class

A device class needs the following parameters:

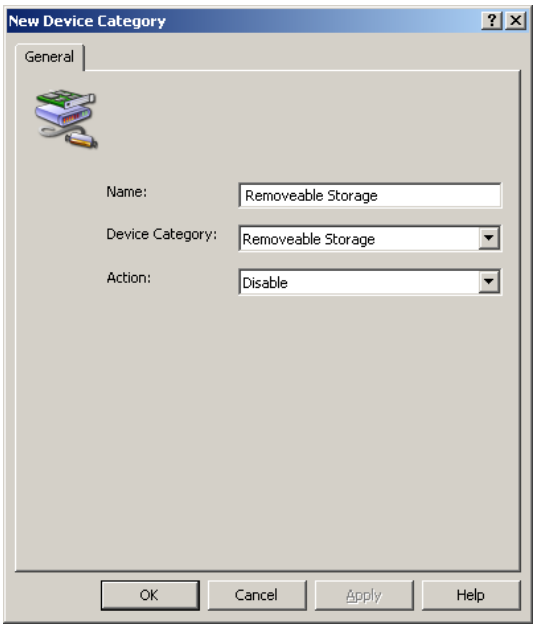
- A **device class name**, only being used within the group policy object editor.
- A device class ID clearly identifying the device class.
- An **action**, that should be executed for all devices within the class. You can activate or deactivate those devices.



Defining a device category

For a device category please select the category-type as well as the action, that should be executed for all devices of that category. The following device categories are available:

- **Removable Storage**
  All plug and play mass storage devices, e.g. USB memory sticks and FireWire hard disks.
- **All Plug and Play devices**
  This device category was designed to give special users, e.g. Administrators access to all devices which were disabled through other group policy objects.



Processing order of device policies

Device policies can be defined in the user settings as well as computer settings. Device definitions in the computer- and user settings may overlap. Moreover, it is possible that device definitions from different group policy objects target the same device. Also, a definition for a device can be defined but a device category or device group definition can apply to the same device, too.

For this reason, there exists a well-defined processing order for device policies:

- First, all computer policies are applied, then all user policies.
- Inside a group policy object, device categories will be applied at first, thereafter device classes will be applied. Last, policies for a single devices are applied.

With this processing order, user settings will overwrite computer settings, and policies for a single device will overwrite policies for device classes and device categories.

Services

The service management of nitrobit policy extensions allows a simple configuration of system services. Primarily services can be defined within the computer configuration. The following adjustments are possible:

- **Start action**
  The service will be started or stopped during the execution of the group policy.

- **Startup type**
  Changes the startup type of the service.

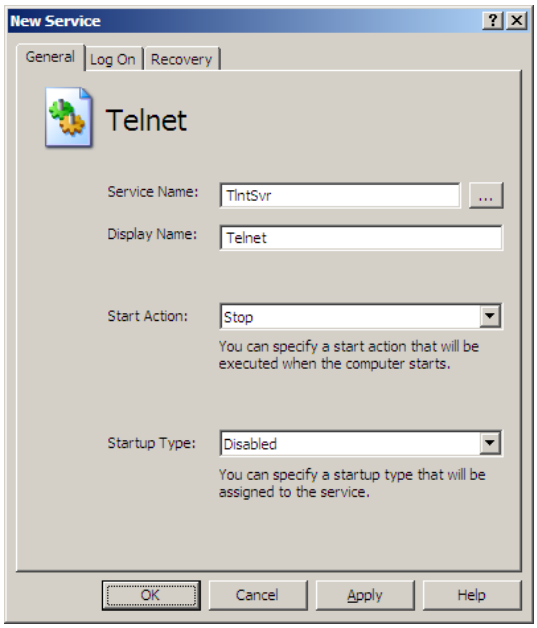
- **Logon account**
  Defines the logon account to be used by the service.

- **Recovery**
  Defines actions, that should be executed when the service fails.

Furthermore you can define services within the user configuration. In that case you can however only define a start action, that should be executed during log-on of the user.
The start actions defined within the user settings are only applied within interactive logons. Thus, they are not used during terminal server sessions.

Defining a definition for a service

In order to create a new definition for a service, please carry out the following steps:



- Start the group policy object editor and open the group policy you would like to use for creating the service definition.

- In the tree view, open the folder “Nitrobit Policy Extensions (Computer)”, if you would like to create the service within the computer settings. Open “Nitrobit Policy Extensions (User)”, in case the service shall be created within the user settings.

- Select the services object.

- In the action menu or in the context menu under “New” select “New Service”.

Specifying parameters for a service

You can define the following parameters for a service:

- The **service name** of the service, that you would like to configure. For taking over a name of a local service, please use the search-button next to the input field.
- The **display name** of the service
- Optionally you can choose a **start action**, that should be executed. For services defined in the computer settings, the selected action will be executed during the start of the computer.
  Start actions for services defined within the user settings will be executed during the logon of the user.

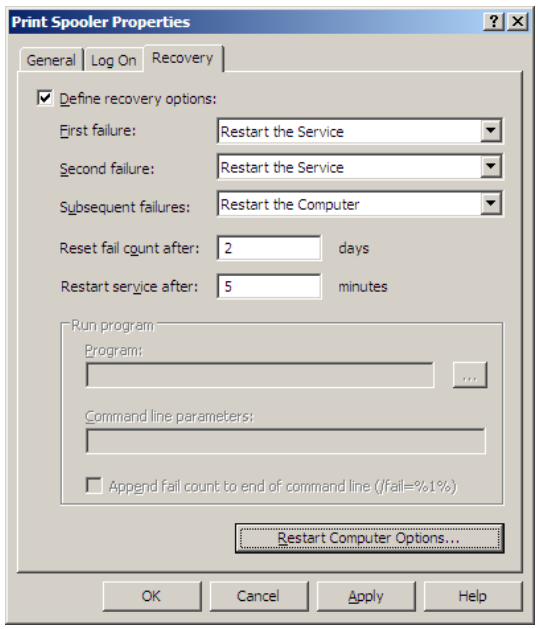
Services within the computer settings additionally have the following parameters, which can be optionally defined:

- The **start type** of the service

- The used **logon account**.
  You can either use the local system account or an account specified by you. If you are using the local system account, you can decide furthermore, if the relevant service is allowed to interact with the desktop. For other accounts you can check at the target computer, if the account has the local right to logon as service.

- **Recovery options**
  You can determine, which action should be taken when the service fails.

  The actions for the first, second and all further failures can be defined separately. A possible action can be to restart the service, to execute a program or to restart the computer.



Registry

Nitrobit policy extensions helps you to change registry variables fast and easy. Similar to the administrative templates all changes will be undone when a different user logs on or a policy no more applies.

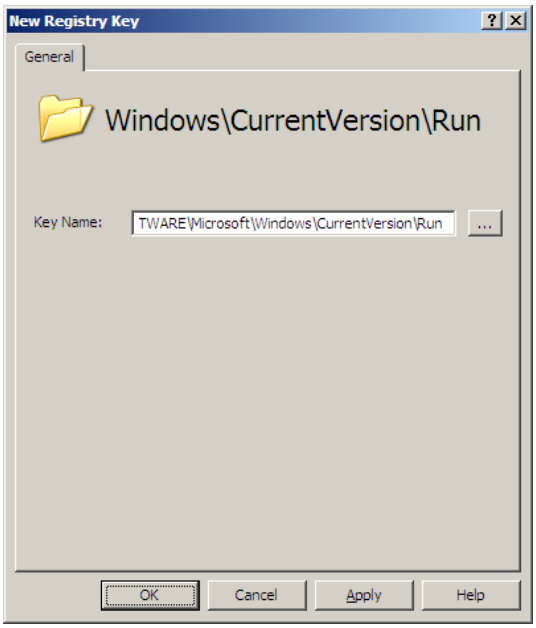
Using the registry extension of nitrobit policy extensions always makes sense when you want to manage only a few values within the registry.

If you need to manage a large amount of values, you should create a script for the administrative templates.

Creating a Registry Key

For inserting a registry key please carry out the following steps:

- Start the group policy object editor and open the group policy you would like to use for creating the registry key.
- In the tree view, open the folder “Nitrobit Policy Extensions (Computer)”, if you would like to create the key within the computer settings. Open “Nitrobit Policy Extensions (User)”, in case the key shall be created within the user settings.
- Select the registry object.
- In the action menu or in the context menu under “New” select “New Registry Key”.



Parameters for a registry key

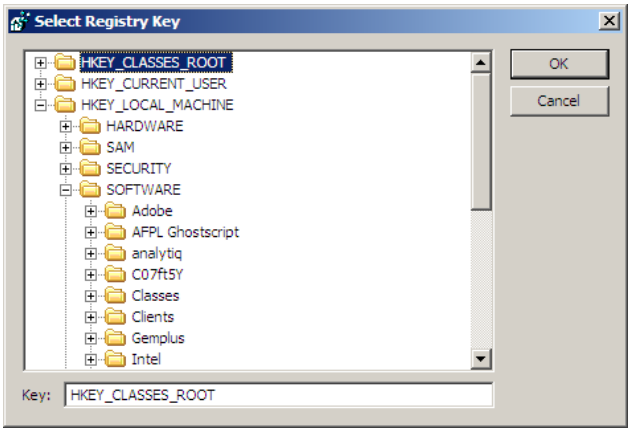
For a registry key you only have to specify its path. Please insert the complete path beginning at the root key. The single key names should be separated by “\”. Possible root keys are:

- **HKEY_CLASSES_ROOT**
- **HKEY_LOCAL_MACHINE**
- **HKEY_CURRENT_USER**

Within the user settings you can furthermore use as root key:

- **HKEY_CURRENT_USER**

For choosing a key out of the local registry, you can use the browse-button.

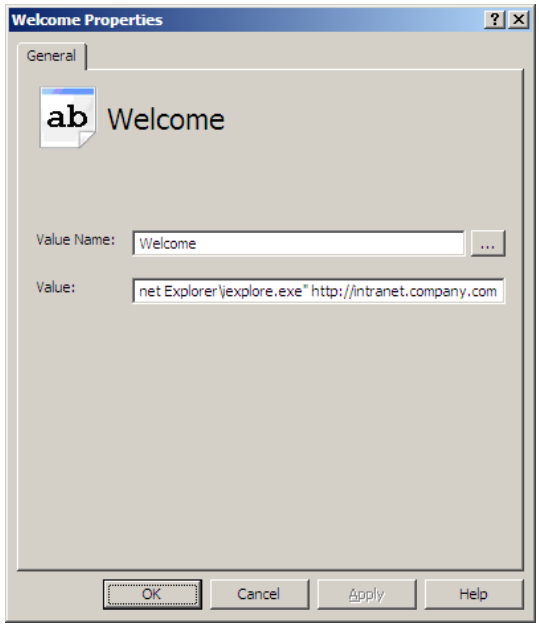


Defining a Registry Value

Within a registry key you can insert different values. The following types of registry values are possible:

- **String Value**
- **Binary Value**
- **DWORD Value**
- **Multi-String Value**
- **Expandable String Value**

For the registry value please insert the value name as well as the value itself.



Volume Access

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

Nitrobit policy extensions 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 policy extensions 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

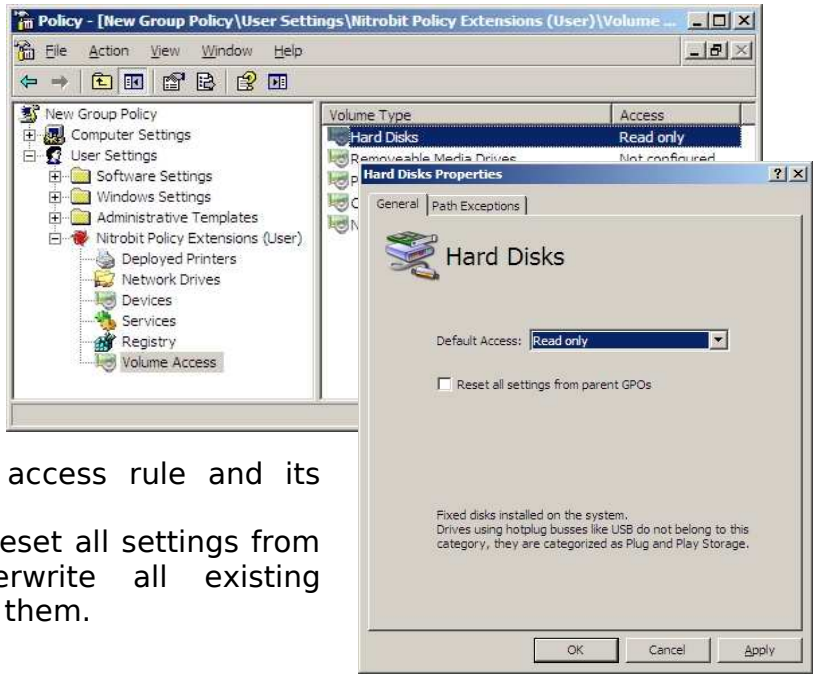
Device exceptions allow to define a different access rule for a specified device. The access rule consists of an access rule, a vendor ID, a product ID and an optional serial number.
Use the product and vendor ID to target specific devices of the same kind. For example a specific USB memory stick product.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

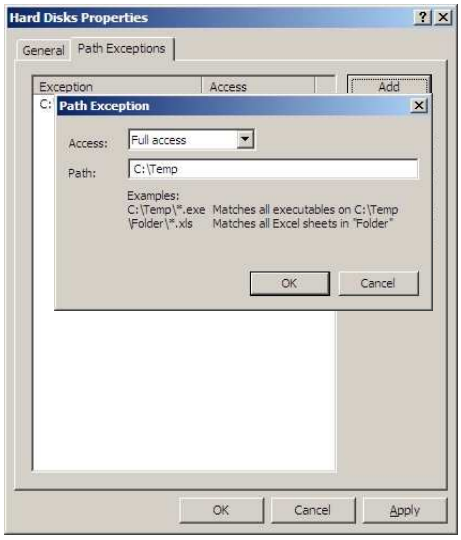
- Not configured (default)
- No Access
- Read only
- Full Access



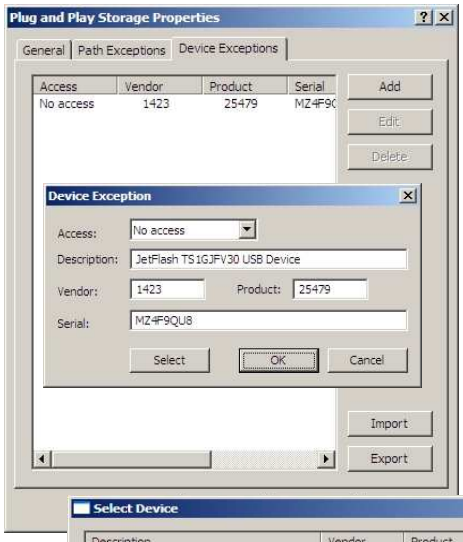
If you set the default access rule to “Not configured”, the access rule and its exceptions are inactive.
Additionally, you can define to reset all settings from parent GPOs. This will overwrite all existing exceptions instead of appending them.

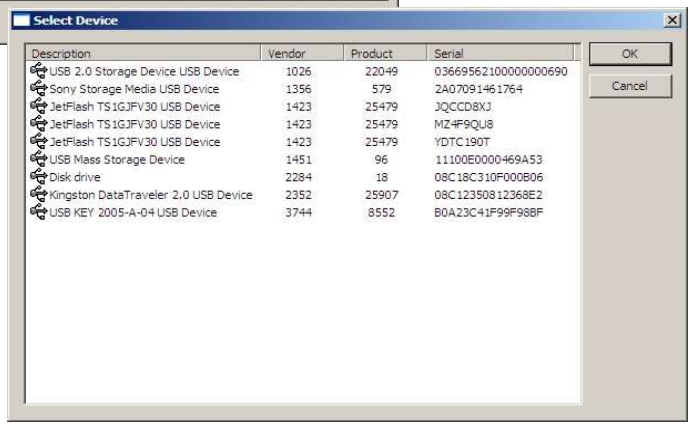
Define a volume path exception

To add a new volume path exception, click the “Add” button on the path exceptions tab. 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 22.



Define a volume device exception





To add a new device exception, click the “Add” button on the device exceptions tab. 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.

You can export the list of devices shown in the device exceptions tab by clicking the “export” button. The list of devices is exported to a CSV formatted file. You can also import devices from a file by clicking the “import” button.

IV. Managing Clients

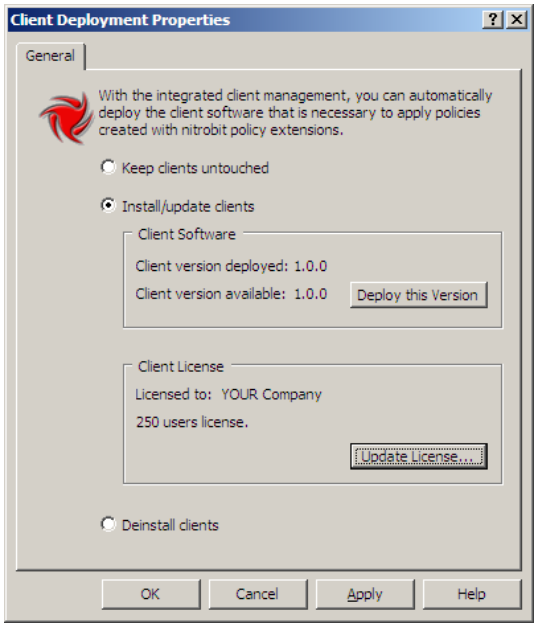
Client Setup

In order to use nitrobit policy extensions, you need to install the client component on every workstation. You can install the nitrobit policy extensions 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.

Integrated Client Management

A very effective method to deploy nitrobit policy extensions is available with the integrated client management. To use it, you need to install nitrobit policy extensions on your administration workstations. The client component that needs to be installed on the user's workstations, can now be deployed with a group policy. You need to accomplish the following steps:

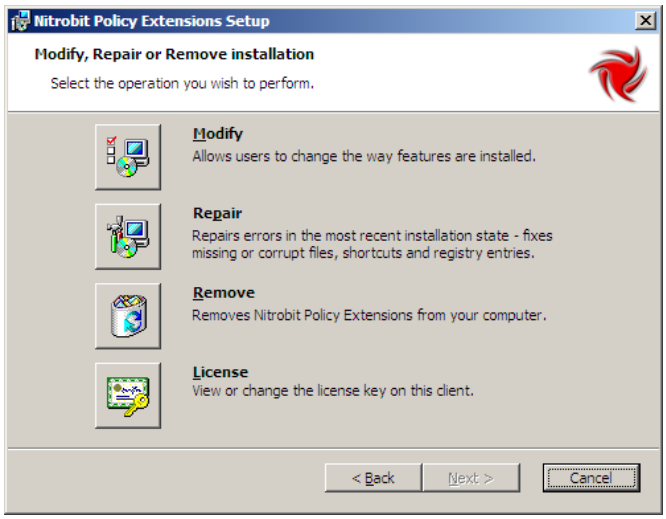
- Start the group policy object editor and open the group policy you would like to use for deploying the client.
- In the tree view, open the folder “Nitrobit Policy Extensions (Computer)”.
- In the list view, open the object “Client Deployment” by double-clicking it.
- Now you can specify if this policy should install or deinstall the client software, or if clients should be left untouched.
- If you want to install clients, you can update the software version to be deployed with the version present on your workstation.



- Furthermore you can add a license key which will be installed on the workstations.

Manual Installation

In order to install the client component manually, you can directly execute the nitrobit policy extensions installer file named NitrobitPolicyExtensions.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\NitrobitPolicyExtensions.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\NitrobitPolicyExtensions.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 policy extensions, use the following sample command line:

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

Your installed license key remains intact.

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

Client Management

The nitrobit policy extension client can be managed by means of group policies. Your setup sources should contain a Folder Administration containing a file named npe.adm. Using this administrative template file, you can control the client's, logging level and license key through a group policy object. In order to add the administrative template to a group policy object, you need to accomplish the following tasks:

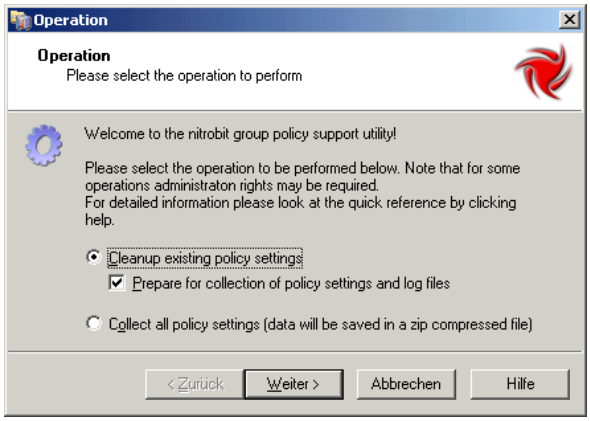
- Open the group policy object editor for the respective group policy object.
- Select the Computer Settings/Administrative Templates folder.
- Use the Add/Remove Templates command from the Action menu.
- Select the Add button and use the file select dialog to navigate to the npe.adm file.

Detecting and Resolving Problems

In order to find any problems regarding the nitrobit policy extensions client, you should check the event log. The nitrobit policy extensions client reports any error condition to the application event log. Moreover, you can get a detailed report of the group policy execution 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 policy extensions. It is located in the Support folder of your installation source and called Support.exe.



The tool provides a cleanup mode in order to reset misconfigured clients. Additionally, 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 policy
   extensions
```

`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