uNAS – tNAS

User Manual

Ver 1.0

DATOptic Inc

www.datoptic.com

Disclaimer

DATOptic Inc assumes no responsibility for errors or omissions in this document, and DATOptic Inc does not make any commitment to update the information contained herein.

1 Before you get started

Congratulations on purchasing uNAS/tNAS, the ideal solution for network-based storage management. This manual will assist you as you install and configure the hardware. In order to quickly reach the desired configuration, please read the following pages thoroughly. The time invested is well spent - after all, you have purchased this solution for your invaluable data.

1.1 Content of this package

Before you begin installing uNAS/tNAS, make sure that the package contains the following items:

- uNAS/tNAS module,
- User Guide – this document,
- LAN cables,
- Source CD.
  If something is missing, please contact your dealers/resellers

1.2 Supported clients

- Microsoft Windows (all versions)
- Linux, Unix, Mac OS 8.0, 9.0 and OS X

1.3 Supported network protocols

- TCP/IP, NetBEUI, SNMP

1.4 Supported network file protocols

- SMB / CIFS / Samba, Apple Talk, FTP/sFTP

1.5 Safety precautions

1.5.2 Personal safety

High voltages may occur inside computer equipment. Before removing the enclosure, please turn off the power switch and disconnect the power cords.

1.5.2 Safety for your data

If you are not using new hard drives for operating uNAS/tNAS, please backup all important data prior to installation. Adding a hard drive to uNAS/tNAS goes hand in hand with complete formatting of the hard drive, which can possibly delete existing data.

1.5.3 ESD precautions

In order to avoid damage to uNAS/tNAS, please ensure you are grounded before opening the system or the ESD package that contains uNAS/tNAS. Using grounding straps or mats is the best way to ensure this safety. If you don't have grounding equipment handy, please make sure you are grounded before working with uNAS/tNAS, for instance, by touching a heater.

- Avoid unnecessary touching of the components inside the PC,
- Please touch uNAS/tNAS only on the edges.

2 Features

2.1 What is NAS?

NAS (Network Attached Storage) solutions are defined as storage systems that are directly hooked up to a network infrastructure. Also, they operate independently and do not have to be connected to a server via a controller or host adapter. The term "storage" here generally refers to all systems that either provide data storage or actually store or organize data. Currently, data storage is the most common and most widespread type of NAS systems.

NAS solutions are based on a separate operating system (and often also on special hardware), which operates independently from the servers on a network. Typically, this operating system is software that is optimized for providing data (file server). NAS solutions allow users to add additional storage to existing networks quickly, easily, and cost-efficiently.

2.2 Description of the functions

To begin working with uNAS/tNAS, all you need to do is assign an IP address to the NAS server – either automatically through an existing DHCP server or by assigning it manually. All other settings are handled via a web front-end which can be easily accessed through the IP address of uNAS/tNAS using the encrypted https protocol.
uNAS/tNAS allows users to create so-called shares (i.e., resources within a network that numerous users or user groups have certain access too). The access rights to the shares are controlled through the user and user group settings.

Within a few minutes, you will have up to several hundred gigabytes available on your network – without much effort and any downtime.

2.3 RAID types

This manual is not intended to explain the raid function in detail. But we want to provide you with an overview of common RAID types so that you can make an informed decision on which type to choose. Depending on whom you ask, RAID means either Redundant Array of Independent Disks or Redundant Array of Inexpensive Disks. Both are correct. In essence, you combine the capacity, speed and security of several disks into one.

RAID 0 forms one large hard disk by concatenating stripes from each member drive.

Stripe size is configurable roughly between 64 KB and 1 MB. The result is a lightning fast RAID, but with no added security. One failing drive may ruin the entire RAID.

RAID 1 mirrors hard drives. By writing identical data onto more than one drive, security is enhanced. A completely defective drive does not cause any loss of data. The drawback is reduced performance and capacity.

RAID 5 combines data striping from RAID 0 with parity checking, therefore combining speed and improved security. The loss of one drive is tolerable.

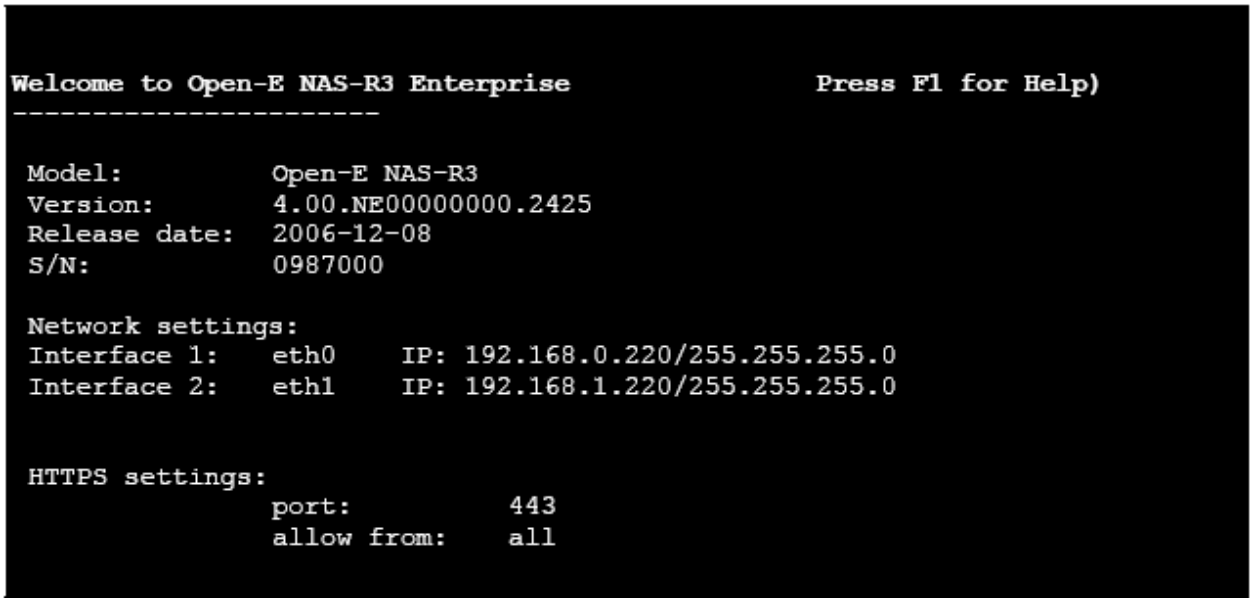
RAID 6 extends RAID 5 by adding an additional parity block, thus it uses block-level striping with two parity blocks distributed across all member disks. It was not one of the original RAID levels. The user capacity of a RAID 6 array is N-2, where N is the total number of drives in the array. RAID 6 does not have a performance penalty for read operations, but it does have a performance penalty on write operations due to the overhead associated with the additional parity calculations.

RAID 10 is a combination of RAID 1 and 0, hence the name. Data is written in a striped and mirrored configuration, providing high performance and robust security.

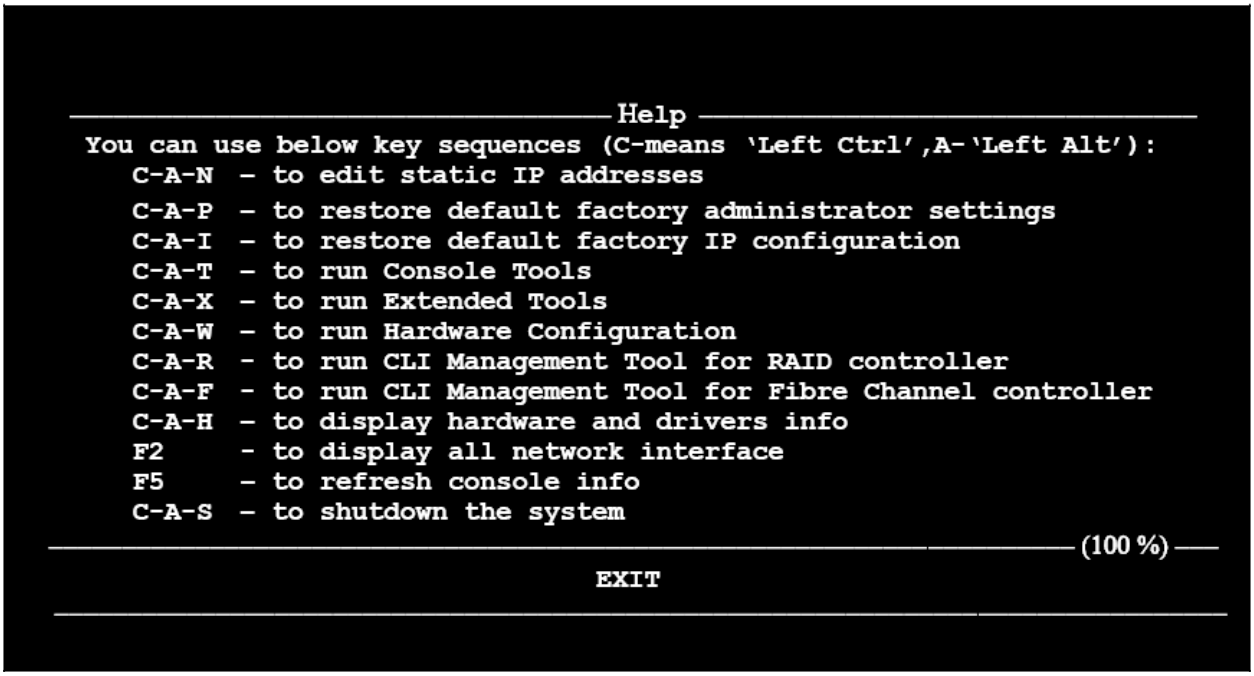
3 Hardware Installations

3.1 Installing uNAS/tNAS

Remove the unit out of shipping material
Plug in AC cord, uNAS/tNAS AC input is 90-250VAC so there is no worry for the AC input is incorrect
Connect Ethernet cable to uNAS/tNAS and your network
Connect the keyboard and monitor (they will be needed for setup only). Later you can run the server in the "headless mode" (without keyboard and monitor).
Power the system
After boot-up complete, if the network has a DHCP server, uNAS/tNAS should gain access to the IP settings automatically.



If that is the case, you can proceed at 4.3. If your network does not have a DHCP server, uNAS/tNAS will start with the default settings: IP address 192.168.0.220 and subnet mask 255.255.255.0.
You can change these values again by typing in the following key combination: left CTRL, left ALT and N. You can select a different IP address now. All other available functions on of the console will appear after pressing F1 key (see below).



After a connection has been established, all settings can also be changed remotely via the web browser. If your network requires it, the address of the standard gateway and the broadcast address can be changed.

For additional information, please read the chapter “Functions of the console display.”

4.3 Logging into uNAS/tNAS

You can establish a connection to uNAS/tNAS from every network computer. To establish this connection, use a browser (e.g. Microsoft Internet Explorer) and enter the IP address or the name of the computer hosting the NAS-R3 R server into the URL entry line: https://192.168.0.220 (standard address) or https://nas (this name can be changed in the installation of uNAS/tNAS).

For security reasons, uNAS/tNAS uses the encrypted SSL protocol (https).

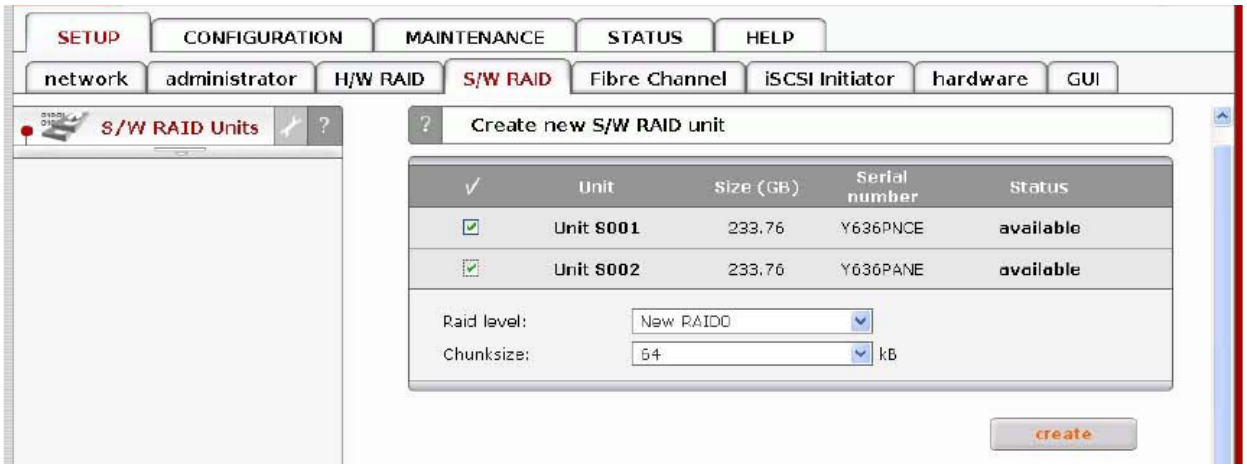
You will now be asked for verification of the encryption certification. Since uNAS/tNAS does not allow for creating shares on the Internet but only on the Intranet, there is no need for global certification by an authorized body. You can accept the certificate for the session only, but also for all future use. Now you have to accept the license in order to use the Open-E software and you can choose the language you want to use. Page with the software agreement and available language option will be shown after first launching uNAS/tNAS. Later you can change the language you can change using Language Settings, which are located in “server” through “setup”.

You can log into uNAS/tNAS using the standard password “admin” (this can be changed later). In order to start working, you can now set all parameters.

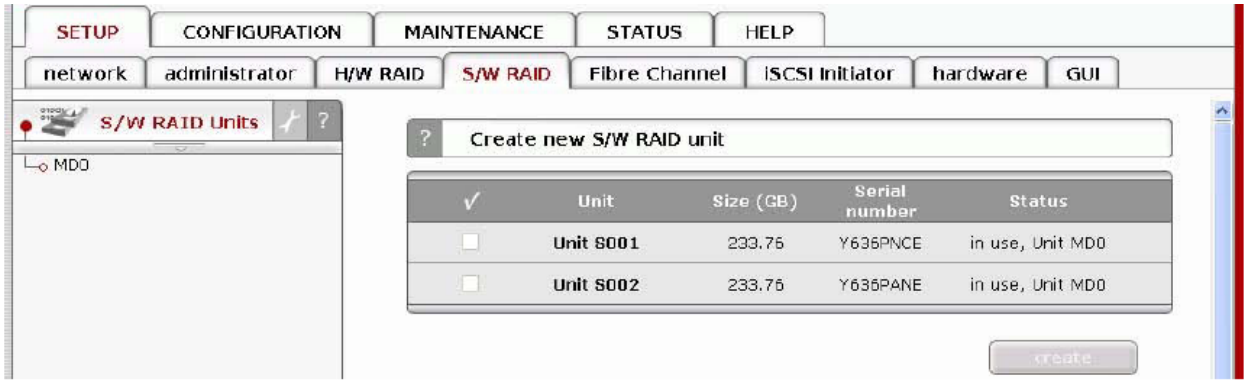
Password checking is case-sensitive. If you cannot log into uNAS/tNAS, please check the status of the Shift and Caps Lock keys. In case your web browser will show something different then expected, please delete the cache & cookies in settings menu of your web browser.

4.4 Create Disk Array

If system has Hardware RAID, please create RAID array in RAID controller setup. Please refer to the RAID controller manual. You do not have to install drivers or RAID array monitoring and maintenance software. If system has only "on motherboard BIOS RAID", please do not use it. Such on motherboard RAID are not supported. In case you want use software RAID with single drives or even with installed hardware RAIDs, please go to menu “SETUP” “SW/RAID” first. Here all available units are listed. A unit can be a single hard disk or a disk array (if using a hardware RAID controller). Software RAID can be created over a single hard disk or hardware disk arrays. To create a software RAID, please select units, choose the RAID level and click on “create” button.

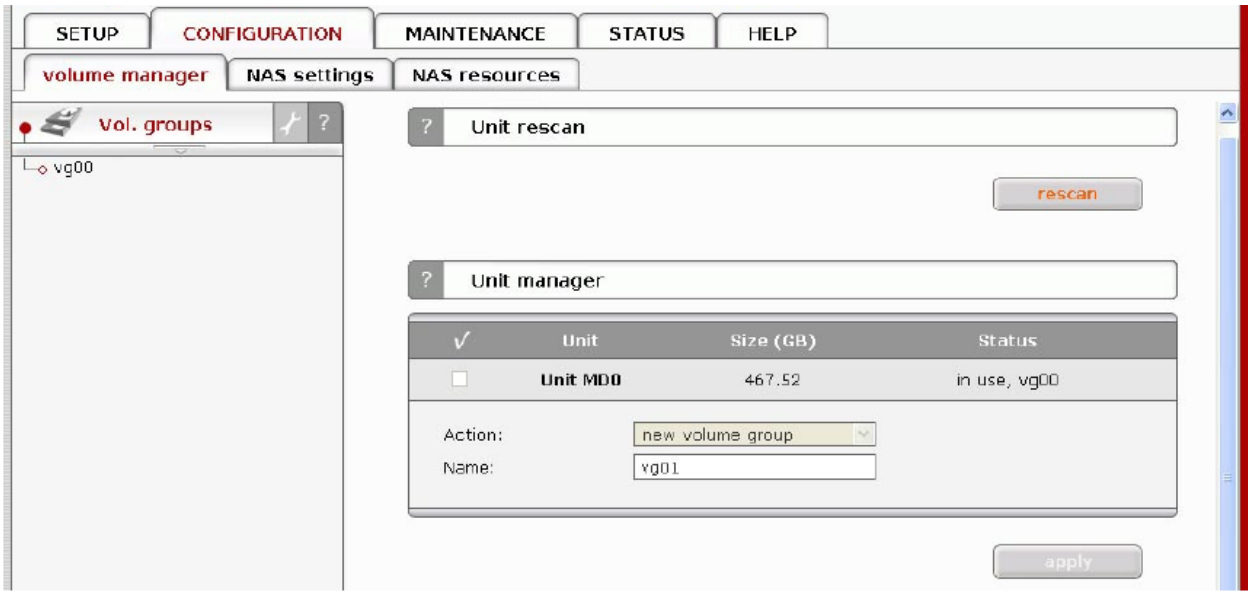


After clicking “create” button, the status will change to “in use” with additional information describing the kind of a disk array (e.g. MD0 is RAID 0)

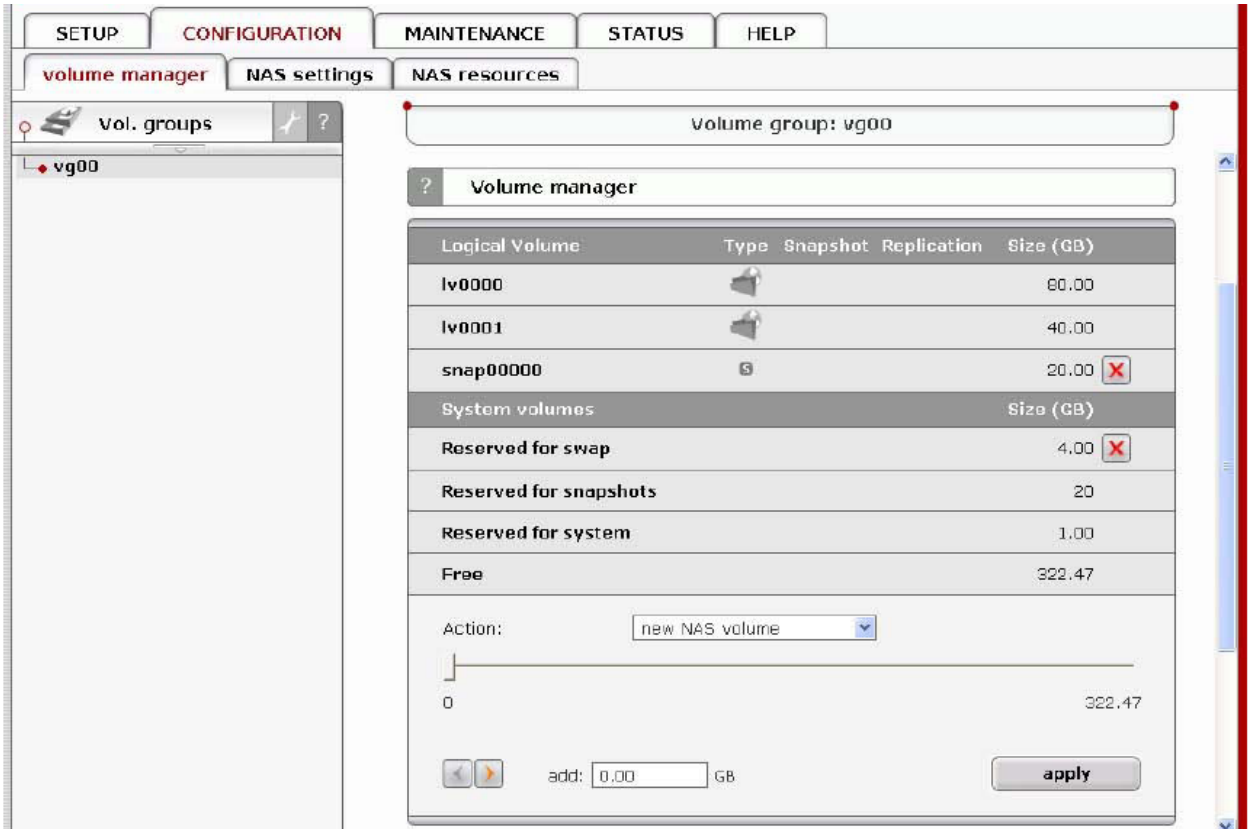


4.5 Adding Disk Array

- In the menu, please select the “CONFIGURATION” ”volume manager” and “Unit manager” function.
- You find a list of available drives/arrays (units) that can be used,
- While creating the “new volume group”, the system adds selected units only. You can use default volume group name or change it. After creating, the page is reloaded and the “Status” field should show your drives/arrays as "in use"



- You can possible to combine two (or more) units into one Volume Group. ext, by clicking on the right-hand side of the tree diagram on volume group name e.g. “vg00” and use function “Volume Manager” you can create new NAS volume.
- If you want to use snapshot feature you should create snapshot volume.



- Next, with use of function “Volume Manager” you can add disk volume to a new LV, or increase size of existing LV’s (you can’t decrease LV size). To set needed LV size just use scrollbar, next to which, on the right side is shown size available to use. This function can be also used to reserve disk space for swap, snapshots and system.

4.6 Creating uNAS/tNAS shares

In the menu, please select “CONFIGURATION” followed by “NAS settings.” Here, you select the type of authentication. In smaller networks, this should be done via the used workgroup name, which has to correspond with the workgroup name of the client PC.

In the menu “CONFIGURATION” “NAS Resources,” select “Shares” on the right hand side of the tree diagram. Now create the first share.

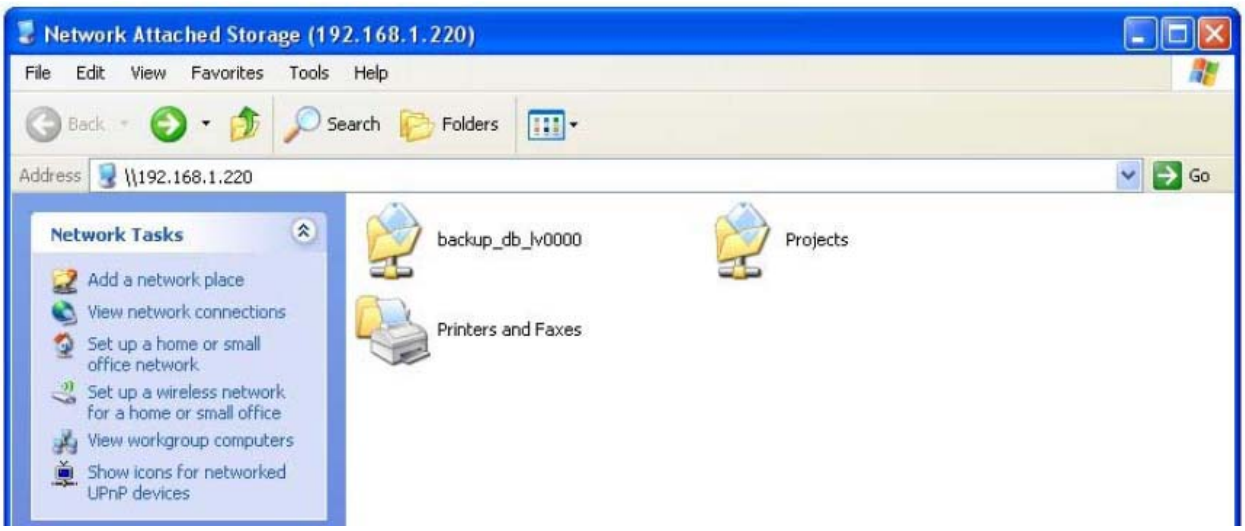
The workgroup/domain name that was configured in uNAS/tNAS has to match with the network settings. Otherwise, the configured shares are not visible in the network environment.

If you made changes to the workgroup and server name in uNAS/tNAS configuration, it can take some time until each workstation computer in the Windows network detects the new name.

4.6.1 Access to Windows Shares

The access to newly created shares is generated via the Windows Explorer. After entering the IP address of your uNAS/tNAS (in this example \\192.168.1.220), all visible shares should be available immediately. Please keep in mind that sometimes it takes a few minutes for the new shares or changes to become accessible.

When accessing invisible shares, you need to know beforehand the corresponding share name and attach it to the IP address with a backslash (\\):



uNAS/tNAS supports Windows ACL (Access Control List) for read, write and execute options, but based on the POSIX standard written by SGI.

Some examples how to use ACL (with ADS or PDC authentication):

1. Deny access to a Directory for every user (group):
   a. Create a new folder or select one of your existing folders (you must be the owner or super user to set ACL permissions)*
   b. Go to the “directory properties” (right mouse click on the directory then choose "Properties")
   c. Select a the “security” tab
   d. Choose the group "Everyone"
   e. Click the "Remove" button – only you and your group will have access to the selected directory **
   f. Click the "Apply" button

   Now only you have permissions to access this directory.

2. Allow full access for a group "WORK" to this Directory:
   a. Make sure that the group WORK is created
   b. In the security window click the "Add" button
   c. Click the "Remove" button (point 1)
   d. Select the group "WORK" (Advanced Find Now will show you all users and groups) and click OK
   e. Enable Full Control in the “Allow” column
   f. Click the "Apply" button

3. Set “read only” permissions to the file for everyone:
   a. Create a new file (you must be the owner or superuser to set permissions)*
   b. Go to the permissions window
   c. Select the “Everyone” group
   d. Leave only a ”read” permission in "Allow" column
   e. Click the "Apply" button
   f. Make the same for your group and yourself Now the group “Everyone” has "read only" permissions to this file.

4. Changing the directory owner:
   a. On Open-E web interface go to resources shares
   b. In the "Set Superuser" function select your user and restart connection (maintenance shutdown Function Connections reset) or wait about 15 minutes
   c. Go to the directory/file properties (right mouse click properties on the directory and click the "security" tab)
   d. Click the "Advanced" button
   e. Select the Owner tab
   f. Click the "Other Users or Group" button and select the user that will be a new owner (Advanced Find Now will show all users and groups), click OK***
   g. Select the user from the list and click OK and the "Apply" button
   h. Click OK and re-open this window to refresh owner.

5. Allow a full access for the user "BIG BOSS" to this Directory
   a. Make sure that the "BIG BOSS" exists
   b. In the security window click the "Add" button
   c. Select the user "BIG BOSS" (Advanced Find Now will show you all users and groups) and click OK

d. Enable Full Control in the Allow column
e. Click the "Apply" button

6. Allow “read” access for a group "COMPANY" to this directory
   a. Make sure that the group "COMPANY" exists
   b. In security window click the "Add" button
   c. Select the group "COMPANY" (Advanced Find Now will show you all users and groups) and click OK
   d. Enable "Read & Execute" in the Allow column
   e. Click the "Apply" button

7. Make “read only” directory with a full access subdirectories for the group “ALL” (using inheriting permissions)
   a. Create a folder "ROOT"
   b. Go to the security window
   c. Remove both “Everyone” and “Your” group
   d. Click the “Advanced” button and then the “Add” button
   e. Select the “ALL” group and click OK
   f. Change “Apply onto” to “This folder only”
   g. In permissions leave only “Traverse Folder / Execute File” and “List Folder / Read Data”. Click OK
   h. Click once again the “Add” button and add ALL group
   i. This time select “Apply onto” to “Subfolders and files only” (this step will submit any inherited permissions)
   j. Select “Full Control” and OK
   k. Click “Apply” to save permissions.

   With these settings users from the group “ALL” cannot remove the “ROOT” folder or make any changes to its contents. All new files/folders will be created based on the access given by inherited permissions.
   Example:
   - file /ROOT/some_file.txt can be changed but can not be removed
   - directory /ROOT/directory can not be removed but a users from the group ALL can create folders and files in this directory.
   - file /ROOT/directory/my_file.txt can by removed and changed by the group ALL (if inherited permissions wasn't changed)

8. Inherited permissions. If the file or directory has inherited permissions, all newly created subfolders will inherit the main folder permissions. All permissions can be changed. Please keep in mind that changing permissions in the main folder will trigger the same changes to the inherited permissions of any subfolder within.

9. UNIX Rights in Windows

Folders permissions

Permissions	- - x	r - -	- w -	r - x	r w -	- w x	r w x
Traverse Folder / Execute File	√			√		√	√
List Folder / Read Data		√		√	√		√
Read Attributes	√	√		√	√	√	√
Read Extended Attributes		√		√	√		√
Create Files / Write Data			√		√	√	√
Create Folders / Append Data			√		√	√	√
Write Attributes			√		√	√	√
Write Extended Attributes			√		√	√	√
Delete Subfolders and Files							√
Delete							√
Read Permissions	√	√	√	√	√	√	√
Change Permissions							√
Take Ownership							√

Example application of ACL permission in a small company.

The company has 10 users

Name	Group	Position	Rights
Chris	Firma	Director	All rights for everything
Robert	Firma	Manager	All rights for everything besides Directors home directory
Jennifer	Firma	Secretary	Read access to "DOCUMENTS" directory
Clint	Firma Developers	Main Developer	Read and write to “DEVELOPERS” directory read and write to “CHANGES” directory
Brad	Firma Developers	Developer	Read in „DEVELOPERS“ Read and write in „Changes“
Johnny	Firma Developers	Developer	Read in „DEVELOPERS“ Read and write in „Changes“
Tom	Firma Developers	Developer	Read in „DEVELOPERS“ Read and write in „Changes“
John	Firma Graphics	Graphic Designer	Read in „GRAPHICS“ Read and write in „Changes“
Ben	Firma Graphics	Graphic Designer	Read in „GRAPHICS“ Read and write in „Changes“
Bill	Firma	Cleaner	Only access to his home directory

First create users and groups in Your Domain:

1. Run Menu Start Programs Administrative Tools Active Directory Users and Computers
2. Right mouse click on your domain name and select New User
3. Enter all necessary fields to create user Chris.
4. Create all users (back to point 2).
5. Click with right mouse click on your domain name and select New Group
6. Create groups: Developers, Graphics, and Company.
7. Add users to groups - right mouse click on group Developers. In Members tab click Add. Add users to groups (groups Company, Developers, Graphics)

Connection to windows domain:

a. Go to uNAS/tNAS Web interface "CONFIGURATION" "NAS settings"
b. Select ADS or PDC (depends on your system - if you have NT4 Domain or Windows 2003 (with no Kerberos**** fix) then select PDC, else select ADS).
c. Enter your domain name - in PDC this will be the number IP and administrator password in ADS enter the full domain name (example. COMPANY.COM.DE).
d. Enter your domain/Kerberos server IP
e. Enter the name and password of an existing Administrator user account on your domain.
f. Click the "Apply" button to join the domain. Creation of shares and set permissions:
    1. Create a Company share (Open-E NAS-3 Web interface "CONFIGURATION" "NAS Resources" "Shares").
    2. Set permissions for all or select only Company groups.
    3. Go to share \\YOUR_NAS_SERVER_NAME\\Company
    4. Create folders "WORK", "HOME" and "FORALL".
    5. Set permissions for the folder WORK - right mouse click properties security.
    6. Deny access for everyone (point 1), change the owner to Chris user (point 4) with a full access and add Robert with a full access.
    7. In the folder WORK create folders DEVELOPER, GRAPHIC, DOCUMENTS and CHANGES.
    8. Change the owner of the DEVELOPER directory to Clint (with full rights). Add group Developers with a "read only" access.
    9. Add group Graphics with a full access to the directory GRAPHIC.
    10. Change the owner of the CHANGES directory to Clint (with full rights). Add groups Graphics and Developers with full rights.
    11. Add a secretary to the DOCUMENTS directory with a "read only" access.
    12. In the home directory create own private directory for each user, change user (make that the owner and the directory name are the same). Remove an access for the Company group (point 1).
    13. Add the group Company with a full access to the directory "FOR ALL".

** If you use the SUPERUSER all files and directories will be created as a local ROOT user.*
*** New directories with no inherited permissions do not have ACL permissions at the beginning - they have only standard UNIX permissions 0777 (Windows 2003 shows - in a normal view in the security window - every special permission. Windows 2000 does not show any permission in normal view - only in the advanced view). To enable ACL for this directory, first select "Full Access" for everyone and click the "Apply" button.*

Subsequently do the same for your group and your user. Subdirectories created in this directory should have ACL permissions inherited from the parent. If permissions are inherited then the "ALLOW" column is grey. To disable permission just use the "Deny" column.

If you change ACL permissions always check that a new set of permissions for one group does not interfere with permissions for the other user/groups or any connections between these accounts. Windows 2003 handles much better such changes than Windows 2000.

**** This function is available in Windows 2003 - in other Windows versions only your user can be selected.*

***** Kerberos is a server for distributing security keys. Normally it is only on the domain but it can be on some external server. In Windows 2003 this server is ignoring specified key types, and authorization works only when entering IP not the NAS-R3 name.*

4.6.2 Access uNAS/tNAS shares under Linux

Please use following line to mount an NFS share:

- mount -t nfs 192.168.0.220: /share/share_name /local_mount_point where:
  192.168.0.220 is the uNAS/tNAS IP

Please use following line to mount an SMB share:

In a shell:

- mount -t smbfs -o username=root,password=12345 //192.168.0.220/test /mnt-smb

where 'test' is the share name

In X-windows:

- Smb://root@192.168.0.220/

5 Descriptions of function

5.1 Functions of the console display

While uNAS/tNAS can be fully administered remotely through a secure Web interface, some of the functions you can access on the console. uNAS/tNAS constantly displays following basic parameters:

- IP address
- Https settings

CTRL+ALT+n

If you press the left CTRL key + the left ALT key + n, you will be asked for the new IP address and the subnet mask. The DHCP server will be shut down.

CTRL+ALT+p

If you press the left CTRL key + the left ALT key + p, the access restrictions are lifted by entering the administrator password (in addition, there is a reset to the standard https port 443).

CTRL+ALT+i

By pressing a combination of left CTRL key, left ALT key and i, you can reset the original IP address (192.168.0.220) and the subnet settings (255.255.255.0). In this process, the DHCP server support is turned on.

CTRL+ALT+t

By pressing a combination of left CTRL key, left ALT key and t, you can run Console Tools. The menu will appear, with choice of following functions: Ping, DHCP Ping, Hardware info, Memory info, Time configuration and DNS configuration.

CTRL+ALT+x

By pressing the left CTRL key, left ALT key and x, it will display extended tools.

CTRL+ALT+w

By pressing the left CTRL key, left ALT key and w, it will display hardware configuration.

CTRL+ALT+r

By pressing the left CTRL key, left ALT key and r, it will display CLI Management Tool for RAID controller

CTRL+ALT+f

By pressing the left CTRL key, left ALT key and f, it will display CLI Management Tool for Fibre Channel controller.

CTRL+ALT+h

By pressing the left CTRL key, left ALT key and h, it will display hardware and driver information.

F1, F2 and F5

Function key F1 is available to display help information while F5 will reset the console display to default. If you press F2 key all network interface will be displayed.

Shutting down and restarting

With Ctrl + ALT + DEL the uNAS/tNAS host computer will be shut down and restart, while CTRL + ALT + S shut it down. Please be careful with this option when users are connected.

ESC menu

Boot menu is available by pressing ESC after POST (Power-on self-test) during the initial start of uNAS/tNAS system. After pressing ESC, there will appear menu with possibility of launching NAS-R3 in different procedures of work or memory testing:

- -Single - system launch with (kernel) for one CPU,
- -SMP - system launch with (kernel) for more CPU's system,
- -x86 - system launch with restrictions of 4GB RAM(this procedure should work on every unit with CPU better than 386 and with CPU C3),
- -Single (Intel I/TA support) - system launch in procedure with one CPU,
- -SMP (Intel I/TA support) - system launch in multiple-CPU,
- Memtest - after choosing this option, memory of the system, where uNAS/tNAS is installed, will be tested, Apart from test, there are also available information about the memory itself and its settings,
- RESCUE_MODE - in this option, only driver which enables access to the net are loaded (if there is a need to connect using remote support).

5.2 Functions of uNAS/tNAS via browser access

On the following pages, we will thoroughly describe every function of uNAS/tNAS. The functions are divided by menu options, which are located at the top part of the screen.

5.2.1 SETUP

In this place you can manage network interfaces, administrator settings, hardware RAID controllers, create disk array using software RAID, Fibre Channel, iSCSI initiator, hardware and GUI settings.

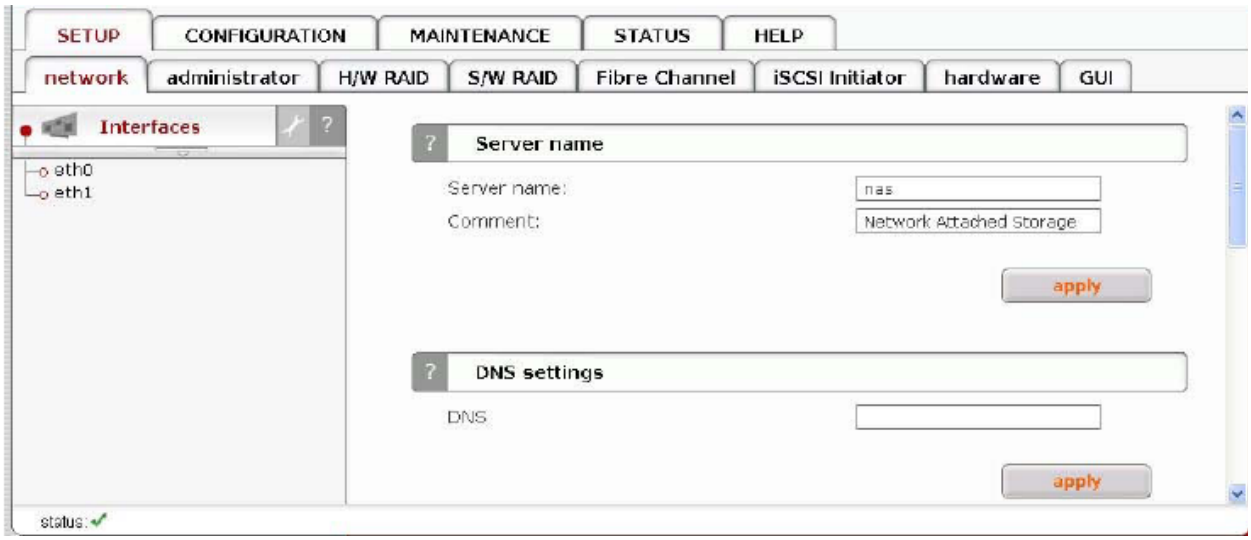
5.2.1.1 Network

Here you can find tree containing network interfaces. Click on Interface name to see more information about selected interface.

Function: Server name

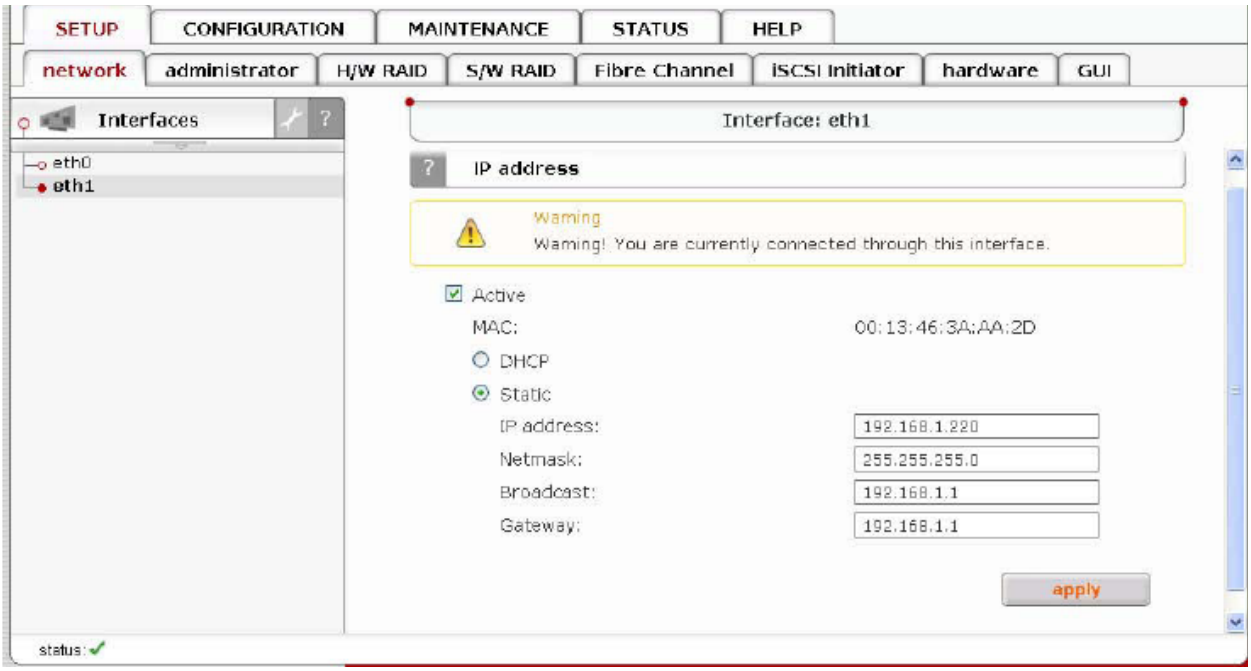
Please enter server name to clearly identify your server. In the field “Comment,” please enter short description of your server. Server Name and Comment rules:

- Please make sure the server name is unique in your network.
- Select a server name that clearly identifies your new server.
- Please do not use spaces and special characters like:~!@#$^&()+[]{}*;:'".,%|<>?/\=`_
- Server Name can not consist of digits only.
- Comment is not displayed in some systems.



Function: DNS settings

This function enables you to enter DNS addresses. Please use semicolons to separate addresses.



Function: Create new bond interface

Bonding allows for load-balancing or fail-over for the incoming and outgoing connections. Here you can create or edit bonding network interface. In order to create bonding interface:

- select network interfaces from which you want to create a new bonding interface.
- select desired bonding mode from Create drop down menu.
- select dynamic (DHCP) or static configuration of network interface.
- if you want to dynamically get DNS address, select "get DNS".
- when using static configuration of network interface enter address IP, netmask, broadcast and gateway apply Create button, new bonding interface will be created now.
  In order to take advantage of bonding more than one Ethernet NIC needs to be plugged into the box.

Each network interface is described by following fields:

- Primary - A string (eth0, eth2, etc) specifying which slave is the primary device. The specified device will always be the active slave while it is available. Only when the primary is off-line will alternate devices be used. This is useful when one slave is preferred over another, e.g., when one slave has higher throughput than another. The primary option is only valid for active-backup mode.
- Interface - Network interface name.
- Cable - Shows if cable is connected to NIC.
- State - Describes state of the network interface. NIC can be in bonding state or single.

Bonding modes:

- balance-rr : Transmissions are received and sent out sequentially on each bonded slave interface. This mode provides fault tolerance and load balancing.

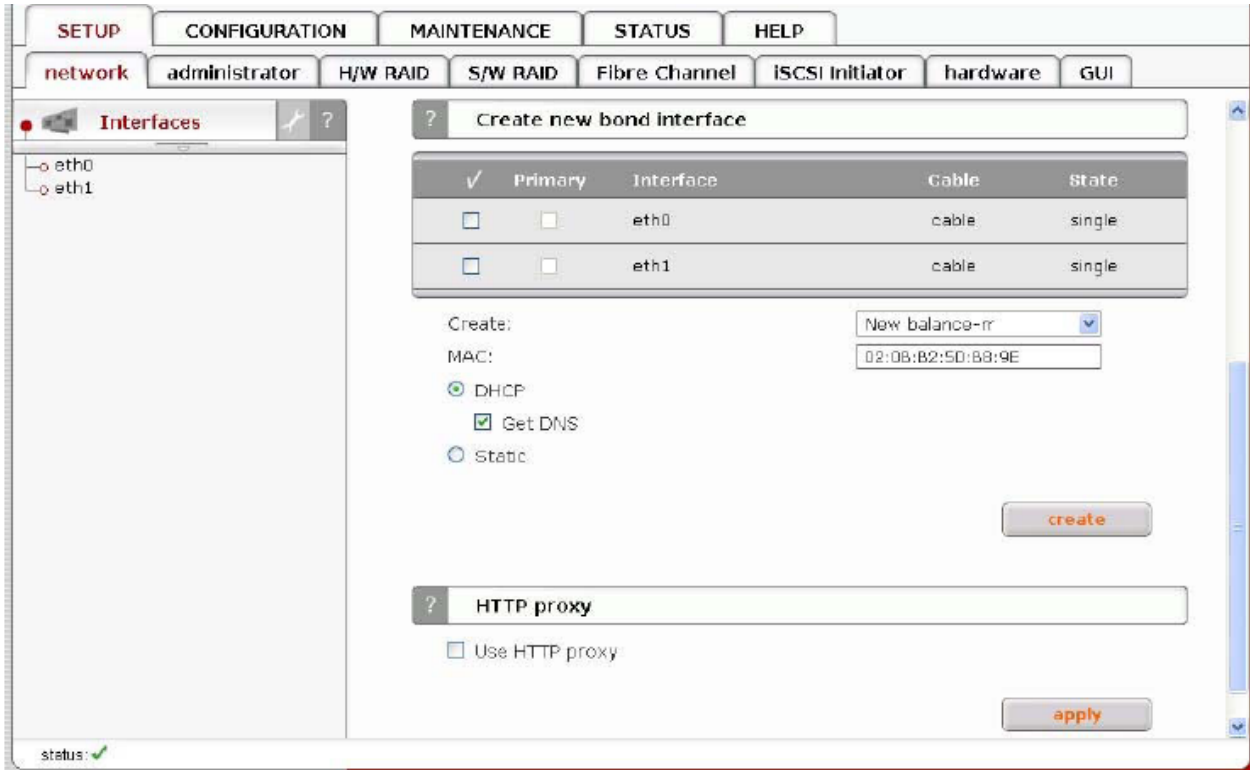
- active-backup : Only one slave in the bond is active. Another bonded slave interface is only used if the active bonded slave interface fails. This mode provides fault tolerance.

- balance-xor: Transmit based on [(source MAC address XOR'd with destination MAC address) modulo slave count]. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance. This mode provides fault tolerance and load balancing.

- broadcast: Transmits everything on all slave interfaces. This mode provides fault tolerance.

- 802.3ad: IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification. Requires a switch that supports IEEE 802.3ad Dynamic link aggregation.

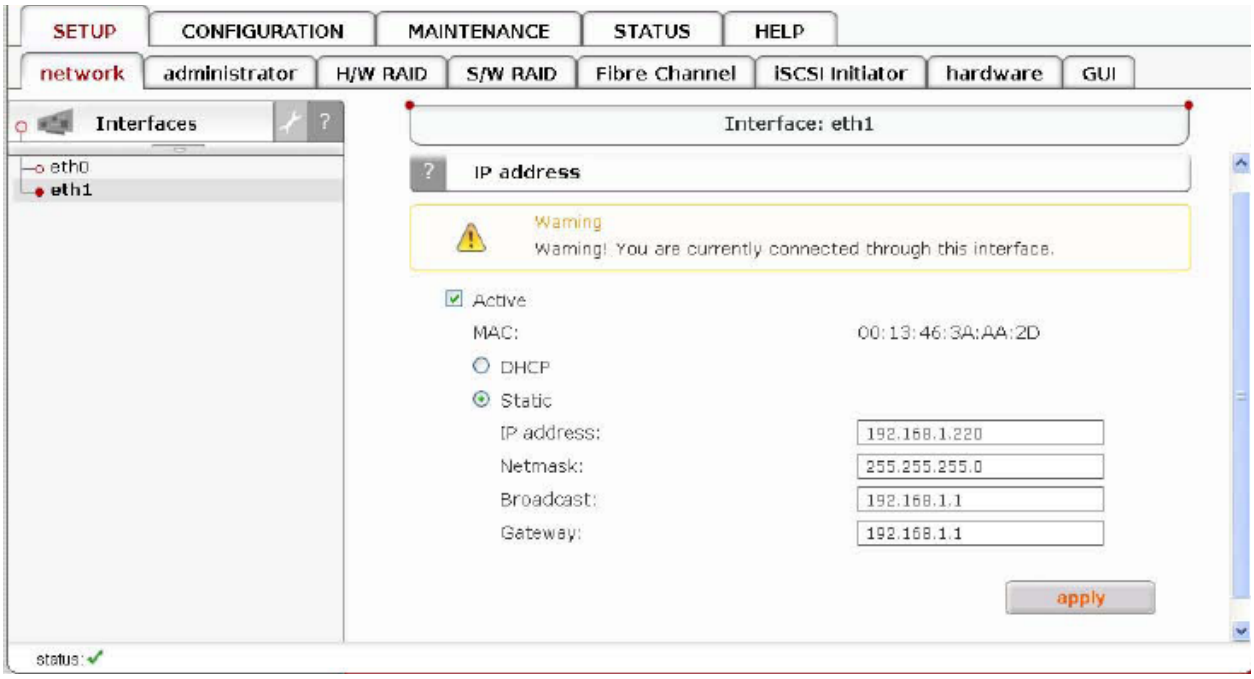
- balance-tlb: Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave. This mode provides fault tolerance and load balancing.



Function: HTTP proxy

With this function you can enable or disable HTTP proxy.
To enable HTTP proxy:

- select "Use HTTP proxy"
- enter server name, port, user and password
- click "apply" button



Function: IP address

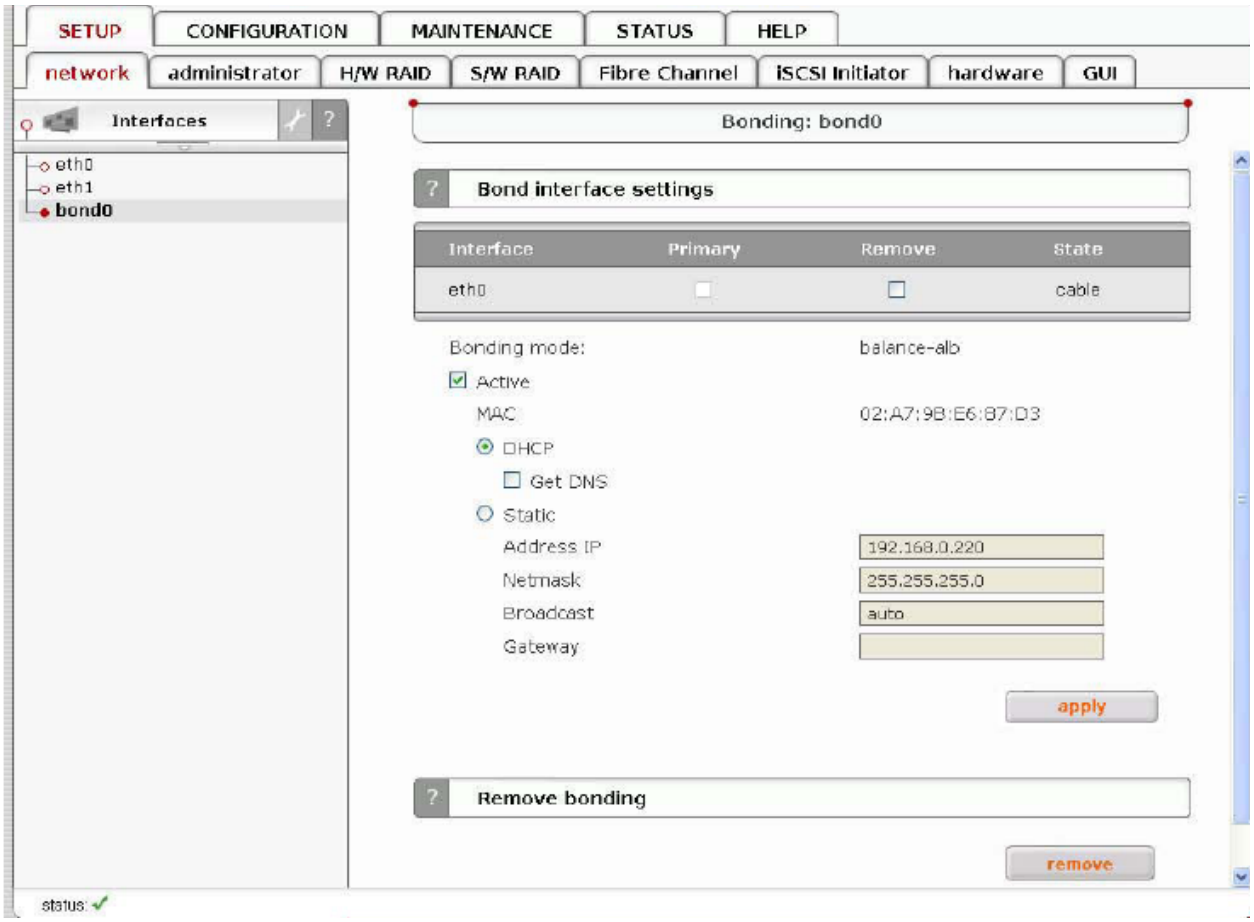
Here you can set TCP/IP parameters for selected NIC.
Activate - You can activate or deactivate network interface by setting this checkbox. DHCP / Static. You can use static or dynamic (DHCP) network interface configuration.
Get DNS - If you want to dynamically get DNS address, select "get DNS". When using static configuration of network interface, enter:

- address IP,
- netmask,
- broadcast,
- gateway.

If you set new IP address, during activation, you will lose your connection to the server and you will have to log in again. In the URL entry line of your browser, please enter the new IP address. If you do not get access, please try the console to set new IP address. In order to access servers in another subnet, you need to enter the address of a router as Gateway.

In case you use NTP server to maintain proper time & date, please make sure you have proper Gateway and DNS settings.

In case of creating bonding interface on left page will appear new branch “bond0”. By clicking on the branch “bond0” you have the possibility of bonding’s settings and removal (see below).



Function: Bond interface settings

Here you can edit a bonding network interface.
To remove network interface form bonding select it in field remove and click "apply" button. Bonding can be deactivated by setting of "Active" option. You can change bonding interface network configuration, you can use static or dynamic (DHCP) network configuration.

Each network interface is that belongs to bonding interface is described by following fields:
Primary - A string (eth0, eth2, etc) specifying which slave is the primary device. The specified device will always be the active slave while it is available. Only when the primary is off-line will alternate devices be used. This is useful when one slave is preferred over another, e.g., when one slave has higher throughput than another. The primary option is only valid for active-backup mode.
Interface - Network interface name
State: - Shows if NIC is connected.

Function: Remove bonding

Here you can remove a bonding interface.

5.2.1.2 Administrator

Function: Administrator access

Use this function to restrict access to the server administration.

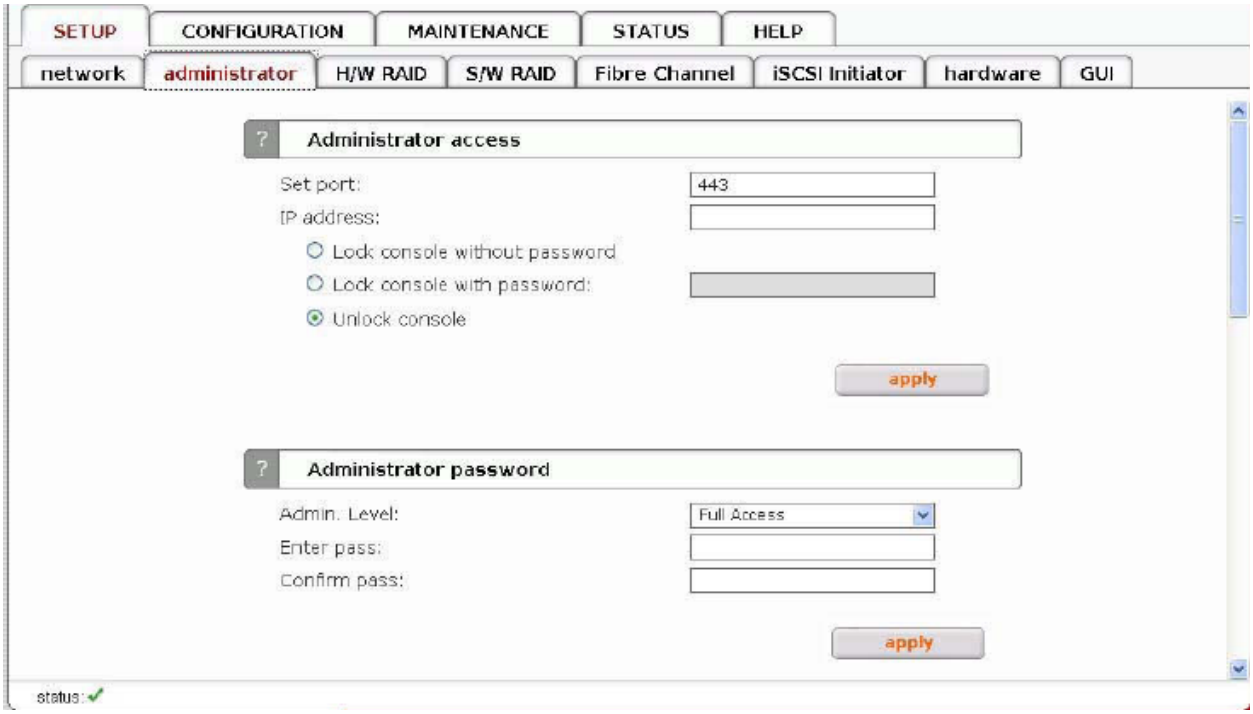
Set port - You can change https port (default 443)

IP address - You can assign IP addresses (separated by a semicolon) that are granted to access the Server Web administration. This field left blank means no restriction.

Lock console without password - Disables access to the console (and LCD keys)

Lock console with password - To get access to the console (and LCD keys) you need to type password. Note that this password should be exactly 8 characters long and include only 1-4 digits.

Unlock console - Unrestricted access to the console.
Please exercise caution with this function if all computers in the network receive IP addresses via DHCP: current IP can be replaced by a new one after the lease ends. Please pay attention using Lock console feature - you will not be able to reset default administrator access from the console in case of any mistake setting IP address. To restore default settings you have to re-update software in the uNAS/tNAS module or contact technical support.



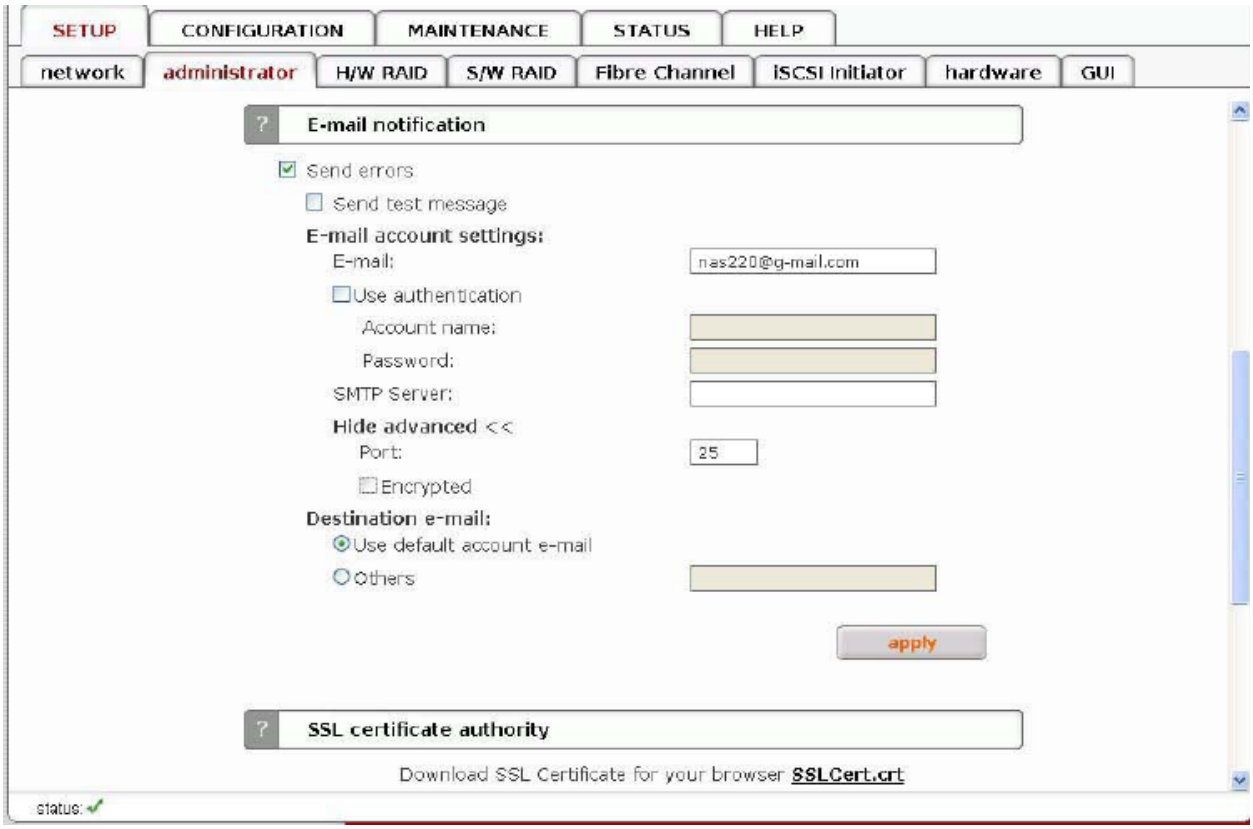
Function: Administrator password

Using this function, you can change the passwords of the server administration accounts.

Enter password - Please enter your new password.

Confirm password - Please retype your new password.
Password cannot contain:
- characters: ' " `
- spaces.

The default password for each account is “admin”.
Password-checking is case-sensitive. For security reasons, the password you enter will not be displayed. Please check the status of the Shift and Shift Lock keys.



Function: E-mail notification

The server can send an e-mail notification to the administrator in case of significant events, critical errors, warnings, etc. To enable this feature check Send errors.

E-mail - E-mail from which notifications will be send.

Account name - Account name for e-mail from which notifications will be sent.

Password - Password for account name provided above.

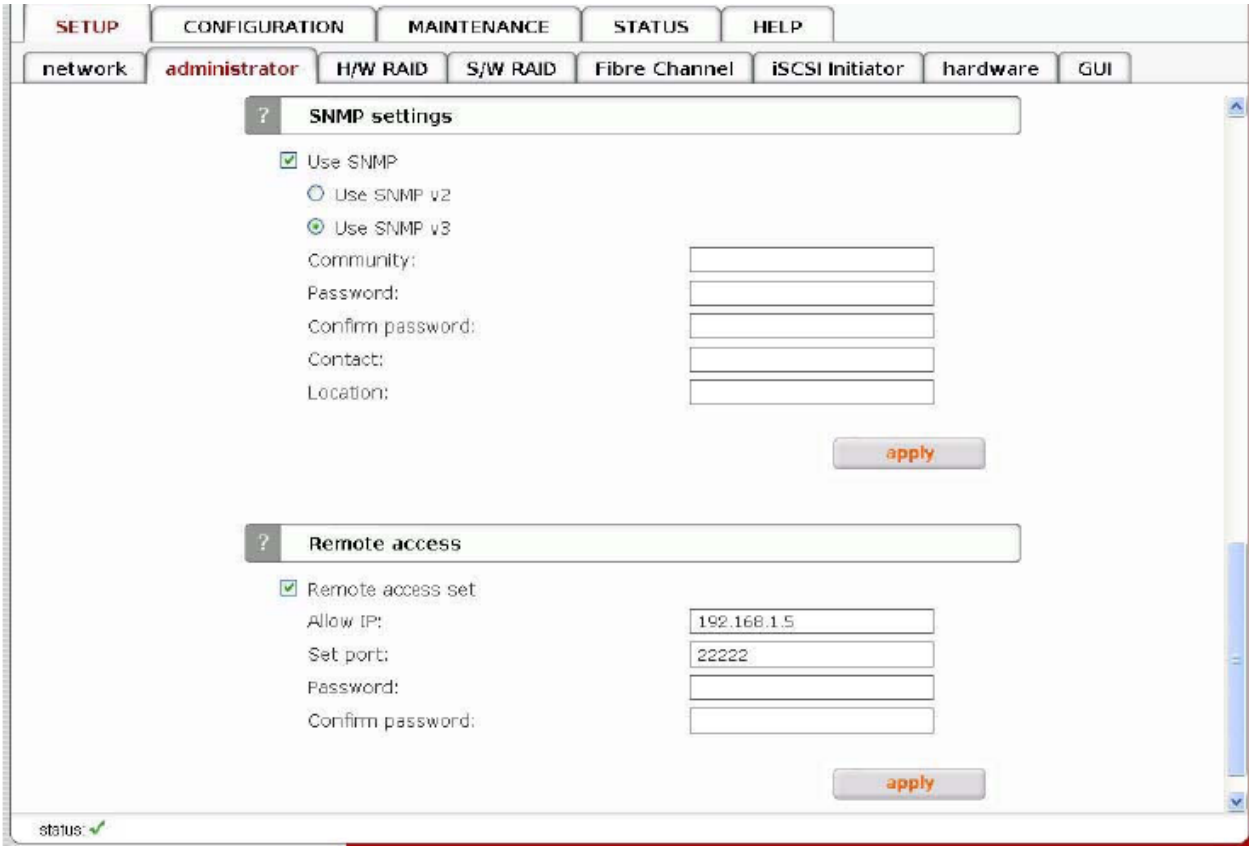
SMTP server - SMTP server name.

Destination e-mail - Administrator e-mail address to which notifications will be sent.

Port - Port number for SMTP server.
If you want to send a test message, please check option Send test message.
If you want to have e-mail notifications encrypted, check option Encrypted.

Function: SLL certificate authority

To ensure the identity of the web administration tool by letting your web browser automatically check it whenever you connect for administration tasks, click the SSLCert.crt link to download and install the certificate into the certificate management system of your browser.



Function: SNMP settings

This function enables you to change the access over the SNMP protocol in version 2 or 3. With SNMP you can get a lot of information (usage of CPU, system load, memory info, Ethernet traffic, running processes).

System location and system contact are only for your information, for example when you connect from SNMP client, you will see your location and name. SNMP in version 3 has encrypted transmission and authentication by community and password.

SNMP in version 2 does not have encrypted transmission and authentication is only by community.
The community you are setting can be max up to 20 characters and password min 8 characters.
Links to SNMP clients:
• http://www.muonics.com

- http://www.mg-soft.com
- http://www.adventnet.com

Function: Remote access

Using this function, you can administrate console tools remotely by ssh protocol (secure shell). Default user is 'cli' and you cannot change it, but password can be change.

Allow IP - You can assign IP addresses (separated by a semicolon) that are granted to server remote access. The field left blank means no restriction.

Set port - Default port is 22222 for security reasons, because high ports are invisible for port scanners. You can change it only from range 1024-65535 except ports already used.

Password - Length of password is minimum 8 characters. Be sure to use strong passwords.

Confirm password - Please retype your new password.

Password cannot contain - • characters: ' " ` ^ & $ # [ ] \/ | * and spaces.

To connect to server from Linux/MacOSX systems use:
ssh -2 -p 22222 -l cli address_ip
where:
- option: -2 is a version of ssh protocol used for connection.
- option: -p is a port for Remote Access.
- option: -l is a user (In our product the user must be "cli").
- option: address_ip is a address of server you want to connect to.

You will be asking for a password you entered on server for Remote Access.

To connect to server from Microsoft Windows, download free ssh client Putty (www.putty.nl). Please follow step-by-step below in order to configure putty client:
- In Host Name (or IP address) field please enter IP address of the server
- In Port field please enter the same port as in the server GUI (default 22222)
- In Protocol please choose SSH
- In Category: Connection -> Data -> Auto-login-username please enter: "cli"
- In Terminal -> Keyboard -> The Function Keys and keypad please select "VT100+"
- Go back to Category Session, enter session name in field Saved Sessions and click on "Save" button.
- Then click on new saved session, click "Open" and enter the "password". (In case you did not enter Auto-login-username, it will prompt for username, so please enter: "cli")

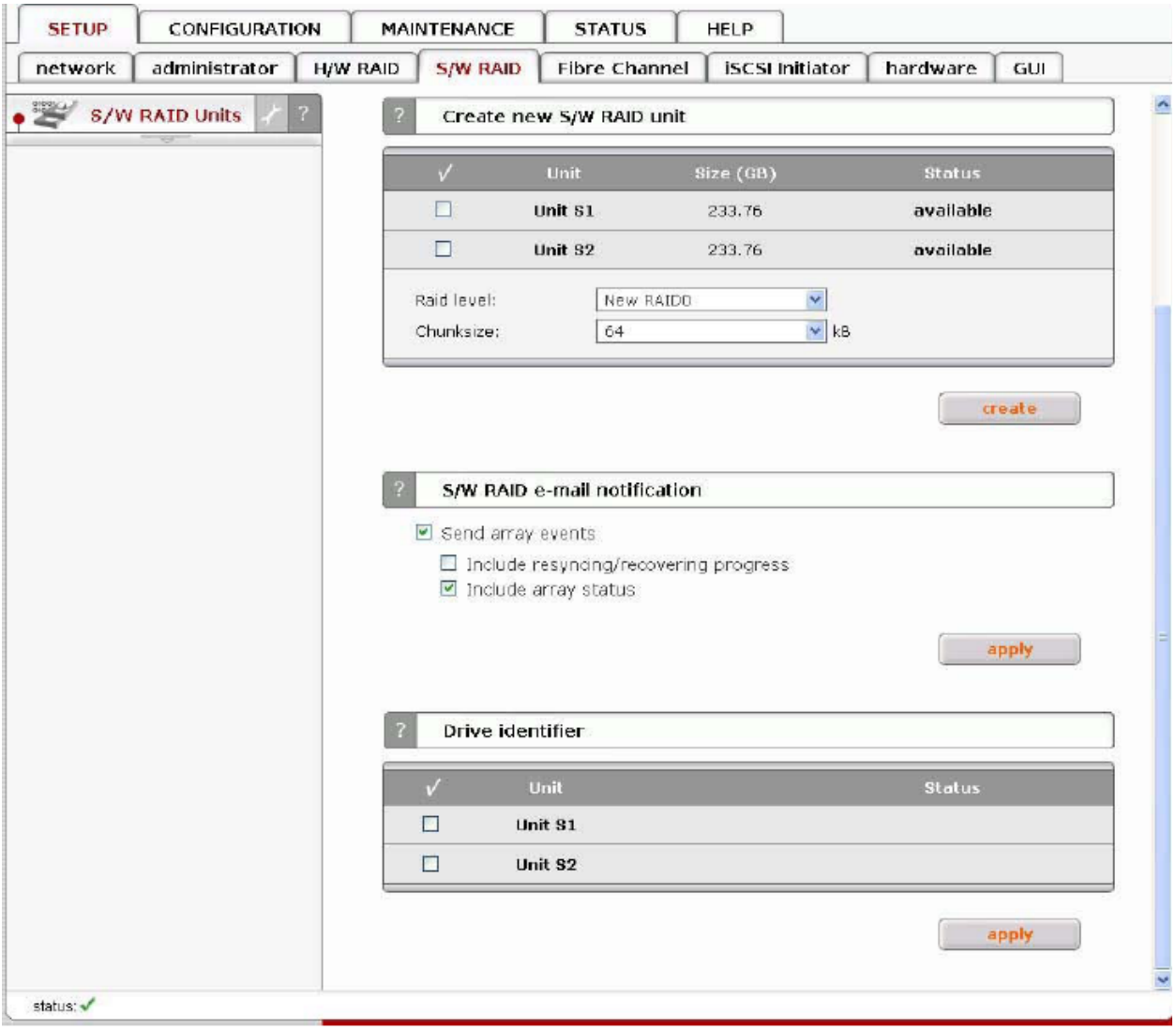
5.2.1.3 H/W RAID

Please note that the RAID controller MUST be supported by the our NAS system. For list of support HBA please contact us

5.2.1.4 S/W RAID

Function: Create new S/W RAID unit

In this function you can create software RAIDs from free (not used) units. If you want to create RAIDs from used units, you need first to delete content of units in console, be aware this would ERASE all data from units.



To create a RAID select units, then from ListBox select what type of RAID it will be, then select desired Chunk size. After setting all demanded parameters press Create button.

Allow to create degraded mode - It allows to create RAID1 with one unit, RAID5 with two units or RAID6 with three units, even if minimal number of units is not meet.
Chunk size - its a minimal portion of data that is written at a time.

Available RAIDS
- RAID 0: it is stripe array and requires [minimum] 2 units. In RAID 0 you can set the Chunksize 4k ÷ 256k. The destination size of the RAID Array will be the sum of each drive size in array.

- RAID 1: mirror array requires 2 units. Destination size will be equal: SINGLE) UNIT_SIZE, where (SINGLE) UNIT_SIZE is the size of the smallest unit in array.

- RAID 5: stripe + parity algorithm array (required [minimum] 3 units - with the same capacity). You can choose from the ListBoxes: (layout) parityalgorithm [left/right] [symmetric/asymmetric].

DESTINATION SIZE: (NR_OF_UNITS-1)*(SINGLE)UNIT_SIZE, where (SINGLE) UNIT_SIZE is the size of the smallest unit in array.

The (layout) parity-algorithm in RAID 5 is described below.

RAID 5 (layout) parity-algorithms

It is possible to set one of four algorithms of placement data blocks and parity blocks in matrix. Our default option is left-symmetric, which is the best for large reads. Other recommended value is left-asymmetric.

Software RAID 5 is not a good choice for writing a lot of very small files!

Left-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	2	Parity
3	4	Parity	5
6	Parity	7	8
Parity	9	10	11
12	13	14	Parity

Right-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	0	1	2
3	Parity	4	5
6	7	Parity	8
9	10	11	Parity
Parity	12	13	14

Left-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	2	Parity
4	5	Parity	3
8	Parity	6	7
Parity	9	10	11
12	13	14	Parity

Right-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	0	1	2
5	Parity	3	4
7	8	Parity	6
9	10	11	Parity
Parity	12	13	14

RAID6: stripe + parity algorithm array (required, minimum 4 units - with the same capacity). You can choose from the ListBoxes: (layout)parityalgorithm [left/right] [symmetric/asymmetric].

DESTINATION SIZE: (NR_OF_UNITS-2)*(SINGLE)UNIT_SIZE, where (SINGLE) UNIT_SIZE is the size of the smallest unit in array.

The (layout) parity-algorithm in RAID 6 is described below.

RAID 6 (layout) parity-algorithm

It is possible to set one from four algorithms of placement data blocks and parity blocks in matrix. Our default option is left-symmetric which the best is for large reads. Other recommended value is left-asymmetric.

Left-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	Parity	Parity
2	Parity	Parity	3
Parity	Parity	4	5
Parity	6	7	Parity
8	9	Parity	Parity

Right-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	Parity	0	1
2	Parity	Parity	3
4	5	Parity	Parity
Parity	6	7	Parity
8	9	Parity	Parity

Left-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	Parity	Parity
3	Parity	Parity	2
Parity	Parity	4	5
Parity	6	7	Parity
8	9	Parity	Parity

Right-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	Parity	0	1
3	Parity	Parity	2
4	5	Parity	Parity
Parity	6	7	Parity
Parity	Parity	8	9

To remove RAID, if previously added to Volume Group please enter console Extended tools (press F1 on console to find out keyboard shortcuts) and first delete Volume Group of the RAID (Delete content of units function in Extended tools menu). Then the Remove button will be enabled. Otherwise simply press Remove button.

You can add spare units to RAID1, RAID5 and RAID6 arrays. Please remember that after creation of an RAID, in Function: 'Info' will be shown progress of Synchronization. Till end of this process all actions done on this array will be performed a bit slower.

If Units are connected through Fibre Channel with only one Storage or LUNS(under iSCSI) come from the same target, then its not recommended to create s/w raids on these Units, because this would slow down the system. If Units come from two different Storages or LUNS come from two different targets, then you can create s/w raids with no problem.

Function: S/W RAID e-mail notification

It is possible to send notification by e-mail about events on software RAID arrays (e.g. rebuild started, rebuild finished, span is active). In order to do so please check Send array events. In order to Send array events you must enable “E-mail notification” in “setup” “administrator”.

Include re-syncing / recovering progress

This enables informing about progress of re-sync /rebuild, if it's currently running. E-mail will be send for every 20 % done.

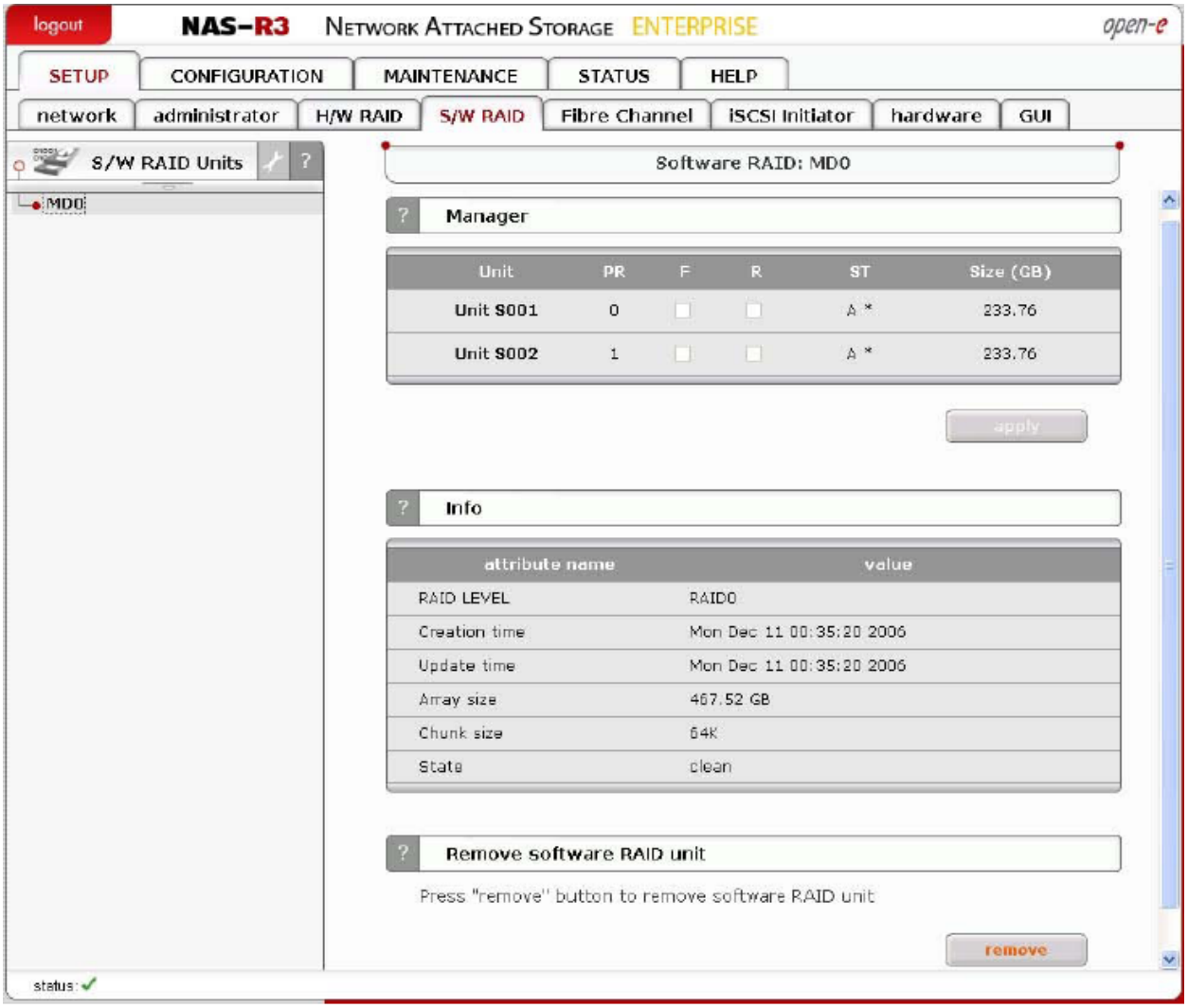
Include array status

Information about the status of event-related array will be added every event.

Function: Drive identifier

This function helps find disks in the cage of your NAS server. In case of hardware RAID installed, the whole RAID array is shown as a single drive. In this case you may not be able to determine which drive unit is which disk when using S.M.A.R.T. tool or hardware RAID management tool (depends on manufacturer of RAID controller).

When you click on "start" button then the appropriate disk will start reading and you can determine which disk is it by watching "disk-activity LEDs". For proper operation of this function there should be no other activity on hard drives. Identification will stop automatically after one minute if you will not stop it before (by unsetting appropriate checkbox and applying form). Using this function during normal operation is not highly recommended and will cause of your server to slow down.



Function: Manager

In this function you can manage the RAID array. Available operations:

RAID 0:

• construction of this RAID does not allow to manage it anyway. Every unit must not be Failed. If any would be the whole array would be destroyed.

RAID 1:

• To set unit as a Faulty one mark proper checkbox (in the column F) and click on Apply button.
• To delete any unit from an array mark proper checkbox (in the column R) and click on Remove button.

RAID 5:

• To set unit as a Faulty one mark proper checkbox (in the column F) and click on Apply button.
• To delete any unit from an array mark proper checkbox (in the column R) and click on Remove button.

RAID 6:

• To set unit as a Faulty one mark proper checkbox (in the column F) and click on Apply button.
• To delete any unit from an array mark proper checkbox (in the column R) and click on Remove button.

RAIDs notation:

• PR - priority in array - describes priority of unit that will be added to array if another is set to Faulty.
• F - faulty - unit can be turned off from array
• R - hot remove - unit can be removed from array without shutting down the system.
• ST - describes state of unit in array, which can be:
• A - This means that Unit is active in array
• * - Number of Unit that belongs to the array
• S - Spare or spare rebuilding - this means that unit is free and can be added to the array or is free and currently is rebuilding.

Limitations:

• There is no possibility to set any unit as faulty if the matrix is degraded or during re-sync/rebuild.
• While using RAID 1 and RAID 5 there is possibility to set only one disk from active as faulty. This regulation is not valid for Spare units in array.
Only one disk from Active in Array can be set as Faulty or Removed

Function: Info

From this function you can obtain information like Creation Time, RAID Level, Array and Device Size, Update Time and state. During syncing or rebuilding of array it is recommended

to perform as few disk operations as possible. Status of syncing/rebuilding will be showed "live" - without need to refresh page manually.

Function: Remove software RAID unit

This function allows you to remove Software RAID unit (MD[nr]). This function is available only when no Logical Volume is created on appropriate MD[x] and unit is not resyncing. If you want to remove software RAID unit with Logical Volume please use console Extended tools (press F1 on console to find out keyboard shortcuts) and remove Logical Volume first.

5.2.1.5 Fibre Channel

Intention Blank

5.2.1.6 iSCSI Initiator

Here you can view list of all connected iSCSI server portals. Click on portal IP to manage portal targets or remove the portal.

Function: Create new portal server

With this function you can connect to remote iSCSI server and add it as New Portal Server. It will be visible in iSCSI Initiator on the left. You can use following options:

Portal IP:

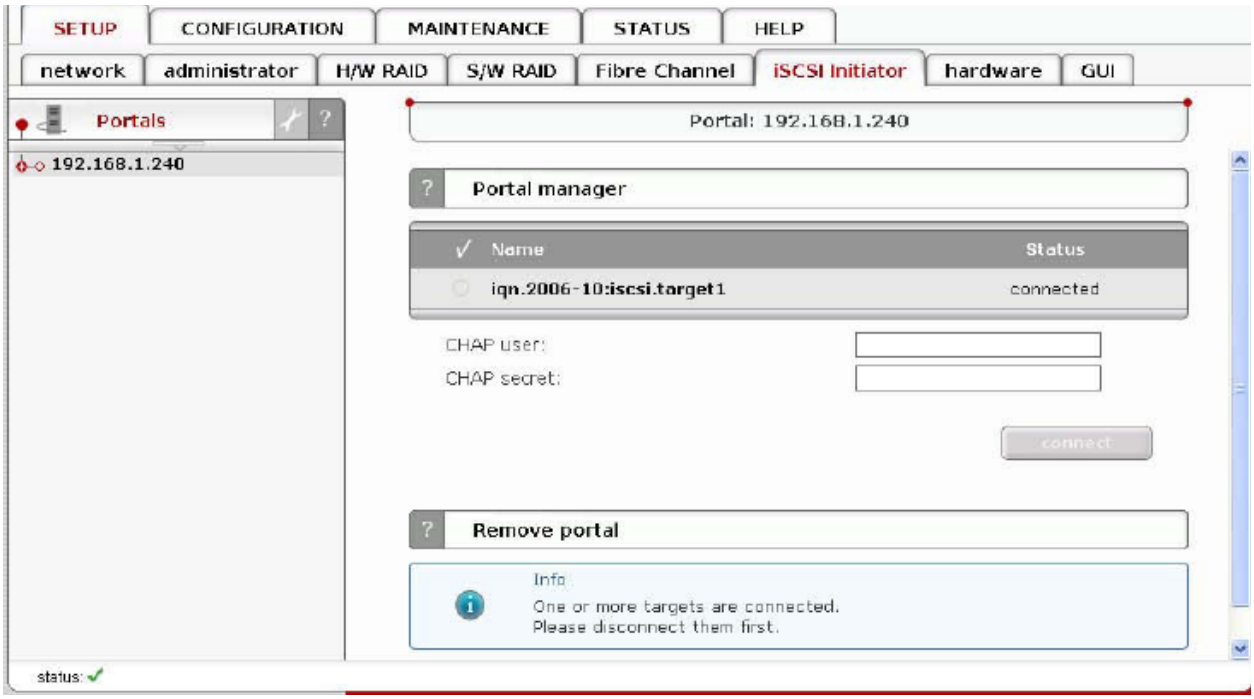
Please enter IP address of iSCSI server.

Portal Port

Enter Port on which iSCSI server runs(default 3260)

CHAP enable

If you want to enable CHAP user authentication please check box CHAP enable and enter CHAP user name and its secret.



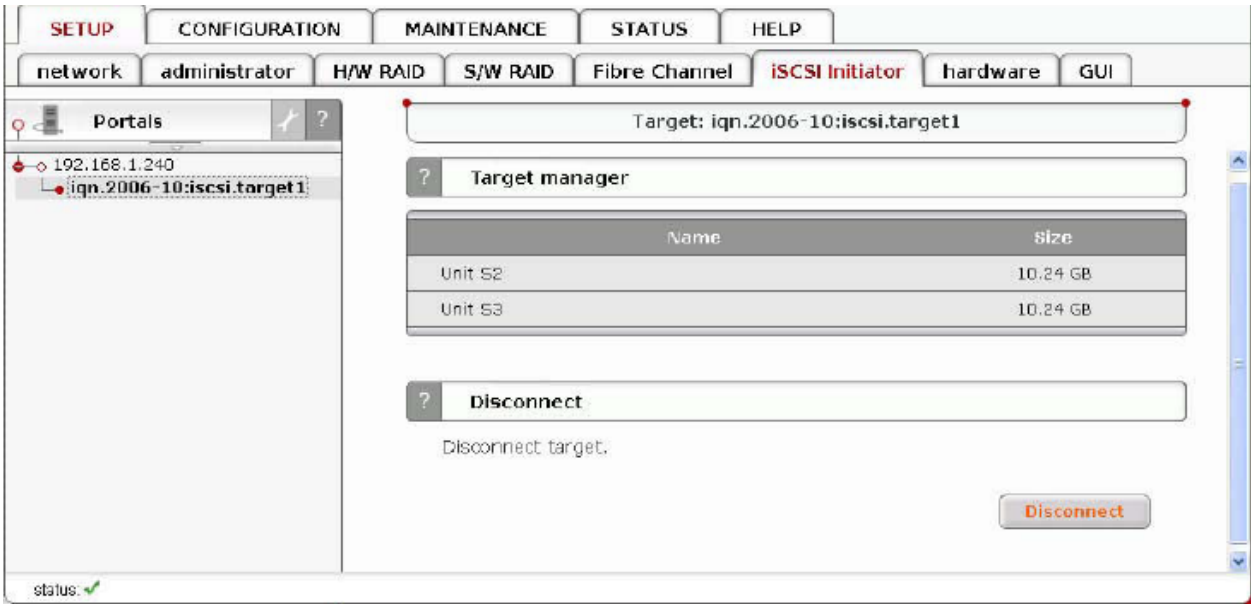
Function: Portal manager

This function displays available targets from selected iSCSI Portal Server. In order to connect to iSCSI target, select its name and click button "connect". If authentication for target is enabled, then also enter target name and its secret. Connected targets will be available in server -> disk manger as Units. You can manage them and do the same operations as it would be local Units. In order to disconnect from target, select its name in iSCSI Initiator tree and click "disconnect" button. To remove iSCSI Portal server, first you need to disconnect all targets from it.

Function: Remove portal

Here you can remove selected Portal Server.

You can only remove Portal Server if all its targets are disconnected from it. In order to disconnect a target from Portal Server, please select it from iSCSI initiator tree and click on "disconnect" button.



Function: Target manager

Here you can view connected targets name and its size. You can also disconnect target from Portal Server with function Disconnect.

Function: Disconnect

Here you can disconnect selected target from Portal Server. You can only disconnect target from a Portal Server if volume group or S/W RAID unit does not exist. In another case please first remove a volume group or S/W RAID unit in console tools(press F1 on console to find out keyboard shortcuts).

5.2.1.7 Hardware

Function: UPS settings

In the UPS menu you can select an UPS device (Uninterrupted Power Supply). In the settings you can select the UPS model, cable type, connection port (serial port or USB) and the length of the time-out. The time-out defines the time between a power failure and the moment the system will shut down.

Single

Means, that the server is the only system attached to this UPS and that there is no action necessary to do remote shutdown for other systems in the network.

Master

Means, that the server is connected to the UPS and sends a signal through the network to shutdown other systems in the network.

Slave

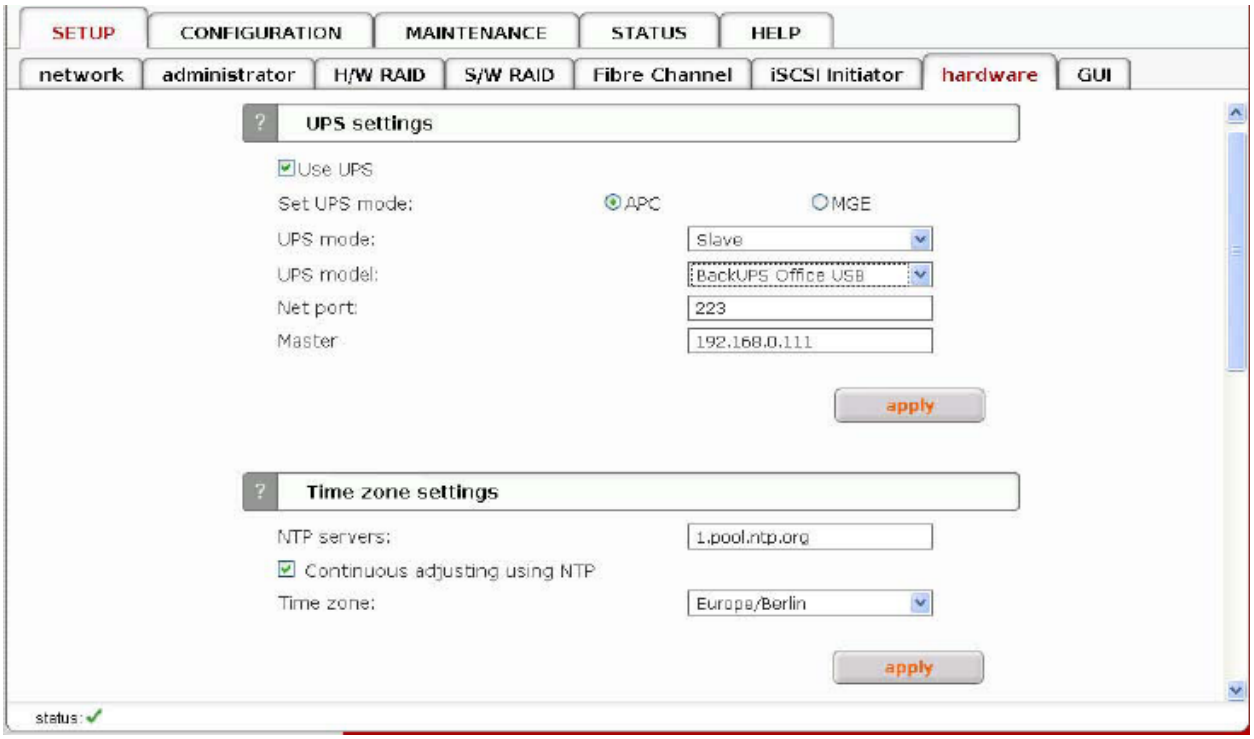
Means, that the server is reacting on a "power down-signal" from an UPS master. When using SMART UPS with APC mode there are additional options:

Timeout - Battery Limit

This option enables sub staining the system as long as battery holds(the system will shutdown when battery charge drops to 5% or when there are 3 minutes time to total discharge of battery)

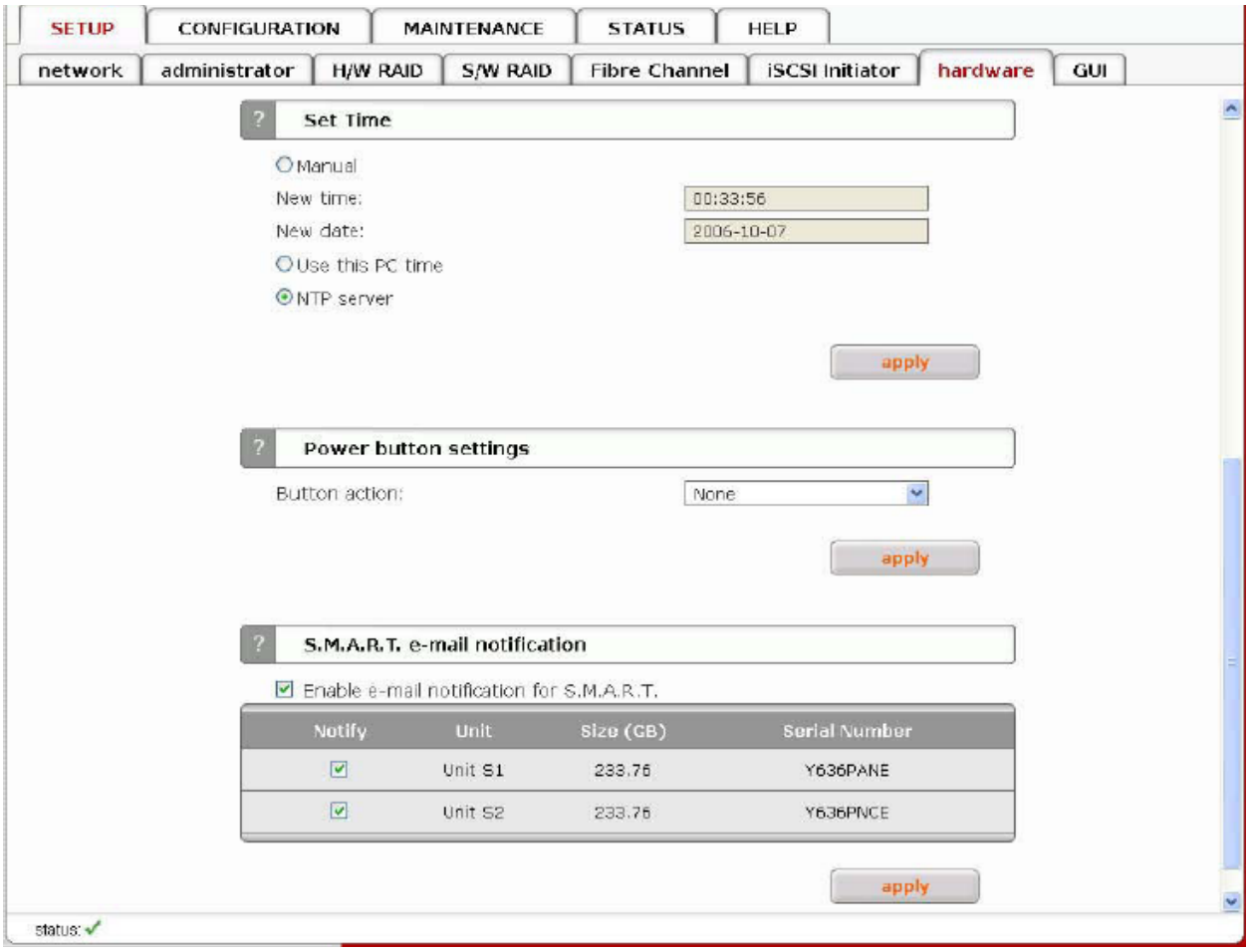
Turn off UPS after system shutdown

This will turn off the UPS after time that is set by parameter Shutdown grace delay(SLEEP) in EEPROM of UPS.



Function: Time zone settings

This function allows to set NTP server settings.
Please choose a NTP server (Network Time Protocol: for more info: www.ntp.org)
You may provide a fully qualified host name or IP address. Select time zone accordingly to your location.
There is also option Continuous adjusting using NTP, this will watch your system time and will correct it, if the difference between local time and server time has change. Setting this option on is specially recommended when using domains.
Time setting is very important for proper work of the server.
You must have set gateway and (in case of host name) DNS network settings.



Function: Set time

With this function you can set time and date:

Manual

Just type in time & date using following format: hh:mm:ss yyyy-mm-dd.

Use this PC time

It will pick up the time & date of the PC you run the web browser.

NTP server

It will pick up the time & date from NTP server. In this case please make sure you have Internet access and proper network setup, specially gateway and DNS. You can check proper Internet access using ping from the NAS console (press F1 on console to find out keyboard shortcuts). To use this option you must set correct NTP server in function Clock settings. Time setting is very important for proper work of the server.

Function: Power button settings

In this section you specify which action will be performed in case of power button is pressed
Options:

Reboot

Restart computer.

Halt
Power off computer.
None
No action.

Function: S.M.A.R.T. e-mail notification

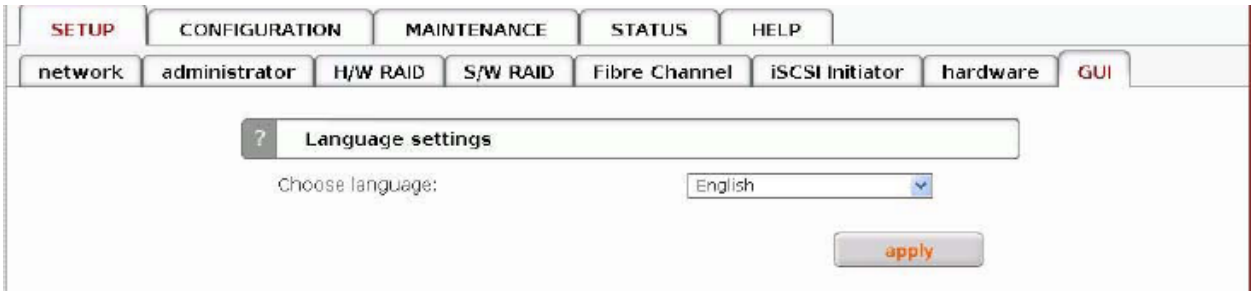
This function allows you to check S.M.A.R.T. status of hard disks and send it to e-mail address. S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) is a monitoring system for computer hard disks to detect and report on various indicators of reliability, in the hope of anticipating failures. In order to enable S.M.A.R.T. e-mail notification, you have to:

- First enable E-mail notification function in setup -> administrator menu.
- Enable S.M.A.R.T. in Hardware configuration tool on console (press F1 on console to find out keyboard shortcuts).
- When S.M.A.R.T. is enabled you will see all detected hard drives with information about unit number, size and serial number.
- Select the checkbox of unit, from which you want to receive S.M.A.R.T. status and press "apply".
- If everything is ok, then status will be PASSED, in another case FAILED.

5.2.1.8 GUI

Function: Language settings

Select preferred language and press "apply" button.



5.2.2 CONFIGURATION

5.2.2.1 Volume manager

Function: Unit rescan

This function rescans your system for new units.

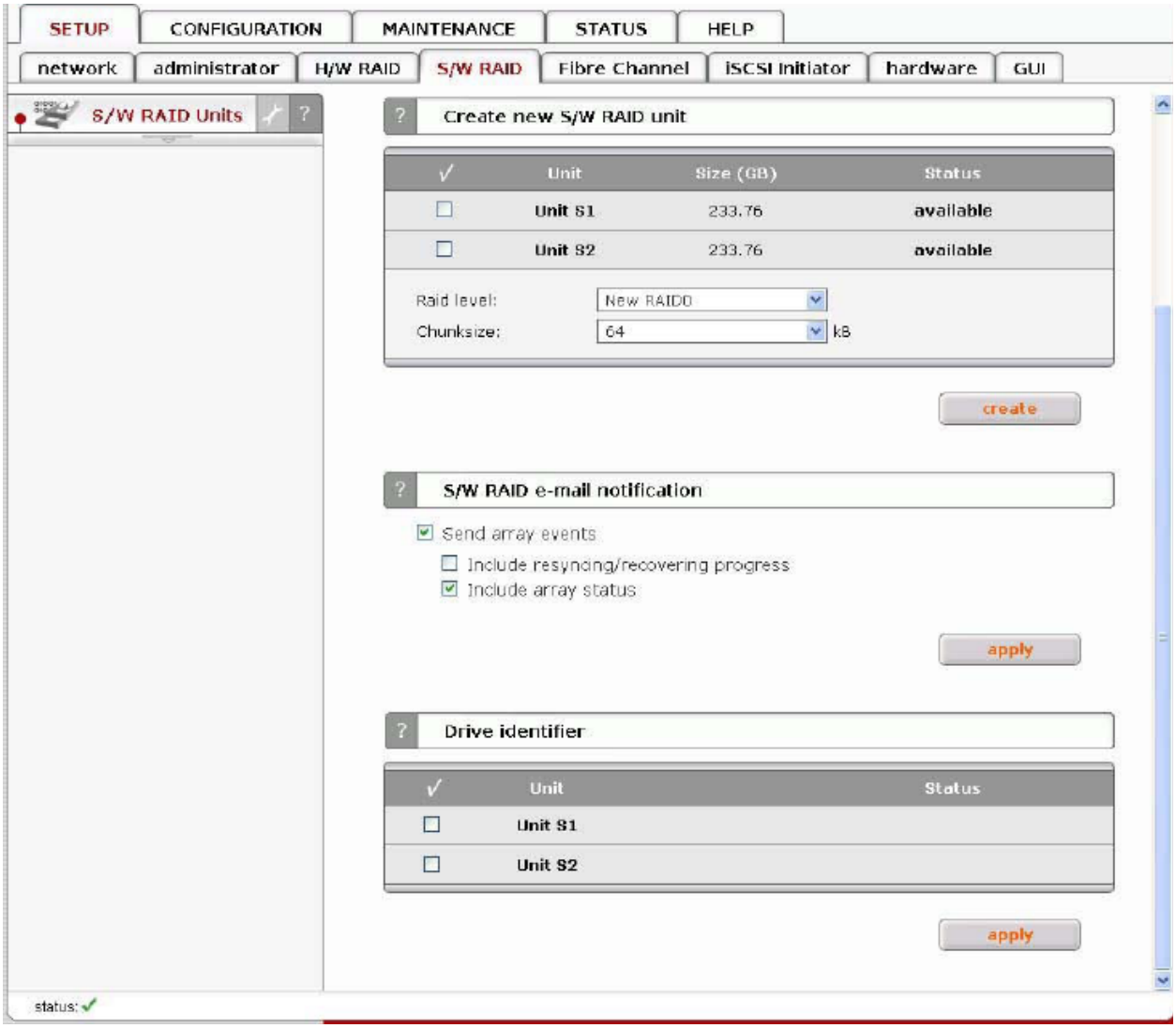
Function: Unit manager

This function enables you to manage physical storage devices - units (hard drives or raid-arrays). After adding a new unit you can define Logical Volume, swap, and space reserved for snapshot in Volume Manager function. Unit can be added only when it's not in use already.

Disk notations:

- S0,S1, ..., S[x] - every disk with S notation is one of SATA / JBOD / RAID units.
- H0,H1, ..., H[x] - units with H letter are IDE units.
- MD0,MD1, ..., MD[x] - this way are softRAIDs denoted.

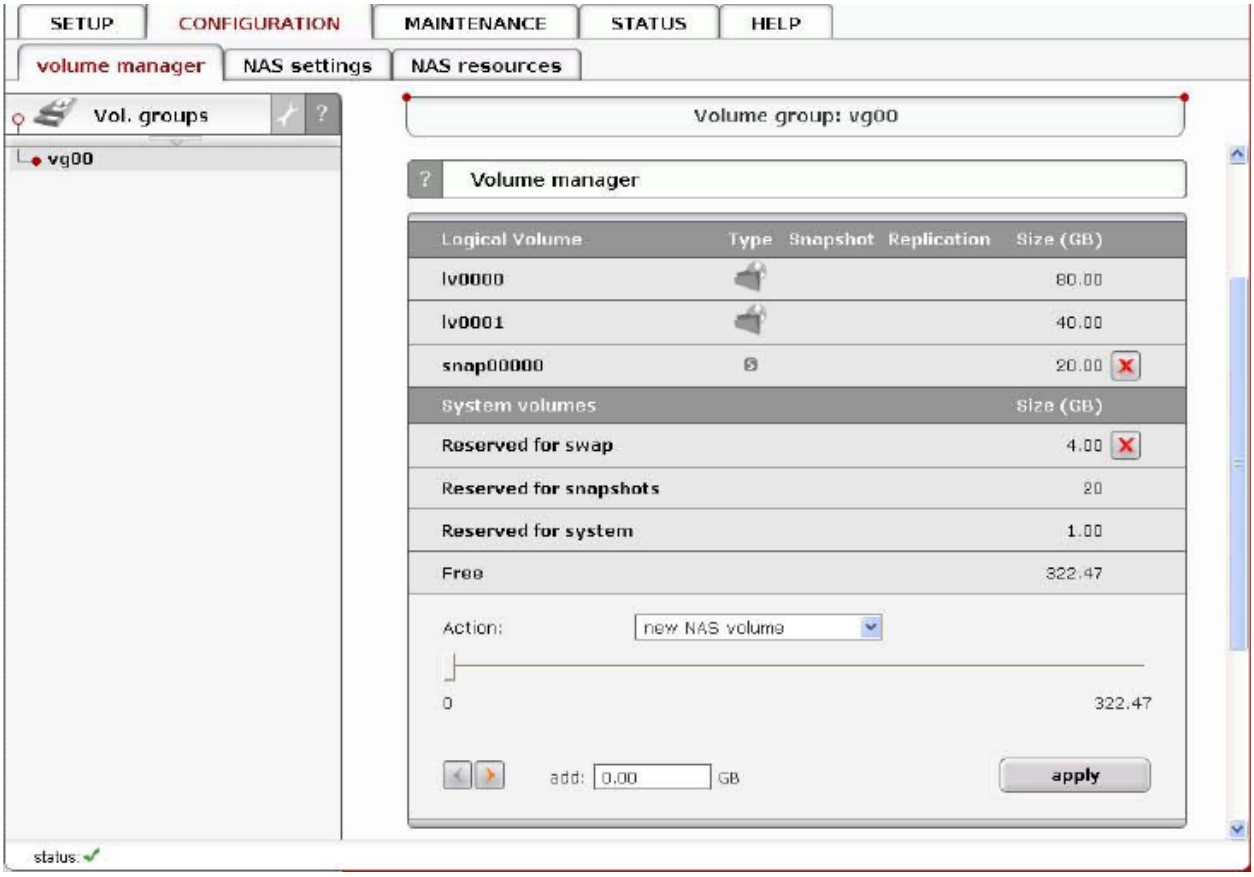
If the unit is already added, it can not be removed it in Web management. Units that are already used in a volume group can be made available again by using function Delete content of units under console (Ctrl+alt+x). Be aware that this will remove all data from a Unit! You can only use units with capacity greater than 5 GB, smaller units are not supported.



Function: Drive identifier

This function helps find disks in the cage of your NAS server. In case of hardware RAID installed, the whole RAID array is shown as a single drive. In this case you may not be able to determine which drive unit is which disk when using S.M.A.R.T. tool or hardware RAID management tool (depends on manufacturer of RAID controller).

When you click on "start" button then the appropriate disk will start reading and you can determine which disk is it by watching "disk-activity LEDs". For proper operation of this function there should be no other activity on hard drives. Identification will stop automatically after one minute if you will not stop it before (by unsetting appropriate checkbox and applying form). Using this function during normal operation is not highly recommended and will cause of your server to slow down.



Function: Units assigned

In this function you can view physical units attached to this volume group.

Function: Volume manager

This function allows:
- increasing existing and creating new NAS volume,
- reserving disk space for swap,
- creating, expanding and deleting snapshots

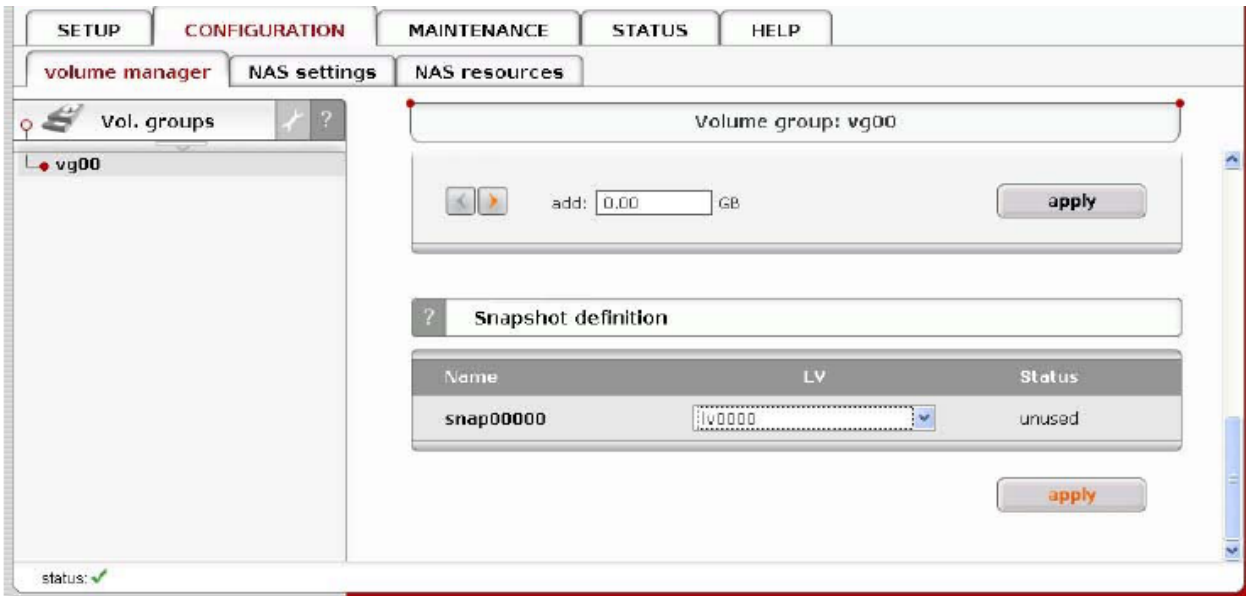
In order to add storage space to existing NAS volume, select "LV" from the dropdown menu. Use scroll bar to choose the size. While adding each new Unit there will be 4 GB space reserved for swap (if there is no swap already created). Additionally there is 1 GB space reserved for system internal use.

Function: Snapshot definition

This function allows you to define parameters of every snapshot.
You can set:
• Logical Volume, which the snapshot will be taken for.
• Schedule the time of automatic creation of the snapshot, if inactive - only manual snapshot activation is possible.
• RO - the snapshot will be visible as a write protected disk. The Snapshot function of the server enables the system administrator to freeze the data content of the volume at a certain time. From this moment on, the users work on a virtual data volume, all changes to the volume are stored in a different partition. The storage of all changes is independent of the file-system - it takes place on block-level. Only when the snapshot is deactivated / removed the changes are permanently transferred to the actual data volume. Snapshots can be activated/deactivated manually or automatically.

Please be reasonable, when you are calculating the space reserved for snapshots. Please set as snapshot size as much space as you expect to change during active snapshot.

E.g. when you are doing backup from snapshot which takes one hour please set this snapshot size to as much space that will be changed during one hour. The snapshot will become inactive if the content (data changed on Logical Volume) exceeds the snapshot capacity. You do not lose data in that case, just the dataset, which is virtual for the users at the moment, will be written to the data volume. The old dataset, which has been frozen with the snapshot, is not available any longer. When you define the schedule, use only as many snapshots in the same time as really needed. A large count of active snapshots can slow down the system considerably.
Manual creating and removing of snapshots can be done in the SETUP
volume manager vg[nr] Function: Volume Manager.

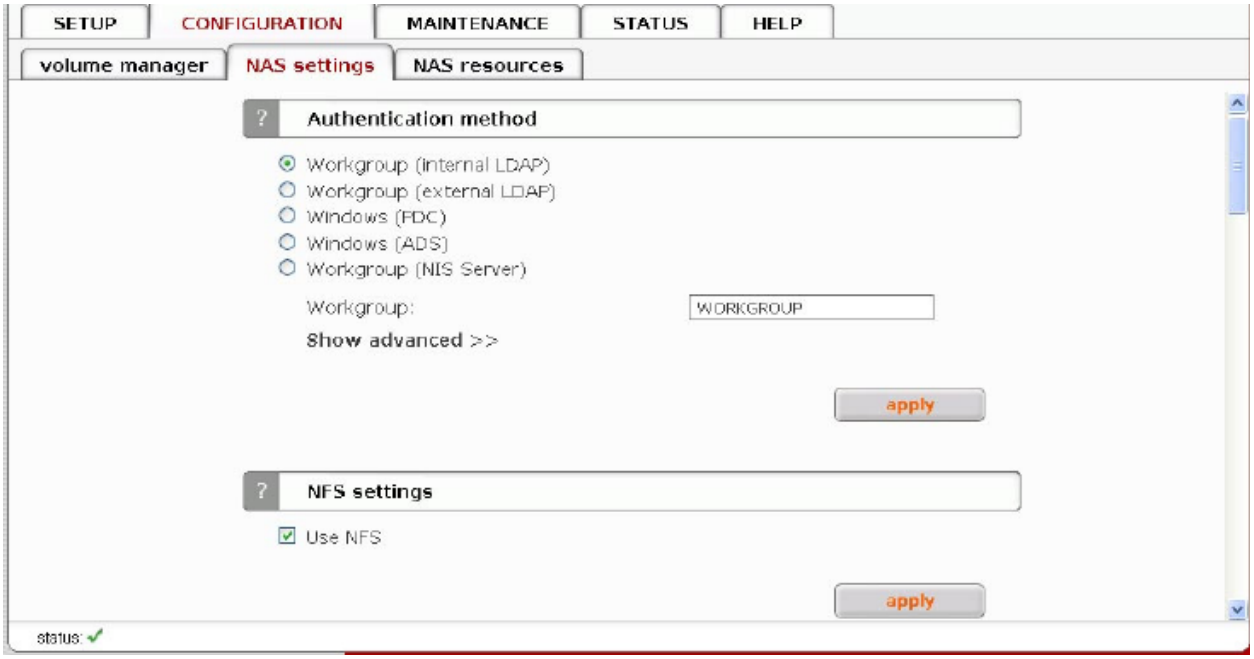


How to access NAS snapshot

After snapshot has been created and activated, you can access it by following:

• Go to menu CONFIGURATION NAS settings and select on which network protocol snapshots will be accessible. This need to be done only once. When creating access to snapshot on second time, this action is not necessary. You can activate access to snapshots on following protocols:,
• NFS,
• SMB(Network neighborhood),
• FTP,
• AFP.
• Create a new share that will be assigned to previous activated snapshot,
• Go to menu CONFIGURATION NAS resources,
• In function Create new share:,
• enter share name,
• Use option Specified path and select snapshot that you want to have access to,
• Click on apply button to create a share.
• Now you can start to explore your share(snapshot) using specified network protocol.

5.2.2.2 NAS settings



Function: Authentication method

The server administrator can choose one of following authentication method for users:

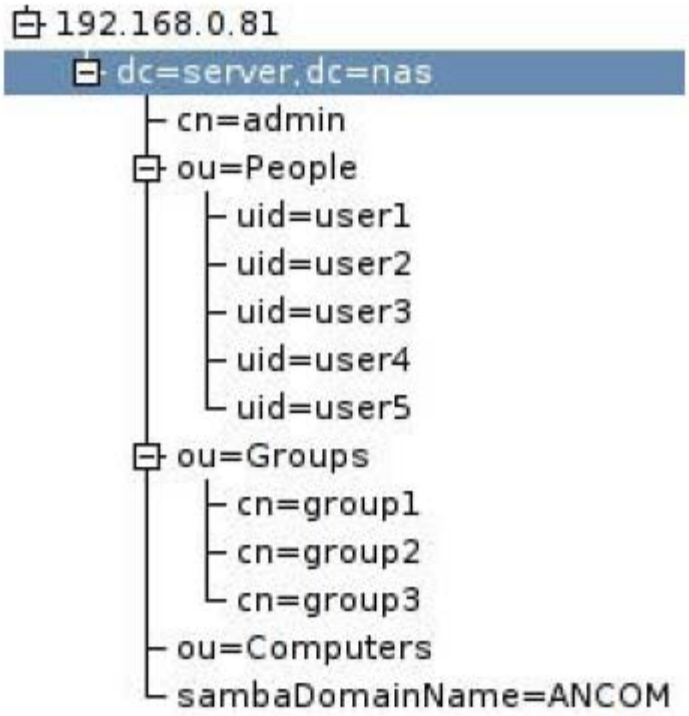
Workgroup (internal LDAP)

In this case you must create all users/groups accounts in resources menu. In the field Workgroup please enter your network workgroup name.

Workgroup (external LDAP)

In case of external LDAP (Lightweight Directory Access Protocol), the NAS server will use users/groups from external LDAP server. Please fill-in all fields accordingly. In advanced setting you can set Base DN, LDAP administrator DN (Distinguished Name) and LDAP administrator password. Base DN should looks like "dc=server,dc=nas" (DC - Domain Component), where "server" and "nas" can be set as they are set on remote LDAP server. In

LDAP administrator DN you should set previously entered base DN with prefix like "cn=admin," (CN - Common Name). Users should be stored in Organization Unit (ou) "People", groups in "Groups", and computers in "Computers". Sample organization can look like showed below:



Windows (PDC)

In this case NAS server will use Windows Primary Domain Controller user database for user authentication. This method can be used for NT4/2000/2003 servers. In case Windows 2000/2003 server run ADS native mode, please use Widows (ADS) method.
In case of PDC server running under NT4, please use following procedure if you experience problem to get connection:

1. Run Server Manager program from Menu Start Programs Administrative Tools (Common) Server Manager.
2. From Server Manager menu select Computer Add to Domain WARNING: If NAS resource is already added, you must remove it.
3. In Computer Name field enter NAS Server-Name (NetBIOS name).
4. Click Add button Set Windows (PDC) in NAS.
5. Next, in NAS server web administration: choose “CONFIGURATION” “NAS-Settings”.
6. Choose Windows (PDC) as Authentication method.
7. In Server IP field enter NT server IP address.
8. In Name & Password fields enter NT4 administrator account name and password
9. Click apply button. WARNING: If connection fails, the next try you must restart from point 1.

Windows (ADS)

This option can be used for Windows 2000/2003 ADS servers:

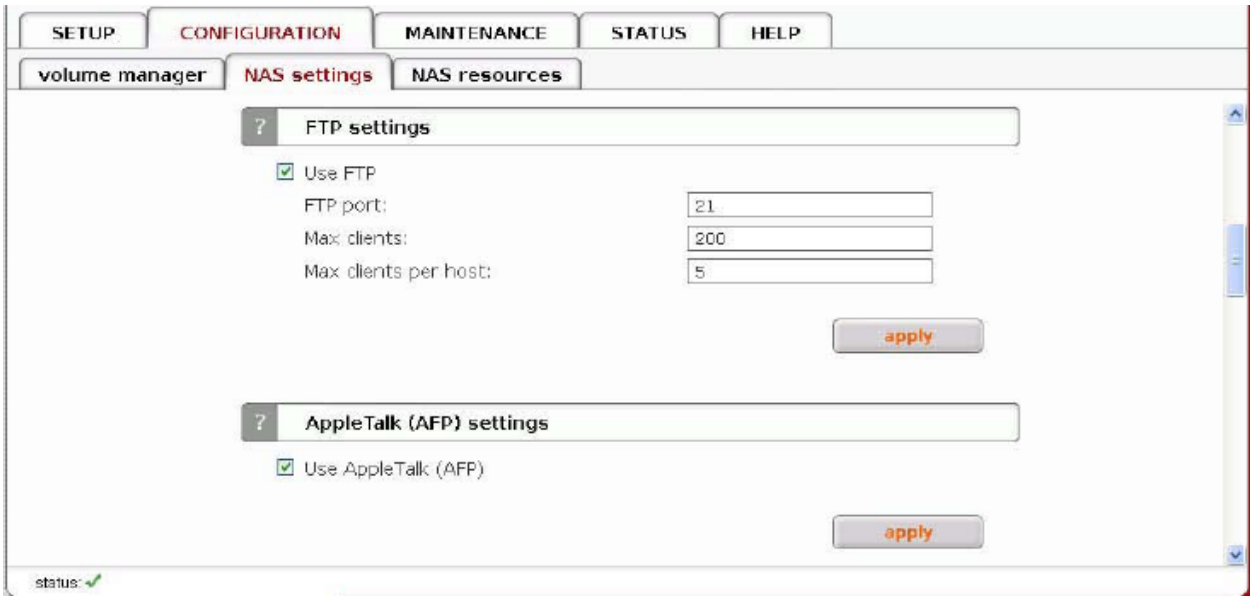
- Please enter Realm name of your Windows 2000/2003 server.
- It can be found under Windows system by clicking right mouse button on My Computer and selecting Properties, then clicking tab Computer name, Realm name is the Domain name.

• The KDC IP address must be taken from the same system as the Realm.
• Enter administrator login and password.
• Click "apply" to connect to Windows (ADS) domain.
• Workgroup (NIS server)
• Please choose this option in case user wants to use user/group database from Network Information Service server.

1. Workgroup name cannot begin/end with space and can not contain special characters like: ~!@#$^&()+[]{}*;:'".,%|<>?/\=`
2. Changing the authentication method may cost lost of ACL (Access Control Lists) In such a case please set users/groups access rights for every share and reset ACLs.
3. If smb authentication is enabled, please edit windows registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters\ and change the value of the key Dword 'enableplaintextpassword' to '1' hexadecimaly.

Function: NFS settings

Click “Use NFS” to enable access to shares and/or snapshot via NFS.
Network File System (NFS) is a protocol for distributed file system which allows a computer to access files over a network as easily as if they were on its local disks.
If host has entry in dns field but doesn't have reverse dns entry then connection to nfs will not work.



Function: FTP settings

To enable FTP services check use ftp.
FTP port - Provides port the FTP service is listening to.
Max Clients - Limits the total number concurrent ftp connections.
Max client per host - Limits the total number connections originating from a single host.
The option to access Server via FTP (File Transfer Protocol) offers additional flexibility, as users can access storage either from the Intranet or Internet. An FTP client is ideal (e.g., SmartFTP), but the Internet Explorer or a similar browser are also suitable.

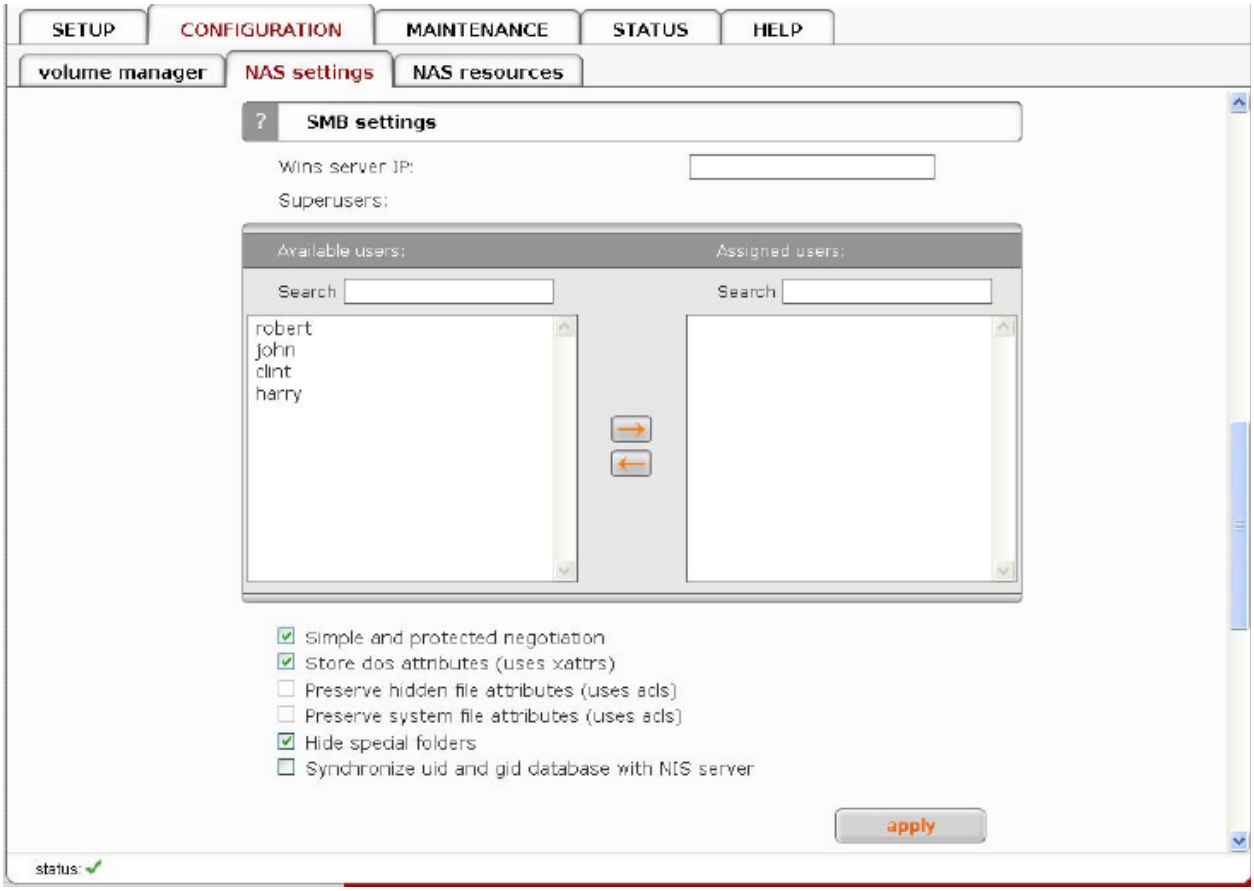
To establish a connection, the FTP client needs several pieces of data: IP address: 192.168.0.220 (this is the standard address) Port: 21 User: anonymous Password: 123. The allocation of access rights is done via the IP address of the PC currently in the process of accessing. A read access is, therefore, granted with these generally typical and anonymous login data. As a standard, server for FTP uses port 21, which can be changed in the configuration menu (If you use the Internet Explorer when accessing, you need to enter the following data into the entry line: ftp://192.168.0.220. You are not prompted to enter the user name and password, as the Internet Explorer first establishes as an anonymous connection. If you changed the FTP port, add this information to the entry line the following way: ftp://192.168.0.220:4711 (in this example, 4711 represents the new port number). In order to grant specific computers write access to the FTP area, enter the desired IP addresses into the line "IP address complete access"

Function: AppleTalk (AFP) Settings

Here you may activate the AppleTalk protocol in the network to access shares on the NAS Server.

How to use AppleTalk with the NAS server:

- In the setup -> NAS server enable AppleTalk,
- In setup ->NAS resources menu select a share that you want to be shared with AppleTalk,
- Enable AppleTalk for this share.



Function: SMB settings

This function allows you to edit SMB protocol specific parameters.
There are several options you can change:

Wins server IP

If you have a WINS server on your network then you should set this to the WINS server's IP.

Superuser

Superuser is a user, who has permission to take ownership of folder and files which belong to other users. It can be useful when administrator want to change access right (ACL) for folder or file established by other users. To give superuser privileges to a user pick them up from the menu. Superuser privilege allows modifying, removing and adding new files in the share, also to any files and directories that even those that the superuser has not got the ownership of.

Simple and protected negotiation

Simple and Protected Negotiation (SPNEGO) is a negotiation protocol. If you use PDA Device to access shares on NAS please uncheck it. For connect to your PDA Device use netbiosname, not IP address.

Store dos attribute (uses xattrs)

This option enables preserving all MS-DOS attributes using Linux xattrs attributes. It cannot be set when you are using option Preserve hidden file attributes or Preserve system file attributes.

Preserve hidden file attributes and Preserve system file attributes (uses acls)

These options enable preserving of MS-DOS attributes: hidden and system.
These attributes are mapped to x (EXECUTE) attributes for group and for others in Linux POSIX ACL. Windows ACL permissions are also mapped to Linux attributes. In order to avoid attribute mismatch, it is strongly recommended to disable these options. These cannot be set when you are using Store dos attributes option.

Hide special folders

This option hides special folders that are created by MAC OS/OSX systems.
Thanks to this, users can't see MAC OS/OSX system files by SMB protocol.

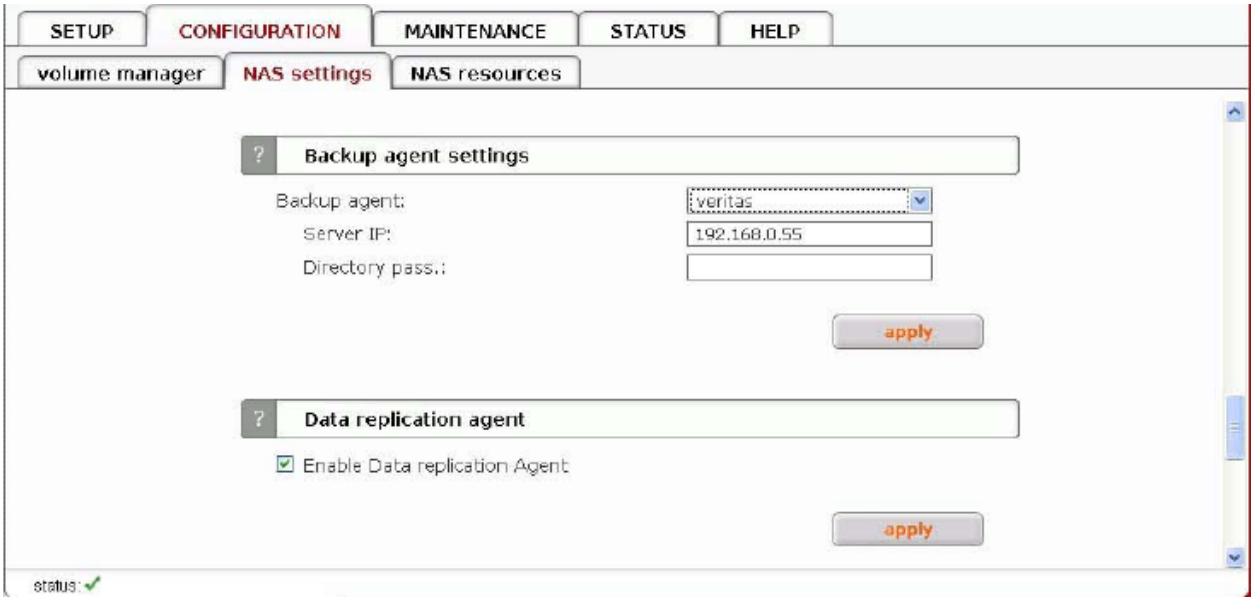
MAC OS/OSX system files:

1. .DS_Store,
2. .AppleDouble,
3. Temporary Items Network,
4. Trash Folder,
5. TheFindByContentFolder,
6. TheVolumeSettingsFolder,
7. .AppleDesktop,
8. .AppleDB,
9. Icon?,
10. .VolumeIcon.icns,
11. .FBIndex,
12. .FBClockFolder.

Synchronize UID and GID database with NIS server

This option allows synchronization UIDs/GIDs between NAS Server and NIS Domain. To have an properly working synchronization please fill: NIS server-domain name, NIS server IP and Synchronize interval.
Change of the acls and/or xattrs settings need to be accepted, because these changes can make the files will not be visible for user. Change of these settings is not recommended on severs that already have some data stored. If after changing of Preserve hidden file attributes

(uses acls) and/or Preserve system file attributes (uses acls) files are not visible, user can use command that will remove hidden attribute from files : attrib -S -H x:*.* /s /d ,where: x - network drive.
Any change in SMB settings will disconnect users that are currently connected. These also need to be accepted by user, acceptation form will only appear if any user is connected to SMB. If user click "cancel" button settings will be saved but connection to SMB will not be reseted.



Function: Backup agent settings

Here you can enable one of pre-installed backup agent (client). Currently, agents are supported:
- Veritas - Backup Exec,
- Dantz - Retroclient,
- CA - BrightStor.

If you enable the backup agent, your backup server will find the agent running on the NAS server and will use it for backup.
Alternatively, you can find and backup the NAS shares over the network neighborhood. But backup using an agent will be much faster.

Veritas:

Here you need to provide an IP address of a server running the Backup Exec. The "Directory Pass" is a password that the Backup Exec might prompt for.

Backup:

a. In Veritas Backup Exec set a user in the menu Network Logon Account Management,
b. Next enter the password such as earlier provided in the NAS Server function "Backup client setting",
c. By choosing "Backup" a "Backup Job Properties" window will appear,
d. A list of network shares will be shown in that window,

e. By clicking on the "Remote Selections" branch, and next on "Unix Agents", a NAS server name will appear,
f. After clicking the server "NAS_server/logical volume", a window "Logon Account Selection" will be displayed where you need to choose the same user name as in the point "1". In some settings, the window "Logon Account Selection" will not appear automatically. In this case you must right mouse click on the name "NAS_Server/share_volume", and then in the context menu choose "Connect As...". Only then the "Logon Account Selection" window will appear.
g. After choosing a user, the "Logical Volume" and NAS server shares will appear. By selecting the correct share and clicking the "Run Now" button, selected shares will be backed-up.

Restore:

a. By choosing "Restore", a "Restore Job Properties" window will appear.
b. On the left side of the window, in Properties Source click "Selection", and the name of the NAS server which shares were earlier backed-up will be displayed.
c. Choose a folder you want to be restored from the correct backup file.
d. From the Source Resource Credentials menu choose a user account for the NAS (NAS_server/ share_volume) server and click the "Run Now" button. In order to use a Incremental method, choose it from the Setting General Backup Method menu. Please use method "Incremental - Using modified time" (Reset Archive bit - does not work on the XFS partition types).

BrightStor:

Allow IP or Network IP:

Please enter the Backup server's IP address in order to grant access to the NAS. If you leave this field empty, all BrightStor backup servers in the network will have access to the NAS server.

User:

By providing a user name, only this BrightStor user will have access to the NAS. If left empty, all users will be able to access the NAS server. Before you'll start to backup your data, you have to configure device that backup will be made to and add your NAS server as source. Please follow these steps in order to complete it.

a. From menu bar chose Configuration, then Device configuration. Device configuration wizard will appear, it will help you to configure backup devices on your server.
b. Chose Windows Server and click button Next.
c. From options select File System Device and click Next.
d. Click on Add button, File System Device will be added to the list.
e. Click on Location field from newly created entry and select path that will be mapped to File System Device.
f. Click on Finish button to complete Device configuration wizard.
g. Click Exit to quit Device configuration.
h. The last thing to do is to format your newly created File System Device. In order to do it select Device from Quick start menu, select your newly created File System Device.
i. Click on Format button, format form will appear.
j. Enter media name and click OK to format media.

Configuration of NAS server:

a. From Quick start menu, select Backup.
b. From branch Source, select Unix/Linux Systems and click on it with right mouse button
c. Select Add Machine/Object. Add client form will appear.
d. Enter host name and IP address of your NAS server.
e. Click on button Add in order to add your NAS to the list.
f. Click on Close to quit Add Machine/Object form

Backup:

a. From Quick start menu, select Backup.
b. From branch Source, select your NAS server volumes that you want to backup.
c. Click on Start button, Security and agent information form will appear.
d. Click on Agent button if you want to modify NAS server information
e. Click OK button, Submit job form will appear.
f. If you want to start backup process later make sure that Job Execution Time is properly set.
g. Enter job description, click OK to start backup process

Restore:

a. Form Quick start menu, select Restore.
b. From branch Source, select your NAS server volumes that you want to restore.
c. Click Start button and then OK, Submit job form will appear.
d. If you want to start backup process later make sure that Job Execution Time is properly set
e. Enter job description; click OK to start restore process.

Retroclient:

Configuration of NAS server:

1. From menu, select Configure, then click on Clients, Backup Clients form will appear.
2. Click on Add button, Add backup client form will appear.
3. Enter IP address of your NAS server and click on Add button, connection form will appear.
4. Enter password to connect to NAS server and click Ok. Password for Dantz Retroclient is set to "admin". NAS server is now properly configured to work with Dantz Retroclient.

Creation of backup sets:

1. From menu, select Configure, then Backup sets, Backup sets form will appear.
2. Click on Create New button, Backup sets creation wizard will appear. Click on Next.
3. From backup media options, select File and click on Next.
4. Enter name and location where backup will be made. Click on Next.
5. Select backup set security and click Next.
6. Click on Finish button, Backup set creation process is completed.

Backup

1. From menu select Backup, then click on Backup button. Source selection form will appear.
2. Select NAS server volumes from which you want to make backup. Click on Ok.
3. Backup process form will appear, click on Backup to start backup process.

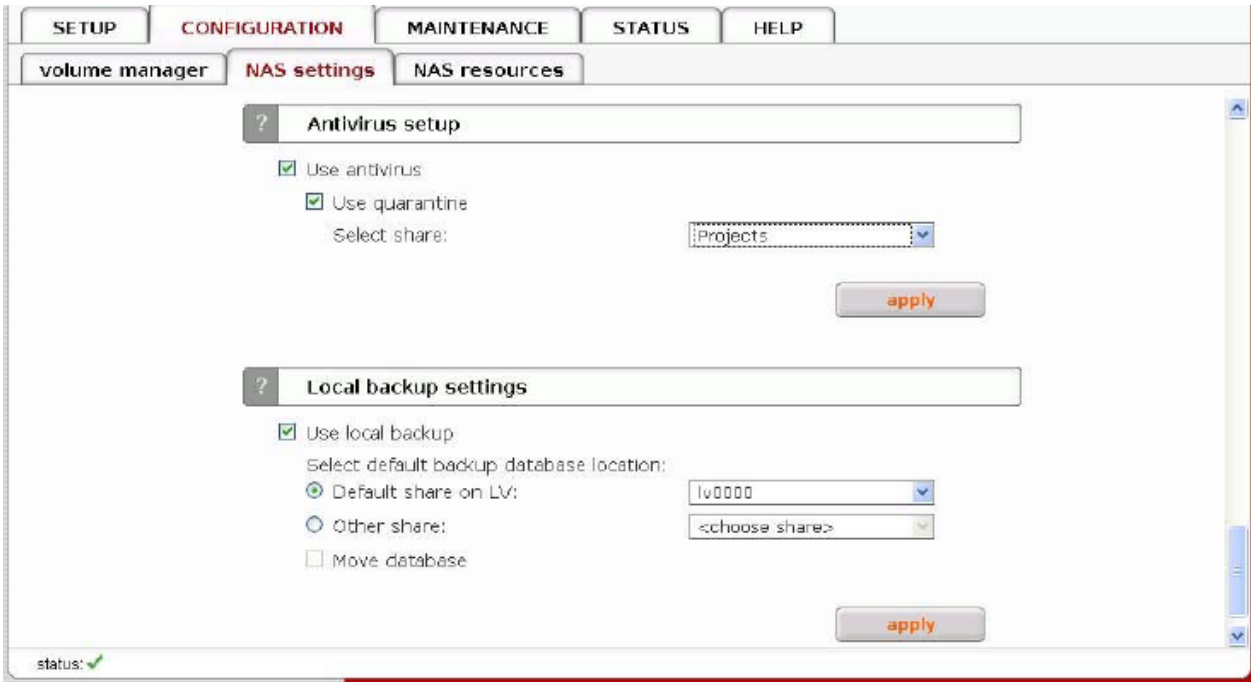
Restore

1. From menu select Restore, then click on Entire volume button.
2. Select source backup set from which you want to make restore process.

3. Select destination NAS server volume.
4. Click on Ok button, then click on Replace to begin restore process.
5. Password for Dantz Retroclient is set to "admin".

Function: Data replication agent

This function enables the Data replication agent. This is necessary to replicate as destination share



Function: Antivirus setup

This function provides Antivirus protection for your data. Antivirus scans the following file types:

- Archives and compressed files:,
- Zip,
- RAR (2.0),
- Tar,
- Gzip,
- Bzip2,
- MS OLE2,
- MS Cabinet Files,
- MS CHM (Compiled HTML),
- MS SZDD compression format,
- UPX (all versions),
- FSG (1.3, 1.31, 1.33, 2.0),
- Petite (2.x).
- Mail files,
- MS Office document files,
- executables files.

The feature quarantine allows you to choose, whether you want to move the infected files to default folder (quarantine dir), automatically created in shares, or option manual which allows you to choose the place of quarantine, in previously created share (in example share named "Quarantine"). If there is no option "quarantine" you will be only informed about the infected file. To verify the information about the infected files look in logs. You will get the info which files are infected and with what viruses.

Function: Local backup settings

This function enables local backup functionality.

Use default share on LV

With this option you can store database of all backups on default share on selected logical volume.

Use other share

With this option you can store database of all backups on selected share.

Move database

If this option is checked then existing backup database will moved to selected share.
If selected share has any other files then backup database files, then it will not be possible to create a backup database in that share. If you want to create a backup database in that share anyway, you have to first delete files from that share. You can only move a backup data base between default share on logical volumes and between other shares. You cannot move a backup database from a default share on LV to other share.

5.2.2.3 NAS resources

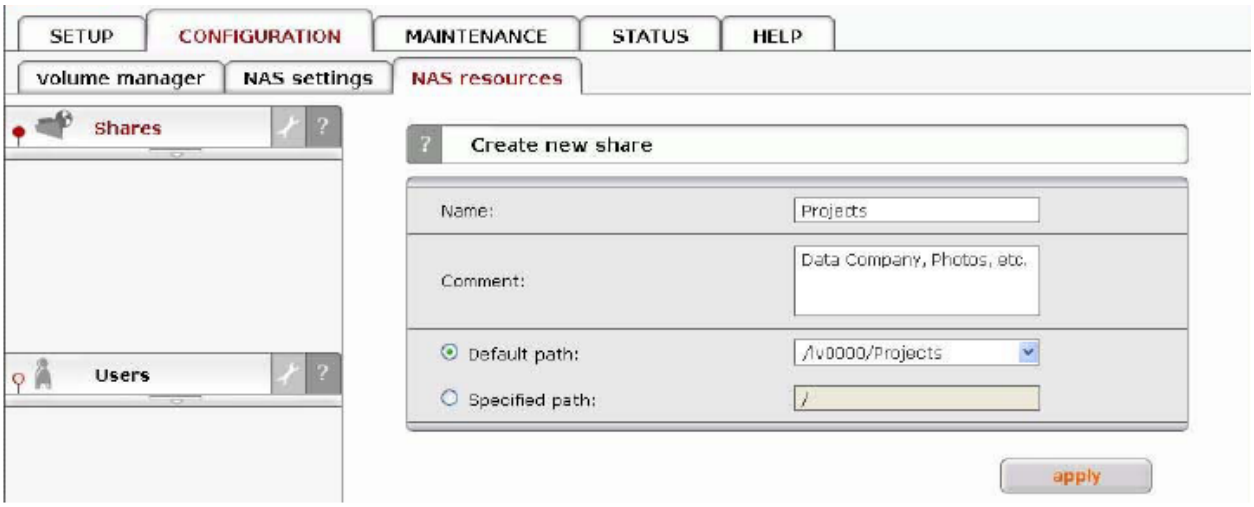
Here, you can configure NAS resource operations. All that may be accomplished by using tree diagrams on the left side. This will help you manage all shares, users, user groups in a structured manner.

5.2.2.3.1 Shares

Here, all shares on your uNAS/tNAS are listed. By clicking on “Shares,” with Function “Create new share” you can define a new share or comment it (optional) or set the path. Organized below, you will find all existing shares, which you can edit with a simple click. With the exception of the name, you may alter all parameters. If, however, you must change a name, delete it and assign a new name.

Windows users will see the name of the share in the folders of their network environment when they click on the icon for the uNAS/tNAS server. The comment is only visible if the users take a look at the share properties, or if shares are listed in detail.

The path represents the physical location of the data on the share volume of the uNAS/tNAS. The user does not know this information. In order to simplify navigation through the directories, you can use the browser function.

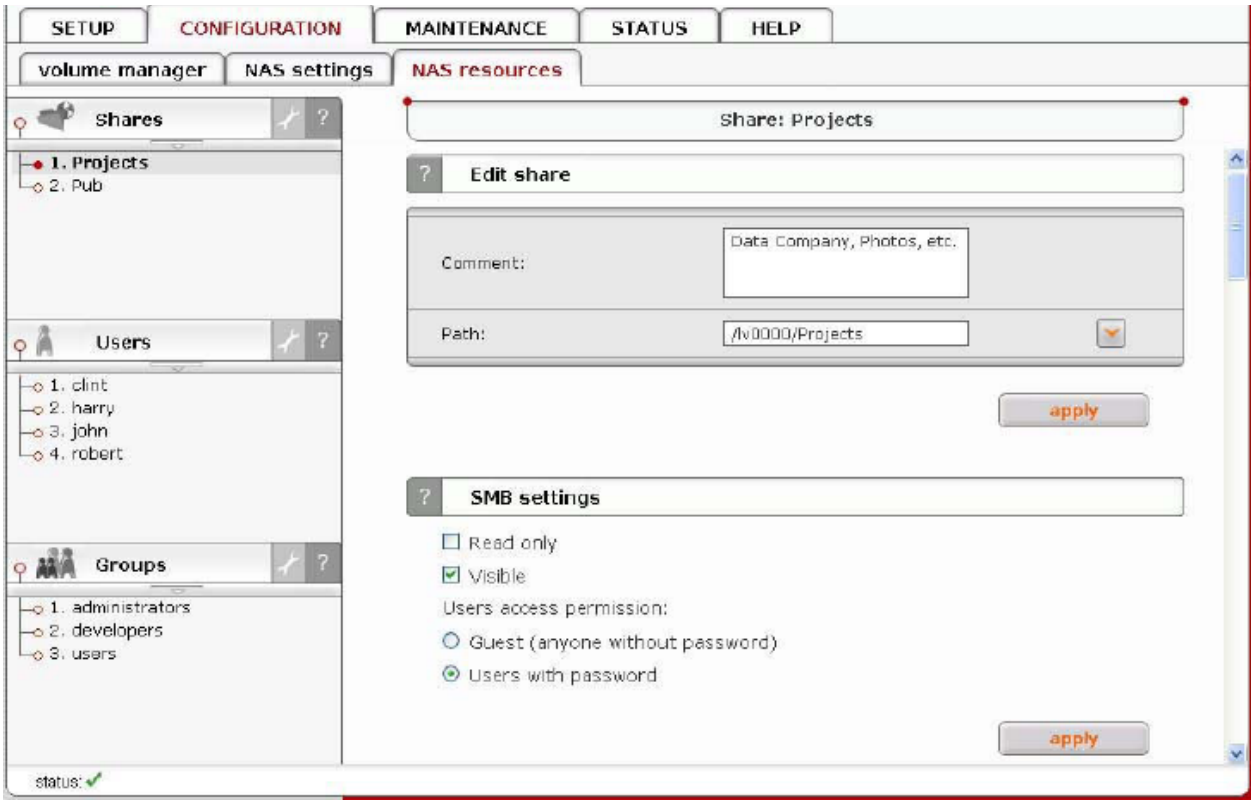


Function: Create new share

To create a share, enter the share name, comment (optional) and set the path.
To use default path to share, leave the checkbox Default path checked. If you want to use specified path, please check the checkbox Specified path and select path to share.

- Please do not use spaces and special characters like: ~!@#$^&()+[]{}*;:'".,%|<>?/\=`,
- The workgroup/domain name that was configured in the NAS has to match with the network settings. Otherwise, the configured shares are not visible in the network environment. If you made changes to the workgroup and server name in the NAS configuration, it can take some time until each workstation computer in the Windows network detects the new name.

After clicking “create” button on left page, will appear the name of earlier established share, in this case “Projects”. Then by clicking on name “Project”, you will see all available functions helpful for setting the share:



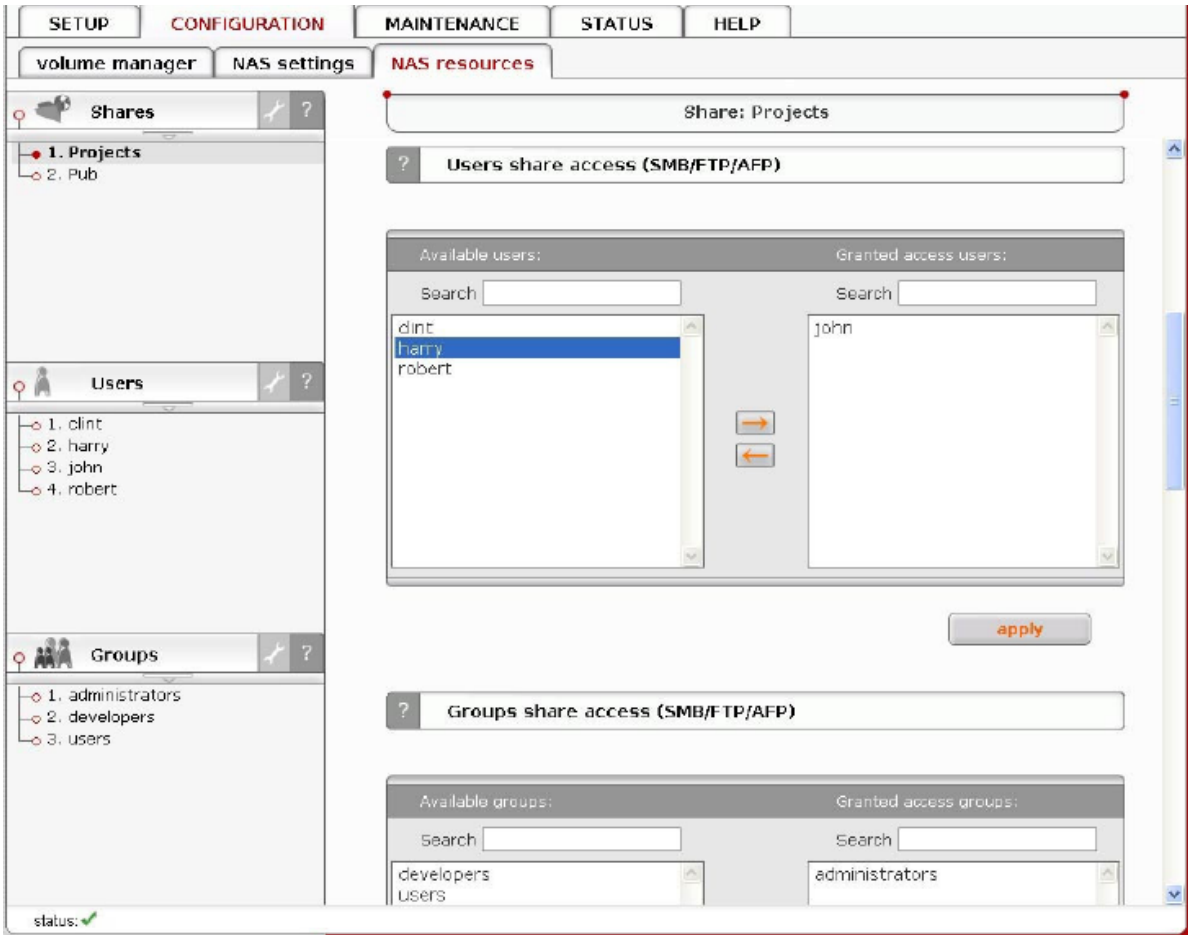
Function: Edit share

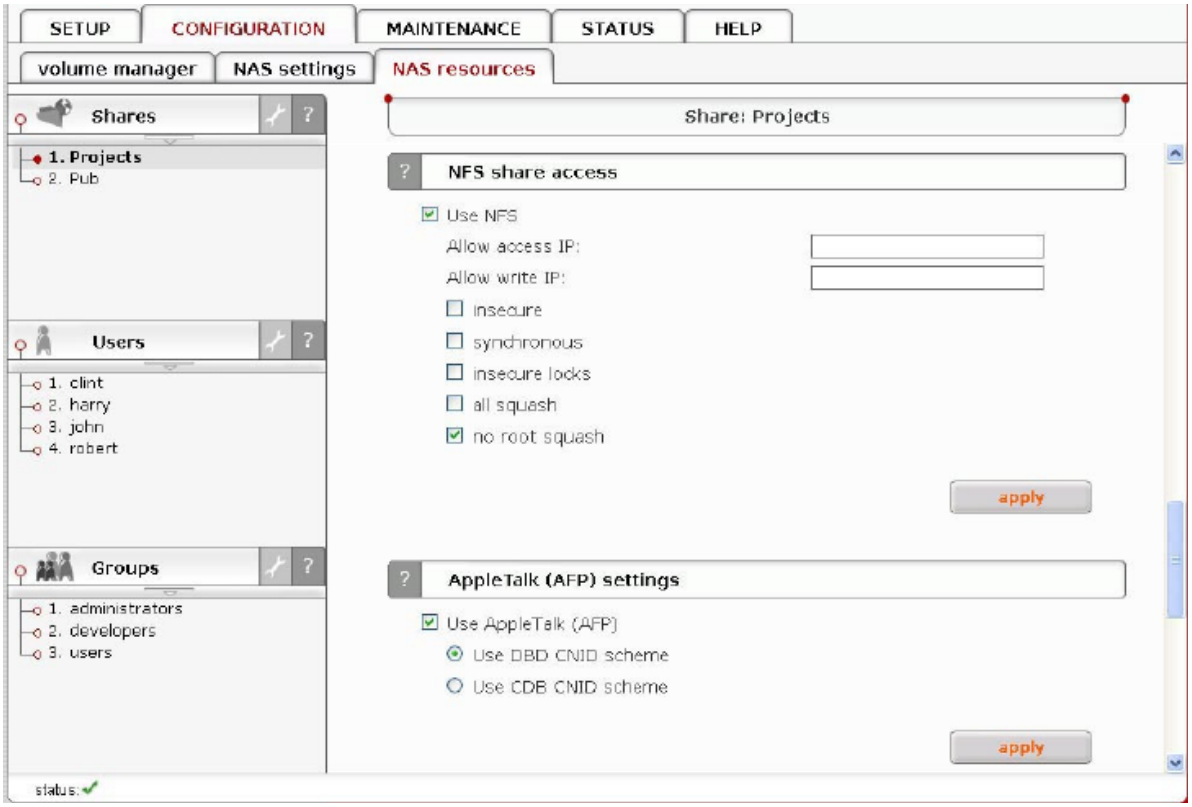
Here you can edit the path for a share, add or delete directories. You can also view files in directories by click on button.

Function "SMB Settings"

This function allows you to change SMB protocol settings for this share. Please check Read only to restrict the access to read-only operation. Uncheck Visible to hide the share in the browse list. Select Guest to allow anonymous access to the share. Select Users with password to enforce user authentication.

In Functions "Users share access (SMB/FTP/AFP)" and "Groups shareaccess (SMB/FTP/ASP)" you can set the access to the shares to available users and/or groups.


SETUP
CONFIGURATION
MAINTENANCE
STATUS
HELP
volume manager
NAS settings
NAS resources
Shares
1. Projects
2. Pub
Users
1. clint
2. harry
3. john
4. robert
Groups
1. administrators
2. developers
3. users
Share: Projects
Users share access (SMB/FTP/AFP)
Available users:
Granted access users:
Search
clint
harry
robert
john
apply
Groups share access (SMB/FTP/AFP)
Available groups:
Granted access groups:
developers
users
administrators
status:


SETUP
CONFIGURATION
MAINTENANCE
STATUS
HELP
volume manager
NAS settings
NAS resources
Shares
1. Projects
2. Pub
Users
1. clint
2. harry
3. john
4. robert
Groups
1. administrators
2. developers
3. users
Share: Projects
NFS share access
Use NFS
Allow access IP:
Allow write IP:
insecure
synchronous
insecure locks
all squash
no root squash
apply
AppleTalk (AFP) settings
Use AppleTalk (AFP)
Use DBD CNID scheme
Use CDB CNID scheme
apply
status:

Function: “NFS share access”

Using this function you activate access to particular share via NFS. In order activate NFS on uNAS/tNAS server, you must enable usage of NFS in menu “SETUP” ”NAS settings” in Function NFS settings.

In order to mount this share via NFS, please use following syntax:

- mount -t nfs IP_addr:/share/share_name /local_mount_point

Word share is a key word and must be always added to the syntax.

In order to mount a in synchronous mode please use:

- mount -t nfs IP_addr:/share/share_name /local_mount_point -o sync

In order to mount a share in asynchronous mode please use:

- mount -t nfs IP_addr:/share/share_name /local_mount_point -o async

When using synchronous mode, data is not stored in buffer, but transferred at once. In asynchronous mode the data is first stored in a buffer and then transferred.

You can use following NFS option fields:

Allow access IP

Please enter an IP or address range that is allowed to access NFS. You can enter single IP or multiple IP separated with semicolon or IP address range. IP addresses that will not be added to allow write list will have read only access.

Allow write IP

Please enter an IP or address range that is allowed to write to NFS. You can enter single IP or multiple IP separated with semicolon or IP address range.

insecure

Allows incoming connection to originate from ports > 1024

synchronous

When this option is enabled, local file system is waiting for the data to be written to the NAS server. NFS performance will be lowered, however it will ensure that the data will be written directly to the NAS server and will not be stored in the system cache.

insecure locks

Disables authorization of locking requests. Some NFS clients don't send credentials with lock requests, and hence work incorrectly with secure locks, in which case you can only lock world-readable files. If you have such clients you can use the insecure locks option.

all squash

Map all users id to nobody user and all groups id to nogroup group.

no root squash

Please select this option to grant user root from a client machine, the same level of access to the files on the NAS server. Otherwise user root from a client machine will be mapped to user nobody on the NAS server. When you leave allow access IP and allow write IP fields blank, then all computers in subnet will have write access to NFS. When you set allow access and leave allow write IP field blank, then specified computers will have read only access and none will have write access. When you set allow write IP without allow access IP, then specified IPs will have write access and all computers in the subnet will have read only access.

- xxx.xxx.xxx.xxx
- xxx.xxx.xxx.xxx;xxx.xxx.xxx.xxx; ....
- xxx.xxx.xxx.xxx/network_prefix_length.

If host has entry in DNS field but doest have reverse DNS entry then connection to nfs will not work.

Function: AppleTalk (AFP) Settings

Here you may activate the AppleTalk protocol in the network to access shares on the NAS Server.

How to use AppleTalk with the NAS server:

- In the “SETUP” “NAS settings” enable AppleTalk,
- In “SETUP” “NAS resources” menu select a share that you want to be shared with AppleTalk,
- Enable AppleTalk for this share.

'"How to connect to the NAS AppleTalk server:"'

In MAC OS 9:

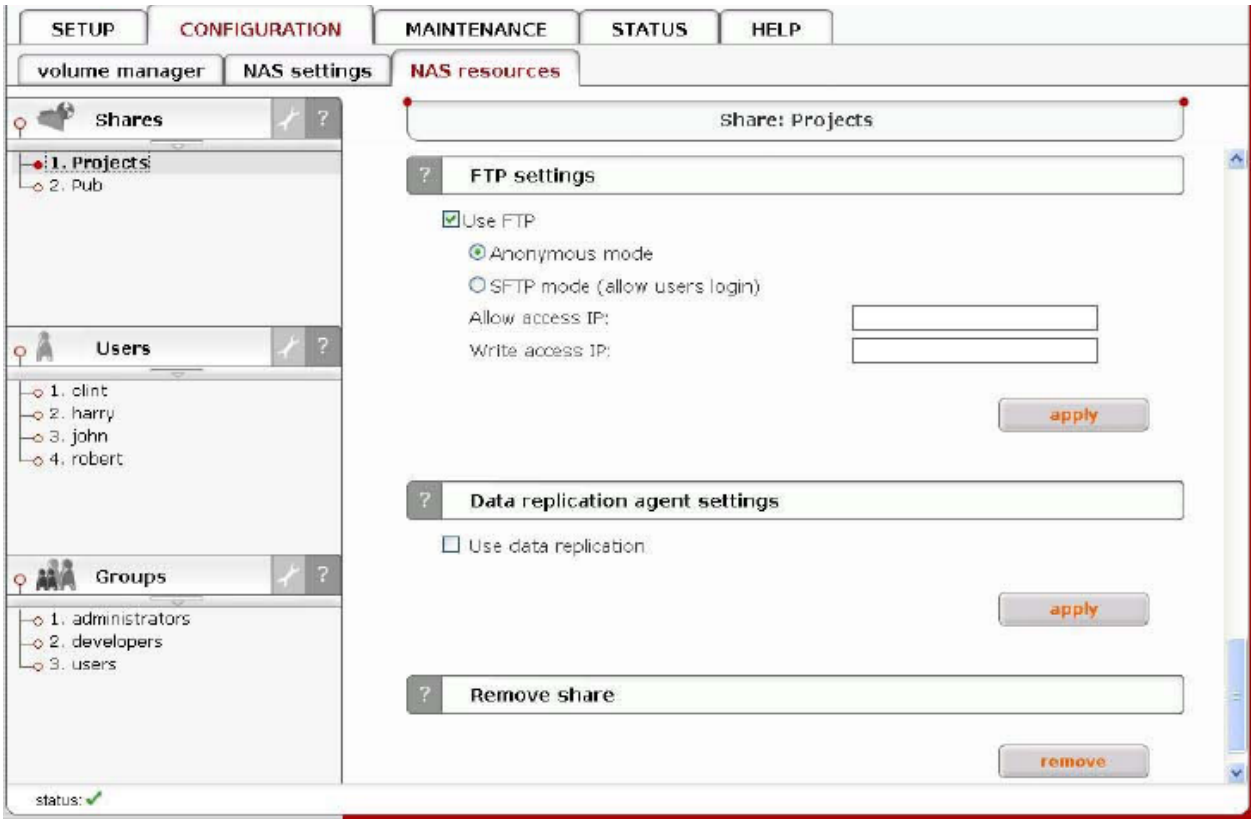
- Open the Chooser (APPLE MENU Chooser),
- Click on AppleShare,
- If the Server "NAS" does not appear in the fileserver list click "Server IP address" and enter the NAS server IP,
- Click "OK" and choose a login type. Enter a user name and password if you want to login as a specified user,
- From available options select shares that you want to mount,
- The icon of the mounted share will appear on the desktop,
- To open the share click on its icon,
- To unmount the share drop its icon onto the trash.

In MAC OSX 10.3:

- Click on the MAC HD, then Applications then Utilities,
- From the Directory Access check if AppleTalk is active; if not activate it,
- If the server "NAS" does not appear in the Network list, open a web browser and enter the IP address of the AppleTalk server. afp://192.168.1.3 (very important "afp://"),
- Choose a login type. Enter a user name and password when you want to login as a specific user,
- If you can not log in, click on the Directory Access/Authentication and change the path to search for authentication information,
- From available shares select all you want to mount,
- The icon of any mounted share will appear on the desktop.

or second example is:

- Click on "Connect to server" from the Finder (GO submenu),
- Enter: afp://address_ip,
- You can add a link to the AFP server by clicking on the "+" sign. This adds a link to the computer in the Favorite Servers field,
- Choose a login type, enter a password if you want to login as a specific user,
- From available shares select all you want to mount,
- The icon of the mounted share will appear on the desktop.



Function: "FTP Settings"

You can enable FTP services for every share separately. You can choose :

- Anonymous,
- SFTP (Secure FTP).
- Selecting Anonymous mode will enable FTP sharing with anonymous user. For all IPs the access is set to READ+WRITE by default. To change that, activate Allow access IP and Write access IP options. Clicking apply will make the share available over FTP.
- To connect to this share a FTP client software is required – i.e. Internet Explorer has the FTP support. To connect from IE, when using Anonymous mode, please use following syntax:
- ftp://<NAS IP>/pub/, (e.g. ftp://192.168.0.220/pub/).

When using SFTP client, please use:

- ftp://<NAS IP>/share/, (e.g. ftp://192.168.0.220/share/).

Many FTP client programs need a user name and a password to establish connection. In the Anonymous mode the user name is "anonymous" and there is no password (empty field). All anonymous shares are in the "share" folder. Any user connecting from the IP without a full access will see all shares but will not be able to see any directories that are prohibited.
For Anonymous login please use e-mail address as password. Anonymous user will see only files and directories that he owns. Selecting SFTP mode will enable secure FTP sharing with the user and password authorization. Only few FTP clients support SFTP, and even fewer SFTP clients support SSL/TLS encryptions.

Here is a list of the tested software:

• CoreFTP (Windows),
• FileZilla (Windows),
• IgloFTP (Windows and Linux),
• SSLFTP (Linux console client).
When SFTP is enabled, the user has the access to the share through the authorized user name and password.

If the NAS server uses Windows domain authorization then a short name of the domain must precede a user name – connected with a plus sign, i.e. “DOMAIN+Administrator”.

To connect to a share via SFTP, in the selected encryption, type in SFTP client NAS support SSL and TLS explicit encryption. All SFTP shares are in the “shares” folder. Users see only the allowed shares.

If you are unable to see any directories when connected to ftp server please make sure that you have rights to access any share over ftp. If still you cannot see any directories please change your ftp client to passive mode.

Most FTP clients have bookmarks allowing to set up IP, port home folder, etc. Suggested home folder for the Anonymous is “pub” and for SFTP is “shares”.

Function: Data replication agent settings

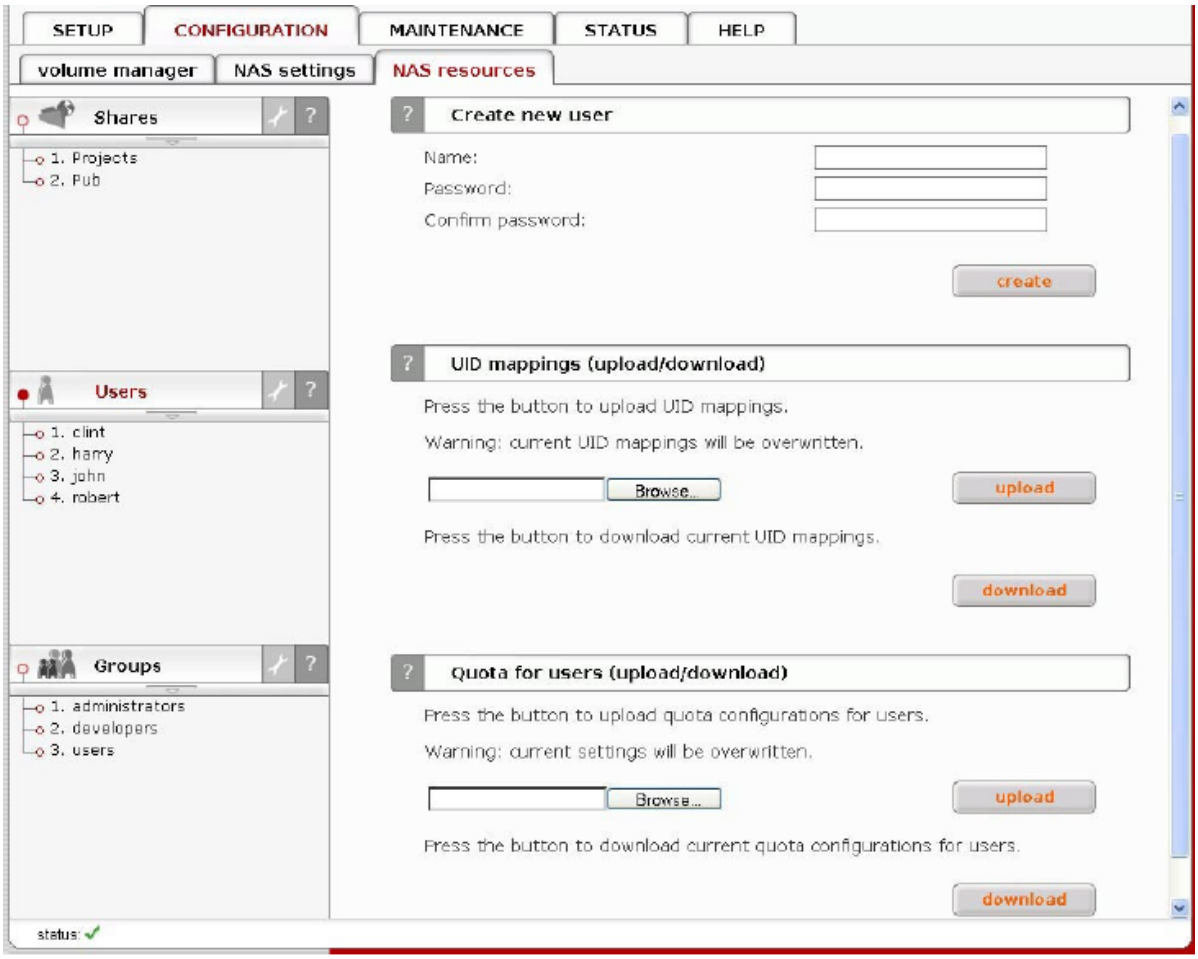
This function allows you to set configuration for a data replication of the share. In order to enable replication for a share, check box Use data replication.
It is recommended to set Login name, Password and list of Allow access IPs that have access to the share, in another case everyone will have access to the share.

Function: Remove share

Click "remove" button to remove the share.
No data (directories and files) will be deleted on the logical volume. You can re-create deleted share any time. Just go to NAS resources menu, click on Shares (as you create new share), browse directories structure to find the folder you want to assign the share. Finally in the field Name please enter your share name and click on "apply" button. Now you will find again the deleted share in your network neighborhood.

5.2.2.3.2 Users

In the mode “Workgroup internal LDAP” the category “Users” serves as data entry mask for user accounts. In principal, the process is the same as when you create shares. Enter new users here and assign each of them a name and a password. For security reasons, you have to enter the passwords twice.
User name cannot:
• contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " ., ; % | < > ? / \ = `,
• begin or end with a space.
• Password cannot:
• contain characters: ' " `,
• spaces.
If users forget their password, there is no way to retrieve it. You can only set a new password.



Function: Create new user

To create user, enter name, password, retype password and press create button.
User name cannot:

- contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " ., ; % | < > ? / \ = `,
- begin or end with a space.

Password cannot:

- contain characters: ' " `,
- spaces.

If users forget their password, there is no way to retrieve it. You can only set a new password.

Function: UID mappings (upload/download)

This function allows you to upload and download UIDs (users IDs).
Using this function you are able to change a lot of users ids at one time.

To upload UID:

- In resources menu create share settings (on lv00),
- Copy configuration file uid_mappings.csv (format:user_name;uid) into settings folder. This file should be in UTF-8 encoding,
- Press "upload" button to import uid mappings,

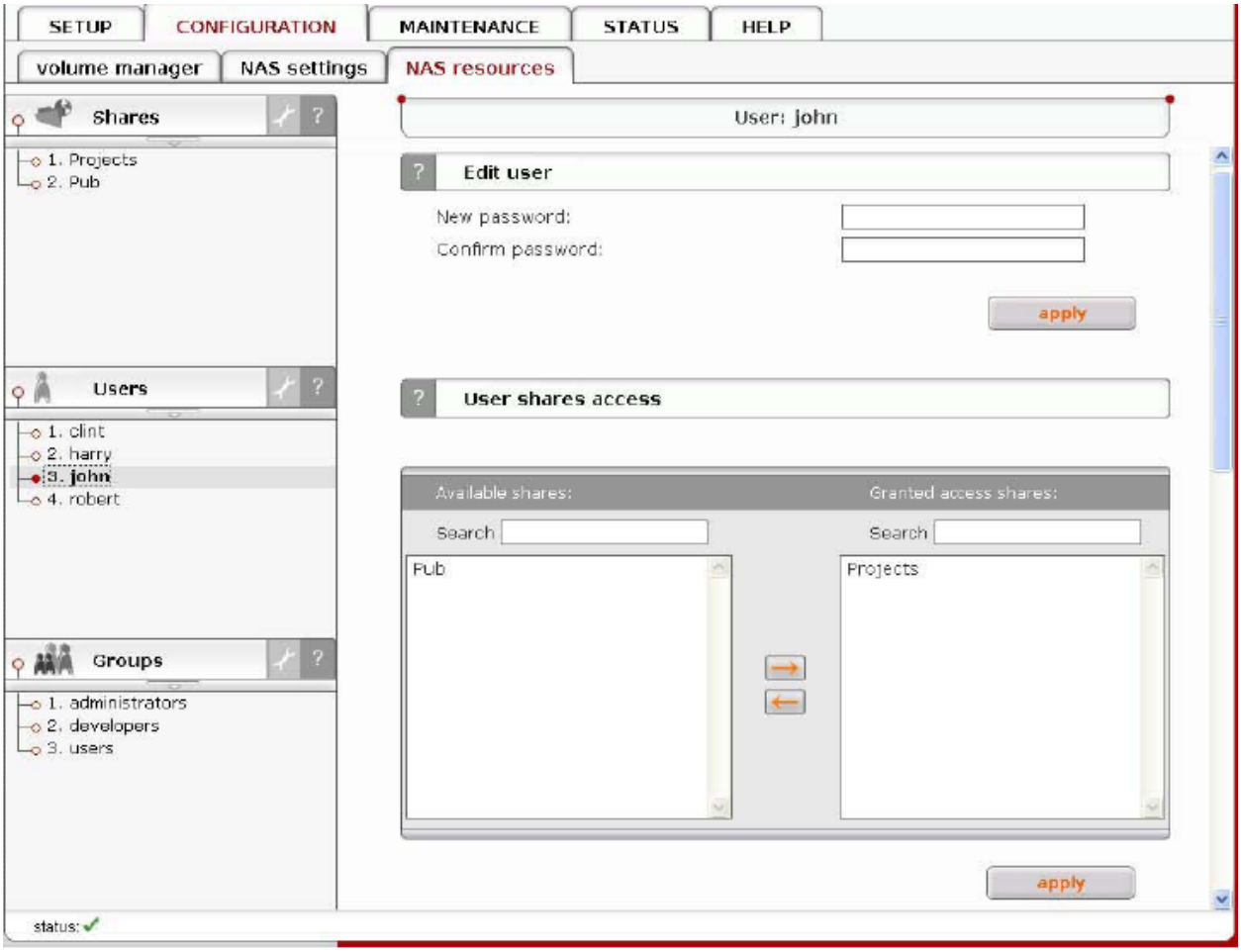
• If there will be some errors while importing uids please read uid_mappings_import.log file in settings share.
Warning: current uid mappings will be overwritten. Press "download" button to download uid_mappings.csv.

Function: Quota for users (upload/download)

This function allows you to upload and download quota (users quota).Using this function you are able to change a lot of users quota at one time.

To upload quota

• In resources menu create share settings (on lv00),
• Copy configuration file quota_users.csv (enconding: UTF-8; format:user_name; hard_quota-in kbytes) into settings folder,
• Press the button to upload quota configurations for users,
• If there will be some errors while uploading quota please read quota_users_import.log in settings folder.
Warning: current settings will be overwritten. Press "export" to download quota_users.csv.
Then by clicking on name e.g. “john”, you will see all available functions helpful for setting the user:



Function: Edit user

To change user password enter and confirm password, and press "apply" button.

Password cannot:

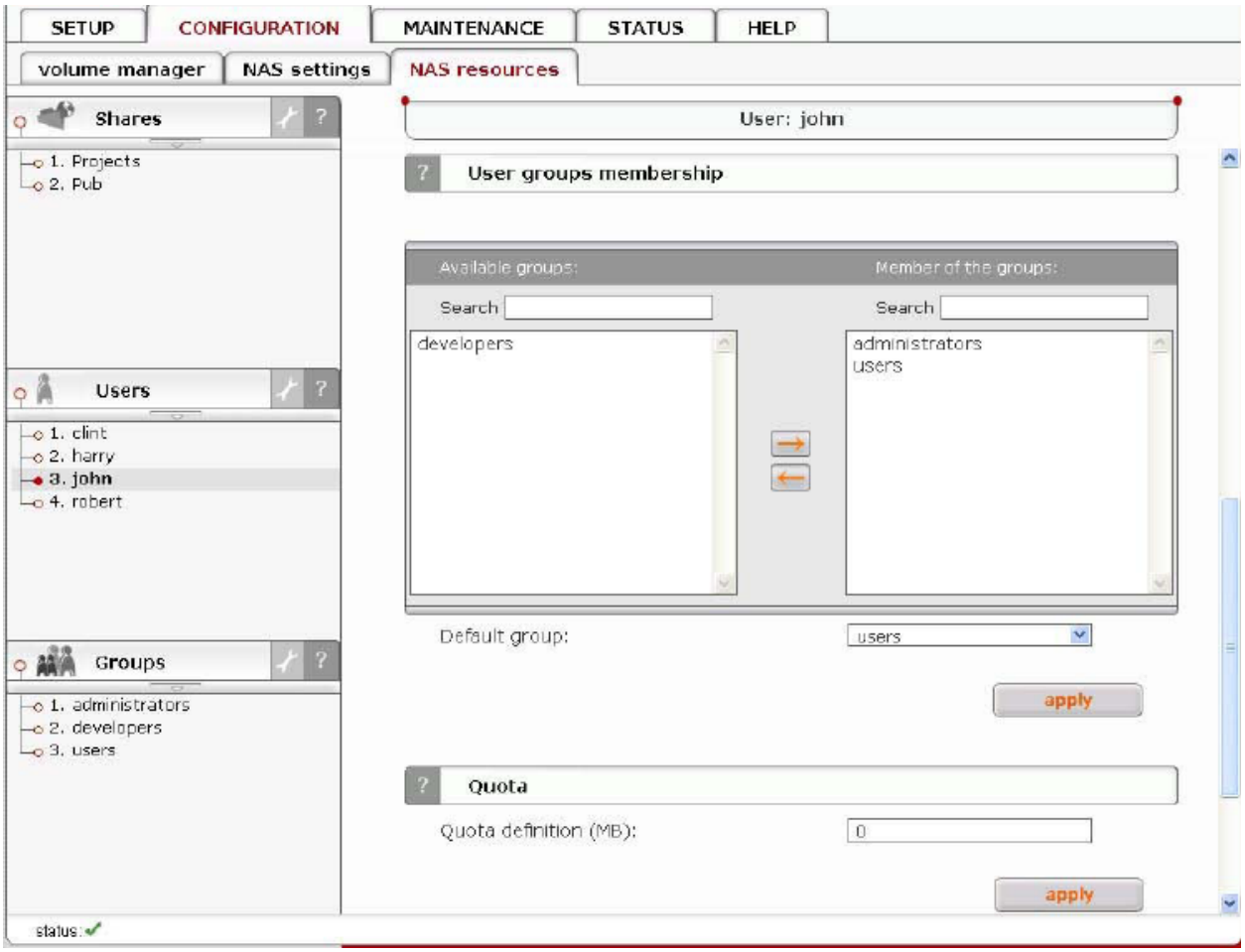
- contain characters: ' " `,
- spaces.

Function: Users share access

Add the users access to the shares by selecting the users and clicking the button. To remove access for users to the specified shares select the users and click the appropriate arrow button to remove them from the Granted access users list.

You can use following keyboard keys in the lists (first set focus to desired list):

- Home: jump to the first,
- End: jump to the last,
- Shift + arrow key: for multi-select,
- letter key: jump to the first position starting with pressed key.



Function: Users group membership

While connected to local LDAP users and groups database this function allows you to view and change user groups membership. To add user to a group or groups select group/groups on Available list and click on .To remove user from group or groups select them on Member of list and click on. While connected to external users and groups database you are able to check which groups user is member of.

You can use following keyboard keys in the lists (first set focus to desired list):

- Home: jump to the first,
- End: jump to the last,
- Shift + arrow key: for multi-select,
- letter key: jump to the first position starting with pressed key.

Function: Quota

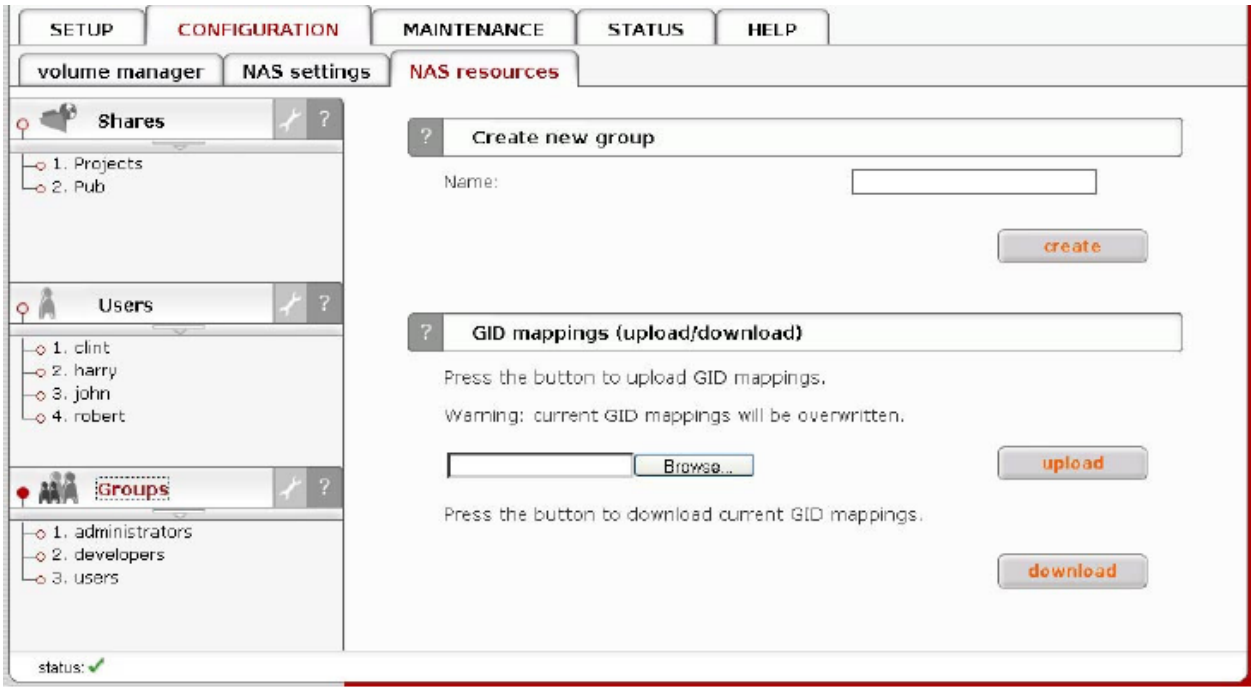
You can assign quota (limit) on amount of space a user is allowed to allocate on shares the user has access to. To remove any limitation the user has set quota to 0.

Function: Remove user

Click "remove" button to remove the user from the system. All the files the user has ownership of will be preserved.

5.2.2.3.3 Groups

In the mode “Workgroup internal LDAP,” you can define entire groups consisting of different users. In addition, you can assign these groups certain access rights. By clicking on “Groups,” a data entry mask opens up, allowing you to create a new group. Assigning the access rights is done the same way
as for users (see 5.2.2.3.2). In the modes “Workgroup (external LDAP)” and “Windows (PDC)” and “Windows (ADS)” the groups are automatically synchronized with the external server.

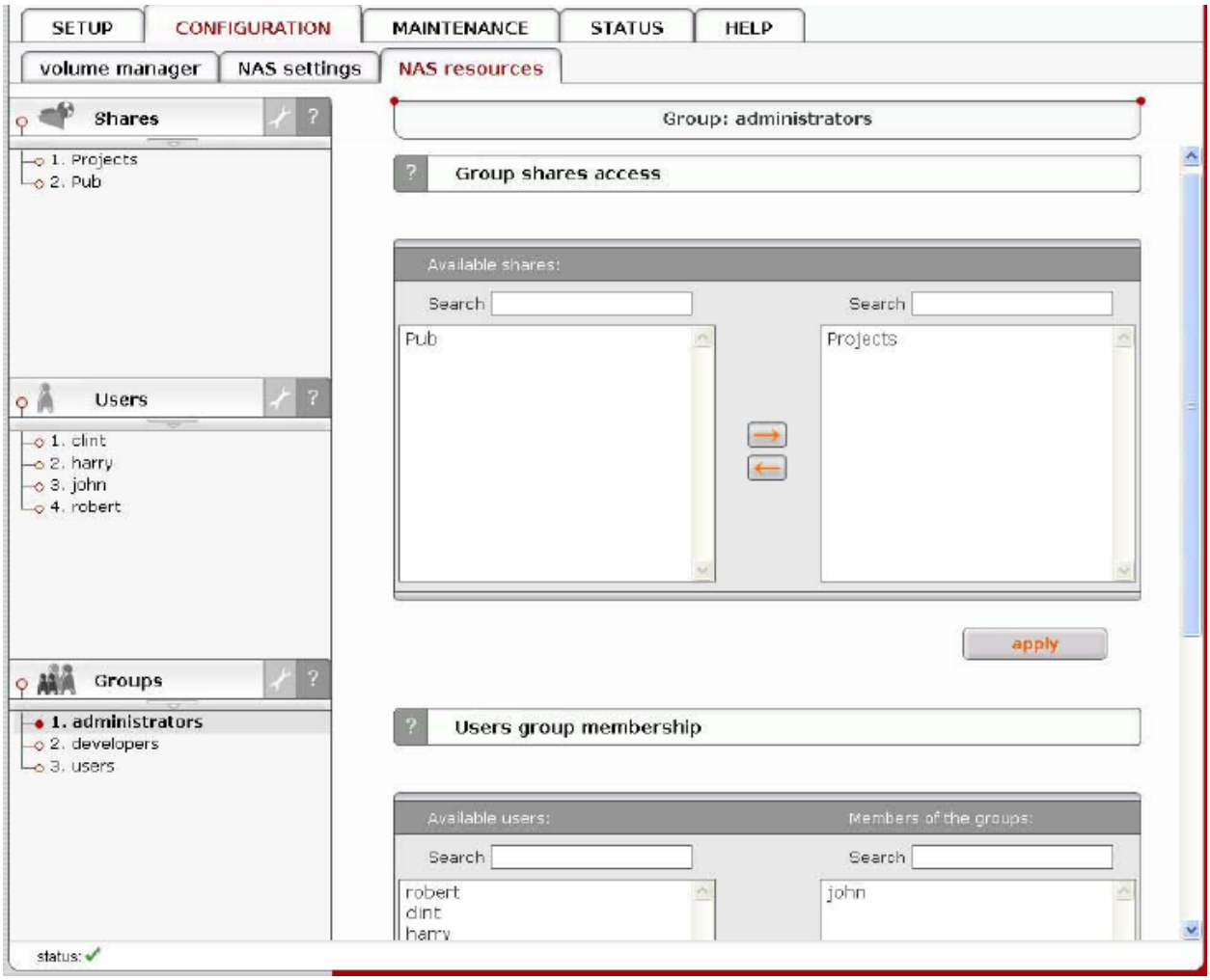


Function: Create new group

To create a group, enter the name and press create button.
Group name cannot:

- contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `,
- begin or end with a space.

Then by clicking on group name e.g. “administrators”, you will see all available functions helpful for setting the groups:



Function: GID mappings (upload/download)

This function allows you to upload and download GIDs (groups IDs). Using this function you are able to change a lot of groups IDs at one time.

To upload gids:

1. In resources menu create share settings (on lv00),
2. Copy configuration file gid_mappings.csv (format:group_name;gid) into settings folder. This file should be in UTF-8 encoding,
3. Press "upload" button to upload GID mappings,
4. If there will be some errors while importing GIDs please read gid_mappings_import.log file in settings share.

Warning: current GID mappings will be overwritten. Press "download" button to download gid_mappings.csv.

Function: Group shares access

Here you can add the shares for this group, which has access to, by selecting the shares and clicking the button. To remove the access from this group, that has the specified shares,

select the shares and click the button. You can use following keyboard keys in the lists (first set focus to desired list):
- "Home": jump to the first,
- "End": jump to the last,
- "Shift" + arrow key: for multi-select,
- "letter key": jump to the first position starting with pressed key.

Function: Users group membership

While connected to local LDAP users and groups database this function allows you to view and change user groups membership.
To assign users to this group, select users from "Available users" list and click on button. To remove membership from a user select users from the Members list and click on button. While connected to external users and groups database you are able to check which users are members of this group

Function: Remove group

Click "remove" button to remove the group.

5.2.3 MAINTENANCE

This page accessed with the Maintenance tab contains settings and functions pertaining to general management operations.

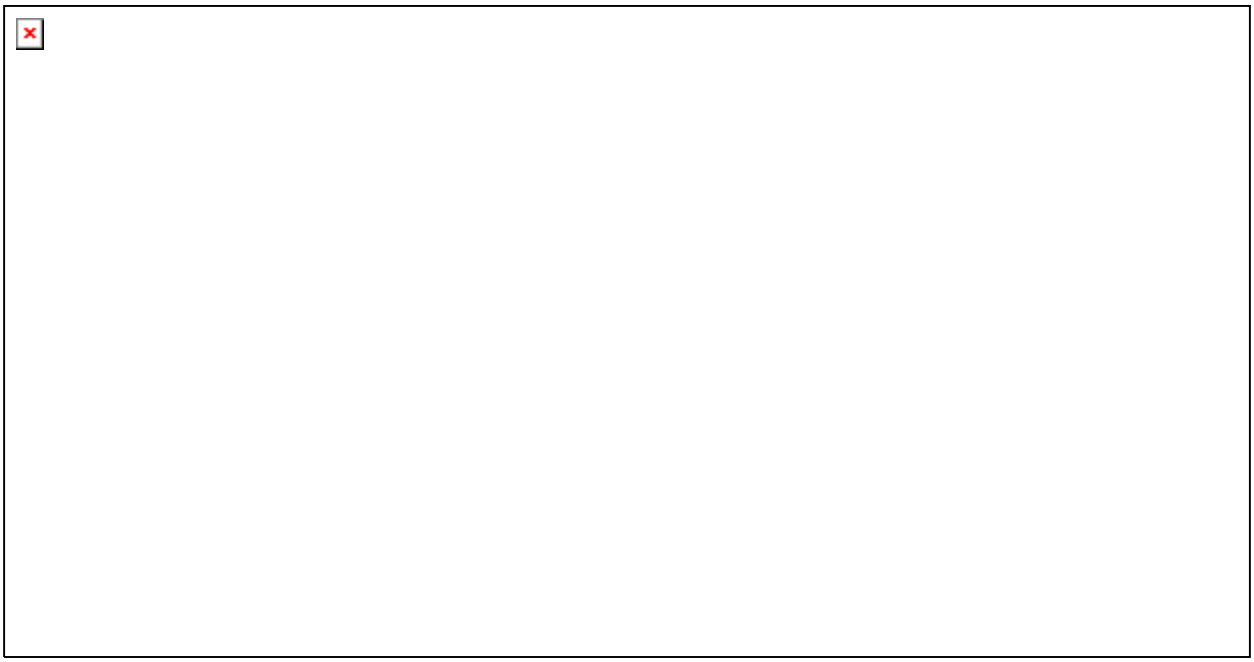
5.2.3.1 Shutdown

Function „System shutdown"

When using this function, you can shut down the uNAS/tNAS. If any of your users are currently connected, you will be asked to confirm the shutdown. If no users are connected, the process will be executed immediately without any delay.
The uNAS/tNAS can only be turned on again manually.

Function: Schedule for shutdown

This control allows you to specify a time for a scheduled system shutdown.

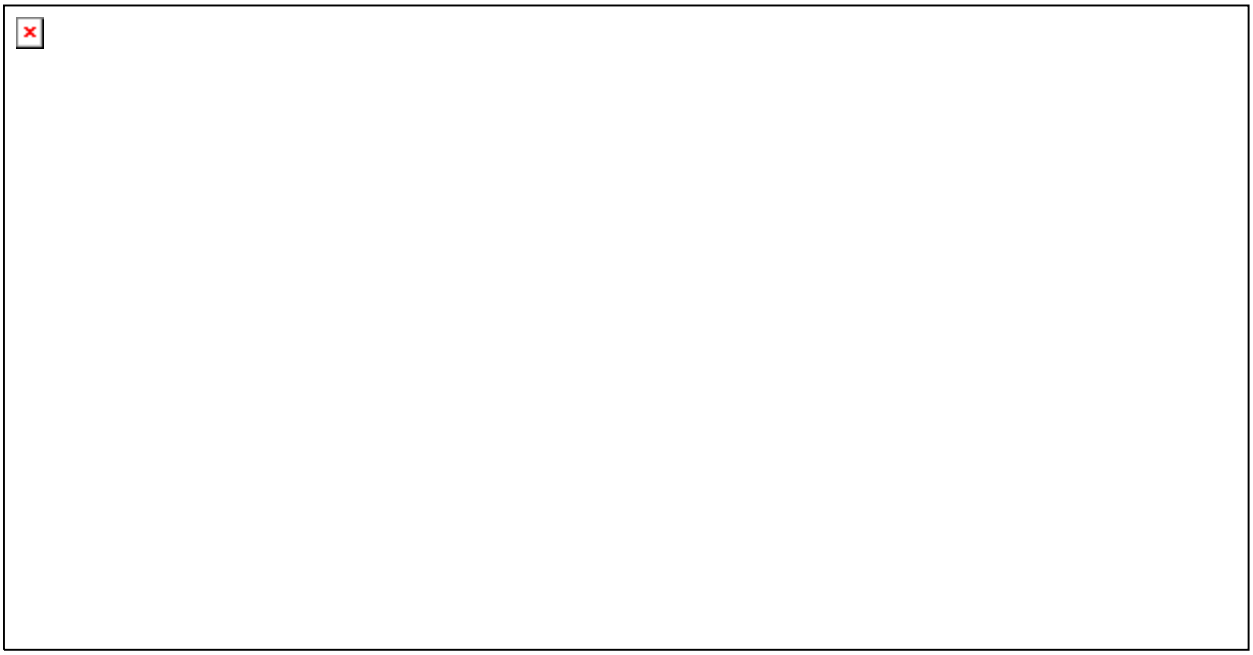


Function: System restart

This function allows you to restart your system.

Function: Schedule for restart

This control allows you to specify a time for a scheduled system

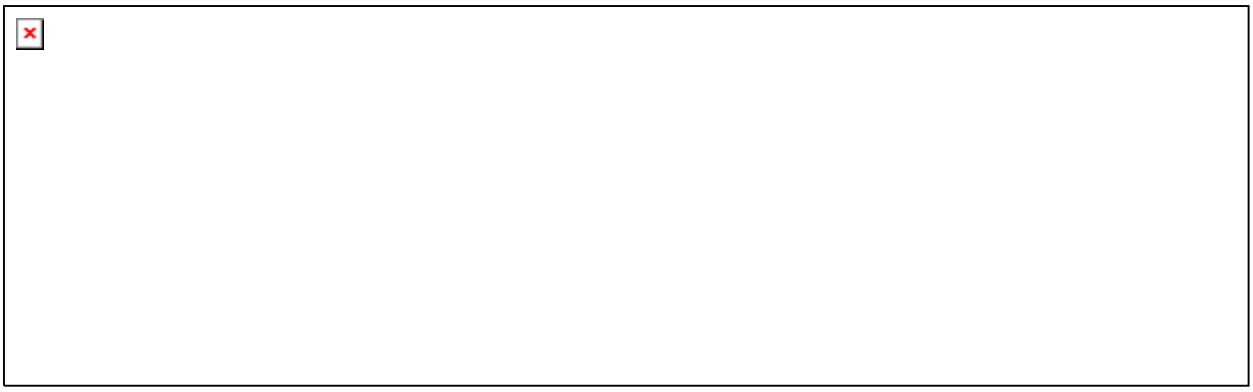


5.2.3.2 Connections

Function: NAS connections reset

This function forces an immediate broadcast of changes to shares or access rights you have made over your network. It is dedicate for SMB and FTP connections. You can check or uncheck corresponding check boxes.

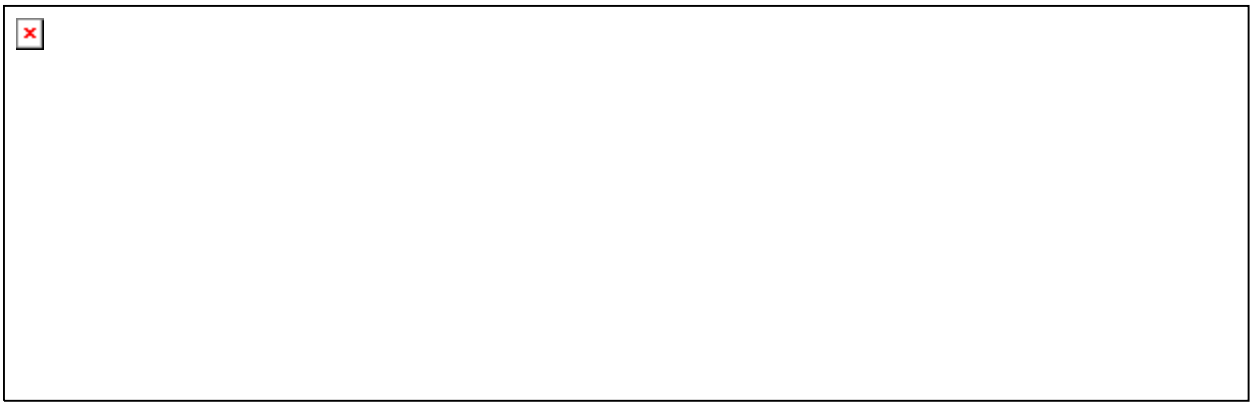
This function disconnects all users connected to the shares on specified protocol, which may lead to data loss if any files are open.



5.2.3.3 Snapshot

Function: Snapshot tasks

This function enables you to manually activate (start) or deactivate (stop) snapshots. Activation of a snapshot is only possible for unscheduled snapshots (with inactive schedule setting). When logical volume is set as a destination replication mode and data are inconsistent then there might be problems while reading data from disks on iSCSI initiator.



Function: Snapshot info

Here you view see information for selected snapshot.

Name

Name of snapshot.

LV

Logical volume for which snapshot is assigned.

Status

Status of snapshot. Can be one of following:

Active

Snapshot is in active state.

Inactive

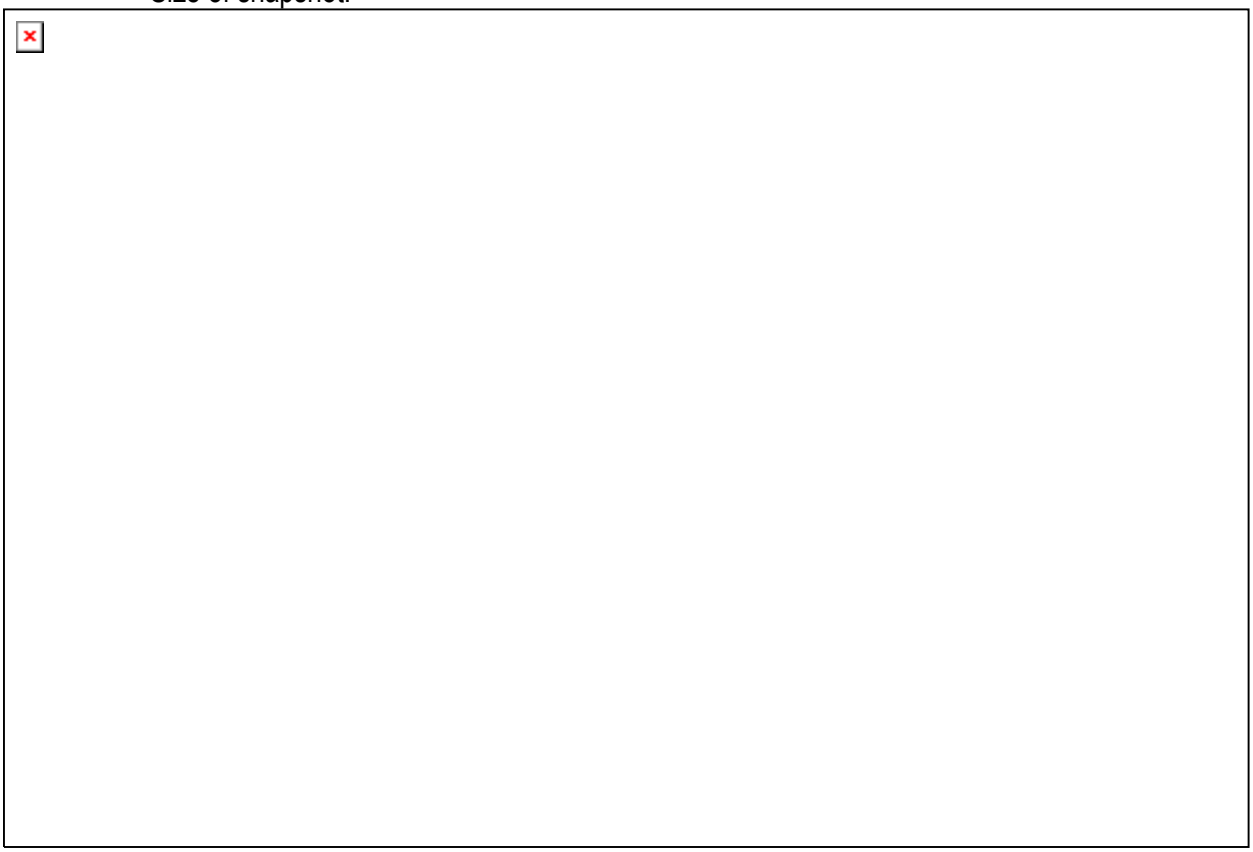
Snapshot is inactive, probable reason: overflow.

Unused

Snapshot is currently unused.

Size

Size of snapshot.



Function: Create schedule for snapshot task

Here you can create schedule for selected snapshot task.

Comment

You can enter comment for snapshot schedule.

Time select

You can start creating the snapshot immediately by selecting "Now" from Time select drop down list or add to schedule.

Interval

Select time period in which snapshot will be created.

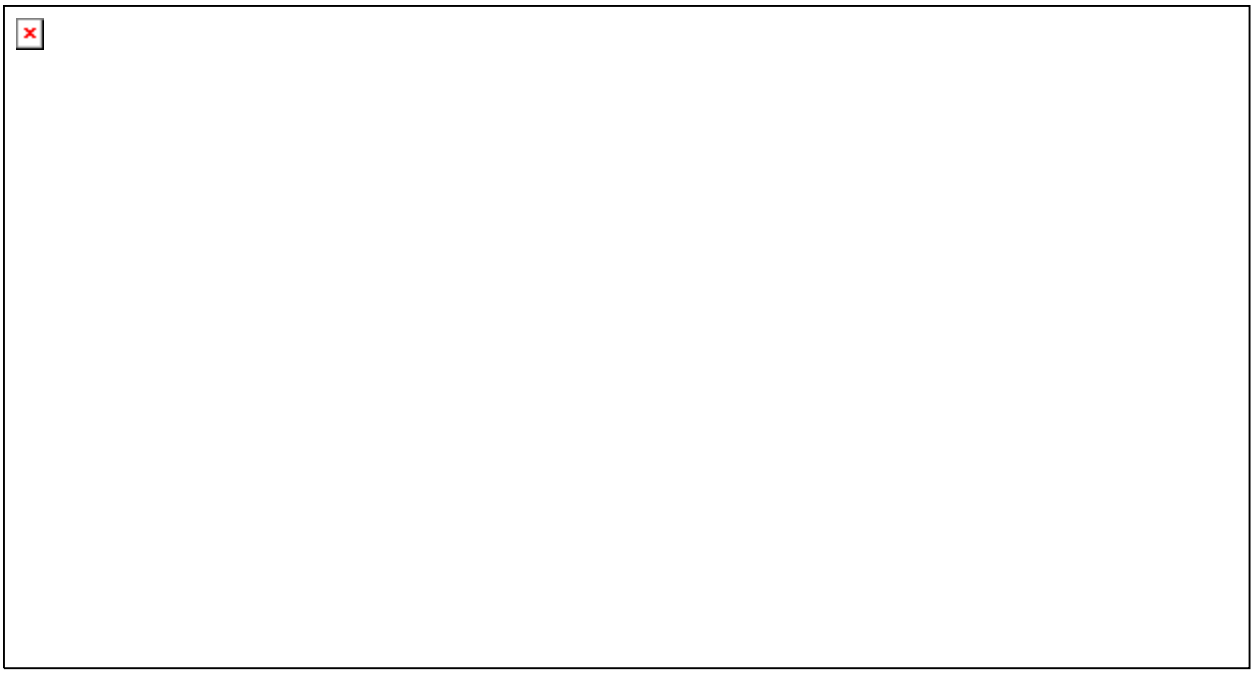
Function: Schedules for snapshot task

Here you can see all schedules created for a snapshot task.

5.2.3.4 Backup

5.2.3.4.1 Backup devices

Here you can view list of all backup devices. Click on device name to edit device settings, create new tape for the device, manage tapes or remove the device. In case when tape backup device (physical device) is connected, "Tape Drive" entry will appear on backup devices tree.

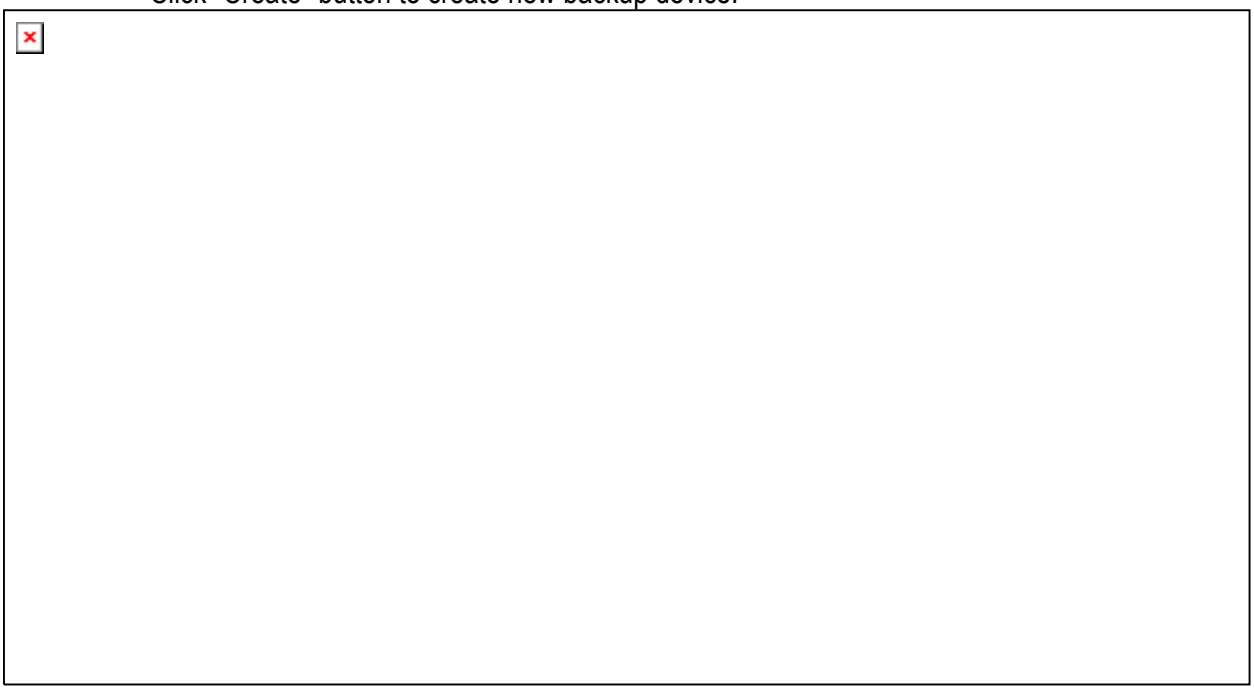


Function: Create new virtual backup device

Here you can create a new backup device, this device will be used as destination when making backups of your data. Please provide:

- Name for device,
- Select share for device,
- Time retention of tape,
- If you want to make one backup on one tape only, select option use each tape only once.

Click "Create" button to create new backup device.



Function: Backup device settings

Here you can set settings for selected backup device.

Time retention of tape

Time after the tape will be rewritten from the beginning.

Use each tape only once

Means that each backup will be made on one tape only.

Function: Label new tape

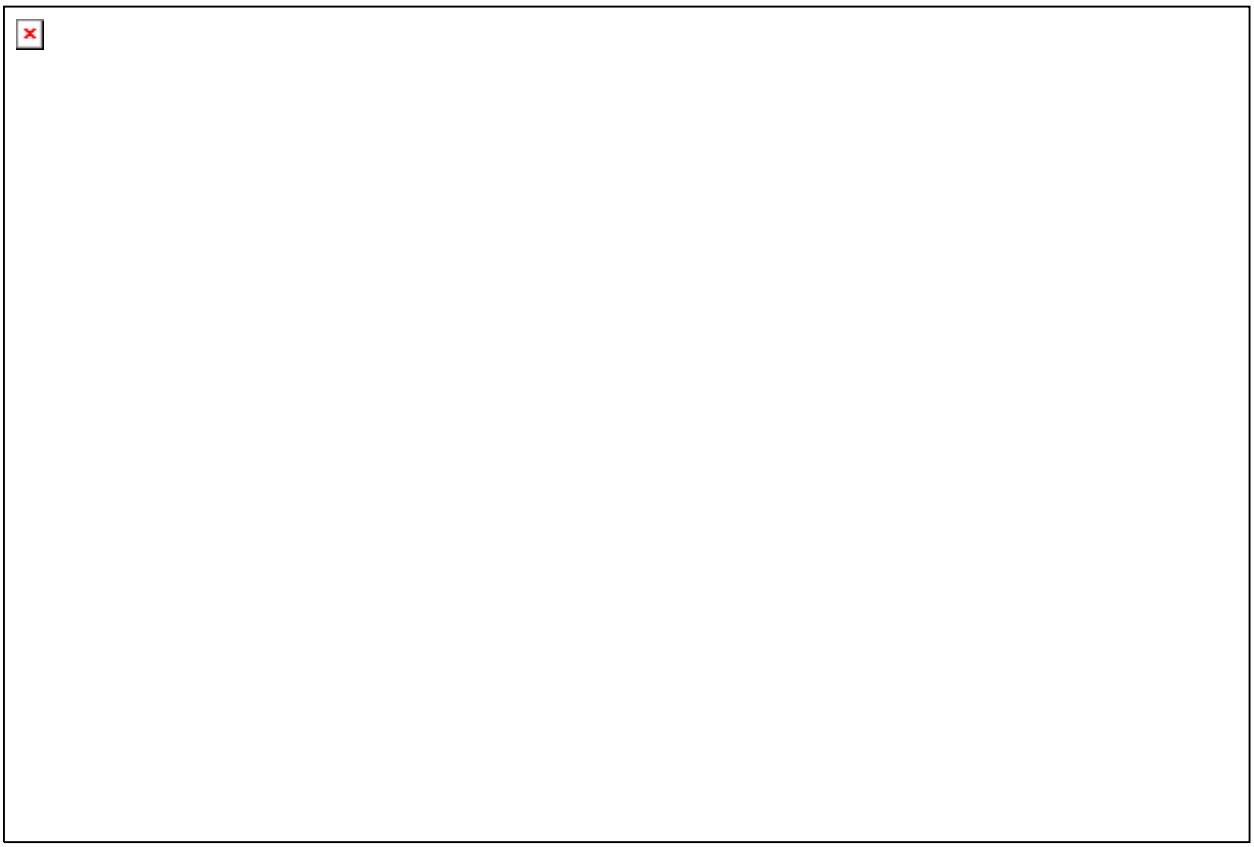
With this function you can label new tape that will be used to make backup. In order to label a new tape:

- enter tape name,
- select slot,
- optionally you can limit tape size,
- click "Apply".

Make sure to insert tapes in to streamer device in proper order, otherwise tapes may have wrong slot number assigned after making backup.

Function: Remove backup device

This function removes selected backup device.



Function: Tapes

Here you can view information on all tapes used with selected backup device and manage them.

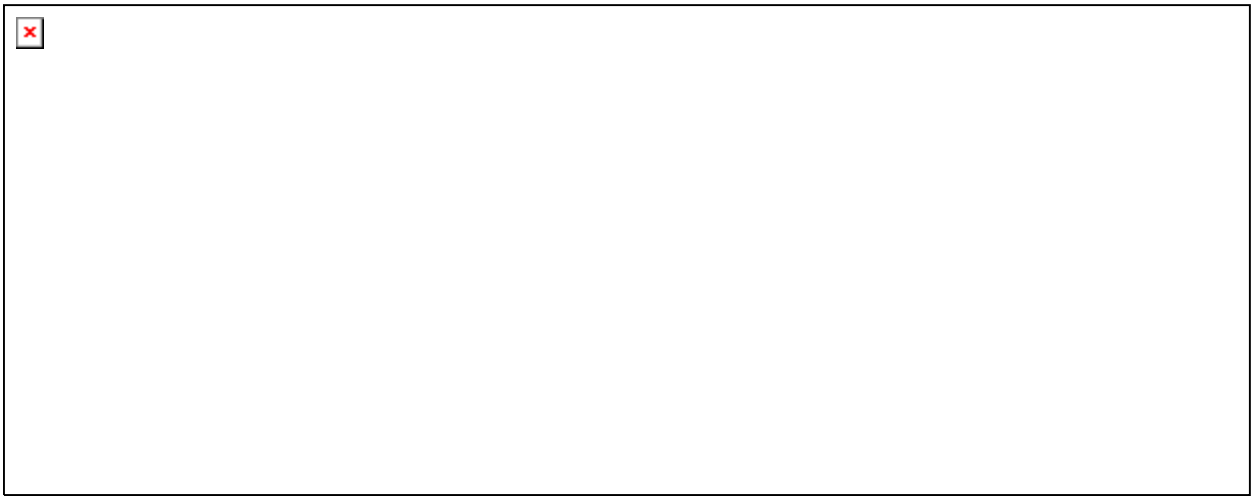
Function provides following information:
Name: Name of the tape.
Status: Status of the tape. Status can be one of following:
• Full - tape is full and will not be used for backup until retention time is over,
• Append - new backups will be written at the and of the tape,
• Recycle - the tape will be set to this state when tape status has been set to purged and there is no other appendable tapes available. Tape will be set for new write from the beginning of the tape(old data will be deleted),
• Purged - this status will show up when tape retention time is over(old data is still on tape),
• Error - tape will not be used because of errors on tape,
• Used - tape has been set as used once only and cannot be append any more,
• Busy - tape is actually used for backup write.
Used/size: Shows how many MB of data has been written to tape and how many MB of data can be written to that tape
Action: Action that can be performed on tape:
• Show more info on tape,
• Manually set tape to purged status,
• Remove the tape.

Function: Tape tools

This function provides tools to manage your tape device.
Tape tools:
• tape rewind,
• tape erase,
• tape unload / eject,
• tape load.
When tape library device is connected then tape unload tool will appear. If streamer device is connected then tape eject tool will appear.

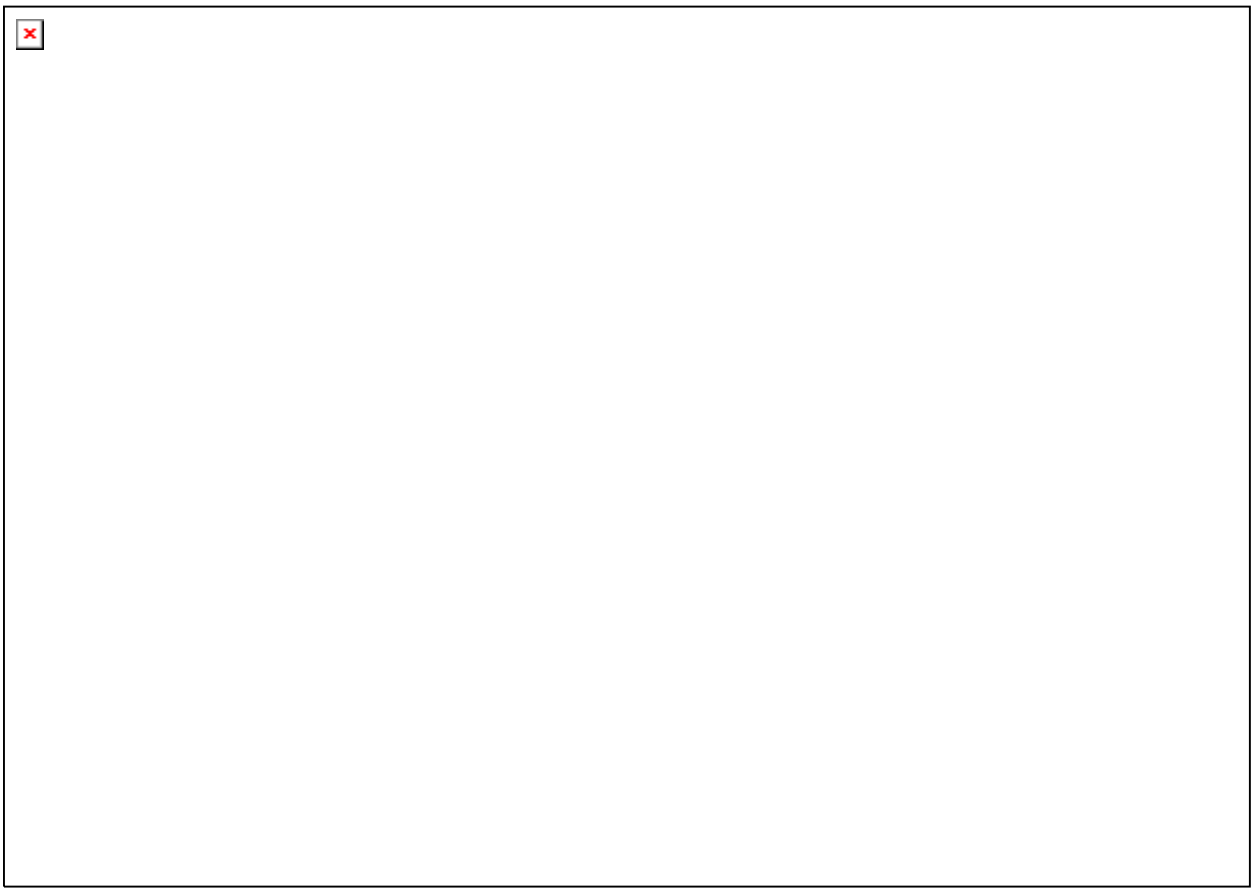
5.2.3.4.2 Backup tasks

Here you can view list of all created backup tasks. Click on backup task name to see more information about it.



Function: Backup tasks

Here you can view information on selected task
Shares - List of shares that are used for backup
Device - Backup device to which backup task is assigned
LV - Logical volume that is used for backup device
Snapshot - Snapshot that is used for backup task
Level - Backup level used
Compression - Compression info



Function: Create new backup task

Here you can create new backup task. In order to create backup task:

- Enter task name,
- Select Logical Volume,
- Select Shares for backup,
- Select Snapshot from which backup will be made,
- Select backup device on which backup will be made,
- Select backup level,
- If you want to compress data on backup, select option compress data,
- Select option un-mount tape after backup to un-mount tape after backup.

Backup levels:
Full - This will backup all your data.

Incremental - This will backup only new data.
Differential - This will backup all new data from last full backup.

Function: Schedules for backup task

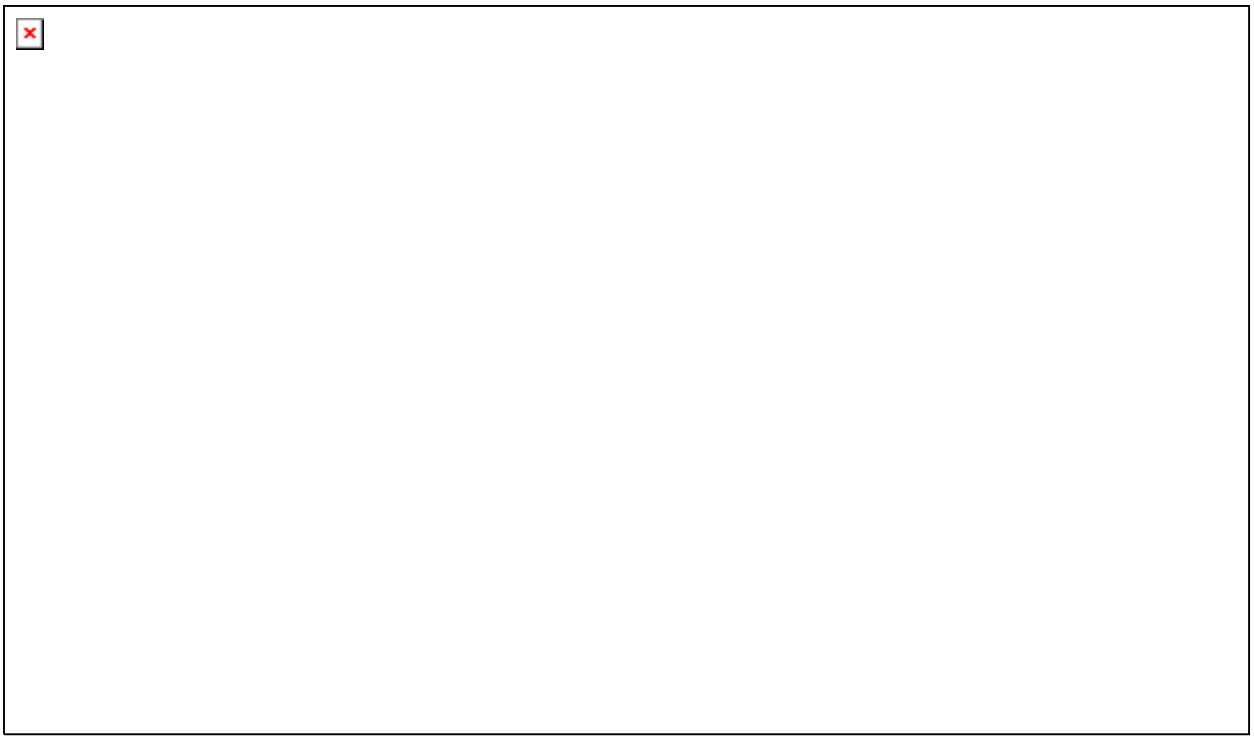
Here you can see information on all schedules created for selected backup task. You can also delete any schedule by clicking "delete schedule" action button.

Function: Restore from backup

Here you can restore data from created backup. In order to restore data from backup:

- select backup to restore,
- select share to which backup will be restored,
- select type of files overwrite,
- click "apply" button to begin restore process.

For every backup you view following backup info:
Files - Number of backuped files.
Size - Total size of data in MB.
Required tape(s) - List of tapes required for backup restore.



5.2.3.4.3 Data replication

Here you can view list of all data replication tasks.

Function: Create new data replication task

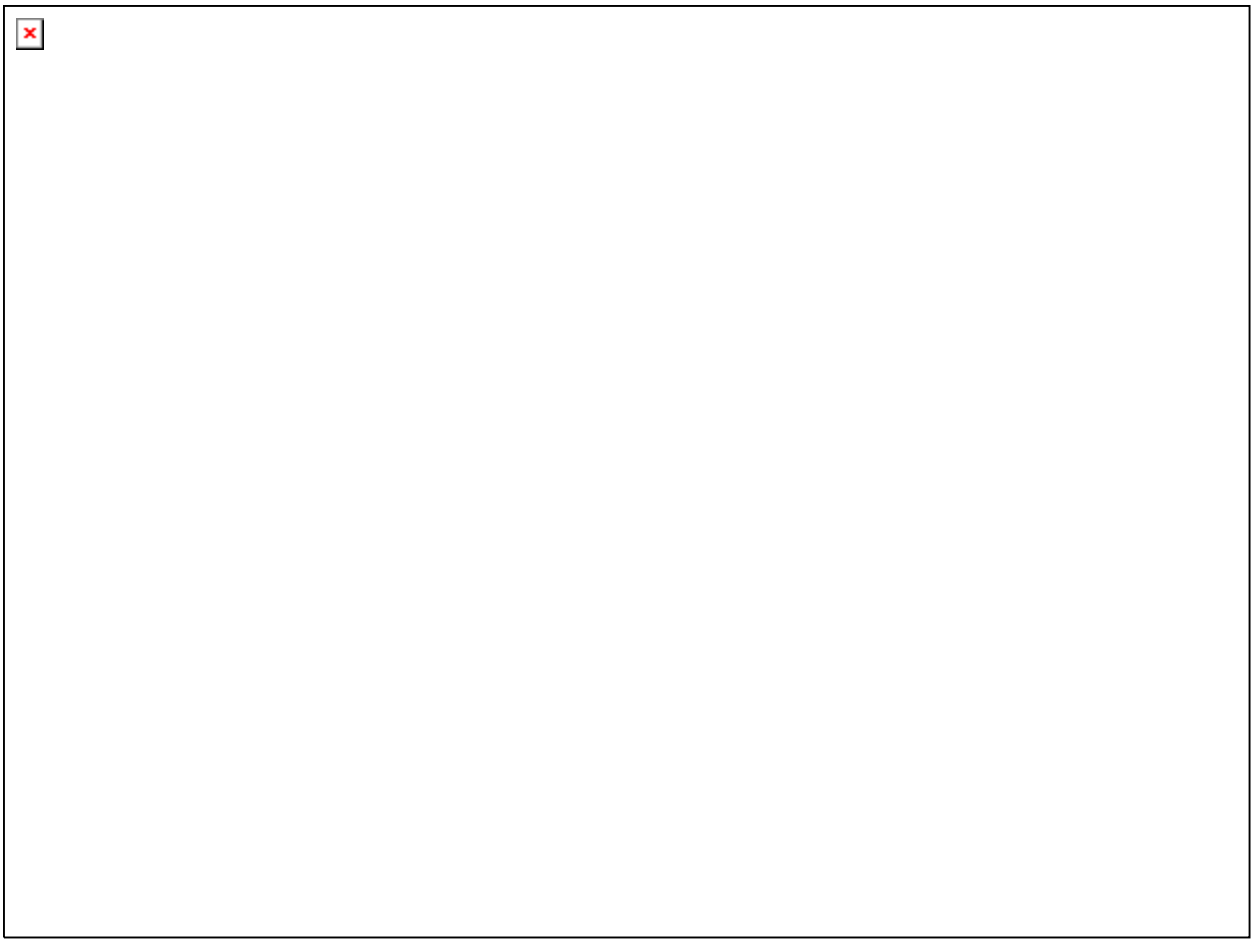
This function allows you to create new data replication task. Data can be replicated as source or destination in the same time.
Task name - Please enter task name.

Source share - In order to set share as source, select it from the drop down list and enter Destination IP, Where share will be replicated.
Snapshot - Snapshot assigned for data replication.
Destination share - Select destination share from the drop down list and enter destination agent login and password.
Dest. agent login - Enter destination agent login.
Dest. agent password - Destination agent password.
Log replication errors - Turn it on, if you want to log replication errors.
Replicate whole files - If this option is turn on, then all parts of a file will be replicated, if not only changed part of a file will be replicated. It's recommended to turn it on, if speed of network is faster then local partition write speed. In order to set share as a destination, one should enable Data replication agent in setup NAS settings menu, then enable replication option for each share. There is no need to enable Data replication agent, if replication would be only set as source. It's not possible to make data replication and backup in the same time. Backup has higher priority then data replication. Data replication will be stopped, if it has been setup in the same time with Backup, when using snapshots from the same Logical Volume. You will see snapshot error in Data replication status, because snapshots can not be used twice in a same time, if they are set to the same Logical Volume. In order to make data replication over the internet you have to configure the firewall port to: 873.

Function: Data replication tasks

Here you can run, stop and delete previously created data replication tasks.
For every task you can view additional details:

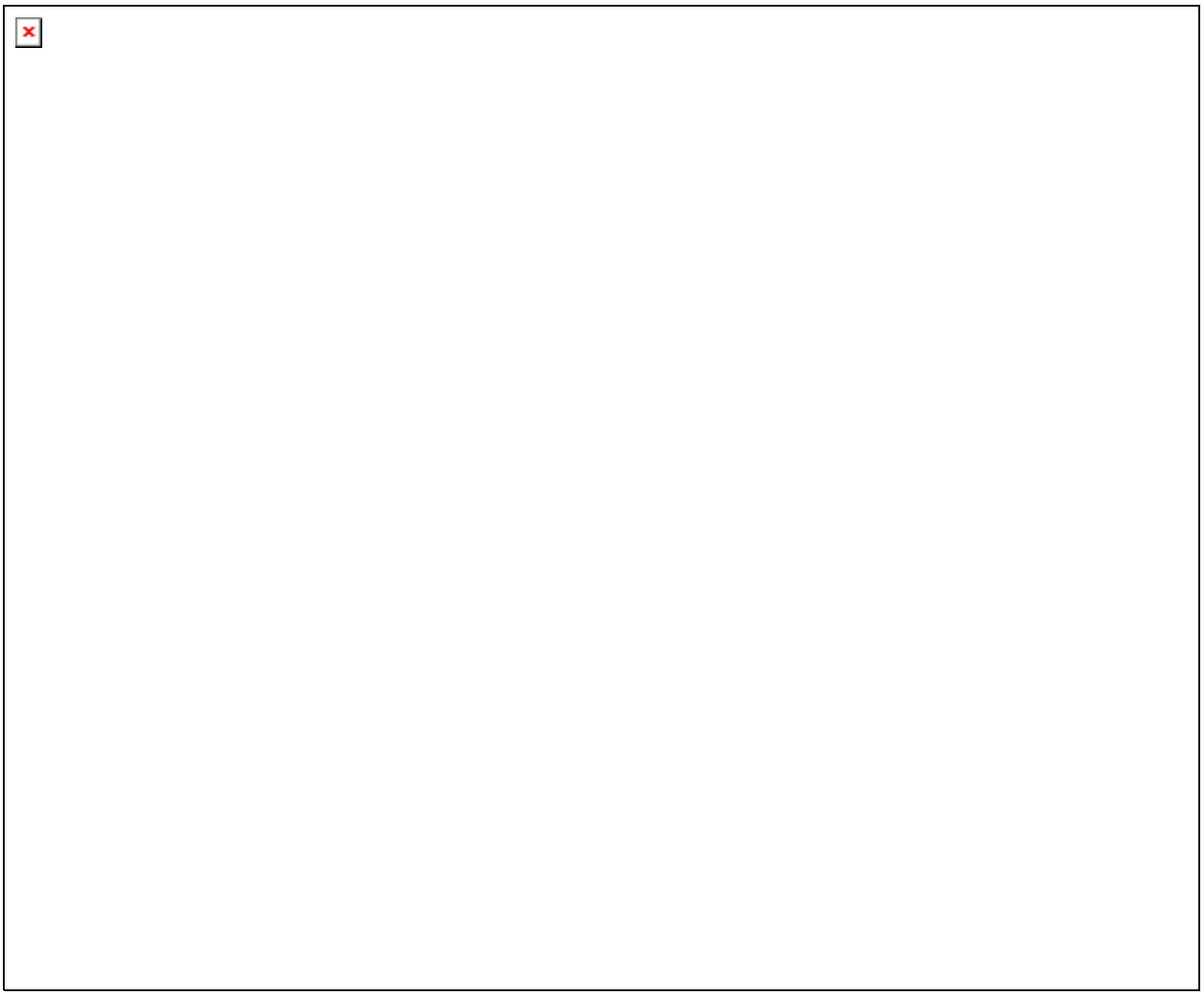
- Destination IP,
- Source share,
- Snapshot,
- Destination share,
- Destination agent login,
- Replicate whole files info,
- Log replication errors info.



Function: Data replication task

Function shows information on selected data replication task.
You can view:

- Destination IP,
- Source share,
- Snapshot,
- Destination share,
- Log replication errors info,
- Replicate whole files info.



Function: Create schedule for data replication task

Here you can create schedule for selected data replication task.

Comment

You can enter comment for replication schedule.

Time select - You can start replication immediately by selecting "Now" from Time select drop down list or add to schedule.

Interval - Select time period that replication will be run.

Function: Schedule for data replication task

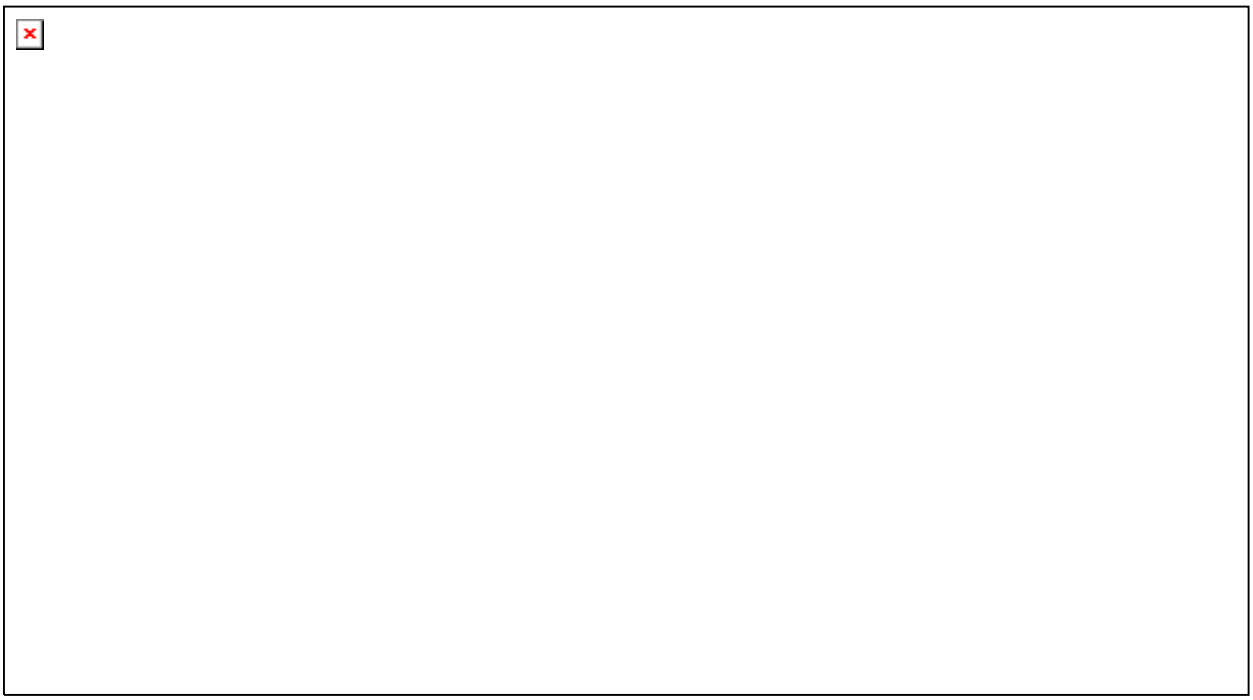
Here you can manage all schedules created for selected data replication task.

5.2.3.5 Antivirus

Function: Create new antivirus task

Here you can create a new antivirus scan task.

- Enter task name,
- Select shares for scan,
- Click "apply" to create a task.



Function: Antivirus tasks

Here you can run, stop or delete desired antivirus task. All previously created tasks will be visible here.

Function: Update virus definitions

With this function you can update virus definitions. Select mirror from which definitions will be downloaded. Select when update should be made. If you select "now", update will be made instantly. In another case update will be made now and every selected time.

Function: Antivirus online

This function gives Antivirus online protection for your network protocols. Any files transferred on the server will be scanned. The feature Enable SMB protocol scanning allows scanning online files via SMB.

Options:

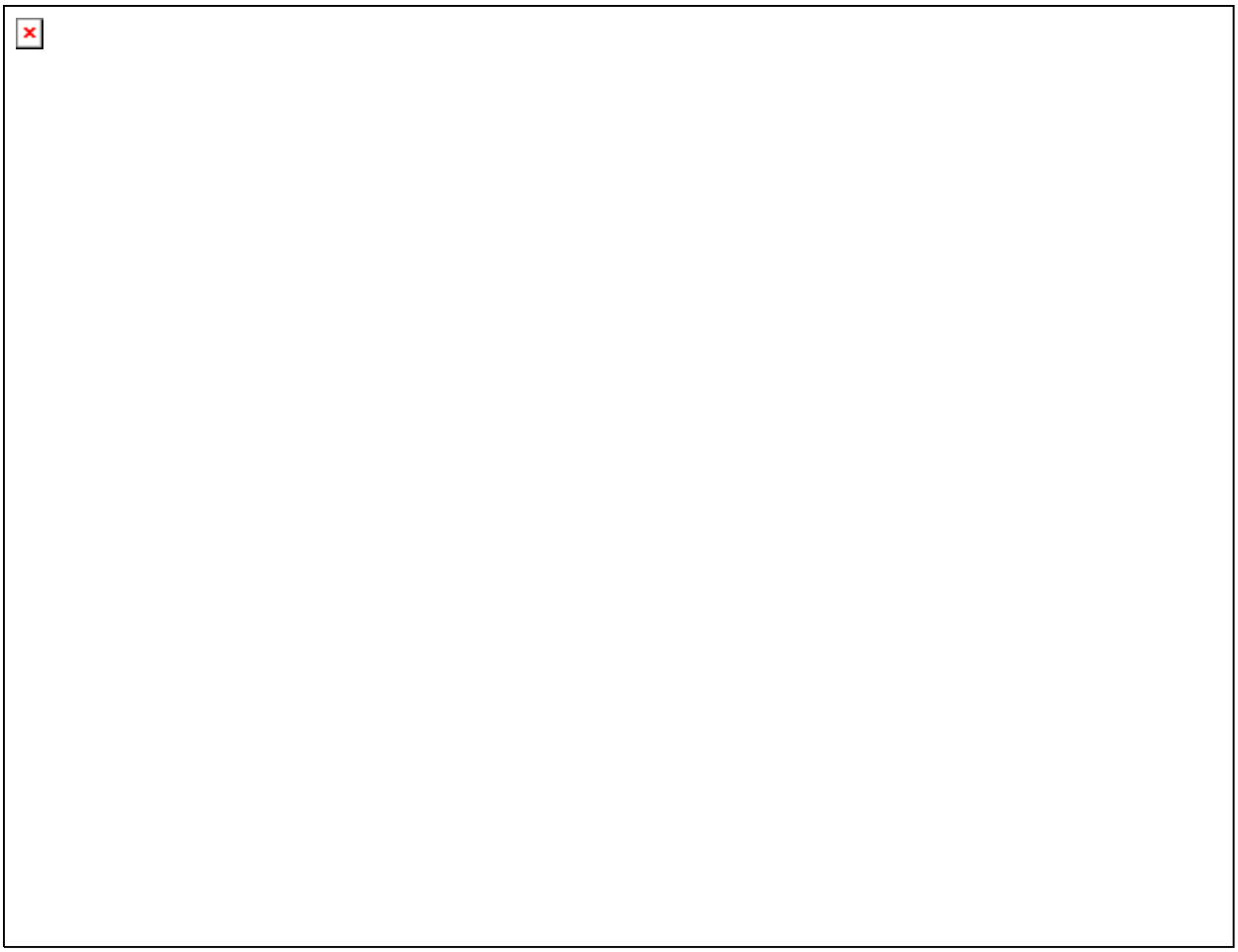
Move to quarantine

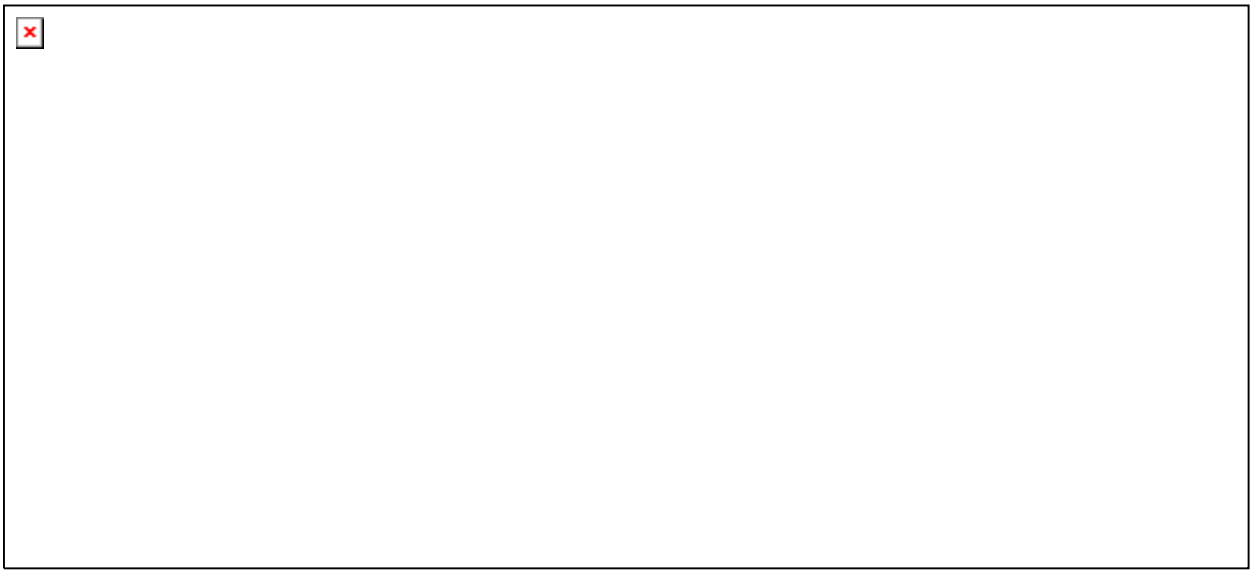
Allows moving infected files to quarantine share previously chose. Name of infected files will change with prefix vir- and randomly signs without extension.

Delete infected files - Allows automatically deleting infected files without warning!

No action - Allows to choose no action on founded infected files.

Notify by messenger - Allows to get fast information about infected files by Windows Messenger (net send). To verify the information about the infected files look in logs. You will get the info which files are infected and with what viruses.





Function: Create new schedule for antivirus task

Here you can create new schedule for selected antivirus task.

Comment - You can enter comment for antivirus schedule.

Time select - You can start antivirus task immediately by selecting "Now" from Time select drop down list or add to schedule.
Interval - Scan will be made every "selected time". E.g. if you choose interval 1 h. – each one hour share will be scanned.
Weekly - Scan will be made in selected days at specified time.

Function: Schedules for antivirus task

Here you can manage all schedules created for selected antivirus task.

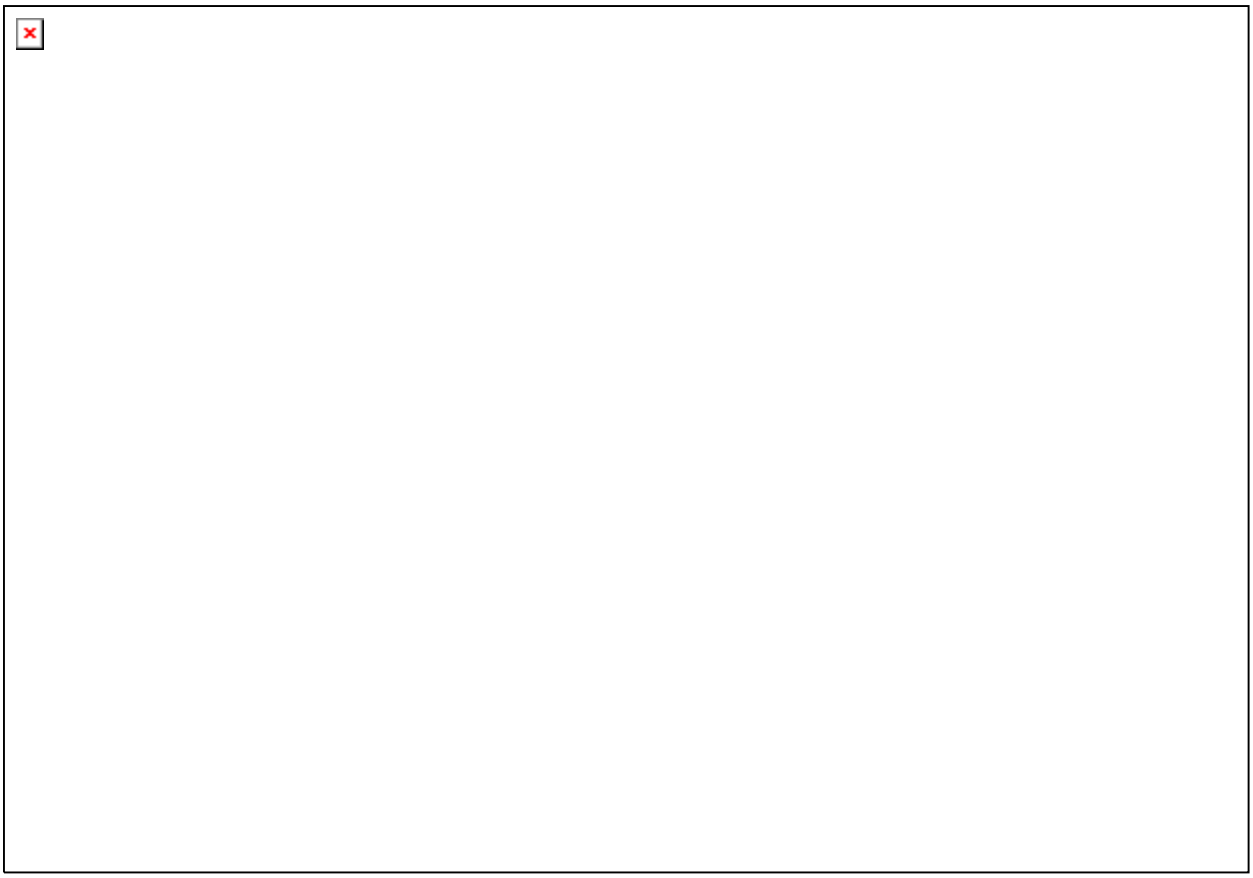
5.2.3.6 Miscellaneous

Function: Save settings

With this function you can store the configuration settings. You can save such setting as:

- Server setup,
- Network settings,
- Administrator setup,
- Hardware setup,
- Target settings,
- Users.

Select settings you want to store and click Apply. Settings can be saved locally on the server(it will be visible in function Restore setting) and/or downloadable file. Each time you save settings locally, new entry will be created and during restoring you can select witch settings to restore. You can restore the settings using function Restore settings.



Function: Restore settings

With this function you can store the configuration settings. You can save such setting as:

- Server setup,
- Network settings,
- Administrator setup,
- Hardware setup,
- Users.

Select settings you want to store and click Apply. Settings can be saved locally on the server(it will be visible in function Restore setting) and/or downloadable file. Each time you save settings locally, new entry will be created and during restoring you can select witch settings to restore.

You can restore the settings using function Restore settings.

Function: Save settings

With this function you can restore the configuration settings (previously saved). You can restore settings from files saved locally or upload configuration settings file(previously downloaded).For each entry you can see configuration file name, date of creation and actions that can be applied. By clicking Details action button you can select witch settings to restore. To restore settings click on Restore action button.

You can restore following settings:

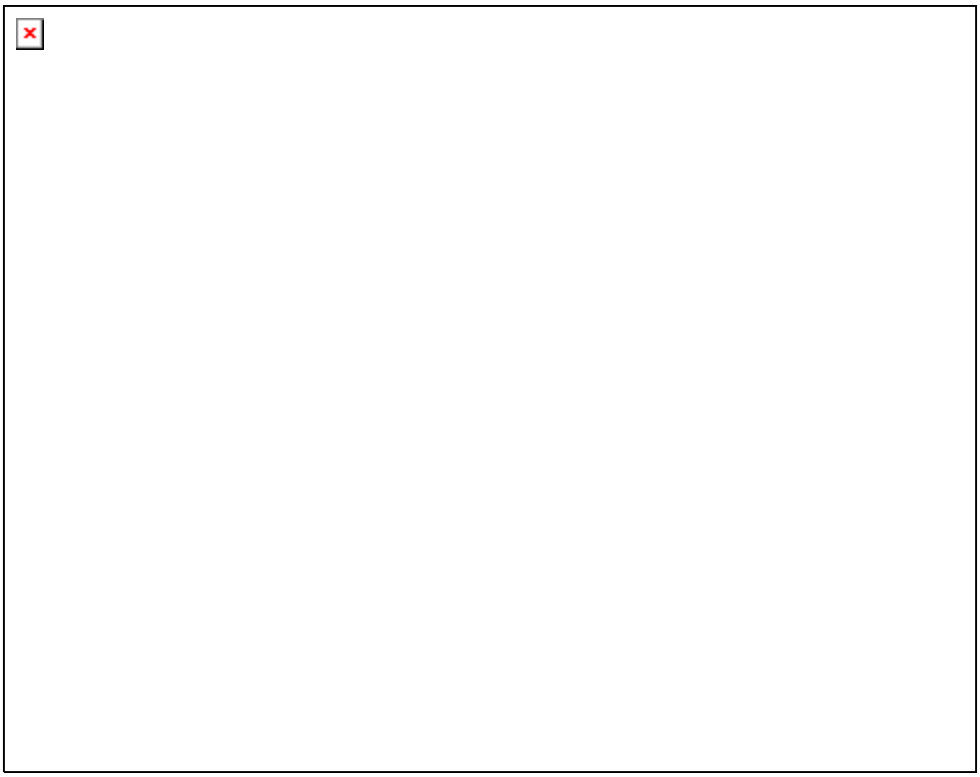
- Server setup,
- Network settings,
- Administrator setup,
- Hardware setup,
- Users.

You can delete configuration settings file by clicking Delete action button. You can download configuration settings file by clicking its name. In order to upload configuration settings file(previously saved) browse a file name and click on Upload button.

You can save the settings using function Save settings.

5.2.3.7 Software update

This function allows you to update the system software. There are two ways of updating uNAS/tNAS software.



Function: Update downloader

With this function you can check if there is new update available and download it. In order to download a new update you need to be registered at Open-e.com. You also have to remember to setup correct DNS and Gateway address in “SETUP” “network” menu.

Function: System software update

This function allows you to update the system software. When you upload update file you will see its name and size. With each update file you do following action:

- See release notes,
- Make update (Update button),
- Delete update file (Delete button).

Some updates need a system restart. In this case you will be informed about needed restart in confirmation message.

Function: Run previous system

With this function you can restore old system.

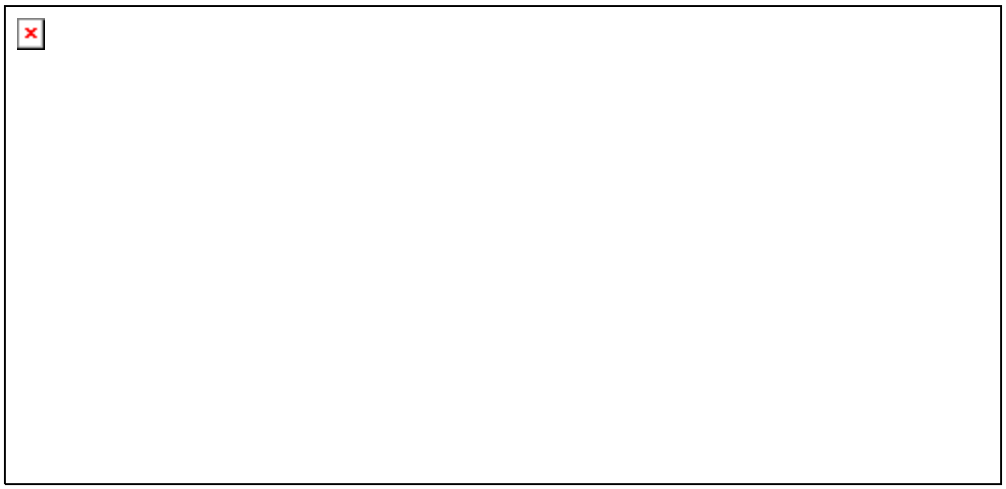
5.2.4 STATUS

This function provides a quick overview of the most important system parameters of your uNAS/tNAS. The corresponding sub-functions are network, logical volume, connections, hardware, tasks and S.M.A.R.T.

5.2.4.1 Network

Function: Interfaces

Here you can view network interfaces info. In table you can see network interface name and IP address, DHCP information, cable status.

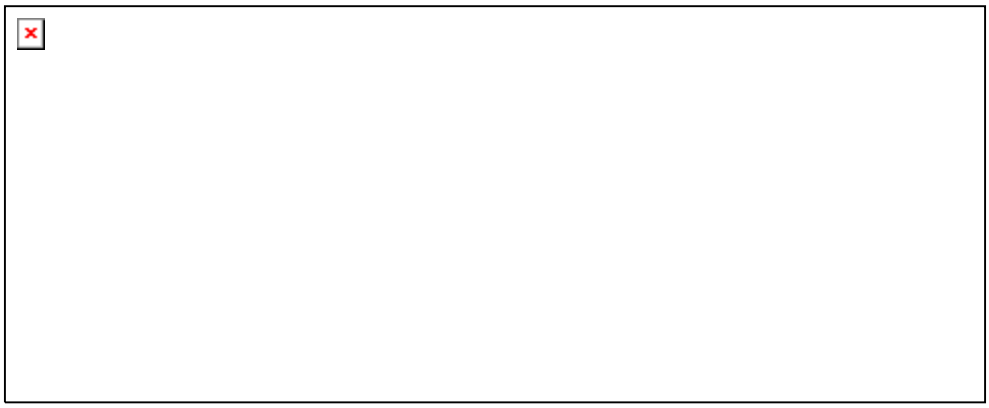


Function: DNS info

Here you can view network interfaces DNS information.

Function: HTTP proxy info

With this function you can view HTTP proxy information. You can see if proxy is enabled and which HTTP proxy IP address is assigned to it.



Function: Interfaces info

This function shows information about selected network interface. You can view here:

- MAC address,
- State,
- DHCP status,
- IP address,
- Mask,
- Broadcast address,
- Gateway address.

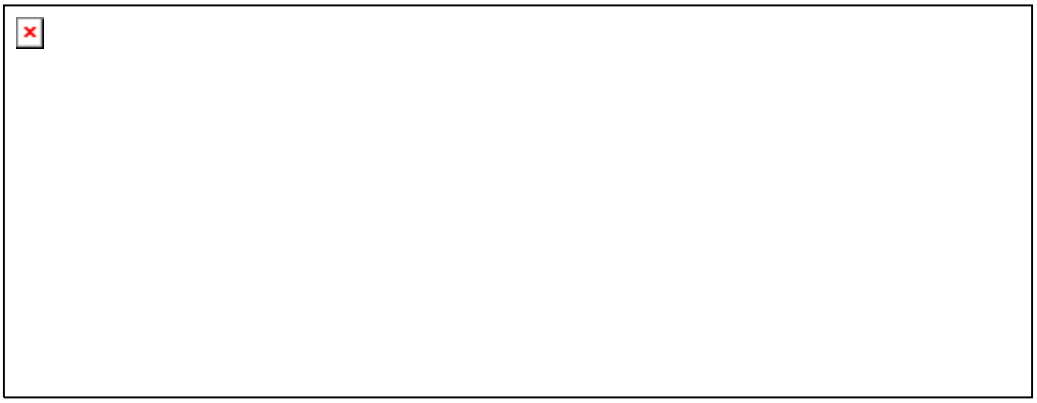
5.2.4.2 Logical volume

Function: Share volume statistics

This function contains statistical data on the share volume.

Function: Dynamic volume statistics

This function contains statistical data on the dynamic volume.



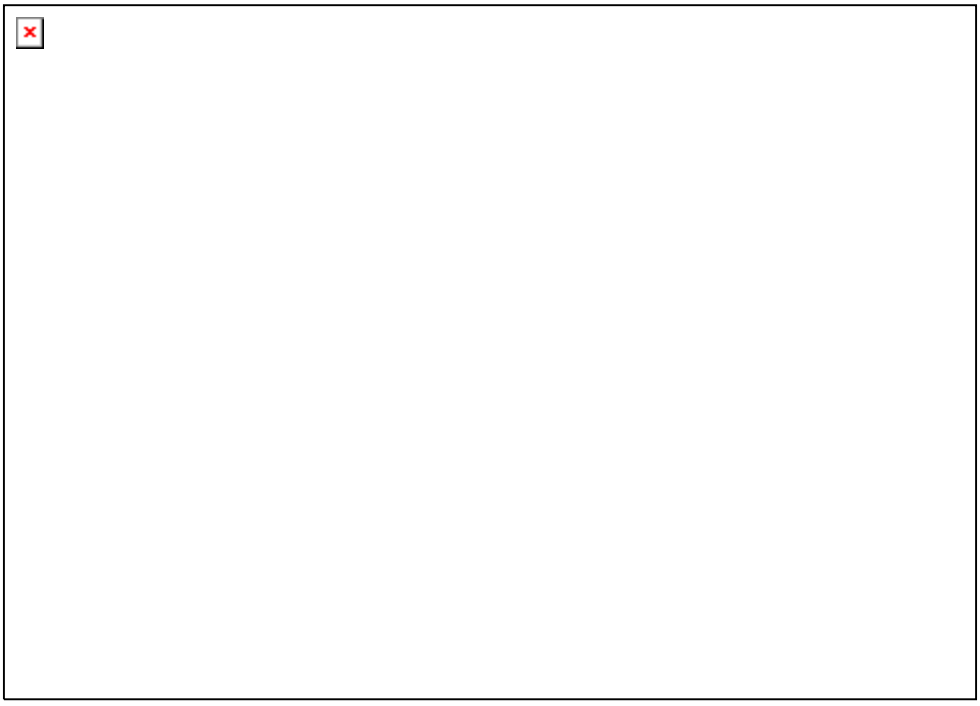
Function: Logical volume statistic

Here you can see information on selected share volume. Function provides following information:

Usage - Percentage usage of space by share volume.
Size - Size of share volume.
Used - Current date usage of space on share volume.
Available - Available space on share volume.
Total snapshots - Number of all snapshots assigned to share volume.
Snapshots active - Number of active snapshots.

5.2.4.3 Connections

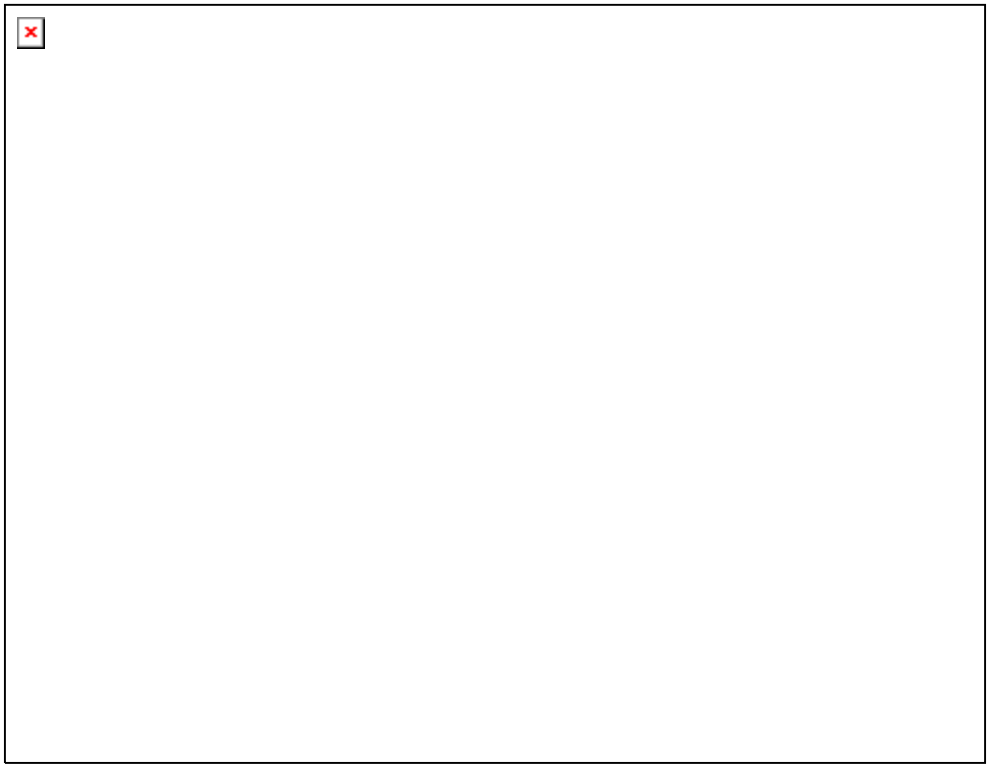
This function displays what user connections are currently active.

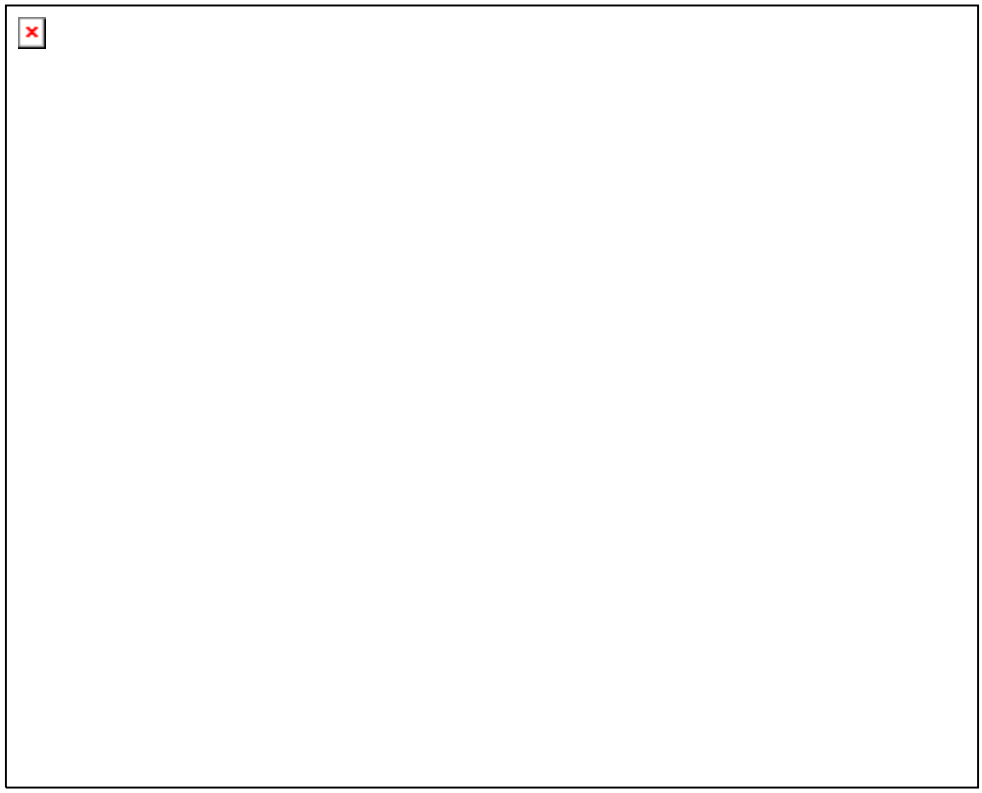


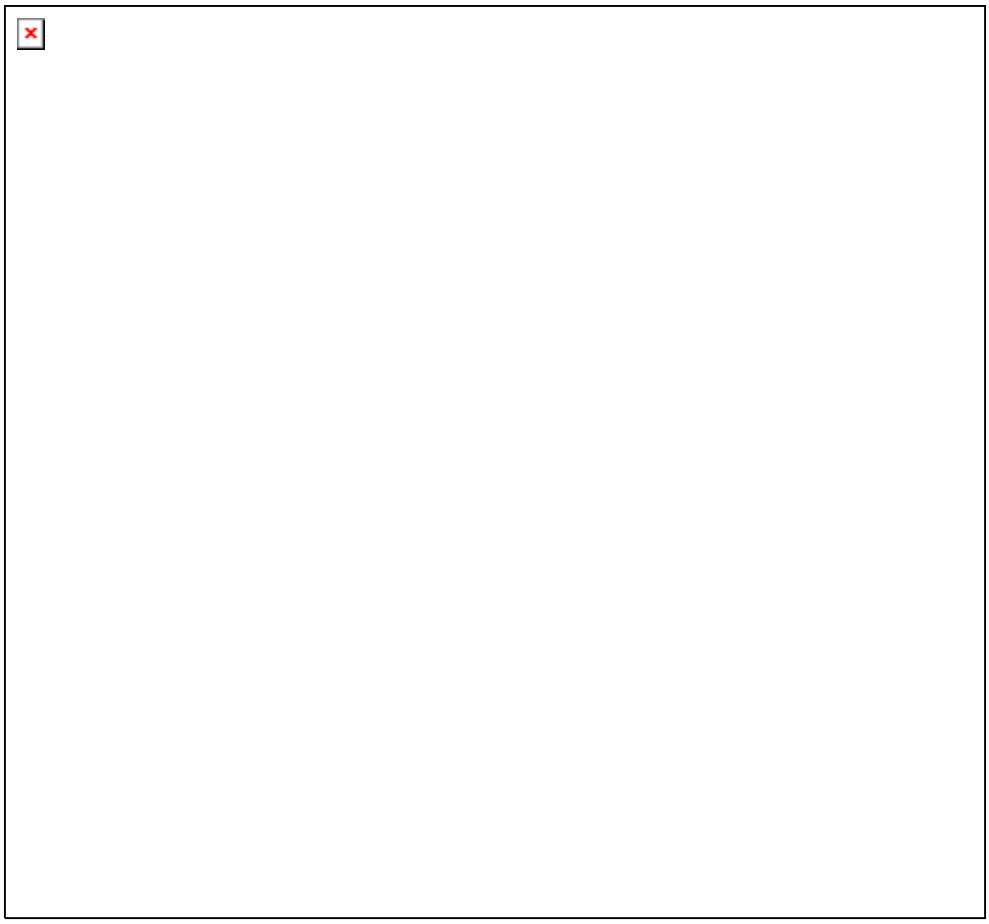
5.2.4.4 Hardware

The “Hardware” option provides you with information on storage and network controllers and the drivers (e.g. network driver and RAID driver).

In addition, you may also download the latest uNAS/tNAS log files or view specified or all log files without downloading in compressed form. You can also check usage of memory (RAM) and (SWAP) and also hardware monitoring.





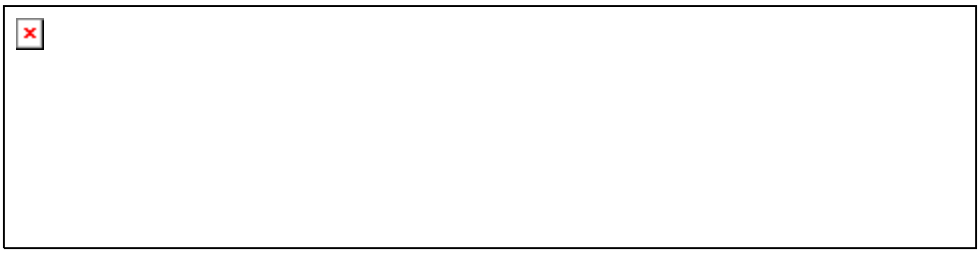


5.2.4.5 Tasks

Here you can view statistical information on tasks from backup, restore from backup, data replication, antivirus and snapshots.

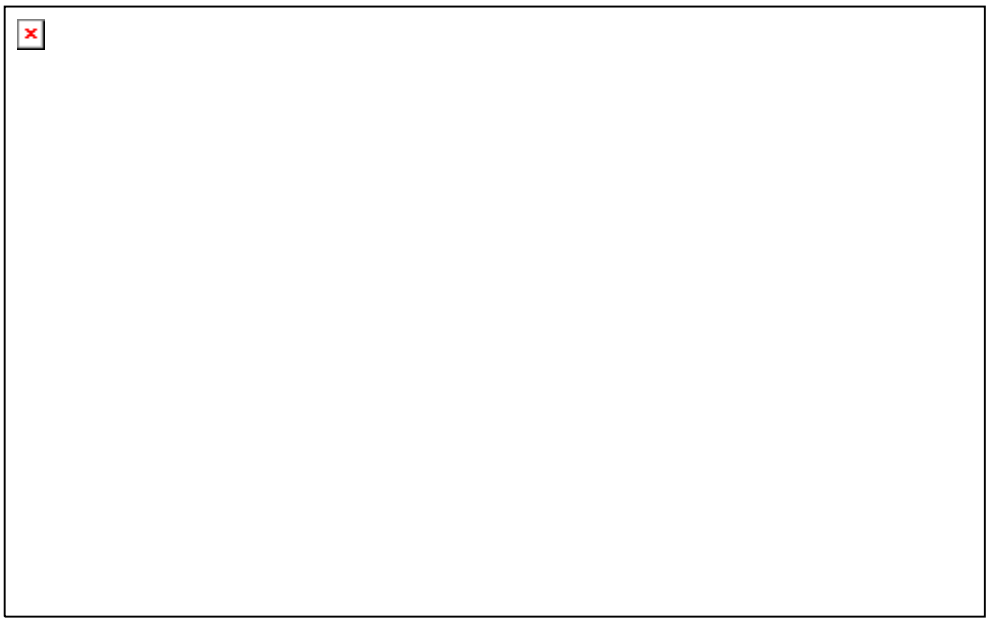
5.2.4.6 S.M.A.R.T.

Through the S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) system, modern hard disk drives incorporate a suite of advanced diagnostics that monitor the internal operations of a drive and provide an early warning for many types of potential problems. When a potential problem is detected, the drive can be repaired or replaced before any data is lost or damaged. Here you can find tree with hard drives for which you can view S.M.A.R.T. information. It is possible to view information about separate hard drive or summary for all drives in the system.
To view S.M.A.R.T. information for a hard drive - please click on appropriate drive name.
To view summary please click on "all units"



Function: S.M.A.R.T. units health status

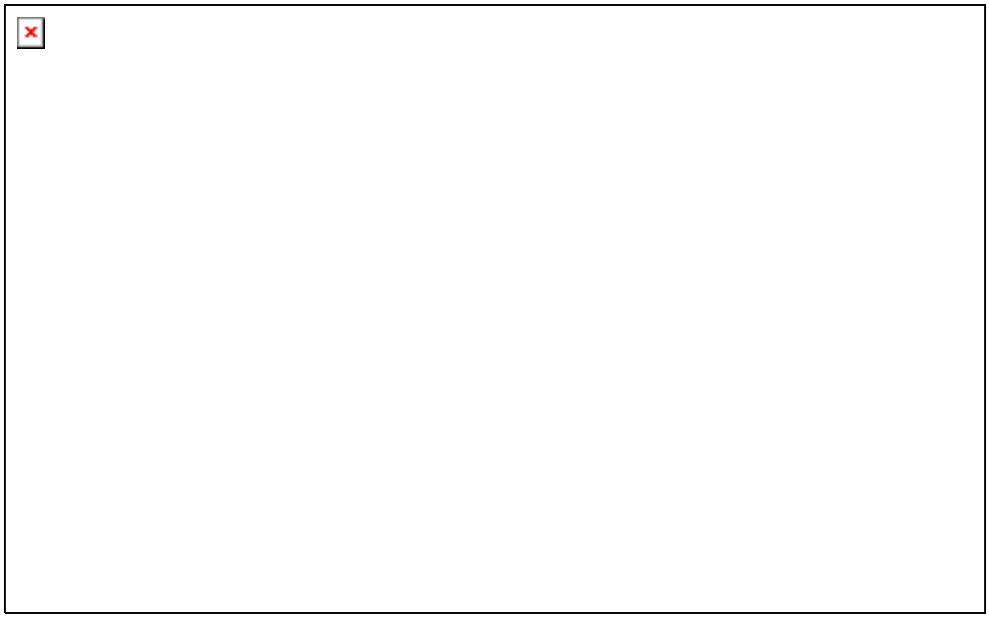
This function allows you to check S.M.A.R.T. status of hard disks. S.M.A.R.T. is a monitoring system for computer hard disks to detect and report on various indicators of reliability, in the hope of anticipating failures. To enable S.M.A.R.T. checks you need to use Hardware Configuration tool on console and enable it in Functionality options (press F1 on console to find out keyboard shortcuts).



Function: S.M.A.R.T. info

This function allows you to view S.M.A.R.T. parameters which this disk is able to return. In the upper part of this function you can see elementary parameters of hard drive such as device model or serial number. Below there is a table with S.M.A.R.T. attributes. In first column you

will find an attribute name, in second - minimum threshold value of this parameter, then current value, next worst value and after the status.
If value of attribute have ever exceeded worst of this value then the status will be "failed".
If value of attribute is on the edge of worst value then the status can be "pre-failed".
On some hard drives part of attributes can be displayed as "Unknown_Attribute" - this can happen when producer of that hard drive have done some modifications in S.M.A.R.T. and this changes are not yet supported by our software.
Button "view errors" provide you ability to view S.M.A.R.T. log of that drive which is generated automatically.



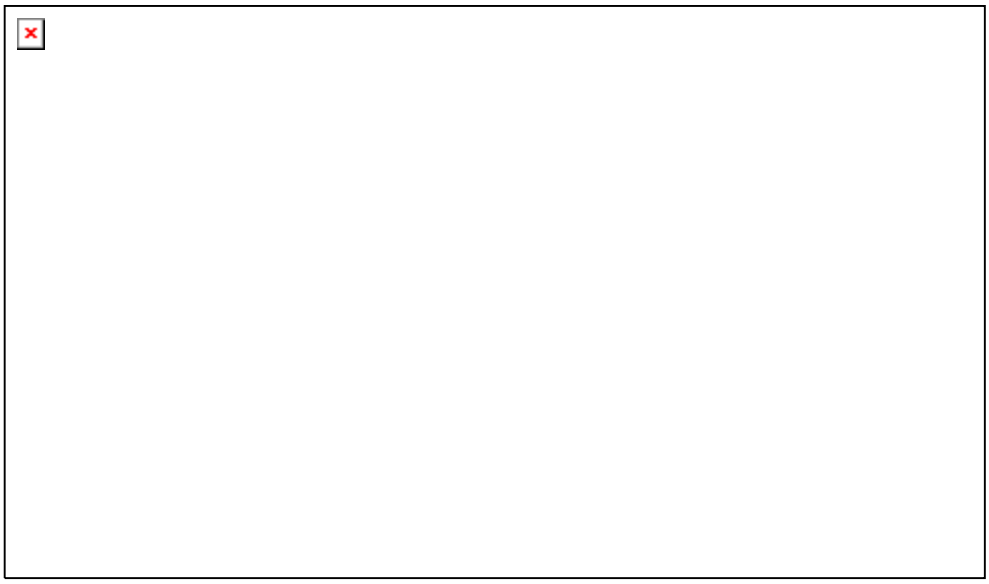
Function: S.M.A.R.T. test

This function allows you to perform short and long test of hard drive. You will be informed about progress of test. After finish of test please click on "results" button to view test log. Performing a test is not recommended during normal (daily) usage of that hard drive. It can happen that on some motherboards and controllers S.M.A.R.T. tests will not work.

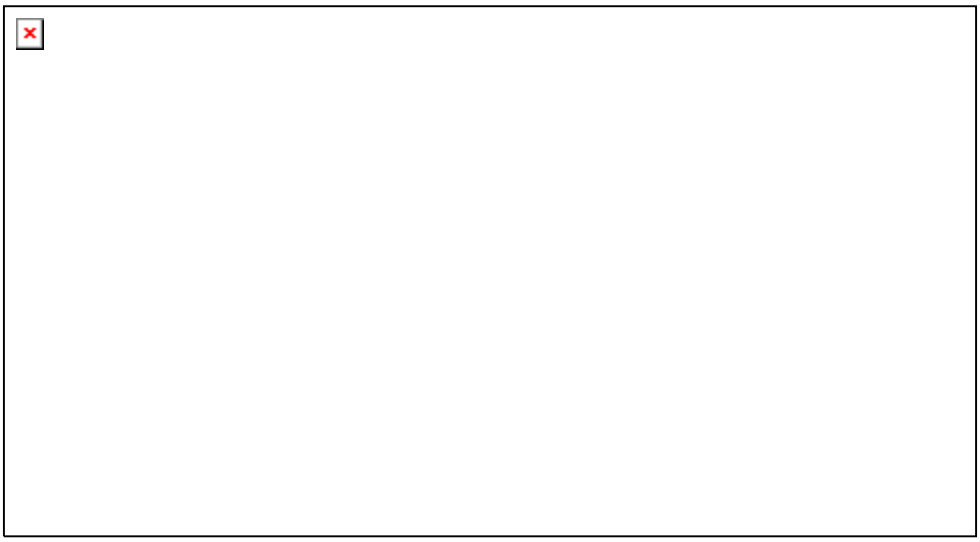
5.2.5 HELP

5.2.5.1 Software License

When accessing Help - “software License” you can read the license for software included in uNAS/tNAS



5.2.5.2 About uNAS/tNAS



Function: Register

In this function you can find link to our registration form. Note that registration is required to receive updates and new versions. Registration gives you also opportunity to receive e-mail notification about software news.

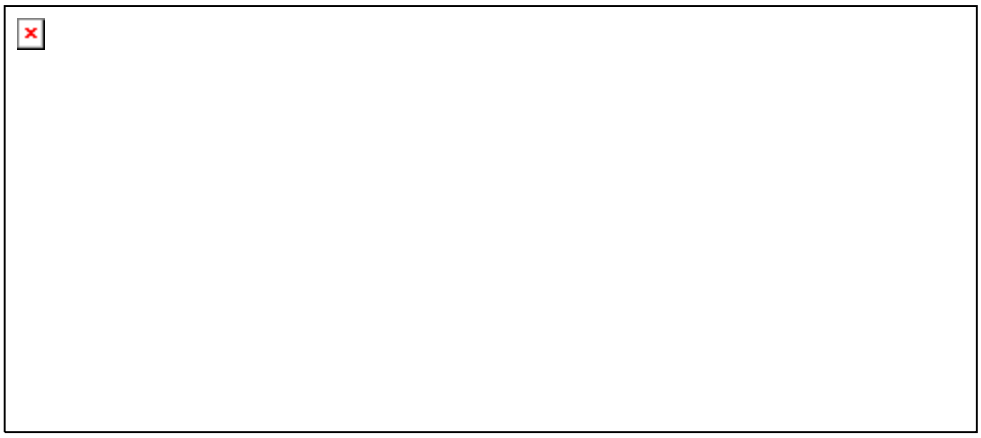
Function: Manual

You can download the manual here and print for fast reference.
In order to read the manual, you need a PDF viewer such as the Acrobat Reader (http://www.adobe.com).

Function: Service

Please have the following information available before contacting Technical Support team:

Logs which you can download in menu: “status” ▯ “hardware” ▯ “logs”.
Your software version which you can find in menu: “help” ▯ “about”



Function: Add license key

Here you can enter license key to expand functionality of server. For example you can add a license key for bigger capacity of storage volume. You log out by closing the browser window.

6 Troubleshooting Guide

Here is a list of common error messages and their meanings as well as corresponding tips on how to resolve the underlying problem. If your error message is not listed here please contact Open-E's support and service team (see section “help” above). Our staff will help you find a solution.

Error: user already exists

There cannot be more than one user with the same name. You cannot create a user twice. Check your spelling. Remember, user names are not case-sensitive. You can check existing user names by expanding the tree diagram on the left.

Error: values are not valid

You have entered an invalid parameter. IP addresses have the form aaa.bbb.ccc.ddd: All four parameters range between 0 and 255 and are always separated by periods.

Error: resource already exists

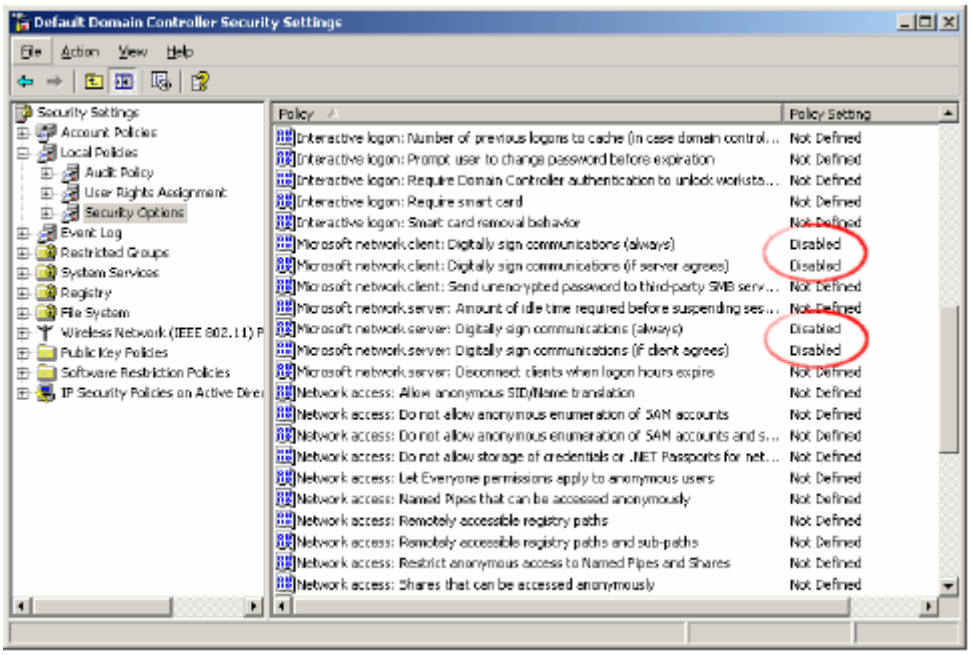
You cannot create more than one resource with the same name. You cannot create a resource twice. Check your spelling. Remember that resource names are not case sensitive. You can check existing resource names by expanding the tree diagram to the left.

Error: passwords do not match

Make sure that you type the same password in each entry field. For safety reasons, the passwords are not displayed. Type slowly. Check the status of the Shift, Caps Lock, Control, and Alt-keys.

Error: uNAS/tNAS cannot import the user database from a Windows Server 2003 domain.

In this case the following setting within the local security guideline may solve this problem:



Error: Update file not found

You instructed uNAS/tNAS to perform a systems update, but did not supply a valid uNAS/tNAS update file. Download the latest uNAS/tNAS update file from the www.open-e.com Web site. Next, copy the upgrade file into your "update" folder (please spell upgrade lower case). Finally, select "update" from the menu.

Error: No share volume

You must create a volume for file sharing before you can create any resource shares or search for shares. Look into the “Getting Started” section of this manual for instructions on creating a share volume.

Error: No share volume to browse

You must create a volume for file sharing before you can browse it in order to create resource shares.

Error: Invalid user name!

User name cannot:
(1) Contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `
(2) Begin or end with a space
The use of the SMB (Server Message Block) protocol from Windows, also known as CIFS or Samba, places some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. User names must not contain any of the above mentioned characters.

Error: invalid user password

A user password cannot begin or end with a space. Spaces are not legitimate characters at the beginning and end of a password. Maybe you inadvertently hit the space bar during password entry. Please reenter your password.

Error: invalid administrator password

Administrator password cannot begin or end with a space. Spaces are not legitimate characters at the beginning and end of a password. Maybe you inadvertently hit the space bar during password entry. Reenter your password.

Error: invalid resource name

Resource name cannot:
(1) Contain characters: * : " | < > ? / \ ` # $ & ( ) + ; ' .
(2) Begin or end with a space
The use of the SMB (Server Message Block) protocol from Windows, also known as CIFS or Samba, lays some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Resource names cannot contain any of the above mentioned characters. Note that the list of invalid characters is slightly different than that for other name fields.

Error: invalid workgroup name

Workgroup name cannot:
(1) Contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `
(2) Begin or end with a space
The use of the SMB (Server Message Block) protocol from Windows, also known as CIFS or Samba, lays some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Workgroup names cannot contain any of the characters listed above. Note that the list of invalid characters is slightly different than that for other name fields.
The invalid characters for workgroup names are different than the ones for other fields.

Error: invalid server name

Server name cannot contain:
(1) Characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `
(2) Spaces
(3) Digits only
The use of the SMB (Server Message Block) protocol from Windows, also known as CIFS or Samba, lays some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Server names cannot contain any of the above mentioned characters. Note that the list of invalid characters is slightly different than that for other name fields. In addition, server names cannot be constructed from numbers only, they must contain alpha characters.

Error: invalid resource comment

Resource comment cannot be longer than 256 characters
Resource comments have a limit of 256 characters, a limit which cannot be exceeded.
Use a shorter comment.

Error: invalid directory name

Directory name cannot:
(1) Contain characters: * : " | < > ? / \ ` # $ & ( ) + ; ' .
(2) Begin or end with a space
The internal operating system of uNAS/tNAS does not allow certain characters to be used for directories. The above mentioned characters are invalid, just as trailing or leading spaces. Choose a different name.

7 Appendix A

Open-E Software License agreement

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. OPEN-E GMBH AND/OR ITS SUBSIDIARIES ("OPEN-E") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT.

THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND OPEN-E. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN NINETY (90) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

The terms of this software license agreement, do not apply to the Free Software Programs distributed with Open-E software. Instead, those programs are covered by other licenses, including the GNU General Public License. A copy of the GPL along with the other applicable Free Software Licenses, can be found in Appendix B.

Ownership and Copyright

The Open-E software is non-exclusive licensed and sold to you for use only as permitted by this License Agreement. Open-E GmbH reserves any rights not expressly granted to you. Copying of the software is prohibited by law unless specifically authorized in writing by Open-E GmbH. You may not use copy, modify, sell, lease, sublease or otherwise transfer Open-E software in whole or in part.

Intellectual Property Rights

The Open-E software contains intellectual property rights, and in order to protect them, you may not decompile, reverse engineer, disassemble or otherwise reduce the Open-E software to a human perceivable form.

Termination

This license will be automatically terminated without notice from Open-E GmbH if you fail to comply with any term or condition of this agreement. If you do not agree to be bound by these terms and conditions, you may not use the Open-E or any of its software components.

Disclaimer of Warranties

Open-E software are licensed "as is" without warrantee of any kind. Open-E GmbH hereby disclaims all warranties express and implied, relating to Open-E , the installation utilities and the embedded software including, without limitation, any implied warrantee of merchantability, fitness for a particular purpose or non-infringement.

Limitation of Liability

In no event will Open-E GmbH liability under this agreement exceed the price that you paid for your Open-E software. Furthermore, in no event will Open-E GmbH be liable for any lost profits, lost data, cost of procurement of substitute goods or services, or any special consequential, incidental, indirect or punitive damages arising out of or under this agreement.
The limitation of liability set forth in this paragraph will apply, whether or not Open-E GmbH was advised of the possibility of the loss, liability or damages and notwithstanding any failure of essential purpose of any limited remedy.

Waiver

No delay or failure of Open-E GmbH to exercise any right under neither this agreement nor any partial exercise thereof shall be deemed to constitute a waiver or any rights granted hereunder or under law.

Unlawful Provisions

If any provision of the agreement is held to be unenforceable for any reason, all other provisions of this agreement shall nevertheless be deemed valid and enforceable to the fullest extent possible.

Entire Agreement

This agreement constitutes the sole and exclusive agreement between the parties concerning the subject matter hereof.

LIMITED WARRANTY

Open-E warrants that the media on which the software is distributed will be free from defects for a period of ninety (90) days from the date of delivery of the software to you. Your sole remedy in the event of a breach of this warranty is that Open-E will, at its option, replace any defective media returned to Open-E within the warranty period, or refund the money you paid for the software. Open-E does not warrant that the software will meet your requirements, that operation of the software will be uninterrupted, or that the software will be error-free.

Authorized Service

Only an authorized service representative can service Open-E software. Failure to comply with this requirement will void the warranty.

Applicable Law

This agreement shall be governed by German law. You agree to jurisdiction and venue in the courts located in Munich, Germany for all claims, disputes and litigation arising under or related to this agreement.

102

8 Appendix B

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. or example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you". A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library

or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".) "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying,

distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the

Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version

than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.
Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.
This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.
If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.
5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License. However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.

Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.
If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.
6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.
You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then

relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions).

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

f) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

g) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work. 8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. .Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.
If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).
To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.
<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>
This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.
This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public
License for more details.
You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Also add information on how to contact you by electronic and paper mail. You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary.
Here is a sample; alter the names:
Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.
<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!