nitrobit group policy

Administrator's Guide

Content

Document Version: 2.14

I. Introduction

Overview

Nitrobit group policy is a configuration system for Microsoft Windows operating systems. It was designed as a replacement for Microsoft's Group Policy System, since it has a major disadvantage: It does not work without Microsoft Active Directory.

Components of the Nitrobit Group Policy System

The nitrobit group policy system consists of a client component to apply group policy objects to the target computer and an editor environment to administer the group policy system.
The client component needs to be installed on every computer that should process nitrobit group policies. The nitrobit group policy client is invoked during the computer startup process to apply machine group policy objects. And it is invoked during the user logon process to apply user group policy objects. Additionally, the nitrobit group policy client is invoked periodically to apply background updates.

System requirements

The nitrobit group policy system can use the following operating systems as group policy clients and administrative workstations:

- Microsoft Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.
- Windows Terminal Servers and Citrix Presentation Server are supported clients.

The system can work with user accounts from domains maintained by Samba 3.x, 4.x, Windows NT 3.51/4 or Microsoft Active Directory. Alternatively, local accounts on Workstations or (Terminal-) Servers can be used.

About Group Policy Objects

Group policy objects are a collection of configuration parameters. They can be applied to computers or to users. The configuration parameters can be edited with Microsoft Management Console snap-in extensions. Group policy objects are applied to computers and users with the help of group policy client extensions.

How Group Policies are stored

Group policy extensions can use three different storage types to persist their data: File storage, registry storage, and LDAP storage.
The nitrobit group policy system itself only uses a central file share to store its data. Files created by group policy extenstions are stored on that share. Registry data as well as LDAP data is stored in database files. These database files are also written to that share.

Assigning Group Policies to Users and Computers

The nitrobit group policy system uses groups to decide wether a group policy object is to be applied to a certain user or computer. You can assign multiple groups to a group policy object. Different types of groups and different group behaviors are available to create a ruleset. If a target computer or user passes the ruleset, the group policy object will be applied.

II. System Administration Guide

Hands-On Tasks

This chapter will give you an overview of the most important administrative tasks.

Creating a Group Policy Hierarchy

To manage a group policy hierarchy, use the **nitrobit group policy system editor**. It is a Microsoft Management Console snap-in. You can use the shortcut named Nitrobit Group Policy from the start menu to launch the nitrobit group policy system editor. Alternatively, you may add the system editor snap-in to any other mmc-instance. In either case, you will be asked to enter the path to your group policy hierarchy. If you want to create a new group policy hierarchy, enter the path where the new group policy hierarchy is to be created. After you specified the path to your policy hierarchy, the central configuration file (Policy.ini) is read, or a new configuration file generated. You should save the Microsoft Management Console in order to store the path information you entered. Otherwise, you need to reenter the policy path next time you start the nitrobit group policy system editor.

Server requirements

- In order to setup a nitrobit group policy hierarchy, you need to configure a network share with read/write access for all policy administrators and read access for all users and machine accounts. You may enable read access for guests, especially if you want to use group policy clients on standalone workstations (i.e. workstations that are not members of any domain).
- If you are using serverbased user profiles, you need to ensure that the profiles can be read during user logon and written back as the user logs off. If there are any problems reading or writing back the user's profile, the group policy applying process might not work.

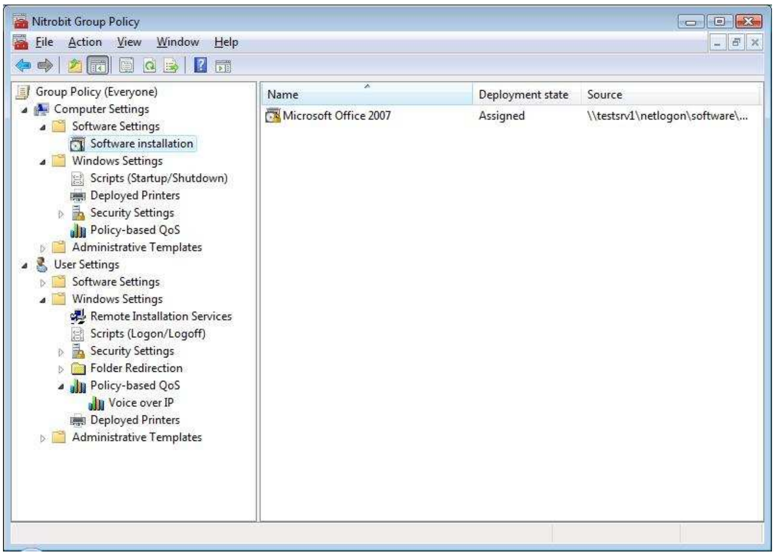
Creating a new Group Policy Object

New group policy objects are created with the **nitrobit group policy system editor**. You need to perform the following steps to create a new Group Policy Object:

- Open the nitrobit group policy system editor.
  Read the chapter “Creating a Group Policy Hierarchy” for further information.
- Right-click the Nitrobit Policy object at the tree view to open its context menu.
- Select New->New Policy...
- The new Group Policy Object will be created and should appear on the left side.
- You should rename the new Group Policy object in order to have a more descriptive display name than a UUID.

Editing Group Policy Objects

Group policy objects are edited with the **nitrobit group policy object editor**. You can edit a group policy object by adding the nitrobit group policy editor snap-in to any mmc-instance. A wizard will ask you for the policy path and the policy you want to edit. You can also launch the group policy object editor from the group policy system editor. This is done as follows:

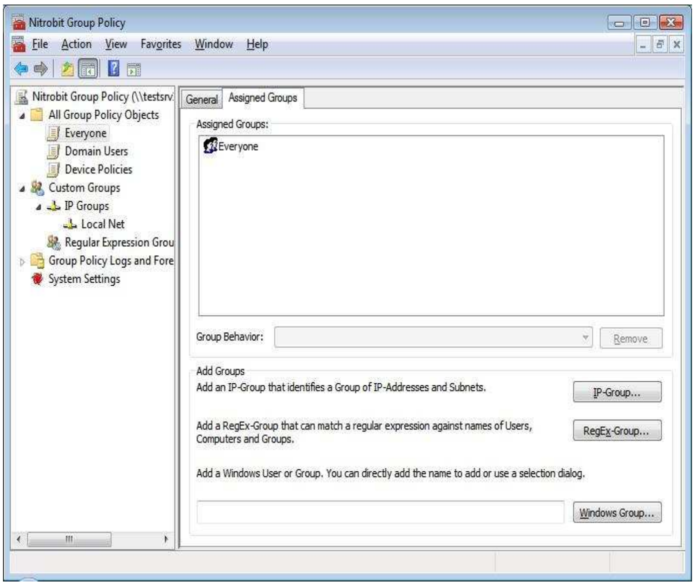


Name	Deployment state	Source
Microsoft Office 2007	Assigned	\\testsrv1\netlogon\software\...

- Open the nitrobit group policy system editor.
  Read the chapter “Creating a Group Policy Hierarchy” for further information.
- Right-click the group policy object you want to modify.
- Select Open Policy...
- A new group policy object editior should appear.

Assigning Groups to a Group Policy Object

Every group policy object has a list of groups assigned to it. If a user or computer is a member of at least one of these groups, the policy will be applied. In order to modify the list of assigned groups, you need to accomplish the following steps:



Add an IP-Group that identifies a Group of IP-Addresses and Subnets.

Add a RegEx-Group that can match a regular expression against names of Users, Computers and Groups.

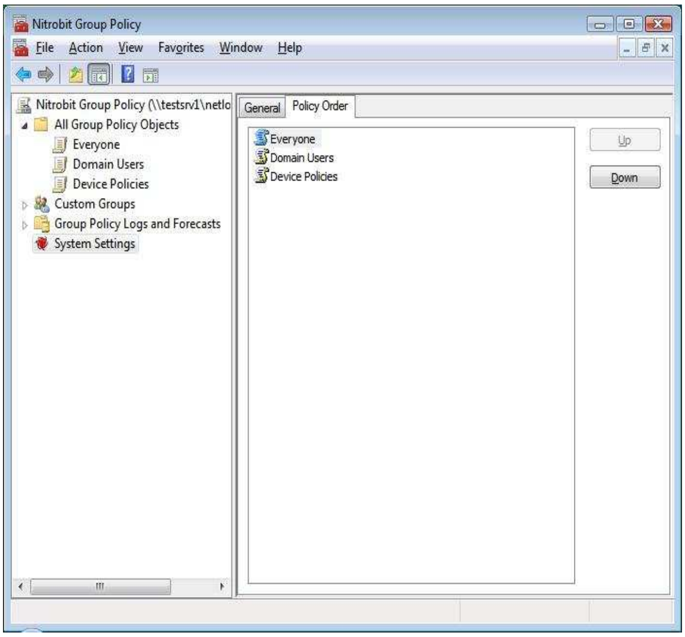
Add a Windows User or Group. You can directly add the name to add or use a selection dialog.

- Open the nitrobit group policy system editor.
  Read the chapter “Creating a Group Policy Hierarchy” for further information.
- Double-click the group policy object you want to modify.
- Switch to the Assigned Groups Tab.
- Use the add- and remove-buttons to modify the list of assigned groups.
- Change the Group Behavior as needed.

Changing the processing sequence of Group Policy Objects

The processing sequence for group policy objects is maintained in a global list. In order to change the processing sequence, you need to accomplish the following steps:

- Open the nitrobit group policy system editor. Read the chapter “Creating a Group Policy Hierarchy” for further information.
- Right-click the Nitrobit Policy object at the tree view to open its context menu.
- Select Properties.
- Select the tab Policy Order.
- Select a group policy object and use the up- and down-buttons to modify its position in the list.

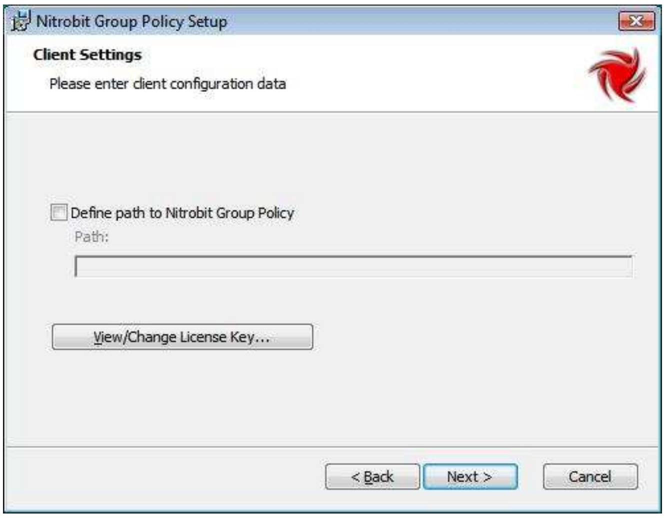


Client Setup

In order to apply policies, you need to install the client component on the client computer. You can install the nitrobit goup policy Client in different ways. If you plan to install a larger number of clients, you may consider the automated client rollout options described below.

Manual Installation

In order to install the client component manually, you can directly execute the nitrobit group policy installer file named NitrobitPolicy.msi. During the installation, you can supply the policy path and 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.



Nitrobit Group Policy Setup

Client Settings

Please enter client configuration data

□ Define path to Nitrobit Group Policy

Path:

Automated Client Rollout

The client installation can be automated. See the Reference Section for further details.

Automated Client Update with nitrobit group policy

You can use the nitrobit group policy Software Installation to update the nitrobit group policy client. This feature is supported for version 1.3.4 and higher. To update the client, create a group policy object with a machine software package. Assign the group policy to the respective machines. Note that the workstation will automatically reboot after the update.

Client Management

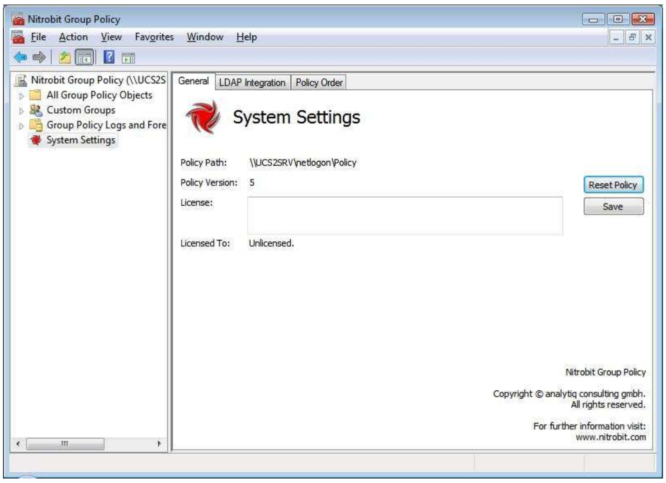
System Settings

On the “System Settings” tab, you can view the actual policy path and the version of your policy.

You can also reset the policy by clicking the button “Reset Policy”. Resetting the policy will force the re-application of the whole policy to all of your clients.

On this page you can also enter your license key. After entering your license key, click “Save” to store it in your policy.

If you store the license key in your policy, it will be preferred over a license key deployed during the setup or a license key that was deployed with the supplied administrative template.



System Settings

Policy Path: \\UCS2SRV\netlogon\Policy

Policy Version: 5

License:

Licensed To: Unlicensed.

Nitrobit Group Policy

Copyright © analytiq consulting gmbh.
All rights reserved.

For further information visit:
www.nitrobit.com

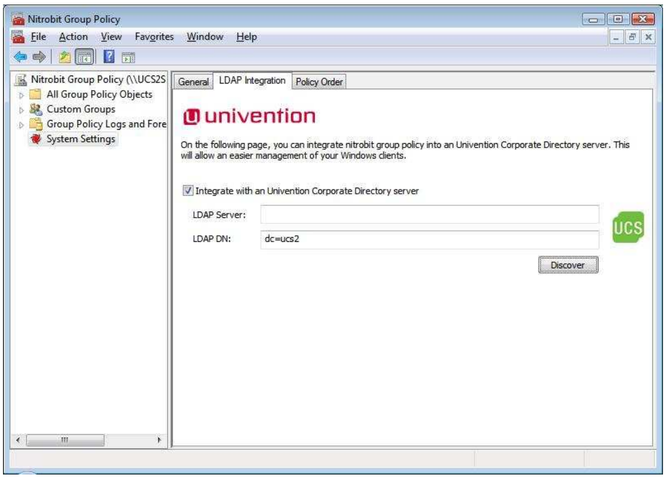
Integration into an Univention Corporate Server

nitrobit group policy can be integrated into an existing Univention Corporate Server installation. If the directory integration is enabled, the Univention Directory Manager can be used to control which computers will process nitrobit group policies.

To enable integration, click “Integrate with an Univention Corporate Directory server”. Then you can enter the address and disinguished name to your Univention Corporate Directory server.

If you leave the “LDAP Server” field blank, the logon server (%LOGONSERVER%) will be used.

By clicking the button “Discover”, nitrobit group policy tries to resolve the distinguished name by itself.



On the following page, you can integrate nitrobit group policy into an Univention Corporate Directory server. This will allow an easier management of your Windows clients.

☑ Integrate with an Univention Corporate Directory server

LDAP Server:

LDAP DN: dc=ucs2

Client Management through nitrobit group policy

The nitrobit group policy client can be managed by means of nitrobit group policy. Your setup sources should contain a Folder Administration containing a file named ngp.adm. Using this administrative template file, you can control the client's policy path, 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:

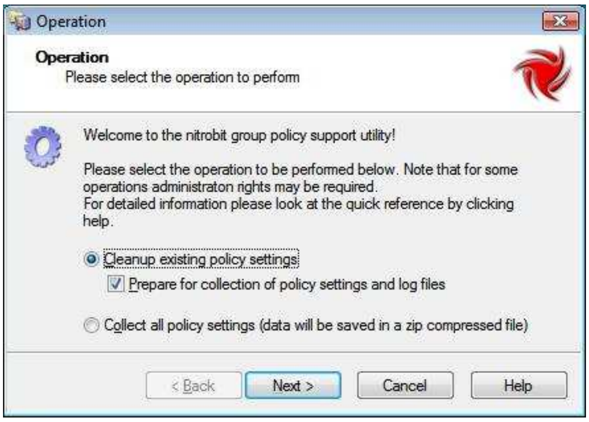
- Open the group policy object editor for the respective group policy object.
- Select the Computer Settings/Administrative Templates folder.

- Use the Add/Remove Templates command from the Action menu.
- Select the Add button and use the file select dialog to navigate to the ngp.adm file.

If you use this feature to change the license key or the policy path of your clients, special care is needed. Once you changed one of these parameters to an invalid value, you cannot reach your clients through nitrobit group policy any more!

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 group policy. It is located in the Support folder of your installation source and called Support.exe.



Operation

Please select the operation to perform

Welcome to the nitrobit group policy support utility!

Please select the operation to be performed below. Note that for some operations administraton rights may be required.
For detailed infomation please look at the quick reference by clicking help.

● Cleanup existing policy settings

☑ Prepare for collection of policy settings and log files

○ Collect all policy settings (data will be saved in a zip compressed file)

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.

Command Line Syntax

In order to run the Support Tool from a Script, you can use the following Command Line Options:

`/p` Pepare the workstation for collection of policy settings and log files.

`/c <file>` Collect all policy settings and write zip compressed to the file specified in <file>.

`/x` Optional. Can only be used in conjunction with `/c`. Do not export group policy files.

Eventlog Messages

In order to find any problems regarding the nitrobit group policy client, you should check the event log. The nitrobit group policy 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.

III. Reference

Policy Assignment

Group Types and Group Behavior

Nitrobit group policy uses groups to evaluate wether a group policy object needs to be applied to a target user or computer. Three different types of groups are available:

- Windows Groups
- IP-Groups
- RegEx-Groups

Additionally, groups can behave in three different ways:

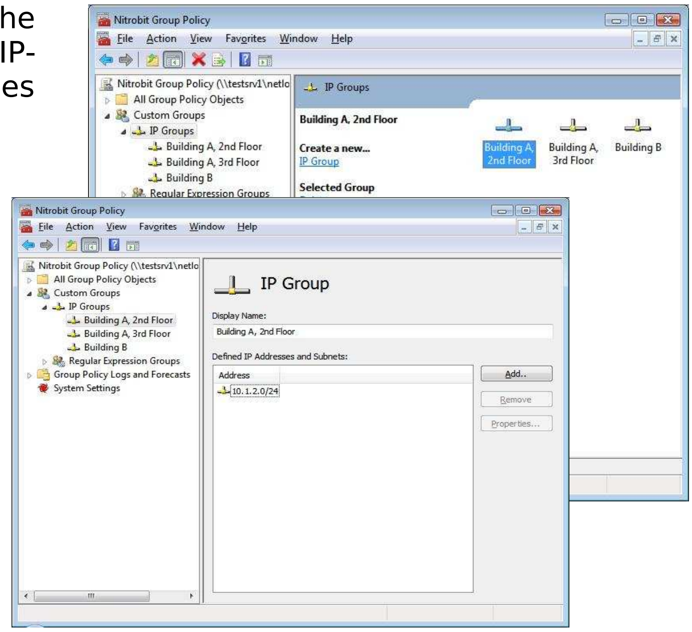
- Standard Group Behavior
- Deny Group Behavior
- Mandatory Group Behavior

Windows Groups

Nitrobit group policy can use groups provided by the Windows operating system. You can assign global domain groups, local groups as well as computer- or useraccounts to a group policy object.

IP-Groups

IP-Groups are maintained inside the nitrobit group policy system. Every IP-Group consists of a list of IP-Addresses and IP-Subnets.
If the IP-Address of a workstation matches one IP-Address or IP-Subnet of that list, the workstation is part of the respective IP-Group. A user is part of an IP-Group, if the workstation he is currently using is part of that IP-Group.
All network interfaces with an active connection are evaluated. For multihomed network interfaces, all IP-Addresses are checked. Additionally, for every workstation a loopback adapter with IP-Address 127.0.0.1 is assumed.



Display Name: Building A, 2nd Floor

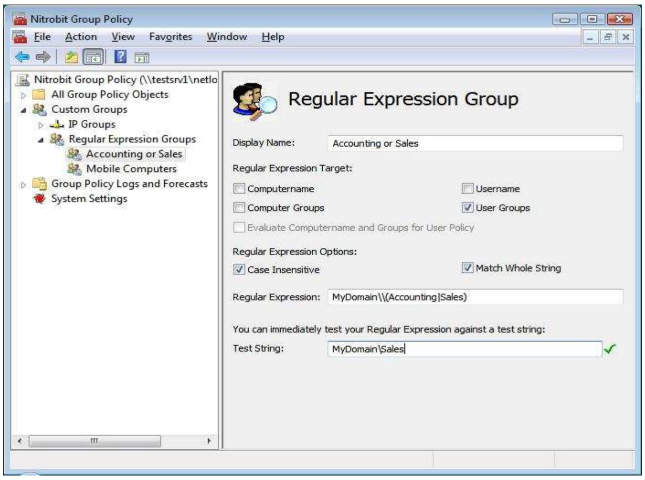
Defined IP Addresses and Subnets:

Address
10.1.2.0/24

RegEx-Groups

RegEx-Groups are maintained inside the nitrobit group policy system. They consist of a regular expression and different targets that will be tested for that regular expression. Possible targets are:

- Computer Name
  The NetBIOS name of the local computer, e.g. “MYCOMPUTER”
- Computer Group Names
  All domain global groups and local groups the workstation account is member of, e.g. “MYDOMAIN\Doman Computers”, “Authenticated Users”
- User Name
  The User's account name, e.g. “MYDOMAIN\JDoe”
- User Group Names
  All domain global groups and local groups the user account is member of, e.g. “MYDOMAIN\Accounting”, “INTERACTIVE”



Regular Expression Group

Display Name: Accounting or Sales

Regular Expression Target:

☐ Computername ☐ Username
☐ Computer Groups ☑ User Groups
☐ Evaluate Computername and Groups for User Policy

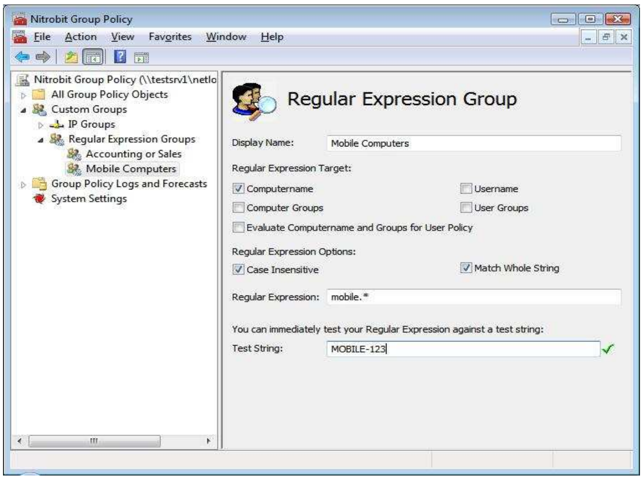
Regular Expression Options:

☑ Case Insensitive ☑ Match Whole String

Regular Expression: MyDomain\\(Accounting|Sales)

You can immediately test your Regular Expression against a test string:

Test String: MyDomain\Sales ✓



Regular Expression Group

Display Name: Mobile Computers

Regular Expression Target:

☑ Computername ☐ Username
☐ Computer Groups ☐ User Groups
☐ Evaluate Computername and Groups for User Policy

Regular Expression Options:

☑ Case Insensitive ☑ Match Whole String

Regular Expression: mobile.*

You can immediately test your Regular Expression against a test string:

Test String: MOBILE-123 ✓

A computer or user is part of a RegEx-Group, if one of the defined targets matches the regular expression. For computers policies, only the Computer Name and Computer Group Names can be checked as regular expression targets. For users policies, the User Name and User Group Names will be checked as regular expression targets. Additionally, Computer Name and Computer Groups Names can be used for user policies if the option “Evaluate Computername and Computer Groups for User Policy” is selected.

Standardized Regular Expression Targets

In order to deal with localized or renamed account names, nitrobit group policy uses the following rules when converting windows account information to strings:

- The Computer Name is always the NetBIOS-Name in uppercase.
- User Names and Group Names are prefixed with the Domain Name and a back-slash if they belong to a Domain.
- User Names and Group Names are never prefixed with the Computer Name, “NT AUTHORITY” or “BUILTIN”.
- Well-Known Accounts and Alias Groups are always converted to their English names, regardless of any Server- or Clientside locales or renamed Accounts.
  See the following list for Well-Known Accounts and Alias Groups.

DIALUP
NETWORK

BATCH
INTERACTIVE

SERVICE
ANONYMOUS LOGON
PROXY
ENTERPRISE DOMAIN CONTROLLERS
SELF
Authenticated Users
RESTRICTED
TERMINAL SERVER USER
REMOTE INTERACTIVE LOGON
This Organization
SYSTEM
LOCAL SERVICE
NETWORK SERVICE

Administrator
Guest

Domain Admins
Domain Users
Domain Guests
Domain Computers
Domain Controllers
Cert Publishers
Schema Admins
Enterprise Admins
Group Policy Creator Owners

Administrators
Users
Guests
Power Users
Account Operators
Server Operators
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators

Distributed COM Users
Cryptographic Operators

Evaluation sequence for Groups assigned to a Group Policy Object

The nitrobit group policy client uses the following sequence to determine if a group policy object needs to be applied to a user or computer:

1. All assigned Deny Groups are evaluated.
   If the user or computer is member of at least one Deny Group, the group policy object won't be applied.
2. All assigned Mandatory Group are evaluated.
   If the user or computer is not member of all Mandatory Groups, the group policy object won't be applied.
3. All assigned Standard Groups are evaluated.
   If the user or computer is member of at least one Standard Group, the group policy object will be applied.

Policy.ini Reference

[General]

Version

The Version Key defines the Version of the Policy.ini file. It should be incremented every time the file is modified.

Example:

```
Version=11
```

ResetCookie

The ResetCookie is a numerical Value. It is optional and can be used in addition to the Version Key.
By default, the Policy.ini is treated as outdated if its Version is lower than the Version cached on the client. This indicates a replication error, and the nitrobit group policy client stops applying policies.
If the Policy.ini file contains a ResetCookie value which differs from the one cached on the client, the Policy.ini is treated as newer, regardless of its Version value.
In Contrast to the Version value, the ResetCookie just needs to be different, not greater than the value on the client.

Example:

```
ResetCookie=112
```

[Policies]

The Policies section defines existing policies and their execution order. Each key is a GPO UUID, the value defines the execution order of the GPO.

Syntax:

```
<Policy-UUID>=<Order>
```

Example:

```
{6C76BB6C-7BEB-4E61-8AB7-77079BCDDE86}=0
{5B86BC60-F48B-416E-9173-78A1978823DD}=1
```

[IP-Groups]

This section defines IP-Groups that can be assigned to group policy objects. Each key is an IP-Group ID, the value is the IP-Group Definition.
The IP-Group Definition consists of an optional UTF-8 encoded Display Name and a list of IP-Addresses of IP-Subnet definitioins in CIDR notation.

Syntax:
```
<IP-Group ID>=[<Display Name>:]<IP-Subnet>[;<IP-
              Subnet>...]
```

Example:
```
2=My IP-Group:10.1.1.1;10.2.0.0/16
```

[RegEx-Groups]

This section defines RegEx-Groups that can be assigned to group policy objects. Each key is a RegEx-Group ID, the value is the RegEx-Group Definition.
The RegEx-Group Definition consists of an optional Display Name, a list of Flags and the Regular Expression. The string values are UTF-8 encoded.

Defined Flag Values:

- UN: Evaluate regular expression against the User Name
- UG: Evaluate regular expression against User Groups
- MN: Evaluate regular expression against the Computer Name
- MG: Evaluate regular expression against Computer Groups
- IC: Ignore Case
- WS: Evaluate whole strings

Syntax:
```
<RegEx-Group ID>=[<Display Name>]:[<Flag>[+
                 <Flag>...]:<Regular Expression>
```

Example:
```
{6C76BB6C-7BEB-4E61-8AB7-77079BCDDE86}=0
```

[SidAssignment]

[SidDeny]

[SidMandatory]

The SidAssignment, SidDeny and SidMandatory sections define which Windows Groups are assigned to a group policy object with the respective Standard-, Deny- or Mandatory-Behavior. Each key is a GPO UUID, the value is a semicolon separated list of Windows Security Identifiers (SIDs).

Syntax:
```
<Policy-UUID>=<SID>[;<SID>...]
```

Example:
```
{6C76BB6C-7BEB-4E61-8AB7-77079BCDDE86}=
        S-1-5-32-545
```

[IPAssignment]

[IPDeny]

[IPMandatory]

The IPAssignment, IPDeny and IPMandatory sections define which IP-Groups are assigned to a group policy object with the respective Standard-, Deny- or Mandatory-Behavior. Each key is a GPO UUID, the value is a semicolon separated list of IP-Group Ids.

Syntax:

```
<Policy-UUID>=<IP-Group ID>[;<IP-Group ID >...]
```

Example:

```
{6C76BB6C-7BEB-4E61-8AB7-77079BCDDE86}=1;3
```

[RegExAssignment]

[RegExDeny]

[RegExMandatory]

The RegExAssignment, RegExDeny, RegExMandatory sections define which RegEx-Groups are assigned to a group policy object with the respective Standard-, Deny- or Mandatory-Behavior. Each key is a GPO UUID, the value is a semicolon separated list of RegEx-Groups.

Syntax:

```
<Policy-UUID>=<RX-Group ID>[;<RX-Group ID >...]
```

Example:

```
{6C76BB6C-7BEB-4E61-8AB7-77079BCDDE86}=1;3
```

[Editor]

This section contains configuration parameters for the nitrobit group policy editor.

`NoIEAK`

Removes the Internet Explorer Administration Kit Extension from the nitrobit group policy editor.

Defined Values:

- 1: Remove IEAK Editor Extension
- 0: Enable IEAK Editor Extension (Default Value)

[Client]

This section contains configuration parameters for the nitrobit group policy client.

`NoIEAK`

Disables the execution of the Internet Explorer Administration Kit.

Defined Values:

- 1: Remove IEAK Client Extension
- 0: Enable IEAK Client Extension (Default Value)

[UCS]

This section contains configuration parameters to integrate nitrobit group policy into an existing Univention Corporate Server installation.

`LdapServer`

The address of the Univention Corporate Server LDAP directory. If not present, %LOGONSERVER% will be used.

`LdapDn`

The base DN that will be used. If not present, the Univention Corporate Server integration is disabled.

Client Registry Reference

The client component uses the following registry values stored at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Nitrobit\GPClient
```

`PolicyPath`	Path to the group policy hierarchy. You can use %DomainController%, it will be resolved to the next available domain controller when the client needs to access group policy data. Examples: c:\mytestpolicy; \\MyServer\Policy; \\%DomainController%\netlogon\Policy
`LogPath`	Path, where nitrobit group policy will save its logs automatically.
`LogLevel`	DWORD-Value defining the logging level for EventLog messages. Values: 0: default; 1: high.
`License`	Client License
`RetryMachinePolicy`	DWORD-Value, if set to 1, retry to apply the machine policy during user logon if it previously failed. Values: 0: default; 1: retry machine policy.

Automated Client Setup

Automated Client Rollout

The client installation can be automated. The properties `POLICYPATH` and `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\NitrobitPolicy.msi /qn
POLICYPATH=”\\MyServer\Myshare”
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 policy path and licensing information during an administrative installation. Use the following command line to start the administrative installation:

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

During the administrative installation, you can supply the policy path and licensing information. 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 group policy, use the following sample command line:

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

Your registry settings regarding policy path and license remain intact.

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

IV. 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