SoftNAS CLOUD®

Powerful and Frictionless Storage Administration

SoftNAS™ Cloud Reference Guide

Table of Contents

SoftNAS Overview and Links

SoftNAS™ is a network attached storage (NAS) that serves as a virtual storage appliance (VSA). **SoftNAS** provides commercial-grade storage management capabilities for small to large businesses that require high-speed, reliable storage at affordable prices.

The NAS software virtual appliance can run in any of the following different platforms.

1. Cloud Computing Environments such as **Microsoft Azure, Amazon Web Services,** and **VMware vCloud Air.**

2. Local virtual server environment such as **VMware.**

Note: Before you start working on **SoftNAS**, please refer to the **SoftNAS Installation and User Guide.**

For more information on working with SoftNAS, refer to the following links in this guide.

- **Interface Elements**
- **Managing Dashboard**
- **Working with Storage Section**

Notices

This document is provided for informational purposes only and **SoftNAS, Inc.** makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user.

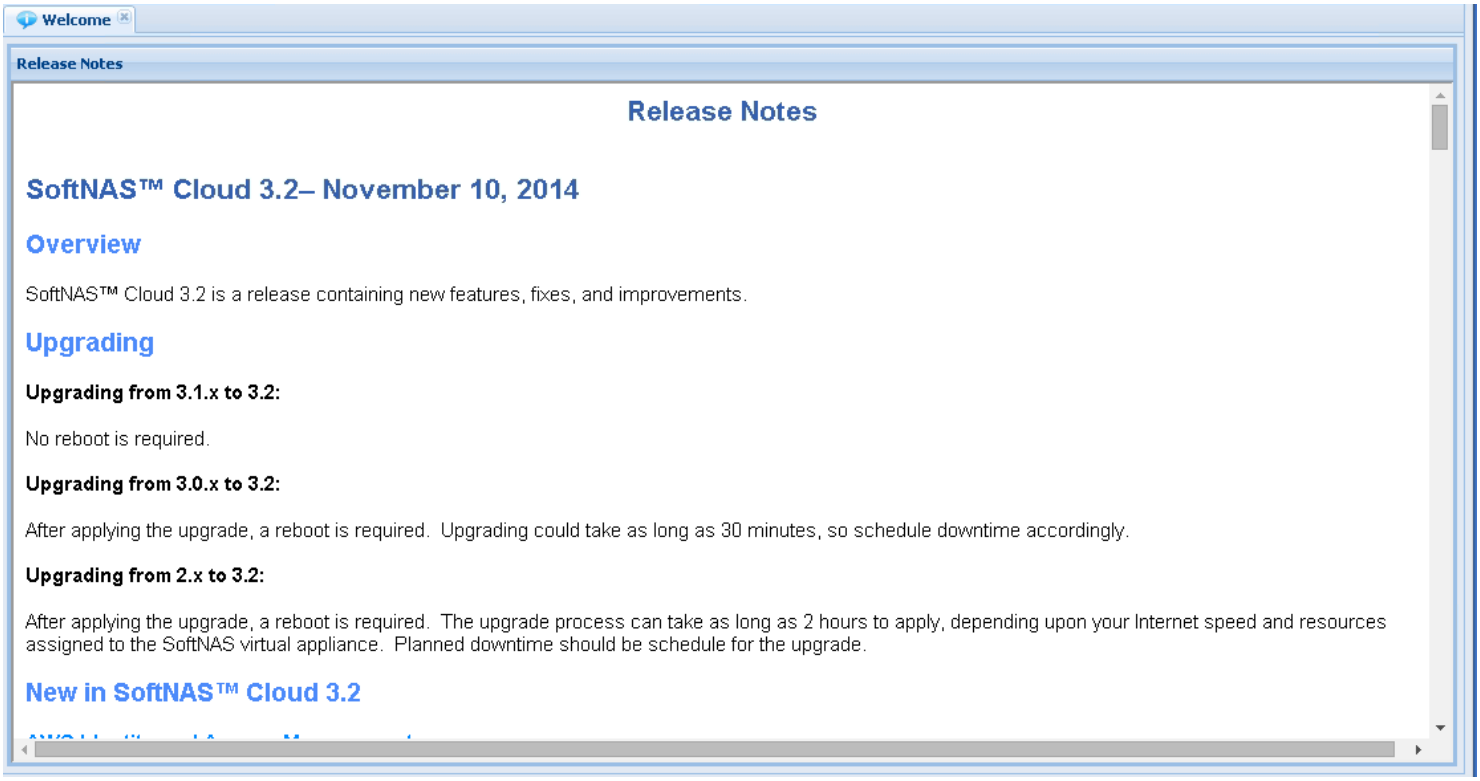
Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of **SoftNAS, Inc.**

SoftNAS, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from **SoftNAS, Inc.,** the furnishing of this document does not guarantee any license to these patents, trademarks, copyrights, or other intellectual property.

SoftNAS StorageCenter™, SnapReplicate™, and **SNAP HA™** are trademarks of **SoftNAS Inc.** All other trademarks referred to in this guide are owned by their respective companies.

Welcome

The **Welcome** panel displays the Release Notes for the latest version of SoftNAS available. As such, the Welcome Panel is the best place to stay up to date with the latest changes to the platform. (Information may have changed since the publication of this document.)



Getting Started Checklist

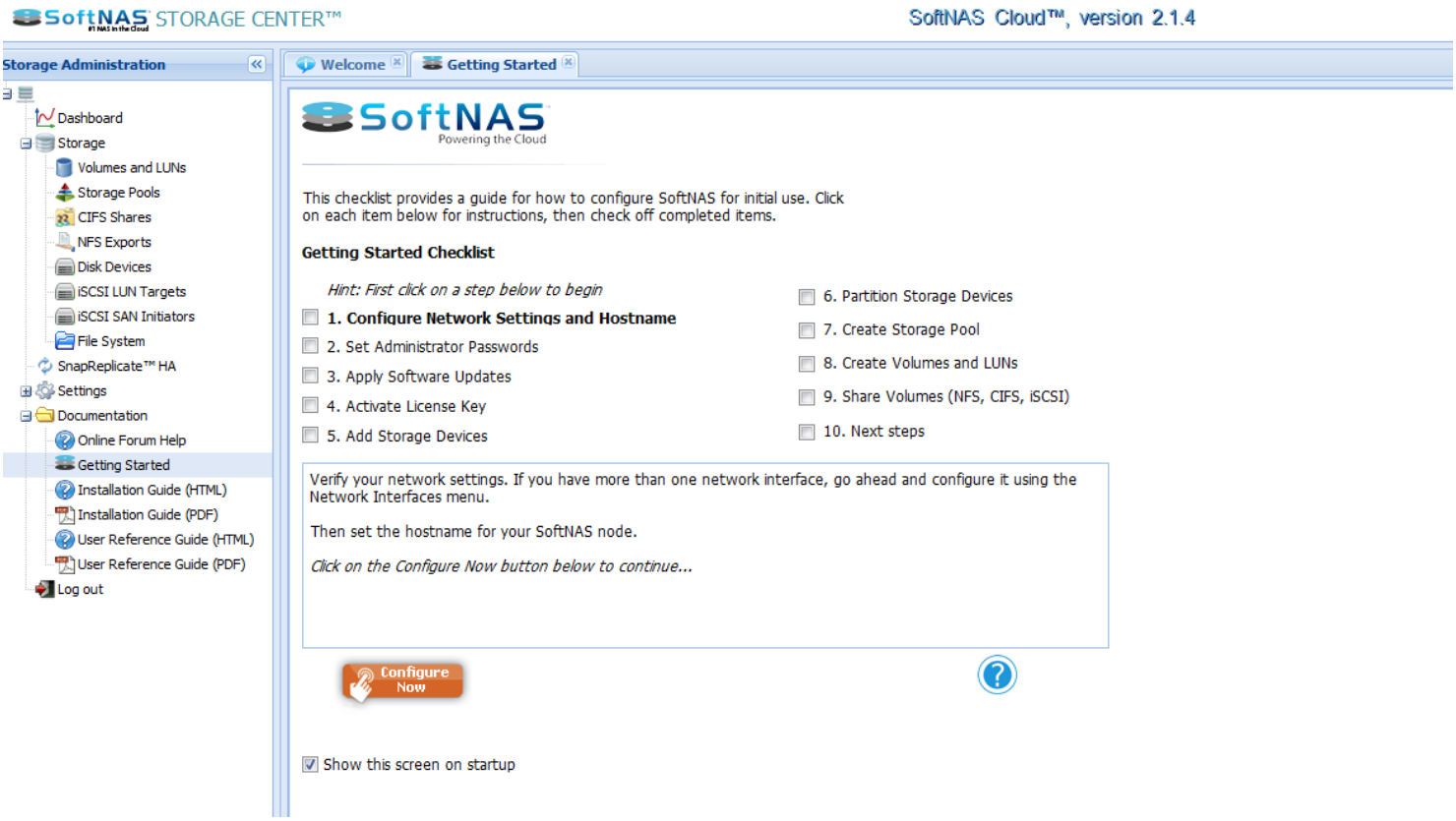
When **SoftNAS StorageCenter** is first started, the **Getting Started Checklist** will be displayed. This helper provides a set of step-by-step, on-screen instructions designed to make initial configuration, setup and use of **SoftNAS** faster and easier for first-time users.

Access this option from the **SoftNAS Documentation** section.

1. Log on to **SoftNAS StorageCenter.**

2. In the **Left Navigation Pane,** select the **Getting Started** option under the **Documentation** section.

The **Getting Started Checklist** panel will be displayed.



1. Click the step to configure.

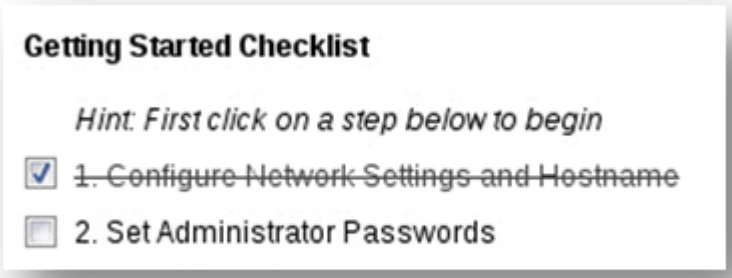
2. Follow the steps as described in the **Instruction Box.**

3. Click the help button (**?**) for more information and detailed instructions on how to configure the item in the selected step.

4. Click the **Configure Now** button to launch the configuration settings window for the step.

5. When the configuration task for the selected step is completed, click the checkbox in the next step.

The step will be marked off the list to show that it is completed.



6. Repeat the procedure to complete the tasks of each configuration step.

7. When all the initial configuration steps are completed, check the box in the **Show this screen on startup** field.

8. Close the **Getting Started Checklist** panel.

Changing Default Passwords

When logging in to the **SoftNAS StorageCenter** for the first time, use the super-user login credentials such as **root** and **softnas** as users and **Pass4W0rd** (that's a zero) as system default password.

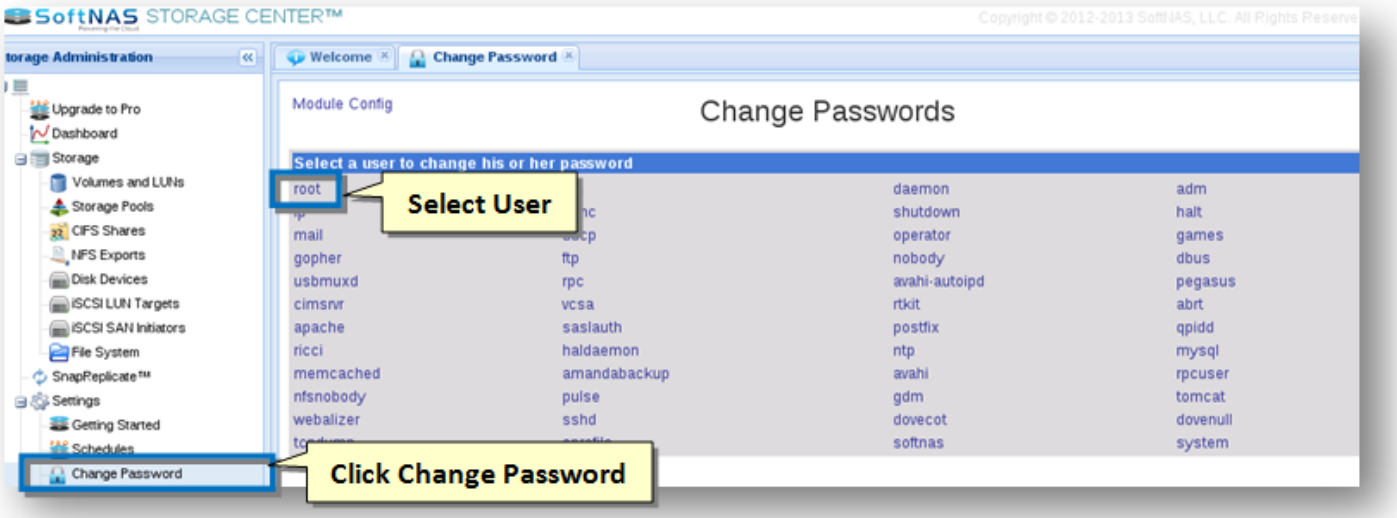
For security reasons, it is recommended to change these passwords to unique, secure passwords to increase the security of mission-critical data managed by **SoftNAS.**

To Change a Password

1. Log on to **SoftNAS StorageCenter.**

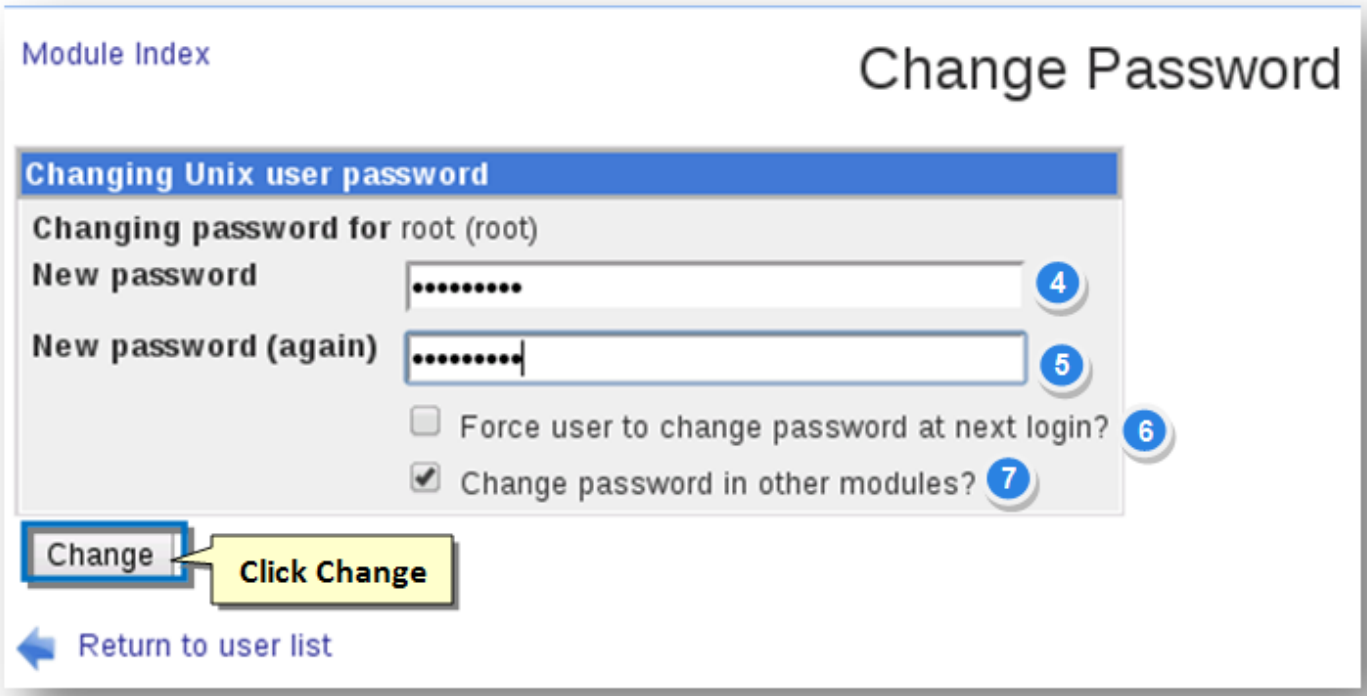
2. In the **Left Navigation Pane,** select the **Change Password** option under the **Settings** section.

The **Change Password** panel will be displayed.



3. Select the user to which you wish to change the password from the list of users.

The **Changing Unix User Password** section will be displayed.



4. Enter the new password in the **New Password** text entry box.
5. Confirm the password by re-entering it in the **New Password (Again)** text entry box.
6. Check this box if you want to force the user to change the password when he logs on to the system next time.
7. Check this box if you want to enforce the change of password in other modules also.
8. Click the **Change** button.

The password of the selected user will now be changed and he/she can now log on to the system with the new password.

Updating to Latest Version

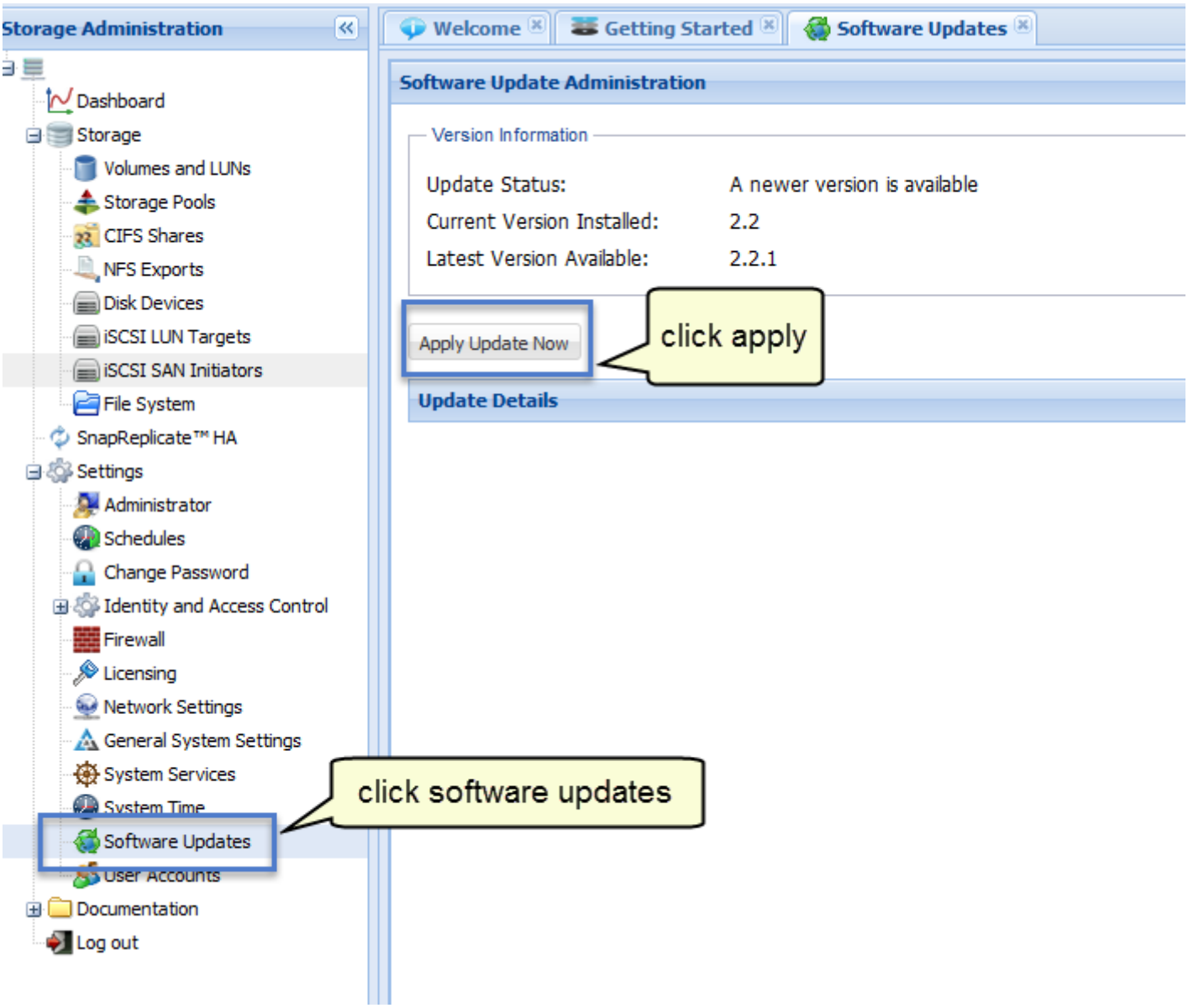
After installing **SoftNAS,** it is recommended to perform a software update to ensure that you are running the latest version.

Updating **SoftNAS** to latest version is very easy. Simply follow the steps given below.

1. Log on to **SoftNAS StorageCenter.**

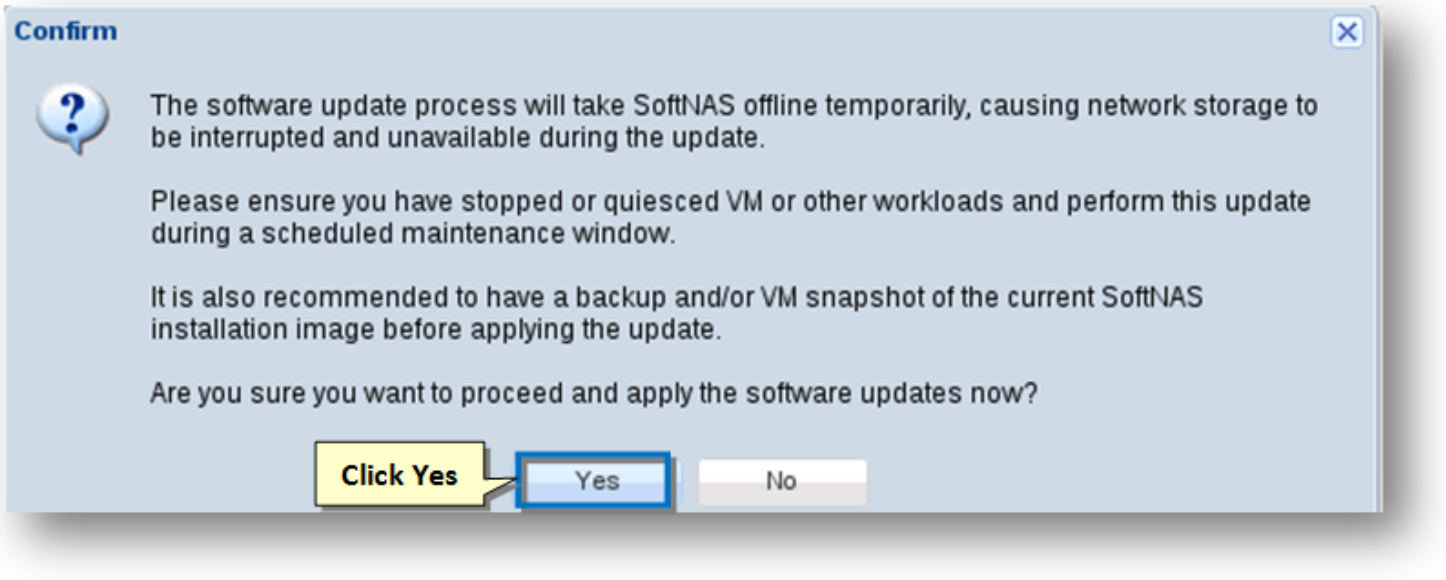
2. Click the **Software Updates** option under the **Settings** section in the **Left Navigation Pane.**

The **Software Updates** panel will be displayed.



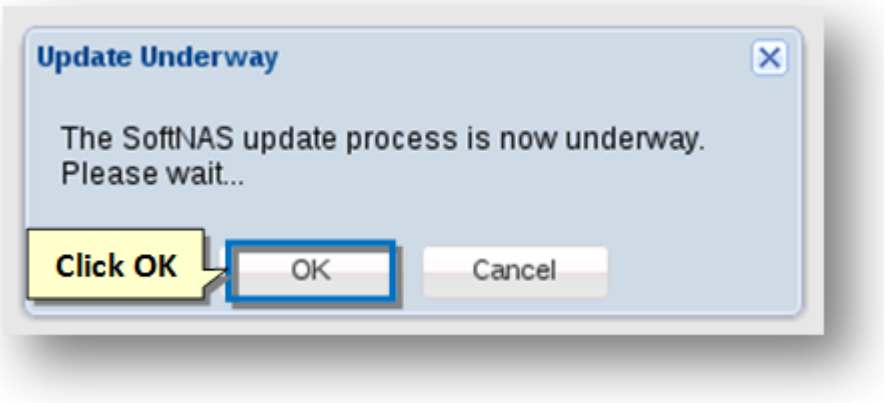
3. Click the **Apply Update Now** button.

The **Confirm** message box is displayed, recommending that a backup/VM Snapshot be taken before applying the update.



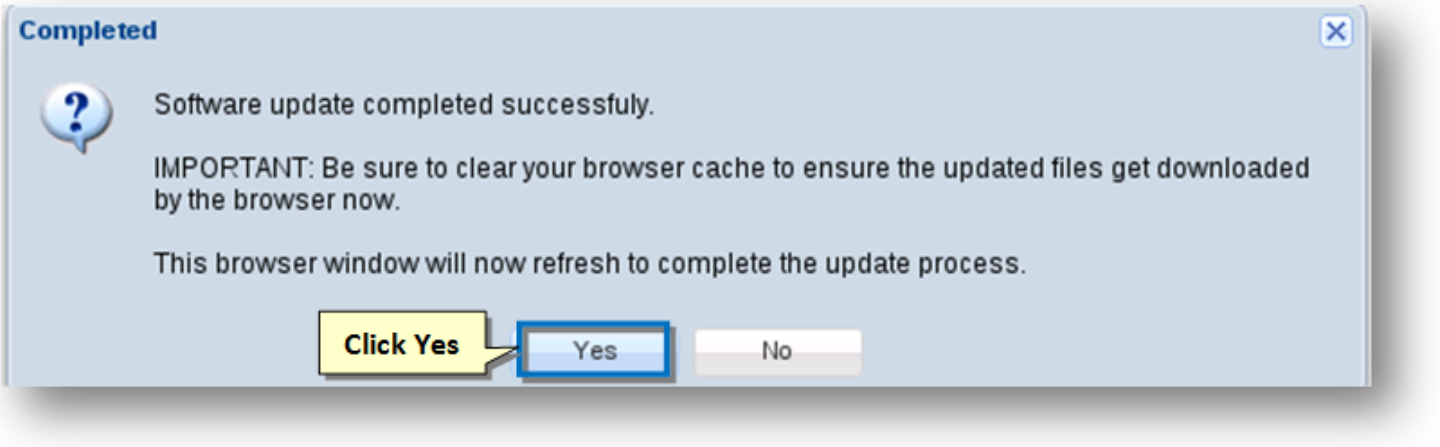
4. Click the **Yes** button.

The **Update Underway** message box informing you about the progress of the update process will be displayed.



5. Click the **OK** button.

The **Completed** message box informing you of the successful completion of the update process will be displayed.



6. Click the **Yes** button.

The software update will be performed.

Note: It is recommended to clear the browser cache and reload the application.

Activating Your SoftNAS License

Each of the **SoftNAS** versions use the same installation images. The differences in capabilities are based upon the type of license key assigned after installation.

By default, **SoftNAS** contains a built-in SoftNAS Cloud® Free Trial with 20 TB of storage. To gain access to additional storage capacity and features and personalize your **SoftNAS** product after installation, be sure to activate **SoftNAS** using the license key found in your customer control panel.

The available versions of SoftNAS that have different license keys are:

SoftNAS Cloud® - 20 TB of storage.

- Annual Redundant
- Annual Subscription
- Monthly Redundant
- Monthly Subscription

SoftNAS Cloud® Enterprise™ - 16 PB of storage

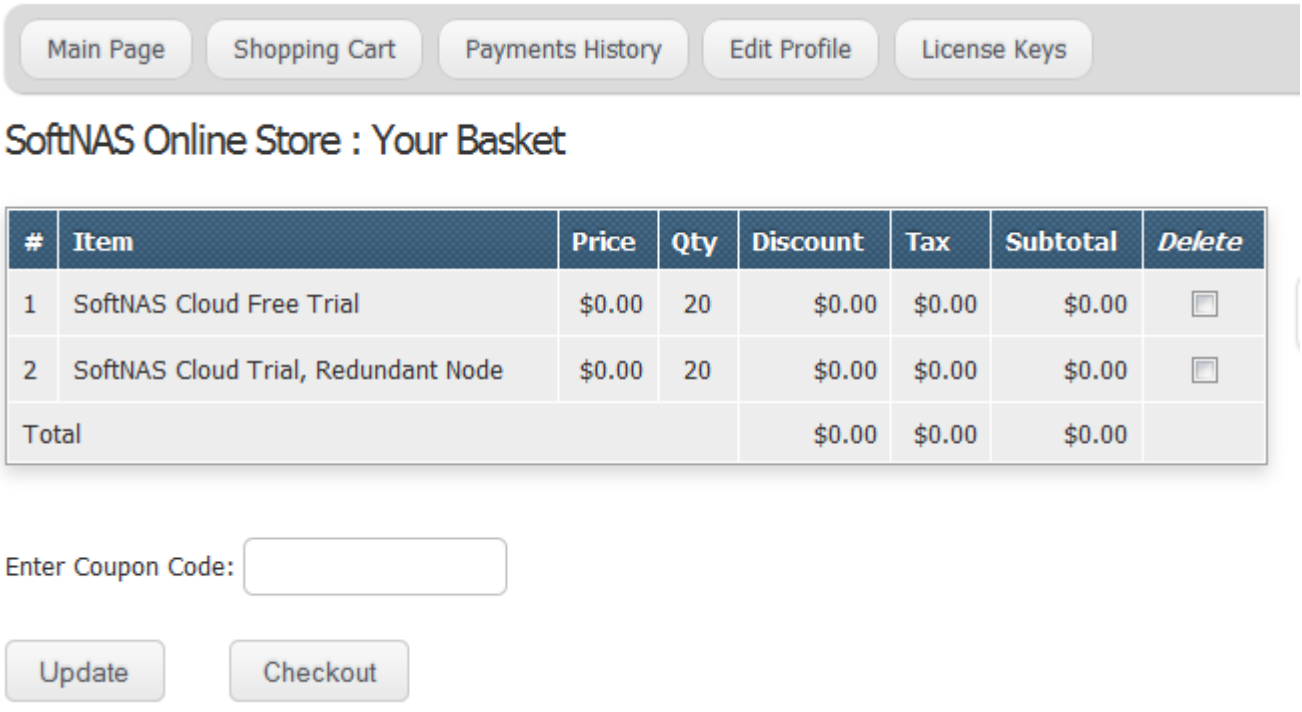
- Annual Redundant
- Annual Subscription
- Monthly Redundant
- Monthly Subscription

To activate your **SoftNAS** product

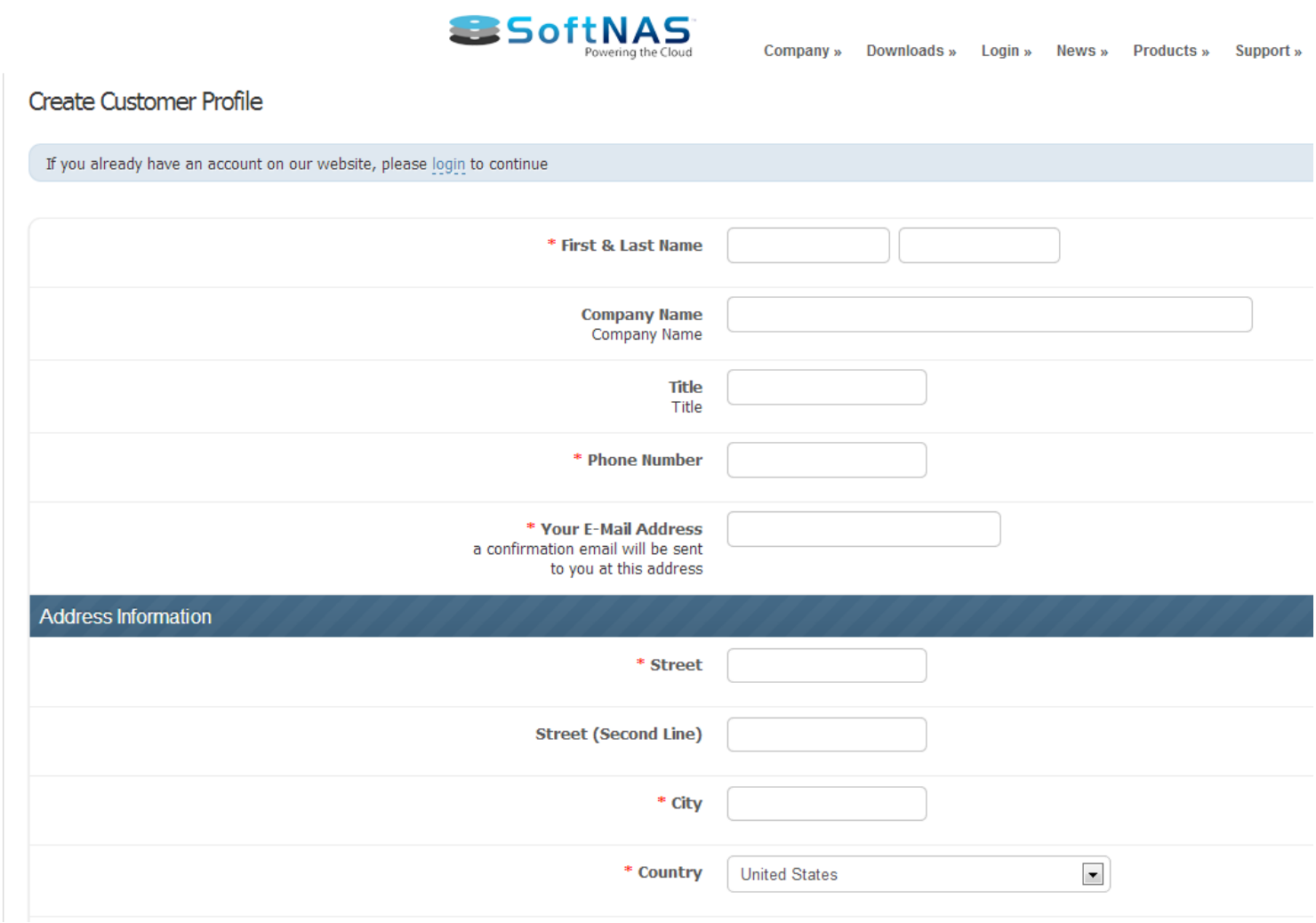
1. Using a web browser, visit www.softnas.com and click on the Login link, then click on **Register.**

2. You will see a screen that says **Adding Trial to Cart...**.

The screen will display the trial items that you are qualified for, as per the screenshot below.



3. Click **Checkout** to continue with the registration process.



4. Fill out the registration form to create a customer profile. On the thank you page, press the link to access the customer area and your license keys.

Note: If you are an existing customer, simply use the Login link on the site and log in. the following steps apply to both new sign-ups and existing customers.

5. Click the **License Keys** tab to access your download license information.

The **License Keys, Downloads and Support** information will be displayed.

6. Copy or note down the license key from the required **SoftNAS** product version.

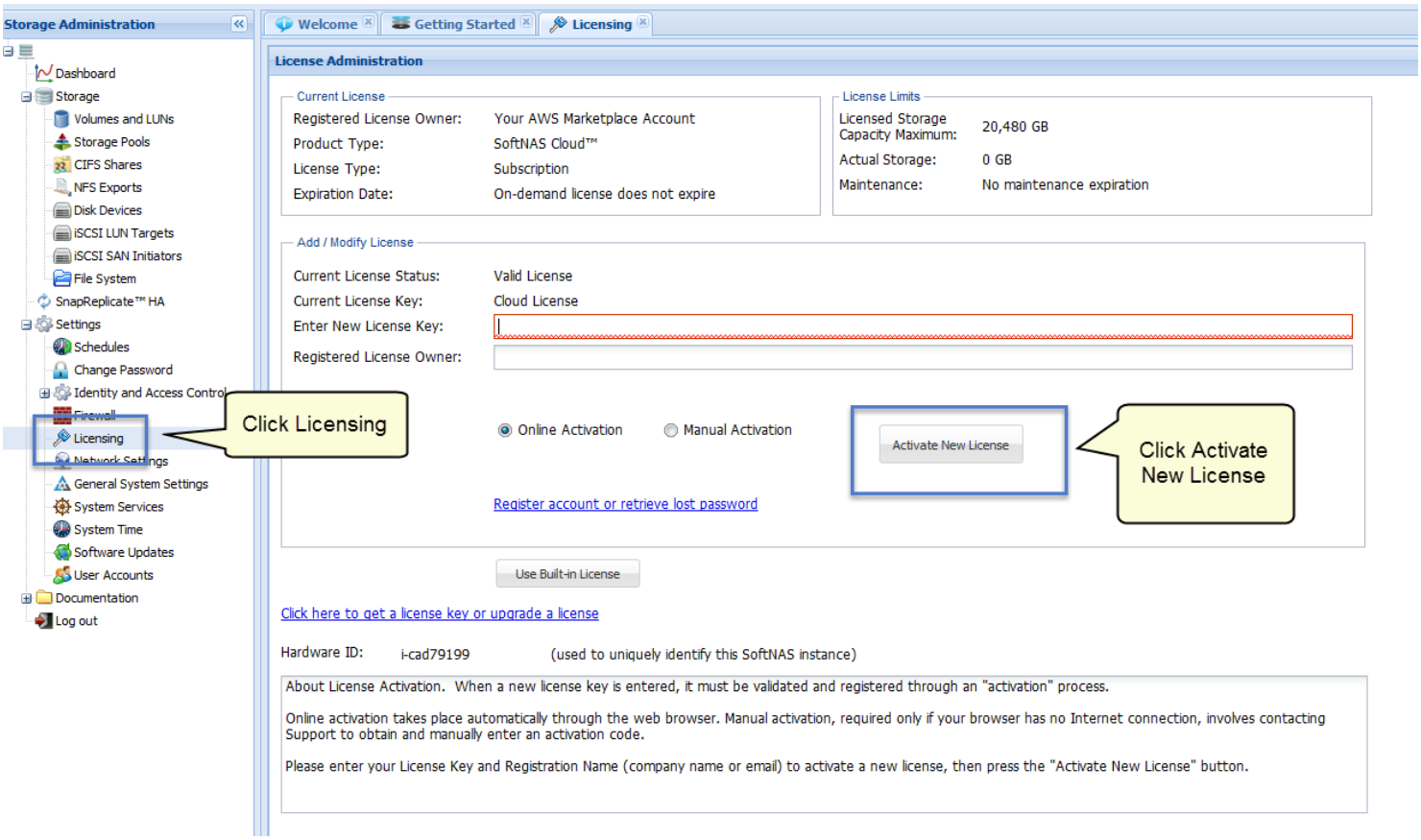
7. Now log on to **SoftNAS StorageCenter.**

8. In the **Left Navigation Pane,** select the **Licensing** option under the **Settings** section.

The **Licensing** panel will be displayed.

Note: If you are using the Internet Explorer browser with Extended Security Configuration (ESC), you must **disable ESC before activating**. ESC interferes with normal Javascript operation and is not supported. If ESC is enabled, activation will not operate correctly, so be sure to verify it is disabled.

Note: Before activating the license key, if you are using a dynamic IP address assigned by DHCP, **be sure to configure SoftNAS with a static IP address** first. The activation process will lock your NAS to its operational IP address for production use (on Amazon EC2, this does not apply - instance ID is used instead of IP address).



10. Paste the copied license key or manually enter the key in the **Enter New License Key** text entry box.

11. Enter the name of the license owner in the **Registered License Owner** text entry box.

12. Click the **Activate New License** button.

The license is activated.

Note: The license activation associates your **SoftNAS** license to the IP address (**VMware**) or EC2 instance (**Amazon EC2**).

This IP address (or EC2 instance ID) is fixed and will not change during normal production operation. In case you wish to move your **SoftNAS** license to a different machine. please contact our support team. We will help you in deactivating your old license and activate it at new machine.

If you are using **SnapReplicate** between two **SoftNAS** nodes, then you will need a unique license key for each node.

Manual Activation

In cases where **SoftNAS** does not have outbound Internet access (for security or other reasons), the license must be activated manually.

Note: For manual activation, please contact **SoftNAS Support** and we will provide you with a unique **Activation Code** that you can enter to manually activate **SoftNAS**.

Automatic Recurring Subscription Updates

Once per month or year, depending on your **SoftNAS** subscription period, **SoftNAS** will automatically contact the **SoftNAS** license activation server to verify the renewal of your subscription. If it was renewed successfully, the new license key will be automatically downloaded and activated.

Note: Please ensure that **SoftNAS** has outbound Internet access for auto renewal to take place.

License Grace Period

In the event you are running **SoftNAS** In a production environment and your license expires, it will enter the grace period. During this grace period, all functions continue to be available, and each time you access the **StorageCenter UI,** you will receive a license expiration warning notice, reminding you that auto-renewal has not occured for some reason (e.g., **SoftNAS** not connected to Internet, credit card on file failed or expired, etc.). You will also have received email notifications about renewal separately.

Note: The grace period defaults to one week (7 days) for **SoftNAS Professional Edition**, providing ample time to resolve any license renewal issues. If there is a billing error, once that is corrected, the system will automatically download and install the renewed license key. If you are operating **SoftNAS** without an Internet connection, it is recommended to use the annual subscription method, so you only need to enter a license key once a year (or you can license **SoftNAS** for multiple years if you prefer).

Accessing Online Help

You can access Online Help and documentation from your **SoftNAS** members area.

For more information, refer to **Support**

Support

Support for Premium SoftNAS Subscribers

Premium Paid SoftNAS Professional subscribers have the following support options:

- **Regular Phone Support:** Contact the helpdesk by phone during regular business hours 9 a.m. to 5 p.m. CST, Monday through Friday
- **24 x 7 Phone Support:** if you had purchased 24 x 7 business-critical support, you can contact the help desk anytime, 24/7
- **Helpdesk Tickets:** Open a help desk ticket for issue tracking and faster support
- **Email Support:** Email our support team (they will open a help desk ticket)

Support for Free Trial SoftNAS Subscribers

Free Trial and SoftNAS Essentials subscribers have the following support options:

- **SoftNAS Forums**

Accessing Premium Support Services

1. Log in to your **SoftNAS** customer account.

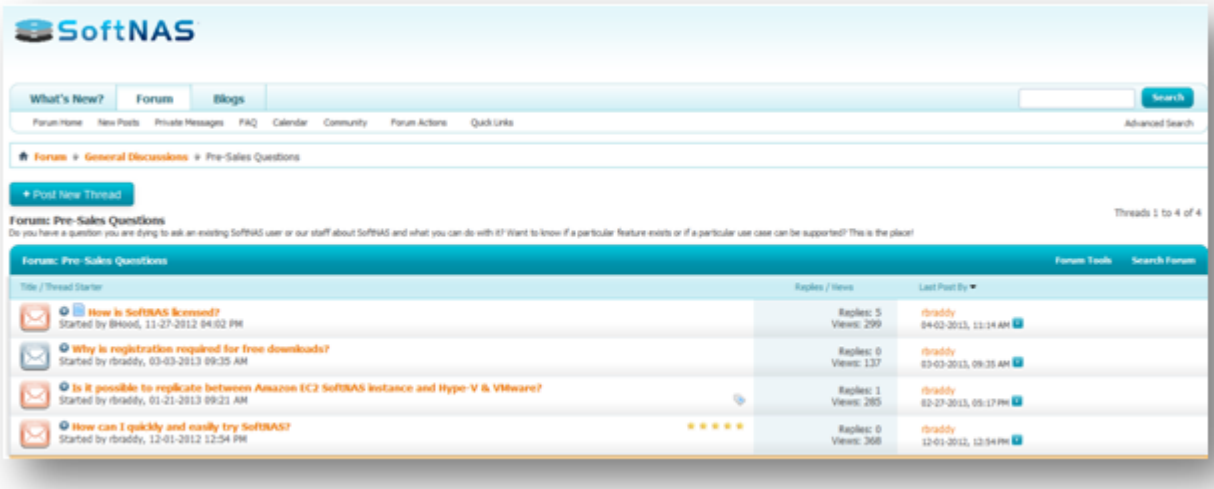
Your **SoftNAS** membership page will be displayed.

2. Click the **License Keys** tab to access your Premium Support services.

Accessing Pre-Sales Support Forums

You can access the pre-sales support forums in the following link -or- call us at the phone number listed on the website www.softnas.com.

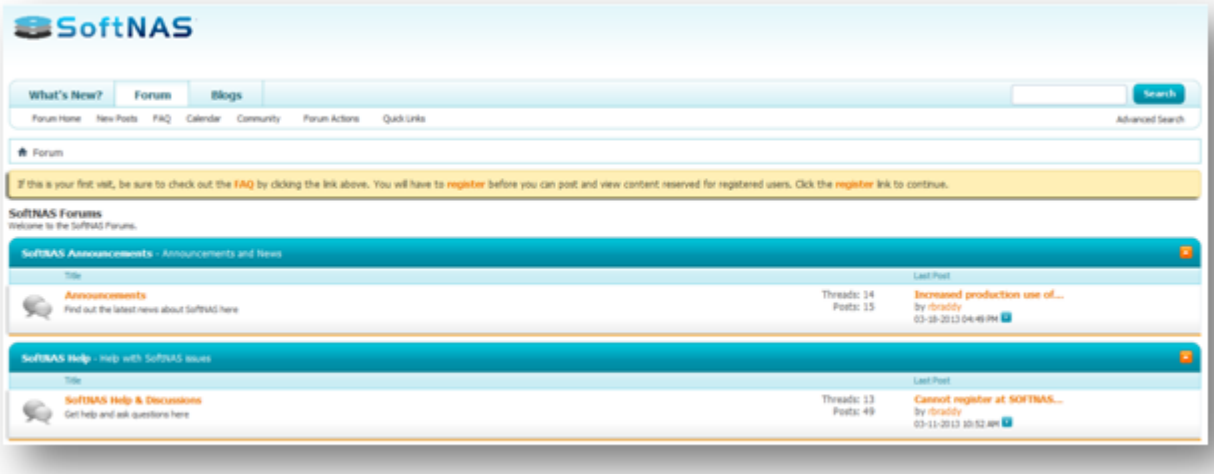
Pre-Sales Support Forums



Accessing Customer Support Forums

All **SoftNAS** customers can access the customer support forums in the following link.

Customer Support Forums

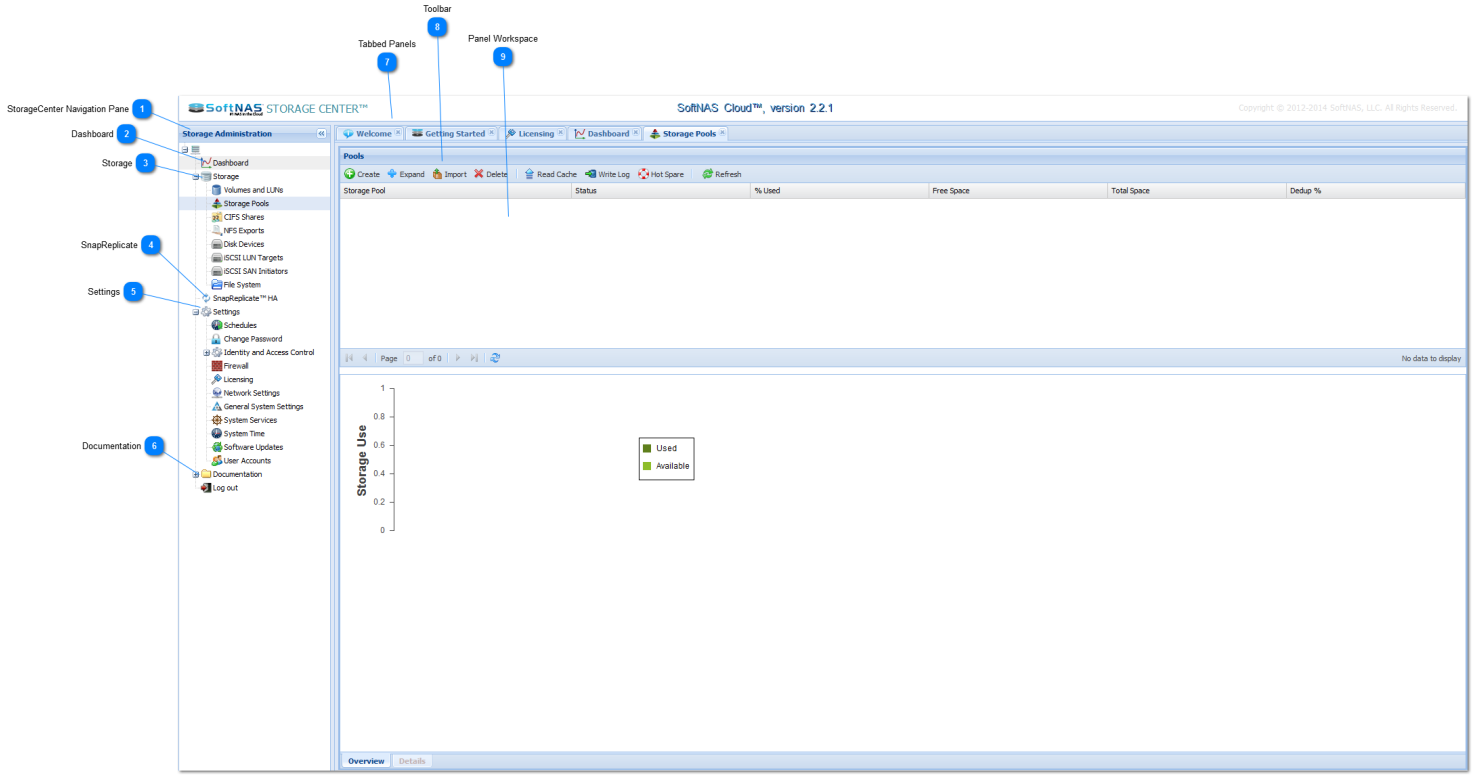


SoftNAS® Interface Elements

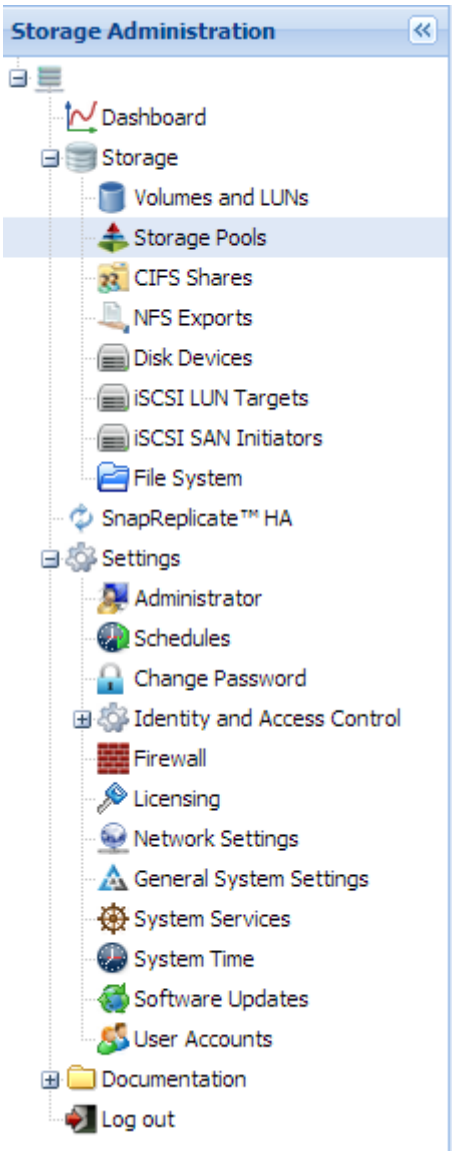
The **SoftNAS StorageCenter** administration interface provides you an easy and quicker access to various components and modules of the **SoftNAS** application.

The various components of **SoftNAS StorageCenter** interface are as follows:

- StorageCenter Navigation
  - Dashboard
  - Storage
  - SnapReplicate
  - Settings
  - Documentation
- Tabbed Panels
- Toolbar
- Panel Workspace

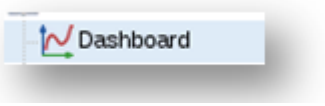


1 StorageCenter Navigation Pane



The **StorageCenter Navigation Pane** provides access to the core components and modules of the **SoftNAS** application. Simply click the required option in the navigation pane to open the related panel in the right section of the screen.

2 Dashboard

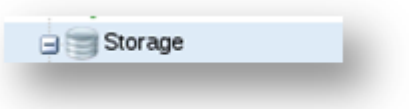


The **Dashboard** provides a quick summary of the key statistics and performance indicators.

For more information, refer to the following link.

Managing Dashboard

3 Storage



The **Storage** is one of the core sections of **SoftNAS StorageCenter.** It has the modules to configure **Volumes and Luns, Storage Pools, CIFS Shares, NFS Exports, Disk Devices, ISCSI LUN Targets, ISCSI LUN Initiators** and **File System.**

For more information, refer to the following link.

Working with Storage

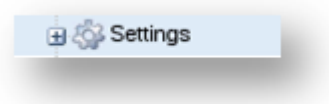
4 SnapReplicate

The **SnapReplicate** provides a simple yet powerful means of defining a replication relationship between two **SoftNAS** controllers - the **source node** and the **target node.**

For more information, refer to the following link.

Managing SnapReplicate

5 Settings

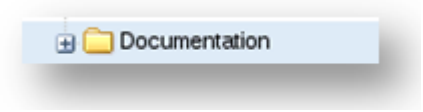


The **Settings** section allows you to configure many general and advanced and performance configurations common to all platforms. It has the modules to configure **Schedules, Change Password, Kerberos, Firewall, Licensing, Network Settings, General System Settings, System Services, System Time** and **Software Updates.**

For more information, refer to the following link.

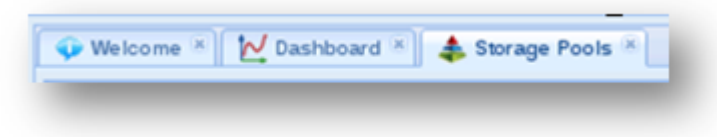
Working with Settings

6 Documentation



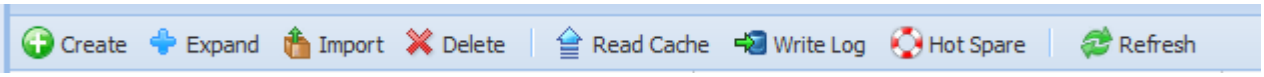
The **Documentation** section has all the links to all the documents of the SoftNAS application. You can find the links to the Installation and Reference guides of the application. You can also use the **Getting Started** helper in this section to quickly configure the required steps.

7 Tabbed Panels



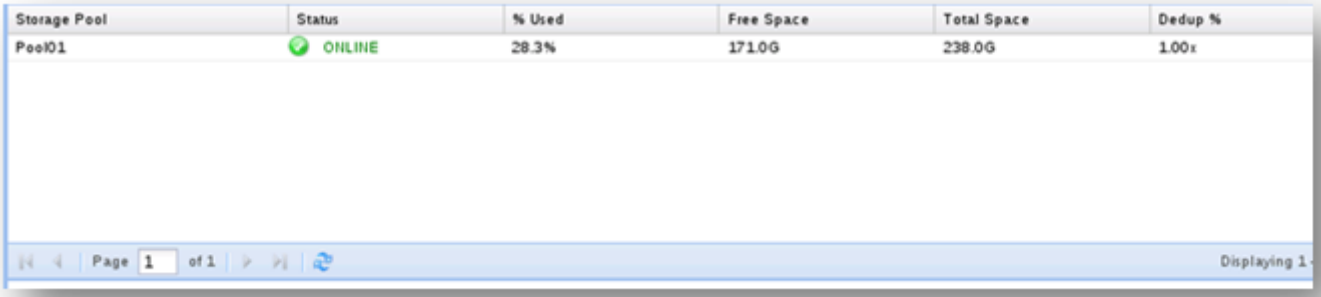
The **Tabbed Panels** section displays all the panels that are opened. You can navigate to any panel by simply clicking the title of the required panel in this section. To close a panel, simply click the close (**X**) button of that panel.

8 Toolbar



The **Toolbar** is available in several modules of the **SoftNAS** application. Based on the module, the tools in the toolbar are specific to each of those modules.

9 Panel Workspace

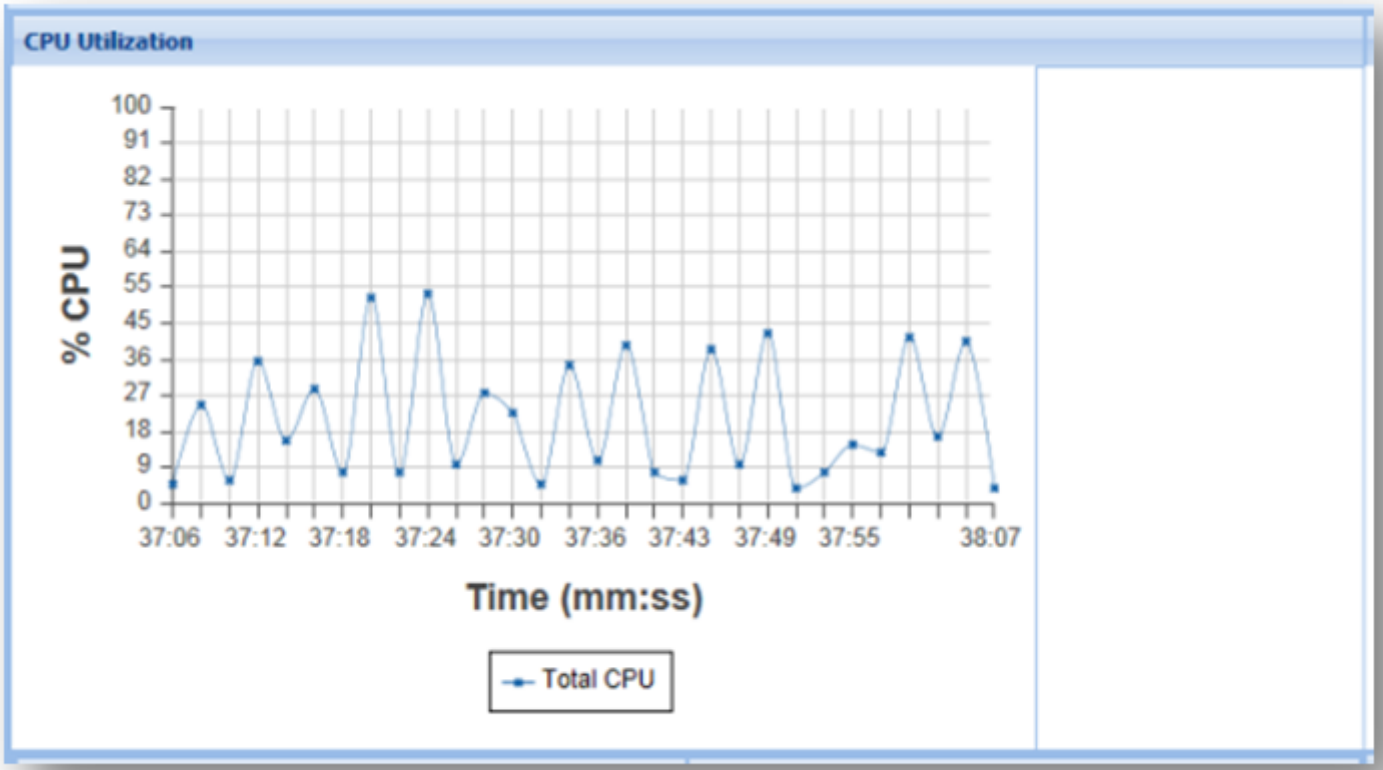


The **Panel Workspace** is the area in the panel where you perform several actions specific to the module. All the changes made to the module are displayed in this area.

Managing Dashboard

The **SoftNAS Dashboard** provides a quick summary of the key statistics and performance indicators.

1 CPU Utilization

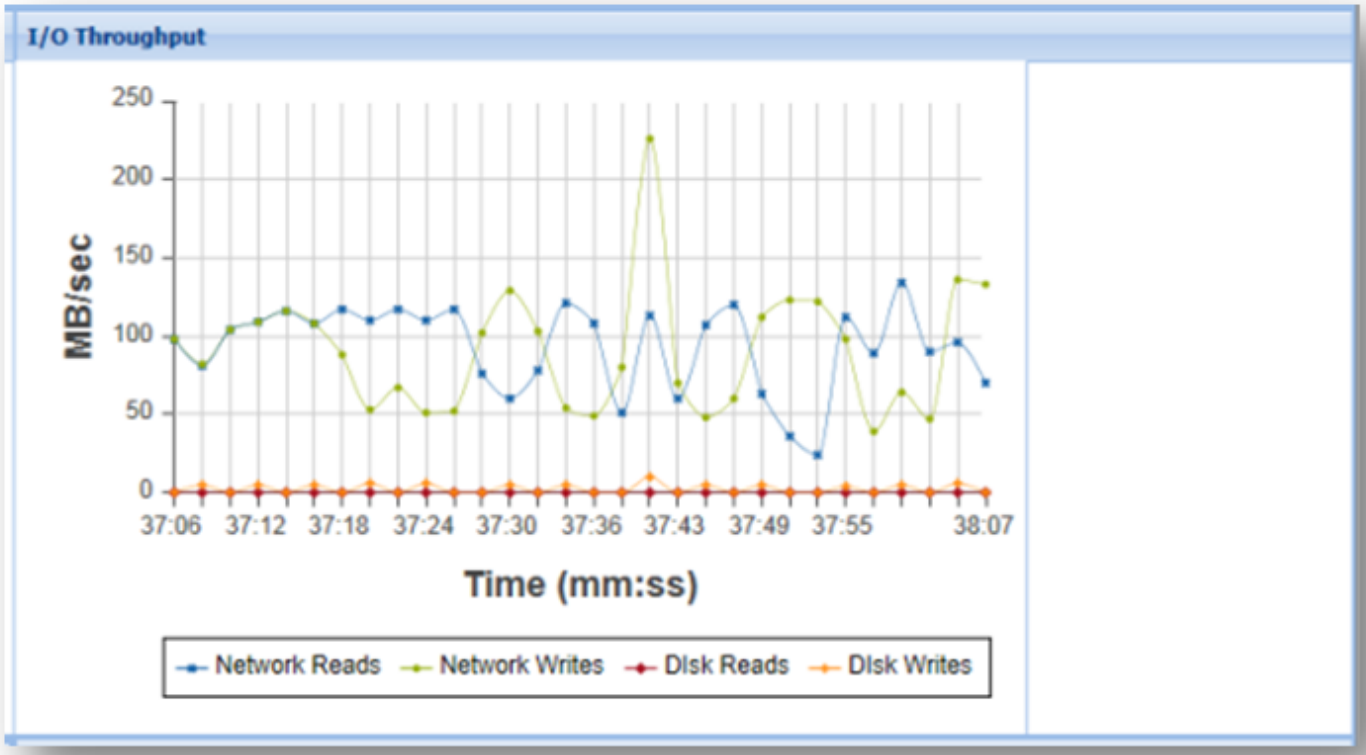


The **CPU Utilization** chart displays the real-time CPU usage information. You can use this chart to determine much the storage processing load is impacting CPU.

Note: If you see an average CPU utilization that is above 60%, consider adding more CPU capacity to improve the performance and response time. Also, if CPU load gets too high, then the **SoftNAS StorageCenter** respo times may become unacceptably slow.

High CPU utilization may be caused by specifying compression on volumes with high I/O workloads or other h I/O workloads. Increasing the number of vCPU (virtual CPU's) assigned to the **SoftNAS VM** usually resolves C workload issues.

2 I/O Throughput



The **I/O Throughput** chart displays the network and disk I/O throughput statistics in MB/sec over time.

You can use this chart to observe the system input/ouput levels and throughput of the network and disk subsys

1. To highlight a particular chart line (e.g., **Network Reads**), hover the mouse over the legend label text **Netw Reads.**

The selected chart line will be highlighted and you can easily view its trends.

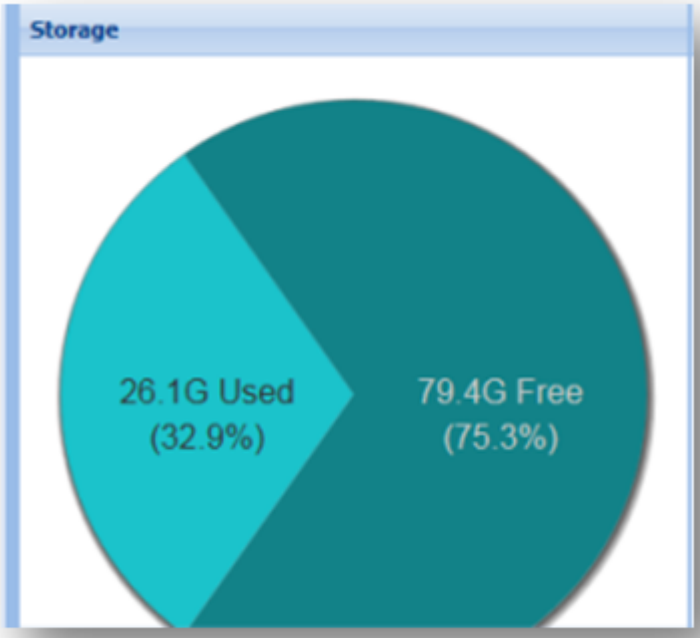
2. To disable a particular chart line, click on the legend label text.

The corresponding chart line will be disappeared.

3. To enable or restore it back, click on the legend label text again.

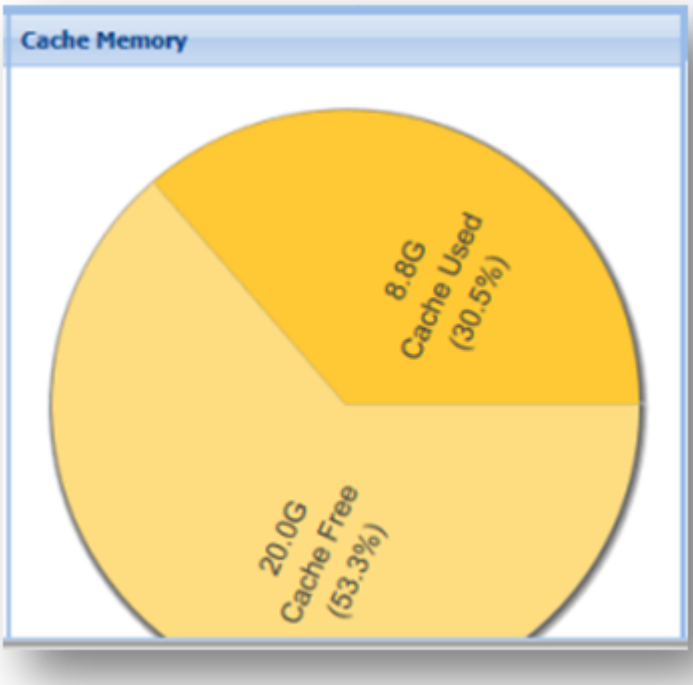
Note: If you observe a high amount of network I/O and a relatively low amount of disk I/O, that usually means the I/O workload is being cached in memory; i.e., the system's cache memory is working well, minimizing the a of disk I/O required for commonly accessed data.

3 Storage



The **Storage** pie chart shows the overall **Used** vs. **Free** space of all the **Storage Pools.**

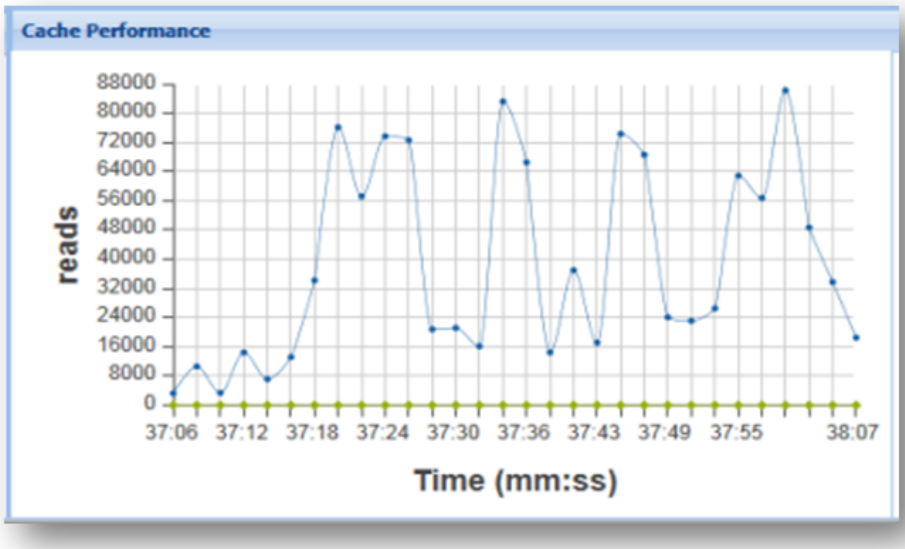
4 Cache Memory



The **Cache Memory** pie chart shows how much of main memory is allocated to cache, the amount of cache that's unused (free) and the amount that is used (contains active data available for fast read operations).

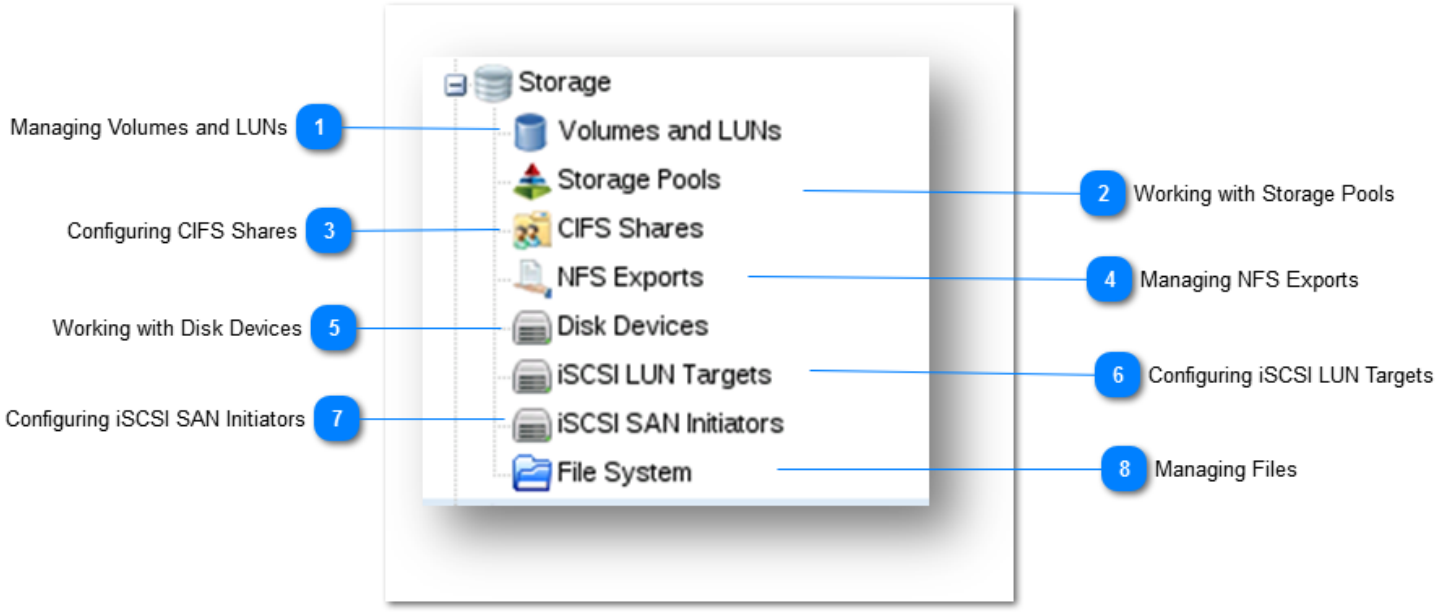
5 Cache Performance

The **Cache Performance** chart shows the number of read operations being serviced from cache memory (instead of being read from disk). In many applications, after applications have been running for a time, the majority of reads will be serviced from cache memory instead of requiring disk read operations.



Managing Storage

The Storage is one of the core sections of **SoftNAS StorageCenter.** It has the modules to configure **Volumes and LUNs, Storage Pools, CIFS Shares, NFS Exports, Disk Devices, ISCSI LUN Targets, ISCSI LUN Initiators** and **File System.**



1 Managing Volumes and LUNs

Volumes and LUNs

Volumes provide a way to allocate storage available in a storage pool and share it over the network. The **Volumes and LUNs** section of SoftNAS allows you to create, edit, remove and manage storage volumes and their snapshots.

For more information, refer to the following link.

Managing Volumes and LUNs

2 Working with Storage Pools

Storage Pools

The **storage pools** are used to aggregate disk storage into a large **pool** of storage that can be conveniently allocated and shared by **volumes.** The **Storage Pools** tab is where you view and manage all the storage pools.

For more information, refer to the following link.

Working with Storage Pools

3 Configuring CIFS Shares

The **Common Internet File System (CIFS)** is the standard way that computer users share files across corporate intranets and the Internet. It provides users with seamless file and print interoperability between VMs and Windows-based clients. **CIFS** allows multiple clients to access and update the same file while preventing conflicts by providing file sharing and file locking.

For more information, refer to the following link.

Configuring CIFS Shares

4 Managing NFS Exports

You can configure the volume for sharing as NFS Share so that storage is available for use by the applications, servers and clients on the network.

For more information, refer to the following link.

Managing NFS Exports

5 Working with Disk Devices

Disk Devices provide the underlying storage for **SoftNAS** and **Storage Pools.** Disk devices are attached to SoftNAS at the virtualization platform layer, often as virtual hard disks (e.g., VMDK in VMware, EBS volumes in EC2).

For more information, refer to the following link.

Working with Disk Devices

6 Configuring iSCSI LUN Targets

Sharing block devices via **iSCSI** is a common way to make network-attached storage available. An **iSCSI LUN** is a logical unit of storage. In **SoftNAS,** the basic storage **LUN** is a volume that is accessed as a **blockdevice.** The blockdevice volumes have a mount point in the **Linux /dev/zvol** filesystem because they are disk block devices.

For more information, refer to the following link.

Configuring iSCSI LUN Targets

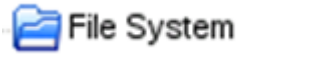
7 Configuring iSCSI SAN Initiators

The **iSCSI SAN Initiators** module helps to configure various initiator components such as **Authentication Options, iSCSI Timeouts, iSCSI Options, iSCSI Interfaces** and **iSCSI Connections.**

For more information, refer to the following link.

Configuring iSCSI SAN Initiators

8 Managing Files



The **File System** browser is a Java-based applet providing the ability to view and manage the filesystem.

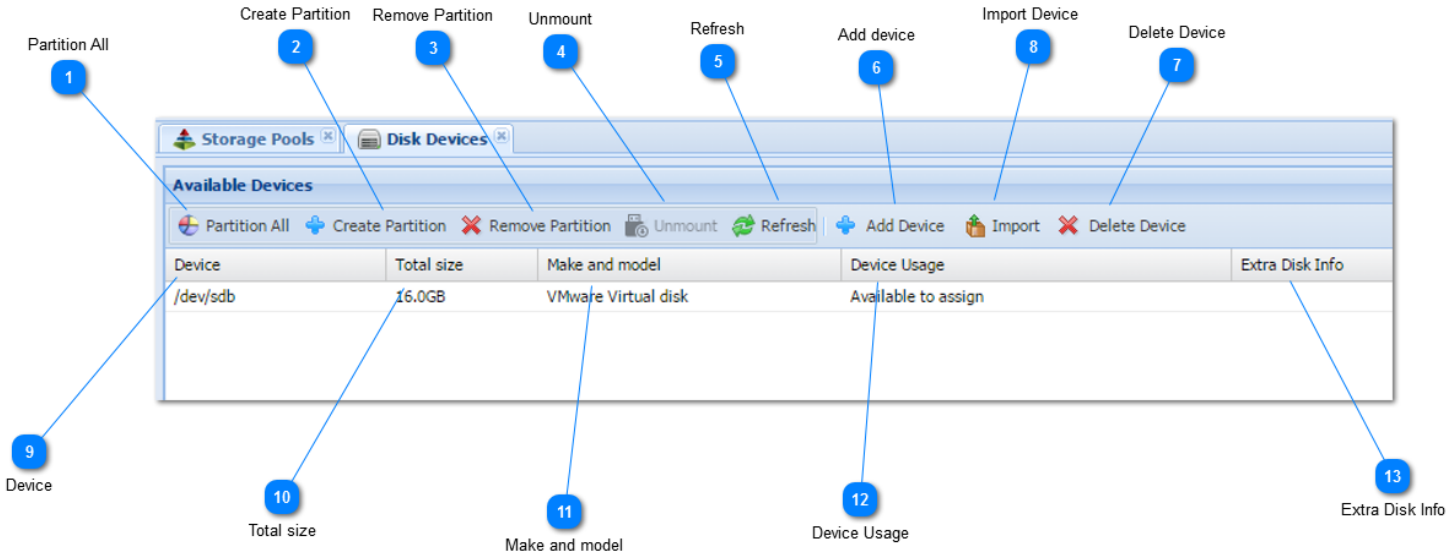
For more information, refer to the following link.

Managing Files

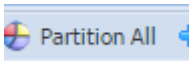
Working with Disk Devices

Disk Devices provide the underlying storage for **SoftNAS** and **Storage Pools.** Disk devices are attached to SoftNAS at the virtualization platform layer, often as virtual hard disks (e.g., VMDK in VMware, EBS volumes in EC2).

When a new disk device is attached, it usually starts out in a raw, unpartitioned state. Before it can be used, the disk device must be partitioned. The Disk Devices panel provides a list of disk devices, their status and the ability to manage the devices.

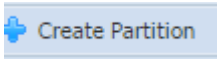


1 Partition All



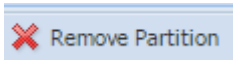
The **Partition All** button finds all devices without a partition and creates a partition on each device. Devices which are in use or already contain a partition are ignored.

2 Create Partition



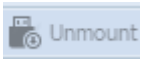
The **Create Partition** button adds a partition to a device that does not contain a partition. First, select a device in the device list grid by choosing a row, then press the Create Partition button.

3 Remove Partition



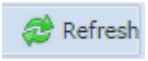
To remove a partition, select a device that is not in use and then press the **Remove Partition** button. Devices which are marked as "Used in pool" are not eligible for partition removal.

4 Unmount



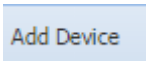
Unmount the disc device.

5 Refresh



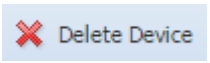
Press the Refresh button to rescan the available devices and display the currently available devices.

6 Add device



Certain types of devices can be added at run-time. Click **Add Device** and choose the type of device to add, then follow the on-screen instructions for adding the device.

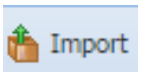
7 Delete Device



Certain types of dynamic devices can be removed at run-time. To delete a dynamic device that is no longer in use within a pool, select the device in the list to choose its grid row, then press the Delete Device button and confirm deletion of the device.

Note: Many devices, once deleted, may not be recoverable.

8 Import Device

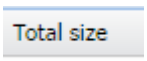


It is possible to import an existing disk. To import an existing disk, click **Import**, and follow the prompts.

9 Device

List of devices.

10 Total size



The total amount of data storage available on the raw device, before partitioning and addition to a storage pool.

11 Make and model

Make and model

The make (vendor) and model of the device, with the type of device shown in parenthesis.

12 Device Usage

Device Usage

How the device is currently used, or what it needs to become useful. The device can be in one of several states:

- Needs partitioning
- Available to assign to a storage pool
- Used in a pool, along with the name of the pool in which it is used

13 Extra Disk Info

Extra Disk Info

Some devices have additional information available. For example, S3 Cloud Disk devices are associated with an S3 bucket, which is displayed.

Add Disk Device

The **Add Device** wizard shown below is seen in AWS and VMware instances.

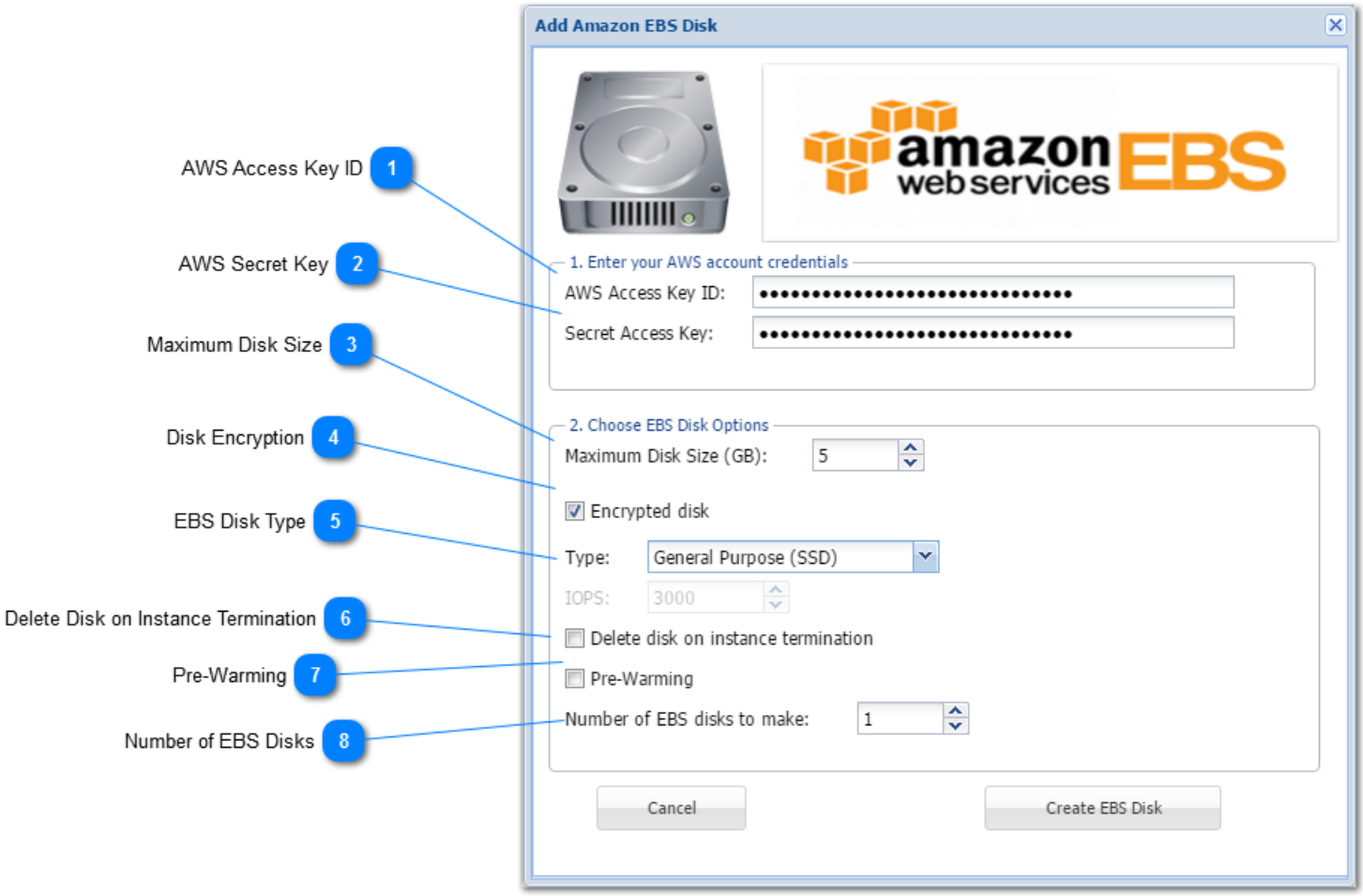
In Azure, the **Add Device** is very similar, but the disk options are different.

This dialog is used to choose the type of device to add dynamically at runtime. Choose a device type and click the Next button to continue.

Add EBS Disk

About EBS Disks

Amazon Elastic Block Store (Amazon EBS) provides persistent block level storage volumes for use with Amazon EC2 (and SoftNAS) instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes offer the consistent and low-latency performance needed to run your workloads.



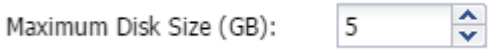
1 AWS Access Key ID

The AWS Access Key is an authentication identifier which uniquely identifies an AWS(Amazon Web Services) account.

2 AWS Secret Key

The AWS Secret Key is the secret password component used to authenticate the AWS Access Key and provide access to Amazon EBS storage.

3 Maximum Disk Size

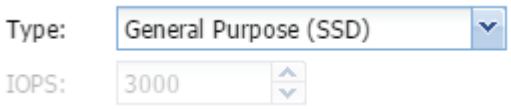


Enter a numeric value and choose the units (GB) representing the maximum size of the EBS disk. The EBS disk can provide up to 1024 GB of storage capacity.

4 Disk Encryption

EBS Disk contents can be encrypted and signed. When encryption is enabled, SHA1 HMAC authentication is also automatically enabled, and any blocks that are not properly encrypted and signed are rejected.

5 EBS Disk Type



Select the type of EBS Disk you would like to provision. Options include:
- General Purpose (SSD)
- Provisioned IOPS (SSD)
- Magnetic
- Throughput Optimized HDD
- Cold HDD

General Purpose:
General purpose SSD volume that balances price and performance for a wide variety of transactional workloads.

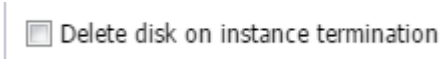
Provisioned IOPS:
Highest-performance SSD volume designed for mission-critical applications. Provisioned IOPS is configurable, allowing you to set an IOPS performance benchmark, allowing AWS to promise single-digit millisecond latencies and to deliver the provisioned performance 99.9% of the time. Configure the Provisioned IOPS threshold with the dropdown that appears below the option once selected.

Magnetic:
Low Cost HDD volume can be used for workloads with smaller datasets where data is accessed infrequently or when performance consistency isn't of primary importance.

Throughput Optimized HDD:
Low cost HDD volume designed for frequently accessed, throughput-intensive workloads.

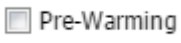
Cold HDD:
Lowest cost HDD volume designed for less frequently accessed workloads.

6 Delete Disk on Instance Termination



Determine whether the disk you are creating should be persistent, or whether it should be deleted upon termination of the host instance.

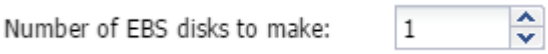
7 Pre-Warming



Enabling pre-warming avoids the initial performance penalty the first time each block is accessed.

However, the disk(s) will be inaccessible until the pre-warming is completed. This can take hours for large disks.

8 Number of EBS Disks



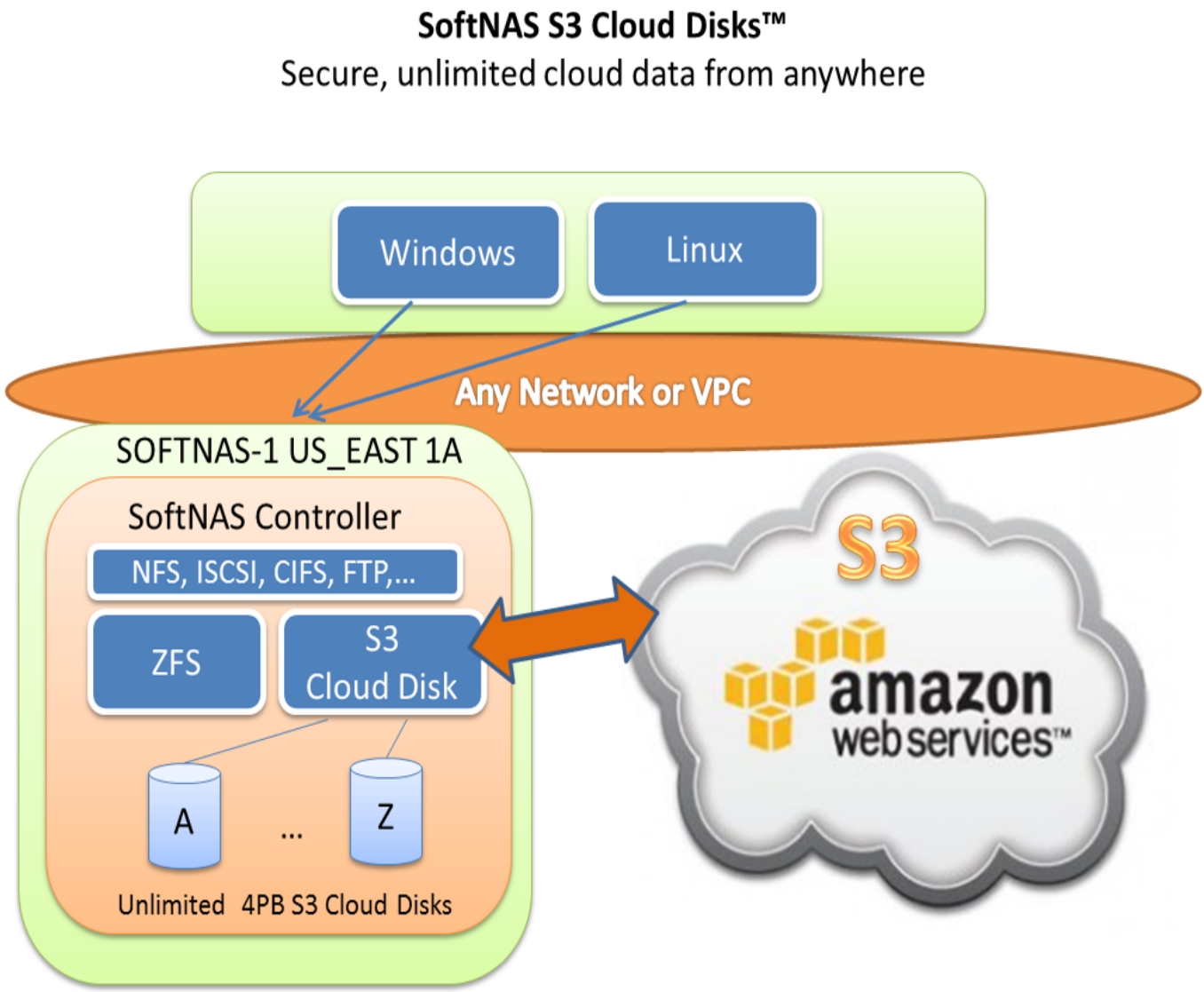
Select the number of EBS disks you wish to create with the defined settings.

Add S3 Cloud Disk

About SoftNAS S3 Cloud Disks

Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier. Amazon S3 and SoftNAS S3 Cloud Disks provides access to store and retrieve any amount of data, at any time, from anywhere on the web. It gives anyone access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits on to customers.

As shown below, SoftNAS S3 Cloud Disks are block devices created from Amazon S3 storage.



Each S3 Cloud Disk device can store up to 4 petabytes (PB) of data. An unlimited number of S3 Cloud Disks are supported. Each S3 Cloud Disk is thin-provisioned, so storage space is only consumed when data is actually written to the device and actually used.

S3 Cloud Disks are attached to SoftNAS Storage Pools and provide unlimited cloud storage. Each cloud disk is encrypted and authenticated to provide added security.

S3 Cloud Disks can be created and accessed on-premise from VMware ESXi, as well as within the Amazon EC2 cloud environment.

Cloud disks can also be combined in a RAID-1 mirror configuration with local disks (VMware) or EBS disks (AWS), so you get the best of both worlds: I/O performance plus highly-redundant cloud storage in real-time.

Cloud disks benefit from other SoftNAS features, including RAM caching, SSD caching, compression, deduplication, scheduled snapshots and read/write clones. This means you get the best balance of performance and NAS features combined with the off-site data storage redundancy of S3.

Amazon S3 storage costs start at just $10 per TB per month in lower terabyte quantities and are available as low as $5 per TB per month in higher quantities. Consult Amazon S3 product information pricing for latest details and pricing.

S3 Cloud Disks can also be copied for long-term archive storage into AWS Glacier (functionality that is built into the AWS console).

Amazon S3 Cloud Disk Configuration

The S3 Cloud Disk Extender provides the addition of block devices that can be added to SoftNAS at any time. Each S3 Cloud Disk block device includes a pseudo-device designation of /dev/s3-NNN, where NNN is a sequential device number starting from zero.

Use the S3 Cloud Disk Extender configuration dialog shown below to configure and add S3 Cloud Disk devices to SoftNAS.

Amazon Web Services Gov Cloud

1 AWS Access Key

AWS Access Key ID:

The AWS Access Key is an authentication identifier which uniquely identifies an AWS (Amazon Web Services) account.

2 AWS Secret Key

Secret Access Key:

The AWS Secret Key is the secret password component used to authenticate the AWS Access Key and provide access to Amazon S3.

3 Region

Region:

S3 Cloud Disks can be created in any of the worldwide AWS regional data centers. By specifying a specific region for S3 Cloud Disks, the data can be maintained within only that specific data center. Benefits of regional S3 Cloud Disks include:

a) the data remains within the country where the regional data center is located, to meet certain regulatory compliance requirements, and
b) S3 Cloud Disks are located nearby the SoftNAS EC2 instance, reducing latency and improving throughput and performance.

By default, S3 Cloud Disks and their associated S3 buckets are created in the "U.S. Standard" region (US East, Virginia) and replicated to other U.S. regions in Oregon and N. California, and provide eventual consistency for all requests. This region automatically routes requests to facilities in Northern Virginia or the Pacific Northwest using network maps.

4 Bucket Basename

Bucket Basename:

The Bucket Basename is used for automatically generating unique bucket names. The bucket base name is used as a prefix for an automatically generated bucket name for the S3 Cloud Disk. This base name makes it quick and easy to generate any number of S3 Cloud Disks, each with a common base name. Choose a base name that's meaningful for your application, company or use of S3 Cloud Disks. Valid bucket base names are comprised of lower-case characters only.

5 S3 Bucket

S3 Bucket:

This is the S3 Bucket name that will be associated with the S3 Cloud Disk. All bucket names within S3 must be unique. S3 bucket names can be any lower-case alpha and/or numeric text characters, plus embedded dashes and periods within the bucket name string.

By default, a unique bucket name is automatically generated for your convenience, using the Bucket Basename as a prefix, plus a random number and suffix of "s3disk" followed by the S3 Cloud Disk device number.

You can type your own bucket name into the S3 Bucket field using lower-case alpha and/or numeric characters, plus embedded dashes and periods within the bucket name string.

To select an existing bucket, click on the drop down menu and choose from the available S3 buckets shown.

6 Maximum Disk Size

Maximum Disk Size:

Enter a numeric value and choose the units (GB or TB) representing the maximum size of the S3 Cloud Disk. Since S3 Cloud Disks are thin-provisioned, this value is the maximum disk size this S3 Cloud Disk can grow to over time as data is added to the device.

Please note that while a very large S3 Cloud Disk can be created, the usable storage must fit within the licensed SoftNAS storage maximum size available.

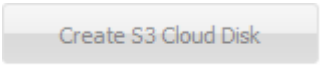
7 Encrypted disk

S3 Cloud Disk contents can be encrypted and signed. When encryption is enabled, SHA1 HMAC authentication is also automatically enabled, and any blocks that are not properly encrypted and signed are rejected. When encryption is enabled, data compression is also automatically enabled.

AES-256 CBC encryption is used to provide a balance of performance and security strength.

The encryption key is determined based upon the Disk Password provided.

8 Create S3 Cloud Disk



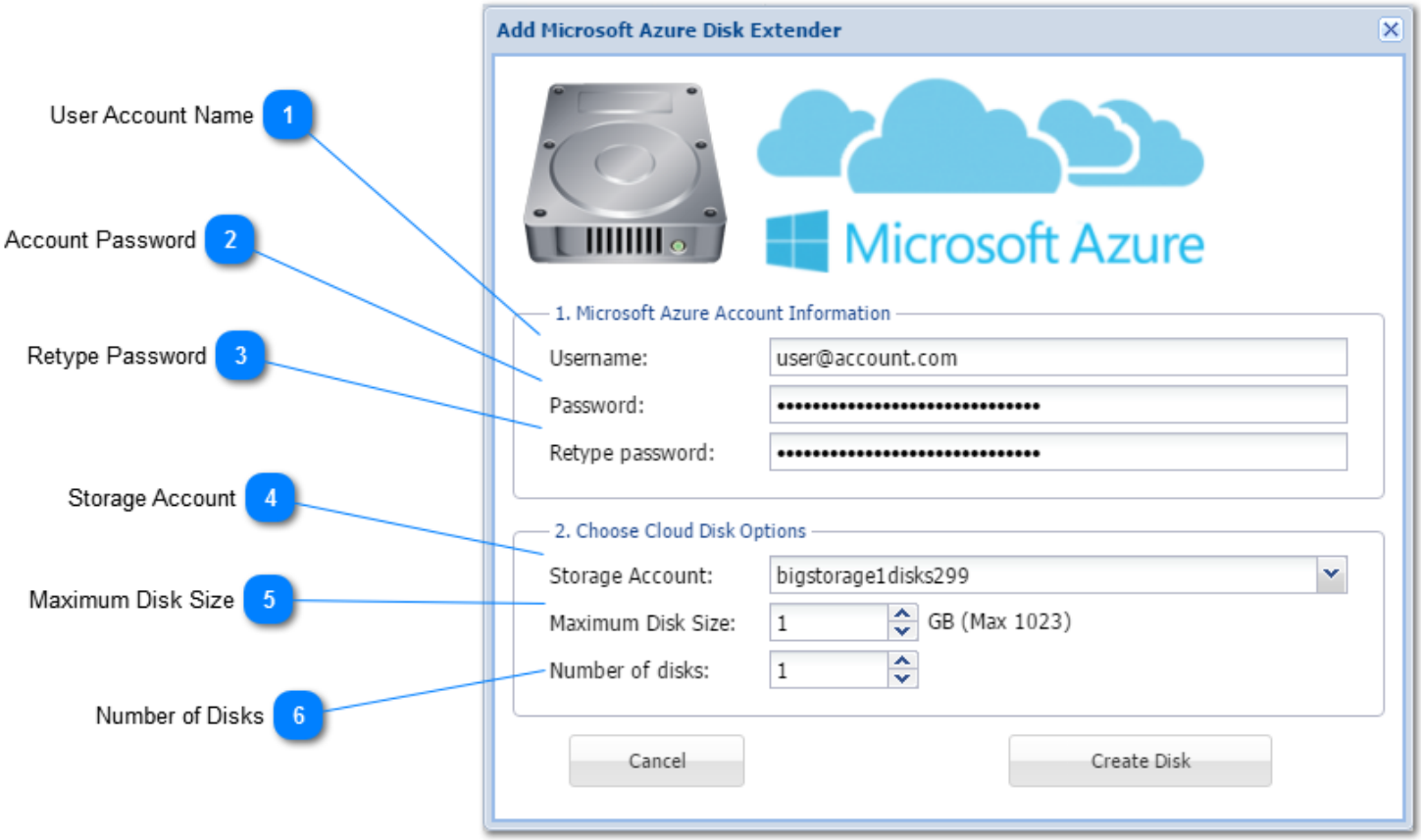
After filling out the form with the desired values, press the Create S3 Cloud Disk button to create the S3 Cloud Disk device.

Add Azure Block Disk

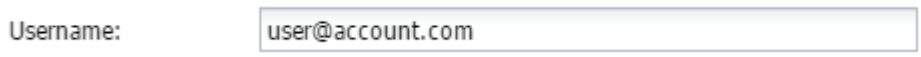
About Azure Block Storage

Block Storage provides fixed size raw storage capacity where each storage volume can be treated as an independent disk. Block Storage is only accessible from an OS, such as SoftNAS' linux -based application. It is typically formatted with FAT_{32}, NTFS, EXT_3, and EXT_4. It is the most common storage type used with databases that require high performance and low-latency, and for mission-critical applications.

Azure offers various VM sizes, with pricing based on the amount of block storage disks it makes available. When adding block storage through the SoftNAS UI, your instance will be subject to the limits of your selected instance Size.



1 User Account Name



Provide the Administrative or Service Admin Azure account used to create your instance or storage accounts in the portal.

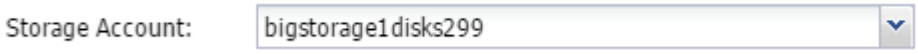
2 Account Password

Provide the password for your Azure Admin or Service Admin Account.

3 Retype Password

Retype the Azure Admin or Service Admin account password to confirm.

4 Storage Account



Available storage accounts will populate once the Admin or Service Admin Account Username and Password are provided. Select the appropriate account from the listed options.

5 Maximum Disk Size

Select the size of the disk you wish to create, up to the maximum.

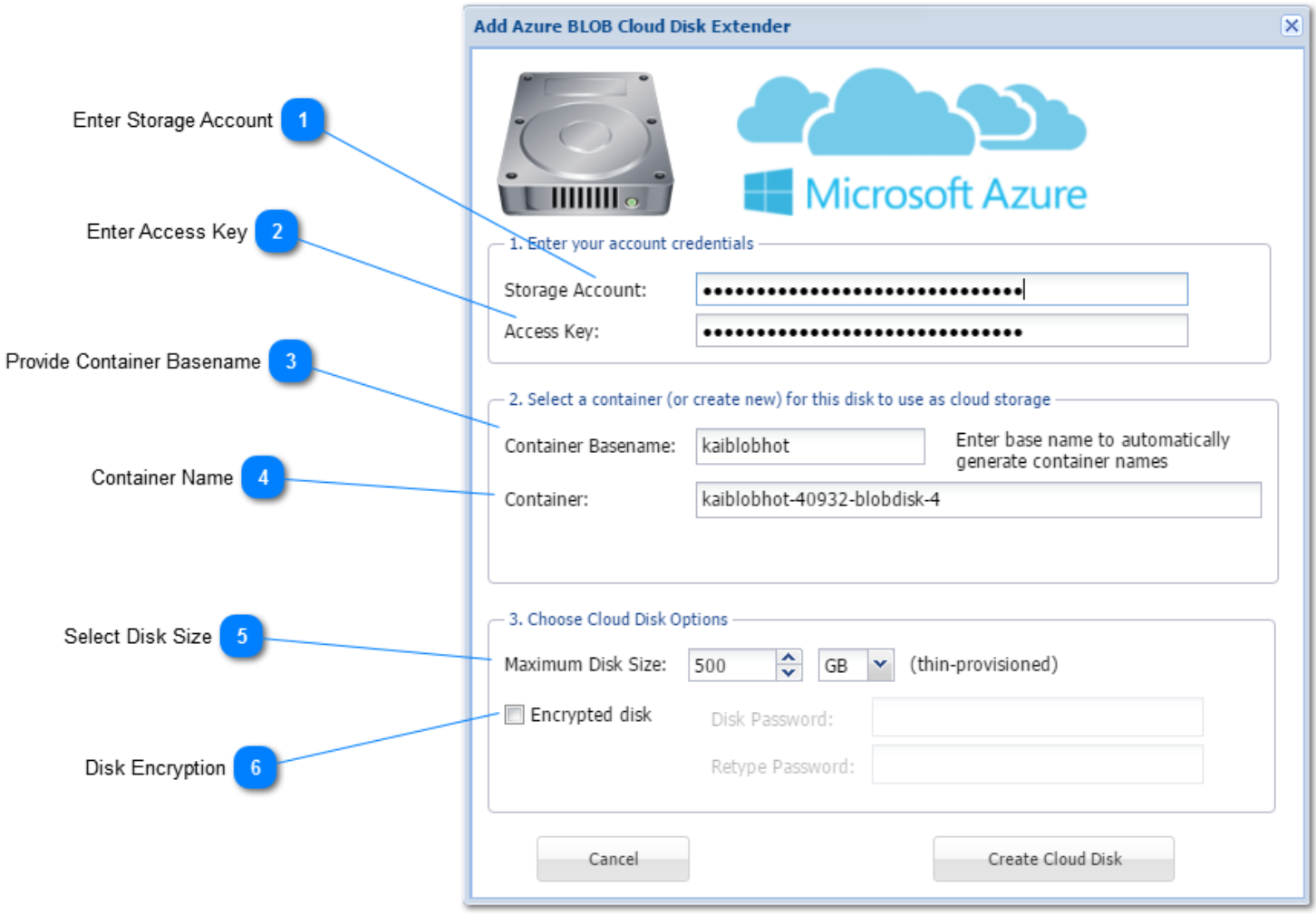
6 Number of Disks

Provide the number of disks you wish to provide, subject to the limits imposed by the Azure VM size selected.

Add Azure Blob Disk

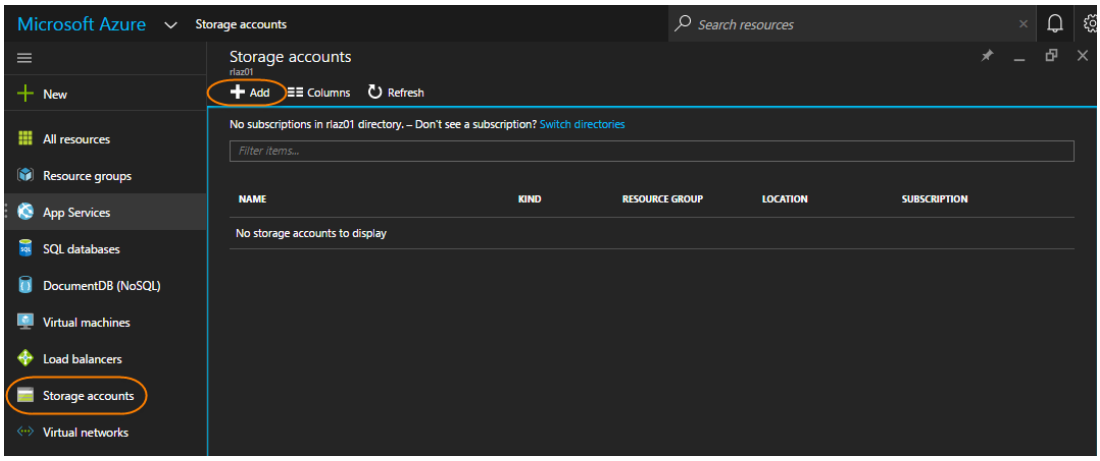
SoftNAS Cloud® leverages object-based scalable Azure blob object storage to present NFS, CIFS/SMB, iSCSI or AFP file sharing protocols for enterprise workloads. SoftNAS Cloud allows easy workload migrations to the Azure cloud without changing existing application data structures or workflows. Offering support for both Hot and Cool Azure blob storage accounts ensures that whether you are looking for inexpensive, low performance, large scale storage for infrequently accessed archive files, or performance-optimized application ready storage, SoftNAS has you covered.

Azure supports up to 500 Terabytes of storage per Azure Blob Storage Account. Extend your capacity up to 16 petabytes by leveraging multiple storage accounts. The following menu is available if you select Azure Blob from **Add Device**.



1 Enter Storage Account

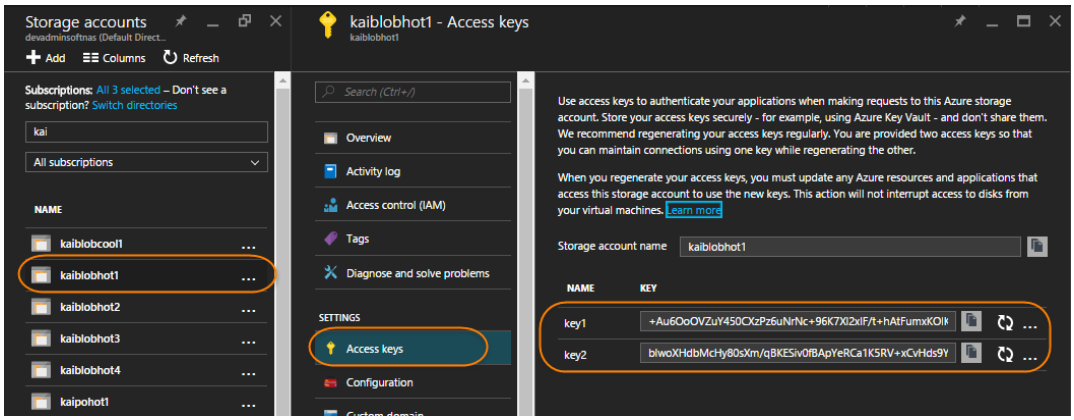
Enter the name of your Azure Blob Storage Account. If you have not yet created one, your blob storage account can be created in Storage Accounts in the Azure Portal.



2 Enter Access Key

Access Key: ••••••••••••••••••••••••••••••••

Enter the Access Key for your blob storage account. Your Access Key can be found in the Azure Portal by opening the desired storage account, and selecting Access Keys.



3 Provide Container Basename

Container Basename: kaiblobhot

Enter a basename for the blob storage container. This basename will be used to auto-generate the name of the container which is created when adding blob storage.

4 Container Name

Container: kaiblobhot-40932-blobdisk-4

This displays the automatically generated container name derived from the container basename. This name is editable, but you must ensure that any name created is unique.

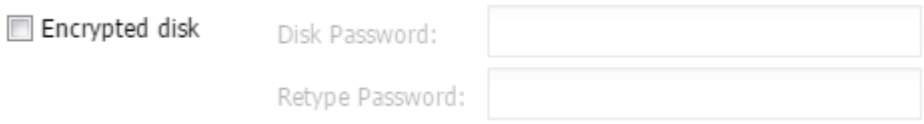
5 Select Disk Size

Maximum Disk Size: 500 GB (thin-provisioned)

Select the size of the disk you wish to create, up to 500 Terabytes (TB). You can create several disks from the same storage account, provided you do not exceed the storage account limit (though only one at a time). You can also leverage the entire storage account by creating a disk of 500 TB.

It is possible to leverage several storage accounts to stretch the storage capacity within the same SoftNAS instance to create a large pool or volume of up to 16 petabytes.

6 Disk Encryption

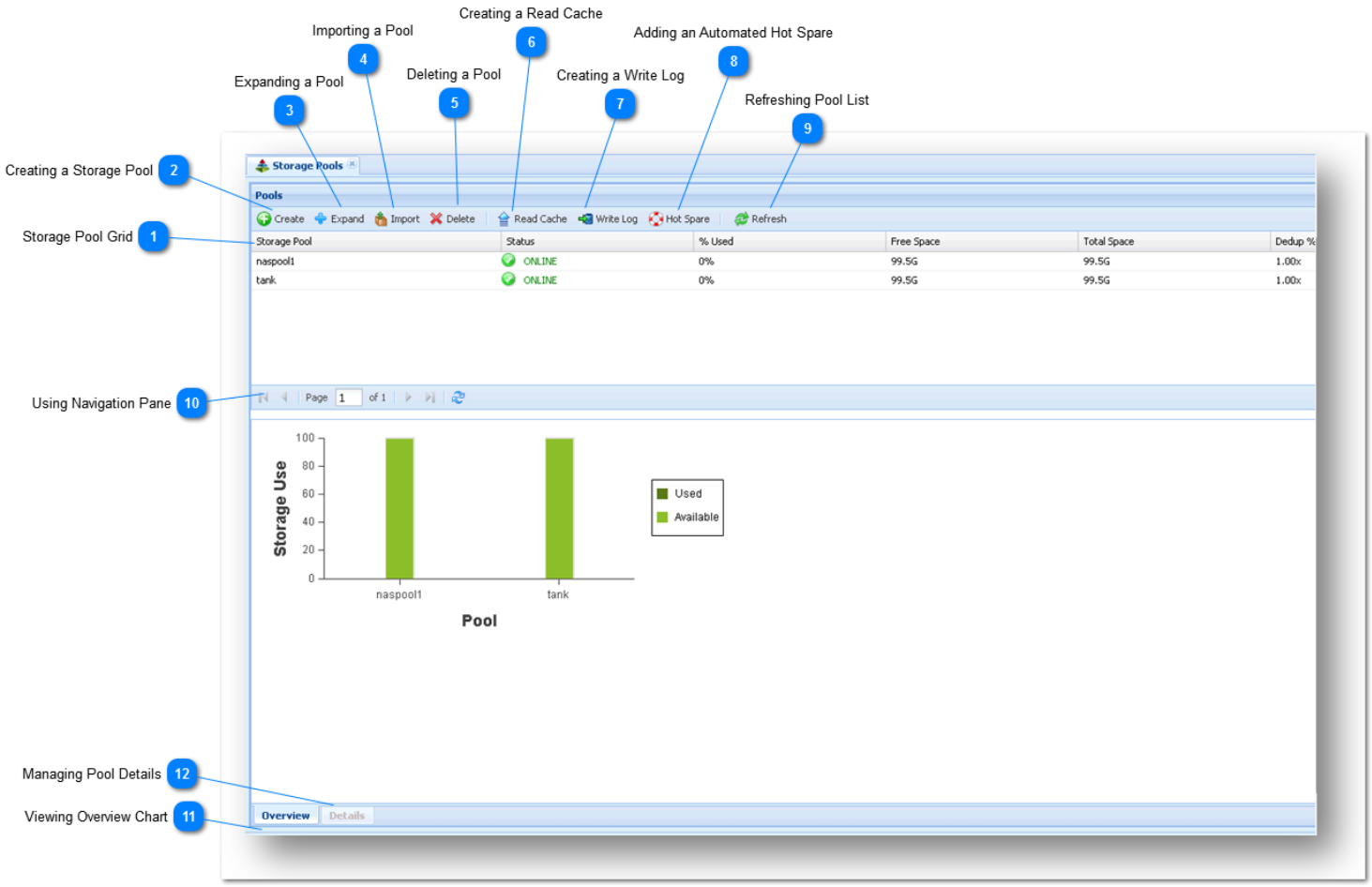


Your SoftNAS instance makes it possible to leverage disk encryption. Provide a password, and confirm your selection. This will encrypt the data on your disk, but will allow you access via the password provided.

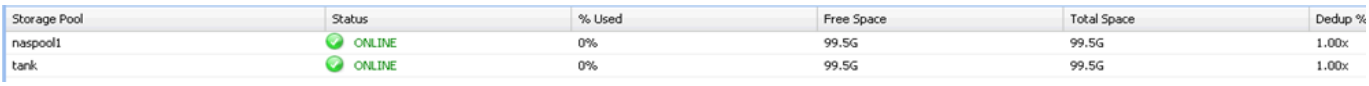
Working with Storage Pools

The **storage pools** are used to aggregate disk storage into a large **pool** of storage that can be conveniently allocated and shared by **volumes**. The **Storage Pools** tab is where you view and manage all the storage pools.

A storage pool is an aggregated set of storage comprised of one or more underlying storage devices. It is comprised of devices (object and block storage, or VMDKs) created during the **Add Disk Device** process, or imported. The storage on these devices is **aggregated** into a unified pool of storage that can be managed and deployed as a single **pool.** Each pool provides storage which is then allocated for use into **volumes.**



1 Storage Pool Grid



Storage Pool	Status	% Used	Free Space	Total Space	Dedup %
naspool1	ONLINE	0%	99.5G	99.5G	1.00x
tank	ONLINE	0%	99.5G	99.5G	1.00x

The **Storage Pool Grid** displays the list of storage pools in a tabular grid format. The volume table has the following fields.

Field	Description
Storage Pool	It shows the name of the storage pool.
Status	It shows the current status of the pool. Based on the status, it shows the following types of indicators: • ONLINE icon- indicates the pool is online, healthy and operating normally. • DEGRADED icon -indicates the pool is in a degraded state, continues to process data normally, but is at increased risk and requires attention; e.g., replace a failed disk in a RAID array. • UNAVAIL or FAILED icon indicates the pool is in a failed state and is not currently processing storage requests. This usually means there are disk failures exceeding RAID protection.
% Used	It shows the percentage of available storage used.
Free Space	It shows the amount of free space available for use in gigabytes.
Total Space	It shows the total amount of space in the pool, in gigabytes.
Dedup %	It shows the percentage of Dedup

2 Creating a Storage Pool

Before creating the **Storage Pool,** you will need to have created several EBS volumes for **Amazon EC2 based SoftNAS** instance and several VHDs for **VMware** based **SoftNAS VM.** These EBS volumes or VHDs provide the underlying storage for **SoftNAS** storage pools. Whenever a volume or VHD is added, it begins as a **raw disk** which means that the disk has no partitions.

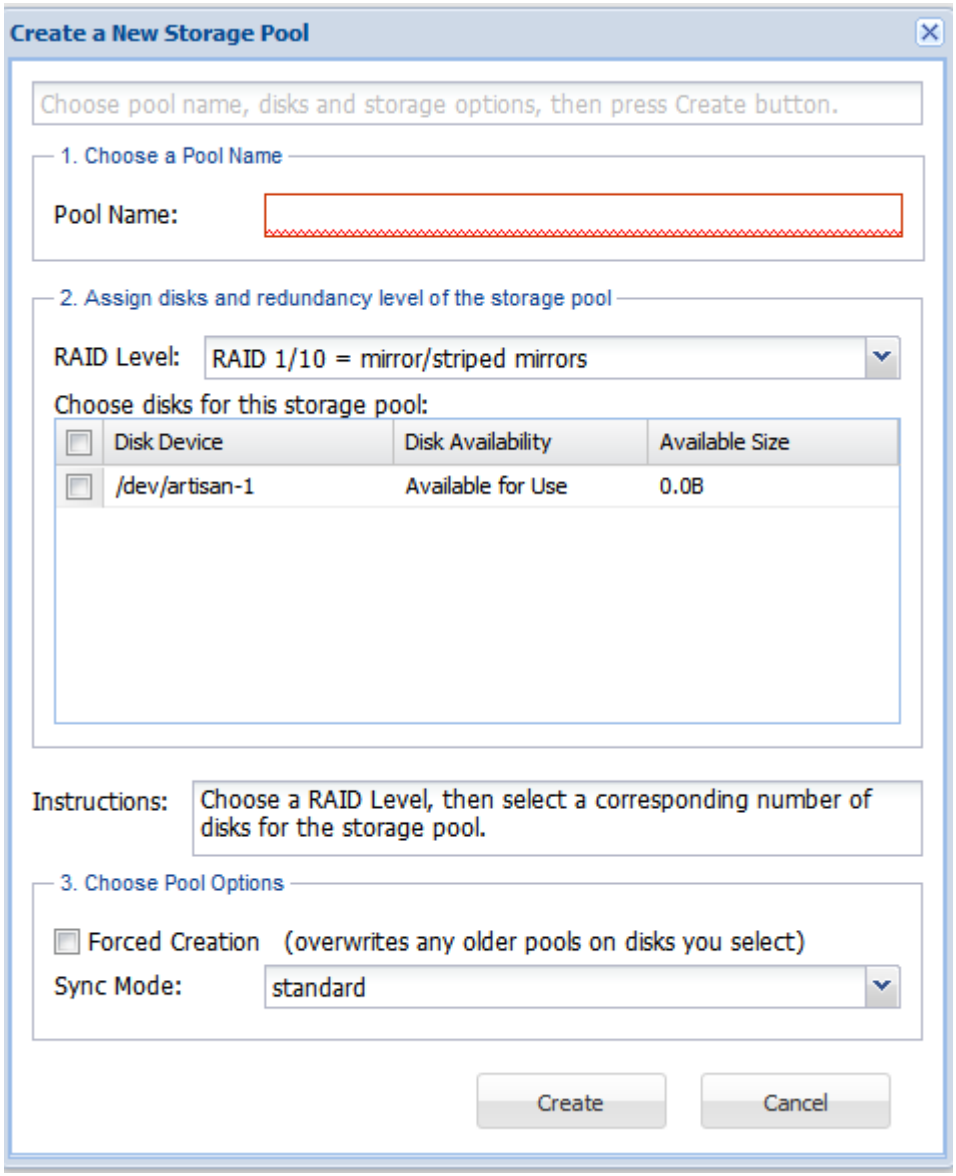
Note: Before you assign disk devices to a **storage pool,** you must partition the disks.

1. Click the **Storage Pools** option under the **Storage** section in the **Left Navigation Pane.**

The **Storage Pools** panel will be displayed with the list of all the existing storage pools that are already allocated.

2. To create a new storage pool, click the **Create** button.

The **Create New Storage Pool** dialog will be displayed.



3. Enter the name for the storage pool that you wish to create in the Pool Name text entry box.

Some example storage pool naming schemes might include:

- **Generic naming:** naspool1, naspool2, ...
- **Disk-type naming:** SAS1, SAS2, SATA1, SATA2
- **Use-case naming:** OS1, OS2, Exchange1, SQLData1, UserData1, Geology, Accounting, IT, R&D, QA, Corp01, etc.

4. Select the redundancy level from the **RAID Level** drop down list.

Note: If you are using hardware RAID at the disk controller level and have a single data disk presented to **SoftNAS** for your storage pool, then you may not need software RAID - in sucg case, select No RAID/ JBOD, as the RAID is implemented at a lower level and have no need for software RAID.

5. Select the disks for which you wish to allocate to this storage pool.

Note: Each of the devices show the **Disk Availability** status as **Available for Use.** This implies that these disks are already partitioned. New disk devices must be partitioned before use.

6. In the **Choose Pool Options** step, check the box in the **Forced Creation** field if you wish to overwrite any older pools on the disks that you have selected.

Note: If any of the disk devices you choose have been used as a part of another storage pool in the past (e.g., one that was deleted), you must use the **Forced Creation** option to overwrite the previous data in order to use the disk in a different pool (a precaution to prevent accidental data loss).

7. Choose the required Sync Mode:

• **standard:**

This is the default option. Synchronous file system transactions (fsync, O_DSYNC, O_SYNC, etc) are written out (to the intent log) and then secondly all devices written are flushed to ensure the data is stable (not cached by device controllers).

• **always:**

For the ultra-cautious, every file system transaction is written and flushed to stable storage by a system call return. This obviously has a big performance penalty.

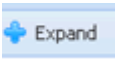
• **disabled:**

Synchronous requests are disabled. File system transactions only commit to stable storage on the next DMU transaction group commit which can be many seconds. This option gives the highest performance. However, it is very dangerous as ZFS is ignoring the synchronous transaction demands of applications such as databases or NFS. Setting sync=disabled on the currently active root or /var file system may result in out-of-spec behavior, application data loss and increased vulnerability to replay attacks. This option does *NOT* affect ZFS on-disk consistency. Administrators should only use this when these risks are understood.

8. Click the **Create** button at the end.

The new storage pool is created and is ready for use.

3 Expanding a Pool



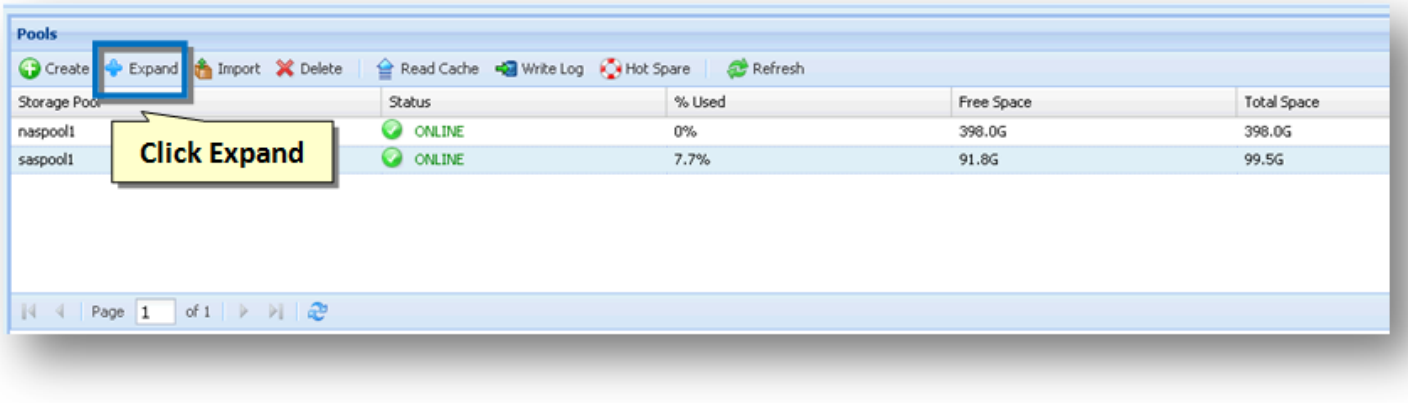
You can expand an existing storage pool by adding additional RAID arrays to the pool.

Note: You cannot add devices to an existing RAID array - you must add a new array to create a larger storage

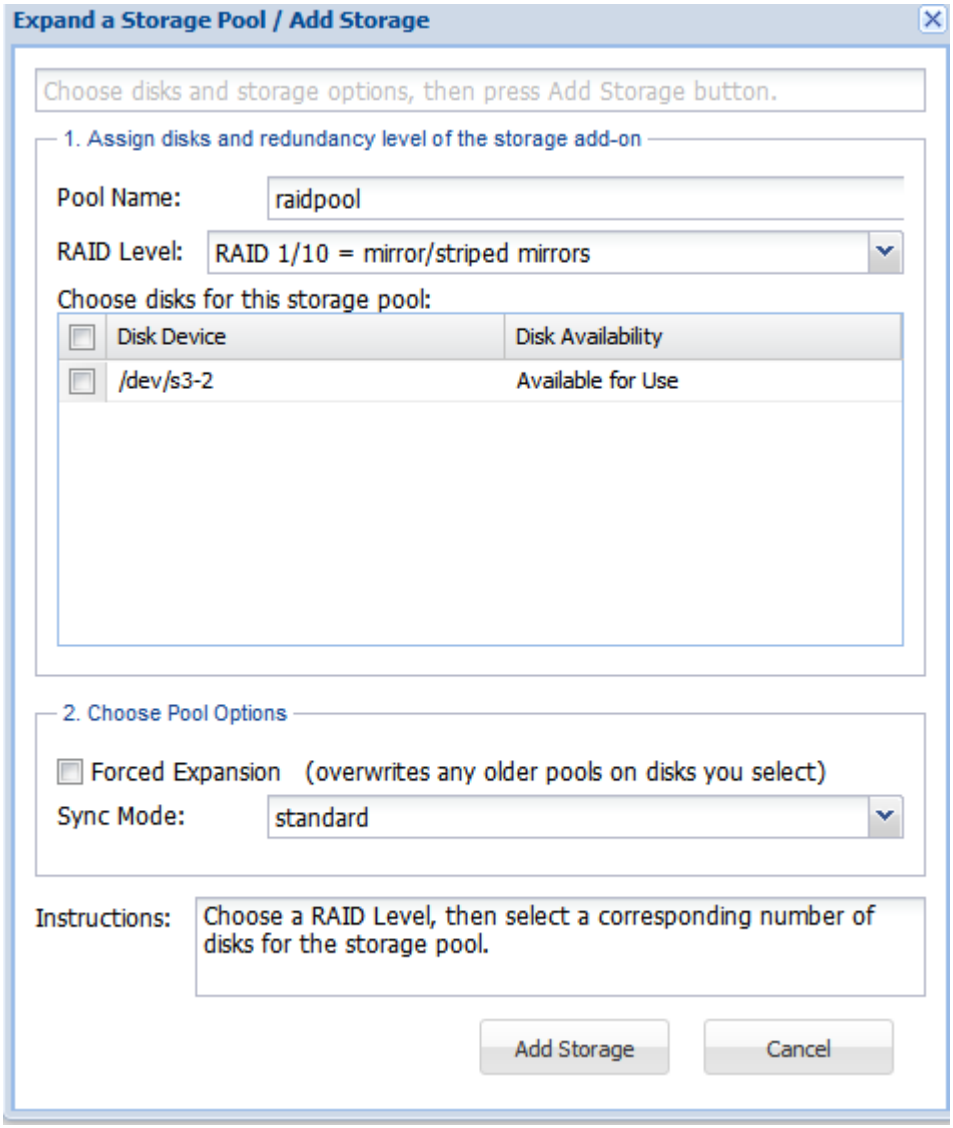
To do so, simply follow the steps given below.

1. Select the pool that you wish to expand in the **Pools** list.

2. Click the **Expand** button in the toolbar.



The **Expand a Storage Pool/Add Storage** dialog will be displayed.



3. Choose the disk for the storage pool.
4. In the **Choose Pool Options** section, check the box for **Forced Expansion** in order to overwrite any older
5. Select the Sync Mode: standard, always, disabled.
6. Click the **Add Storage** button.

The additional storage will be added to the selected pool.

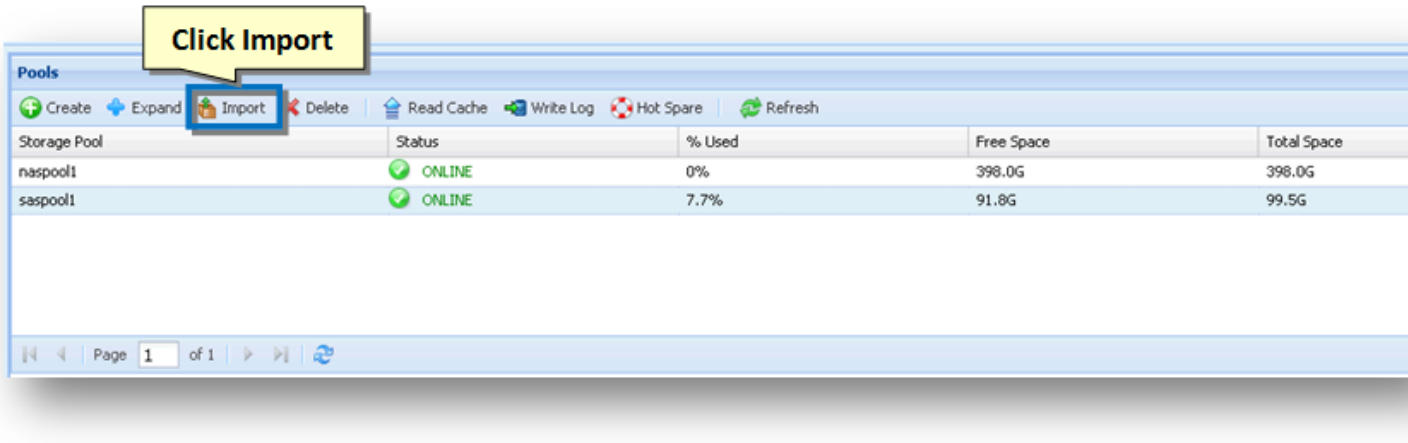
4 Importing a Pool

Import

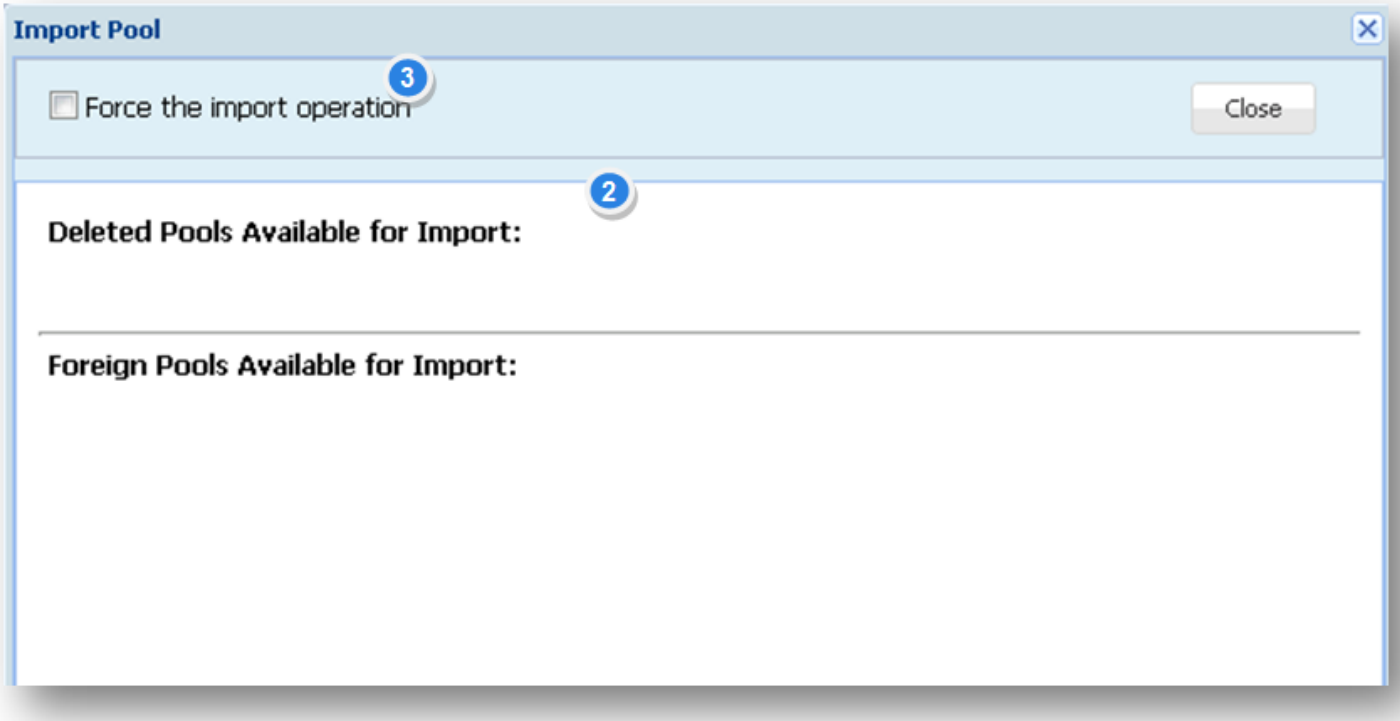
Import pools that were previously deleted or created on a different system. For example, a foreign pool create system can be imported into SoftNAS and used.

Note: All disk devices used in the pool must be available and unmodified for imported pools to be valid.

1. Click the **Import** option in the toolbar.



The **Import Pools** dialog will be displayed.



It has two sections such as **Deleted Pools Available for Import** and **Foreign Pools Available for Import.**

The **Foreign Pools** are the storage pools created on a different **SoftNAS** system.

2. If the pools are ready to import, there will be a button labeled **Import <poolname>,** where poolname will be import. Click that button.

3. You will need to select the **Force Import** checkbox, to force the system to import foreign pools from anothe

4. For each volume, configure the volume's **Snapshots** to use the desired schedule.

Note: They are not imported automatically, but can be manually copied from the old system by copying the sna files in the **/var/www/softnas/snserver** folder.

5. For each NFS and CIFS share you want, create the appropriate NFS exports and CIFS shares (they are not

6. For each iSCSI target (if any), define the appropriate iSCSI devices and targets.

Note: They are not imported automatically, but can be manually copied from the old system by copying the file new system, then restart the iSCSI Server.

The data disks will now be ready for use.

7. Click the **Refresh** button on the **Storage Pools** panel.

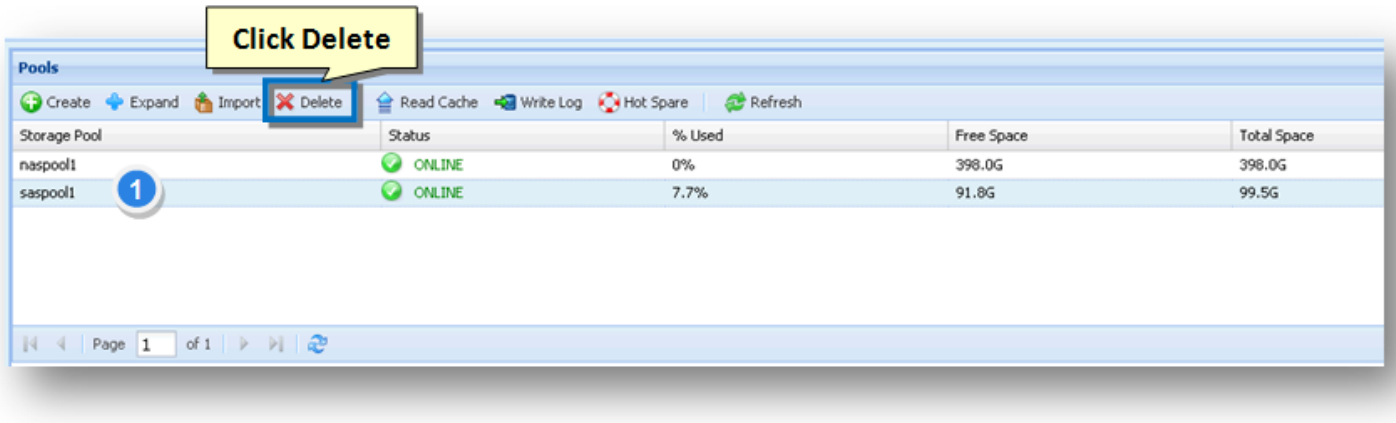
5 Deleting a Pool

Delete

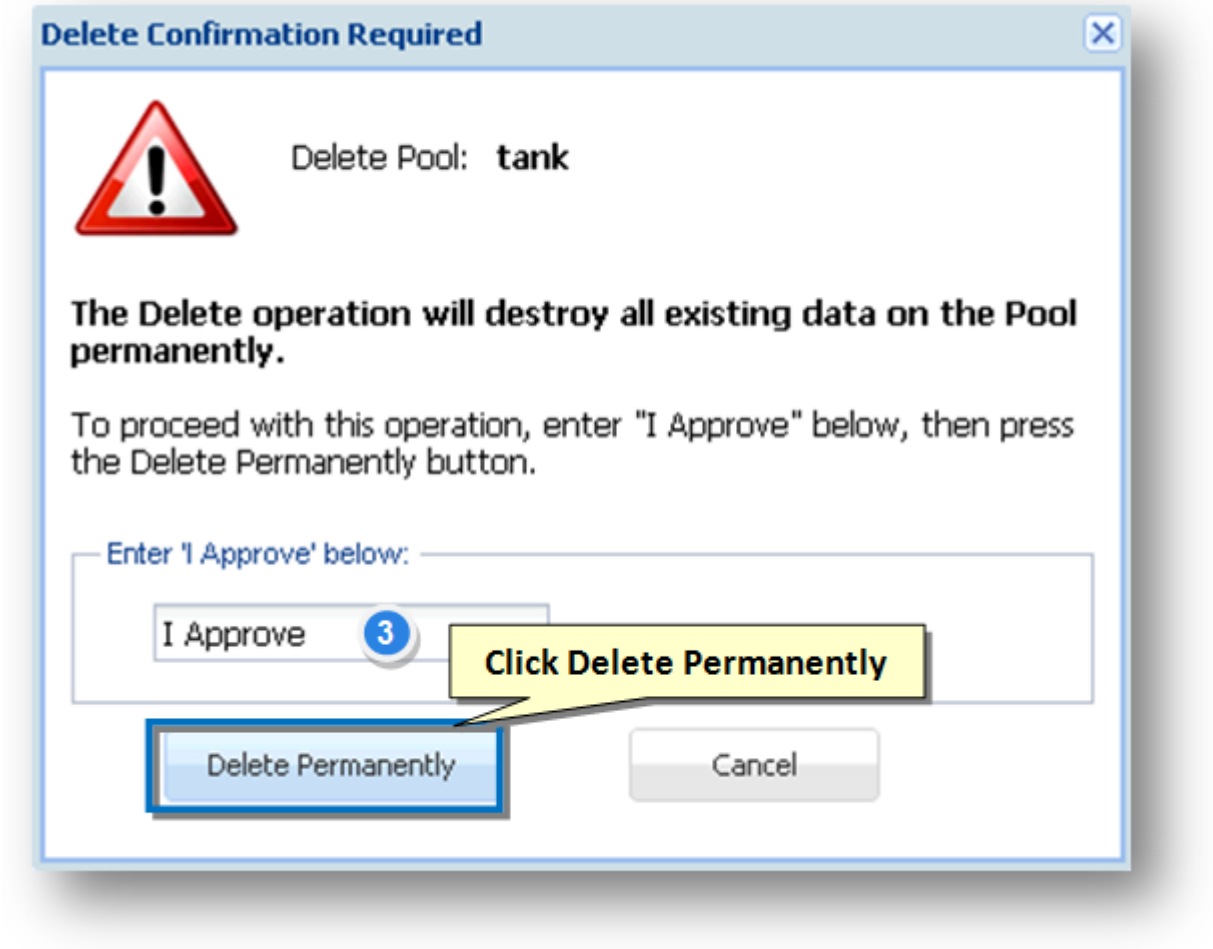
You can delete any selected pool. To do so, simply follow the steps given below.

1. Select the pool that you wish to delete from the **Pools** list.

2. Click the **Delete** button in the toolbar.



The **Delete Confirmation Required** dialog will be displayed.



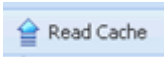
3. Enter the text **I Approve** in the text entry box.

4. Click the **Delete Permanently** button.

The selected pool will be removed.

Note: In the unlikely event you want to recover a deleted pool (immediately after deletion, use the **Import** butt
deleted pool. When importing a deleted pool, you will have to select the "**Force the Import Operation**" checkb

6 Creating a Read Cache



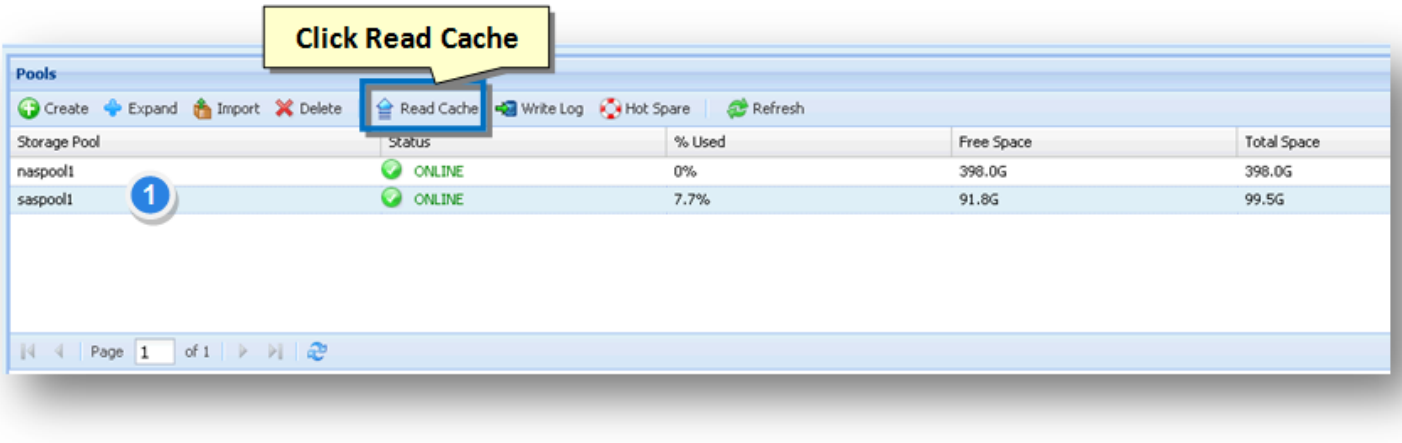
The **Read Cache** provides an additional layer of cache, in addition to RAM memory cache. SSD is recommen
provides a large, fast read cache that is much larger than available cache memory.

Before you create a read cache, you need to verify that disk drives are available that have not been assigned t

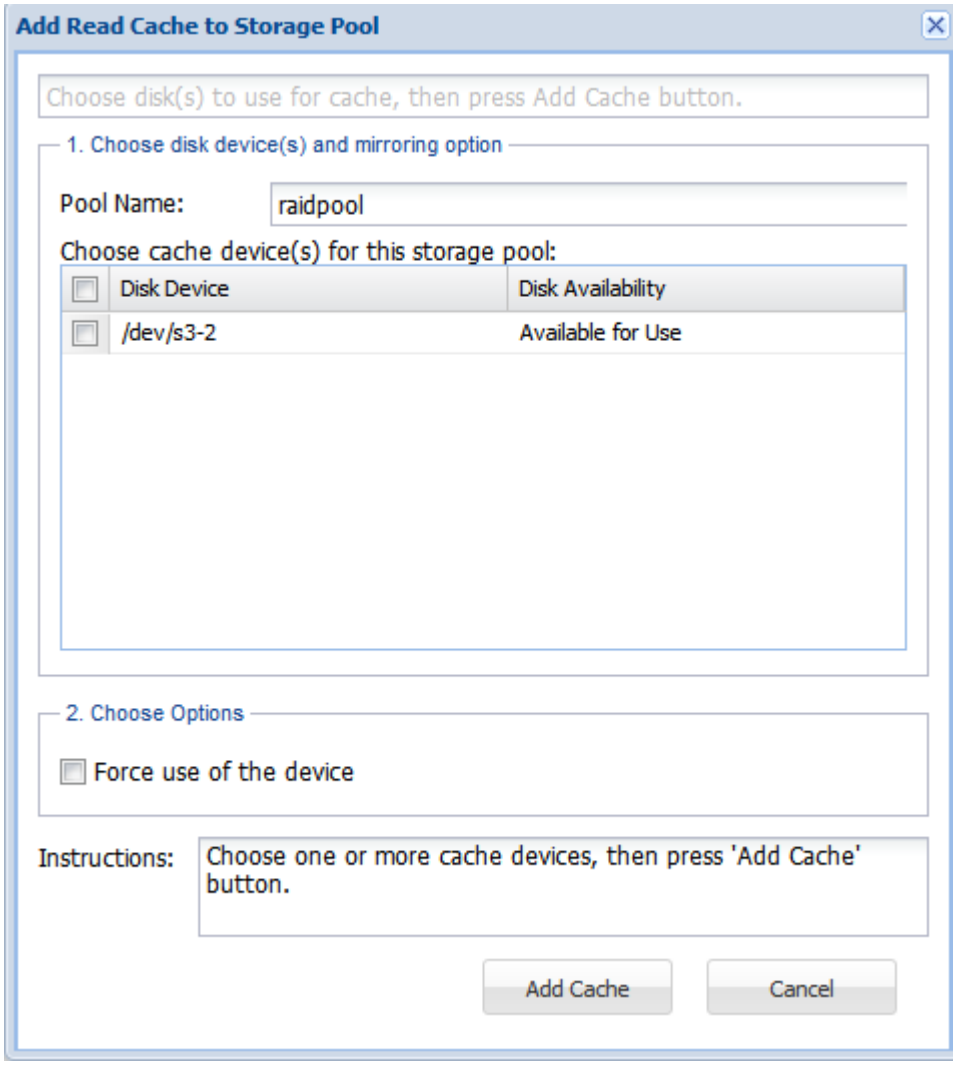
Note: These should be high speed drives: SAS or SSD.

1. Select the **Storage Pool** to which you wish to add **Read Cache / Write Log.**

2. Click the **Read Cache** option in the toolbar.



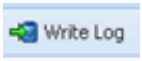
The **Add Read Cache to Storage Pool** dialog will be displayed.



3. Choose the disk for the storage pool.
4. In the **Choose Options** section, check the box for **Force use of the device** to overwrite any older pools or
5. Click the **Add Cache** button.

The read cache will be added to the selected pool.

7 Creating a Write Log



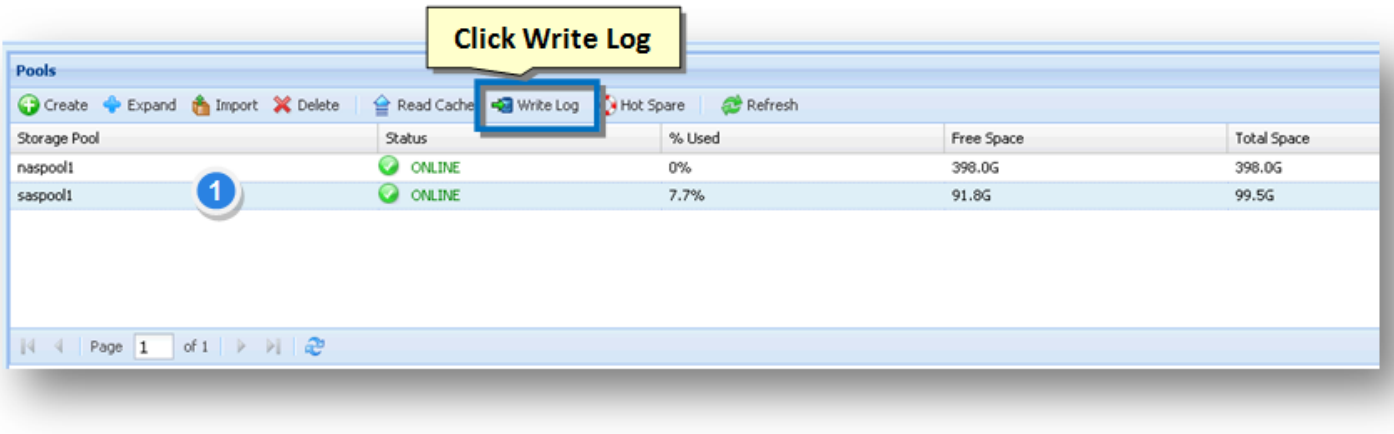
The **Write Log** provides a cache for incoming writes to be written temporarily to high-speed storage, then later spindle-based storage. SSD is recommended for **Write Log.**

Important: The **Write Log** becomes a critical element of your storage pool, so it is highly-recommended to al **Write Log** (that way, if a write log device fails, you won't risk invalidating your storage pool, as the write log in

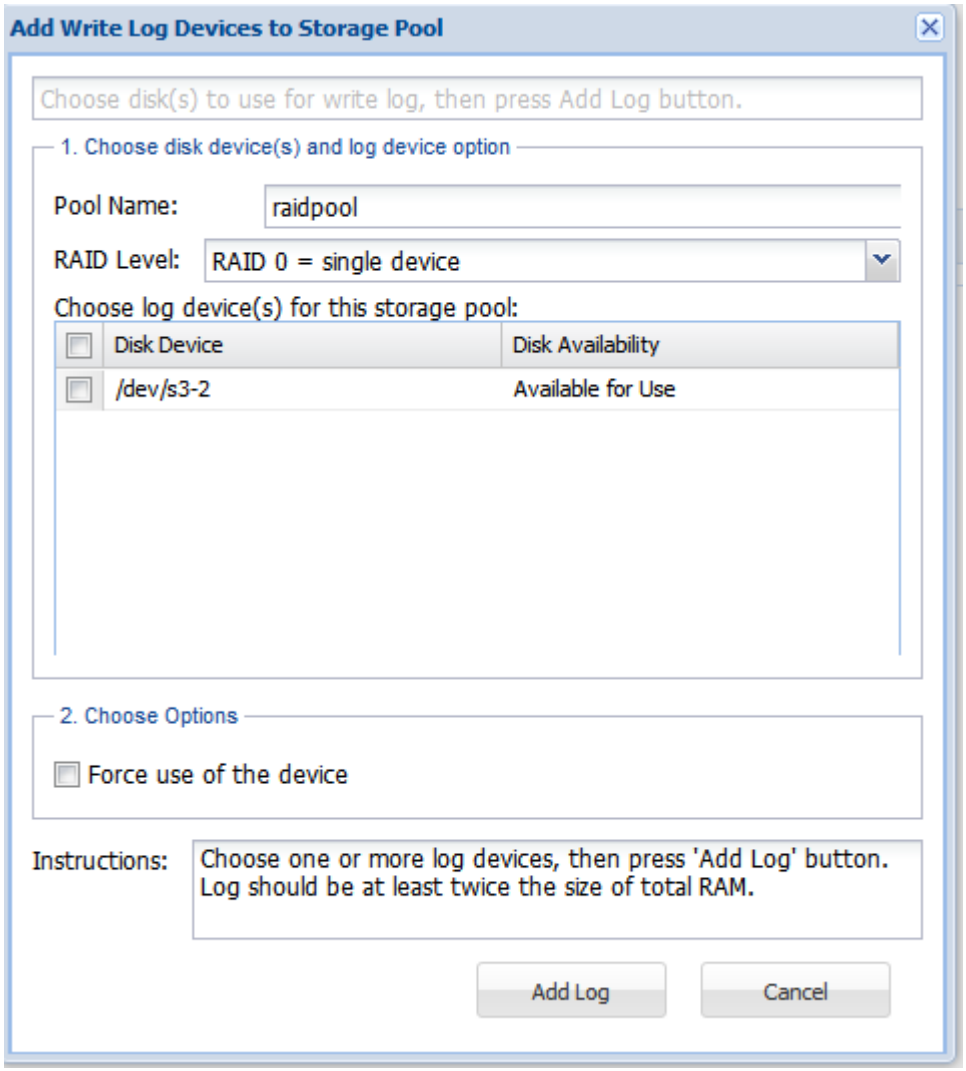
You can add a write log to any selected pool. To do so, simply follow the steps given below.

1. Select the pool to which you wish to add write log in the **Pools** list.

2. Click the **Write Log** button in the toolbar.



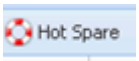
The **Add Write Log Devices to Storage Pool** dialog will be displayed.



3. Choose the disk for the storage pool.
4. In the **Choose Options** section, check the box for **Force use of the device** to overwrite any older pools or
5. Click the **Add Log** button.

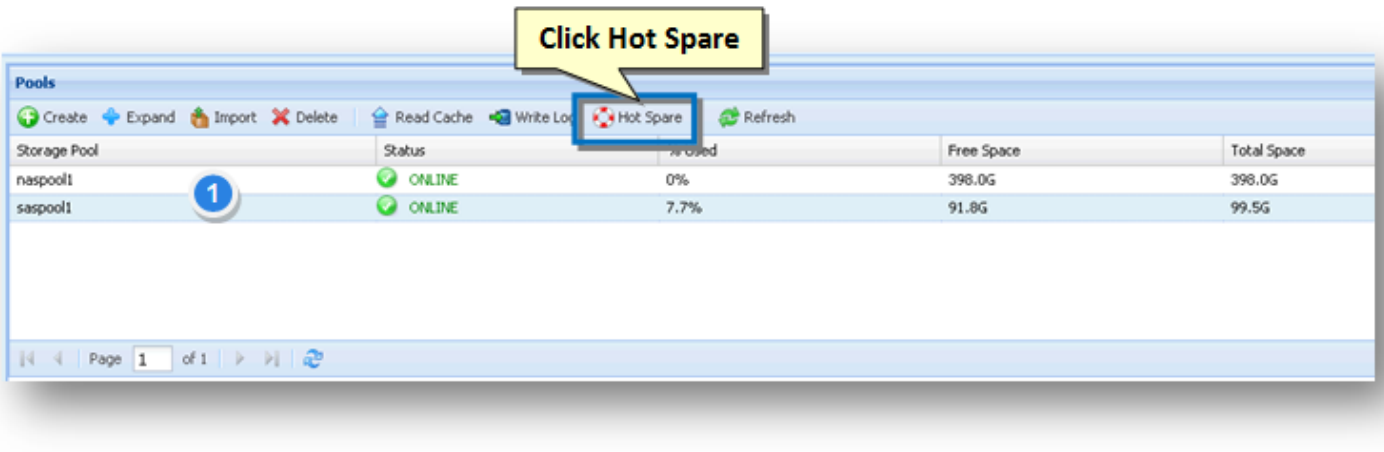
A write log will be added to the selected pool.

8 Adding an Automated Hot Spare

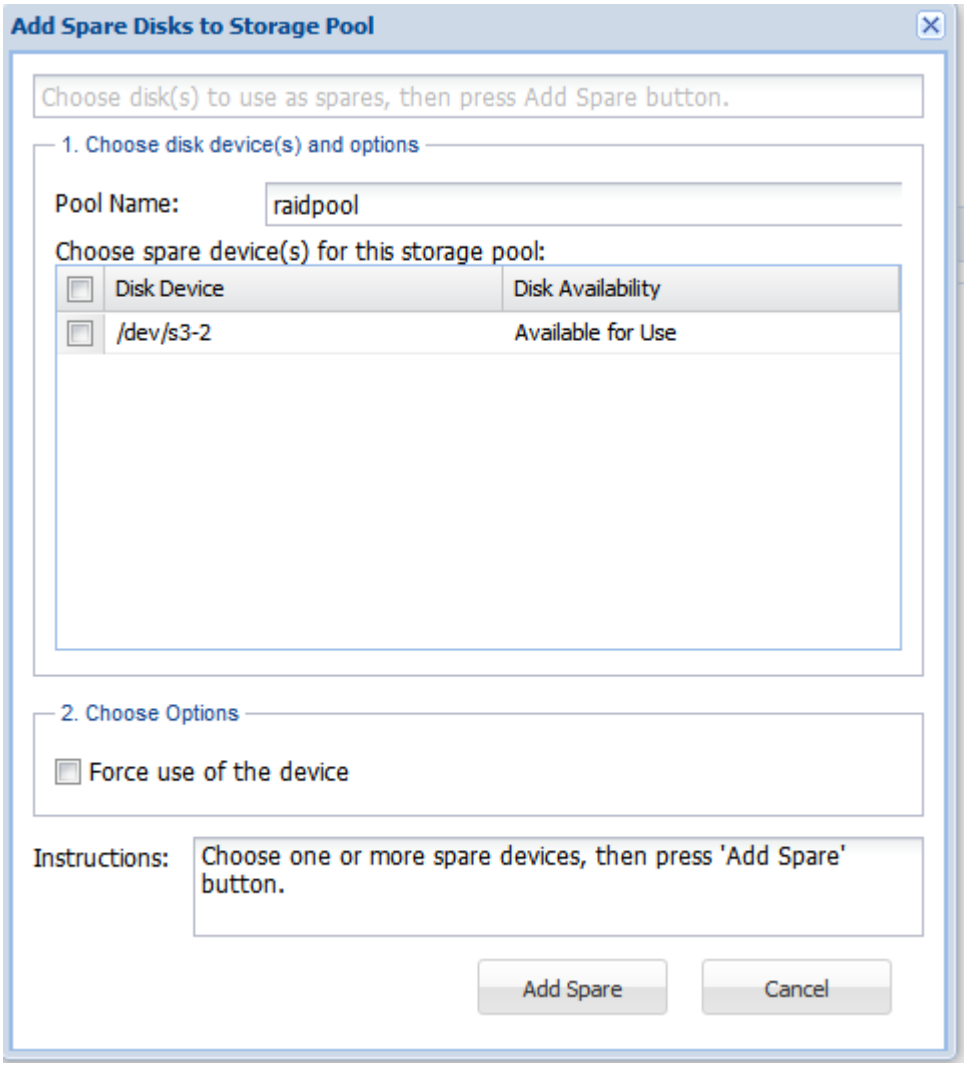


You can add a hot spare for any selected pool. In addition, sparing is automated, with failover to the spare occ
without the need for administrator intervention. To setup automated sparing, simply follow the steps given belo

1. Select the pool to which you wish to add hot spare in the **Pools** list.
2. Click the **Hot Spare** button in the toolbar.



The **Add Spare Disks to Storage Pool** dialog will be displayed.



3. Choose the disk for the storage pool.

4. In the **Choose Options** section, check the box for **Force use of the device** to overwrite any older pools or you select.

5. Click the **Add Spare** button.

The selected spare device will be added to the pool. Sparing is automated, meaning that upon creation of the according to the above instructions, your data will fail over to the hot spare automatically, without requiring adm approval. This feature does not require any additional configuration.

9 Refreshing Pool List

You can refresh the **Pools** list and update it with the latest information. To do so, simply click the **Refresh** button in the toolbar.

The **Storage Pools** list will be reloaded with the most current values.

10 Using Navigation Pane

You can use the **Navigation Pane** to navigate between storage pool records. It has the following set of buttons.

 **First Page** - Press to navigate to the First page of pools (when the number of pools exceeds the number that can be displayed on a single page).

 **Previous Page** - Press to navigate to the Previous page of pools (when the number of pools exceeds the number that can be displayed on a single page).

Page Number - Displays the current page of pools (when the number of pools exceeds the number that can be displayed on a single page). You can also enter the page number in the box to navigate to that page.

 **Next Page** - Press to navigate to the Next page of pools (when the number of pools exceeds the number that can be displayed on a single page).

 **Last Page** - Press to navigate to the Last page of pools (when the number of pools exceeds the number that can be displayed on a single page).

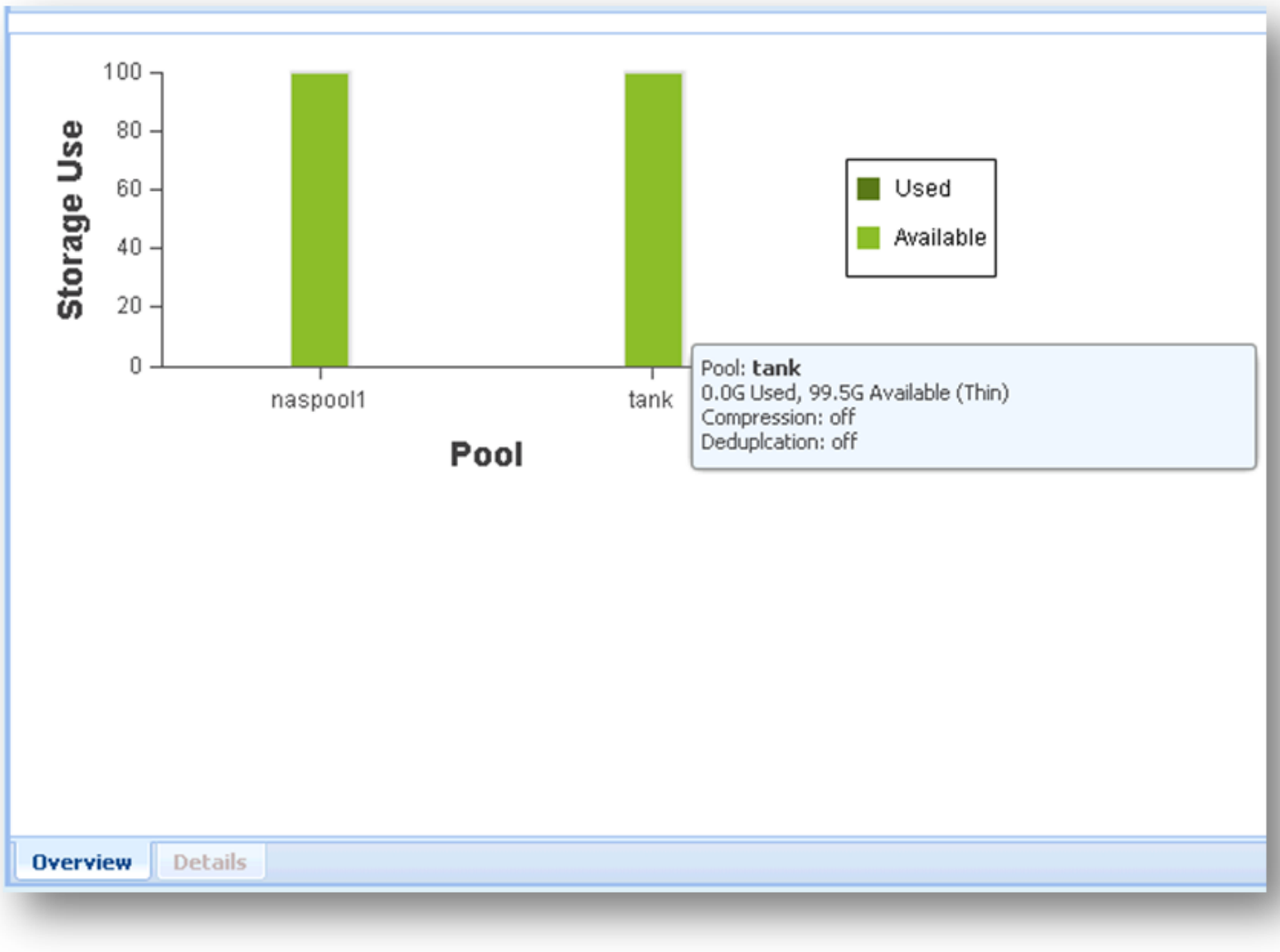
 **Refresh Page** - Press to update the pools list with the latest information.

11 Viewing Overview Chart

You can view the summarized details of storage pools in the **Overview Chart.**

1. To do so, simply navigate to the **Overview** tab in the left corner, at the end of the **Storage Pool** panel.

The **Storage Usage Chart** with a bar chart summarizing storage usage by pool will be displayed.



2. Move the mouse cursor over the top of a pool's bar. You can view the a summary of usage in a tooltip popu

3. To view the **Overview Chart** of a selected pool, click that pool to select it in the **Storage Pools** list.

The **Overview Chart** of the selected pool will be displayed.

12 Managing Pool Details

Details

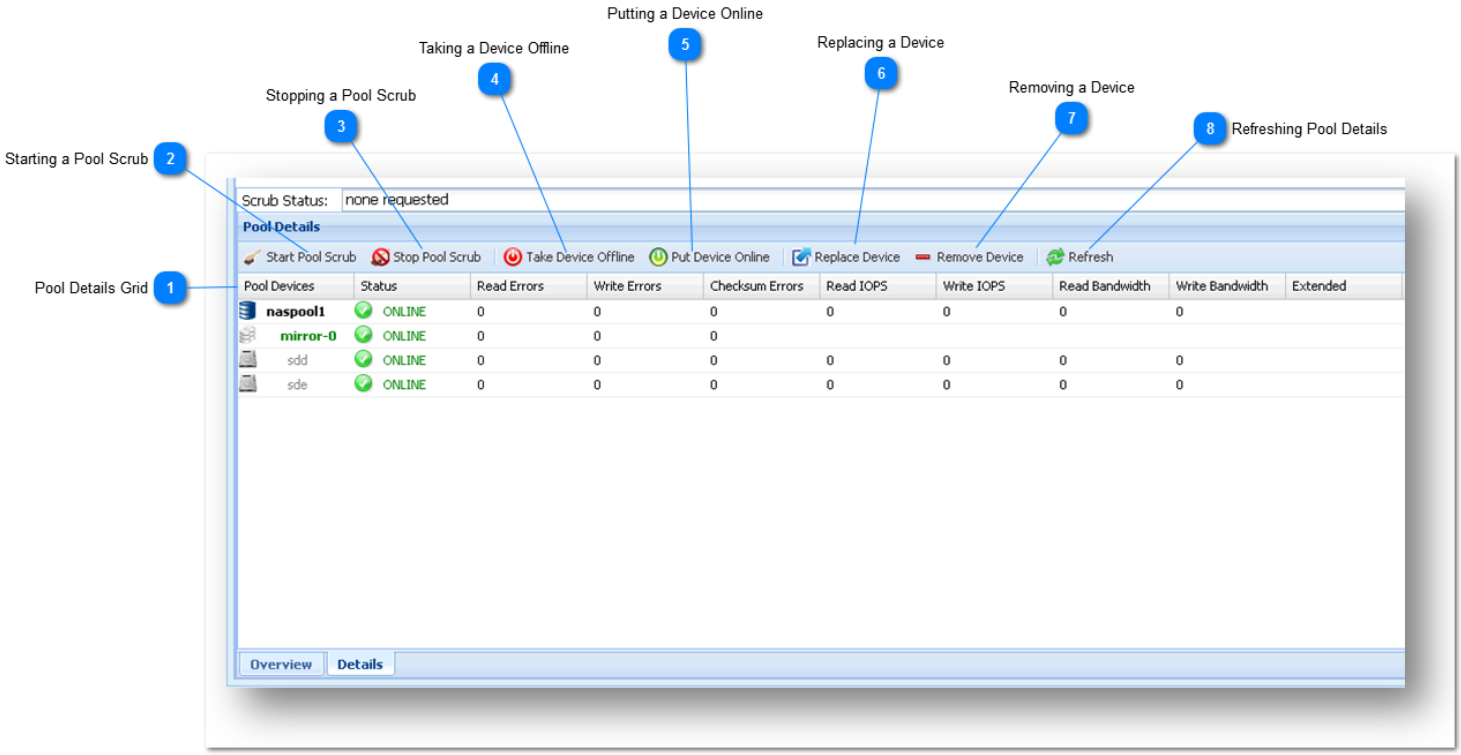
You can manage **Storage Pool** details from the **Details** tab. There are a number of useful pool and device statistics available. It provides detailed information about the storage pool, along with buttons that can be used to control the pool and its devices.

For more information, refer to the following link

Managing Pool Details

Managing Pool Details

You can manage **Storage Pool** details from the **Details** tab. It provides detailed information about the storage pool, along with buttons that can be used to control the pool and its devices.



1 Pool Details Grid

The **Pools Details Grid** displays the list of pool devices in a tabular grid format. There are a number of useful pool and device statistics available.

The pool details table has the following fields.

Field	Description
Pool Devices	It is the name of the volume. You can click this name of a volume in the list to select it.
Status	It shows the current status of the pool device. Based on the status, it shows the following types of indicators: • ONLINE icon- indicates the pool device is online, healthy and operating normally. • DEGRADED icon -indicates the pool device is in a degraded state, continues to process data normally, but is at increased risk and requires attention. • UNAVAIL or FAILED icon indicates the pool device is in a failed state
Read Errors	It shows the number of read errors during the last refresh period.
Write Errors	It shows the number of write errors during the last refresh period.

Checksum Errors	It shows the number of checksum errors detected.
Read IOPS	It shows the number read I/O operations on the device.
Write IOPS	It shows the number of write I/O operations.
Read Bandwidth	It shows the read bandwidth of the device.
Write Bandwidth	It shows the write bandwidth of the device.
Checksum Errors	It shows the number of checksum errors detected.
Write Bandwidth	It shows the write bandwidth to the device.
Extended	It shows the additional information (if any) that may be available for a device.

2 Starting a Pool Scrub

A scrub is an operation which examines the integrity of all data across the entire pool. Any errors or issues in corrected. Press the "Refresh" button for an update on the scrub operations progress.

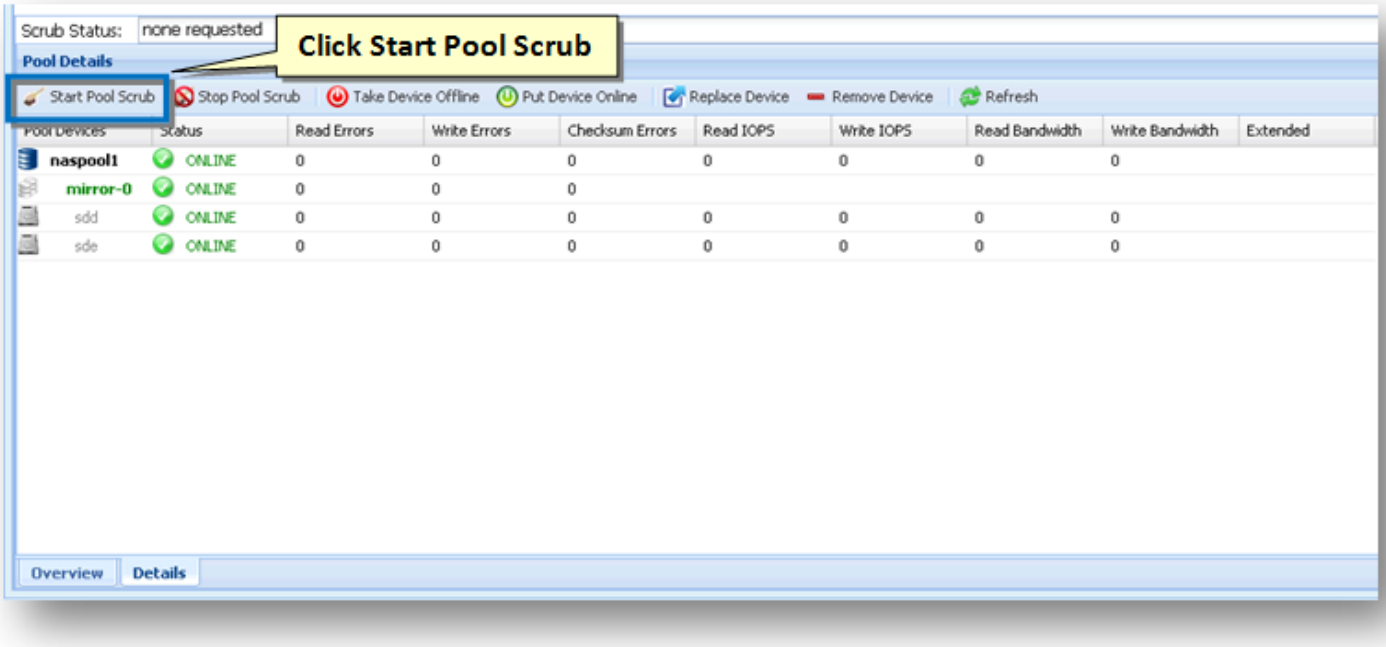
Note: Scrub operations on large pools or pools with a large number of small files can take an extended perioc complete. Please be patient when a scrub (or resilver) operation is in-progress - it will complete eventually, ev several days for extremely large pools.

Starting a Scrub is very easy.

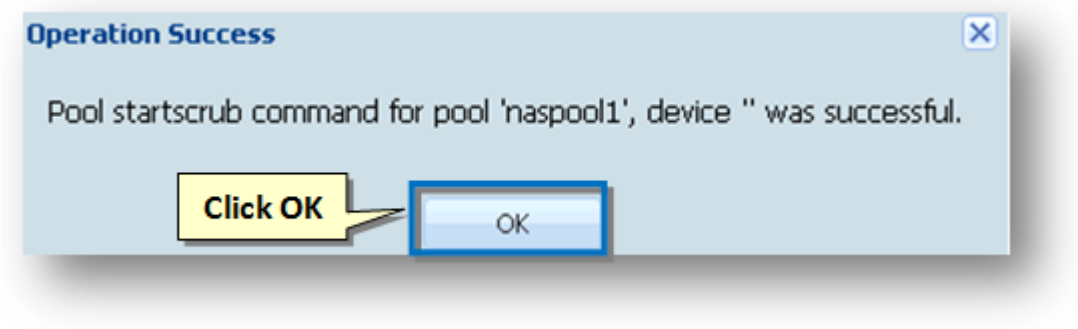
1. Navigate to **Pool Details** tab.

The **Pool Details** will be displayed.

2. Click the **Start Pool Scrub** button in the toolbar.



The **Operation Success** message box informing you about the successful starting of the pool scrub will be dis



3. Click the **Ok** button.

The start pool scrub will be initiated.

3 Stopping a Pool Scrub

You can stop a pool scrub operation that is in progress. It is not normally required to stop a pool scrub operation, as pool scrubs take place as lower-priority, background tasks.

1. To stop the pool scrub operation, simply click the **Stop Pool Scrub** button in the toolbar.

The pool scrub operation will be stopped.

4 Taking a Device Offline

You can take a selected device offline. Be careful when taking devices offline in an active, production storage pool, as it could potentially cause the pool to become unavailable, or at a minimum degrade the pool's ability to recover from an actual device failure. Taking devices offline should only be required if a device requires maintenance, which should be rare.

1. Select the device that you wish to take offline.

2. Click the **Take Device Offline** button in the toolbar.

The selected device will be taken offline.

Note: If a device is taken offline for a period of time, it will require **resilvering** to rebuild its integrity with the data changes that have occurred while it was offline.

5 Putting a Device Online

You can put a device online.

1. Select the device that you wish to put to online.
2. Click the **Put Device Online** button in the toolbar.

The selected device will be put to online.

6 Replacing a Device

Replacing a device is usually done when a device has failed.

1. To replace a device, select the device in the **Pool Details** Grid list.
2. Click the **Replace Device** button.

The selected device will be replaced by the Spare device.

Note: You must have a spare device available - the next available spare will be used if there are multiple spares.

7 Removing a Device

A device can be removed from the pool.

1. To remove a device, select the device in the **Pool Details** Grid list
2. Click the **Remove Device** button.

Note: You must take appropriate care when removing devices from an active pool, as it could degrade or fail the storage pool and cause data loss if the pool is unable to tolerate the device being removed.

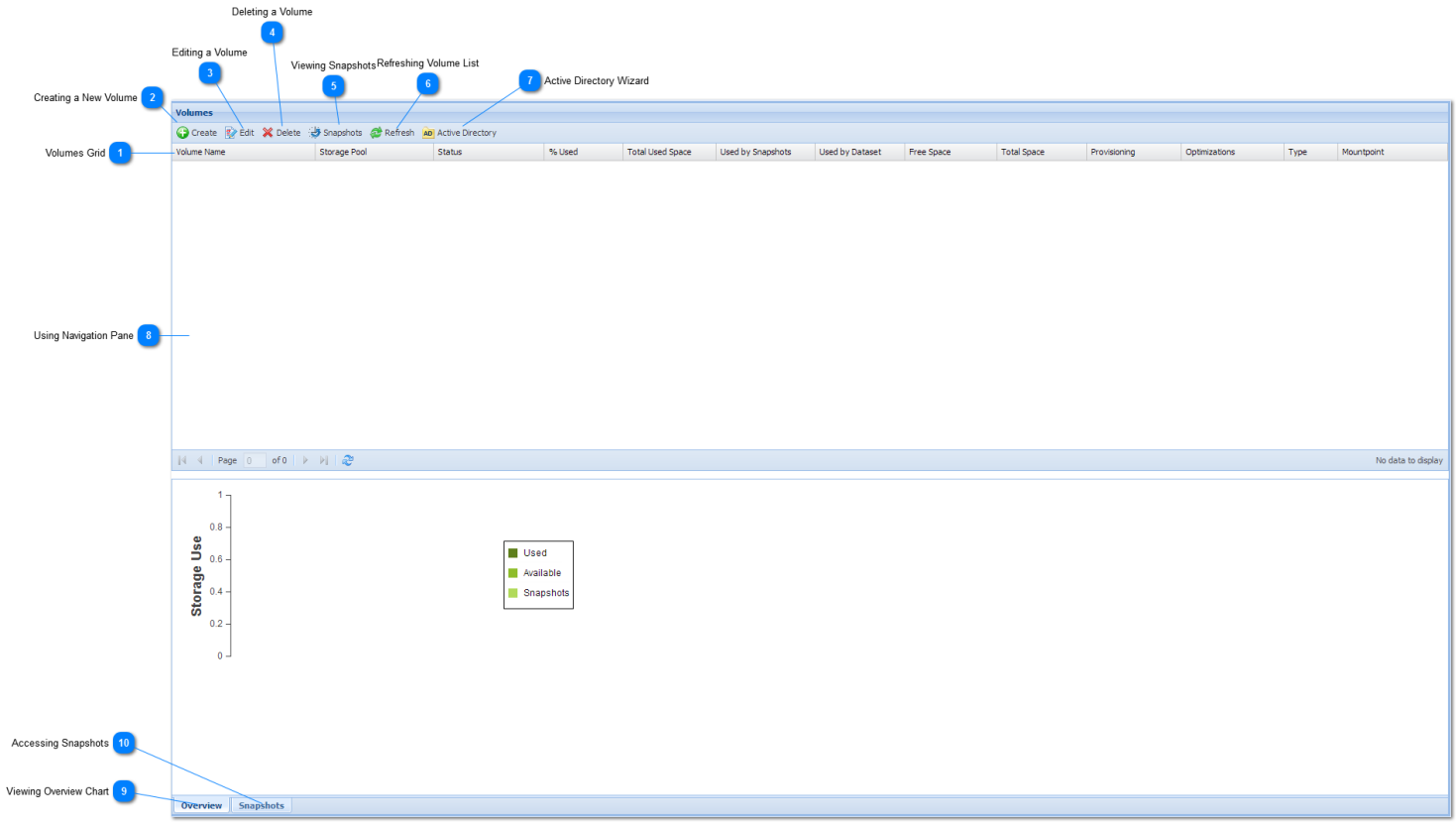
8 Refreshing Pool Details

You can refresh the pool detail list and update it with the latest information. To do so, simply click the **Refresh** button in the toolbar.

The **Pool Detail** list will be reloaded with the most current values.

Managing Volumes and LUNs

Volumes provide a way to allocate storage available in a storage pool and share it over the network. The **Volumes and LUNs** section of **SoftNAS** allows you to create, edit, remove and manage storage volumes and their snapshots.



1 Volumes Grid

The **Volumes Grid** displays the list of storage volumes in a tabular grid format. The volume table has the following fields.

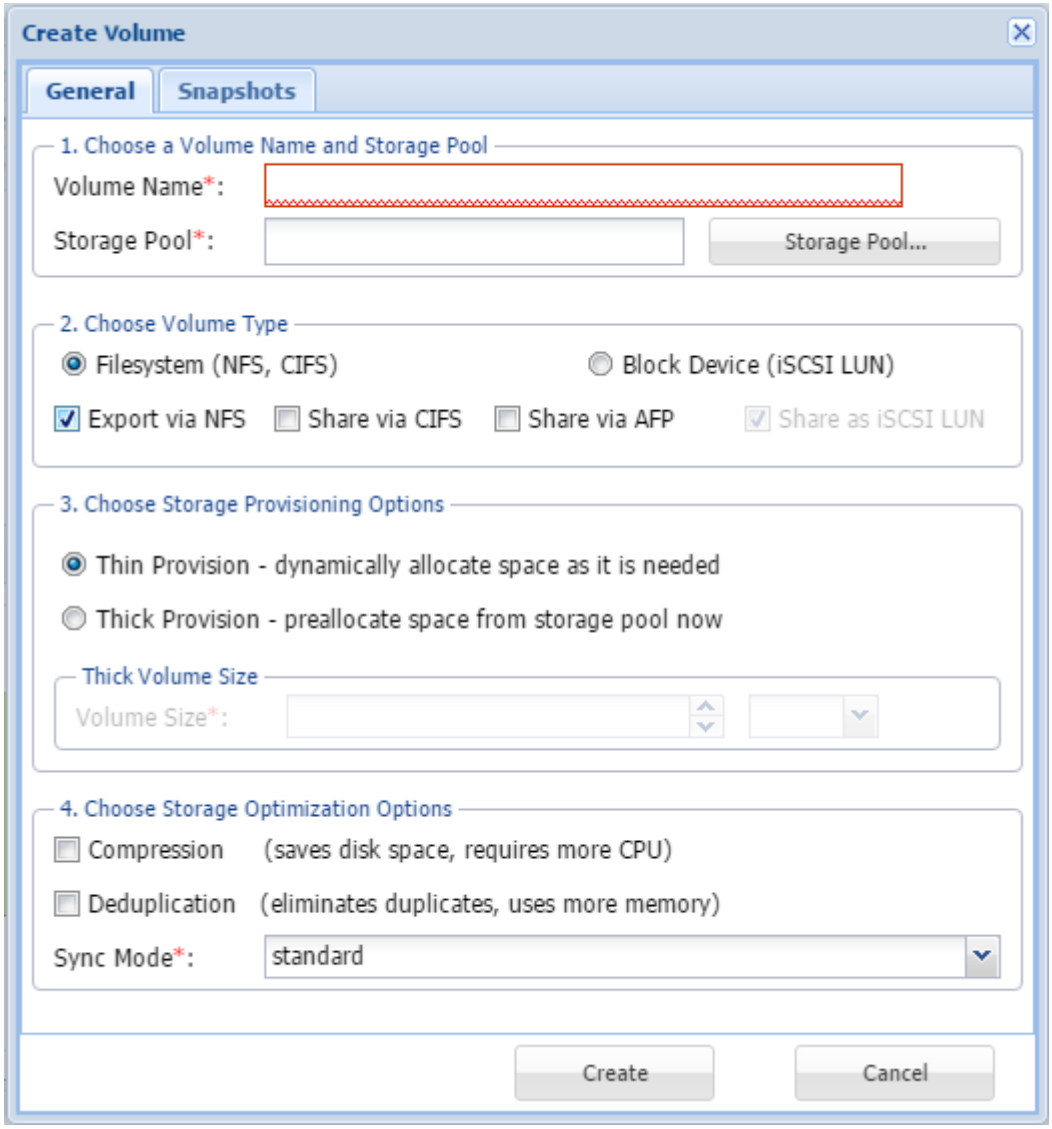
Field	Description
Volume Name	It is the name of the volume. You can click this name of a volume in the list to select it.
Storage Pool	It shows the name of the storage pool that is assigned to the volume.
Status	It shows the current status of the volume. Based on the status, it shows the following types of indicators: • ONLINE icon- indicates the volume and pool are online, healthy and operating normally. • DEGRADED icon -indicates the volume's pool is in a degraded state, continues to process data normally, but is at increased risk and requires attention; e.g., replace a failed disk in a RAID array. • UNAVAIL or FAILED icon indicates the volume's pool is in a failed state and is not currently processing storage requests. This usually means there are disk failures exceeding RAID protection.

% Used	It shows the percentage of available storage used. For thin-provisioned volumes, this is the percentage of the storage pool used. For thick-provisioned volumes, this is the percentage of the volume's allocated space used.
Total Used Space	It shows the amount of used up space in gigabytes.
Used by Snapshot	It shows the amount of space used by snapshots in gigabytes.
Used by Datasets	It shows the amount of space used by volume data sets in gigabytes.
Free Space	It shows the amount of free space available for use in gigabytes.
Total Space	It shows the total amount of space in the volume, in gigabytes. For thin-provisioned volumes, this is the same as the underlying storage pool's size. For thick-provisioned volumes, this is the volume size that was assigned.
Provisioning	It shows the provisioning type of the volume as Thick or Thin.
Optimizations	It shows the configured optimization option of the volume. The available options include the following: # None - no optimizations configured # Dedup - deduplication is enabled # Compress - data compression is enabled # Dedup+Compress - both deduplication and compression are enabled
Type	It shows the type of the volume. The available types of volume include: • Blockdevice – Refers to the volume that is a block device type, commonly used for iSCSI LUN creation and sharing. Block device mount points are in the /dev/ filesystem. • Filesystem- Refers to the volume that is a a filesystem type, commonly used for NFS and CIFS sharing (or FTP and other supported protocols).
Mountpoint	It shows the mount point used to access the volume in the Linux filesystem.

2 Creating a New Volume

1. Click the **Create** button in the toolbar.

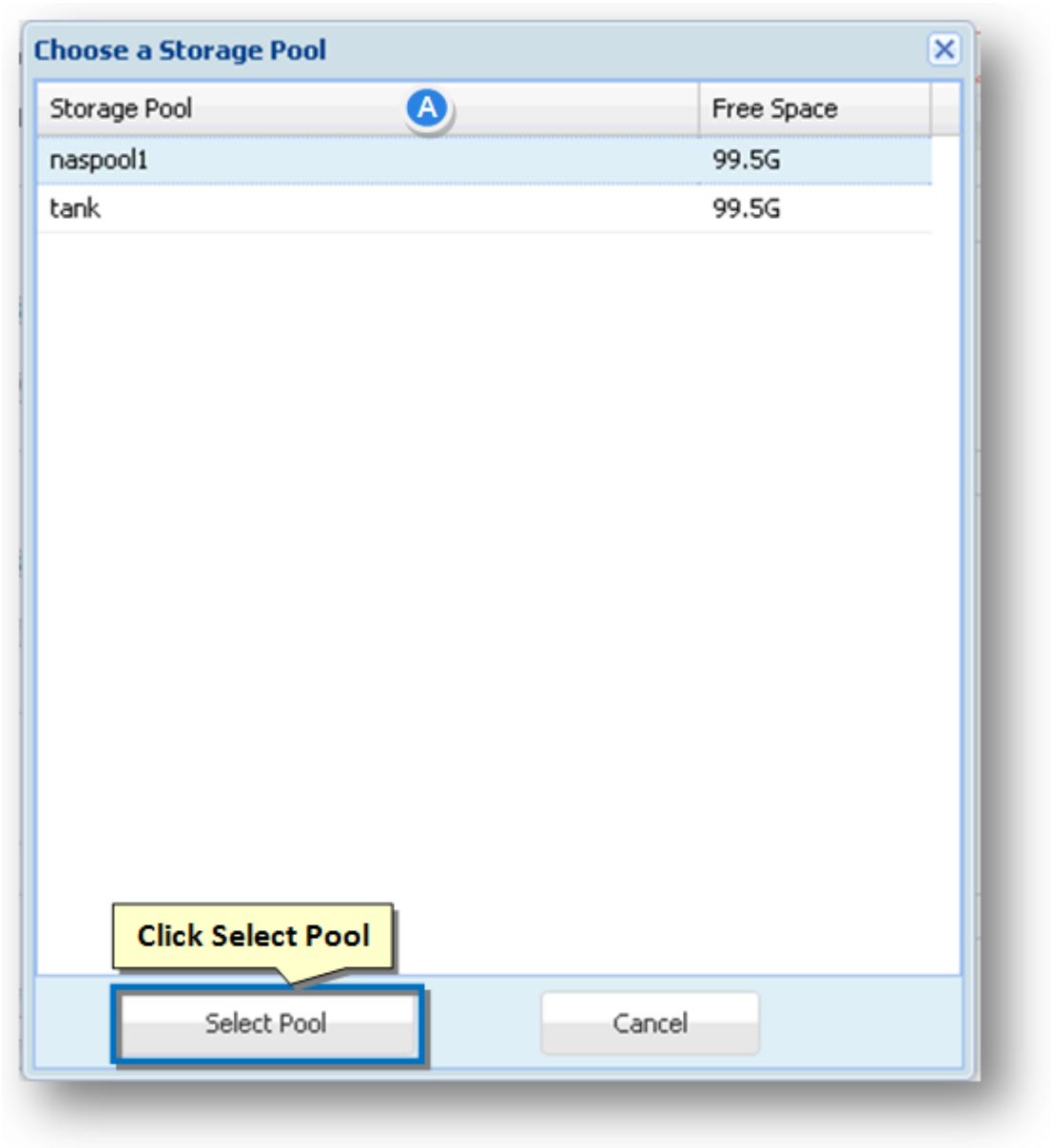
The **Create Volume** dialog will be displayed.



2. Enter the name of the volume in the **Volume Name** text entry box.

3. To select the storage pool where the storage space for the volume has to be reserved, click the **Storage Pool** button.

The **Choose a Storage Pool** dialog will be displayed.



A. Select the required storage pool from the list of available storage pools.

B. Click the **Select Pool** button.

Back in the **Create Volume** dialog, the name of the selected storage pool will be displayed in the **Storage Pool** field.

4. Select the type of the volume from the **Volume Type** section. The available volume types are **File System (NFS, CIFS, AFP)** and **Block Device (iSCSI LUN).**

Note: If you want to share the volume via iSCSI, then choose **Block Device** instead of accepting the default **File System** volume type.

5. **One-click Sharing - SoftNAS** supports **one-click sharing** during Volume creation. Choose the appropriate sharing option checkboxes to **Export to NFS** and/or **Share via CIFS**, **Share Via AFP** as appropriate. Verify the type of one-click sharing selected. The available options are **Export via NFS, Share via CIFS** and **Share via AFP** for the **File System** volume type and **Share as iSCSI LUN** for **Block Device** volume type.

6. Select the type of the storage provisioning option. The available options include **Thin Provision - Dynamically allocate space as it is needed** and **Thick Provision - Preallocate space from storage pool now.**

Thin Provision and Thick Provision

Thin-provisioning allows a volume to acquire storage from its Storage Pool on an as-needed basis, as new data is written to the volume. Thin-provisioning enables many volumes to share a storage pool without an upper limit being placed on the volume itself (the only upper limit to the volume's size is available space in the pool). Thick-provisioned volumes reduce the amount of space available in the Storage Pool by reserving this space for use by a specific volume. When a thick-provisioned volume reaches its maximum volume size, no more data can be written and a volume full error will be returned for writes to a full volume. Thick-provisioned volumes can be re-sized at any time to add space (or return space to the storage by by reducing the volume size).

Volume Size:

7. If you select the type of the storage provisioning option as **Thick Provision** in the previous step, then specify the size of the volume in the **Volume Size** field and select the size unit**.**

Once a Storage Pool has been selected for a thick-provisioned volume, the amount of available space to allocate is displayed below the **Volume Size** field, as shown in the example below.

The **Volume Size** value can be any valid numeric value; e.g., 10, 12.5, 100.0, 1.25

8. The **Size Units** selector is used to choose the units for the **Volume Size.** Select the required size unit from the drop down list. The available units include MB – Megabytes, GB - Gigabytes (default) and TB – Terabytes.

Storage Optimization

9. Select the required option for storage optimization in the **Storage Optimization Options** section. The available options are **Compression** and **Deduplication.** The **Compression** type saves disk space, but requires more of CPU space. The **Deduplication** type eliminates duplicates, but consumes more memory space.

The **Compression** type saves disk space, at the expense of additional CPU overheads for each read and write request (to decode and encode the data). Depending on how compressible the data is, it is common to see data compression rates up to 50% or more.

Note: If you compress a significant amount of data, be sure to observe the amount of actual CPU consumed during a typical day, and if necessary, add more CPU capacity to the SoftNAS VM as required to ensure compression is fast and efficient. If data is not highly-compressible, then disabling compression provides a better performance tradeoff.

- The **Deduplication** type eliminates duplicates, but consumes more memory space. For certain types of data (e.g., Windows virtual machine images, which are highly-redundant in virtual desktop applications), deduplication can save up to 80% on storage requirements by eliminating duplicate data. Each time a duplicate data block is to be written, a pointer to the existing duplicate block is created instead, along with increasing the duplicate block reference count. To make these operations as fast as possible, a table of deduplicated blocks is maintained. A hash table of deduplicated blocks is kept in memory to make lookups very fast. When a duplicate block is read, it is usually in cache memory and is simply returned with no disk I/O required.

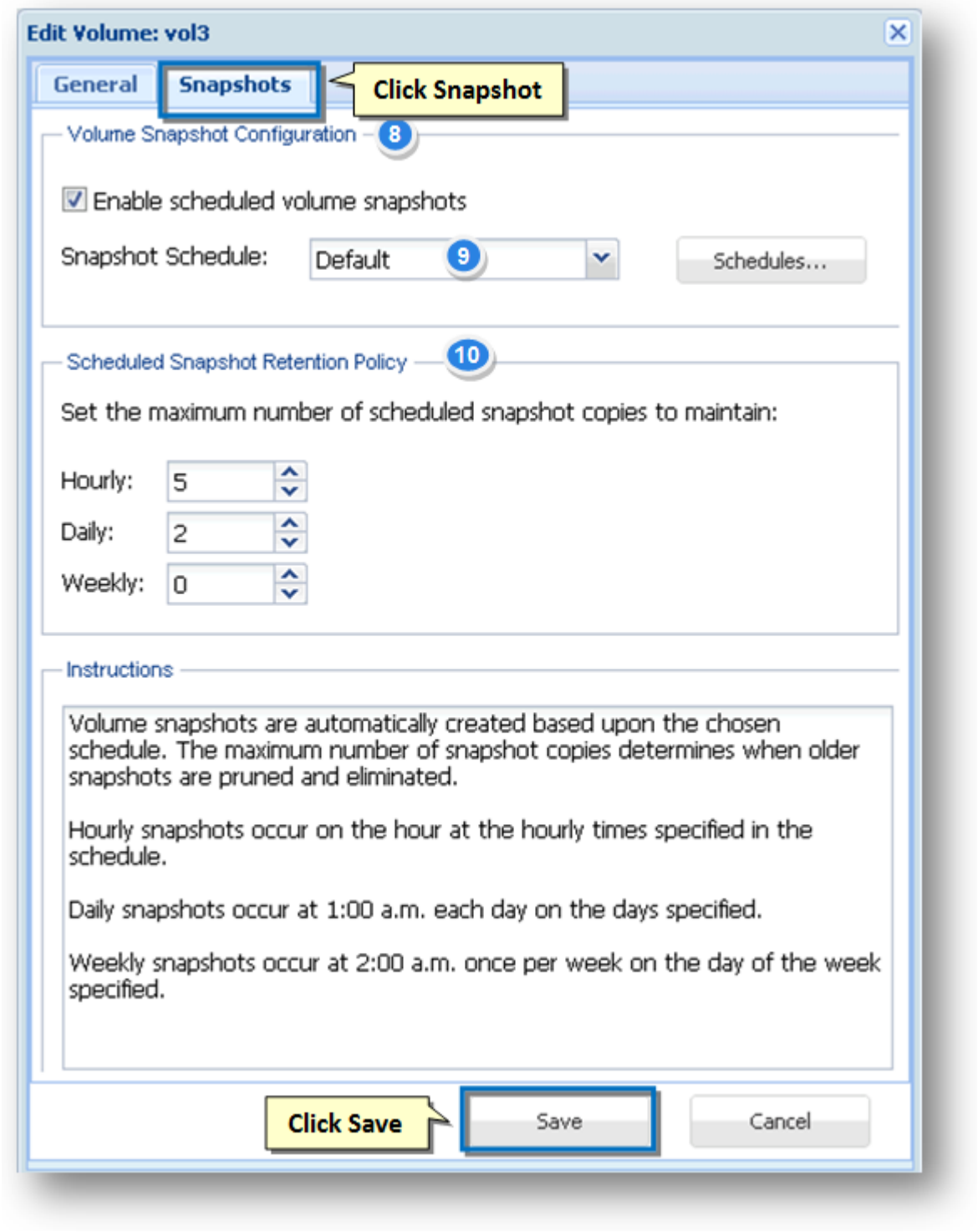
Note: It is recommended to avoid using deduplication unless the data is highly-duplicative, because of the memory impact of deduplication. It is estimated that for every terabyte of deduplicated data

managed, one gigabyte of memory is required for the deduplication lookup tables. These tables compete with cache memory, which can reduce the overall performance of SoftNAS.

Snapshots

10. Optionally, you can click the **Snapshots** tab to configure the same.

The **Snapshots** section of the dialog will be displayed.



Volume snapshots are automatically created based upon the chosen schedule. The maximum number of snapshot copies determines when older snapshots are pruned and eliminated.

11. In the **Volume Snapshot Configuration** section, check the box in order to enable the scheduling of volume snapshots.

12. Select the type of snapshot schedule from the **Snapshot Schedule** drop down list. The available options include are **Default, 24 x 7, Maximum Snapshots** and **Business.**

13. In the **Scheduled Snapshot Retention Policy** section, set the maximum number of scheduled snapshot copies to maintain in the **Hourly, Daily** and **Weekly** fields by either manually entering the value or by using the scroll bar to increase or decrease the value.

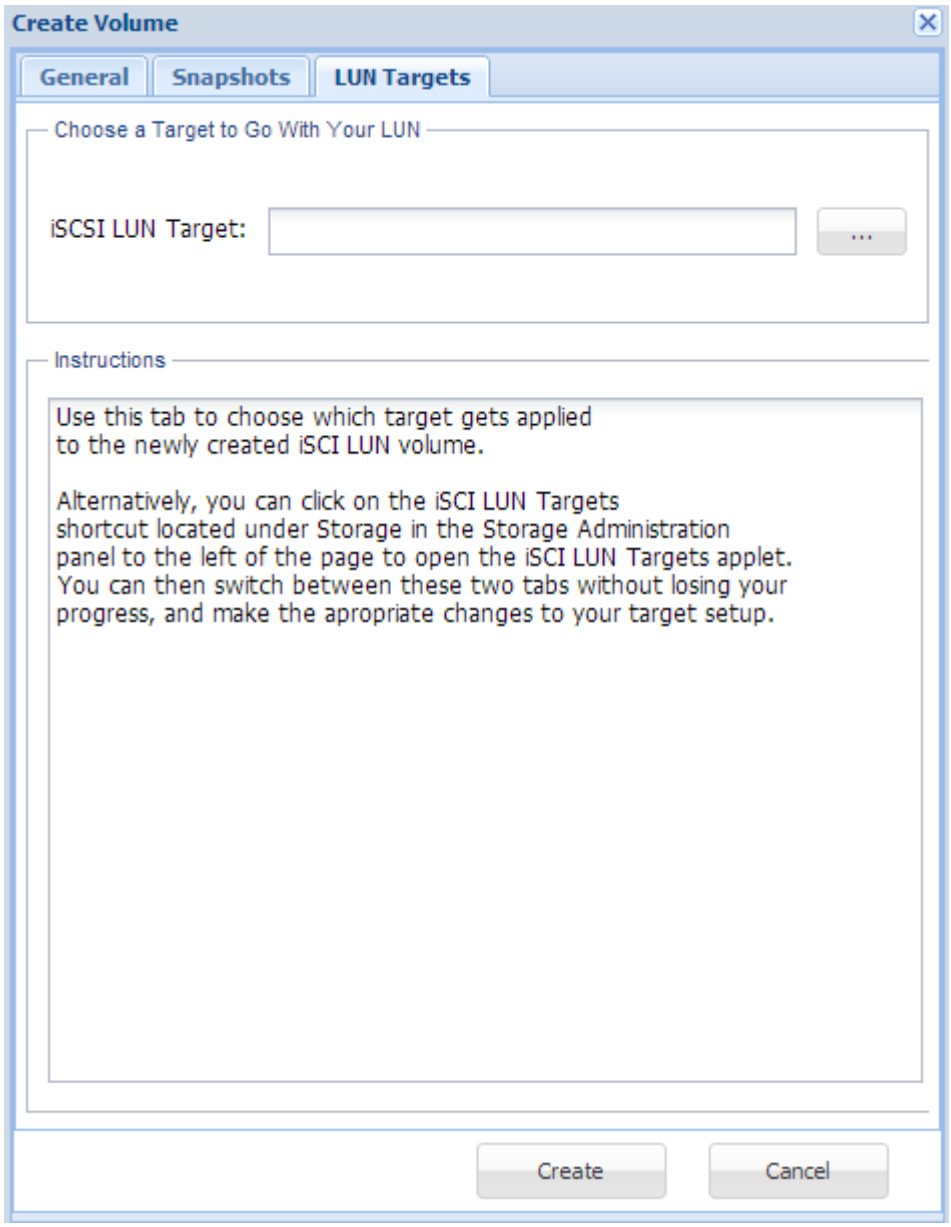
Note:
- Hourly snapshots occur on the hour at the hourly times specified in the schedule.
- Daily snapshots occur at 1:00 a.m. each day on the days specified.
- Weekly snapshots occur at 2:00 a.m. once per week on the day of the week specified.

14. Click the **Create** button at the end.

The new volume is created and it shared on the network.

Block Device (iSCSI LUN)

If **Block Device (iSCSI LUN)** is selected during Volume Creation, the LUN Targets tab is displayed. You can use the LUN Targets tab to select an available iSCSI LUN Target as part of your create Volume workflow.



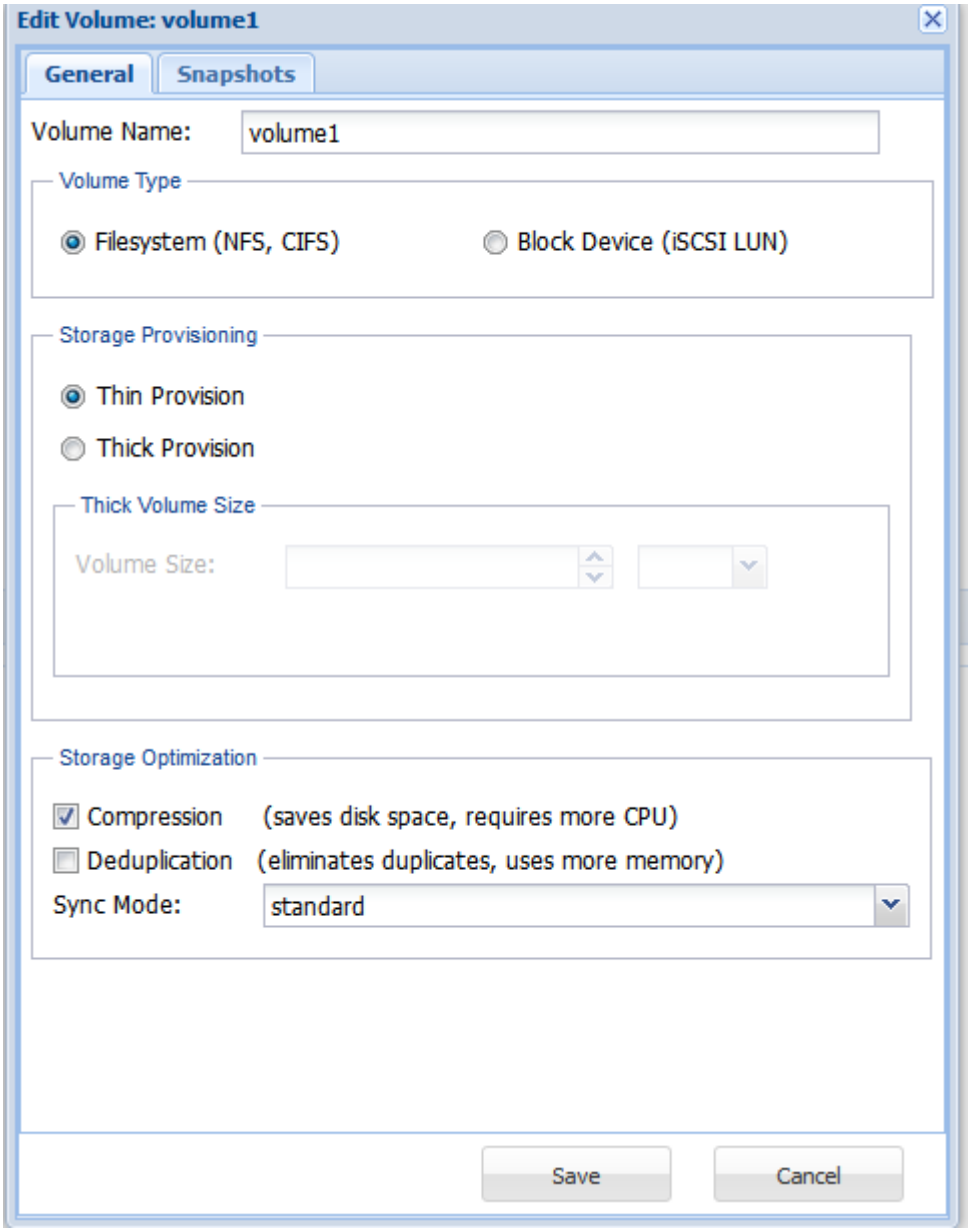
You are prompted to select the appropriate target

3 Editing a Volume

You can edit any selected volume. To do so, simply follow the steps given below.

1. Select the volume that you wish to edit in the **Volumes** list.
2. Click the **Edit** button in the toolbar.

The **Edit Volume** dialog will be displayed.



Note: You cannot edit the name and type of the volume.

3. Select the type of the storage provisioning option. The available options include **Thin Provision** - Dynamically allocate space as it is needed and **Thick Provision** - Preallocate space from storage pool now. By default, volumes are thin-provisioned.

4. If you select the type of the storage provisioning option as **Thick Provision** in the previous step, then specify the size of the volume in the **Volume Size** field.

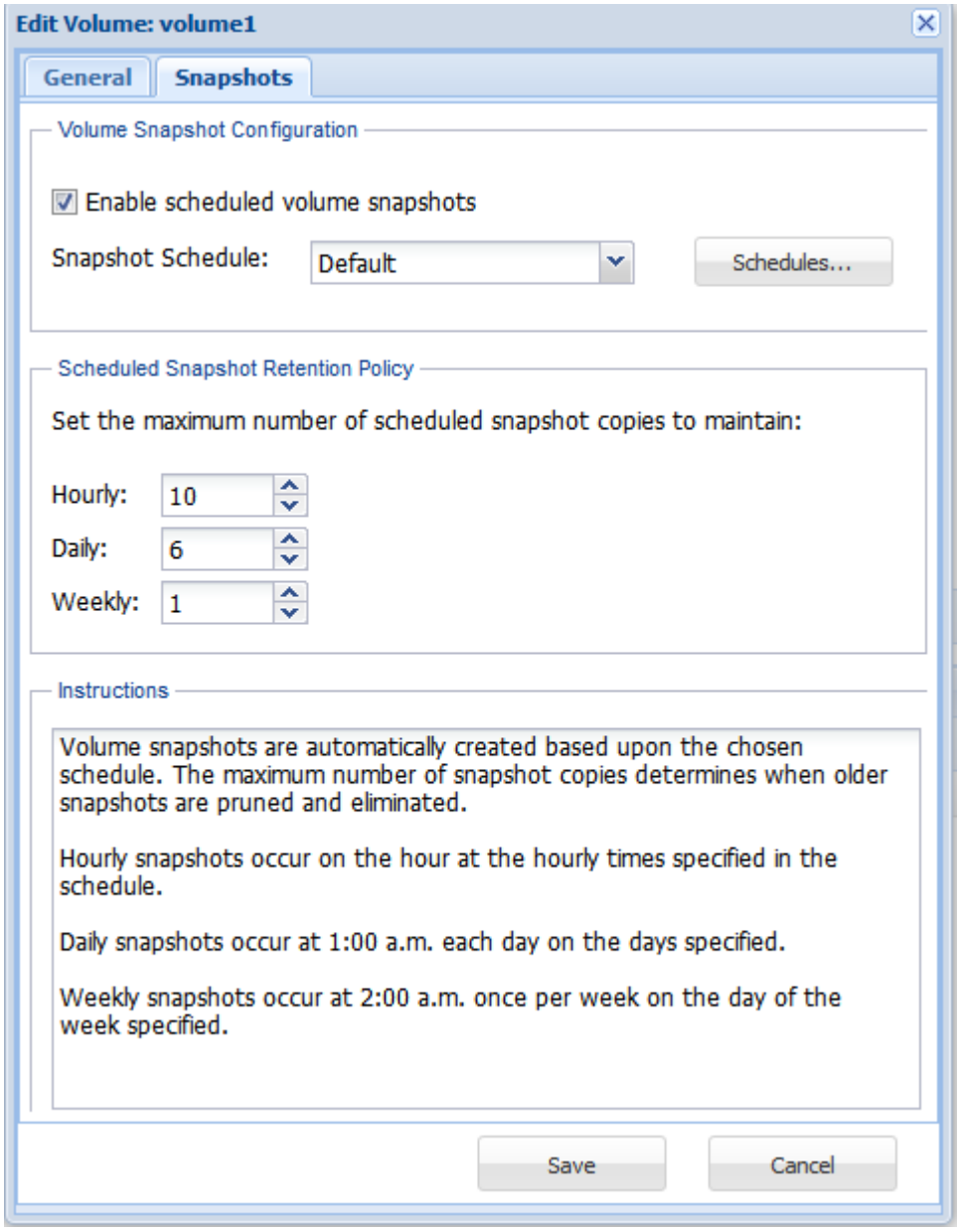
Note: When **Think Provision** is selected the **Volume Size** specifies how much space is to be pre-allocated to the volume. Space is determined by entering a **Volume Size** amount as a floating point value, along with choosing the Size Units.

6. Select the required option for storage optimization in the **Storage Optimization Options** section. The available options are **Compression** and **Deduplication.**

7. Select the Sync Mode: standard, always, disabled.

8. Click the **Snapshots** tab.

The **Snapshots** section of the dialog will be displayed.



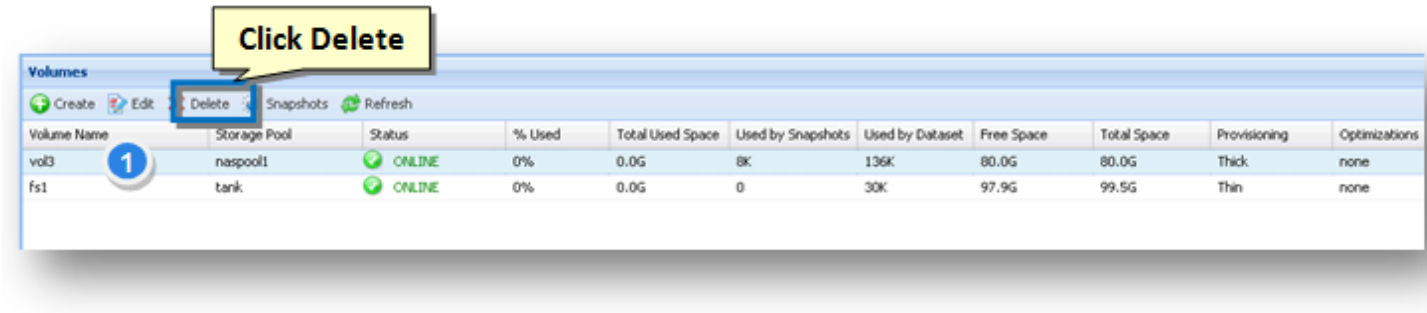
8. Edit the parameters of the Snapshots configuration as necessary.
9. Click the **Save** button.

The changes made to the volume will be updated.

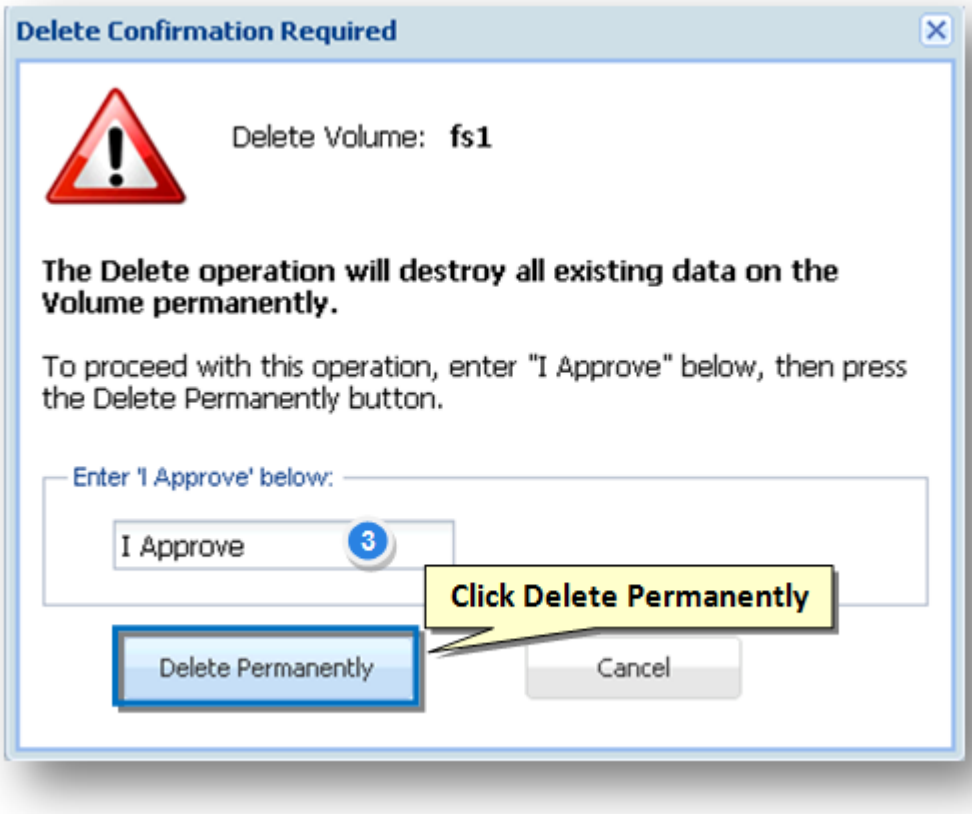
4 Deleting a Volume

You can delete an ununsed volume. To do so, simply follow steps given below.

1. Select the volume that you wish to delete in the **Volumes** list.
2. Click the **Delete** button in the toolbar.



The **Delete Confirmation Required** dialog will be displayed.



3. Enter the text as **I Approve** in the text entry box.
4. Click the **Delete Permanently** button.

The selected volume will be removed.

5 Viewing Snapshots

You can access, view and manage storage snapshots. To do so, click the **Snapshots** button in the toolbar.

The **Snapshots** tab will be displayed in the lower part of the **Volume** panel.

For more information, refer to the Managing Snapshots section.

6 Refreshing Volume List

You can refresh the volumes list and update it with the latest information. To do so, simply click the **Refresh** button in the toolbar.

The **Volumes** list will be reloaded with the most current values.

7 Active Directory Wizard

You can click on **Active Directory** to launch the Active Directory Wizard.

Features include:

• Step by step configuration wizard
• Configures AD by collecting configuration settings (e.g., domain name, Windows admin ID/password, etc.).
• Verifies AD integration and authentication are operating correctly (and reports any errors or issues).

For more information and step by step instructions, see the document "SoftNAS Installation Guide."

8 Using Navigation Pane

You can use the **Navigation Pane** to navigate between volume records. It has the following set of buttons.

 **First Page** - Press to navigate to the First page of volumes (when the number of volumes exceeds the number that can be displayed on a single page).

 **Previous Page** - Press to navigate to the Previous page of volumes (when the number of volumes exceeds the number that can be displayed on a single page).

Page Number - Displays the current page of volumes (when the number of volumes exceeds the number that can be displayed on a single page). You can also enter the page number in the box to navigate to that page.

 **Next Page** - Press to navigate to the Next page of volumes (when the number of volumes exceeds the number that can be displayed on a single page).

 **Last Page** - Press to navigate to the Last page of volumes (when the number of volumes exceeds the number that can be displayed on a single page).

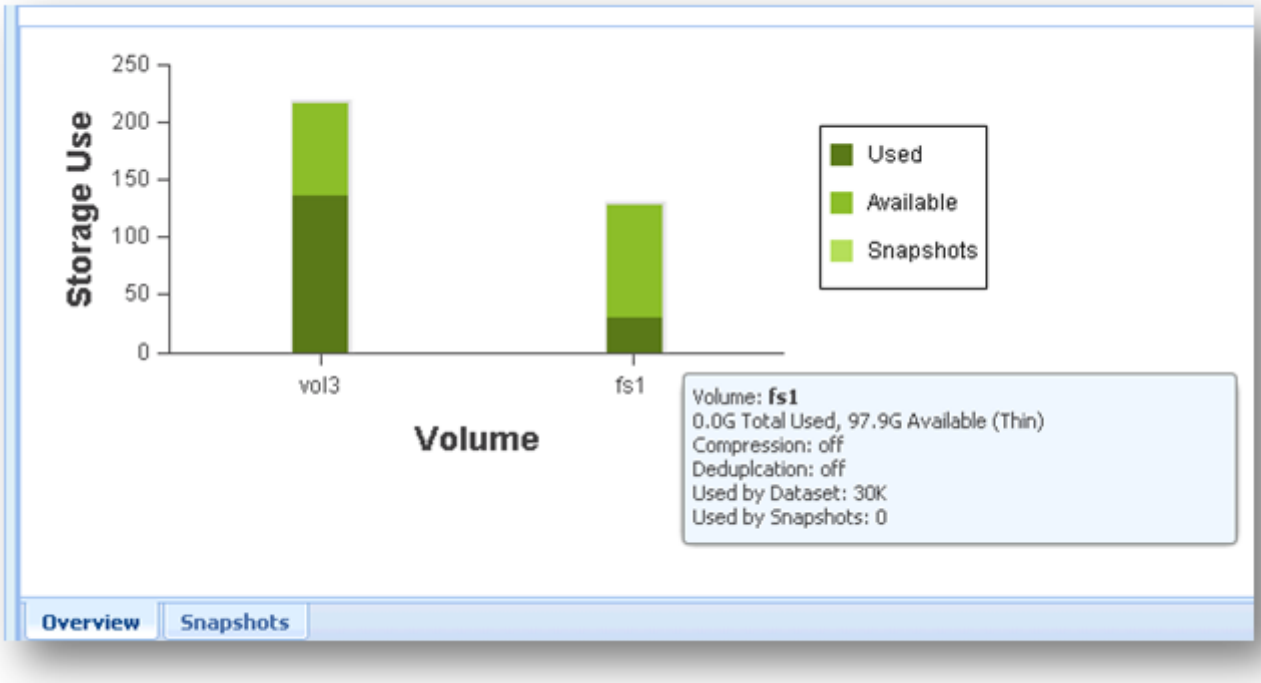
 **Refresh Page** - Press to update the volumes list with the latest information.

9 Viewing Overview Chart

You can view the summarized details of volume in the **Overview Chart.**

1. To do so, simply navigate to the **Overview** tab in the left corner, at the end of the **Volumes** panel.

The **Volume Usage Chart** with a bar chart summarizing storage usage by volume will be displayed.



2. Move the mouse cursor over the top of a volume's bar. You can view the a summary of usage in a tooltip popup window.

3. To view the **Overview Chart** of a selected volume, click that volume to select it in the **Volumes** list.

The **Overview Chart** of the selected volume will be displayed.

10 Accessing Snapshots

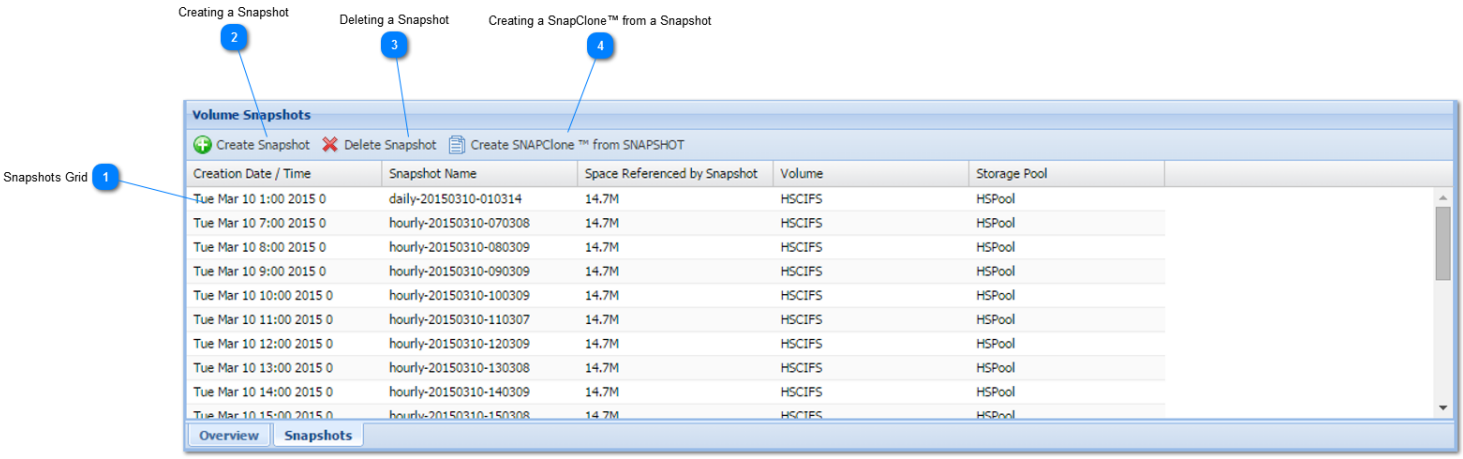
You can access, view and manage storage snapshots. To do so, click the **Snapshots** tab.

The **Snapshots** tab will be displayed with the list of all volume snapshots.

For more information, refer to the **Managing Snapshots** section.

Managing Snapshots

The **Snapshots** tab contains the Volume Snapshot Control Panel.



1 Snapshots Grid

The **Snapshots** grid shows a list of snapshots for the currently selected volume (in the upper grid on the page). If no single volume is selected, then snapshots for all volumes are shown (default until a volume is selected). The **Snapshots** table has the following fields.

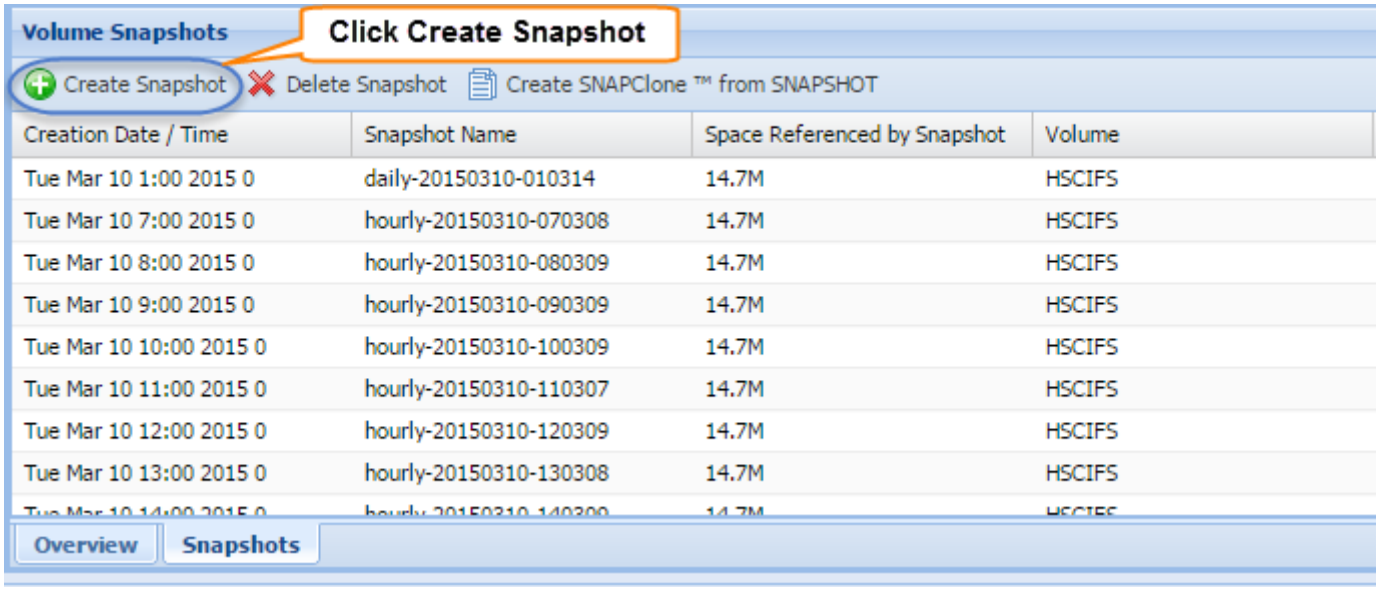
Field	Description
Creation Date/Time	It is the date and time when the snapshot was created. This is the point in time at which an index to the volume's state was marked.
Snapshot Name	It is the unique name given to every snapshot that is identified with a volume. Scheduled snapshots have names corresponding to the frequency at which snapshots are taken; i.e,, hourlyNN, dailyNN, weeklyNN. When an ad-hoc snapshot is created, it is receives a name in the form "snapMMMDDYYYY-HHMMSS; e.g., snapJun242013-135901 would have been taken on June 24, 2013 at 1:59:01 p.m.
Space Referenced By Snapshot	It is the space referenced by the snapshot
Volume	It is the volume to which the snapshot is referred to.
Storage Pool	The snapshot's storage pool

2 Creating a Snapshot

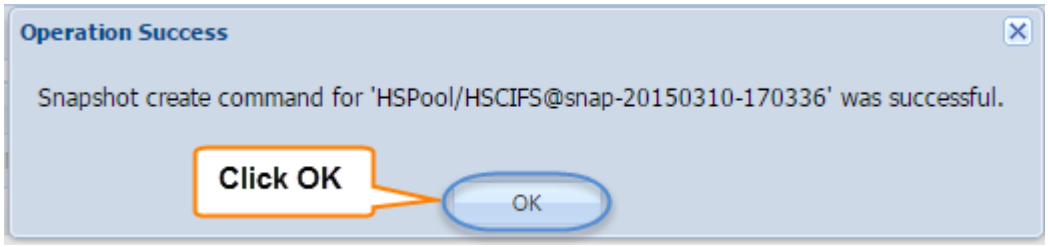
You can create an ad-hoc snapshot of the currently selected volume. To do so, simply follow the steps given below.

1. Select the volume to which the snapshot needs to be created.
2. Navigate to the **Snapshots** tab.

3. Click the **Create Snapshot** button in the toolbar.



The **Operation Success** message confirming the successful creation of the snapshot will be displayed.



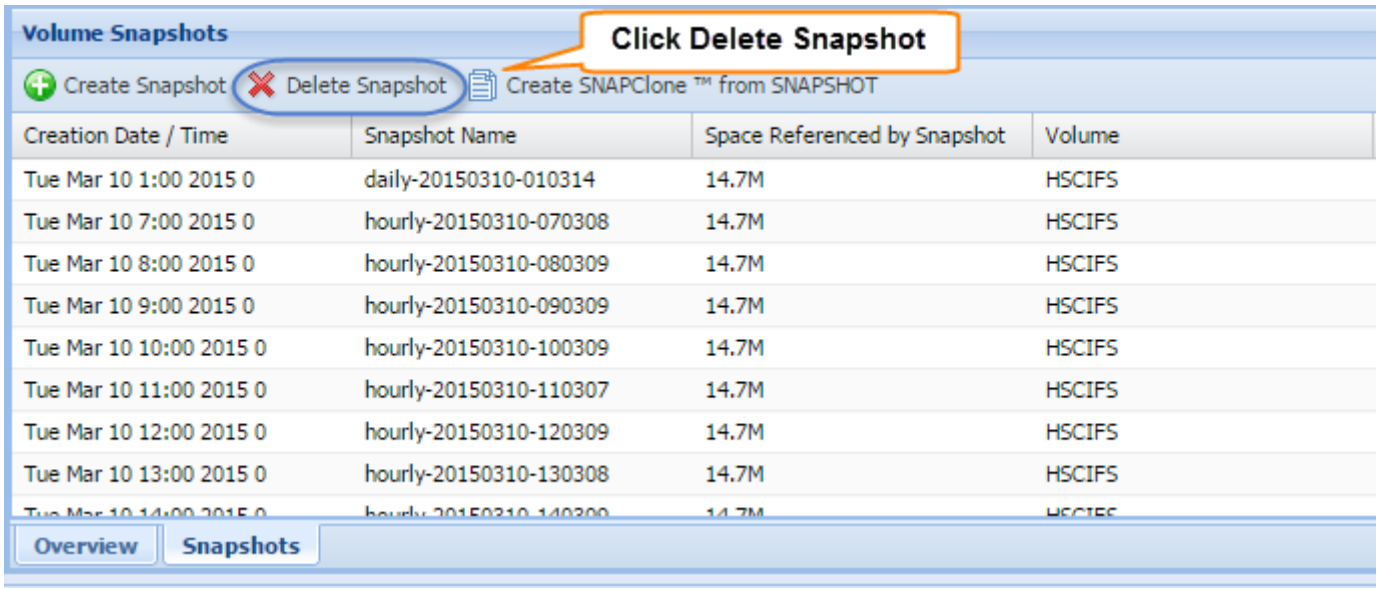
4. Click **OK**.

The new snapshot volume will be created.

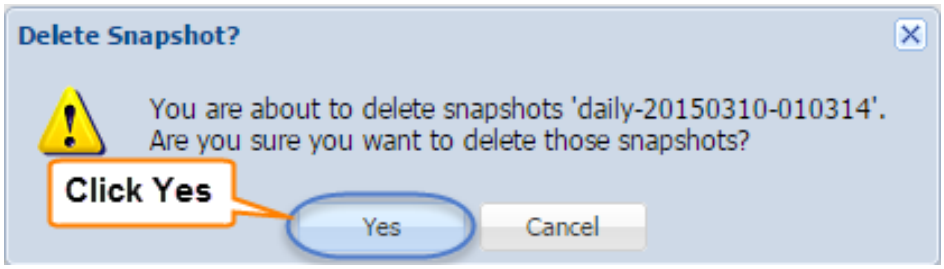
3 Deleting a Snapshot

You can easily delete a snapshot. Simply follow the steps given below.

1. Select the volume from which you wish to remove the snapshot.
2. Navigate to the **Snapshots** tab.
3. Click the **Delete Snapshot** button in the toolbar.



The **Delete Snapshot** message asking you to confirm the deletion of the snapshot will be displayed.



4. Click **Yes.**

The selected snapshot will be removed.

Note: Removing a snapshot removes the recovery point, along with any older disk blocks that were associated with the snapshot (it does not affect any current data blocks).

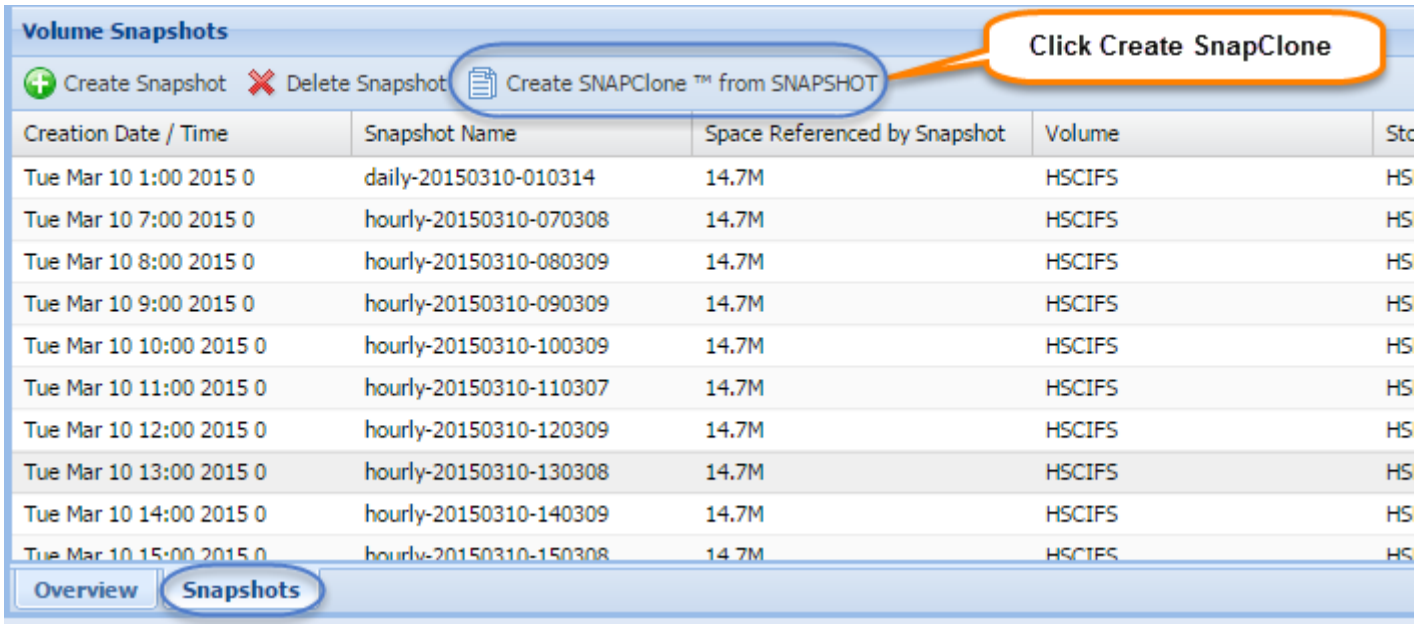
4 Creating a SnapClone™ from a Snapshot

You can create a new volume as a writable clone of the snapshot. The writable clone volume is an exact replic of the volume at the time the snapshot was originally taken. The cloned volume doesn't take up any appreciable additional space; however, as changes are made to the cloned volume, new data blocks are created as **difference blocks.**

Simply follow the steps given below.

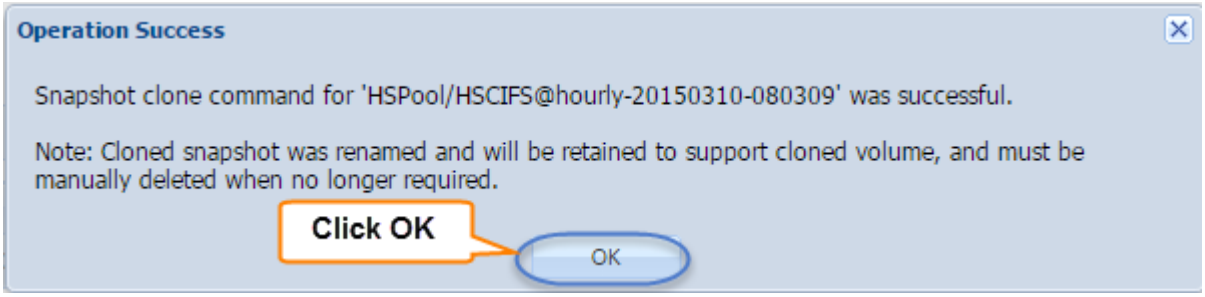
1. Navigate to the **Snapshots** tab.

2. Click **Create SnapClone™ from Snapshot** in the toolbar.



Note: It is best practice to recover any data you may need from the cloned volume, then delete the clone and its snapshot as soon as possible; otherwise, the snapshot and clone will continue to keep the older disk blocks **locked up** (allocated), occupying additional disk space over time.

The **Operation Success** message confirming the successful creation of the cloned, writable volume from snapshot will be displayed.



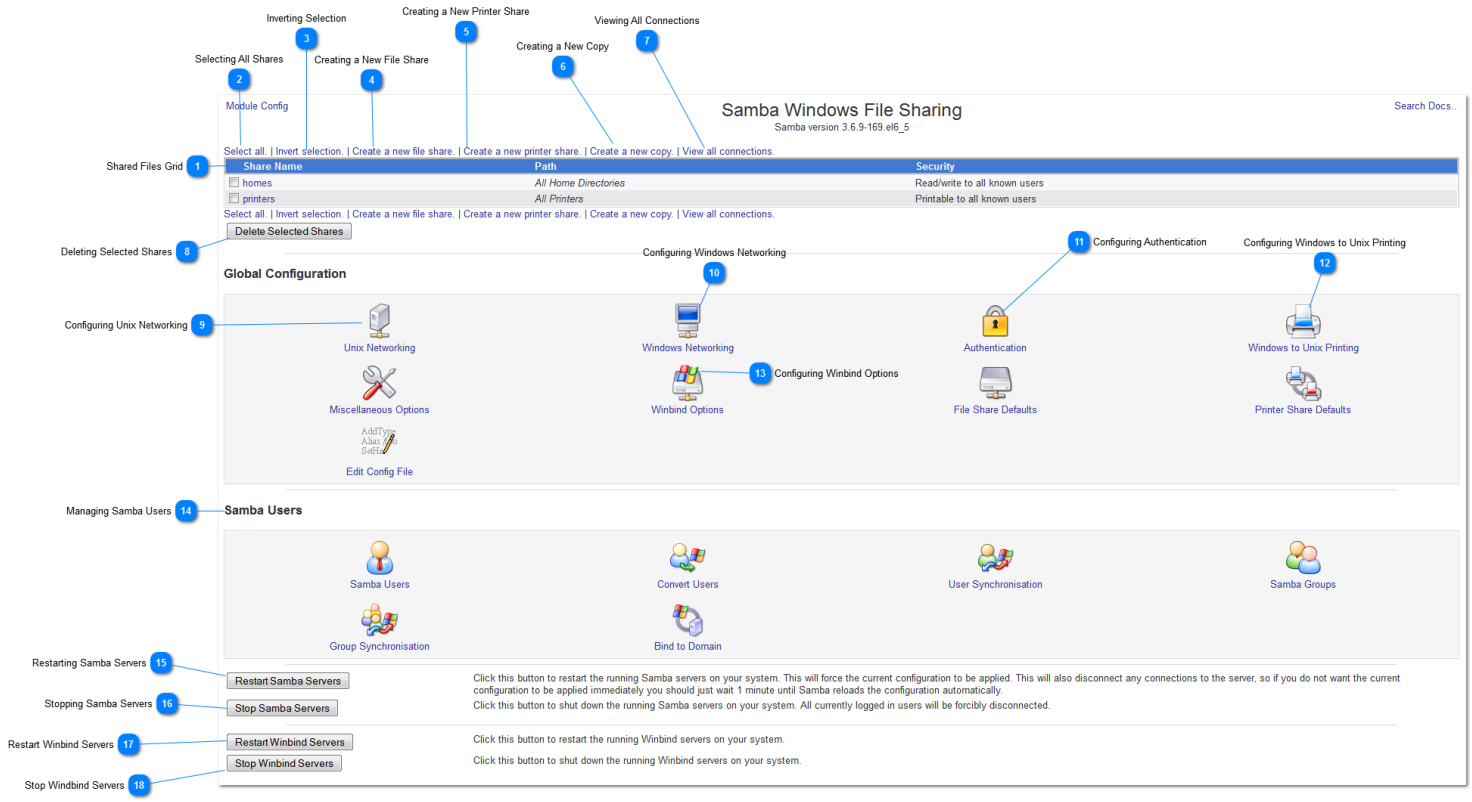
3. Click **OK.**

The new SnapClone™ volume from snapshot will be created and added to the list of existing volumes.

Configuring CIFS Shares

The **Common Internet File System (CIFS)** is the standard way that computer users share files across corporate intranets and the Internet. It provides users with seamless file and print interoperability between VMs and Windows-based clients. **CIFS** allows multiple clients to access and update the same file while preventing conflicts by providing file sharing and file locking.

SoftNAS uses **Samba Windows File Sharing** for secured, stable and fast file sharing and print services. It allows the networking of Microsoft Windows®, Linux, UNIX, and other operating systems together, enabling access to Windows-based file and printer shares. **Samba** seamlessly integrates Linux/Unix Servers and Desktops into Active Directory environments using the winbind daemon.



1 Shared Files Grid

The **Shared Files Grid** displays the list of all shared files in a tabular grid format. It has the following fields.

Field	Description
Share Name	It is the name of the share.
Path	It specifies the path that is shared.
Security	It shows the type of security available for the share.

2 Selecting All Shares

You can select all the file shares. To do so, simply click the **Select All** button.

All the shared files in the list will be selected.

3 Inverting Selection

You can invert the selection of the file shares. To do so, simply click the **Invert Selection** button.

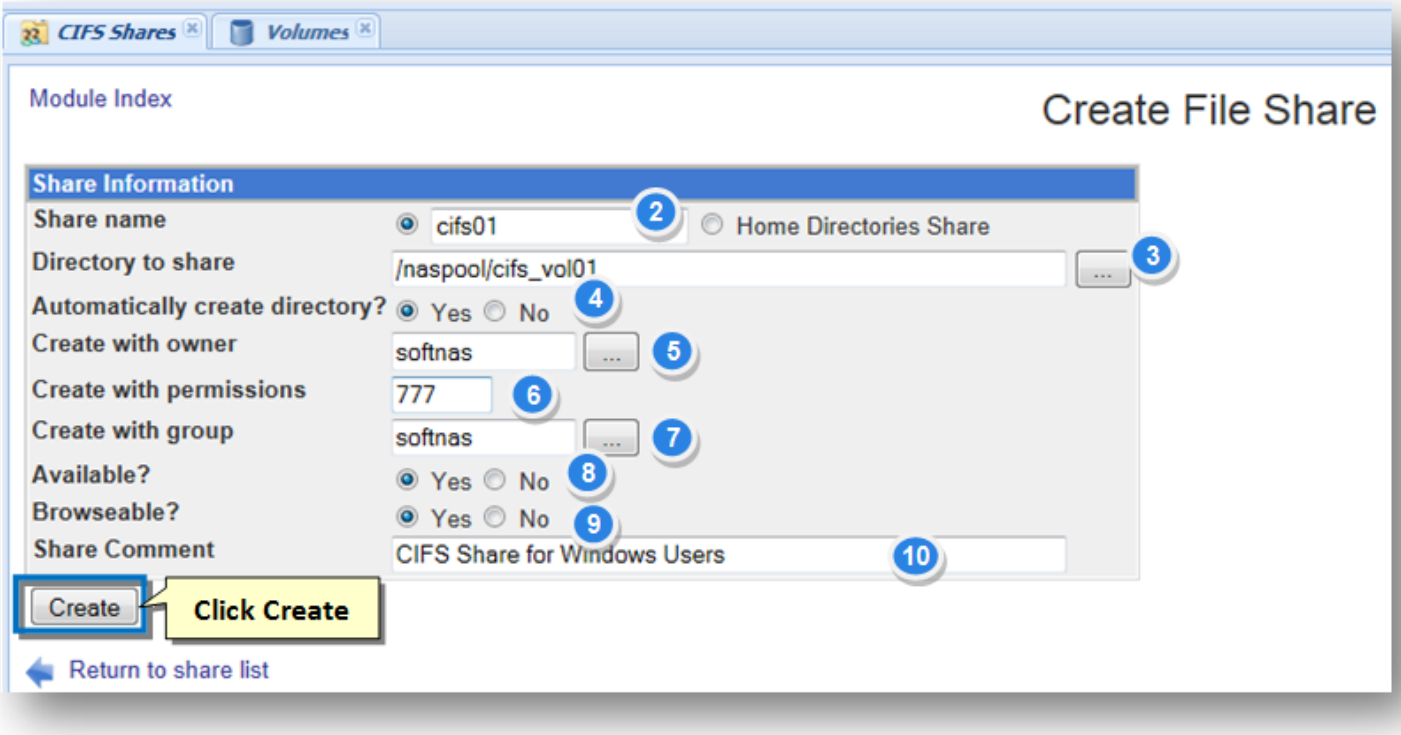
The selection of the shared files in the list will be inverted.

4 Creating a New File Share

Note: Before you start creating a new file share, it is better to configure the default windows network environm

1. On the **CIFS Shares** panel, click the **Create a New File Share** link.

The **Create File Share** section of the panel will be displayed.



2. Enter the name of the share that will appear as the network mount point in the **Share Name** text entry box.

3. The **Directory to share** is the path to the **Volume** that was created in the prior step. Click the **Browse** butt
Volume from the filesystem for sharing.

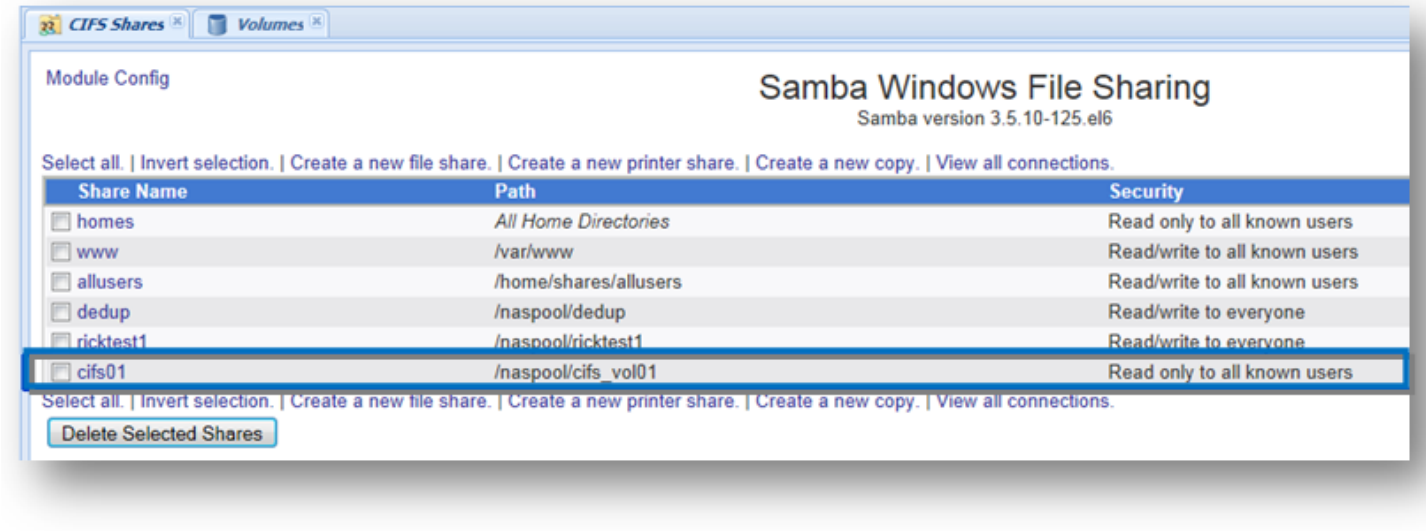
4. Set the **Automatically Create Directory** field option to be **Yes.**

5. The **Create with Owner** field determines which Linux user will be assigned to the shared folder.

6. Enter the permission mask in the **Create with Permissions** text entry box. Example, 777 is read/write/excu

7. The **Create with Group** field determines which Linux group will be assigned to the shared folder.
8. To make the share to be available on the network, check the **Yes** option in the **Available** field.
9. To make the share to be browseable on the network, check the **Yes** option in the **Browseable** field.
10. Enter the comment if any to display to users who browse the share, in the Share Comment text entry box.
11. Click the **Create** button.

The new file share will be created and published for access by windows servers and clients.

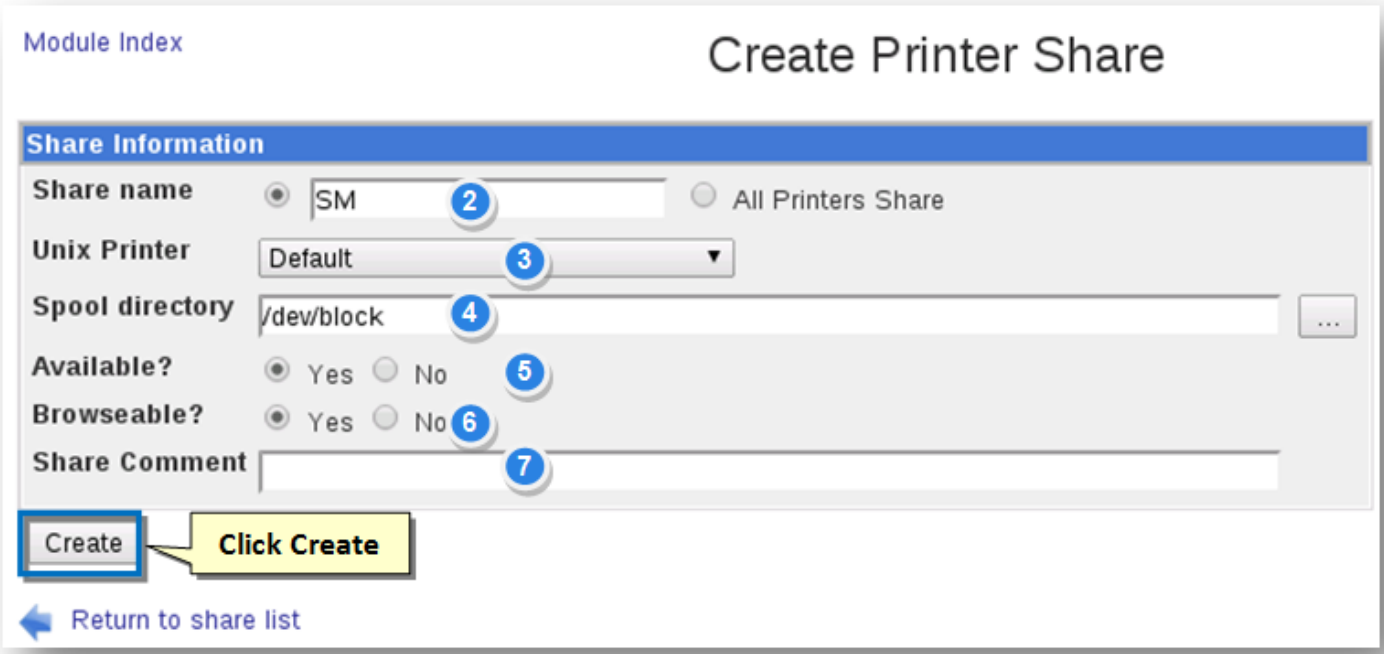


5 Creating a New Printer Share

Creating a new printer share is easy. Simply follow the steps given below.

1. Click the **Create a New Printer Share** button.

The **Create Printer Share** page will be displayed.



2. In the **Share name** field, make sure the first button is selected and enter a unique alphanumeric name for y the text box. This should be the same as the name of the Unix printer you select in the next step to avoid confu automatically created printer share with the same name already exists, this new one will override it.

3. From the **Unix printer** drop down list, select the printer to make available to SMB clients.

4. In the **Spool directory** field, enter the name of a directory in which temporary files for printing are stored.

5. To disable this printer so that it cannot be used, change the **Available?** field to **No.**

6. To hide this printer from the list that appears when the server is browsed, change the **Browseable?** field to directly accessible using a \\servername\printername path though.

7. In the **Share** comment field, enter a short description for this printer.

8. Click the **Create** button to add the share to the **Samba** configuration.

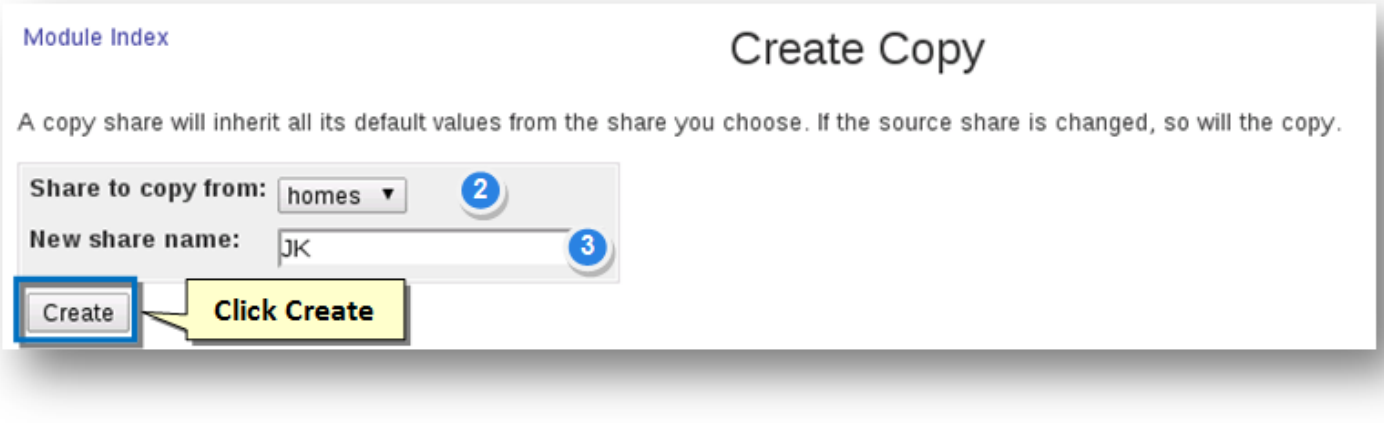
You can edit this share and configure security options.

6 Creating a New Copy

To create a new copy share

1. Click the **Create a New Copy** button.

The **Create Copy** page will be displayed.



2. Select the name of the share from the existing shares drop down list.
3. Enter the new name for the share in the text entry box.
4. Click the **Create** button.

The new copy share will be created.

7 Viewing All Connections

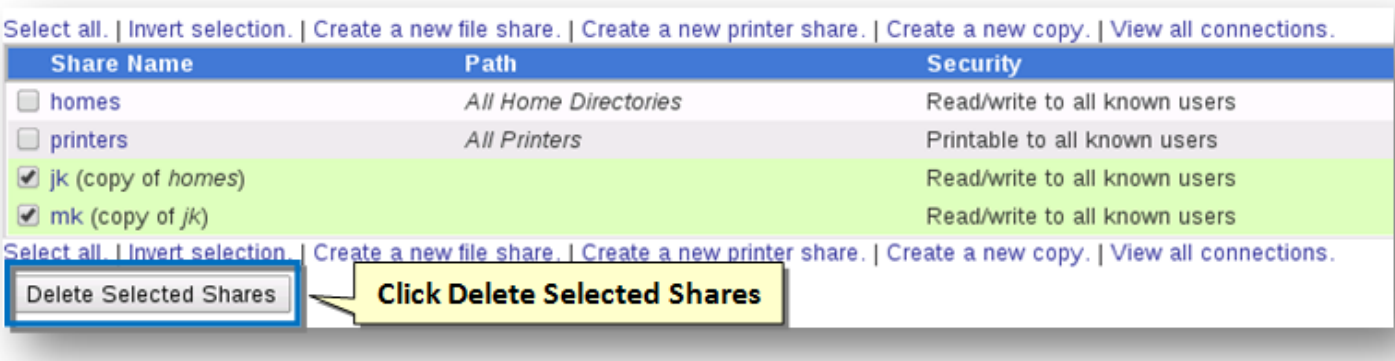
You can view all users and their connections through file sharing. To do so, simply click the **View All Connections** button.

All the users of the shared files will be displayed.

8 Deleting Selected Shares

You can delete a share that is no longer being used.

1. Select the shares that you wish to delete from the list of shares.
2. Click the **Delete Selected Shares** button.



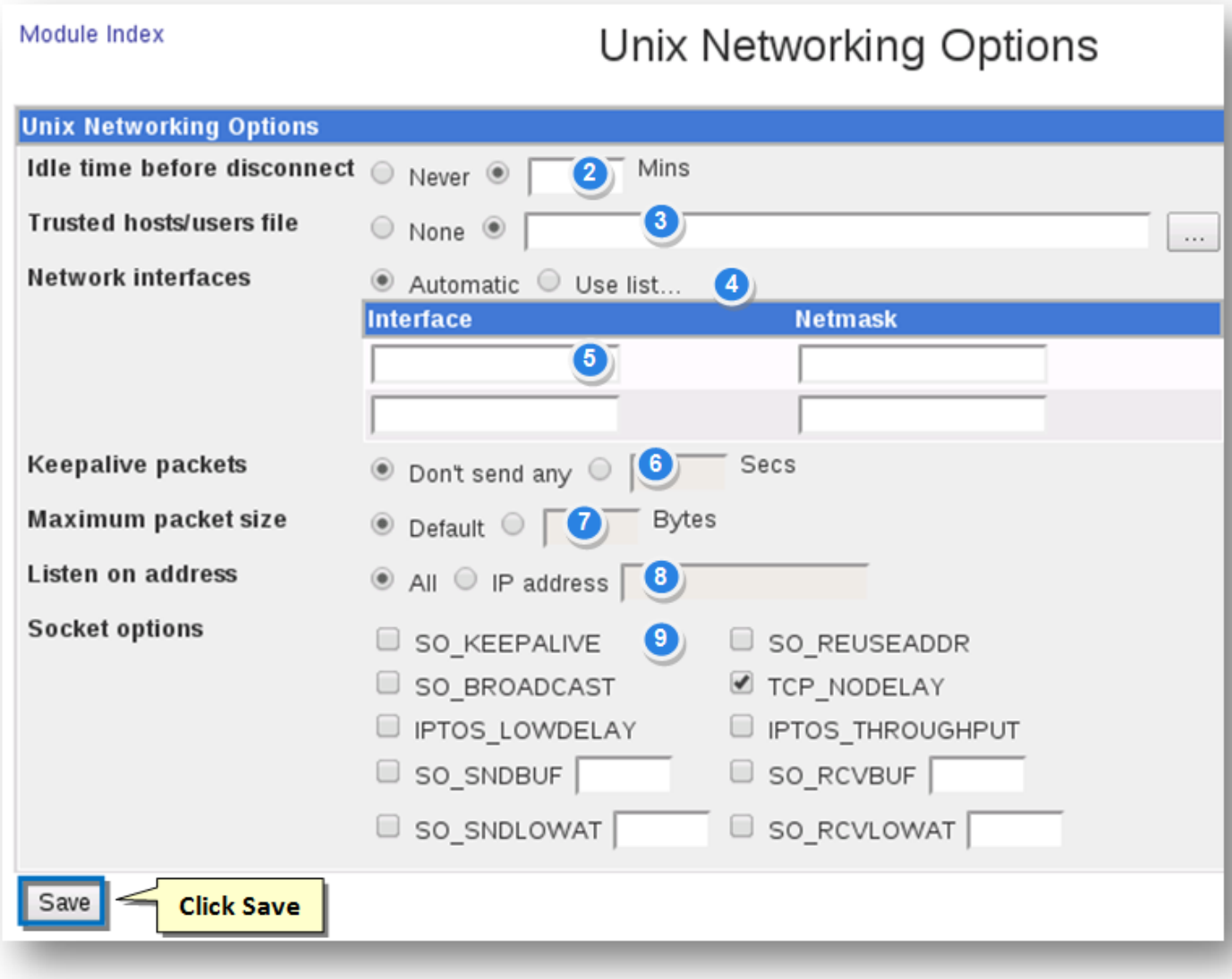
All the selected shares will be removed.

9 Configuring Unix Networking

You can configure Unix networking options.

1. To do so, click the **Unix Networking** icon in the **Global Configuration** section.

The **Unix Networking Options** page will be displayed.



2. Specify the **Idle time before disconnect** in the field. The default is **Never.**
3. Specify the **Trusted hosts/users file** in the field. The default is None.
4. Specify the **Network interfaces** with interface and netmask details.
5. Specify the **Keep alive packets** in the field.
6. Specify the **Maximum packet size** in the field.
7. Specify the **Listen on address** in the field.
8. Specify the **Socket options** details.
9. Click the **Save** button.

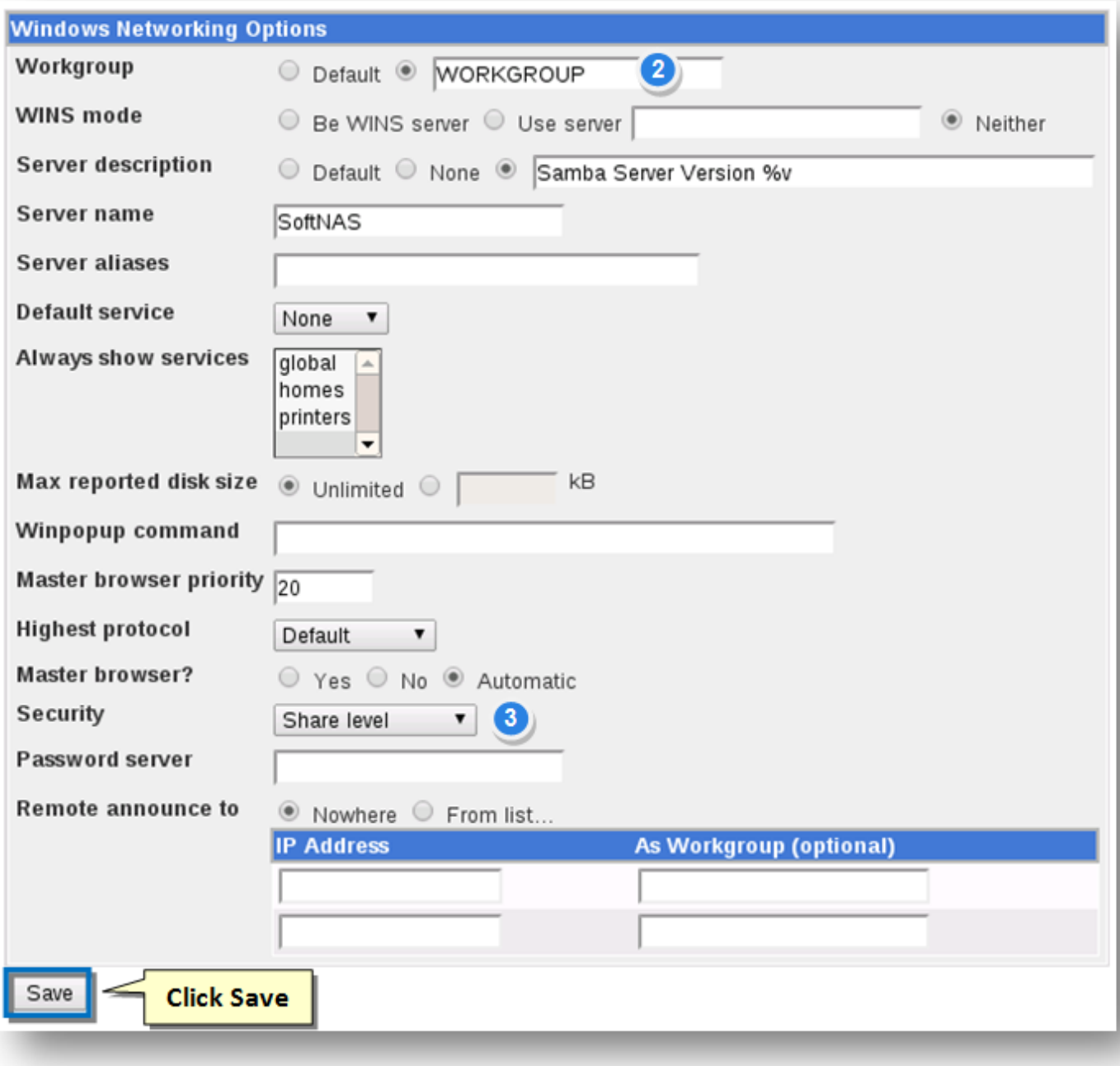
The changes made to Unix networking options will be updated.

10 Configuring Windows Networking

You can configure Windows networking options.

1. To do so, click the **Windows Networking** icon in the **Global Configuration** section.

The **Windows Networking Options** page will be displayed.



2. Set the name of the workgroup in the **Workgroup** field. This setting should be appropriate to your environm should match your Windows workgroup or domain environment.

3. Select the appropriate security option for your particular environment from the **Security** drop down list. The available options include **Default, Share Level, User Level, Password Server, Domain** and **Active Director**

Note: Configuring other settings in the **Windows Networking Options** dialog is optional.

4. Click the **Save** button.

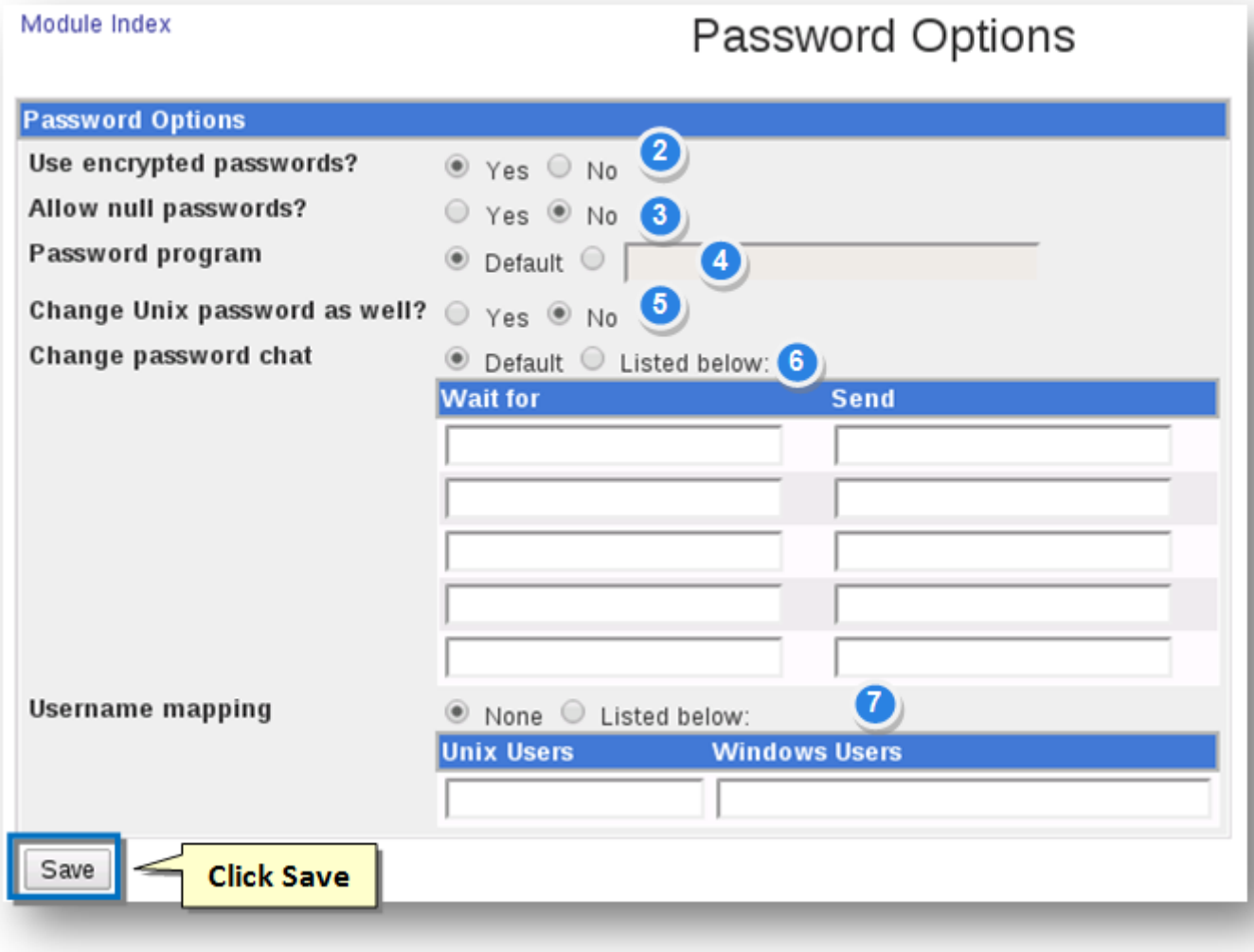
Now your environment is ready for CIFS sharing.

11 Configuring Authentication

You can configure authentication options.

1. To do so, click the **Authentication** icon in the **Global Configuration** section.

The **Password Options** page will be displayed.



2. The **Use encrypted passwords** field determines if Samba uses its own separate password file or the standard Unix user database. Because all recent versions of Windows use a password encryption format that incompatible with the Unix format, this field should generally be set to Yes.

3. To allow logins by users who have no password set, select **Yes** for the **Allow null passwords** field.

4. The **Password program** field sets the program that Samba will use to change a user's Unix password if synchronization is enabled. If Default is selected /bin/passwd will be used.

5. To change a user's Unix password when his SMB password is changed over the network, set the **Change Unix password as well** field to **Yes.**

6. Similarly specify password in the **Change Password Chat** field.

7. To define fake SMB accounts, select Listed below in the **Username mapping** field. Enter a valid Unix username, and an SMB login name of your choice.

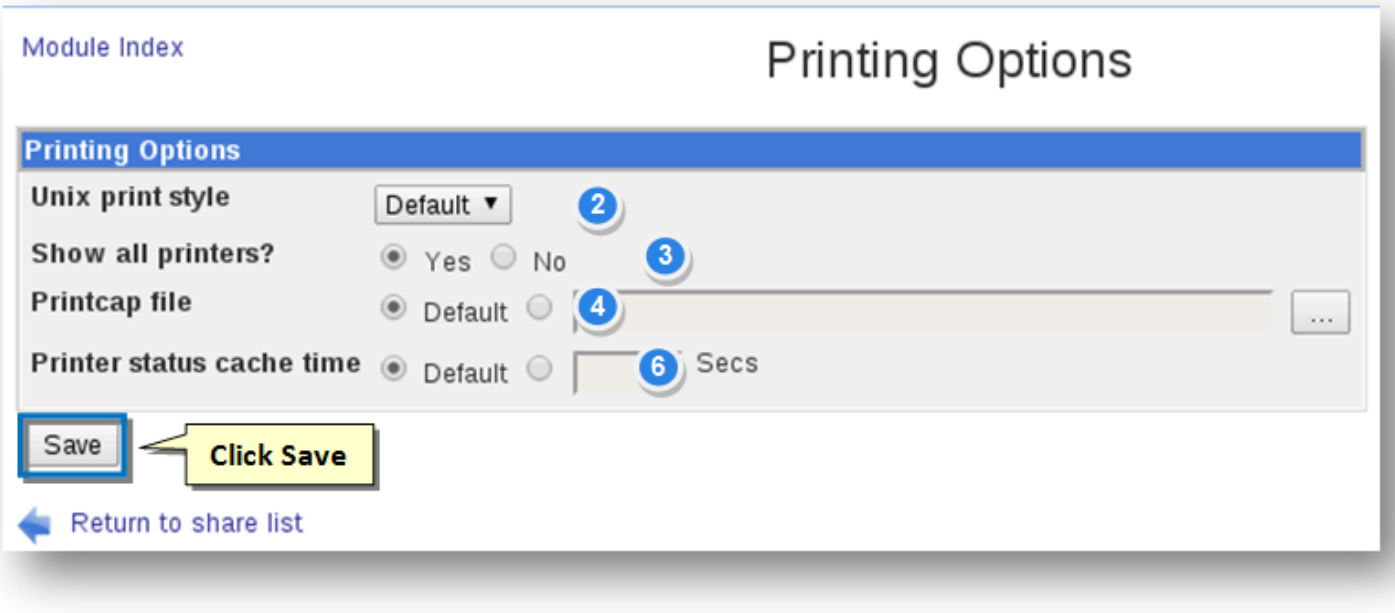
8. Click the **Save** button.

12 Configuring Windows to Unix Printing

You can configure **Windows to Unix Printing** options.

1. To do so, click the **Windows to Unix Printing** icon in the **Global Configuration** section.

The **Printing Options** page will be displayed.



2. Select the type of print system in use on your box from the **Unix print style** drop down list. The available op

- **BSD** -The traditional Unix print software, found on FreeBSD? , NetBSD? and older Linux distributions
- **SYSV** - The print system used on Solaris, UnixWare? and a few other versions of Unix.
- **HPUX** -The print system shipped with HP/UX.
- **AIX** -The print software that comes with AIX, IBM's version of Unix.
- **CUPS** -The superior Common Unix Print System, which is included with many new Linux distributions
- **LPRNG** - An improved version of the old BSD print system, used on all Linux systems that do not run

3. Normally, Samba will find all the printers on your system and make them visible to clients when the special exists. To disable this, change the **Show all printers?** field to **No.**

4. When the Printcap file field is set to **Default,** Samba will get the list of printers available on your system fron etc/printcap file.

5. Samba caches the output from whatever command is used to list waiting print jobs (such as lpq) in order to frequency with which it is run. By default this cache time is 10 seconds, but you can increase or decrease it us **status cache time** field.

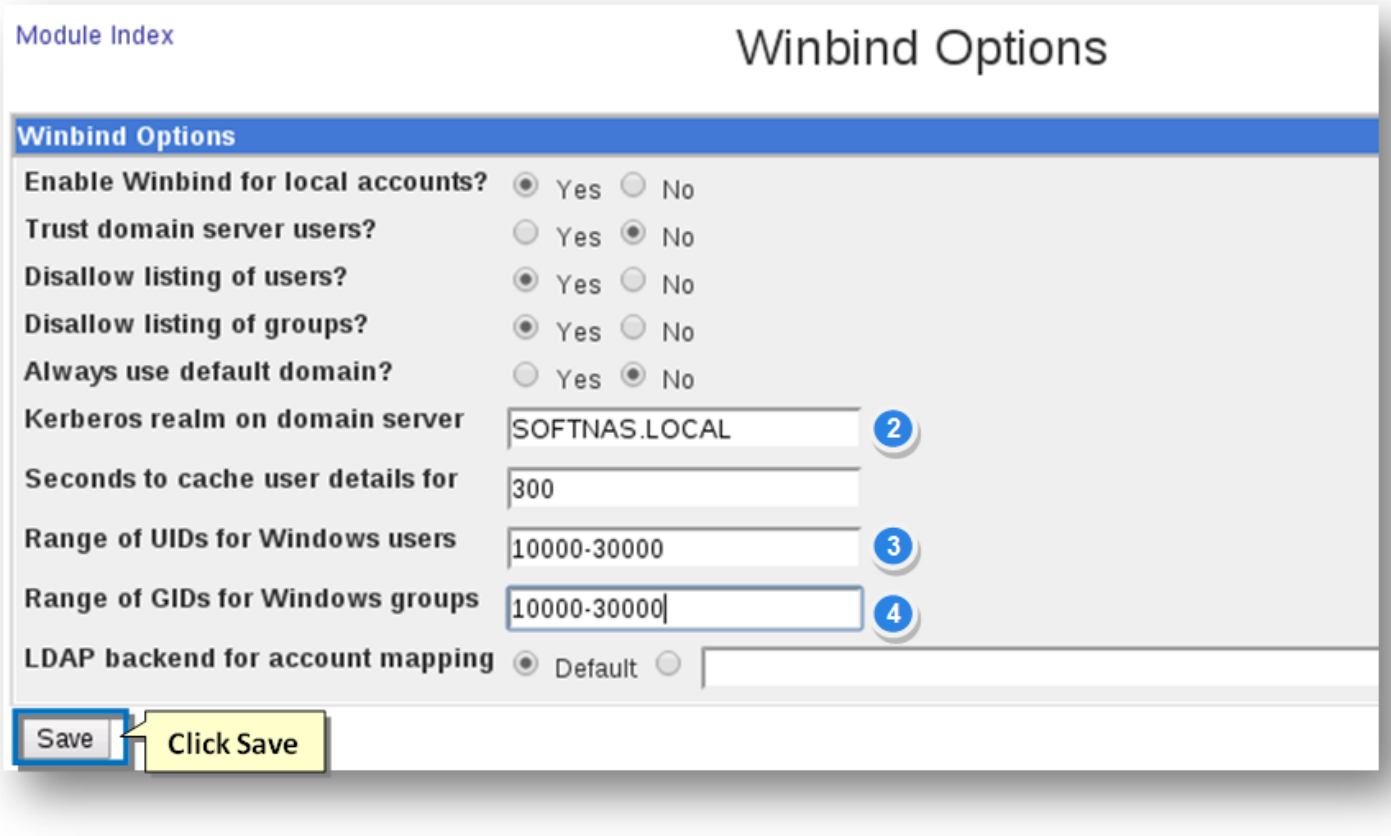
6. Click the **Save** button to activate your new printing settings.

13 Configuring Winbind Options

You can configure **Winbind** options.

1. To do so, click the **Winbind Options** icon in the **Global Configuration** section.

The **Winbind Options** page will be displayed.



2. Enter the full domain name of your Windows domain; e.g., **SOFTNAS.LOCAL, MYDOMAIN.COM,** etc. in th **Domain Server** text entry box.

3. Enter the range as **10000-30000** in the **Range of UIDs for Windows Users** text entry box. Using this nume Windows user ID's to Linux UID's occurs dynamically.

4. Similary enter the range as **10000-30000** in the **Range of UIDs for Windows Groups** text entry box for ma

5. Click the **Save** button.

14 Managing Samba Users

The **Managing Samba Users** section allows you to create, edit, delete and synchronize Samba users. It has the following options.

- **Samba Users** – It allows you to define Samba users.
- **Convert Users** – It allows you to synchronize the Unix and Samba user list.
- **User Synchronization** - It allows you to configure Webmin so that changes to the Unix user list will automatically applies to the Samba user list also.
- **Samba Groups** – It allows you to define Samba groups.
- **Group Synchronization** – It allows you to synchronize all Unix user groups and Samba user groups.
- **Bind to Domain** –It allows to bind Samba server to Windows domain typically managed by a different server.

15 Restarting Samba Servers

You can restart Samba servers. To do so, simply click the **Restart Samba Servers** button.

This will force the current configuration to be applied and also all the connections to the server will be disconnected.

16 Stopping Samba Servers

You can stop or shut down the working of Samba servers. To do so, simply click the **Stop Samba Servers** button.

This will force the samba servers running on your system to shut down and also all the connections to the server will be disconnected.

17 Restart Winbind Servers

You can restart Samba servers. To do so, simply click the **Restart Winbind Servers** button.

This will force the current configuration to be applied and also all the connections to the server will be disconnected.

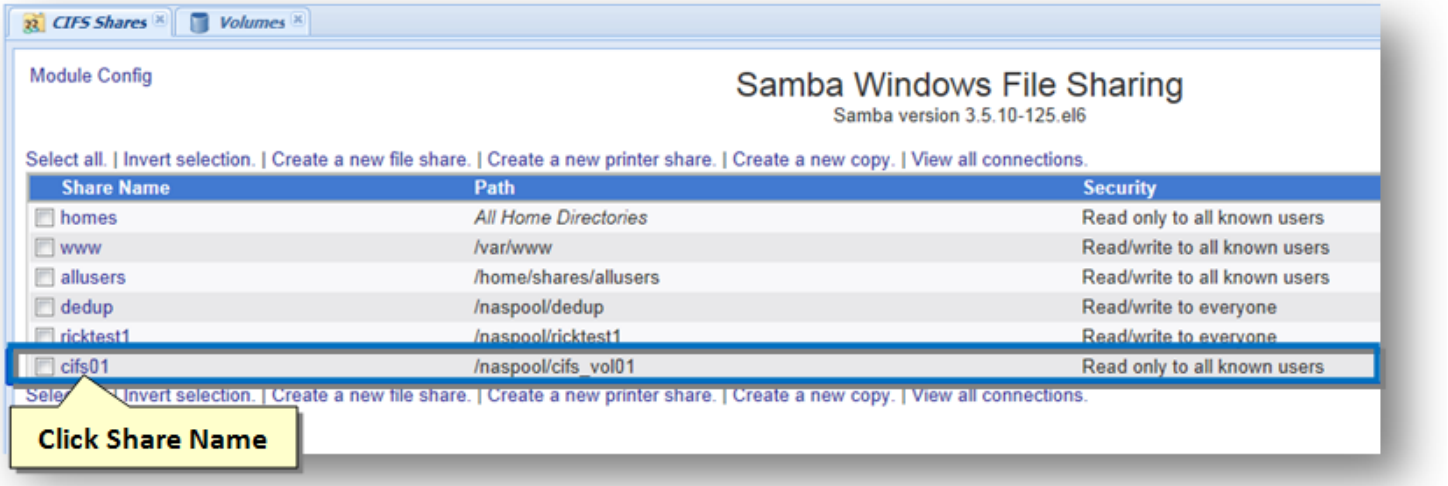
18 Stop Windbind Servers

You can stop or shut down the working of WinBind servers. To do so, simply click the **Stop Winbind Servers** button.

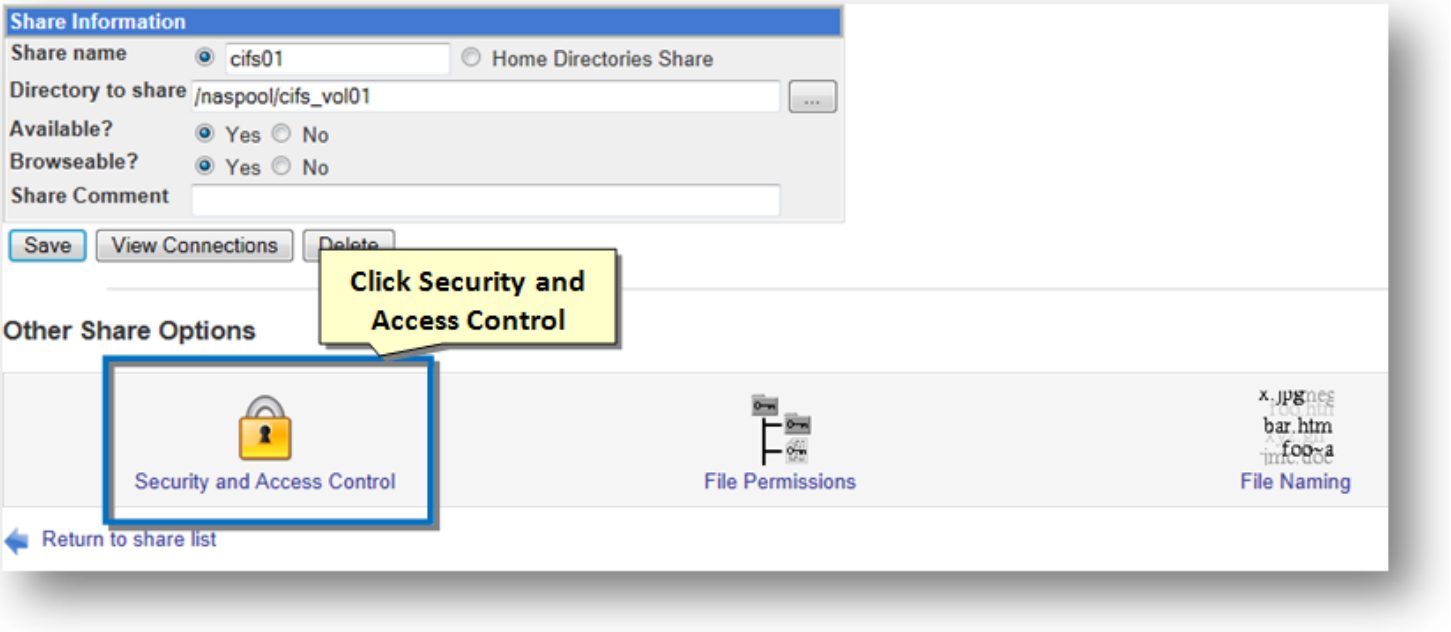
This will force the samba servers running on your system to shut down and also all the connections to the server will be disconnected.

Managing Security and Access Control

1. On the **CIFS Shares** panel, click the name of the CIFS share link.



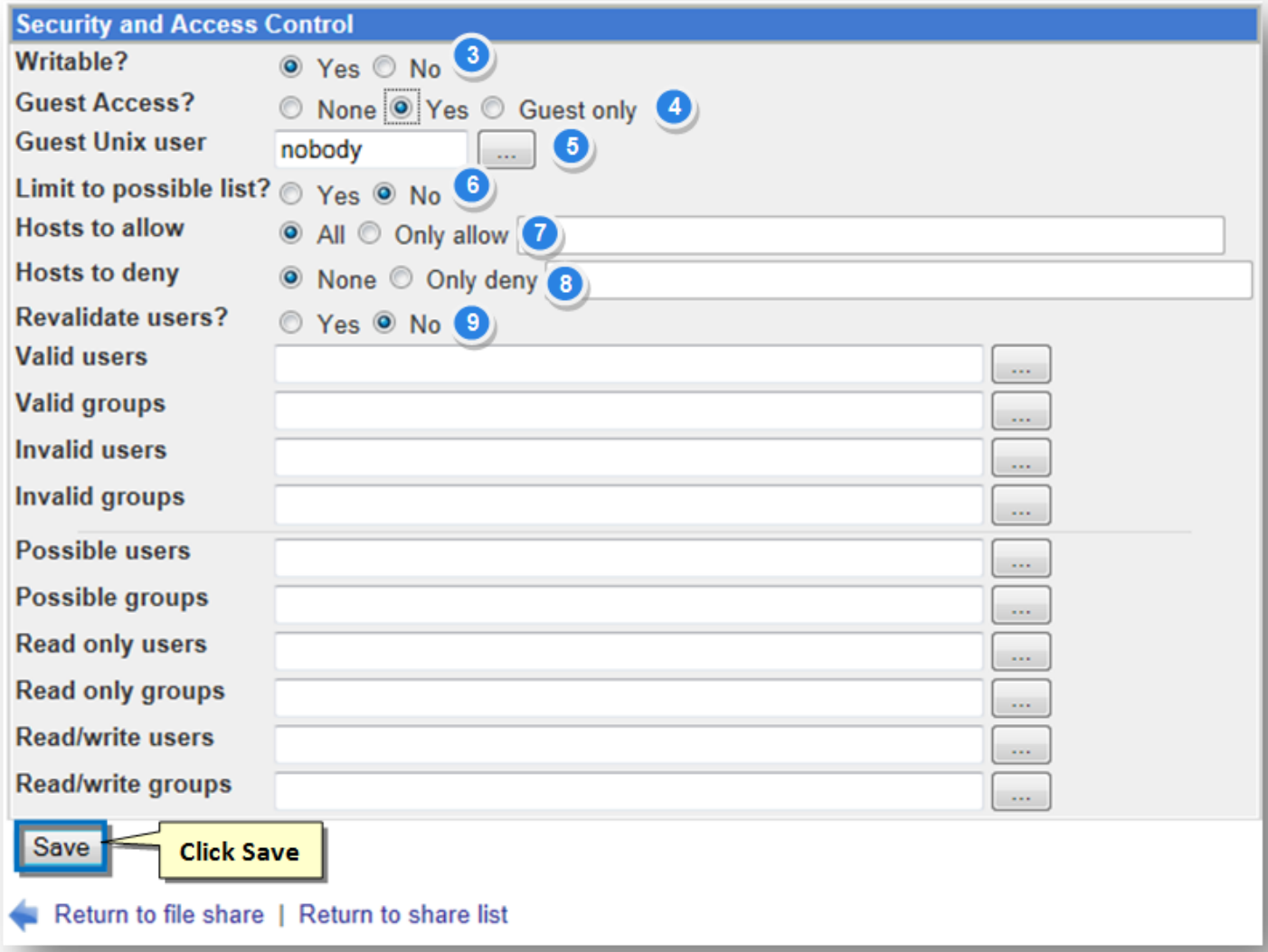
The **Edit File Share** dialog will be displayed.



2. To configure and manage security and access control, click the **Security and Access Control** icon.

The **Security and Access Control** dialog will be displayed. Choose the settings that best match your particular needs and use case for this share.

The settings shown below allow full read/write access by all users.



3. Set the **Writable** field to **Yes** so that writing is allowed in the files that are shared.
4. Set the **Guest Access** field to **Yes** in order to allow the guest users to access the files.
5. Set the **Guest Unix User** to **Nobody** so that other guest unix users are not allowed to access the file sharing.
7. Set the **Limit to Possible List** to **No** in order to allow unlimited sharing.
8. Set the **Hosts to Allow** to **Yes** in order to allow all hosts access file sharing.
9. Accordingly, set the **Hosts to Deny** to **None.**
10. Click the **Save** button.

The share security permission settings are now configured.

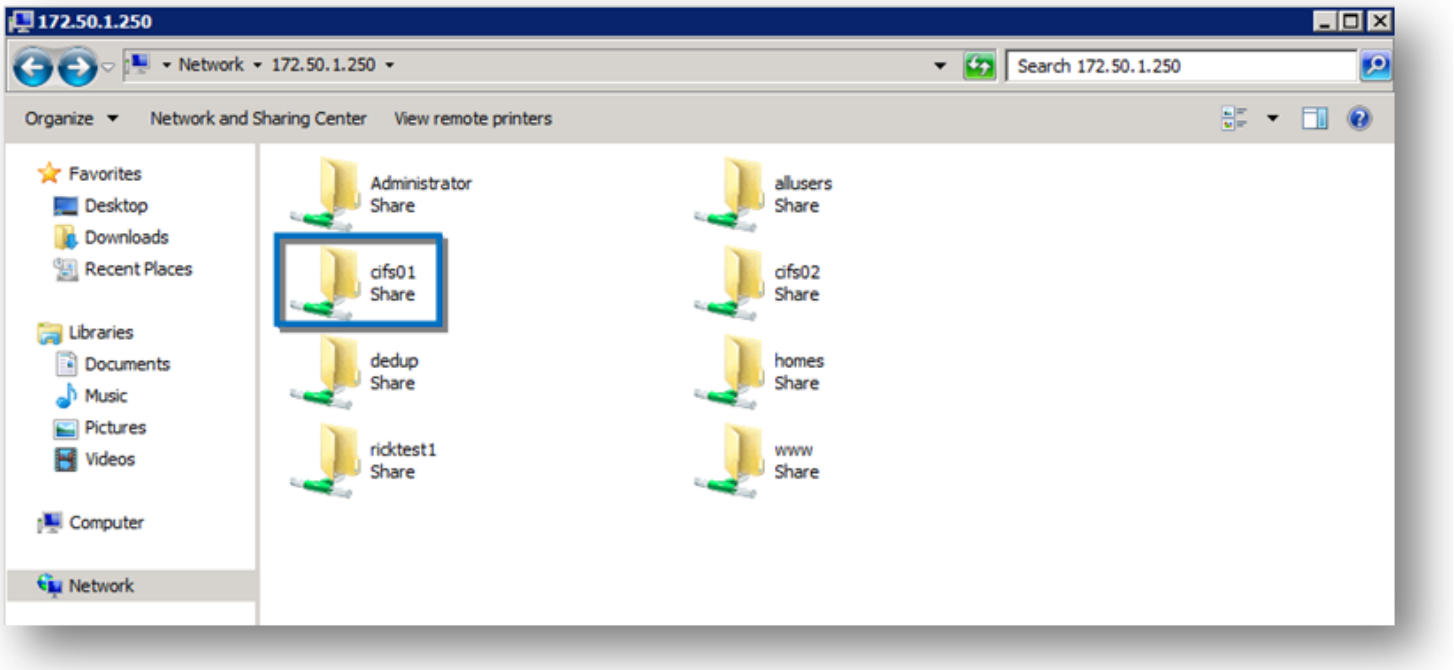
Verifying Access to CIFS Share

1. To verify access to the CIFS share, navigate to **Windows system >Windows Explorer.**

2. Enter the UNC path of the **SoftNAS** server (or the DNS hostname if you have assigned one to **SoftNAS**).

3. Click on the **Share** icon and verify access permissions are set correctly from the Windows perspective.

4. Create a folder or text file and then right-click on the file/folder to verify that the **Security** permissions are as expected.



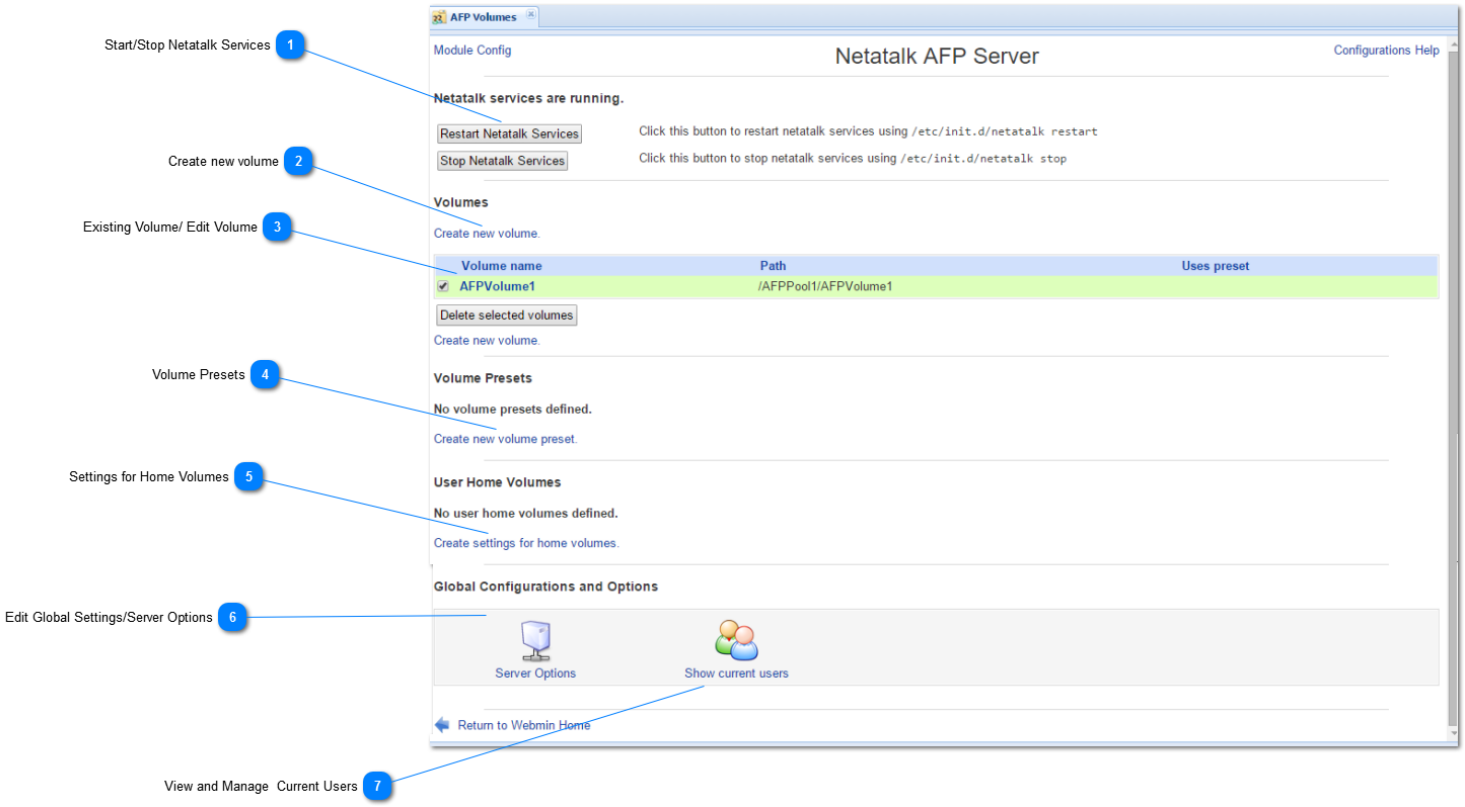
The CIFS share that was created is now available and ready for use.

Note: You can also use **File Share Defaults** to set defaults for all shares so that there is no need to configure settings for each share.

Configuring AFP Shares

SoftNAS allows you to create shares via the Apple Filing Protocol(AFP). This will allow Mac users to integrate our storage quickly and easily. Much like a CIFS share, AFP allows multiple clients to access and update the same file while preventing conflicts by providing file sharing and file locking.

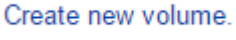
SoftNAS Cloud® uses Netatalk AFP server for secure, stable, and fast file sharing and print services. Using Netatalk's AFP 3.3 compliant file-server leads to significantly higher transmission speeds compared with Macs accessing a server via SaMBa/NFS, while providing clients with the best possible user experience (full support for Macintosh metadata, flawlessly supporting mixed environments of classic Mac OS and OS X clients).



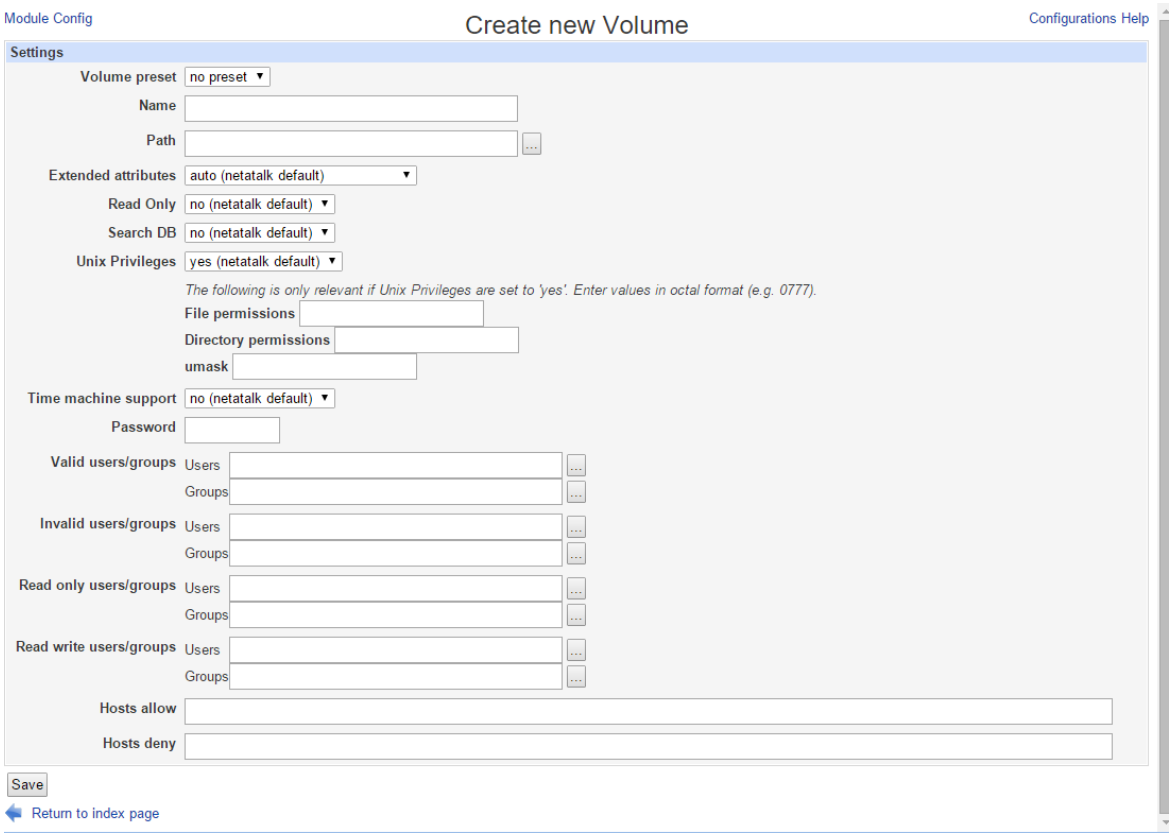
1 Start/Stop Netatalk Services

Much like rebooting a server, this can be a quick troubleshooting method to restore connectivity. It can also be used to stop Netatalk Services while you make changes, allowing it to start afresh with the new settings.

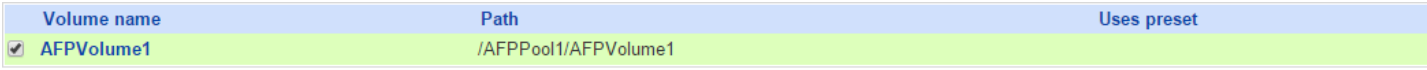
2 Create new volume



Create new volume allows you to open the Create New Volume Settings page. Here you can configure and create a new volume by filling in the fields with the appropriate data.



3 Existing Volume/ Edit Volume

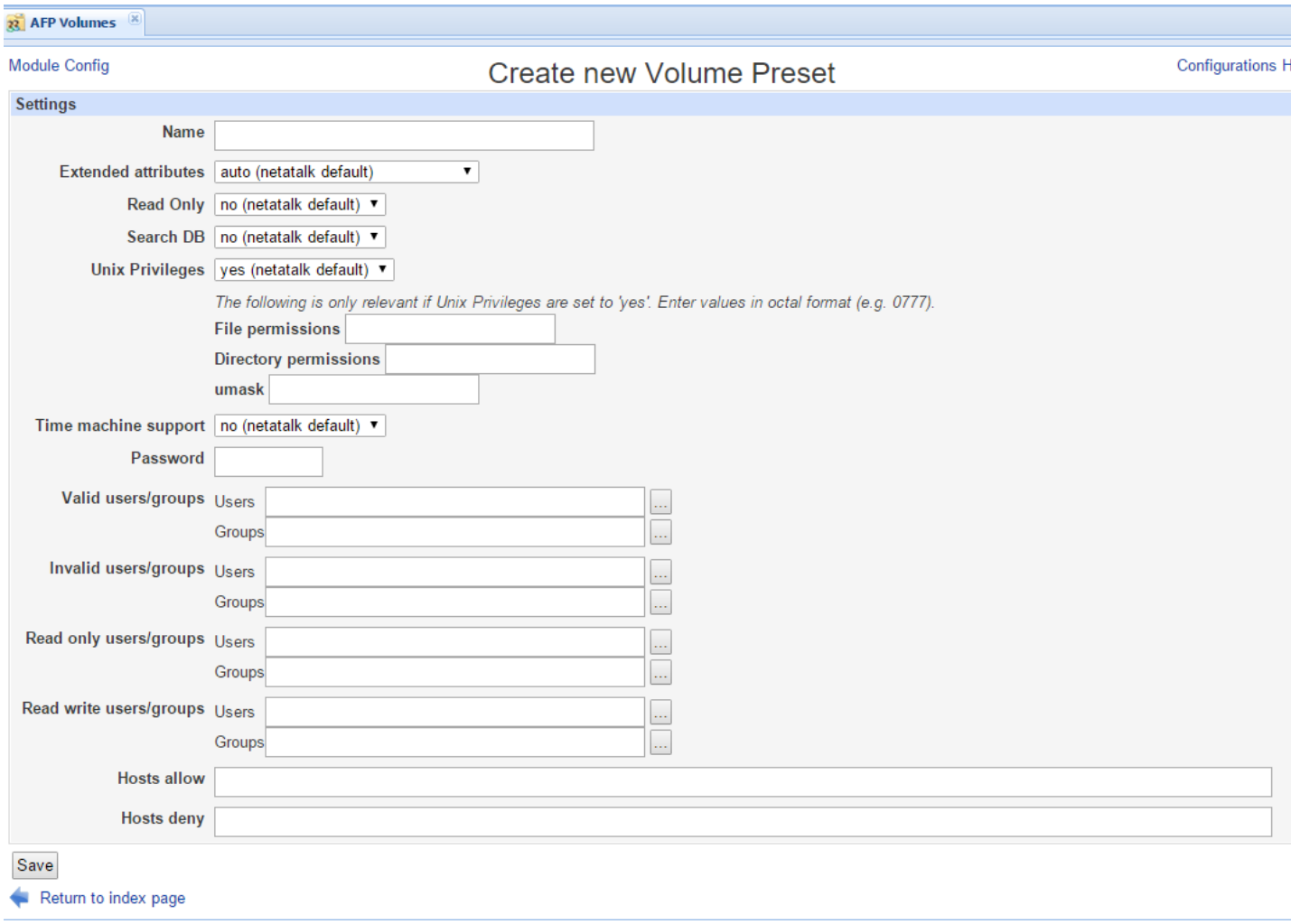


Clicking the name of an existing volume will allow you to edit its settings via the Edit Volume Settings page. Th page, save that the existing volume settings are automatically populated.

4 Volume Presets

Create new volume preset.

Clicking Create new volume preset allows you to create 'presets' or templates of AFP volume configurations th be autopopulated on any new volume. The following menu will appear.

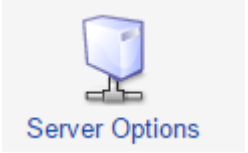


5 Settings for Home Volumes

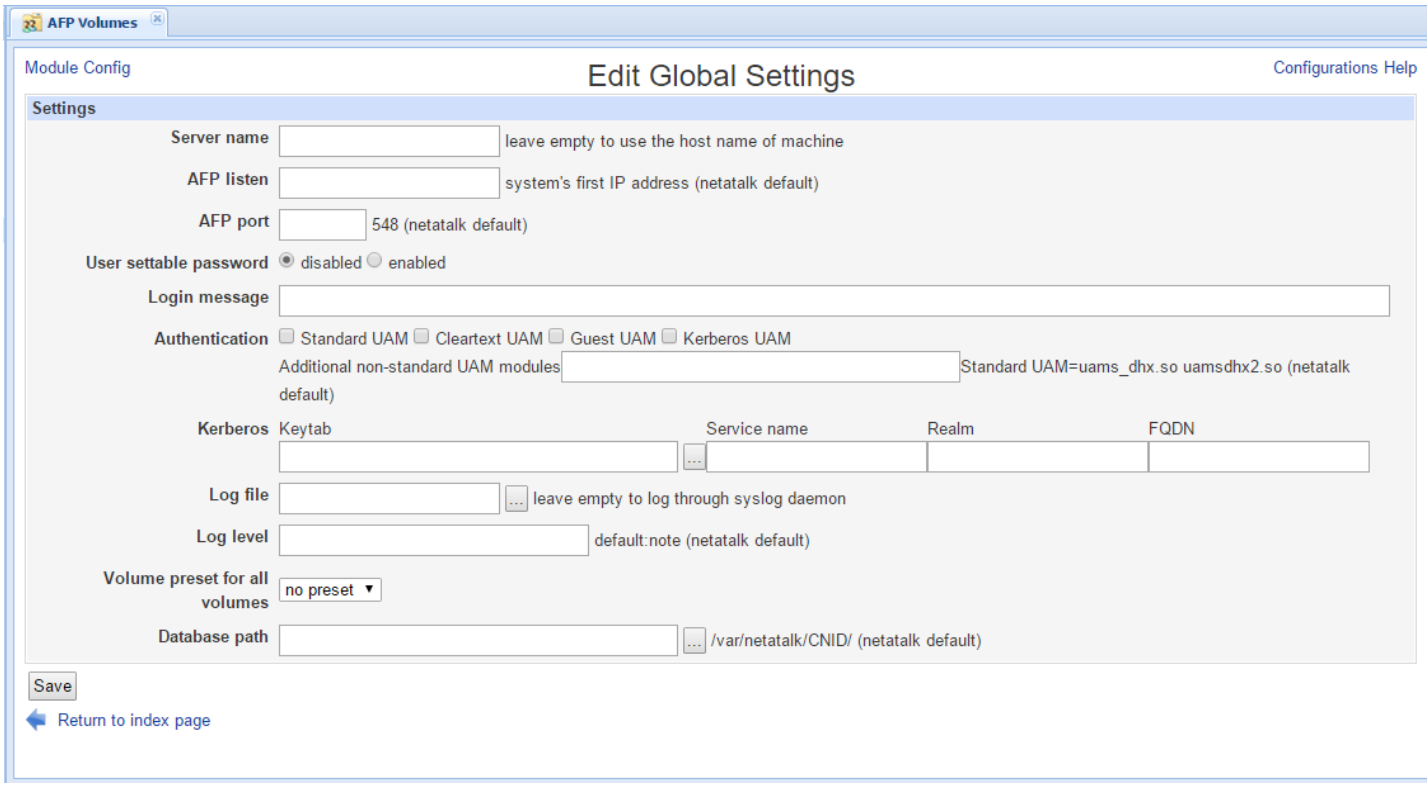
Create settings for home volumes.

Need more info

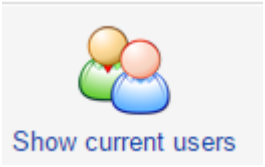
6 Edit Global Settings/Server Options



Here you can configure the global settings used on the host server to present your AFP share. This includes settings such as configuring alternate ports for AFP (default is 548), authentication methodology, volume prese for all volumes on this server, and more.



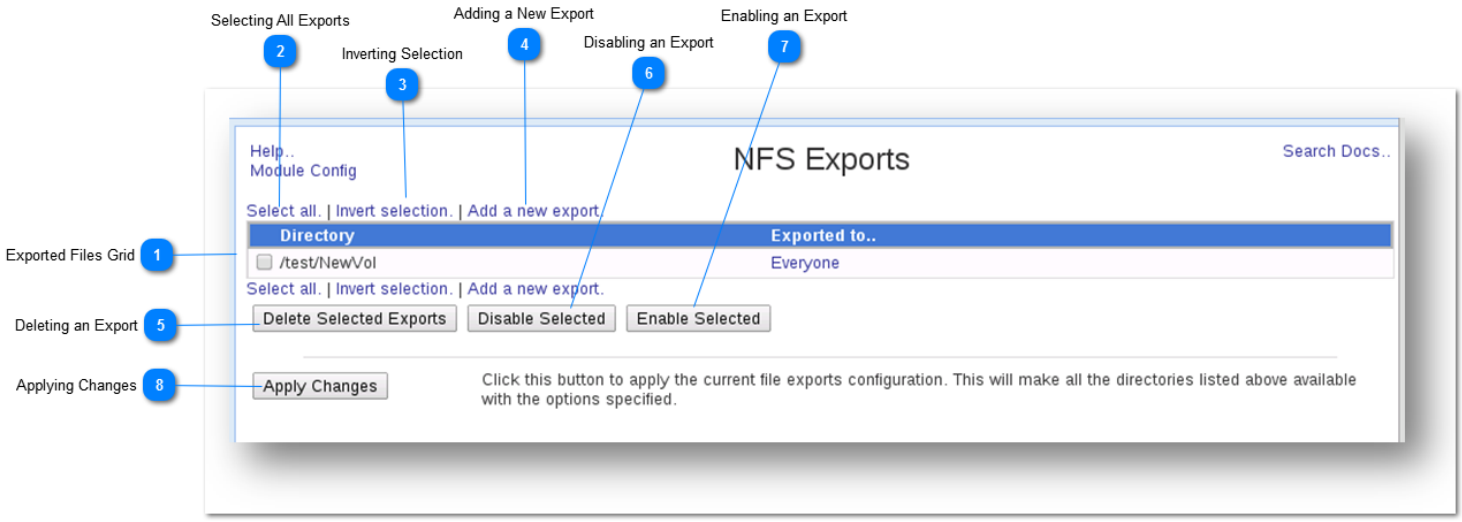
7 View and Manage Current Users



By clicking Show Current Users, you can view the users currently logged in and accessing your files, and how long they have been connected. This means you can improve performance by kicking "zombie" users, or those suspected of suspicious activity. This can also help in situations where users are disconnected, and cannot log back on, because their last session did not close.

Managing NFS Exports

You can configure the volume for sharing as NFS Share so that storage is available for use by the applications, servers and clients on the network.



1 Exported Files Grid

The **Exported Files Grid** displays the list of all exports in a tabular grid format. It has the following fields.

Field	Description
Directory	It is the name of the directory that is shared.
Exported To	It shows the users to whom the directory is exported.

2 Selecting All Exports

You can select all exports. To do so, simply click the **Select All** button.

All the exports in the list will be selected.

3 Inverting Selection

You can invert the selection of exports. To do so, simply click the **Invert Selection** button.

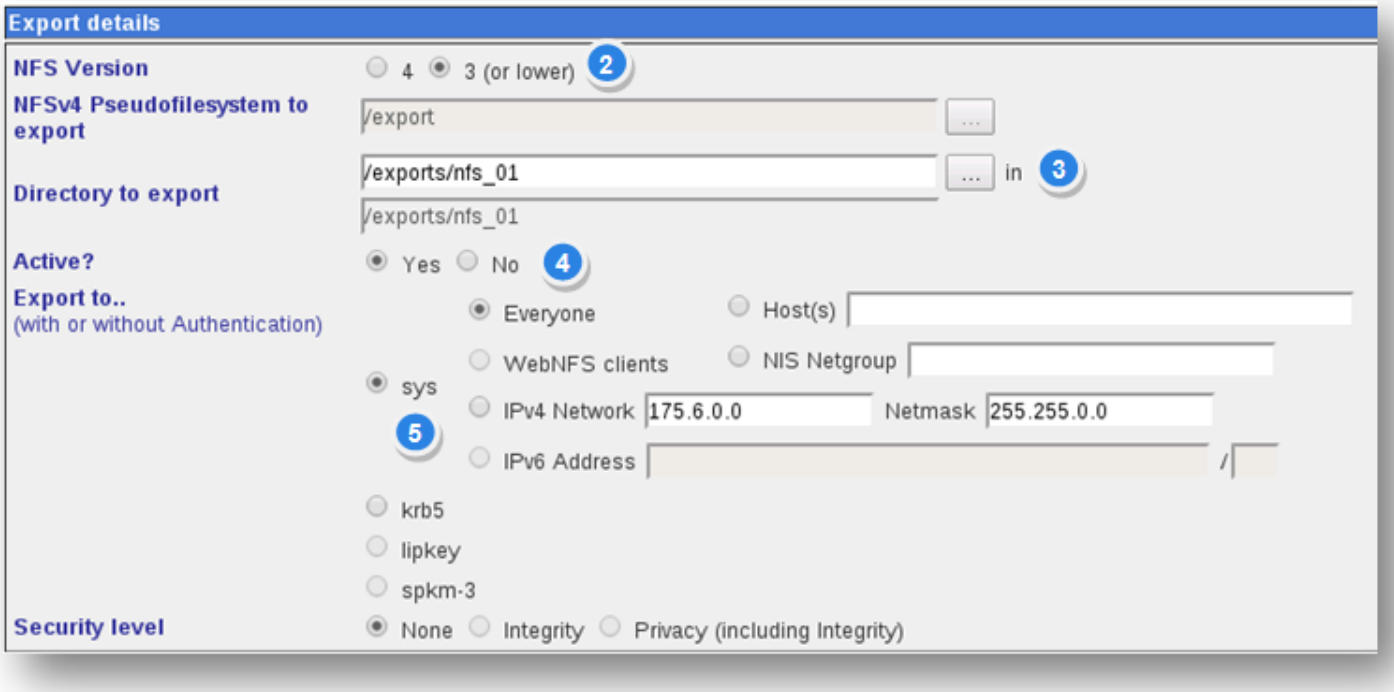
The selection of the exported directories in the list will be inverted.

4 Adding a New Export

Note: Before you can do NFS Share, you need to create a volume to share.

1. Click the **Add a New Export** link.

The **Create Export** section of the panel will be displayed.



2. In the **Export Details** section, specify the NFS version in the **NFS Version** field.

Note: The example has NFS version 3, but other settings such as NFS version 4 may also work better in some Choose the most appropriate settings for your particular environment, security and operational needs.

3. In the **Directory to Export** field, click the ... button to select the directory that you wish to export.

4. Set the **Active** field to **Yes.**

5. In the **Export to** field, specify the system **IPV4 Network** and **Netmask** addresses in the respective text ent

6. In the **Export Security** section, specify the **Read-only** field as **No.**

7. Set the **Disable Subtree Checking** field to **Yes.**

8. Set the **Immediately Sync All Writes** filed to **No.**

Note: For best performance throughput, choose **No** for **Immediately Sync All Writes** field. This option allows the write and return to the caller immediately (up to 10 times better throughput has been observed by not imme writes, so **No** setting makes a big difference in performance sensitive applications).

9. Set the Clients Must be On Secure Port to No.

10. Set the Hide the Filesystem field to Yes.

11. Set the **Trust Remote Users** field to **Nobody.**

Note: If you are planning to mount this NFS share from **VMware,** you must select **Nobody** as the **Trust Reme** VMware hosts do not authenticate by default, so it's also best to restrict the IP address range appropriately.

12. Specify the untrusted users in the **Treat Untrusted Users** as **Default** or **softnas.**

13. Specify the untrusted groups in the **Treat Untrusted Groups** as **Default** or **softnas.**

14. Set the **Make Symbolic Links Relative** field to **No.**

15. Set the **Deny Access to Directory** field to **No.**

16. Set the **Don't Trust UIDs** field to **None.**

17. Set the **Don't Trust GIDs** field to **None.**

18. Click the **Create** button.

The **NFS Exports** panel will be displayed.

19. Click the **Apply Changes** button.

The NFS export settings will be activated.

5 Deleting an Export

You can delete an unused export.

1. To do so, select the export that you wish to delete from the lsit.

2. Click the **Delete Selected Exports** button in the toolbar.

The message that you are not exporting directory will be displayed.

3. Click the **Apply Changes** button.

The selected export will be removed from the list.

6 Disabling an Export

You can disable an export.

1. To do so, select the export that you wish to disable from the lsit.
2. Click the **Disable Selected** button in the toolbar.

The selected export will be disabled and an inactive status will be shown.

7 Enabling an Export

You can enable an export.

1. To do so, select the export that you wish to enable..
2. Click the **Enable Selected** button in the toolbar.

The selected export will be enabled.

8 Applying Changes

After you make changes to the NFS exports, you can click the **Apply Changes** button to apply the changes made to the exports.

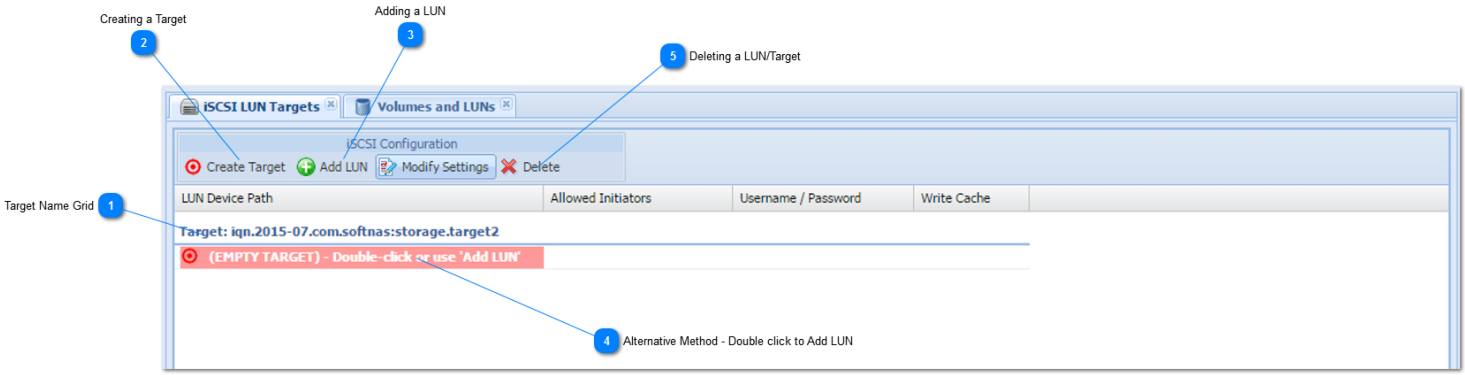
Configuring iSCSI LUN Targets

Sharing block devices via **iSCSI** is a common way to make network-attached storage available. An **iSCSI LUN** is a logical unit of storage. In **SoftNAS,** the basic storage **LUN** is a volume that is accessed as a **blockdevice.** The blockdevice volumes have a mount point in the **Linux /dev/zvol** filesystem because they are disk block devices.

For example, a storage pool **naspool1** with volume name **lun01** would be named **/dev/zvol/naspool1/lun01** as its mount point. These device references are links to Linux block devices used to access the volume's raw data blocks via **iSCSI.**

iSCSI targets are used by **iSCSI initiators** to establish a network connection. The target serves up the **LUNs,** which are collections of disk blocks accessed via the **iSCSI** protocol over the network. A target can offer one or more **LUNs** to the **iSCSI** clients, who initiate a connection with the **iSCSI** server.

For example, **VMware** or **Windows** connects to the **iSCSI** server and retrieves a list of available targets. Then, for each target, the list of its published **LUNs** are available for use.

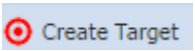


1 Target Name Grid

The **Target LUN Grid** displays the list of targets and LUNs in a tabular grid format. It has the following fields.

Field	Description
Target Name	It shows the complete path and name of the target.
Delete Target	Link to delete target.

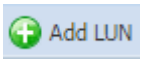
2 Creating a Target



Note: You can publish any number of block device volumes via a single iSCSI target. A default iSCSI target is ready for use. However, if you need another, use the **Create A Target** link to add new targets as needed.

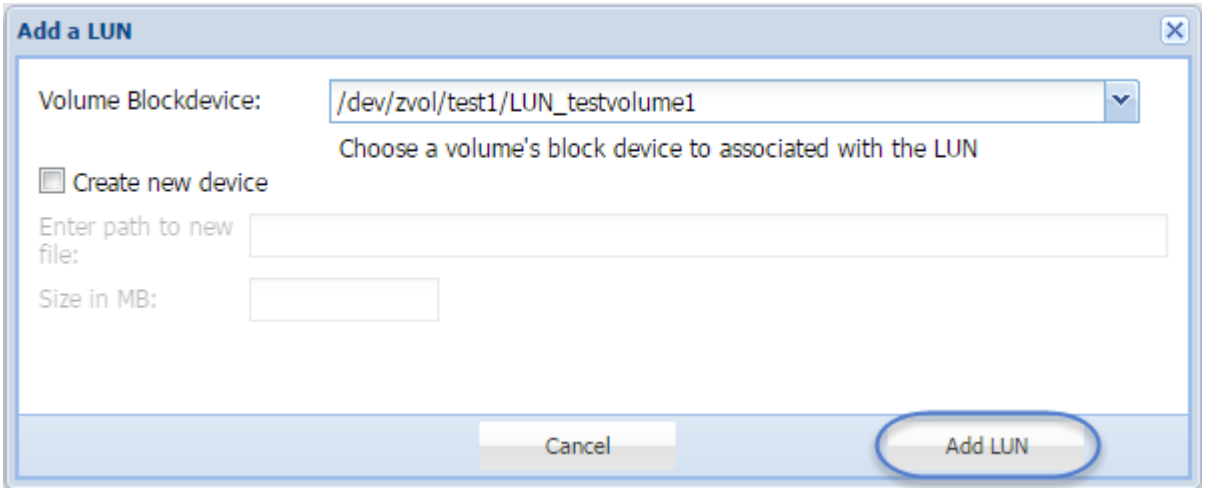
To do so, simply click the **Create a Target** option in the toolbar. The additional target will be created automatically, without additional steps.

3 Adding a LUN

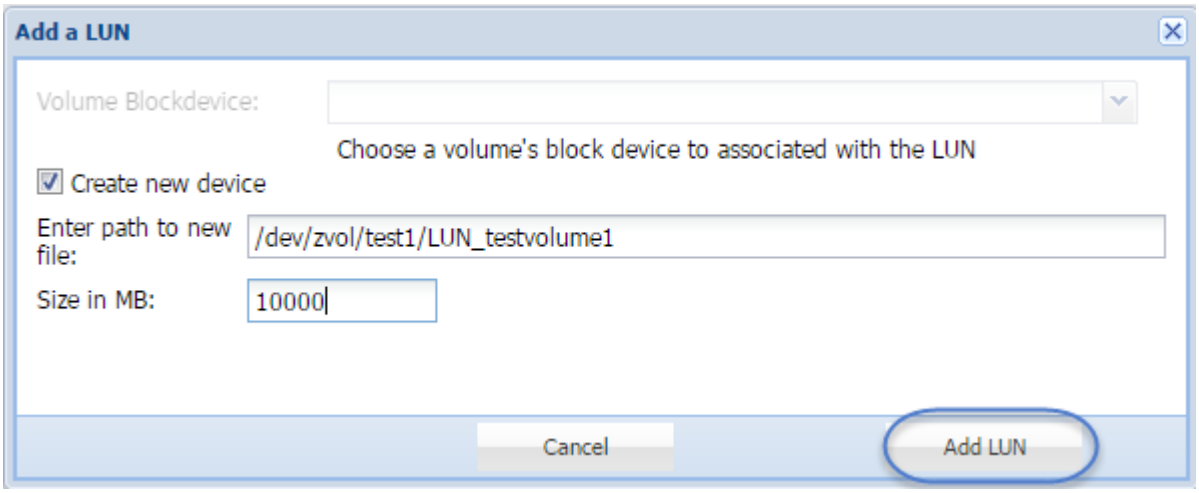


You can create one or more volumes assigned as LUNs (iSCSI logical units) for each target. To do this, select the target, and click Add LUN, or double-click the desired target.

Either select the volume's block device from the dropdown (which will show available volumes)...



...or check the box for Create a New Device, and enter the path, and the desired size to associate with the LUN.



Click **Add LUN** to link the block device to the iSCSI Target as a LUN.

You may need to refresh the screen to see the changes.

4 Alternative Method - Double click to Add LUN

Instead of selecting the target and clicking Add LUN, you can simply double-click here, as it states. Follow the steps in #3 to finish adding your LUN

5 Deleting a LUN/Target

You can now delete LUNs from a target, without deleting the target. An empty target can be deleted separately.

To delete a LUN, select it from the list.

1. Click the **Delete** link at the end of the Target Name Grid.
2. The **Delete Confirm** message box asking you to confirm the deletion of the LUN will be displayed.

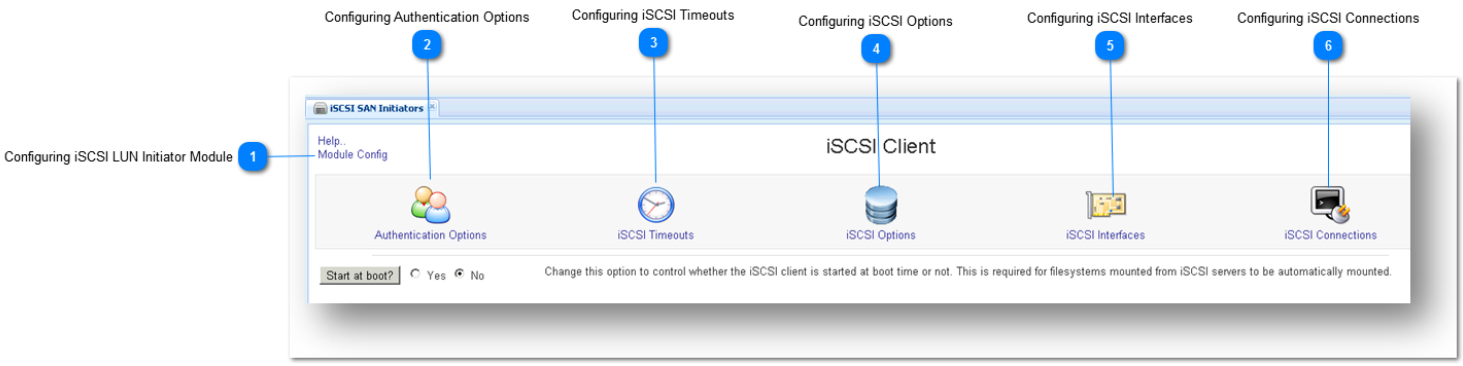
3. Click the **Yes** button.

The selected LUN will be removed.

To delete a target, the same process is followed.

Configuring iSCSI SAN Initiators

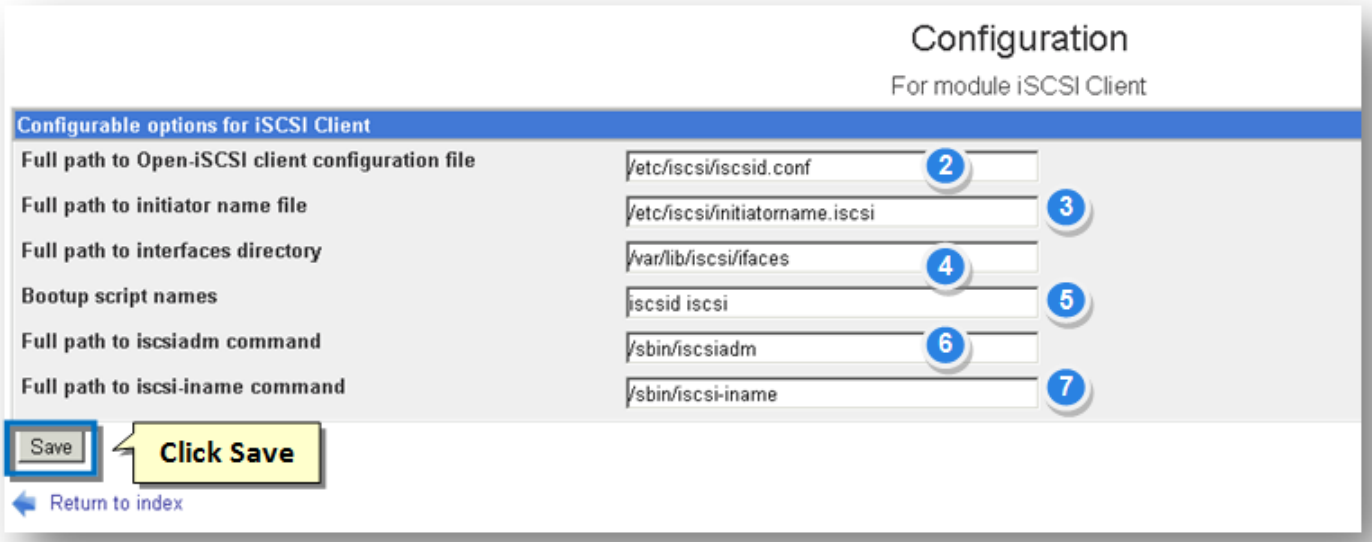
The **iSCSI SAN Initiators** module helps to configure various initiator components such as **Authentication Options, iSCSI Timeouts, iSCSI Options, iSCSI Interfaces** and **iSCSI Connections.**



1 Configuring iSCSI LUN Initiator Module

1. To configure the iSCSI LUN Initiator module, click the **Module Config** link at the top right corner of the scre

   The **Configuration for Module iSCSI Client** page will be displayed.



2. Enter the complete directory path for the iSCSI client configuration file in the text entry box.
3. Enter the complete directory path for the initiator name file in the text entry box.
4. Enter the complete directory path for the interfaces directory in the text entry box.
5. Enter the script names of bootup in the Bootup Script Names text entry box.
6. Enter the complete directory path to the iscsiadm command in the text entry box.
7. Enter the complete directory path to the iscsi-iname command in the text entry box.

8. Click the **Save** button.

The iSCSI Client module will be configured.

2 Configuring Authentication Options

1. To configure authentication options for iSCSI LUN Initiators, click the **Authentication Options** button.

The **Authentication Options** page will be displayed.

2. Enter the initiator name for the local system in the Local system initiator name text entry box or you can als generate a new random name automatically.

3. Select the type of the authentication used in the Authentication method drop down list. The available option Authenticate and CHAP.

4. Enter the server login credentials of username and password in the Login to server fields.

5. Enter the client login credentials of username and password in the Login to client fields.

6. Select the type of the discovery authentication used in the Discovery Authentication method drop down list. options include Don't Authenticate and CHAP.

7. Enter the discovery server login credentials of username and password in the Discovery Login to server fiel

8. Enter the discovery client login credentials of username and password in the Discovery Login to client fields

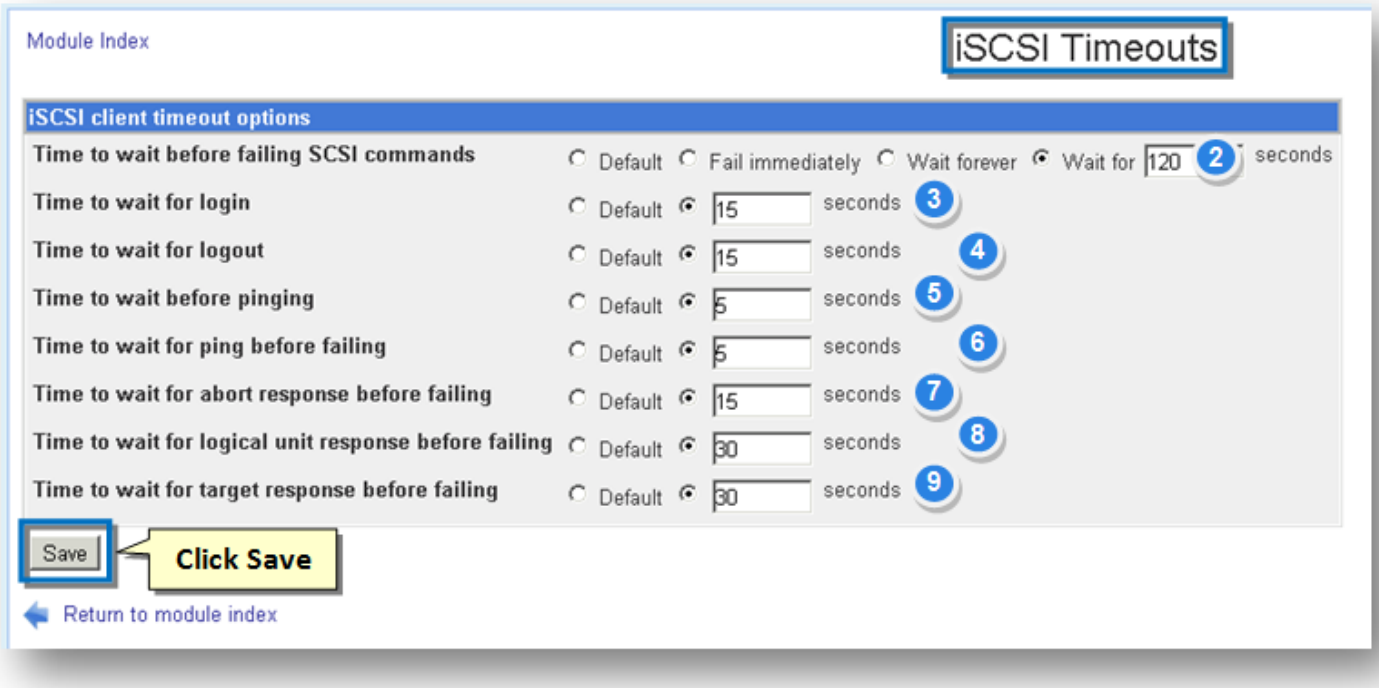
9. Click the **Save** button.

The iSCSI authentication options will be configured.

3 Configuring iSCSI Timeouts

1. To configure iSCSI timeout sessions, click the **iSCSI Timeouts** button.

The **iSCSI Timeouts** page will be displayed.



2. Specify the time required to wait in seconds for failing the SCSI commands. The available options include D immediately, Wait forever and Wait for seconds.
You can manually enter the value also.

3. Select the default option or enter the manual time required to wait for login.

4. Select the default option or enter the manual time to wait for logout.

5. Select the default option or enter the manual time to wait before pinging.

6. Select the default option or enter the manual time to wait for ping before failing.

7. Select the default option or enter the manual time to wait for abort response before failing.

8. Select the default option or enter the manual time to wait for logical unit response before failing.

9. Select the default option or enter the manual time to wait for target response before failing.

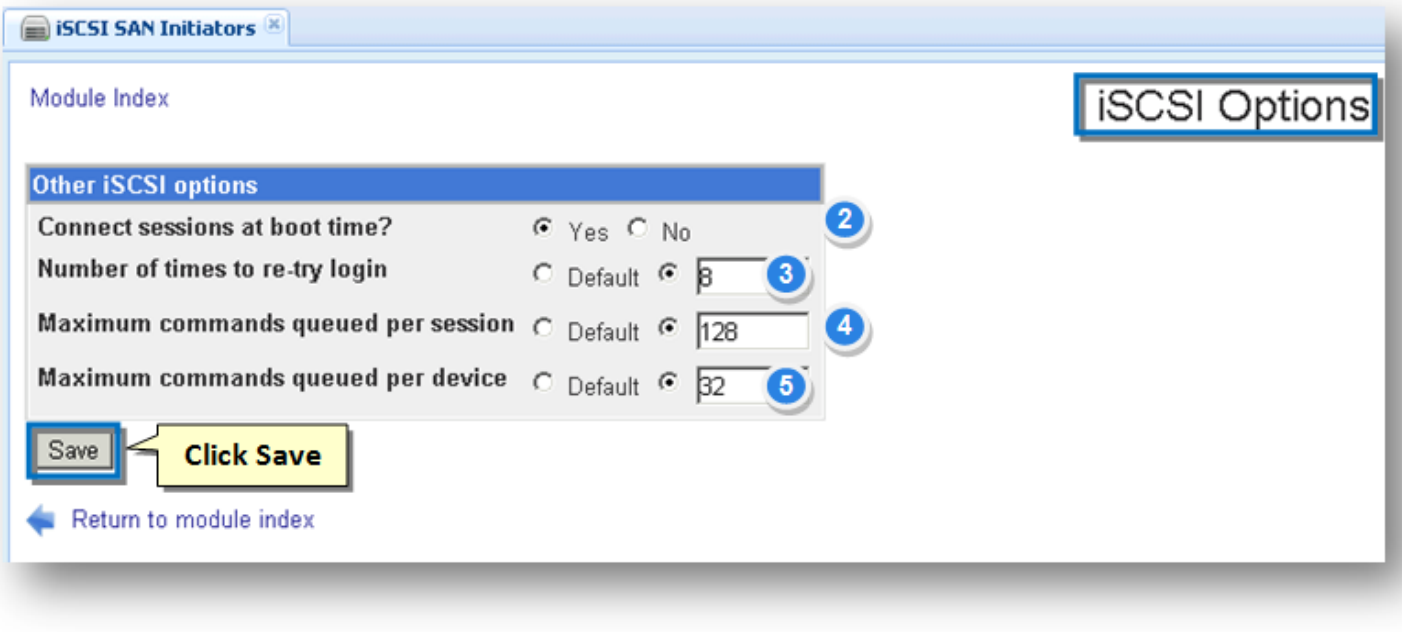
10. Click the **Save** button.

The iSCSI Timeouts page will be configured.

4 Configuring iSCSI Options

1. To configure iSCSI Options, click the **iSCSI Options** button.

The iSCSI Options page will be displayed.



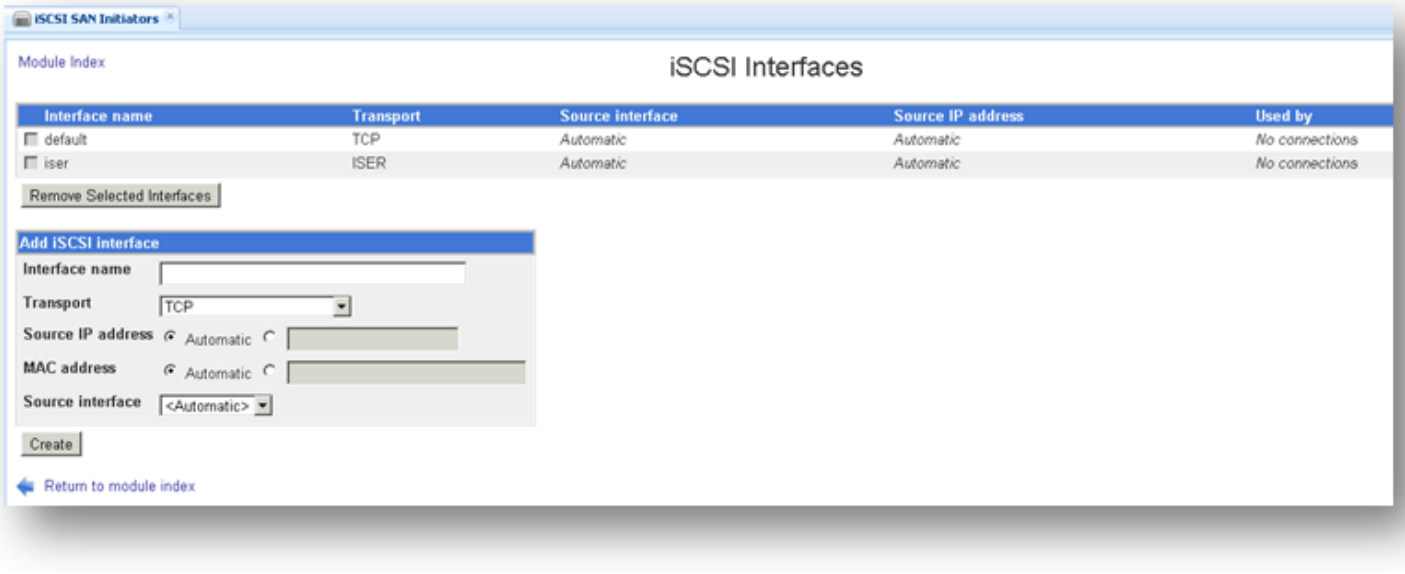
2. Specify whether the sessions should connect at boot time or not by selecting **Yes** or **No** option.
3. Select the default option or enter manually the number of times allowed to try the login attempts.
4. Select the default option or enter manually the maximum commands queued per session.
5. Select the default option or enter manually the maximum commands queued per device.
6. Click the **Save** button.

The iSCSI Options will be configured.

5 Configuring iSCSI Interfaces

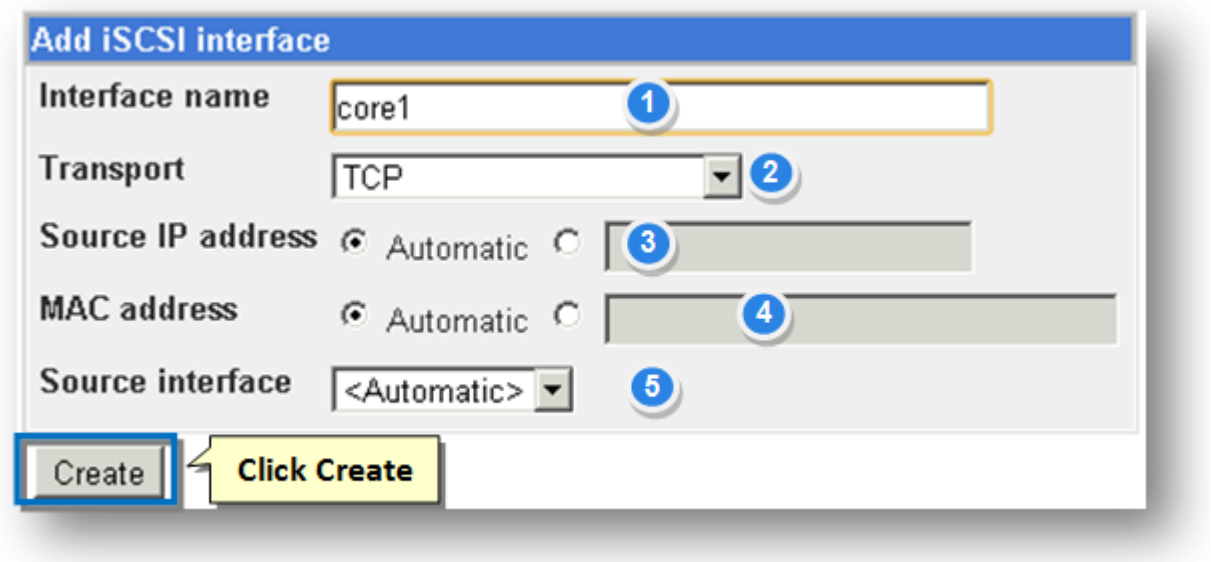
1. To configure iSCSI Interfaces sessions, click the **iSCSI Interfaces** button.

The iSCSI Interfaces page will be displayed.



From here, you can add a new iSCSI Interface or remove an existing interface.

Adding a New iSCSI Interface

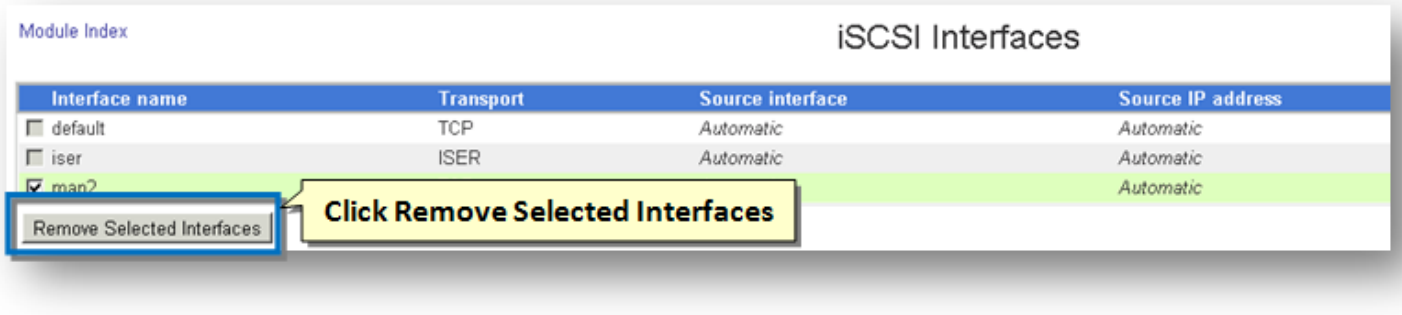


1. In the **Add iSCSI Interface** section, enter the name for the interface in the **Interface Name** text entry box.
2. Select the type of transport from the **Transport** drop down list.
3. Select the automatic option or enter manually the **Source IP address.**
4. Select the automatic option or enter manually the **MAC address.**
5. Select the source interface from the **Source interface** drop down list.
6. Click the **Create** button.

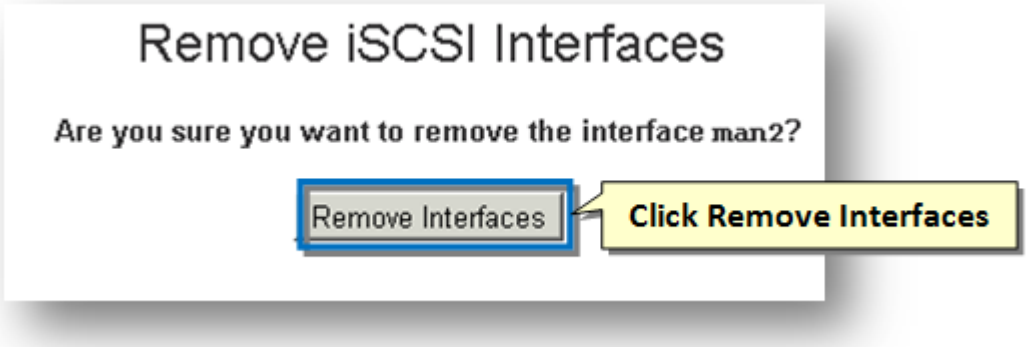
The new iSCSI interface will be added.

Removing an iSCSI Interface

1. To remove an iSCSI Interface, select it from the list.
2. Click the **Remove Selected Interfaces** button.



The **Remove iSCSI interfaces** page asking you to confirm the deletion of the selected interface will be displa



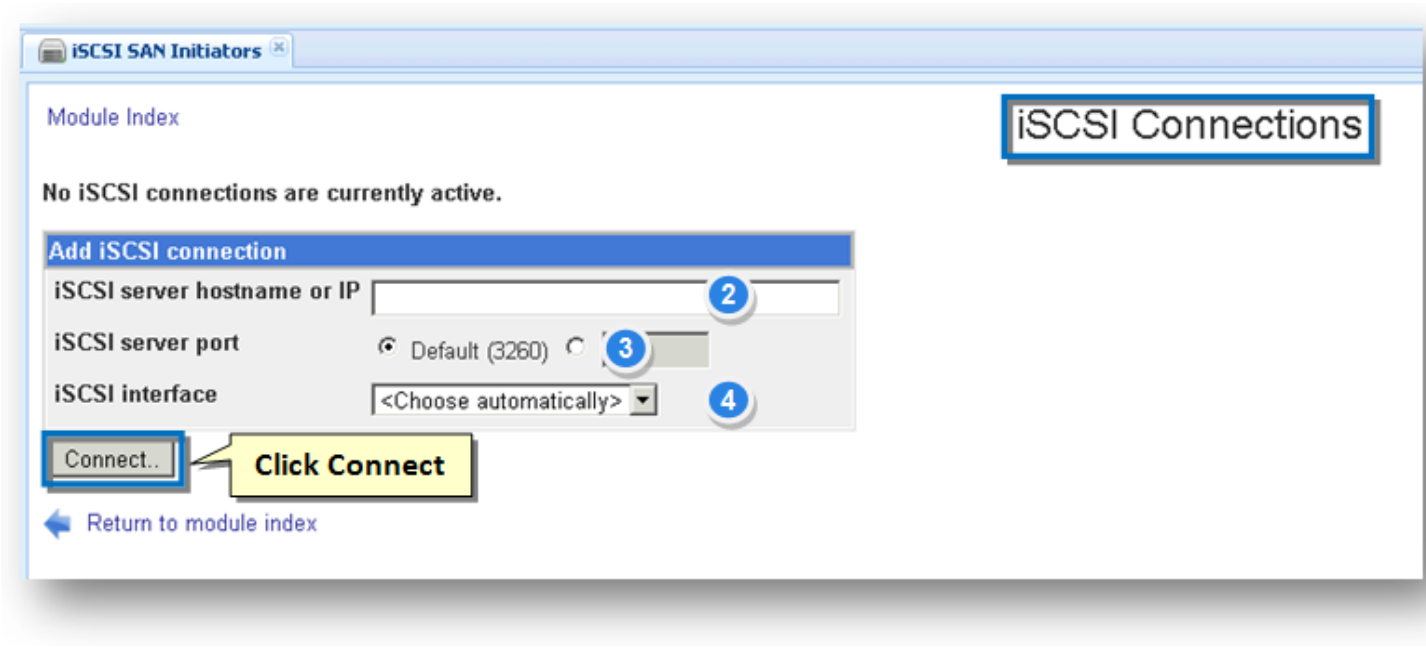
3. Click the **Remove Interfaces** button.

The selected iSCSI Interface will be removed.

6 Configuring iSCSI Connections

1. To configure iSCSI Connections, click the **iSCSI Connections** button.

The **iSCSI Connections** page will be displayed.



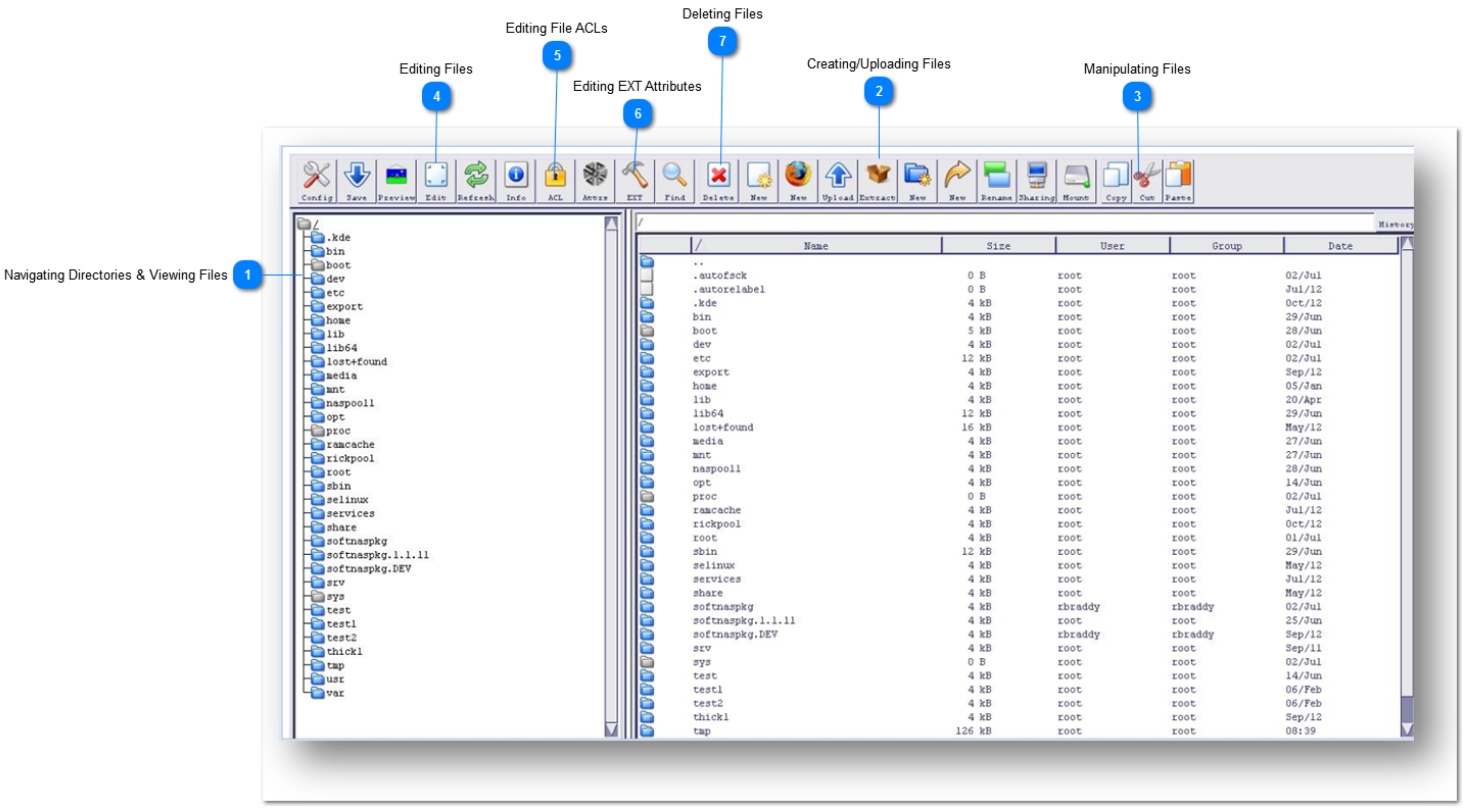
2. Enter the iSCSI server host name or IP in the text entry box.
3. Select the default option or enter manually the iSCSI server port value.
4. Select the type of iSCSI interface from the drop down list.
5. Click the **Connect** button.

The iSCSI Connection will be established.

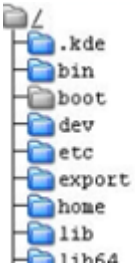
Managing Files

The **File System** browser is a Java-based applet providing the ability to view and manage the filesystem.

Note: You must have Java installed on the machine where your browser is running for the file system browser to operate.



1 Navigating Directories & Viewing Files



When you first load the file manager, the right-hand pane will display the contents of the root directory on your system. To enter another directory, just double-click on it in the list. To go back up a directory, double-click the .. link at the top the current directory's listing. You can also view the contents of a directory by clicking on it in the tree in the left-hand pane. Double-clicking will open the directory in the tree, causing any subdirectories under it to appear. Double-clicking again will close it. Whenever you enter a directory using the right-hand pane, it will be opened in the tree on the left as well. Similarly, when the .. link is double clicked to go back to the parent, the old directory will be closed in the tree.

The contents of any file on your system can be displayed by double-clicking on it in the right-hand pane. A separate browser window will be opened and the contents of the file will be displayed by your browser. Any file type that the browser supports, therefore, can be viewed using the file manager.

2 Creating/Uploading Files

The **File Manager** module offers two methods for creating new files—you can either create a text file from scratch, or upload data from the host on which your web browser is running. To create a new empty text file, click on the **New** document button on the toolbar to the right of the **Delete** button. This will bring up a window in which you can enter the full path to the file and its contents. When you are done editing, click the Save button at the bottom of the file creation window.

To upload a file from the PC on which your browser is running, click the **Upload** button on the toolbar. This will open a small browser window with two fields. The File to upload field is for selecting a file on your PC, while the Upload to directory field is for entering the directory to which the file will be uploaded. When both fields have been filled in, click the **Upload** button to have the file sent to your Webmin server. Once the upload is complete, the directory list will be updated to show the new file.

3 Manipulating Files

The **File Manager** module allows you to rename, move, and copy files in the just the same way that any other file manager would. To select the file that you want to manipulate, just click on it in the right-hand pane. To select multiple files, hold down the control key while clicking, or hold down the shift key to select an entire range.
To move files to a different directory, select one or more and click the **Cut** button on the toolbar.

Then navigate to the destination and click the **Paste** button. If a file with the same name already exists, Webmin will prompt you to rename the pasted file to avoid the clash. If you choose not to rename, the file in the destination directory with the same name will be overwritten.

To copy files, select them in the right-hand pane and click the **Copy** button. Then go to the directory to which you want them to be copied, and click Paste. As when moving files, you will be prompted to rename any that clash with files that already exist in the destination directory.

Multiple copies of a file can be made by pasting in different directories. To create a copy of a file in the same directory, just select it, click the **Copy** button and then the **Paste** button, and enter a new filename..

4 Editing Files

You can edit the file from the **File Manager.** Each file or directory on a UNIX filesystem is owned by a single user and group and have a set

of permissions that determines who can access it. You can edit that also by clicking the **Info** button on the toolbar.

Once you have edited the file, click the **Save** button to retain the changes.

5 Editing File ACLs

By setting up an ACL for a file, you can grant permissions to additional users or groups in addition to the normal owner and group.

Open the file and click the **ACL** button. The ACL for a directory can include several special default entries that determine the initial ACL of any file created in the directory. Default user, group, and mask entries can be created, and the default user and group can apply to either a specific user or the owner of the file.

6 Editing EXT Attributes

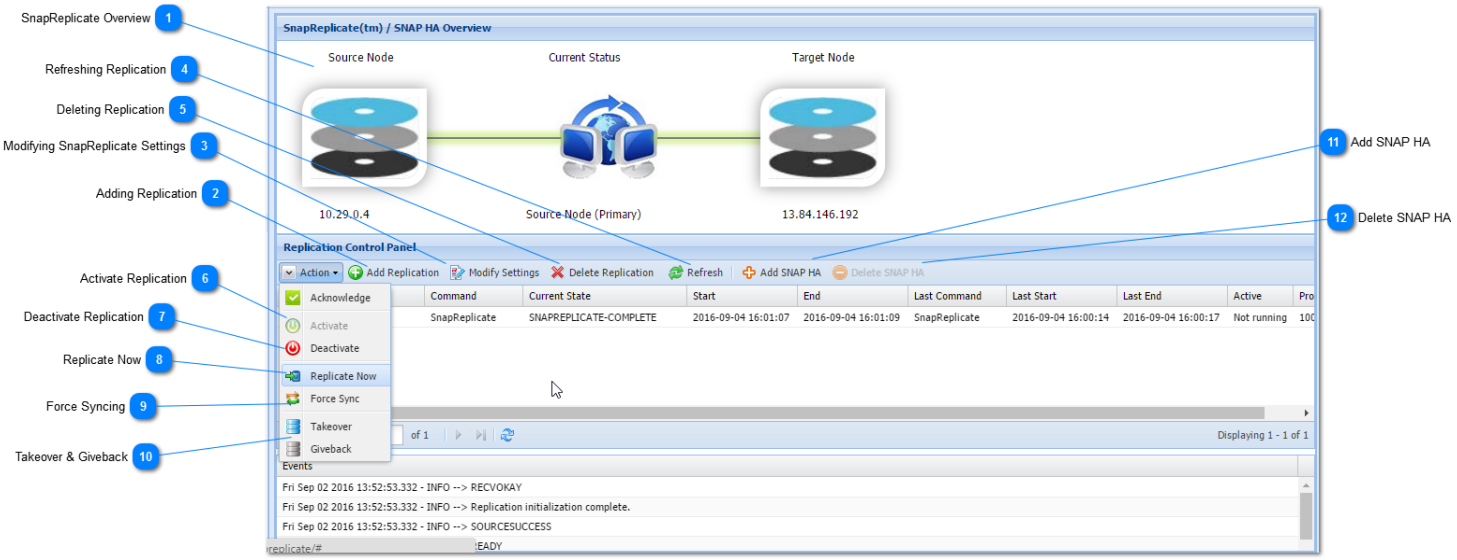
Several UNIX filesystem types support special attributes on files beyond those that can be set with the normal chmod and chown commands. You can change the EXT attributes for files if the files contain those attributes.

Open the file that contains EXT attributes and click the **EXT** button. You can control and stop access time updates, processes that modify content and prevent file from modification or deletion. You can also make the kernel automatically compress the contents of the file.

7 Deleting Files

You can delete one or more files and directories by selecting them and clicking the **Delete** button on the toolbar. Before they are actually removed, a confirmation window listing all chosen files will be displayed. When the Delete button in the window is clicked, all chosen files, directories, and their contents will be permanently deleted.

Managing SnapReplicate and SNAP HA

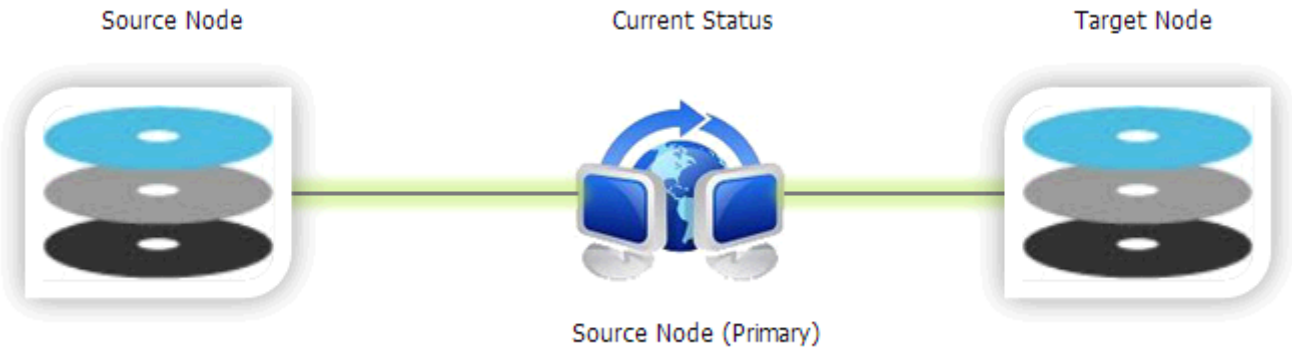


SnapReplicate provides a simple yet powerful means of defining a replication relationship between two **SoftNAS** controllers - the **source node** and the **target node.**

1 SnapReplicate Overview

SnapReplicate can be used for backup purposes, to create a hot-spare for failover and disaster recovery, and for site-to-site data transfers (e.g., region-to-region data replicas across **Amazon EC2** data centers, **VMware** failover across data centers, etc.).

In the following example, you can see a source node and a target node. The data is always replicated from the source to the target. The **Current Status** shows the replication active symbol (the two computers with blue arrow), along with the green transfer indicator.



The replication relationships works both the ways. The controller can become the primary source node, to facilitate failover operation. If the source node fails or requires maintenance, then the administrator can log into **SoftNAS StorageCenter** on the target node, and issue a **Takeover** command, which will cause the target to take over the role of source. Once the source node is repaired and back operational, a **Giveback** command can be used to revert the control back to the original source node.

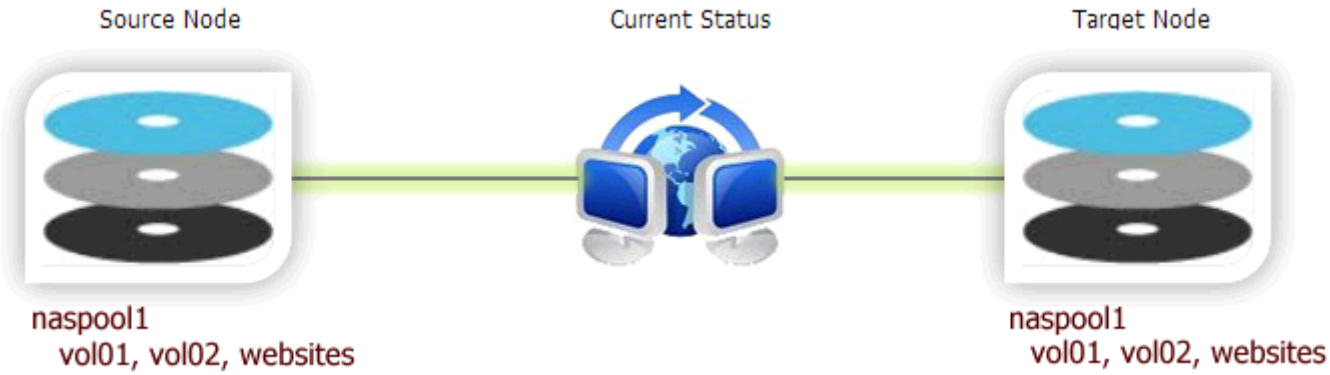
Preparing the SnapReplicate Environment

The first step in preparing a **SnapReplicate** deployment is to install and configure two **SoftNAS** controller nodes. Each node should be configured with a common set of storage pools with the same pool names.

Note: Only storage pools with the same name will participate in **SnapReplicate.** Pools with distinct names on each node will not be replicated.

For best results, it is recommended (but not required) that pools on both nodes be configured identically (or at least with approximately the same amount of available total storage in each pool).

In the following example, we have a storage pool named **naspool1** on both the nodes, along with three volumes: **vol01, vol02** and **websites.** In such cases, the **SnapReplicate** will automatically discover the common pool named **naspool1** on both nodes, along with the source pool's three volumes, and auto configure the pool and its volumes for replication. This means you do ***not*** have to create duplicate volumes (**vol01**, **vol02**, and **websites**) on the replication target, as **SnapReplicate** will perform this action.



Other important considerations for the **SnapReplicate** environment include:

- Network path between the nodes
- NAT and firewall paths between the nodes (you must open port 22 for SSH between the nodes)
- Network bandwidth available and whether to configure throttling to limit replication bandwidth consumption

Please note that **SnapReplicate** creates a secure, two-way SSH tunnel between the nodes. Unique 2048-bit RSA public/private keys are generated on each node as part of the initial setup. These keys are unique to each node and provide secure, authenticated access control between the nodes. Password-based SSH logins are disabled and not permitted (by default) between two **SoftNAS** nodes configured with **SnapReplicate.** Only PKI certificate-based authentication is allowed, and only from **known hosts** with pre-approved source IP addresses; i.e., the two **SnapReplicate** nodes (and the configured administrator on **Amazon EC2**).

After initial setup, SSH is used for command and control. SSH is also used (by default) as a secure data transport for authenticated, encrypted data transmission between the nodes.

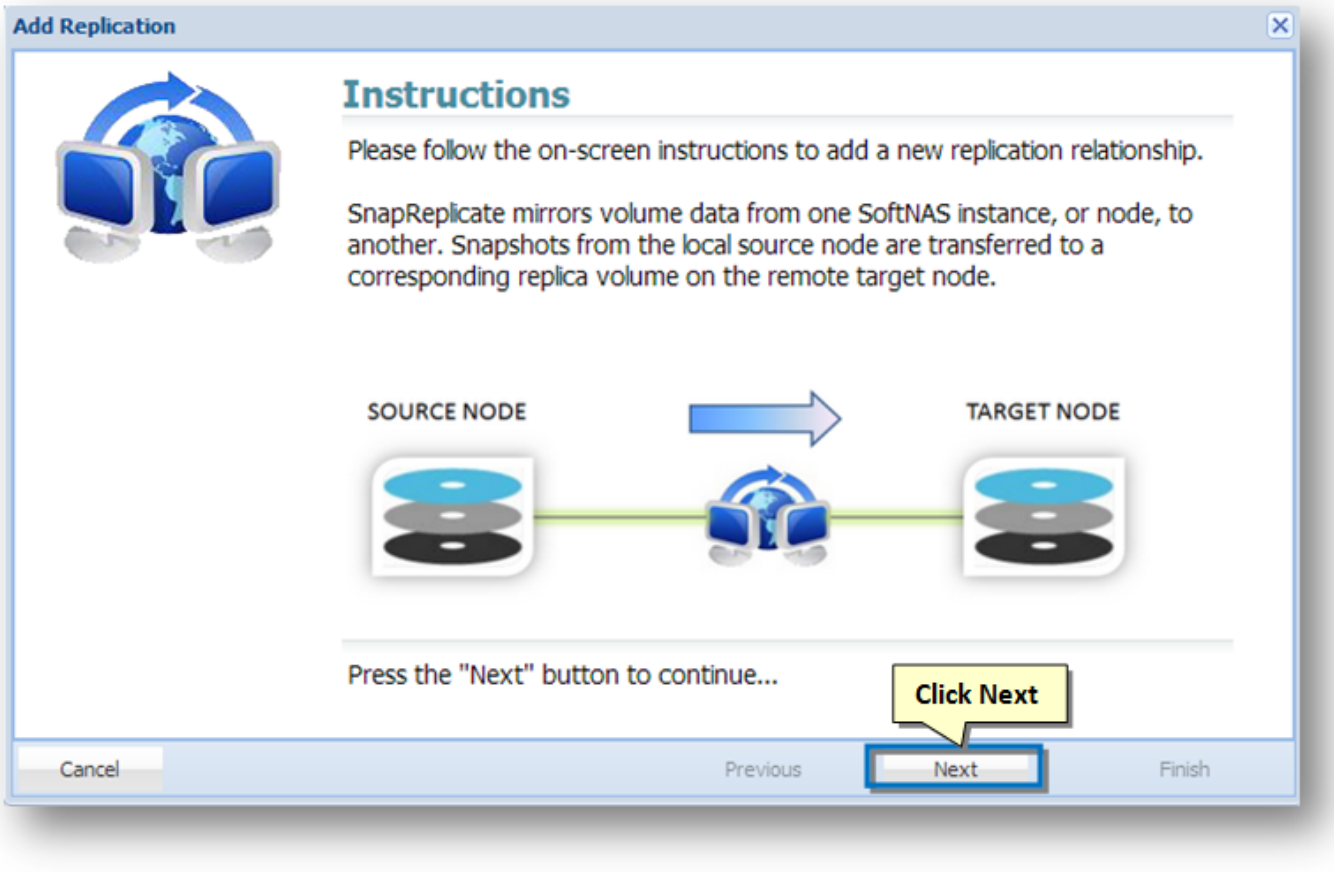
2 Adding Replication

You will need to be prepared with the IP address (or DNS name) of the target controller node, along with the **SoftNAS StorageCenter** login credentials for that node.

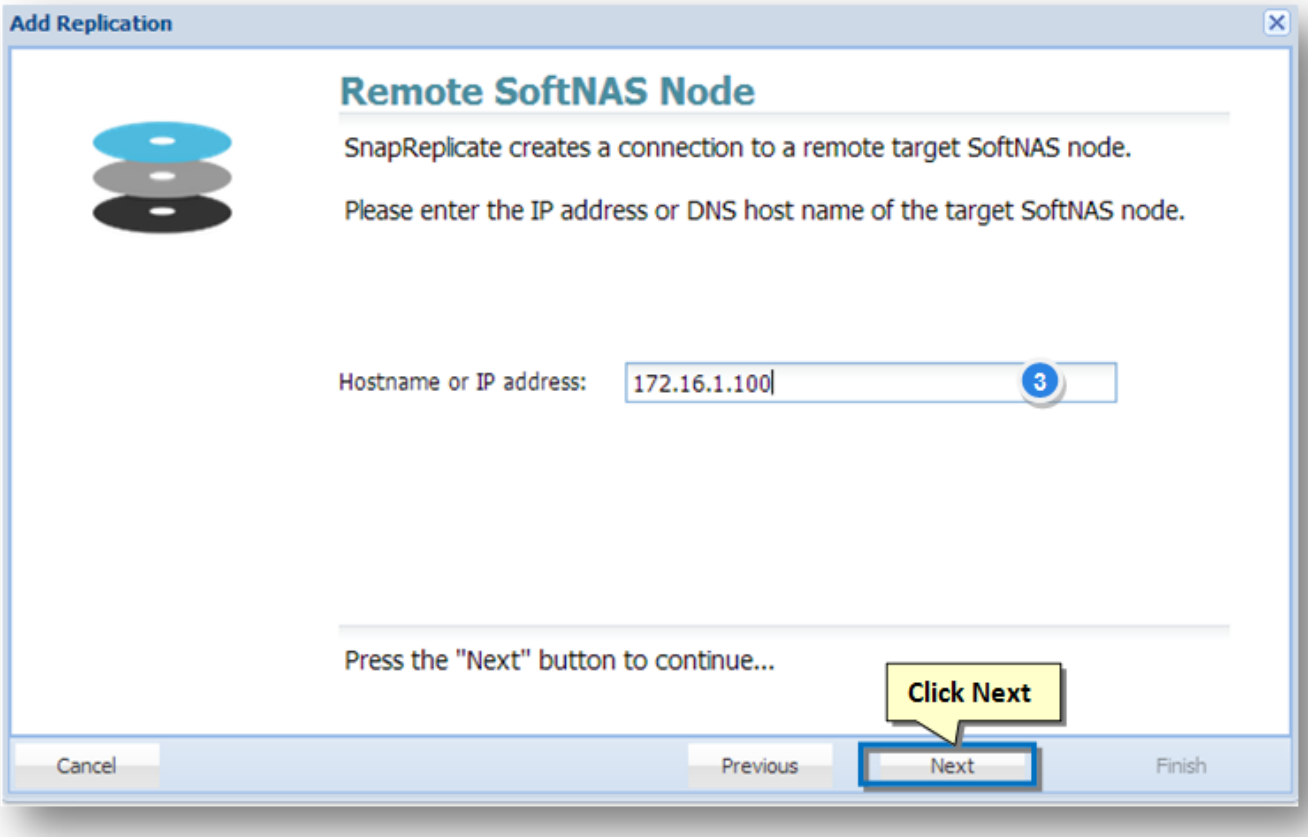
To establish the secure **SnapReplicate** relationship between two **SoftNAS** nodes, simply follow the steps given below.

1. Click the **Add Replication** button in the **Replication Control Panel.**

The **Add Replication** wizard will be displayed.



2. Read the instructions on the screen and then click the **Next** button.



3. In the next step, enter the IP address or DNS name of the remote, target **SoftNAS** controller node in the **Hostname or IP Address** text entry box.

There are two ways to set up AWS EC2 nodes for high availability. Previously, only Elastic IPs could be used. Private HA is now supported, using Virtual IPs. A Virtual IP is a HUMAN ALLOCATED IP address outside of the CIDR (Classless Inter-Domain Routing) range. For example, if you have a VPC CIDR range of 10.0.0.0/16 one can use 20.20.20.20. This will then be added to the VPC Route Table, and will be pointed to the ENI device (NIC) of one of the SoftNAS HA Nodes. A private high availability setup is recommended, as it allows you to host your HA setup entirely on an internal network, without a publically accessible IP. In order to access your high availability EC2 cluster, an outside party would need to access your network directly, via a jumpbox, or VPN, or other solution. This is inherently more secure than a native Elastic IP configuration.

To connect the nodes, the source node must be able to connect via HTTPS to the target node (similar to how the browser user logs into **StorageCenter** using HTTPS). HTTPS is used to create the initial **SnapReplicate** configuration. Next, several SSH sessions are established to ensure two-way communications between the nodes is possible. SSH is the default protocol that is used for **SnapReplicate** for replication and comand/control.

Amazon EC2 Node: Whether using a Virtual or Elastic IP setup to create a **SnapReplicate** relationship between two EC2 nodes, the source node must be able to connect via HTTPS to the target node (similar to how the browser user logs into **StorageCenter** using HTTPS). HTTPS is used to create the initial **SnapReplicate** configuration. Next, several SSH sessions are established to ensure two-way communications between the nodes is possible. SSH is the default protocol that is used for **SnapReplicate** for replication and command/control. When connecting two **Amazon EC2** nodes, keep in mind that you will need to use the internal instance IP addresses (not the the human allocated virtual IP outside the CIDR range mentioned above, or the Elastic IP, which is a public IP). That's because the traffic gets routed internally by default between instances in EC2 by default. Be sure to put the internal IP addresses of both EC2 instances in the Security Group to enable both HTTPS and SSH communications between the two nodes.

To view the internal IP address of each node, from the EC2 console, select **Instances,** then select the instance - the **Private IPs** entry shows the instance's private IP address used for **SnapReplicate.**

For example:

Node 1 - Virginia, East (zone 1-a) Private IP: 10.120.1.100 (initial source node)

Node 2: Virginia, East (zone 1-b) Private IP: 10.39.270.23 (initial target node)

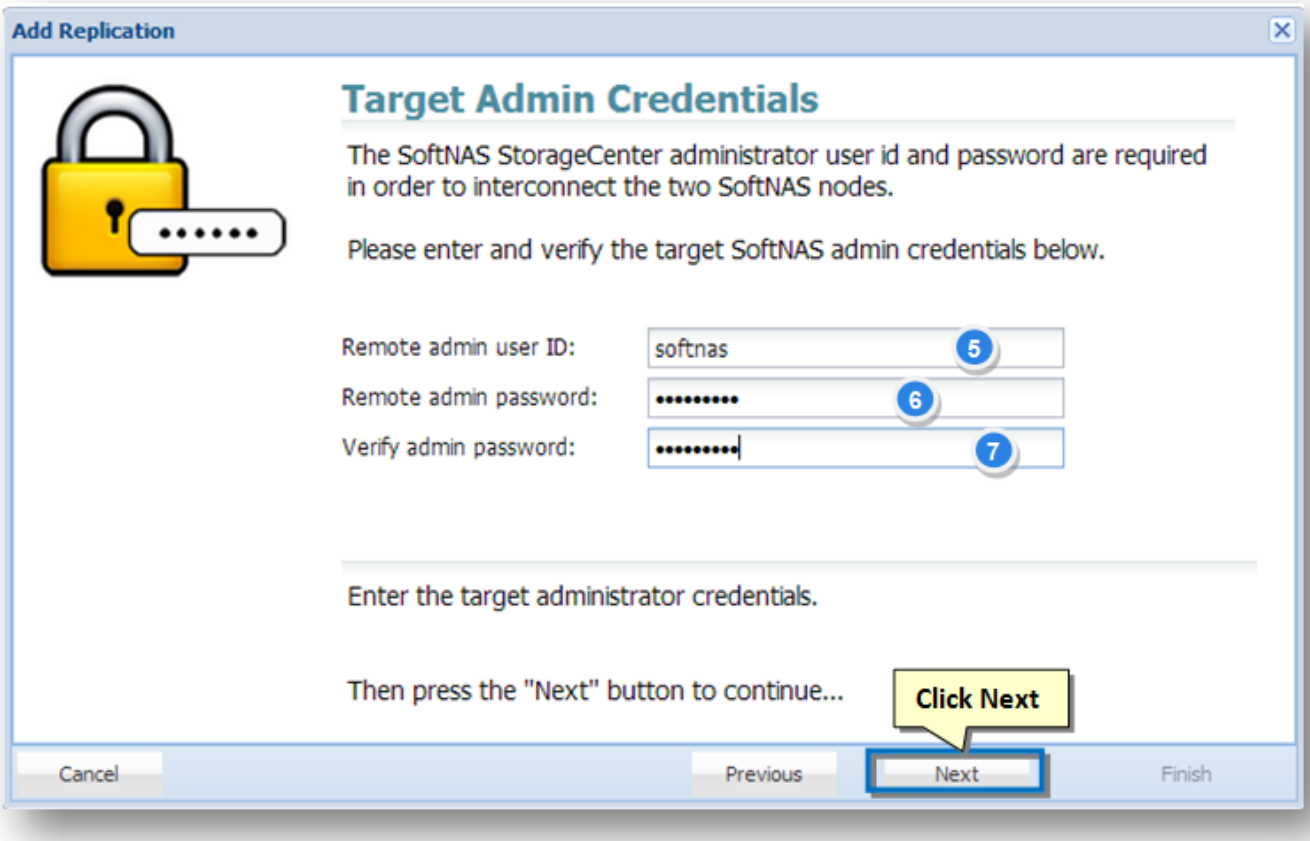
Add the following Security Group entries:

SSH 10.120.1.100/32
SSH 10.39.270.23/32
HTTPS 10.120.1.100/32
HTTPS 10.39.270.23/32

VMware: Similarly, it is important to understand your network topology and the IP addresses that will be used - internal vs. public IP addresses when connecting the nodes.

4. Click the **Next** button.

In the next step, provide the target node's admin credentials.



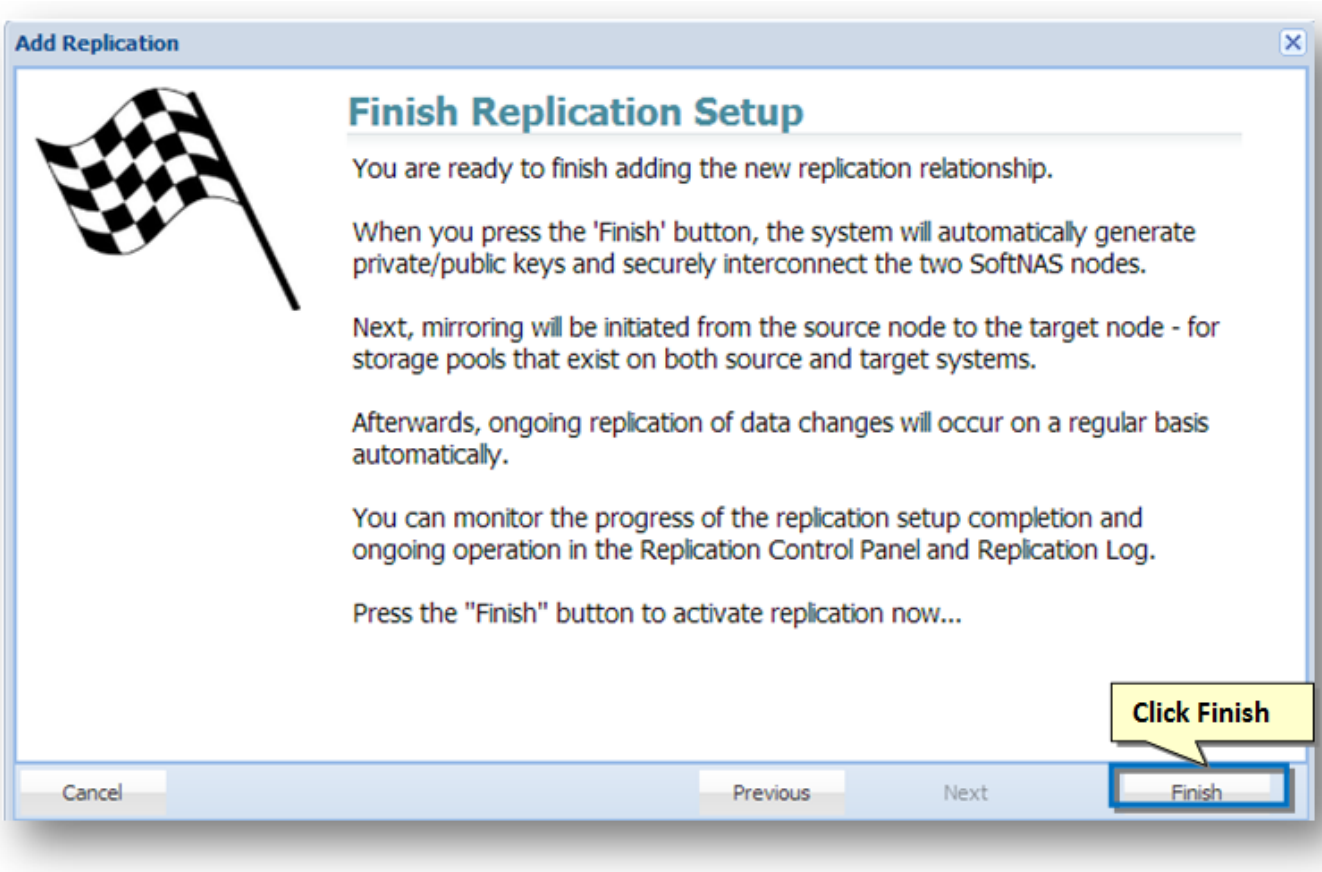
5. Enter the administrator's email ID for the target node in the **Remote Admin User ID** text entry box.

6. Enter the administrator's password for the target node in the **Remote Admin Password** text entry box.

7. Re-enter the administrator's password for the target node to confirm the same, in the **Verify Admin Password** text entry box.

8. Click the **Next** button.

The IP address/DNS name and login credentials of the target node will be verified. If there is a problem, an error message will be displayed. Then you need to click the **Previous** button to make the necessary corrections and then click the **Next** button to continue.



9. In the next step, read the final instructions and then click the **Finish** button.

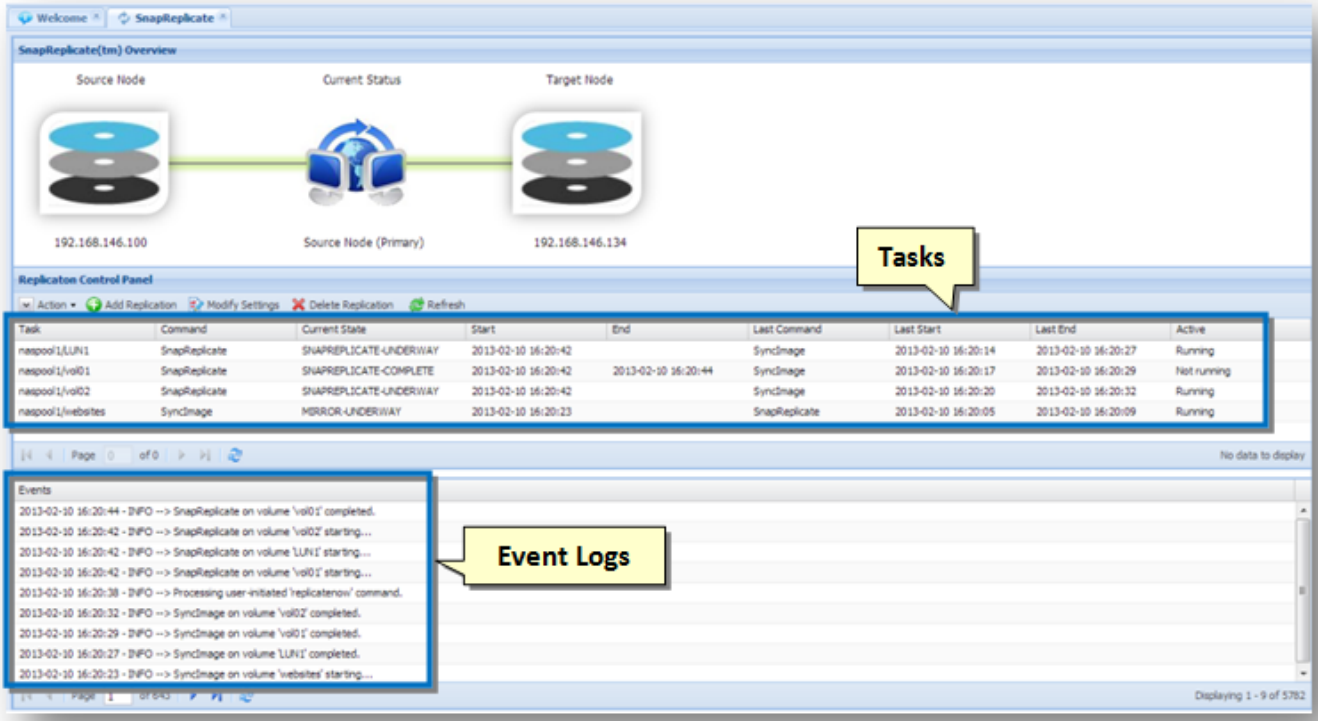
The **SnapReplicate** relationship between the two SoftNAS controller nodes will be established. The corresponding **SyncImage** of the **SnapReplicate** will be displayed.

The **SyncImage** compares the storage pools on each controller, looking for pools with the same name. For example, let's say we have a pool named "naspool1" configured on each node. Volume discovery will automatically add all volumes in "naspool1" from the source node to the replication task list.

For each volume added as a **SyncImage** task, that volume will be created on the target node (if it exists already, it will be deleted and re-created from scratch to ensure an exact replica will be created as a result of **SyncImage**). The **SyncImage** then proceeds to create exact replicas of the volumes on the target.

After data from the volumes on the source node is mirrored to the target, once per minute **SnapReplicate** transfers keep the target node **hot** with data block changes from the source volumes.

The tasks and an event log will be displayed in the **SnapReplicate Control Panel** section.

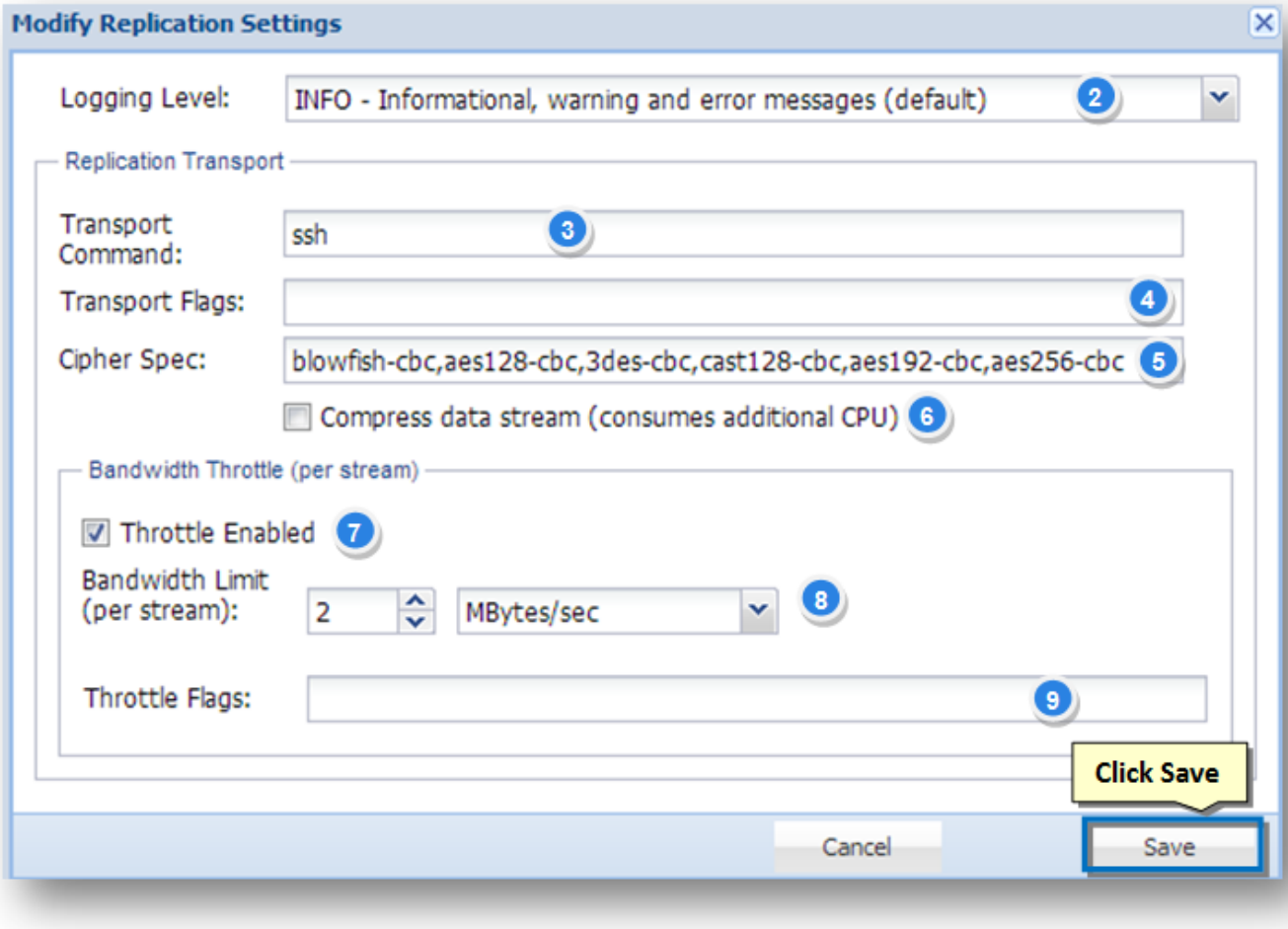


This indicates that your **SnapReplicate** relationship is established and the replication should be taking place.

3 Modifying SnapReplicate Settings

1. To modify **SnapReplicate** settings, click on the **Modify Settings** button.

The **Modify Replication Settings** dialog will be displayed.



This dialog helps you to control various **SnapReplicate** settings.

2. Select the level of information to be shown in the Events Log area from the Logging Level drop down list. The available options include:

- INFO - Informational, Warning and Error Messages (Default)
- DEBUG - Debug, Informational, Warning and Error Messages (All Messages)
- WARN - Warning and Error Messages
- ERROR - Error Messages Only
- FATAL - Fatal Messages Only
- OFF - No Messages (Not Recommended)

3. In the **Replication Transport** section, enter the Linux command line string used to create a transport tunnel from source to target, in the **Transport Command** text entry box.

Note: Do not modify this field unless you are sure about this.

4. Enter additional flags and options for the transport command line in the **Transport Flags** text entry box.

5. Enter the list of ciphers, in the priority order, that will be used by SSH for encryption of command & control and transport sessions, in the **Cipher Spec** text entry box.

6. To compress the data stream, check the box in the **Compress Data Stream** field. This actually consumes additional CPU.

7. In the **Bandwidth Throttle (Per Stream)** section, check the box in the **Throttle Enabled** field to limit the maximum network bandwidth used for each replicated volume.

8. Specify the numeric value for the maximum bandwidth amount, per stream / volume and select the units (e.g., MBytes/sec, Kbits/sec, etc.) in the Bandwidth Limit (per stream) field.

9. Enter the optional flags which can be used to further customize the throttle (advanced - ignore for now), in the Throttle Flags text entry box.

10. Click the **Save** button.

The changes made to the **SnapReplicate** will be updated.

4 Refreshing Replication

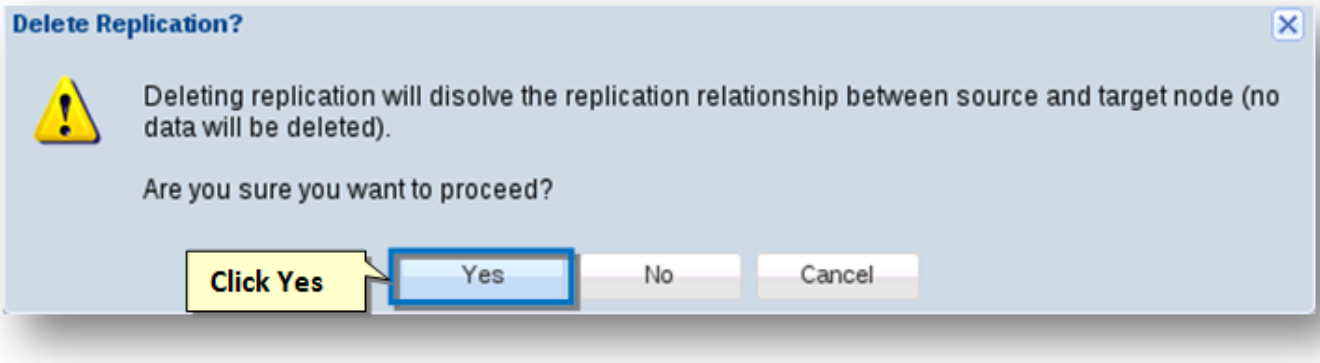
You can refresh the replication and update it with the latest information. To do so, simply click the **Refresh** button in the toolbar.

The replication will be reloaded.

5 Deleting Replication

1. In order to dissolve a **SnapReplicate** relationship between the two nodes, click the **Delete Replication** button.

The message box asking you to confirm the dissolving of the replication relationship between the two nodes will be displayed.

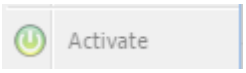


2. Click the **Yes** button.

The replication relationship between the source and the target nodes will be dissolved.

Note: No data is deleted. All volumes on both source and target nodes remain intact. **Snapshots** associated with **SnapReplicate** on the affected volumes are purged; otherwise, no changes to pools or volumes occurs when the replication relationship is deleted. The SSH relationship between the nodes is also dissolved, along with the PKI public/private keys and SSH login rights.

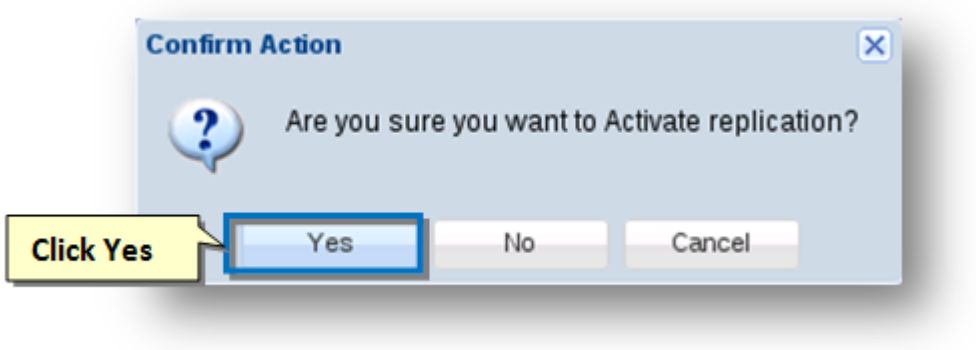
6 Activate Replication



You can activate a replication.

1. Select the replication that you want to make active.
2. To do so, click the **Activate** option from the **Actions** drop down list.

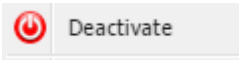
The **Confirm Action** message box asking you to confirm the activation of replication will be displayed.



3. Click the **Yes** button.

The replication will become active.

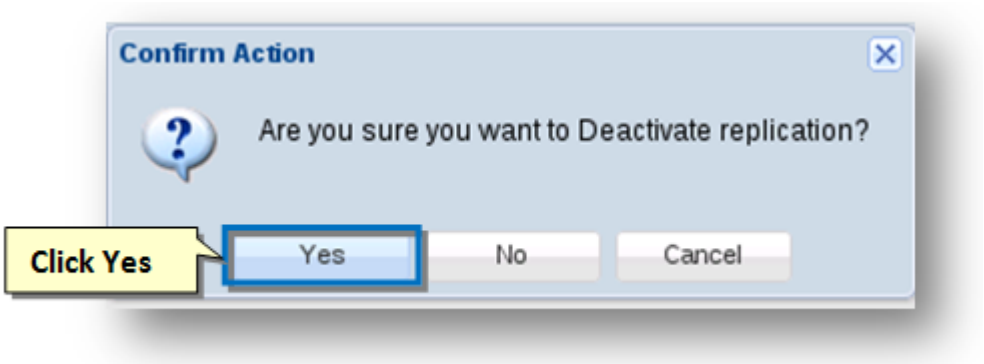
7 Deactivate Replication



You can deactivate a replication.

1. Select the replication that you want to deactivate.
2. To do so, click the **Deactivate** option from the **Actions** drop down list.

The **Confirm Action** message box asking you to confirm the deactivation of replication will be displayed.



3. Click the **Yes** button.

The replication will be deactivated.

About NAT and Firewalls

The **SnapReplicate** attempts to automatically discover the proper return path from the target node to the source. It does this on the target by analyzing the IP address of the **SoftNAS StorageCenter** webserver involved in establishing the relationship phase.

Consider the following scenarios.

Scenario 1 - Same data center deployment

When deployed in the same data center, the IP addresses will likely be locally routable, with no firewall between the controllers.

Scenario 2 - Different data center deployment

When the source and target are deployed in different data centers, each node will exist on different networks separated by several layers of firewalls. To determine its return path (from target-to-source), the automated setup process will use the source data center's public IP address. For example:

```
source node  ------  Data Center 1 ------  Firewall 1------      Internet/cloud    ------
Firewall  2------  Data Center 2  ------  target node

172.16.1.100  ==>  172.16.1.0/24  ==>    NAT   ==>  54.188.13.227   ==>  215.100.1.7  NAT
  ==>  172.16.30.0/24 ==>  172.16.30.225
```

The above path shows a network topology involving two data centers, connected via two firewalls using NAT. In this example, the source's IP address will appear to be 54.188.13.227, the public IP of Firewall 1. **SnapReplicate** on the target node will use the public IP address 54.188.13.227 to communicate from target-to-source (during a **takeover,** where the target takes over as source during a failover event). It is important that Firewall 1 be configured to allow SSH (port 22) inbound traffic from data center 2 public IP 215.100.1.7, and NAT route that traffic to the source node at 172.16.1.100, as shown below:

```
172.16.1.100  <= =   172.16.1.0/24      <= =    NAT   <= =  54.188.13.227   <= =
215.100.1.7  NAT    <= =  172.16.30.0/24  <= = 172.16.30.225
```

VPN Tunnels

VPN tunnels may be used to provide added security with IPSec encapsulation of the SSH traffic (vs. opening port 22 directly on the Internet), and are highly-recommended when connecting SoftNAS nodes across data centers involving the public Internet. While the SSH transports use the strongest commercially-available PKI authentication and encryption, use of IPSec provides another layer of security and authentication that is likely required from a security policy standpoint in many environments.

WAN Deployment

SnapReplicate is intended for deployment using typical WAN links. For best results with WAN deployment, it is recommended to configure a bandwidth throttle which limits the amount of network bandwidth each **stream** is allowed to consume. Bandwidth is throttled on the **outbound** side; i.e., from source to target.

A unique stream (e.g., SSH session) is created for each **SyncImage** and **SnapReplicate** task. Each time a volume is replicated by one of these tasks, the bandwidth throttle will limit the amount of bandwidth allowed per stream.

For example, if you have 10 volumes and wish to limit the maximum WAN bandwidth consumption to 2 Mb/sec, then set a conservative per stream bandwidth to 200 Kb per stream (2 Mb / 10). If instead you know your data changes from the busiest volume no more than 2 Mb/sec worth of data changes each minute, then you can choose a more aggressive throttle setting of 2 Mb/sec for maximum burst throughput (in this case, if all 10 streams were to simultaneously experience significant change, a brief burst of up to 20 Mb/sec would be theoretically possible).

You may also wish to employ other methods of WAN bandwidth management; e.g., at the router or other network level.

What Gets Replicated

The **SyncImage** creates an exact replica of each configured source volume on the target. It first deletes the volume (if it exists) on the target, so be certain to choose the initial source and target nodes correctly.

The **SnapReplicate** keeps each target volume up to date with the latest data changes applied to the source volume. SnapReplicate runs once per minute as a cron job.

During each replication cycle (once per minute or anytime an ad-hoc **Replicate Now** cycle occurs), certain configuration information is also transferred from source to target, to facilitate a complete failover. Information transferred includes NFS exports and CIFS (Samba) configuration files.

Limitations

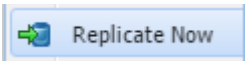
Takeover and **giveback** commands only affect which node is source and which is target, and the direction replication data flows between the nodes. It does not alter either node's IP address, DNS name or network identity in any way.

It is recommended to use DNS names as a means of redirecting incoming NFS, CIFS and iSCSI requests from one node to the other (which is a manual process that should be planned for and handled accordingly during a failover event).

It is certainly possible to integrate third-party failover systems using SnapReplicate scripting (see the SoftNAS User Reference Guide for information on SnapReplicate command line usage), which is beyond the scope of this installation document.

An automatic failover module is on the SoftNAS roadmap in 2013, which will automate the entire failover process.

8 Replicate Now



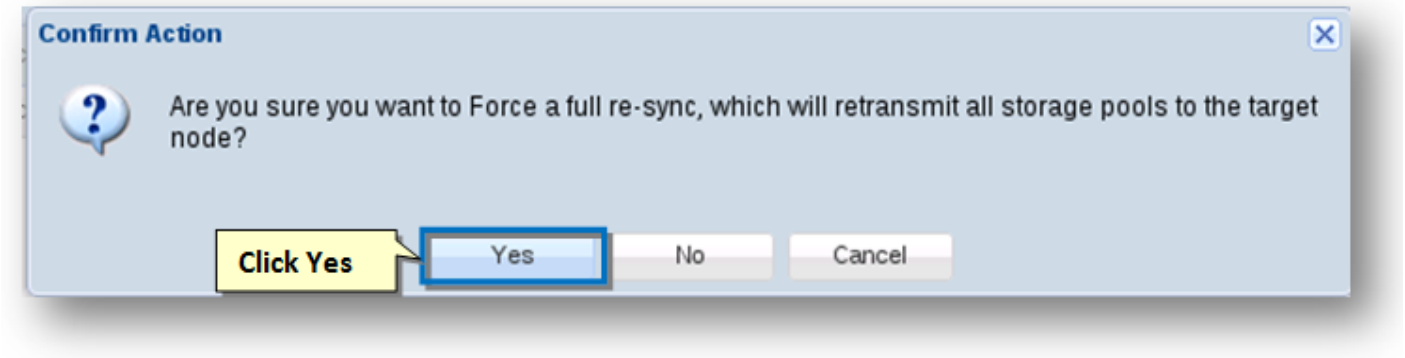
Unlike Force Sync, which forces all pools to replicate across to the target node, Replicate Now will trigger a replication cycle to update recent changes.

9 Force Syncing

You can force a sync that will retransmit all storage pools to the target node.

1. To do so, click the **Force Sync** option from the **Actions** drop down list.

The **Confirm Action** message box asking you to confirm the force syncing of the replication will be displayed.



3. Click the **Yes** button.

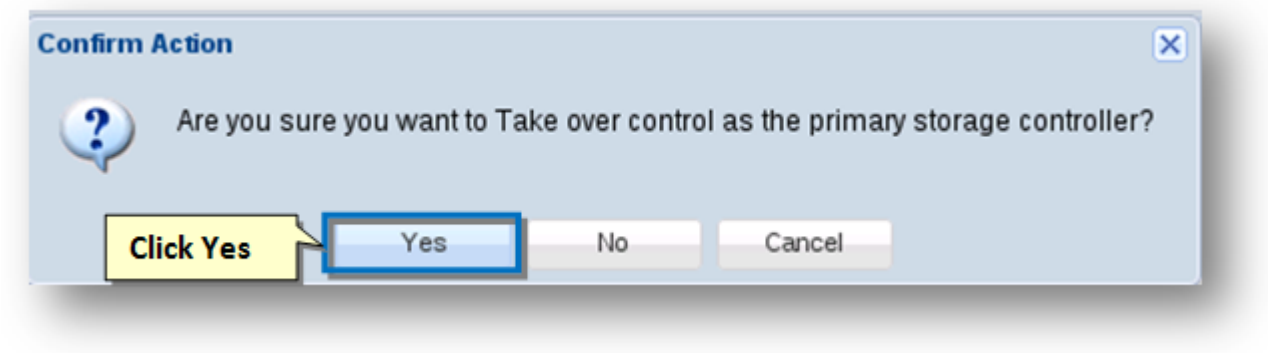
All the storage pools are retransmitted to the target node.

10 Takeover & Giveback

A **takeover** command can be issued from the **SnapReplicate** control panel on the target node. For clarity, we will use **node 1** to indicate the original source node and **node 2** to indicate the original target node (before a takeover occured).

1. To do so, click the **Takeover** option from the **Actions** drop down list.

The **Confirm Action** message box asking you to confirm the take over control as the primary storage controller will be displayed.



3. Click the **Yes** button.

When a takeover is issued from at the target node, the following occurs:

- The target node 2 configures itself as the new source node, assuming all duties of the source.

- The target applies the saved configuration changes (NFS exports, CIFS and iSCSI configs, etc.) and then restarts the affected services (NFS, Samba, iSCSI) with the proper configuration. This enables the target to begin serving storage requests as if it was the former source controller.

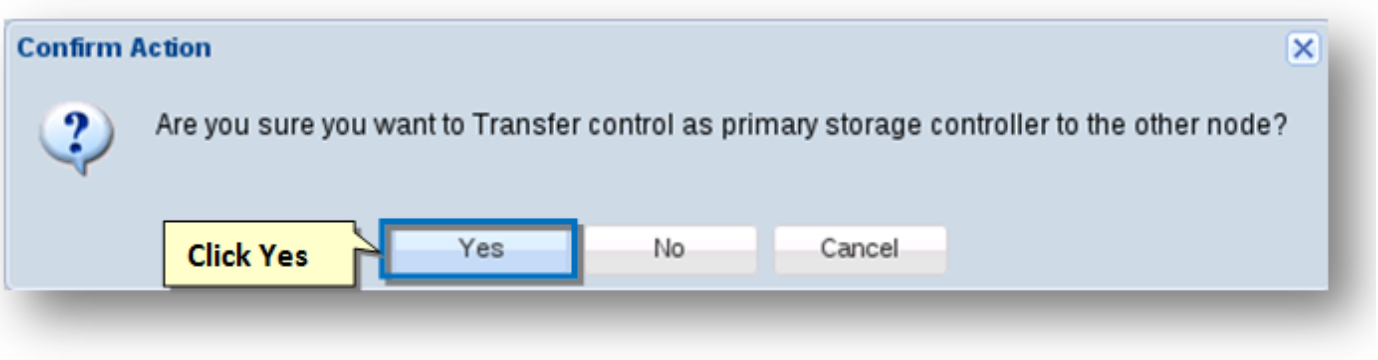
- The new source node 2 will reset its replicate state back to a **start** state, which means when the target node 1 (the former source node) comes back online, replication will start over with a fresh SyncImage, followed by incremental **SnapReplicate** cycles once per minute, from node 2 to node 1. This will automatically re-synchronize the two nodes. If you want to manually control when re-synchronization from node 2 to node 1 occurs, then place node 2 into a deactivated state using the **Deactivate** command immediately following a successful takeover.

- A takeover timestamp was stored on the target node 2 at the time the takeover was initiated. This timestamp is used to inform the old source node 1 (which may have failed) of the takeover event. When the failed source node 1 is reactivated, it will see the takeover timestamp of node 2, which took control, and node 1 will assume the role of **target** appropriately.

Once the node 1 is repaired and back online, to fail back to the original node 1, use the **Giveback** command from node 2.

4. To do so, click the **Giveback** option from the **Actions** drop down list.

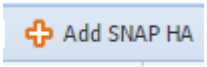
The **Confirm Action** message box asking you to confirm the transfer control as the primary storage controller to the other node will be displayed.



3. Click the **Yes** button.

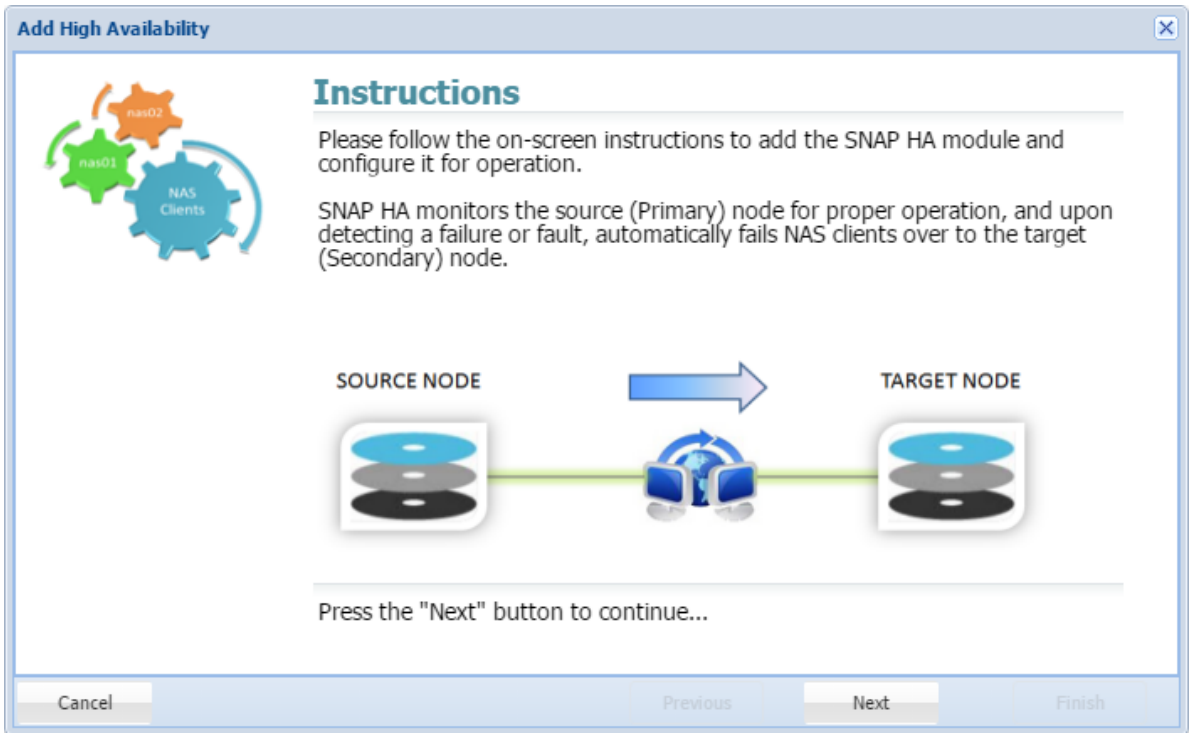
Alternatively, you can issue a **Takeover** command from node 1, which will cause node 1 to assume its original duties as the primary source node.

11 Add SNAP HA

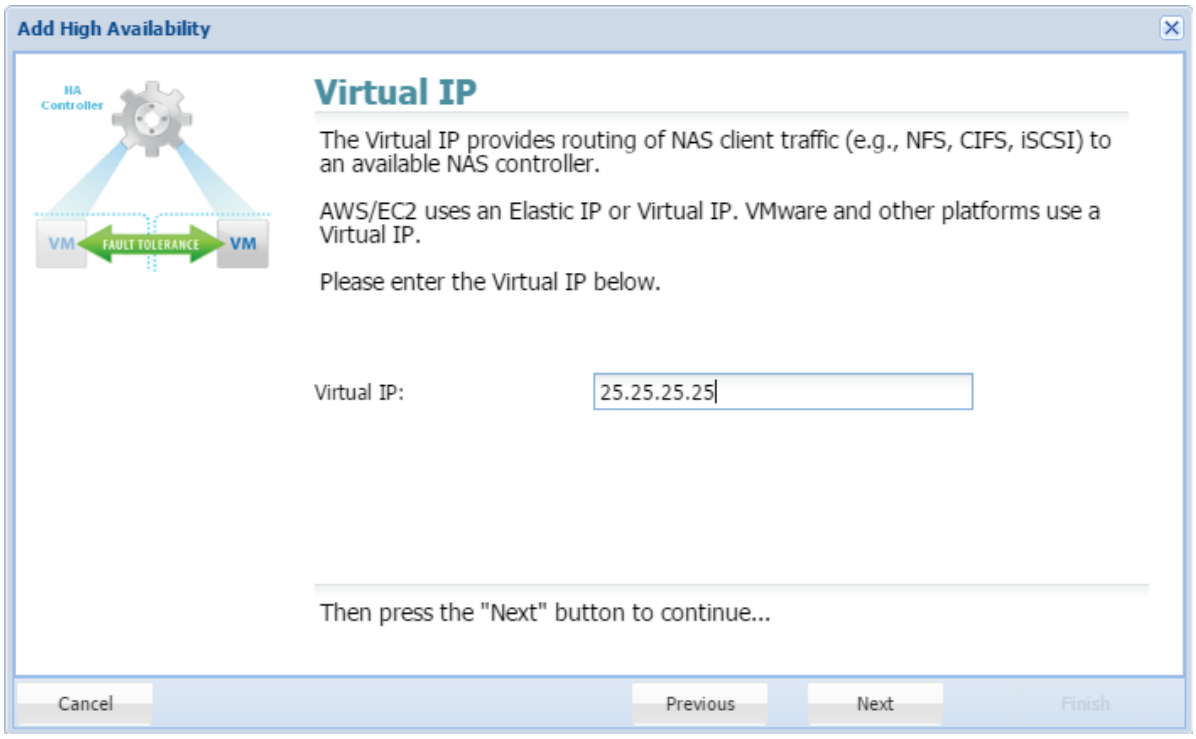


Once a SnapReplicate pairing is established, SNAP HA can be implemented. SnapReplicate established easy manual failover, including forced synchronization and manual takeovers and givebacks. SNAP HA establishes a heartbeat which will trigger automated failover,ensuring that your dataset is protected.

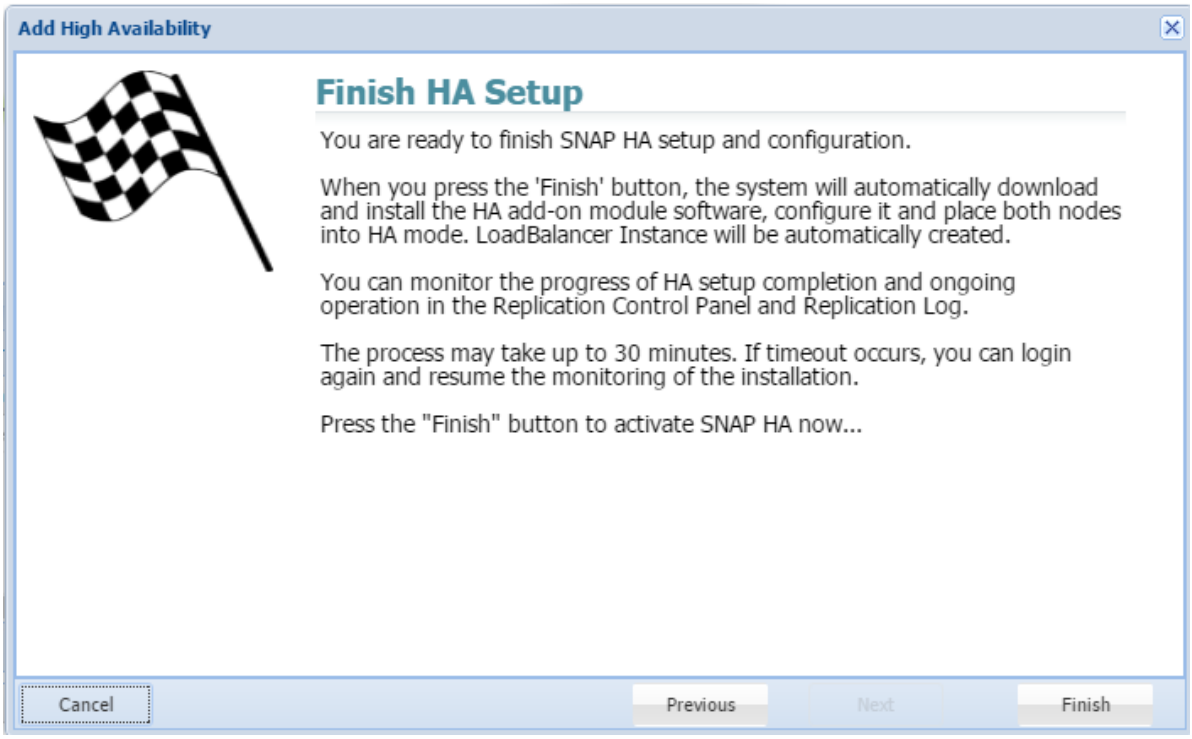
Clicking **Add SNAP HA** will trigger the following wizard. Click **Next**.



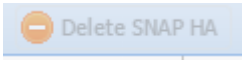
Provide a Virtual IP. This is a human-configured (chosen by you) IP address. It must be outside the CIDR block of the two SoftNAS instance IP addresses.



Click **Finish**. Your Snap HA pairing will be complete.



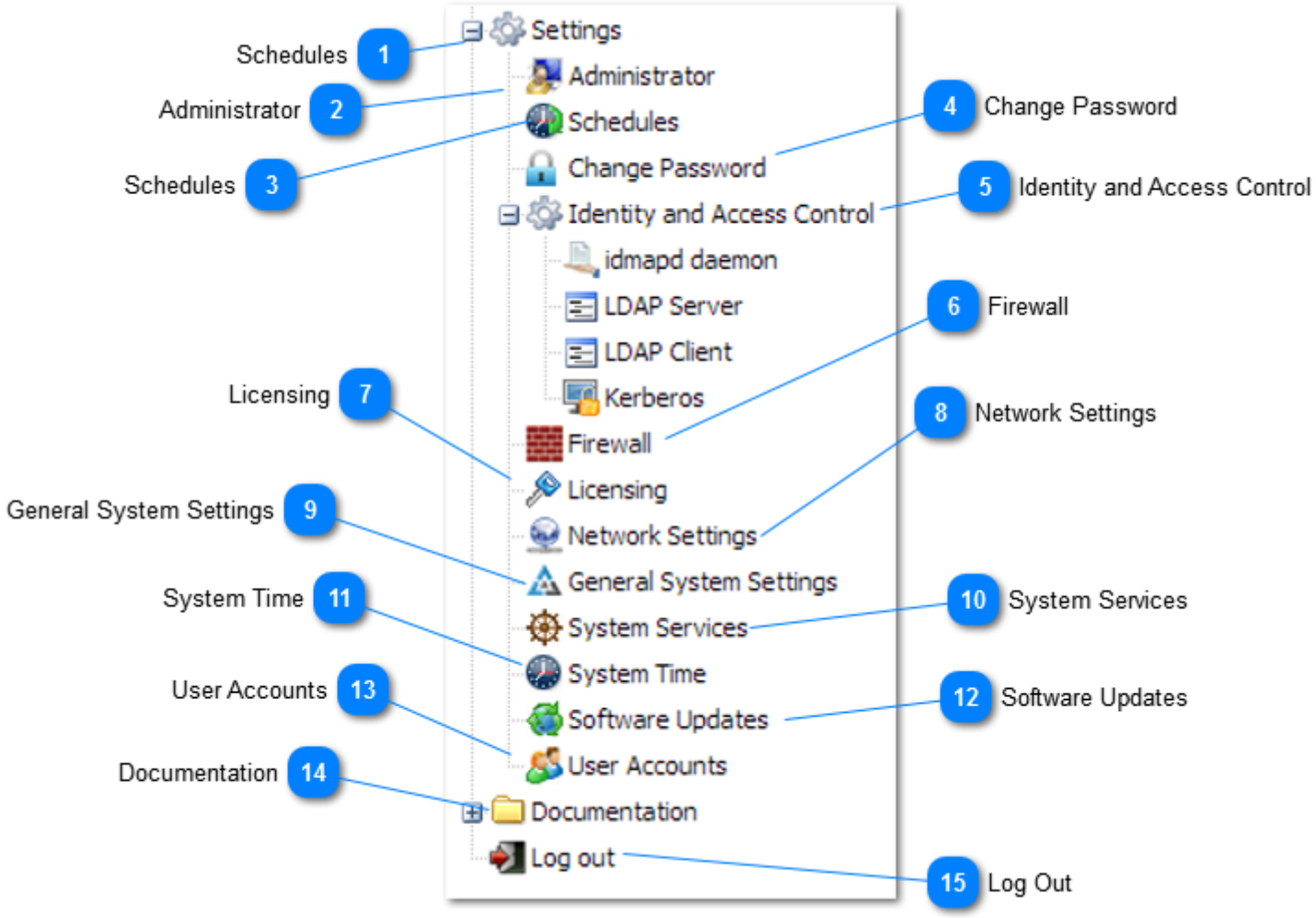
12 Delete SNAP HA



To remove the SNAP HA relationship, click here, and accept the prompts.

Working with Settings

The **Settings** section allows you to configure core modules.



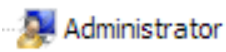
1 Schedules

SoftNAS includes a task scheduler, used to execute various tasks on a periodic basis; e.g., scheduled snapshots, scheduled replication, etc.

For more information, refer to the following link.

Managing Schedules

2 Administrator

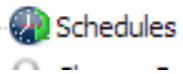


The administrator settings enable the SoftNAS administrator to make settings for standard server and network administration.

For more information

[Administrator]

3 Schedules

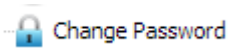


SoftNAS includes a task scheduler, used to execute various tasks on a periodic basis; e.g., scheduled snapshots, scheduled replication, etc.

For more information

[Managing Schedules]

4 Change Password

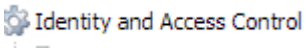


You can configure and manage all users's passwords from **Passwords** panel.

For more information, refer to the following link.

[Managing Passwords]

5 Identity and Access Control



You can use identity and Access Control to configure the following:

- idmapd daemon
- LDAP Server
- LDAP client
- Kerberos

idmapd daemon:

Configuration file for libnfsidmap. Used by idmapd and svcgssd to map NFSv4 name to and from ids.

For more information

[idmapd configuration]

LDAP Server:

LDAP Server enables you to configure the fields of the LDAP configuration.

SoftNAS provides support for NFSv4 Kerberos and LDAP Support, which enables multi-user security access rights to files and directories managed by the SoftNAS filer.

For more information

LDAP Server

LDAP client:

For more information

LDAP Client

Kerberos:

The **Kerberos** helps in communicating over a non-secure network to prove identity to one another in a secure manner. You can configure **Kerberos** from **SoftNAS.**

For more information, refer to the following link.

Configuring Kerberos

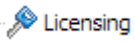
6 Firewall

The **Firewall** in **SoftNAS** helps you to control the incoming and outgoing network traffic in VPN.

For more information, refer to the following link.

Managing Firewall

7 Licensing

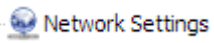


You can enter license key and activate your copy of **SoftNAS.**

For more information, refer to the following link.

Activating License

8 Network Settings

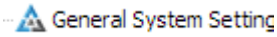


You can administer network interfaces, routing and gateways, hostname, DNS and other network-related configuration.

For more information, refer to the following link.

[Configuring Network Settings]

9 General System Settings

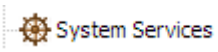


The **System Settings** in **SoftNAS** allows configuring general system settings through the standard Webmin control panel. SoftNAS uses Webmin to provide robust Linux administration functionality. It provides a rich, extensive set of Linux administration tools for advanced users.

.For more information, refer to the following link.

[Configuring General System Settings]

10 System Services

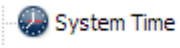


The **System Services** allows you to manage all bootup and shutdown processes and services. You can also create a new upstart service.

For more information, refer to the following link.

[Managing System Services]

11 System Time

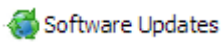


The **System Time** module allows you to configure system time and hardware clock. You can also change time zone and synchronize the system time with a remote server.

For more information, refer to the following link.

[Configuring System Time]

12 Software Updates

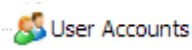


After installing **SoftNAS,** it is recommended to perform a software update to ensure that you are running the latest version.

For more information, refer to the following link.

[Updating Software]

13 User Accounts

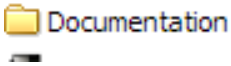


The **User Accounts** section of **SoftNAS** allows you to add, edit, remove and manage user groups and users.

For more information, refer to the following link.

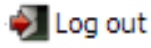
Managing User Accounts

14 Documentation



Access SoftNAS documentation.

15 Log Out



Log out of SoftNAS.

Administrator

The Administrator Panel provides standard server and network administration options. These provided settings allow the SoftNAS administrator to monitor the instance, review logs, perform key management tasks, and configure backup services.

The following server and network administration settings are available:

Mail server

Monitoring

Support Tab

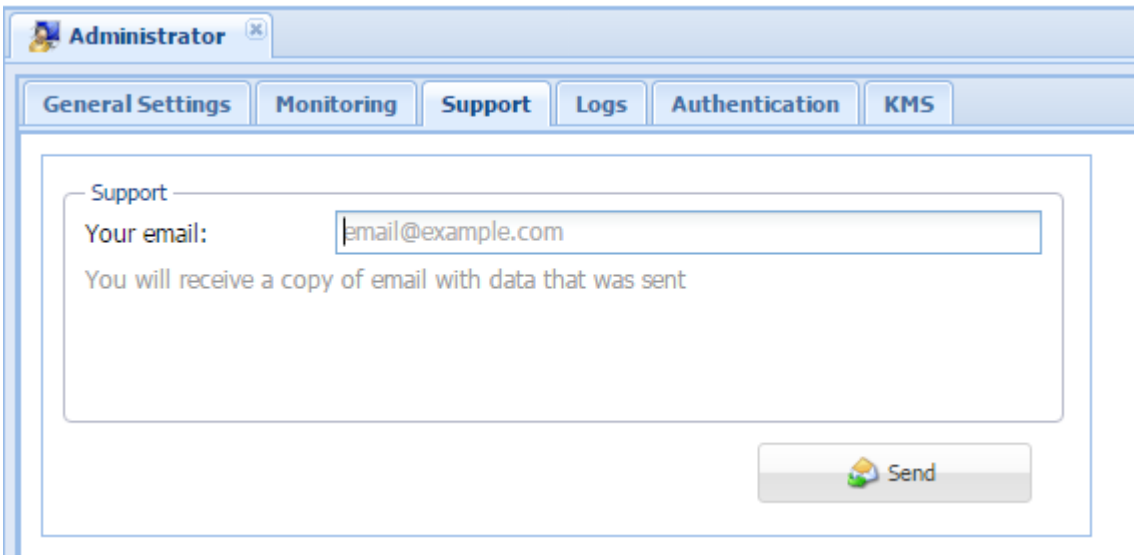
Logging

Authentication

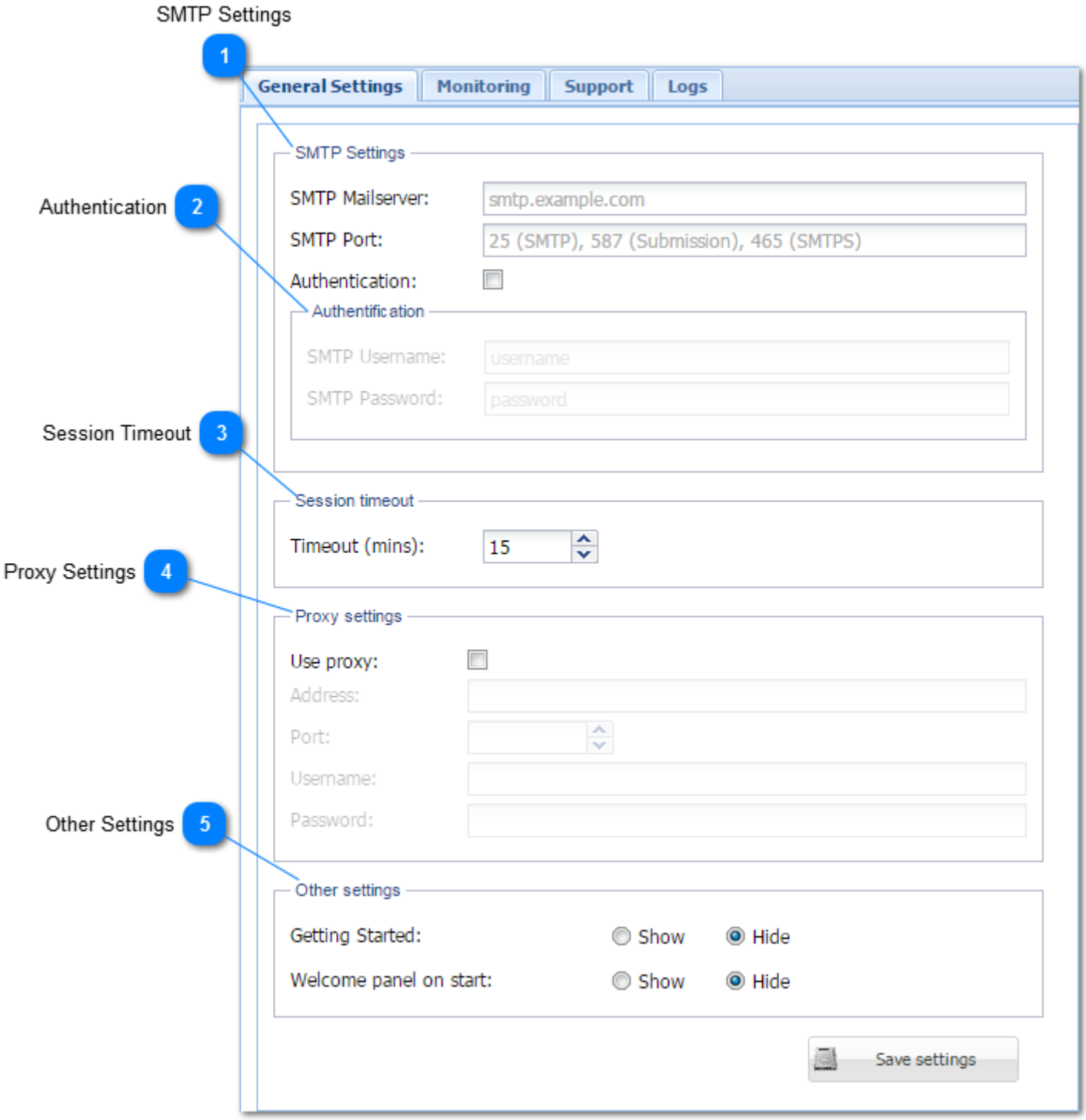
Key Management System (KMS)

Support

The Support Tab generates a help ticket in SoftNAS support. Providing your email and clicking "Send" will create a support ticket, and automatically attach logs from your instance to help our support staff troubleshoot your issue.



General Settings



1 SMTP Settings

SMTP Settings

The SMTP settings enable the Administrator to specify the organization's corporate mail server. SoftNAS will then use this mail server when sending email notifications to stakeholders.

Parameter	Description

SMTP Mailserver	Enter the FQDN of the corporate mail server.
SMTP Port	Enter the port which SoftNAS will use to contact the mail server. Possible values: • 25 • 587 • 465

2 Authentication

Authentification

Authentication can be enabled to create a secure connection between SoftNAS and the mail server. If authentication credentials are required they can be entered here.

Parameter	Description
SMTP Username	Username used to authenticate with the mail server.
SMTP Password	Password used to authenticate with the mail server.

3 Session Timeout

Session timeout

Setting which controls how long an inactive session SoftNAS browser session will remain up before the server terminates the connection. Default setting is 15 minutes.

4 Proxy Settings

Proxy settings

Allows you to connect to SoftNAS instances using a proxy server intermediary.

Parameter	Description
Use proxy	Enable/disable connection to SoftNAS via proxy server.
Address	IP Address of the proxy server.
Port	Port to connect to the proxy server.
Username	Username to connect to the proxy server.
Password	Password to connect to the proxy server.

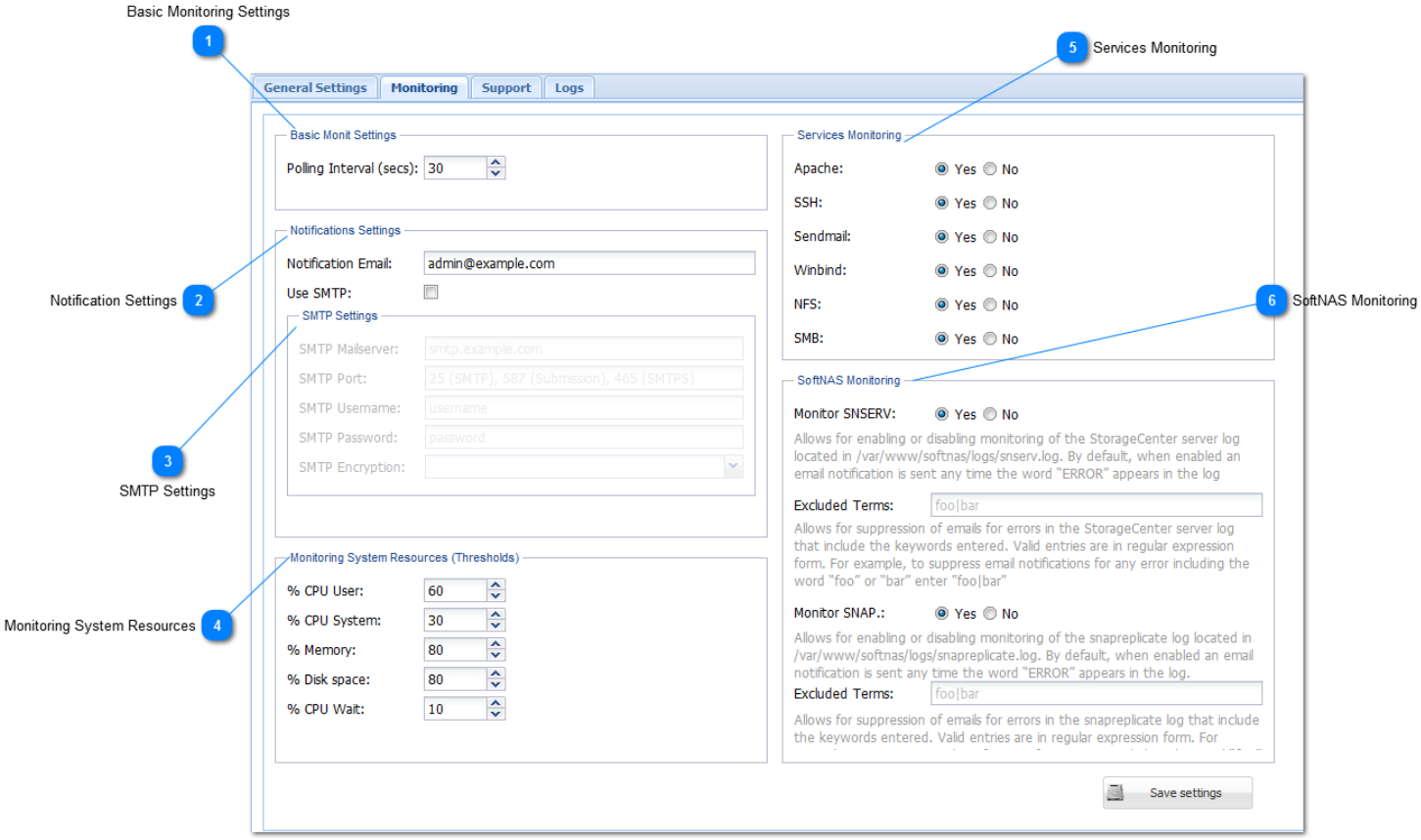
5 Other Settings

Other settings

The following other settings can be configured

Parameter	Description
Getting Started	Enables/disables the Getting Started panel from launching when logging into SoftNAS.
Welcome panel on start	Enables/disables Welcome panel when logging into SoftNAS.

Monitoring



1 Basic Monitoring Settings

Basic Monit Settings

SoftNAS performs monitoring of system resources, services and SoftNAS logging by polling the system based on the Polling Interval (secs). The default setting is 30 seconds.

2 Notification Settings

Notifications Settings

The Notification settings are used to specify the administrator email address that will be sent monitoring alerts. You can also send monitoring alerts to the corporate SMTP server.

3 SMTP Settings

SMTP Settings

If "Use SMTP" is enabled the following fields are available for the SMTP server configuration:

Field	Description

SMTP Mailserver	FQDN of the mail server.
SMTP Port	SMTP Port that will be used to send email notifications (25, 587, 465)
SMTP Username	Username required for SMTP server authentication
SMTP Password	Password required for SMTP server authentication.
SMTP Encryption	Encryption setting for the SMTP server connection. The following settings are possible: • SSLV2 • SSLV3 • TLSV1

4 Monitoring System Resources

Monitoring System Resources (Thresholds)

These thresholds control the percentage usage levels above which monitoring notifications will be issued. The following independant thresholds can be sent:

Parameter	Description
% CPU	Threshold setting above which a monitoring notification will be issued for the system resource.
%CPU System	Ibid.
% Memory	Ibid.
% Disk space	Ibid.
% CPU Wait	Ibid.

5 Services Monitoring

- Services Monitoring -

You can setup SoftNAS to monitor the core system services and issue monitoring notifications accordingly. The following services can be monitored by SoftNAS:

Parameter	Description
Apache	Apache web server service running on SoftNAS
SSH	secure shell service running on SoftNAS, enabling secure data communication.
Sendmail	Sendmail email routing facility running on SoftNAS.
Winbind	samba service running on SoftNAS which enables connections to domain controllers.

NFS	Distributed file system protocol running on SoftNAS.
SMG	Server Message Block service.

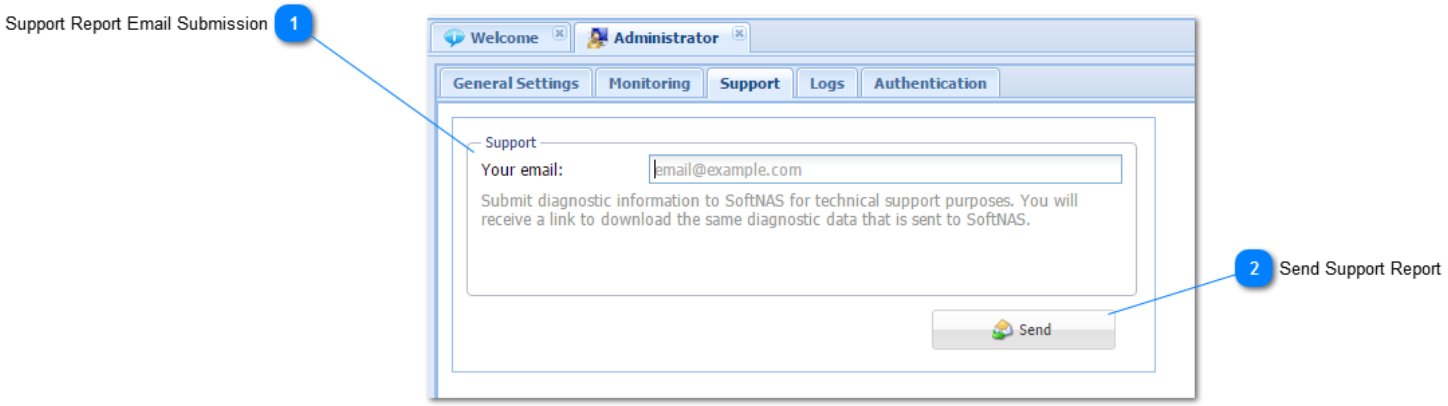
6 SoftNAS Monitoring

SoftNAS Monitoring

SoftNAS Monitoring can be used to monitor a variety of logs. By default, when enabled an email notification is sent any time the word “ERROR” appears in the log.

Parameter	Definition
Monitor SNSERV:	(Yes/No) Allows for enabling or disabling monitoring of the StorageCenter server log located in /var/www/softnas/logs/snserv.log. By default, when enabled an email notification is sent any time the word “ERROR” appears in the log
Excluded Terms	Allows for suppression of emails for errors in the StorageCenter server log that include the keywords entered. Valid entries are in regular expression form. For example, to suppress email notifications for any error including the word “foo” or “bar” enter "foo|bar"
Monitor SNAP	(Yes/No) Allows for enabling or disabling monitoring of the snapreplicate log located in /var/www/softnas/logs/snapreplicate.log. By default, when enabled an email notification is sent any time the word “ERROR” appears in the log.
Excluded Terms	Allows for suppression of emails for errors in the snapreplicate log that include the keywords entered. Valid entries are in regular expression form. For example, to suppress email notifications for any error including the word “foo” or “bar” enter "foo|bar"

Support Tab



1 Support Report Email Submission

Your email: email@example.com

By providing your email address in the space above, a copy of the support report received by SoftNAS support will also be sent to you, to allow you to participate in the support process, and have on hand a frame of reference for a given solution or explanation.

2 Send Support Report

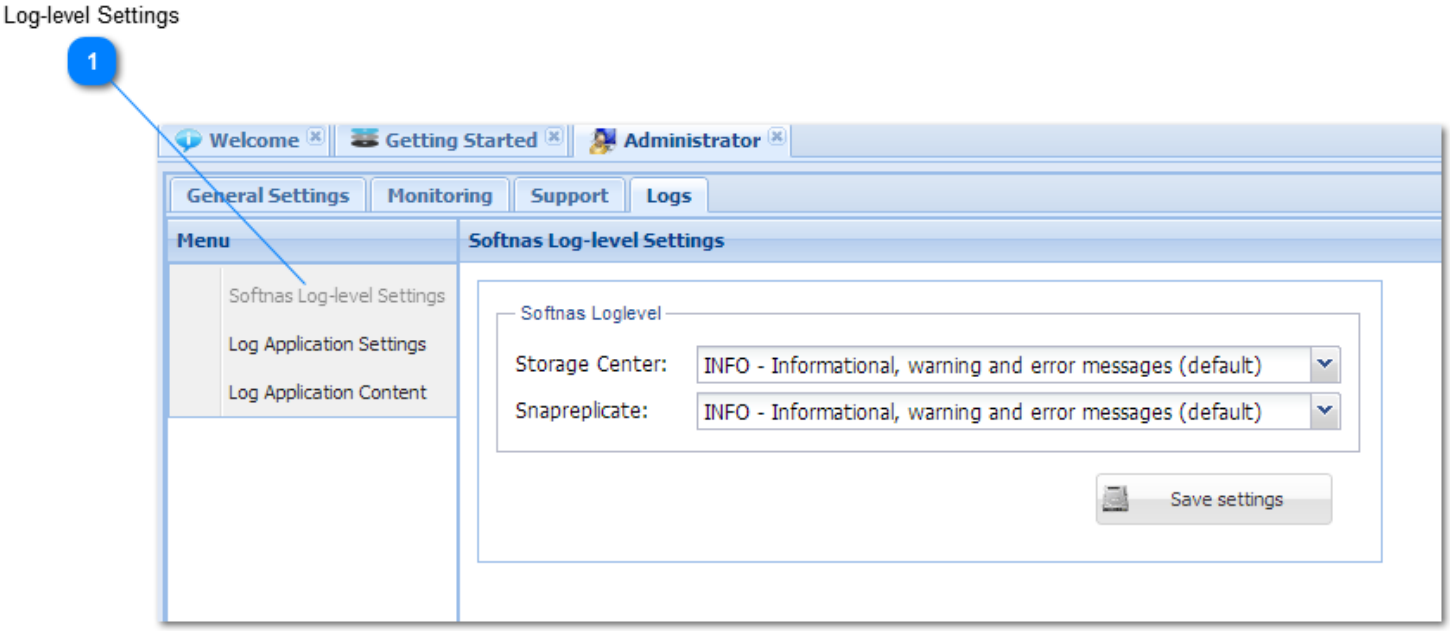
Send

Click send to send your support logs to SoftNAS support.

Note: You can also generate a support report via command line, either through SoftNAS' Command Shell (accessed via **General System Settings**, and the Webmin Panel, and expanding **Others**) or by connecting to your instance via SSH, and running the following command:

```
su -l root -c "curl https://www.softnas.com/getsupport/ | php --
ticket-3606@softnas.com"
```

Logs



1 Log-level Settings

Softnas Log-level Settings

Log Level Settings enable you to set the logging verbosity for the **SoftNAS StorageCenter** software and its modules (eg. **SnapReplicate).** You can configure separate logging verbosity evels for each module that is available from this page.

The following settings are possible:

DEBUG - Debug, informational, warning and error messages (all messages)

INFO - Informational, warning and error messages (default)

WARN - Warning and error messages

ERROR - Error messages only

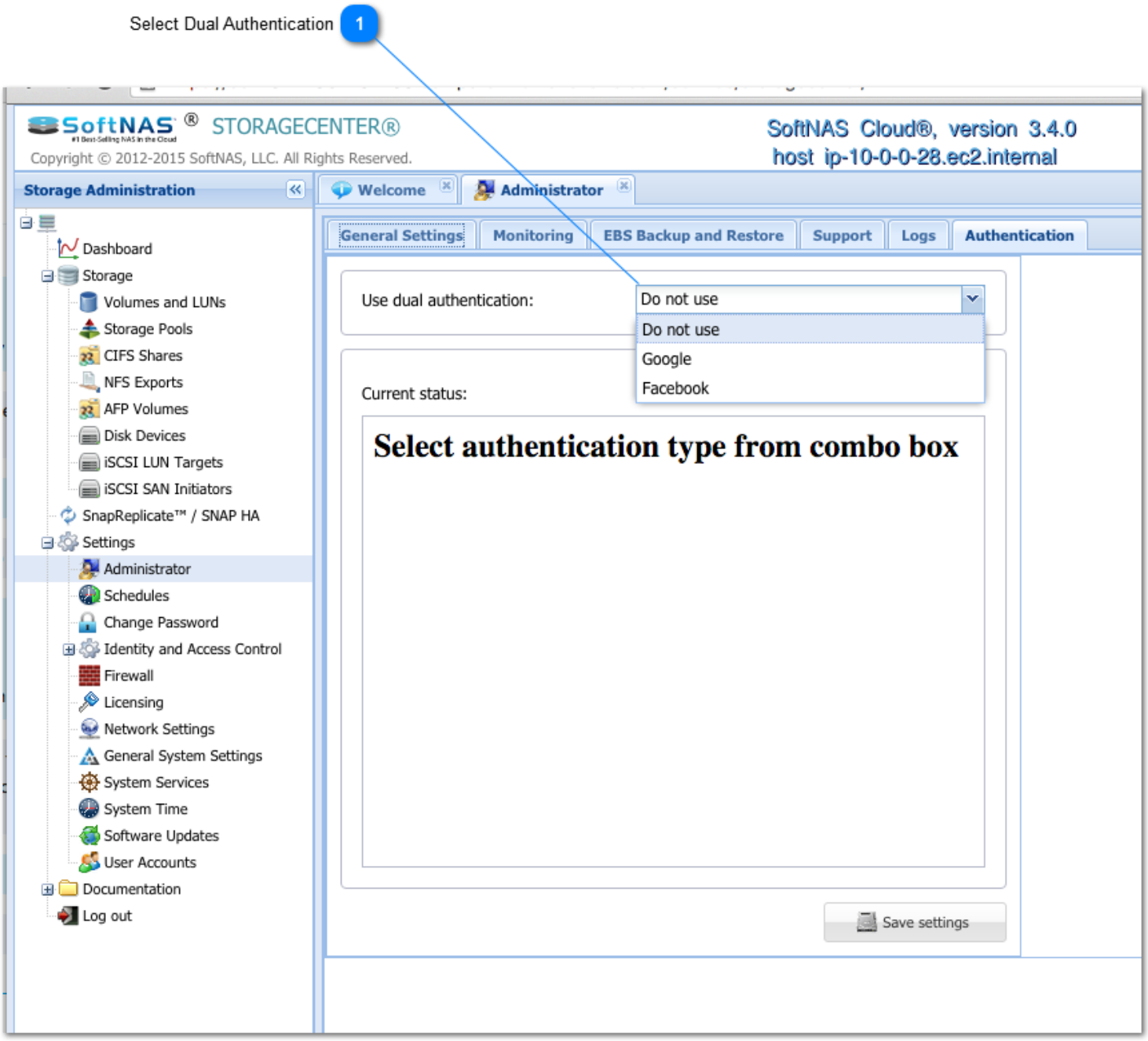
FATAL - Fatal messages only

OFF - No messages (not recommended)

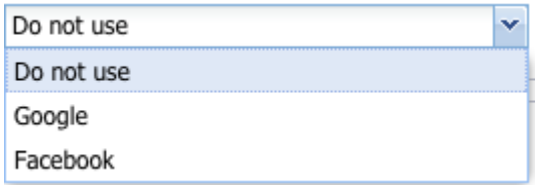
Log level settings can be set for the following:

Parameter	Description
StorageCenter	Setting which determines logging verbosity for the indicated service/ module.
SnapReplicate	Ibid.

Authentication

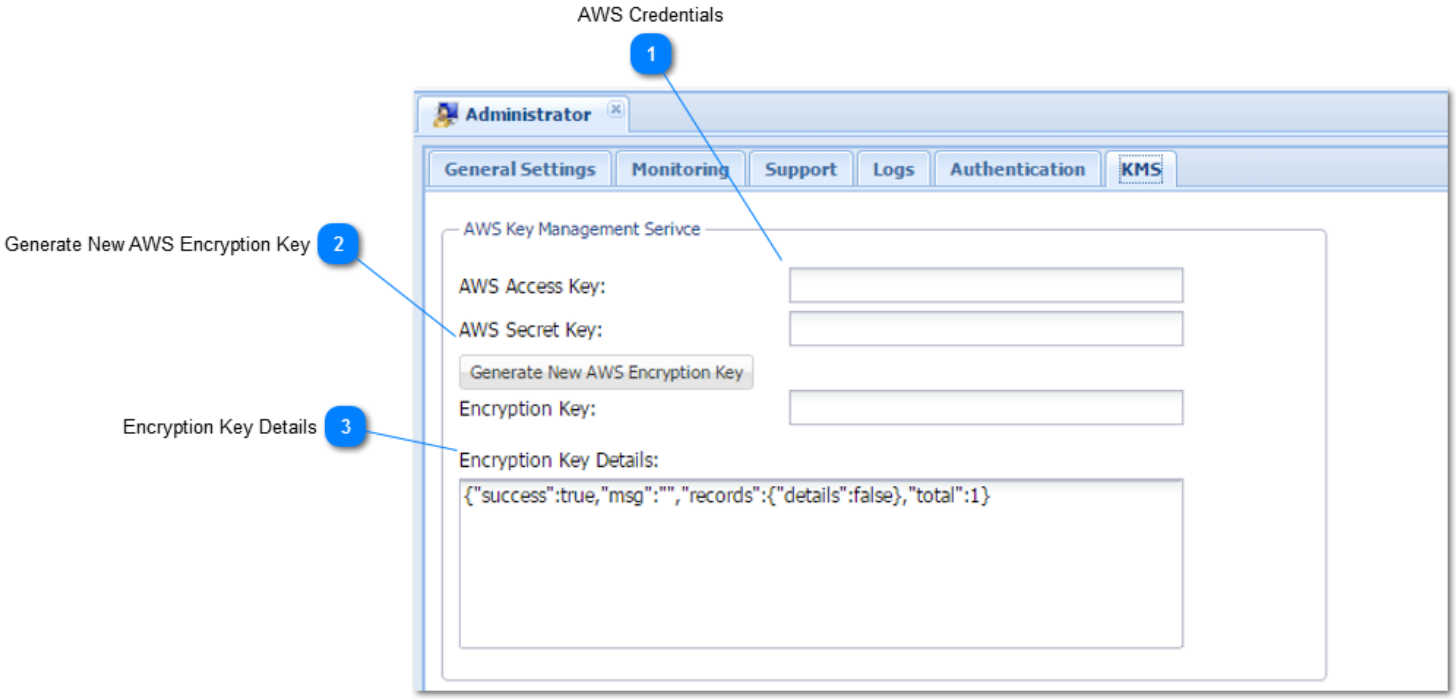


1 Select Dual Authentication



SoftNAS supports authentication via Google or Facebook, in order to provide the improved security of dual authentication. By requiring both SoftNAS credentials and your selected social media account credentials to authenticate, your login security is improved, while simultaneously making repeated sign-ins simpler. Your Google or Facebook credentials allow you to login to a saved session and by-pass the login screen through cached credentials.

Key Management System (KMS)



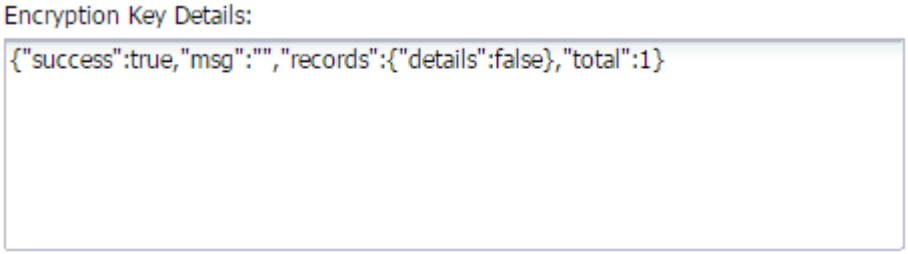
1 AWS Credentials

Provide your AWS credentials here. In order to enable encryption for an AWS instance, your credentials must be verified.

2 Generate New AWS Encryption Key

Users can generate a new random encryption key by pressing the button above.The key will display in the box below. Alternatively, users can enter their own personal encryption key in the field provided. If creating your own encryption key, keep it secure by ensuring adequate length and complexity.

3 Encryption Key Details

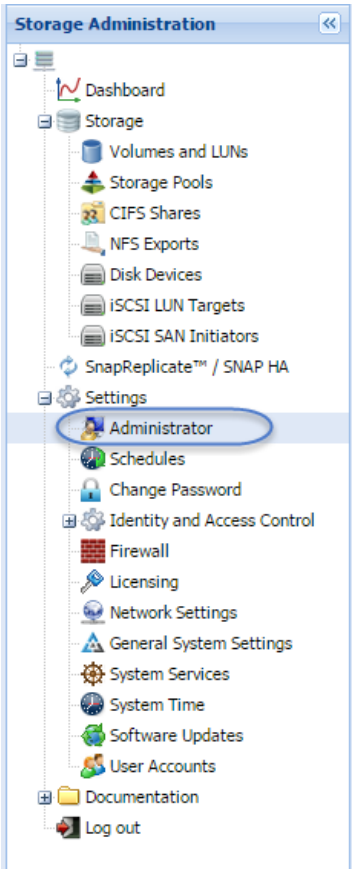


Encryption Key Details allows you to review the details of your attempt to set up AWS encryption, providing a summary of the attempt and listing any errors that occurred in your process, if applicable.

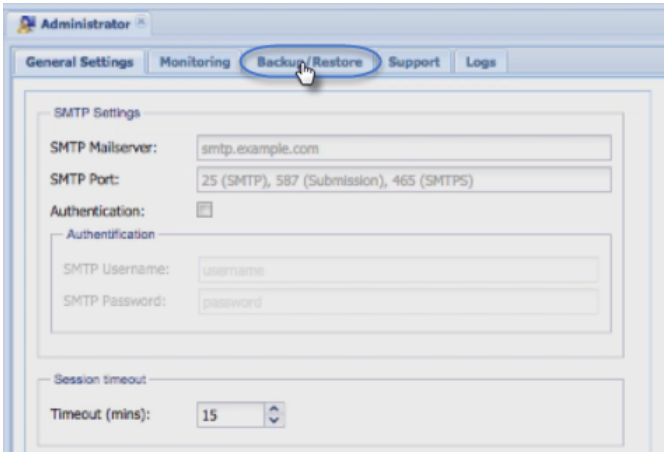
Configuring Consistent Backup and Restore

In Amazon Web Services, it is possible to set up Consistent Backup and Restore. To do so, perform the following steps:

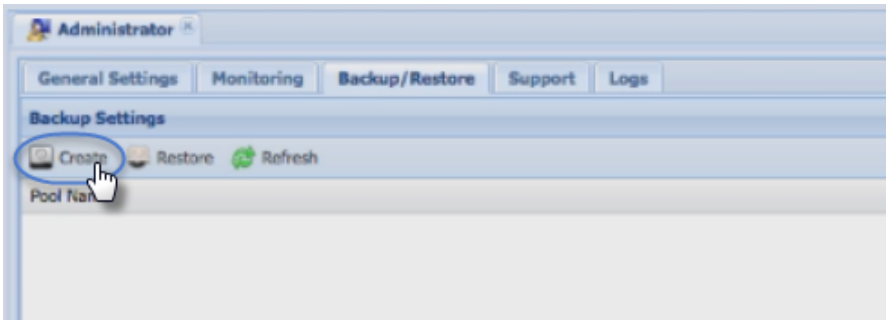
1. In order to configure consistent backup and restore within SoftNAS StorageCenter, navigate down to **Settings** in the left **Storage Administrator** pane, and select **Administrator**.



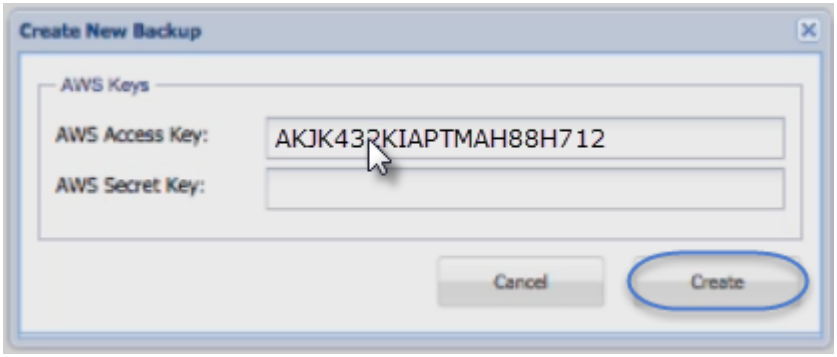
2. The **Administrator** panel will open. Within the panel, select the **Backup/Restore** tab.



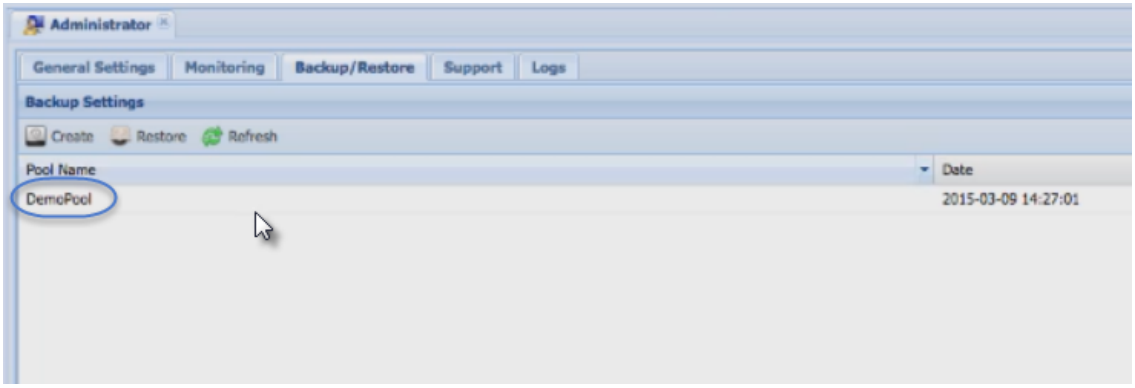
3. In the **Backup/Restore Tab**, select **Create**.



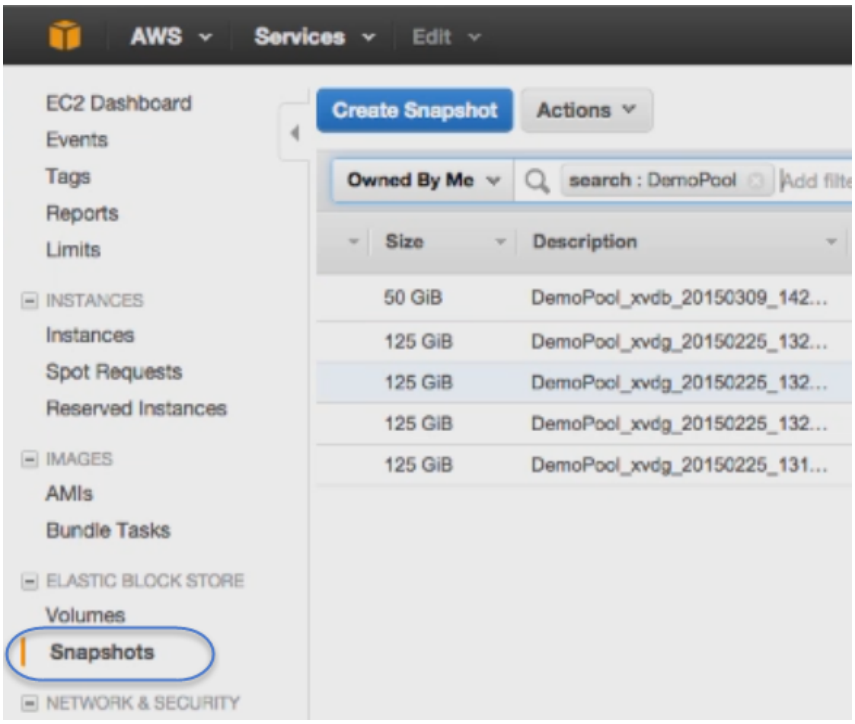
4. A dialog box will appear center screen, requesting verification via your AWS credentials. Enter your credentials. Click **Create** when done.



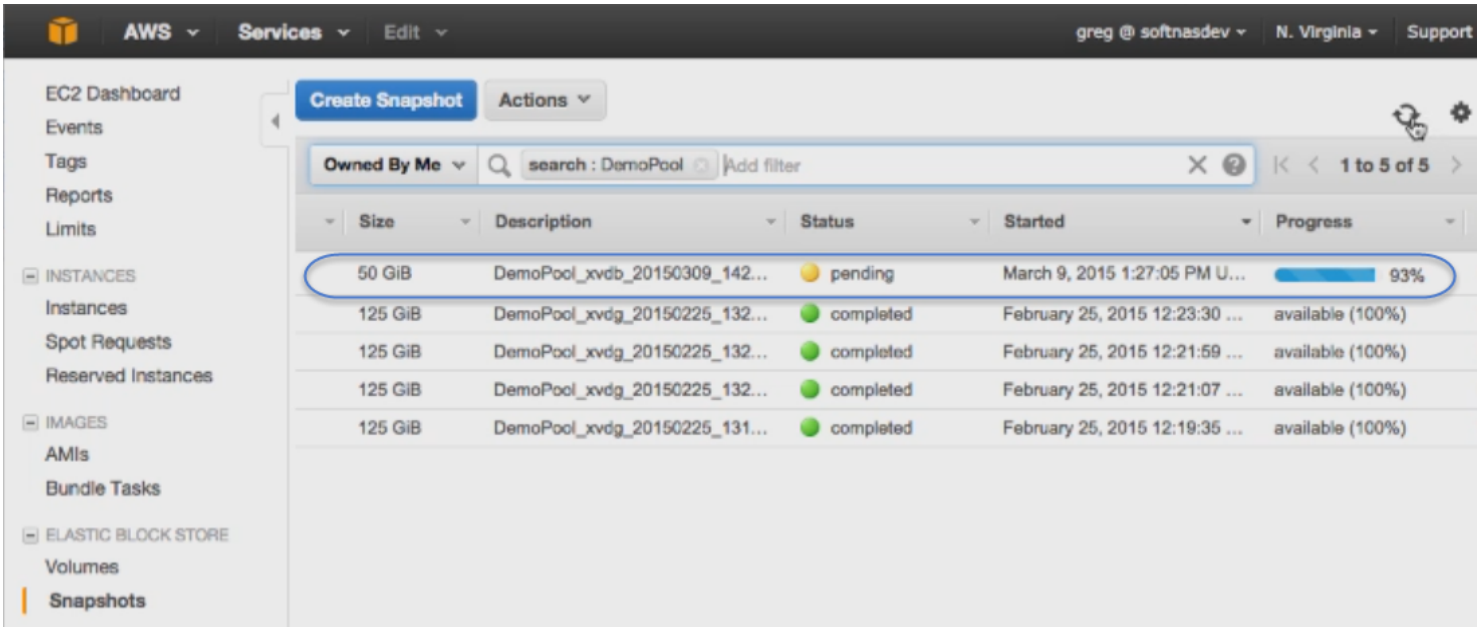
5. A progress bar will appear, notifying you when this step is complete. The backup will be created, defaulting to a name of "DemoPool".



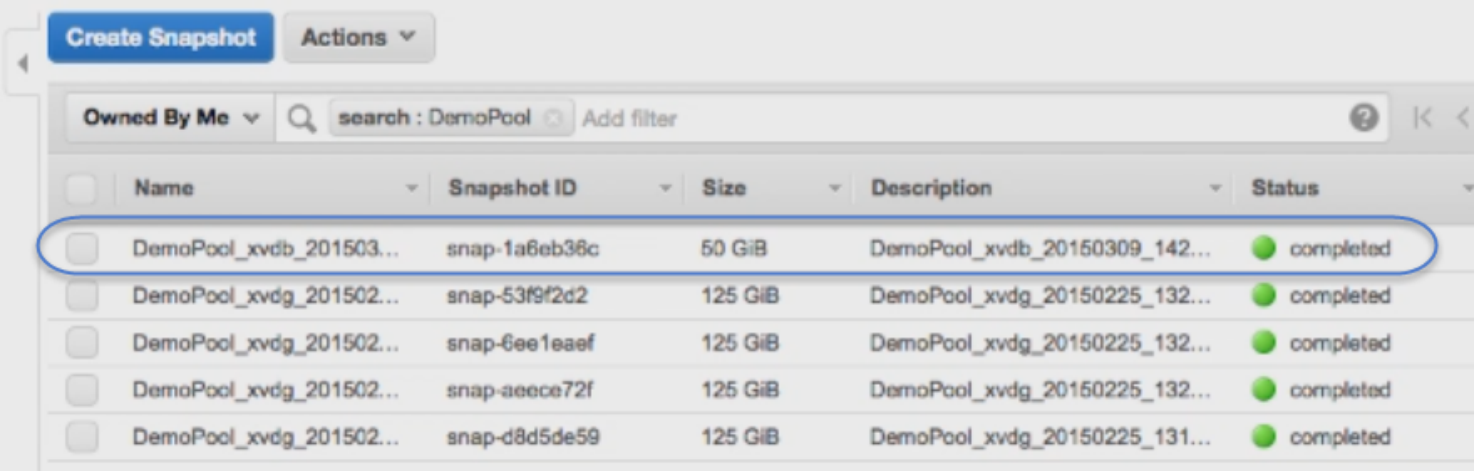
6. Next, open the AWS console, and go to **Snapshots** under **Elastic Blockstore** in the left **Administration** pane.



7. Confirm that your snapshot has been (or is being) created within the AWS Console.



8. Once complete, you have set up Consistent Backup and Restore for AWS.



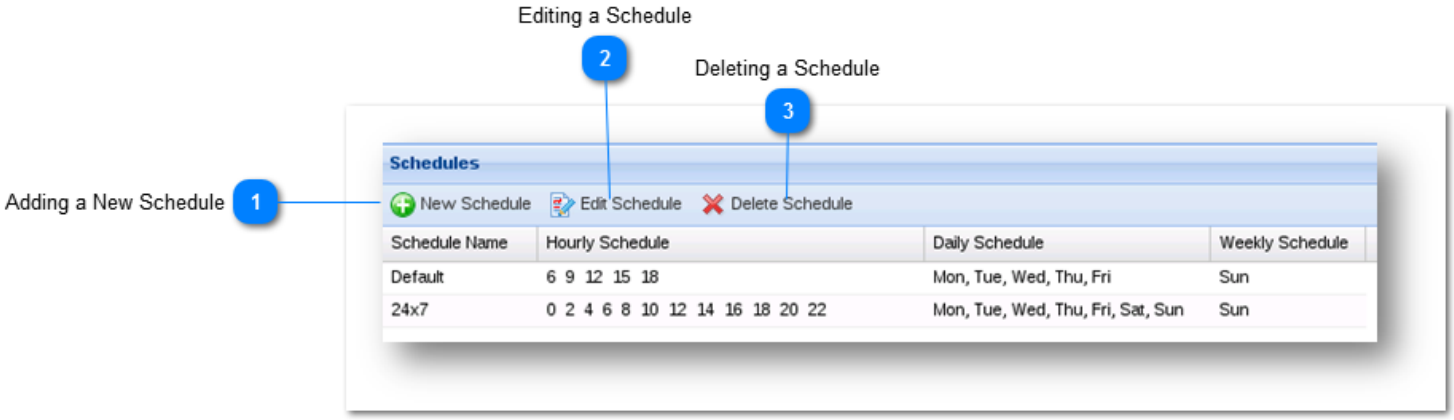
Managing Schedules

SoftNAS includes a task scheduler, used to execute various tasks on a periodic basis; e.g., scheduled snapshots, scheduled replication, etc.

A **schedule** is a definition of when and how often tasks should run. A task, such as a scheduled volume snapshot, is assigned a schedule on which the task will run. For example, a volume can be assigned to have snapshots taken on the **Business** schedule (e.g., Mon-Fri at certain hours during the business day, but not on weekends).

1. Navigate to **Settings > Schedules.**

The **Schedules** panel will be displayed.



Column Name	Description
Schedule Name	Name of the schedule
Hourly Schedule	Shows which hours of the day the schedule is configured to execute.
Daily Schedule	Shows the days of the week the daily schedule runs.
Weekly Schedule	Shows the day of the week for the weekly tasks.

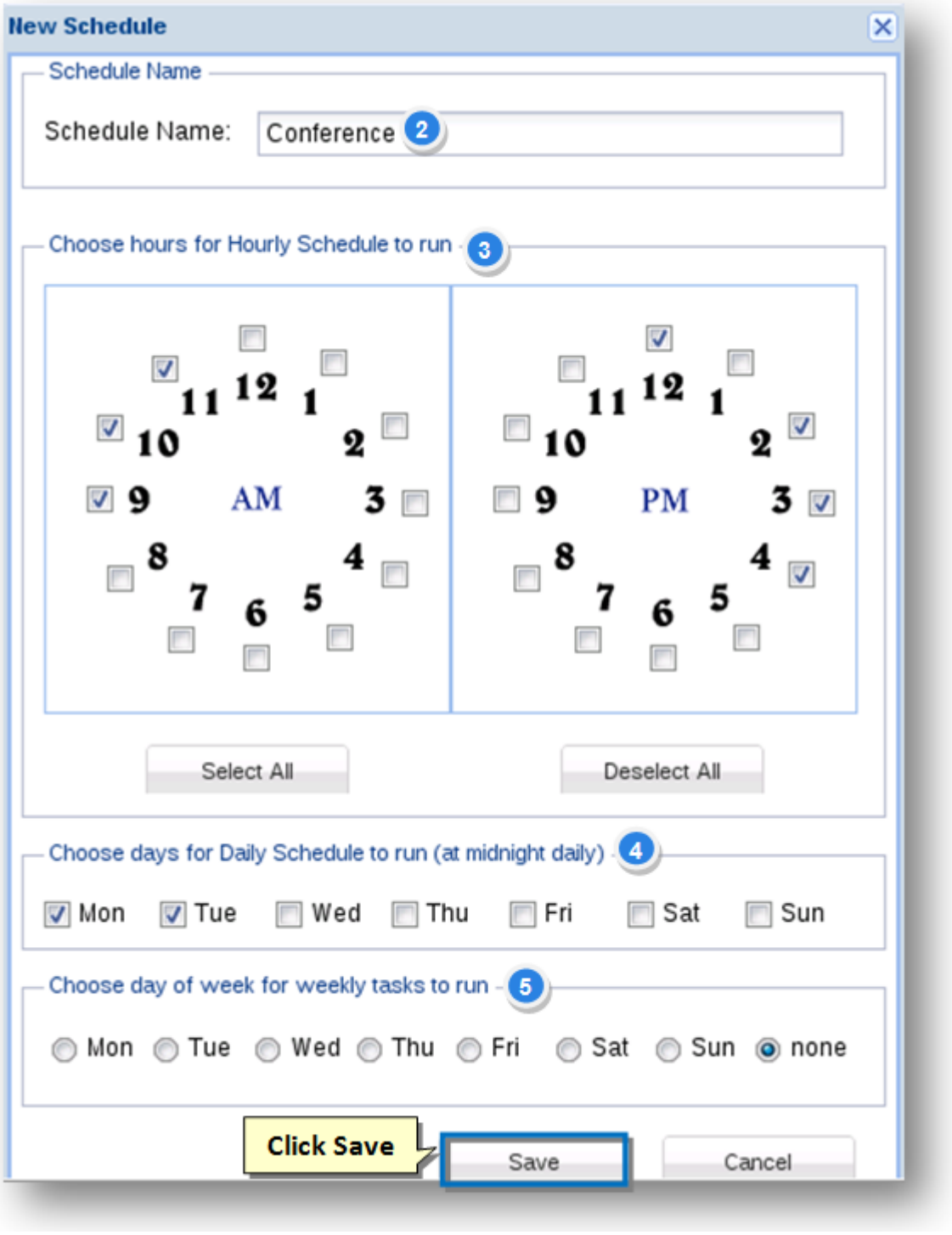
1 Adding a New Schedule

You can configure scheduled tasks to take place on an hourly, daily and/or weekly basis.

Adding a new schedule is very easy. Simply follow the steps given below.

1. On the **Schedules** panel, click the **New Schedule** button.

The **New Schedule** dialog will be displayed.



2. Enter the name of the schedule in the **Schedule Name** text entry box. Names must begin with an alphabetical character and contain any combination of upper and lower case alphanumeric.

3. In the **Choose Hours for Hourly Schedule to Run** on section, select the hours of the morning schedules in the **AM Clock** to the left and the hours of the afternoon and evening schedules in the **PM Clock** to the right.

Note: To select all 24 hours, click the **Select All** button. To unselect all selected hours, click the **Deselect All** button.

4. In the **Choose Days for Daily Schedule to Run** section, check the boxes in the required days for daily schedules.

5. Similarly, In the **Choose Days of Week for Weekly Tasks to Run** section, check the boxes in the required days for weekly schedules.

6. Click the **Save** button.

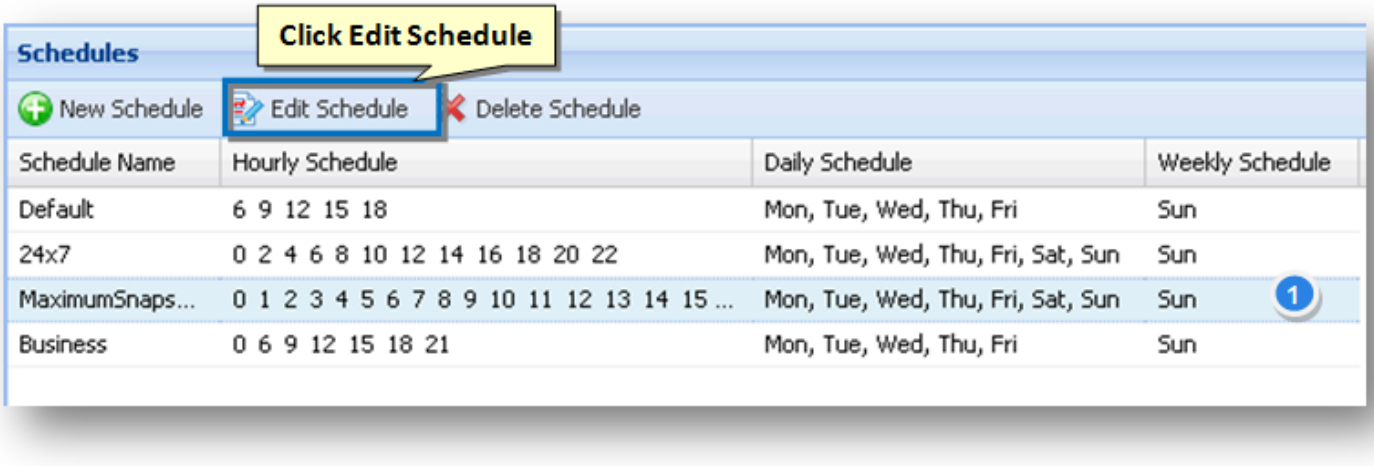
The new schedule will be added.

2 Editing a Schedule

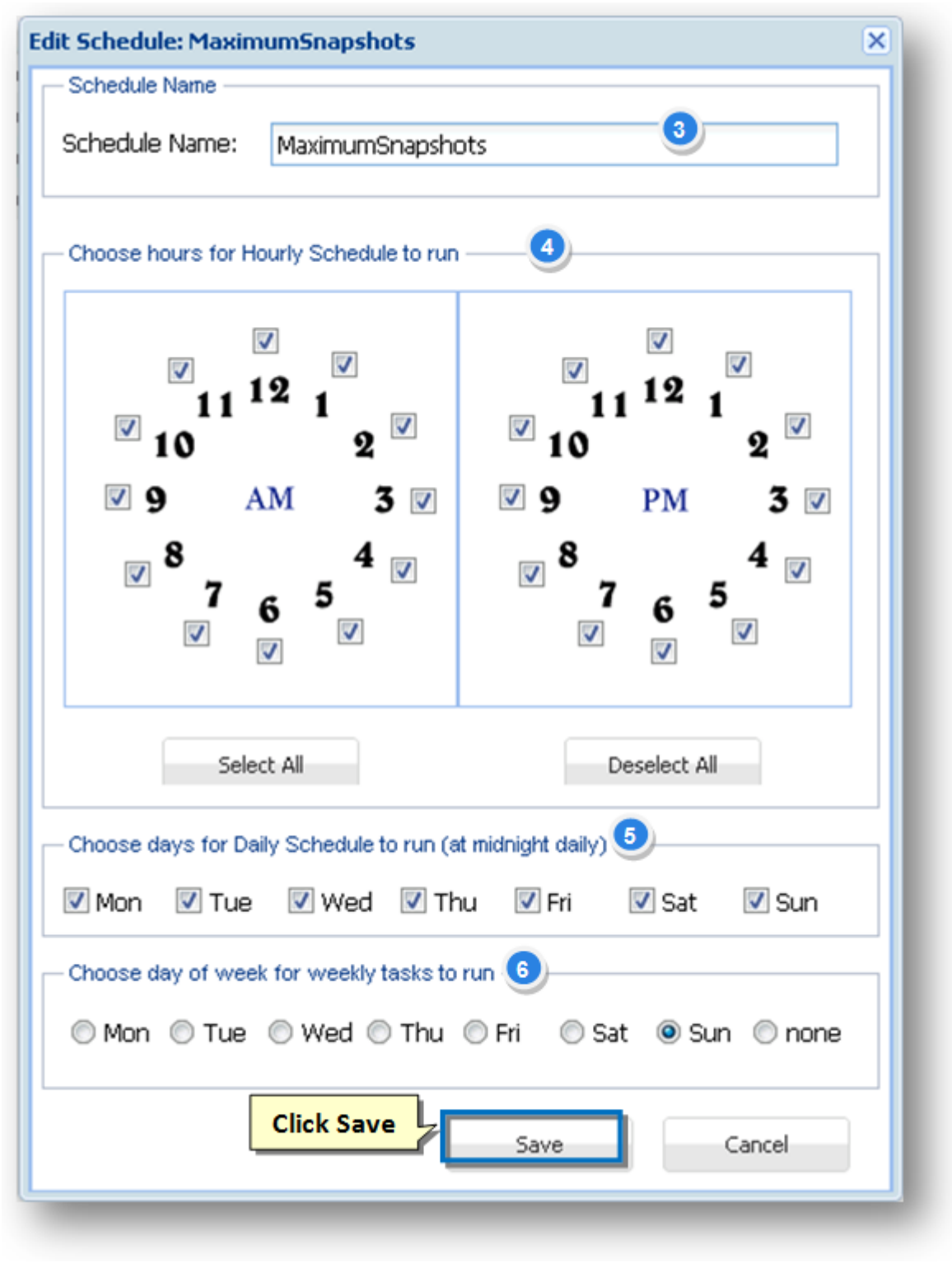
Editing a Schedule is very easy. Simply follow the steps given below.

1. On the **Schedules** panel, select the schedule that you wish to edit.

2. Click the **Edit Schedule** button.



The selected schedule will be displayed in edit mode.



3. Edit the name of the schedule in the **Schedule Name** text entry box. Names must begin with an alphabetic contain any combination of upper and lower case alphanumeric.

4. In the **Choose Hours for Hourly Schedule to Run** on section, edit the selected hours of the morning sche **Clock** to the left and the hours of the afternoon and evening schedules in the **PM Clock** to the right.

Note: To select all 24 hours, click the **Select All** button. To unselect all selected hours, click the **Deselect All** b

3. In the **Choose Days for Daily Schedule to Run** section, check the boxes in the required days for daily sch

4. Similarly, In the **Choose Days of Week for Weekly Tasks to Run** section, check the boxes in the required schedules.

5. Click the **Save** button.

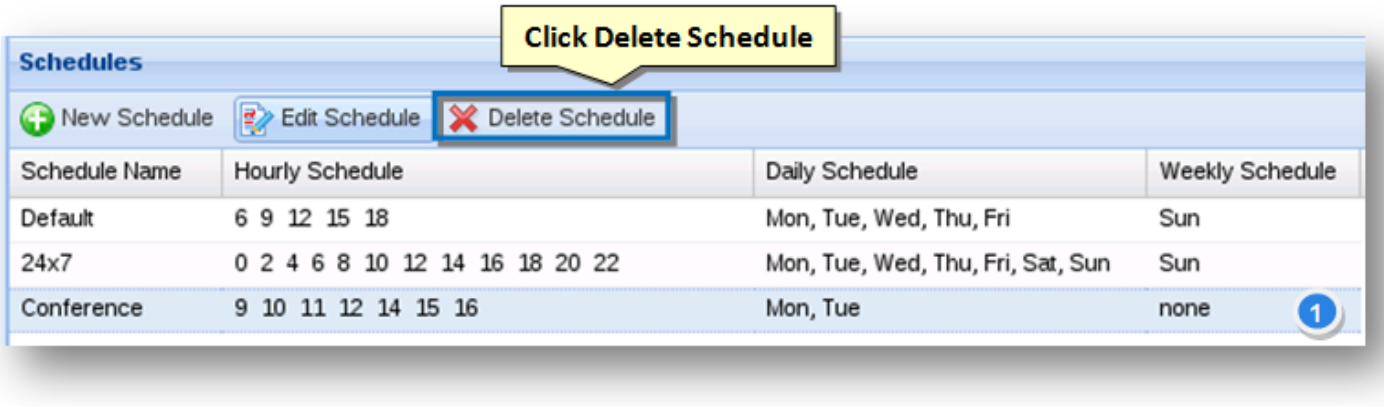
The changes made to the selected schedule will be updated.

3 Deleting a Schedule

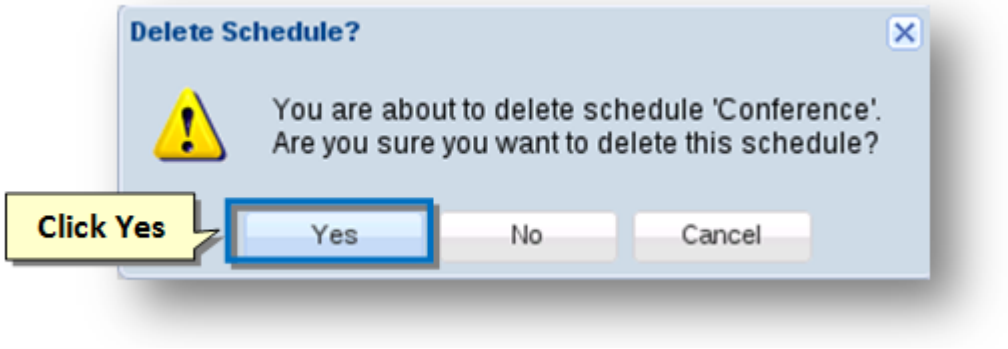
Deleting a Schedule is very easy. Simply follow the steps given below.

1. On the **Schedules** panel, select the schedule that you wish to edit.

2. Click the **Delete Schedule** button.



The **Delete Schedule** message box asking you to confirm the deletion of the schedule will be displayed.



3. Click the **Yes** button.

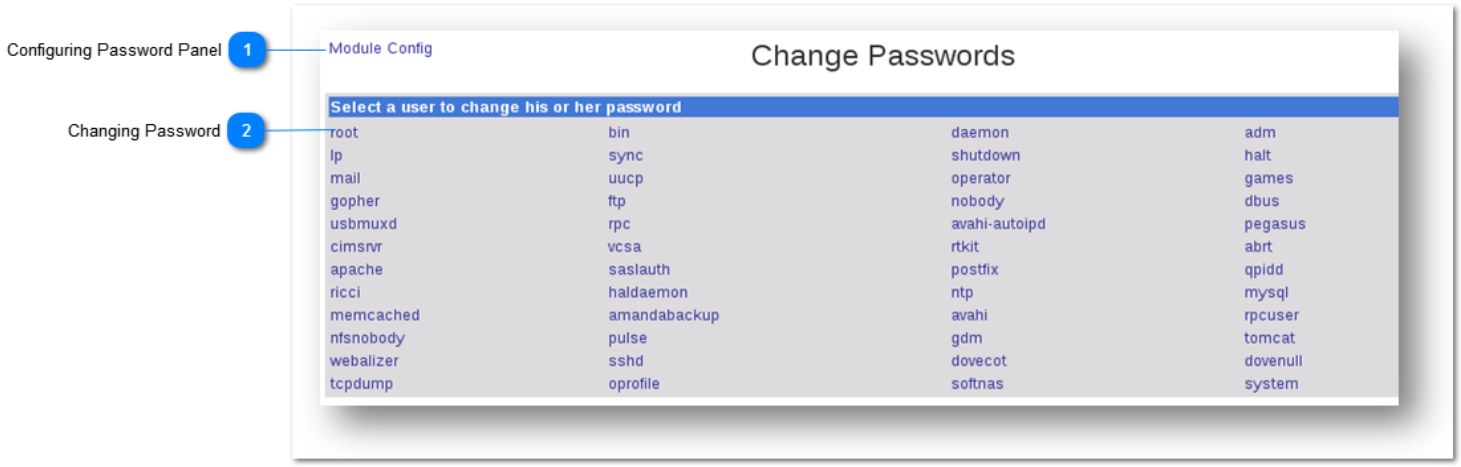
The selected schedule will be removed.

Managing Passwords

You can configure and manage all users's passwords from **Passwords** panel.

1. To do so, navigate to **Settings >Change Password.**

The **Change Passwords** panel will be displayed.

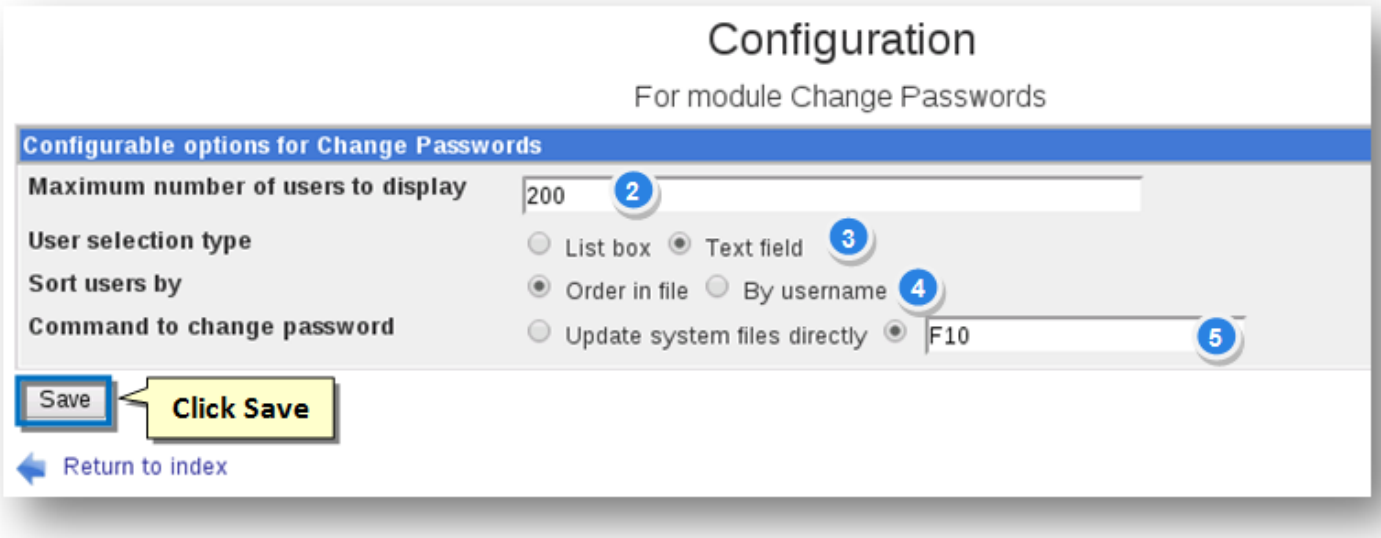


1 Configuring Password Panel

You can configure **Password** panel to display the number of users on the screen and also other user related s

1. On the **Passwords** panel, click the **Module Config** button.

The **Configuration for Change Passwords** section of the panel will be displayed.



2. Enter the maximum number of users to be displayed on the panel, in the text entry box.

3. Specify the type with which the users can be selected on the panel in the **User Selection Type** field. The a
are **List box** and **Text field.**

4. Specify the sort order for the users in the **Sort Users By** field. The available options are **Order in File** and

5. Specify the command to change the password by selecting the appropriate option. The available options a **System Files Directly** and text box for entering the command.

6. Click the **Save** button.

The changes made to the **Change Passwords** module will be updated.

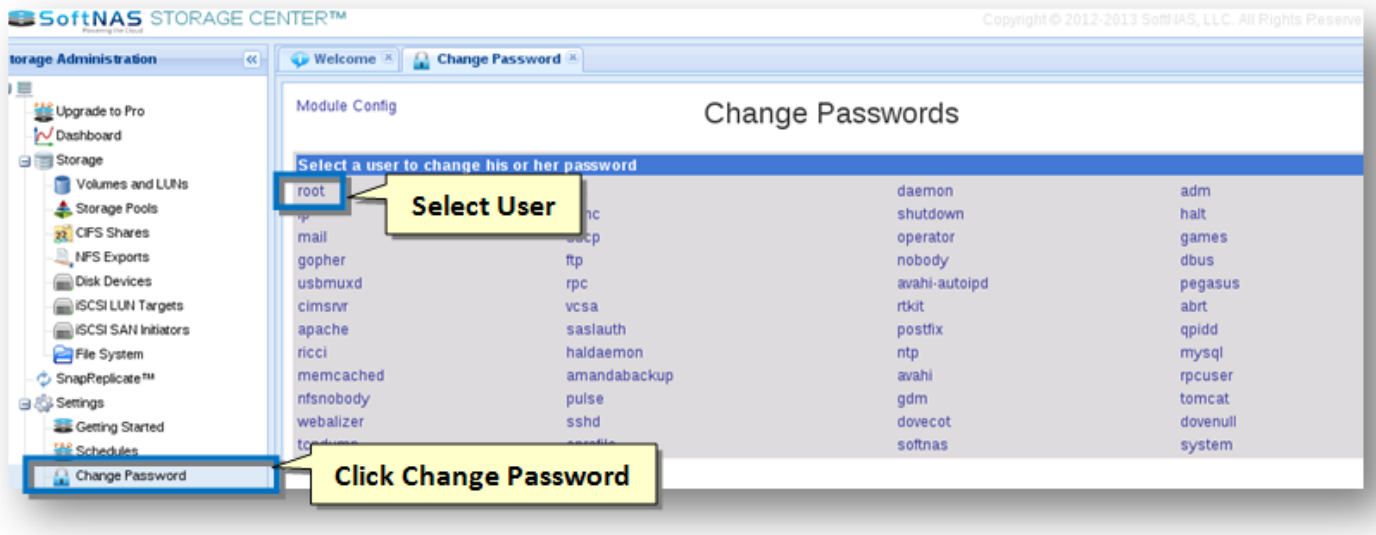
2 Changing Password

When you log in to the **SoftNAS StorageCenter** for the first time, you will use the super-user login credentials **softnas** as users and **Pass4W0rd** (that's zero) as system default password.

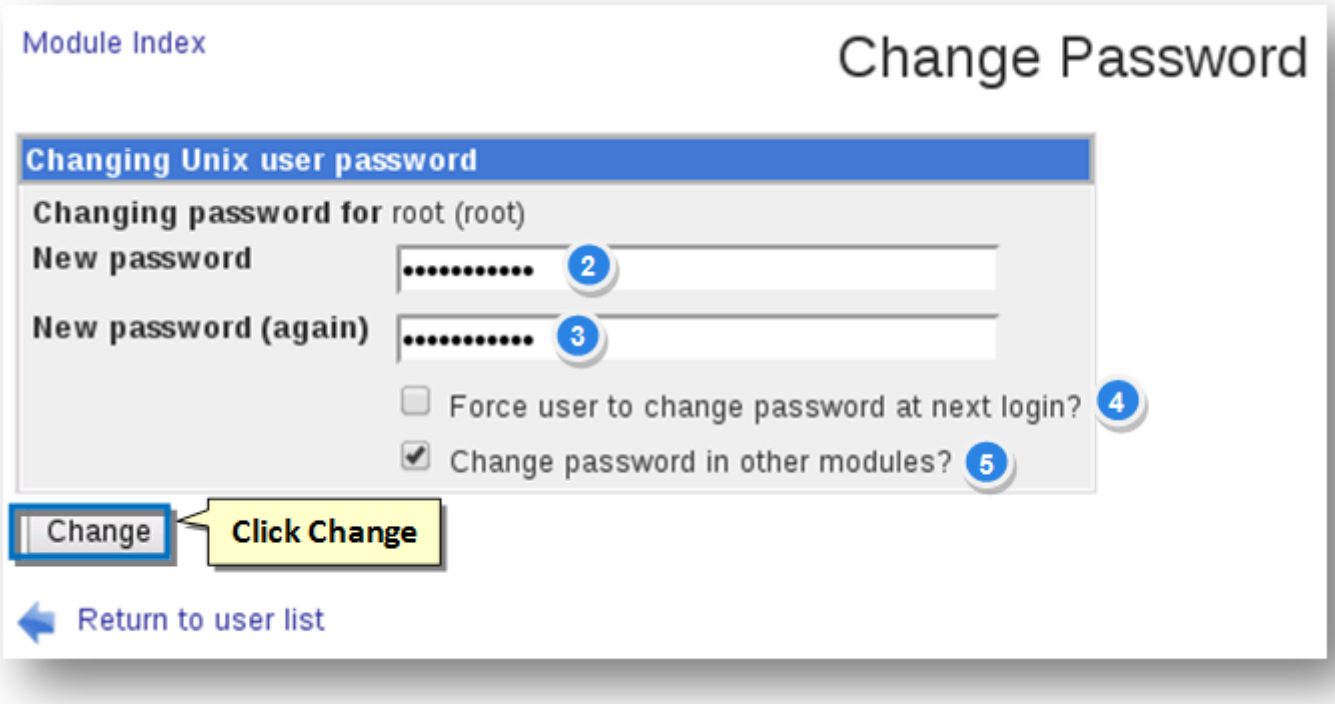
For security reasons, it is recommended to change these passwords to unique, secure passwords to increase important data managed by **SoftNAS.**

Changing the password is very easy. Simply follow the steps given below.

1. On the **Passwords** panel, select the user whose password is to be changed.



The **Changing Unix User Password** section will be displayed.



2. Enter the new password in the **New Password** text entry box.
3. Confirm the password by re-entering it in the **New Password (Again)** text entry box.
4. Check this box if you want to force the user to change the password when he logs on to the system next tin
5. Check this box if you wan to enforce the change of password in other modules also.
6. Click the **Change** button.

The password of the selected user will now be changed and he/she can now log on to the system with the new

Note: Do not change the password for the user **system.** This is a special, no-login service account used by W for internal authentication between **SoftNAS** running in Apache and the Webmin service.

Identity and Access Control

You can use Identity and Access Control to configure the following:

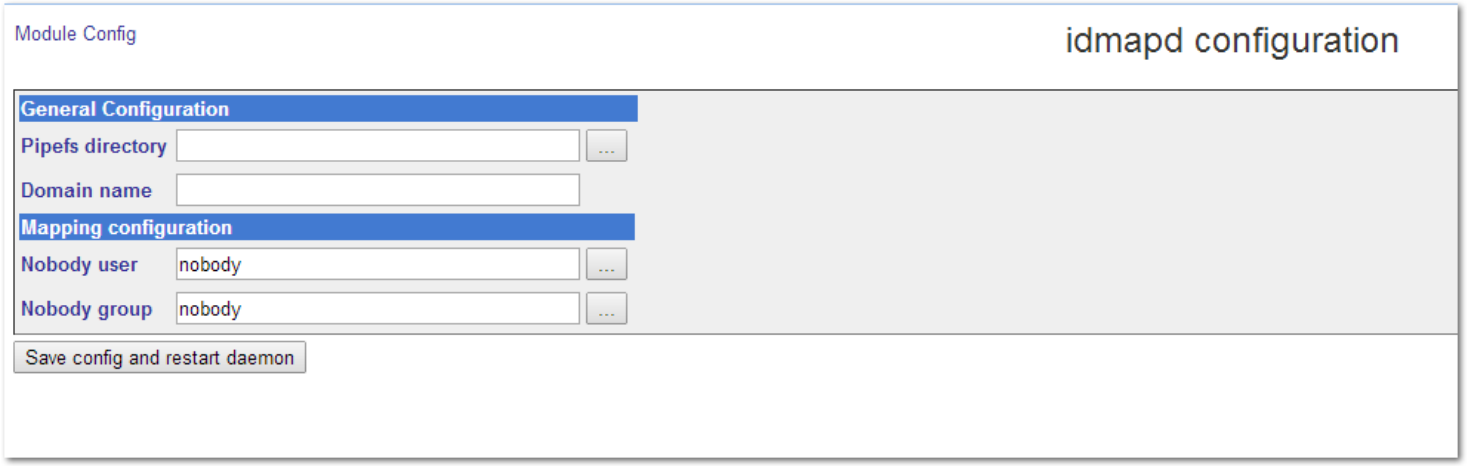
idmapd configuration

LDAP Server

LDAP client

Kerberos

idmapd configuration



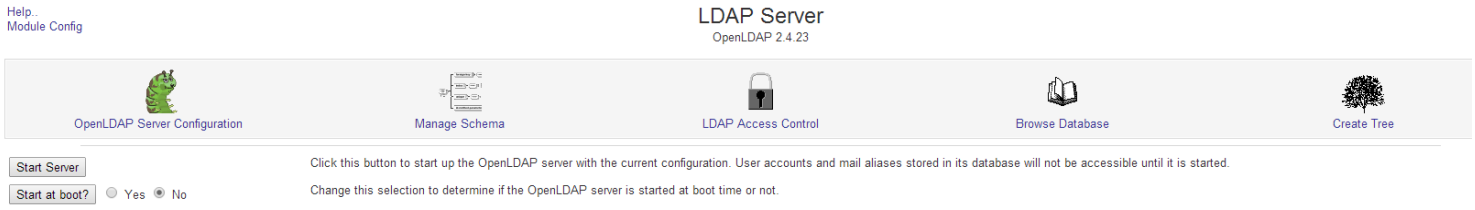
The idmapd.conf configuration file consists of several sections, initiated by strings of the form [General] and [Mapping]. Each section may contain lines of the form

Parameter	Definition
Pipefs directory	LDAP server directory.
domain name	The local NFSv4 domain name. An NFSv4 domain is a namespace with a unique username<->UID and groupname<->GID mapping. (Default: Host's fully-qualified DNS domain name)
Nobody user	Local user name to be used when a mapping cannot be completed.
Nobody group	Local group name to be used when a mapping cannot be completed.

LDAP Server

LDAP Server enables the configuration of the fields of the LDAP configuration.

SoftNAS provides support for NFSv4 Kerberos and LDAP Support, which enables multi-user security access rights to files and directories managed by the **SoftNAS** filer.



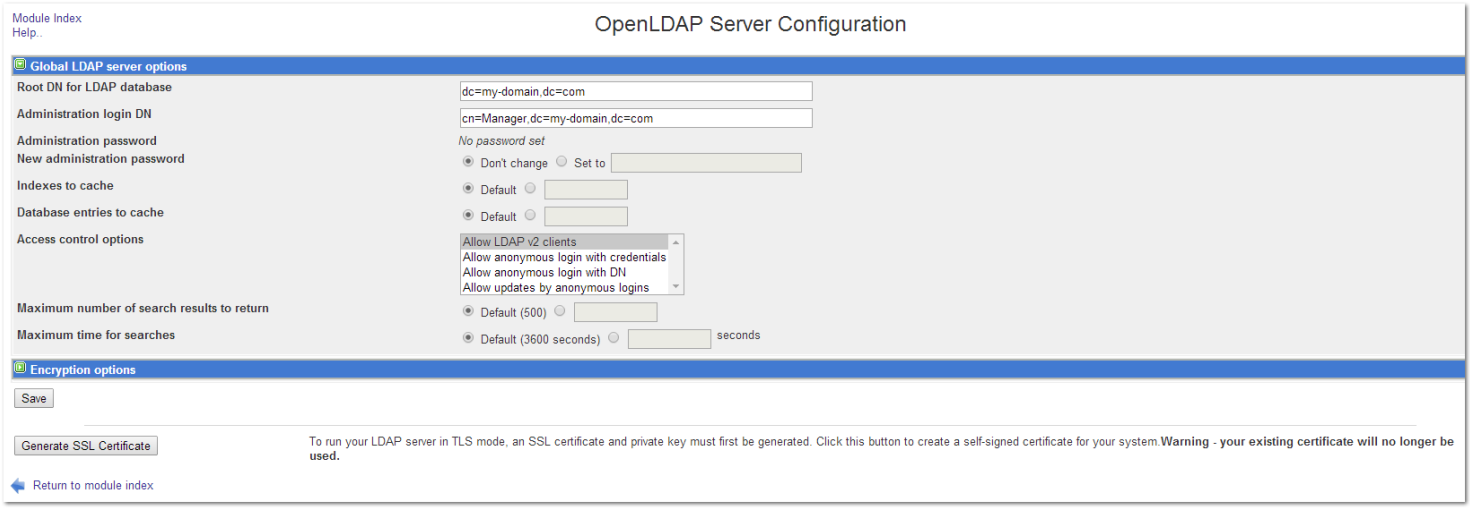
[OpenLDAP Server Configuration]

[Manage Schema]

[LDAP Access Control]

[Create Tree]

OpenLDAP Server Configuration



LDAP Server configuration allows the establishment of a connection between **OpenLDAP** and domain users.

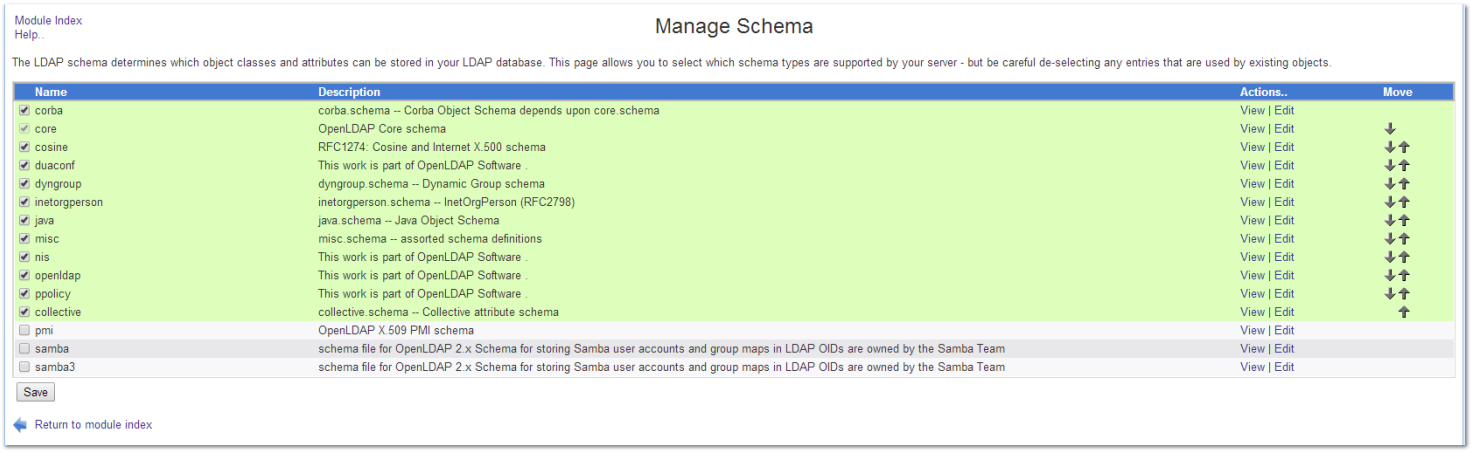
Parameter	Description
Root DN for LDAP database	The domain of the local domain controller that hosts the users. The directory starts out completely empty, without even a root structure present. Initializing the directory with a root record and other supporting directory sub-structures (i.e., sub-directories) is required before adding any user data.
Administration login DN	By default, Active Directory does not allow anonymous LDAP connections. To change this, to enter the DN of a user that's allowed to connect to the server and read all user and group data. Unless a special user account has already been created for this purpose, an easy choice is to use the built-in administrator account. By default, the administrator DN is in the form cn=Administrator,dc=<Local Domain>.
Administration password	Existing Administration password.
New administration password	Create a new password for OpenLDAP directory management.
Indexes to cache	Number of indexes to cache to improve performance tuning for user lookups.
Database entries to cache	Number of database entries to cache to improve performance tuning for user lookups.

Access control options	Setting which determines access control setting between SoftNAS and the LDAP server.
Maximum number of search results	Max. number of search results for user lookups.
Maximum time for searches	Max. amount of time for user lookup searches.

Encryption Options

Encryption options enables generation of an SSL Certificate. It enables the creation of a self-signed certificate for the LDAP system.

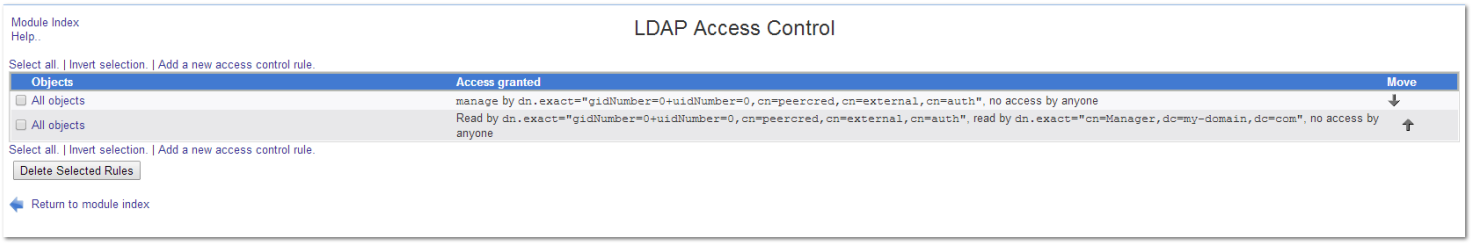
Manage Schema



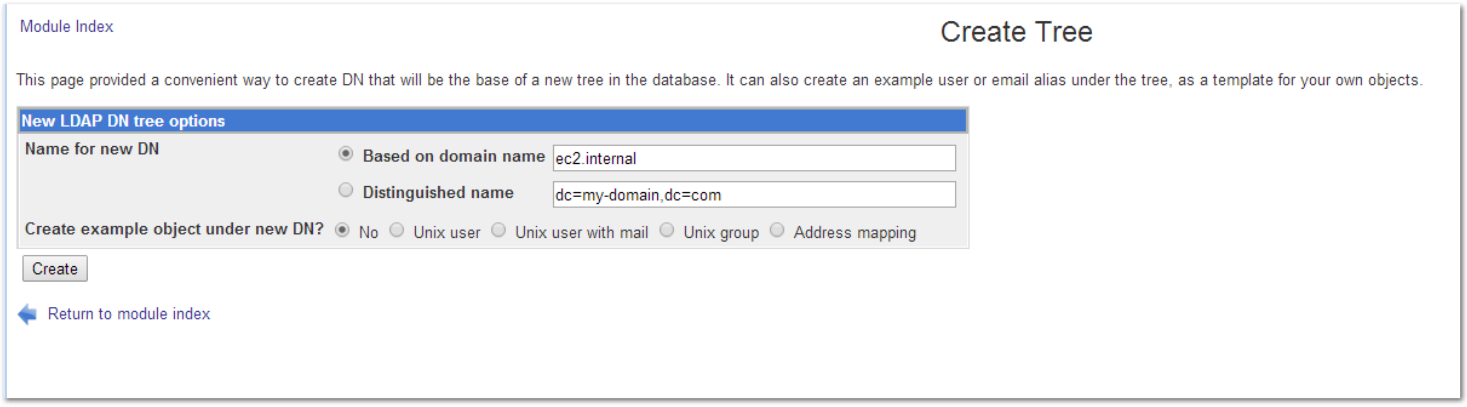
The LDAP schema determines which object classes and attributes can be stored in the LDAP database. This page allows administrators to decide which schema types are supported by the server - but be careful de-selecting any entries that are used by existing objects.

LDAP Access Control

Grant different access permissions on a per Object basis.



Create Tree



This page provided a convenient way to create DN that will be the base of a new tree in the database. It can also create an example user or email alias under the tree as an object template.

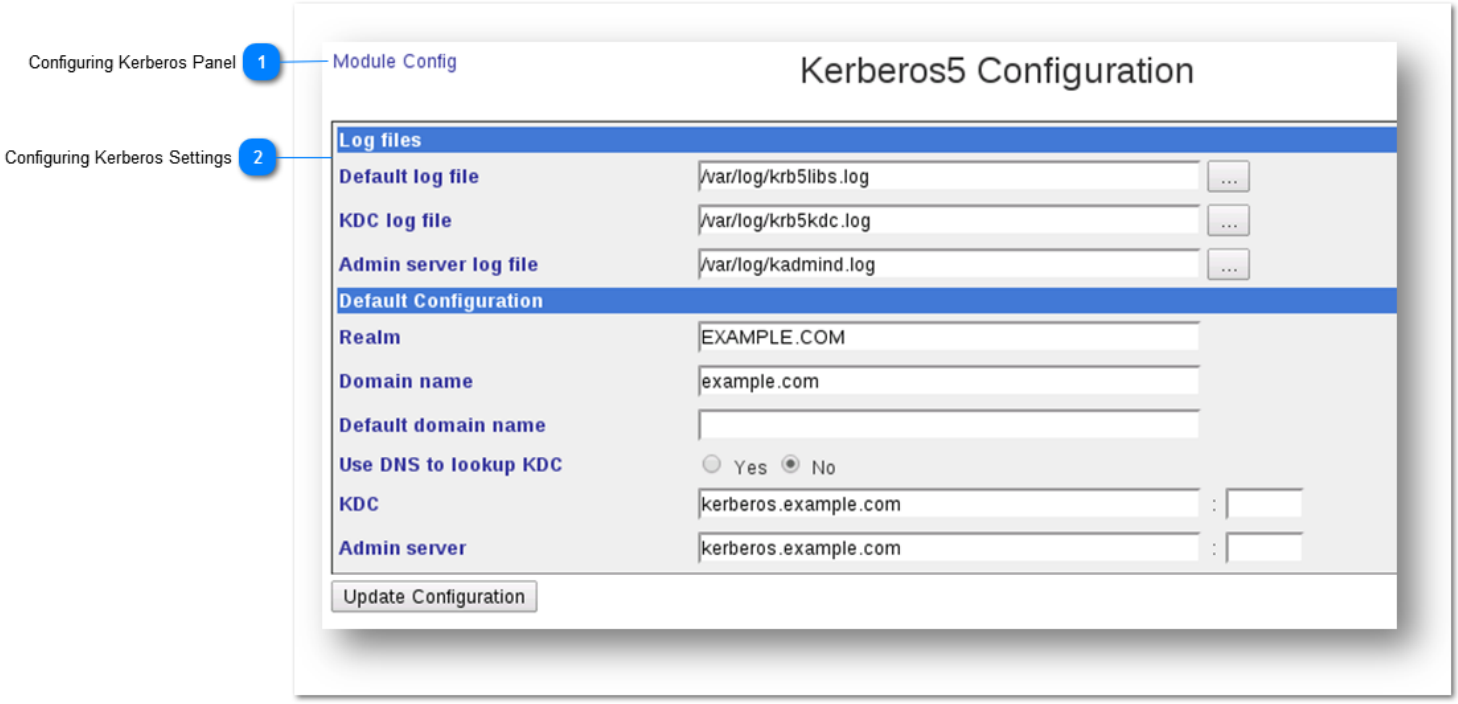
Parameter	Description
Name for new DN	name of the new Domain name to be created.
Create example object under new DN?	Setting which determines if a new object will be created under the newly created tree. One of the following: • Unix user • Unix user with mail • Unix group • Address mapping

LDAP Client

<TODO>:

Configuring Kerberos

The **Kerberos** helps in communicating over a non-secure network to prove identity to one another in a secure manner. Configure **Kerberos** from **SoftNAS.**



1 Configuring Kerberos Panel

Set the path to the **Kerberos** configuration file in the **Kerberos** module configuration.

1. To do so, click the **Module Config** link.

The **Configuration for Kerberos5 Module** page will be displayed.

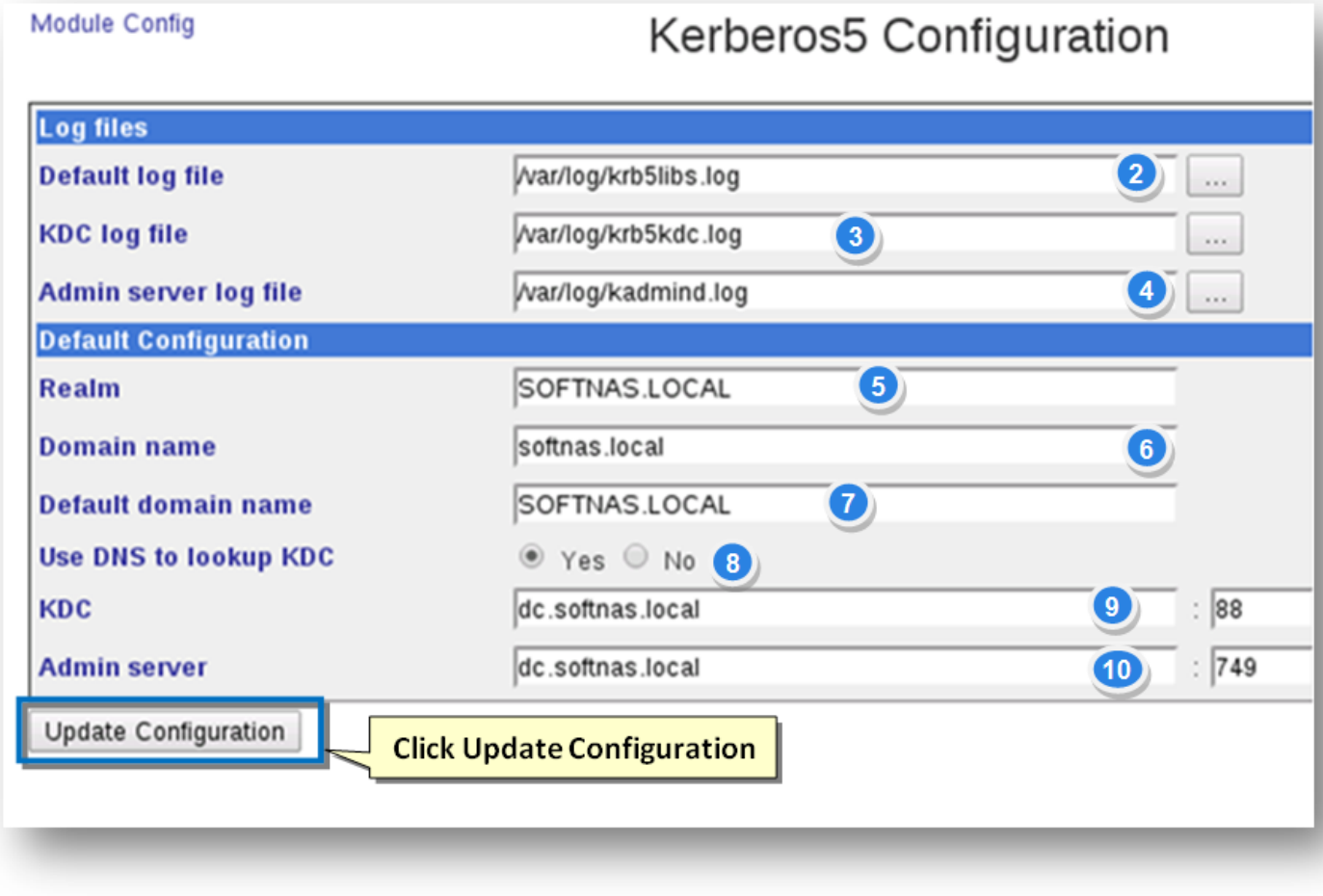
2. Enter the path for the **Kerberos5** configuration file in the text entry box.
3. Click the **Save** button.

The **Kerberos** module will be configured.

2 Configuring Kerberos Settings

1. Navigate to **Settings > Kerberos.**

The **Kerberos5 Configuration** page will be displayed.



2. Enter the default log file path in the **Default Log File** text entry box.
3. Enter the path for the KDC log file in the **KDC Log File** text entry box.
4. Enter the path for the KDC log file in the **Admin Server Log File** text entry box.
5. Enter the server name in upper case in the **Realm** text entry box.
6. Enter the domain name in the **Domain Name** text entry box.
7. Enter the default domain name in the **Default Domain Name** text entry box.
8. Specify whether DNS be used to lookup KDC by choosing **Yes** or **No** option.
9. Enter the server name for KDC in the **KDC** text entry box.
10. Enter the admin server name in the **Admin Server** text entry box.
11. Click the **Save** button.

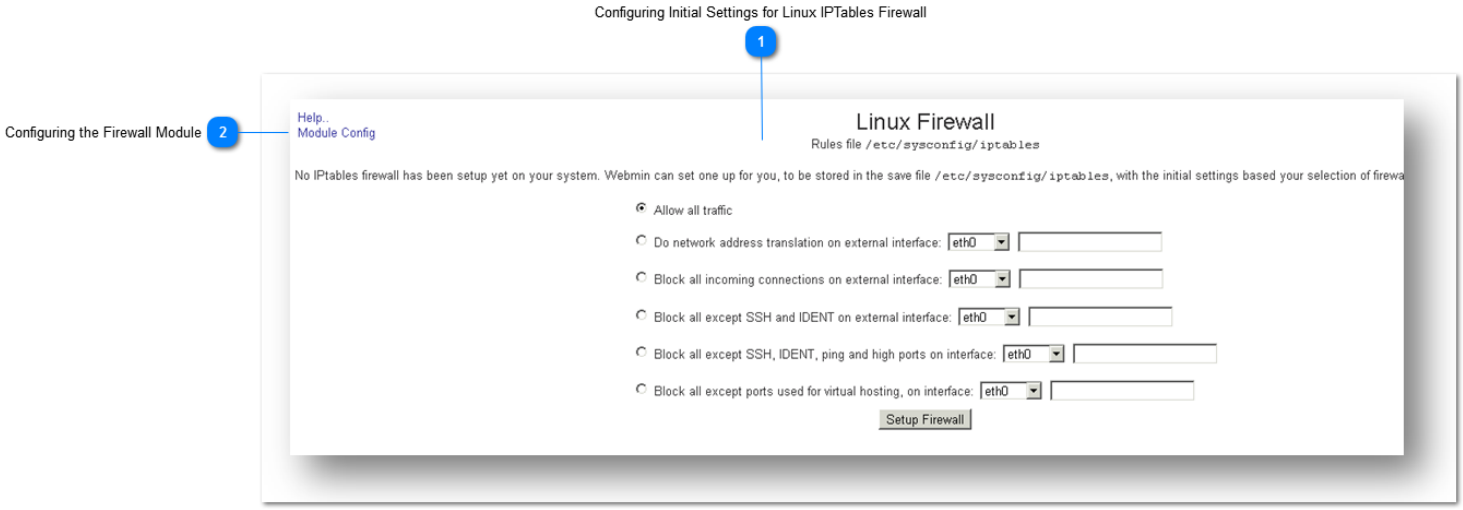
The changes made to the **Kerberos** will be updated.
.

Managing Firewall

The **Firewall** in **SoftNAS** helps to control the incoming and outgoing network traffic in VPN.

Typically, storage servers are deployed within an internal, secure network (often on their own VLAN on a protected network segment, perhaps even with dedicated switches). While SoftNAS can be deployed in this, or any other appropriate configuration, it's most common that some other firewall(s) protect the perimeter of the enterprise (from the Internet) and the data center (from the intranet). Use appropriate judgment as to whether or not to employ the Linux firewall, in addition to other security measures in the environment.

If enabling the firewall, be sure to open up the appropriate set of ports for SSH, HTTP. HTTPS, NFS/bind, iSCSI, CIFS, etc.

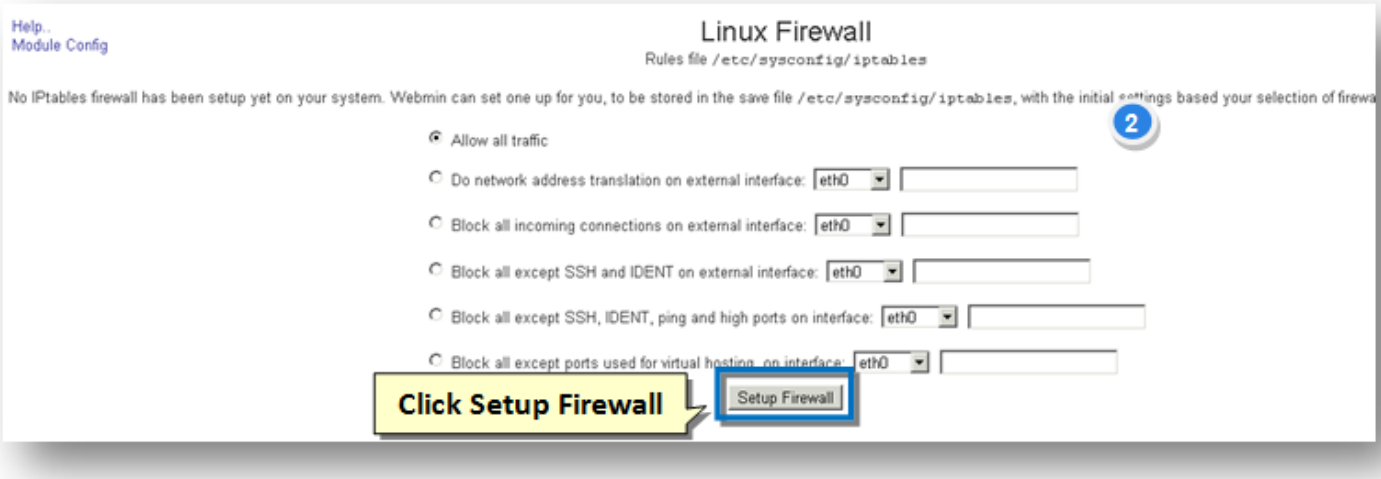


1 Configuring Initial Settings for Linux IPTables Firewall

Set the **Webmin** to setup **IPtables** to be stored as file. First, provide the initial settings.

1. Navigate to **Settings > Firewall.**

The **Linux Firewall** page will be displayed.

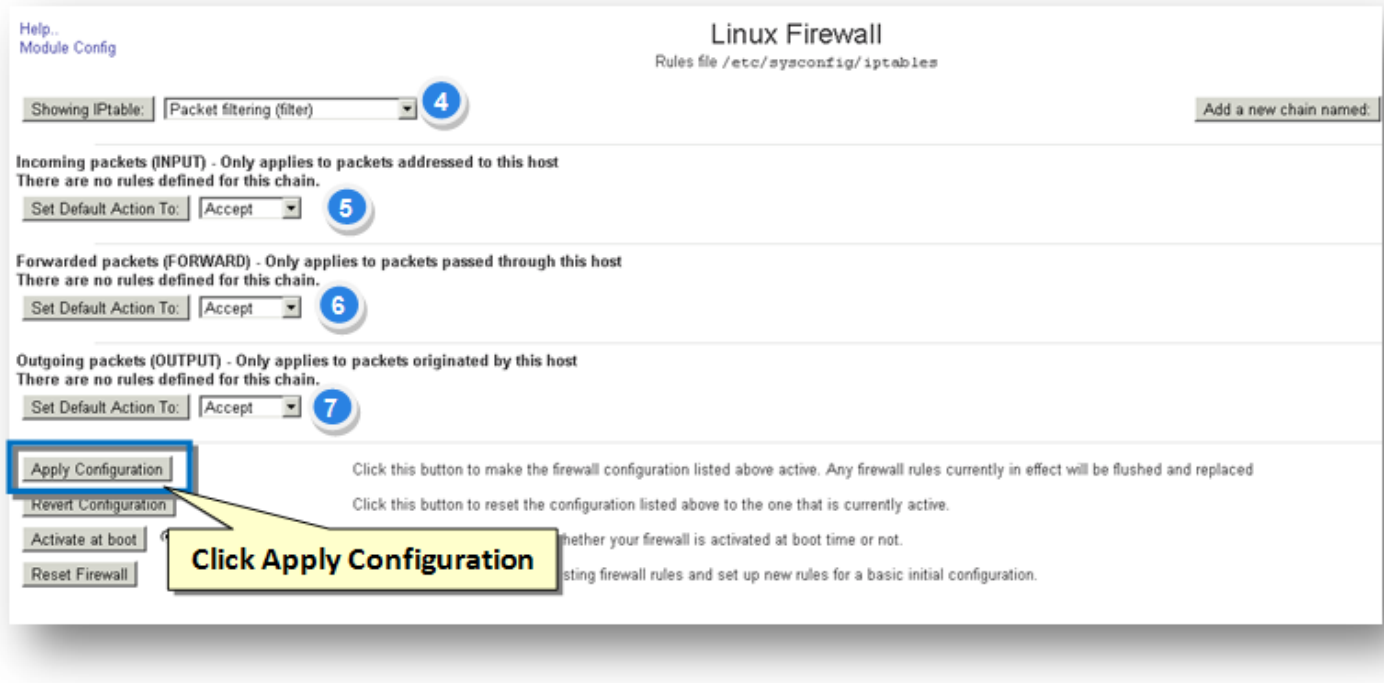


2. Select any of the required options for firewall setting. The available options include

   - Allow all traffic
   - Do network address translation on external interface
   - Block all incoming connections on external interface
   - Block all except SSH and IDENT on external interface
   - Block all except SSH, IDENT, ping and high ports on interface
   - Block all except ports used for virtual hosting, on interface

3. Click the **Setup Firewall** button.

The **Linux Firewall Rules** page for Iptables will be displayed based on the initial settings.



4. Select what IPtable should be showing from the drop down list. The available options include **Packet Filter Packet Alteration (Mangle)** and **Network Address Translation (NAT).**

5. Specify the default action to the incoming packets (INPUT) - Only applies to packets addressed to this host down list. The available options are **Accept, Drop, Userspace** and **Exit Chain.**

6. Specify the default action to the forwarded packets (FORWARD) - Only applies to packets passed through available options are **Accept, Drop, Userspace** and **Exit Chain.**

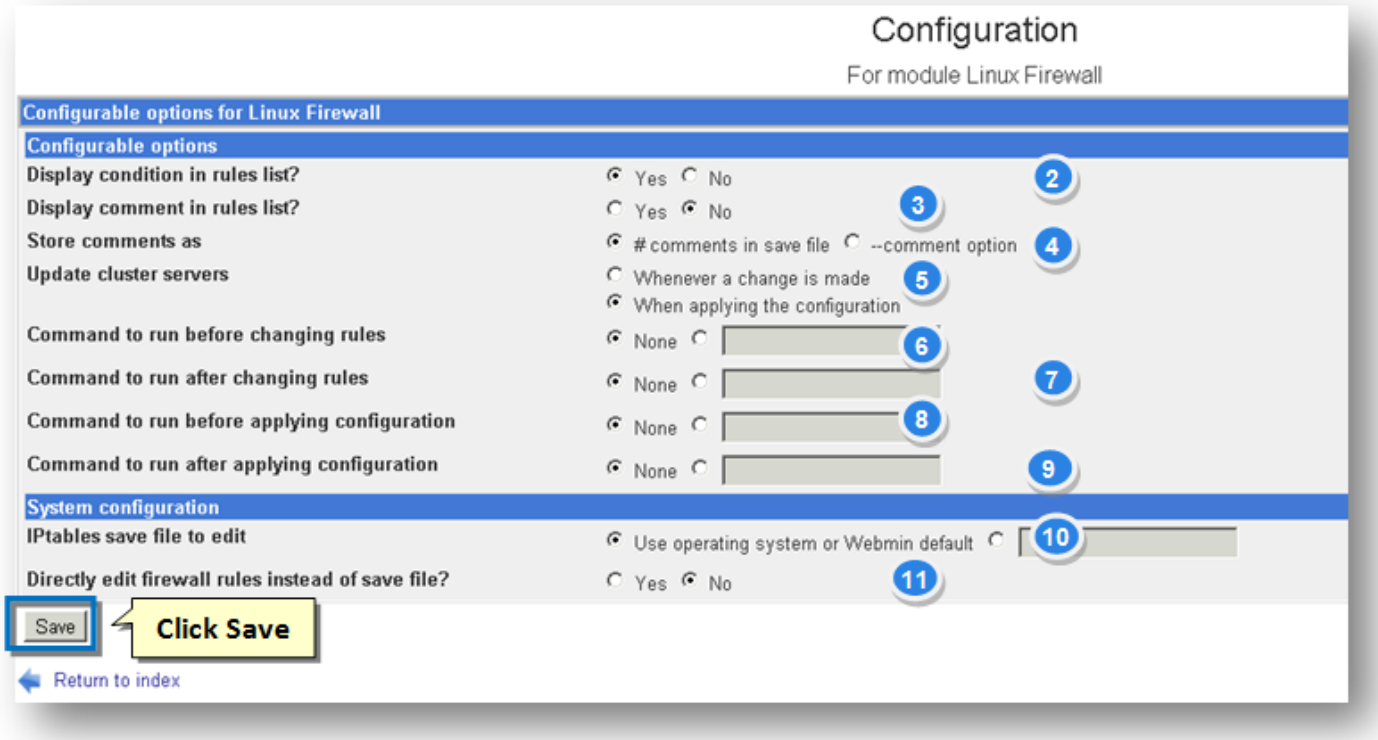
7. Specify the default action to the outgoing packets (OUTPUT) - Only applies to packets originated by this ho rules defined for this chain. The available options are **Accept, Drop, Userspace** and **Exit Chain.**

8. Click the **Apply Configuration** button to make the changes made to the firewall configuration active. Any fi currently in effect will be flushed and replaced.

2 Configuring the Firewall Module

1. On the **Firewall** page, click the **Module Config** button.

The **Configuration for Linux Firewall** module will be displayed.



2. Specify whether to display condition in rules list or not in the field by choosing either **Yes** or **No** option.

3. Specify whether to display comment in rules list or not in the field by choosing either **Yes** or **No** option.

4. Specify the mode of storing the comments in the field by selecting the appropriate option.

5. Specify when the cluster servers must be updated in the field by choosing the appropriate option.

6. Specify the command to run before changing rules in the field by choosing the option as **None** or entering c box..

8. Specify the command to run after changing rules by choosing the option as None or entering comment in th

9. Specify the command to run before applying configuration by choosing the option as None or entering comm

10. Specify the command to run after applying configuration by choosing the option as None or entering comm

11. Specify whether the IPtables save file to edit must use operating system or webmin default in the field.

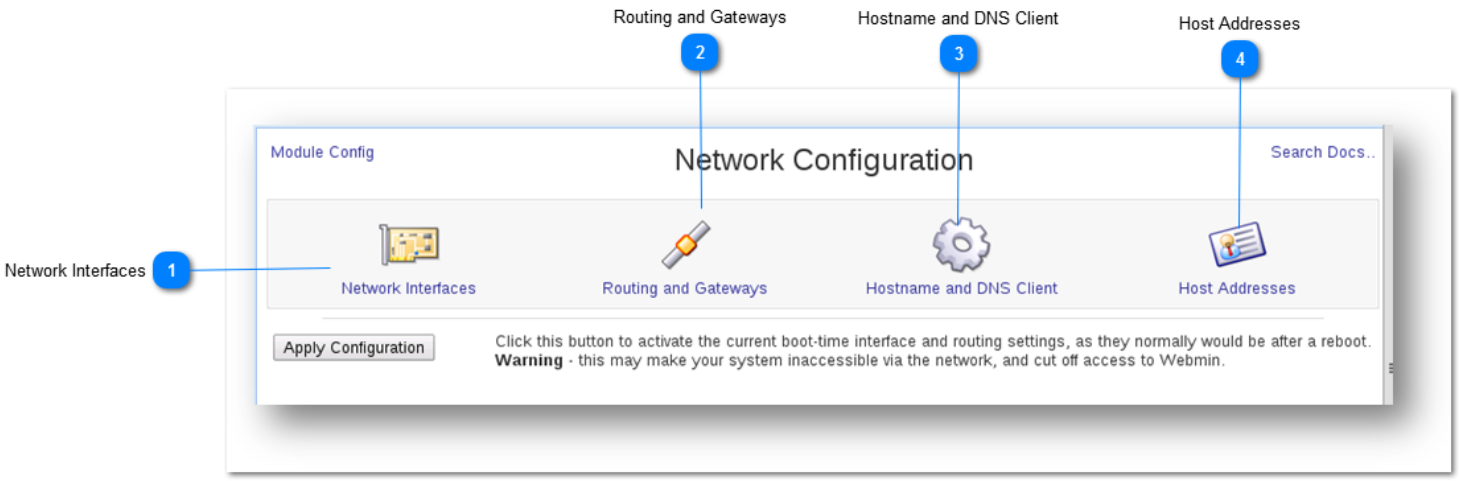
12. Specifiy whether firewall rules can be directly edited instead of save file by choosing **Yes** or **No** option.

13. Click the **Save** button.

The changes made to the firewall configuration module will be updated.

Configuring Network Settings

The **Network Settings** panel is used to administer network interfaces, routing and gateways, hostname, DNS and other network-related configuration.



1 Network Interfaces

The **Network Interfaces** module allows administrative control over adding, editing, or removing network interfaces. From here, add vlan tagged interface, new bridge and new address.

For more information, refer **Network Interfaces**.

2 Routing and Gateways

The **Routing and Gateways** section allows configuration of the routes that are activated when the system boots up or when the network settings are fully re-applied. It shows both boot time configuration and the current, active configuration.

For more information, refer **Routing and Gateways**.

3 Hostname and DNS Client

The **Hostname and DNS Client** module allows for configuration of host name, resolution order and DNS servers.

For more information, refer **Hostname and DNS Client**.

4 Host Addresses

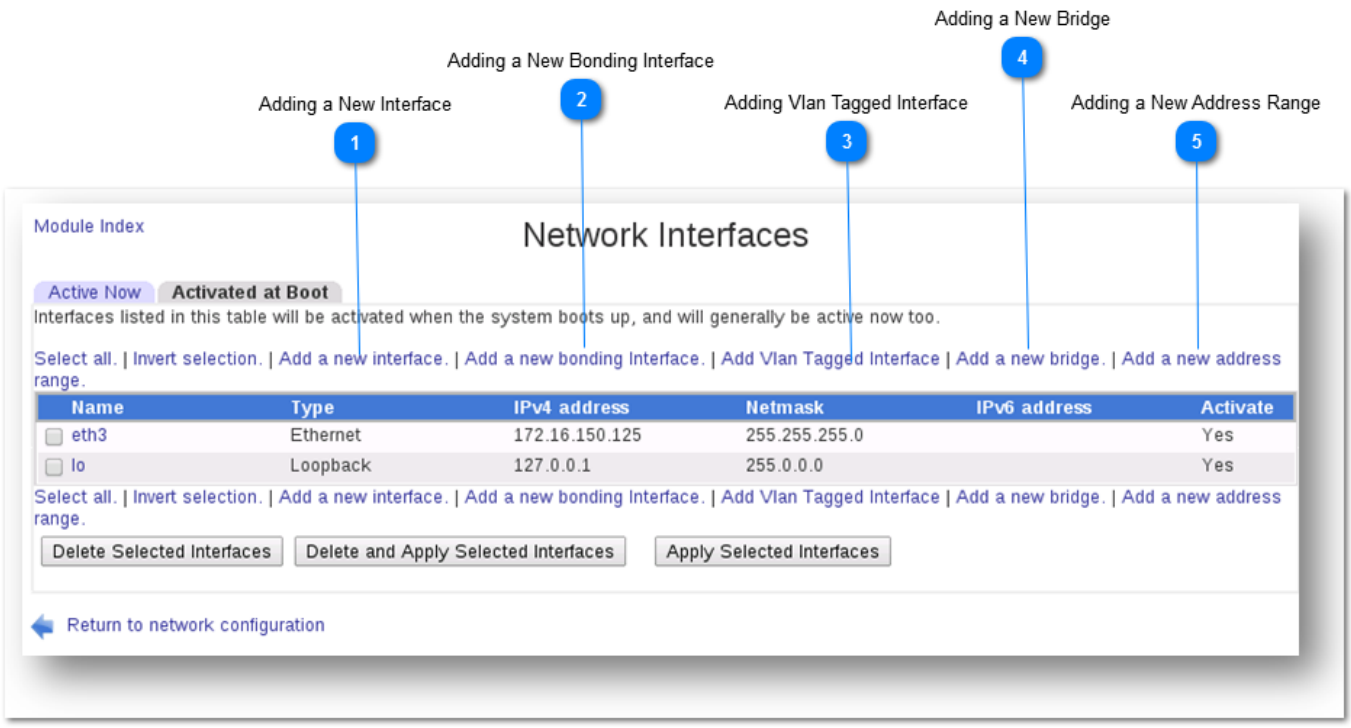
The **Host Addresses** module helps to add, edit or remove host addresses.

For more information, refer **Host Addresses**.

Network Interfaces

The **Network Interfaces** module allows administrators to add, edit or remove network interfaces. From here, add vlan tagged interface, new bridge and new address.

The interfaces listed in this table are currently active on the system. In most cases, it is best to edit them under the **Activated at Boot** tab.

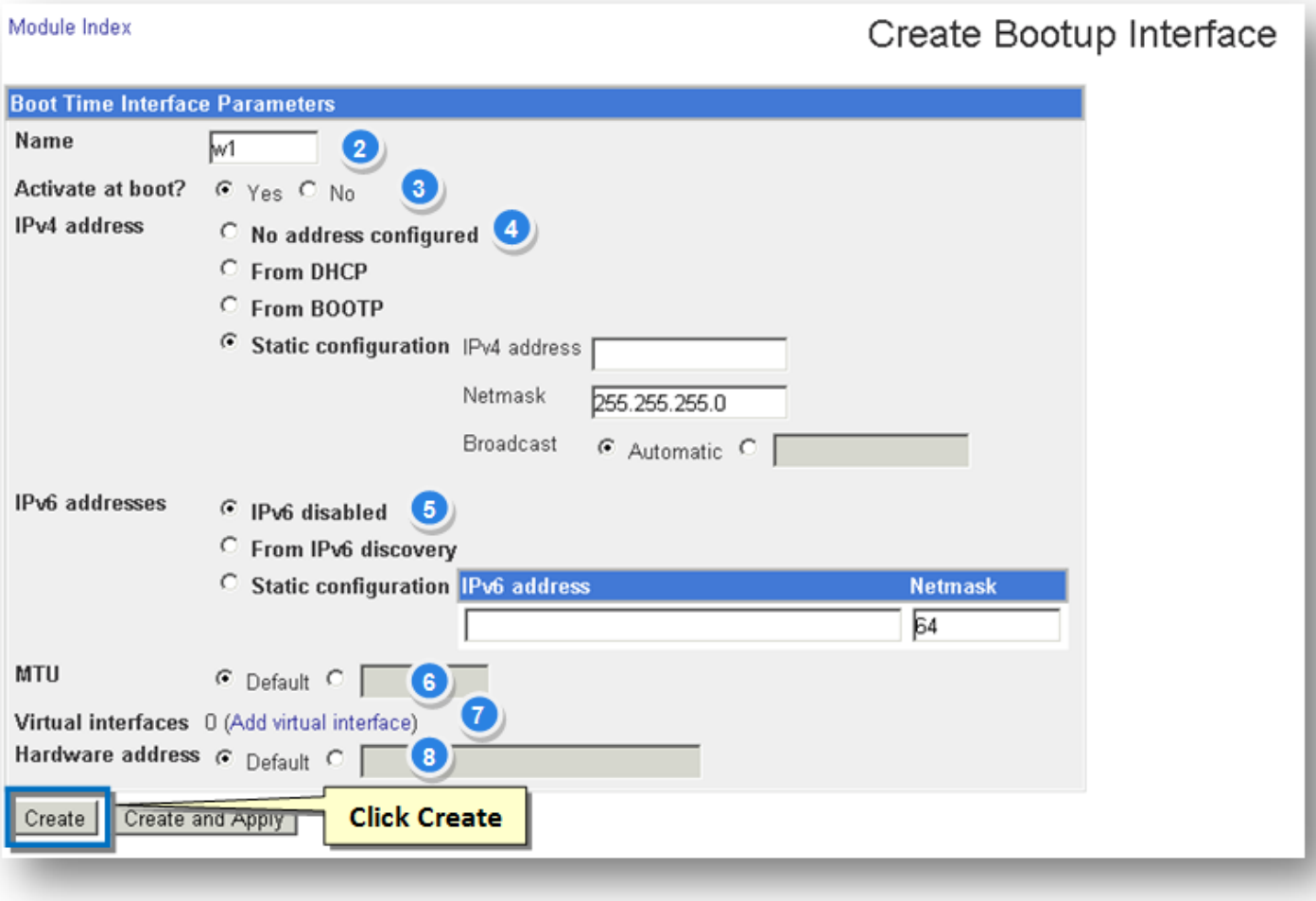


1 Adding a New Interface

Adding a new interface is easy. Simply follow the steps given below.

1. Click the **Add a New Interface** button.

The **Create Bootup Interface** page will be displayed.



2. Enter the name of the interface in the **Name** text entry box.
3. Specify whether to activate this interface at boot time or not by choosing **Yes** or **No** option in the field.
4. Specify the type of the **IPv4 address** to be configured in the field. The available options are
    - No address configured
    - From DHCP
    - From BOOTP
    - Static Configuration with netmask and broadcast IPs
5. Specify the type of the **IPv6 address** to be configured in the field. The available options are
    - IPv6 disabled
    - From IPv6 directory
    - Static Configuration
6. Specify the value for **MTU** either as Default or enter manually.
7. Select the virtual interface. Adding a new interface is also possible here.
8. Specify the value for **Hardware Address** either as Default or enter manually.
9. Click the **Create** button.

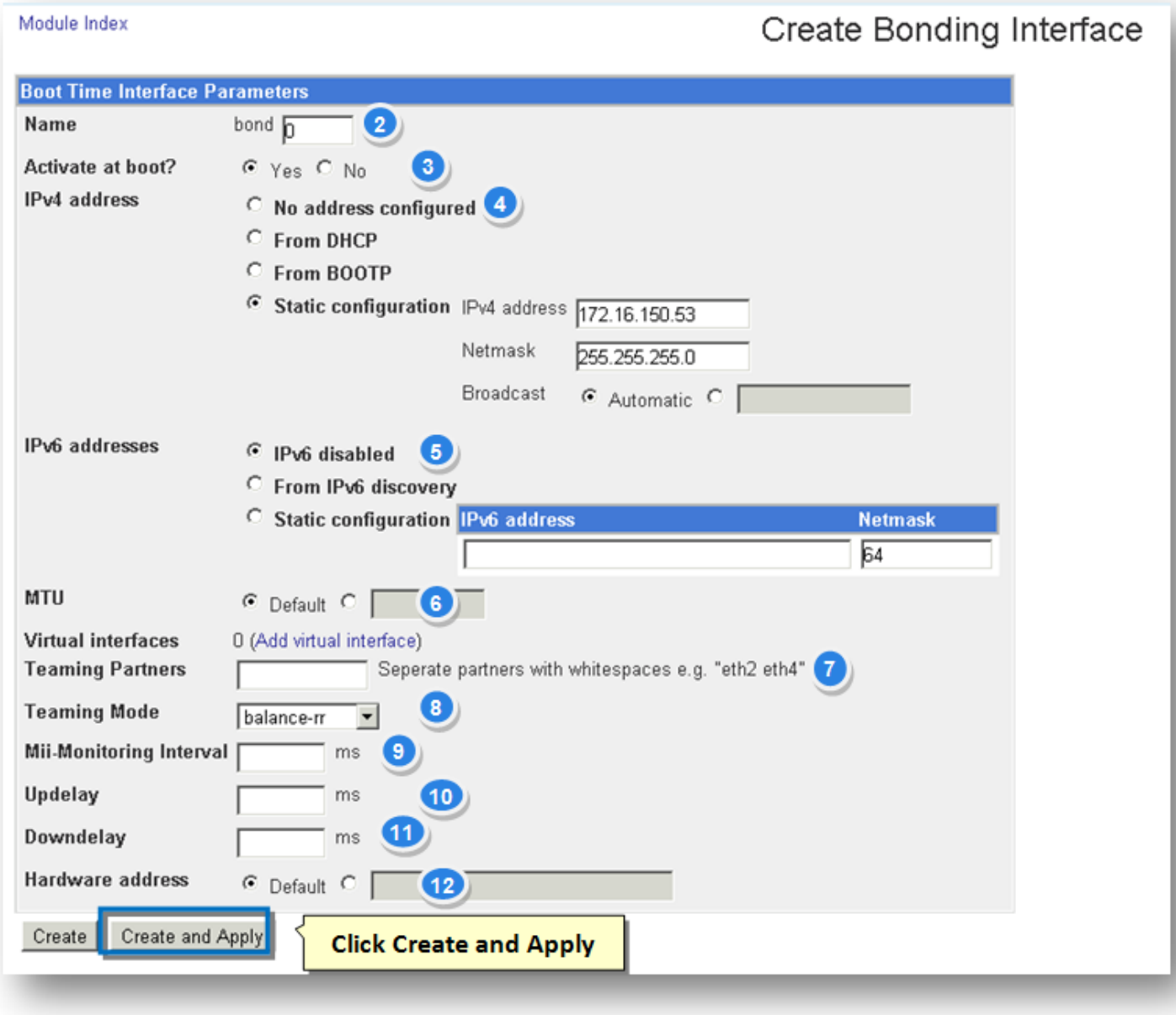
The bootup interface will be added.

2 Adding a New Bonding Interface

Adding a new bonding interface is easy. Simply follow the steps given below.

1. Click the **Add a New Bonding Interface** button.

The **Create Bonding Interface** page will be displayed.



2. The name of the bonding interface is automatically assigned.
3. Specify whether to activate this interface at boot time or not by choosing **Yes** or **No** option in the field.
4. Specify the type of the **IPv4 address** to be configured in the field. The available options are

   - No address configured
   - From DHCP
   - From BOOTP
   - Static Configuration with netmask and broadcast IPs

5. Specify the type of the **IPv6 address** to be configured in the field. The available options are

    - IPv6 disabled
    - From IPv6 directory
    - Static Configuration

6. Specify the value for **MTU** either as Default or enter manually.

7. Select the virtual interface. Adding a new interface is also possible here.

8. Enter the name of the teaming partners in the **Team Partners** text entry box, each seperated by white spac

9. Select the mode of teaming from the **Teaming Mode** drop down list.

10. Enter the value for Mii-Monitoring interval in milliseconds in the **Mi-Monitoring Interval** text entry box.

11. Enter the value for updelay in milliseconds in the **Updelay** text entry box.

12. Enter the value for downdelay in milliseconds in the **Downdelay** text entry box.

13. Specify the value for **Hardware Address** either as **Default** or enter manually.

14. Click the **Create** button.

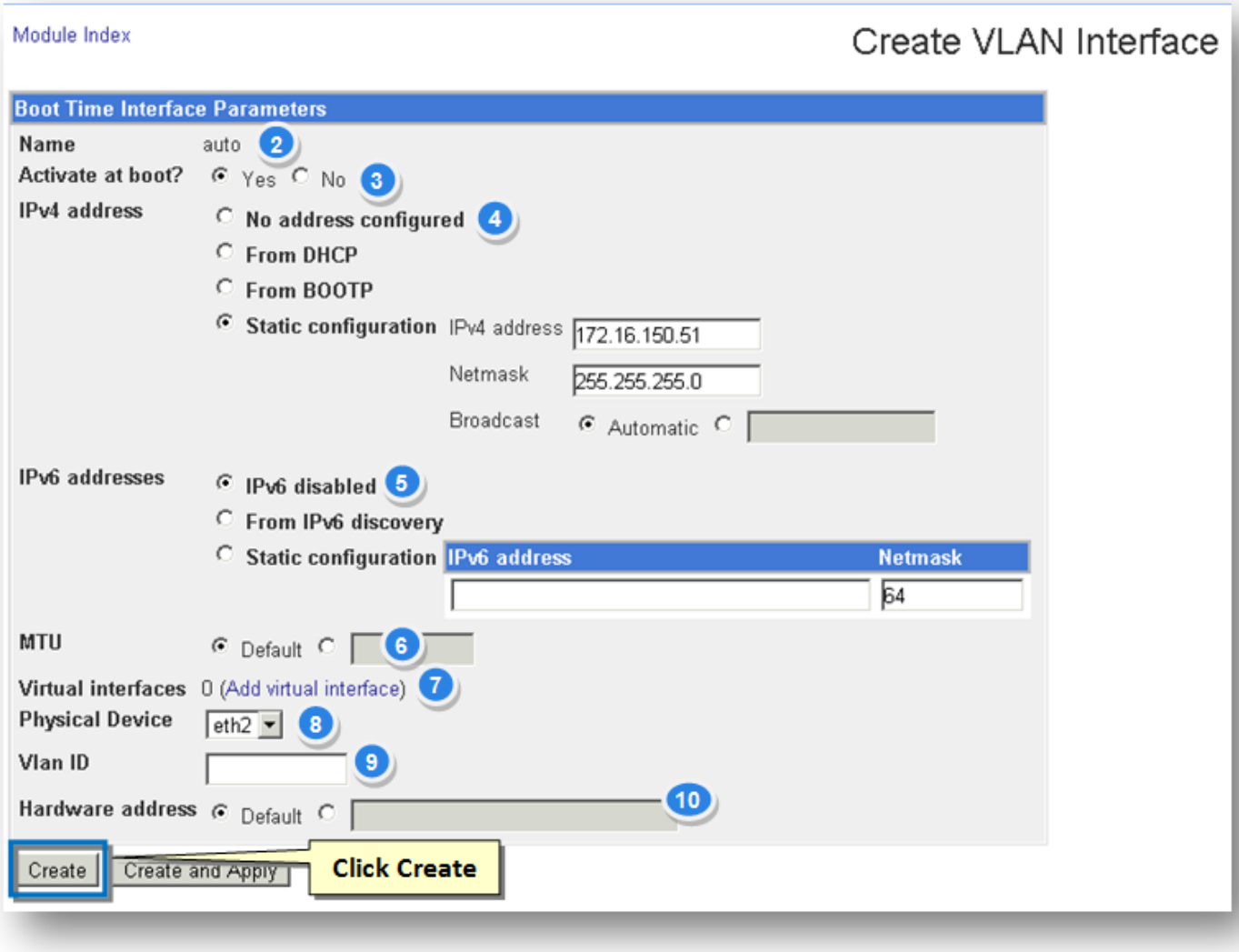
The new bonding interface will be added.

3 Adding Vlan Tagged Interface

Adding a new vlan tagged interface is easy. Simply follow the steps given below.

1. Click the **Add a New VLAN Tagged Interface** button.

The **Create VLAN Interface** page will be displayed.



2. The name of the vlan interface is automatically assigned.

3. Specify whether to activate this interface at boot time or not by choosing **Yes** or **No** option in the field.

4. Specify the type of the **IPv4 address** to be configured in the field. The available options are

    - No address configured
    - From DHCP
    - From BOOTP
    - Static Configuration with netmask and broadcast IPs

5. Specify the type of the **IPv6 address** to be configured in the field. The available options are

    - IPv6 disabled
    - From IPv6 directory
    - Static Configuration

6. Specify the value for **MTU** either as Default or enter manually.

7. Select the virtual interface in the **Virtual Interfaces** field. Adding a new interface is also possible here.

8. Select the physical device from the **Physical Device** drop down list.

9. Enter the ID of vlan in the **Vlan ID** text entry box.

10. Specify the value for **Hardware Address** either as Default or enter manually.

11. Click the **Create** button.

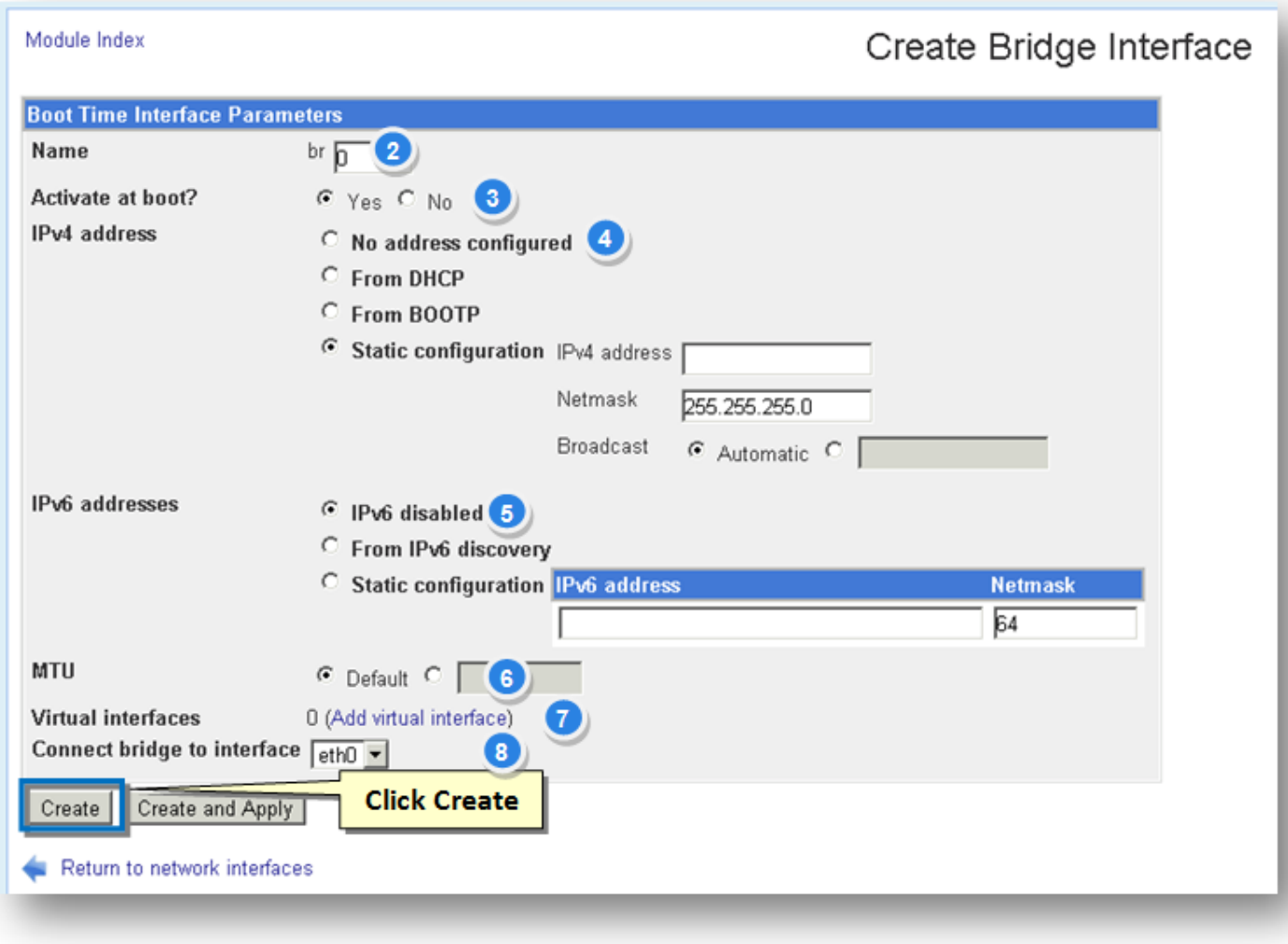
The new vlan tagged interface will be added.

4 Adding a New Bridge

Adding a new bonding interface is easy. Simply follow the steps given below.

1. Click the **Add a New Bridge** button.

The **Create Bridge Interface** page will be displayed.



2. The name of the bridge interface is automatically assigned.

3. Specify whether to activate this interface at boot time or not by choosing **Yes** or **No** option in the field.

4. Specify the type of the **IPv4 address** to be configured in the field. The available options are

    - No address configured
    - From DHCP

- From BOOTP
- Static Configuration with netmask and broadcast IPs

5. Specify the type of the **IPv6 address** to be configured in the field. The available options are

   - IPv6 disabled
   - From IPv6 directory
   - Static Configuration

6. Specify the value for **MTU** either as Default or enter manually.

7. Select the virtual interface. Adding a new interface is also possible here.

8. Select the bridge to interface connection from the **Connect Bridge to Interface** drop down list.

9. Click the **Create** button.

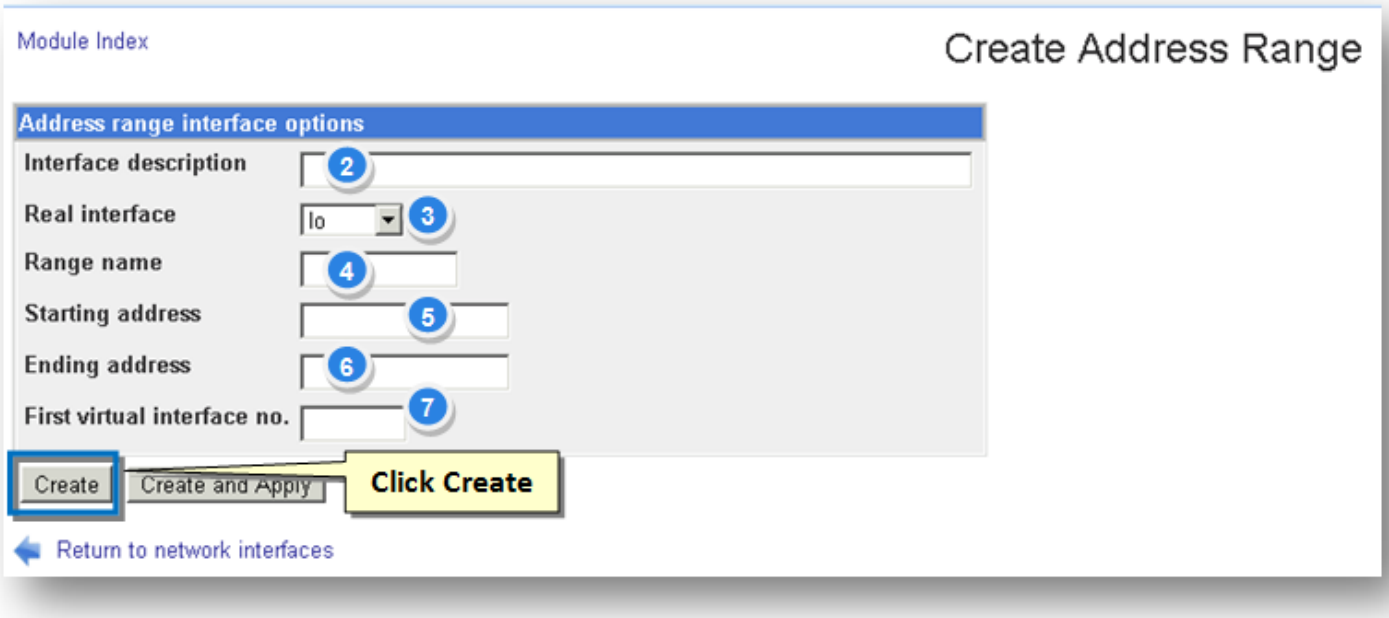
The bridge interface will be added.

5 Adding a New Address Range

Adding a new address range is easy. Simply follow the steps given below.

1. Click the **Add a New Address** button.

The **Create Address Range** page will be displayed.



2. Enter the description of the interface in the Interface Description text entry box.

3. Select the real interface from the Real Interface drop down list.

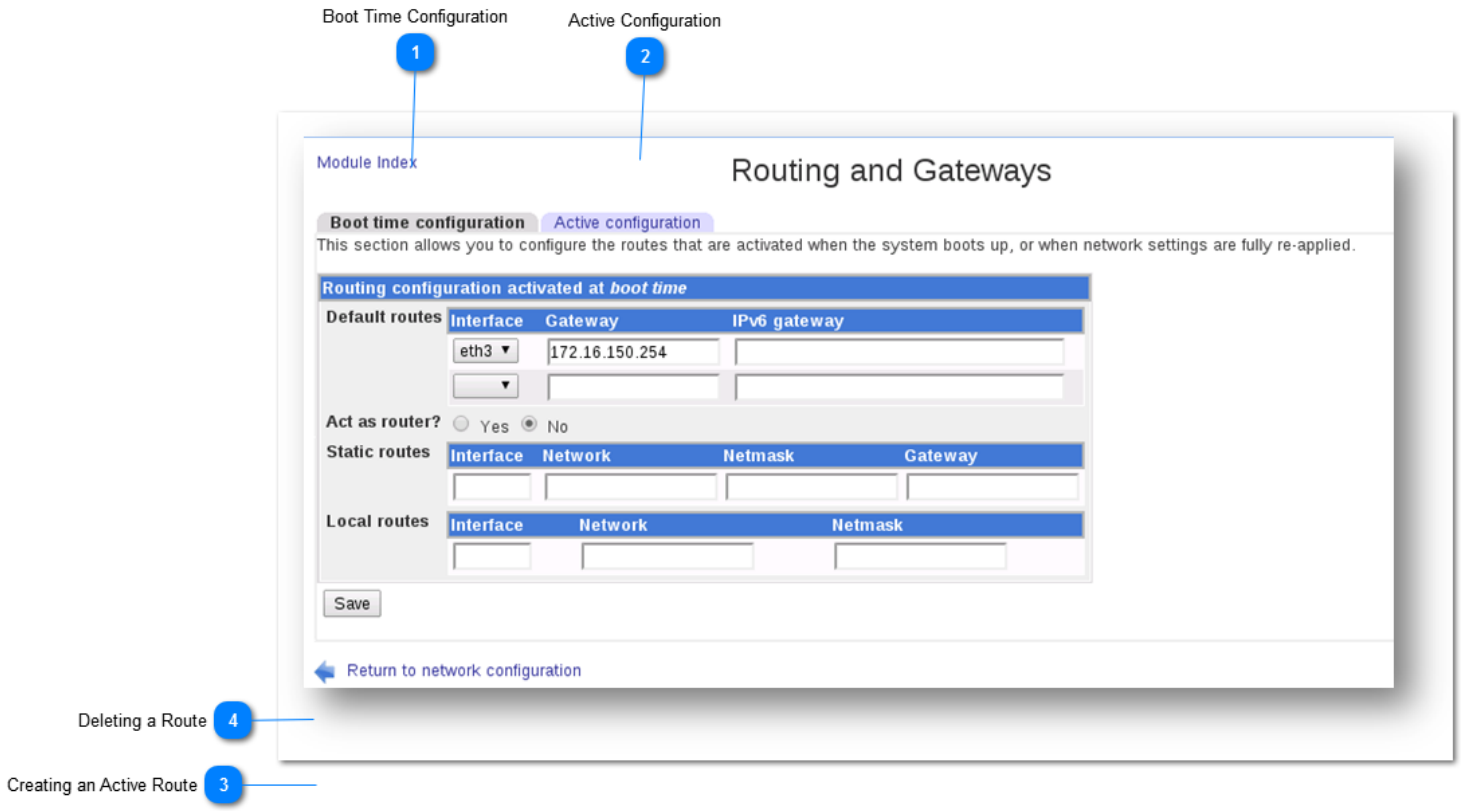
4. Enter the name for the range in the Range Name text entry box.

5. Enter the starting address of the range in the Starting Address text entry box.
6. Enter the ending address of the range in the Ending Address text entry box.
7. Enter the value for the virtual interface in the First Virtual Interface No. text entry box.
8. Click the **Create** button.

The new address range will be added.

Routing and Gateways

The **Routing and Gateways** section allows the configuration of the routes that are activated when the system boots up or when the network settings are fully re-applied. It shows both boot time configuration and the current, active configuration.

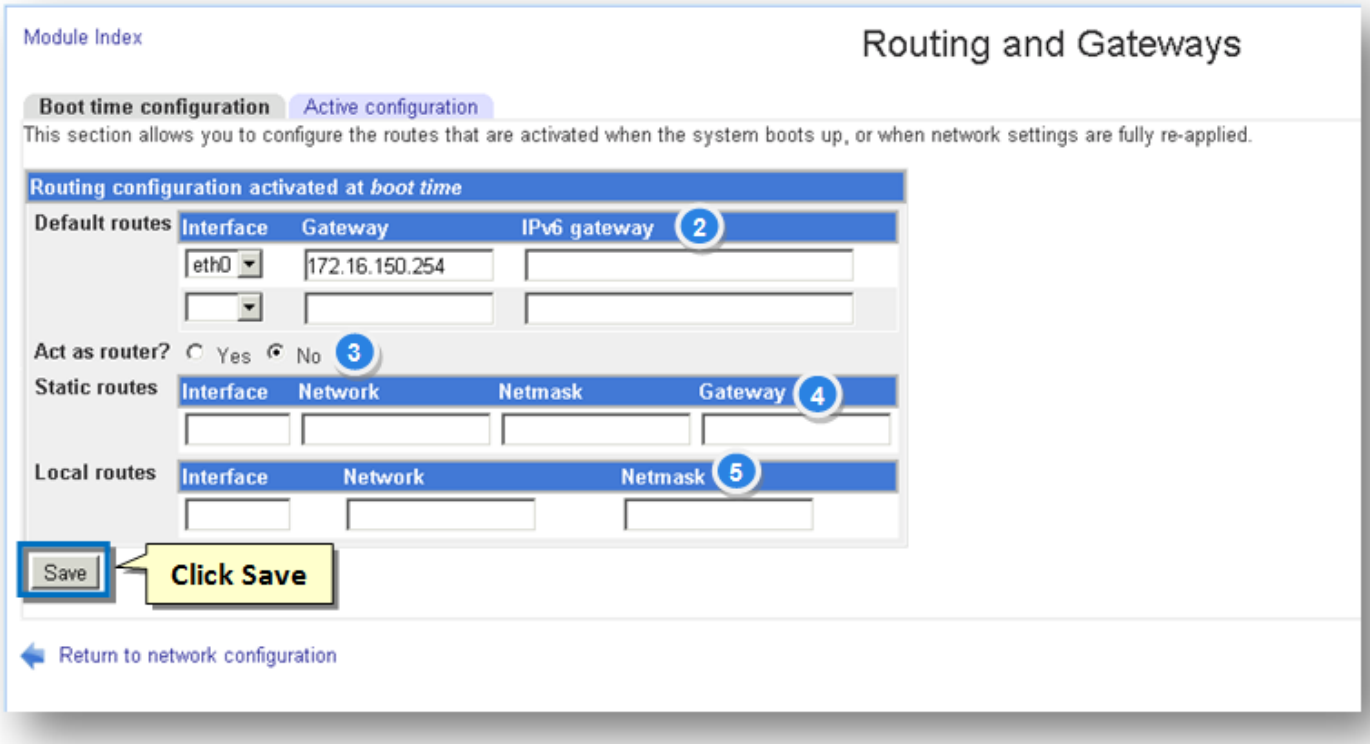


1 Boot Time Configuration

The **Boot Time Configuration** section allows the configuration of the routes that are activated when the syste when the network settings are fully re-applied.

Note: Be careful when configuring this section as incorrect changes may affect the system and cut the system off from the rest of the network.

1. Navigate to **Boot Time Configuration** tab.



2. Specify the default routes by entering the **Interface, Gateway** and **IPv6 Gateway** values in the **Default Ro**
3. Specify whether it should act as a router or not by choosing **Yes** or **No** option in the **Act as Router** field.
4. Specify the static routes by entering the **Interface, Gateway** and **IPv6 Gateway** values in the **Static Route**
5. Specify the local routes by entering the **Interface, Gateway** and **IPv6 Gateway** values in the **Local Routes**
6. Click the **Save** button.

The changes made for the boot time configuration will be updated.

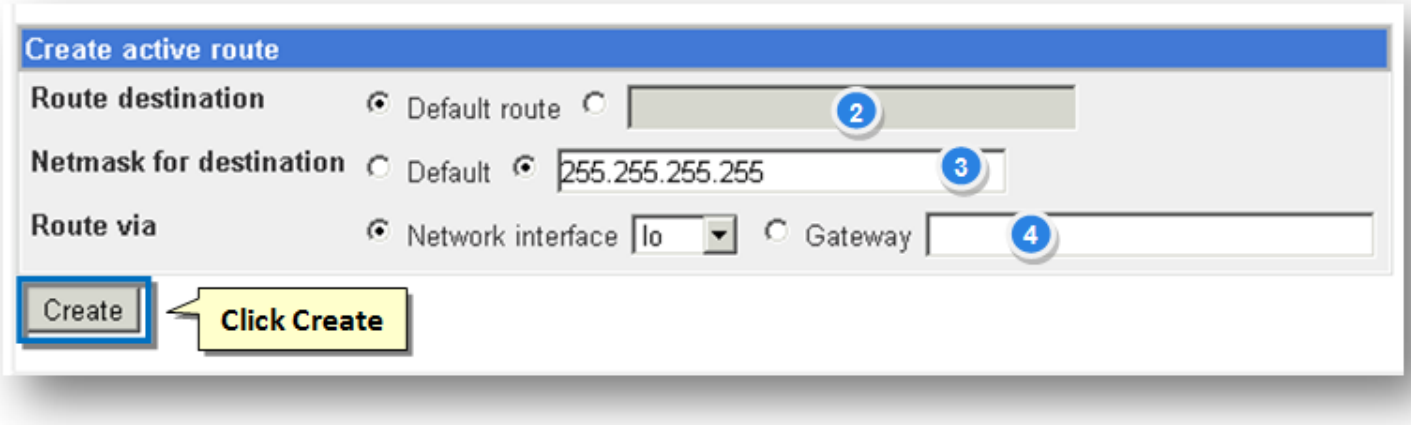
2 Active Configuration

The **Active Configuration** section lists the routes that the system currently has configured. It allows active routes to be added or removed on some systems.

Note: Be careful when configuring this section as incorrect changes may affect the system and cut the system running Webmin off from the rest of the network.

3 Creating an Active Route

Create an active route in the **Create Active Route** section under the **Active Configuration** tab.



1. Specify the destination of the route in the Route Destination field either by choosing the Default value or en manual value.

2. Specify the netmask for destination route in the Netmask for Destination field either by choosing the Defaul entering the manual value.

3. Specify the via route by entering the **Network Interface, Gateway** and **IPv6 Gateway** values in the **Local**

4. Click the **Create** button.

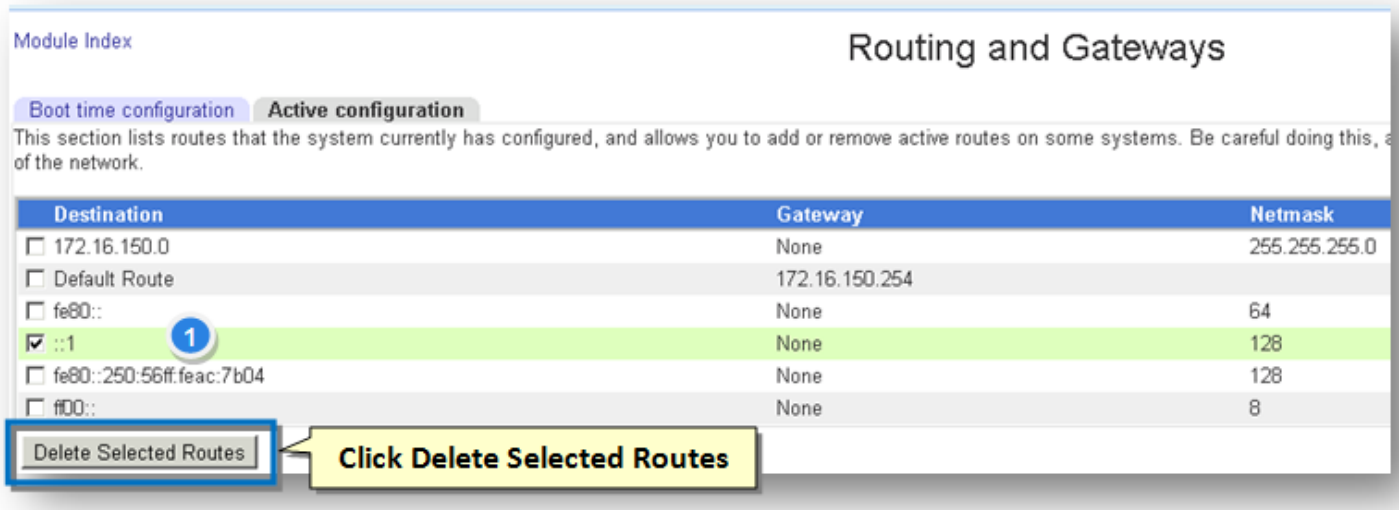
An active route will be created.

4 Deleting a Route

Delete a route in the **Create Active Route** section under the **Active Configuration** tab.

1. Select the route to be deleted from the list of routes.

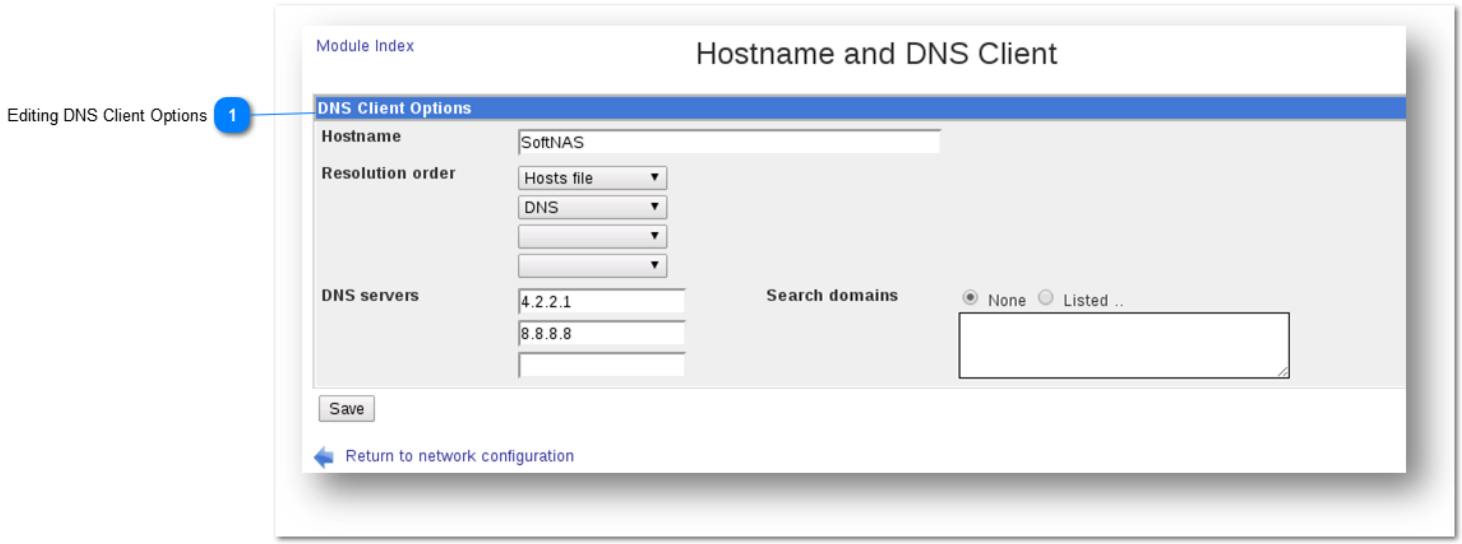
2. Click the **Delete Selected Routes** button.



The selected route will be removed.

Hostname and DNS Client

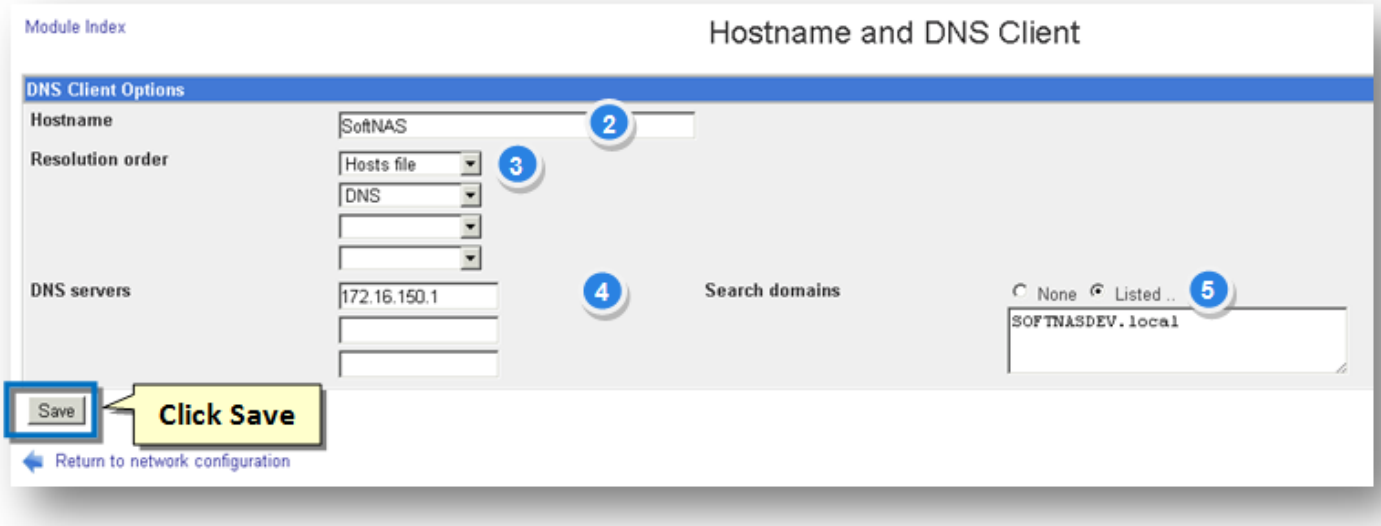
The **Hostname and DNS Client** module provides options to configure host name, resolution order and dns servers.



1 Editing DNS Client Options

Edit the hostname and DNS Client.

1. Navigate to **Hostname and DNS Client.**



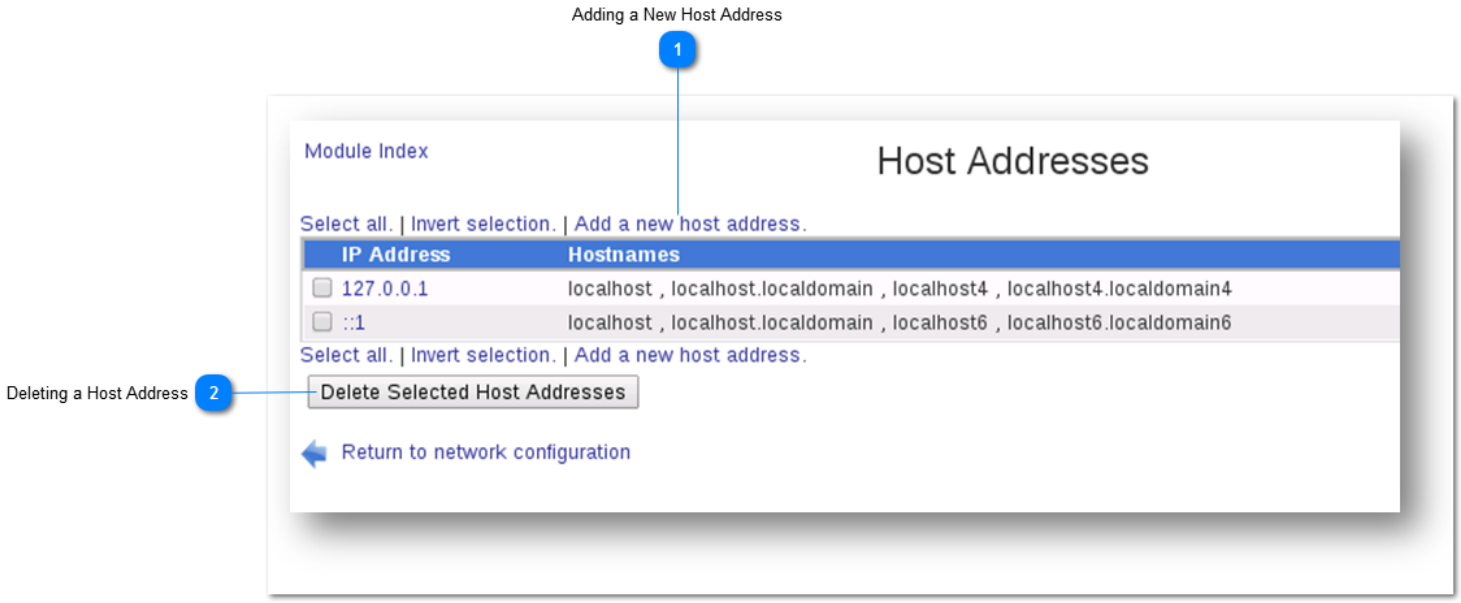
2. Enter the host name in the **Hostname** text entry box.
3. Select the reolution order from the **Resolution Order** drop down list.
4. Enter the address of dns servers in the **DNS Servers** text entry box.
5. Specify the search domain and enter **SOFTNASDEV.local** in the text entry box.

6. Click the **Save** button.

The **Host name** and **DNS client** will be configured.

Host Addresses

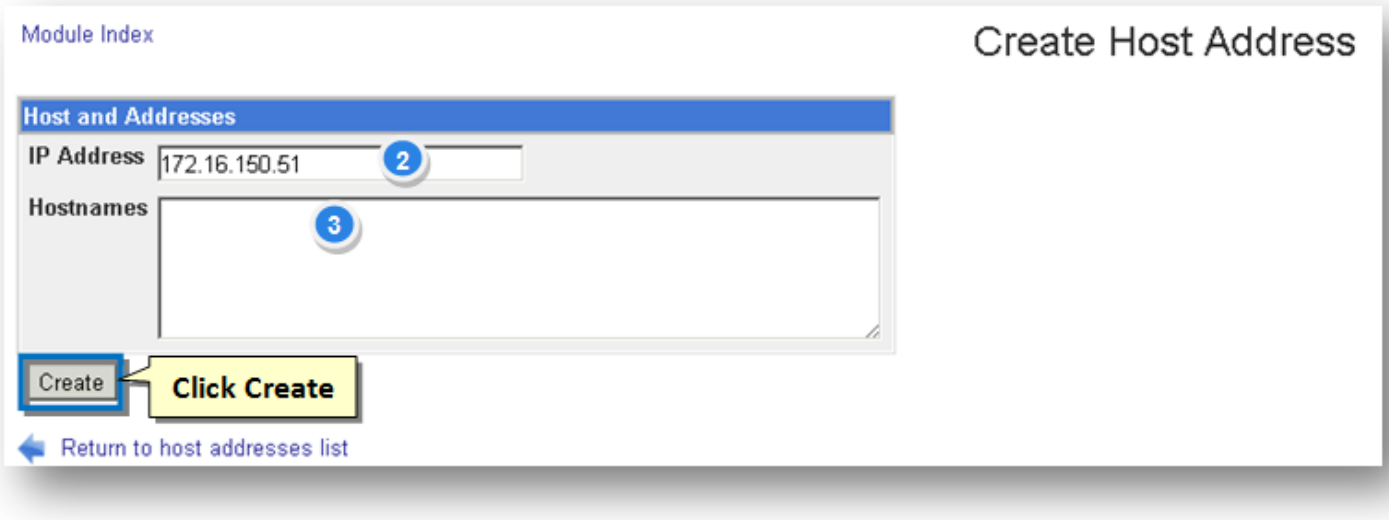
The **Host Addresses** module helps to add, edit or remove host addresses.



1 Adding a New Host Address

1. Click the **Add a New Host Address** button.

The **Create Host Address** page will be displayed.



2. Enter the IP address in the **IP Address** text entry box.
3. Enter the host names in the **Host Names** text entry box.
4. Click the **Create** button.

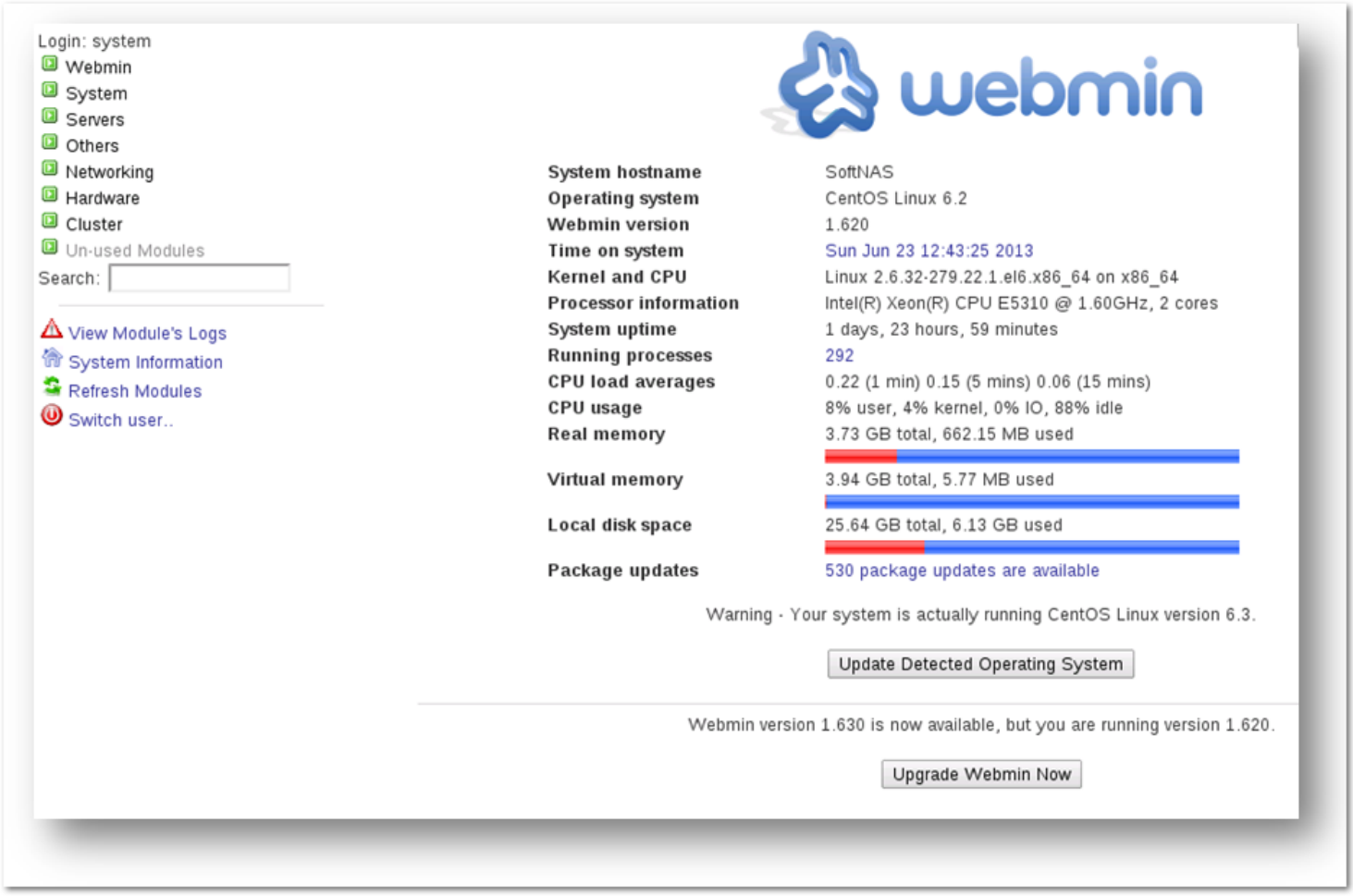
2 Deleting a Host Address

1. To remove an IP address, simply select it from the list.
2. Click the **Delete Selected Host Addresses** button.

The selected host address will be removed.

Configuring General System Settings

The **System Settings** in **SoftNAS** allows configuring general system settings through the standard Webmin control panel. SoftNAS uses Webmin to provide robust Linux administration functionality. It provides a rich, extensive set of Linux administration tools for advanced users.



Note: Only upgrade Webmin if advised to do so by **SoftNAS Support,** as upgrades could affect some integration functionality (it's usually best to pick up any Webmin updates when **SoftNAS** provides an update or upgrade, but please follow the latest **SoftNAS Support** advice and recommendations).

To use Webmin, click on the menu items on the left side to expose the full feature set available. Additional Webmin add-on modules are available (but are not supported by **SoftNAS Support**).

Some of the more useful Webmin administration functions include:

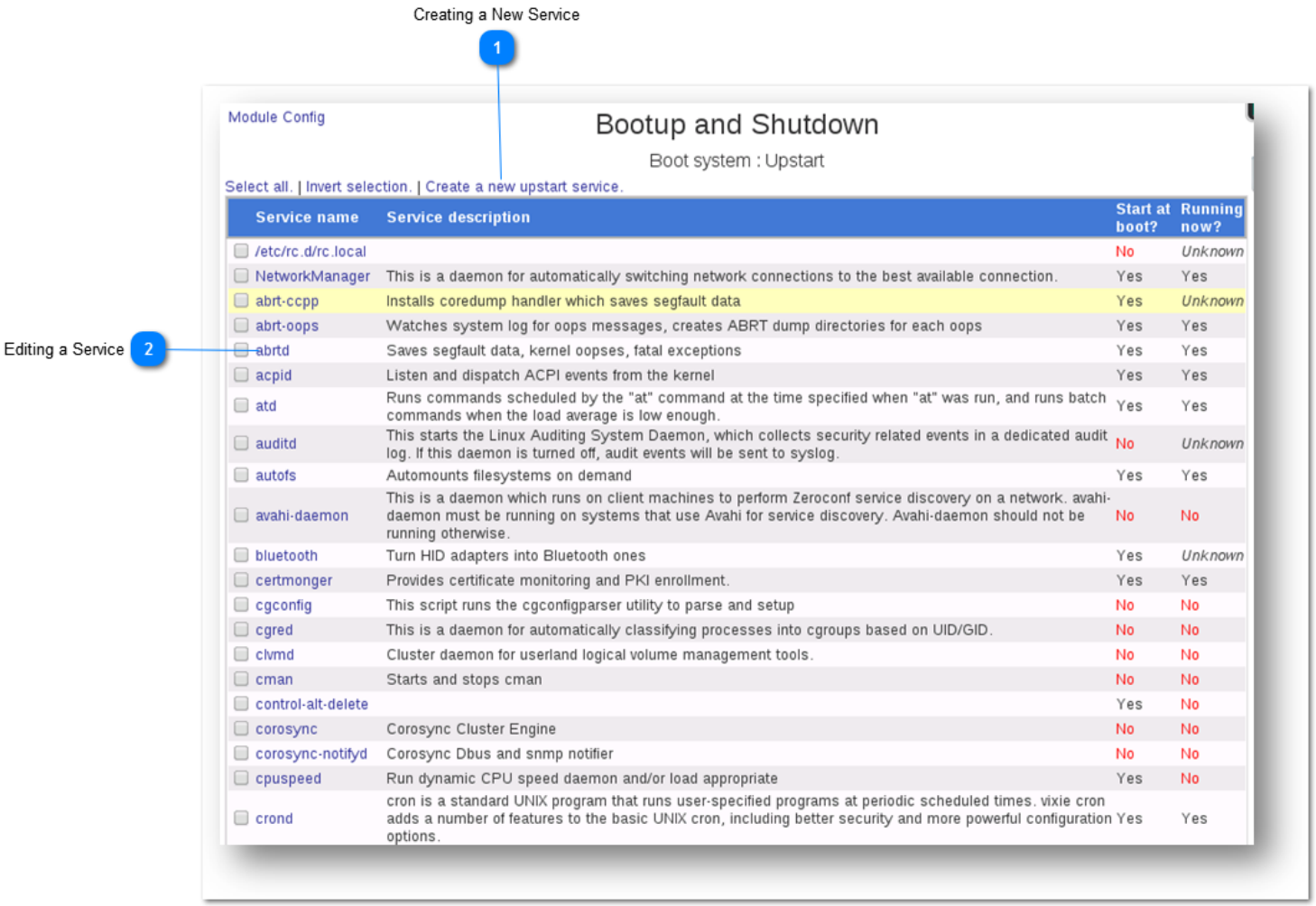
- Log file rotation
- PAM authentication options
- Scheduled cron jobs
- Users and groups
- Apache webserver administration (SoftNAS uses Apache for StorageCenter user interface)
- SSH Server (to manage secure shell access, which is also used for SnapReplicate)

For more information on Webmin, please visit the **Webmin website**.

Managing System Services

The **System Services** module provides management of all bootup and shutdown processes and services, or create a new upstart service.

The **System Services** provides a list of services that are running (or available to run) and that are activated at boot time. These service configurations normally should not need to be changed, but advanced users may have additional needs that can only be met by enabling certain Linux services not enabled by default in **SoftNAS.** From here, it is possible to start, restart, reload, show status, stop or delete a service.

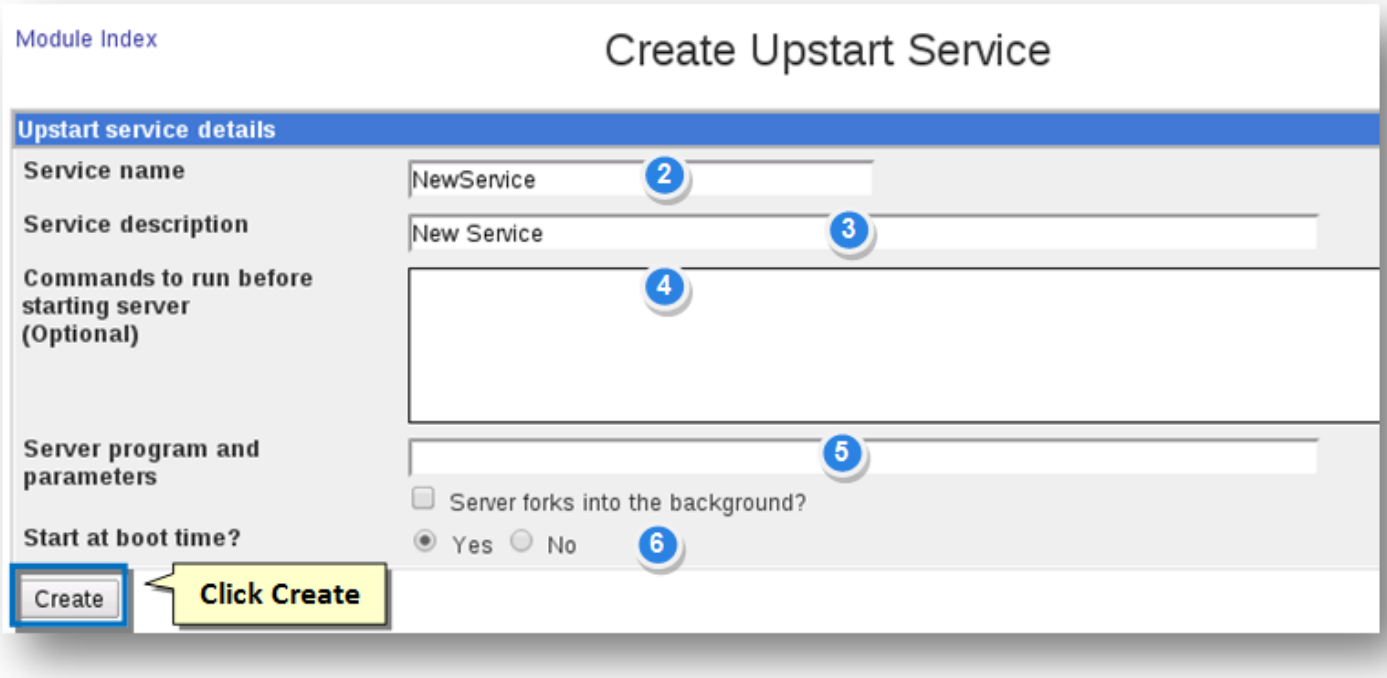


1 Creating a New Service

Creating a new service is very easy. Simply follow the steps given below.

1. Click the **Create a New UpStart Service** button.

The **Create Upstart Service** page will be displayed.



2. Enter the name of the service in the **Service Name** text entry box.
3. Enter the description of the service in the **Service Description** text entry box.
4. Enter the commands if any, to run before starting the server in the text entry box. Note that this is an option
5. Enter the details of server programs and parameters in the text entry box.
6. Specify whether the service should start at a boot time or not by choosing **Yes** or **No** option.
7. Click the **Create** button.

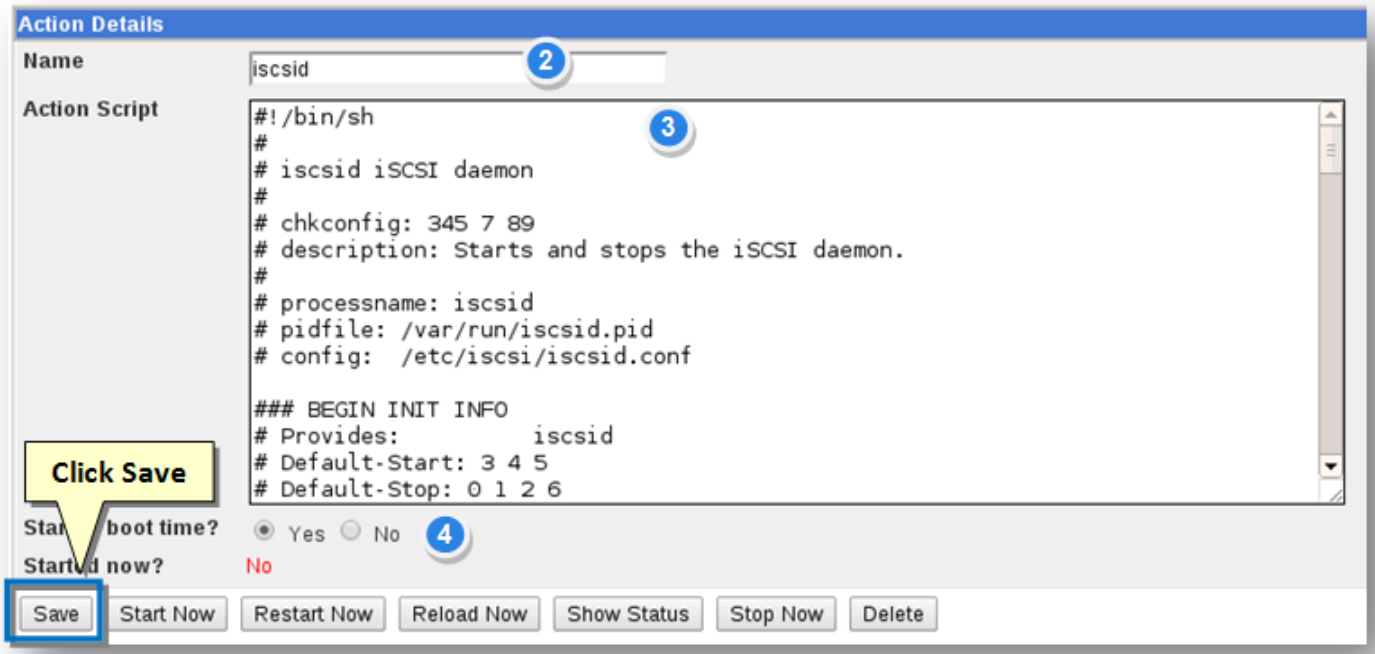
The new service will be created.

2 Editing a Service

Note: Be careful while editing a service. It may affect the smooth functioning of the system.

1. To edit a service, simply click the name of the service.

The service will be displayed in edit mode.

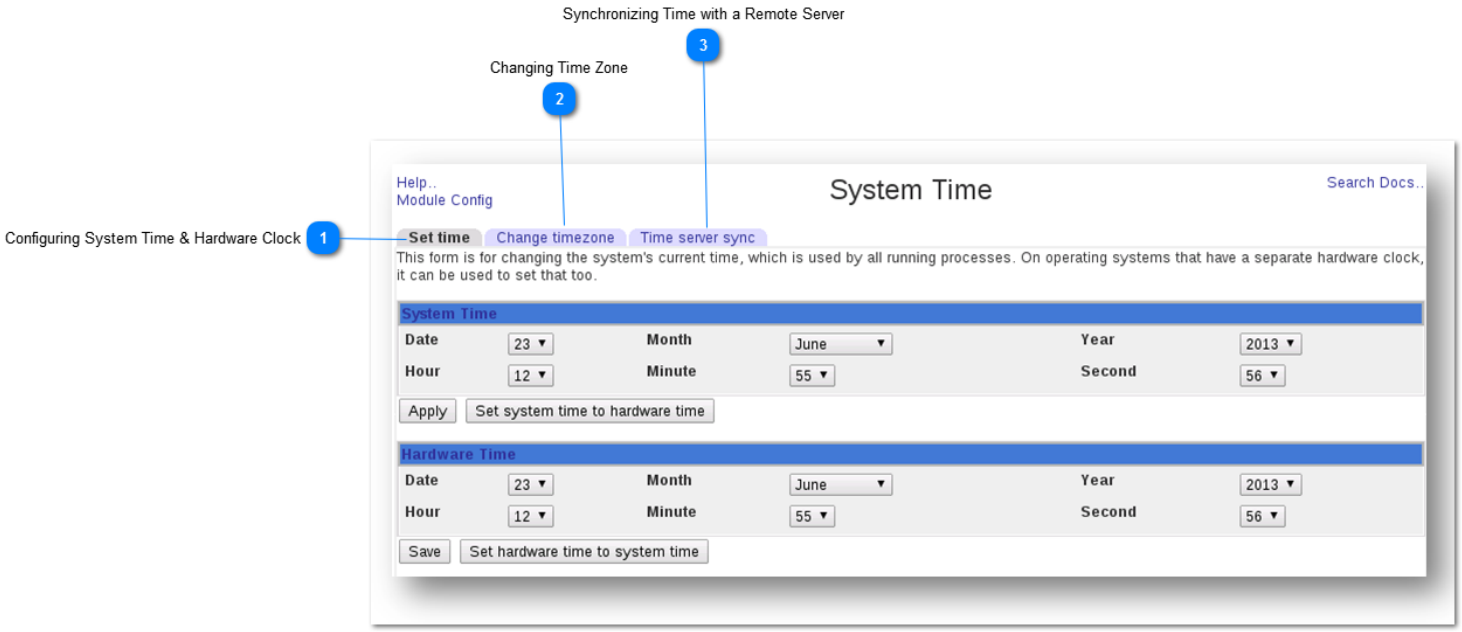


2. In the **Action Details** section, edit the name of the service in the **Name** text entry box.
3. Edit the script related to the action, in the **Action Script** text entry box.
4. Specify whether the service should start at a boot time or not by choosing **Yes** or **No** option.
5. Click the **Save** button.

The changes made to the service will be saved.

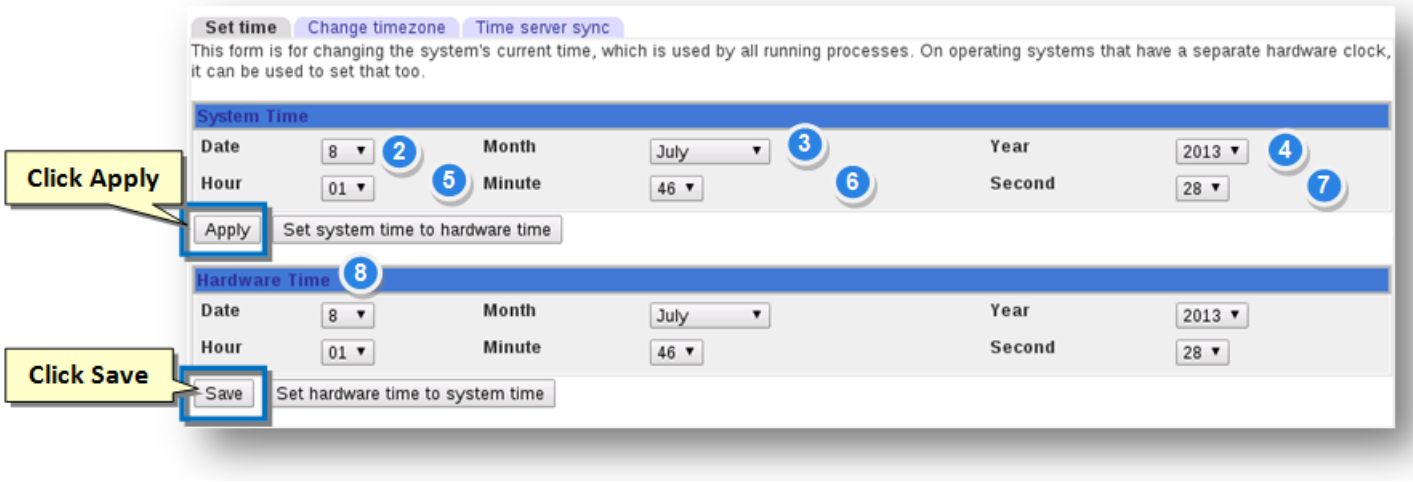
Configuring System Time

The **System Time** module provides configuration variables for system time and hardware clock; change time zone and synchronize the system time with a remote server.



1 Configuring System Time & Hardware Clock

Set both the system time and hardware clock in this section.



1. Navigate to the **System Time** page.
2. Select the date from the **Date** drop down list.
3. Select the month from the **Month** drop down list.
4. Select the year from the **Year** drop down list.

5. Select the hour from the **Hour** drop down list.
6. Select the minute from the **Minute** drop down list.
7. Select the second from the **Second** drop down list.
8. Click the **Apply** button.
9. To set the same system time to the hardware clock also, click the **Set System Time to Hardware Time** but
10. Similarly to set the hardware clock separately, select the required time from the drop down lists in the **Har**
11. Click the **Save** button.
12. Set the system time from the hardware clock. To do so, click the **Hardware Time to System Time** button.

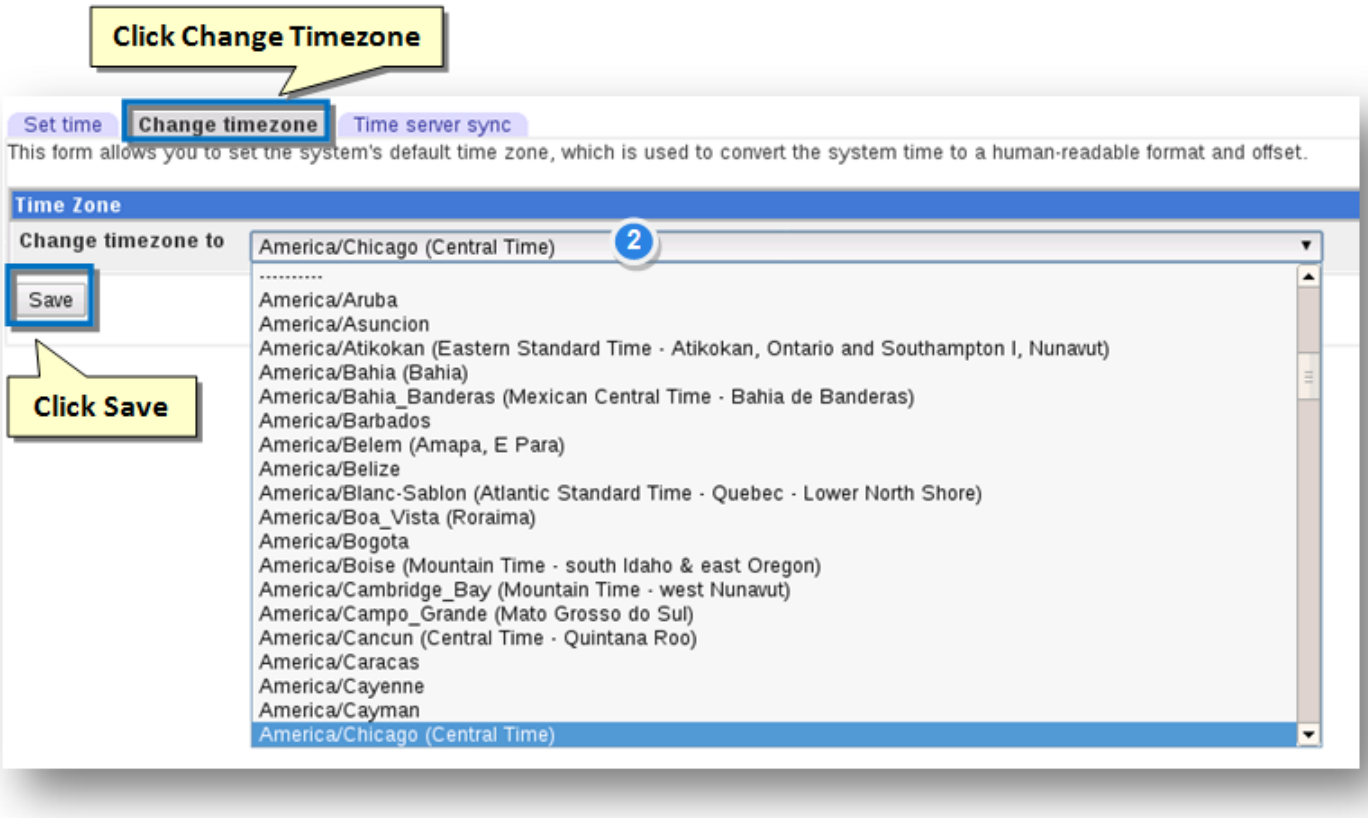
The changes made to the system time and hardware clock will be saved.

2 Changing Time Zone

This section provides the variables to set the system's default time zone, which is used to convert the system t readable format and offset.

1. Click the **Change Timezone** tab.

The **Time Zone** page will be displayed.



2. Select the required timezone from the **Change Timezone To** drop down list.
3. Click the **Save** button.

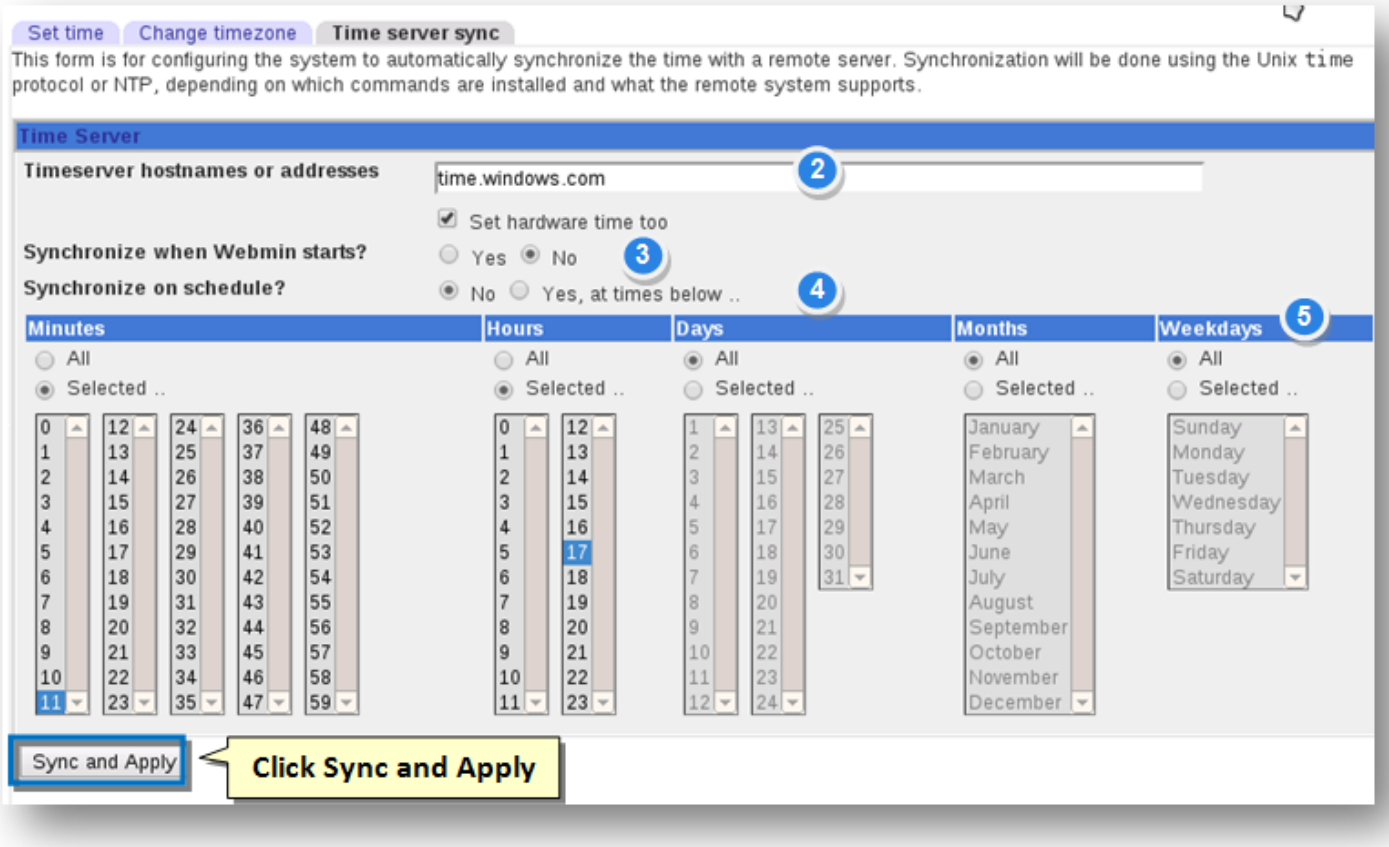
The new timezone will be set.

3 Synchronizing Time with a Remote Server

This section provides the variables to configure the system for automatic time synchronization with a remote s
Synchronization will be done using the Unix time protocol or NTP, depending on which commands are installe
remote system supports.

1. Click the **Time Server Sync** tab.

The **Time Server Sync** page will be displayed.

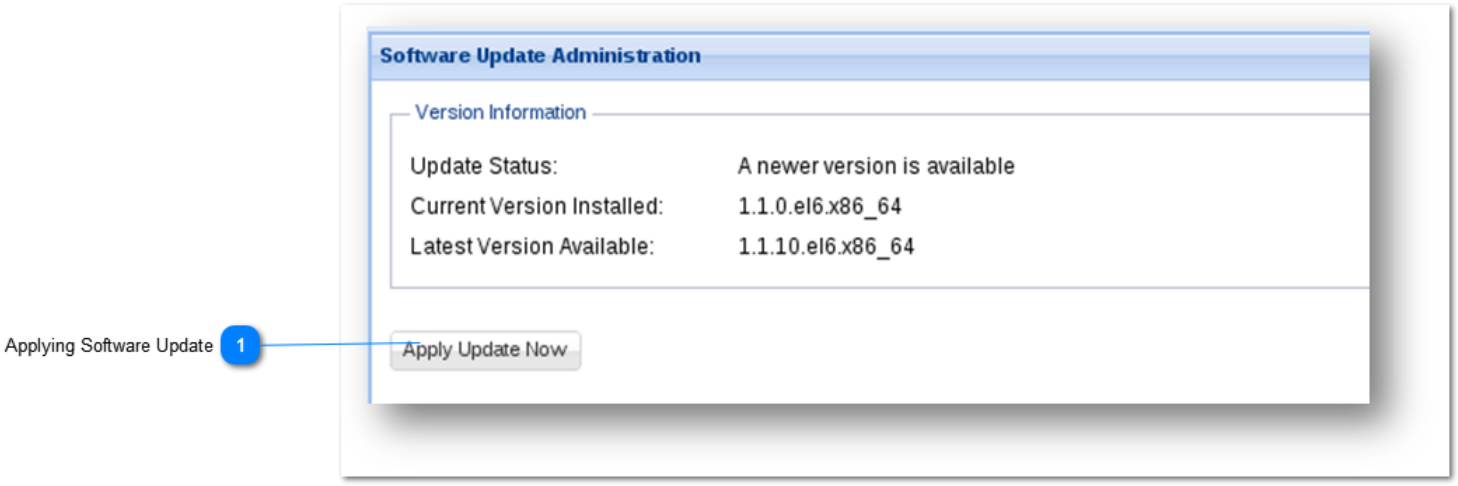


2. Enter the host names or address of the time server in the **Time Server Hostnames** or **Addresses** text entr
3. Choose whether to synchronize the time when Webmin starts or not by choosing **Yes** or **No** option.
4. Choose whether to synchronize the time on schedule. Choose the option as either **No** or **Yes** at times belo
5. If Yes, select the required time from the **Minutes, Hours, Days, Months** and **Weekdays** section.
6. Click the **Sync and Apply** button.

The system will be configured to automatically synchronize the time with a remote server.

Updating Software

After installing **SoftNAS,** it is recommended to perform a software update to ensure the latest version is installed.



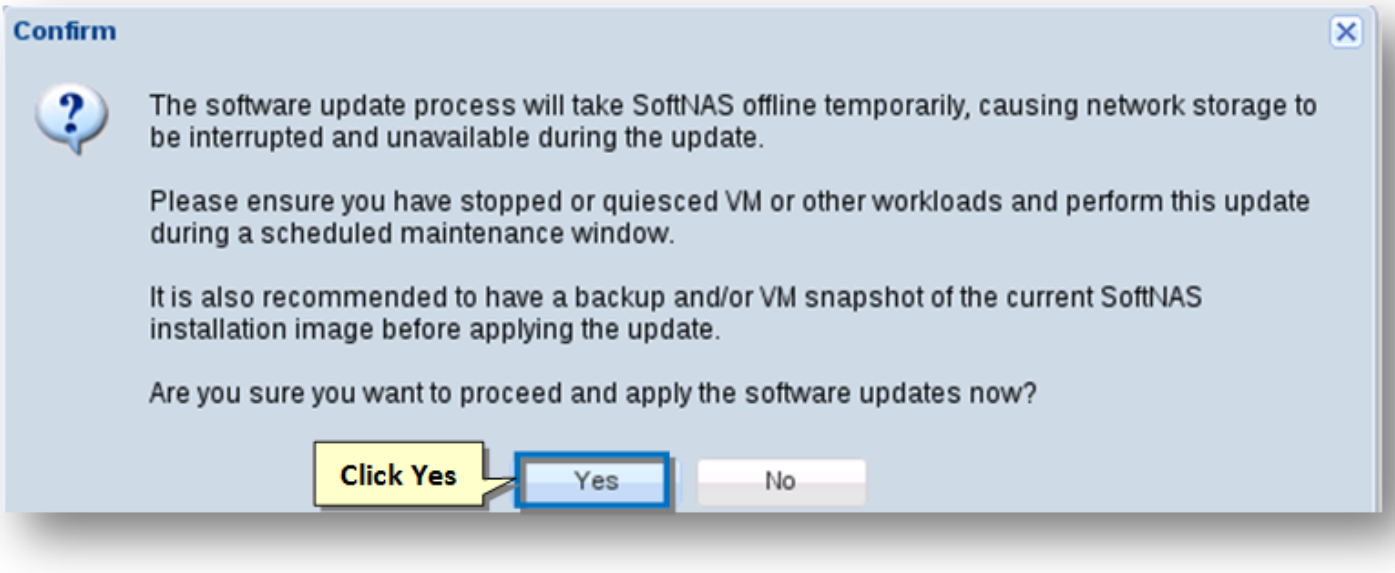
1 Applying Software Update

1. Click the **Software Updates** option under the **Settings** section in the **Left Navigation Pane.**

The **Software Updates** panel will be displayed.

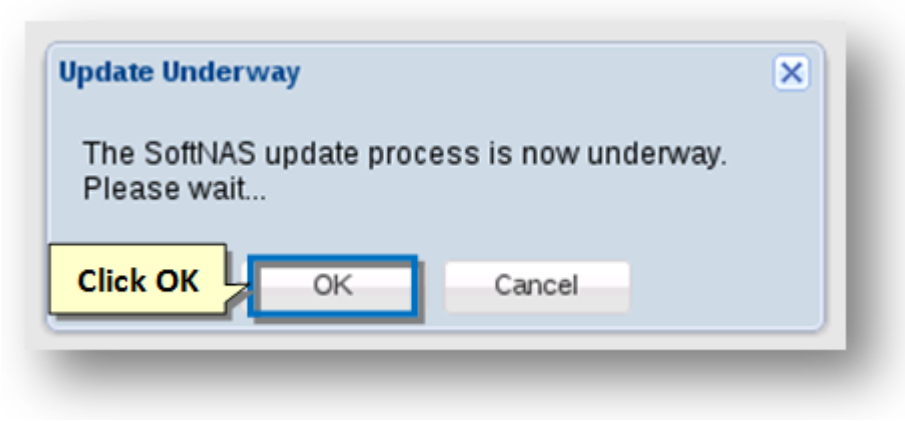
2. Click the **Apply Update Now** button.

The **Confirm** message box will emphasize best practices, such as creating a backup or VM Snapshot of the c
installation image and confirming the process of updating will be displayed.



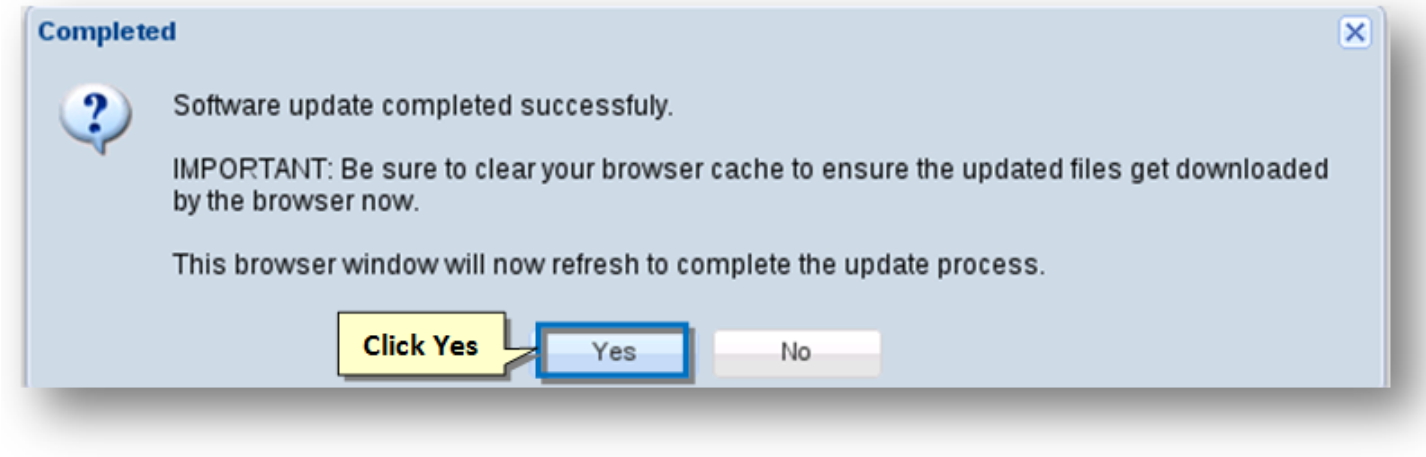
3. Click the **Yes** button.

The **Update Underway** message box informing the progress of the update process will be displayed.



4. Click the **OK** button.

The **Completed** message box confirming the successful completion of the update process will be displayed.



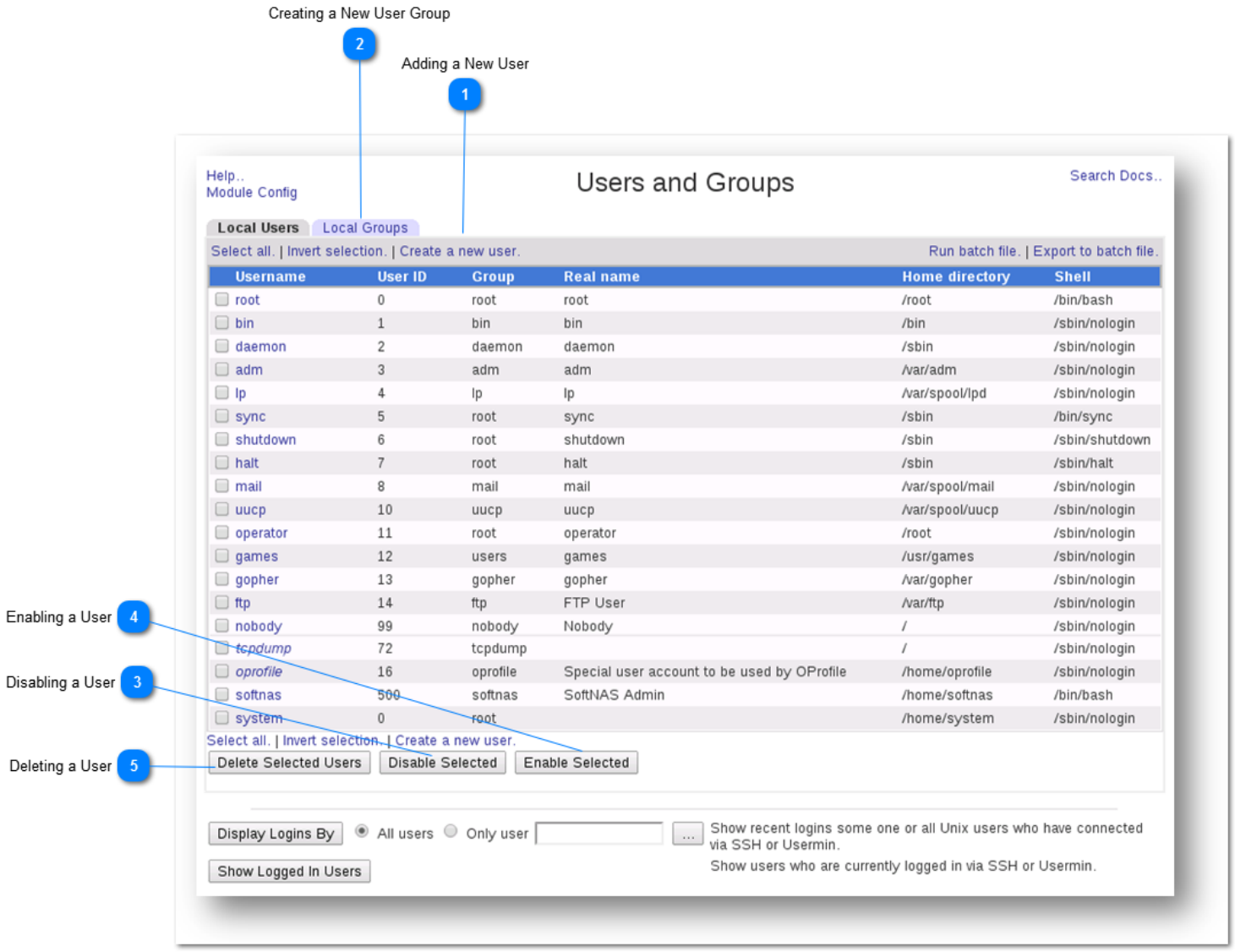
5. Click the **Yes** button.

The software update will be performed.

Note: It is better to clear the browser cache and reload the application.

Managing User Accounts

The **User Accounts** section of **SoftNAS** allows administrators to add, edit, remove and manage user groups and users.

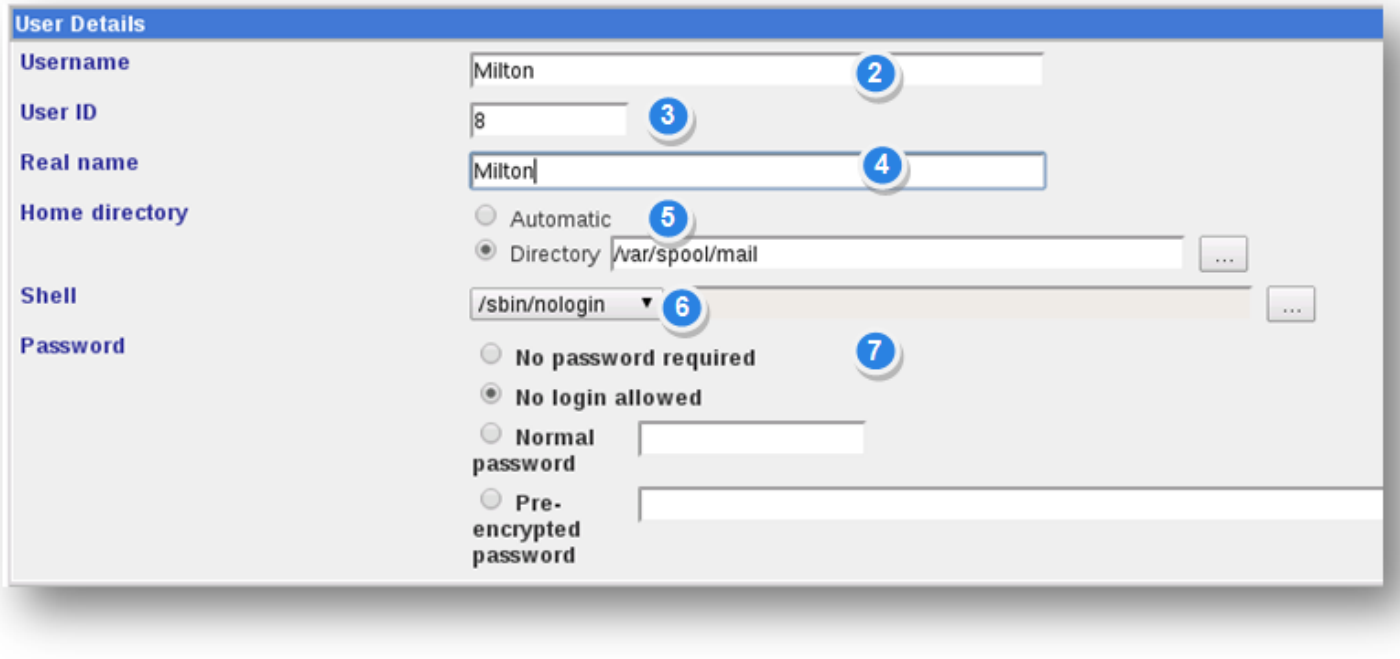


1 Adding a New User

Adding a new user is very easy. Simply follow the steps given below.

1. On the **Local Users** tab, click the **Create a New User** button.

The **Create a User** page will be displayed.



2. In the **User Details** section, enter the name of the user in the **Username** text entry box.

3. Enter the user ID in the **User ID** text entry box.

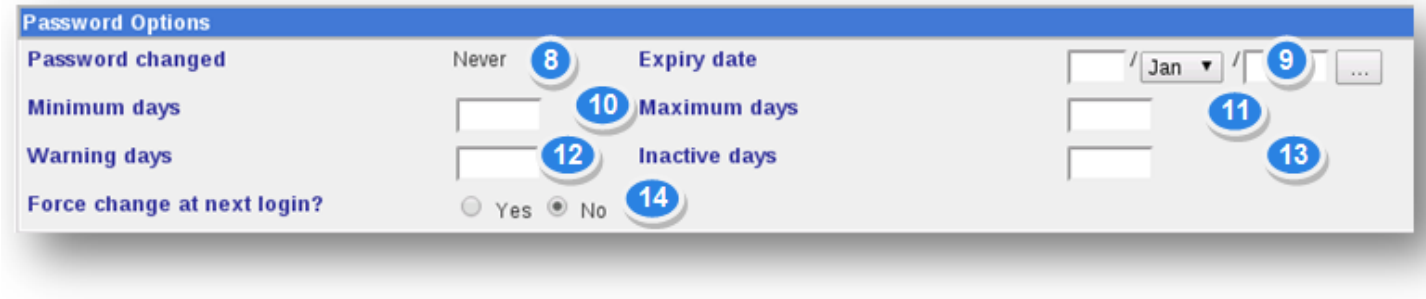
4. Enter the real name of the user in the **Real Name** text entry box.

5. Enter the home directory to which the user has access in the **Home Directory** field.

6. Select the shell from the **Shell** drop down list.

7. Specify the type of the access for the user in the **Password** field. The available options are **No password r login allowed, Normal password** and **pre-encrypted password.**

Scroll down to access more options.



8. In the **Password Options** section, the **Password Changed** field specifies when the password has been ch user.

9. Specify the date of expiry of password in the **Expiry Date** field.

10. Enter the minimum number of days for password change in the **Minimum Days** text entry box.

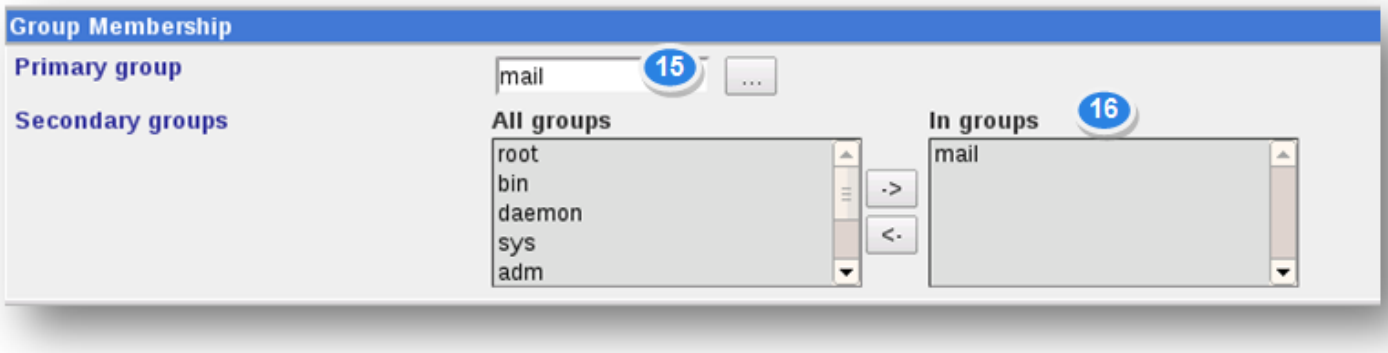
11. Enter the maximum number of days for password change in the **Maximum Days** text entry box.

12. Enter the number of days to warn in the **Warning Days** text entry box.

13. Enter the number of inactive days allowed for the user in the **Inactive Days** text entry box.

14. Specify whether the user must be forced to change the password in the next login or not by choosing **Yes**

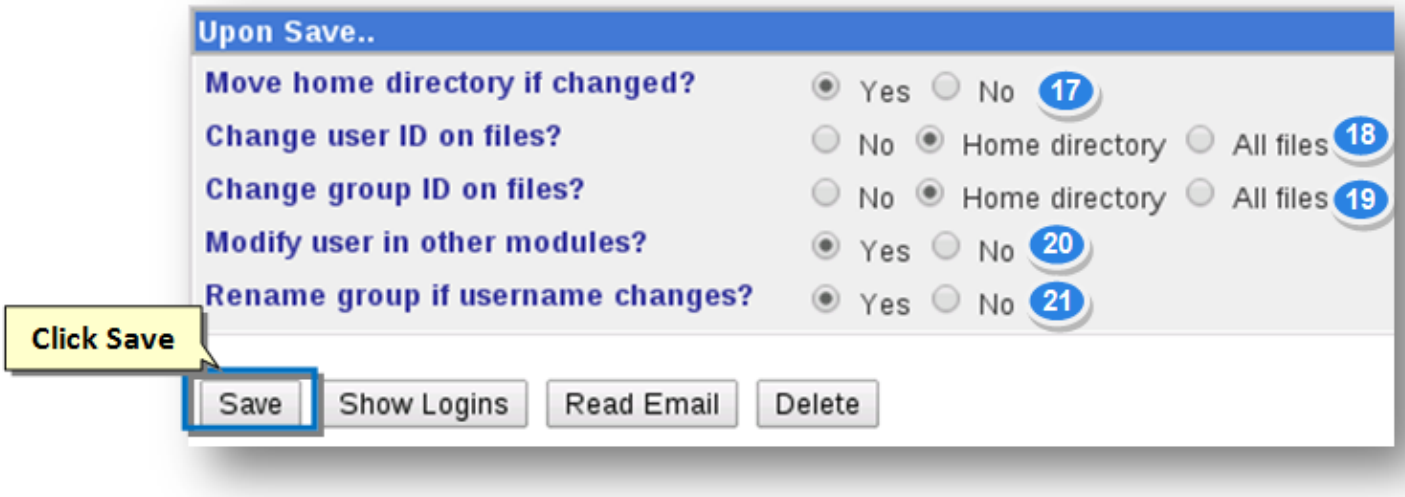
Scroll down for more options.



15. In the **Group Membership** section, select the primary group to which the user belongs to, in the **Primary**

16. Select the secondary groups for the user by choosing the groups in **All Groups** section and pressing the > them to **In Groups** section.

Scroll down for more options.



17. Specify whether the user must be moved to home directly when the directory is changed or not by choosin option.

18. Specify whether the user ID must be changed on files or not by choosing **No, Home Directory** or **Yes** opt

19. Specify whether the user group ID must be changed on files or not by choosing **No, Home Directory** or **Y**

20. Specify whether the user can be modified in other modules or not by choosing **Yes** or **No** option.

21. Specify whether the group be renamed when the user name is changed or not by choosing **Yes** or **No** opt

22. Click the **Save** button.

The new user will be added to the list of existing users.

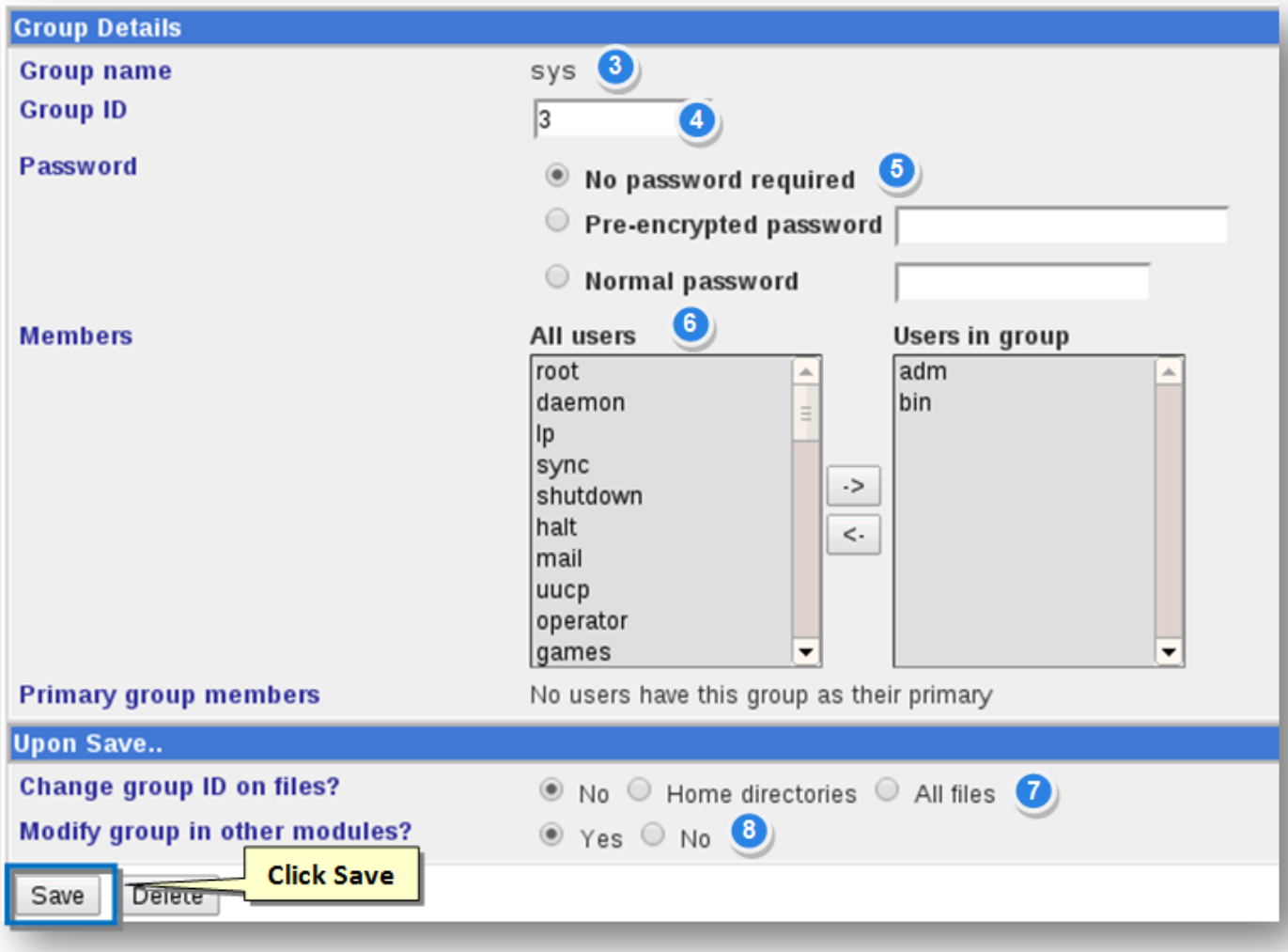
2 Creating a New User Group

Creating a New User Group is very easy. Simply follow the steps given below.

1. Navigate to **Local Groups** tab.

2. Click the **Create a New Group** button.

The **Create User Group** page will be displayed.



3. Enter the name of the group in the **Group Name** text entry box.

4. Enter the group ID in the **Group** ID text entry box.

5. Specify the type of the access for the group in the **Password** field. The available options are **No password encrypted password** and **Normal password.**

6. Select the users for the group by choosing the users in **All Users** section and pressing the **>** button to mov **Group** section.

7. In the **Upon Save** section, specify whether the group ID must be changed on files or not by choosing **No, H Yes** option.

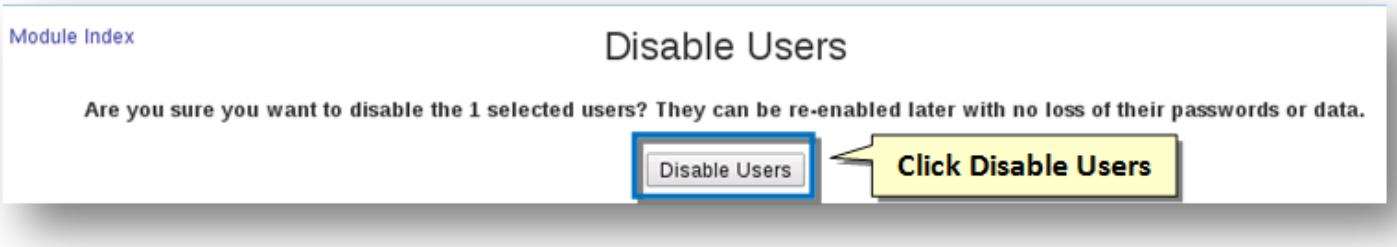
8. Specify whether the group must be modified in other modules or not by choosing **Yes** or **No** option.
9. Click the **Save** button.

The new user group will be added.

3 Disabling a User

1. Select the user ID to be disabled from the **Local Users** list.
2. Click the **Disable Selected Users** button.

The **Disable Users** page asking to confirm the disabling of the selected user will be displayed.



3. Click the **Disable Users** button.

The selected user will be disabled.

4 Enabling a User

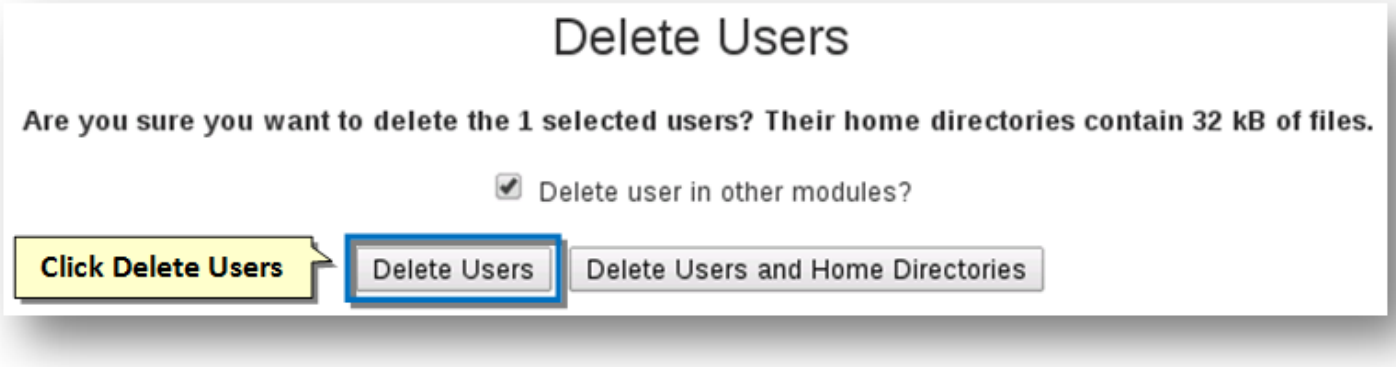
1. Select the user to enable from the **Local Users** list.
2. Click the **Enable Selected Users** button.

The **Enable Users** page confirming the enabling of the selected user will be displayed.

5 Deleting a User

1. Select the user to be deleted from the **Local Users** list.
2. Click the **Delete Selected Users** button.

The **Delete Users** page asking to confirm the deleting of the selected user will be displayed.



3. Click the **Delete Users** button.

The selected user will be deleted from all the entries at different modules.