NAS

SNAZ
USER GUIDE

Plasmon

Raidtec
SOLUTIONS

Preliminaries

Copyright statement

Trademarks

Limited warranty

Plasmon PLC makes no representation or warranties with respect to the contents or use of this user's guide, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Plasmon PLC reserves the right to make revisions on this documentation without obligation to notify any person or entity of such changes.

Modifications

Changes or modifications not expressly approved by Plasmon PLC could void the warranty.

Changes

The material in this user manual is for information only, and is subject to change without notice.

Plasmon PLC reserves the right to make changes in the product design and installation software without reservation and without notification to its users.

Additional information may be obtained from your supplier, or from the address on the back cover of this guide.

NAS

Table of Contents

NAS

Chapter 1

Introduction

SNAZ network attached file servers

The SNAZ family of network attach file servers (NAS) provide robust and easily managed file serving for departmental, branch office and medium sized company applications.

- S4-350 is a 1U 19 inch rack mount unit with 4 drive bays offering user storage of between 750GB and 1.5TB (Usable Capacity using RAID 5; the S4-350 is configured without a hot spare)
- S8-350 is a 2U 19inch rack mount unit with 8 drive bays offering user storage of up to 2TB (Usable Capacity using RAID 5). For larger capacity requirements, the associated 2U SNAZ Expansion unit extends the S8 capacity to 4TB and 6TB of user storage (Usable Capacity using RAID 5).

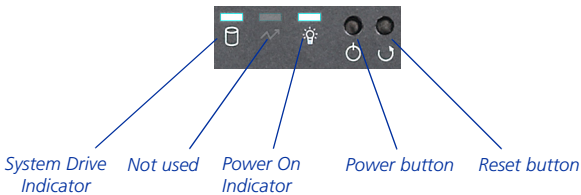
Key Features include:

- 750GB to 6TB of user storage
- SNAZ OS v4 is a dedicated Linux based, XFS journaled operating system for fast, reliable operation
- Windows CIFS and UNIX NFS support enable file sharing between Window, Linux and UNIX users.
- Dual Gigabit Ethernet (with teaming and failover) connection to the network(s)
- Powerful Xeon processor supports many simultaneous client users
- RAID 5 fault tolerance is standard with administrator configurable RAID 0, 1.

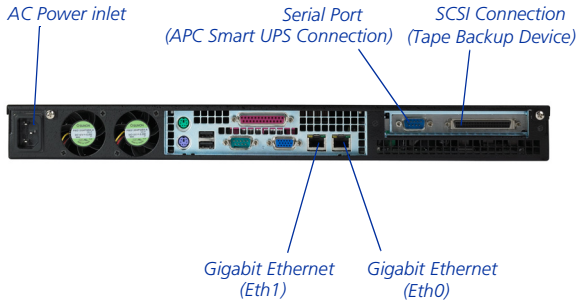
- Hot swappable SATA disk drives and hot spare disk(s) (the S4-350 is configured without a hot spare) for resilient operation.
- Browser based SNAZ Manager, gives easy installation and ongoing management with extensive context related on-screen help
- Convenient user storage management capabilities such as Group and User Quotas and on-line volume expansion
- Configurable stand alone User and File access rights as well as easy integration with Windows Active Directory.
- Powerful, built-in BakBone NetVault backup utility ensures extensive compatibility with tape drives, autoloaders and libraries and flexible back-up.
- Snapshot important data to a separate volume for almost instantaneous backup
- Replicate between SNAZ units with SNAZ Replifile for data protection.

Front panel features

The SNAZ front panel controls have the following features:



Rear panel features



Note: *SNAZ S4 rear view shown (SNAZ S8 similar)*

Chapter 2

The SNAZ Manager

Overview

This chapter describes the features of the SNAZ Manager, which administrator's use to configure and monitor the SNAZ and its Users, Groups and Shares.

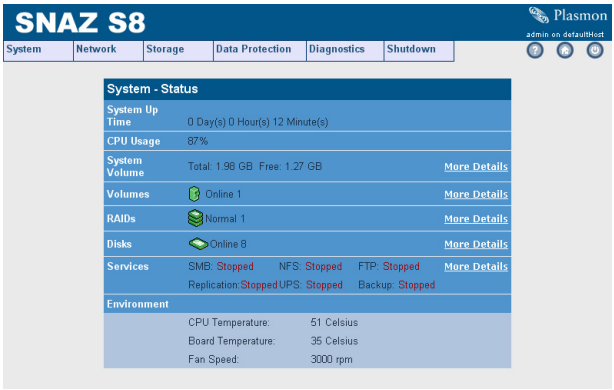
SNAZ Manager Server Configuration Wizard

The first time you start the SNAZ Manager, you'll see is the **Server Configuration Wizard**. This page allows you to perform the initial configuration of your SNAZ.

For further details of the **Server Configuration Wizard**, please refer to the *SNAZ Quick Start Guide*.

Home page features

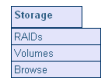
The SNAZ Manager home page gives an overview of current system status, and allows you to access all the system configuration and monitoring operations, via a menu bar along the top of the page.



Menu bar

The menu bar lets you access all the SNAZ's configuration and monitoring options, as well as the on-line help.

1 Move the pointer over a top-level menu item to reveal submenu options, for example:



2 Click on your chosen option, refer to *Table 2-1* for further information.

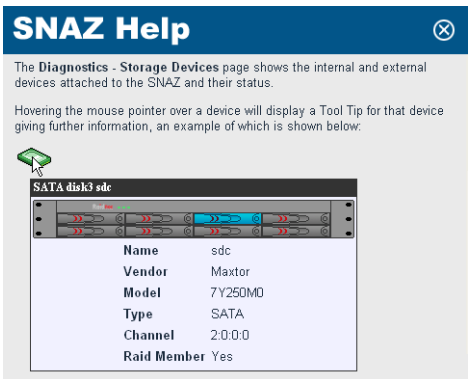
Table 2-1 SNAZ Manager menu bar

Menu/Icon	Description
System	Lets you set the time and date, update system software, manage system services and define notification recipients.
Network	Lets you configure the network settings and define users, groups and shares
Storage	Lets you define and monitor the status of volumes and RAIDs
Data Protection	Lets you configure snapshots, replications, perform a configuration backup and describes how to backup the SNAZ
Diagnostics	Lets you monitor the status of devices in and attached to the SNAZ and view the system information (serial number, software version, etc.)
Shutdown	Lets you shutdown or reboot the SNAZ
	Displays context-sensitive on-line help
	Returns you to the System - Status (home) page
	Logs you out of the current Web interface session

On-line help

Each page of the Web interface has an on-line help page associated with it. To access the on-line help for a page:

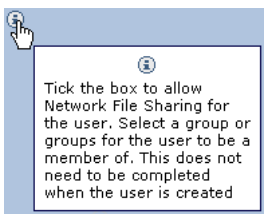
1 From the page you require help with, click the icon.
The SNAZ Help page will open in a pop-up browser Window. For example:



2 When you are finished using the on-line help, click the icon to close the Window.

Tool Tips

Whenever you see the icon next in the Web interface, you can hover over the icon to view a Tool Tip for that item.
For example:



System status

The SNAZ Manager **System - Status** (home) page automatically refreshes its content every 30 seconds and displays the following information:

- System Up Time - The amount of time which has elapsed since the SNAZ was last rebooted
- CPU Usage - The current CPU utilisation, as sampled over 3 seconds
- System Volume - The total size and amount of free space available in the System Volume
- Volumes - The number of storage Volumes present on the System and their status:

Icon	Meaning
	The volume(s) that are Online
	The volume(s) that are Offline
	The volume(s) that are Faulty

- RAIDs - The number of RAIDs present on the System and their status:

Icon	Meaning
	The RAID(s) that are Online
	The RAID(s) that are Degraded and/or Resynchronising
	The RAID(s) that are Offline

Icon	Meaning
	The RAID(s) that are Faulty

- Disks - The number of Disks present on the System and their status:

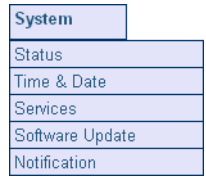
Icon	Meaning
	The Disk(s) that are Online
	The Disk(s) that are Offline
	The Disk(s) that are Faulty

- Services - The Services configured on the System and their status (Started or Stopped).

The following is shown only if your version of SNAZ enclosure has environmental monitoring hardware:

- Environmental - The SNAZ will display the CPU and motherboard temperature.

System menu



The **System** menu allows you to access:

- Status (home) page - see *System status* on page *11*
- *Time & Date*
- *Services* - see *page 15*
- *Software Update* - see *page 23*
- *Notification* - see *page 24*.

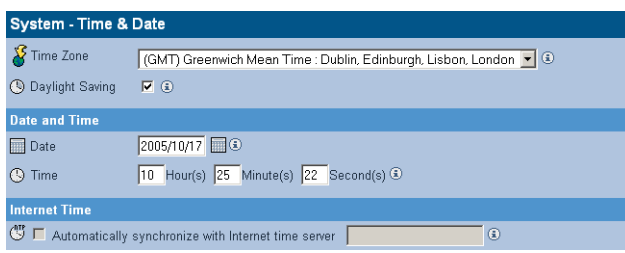
Time & Date

The **System - Time & Date** page allows you to:

- Set the time and date manually
- Synchronize the system's time with a Network Time Protocol (NTP) Server.

To set the time and date manually:

1 From the menu bar, select **System - Time & Date**.



2 Use the drop-down menus to select a **Time Zone** from the list.

3 If appropriate, tick the box for **Daylight Saving** time.

4 Set the **Date**, you can either type in the date in the format YYYY/MM/DD (e.g. 2006/07/24 for the 24th July 2006) or click on the calendar icon ( ) to show the **Select Date** pop-up:

5 Set the **Time** in the format Hour(s), Minute(s) and Second(s).

6 Click save to save the changes.

Synchronising the time and date with an NTP server

To set the time and date using an NTP server:

1 From the menu bar, select **System - Time & Date**.

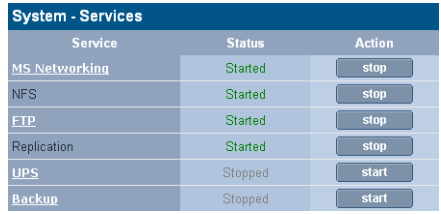
2 Tick the **Automatically synchronize with Internet time server** box and enter an NTP server URL to automatically synchronize the time with an Internet time server.

You can test the connection to the NTP server by clicking test ntp.

Note: *If you are using a SNAZ and an Active Directory Server, it is essential that their system time be synchronised. We recommend that the same NTP server is used for both the SNAZ and the Active Directory Server.*

3 Click save to save the changes.

Services



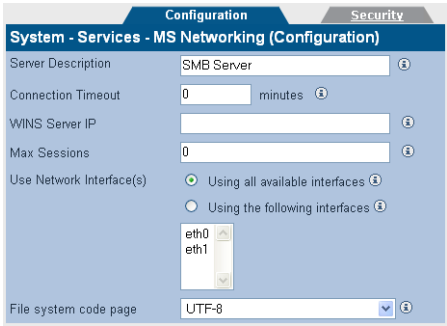
The **System - Services** page allows you to start, stop and, in some cases, configure:

- *MS Networking* - see *page 16*
- NFS - This is configured via the **Network - Shares** page - see *page 37*
- *FTP* - see *page 23*
- Replication - This is configured via the **Data Protection - Replication Target** page - see *page 63*
- *UPS* - see *page 20*
- *Backup* - see *page 22*.

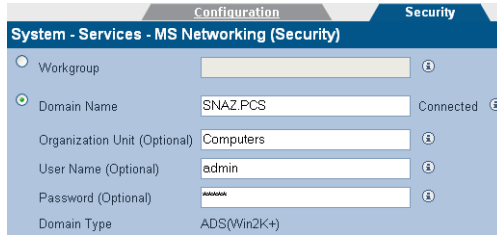
MS Networking

To configure MS Networking:

1. From the menu bar, select **System - Services** and click on **MS Networking**. The **MS Networking (Configuration)** page opens:



2. Enter a **Server Description**. This is a name (or type) description for the server.
3. If required, enter a **Connection Timeout** in minutes. This is the amount of time that connections may remain idle, with no open files, before disconnecting them from the share. The default timeout is 30 minutes.
4. If required, enter a **WINS Server ID**. This is the IP address of the Windows Internet Naming Service (WINS) server.
5. If required, enter the number of **Max Sessions**. This is the maximum number of concurrent MS Networking sessions that the SNAZ will accept. The default is 60 sessions.
6. Select whether MS Networking connects:
   - **Using all available interfaces** - to use any and all available network ports
   - **Using the following interfaces** - to use a network port specified from the drop-down list.
7. Click on the **Security** tab. This gives access to the Active Directory Server user authentication features.



8 If required, enter a **Workgroup**.
OR
Enter a **Domain Name**. This is the domain name the MS Networking service will use and is not the same as a DNS domain name.

9 If required, enter the name of the **Organization Unit** (OU) within the Active Directory structure in which the SNAZ will appear. By default, the server will appear within the OU named “Computers”.

10 If required, enter the Windows **User Name**. If a Windows User Name is entered, their **Password** must be supplied.

11 The **Domain Type** is derived from the connection to the Active Directory Server. The two types of domain are:

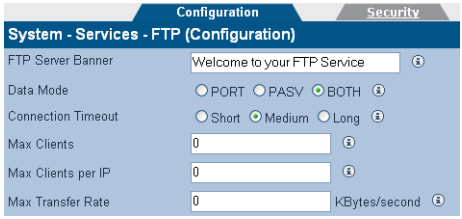
- ADS (Win2K+)
- NT Compatible.

12 Click save to save the changes.

FTP

To configure FTP access to the SNAZ:

1 From the menu bar, select **System - Services** and click on **FTP**. The **FTP (Configuration)** page opens:



2 If required, enter an **FTP Server Banner**. This is a message which will be displayed to users when they access the SNAZ via FTP.

3 Enter a **Data Mode**. The data mode can be:

- **PORT** - The client connects from a random unprivileged port (N > 1024) to the FTP server's command port, port 21. Then, the client starts listening to port N+1 and sends the FTP command PORT N+1 to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20
- **PASV** - The client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1024 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port (P > 1024) and sends the PORT P command back to the client. The client then initiates the connection from port N+1 to port P on the server to transfer data
- **BOTH** - The FTP client defines the connection method (PORT or PASV) and the server responds accordingly.

4 Enter a **Connection Timeout**. This defines how long the SNAZ should remain connected, but idle, before disconnecting.

The timeout settings for connections are:

- 30 seconds for Short
- 60 seconds for Medium
- 300 seconds for Long.

The timeout settings for transfers are:

- 150 seconds for Short
- 300 seconds for Medium
- 1500 seconds for Long.

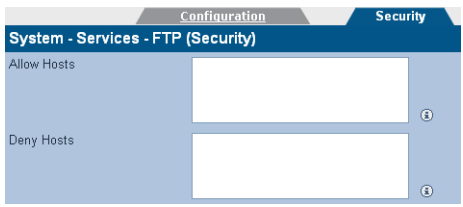
5 Enter **Max Clients**. This is the maximum number of concurrent FTP client connections.

6 Enter **Max Clients per IP**. This is the maximum number of concurrent FTP client connections per IP address.

7 Enter the **Max Transfer Rate**. This is the maximum rate, in Bytes, of FTP data transfer.

8 Click on the **Security** tab. This allows you to enter IP addresses and/or hostnames which you wish to explicitly Allow or Deny FTP access to the SNAZ.

Note: *When hosts are added to either the Allow or Deny lists, all other hosts automatically become marked as the opposite, unless they are specified otherwise.*



9 Click save to save the changes and, as appropriate, click start to start or click stop to stop the service.

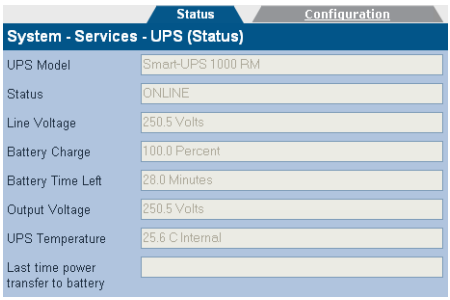
UPS

The information in the **System - Services - UPS** page is derived from the UPS itself.

Refer to your UPS's documentation for further details.

> Note: *The SNAZ only supports APC Smart brand UPSs.*

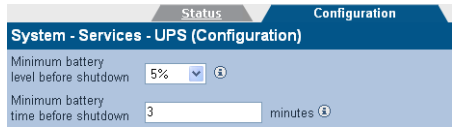
1 From the menu bar, select **System - Services** and click on **UPS**. The **UPS (Status)** page opens:



- **UPS Model** - The type of UPS attached to the SNAZ
- **Status** - The UPS's status (e.g ONLINE,)
- **Line Voltage** - The UPS's input voltage
- **Battery Charge** - The amount of battery charge, in percent, remaining
- **Battery Time Left** - The amount of battery charge, in minutes, remaining
- **Output Voltage** - The UPS's output voltage (to the SNAZ)
- **UPS Temperature** - The temperature of the UPS enclosure
- **Last time power was transferred to UPS** - The last time the power was transferred from the mains supply to the UPS.

2 Click on the **Configuration** tab. This allows you to configure:

- **Minimum battery level before shutdown** - Select the minimum UPS battery level, in percent, prior to the SNAZ shutting down from the drop-down list
- **Minimum battery time before shutdown** - Enter the minimum UPS battery time remaining, in minutes, prior to the SNAZ shutting down.

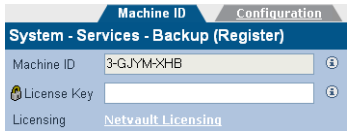


3 Click save to save the changes and, as appropriate, click start to start or click stop to stop the service.

Backup

The SNAZ uses preinstalled BakBone NetVault software to perform system data backups.

1 From the menu bar, select **System - Services** and click on **Backup**. The **Backup (Register)** page opens:



The **Machine ID** was automatically generated at the time the NetVault Software was installed on the SNAZ.

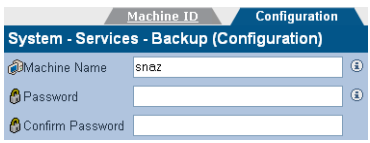
2 Enter the **License Key**. When the SNAZ system is registered, via the Plasmon Warranty Registration website, the License Key will be supplied by email and should be entered here.

3 Click the register button to complete the software registration.

A message bar will indicate the success or failure of the registration, along with troubleshooting information. In the event of any errors or problems, please contact Plasmon Technical Support.

A hyperlink to the Plasmon Warranty Registration website is also presented.

4 Click on the **Configuration** tab.



5 Enter a **Machine Name**. To allow the distinction between different devices within a NetVault environment, a unique Machine Name will be generated for your SNAZ.

6 Enter a Password and then **Confirm Password** if you wish to restrict client access to the Backup services.

7 Click save to save the changes and, as appropriate, click start to start or click stop to stop the service.

Software Update

The **System - Software Update** page allows you to update the System software using:

- *HTTP* - from a local computer
- *FTP* - from the ftp.plasmon.com website.

HTTP

To update the System software using HTTP:

1 From the menu bar, select **System - Software Update**. The **Software Update (HTTP)** page opens:

2 Enter the **Software Image File** path to a local copy of the SNAZ OS software image or click browse to search.

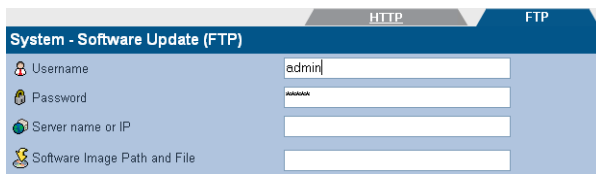
3 Click upload to begin the software update.

Follow the on-screen instructions to complete the installation.

FTP

To update the System software using FTP:

1 From the menu bar, select **System - Software Update**. Click on the **FTP** tab.



2 Enter an FTP **Username** and that username's **Password**.

3 Enter the **Server name or IP** address for the FTP site.

4 Enter the **Software Image Path and File** to the copy of the SNAZ OS software image.

5 Click transfer to begin the software update.

Follow the on-screen instructions to complete the installation.

Notification

The SNAZ allows for system administrator's to be notified of system events and errors by means of:

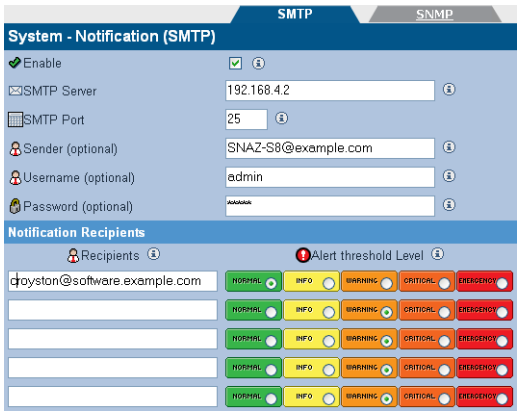
- *Email (SMTP) Notification*
- *SNMP Notification* - see *page 26*.

> Note: *Both email and SNMP notification services can be running at the same time.*

Email (SMTP) Notification

To enable email (SMTP) notification:

1 From the menu bar, select **System - Notification**. The **System - Notification (SMTP)** page opens:



2 Tick the **Enable** box to enable, or un.tick to disable, the email notification service.

3 Enter an **SMTP Server** (mail server) name or IP address.

4 Enter an **SMTP Port**. The normal port used for email is 25.

5 If required, you can add a **Sender** to your notifications.

6 If required, you can add a **Username** to the notifications. If a username is added, that user's **Password** also needs to be entered.

7 Enter the email address(es) of up to five email notification **Recipients**.

8 Select an **Alert Threshold Level** for each recipient. These are described below:

Table 2-2 Notification Alert Threshold Levels

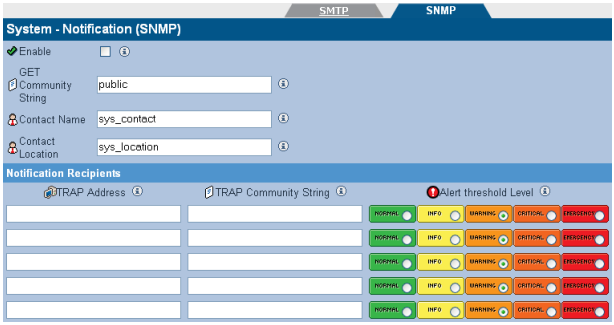
Level	Meaning
NORMAL	These notifications require no action. This level includes all notifications
INFO	These notifications may require some action to be taken. This level includes Warning, Critical and Emergency level notifications
WARNING	These notifications require that action should be take to keep the SNAZ operating at maximum efficiency. This level includes Critical and Emergency level notifications
CRITICAL	These notifications require that action must be taken. This level includes Emergency level notifications
EMERGENCY	These notifications require that action must immediately be taken. This level includes only Emergency level notifications

9 Click save to save the changes, test alert to test SNMP notification (a test notification is sent to each recipient) or click history to view the **Notification Log**.

SNMP Notification

To enable SNMP notification:

1 From the menu bar, select **System - Notification**. Click on the **SNMP** tab. The **System - Notification (SNMP)** page opens:



2 Tick the **Enable** box to enable, or untick to disable, the SNMP notification service.

3 Enter a **GET Community String**. By default the SNAZ does not use Community Strings to authenticate sent notifications. However, if required, a Community String can be entered here to enable this function.

4 Enter a **Contact Name** for SNMP notifications. The Contact Name specifies the person to contact for the host, and how you can contact this person (such as by telephone extension or email address), for example: *John Smith, X 1234, smith@plasmon.com*.

5 Enter a **Contact Location** for SNMP notifications. The Contact Location specifies the geographical location of the host, for example: *SNAZ-S4, Server Room 2, Plasmon HQ, UK*.

6 Enter the **TRAP Address** (IP addresses) and **TRAP Community String** of up to five SNMP notification **Recipients**.

7 Select an **Alert Threshold Level** for each recipient. These are described below:

Table 2-3 Notification Alert Threshold Levels

Level	Meaning
NORMAL	These notifications require no action. This level includes all notifications
INFO	These notifications may require some action to be taken. This level includes Warning, Critical and Emergency level notifications
WARNING	These notifications require that action should be take to keep the SNAZ operating at maximum efficiency. This level includes Critical and Emergency level notifications
CRITICAL	These notifications require that action must be taken. This level includes Emergency level notifications
EMERGENCY	These notifications require that action must immediately be taken. This level includes only Emergency level notifications

8 Click save to save the changes, test alert to test SNMP notification (a test notification is sent to each recipient) or click history to view the **Notification Log**.

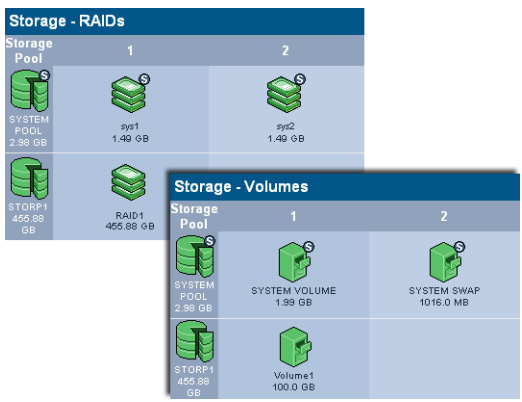
Shares on the SNAZ

Shares are used to give specified users controlled access to specific folders and subfolders on the SNAZ system, from their client computers.

This section does not detail how to create the individual components of the Share (such as RAIDs and Volumes), it is intended to demonstrate the process involved in creating a Share.

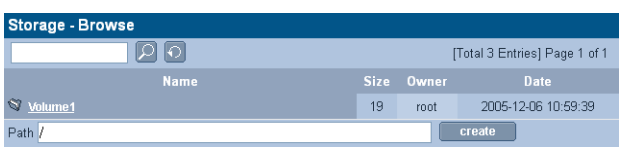
How a Share is created

Our example SNAZ system has a previously created RAID (called RAID1), containing a Volume (called Volume1):



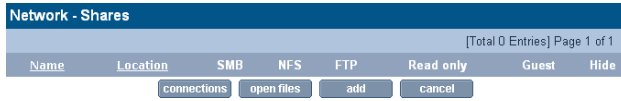
Our example SNAZ system also has some users (called User2 and User3), who are members of a group (called Group1).

From the **Storage - Browse** screen, the Volume looks like this:



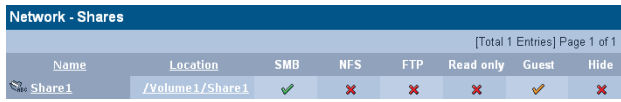
To create an accessible Share (in this example Windows SMB):

1 From the menu bar, select **Network - Shares**:

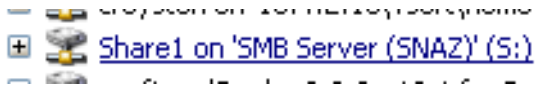


Then click add.

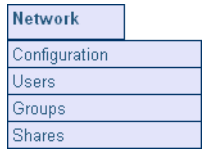
2 A Share is then created, as shown in *Adding a Share* on page *37*, called Share1 (with Group1 given access):



A Share now exists that users can access from their Windows client computers, as they would for any other network file share:



Network menu



The Network menu allows you to access:

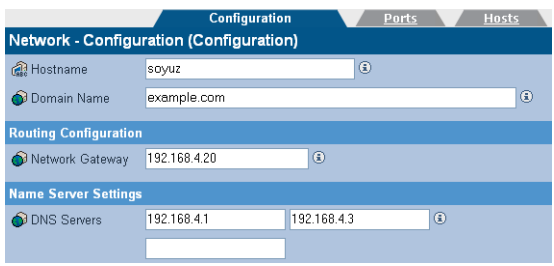
- *Configuration*
- *Users*
- *Groups*
- *Shares*

Configuration

The information in the **Network - Configuration** page is usually entered via the Server Configuration Wizard (which runs automatically during the initial installation of the SNAZ system).

To configure the Network settings:

1 From the menu bar, select **Network - Configuration**.



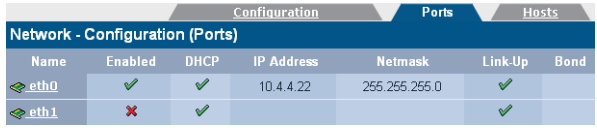
2 Enter a **Hostname** for the SNAZ.

3 Enter the **Domain Name** which the SNAZ is attached to.

4 Enter your **Network Gateway** IP address or hostname.

5 Enter the IP address(es) of up to 3 **DNS Servers**. Multiple DNS Servers are usually used to provide fail-over Domain Name resolution.

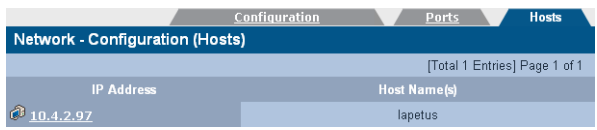
6 Click on the **Ports** tab. The SNAZ's network (Ethernet) ports are listed:



The following information is also displayed:

- **Name** - The Ethernet port name. The SNAZ has two Ethernet ports *eth0* and *eth1*. Clicking on the port Name allows you to view the network ports configuration.
- **Enabled** - Shows whether the Ethernet port is enabled.
- **DHCP** - Shows whether the DHCP is enabled.
- **IP Address** - Shows the IP address of the port
- **Netmask** - Shows the Network mask of the port
- **Link up** - Whether the two ports are linked
- **Bond** - Whether or not the ports are bonded. This is used to provide load balancing (where the two ethernet cards share network activity to prevent overloading) or fault tolerance (where one ethernet card is used, the other being kept as a backup in case of failure of the first).

7 Click on the **Hosts** tab.



8 Click 

to add a host. This page allows you to enter a list of Hosts which are known to the SNAZ. This list is used to resolve hosts when DNS is not available.

9 Click 

to save the changes.

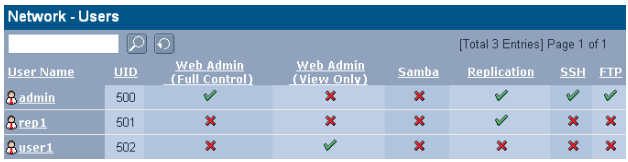
Users

The **Network - Users** page lists all the Users known to the system.

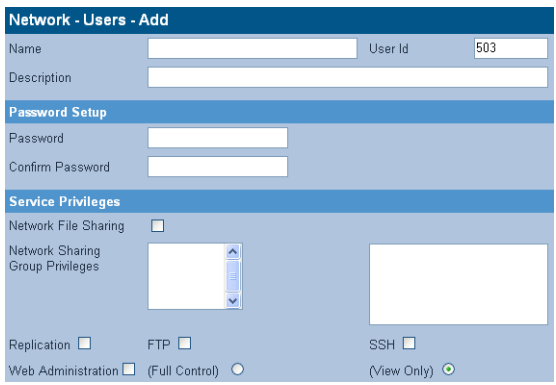
Adding a User

To add a User:

1 From the menu bar, select **Network - Users**.



2 Click add. The **Network - Users - Add** page is displayed:



3 Enter the User's **Name**. A **User Id** is automatically generated.

4 Enter a **Description** for the User.

5 Enter a and confirm the User's **Password** (this is mandatory).

6 Tick the **Network File Sharing** box to enable NFS for the User and select a Group from the **Network Sharing Group Privileges** list.

7 If the User is to have replication privileges, tick the **Replication** box.

8 If the User is to have FTP access privileges, tick the **FTP** box.

9 If the User is to have SSH access privileges, tick the **SSH** box. SSH is a way to log into another computer over a network using a command line (console) interface.

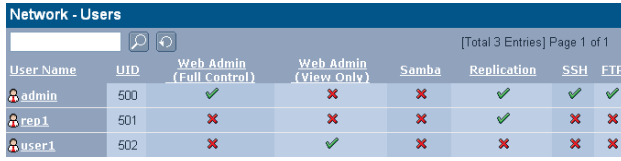
10 If the User is to have Web administration access privileges, tick the **Web Administration** box. By default the User will have **View Only** privileges. If required, select the **Full Control** radio button.

11 Click add to add the User.

Deleting a User

To delete a User:

1 From the menu bar, select **Network - Users**.



2 Click the User Name of the User you wish to delete. The **Network - Users - Update** page is displayed.

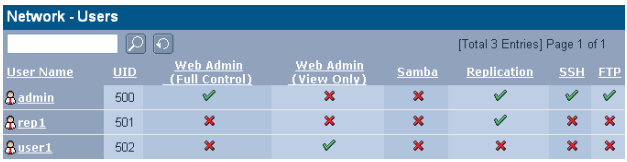
3 Click delete.

4 A warning message is displayed. Click delete to confirm deletion of the user.

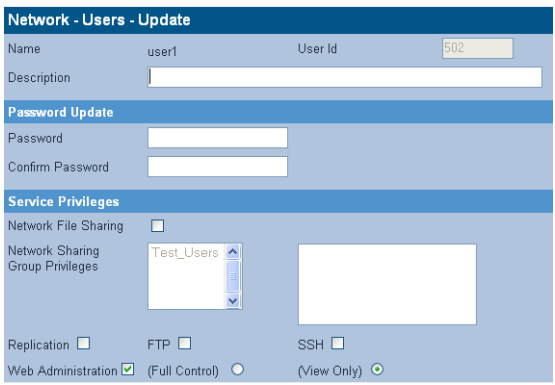
Editing a User's details

To edit a User's details:

1 From the menu bar, select **Network - Users**.



2 Click the **User Name** of the User you wish to edit. The **Network - Users - Update** page is displayed:



3 You can edit the User's **Description**, **Password** or change their **Service Privileges**.

4 Click save to save the changes.

Groups

The **Network - Groups** page lists all the Groups known to the system and allows you to add, edit or delete Groups from the system.

Adding a Group

To add a Group:

1 From the menu bar, select **Network - Groups**:

2 Click add. The **Network - Groups - Add** page is displayed:

3 Enter a **Name** for the Group.

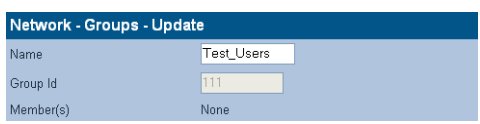
4 Click add to add the Group.

Editing a Group's details

You can only edit the Name of a Group. To edit a Group's name:

1 From the menu bar, select **Network - Groups**.

2 Click the **Name** of the Group you wish to edit. The **Network - Groups - Update** page is displayed:



3 Edit the Group's **Name**.

4 Click save to save the changes.

Deleting a Group

To delete a Group:

1 From the menu bar, select **Network - Groups**.

2 Click the **Name** of the Group you wish to delete. The **Network - Groups - Update** page is displayed:

3 Click delete.

4 A warning message is displayed. Click delete to confirm deletion of the Group.

Shares

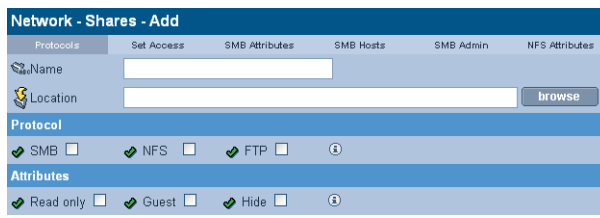
The **Network - Shares** page allows you to view, edit and delete Shares from the system. It is also used to view active connections and open files and configure access (ACLs) to the various Shares on the system.

Adding a Share

To add a Share:

1 From the menu bar, select **Network - Shares**.

2 Click add. The **Network - Shares - Add** page, **Protocols** tab is displayed:



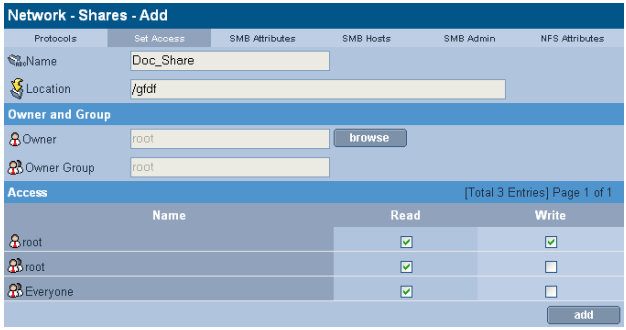
3 Enter a **Name** for the Share.

4 Enter a **Location** for the Share or click browse to browse for a location.

5 Tick one or more **Protocol** box. This defines how the Users will access the Share.

6 Tick one or more **Attributes** box. This defines what access privileges Users will have on the Share.

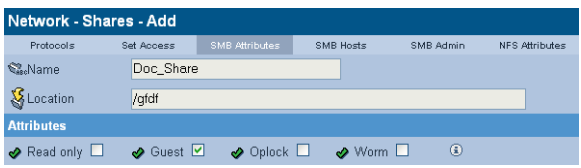
7 Click next >>, the **Set Access** tab is displayed:



8 The default **Owner** and **Owner Group** are displayed (The current logged in User). Click browse to browse for a specific User.

9 To give specific Users access to the share, click add to browse.

10 Click next >>, the **SMB Attributes** tab is displayed:



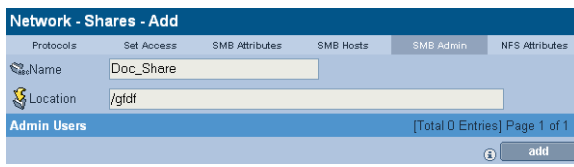
11 Enter the **Attributes** for Windows (SMB) access to the Share.

12 Click next >>, the **SMB Hosts** tab is displayed:

13 Enter the hostnames or IP addresses of Hosts you specifically want to be allowed or denied access to the Share.

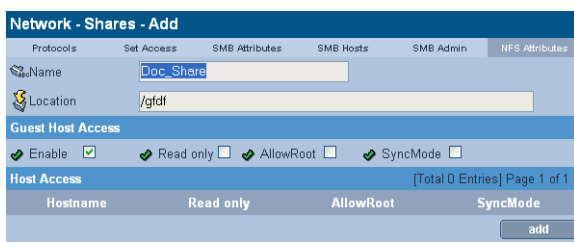
Note: *When hosts are added to either the Allow or Deny lists, all other hosts automatically become marked as the opposite, unless they are specified otherwise.*

14 Click next >>, the **SMB Admin** tab is displayed:



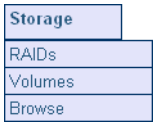
15 Click add to add an Administrator User for this Share.

16 Click next >>, the **NFS Attributes** tab is displayed:



17 Click add to add NFS Hosts to the Share.

Storage menu



The Storage menu allows you to access:

- *RAIDs*
- *Volumes*
- *Browse*

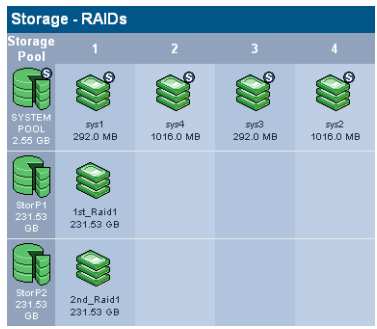
RAIDs

The **Storage - RAIDs** page allows you to view, add or remove RAIDs on the system. You can also define hot spare disks.

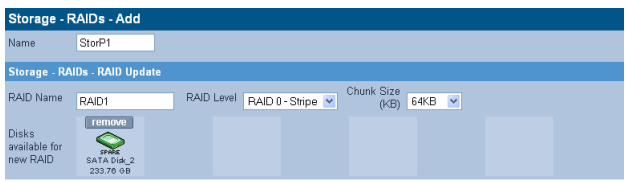
Adding a RAID

To add a RAID:

1 From the menu bar, select **Storage - RAIDs**.



2 Click new. The **Storage - RAIDs - Add** page opens:



3 A Pool **Name** is automatically generated for the RAID to be a member of. You can also enter your own (up to 7 characters e.g. StorP1).

4 A **RAID Name** is automatically generated. You can also enter your own (e.g. RAID1 or 1st_RAID).

5 Select a **RAID Level** from the drop-down list. This can be either:

- **RAID 0** - RAID 0 is a striped disk array without fault tolerance. Provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost
- **RAID 1** - RAID 1 provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks
- **RAID 5** - RAID 5 provides data striping at the byte level and also stripe error correction information. This results in excellent performance and good fault tolerance. Level 5 is one of the most popular implementations of RAID.

6 Select a **Chunk Size (KB)** from the drop-down list. This is the size of the data chunks written to each disk.

7 Select the disks you wish to be members of the RAID from the **Disks available for new RAID** list. The new RAID will allocate all available storage space on those disks to the RAID.

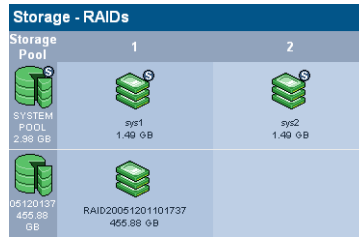
8 Click 

to add the new RAID.

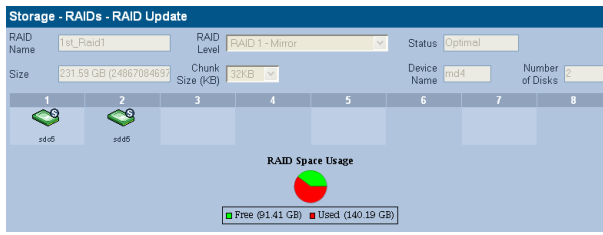
Removing a RAID

To remove a RAID:

1 From the menu bar, select **Storage - RAIDs**.



2 Click on the RAID you wish to remove. The **Storage - RAIDs - RAID Update** page opens.



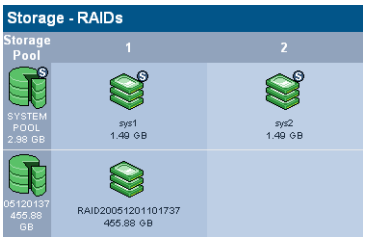
3 Click remove. You will be prompted to confirm you wish to delete the RAID. Click remove again to confirm or click cancel to cancel.

Defining Hot Spares

Hot spare disks can be defined to provide fault tolerance in RAIDs. A disk which has been marked as a hot spare will automatically take the place of a failed disks in any RAID.

To mark a disk as a hot spare:

1 From the menu bar, select **Storage - RAIDs**.



2 Click hot spares. The **Storage - RAIDs - Hot Spares** page will open:

3 Tick the box(es) of disk(s) which you wish to mark as hot spare.

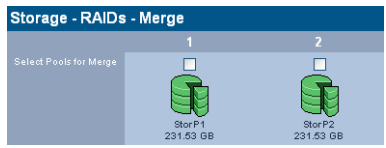
4 Click set to set the hot spare(s).

5 Click finish to save the changes and return to the **Storage - RAIDs** page.

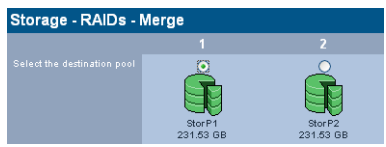
Merging RAIDs (Pools)

To merge storage pools:

1. Create a new RAID - see *Adding a RAID* on page *41*.
2. From the menu bar, select **Storage - RAIDs**.
3. Click merge. The **Storage - RAIDs - Merge** page will open:



4. Select the pools (RAIDs) to merge and click next >>.
5. Select the destination pool (the pool which will remain after the merge):



6. Then click merge. When the pools have successfully merged, the SNAZ Manager will return to the **Storage - RAIDs** page.

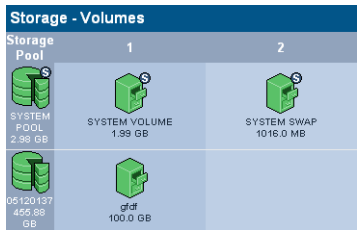
Volumes

The **Storage - Volumes** page allows you to view, add or remove Volumes from the system.

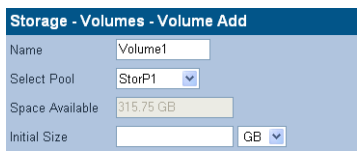
Adding a volume

To add a Volume:

1 From the menu bar, select **Storage - Volumes**.



2 Click add. The **Storage -Volumes - Volume Add** page opens:



3 A **Name** is automatically generated. You can also enter your own (up to 32 characters; a-z, A-Z, 0-9, - (hyphen) and _ (underscore) e.g. Volume_1).

4 Select a Pool that the Volume should be in from the **Select Pool** drop-down list.

5 Enter an **Initial Size** for the Volume.

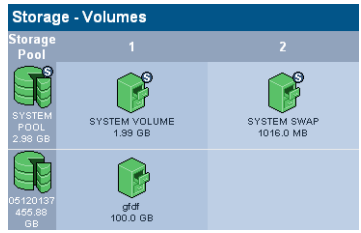
Note: *When creating an initial size for the new volume, we recommend that 20% of the available space should be kept for Snapshot use or for future expansion of the Volume. The system will warn you if this is not the case.*

6 Click add to add the new Volume.

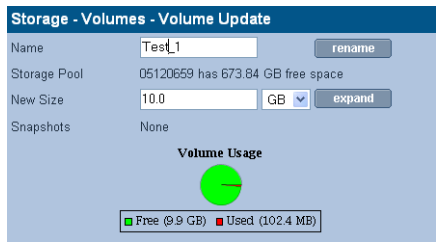
Removing a Volume

To remove a Volume:

1 From the menu bar, select **Storage - Volumes**.



2 Click on the Volume you wish to remove. The **Storage - Volumes - Volume Update** page opens:



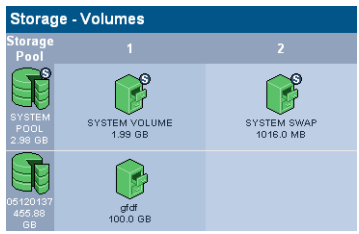
3 Click remove. You will be prompted to confirm you wish to delete the Volume. Click remove again to confirm or click to cancel.

Changing a User's Volume Quota

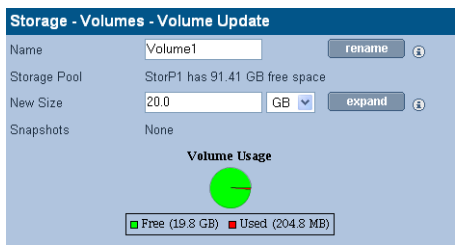
Users can be allocated a specific amount of a Volume which they can use. This amount is called their Quota.

To change a user's Quota:

1 From the menu bar, select **Storage - Volumes**:

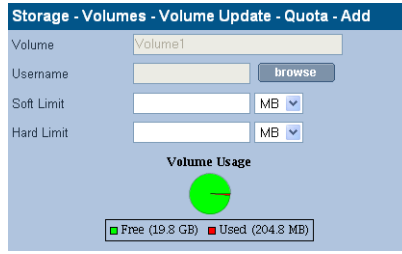


2 Click on the Volume you wish to change the Quota of. The **Storage -Volumes - Volume Update** page opens:

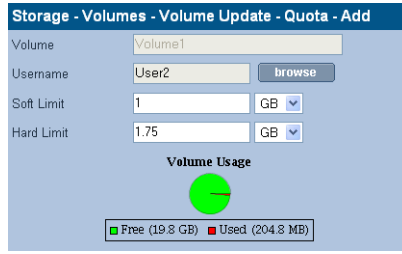


3 Click quota. The **Storage - Volumes - Volume Update - Quota** page opens:

4 Click add. The **Storage - Volumes - Volume Update - Quota - Add** page opens:



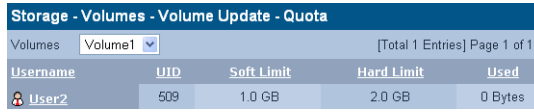
5 Click browse to add a User to allocate the Quota to:



For that user, enter:

- **Soft Limit** - to restrict the users quota, however, if a file is written which exceeds the Soft Limit, the file will still be written, as long as the Hard Limit is not exceeded
- **Hard Limit** - The total amount of disk space allocated to the specified user. The user cannot exceed this limit.

6 Click add. The **Storage - Volumes - Volume Update - Quota** page opens, displaying the user's new quota:



Browse

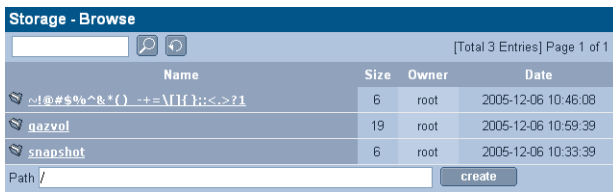
The **Storage - Browse** page allows you to search or browse through the directories present on the system.

> Note: *If you are using Active Directory to provide access control, ignore this section and refer to MS Networking on page 16.*

Finding data

To search for a file:

1 From the menu bar, select **Storage - Browse**.



Enter a search string in the text box and click .

Click to reset the content of the text box.

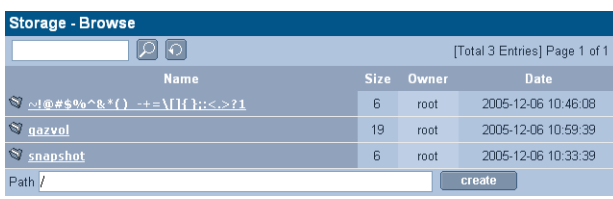
Alternatively, you can manually browse the directory tree for a file.

Setting or modifying an ACL

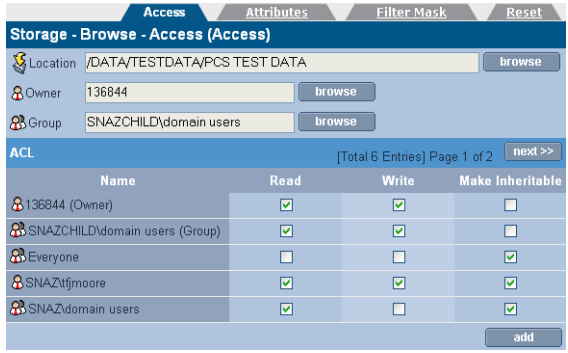
Clicking on a file or directory will take you to the **Storage - Browse - Access** page. From there you can change the access privileges, known as Access Control Lists or ACLs, Groups and Users have.

To change a Group's or User's access privileges (set or modify ACLs):

1 From the menu bar, select **Storage - Browse**.



2 Search or browse to a directory or file. Click on access. The **Storage - Browse - Access** page opens.

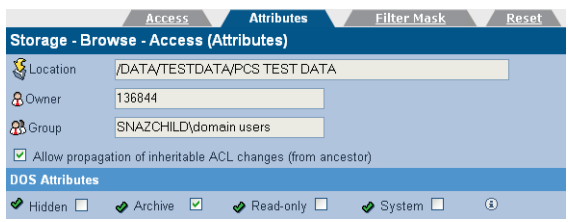


From this page you can:

- View the current **Location**. Click browse to browse to another directory
- View the directory's **Owner** and **Owner Group**. Click browse to browse for another Owner or Owner Group
- **ACL** - This section lists the Users and Groups who have access to the directory and their access privileges.

  Click add to add more Users or Groups.

3 Click the **Attributes** tab.



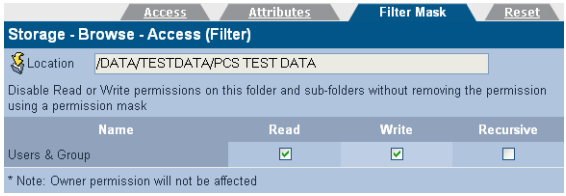
From this tab you can:

- **Allow propagation of inheritable ACL changes (from ancestor)** - This can be used to pass access privileges from the current directory to its sub-directories. In this way, you

can place a single ACL high up in the directory tree to control access

- You can also set the **DOS Attributes** for the directory.

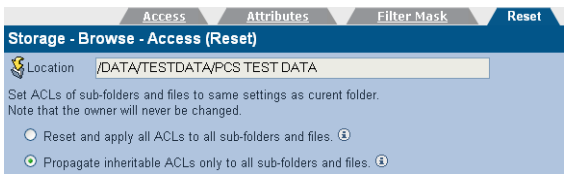
4 Click the **Filter Mask** tab.



From this tab you can:

- Set a **Filter Mask** - This is a way of temporarily modifying the access privileges of the current directory, without changing all the ACLs beneath it.

5 Click the **Reset** tab.



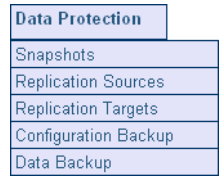
From this tab you can reset the access permission of sub-directories to be the same as the current directory, as follows:

- **Reset and apply all ACLs to all sub-folders and files** - This option will reset and then apply the current folder's access properties to all sub-folders and files
- **Propagate inheritable ACLs only to all sub-folders and files** - This option will apply the current folder's access properties, which are marked as Make Inheritable, to all sub-folders and files.

6 When the ACLs have been satisfactorily set, click 

to save the changes.

Data protection menu



The Data Protection menu allows you to access:

- *Snapshots*
- *Replication Sources* - see *page 59*
- *Replication Targets* - see *page 63*

  Note: *Replications require at least two SNAZ (OS version 4) systems to operate; a Source which generates the data to be replicated and a Target (or targets) for the replicated data to be written to.*

- *Configuration Backup* - see *page 64*
- *Data Backup* - see *page 66*. The **Data Protection - Data Backup** page only contains details of how the NetVault software should be configured. To change the settings or enter the BakBone NetVault License Key, via the **System - Services - Backup** page - see *page 22*.

Snapshots

The **Data Protection - Snapshot** page lists all the snapshot schedules on the system and allows you to add or modify snapshots.

> Note: *A snapshot can only be added when a Volume has been created.*

Estimating snapshot volume requirements

When estimating the snapshot volume requirements, the following considerations should be made:

- Allocate 10% of available space if
  - Activity on the SNAZ is write light
  - Write access is concentrated in a few places.
- Allocate 25% of available space if
  - Activity on the SNAZ is write heavy
  - Write access is not concentrated, but is randomised across the volumes.

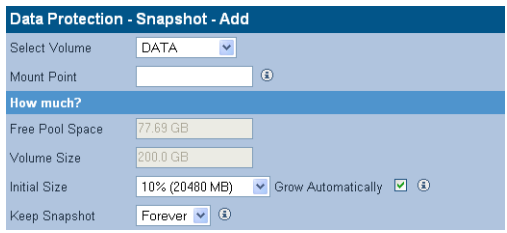
Scheduling a snapshot

To schedule a snapshot:

> Caution: *System performance may degrade while a snapshot is being performed. Snapshots should be scheduled appropriately to minimise user impact.*

1 From the menu bar, select **Data Protection - Snapshots**.

2 Click on add. The **Data Protection - Snapshot - Add** page opens.



From this page you need to:

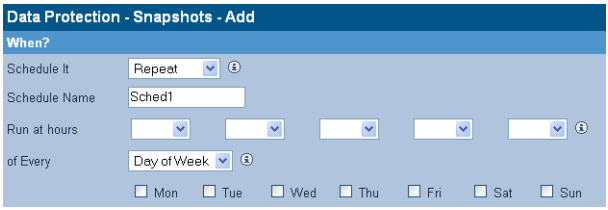
- **Select Volume** - Choose a Volume to make the snapshot of from the drop down list
- **Mount Point** - By default snapshots are kept in the snapshot folder in each volume. If required, specify a location (directory) for the Snapshot within the snapshot directory, which will then automatically be created
- **Initial Size** - Select an initial size for the snapshot and if required, tick the **Grow Automatically** box to change the snapshot size as required.
- **Keep Snapshot** - Select whether to keep the snapshot **Forever** or **For ... Days** from the drop down list(s).

> Note: *A maximum of 5 snapshots may be scheduled every day. However, only 4 snapshots will be preserved by the system at any one time in order to maintain reasonable system performance.*

3 Click on next >>.

4 Select when to schedule the snapshot for:

- **Now** - Perform the snapshot immediately
- **Once Later** - Perform a single snapshot at a time you specify
- **Repeat** - Perform a snapshot at the regular intervals you specify.

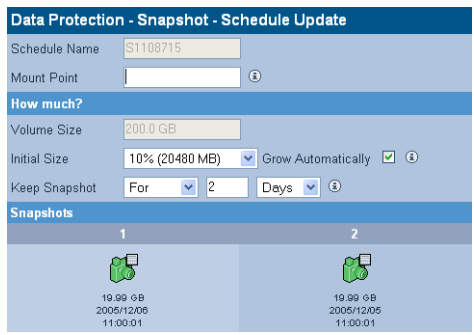


To modify an existing schedule

To modify an existing snapshot schedule:

1. From the menu bar, select **Data Protection - Snapshots**.
2. Click on the schedule you wish to modify.

The **Data Protection - Snapshot - Schedule Update** opens.



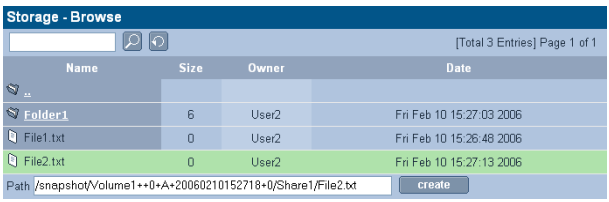
3. You can modify the **Mount Point**, **Initial Size** (including **Grow Automatically**) and **Keep Snapshot** period. You can also click next >> and change the time(s) the snapshot is scheduled for.
4. Click save to save the changes, click deactivate to deactivate or click delete to delete the snapshot.

To rollback previous version of a file using a snapshot

Snapshots can only be used to reinstate (rollback) a previous version of a file.

To rollback a file from a snapshot:

1. From the menu bar, select **Storage - Browse**:
2. Click the snapshot directory.
   Click on the required version of the snapshot, then navigate the directory tree to the required file and click on it (the background will highlight green to indicate selection):



3. Click rollback.

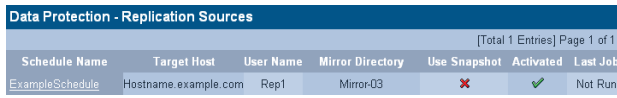
   A warning will be displayed, click rollback to confirm the file rollback. A message will indicate when the file rollback has completed.

Replication Sources

A replication is a copy of the contents of a folder, it's sub-folders and files which must be located on another system.

A replication Source is the system the replicated data originates from.

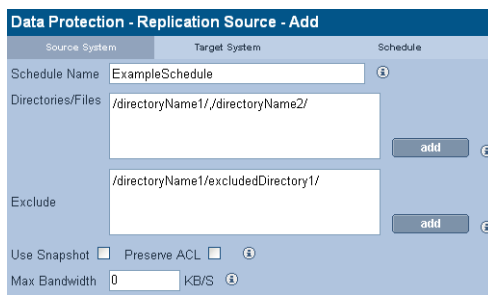
The **Data Protection - Replication Sources** page lists all the replications made or scheduled by the system.



Adding a replication source

To add a replication source:

1 From the menu bar, select **Data Protection - Replication Source**. Click add. The **Data Protection - Replication Source - Add** page opens:



2 From this page, enter:

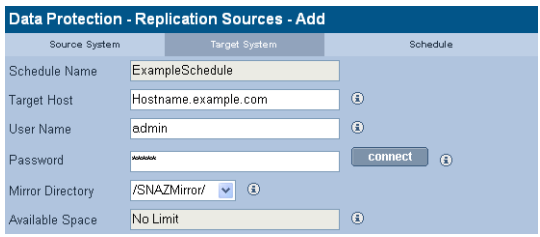
- **Schedule Name**
- **Directories/Files** - Click add to browse for files or folders to include in the Replication
- **Exclude** - Click add to browse for files or folders to exclude from the Replication
- **Use Snapshot** - Select to replicate a snapshot. When this option is selected, a snapshot is taken and is replicated to the target system. This can be used to ensure that no

further changes are made (i.e. the Replication is in a known state) to the Replication during the replication process.

- **Preserve ACL** - Select to preserve the ACLs of the data being replicated
- **Max Bandwidth** - You can specify the maximum network bandwidth the Replication may use.

3 Click next >>.

4 The **Target System** tab will open.



From this page, enter:

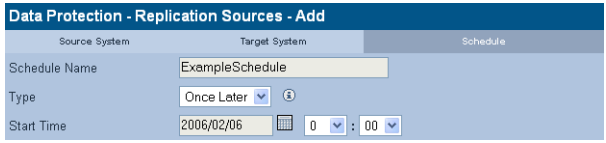
- **Target Host** - The IP address or hostname of the replication target system, this system must have a previously configured replication target defined
- **User Name** and **Password** - The user name and password of the User who has replication privileges on the target system.

Click connect, then enter:

- **Mirror Directory** - A mirror directory is selected from the drop-down list. This information and the **Available Space** is derived from the connection to the replication target system.

5 Click next >>.

6 The **Schedule** tab will open.



From this page, enter:

- **Type** - Select **Once Later**, **Weekly** or **Monthly** from the drop-down list. The field(s) below will change to the appropriate type of schedule

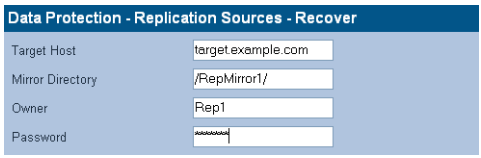
7 Enter the required information and click finish to finish.

Recovering a replication source

To recover from a failure using a replication target's copy of system data:

1 From the menu bar, select **Data Protection - Replication Source**.

Click recover. The **Data Protection - Replication Sources - Recover** page opens:



2 Enter:

- **Target Host** - The hostname or IP address of the Replication target system
- **Mirror Directory** - The directory on the target system that the Replication was written to
- **Owner** - The user name of the Replication source owner
- **Password** - The Replication source owner's password.

3 Click recover. A warning message is displayed, click recover to confirm. A message will indicate when the recovery is completed.

Replication Targets

A replication is a copy of the contents of a folder, it's sub-folders and files which must be located on another system.

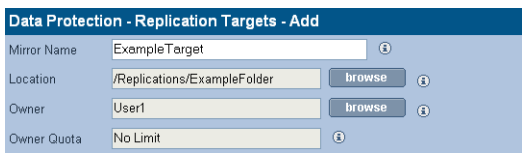
A replication Target is the system the replicated data is being written to.

The **Data Protection - Replication Targets** page lists all the replications made or scheduled by the system.

Adding a replication target

To add a replication target:

1 From the menu bar, select **Data Protection - Replication Source**. Click on add. The **Data Protection - Replication Source - Add** page opens:



From this page, enter:

- **Mirror Name** - Enter a name for the replication target
- **Location** - Click browse to browse for a location of the replication target
- **Owner** - Click browse to select a replication Owner. This user must have replication privileges assigned to them. The **Owner Quota** field will also be derived from the Owner's privileges.

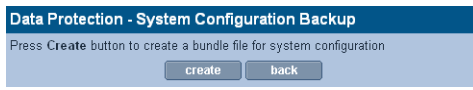
2 Click add.

Configuration Backup

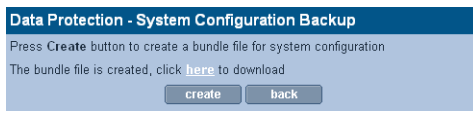
The **Data Protection - Configuration Backup** page allows you to create a bundle containing the configuration files from the SNAZ.

To create a Configuration Backup bundle:

1 From the menu bar, select **Data Protection - Configuration Backup**.



2 Click create. The configuration bundle will be created and a download link displayed:



The configuration bundle can now be saved to another system.

Restoring the configuration backup

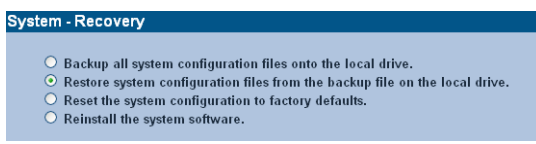
To restore the configuration backup:

1 From the menu bar, select **Shutdown**.

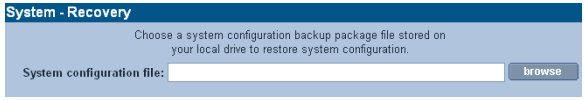
2 Select **Reboot into Maintenance Mode**.

3 When the SNAZ has rebooted, from the menu bar, select **System - Recovery**.

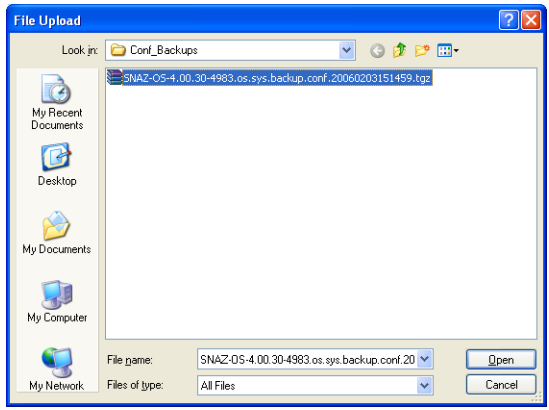
4 Select the **Restore system configuration files from the backup file on the local drive** radio button.



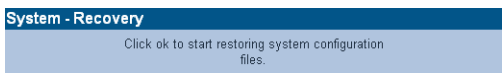
5 Click ok.



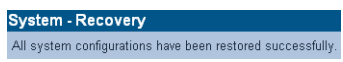
6 Click browse. Select the location of the configuration backup file and click **Open**.



7 Click ok to upload the configuration file bundle.



8 Click ok to restore the configuration. When the restore is complete the following is displayed:



9 Click ok to return to the main **System - Recovery** page.

10 From the menu bar, select **Shutdown** then **Reboot** and click ok.

Data Backup

The **Data Protection - Data Backup** page lists information required to configure the BakBone NetVault backup software, as follows:

Definitions

The SNAZ has both a NetVault Server and Client running on it:

- **NetVault Server** - controls the backup process
- **NetVault Client** - accesses the data which is to be backed up.

A separate PC is used to run the **NetVault GUI**, which is used to administer the backup process.

> Note: *The NetVault GUI must be installed as a Server.*

Licensing

A full BakBone NetVault License Key must be entered for ongoing operation of the backup utility.

The License Key will be emailed to you following registration via the Plasmon Warranty Registration website. For further information refer to *Backup* on page *22*.

Backup Devices

Backup devices should be attached via the supplied U320 HD68 SCSI interface on the rear of the SNAZ unit.

> Note: *SCSI termination of the backup device(s) may be necessary. Refer to the backup device manufacturer's documentation for further details.*

Confirmation that the backup device(s), either as a stand alone tape drive or an Autoloader comprising the Autoloader itself and a number of drives, have been recognised by the system may found via the **Diagnostics - Storage Devices** page.

For a list of compatible tape devices, see:

- BakBone NetVault Supported Platforms

Configuration

- **NetVault Server**
  - **Machine Name** - To allow the distinction between different devices within a NetVault environment, each SNAZ will have a unique Machine Name. This can be found on the **System - Services - Backup (Configuration)** page.
  - **Password** - A Password may be configured to restrict client access. This will need to be noted for the NetVault Client installation.
  - **Services** - The backup service must be running (Started) in order for NetVault to communicate with the backup device. The status of the service may be found on the **System - Services** page.
- **NetVault GUI**
  - **Domain Setup** - NetVault is designed to work in an environment in which one machine is configured as a NetVault Server and various other machines throughout the network act as NetVault Clients assigned to it. A single NetVault Server and its NetVault Clients make up a NetVault Domain. Full Domain configuration details may be found in Chapter 12 of the NetVault Administrator's Guide.
  - **Data** - Data stored on the SNAZ may be found in the 'exports' folder. Folders directly under the exports folder will be named by storage volume. In addition the default location for the storage of snapshots may be found within the exports folder, in a folder named 'snapshot'.

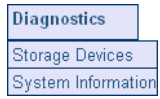
Note: *From the NetVault Client this will appear as: Machine Name\File System\exports*

NetVault Links

Click the hyperlink below to view (requires internet connection):

- NetVault Product Support
- NetVault Support Knowledge Base
- NetVault Getting Started Guide
- NetVault Administrator's Guide
- NetVault Product Licensing

Diagnostics menu

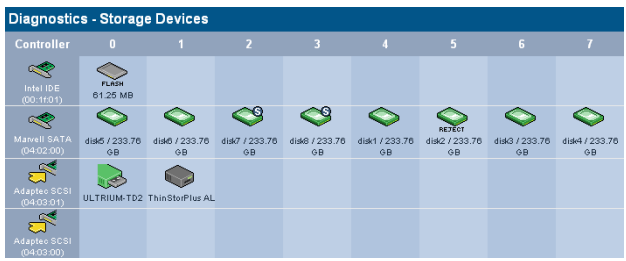


The Diagnostics menu allows you to access:

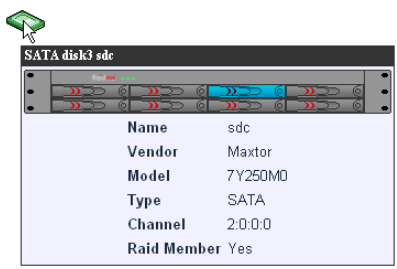
- *Storage Devices*
- *System Information* - see *page 68*

Storage Devices

The **Diagnostics - Storage Devices** page shows the internal and external devices attached to the SNAZ and their status.



Hovering the mouse pointer over a device will display a Tool Tip for that device giving further information, an example of which is shown below:



Disk status icons

- Disks which are marked with an  are system disks. This means they are used to store the system partition, which contains the configuration files of the SNAZ OS. They can still be used as part of any RAID(s)
- Disks which are marked with an  have been detected by the system as being in a prefail state. This means that certain types of errors have been found on them and they are likely to become faulty as a result. The system uses Self-Monitoring Analysis And Reporting Technology (SMART) parameters to track these errors
- Disks which are marked with have SPARE been assigned as hot spare disks. These are used should one of the other disks fail
- Disks which are marked with NO RAID are not currently members of a RAID
- Disks which are marked with have REJECT been rejected by the RAID they were a member of
- Disks which are marked with RESYNC are currently being resynchronised. The system, at all times, has to ensure that all mirrored RAID disks contain exactly the same data. If a difference is found, resynchronisation is performed to bring all the RAID disks back to identical mirrors of one another.

Table 2-4 Disk status icons

Icon	Meaning
	The disk is online and unformatted
	The disk is online, unformatted and the system has detected the disk is about to fail
	The disk is online
	The disk is online and the disk is not part of a RAID
	The disk is online and has been rejected by the system

Icon	Meaning
	The disk is online and has been marked as a spare disk
	The disk is online and the system has detected the disk is about to fail
	The disk is online, is not part of a RAID and the system has detected the disk is about to fail
	The disk is online, has been rejected by the system and the system has detected the disk is about to fail
	The disk is online, has been marked as a spare disk and the system has detected the disk is about to fail
	The disk is online and is a system disk
	The disk is online, is a system disk and is not part of a RAID
	The disk is online, is a system disk and has been rejected by the system
	The disk is online, is a system disk and has been marked as a spare disk
	The disk is online, is a system disk and the system has detected the disk is about to fail
	The disk is online, is a system disk, is not part of a RAID and the system has detected the disk is about to fail
	The disk is online, is a system disk, has been rejected by the system and the system has detected the disk is about to fail
	The disk is online, is a system disk, has been marked as a spare disk and the system has detected the disk is about to fail

Icon	Meaning
	The disk is resynchronising
	The disk is offline
	The disk is missing or information about its status is unavailable
	The disk is faulty and unformatted
	The disk is faulty
	The disk is faulty and is not part of a RAID
	The disk is faulty and has been rejected by the system
	The disk is faulty and is a system disk
	The disk is faulty, is a system disk and is not part of a RAID
	The disk is faulty, is a system disk and has been rejected by the system

Tape drive status icons

If a tape drive is attached, for backup purposes, its status is displayed as follows:
Table 2-5 Tape drive status icons

Icons	Meaning
	The tape drive is empty or its status cannot be determined
	The tape drive is online and/or currently in use
	The tape drive is faulty

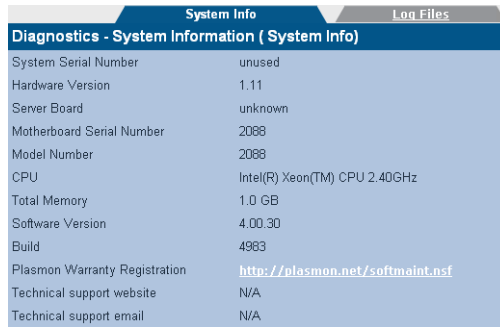
Miscellaneous icons

Table 2-6 Miscellaneous icons

Icons	Meaning
	This icon represents the Flash disk. This is where the SNAZ OS is located
	This icon represents an externally attached device, such as a tape autoloader
	This icon represents an internal (to the SNAZ) controller card, e.g the SNAZ's SATA Controller
	This icon represents an external controller card, i.e. the interface to an external device attached to the SNAZ, e.g connection from the SNAZ to an external SCSI device

System Information

The **Diagnostics - System Information** page allows you to view the following information:



System Info

- **System Serial Number** - The SNAZ's serial number
- **Hardware Version** - The current hardware version
- **Server Board** - Server board information
- **Motherboard Serial Number** - The SNAZ's motherboard serial number
- **Model Number** - The model number details the product configuration of the SNAZ, describing information such as the enclosure type, the memory capacity, the type of controller fitted and many others
- **CPU** - Processor information
- **Total Memory** - The amount of memory (RAM) on the system
- **System ID** - The unique serial number of this unit
- **Software Version** - The currently installed software version
- **Build** - The currently installed software version's build
- **Plasmon warranty registration** - Hyperlink to the Plasmon warranty registration web page (requires an external internet connection)
- **Technical Support Website** - Hyperlink
- **Technical Support Email** - Hyperlink.

Log Files

- **Create Log Files Bundle of** - Log file bundles are used by Technical Support to diagnose failures on your SNAZ. You can specify a time period, using the drop down list, to create a log file bundle of.

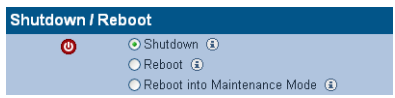
Shutdown menu

The **Shutdown** page allows you to:

- Shutdown
- Reboot
- Reboot into Maintenance Mode - Maintenance Mode is normally only used by Service personnel.

To shutdown or reboot the SNAZ:

1 From the menu bar, select **Shutdown**. the Shutdown page opens:



2 Select the appropriate radio button.

3 Click ok, then click ok again to confirm.

NAS

Worldwide Technical Support
www.plasmontech.com
Tel: +44 (0)1763 262963
Email: support@plasmon.co.uk

Plasmon Sales and Marketing

Plasmon Data Limited
Whiting Way, Melbourn
Hertfordshire SG8 6EN
Tel: +44 (0)1763 262963
Fax: +44 (0)1763 264444
Email: sales@plasmon.co.uk

97707987 Rev A

Plasmon

Raidtec SOLUTIONS