



nitrobit
update server

Administrator's Guide

Content

I. Introduction.....	4
Overview.....	4
Components of the nitrobit update server.....	4
System requirements.....	4
Server.....	4
Client.....	4
How updates are stored.....	4
II. Setup.....	5
Server Setup.....	5
Red Hat Enterprise Linux.....	5
SUSE Linux Enterprise Server.....	5
Debian.....	5
Ubuntu.....	5
Post installation steps.....	6
Red Hat Enterprise Linux.....	6
SUSE Linux Enterprise Server.....	6
Debian.....	6
Ubuntu.....	6
All distributions.....	6
Uninstall.....	7
Red Hat Enterprise Linux.....	7
SUSE Linux Enterprise Server.....	7
Debian.....	7
Ubuntu.....	7
Client Setup.....	8
Registry Settings.....	8
Basic Settings.....	8
Settings for automatic installation without user intervention.....	9
Group Policy Based Configuration.....	10
III. System Administration Guide.....	11
Administration Interface.....	11
Configuration.....	11
Synchronization Options.....	11
Languages.....	13
Schedule Synchronization.....	15
Security Settings.....	15
PAM Authentication.....	15
License.....	16
Setup wizard.....	16
Groups.....	16
Updates.....	17
Deploying updates.....	18
IV. Reference.....	19
nitrobit-support.....	19
Daemon command line parameters.....	19
Configuration file /etc/nus.conf.....	20
V. Legal Notice.....	21
Contact.....	21

Document Version: 1.00

I. Introduction

Overview

The nitrobit update server offers easy-to-use management of updates that are released through Microsoft Update. It offers a professional replacement for the Windows Update Server (WSUS) – and runs on Linux.

Components of the nitrobit update server

The nitrobit update server consists of three components:

- The synchronization daemon receives new updates from a parent server and stores the data.
- The server component supplies updates to all connecting clients – either windows update clients or down level update server.
- The web based user interface is used to administer the nitrobit update server.

System requirements

Server

The nitrobit update server supports the following Linux distributions: Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, CentOS 5, CentOS 6, SuSE Linux Enterprise 11, openSuSE 11.3, Debian 5, Ubuntu 10.4 and Ubuntu 10.10.

The nitrobit update server requires an apache web server to allow windows clients to synchronize with the update server.

To improve the performance, *mod_fcgid* or *mod_fastcgi* should be installed on the apache web server. The nitrobit update server automatically detects these modules and configures them accordingly.

The nitrobit update server also requires a database server. Currently, only MySQL 5.x is supported. The database server does not need to be located on the same computer. The connection will be established through MySQL client libraries.

Client

Microsoft Windows XP SP2 and later Microsoft operating systems are supported.

How updates are stored

The nitrobit update server stores its configuration settings and the update data into a database server. The update packages itself are stored in the file system.

II. Setup

Server Setup

Red Hat Enterprise Linux

Installing nitrobit update server on Red Hat Enterprise Linux can be easily done through *yum*:

```
yum install -nogpgcheck nitrobit-update-server-<version>.el5.<arch>.rpm
```

yum automatically resolves all dependencies required by the nitrobit update server.

SUSE Linux Enterprise Server

Installing nitrobit update server on SUSE Linux Enterprise Server can be easily done through *zypper*:

```
zypper install nitrobit-update-server-<version>.sles.<arch>.rpm
```

zypper automatically resolves all dependencies required by the nitrobit update server.

Debian

Installing nitrobit update server on Debian can be easily done through *dpkg*:

```
sudo dpkg -i nitrobit-update-server-<version>.<arch>.deb
```

To resolve the missing dependencies, use *apt-get*:

```
sudo apt-get install -f
```

Ubuntu

Installing nitrobit update server on Ubuntu can be easily done through *dpkg*:

```
sudo dpkg -i nitrobit-update-server-<version>.<arch>.deb
```

To resolve the missing dependencies, use *apt-get*:

```
sudo apt-get install -f
```

Post installation steps

Red Hat Enterprise Linux

Please restart your apache web server. This can be done with the following command:

```
service httpd restart
```

SUSE Linux Enterprise Server

1. Enable `mod_rewrite` in your apache server. This can be done by adding "rewrite" to `APACHE_MODULES` in the file `/etc/sysconfig/apache2`.
2. Run `SuSEconfig`
3. Change your default server options in the file `/etc/apache2/default-server.conf`. Replace `Options None` with `Options FollowSymLinks` for the directory definition of `/srv/www/htdocs`.
4. Restart your apache web server. This can be done with the following command:

```
service apache2 restart
```

Debian

Enable `mod_rewrite` and the nitrobit update server website:

```
sudo /usr/sbin/a2enmod rewrite
sudo /usr/sbin/a2enmod nitrobit-update-server
```

Restart the apache web server:

```
sudo /etc/init.d/apache2 restart
```

Ubuntu

Enable `mod_rewrite` and the nitrobit update server website:

```
sudo /usr/sbin/a2enmod rewrite
sudo /usr/sbin/a2enmod nitrobit-update-server
```

Restart the apache web server:

```
sudo /etc/init.d/apache2 restart
```

All distributions

1. Visit `http(s)://server-name/nitrobit-update-server` in your web browser to begin the configuration of the nitrobit update server.
2. Run an initial update synchronization: `/usr/sbin/nusd -sync`
3. Synchronize the automatic update (AU) binaries with `/usr/sbin/nusd -au`

Uninstall

Red Hat Enterprise Linux

Removing nitrobit update server is done through the *rpm* command:

```
sudo rpm -e nitrobit-update-server-<version>.el5.<arch>
```

SUSE Linux Enterprise Server

Removing nitrobit update server is done through the *rpm* command:

```
sudo rpm -e nitrobit-update-server-<version>.sles.<arch>
```

Debian

Removing nitrobit update server is done through the *apt-get* command:

```
sudo apt-get remove nitrobit-update-server
```

If you want to also remove all configuration files, please use the following command:

```
sudo apt-get purge nitrobit-update-server
```

Ubuntu

Removing nitrobit update server is done through the *apt-get* command:

```
sudo apt-get remove nitrobit-update-server
```

If you want to also remove all configuration files, please use the following command:

```
sudo apt-get purge nitrobit-update-server
```

Client Setup

This section describes how to configure the Windows Auto Update Client to communicate with a nitrobit update server.

Registry Settings

The Windows Auto Update Client can be configured through a set of registry values located under:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate and the *AU* subkey.

Basic Settings

- **Server URL:** Configure the AU Client to contact your nitrobit update server for updates.
- **Trusted Publishers:** Allow AU Clients to install updates signed by other publishers than Microsoft. Use this option if you want to deploy updates from the nitrobit update channel.
- **Group Targeting:** If you want to use Client Site Targeting, enable this option and specify the group name on your client. Alternatively, you can use Server Site Targeting to modify group membership on the server. Note that you need to configure this option on the server as well.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]

; server-url: use either "http://WSUS-Server-DNS-Name:Port" or an IP-Address based URL.
"WUServer"="server-url"
"WUStatusServer"="http://WSUS-Server-Name oder IP-Adresse:Port"

; Enable this option for nitrobit update channel.
"AcceptTrustedPublisherCerts"=dword:00000001

; Enable this options for Client Site Group Targeting. Needs to be enabled on the server, too.
"TargetGroupEnabled"=dword:00000001
"TargetGroup"="MyGroup;MySecondGroup"

; Use this option for Server Site Group Targeting.
"TargetGroupEnabled"=dword:00000000
```

Settings for automatic installation without user intervention

You can configure the Windows Auto Update Client to install all updates without any user intervention. This option is useful to ensure that users will have all updates installed.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"ElevateNonAdmins"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"NoAUShutdownOption"=dword:00000001
"NoAUAsDefaultShutdownOption"=dword:00000001
"AUPowerManagement"=dword:00000001
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"UseWUServer"=dword:00000001
"DetectionFrequencyEnabled"=dword:00000001
"DetectionFrequency"=dword:00000004
"IncludeRecommendedUpdates"=dword:00000000
"AutoInstallMinorUpdates"=dword:00000001
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
"RebootRelaunchTimeoutEnabled"=dword:00000001
"RebootRelaunchTimeout"=dword:000005a0
"RebootWarningTimeoutEnabled"=dword:00000001
"RebootWarningTimeout"=dword:0000001e
"RescheduleWaitTimeEnabled"=dword:00000001
"RescheduleWaitTime"=dword:0000001e
"EnableFeatureSoftware"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate]
"DisableWindowsUpdateAccess"=dword:00000001
```

Group Policy Based Configuration

You can use Group Policies to configure the Windows Auto Update Client. Configuration options can be found at: Computer Configuration → Administrative Templates → Windows Components → Windows Updates.

Configure the following option to receive updates from your nitrobit update server:

The screenshot shows the 'Specify intranet Microsoft update service location' Group Policy configuration window. The 'Enabled' radio button is selected. The 'Supported on' dropdown is set to 'At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1'. The 'Options' section contains two text boxes, both containing the URL 'http://nitrobit-update-server.analytiq.loc'. The 'Help' section provides detailed instructions on how to use this setting, including the requirement to set two servername values for detection and statistics, and the benefit of enabling this setting to bypass firewalls.

Specify intranet Microsoft update service location

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

(example: http://IntranetUpd01)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying

OK Cancel Apply

If you want to deploy updates from the nitrobit update channel, you also need to enable the option: "Allow signed updates from an intranet Microsoft update service location".

III. System Administration Guide

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

Administration Interface

The nitrobit update server is configured through its web based configuration interface. You can reach the configuration interface by pointing your web browser to `http(s)://server-name/nitrobit-update-server/`.

Since the user's credentials are sent unencrypted during login, we strongly recommend, to only use the administration interface through an SSL-encrypted connection.

Configuration

Synchronization Options

This section describes the synchronization options in detail. You can control which types of updates in which language for which products should be synchronized. You can also select the synchronization source, how to configure group memberships and whether to store updates on the local server or not.

Further you can create automatic approval rules, that are automatically applied to new updates.

General

On this page, you can configure the server that is used for synchronizing updates. You can also select the group configuration mode and whether to store updates locally.

The screenshot shows a web-based configuration interface for the Nitrobit Update Server. It is divided into several sections:

- Update Source:** Contains two radio buttons: "Use Windows Update" (selected) and "Use a custom server:" (with an empty text input field). There is also a checkbox "Enable the nitrobit update channel".
- Configuration:** Contains two radio buttons: "Replicate from Master server" and "Manage own configuration on server" (selected). Below this is a sub-section "Group Memberships" with two radio buttons: "Server-Side Group Membership" and "Client-Side Group Membership" (selected).
- Store Updates:** Starts with a checked checkbox. Below it is a text input field for "Repository Path" containing "/var/lib/nus" and a checkbox "Also store PSF-Files".
- Debug:** Contains a "Log Level:" dropdown menu set to "Debug" and a "Log File:" text input field containing "/var/log/nusd.log".

A "Save" button is located at the bottom of the configuration area.

Update source

You can either synchronize your server with windows update or with a custom server. If you use windows update, you can optionally enable the nitrobit update channel.

The nitrobit update channel is an optional service which delivers updates for popular third-party software.

A custom server is either another nitrobit update server or a microsoft windows server update server (WSUS).

Configuration

If you use a custom server as synchronization source, you can either choose to also replicate the configuration from this server or you can manage your own configuration. If you manage your own configuration, you will need to manage client groups, watch for new updates and assign them to your client computers. If you synchronize the configuration from an up level server, all these tasks are delegated to the up level server administrator.

If you synchronize updates directly from windows update, you have to manage your own configuration in any case.

Group Memberships

If you manage your own configuration on this server, you can choose how to deal with computer groups. You can choose to create groups by yourself and assign computers to these groups.

Alternatively, update clients can report their group membership during synchronization. In this case groups will get automatically created if they don't already exist. Registry, group policies and other tools can be used to configure group membership on the clients.

Store Updates

If you want to store updates locally on the server, please select the option "Store updates". Caching updates on the server will dramatically reduce network bandwidth usage, since your client computers can download updates from your server instead of contacting windows update through the internet.

You can also configure a path where the updates are stored (default is `/var/lib/nus`). The default should be fine in most cases. Changing this value is only recommended to experts.

If you change the storage path, you need to accomplish the following administrative steps:

- Copy the contents of the old path to the new location.
- Change the following lines in the nitrobit update server configuration file for the apache web server:

```
Alias /SelfUpdate/ "<path>"  
Alias /selfupdate/ "<path>"  
Alias /Content/ "<path>"  
Alias /content/ "<path>"
```

The apache configuration file for the nitrobit update server can be found in the following location: `/etc/httpd/conf.d/nitrobit-update-server.conf` for Red Hat based linux distributions and `/etc/apache/conf.d/nitrobit-update-server.conf` for Debian based linux distributions.

Finally, you can decide if you want to store updates in patch storage format (PSF). PSF-files only contain incrementally changes from one version of a file to another. Therefore, updates in patch storage format are very large. We don't recommend to use this option.

Languages

On this page, you can select the languages for which the updates will be synchronized. You can either choose to synchronize updates in all languages or you can select one or more specific language.

The screenshot shows the 'Synchronization Options' page in the Nitrobit Update Server. The 'Languages' tab is active. Below the 'Language Settings' heading, there are two radio buttons: 'Synchronize all languages' (selected) and 'Synchronize only the selected languages'. Below this is a table with the following data:

#	Synchron...	Name	Code	LCID
1	<input checked="" type="checkbox"/>	all	all	0
2	<input type="checkbox"/>	Arabic	ar	1025
3	<input type="checkbox"/>	Bulgarian	bg	1026
4	<input type="checkbox"/>	Chinese (Traditional)	zh-tw	1028
5	<input type="checkbox"/>	Czech	cs	1029
6	<input type="checkbox"/>	Danish	da	1030
7	<input type="checkbox"/>	German	de	1031
8	<input type="checkbox"/>	Greek	el	1032
9	<input checked="" type="checkbox"/>	English	en	1033

Please note that the “neutral” language is always selected and cannot be unselected.

Products

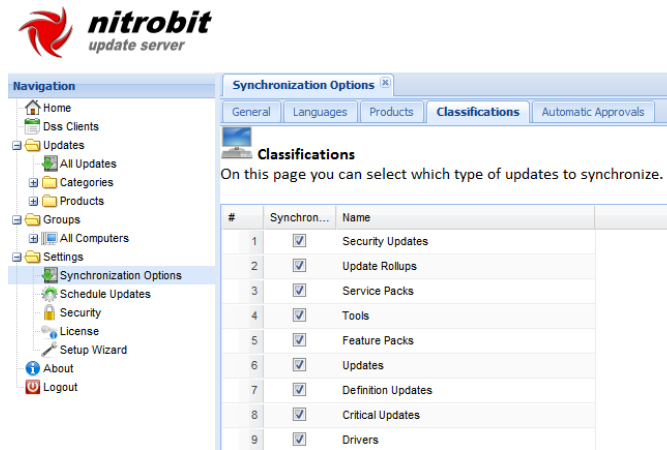
On this page, you can select for which product to synchronize updates. To enable synchronization for a product, check the box beside the product's name. If you want to enable synchronization for a complete product family, check the box beside the product family. The nitrobit update will automatically select all products in that product family.

The screenshot shows the 'Synchronization Options' page in the Nitrobit Update Server. The 'Products' tab is active. Below the 'Products' heading, there is a list of products with checkboxes for selection. The 'Windows' product family is selected, and its sub-items are also visible:

- Windows
 - EU Browser Choice Update-For Europe Only
 - Windows 2000
 - Windows 7
 - Windows Defender
 - Windows Embedded Standard 7
 - Windows Internet Explorer 7 Dynamic Installer
 - Windows Internet Explorer 8 Dynamic Installer
 - Windows Media Dynamic Installer
 - Windows Server 2003
 - Windows Server 2003, Datacenter Edition
 - Windows Server 2008
 - Windows Server 2008 R2

Classifications

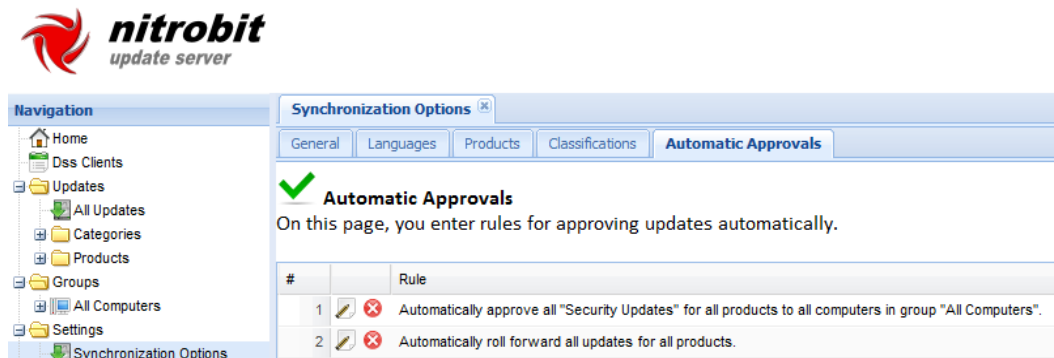
On this page, you can select the type of updates to synchronize. Updates have different classifications like “Security Updates”, “Service Packs”, “Feature Packs” and “Drivers”. If you for example do not intend to deploy drivers, you can filter updates classified as driver.



Automatic Approvals

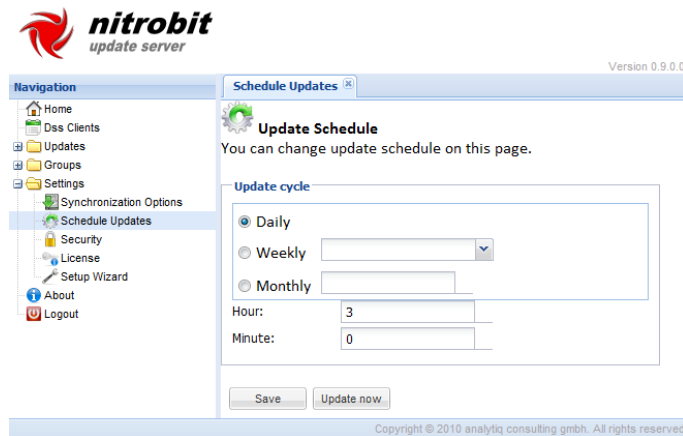
On this page, you can enter rules, that are automatically applied to updates. The nitrobit update server sets up the two rules shown below as a default.

New rules can be added, by clicking the “Add” button. Existing rules can be edited or deleted.



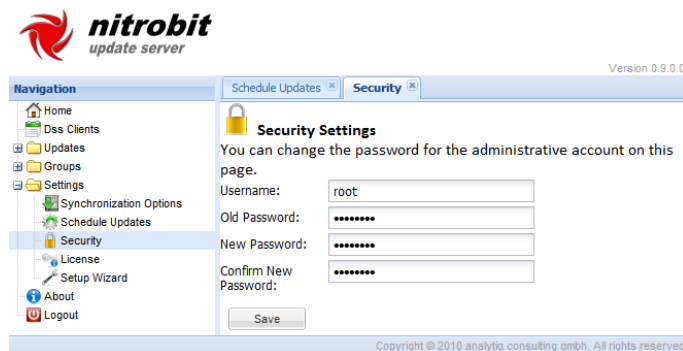
Schedule Synchronization

On this page, you can schedule the time when updates should be synchronized. Additionally, you can manually start a synchronization.



Security Settings

On this page, you can configure an administrative account. The account which is configured on this page will always have access to the administration interface.

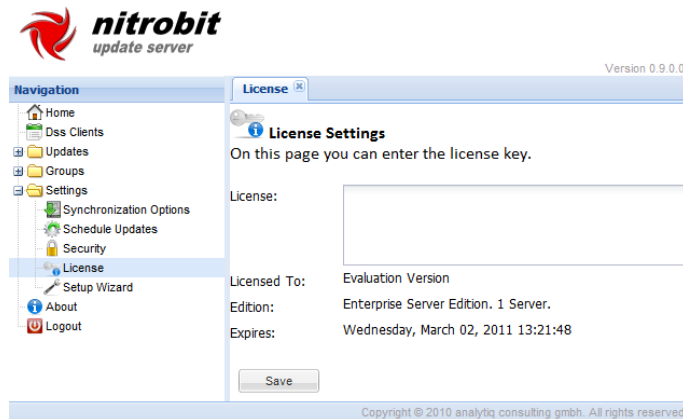


PAM Authentication

Additionally to the configured administrative account, nitrobit update server can use pluggable authentication modules (PAM) for authentication. By default, PAM authentication is denied for all users. To grant access to some PAM authenticated users, you need to modify the PAM configuration file. The configuration file for the nitrobit update server PAM service can be found under `/etc/pam.d/nitrobit-update-server`.

License

On this page, you can enter a license key.



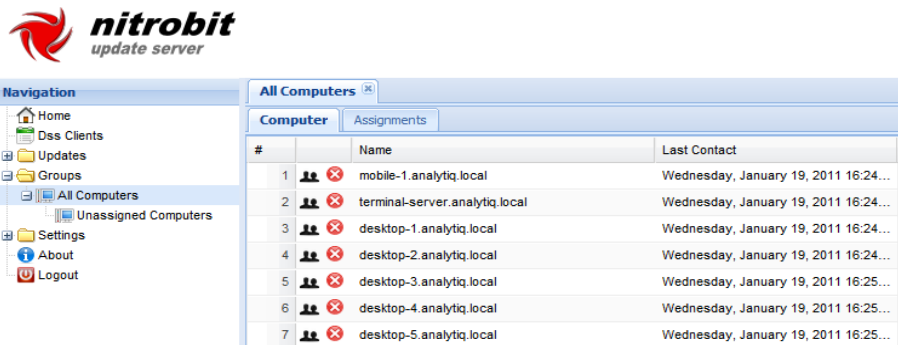
Setup wizard

The setup wizard can be used to easily re-install the nitrobit update server. Please be careful: Re-running the setup wizard will create a new database. If you use the same database name as before, the database will be overwritten.

Groups

The groups entry in the navigation menu gives you access to the computer groups management.

You can use the group management to create or modify computer groups and to manage group membership.



Computer groups form a hierarchy starting at the “All Computers” group.

New groups can be created by right clicking an existing group and selecting “Add group” in the context menu.

The two groups “All computers” and “Unassigned computers” are special system groups. They cannot be changed or deleted and you cannot modify their members. Client computers are always member of the “All computers” group. If a client computer is not a member in any other group than “All computers”, it is also a member of the “Unassigned computers” group.

You can change a computer's group membership by clicking the following icon: 

You can remove a computer from a group by clicking the following icon: 

Updates

The navigation menu offers different views to updates. Additionally to viewing all updates, you can browse into the product tree or the category list for specific updates.

Approval	Name	Category	Last Changed
?	Windows Malicious Software Removal Tool - January 2011 (KB890830)	Software	Wednesday, January 19, 2011 14:07...
?	AuthenTec Inc. driver update for AuthenTec Inc. AES2550	Driver	Wednesday, January 19, 2011 14:07...
?	Conexant - Audio - Conexant HD-Audio SmartAMC HD2	Driver	Wednesday, January 19, 2011 14:06...
?	Conexant - Audio - Conexant HD-Audio SmartAMC HD2	Driver	Wednesday, January 19, 2011 14:06...
✓	Cumulative Security Update for ActiveX Killbits for Windows 7 (KB978262)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for ActiveX Killbits for Windows 7 (KB980195)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for ActiveX Killbits for Windows 7 for x64-based Systems (...)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for ActiveX Killbits for Windows 7 for x64-based Systems (...)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB2183461)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB2360131)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB2416400)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB976325)	Software	Wednesday, January 19, 2011 14:07...
✓	Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB978207)	Software	Wednesday, January 19, 2011 14:07...

You can further filter your view by category, product or approval state. Additionally, you can batch-approve all currently displayed updates to a group.

Filter

Select items to display

Select a category... ▾

Select a product... ▾

Select an approval state.. ▾

Change approval

Select group... ▾

Select new approval state ▾

Apply

If you select an update, additional information is displayed in the details section:

Details | Assignments

Cumulative Security Update for ActiveX Killbits for Windows 7 (KB980195)

Security issues have been identified in ActiveX controls that could allow an attacker to compromise a system running Microsoft Internet Explorer and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this item, you may have to restart your computer.

GUID: 78b3c9bc-0cf1-4052-889e-7725e09200cb, Revision: 106

The “Assignments” tab shows all groups to which this update is currently assigned:

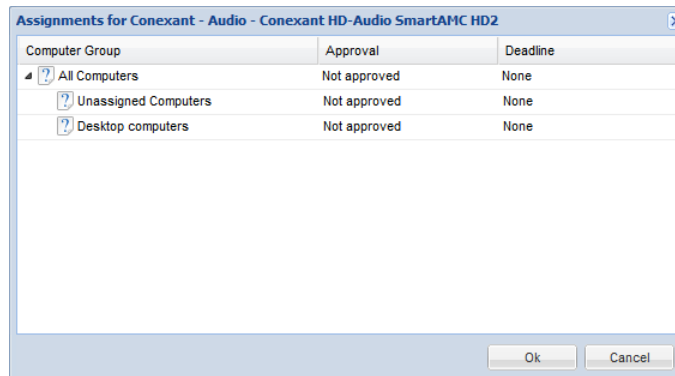
Details | **Assignments**

Approval	Group
✓	All Computers
?	Unassigned Computers
?	Desktop computers

Deploying updates

Right-clicking on the icon in the column “Approval” will show a context menu with two entries: “Change assignment” and “Decline”.

By selecting “Change assignment” you can assign the update to the one or more groups. Declining an update will delete all assignments for this update and will prevent it from being installed on any client computer.



In this dialog, you can select to which group this update should be deployed by right clicking the group and selecting the desired action from the context menu.

IV. Reference

nitrobit-support

The nitrobit support shell script is a small utility intended to help our customer support in case of an error. This shell script automatically collects all information which the nitrobit support team needs to analyze an error.

The nitrobit support tool collects the update server's log file, a complete database dump, a crash dump (if any exists) and some basic system information (kernel version, product version).

The script can be found under `/usr/sbin/nitrobit-support`. It must be run as system administrator and has the following command line parameters:

Parameter	Description
<code>-f</code>	Use an alternate config file (default <code>/etc/nus.conf</code>)
<code>-o</code>	Specify the output file (default <code>./nitrobit-support.tar.gz</code>)

Daemon command line parameters

The daemon binary is installed in `/usr/sbin`.

Parameter	Description
<code>-version</code>	Shows version information.
<code>-sync [-config]</code>	Starts a manual synchronization with the parent server. If <code>-config</code> is also specified, synchronizes only the configuration information.
<code>-syncfiles</code>	Starts file synchronization.
<code>-au</code>	Synchronizes the automatic update (AU) binaries.
<code>-report</code>	Reports all data to the parent server (only to a custom parent server, neither windows update nor the nitrobit update channel).

For example, to manually sync updates, please type the following command on the shell:

```
/usr/sbin/nusd -sync
```

Configuration file /etc/nus.conf

The configuration file stores all parameters which are required by the daemon and administration interface to connect to the database. This file has the format of an INI-file.

Section	Value	Description
Database	DBType	Type of the database
	DBServer	Remote address of the database server
	DBUser	Username which is used to connect to the database
	DBPassword	Password for DBUser
	DBName	Database name

V. Legal Notice

analytiq, the analytiq-Logo, nitrobit and the nitrobit-Logo are registered trademarks. Red Hat is a registered trademark of Red Hat, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. Unix is a registered trademark of The Open Group. Debian is a registered trademark of Software in the Public Interest, Inc. Ubuntu is a registered trademark of Canonical Ltd. SUSE and openSUSE are registered trademarks of Novell, Inc. Other product or service names mentioned herein are the trademarks of their respective owners.

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