UDO ARCHIVE APPLIANCE

ADMINISTRATION GUIDE

Plasmon

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.

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 addresses on the next page.

Safety

This product contains a lithium battery. Please note the following:

- Danger of explosion if battery is incorrectly replaced.
- Replace with only the same or equivalent type recommended by the manufacturer.
- Dispose of batteries according to the manufacturer's instructions.

FCC note

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Changes or modifications not expressly approved by Plasmon could void the user's authority to operate equipment.

All SCSI and Network cables connected to and used on this equipment should be shielded.

Contact details

Europe, Middle East and Africa

Plasmon Data Ltd.
Whiting Way
Melbourn
Near Royston
Hertfordshire SG8 6EN
United Kingdom

Email: sales@plasmon.co.uk

Web: www.plasmon.com

Tel +44 (0) 1763 264400
Fax +44 (0) 1763 264444

North America, South America and Asia Pacific

Plasmon Inc.
370 Interlocken Blvd
Suite 600
Broomfield
CO 80021
United States of America

Email: sales@plasmon.com

Web: www.plasmon.com

Tel: 800-451-6845
Fax: 720-873-2501

How to use this guide

This guide describes in detail the operation of the Plasmon UDO Archive Appliance and its management tools. It is aimed at system administrators.

Related documentation

Please refer to the following document for further information:

- *Plasmon UDO Archive Appliance Quick Start Guide* – Explains how to install the Appliance and get started.
- *Plasmon UDO Archive Appliance Operator's Guide* - Aimed at users who will perform regular operations on the Appliance.

Contents

Chapter 1

Introduction

Appliance concept

The Plasmon UDO Archive Appliance (hereafter referred to as Appliance) provides low cost tiered archival storage. It combines the performance and simplicity of network-attached RAID with the longevity and authenticity of UDO (Ultra Density Optical). Data files are stored on and retrieved from the Appliance over a TCP/IP connection. The Appliance can be managed via a web interface, which is common across the Appliance family; this allows operators to easily transfer their knowledge as archive storage needs change.

UDO technology

UDO™ (Ultra Density Optical), based on blue laser technology, is the underlying foundation to Plasmon's archive solution portfolio, including the Appliance. It's the first storage technology specifically designed for long-term professional data archive requirements. UDO provides absolute data authenticity for any application where archived information must remain dependable and permanently unchanged. UDO has been designed and proven to deliver over a 50-year media life.

Blue lasers achieve far greater data densities, resulting in dramatically higher media capacities. First and second generation UDO products (UDO and UDO2) have a storage capacity of 30GB and 60 GB respectively, with capacity expected to reach 120GB by the third generation.

Appliances

UDO 2 Appliance and Library range

The following Plasmon Appliances (with their Library model numbers in parenthesis) support the new UDO 2 format:

- AA16/AA32 (Gx-32)
- AA80/AA80A8/AA80A12 (Gx-80)
- AA174/AA174A8/AA174A12 (Gx-174)
- AA234/AA438/AA638 (G-238/438/638)

Library components

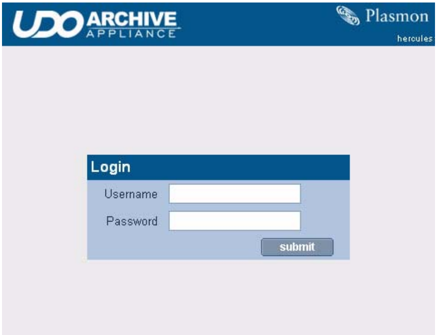
Table 1-1:

Component	Description
Dual Picker	Transfers UDO media between drives, media slots and Mailslot (IEE).
UDO Drive(s)	The number of UDO drives available for reading/writing media is model-dependent: - AA16 = 1 or 2 - AA32 = 2 - AA80 = 2 or 4 - AA174 = 2, 4 or 6 - AA238/AA438/AA638 = 2, 4 or 6
Barcode Reader	Reads the unique identifier on each UDO disk.
Media Slots	Slots internal to the Appliance, housing UDO media.
Mailslot (IEE)	For inserting and removing UDO media.
Server	A PC server board housed in the Appliance enclosure controls library functions and acts as the interface between the unit and the LAN. AA238,AA438, AA638, AA80A8/ AA174A8, AA80A12/AA174A12 Appliances have an integrated unit rack mounted above the library.

Chapter 2
The Archive Appliance

Starting the Web interface

1. On a LAN-attached client, start a web browser (such as Microsoft Internet Explorer).
2. In the URL field, enter the IP address or hostname of the Appliance to configure. For example:
   `http://192.168.0.1`
   The Web interface log-in page loads:



3. Enter a valid Appliance Administrator User Name and Password.
   - This is not the same as a Windows Domain Administrator.
   - The default administrator username and password is **admin**. It is reccommended that this is changed on first login ("Modifying a User's details" on page 42).
   - The default administrator can be used to add or remove additional administrator accounts.
4. Click **OK**.
   The Web Interface **System - Status** page is displayed.

System - Status page features

The **System - Status** page displays an overview of current system status (“System - Status” on page 12), and the menu bar.

Menu bar

The menu bar provides access to all the Appliance’s configuration and monitoring options, as well as to the online help..

Table 2-1: Web interface menus

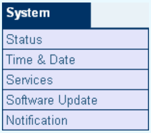
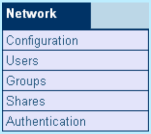
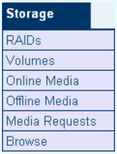
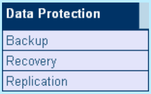
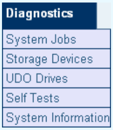
Menu/icon	Use to
 System Status Time & Date Services Software Update Notification	Monitor the Appliance’s status, set the time & date, monitor and configure the services, update the system software and configure alert notifications
 Network Configuration Users Groups Shares Authentication	Define the network configuration, users, groups and shares
 Storage RAIDs Volumes Online Media Offline Media Media Requests Browse	Configure RAIDs, volumes and the library, browse the volume and monitor offline media requests
	Perform a system configuration backup, disaster recovery, and configure system replication

Table 2-1: Web interface menus

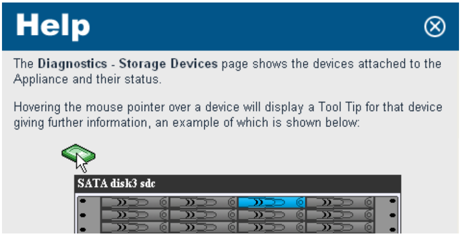
Menu/icon	Use to
 Diagnostics System Jobs Storage Devices UDO Drives Self Tests System Information	Monitor system jobs and devices (disks, libraries, etc.), perform self tests, view system information (software version, serial numbers, hardware revisions, etc.) and create a log file bundle
Shutdown	Reboot or shut down the Appliance.
?	Display context-sensitive online help.
⌂	Return to the Web interface **System - Status** page.
⎋	Log out of the current Web interface session.

Online help

Each page of the Web interface provides access to an associated online help page.

To access help, click the ? icon at any time.

The Appliance Help page will open in a pop-up browser Window, e.g.:



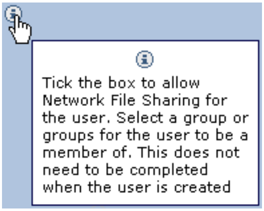
Help

The **Diagnostics - Storage Devices** page shows the devices attached to the Appliance 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:

Tool Tips

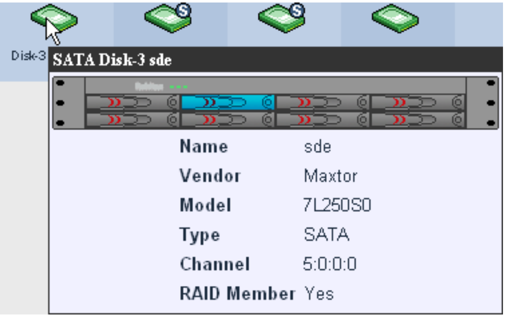
Wherever the ⓘ icon is present, hovering the mouse pointer over it will display a relevant Tool Tip, e.g.:



Tick the box to allow Network File Sharing for the user. Select a group or groups for the user to be a member of. This does not need to be completed when the user is created

Certain devices also have Tool Tips that provide diagnostic information. These are:

- Volumes and Volume Groups
- RAIDs
- Controllers
- Flash Media
- Overflow Libraries



SATA Disk-3 sde

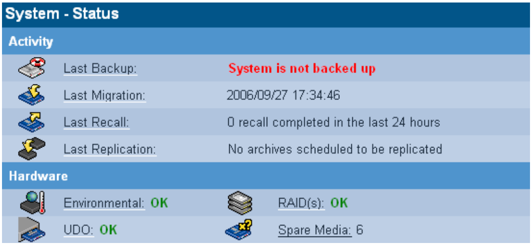
Name	sde
Vendor	Maxtor
Model	7L250S0
Type	SATA
Channel	5:0:0:0
RAID Member	Yes

Chapter 3

System menu

System - Status

The **System - Status** page displays the current status of the Appliance:



System - Status

Activity

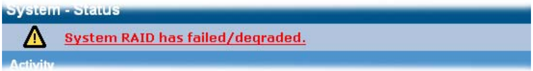
	Last Backup:	System is not backed up
	Last Migration:	2006/09/27 17:34:46
	Last Recall:	0 recall completed in the last 24 hours
	Last Replication:	No archives scheduled to be replicated

Hardware

	Environmental: OK		RAID(s): OK
	UDO: OK		Spare Media: 6

The page is split into three areas

- The area at the top of the page displays any warnings or error messages. This area only becomes visible when an active error message is present, e.g.:



System - Status

⚠ System RAID has failed/degraded.

Activity

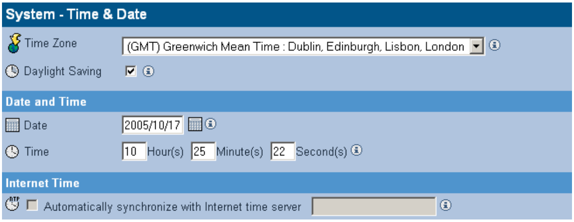
- The **Activity** area displays the time of the **Last Backup**, **Last Migration**, **Last Recall** and **Last Replication**.
- The **Hardware** area displays the **Environmental** status of the Appliance enclosure, the status of the **RAID(s)** and the **UDO** drives. It also displays the quantity of **Spare Media** in the Appliance.

Setting the time and date

Note: File creation dates depend on the date and time setting. It is vital that the date and time are set correctly.

Setting time and date manually

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



System - Time & Date

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight Saving: ☑

Date and Time

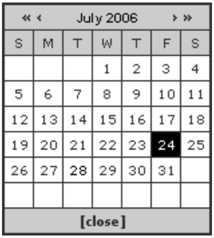
Date: 2005/10/17

Time: 10 Hour(s) 25 Minute(s) 22 Second(s)

Internet Time

□ Automatically synchronize with Internet time server

2. Use the drop-down menu to select the correct **Time Zone** from the list.
3. If appropriate, tick the box for **Daylight Saving** time.
4. Set the **Date**: 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 display the **Select Date** pop-up:



« ‹ July 2006 › »

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

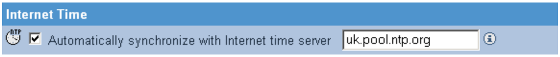
[close]

5. Set the **Time** in the format Hour(s), Minute(s) and Second(s).
6. Click **save** to save the changes.

Note: If the time and/or date is changed after files have been stored on the Archive Appliance, it is strongly recommend that the SSM service is stopped and re-started.
See pages 15 and 16

Synchronising time and date with an NTP server

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



Internet Time

☑ Automatically synchronize with Internet time server uk.pool.ntp.org

2. Tick the **Automatically synchronize with Internet time server** box and enter a Network Time Protocol (NTP) server URL to automatically synchronize the time with an Internet time server.

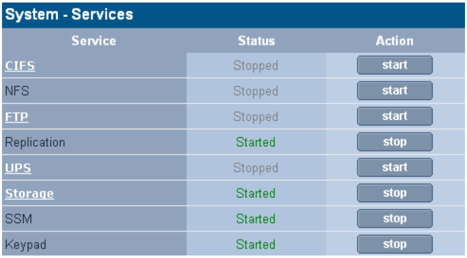
   Note: Time changes can affect the archive and the archiving process. Plasmon strongly recommends the use of an NTP server.

3. The connection to the NTP server may be tested by clicking the **test ntp** button.

   Note: When connecting to the Active Directory for authentication, the Active Directory Server is used for time synchronisation and the NTP server is ignored.

4. Click **save** to save the changes.

Managing services



System - Services

Service	Status	Action
CIFS	Stopped	start
NFS	Stopped	start
FTP	Stopped	start
Replication	Started	stop
UPS	Stopped	start
Storage	Started	stop
SSM	Started	stop
Keypad	Started	stop

The **System - Services** page allows manual starting, stopping and, in some cases, configuration of:

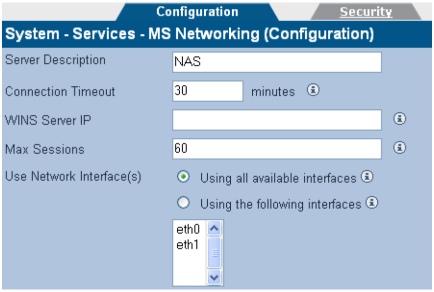
- **CIFS (Common Internet File System)** - also known as SMB (Server Message Block), is the communications protocol used by Windows-based operating systems to support sharing of resources across a network - see page 16
- **NFS (Network File System)** - is a method of making a remote filesystem accessible on the local system. From a user's perspective, an NFS-mounted filesystem is indistinguishable from a filesystem on a directly-attached disk drive. There are no configurable options for the NFS service; however when creating shares using NFS, Host Entry attributes must be configured - .see page 47
- **FTP (File Transfer Protocol)** - FTP is a protocol which allows a user on one host to access, and transfer files to and from, another host over a network - see page 18
- **Replication** - This service controls replication between the Appliance and a partnered Appliance - see page 105.
- **UPS (Uninterruptible Power Supply)** -Displays the status of an attached APC SmartUPS if one is present - see page 19
- **Storage** - The Storage service allows the automatic re-use of disk drives which have been rejected by their RAID due to recoverable read errors. Clicking on the link opens the **System - Services - Storage** page, allowing configuration of the number of times a disk with soft failures may be recycled - see page 21

- **SSM (Storage Space Manager)** - Start or stop the HSM (Hierarchical Storage Management) software on the Appliance. Stopping the SSM service halts communication between the RAID cache and the UDO library. If SSM is stopped, all archive volumes are taken offline and no migration will be performed by the system.
- **Keypad** - Enable or disable the UDO Library Keypad.

Click **start** to start or click **stop** to stop individual services as required.

Configuring CIFS (Including Active Directory Server / NT Domain Server)

1. From the **System - Services** page click on **CIFS**.
   The **CIFS (Configuration)** page opens:



System - Services - MS Networking (Configuration)

Server Description: NAS

Connection Timeout: 30 minutes

WINS Server IP:

Max Sessions: 60

Use Network Interface(s): ● Using all available interfaces ○ Using the following interfaces

eth0
eth1

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 IP**.
   This is the IP address of the Windows Internet Naming Service (WINS) server.
5. If required, enter the number of **Max Sessions**.

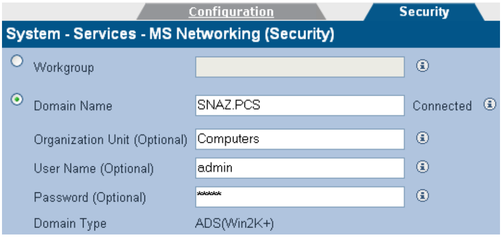
This is the maximum number of concurrent CIFS sessions that the Appliance will accept. The default is 60 sessions.

6. Select to **Use Network Interface(s)**, as follows:
   - **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.

Configuring CIFS Security

1. Click on the **Security** tab.

   The **CIFS (Security)** page opens. This gives access to the Active Directory Server user authentication features. CIFS security allows the Archive Appliance to authenticate share users against a Windows domain and create file permissions for them. By configuring the Windows Domain security, the Archive Appliance has access to all domain users. These users can then be added to the access control list (ACL) from the **Network - Shares - Update (Access)** and the **Storage - Browse - Access (Access)** pages of the Web interface.



System - Services - MS Networking (Security)

○ Workgroup		
● Domain Name	SNAZ.PCS	Connected
Organization Unit (Optional)	Computers	
User Name (Optional)	admin	
Password (Optional)	*****	
Domain Type	ADS(Win2K+)	

2. Enter either:

   A **Workgroup** - To authenticate against the local user database provided by the Appliance.

   or

   A **Domain Name** - This is the name of the domain controlled by the Domain Server. This name must translate to an IP address using the DNS server.

   If joining the Appliance to a Domain, additional details are required: The **Organizational Unit** (OU) within the Active Directory structure in which the Appliance will appear, (by default, the Appliance will appear in the *Computers* OU), a

Windows **User Name** with administrative rights to the Domain, and the user's **Password**.

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

- **ADS (Win2K+)**
- **NT Compatible**.

3. Click **save** to save the changes.

Important: When authenticating users against an Active Directory structure, only the first 32 groups that a user is a member of will be noted by the Appliance.

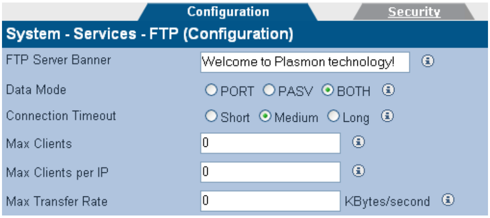
Configuring NFS

The NFS networking service is configured via the **Network - Shares** page - see page 45.

Configuring FTP

1. From the menu bar, select **System - Services** and click on **FTP**.

   The **FTP (Configuration)** page opens:



System - Services - FTP (Configuration)

FTP Server Banner	Welcome to Plasmon technology!
Data Mode	○ PORT ○ PASV ● BOTH
Connection Timeout	○ Short ● Medium ○ Long
Max Clients	0
Max Clients per IP	0
Max Transfer Rate	0 KBytes/second

2. If required, enter an **FTP Server Banner**. This is a message which will be displayed to users when they access the Appliance via FTP.
3. Enter a **Data Mode**. The data mode can be:
   - **PORT** - Otherwise known as Active mode.
   - **PASV** - Passive mode FTP.
   - **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 Appliance should allow an idle client to remain connected.

   The timeout settings for connections are:

   - **Short**: 30 seconds
   - **Medium**: 60 seconds
   - **Long**: 300 seconds

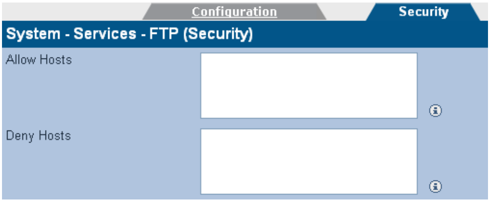
   The timeout settings for data transfers are:

   - **Short**: 150 seconds
   - **Medium**: 300 seconds
   - **Long**: 1500 seconds

5. Enter the maximum number of allowable concurrent FTP client connections (**Max Clients)**.
6. Enter the maximum number of allowable concurrent FTP connections from the same IP address (**Max Clients per IP)**.
7. Enter the maximum rate, in Bytes, of FTP data transfer (**Max Transfer Rate)**.
8. Click on the **Security** tab.

   The **FTP (Security)** page opens. This allows entry of IP addresses and/or hostnames to explicitly Allow or Deny FTP access to the Appliance.

   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.

UPS

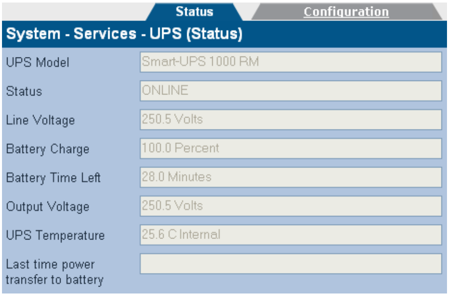
The information in the **System - Services - UPS** page is derived from the Uninterruptable Power Supply (UPS) itself.

Refer to the manufacturer's documentation for details installing and configuring the UPS.

Note: The Appliance only supports APC brand Smart UPS devices.

1. From the menu bar, select **System - Services** and click on **UPS**.

   The **UPS (Status)** page opens:



System - Services - UPS (Status)

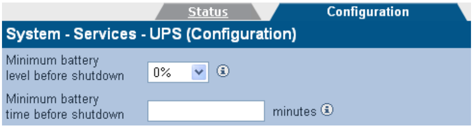
UPS Model	Smart-UPS 1000 RM
Status	ONLINE
Line Voltage	250.5 Volts
Battery Charge	100.0 Percent
Battery Time Left	28.0 Minutes
Output Voltage	250.5 Volts
UPS Temperature	25.6 C Internal
Last time power transfer to battery	

The following information is displayed:

- **UPS Model** - The model code of the UPS attached to the Appliance
- **Status** - The UPS's status (e.g ONLINE, LOW BATTERY, etc.)
- **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 Appliance)
- **UPS Temperature** - The temperature of the UPS enclosure
- **Last time power was transferred to battery** - The last time the power was transferred from the mains supply to the UPS.

2. Click on the **Configuration** tab.

The **UPS (Configuration)** page opens. This allows configuration of:



System - Services - UPS (Configuration)

Minimum battery level before shutdown: 0%

Minimum battery time before shutdown: minutes

- **Minimum battery level before shutdown** - Select the percentage at or below which the UPS will shut down the Appliance.
- **Minimum battery time before shutdown** - Enter the minimum UPS battery time remaining, in minutes, prior to the Appliance shutting down.

The UPS will initiate a shutdown of the Appliance when either of these conditions are met.

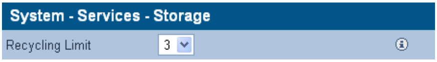
3. Click **save** to save the changes.

Storage

The **System - Services - Storage** defines how many times a RAID disk may be reused by the system, should recoverable errors be encountered. A disk may be reused up to a maximum of five times.

Recoverable failures may be caused by a number of issues, such as Self-Monitoring, Analysis, and Reporting Technology (SMART) monitoring issues or read errors, and these will result in the disk being rejected by the RAID(s) it is in. In this instance, a hot spare replaces the disk, and the system recycles the failed disk by automatically reformatting it and marking it as a hot spare, up to the number of times specified.

1. From the menu bar, select **System - Services** and click on **Storage**:



System - Services - Storage

Recycling Limit: 3

2. Use the drop-down menu to select a **Recycling Limit** from the list.
3. Click save to save the changes or click stop to stop disk recycling.

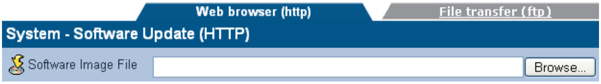
Update the System Software

The **System - Software Update** page enables updates to the system software to be performed using:

- **Web browser (HTTP)** - from a local computer.
- **File transfer (FTP)** - from the Plasmon FTP server.

Update via Web Browser (HTTP)

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



System - Software Update (HTTP)

Software Image File

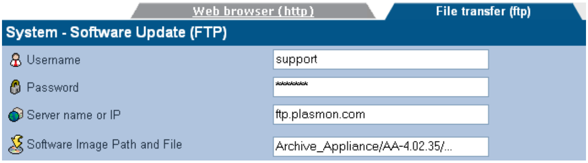
2. Enter the **Software Image File** path to a local copy of the Appliance software image or click **browse** to locate the image file.
3. Click **transfer** to begin the software update.

Note: The file transfer is controlled entirely by the web browser. There may be no visual indication of transfer progress.

Follow the on-screen instructions to complete the installation.

Update via File Transfer (FTP)

1. From the menu bar, select **System - Software Update**.
2. Click on the **FTP** tab.
   The **Software Update (FTP)** page opens:



System - Software Update (FTP)

Username	support
Password	*******
Server name or IP	ftp.plasmon.com
Software Image Path and File	Archive_Appliance/AA-4.02.35/...

3. Contact Plasmon technical support for the FTP server and login details. Enter them into the **FTP Username**, **Password**, **Server name or IP** and **Software Image Path and File** fields.
4. Click **transfer** to begin the software update.

   Follow the on-screen instructions to complete the installation.

Notification

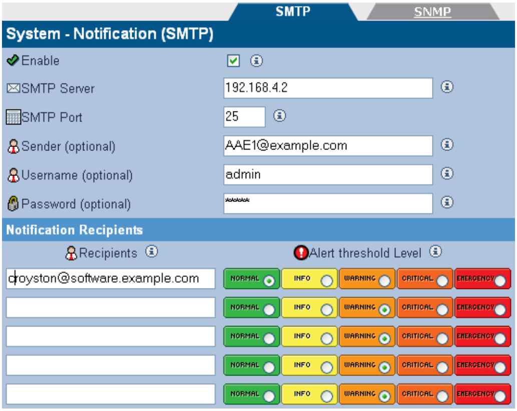
The Appliance can notify system administrators of system events and errors by:

- Email (Simple Mail Transfer Protocol - SMTP) Notification - see below
- Simple Network Management Protocol (SNMP) Notification - see page 24.
- A history of the notifications can be viewed via the Web interface, and should be regularly reviewed and its contents cleared (see page 27).

Both email and SNMP notification services can be running at the same time.

Configure Email (SMTP) Notification

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



System - Notification (SMTP)

Enable	☑
SMTP Server	192.168.4.2
SMTP Port	25
Sender (optional)	AAE1@example.com
Username (optional)	admin
Password (optional)	******

Notification Recipients

Recipients	Alert threshold Level
croyston@software.example.com	NORMAL ● INFO ○ WARNING ○ CRITICAL ○ EMERGENCY ○
	NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
	NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
	NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
	NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○

2. Tick the **Enable** box to enable, or untick to disable, the email notification service.
3. Enter an **SMTP Server** (email server) name or IP address.
4. Enter an **SMTP Port**. The normal port used for email is 25.
5. If required, add a **Sender** to the notifications.

6. If required, add a **Username** to the notifications. If a username is added, that user's **Password** must also 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 in *Table 3-1*.

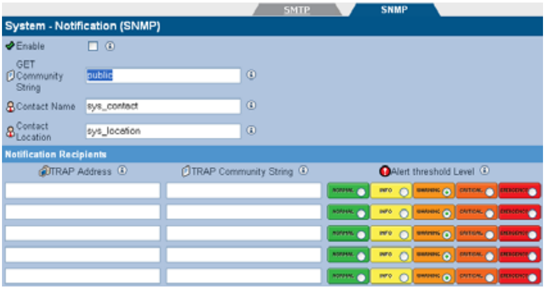
> *Note: For "call home" registered systems, please use the email monitoring service: aa_remote_monitor@plasmon.com. This will allow Plasmon to monitor the Appliance remotely.*

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

Configure SNMP Notification

1. From the menu bar, select **System - Notification**.
2. Click on the **SNMP** tab.

   The **System - Notification (SNMP)** page opens:



System - Notification (SNMP)

Enable □

GET Community String: public

Contact Name: sys_contact

Contact Location: sys_location

Notification Recipients

TRAP Address	TRAP Community String	Alert threshold Level
		NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
		NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
		NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
		NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○
		NORMAL ○ INFO ○ WARNING ● CRITICAL ○ EMERGENCY ○

3. Tick the **Enable** box to enable the SNMP notification service.
4. Enter a **GET Community String**. By default the Appliance does not use Community Strings to authenticate sent notifications. However, if required, a Community String can be entered here to enable this function.
5. Enter a **Contact Name** for SNMP notifications.

The Contact Name specifies the person to contact for the host, and how they may be contacted, e.g.: John Smith, X 1234, smith@plasmon.com.

6. Enter a **Contact Location** for SNMP notifications.

   The Contact Location lists the geographical location of the Appliance, e.g.: Appliance-1, Server Room 2, Plasmon HQ, UK.

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

8. Select an **Alert Threshold Level** for each recipient. These are described in *Table 3-1*.

9. Click **save** to save the changes, **test alert** to send a test notification to each recipient, or click **history** to view the Notification Log.

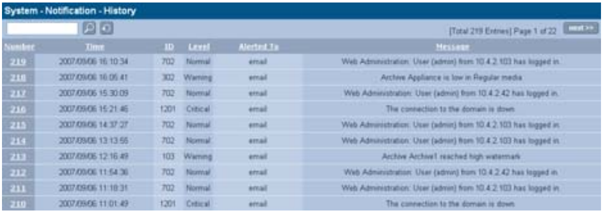
Table 3-1. Notification Alert Threshold Levels

Level	**Meaning**
EMERGENCY	Emergency alerts require immediate action. Setting the Alert Threshold Level to this level will only send notifications of Emergency alerts.
CRITICAL	Critical events require that action must be taken urgently. This level of notification includes notification of both Critical and Emergency events.
WARNING	Warning events need actioning as soon as possible to keep the Appliance operating at maximum efficiency. This level of notification includes Warning, Critical and Emergency events.
INFO	Info alerts may require some action to be taken. This level of notification includes Info, Warning, Critical and Emergency events.
NORMAL	Normal events require no action. This notification level includes all events.

Notification history

The Appliance keeps a log of all notifications that it has sent, and it is strongy reccommended that this log be reviewed and cleared regularly.

1. From the menu bar, select **System - Notification**.
2. Click the **history** button:.



System - Notification - History

[Total 219 Entries] Page 1 of 22

Number	Time	ID	Level	Alerted To	Message
219	2007/09/06 16:10:34	702	Normal	email	Web Administration: User (admin) from 10.4.2.103 has logged in.
218	2007/09/06 16:05:41	302	Warning	email	Archive Appliance is low in Regular media
217	2007/09/06 15:30:09	702	Normal	email	Web Administration: User (admin) from 10.4.2.42 has logged in.
216	2007/09/06 15:21:46	1201	Critical	email	The connection to the domain is down
215	2007/09/06 14:37:27	702	Normal	email	Web Administration: User (admin) from 10.4.2.103 has logged in.
214	2007/09/06 13:13:55	702	Normal	email	Web Administration: User (admin) from 10.4.2.103 has logged in.
213	2007/09/06 12:16:49	103	Warning	email	Archive Archive1 reached high watermark
212	2007/09/06 11:54:36	702	Normal	email	Web Administration: User (admin) from 10.4.2.42 has logged in.
211	2007/09/06 11:18:31	702	Normal	email	Web Administration: User (admin) from 10.4.2.103 has logged in.
210	2007/09/06 11:01:49	1201	Critical	email	The connection to the domain is down

3. Click the **next** and **back** buttons to navigate through a log that spans multiple pages.
4. Click any column header to order the list by that column (i.e. **Number, Time, ID, Level, Alerted To** or **Message**).
5. Once satisfied that all alerts are sufficiently attended to, click **delete all**.
6. A message will appear advising that this will delete all event logs. Click **delete all** again to confirm.

Appliance notifications

The Appliance notifications and their alert levels are listed in *Table 3-2* below:

Table 3-2. Appliance Notifications

Alert ID	Alert Level	Meaning
1	Normal	Archive Appliance self-test message.
2	Emergency	Archive Appliance key process failure.
3	Normal	The server is up and running.
4	Info	The server is shutting down.
9	Warning	The server is rebooting.
10	Critical	The interface in a bond is disabled because its link is down.
11	Critical	The network interface is down.
12	Critical	No active interface is in a bond.
13, 14	Normal	The network interface is up.
101	Info	The RAID has finished resynchronization.
102	Critical	The RAID has degraded. Please check and ensure a hotspare disk has been added to the RAID.
103	Warning	Archive Appliance high watermark.
104	Critical	Failed to stop a RAID.
105	Info	The spare disk has been successfully assigned to a degraded RAID.
106	Critical	Failed to assign a spare disk to a degraded RAID.
107	Critical	No valid hot spare disk is available.

Table 3-2. Appliance Notifications

Alert ID	Alert Level	Meaning
108	Emergency	The disk has failed on a RAID, disabling device. It may be necessary to replace the faulty disk with a new disk.
109	Info	The System disk has been successfully recycled back to the RAID.
110	Info	The data disk has been successfully recycled back to the RAID.
111	Emergency	Failed to start a RAID.
112	Info	Hotspare disk assigned.
201	Warning	The server has lost communication with the UPS.
202	Info	The server has regained communications with the UPS.
203	Critical	The UPS has lost power.
204	Info	The UPS is being powered again.
205, 207, 210	Emergency	The UPS battery has failed.
206	Critical	Library power supply has failed.
208	Info	The UPS is rebooting the system.
209	Critical	The UPS is shutting down the system.
301	Warning	Archive Appliance is low in media.
302	Warning	Archive Appliance is critically low in media.
303	Warning	Archive Appliance media initialization failed.
304	Warning	Archive Appliance medium marked unreliable.

Table 3-2. Appliance Notifications

Alert ID	Alert Level	Meaning
305	Emergency	Archive Appliance offline resource requested.
306	Warning	Archive Appliance backup failure no media.
307	Warning	SSM unknown volume.
308	Normal	Archive Appliance medium available to offline.
311	Warning	Archive Appliance medium marked dirty.
312	Warning	Archive Appliance barcode unreadable.
313	Warning	Media marked unusable.
314	Info	Archive Appliance medium marked clean.
401	Critical	Archive Appliance drive disabled due to error.
402	Critical	No drives are available for migration.
403	Warning	Archive Appliance drive disabled.
404	Normal	Archive Appliance drive enabled.
405	Normal	Archive Appliance status marked as good.
406	Warning	Archive Appliance drive marked dirty.
407	Warning	Archive Appliance drive marked clean.
501	Emergency	Archive Appliance media changer failure.
502	Warning	Archive Appliance library rear fan fault.
503	Info	Archive Appliance library rear fan OK.
504	Emergency	Archive Appliance library temperature critical.
505	Emergency	Archive Appliance drive temperature critical.
506	Info	Archive Appliance library temperature normal.

Table 3-2. Appliance Notifications

Alert ID	Alert Level	Meaning
507	Info	Archive Appliance drive temperature normal.
508	Warning	Archive Appliance library front fan fault.
509	Info	Archive Appliance library front fan OK.
601	Warning	Archive Appliance backup failure.
604	Warning	Archive Appliance backup fail FSC consistency check failure.
605	Warning	Archive Appliance backup failure low media.
701	Warning	Security Warning: A user failed to authenticate.
702	Normal	Web Administration: A user has logged in.
703	Warning	Security Warning: User not recognized.
704	Warning	Security Warning: A user failed to authenticate.
705	Warning	LDAP User list size limit reached.
706	Warning	LDAP user list retrieval has timed out.
708	Warning	Appliance failed to connect to the LDAP server.
709	Warning	Duplicate LDAP user/group name detected.
710	Warning	Duplicate LDAP user/group ID detected.
801	Critical	Self-check failed, the device needs to be replaced soon.
802	Emergency	The core voltage of CPU is incorrect.
803	Emergency	The system temperature is too high. Please check cooling or turn off the Appliance.

Table 3-2. Appliance Notifications

Alert ID	Alert Level	Meaning
804	Emergency	The fan speed is too slow. Please check if the fan is broken.
805	Emergency	The board temperature is too high. Please check cooling or shut down the system.
806	Emergency	The system temperature is dangerously high, the Appliance is shutting down.
807	Emergency	The PC health voltage is incorrect.
808	Emergency	The server power failed.
900	Critical	The system volume is nearly full.
901	Warning	The data volume is nearly full.
902	Emergency	The system volume is full.
903	Warning	The data volume is full.
904	Emergency	The flash disk is full.
905	Critical	The Flash disk is nearly full.
1001	Critical	Failed to start the Logical volume: mount failure. Please try to diagnose the volume.
1003	Warning	Failed to stop the logical volume: unmount failure. It may be necessary to reboot the Appliance.
1005	Emergency	The pool is faulty: one member RAID is dead or missing.
1006	Emergency	Failed to resize a logical volume.
1013	Emergency	XFS file system error detected.
1014	Emergency	XFS file system was shutdown by some errors.

Table 3-2. Appliance Notifications

Alert ID	Alert Level	Meaning
1101	Normal	Replication job finished.
1102	Critical	Replication job failed.
1201	Critical	The connection to the domain is down, the Samba shares maybe inaccessible and domain users and groups can not be retrieved.
1202	Emergency	Syslog-ng service is not running correctly, failed to start the service.
1203	Emergency	Sysman is not running correctly.
1204	Emergency	Storage Daemon Manager is not running correctly, failed to start service.
1205	Emergency	Crond is not running correctly, failed to start service.
1206	Emergency	The web interface service is not running, failed to start service.
1207	Emergency	System flash disk corruption has been detected and fixed, flash may need to be replaced.
1208	Emergency	System flash disk corruption has been detected but attempt to fixed has failed. Replace flash disk.
1301	Warning	Archive Appliance critical watermark.
1302	Critical	Archive Appliance read-only watermark.
1303	Emergency	Archive Appliance read-only no-recall watermark.
1305	Warning	UDO media is unreadable
1306	Warning	Replication job duplicated.

Table 3-2. Appliance Notifications

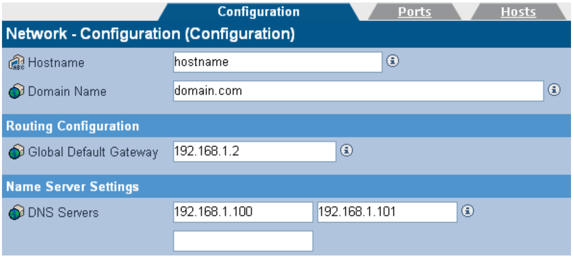
Alert ID	Alert Level	Meaning
1308	Warning	The FSC data has exceeded the capacity of the ssmpart system volume. No further migrations will be performed.
1401	Warning	There has been a failure of a scheduled backup. File system consistency check failed.
1401	Warning	There has been a failure of a scheduled backup. File system consistency check failed.
1402	Warning	There has been a failure of a scheduled backup. Backup size is larger than available backup media space.
1403	Warning	There has been a failure of a scheduled backup.

Chapter 4
Network menu

Network Settings

Configuration

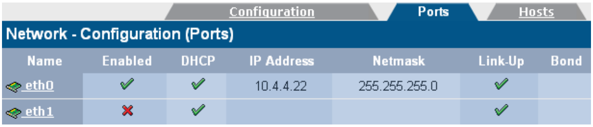
1. From the menu bar, select **Network - Configuration**.



Network - Configuration (Configuration)

Hostname	hostname	
Domain Name	domain.com	
Routing Configuration		
Global Default Gateway	192.168.1.2	
Name Server Settings		
DNS Servers	192.168.1.100	192.168.1.101

2. Enter a **Hostname** for the Appliance
3. Enter the **Domain Name** which the Appliance belongs to.
4. Enter the **Global Network Gateway** IP address.
5. Enter the IP address(es) of up to 3 **DNS Servers**. Multiple DNS Servers are usually used to offer continuity of Domain Name resolution should the primary server fail. See page 38 for details of configuring the Appliance for use with Windows Active directory.
6. Click on the **Ports** tab. The Appliance's network (Ethernet) ports are listed:



Network - Configuration (Ports)

Name	Enabled	DHCP	IP Address	Netmask	Link-Up	Bond
eth0	✓	✓	10.4.4.22	255.255.255.0	✓	
eth1	✗	✓			✓	

The following information is also displayed:

- **Name** - The Ethernet port name, *eth0* (the A12 Appliance has a second port, *eth1)*. Clicking on the port name shows the network port's configuration
- **Enabled** - Indicates whether the Ethernet port is enabled
- **DHCP** - Indicates whether Dynamic Host Configuration Protocol (DHCP) is enabled.

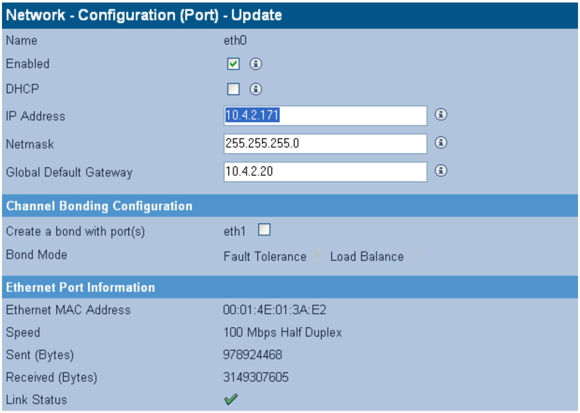
Note: By default, DHCP is enabled.

- **IP Address** - Displays the IP address of the port
- **Netmask** - Displays the Network mask of the port
- **Link up** - Indicates whether or not the network connection is operational.
- **Bond** - On the A12 indicates whether or not the two ethernet ports are bonded. This is used to provide load balancing or fault tolerance. For details on how to configure bonding, see page 38.

7. Click **save** to save the changes.

Setting a static IP address

1. From within the **Network - Configuration (Ports)** page, click on a network port's name:



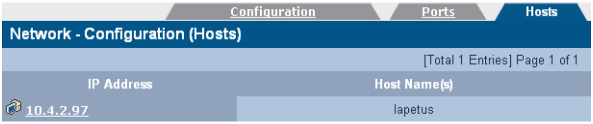
Network - Configuration (Port) - Update

Name	eth0
Enabled	☑ ⓘ
DHCP	□ ⓘ
IP Address	10.4.2.171 ⓘ
Netmask	255.255.255.0 ⓘ
Global Default Gateway	10.4.2.20 ⓘ
Channel Bonding Configuration	
Create a bond with port(s)	eth1 □
Bond Mode	Fault Tolerance ● Load Balance ○
Ethernet Port Information	
Ethernet MAC Address	00:01:4E:01:3A:E2
Speed	100 Mbps Half Duplex
Sent (Bytes)	978924468
Received (Bytes)	3149307605
Link Status	✓

2. Clear the DHCP check-box.
3. Enter the **IP Address**, **Netmask** and **Global Default Gateway**. The network administrator can provide these details.
4. Click the **save** button.

Creating a static hosts table

1. From within the **Network - Configuration** page, click on the **Hosts** tab:



Network - Configuration (Hosts)

[Total 1 Entries] Page 1 of 1

IP Address	Host Name(s)
10.4.2.97	lapetus

2. Click add to add a host. This page allows the creation of a list of Hosts which are known to the Appliance. This list is used to resolve hosts when DNS is not available.
3. Click save to save the changes.

DNS configuration for Windows Active Directory

When using Windows Active Directory, it is essential that the primary DNS address entered when following step 5 of the network configuration procedure (see page 36) is one of the AD domain's specified nameservers. To determine the IP address of the nameserver:

1. Using a Windows PC on the same AD domain as the Appliance, select **Start menu > Run...**
2. Type **cmd** and press **Enter** to open a Windows Shell.
3. At the command line enter: **nslookup** followed by the domain name entered in step 3 of the network configuration procedure. Press **Enter**.
4. Consult the network administrator to determine which of the displayed IP addresses should be used as the primary DNS address.

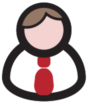
Bonding network ports

The A12 Appliance has two ethernet ports which can be bonded to provide either fault tolerance (where one ethernet card is in use and the other is kept as a backup in case of failure) or load balancing (where the two ethernet cards share network activity to prevent bottlenecks).

1. From within the **Network - Configuration (Ports)** page, click on a network port's name:
2. Check the **Create a bond with port(s)** tick box.

3. The radio buttons for **Fault Tolerance** and **Load Balance** will become enabled. **Fault Tolerance** is selected by default.
4. Select the bond type that is required, then click the **save** button.

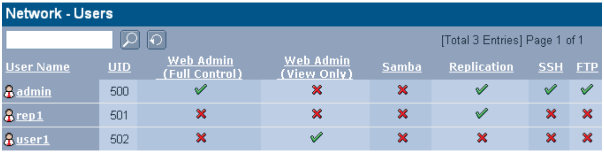
Users



The **Network - Users** page lists all the local users defined on the Appliance.

Adding a User

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

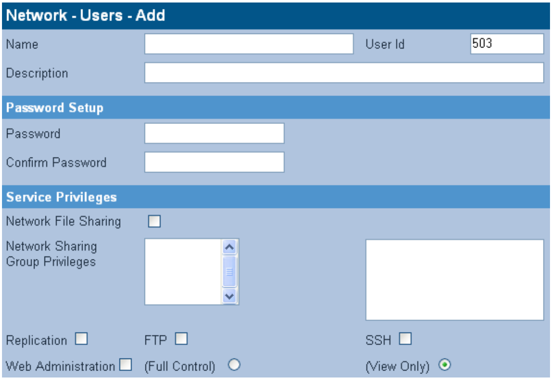


Network - Users

[Total 3 Entries] Page 1 of 1

User Name	UID	Web Admin (Full Control)	Web Admin (View Only)	Samba	Replication	SSH	FTP
admin	500	✓	✗	✗	✓	✓	✓
rep1	501	✗	✗	✗	✓	✗	✗
user1	502	✗	✓	✗	✗	✗	✗

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



Network - Users - Add

Name		User Id	503
Description			

Password Setup

Password	
Confirm Password	

Service Privileges

Network File Sharing □

Network Sharing Group Privileges

Replication □ FTP □ SSH □

Web Administration □ (Full Control) ○ (View Only) ●

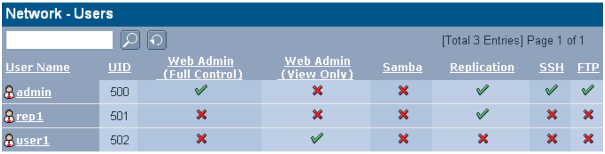
3. Enter the User's **Name**. A **User ID** is automatically generated.

> *Note: User ID (UID) and Group ID (GID) are used to control file access. All file changes will have these IDs set for Owner, Owner Group and other ACL entries. Once an ID has been assigned to a file object, it cannot be easily changed.*

4. Enter a **Description** for the User.
5. Enter and confirm the User's **Password** (required).
6. Tick the **Network File Sharing** box to enable CIFS 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 Secure Shell (SSH) access privileges, tick the **SSH** box. SSH can be used to log into the Appliance over a network using a command line (console) interface.
10. If the User is to have access to the Appliance's Web Interface, tick the **Web Administration** box. By default the User will then have **View Only** privileges. If required, select the **Full Control** radio button.
11. Click add to add the User.

Deleting a User

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



Network - Users

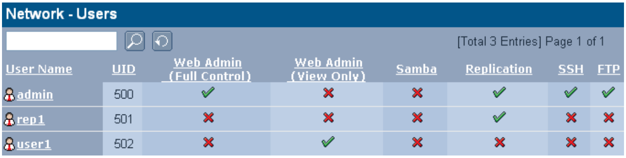
[Total 3 Entries] Page 1 of 1

User Name	UID	Web Admin (Full Control)	Web Admin (View Only)	Samba	Replication	SSH	FTP
admin	500	✓	✗	✗	✓	✓	✓
rep1	501	✗	✗	✗	✓	✗	✗
user1	502	✗	✓	✗	✗	✗	✗

2. Click the User Name of the User to be deleted. The **Network - Users - Update** page is displayed.
3. Click delete.
4. A warning message is displayed. Click delete to confirm deletion of the user.

Modifying a User's details

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

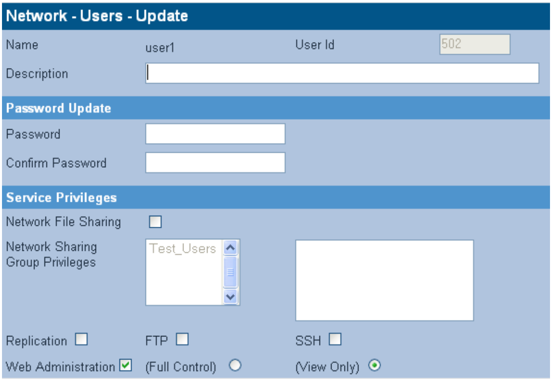


Network - Users

[Total 3 Entries] Page 1 of 1

User Name	UID	Web Admin (Full Control)	Web Admin (View Only)	Samba	Replication	SSH	FTP
admin	500	✓	✗	✗	✓	✓	✓
rep1	501	✗	✗	✗	✓	✗	✗
user1	502	✗	✓	✗	✗	✗	✗

2. Click the **User Name** of the User whose details are to be modified. The **Network - Users - Update** page is displayed:



Network - Users - Update

Name user1 User Id 502

Description

Password Update

Password

Confirm Password

Service Privileges

Network File Sharing □

Network Sharing Group Privileges: Test_Users

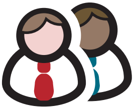
Replication □ FTP □ SSH □

Web Administration ☑ (Full Control) ○ (View Only) ●

3. The user's **Description**, **Password** or **Service Privileges** can be updated.

4. Click save to save the changes.

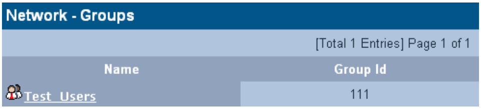
Groups



The **Network - Groups** page lists all the user groups known to the Appliance and allows addition, editing or deletion of groups from the system.

Adding a Group

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

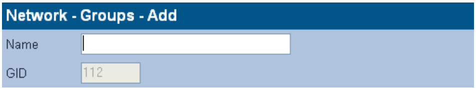


Network - Groups

[Total 1 Entries] Page 1 of 1

Name	Group Id
Test_Users	111

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



Network - Groups - Add

Name	
GID	112

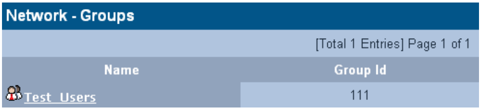
3. Enter a **Name** for the Group.

4. Click add to add the Group.

Editing a Group

Once a group has been created, only its name may be edited.

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

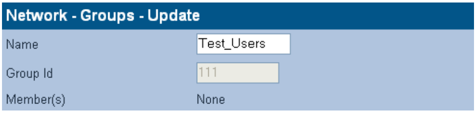


Network - Groups

[Total 1 Entries] Page 1 of 1

Name	Group Id
Test_Users	111

2. Click the **Name** of the group to be changed.
The **Network - Groups - Update** page is displayed:



Network - Groups - Update

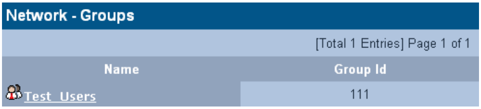
Name	Test_Users
Group Id	111
Member(s)	None

3. Change the group's **Name**.

4. Click save to save the changes.

Deleting a Group

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

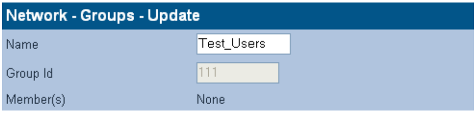


Network - Groups

[Total 1 Entries] Page 1 of 1

Name	Group Id
Test_Users	111

2. Click the **Name** of the Group to be deleted. The **Network - Groups - Update** page is displayed:



Network - Groups - Update

Name	Test_Users
Group Id	111
Member(s)	None

3. Click delete.

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

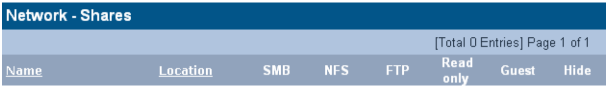
Shares

A network share is a directory on the Appliance that can be accessed by other hosts across the network.

The **Network - Shares** page allows viewing, editing and deletion of shares from the Appliance. It is also used to view active connections and open files and configure access control lists (ACLs) for each share.

Adding a Share

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

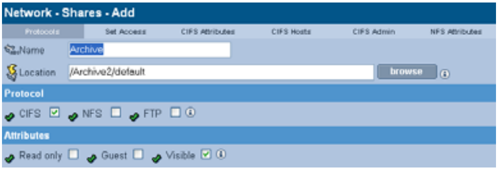


Network - Shares

[Total 0 Entries] Page 1 of 1

Name	Location	SMB	NFS	FTP	Read only	Guest	Hide

2. Click add. The **Network - Shares - Add (Protocols)** page is displayed:



Network - Shares - Add

Name: Archive

Location: /Archive2/default

Protocol

CIFS ☑ NFS □ FTP □

Attributes

Read only □ Guest □ Visible ☑

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

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

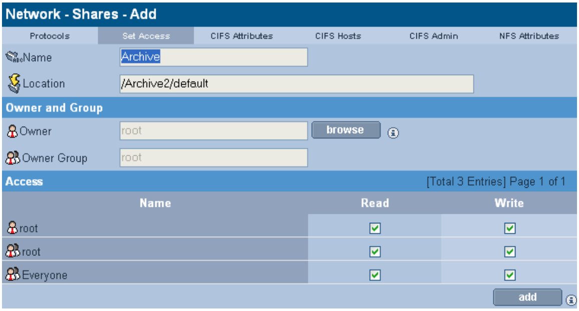
5. Tick the relevant **Protocol** box(es). This defines how the Users may access the Share. The Appliance can share files via Common Internet File System (**CIFS**), Network File System (**NFS**) and File Transfer Protocol (**FTP**).

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

Note: Read only, Guest and Hide are global attributes, and will be set across all protocols selected above.

- **Read-only** - write access is denied through the connecting protocol even though the AA file system is writable
- **Guest** - no authentication required, anybody can access the share
- **Visible** - share may exist but it is not advertised to the network unless ticked.

7. Click next >>. The **Set Access** tab is displayed:



Name: Archive

Location: /Archive2/default

Owner and Group

Owner: root

Owner Group: root

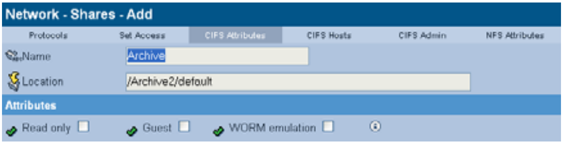
Access [Total 3 Entries] Page 1 of 1

Name	Read	Write
root	☑	☑
root	☑	☑
Everyone	☑	☑

8. The currently logged in user and group are displayed as the default **Owner** and **Owner Group**. Click browse to browse for a specific user.

9. To give specific users access to the share, click add and select from the user list (all local, Active Directory, and LDAP users are displayed).

10. Click next >>. If CIFS was selected in step 5 the **CIFS Attributes** tab is displayed:



Name: Archive

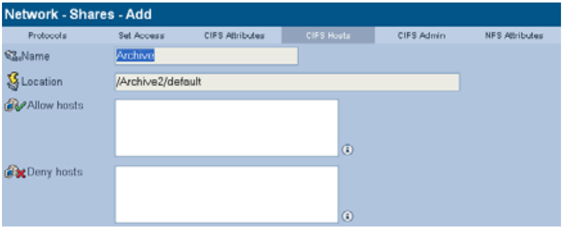
Location: /Archive2/default

Attributes

Read only □ Guest □ WORM emulation □

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

12. Click next >>. The **CIFS Hosts** tab is displayed:



Name: Archive

Location: /Archive2/default

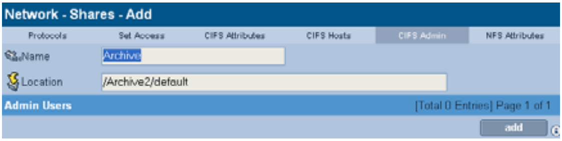
Allow hosts

Deny hosts

Enter the hostnames or IP addresses of Hosts that are to be specifically 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.

13. Click next >>. The **CIFS Admin** tab is displayed:



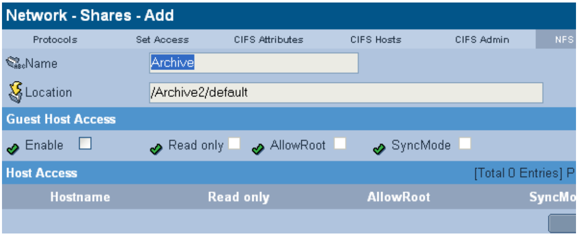
Name: Archive

Location: /Archive2/default

Admin Users [Total 0 Entries] Page 1 of 1

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

15. next >> is only available if NFS was selected in step 5. Clicking it will display the **NFS Attributes** tab:



Name: Archive

Location: /Archive2/default

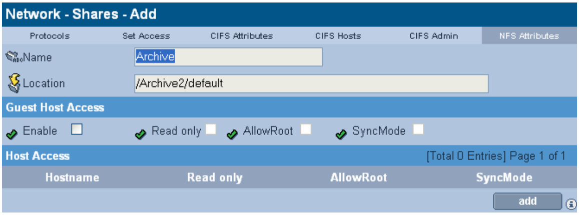
Guest Host Access

Enable □ Read only □ AllowRoot □ SyncMode □

Host Access [Total 0 Entries] P

Hostname	Read only	AllowRoot	SyncMo

16. Click add to add NFS Hosts to the Share.
    The **NFS Host Entry Details** page opens:



Network - Shares - Add

Name: Archive
Location: /Archive2/default

Guest Host Access

Enable □ Read only □ AllowRoot □ SyncMode □

Host Access [Total 0 Entries] Page 1 of 1

Hostname	Read only	AllowRoot	SyncMode

Enter the Hostname, then tick the boxes as required:

- **Read only** - Allow Read Only access to the share.
- **AllowRoot** - allows root user access to the share.
- **SyncMode** - (ticked by default) ensures the reliability of the network share. Plasmon strongly recommends the use of synchronous mode.

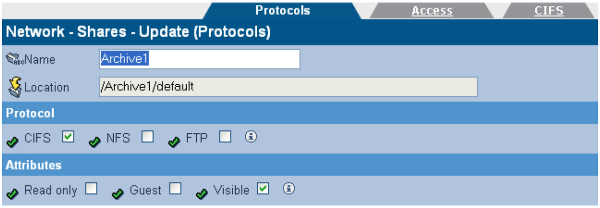
Click ok to continue.

17. Click add to add the share.

Deleting a share

Important: All users must be disconnected before a share can be deleted.

1. From the menu bar, select **Network - Shares**.
2. Click on the name of the share to be deleted.
3. The **Network - Shares - Update (Protocols)** page opens:



Network - Shares - Update (Protocols)

Name: Archive1
Location: /Archive1/default

Protocol

CIFS ☑ NFS □ FTP □

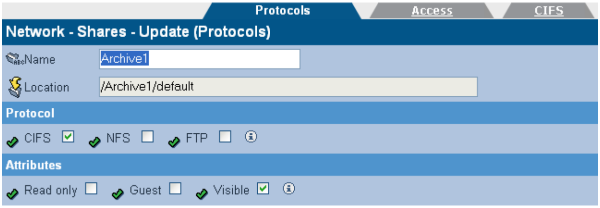
Attributes

Read only □ Guest □ Visible ☑

4. Click **delete**.
   The Appliance warns that the share is about to be deleted. Click **delete** again to confirm.

Modifying a share

1. From the menu bar, select **Network - Shares**.
2. Click on the name of the share to be deleted.
3. The **Network - Shares - Update (Protocols)** page opens:



Network - Shares - Update (Protocols)

Name: Archive1

Location: /Archive1/default

Protocol

CIFS ☑ NFS □ FTP □

Attributes

Read only □ Guest □ Visible ☑

4. To add or remove a networking protocol, click the relevant box. Adding a protocol will add a configuration tab for that protocol, and removing one will dispose of the associated tab.
5. Add or remove attributes by clicking the relevant box.
6. Click on the **Access** tab to change user and group permissions.
7. Click on the **CIFS**, **NFS** or **FTP** tab to change the configuration for the selected protocol.
8. When all required changes have been made, click **save**.

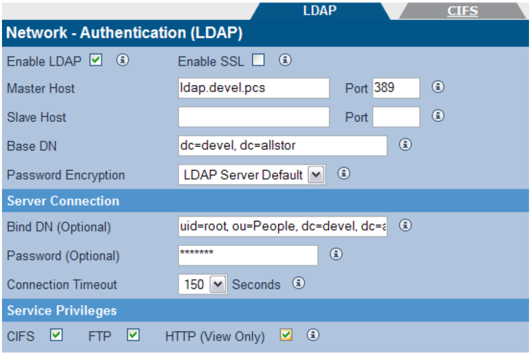
Note: For in-depth detail on the options available in each tab, see See *Adding a Share on page 45*.

Authentication

The **Network - Authentication** page defines access authentication to the Appliance using local users, LDAP or CIFS.

LDAP configuration

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



Network - Authentication (LDAP)

Enable LDAP ☑ Enable SSL □

Master Host: ldap.devel.pcs Port: 389

Slave Host: Port:

Base DN: dc=devel, dc=allstor

Password Encryption: LDAP Server Default

Server Connection

Bind DN (Optional): uid=root, ou=People, dc=devel, dc=a

Password (Optional): *******

Connection Timeout: 150 Seconds

Service Privileges

CIFS ☑ FTP ☑ HTTP (View Only) ☑

2. Tick **Enable LDAP** to enable LDAP authentication.
3. If required, tick **Enable SSL** to enable SSL encryption on the connection to the LDAP server.
4. Enter the **Master Host** hostname (or IP address) and TCP **Port** of the master LDAP server.
5. Enter the **Slave Host** hostname (or IP address) and TCP **Port** of the slave LDAP server.

Note: The Slave Host must have the same connection settings as the Master Host.

6. Enter the **Base DN**. The DN (Distinguished Name) of the base object from which to start the search.
7. Enter a **Password Encryption** type (the encryption type for the POSIX password). This can be either LDAP Server default (the Directory encryption default) or crypt (Unix-Crypt hash encryption).

8. Enter the **Bind DN** (Optional). The Distinguished Name (DN) to use when binding to the LDAP server. Leaving this blank will cause the LDAP connection to be anonymous.

   Note: Note that the user password cannot be set via an anonymous connection.

9. Enter a **Password** (Optional). The password used when binding the LDAP server with the Bind DN.
10. Enter a **Connection Timeout**. Select the LDAP request timeout (in seconds).
11. Click save to save the changes or click Test LDAP to test the connection to the LDAP server.

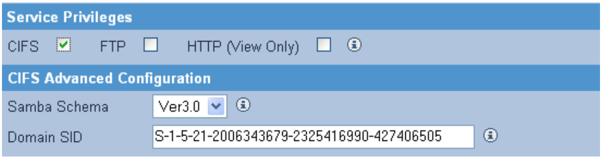
Service Privileges

The Appliance can be configured to enable CIFS, FTP and HTTP (View Only) users to be authenticated against the LDAP directory.

1. If required, tick the **CIFS**, **FTP**, or **HTTP (View Only)** as necessary.

   Note: Read-only administrators can change their own password. This is the only write capability of the read-only administrator.

2. If **CIFS** is selected, the CIFS Advanced Configuration options become available:



Service Privileges

CIFS ☑ FTP □ HTTP (View Only) □

CIFS Advanced Configuration

Samba Schema: Ver3.0

Domain SID: S-1-5-21-2006343679-2325416990-427406505

3 Select a **Samba Schema**. This will be the version of Samba Schema in use on the LDAP server.

  The default schema version is 3.0. The Appliance also supports version 2.2.

4 Enter the **Domain SID**. The Windows Security ID of the LDAP users. The SID defined in the directory is used if it is available.

5 Click **Save** to save the changes or click **Test LDAP** to test the connection to the LDAP server.

LDAP Service authentication configuration

This section describes how to configure some of the more common LDAP implementations for use with the Archive Appliance.

The Schema files referred to in this section can be found on the Archive Appliance System CD-ROM.

OpenLDAP

1. Copy the **samba.schema** file to `/usr/local/etc/openldap/schema/` and edit **slapd.conf** as follows

```
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/corba.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/misc.schema
include /usr/local/etc/openldap/schema/openldap.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/samba.schema
```

2. Save the **slapd.conf** file
3. Restart OpenLDAP service.

iPlanet

1. Copy **samba-schema-netscapeds5.x** to `.\iPlanet\servers\slapd-plz\config\schema` directory and rename it to **99user.ldif**
2. Restart iPlanet service.

Novell eDirectory

1. Copy **samba-nds.schema** to `/opt/novell/eDirectory/lib/nds-schema/ directory`, and rename it to **samba.ldif**
2. In the NDS server (Linux), execute the following command to import the RFC2307 schema if it is not available:

```
# ndssch -h localhost -t Tree_Name Admin_FDN /opt/novell/
eDirectory/lib/nds-schema/rfc2307-usergroup.sch
```

3. Then open ConsoleOne, import `/opt/novell/eDirectory/lib/nds-schema/samba.ldif`.
4. Restart ndsd service to take effect.

Most commonly used Samba schema attributes

To support the challenge/response authentication methods used by Microsoft clients, Samba requires a list of hashed passwords separate from the normal Unix account information stored in */etc/passwd* (or in the posixAccount object class). This collection of LanManager and Windows NT password hashes is normally stored in a file named *smbpasswd*; the format of each entry is:

username:uid:LM_HASH:NT_HASH:account flags:timestamp

This can be addressed by moving the information from a local, flat file into an LDAP directory. This can be achieved by importing the Samba schema, which can be found on the Archive Appliance System CD-ROM. A CLI tool *smbpasswd* is recommended to add a Samba user.

To use a normal LDAP administration tool (for example, LAT) for adding a Samba user:

1 Add the object class sambaAccount/SambaSAMAccount to the user.

2 Set the following attributes:

For Samba Schema 2.2

rid - relative ID,The value should be UID*2+1000

For example, `4097804623`

lmPassword - LanManager hashed password

ntPassword - Windows NT hashed password

For Samba Schema 3.3

sambaSID -Windows security ID, The value should be 'Samba Domain SID'+'-'+'rid'

For example, `S-1-5-21-3312872725-2188076328-4097804623`

sambaLMPassword
sambaNTPassword

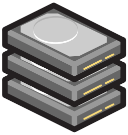
CIFS

The information in this tab is derived from, the **System - Services (CIFS)** page. Refer to “Configuring CIFS (Including Active Directory Server / NT Domain Server)” on page 16.

Chapter 5

Storage menu

RAIDs

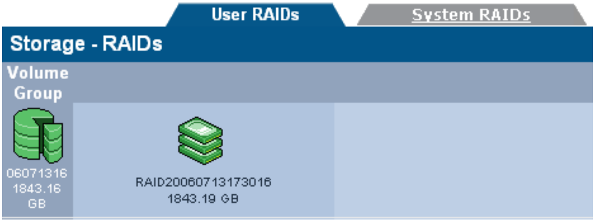


The **Storage - RAIDs** page allows viewing of RAIDs (Redundant Array of Independent Disks) on the system. Global hot spare disks can also be defined.

> *Note: On Archive Appliances with an internal archive controller, the RAID configuration is limited to a single RAID 1 (mirrored pair). On Archive Appliances with an external archive controller, the system RAID configuration is limited to a RAID 1 with a RAID 5 data configuration. System RAIDs are predefined and cannot be altered: they are maintained by the system automatically.*

Viewing RAIDs

1. From the menu bar, select **Storage - RAIDs**. The **User RAIDs** are displayed:



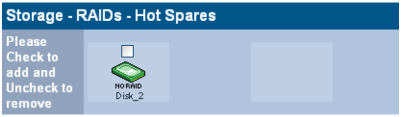
2. Hover over any Volume Group or RAID for a Tool Tip containing status information.s

Assigning global hot spare disks to a RAID

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

Note: Hot spare disks can only be defined if the system has free disks available.

1. From the menu bar, select **Storage - RAIDs**.
2. Click hot spares.
   The **Storage - RAIDs - Hot Spares** page will open:



Storage - RAIDs - Hot Spares

Please Check to add and Uncheck to remove

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

   Click set to set the hot spare(s).

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

RAID storage and filesystem scalability

The table below indicates the scalability of the Archive Appliance RAID cache and filesystem.

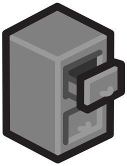
Table 5-1: RAID cache limitations

Description	Limit
Maximum number of RAIDs	12
Maximum size of a single RAID	2 TB
Maximum number of configurable volume groups	10
Maximum size of a configurable volume group	10 TB
Maximum number of logical volumes (archive or unmanaged volume) - Supermicro A12, A8, Foundation A8	12
Maximum number of logical volumes (archive or unmanaged volume) - Winboard, Foundation A2	8
Minimum size of a logical volume (archive or unmanaged volume)	20 GB

Table 5-1: RAID cache limitations

Description	**Limit**
Maximum size of a logical volume (archive or unmanaged volume)	2 TB
Maximum number of files system objects (files or directories) per logical volume (archive or unmanaged volume) - Supermicro A12, A8, Foundation A8.	100 million
Maximum number of files system objects (files or directories) per logical volume (archive or unmanaged volume) - Winboard, Foundation A2.	70 million
Maximum single file size (Appliance with internal controller)	5 GB
Maximum single file size (Appliance with external controller using 500GB SATA disks)	12 GB

Volumes



The **Storage - Volumes** page can view, add or remove volumes from the system.

About volumes

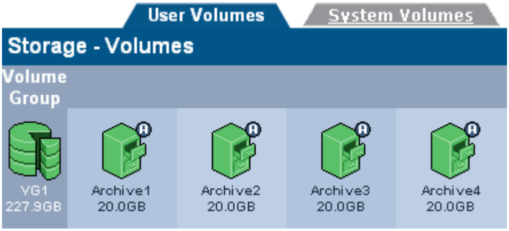
The term volume, in this context, refers to a logical volume (as opposed to a physical volume) which is part of a volume group.

On the Appliance, two types of volume are available:

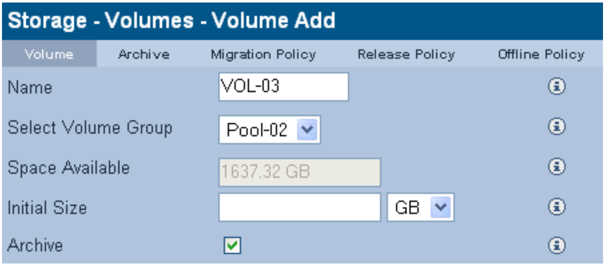
- An archive - where data is written to the Appliance’s RAID(s) and when defined criteria have been met, the data is migrated onto UDO media - see *Creating an archive* on page 59.
- An unmanaged volume - where data is written to the Appliance’s RAID cache only - see *Creating an unmanaged volume* on page 67

Creating an archive

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



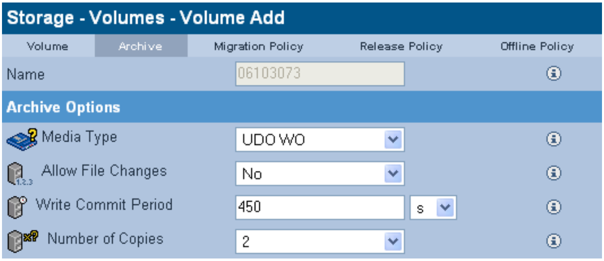
2. Click add.
   The **Storage -Volumes - Volume Add** page opens:



Storage - Volumes - Volume Add

Name	VOL-03
Select Volume Group	Pool-02
Space Available	1637.32 GB
Initial Size	GB
Archive	☑

3. A **Name** is automatically generated, which can be edited. The limit is up to eight characters, which can include; a-z, A-Z, 0-9, - (hyphen) and _ (underscore).
4. Select the Volume Group that the volume will be created in from the **Select Volume Group** drop-down list.
5. The **Space Available** is shown. Enter an **Initial Size** for the volume.
6. If the Volume is to be an archive, tick the **Archive** box.
7. Click next >> to continue.
   The **Storage -Volumes - Volume Add** page, **Archive** tab opens:



Storage - Volumes - Volume Add

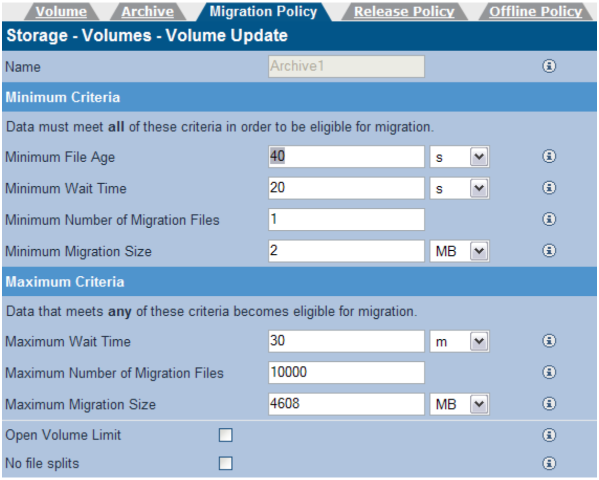
Name	06103073

Archive Options

Media Type	UDO WO
Allow File Changes	No
Write Commit Period	450 s
Number of Copies	2

8. Select the **Media Type** the archive will use:
   - **UDO WO** - UDO WORM media
   - **UDO CWO** - Compliant UDO WORM media.

9. Select whether to **Allow File Changes**:
   - If **Yes** is selected then changes to the file are permitted at any time after the file is written and multiple versions of the file are stored.
   - If **No** is selected, a WORM filesystem is created. After the write commit period has expired, no further file changes are permitted.
10. Enter a **Write Commit Period** in **s**econds, **m**inutes or **h**ours. This sets the time period after the file is closed during which file updates can be made. After this time period has passed no further changes are permitted.
11. Select the **Number of Copies** of the file to make. Copies are made on separate UDO media and can be offlined to provide an additional level of data protection.
12. Click next >> to continue.
    The **Storage -Volumes - Volume Add** page, **Migration Policy** tab opens:



Storage - Volumes - Volume Update

Name	Archive1	
Minimum Criteria		
Data must meet **all** of these criteria in order to be eligible for migration.		
Minimum File Age	40	s
Minimum Wait Time	20	s
Minimum Number of Migration Files	1	
Minimum Migration Size	2	MB
Maximum Criteria		
Data that meets **any** of these criteria becomes eligible for migration.		
Maximum Wait Time	30	m
Maximum Number of Migration Files	10000	
Maximum Migration Size	4608	MB
Open Volume Limit	□	
No file splits	□	

Migration is the process of reading files from the cache and writing them to UDO media. As files are written to the cache they are grouped together into migration jobs.

Migration jobs are started when all of the minimum criteria, or any one of the maximum criteria have been met

13. Enter the following **Minimum Criteria**:
    - **Minimum File Age** - The amount of time a file must remain unchanged to become a candidate for migration
    - **Minimum Wait Time** - Migration will NOT be started if new files are added to migration candidate list in Minimum Wait Time
    - **Minimum Number of Migration Files** - Migration will NOT be started if there are less than Minimum Number of Migration Files to be migrated
    - **Minimum Migration Size** - Migration will NOT be started if the total size is less than Minimum Migration Size.
14. Enter the following **Maximum Criteria**:
    - **Maximum Wait Time** - Migration will be started if the elapsed time since the first file was added to migration candidate list is more than Maximum Wait Time
    - **Maximum Number of Migration Files** - Migration will be started if there are more than Maximum Number of Migration Files waiting to be migrated
    - **Maximum Migration Size** - Migration will be started if the total size exceeds Maximum Migration Size.
15. Select whether there should be an **Open Volume Limit**. Selecting this option will limit the number of open volumes in a media pool to one. This can result in lower migration throughput as multiple volumes are not opened to utilise all of the available drives, but files from the same directory are less likely to be split across different media.
16. In the event that the media becomes full during a migration task, files may be split between different media. Setting the **No file splits** option prevents this.

The following examples illustrate the different migration configurations that can be achieved.

Example 1 - Migration default settings

With the following minimum settings:

- **Minimum File Age:** 10 Secs
- **Minimum Wait Time:** 20 Secs
- **Minimum Number of Migration Files:** 1
- **Minimum Migration size:** 2 MB
-

and the following maximum settings:

- **Maximum Wait Time:** 30 minutes
- **Maximum Number of Migration files:** 10000
- **Maximum migration size:** 4608 MB

Migration will occur as soon as at least one file larger than 2 MB becomes eligible for migration (by remaining unchanged for 10 seconds or more) and no other files have become eligible for migration within the last 20 seconds. Even if not all of the minimum criteria are met, a migration will occur at least once every 30 minutes, or sooner if the number of files eligible for migration number more than 10000 or become collectively larger than 4608 MB in size.

Example 2 - Frequent, low data volume

With the following minimum settings:

- **Minimum File Age:** 10 Secs
- **Minimum Wait Time:** 10 Secs
- **Minimum Number of Migration Files:** 1
- **Minimum Migration size:** 1 MB
-

and the following maximum settings:

- **Maximum Wait Time:** 10 minutes
- **Maximum Number of Migration files:** 1000
- **Maximum migration size:** 100 MB

Migration will occur as soon as at least one file larger than 1 MB becomes eligible for migration (by remaining unchanged for 10 seconds or more) and no other files have become eligible for migration within the last 10 seconds. Even if not all of the minimum criteria are met, a migration will occur at least once every 10 minutes, or sooner if the number of files eligible for migration number more than 1000 or become collectively larger than 100 MB in size.

Example 3 - Less frequent, greater data volume

With the following minimum settings:

- **Minimum File Age:** 10 Secs
- **Minimum Wait Time:** 1 hour
- **Minimum Number of Migration Files:** 1000
- **Minimum Migration size:** 100 MB
-

and the following maximum settings:

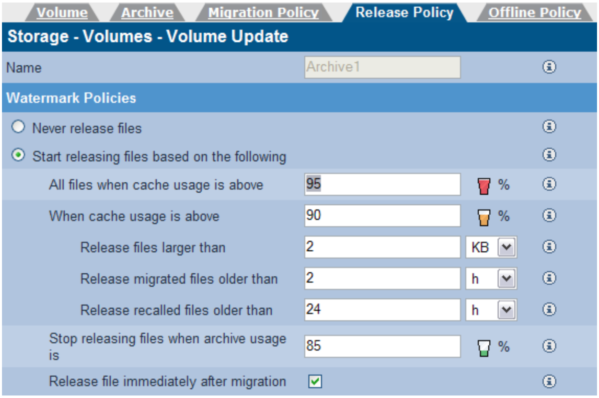
- **Maximum Wait Time:** 4 Hours
- **Maximum Number of Migration files:** 10000
- **Maximum migration size:** 4.5 GB

Migration will occur as soon as at least 1000 files, larger than 100 MB in total become eligible for migration (by remaining unchanged for 10 seconds or more) and no other files have become eligible for migration within the last hour. Even if not all of the minimum criteria are met, a migration will occur at least once every 4 hours, or sooner if the number of files eligible for migration number more than 1000 or become collectively larger than 4.5 GB in size.

Table 5-2: Migration policy setting ranges.

Setting	Min.	Max.
Minimum Wait Time	1 s	1 h
Minimum number of Migrations files	1	1000
Minimum migration size	256 B	100 MB
Maximum wait time	1 s	24 h
Maximum number of migration files	1	10000
Maximum migration size	1 MB	4.5 GB

17. Click next >> to continue.
    The **Storage -Volumes - Volume Add** page, **Release Policy** tab opens:



Storage - Volumes - Volume Update

Name	Archive1	
Watermark Policies		
○ Never release files		
● Start releasing files based on the following		
All files when cache usage is above	95	%
When cache usage is above	90	%
Release files larger than	2	KB
Release migrated files older than	2	h
Release recalled files older than	24	h
Stop releasing files when archive usage is	85	%
Release file immediately after migration	☑	

Releasing is the process of truncating files on the RAID cache following migration to UDO media. The truncated file is retained on the RAID cache as a reference to the migrated file to enable it to be located and recalled if required.

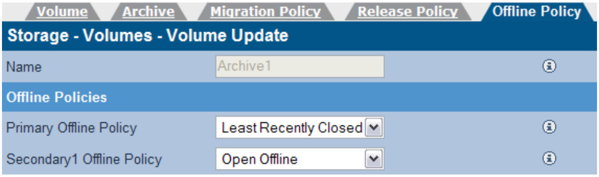
18. To set release policies for the archive, select:
    - **Never release files** - Files are never released from the RAID cache.

- or -

- **Start releasing files based on the following:**
  - **All files when cache usage is above:** When the specified percentage of storage space on the RAID cache is used, the system will start releasing all migrated and recalled files.
  - **When cache usage is above:** When the specified percentage of RAID cache storage space has been used, files which meet all of the following criteria will be released:
    - **Release files larger than:** Only files larger than the specified size will be released.

        - **Release migrated files older than:** Only files that have been migrated longer than the specified time will be released.
        - **Release recalled files older than:** Only files that have been recalled longer than the specified time will be released.
    - **Stop releasing files when archive usage is**: When RAID cache usage reaches the specified percentage, files stop being released.
    - **Release files immediately after migration:** All migrated files are released immediately, irrespective of RAID cache storage space usage.

19. Click next >> to continue.
    The **Storage -Volumes - Volume Add** page, **Offline Policy** tab opens:



Storage - Volumes - Volume Update

Name	Archive1
Offline Policies	
Primary Offline Policy	Least Recently Closed
Secondary1 Offline Policy	Open Offline

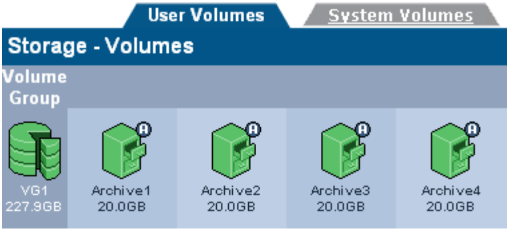
20. Select a **Primary** and **Secondary Offline Policy** from the drop down lists:
    - **Prohibit offline** - Media in the pool cannot be offlined.
    - **Least Recently Used** - Media are offlined in order of media closure. The oldest closed media is offlined first.
    - **Least Recently Closed** - Media are offlined in order of last read/write operation. The closed media with the oldest read/write request is offlined first.
    - **Open Offline** - Media in the pool may be offlined while still open for writing in order to be stored as an offsite backup copy (Open Offline can only be enabled on a single secondary media pool). For further information on Open Offline media, see the *Archive Appliance Operator's Guide*.
21. Click add.
    Once the volume has been created, the Appliance will return to the **Storage - Volumes** page.

Creating an unmanaged volume

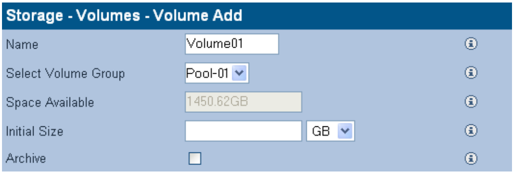
Once a RAID has been created, the associated volume group can be divided into volumes.

To create a standard volume:

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



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



Storage - Volumes - Volume Add

Name	Volume01
Select Volume Group	Pool-01
Space Available	1450.62GB
Initial Size	GB
Archive	□

3. A **Name** is automatically generated, or can beentered (up to 32 characters; a-z, A-Z, 0-9, - (hyphen e.g. Volume-01) and _ (underscore e.g. Volume_1).
4. Select a Pool that the volume should be in from the **Select Volume Group** drop-down list.
5. The **Space Available** is shown.

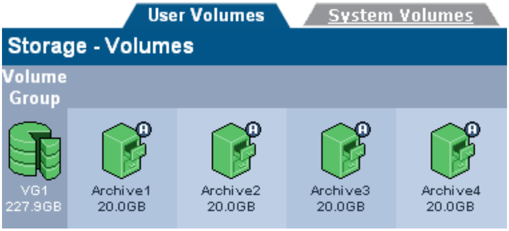
Caution: Volume size can be increased after creation. However, the size of a volume can only be reduced by removing the volume from the volume group and restoring from backup (we recommend that this only be performed by a Service Engineer). We recommend that during creation, the volume size is set to the minimum size that is likely to be required.

Enter an **Initial Size** for the volume.

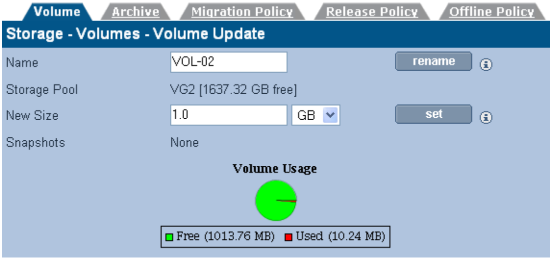
6. Click add. Once the volume has been created, the Appliance will return to the **Storage - Volumes** page.

Viewing and editing volume properties

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



2. Click on the volume to view or update.
   The **Storage -Volumes - Volume Update** page opens:



Storage - Volumes - Volume Update

Name	VOL-02	rename
Storage Pool	VG2 [1637.32 GB free]	
New Size	1.0 GB	set
Snapshots	None	

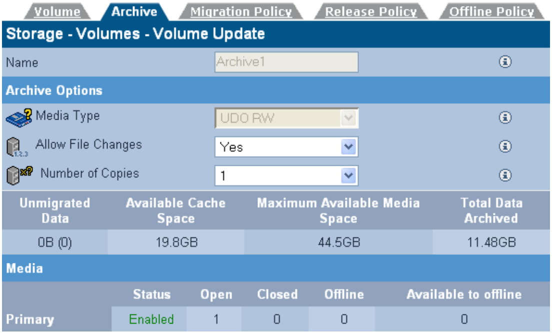
🟩 Free (1013.76 MB) 🟥 Used (10.24 MB)

Items that may be edited are:

- **Name** - (user volumes only) To change the volume name, type in a new name and click rename
- **New Size** - To change the size of the volume, enter a new size and click set.

Note: If the volume is part of a replication pair, remember to also resize the volume on the Appliance hosting the partnered volume.

3. Click on the **Archive** tab.



Storage - Volumes - Volume Update

Name: Archive1

Archive Options

Media Type: UDO RW

Allow File Changes: Yes

Number of Copies: 1

Unmigrated Data	Available Cache Space	Maximum Available Media Space	Total Data Archived
0B (0)	19.8GB	44.5GB	11.48GB

Media

	Status	Open	Closed	Offline	Available to offline
Primary	Enabled	1	0	0	0

Items that may be edited are:

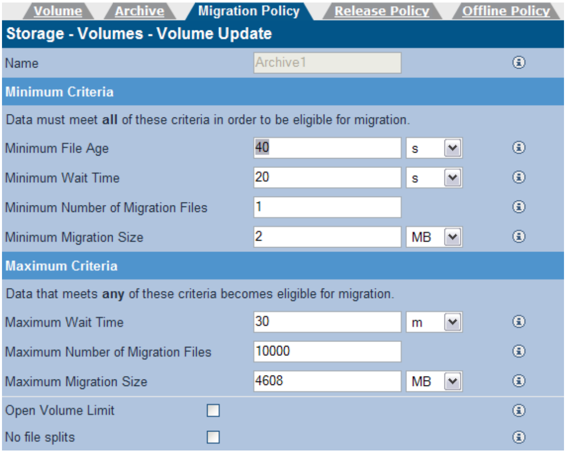
- **Allow File Changes**.
- **Write commit period**
- **Number of copies**

Information-only fields are:

- **Unmigrated Data** - Shows the cumulative size of the files awaiting migration. The value in brackets is the number of files awaiting migration. This value includes directories, files and file attribute changes.
- **Available Cache Space** - This value is the summation of the actual free space on the cache (shown on the Volume tab) plus the space currently taken up by releasable files which will be made available when the release watermarks are met (see Release Policy tab)
- **Maximum Available Media Space** - Is the amount of media space available for migration assuming that all available media gets assigned to this archive. If there are multiple archives configured, then in practise this available media space will be smaller
- **Total Data Archived** - Is the total amount of data from this archive that has been migrated to media

- **Media** - Totals are for each pool (Primary, Secondary1, Secondary2 as appropriate):
    - **Status. Enabled** - data will be migrated to media in this pool, and **Disabled** - data will not be migrated to media in this pool.
        - **Open** - The number of open media in this pool. Open media already have data written to them
        - **Closed** - The number of closed media in this pool. Closed media will have no further data migrated to them
        - **Offline** - The number of offline media from this pool
        - **Available to offline** - The number of media now available to be offlined from this pool. Media can be offlined by using the 'Offline media' option on the keypad.

4. Click on the **Migration Policy** tab:



Storage - Volumes - Volume Update

Name	Archive1	
Minimum Criteria		
Data must meet **all** of these criteria in order to be eligible for migration.		
Minimum File Age	40	s
Minimum Wait Time	20	s
Minimum Number of Migration Files	1	
Minimum Migration Size	2	MB
Maximum Criteria		
Data that meets **any** of these criteria becomes eligible for migration.		
Maximum Wait Time	30	m
Maximum Number of Migration Files	10000	
Maximum Migration Size	4608	MB
Open Volume Limit	□	
No file splits	□	

Items that may be edited are:

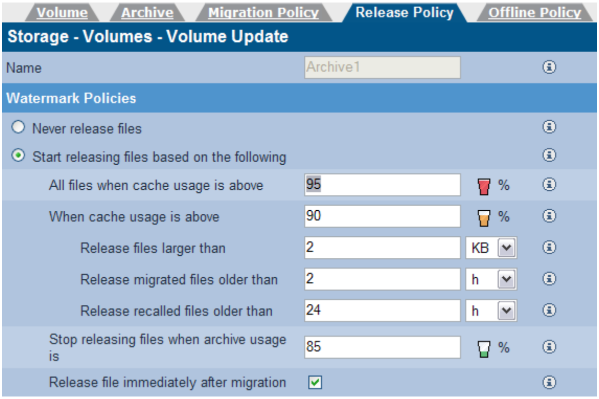
- **Minimum File Age**
- **Minimum Wait Time**
- **Minimum Number of Migration Files**
- **Minimum Migration Size**
- **Maximum Wait Time**

- **Maximum Number of Migration Files**
- **Maximum Migration Size**
- **Open Volume Limit**
- **No file splits**

Information-only fields are:

- **Name**

5. Click on the **Release Policy** tab.



Storage - Volumes - Volume Update

Name	Archive1	
Watermark Policies		
○ Never release files		
● Start releasing files based on the following		
All files when cache usage is above	95	%
When cache usage is above	90	%
Release files larger than	2	KB
Release migrated files older than	2	h
Release recalled files older than	24	h
Stop releasing files when archive usage is	85	%
Release file immediately after migration	☑	

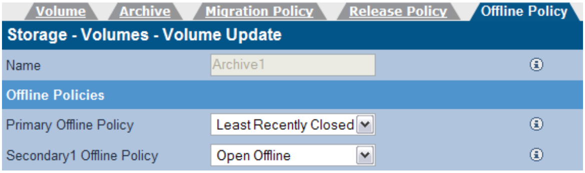
Items that may be edited are:

- **Watermark Policies**:
  - **Never Release Files**
  - **Start releasing files based on the following**
    - **All files when cache usage is above**
    - **When cache usage is above**
      - **Release files larger than**
      - **Release migrated files older than**
      - **Release recalled files older than**
    - **Stop releasing files when archive usage is** -
    - **Release file immediately after migration**.

Information-only fields are:

- **Name**

6. Click on the **Offline Policy** tab:



Storage - Volumes - Volume Update

Name: Archive1

Offline Policies

Primary Offline Policy: Least Recently Closed

Secondary1 Offline Policy: Open Offline

Items that may be edited are:

- **Primary Offline Policy**.
- **Secondary Offline Policy**.

Information-only fields are:

- **Name**

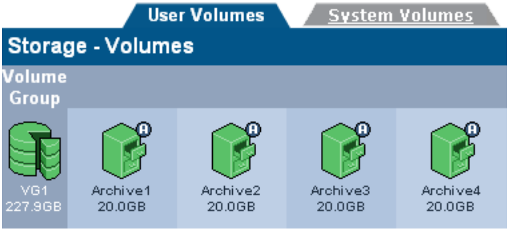
7. When any changes are complete, click **save** to save the changes.

Removing a Volume

Note: An archive volume cannot be removed if there are active migration jobs or online media associated with it.

To remove a volume:

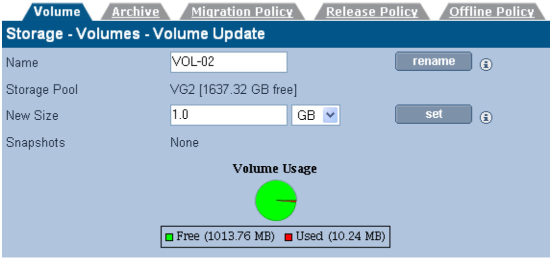
1. Offline all media associated with the volume.
2. From the menu bar, select **Storage - Volumes.**



Storage - Volumes

Volume Group

3. Click on the volume that is to be removed.
   The **Storage -Volumes - Volume Update** page opens:



Storage - Volumes - Volume Update

Name	VOL-02	rename
Storage Pool	VG2 [1637.32 GB free]	
New Size	1.0 GB	set
Snapshots	None	

Volume Usage

🟩 Free (1013.76 MB) 🟥 Used (10.24 MB)

4. Click remove. The system will offer a prompt to confirm deletion of the volume.

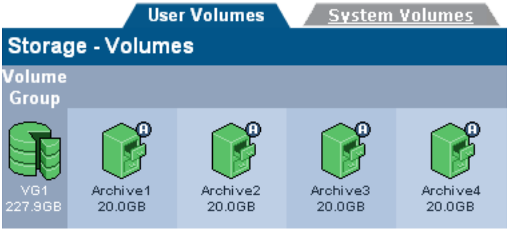
5. Click remove again to confirm or click cancel to cancel.

Volume quotas

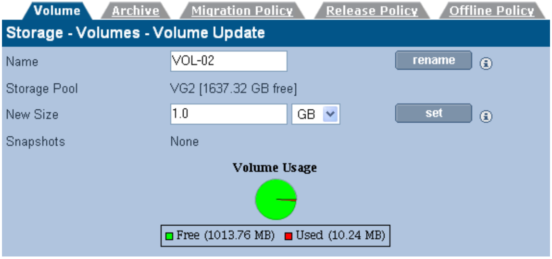
Users can be allocated a specific amount of a volume which they can use. This amount is called their quota.

Defining a user's quota

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



2. Click on the volume to change the quota of.
   The **Storage -Volumes - Volume Update** page opens:



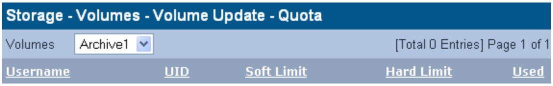
Storage - Volumes - Volume Update

Name	VOL-02	rename
Storage Pool	VG2 [1637.32 GB free]	
New Size	1.0 GB	set
Snapshots	None	

Volume Usage

🟩 Free (1013.76 MB) 🟥 Used (10.24 MB)

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

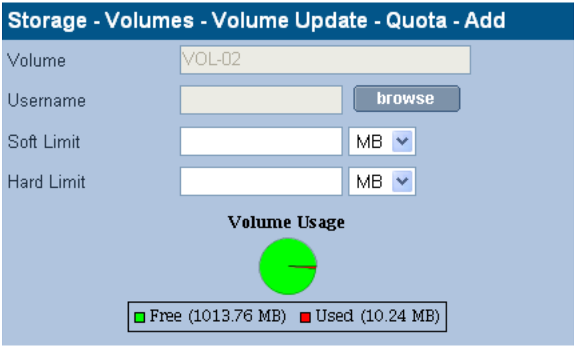


Storage - Volumes - Volume Update - Quota

Volumes Archive1 [Total 0 Entries] Page 1 of 1

Username	UID	Soft Limit	Hard Limit	Used

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



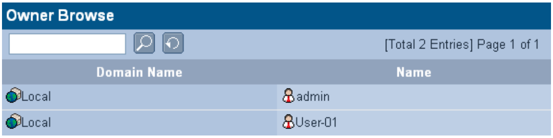
Storage - Volumes - Volume Update - Quota - Add

Volume	VOL-02	
Username		browse
Soft Limit		MB
Hard Limit		MB

Volume Usage

🟩 Free (1013.76 MB) 🟥 Used (10.24 MB)

5. Click **browse** to select a user:



Owner Browse

[Total 2 Entries] Page 1 of 1

Domain Name	Name
Local	admin
Local	User-01

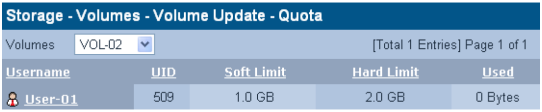
Click the name of the user to allocate the quota to and return to the **Storage - Volumes - Volume Update - Quota - Add** page.

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:



Storage - Volumes - Volume Update - Quota

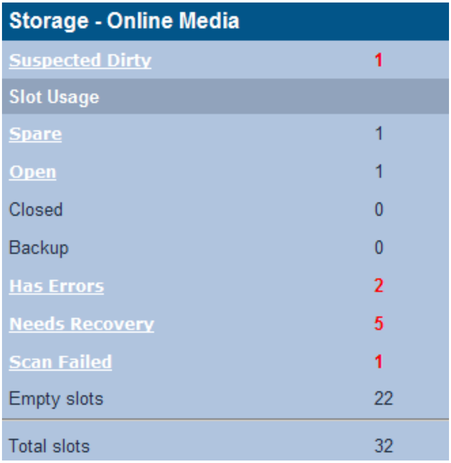
Volumes VOL-02

[Total 1 Entries] Page 1 of 1

Username	UID	Soft Limit	Hard Limit	Used
User-01	509	1.0 GB	2.0 GB	0 Bytes

Online Media

The **Storage - Online Media** page displays:



Storage - Online Media	
Suspected Dirty	1
Slot Usage	
Spare	1
Open	1
Closed	0
Backup	0
Has Errors	2
Needs Recovery	5
Scan Failed	1
Empty slots	22
Total slots	32

- **Slot Usage**:
  - **Needs Scan** - Media which has been added to the Appliance but has not yet been scanned.
  - **Scanning** - Media which is in the process of being scanned.
  - **Scan failed** - Media that cannot be scanned by the appliance.
  - **Spare** - Unused and available pieces of media in the spare pool (i.e. not assigned to any archive).
  - **Open** - Media assigned to an archive and with data still being written to it.
  - **Closed** - Full media. Closed media can be taken offline once the required period of time has elapsed (to ensure it is included in a backup).
  - **Backup** - The number of pieces of backup media in the system. Plasmon recommends that two pieces of backup media are kept in the Appliance at all times.

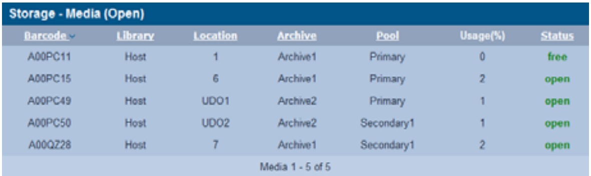
  - **Has Errors** - Media that has generated two or more errors on two separate UDO drives is marked as being in the **Has Errors** state. It should be noted that media which, when read, is discovered to be an unexpected volume (i.e. media that has been moved from it's original slot manually) will also be marked as being in the **Has Errors** state even though the media itself has generated no errors.
  - **Suspected Dirty** - Media with errors that are suspected of being dirty by the system. Media suspected as dirty should be cleaned.
  - **Needs recovery** - Media is in this state prior to being resynchronized during a system recovery.
  - **Failed to initialize** - Media in the Appliance that have failed to initialize. Media in this state does not contain any useful file information and can be safely removed from the Appliance using the keypad interface.

Note: All media types except ***Spare, Open, Closed*** *and* ***Backup*** *are only displayed when media in these states are present.*

  - **Empty slots** - The number of empty storage slots in the library.

- **Total slots** - The total number of storage slots available in the library.

By clicking the category hyperlinks on the summary page, a detailed inventory page for that type of online media is displayed:



Storage - Media (Open)

Barcode	Library	Location	Archive	Pool	Usage(%)	Status
A00PC11	Host	1	Archive1	Primary	0	free
A00PC15	Host	6	Archive1	Primary	2	open
A00PC49	Host	UDO1	Archive2	Primary	1	open
A00PC50	Host	UDO2	Archive2	Secondary1	1	open
A00QZ28	Host	7	Archive1	Secondary1	2	open

Media 1 - 5 of 5

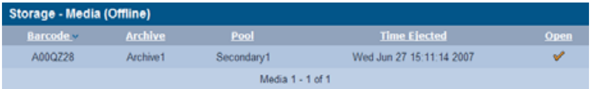
Not all the fields listed below are relevant to all media types and therefore may not be displayed on all online media inventory pages:

- **Barcode** - The media barcode
- **Library** - Indicates if the media resides in the host or the overflow library

- **Location** - The slot or drive number where the media is currently located
- **Archive** - The Archive which the media is assigned to
- **Pool** - The media pool that the media belongs to
- **Usage (%)** - The percentage of storage space used on the media
- **Status** - Current status of the media:
    - **Free** - Media is assigned to an Archive but is not being used for migration
    - **Good** - Backup media which is not in use and has no errors.
    - **Needs Scan** - Media has been inserted into the appliance but has yet to be scanned.
    - **Scanning** - Media is currently being read after being inserted into the appliance.
    - **Scan Failed** - Media cannot be scanned by the Appliance.
    - **Uninitialized** - Media has not yet been initialized or assigned to a spare media pool
    - **Open** - Media is open for writing
    - **Full** - All storage space on the media is used
    - **In use** - Media is currently being used for a migration or recall operation
    - **Unreliable** - Media has suffered a read/write failure in two or more drives
    - **Unusable** - Media identity cannot be verified
    - **Dirty** - media requires cleaning
    - **Recovery** - Media is marked recovery prior to being resynchronized during a system recovery
    - **Unknown** - Media has not yet been scanned and identified by the Appliance (usually following insertion)
    - **Duplicated** - Media bears a duplicate barcode sticker to another media in the Appliance's inventory

Offline Media

The **Storage - Offline Media** page allows the tracking of media which has been offlined by the system, displaying:



Storage - Media (Offline)

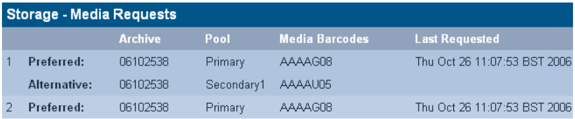
Barcode	Archive	Pool	Time Ejected	Open
A00QZ28	Archive1	Secondary1	Wed Jun 27 15:11:14 2007	✓

Media 1 - 1 of 1

- **Barcode** - The barcode of the offline media,
- **Archive** - The Archive which the media is assigned to,
- **Pool** - The media pool that the media belongs to,
- **Time ejected** - The time and date the media was ejected by the system,
- **Open** - Media's open/closed status. When ticked, this indicates open offline media.

Media Requests

The **Storage - Media Requests** page displays any outstanding data access request(s) for offline media, as follows:



Storage - Media Requests

		Archive	Pool	Media Barcodes	Last Requested
1	Preferred:	06102538	Primary	AAAAG08	Thu Oct 26 11:07:53 BST 2006
	Alternative:	06102538	Secondary1	AAAAU05	
2	Preferred:	06102538	Primary	AAAAG08	Thu Oct 26 11:07:53 BST 2006

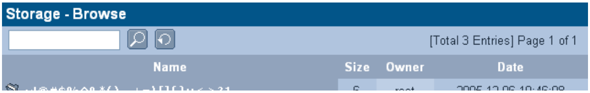
- **Preferred** and/or **Alternative** - indicates the preferred copy to be returned and if that is not available, an alternative copy.
- **Archive** - The archive the media is part of
- **Pool** - The pool (within the archive) which the media is part of
- **Media Barcode** - The barcode of the offline media which has been requested
- **Last Requested** - The time and date the media was requested for a recall by the system

Browse

The **Storage - Browse** page enables searching or browsing through the directories present on the system.

Finding files

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



Storage - Browse

🔍 ↺ [Total 3 Entries] Page 1 of 1

Name	Size	Owner	Date

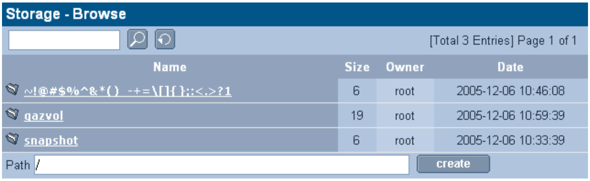
2. Enter a search string in the text box and click 🔍.
3. Click ↺ to clear the content of the text box.
   Alternatively, manually browse the directory tree for a file.

Setting or modifying an ACL

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

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

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



Storage - Browse

🔍 ↺ [Total 3 Entries] Page 1 of 1

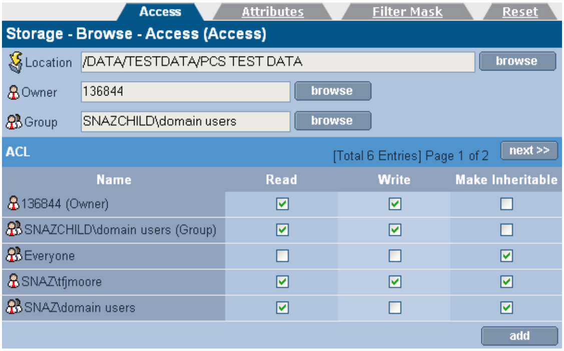
Name	Size	Owner	Date
~!@#$%^&*() -+=\[]{ };:<.>?1	6	root	2005-12-06 10:46:08
gazvol	19	root	2005-12-06 10:59:39
snapshot	6	root	2005-12-06 10:33:39

Path /

create

2. Search or browse to a directory or file.

   Click on access.
   The **Storage - Browse - Access** page opens.



Storage - Browse - Access (Access)

Location /DATA/TESTDATA/PCS TEST DATA

Owner 136844

Group SNAZCHILD\domain users

ACL [Total 6 Entries] Page 1 of 2

Name	Read	Write	Make Inheritable
136844 (Owner)	☑	☑	□
SNAZCHILD\domain users (Group)	☑	☑	□
Everyone	□	□	☑
SNAZ\tfjmoore	☑	☑	☑
SNAZ\domain users	☑	□	☑

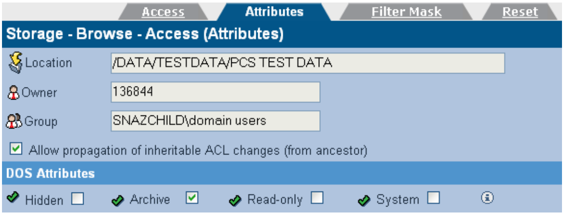
From this page:

- 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
- Set or view **ACL** - This section lists the users and groups who have access to the directory and their access privileges.

3. Click add to add more users or groups.
4. Click the **Attributes** tab.



Storage - Browse - Access (Attributes)

Location /DATA/TESTDATA/PCS TEST DATA

Owner 136844

Group SNAZCHILD\domain users

☑ Allow propagation of inheritable ACL changes (from ancestor)

DOS Attributes

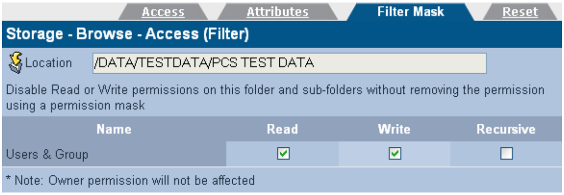
Hidden □ Archive ☑ Read-only □ System □

From this tab:

- **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, a single ACL can be placed high up in the directory tree to control access

The **DOS Attributes** for the directory can also be set.

5. Click the **Filter Mask** tab.



Storage - Browse - Access (Filter)

Location /DATA/TESTDATA/PCS TEST DATA

Disable Read or Write permissions on this folder and sub-folders without removing the permission using a permission mask

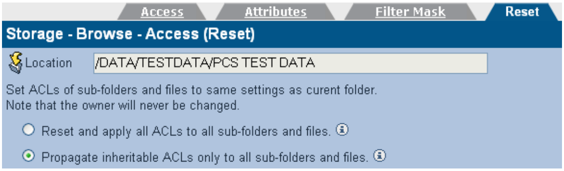
Name	Read	Write	Recursive
Users & Group	☑	☑	□

* Note: Owner permission will not be affected

In this tab:

- **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.

6. Click the **Reset** tab.



Storage - Browse - Access (Reset)

Location /DATA/TESTDATA/PCS TEST DATA

Set ACLs of sub-folders and files to same settings as curent folder.
Note that the owner will never be changed.

○ Reset and apply all ACLs to all sub-folders and files. ⓘ

● Propagate inheritable ACLs only to all sub-folders and files. ⓘ

The access permissions of sub-directories may be set to be the same as the current directory from this tab.

- **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 Propagate Inheritable, to all sub-folders and files.

Note: On systems with large numbers of files, this operation may take an extended period of time to complete.

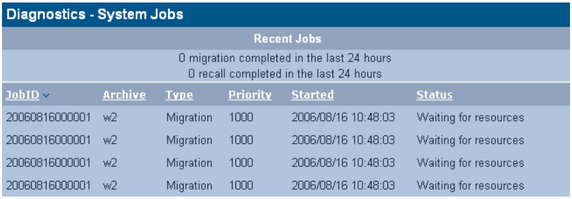
When the ACLs have been satisfactorily set, click save to save the changes.

Chapter 6

Diagnostics menu

System Jobs

The **Diagnostics - System Jobs** page displays recent migration and recall activity.



Diagnostics - System Jobs

Recent Jobs

0 migration completed in the last 24 hours
0 recall completed in the last 24 hours

JobID	Archive	Type	Priority	Started	Status
20060816000001	w2	Migration	1000	2006/08/16 10:48:03	Waiting for resources
20060816000001	w2	Migration	1000	2006/08/16 10:48:03	Waiting for resources
20060816000001	w2	Migration	1000	2006/08/16 10:48:03	Waiting for resources
20060816000001	w2	Migration	1000	2006/08/16 10:48:03	Waiting for resources

The following information is presented:

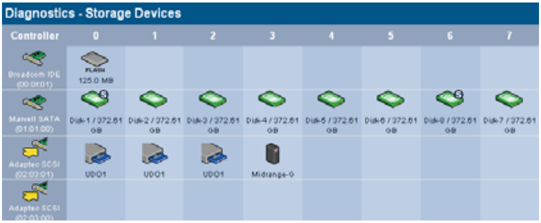
- **Job ID** - The unique identifying number assigned to the job
- **Archive** - The archive which the migration job is a part of
- **Type** - Whether the job is a migration, recall, backup, etc.
- **Media** - The Barcode of the media being used by the system job.
- **Priority** - Jobs are given one of three priorities; recall jobs have the highest priority, migration medium priority and backup the lowest priority
- **Started** - The time the job was started
- **Status** - The job’s status.

Storage Devices

The **Diagnostics - Storage Devices** page shows all interface buses (SATA, SCSI and IDE) and their associated devices and their status.

Viewing the Storage Devices

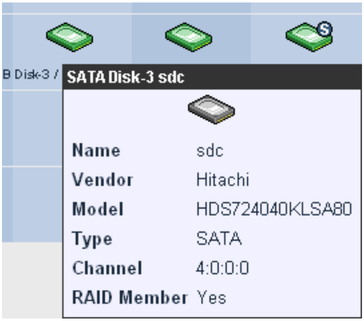
1. From the menu bar, select **Diagnostics - Storage Devices**.



Diagnostics - Storage Devices

Controller	0	1	2	3	4	5	6	7
Broadcom IDE (00:01:01)	FLASH 125.0 MB							
Marvell SATA (01:01:00)	Disk-1 / 372.61 GB	Disk-2 / 372.61 GB	Disk-3 / 372.61 GB	Disk-4 / 372.61 GB	Disk-5 / 372.61 GB	Disk-6 / 372.61 GB	Disk-8 / 372.61 GB	Disk-7 / 372.61 GB
Adaptec SCSI (02:03:01)	UDO1	UDO1	UDO1	Midrange-0				
Adaptec SCSI (02:03:00)								

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:



SATA Disk-3 sdc

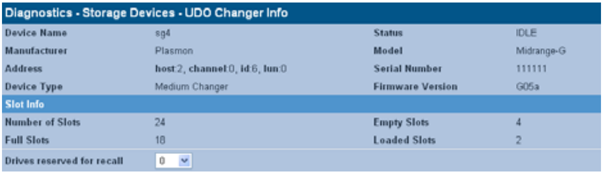
Name	sdc
Vendor	Hitachi
Model	HDS724040KLSA80
Type	SATA
Channel	4:0:0:0
RAID Member	Yes

Reserving UDO drives for recall

The Appliance can reserve one or more of its UDO drives for recall operations, ensuring that a drive is available as quickly as possible when a user requests an archived file.

1. From the **Diagnostics - Storage Devices** page, click on the Appliance (or attached Library) icon:

2. The UDO Changer Info page is displayed:



Diagnostics - Storage Devices - UDO Changer Info

Device Name	sg4	**Status**	IDLE
Manufacturer	Plasmon	**Model**	Midrange-G
Address	host:2, channel:0, id:6, lun:0	**Serial Number**	111111
Device Type	Medium Changer	**Firmware Version**	G05a
Slot Info			
Number of Slots	24	**Empty Slots**	4
Full Slots	18	**Loaded Slots**	2
Drives reserved for recall	0		

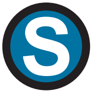
3. Use the **Drives reserved for recall** drop-down box to set aside a suitable number of UDO drives for recall operations. Take the Appliance's average workload into consideration.

4. Click **save**.

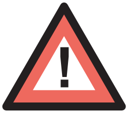
Disk status icons

Table 6-1 describes the disk status icons and their meaning.

- Disks which are marked with:

  are system disks. This means they are used to store the system partition, which contains the configuration files of the Appliance. They can still be used as part of any RAID(s)
- Disks which are marked with:

  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:

  SPARE

  have 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:

  REJECT

  have 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 6-1: Disk status icons

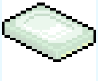
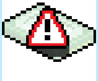
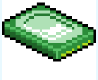
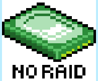
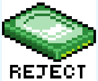
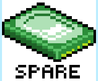
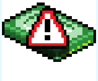
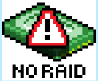
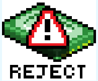
Icon	Meaning
	The disk is online and unformatted
	The disk is online, unformatted and the system has detected the disk is about to fail
	The disk is online
	The disk is online and the disk is not part of a RAID
	The disk is online and has been rejected by the system
	The disk is online and has been marked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

Table 6-1: Disk status icons

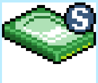
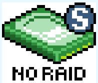
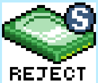
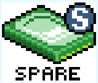
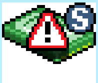
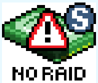
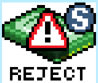
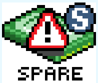
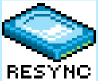
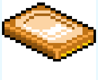
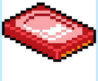
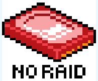
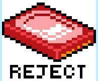
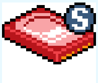
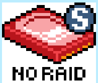
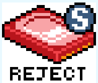
Icon	Meaning
	The disk is online and is a system disk
	The disk is online, is a system disk and is not part of a RAID
	The disk is online, is a system disk and has been rejected by the system
	The disk is online, is a system disk and has been marked as a spare disk
	The disk is online, is a system disk 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
	The disk is resynchronising
	The disk is offline or is physically missing from the Appliance

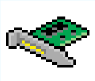
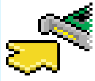
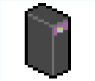
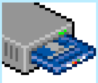
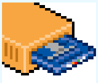
Table 6-1: Disk status icons

Icon	Meaning
	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

Other status icons

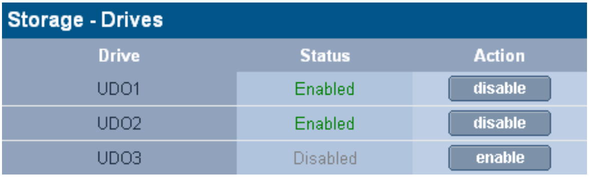
Table 6-1 describes the other status icons and their meaning.

Table 6-2:

Icon	Meaning
	This icon represents an internal controller card
	This icon represents an external controller card, i.e. the interface to an external device attached to the Appliance
	This icon represents the Appliance's UDO library
	This icon represents an online UDO drive
	This icon represents an offline or faulty UDO drive

UDO Drives

The **Diagnostics - UDO Drives** page is used to enable or disable the library's UDO drives and monitor their status.



Storage - Drives

Drive	Status	Action
UDO1	Enabled	disable
UDO2	Enabled	disable
UDO3	Disabled	enable

Drive status can be:

- **enabled** - The drive has been enabled
- **disabled** - The drive has been disabled
- **error** - The drive has an error and has been taken offline by the system
- **enabled-dirty** - The drive has been enabled, but the drive requires cleaning
- **disabled-dirty** - The drive has been disabled, but the drive requires cleaning
- **error-dirty** - The drive has an error and has been taken offline by the system, but the drive requires cleaning.

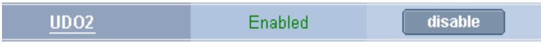
Enabling or disabling a UDO drive

To enable or disable a UDO drive:

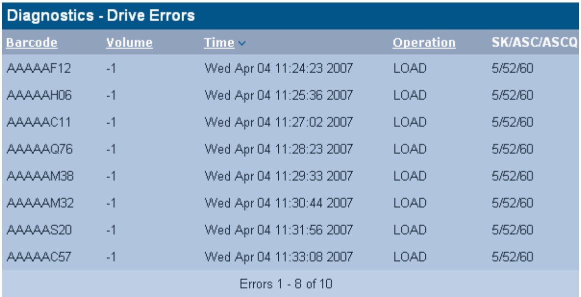
1. From the menu bar, select **Diagnostics - UDO Drives**.
2. Click enable or disable, as appropriate.

Drive Errors

If a UDO drive has errors associated with it, the **Drive** name in the **Diagnostics - UDO Drives** page becomes a hyperlink to the **Diagnostics - Drive Errors** page for that drive.



The **Diagnostics - Drive Errors** page displays:



Diagnostics - Drive Errors

Barcode	Volume	Time	Operation	SK/ASC/ASCQ
AAAAAF12	-1	Wed Apr 04 11:24:23 2007	LOAD	5/52/60
AAAAAH06	-1	Wed Apr 04 11:25:36 2007	LOAD	5/52/60
AAAAAC11	-1	Wed Apr 04 11:27:02 2007	LOAD	5/52/60
AAAAAQ76	-1	Wed Apr 04 11:28:23 2007	LOAD	5/52/60
AAAAAM38	-1	Wed Apr 04 11:29:33 2007	LOAD	5/52/60
AAAAAM32	-1	Wed Apr 04 11:30:44 2007	LOAD	5/52/60
AAAAAS20	-1	Wed Apr 04 11:31:56 2007	LOAD	5/52/60
AAAAAC57	-1	Wed Apr 04 11:33:08 2007	LOAD	5/52/60

Errors 1 - 8 of 10

- **Barcode** - The barcode of the media which was in the drive at the time of the error
- **Volume** - The volume the media is a member of
- **Time** - The time the error occurred
- **Operation** - The operation the media/drive was involved in at the time of the error
- **SK/ASC/ASCQ** - These SCSI error codes allow service engineers to diagnose the precise cause of the error:
    - **SK** - Sense Key
    - **ASC** - Additional Sense Code
    - **ASCQ** - Additional Sense Code Qualifier.

Self Test

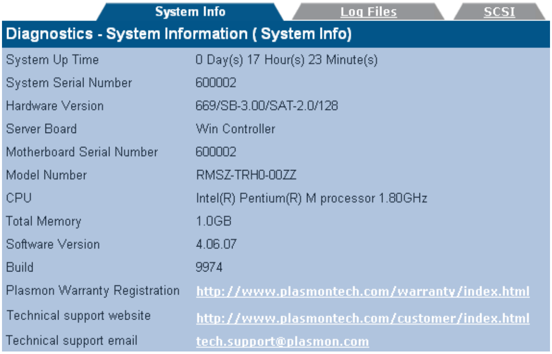
The Diagnostics - Self Test page allows the performance of either:

- **Self Test** - The self test displays the time of the last self test. Clicking **start** will check:
    - **Cache** - The status of the RAID, including SATA (disk) drives. Normally, the system will perform a resynchronisation to fix any problems with the cache. However, if the problem persists, contact Plasmon Technical Support for further assistance
    - **Devices** - The status of the devices attached to the SCSI bus (i.e. UDO library and UDO drives). If any of the devices are faulty, contact Technical Support for further assistance
    - **Notification** - Validates the notification system by pinging the email/SNMP address(es) listed for notification. If this fails, a valid email/SNMP address was not found. Check the System - Notification page to confirm the validity of the email/SNMP address(es)
    - **Services** - The status of the processes, including Services, running on the system. If any services fail, initially check the System - Services page is correctly configured. If this is correct, then contact Technical Support for further assistance.
- **Archive Test** - which creates a small test file, migrates it to media, releases the file from the cache and then recalls the file to check the archive system from end-to-end.

System Information

The **Diagnostics - System Information** page shows the following information:

System Info



Diagnostics - System Information (System Info)

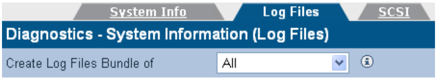
System Up Time	0 Day(s) 17 Hour(s) 23 Minute(s)
System Serial Number	600002
Hardware Version	669/SB-3.00/SAT-2.0/128
Server Board	Win Controller
Motherboard Serial Number	600002
Model Number	RMSZ-TRH0-00ZZ
CPU	Intel(R) Pentium(R) M processor 1.80GHz
Total Memory	1.0GB
Software Version	4.06.07
Build	9974
Plasmon Warranty Registration	http://www.plasmontech.com/warranty/index.html
Technical support website	http://www.plasmontech.com/customer/index.html
Technical support email	tech.support@plasmon.com

The **Diagnostics - System Information (System Info)** page lists:

- **System Up Time** - since last reboot
- **System Serial Number** - The Appliance's serial number
- **Hardware Version** - The current hardware version
- **Server Board** - Server board information
- **Motherboard Serial Number** - The Appliance's motherboard serial number
- **Model Number** - The model number details the product configuration of the Appliance, describing information such as the enclosure type, the memory capacity and many others
- **CPU** - Processor information
- **Total Memory** - The amount of memory (RAM) on the system
- **Software Version** - The currently installed software version
- **Build** - The currently installed software version's build number

- **Plasmon Warranty Registration** - Hyperlink to the Plasmon warranty registration web page (requires an external internet connection)
- **Technical Support Website** - Hyperlink to the Plasmon technical support web page (requires an external internet connection)
- **Technical Support Email** - Plasmon Technical Support email address.

Log Files



Diagnostics - System Information (Log Files)

Create Log Files Bundle of: All

The **Diagnostics - System Information (Log Files)** page enables creation of log file bundles:

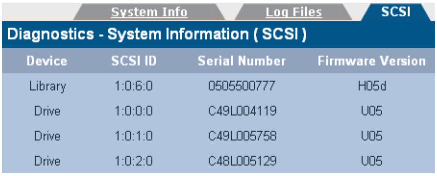
- **Create Log Files Bundle of** - Log file bundles are used by Technical Support to perform diagnostics on the Appliance. Specify a time period, using the drop down list, to create a log file bundle of as follows:
  - **Today**
  - **Last 7 days**
  - **All**
  - **All and config.** - This option produces an **All** type log file bundle with the addition of a text file listing the current system configuration settings. The file can be found in the **\tmp** directory and is named **show_config**.
  - **From custom date**
  - **UDO Logs -** This option produces a log of the Media Library and UDO Drive(s) activity and status.

The log bundle can be downloaded to the local PC and then emailed to Plasmon Technical support.

Note: Creating a log bundle requires the SSM service to be stopped.

Note: The Appliance does not store previous log bundles.

SCSI



Diagnostics - System Information (SCSI)

Device	SCSI ID	Serial Number	Firmware Version
Library	1:0:6:0	0505500777	H05d
Drive	1:0:0:0	C49L004119	U05
Drive	1:0:1:0	C49L005758	U05
Drive	1:0:2:0	C48L005129	U05

The **Diagnostics - System Information (SCSI)** page lists the **Devices** on the SCSI bus (i.e. UDO Drives and Libraries), their **SCSI ID** (in the format Host, Bus, ID and LUN e.g. 1:0:2:0) **Serial Number** and currently installed **Firmware Version**.

Chapter 7

Data Protection menu

Data Protection

> *Note: Data protection in this context refers to the protection of Archive Appliance system and configuration data. It does not refer to the protection of user data files.*

Backup

Scheduling automatic backups

To configure the time at which regular backups are performed:

1. Enter the required time in 24hr clock format (i.e. 13:00 for 1pm).
2. Click save.

> *Note: All Archive Appliances are configured to perform a backup at 02:01 local time by default.*

Monitor the backups

1. From the menu bar, select **Data Protection - Backup**.
2. The following information is displayed:
   - **Backup Job** - The status of any currently active backup job
   - **Last Failed/Last Successful Backup** - the time the last failed or successful (as applicable) backup started and finished
   - **Backup Media** - The amount of backup media in the system.

Perform a backup

1. From the menu bar, select **Data Protection - Backup**.
2. Click start. The following information is displayed:
   - **Backup Job** - The status of the active backup job
   - **Last Failed/Last Successful Backup** - the time the last failed or successful (as applicable) backup started and finished

  - **Backup Media** - The amount of spare backup media in the system.

Recovery

The **Data Protection - Recovery** page allows various parts of the system configuration to be recovered.

> *Warning: Recovery should only be started under the advice of Plasmon Technical Support.*

On a clean system with no archives, the Appliance offers the following options:

- **Full system from backup.**
- **Full system from media.**

If the system already has archives, the Appliance offers these options:

- **Full system from backup**
- **Single Archive FSC (File System Catalog) only**
- **Single Archive FS (File System) only**
- **RMDB (Resource Manager Database) only.**

In general, use the single archive options first if the problem is local to a specific archive. This will be quicker than a full recovery.

The different recovery processes are described in detail below.

Full system from backup

> *Warning: This option will delete UNMIGRATED data and leave all files in the offline state. Check for unmigrated data in the Storage - Volumes page for each archive - see .Viewing and editing volume properties on page 68*

This option recovers the entire system (file systems and system databases/settings) from a backup.

> *Important: Don't use this option if it is known or suspected that the problem is with one particular archive or the RMDB.*

The steps that the system performs are:

- Restore databases and system settings from the backup

- Resync the FSC database to reflect changes on media since the backup was made
- Delete existing file systems then rebuild them using the resynchronised FSC. Note: this deletes unmigrated data and leaves all files on each file system in the offline state.

Full system from media

Warning: Depending on the quantity of data written to the system, a full system recovery from media may take many hours to complete, this recovery method should only be used when all other recovery options have been exhausted.

This option recovers the migrated system data from media. The Appliance will prompt at the start of the recovery process for the insertion of any offline media.

As every disk in the system (including offline disks) are scanned separately, a recovery from media can take an extended period of time to complete.

Note: This recovery option renames the archives found on media to "Archive1", "Archive2", etc. and these names cannot be changed. Recovered shares can be renamed.

In addition, following a recovery from media it is neccessary to reconfigure the list of local users on the Appliance. (see *page 40*).

To ensure users access rights are applied correctly to the recovered files, it is essential that the users are configured with the same User ID (UID) numbers as were configured prior to recovery.

The time, date and base network settings will also require configuration following a complete system recovery.

Single Archive FSC only

Recover a single archive's File System Catalogue (FSC) only, without affecting the archive's file system. To achieve this, the Appliance performs the following steps:

- Restore archive's FSC from backup
- Resync the archive's FSC database to reflect changes on media since the backup was made

Important: Only use this if certain that a particular archive's FSC is corrupt but it's file system is intact. Contact Plasmon Technical Support for further information on how to check an archive's FSC.

Single Archive FS only

Recover a single archive's File System (FS) only

Warning: This option will remove unmigrated data from the archive selected and leave all files in the offline state.

Important: Only use this if an Archive's file system is corrupt, but it's FSC is intact. Contact Plasmon Technical Support for further information on how to check an archive's FSC.

RMDB only

Recover only the Resource Manager Database (RMDB)

Important: Only use this if it is known that the RMDB alone is corrupt. Contact Plasmon Technical Support for further information on how to check the RMDB.

Replication

The **Data Protection - Replication** page enables configuration of replication services between two Appliances, via TCP/IP.

Before beginning, ensure that available volumes are present on both the source and target Appliances. Plasmon reccommends that the source and target volumes are the same size.

For information on creating volumes, see *Creating an archive* on page 59.

Ensure that the target Appliance has a user with Replication rights. See *Adding a User* on page 40.

Note: The Access Control List of a file is not copied during replication.

Note: Files that are moved or deleted on the source volume after replication has taken place are not subsequently moved on or deleted from the target volume.

Important: The maximum supported file size for replication is 2GB.

Configuring Replication

Replication is unidirectional, from the source volume to the target volume. An Appliance may have multiple source and / or target volumes, each volume being one half of a replication pair.

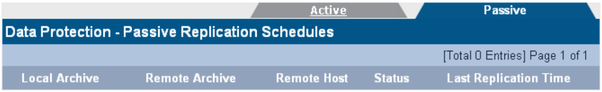
> *Important: It is necessary to configure the replication target (Passive) volume before attempting to configure the source (Active) volume.*

All replication work is controlled by replication schedules. A schedule may be Active or Passive. The Active schedule connects with and transmits data across to the Passive (target) volume. A Passive schedule validates incoming Active connections and routes the data to the correct volume.

The Active schedule resides on the Appliance that holds the source volume, and the Passive schedule resides on the Appliance containing the target volume.

Creating the Passive schedule

1. On the target Appliance, open the **Data Protection - Replication** page and click on the **Passive** tab:

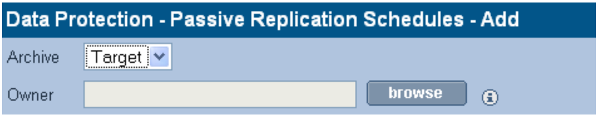


Data Protection - Passive Replication Schedules

[Total 0 Entries] Page 1 of 1

Local Archive	Remote Archive	Remote Host	Status	Last Replication Time

2. Click **add** to open the **Data Protection - Replication Targets - Add** page:

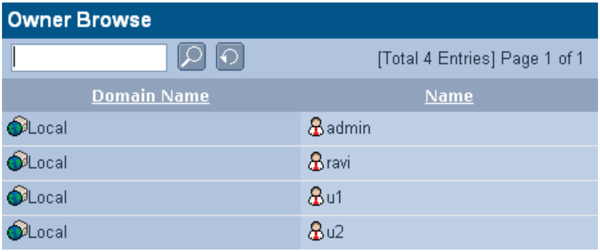


Data Protection - Passive Replication Schedules - Add

Archive: Target

Owner:

3. Select the target volume from the drop-down list and click **browse**:

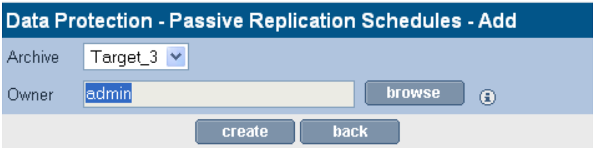


Owner Browse

[Total 4 Entries] Page 1 of 1

Domain Name	Name
Local	admin
Local	ravi
Local	u1
Local	u2

4. Click the user that is to be the owner of this replication volume.



Data Protection - Passive Replication Schedules - Add

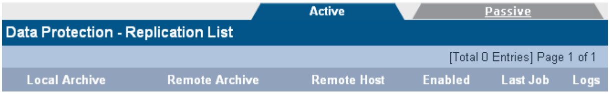
Archive	Target_3
Owner	admin

5. Click **create**.
6. A warning may be displayed that the volume contains data. Click **create** again to confirm only if absolutely certain that the volume is available for use, as any existing data may be overwritten.
7. A link to the **System - Services** page is displayed. Follow it to **start** the Replication service if it is currently stopped.

Note: All shares on a Passive Archive are read-only.

Creating the Active schedule

1. On the source Appliance, open the **Data Protection - Replication** page. The **Active** tab is displayed by default.

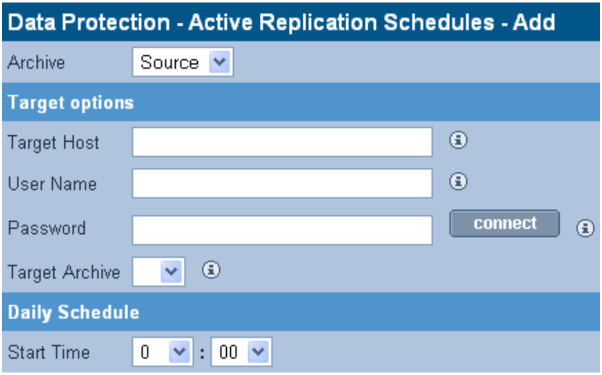


Data Protection - Replication List

[Total 0 Entries] Page 1 of 1

Local Archive	Remote Archive	Remote Host	Enabled	Last Job	Logs

2. Click **add**. The **Data Replication - Sources Add** page is displayed:



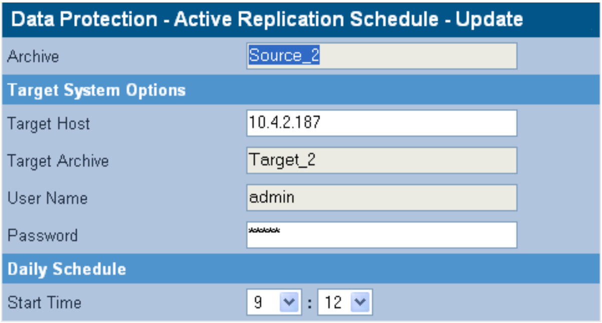
Data Protection - Active Replication Schedules - Add

Archive	Source
Target Host	
User Name	
Password	
Target Archive	
Start Time	0 : 00

3. Select the source volume from the **Archive** drop-down box.
4. Enter the IP address or the Hostname of the target Appliance in the **Target Host** field.
5. Enter the user name and password for the replication selected in Step 4 on *page 106*.
6. Click **connect**.
7. Select the **Target Archive** from the drop-down box.
8. Set a **Start Time** using the drop-down boxes.
9. Click **add**.
10. Go to the **System - Services** page and **enable** the Replication service.

Editing Replication Details

1. On the source Appliance, open the **Data Protection - Replication** page.
2. Click on the the Active Replication schedule to be edited:



Data Protection - Active Replication Schedule - Update

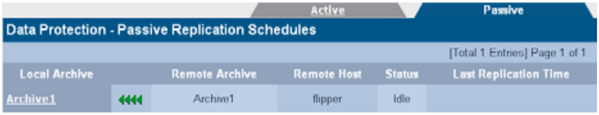
Archive	Source_2
Target System Options	
Target Host	10.4.2.187
Target Archive	Target_2
User Name	admin
Password	*******
Daily Schedule	
Start Time	9 : 12

3. Edit details as required (Target Archive and User Name cannot be changed).
4. Click **save**.

Changing the Passive Replication Schedule Owner

> *Note: Changing the Passive Replication schedule owner involves deleting and reconfiguring both the Active and Passive replication schedules, specifying a new owner and changing the ACL's of all the previously replicated files on the target Archive. This can generate a significant amount of file metadata on certain systems containing large numbers of files. Ensure that it is absolutely necessary to change the owner before proceeding.*

1. On the target Appliance, open the **Data Protection - Replication** page.
2. Click on the Passive tab and select the Passive Replication Schedule to be changed by clicking on the name of the target archive:

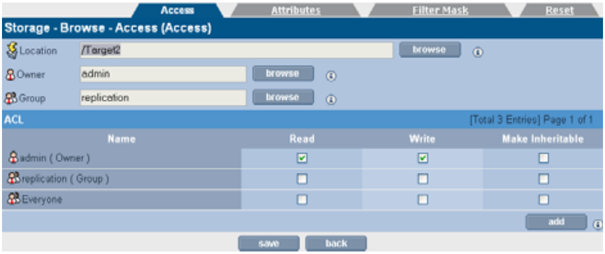


Data Protection - Passive Replication Schedules

[Total 1 Entries] Page 1 of 1

Local Archive		Remote Archive	Remote Host	Status	Last Replication Time
Archive1	◀◀◀◀	Archive1	flipper	Idle	

3. Click **Delete**. At the system's request, click **Delete** a second time to confirm deletion of the Passive Replication Schedule.
4. Recreate the Passive replication schedule as described on *page 105* specifying the new user to be assigned as the Schedule owner.
5. Open the **Storage** - **Browse** page and click the name of the replication target archive.
6. Click **Access**.



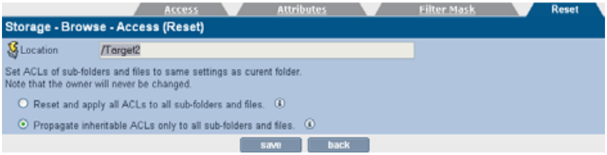
Storage - Browse - Access (Access)

Location	/Target2	browse
Owner	admin	browse
Group	replication	browse

ACL [Total 3 Entries] Page 1 of 1

Name	Read	Write	Make Inheritable
admin (Owner)	☑	☑	☐
replication (Group)	☐	☐	☐
Everyone	☐	☐	☐

7. Click Add and select the user that has been assigned as the new Replication Schedule Owner.
8. Ensure that the user has **Read** and **Write** Access allowed.
9. Ensure that the **Make Inheritable** box is checked for all the users on the ACL, including the root user and group.
10. Click the **Reset** tab.



Storage - Browse - Access (Reset)

Location /Target2

Set ACLs of sub-folders and files to same settings as curent folder.
Note that the owner will never be changed.

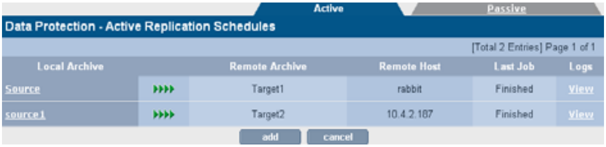
○ Reset and apply all ACLs to all sub-folders and files.

● Propagate inheritable ACLs only to all sub-folders and files.

11. Select the **Propagate inheritable ACLs only to all sub-folders and files** radio button and click **Save**. At the prompt, click **Save** a second time to confirm the ACL change for all directories and files in the volume.

Note: This action can generate a significant amount of file metadata on certain systems containing large numbers of files.

12. On the source Appliance, open the **Data Protection - Replication** page.



Data Protection - Active Replication Schedules

[Total 2 Entries] Page 1 of 1

Local Archive		Remote Archive	Remote Host	Last Job	Logs
Source	▸▸▸▸	Target1	rabbit	Finished	View
source1	▸▸▸▸	Target2	10.4.2.187	Finished	View

13. Select the Active Replication Schedule that corresponds to the Passive Replication Schedule changed above by clicking on the name of the source archive.
14. Click **delete**. At the system’s request, click **Delete** a second time to confirm deletion of the Active Replication Schedule.
15. Recreate the Active Replication Schedule as described on *page 107*. Ensure that the newly configured Passive Schedule owner is entered in the **User** field.

Deleting an Active Replication Schedule

1. On the source Appliance, open the **Data Protection - Replication** page.
2. Click on the name of the **Local Archive** to be edited.
3. Click **delete**. A message is displayed warning that the schedule is about to be deleted.
4. Click **delete** again to confirm deletion.

Deleting a Passive Replication Schedule

1. On the target Appliance, open the **Data Protection - Replication** page.
2. Select the **Passive** tab.
3. Click on the name of the replication schedule to be edited.
4. Click **delete**. A message is displayed warning that the schedule is about to be deleted.
5. Click **delete** again to confirm deletion.

Note: Deleting a replication schedule does not delete the archive. For further information on deleting archives, see Removing a Volume on page 72.

Note: If a passive replication schedule is accidentally deleted or requires reconfiguration following a system recovery, see The log is displayed in plain text that can be copied and pasted for support purposes. on page 113.

Recovering the passive replication schedule

In the event that the passive replication schedule is accidentally deleted or requires reconfiguration following a system recovery, it is essential that the user with the same user ID (UID) as was previously configured is set as the replication schedule owner.

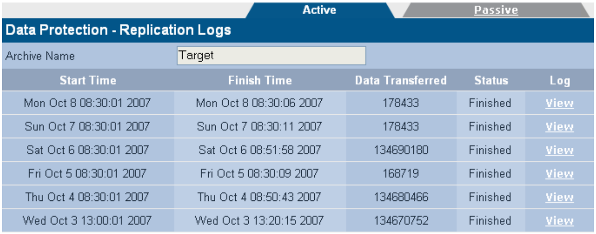
If a different user is to be specified as the Passive Replication Schedule owner, follow the procedure for changing the owner described on *page 109*.

Viewing Replication logs

All active replication schedules automatically log their activity. The log can be viewed at any time.

1. On the source Appliance, open the **Data Protection - Replication** page.
2. In the **Logs** column of the schedule to be examined, click **View.**

   The **Data Protection - Replication Logs** page is displayed, showing the history of the replication schedule:



Data Protection - Replication Logs

Archive Name: Target

Start Time	Finish Time	Data Transferred	Status	Log
Mon Oct 8 08:30:01 2007	Mon Oct 8 08:30:06 2007	178433	Finished	View
Sun Oct 7 08:30:01 2007	Sun Oct 7 08:30:11 2007	178433	Finished	View
Sat Oct 6 08:30:01 2007	Sat Oct 6 08:51:58 2007	134690180	Finished	View
Fri Oct 5 08:30:01 2007	Fri Oct 5 08:30:09 2007	168719	Finished	View
Thu Oct 4 08:30:01 2007	Thu Oct 4 08:50:43 2007	134680466	Finished	View
Wed Oct 3 13:00:01 2007	Wed Oct 3 13:20:15 2007	134670752	Finished	View

Data Transferred is in bytes.

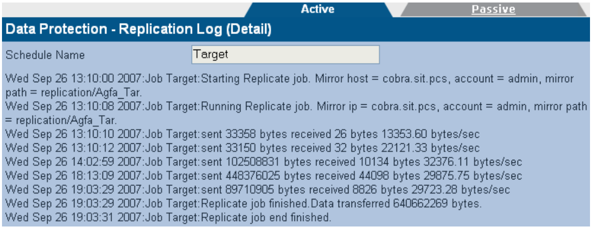
Start Time indicates the time the replication began.

Finish Time indicates the time the replication ended.

Status indicates the overall status of each replication attempt. This will be one of:

- **Running** - A replication is currently in progress.
- **Failed** - The last replication failed (e.g. Network communication with the replication target is lost).
- **Finished** - The last replication completed successfully.
- **Not Run** - The last replication did not run.
- **Unknown** - The status of the last replication is not known.

3. To view an in-depth log for a specific date, click **View**.



Data Protection - Replication Log (Detail)

Schedule Name: Target

```
Wed Sep 26 13:10:00 2007:Job Target:Starting Replicate job. Mirror host = cobra.sit.pcs, account = admin, mirror
path = replication/Agfa_Tar.
Wed Sep 26 13:10:08 2007:Job Target:Running Replicate job. Mirror ip = cobra.sit.pcs, account = admin, mirror path
= replication/Agfa_Tar.
Wed Sep 26 13:10:10 2007:Job Target:sent 33358 bytes received 26 bytes 13353.60 bytes/sec
Wed Sep 26 13:10:12 2007:Job Target:sent 33150 bytes received 32 bytes 22121.33 bytes/sec
Wed Sep 26 14:02:59 2007:Job Target:sent 102508831 bytes received 10134 bytes 32376.11 bytes/sec
Wed Sep 26 18:13:09 2007:Job Target:sent 448376025 bytes received 44098 bytes 29875.75 bytes/sec
Wed Sep 26 19:03:29 2007:Job Target:sent 89710905 bytes received 8826 bytes 29723.28 bytes/sec
Wed Sep 26 19:03:29 2007:Job Target:Replicate job finished.Data transferred 640662269 bytes.
Wed Sep 26 19:03:31 2007:Job Target:Replicate job end finished.
```

The log is displayed in plain text that can be copied and pasted for support purposes.

Chapter 8
Shutdown

Shutdown the Appliance using the Web Interface

Shutdown

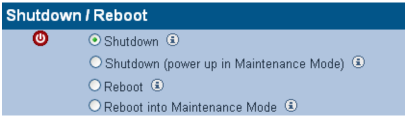
The **Shutdown/Reboot** page allows:

- **Shutdown**
- **Shutdown (power up in Maintenance Mode)** - Used to power down the Appliance, perform hardware maintenance and power the system back up in Maintenance Mode. This is normally only used by Service personnel.
- **Reboot**
- **Reboot into Maintenance Mode** - Reboots directly into Maintenance Mode.

Note: Before using any of these options, be sure to inform any connected users that they will be disconnected, and services will be lost for the duration of the shutdown/reboot.

To shutdown or reboot the Appliance from the Web interface:

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



Shutdown / Reboot

● Shutdown

○ Shutdown (power up in Maintenance Mode)

○ Reboot

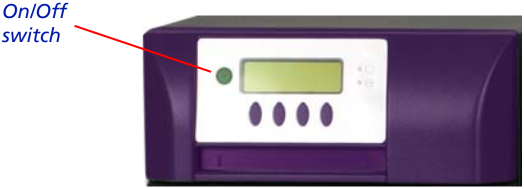
○ Reboot into Maintenance Mode

2. Select the appropriate radio button.
3. Click ok, then click ok again to confirm.

Shutdown the Appliance using the library power switch

AA16, AA32, AA80 and AA174 models only

To shut down an Appliance using the power switch, press the On/Off switch on the library front panel:



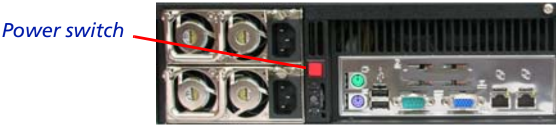
Press the power button and confirm shut down via the keypad.

> *Caution: Holding the power button for more than four seconds initiates a non-graceful shutdown. This should be avoided.*

AA238, AA438 and AA638 models only

To shut down the Appliance:

1. Initiate shutdown using the Web interface.
2. Once complete, press the power switch on the rear of the RAID Cache Unit.



3. Power off the library

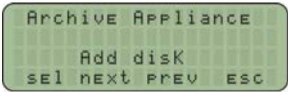
Chapter 9

Using the Keypad interface

Configuration

Setting the IP address

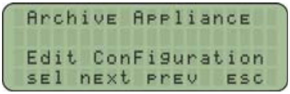
1. With the Appliance switched on and connected to the host LAN / Network, press any key to display the first item in the top-level menu on the LCD panel:



```
 Archive Appliance

    Add disK
 sEl nExt PrEV  Esc
```

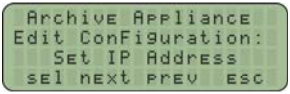
If already in a submenu, press **esc** a number of times until the Add disK menu is displayed.

2. Press **next** twice to display the Edit ConFiguration menu.



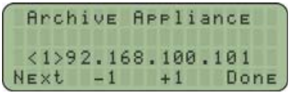
```
 Archive Appliance

 Edit ConFiguration
 sEl nExt PrEV  Esc
```

3. Press **sel** to enter the submenus; the first sub-menu is for setting the IP address:



```
 Archive Appliance
Edit ConFiguration:
   Set IP Address
 sEl nExt PrEV  Esc
```

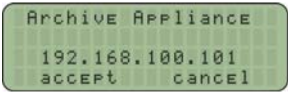
4. Press **sel** to display the IP address. Initially, the current IP address is displayed (in standard dotted-decimal format), with the first digit selected, ready for editing:



```
 Archive Appliance

 <1>92.168.100.101
Next  -1   +1   Done
```

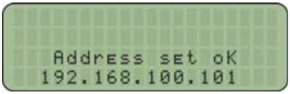
5. Press **-1** and **+1** to change the value inside the brackets (the first digit in any group of three can only be set to 0, 1 or 2).
6. Press **next** to highlight the next digit:
7. Press **-1** and **+1** to change the value inside the brackets (the maximum value for each 3-digit group is 255).
8. Cycle through fields by pressing next and ensure all twelve digits are filled in correctly.

9. Press **done**. The LCD panel shows the newly configured IP address. For example:



```
 Archive Appliance

  192.168.100.101
  accept     cancel
```

10. Press **accept**. The display shows:



```


   Address set oK
  192.168.100.101
```

11. The display returns to the Set IP Address submenu.

Setting the netmask

To edit the netmask, follow the method in *Setting the IP address* on page 120. In step *3*, make sure the Set NetmasK submenu is selected.

Setting the gateway IP address

The gateway IP address allows the Appliance to connect to nodes beyond the local subnet.

To edit the gateway IP address, follow the method in *Setting the IP address* on page 120. In step *3*, select the Set Gateway submenu. The remaining system configuration can be performed via the web interface.

Adding UDO media

UDO media may be added to the Appliance via the Mailslot or via Direct slot access.

- Add new disks (UDO RW only) for backup purposes (can only be added via the mailslot).

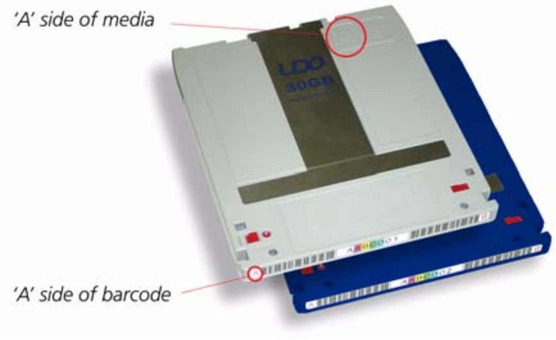
  UDO RW media can be identified by its **Grey** cartridge case.

Caution: It is essential that Backup media is added prior to Data media.

- Add new data disks (UDO WORM or Compliant UDO WORM only) for migration (can be added via the mailslot or direct slot access).

  UDO WORM media can be identified by its **Blue** cartridge case.

Pieces of UDO media must have a unique barcode of the approved format centred on the spine of the disk, ensuring the 'A' side of media and barcode label are oriented as shown below.

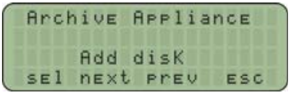


Adding Backup UDO media via the mailslot

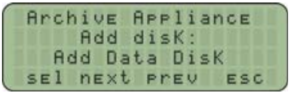
To function correctly, at least one piece of backup UDO media must be added to the system. For disaster recovery, at least two backup UDO media should always be used in the Appliance.

Backup UDO media must always be added, via the mailslot, prior to adding **ANY** data media to the system.

1. Press any key to display the top-level Add disk menu.

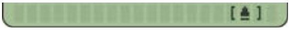


2. Press **sel** to display the first sub-menu (Add Data Disk):



3. Press **next** to display New Backup disk.
4. Press **sel**.
5. Insert the backup UDO media, ‘A’ side facing up, into the Mailslot.

   AA238, AA438 and AA638 models only: Press the eject button, shown below. The library will then take the media and close the mailslot.



6. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see *page 125*).

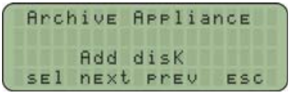
   If all is well, a Disk added OK message is be displayed.
7. Repeat the above steps until all required backup UDO media has been added.

> *Note: At least one piece of backup UDO media **MUST** be added to the system. Plasmon recommend the use of two pieces of backup UDO media.*

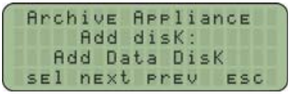
Adding Data UDO media via the mailslot

To add (load) one or more UDO media cartridges via the mailslot:

1. Press any key to display the top-level Add disk menu.



2. Press **sel** to display the first sub-menu (Add Data Disk):



```
Archive Appliance
   Add disk:
 Add Data Disk
sel next prev  esc
```

3. Press **sel**.
4. Insert the media, ‘A’ side facing up, into the Mailslot.

   AA238, AA438 and AA638 models only: Press the eject button, shown below. The library will then take the media and close the mailslot.

```
                [⏏]
```

5. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see *page 125*).

   If all is well, a Disk added OK message is be displayed.
6. Repeat the above steps until all media have been added.

Adding Data UDO media via direct slot access

If a considerable amount of media is to be added to the Appliance, it may be more productive to add media via direct slot access.

AA16/32, AA80 and AA174 models

Removing the library side panel

It is necessary to remove the left hand (when viewed from the front) library side panel.

1. Shut down the Appliance: see *Shutdown the Appliance using the Web Interface* on page 116 or *Shutdown the Appliance using the library power switch* on page 117.
2. Remove the power cord from the supply.
3. Open the library front door.
4. Remove and retain the panel securing screws from the front and rear of the library side panel.
5. Lift the panel up to remove it.

Warning: When adding media via direct slot access, ***do not*** *move or remove any existing media from the Appliance.*

> *Warning: Backup media must **not** be added via direct slot access.*

Adding media

Referring to the slot map appropriate for the Appliance library model, see *page 137*, add media to the lowest numbered available and unassigned slots.

Refitting the library side panel

1. Insert the bottom of the library side panel into the library chassis.
2. Refit the screws to the front and rear of the library panel.
3. Close the library front door.
4. Replace the power cord.
5. Restart the Appliance. The Appliance will rescan the contents of the library and update its inventory.

AA238, AA438 and AA638 models

To return offlined media via direct slot access:

1. Shut down the Appliance.
2. Open the library rear door.
3. Referring to the slot map on *page 143*, add media to the lowest numbered available and unassigned slots.
4. Restart the Appliance. The Appliance will rescan the contents of the library and update its inventory.

Possible problems

Disk errors

If a cartridge is added that is the wrong format, or that does not have a barcode, two things will happen:

- One of the following error messages will be displayed:
  - Not UDO Media
  - Invalid Barcode(s)
  - Barcode not Unique
- The media in question will be ejected.

Remove the cartridge. Another may be inserted.

Other errors

Other error messages are:

- LiBrary Full - The library cannot take any more media. Offline some media or purchase an extension library.
- Media checK Failed - General library hardware error. Contact Plasmon Technical Support.
- Move Failed - Hardware problem with the library picker. Contact Plasmon Technical Support.

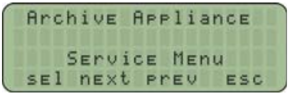
Removing UDO media

If any disks have failed, an administrator will receive an alert via the configured method (see *page 24*) telling them which media needs removing. When this happens, remove UDO media from the Appliance via the Mailslot.

Media can also be removed for Offline Media Management - see *page 129*.

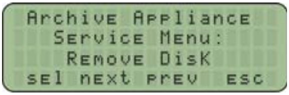
Removing failed UDO media via the mailslot

1. Press any key to display the top-level Add disK menu.
2. Press **next** three times to display Service Menu .



```
Archive Appliance

   Service Menu
sel next prev  esc
```

3. Press **sel** to display the Service Menu sub-menu:



```
Archive Appliance
  Service Menu:
   Remove DisK
sel next prev  esc
```

4. Press **next** or **prev** to display the required option (Failed data disk or Failed backup disk).
5. Press **sel**.

   The library picker will automatically select the first disk to be removed.
6. Remove the cartridge from the Mailslot.

   The Remove DisK submenu will be displayed once more.
7. Repeat the above steps until all failed media are removed.

Cleaning Media

A UDO cleaning kit is available from Plasmon.

To remove dirty media select 'Remove dirty disk' from the 'Service' Menu.

To re-introduce the cleaned media, see*Adding Backup UDO media via the mailslot* on page 122 or *Adding Data UDO media via the mailslot* on page 123.

Chapter 10

Offline Media Management

Storage of offline media

When media is not in the Appliance it can become contaminated due to the ingress of dust particles, and is also susceptible to adverse temperature and relative humidity. It must therefore be stored appropriately to prevent damage or degradation.

Note: The shutter on the media should not be opened manually as this exposes the media to potential contaminants.

In the event that media becomes dirty, media cleaning kits are available from Plasmon.

Plasmon recommends that the media be stored in the plastic sleeve in which it was supplied and in accordance with the following temperature and humidity limits:

Table 1: . UDO operating and storage conditions

Parameter	Value/range
Maximum Temperature Range	5°C to 55 °C/41°F to 131 °F (stable temperature)
Ideal Temperature Range	10°C to 25°C/50°F to 77 °F
Maximum Humidity Range	3% to 90% RH (non-condensing)
Ideal Humidity Range	20% to 80% RH

*Note: Plasmon recommend the use of a media rack, such as those produced by Engineered Data Products (***www.edp-usa.com*** or* **www.edpeurope.com***), for the long term storage of offline media.*

When to offline media

For media to be eligible for OMM:

- The media must be full, of a closed state and in a valid backup,
- The media's retention time must have elapsed.

or

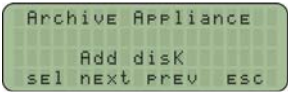
- The media must be in a secondary media pool that is designated as an **Open Offline** media pool - see *Viewing and editing volume properties* on page 68.

The Appliance will determine when either of the above criteria has been met and provide an indication of this in the Web interface.

Offlining media using the Keypad interface

When the Web interface advises that media is eligible for OMM:

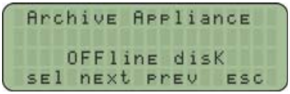
1. Press any key to display the first item in the top-level menu on the LCD panel:



```
Archive Appliance

    Add disk
sel next prev  esc
```

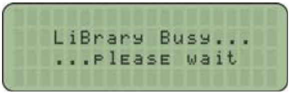
   If already in a submenu, press **esc** (key **4** on the Keypad) a number of times until the Add disk menu is displayed.

2. Press **next** to display the menu.



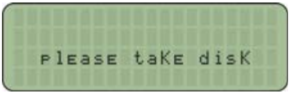
```
Archive Appliance

   OFFline disk
sel next prev  esc
```

3. Press **sel**.
4. Press **next** or **prev** to select which volume to offline the media from, as required, then press **sel**.
5. The library keypad will display:



```
  LiBrary Busy...
  ...please wait
```

6. The media will be ejected from the mailslot and the keypad will display:



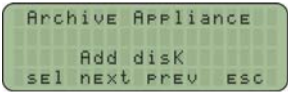
```
please taKe disK
```

Remove the disk and store in accordance with the local OMM procedures.

Offlining open media using the Keypad interface

If the Appliance is configured with a secondary media pool designated as an Open Offline media pool and open media is to be removed from the Appliance for remote storage:

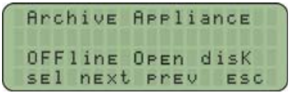
1. Press any key to display the first item in the top-level menu on the LCD panel:



```
Archive Appliance

    Add disK
sel next prev  esc
```

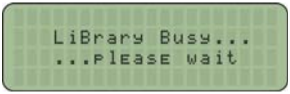
If already in a submenu, press **esc** (key **4** on the Keypad) a number of times until the `Add Disk` menu is displayed.

2. Press **next** three times to display the `Offline OPEN Disk` menu.



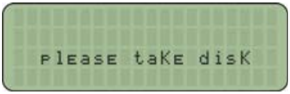
```
Archive Appliance

OFFline Open disK
sel next prev  esc
```

3. Press **sel**.
4. Press **next** or **prev** to select the archive to offline the media from, as required, then press **sel**.
5. The library keypad will display:



```
  LiBrary Busy...
  ...please wait
```

6. The media will be ejected from the mailslot and the keypad will display:



please take disk

Remove the disk and store in accordance with *Storage of offline media* on page 130.

Offline media return requests

Offline media return requests are made via the Web interface or by notifications.

When a request is received, it will detail the barcode of the required piece of media.

> *Note: Requests are only made if both the Primary pool and Secondary pool copies of the requested file are offline.*

Returning offline media

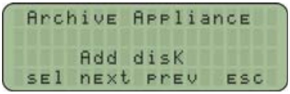
Offline media can be returned to the Appliance in two ways:

- *Via the mailslot* - if a small amount of media is to be returned
- *Via direct slot access* - if a large amount of media is to be returned.

Via the mailslot

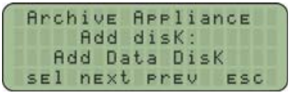
To return one or more offlined media cartridges via the mailslot:

1. Press any key to display the top-level Add disk menu.



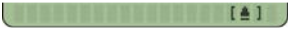
```
 Archive Appliance

     Add disk
sel next prev  esc
```

2. Press **sel** to display the first sub-menu (Add Data Disk):



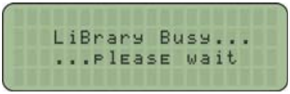
```
 Archive Appliance
     Add disk:
   Add Data Disk
sel next prev  esc
```

3. Press **sel**.
4. Insert the media, ‘A’ side facing up, into the Mailslot.
   AA238, AA438 and AA638 models only: Press the eject button, shown below. The library will then take the media and close the mailslot.



```
                 [⏏]
```

5. The library keypad will display:



```
Library Busy...
...please wait
```

Repeat the above steps until required offline media have been returned.

Via direct slot access

> *Warning: When returning offlined media via direct slot access, **do not** move or remove any existing media from the Appliance, as this will cause the Appliance to mark the media as invalid.*

> *Warning: Returning offlined media which has a duplicate barcode to media currently in the Appliance or an attached Library will cause the Appliance to mark the media as invalid.*

AA16, AA32, AA80 and AA174 models

Removing the library side panel

To return offlined media via direct slot access, it is necessary to remove the left hand (when viewed from the front) library side panel.

1. Using the Web interface, shut down the Appliance.
2. Remove the power cord from the supply.
3. Open the library front door.
4. Remove and retain the panel securing screws from the front and rear of the library side panel.
5. Lift the panel up to remove it.

Returning media

Referring to the slot map appropriate for the Appliance model, see *page 137*, return the offlined media to the lowest numbered available and unassigned slots.

Refitting the library side panel

1. Insert the bottom of the library side panel into the library chassis.
2. Refit the screws to the front and rear of the library panel.
3. Close the library front door.
4. Replace the power cord.
5. Restart the Appliance. The Appliance will rescan the contents of the library and update its inventory.

AA238, AA438 and AA638 models

To return offlined media via direct slot access:

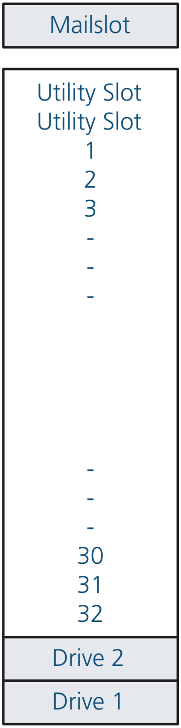
1. Using the Web interface, shut down the Appliance.
2. Open the library rear door.
3. Referring to the slot map on *page 143*, return the offlined media to the lowest numbered available and unassigned slots.
4. Restart the Appliance. The Appliance will rescan the contents of the library and update its inventory.

Library slot maps

The following diagrams show slot assignments and availability and are to be used when returning offlined media via direct slot access.

Warning: Media must not be inserted into the utility slots, as these are used by the Appliance to rotate media.

AA16/32 Appliance



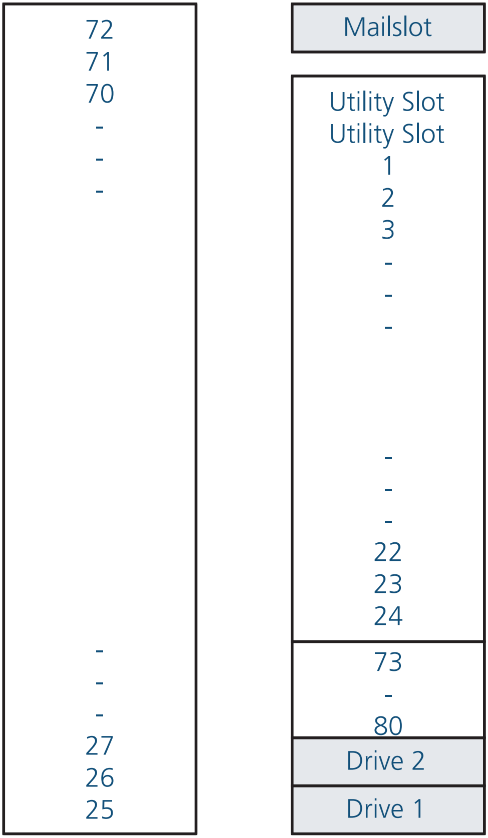
Mailslot

Utility Slot
Utility Slot
1
2
3
-
-
-
-
-
-
30
31
32

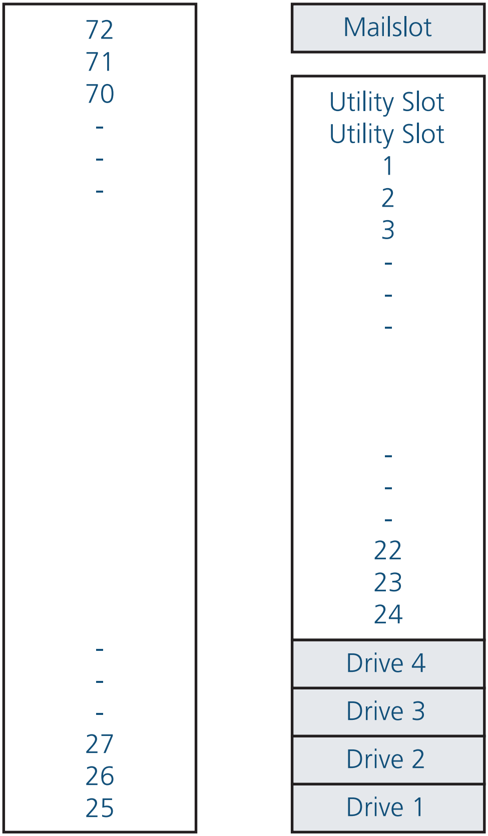
Drive 2

Drive 1

AA80 (2 drive) Appliance



AA80 (4 drive) Appliance



72
71
70
-
-
-
-
-
-
27
26
25

Mailslot

Utility Slot
Utility Slot
1
2
3
-
-
-
-
-
-
22
23
24

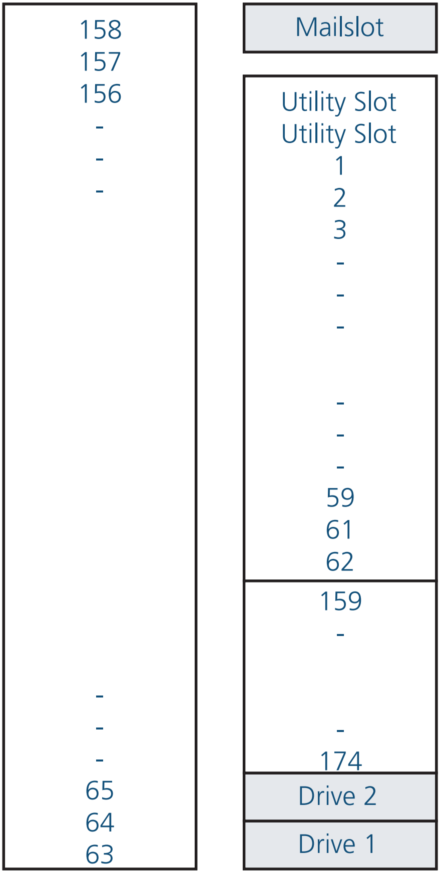
Drive 4

Drive 3

Drive 2

Drive 1

AA174 (2 drive) Appliance



158
157
156
-
-
-

-
-
-
65
64
63

Mailslot

Utility Slot
Utility Slot
1
2
3
-
-
-

-
-
-
59
61
62

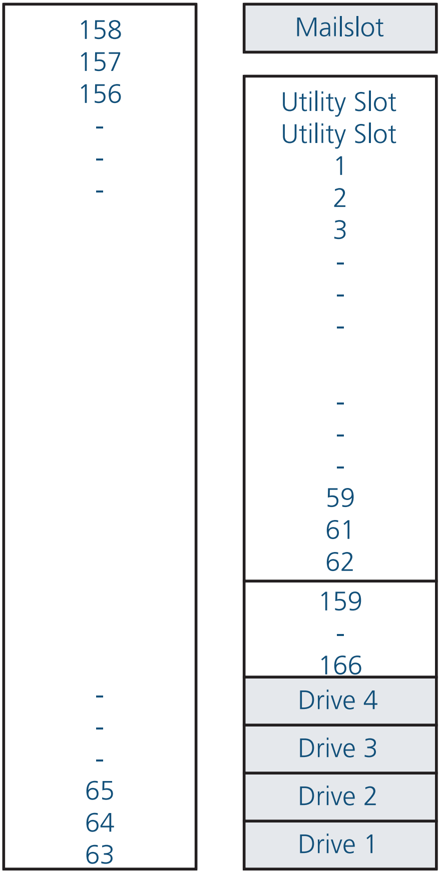
159
-

-
174

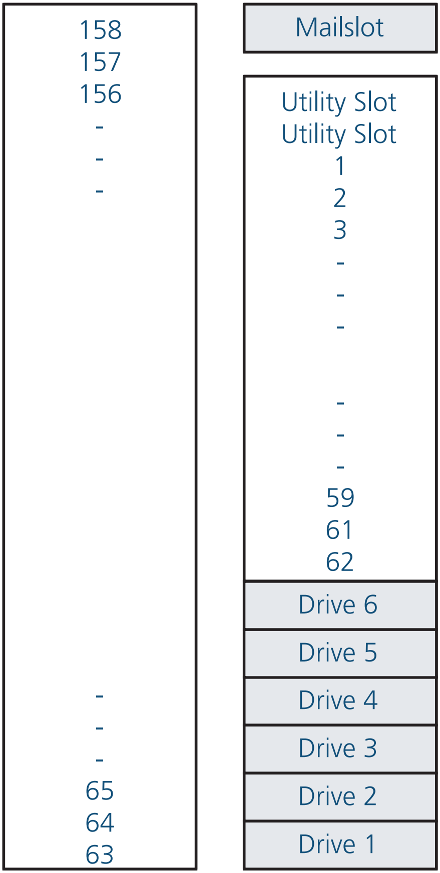
Drive 2

Drive 1

AA174 (4 drive) Appliance



AA174 (6 drive) Appliance



158
157
156
-
-
-

-
-
-
65
64
63

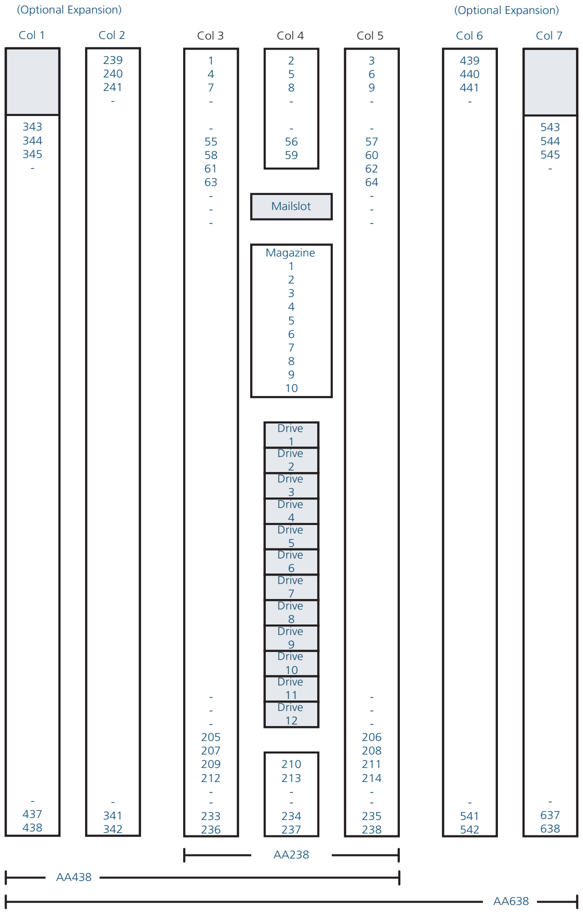
Mailslot

Utility Slot
Utility Slot
1
2
3
-
-
-

-
-
-
59
61
62

Drive 6
Drive 5
Drive 4
Drive 3
Drive 2
Drive 1

AA238, AA438 and AA638 Appliances



Chapter 11

Overflow Library

Overflow Library

An additional overflow library can be purchased and connected to a host Archive Appliance to increase the total number of media slots available, significantly expanding data storage capacity.

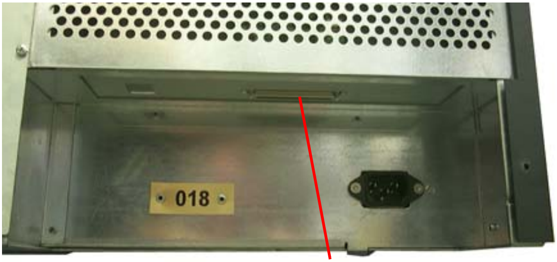
> *Note:* Rewritable backup media cannot be added to the overflow library to provide additional backup storage space for the Archive Appliance. Overflow libraries can only be used to provide increased data storage capacity.

Installing an Overflow library

Plasmon recommend that the Overflow library is situated as close as possible to the host Appliance for convenience of operation.

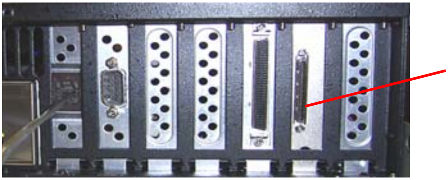
1. Ensure that the host Archive Appliance is properly shut down - see *page 116*.
2. Connect the Overflow library to the host Appliance using the SCSI cable provided:

   AA16 to AA174 models only: SCSI port is located on the lower rear side of the Appliance:



SCSI Port

AA238 to AA638 models only: SCSI port is located on the rear of the Archive Controller:

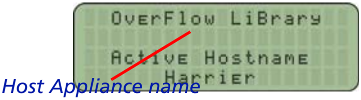


3. Connect the power cord to the overflow library.
4. Power on the Overflow library.

> *Note: It is important to ensure that the Overflow library is fully powered up before powering up the host Appliance. This ensures that the host recognises the Overflow library as a connected device during the initial bus scan.*

5. Power on the Appliance.

By default the overflow library keypad interface displays the IP address and name of the host appliance.



```
OverFlow LiBrary
Active Hostname
Harrier
```

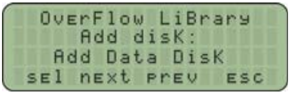
Overflow library keypad interface

The overflow library keypad interface can only be used to add media to the library. All other functions are controlled using the host Appliance keypad interface; refer to the appropriate sections of the Administrator's Guide for:

- Removing failed media - see *page 125*
- Offline Media Management - see *page 129*

Adding UDO media to the overflow library via the mailslot.

1. Press any key on the overflow library keypad to display (Add Data DisK).



```
OverFlow LiBrary
   Add disK:
 Add Data DisK
sEl next prev  esc
```

2. Press **sel**.
3. Insert the media, ‘A’ side facing up, into the Mailslot.

   AA238, AA438 and AA638 models only: Press the eject button, shown below. The library will then take the media and close the mailslot.

4. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see *page 125*).

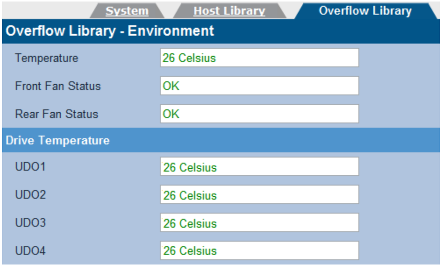
   If all is well, a DisK added OK message is be displayed.
5. Repeat the above steps until all media have been added.

Note: To add media to the overflow library via direct slot access see page 124

Overflow library Web interface

The overflow library can be monitored via the Web interface. information relating to the overflow library are added as additional pages to the following sections of the Web interface:

- System - Environment



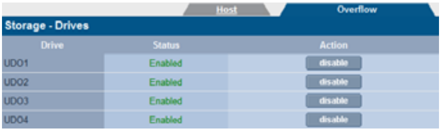
Overflow Library - Environment

Temperature	26 Celsius
Front Fan Status	OK
Rear Fan Status	OK

Drive Temperature

UDO1	26 Celsius
UDO2	26 Celsius
UDO3	26 Celsius
UDO4	26 Celsius

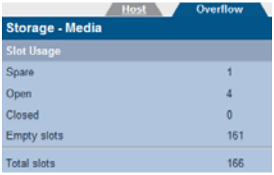
- Storage - Drives



Storage - Drives

Drive	Status	Action
UDO1	Enabled	disable
UDO2	Enabled	disable
UDO3	Enabled	disable
UDO4	Enabled	disable

- Storage - Media



Storage - Media

Slot Usage	
Spare	1
Open	4
Closed	0
Empty slots	161
Total slots	166

Chapter 12

Troubleshooting

Troubleshooting

Table 12-1:Archive Appliance Troubleshooting checklist

The Appliance is not visible on the network, cannot be pinged or the web interface is not responding.

Possible cause	*Suggested action*	*Comments*
The Appliance is still booting.	Wait for boot to complete - approximately six minutes.	
The IP address is invalid.	Use the keypad to check that the IP address is configured correctly.	
Incorrect Ethernet port used (on dual port Appliance).	Test using other Ethernet port.	*eth0* is the port enabled by default.
Faulty Ethernet cable.	Test with a known working Ethernet cable.	
Faulty network Switch / configuration.	Verify the Switch is receiving power, the port is enabled and set to Auto Negotiate. Test the Appliance using another Switch port.	

Table 12-1:Archive Appliance Troubleshooting checklist

System Crash.	Reboot or power-cycle.	If the Web Interface is inaccessible, attempt to reboot via the keypad or serial console. As a last resort press and hold the power button to switch off.
Incorrect Web browser settings.	If a proxy server is being used ensure it is bypassed for local addresses.	
Hardware failure.	Contact Plasmon support.	

The Appliance will not power on (no LED or fan activity).

Possible cause	*Suggested action*	*Comments*
Faulty power cable.	Test with a known working power cable.	
Hardware failure.	Contact Plasmon support.	

The Appliance fails its self-test.

Possible cause	*Suggested action*	*Comments*
A UDO drive is unavailable.	Reboot the Appliance. If this does not resolve the issue contact Plasmon support.	

Table 12-1:Archive Appliance Troubleshooting checklist

Notification ping failure to either SMTP or SNMP server.	Ensure relevant server is available. Check Notification configuration.	
One or more key services are not running.	Check running services and enable any which have stopped. If a service fails to start, reboot the Appliance.	
Hardware failure.	Contact Plasmon support.	
Data is not migrating to media.		
Possible cause	*Suggested action*	*Comments*
Library media full.	Offline closed media and add blank spares.	
SSM Service not started.	Open the **System - Services** page and start SSM. If this fails reboot the Appliance, then attempt to start SSM. If this also fails contact Plasmon support.	

Table 12-1:Archive Appliance Troubleshooting checklist

SSM fault.	Go to the **Diagnostics - Self test** page and run the Archive Test. If this fails, reboot the Appliance, then retest. Contact Plasmon support if problem is not resolved.	
Dirty media.	Clean the media using a Plasmon UDO media cleaning kit and retry.	
Hardware failure.	Contact Plasmon support.	
Data cannot be recalled from media.		
Possible cause	*Suggested action*	*Comments*
A migration job is using all UDO drives.	Wait for the migration job to complete. Select the **Diagnostics - System Jobs** page to view the status of current jobs. Reserve at least one UDO drive for recall operations.	Recalls take priority over migration, but any migrations for the loaded disk must be completed before the media can be ejected to load a different media for recall.

Table 12-1:Archive Appliance Troubleshooting checklist

Required media is offline.	View the **System - Status** page to determine which media to load. Refer to the **Storage - Media Requests** page to see other outstanding media requests.	
SSM service not started.	Go to the **System - Services** page and start SSM. If this fails reboot the Appliance then attempt to start SSM. Contact Plasmon support if problem is not resolved.	
SSM fault.	Reboot the Appliance. Contact Plasmon support if the problem is not resolved.	
Dirty media.	Clean the media using a Plasmon UDO media cleaning kit and retry.	Refer to the Operator’s Guide for media storage and care information.
Hardware failure.	Contact Plasmon support.	

Table 12-1:Archive Appliance Troubleshooting checklist

Backup failure.		
Possible cause	*Suggested action*	*Comments*
No backup media in Appliance.	Add backup media.	
Backup media dirty / damaged.	Replace media.	
Backup media at end of life.	Replace media.	Media can be re-written approximately 5,000 times.
Administrator Notified that a dirty shutdown was performed.		
Possible cause	*Suggested action*	*Comments*
Power failure.	Connect to a UPS.	A UPS is reccommended.
Connected to a UPS but did not shutdown before UPS battery discharged.	Check the serial link to the UPS.	
UPS service not started.	Select **System - Services** and start the UPS service.	
Administrator notified that the RAID has degraded.		
Possible cause	*Suggested action*	*Comments*
Hardware failure.	Contact Plasmon support.	

Table 12-1:Archive Appliance Troubleshooting checklist

SATA drive missing.		
Possible cause	*Suggested action*	*Comments*
SATA drive not inserted correctly.	Shutdown the Appliance. Remove then reinsert the drive fully in its drive bay. Power on the Appliance. Contact Plasmon support if the problem is not resolved.	A missing SATA drive can be determined from the **Diagnostics - Storage Devices** page of the web browser interface.
Unable to add a user.		
Possible cause	*Suggested action*	*Comments*
Invalid user name.	Ensure that no special characters are used.	Use the following: A-Z, a-z, 0-9, - (hyphen) and _ (underscore)
Invalid password.	Ensure that no special characters are used.	Use the following: A-Z, a-z, 0-9, - (hyphen) and _ (underscore)
Unable to connect to network share.		
Possible cause	*Suggested action*	*Comments*
Incorrect username or password.	Ensure the correct username and password is used to connect to the Appliance.	

Table 12-1:Archive Appliance Troubleshooting checklist

Network service not started.	Select **Network - Services**. Ensure the correct network services have been started on the Appliance.	
Incorrect hostname or IP used.	Use the correct hostname or IP address. Check that it is possible to ping the Appliance using the hostname and IP.	Name resolution problems may mean that the IP address has to be used.
The client username does not exist on the Appliance.	See "Adding a User" on page 40.	
The client username does not have permissions to access the share.	If the user should have the required permissions, see *Modifying a share* on page 49.	
Host has been denied access.	If the host should have access, see *Modifying a share* on page 49.	

Table 12-1:Archive Appliance Troubleshooting checklist

Successfully connect to network share but permission denied when writing.		
Possible cause	*Suggested action*	*Comments*
File or directory does not have write access permissions for the connected user.	If the user should have the required permissions, see *Modifying a share* on page 49.	The connected users can be determined by opening the **Network - Shares** page and clicking on **connections**. If the access problem only occurs for a specific path or file in the share use the **Storage - Browse** option to check the access permissions for the file or directory.
The share has been set read-only.	Should the share be writeable, open the **Network - Shares** page and click on the share. Ensure the **Read only** option is not selected.	

Table 12-1:Archive Appliance Troubleshooting checklist

SSM service not started.	Open the **System - Services** page and start SSM. If this fails reboot the Appliance then attempt to start SSM. Contact Plasmon support if problem is not resolved.	
SSM fault.	Go to the **Diagnostics - Self test** page and run the **Archive Test**. If this fails, reboot the Appliance, then retest. Contact Plasmon support if problem is not resolved.	
Successfully connect to network share but permission denied when reading.		
Possible cause	*Suggested action*	*Comments*
File or directory does not have read access permissions for the connected user.	If the user should have read permissions, see *Modifying a share* on page 49.	The connected users can be determined by going to the **Network - Shares** page and clicking on **connections**.

Table 12-1:Archive Appliance Troubleshooting checklist

SSM service not started.	Open the **System - Services** page and start SSM. If this fails reboot the Appliance then attempt to start SSM. Contact Plasmon support if problem is not resolved.	
SSM fault.	Open the **Diagnostics - Self test** page and run the **Archive Test**. If this fails, reboot the Appliance, then retest. Contact Plasmon support if problem is not resolved.	

Unable to overwrite or modify files.

Possible cause	*Suggested action*	*Comments*
The WORM emulation option has been set for the CIFS share.	Deselect WORM emulation on the CIFS tab of the share: see *Modifying a share* on page 49.	
Allow File Changes has been set to NO for the Archive Volume.	If file changes should be allowed, see *Viewing and editing volume properties* on page 68 and set the **Allow File Changes** option to YES.	

Table 12-1:Archive Appliance Troubleshooting checklist

No Free Space reported when writing to the share.		
Possible cause	*Suggested action*	*Comments*
The RAID cache is full.	See the causes and actions for *Data is not migrating to media.*	
The Archive Volume option **Never Release Files** has been set.	See "Viewing and editing volume properties" on page 68. Reconfigure release policy as required.	
Email Noficiations not being received.		
Possible cause	*Suggested action*	*Comments*
SMTP server IP address incorrect.	Enter a valid SMTP service IP address.	
SMTP server hostname not being resolved.	Enter a valid DNS server IP address into the network configuration. Alternatively use the IP address of the SMTP server instead.	

Table 12-1:Archive Appliance Troubleshooting checklist

SMTP server IP address not reachable.	If required, ensure a gateway IP address has been entered into the network configuration. Check it is possible to ping the SMTP server from another server on the same subnet as the Appliance.	
SMTP server port number incorrect.	Enter the correct port number.	
Sender not defined.	Enter a sender address.	This is required by some SMTP servers.
Username and password not defined.	Enter a valid username and password.	These are required by some SMTP servers.
Incorrect recipient email address entered.	Check the recipient email address is entered correctly.	
SMTP not enabled.	Ensure the **enable** check box is checked.	

SNMP traps not being received.

Possible cause	*Suggested action*	*Comments*
Incorrect GET Community String.	Enter the correct GET Community String.	

Table 12-1:Archive Appliance Troubleshooting checklist

Incorrect Trap Address.	Enter the correct Trap Address.	
Incorrect TRAP Community String.	TRAP Community String.	
SNMP not enabled.	Ensure the SNMP **enable** check box is checked.	
Media marked “dirty”.		
Possible cause	*Suggested action*	*Comments*
Dirty media.	Clean the media using a Plasmon UDO media cleaning kit and retry. If further media are marked unreliable, contact Plasmon support.	Refer to the Operator’s Guide for media storage and care information.
Administrator notified that the UDO drive is dirty.		
Possible cause	*Suggested action*	*Comments*
Dirty drive.	If it is a UDO1 drive, insert the cleaning cartridge to perform a cleaning cycle. The dirty status should be reset after the next recall or migration. If it is a UDO2 drive, contact Plasmon support as UDO2 drives are self cleaning.	

Table 12-1:Archive Appliance Troubleshooting checklist

Hardware failure.	Contact Plasmon support.	
Appliance will only boot into MAINTENANCE mode.		
Possible cause	*Suggested action*	*Comments*
Hardware failure.	Contact Plasmon support.	
Unable to join Active Directory or NT4 domain.		
Possible cause	*Suggested action*	*Comments*
Incorrect time on Appliance.	Go to the **System - Time & Date** and correct the time.	When the Appliance joins the domain its time will be synchronised with the domain.
DNS is not / incorrectly configured.	The Appliance must have DNS configured to be able to join a domain. See *DNS configuration for Windows Active Directory* on page 38.	
Unable to connect to LDAP server.		
Possible cause	*Suggested action*	*Comments*
Incorrect time on Appliance.	Go to the **System - Time & Date** and correct the time.	

Table 12-1:Archive Appliance Troubleshooting checklist

Unable to create replication schedule.		
Possible cause	*Suggested action*	*Comments*
Invalid name.	Ensure that no special characters are used.	Use the following: A-Z, a-z, 0-9, - (hyphen) and _ (underscore)
Incorrect order.	Create the target schedule before creating the source schedule.	
No volumes available.	Ensure a volume is available for the recplication schedule.	
Replication fails.		
Possible cause	*Suggested action*	*Comments*
Active / Passive Appliance unavailable.	Ensure both Appliances are operational and that no network problems exist between them.	
Replication schedule removed.	Check that both Appliances still have their replication schedule configured.	
Passive volume full.	Enlarge the Passive volume to match the Active volume.	

Table 12-1:Archive Appliance Troubleshooting checklist

Files on the Active volume were offlined before replication took place.	Return offline media to Appliance.
Hardware failure.	Contact Plasmon support.

Chapter 13

Glossary of terms

Glossary of terms

The glossary below describes the meaning of some common terms used throughout the Appliance Administrator's guide.

Table 13-1:

Term	**Meaning**
Archive	An archive is a set of system resources allocated for the storage of data.
Cartridge	The plastic housing that contains and protects the UDO media.
CIFS	Common Internet File System - the network protocol used by the Archive Appliance to allow access by windows clients.
Degraded	A RAID becomes degraded when one of a it's member disks fail.
DHCP	Dynamic Host Configuration Protocol - a method by which IP information is dynamically assigned to a client computer.
Directory	A file system entity which contains a group of files and/or other directories.
DNS	Domain Name Service - Translates meaningful domain names into IP addresses for network communication.
Ethernet	A standard for sending data packets across networks.
FSC	File System Catalog.

Table 13-1:

Term	Meaning
FTP	File Transfer Protocol - a protocol used for transferring data files across a TCP/IP network.
FQDN	Fully Qualified Domain Name - A fully qualified domain name is an unambiguous domain name that specifies the a computer's position in the DNS tree hierarchy absolutely.
GUI	Graphical User Interface - A program which allows a user to interact with computer systems without typing commands directly.
Host	A computer attached to a network.
Hostname	A name by which a host is known to other hosts on a network.
Hot spare	A Hot spare disk is used to replace a failed or removed SATA drive in a RAID configuration.
HTML	HyperText Markup Language - The text-based language used to transmit web pages for interpretation by browser programs.
IP	Internet protocol - a data-oriented protocol used for communicating data across a network.
IP Address	Internet Protocol Address uniquely identifies the Appliance on the TCP/IP network.
LAN	A Local Area Network is a computer network covering a small geographic area.

Table 13-1:

Term	Meaning
Migration	Moving files from the Appliance's RAID storage volume to UDO media.
NAS	Network Attached Storage - dedicated data storage technology which can be connected directly to a computer network to provide centralized data access and storage to heterogeneous network clients.
Network Shares	A network share is a location on an Archive appliance accessible via any of the configured network protocols.
NFS	Network File System - the network protocol used by the Appliance to allow access by Unix and Linux clients.
Operating system	A program that manages system resources and provides a user interface and an application interface, making it possible for programs to run.
Partition	An area of hard disk (or RAID) reserved for a particular operating system or application.
RAID	Redundant Array of Inexpensive Disks - a data storage scheme using multiple SATA disks to share or replicate data among the disks for the purposes of data protection.
Recall	Copying files that have been migrated to UDO media back to the RAID storage volume.

Table 13-1:

Term	Meaning
Resynch	Following a single disk RAID failure, data on the remaining operational disk(s) is used to rebuild the data set on a replacement disk.
SATA	Serial Advanced Technology Attachment - a computer bus technology designed for transfer of data to and from hard disks and optical drives.
SCSI	Small Computer System Interface - a set of standards for physically connecting and transferring data between computers and peripheral devices.
Server	A program which responds to clients requests, which are generally transmitted over a network.
Sequence Number	The Appliance assigns a unique sequence number to each piece of UDO media during initialization.
Shutter	Spring-loaded door protecting the surface of the UDO media.
SMTP	Simple mail transfer protocol - The defacto standard for e-mail transmissions across the Internet.
SNMP	Simple Network Management Protocol - Used by network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Table 13-1:

Term	Meaning
SSH	Secure SHell, a protocol that allows data to be transferred securely between two hosts.
Storage Volume	Dedicated storage area on the Appliance RAID where user files are stored before being moved to UDO media for permanent storage.
TCP	Transmission Control Protocol - one of the core protocols of the Internet protocol suite and allows applications on networked hosts to create connections to one another, over which they can exchange streams of data.
UPS	Uninterruptible Power Supply - A device which maintains a continuous supply of electric power to the Archive Appliance by supplying power from a separate source (usually a battery) when mains power is not available.
UDO	Ultra Density Optical - Plasmon’s optical disk format designed for high-density data storage.
WORM	Write-once, read many - storage media that can only be written to once, but read from multiple times.

Worldwide Technical Support

Europe, Africa and Middle East
Tel: +44 (0)1763 262963
Fax: +44 (0)1763 264407
Web: http://www.plasmontech.com
Email: support@plasmon.co.uk

North America, South America and Asia/Pacific
Tel: +1-877-585-6793 or +1-719-593-4437
Fax: +1-719-593-4192
Web: http://www.plasmontech.com
Email: tech.support@plasmon.com

Sales

Plasmon Data Limited
Whiting Way,
Melbourn
Hertfordshire
SG8 6EN
United Kingdom

Tel: +44 (0)1763 264400
Fax: +44 (0)1763 264444
Web: http://www.plasmon.com
Email: sales@plasmon.co.uk

Plasmon Denver
370 Interlocken Blvd.,
Suite 600,
Broomfield,
CO 80021
United States of America

Tel: +1-720-873-2500
Fax: +1-720-873-2501
Web: http://www.plasmon.com
Email: sales@plasmon.com

Plasmon