UDO ARCHIVE APPLIANCE

ADMINISTRATION GUIDE

Alliance Storage Technologies Inc.

Plasmon

Preliminaries

Copyright statement

Trademarks

Limited warranty

Alliance 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, Alliance 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.

Alliance 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 Alliance 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

Alliance Storage Technologies Inc.
10045 Federal Drive
Colorado Springs, CO 80908 USA
United States of America

Email: sales@astiusa.com

Web: www.astiusa.com

Tel: 719.593.7900
Fax: 719.592.4164

Support

Email: tech.support@astiusa.com

Tel: 877.585.6793/719.593.4437

Fax: 719.593.4164

How to use this guide

This guide describes in detail the operation of the Alliance’s 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:

- *Alliance’s Plasmon UDO Archive Appliance Installation Guide* – Explains how to install the Appliance and get started.

Revision history

Document revision number	System software version	Major Features
860-102532-02 Rev A	4.08.xx	• Replication.
860-102532-03 Rev A	4.11.xx	• UDO Guard • Additional Libraries • Network Backup
860-102532-04 Rev B	4.12.xx	• Enhanced File and media Management • File Exclusion • Network port usage configuration • Slot Licensing • Software Licensing • Considerations for Bulk migration • Update Dirty media handling • added note to UPS section regarding MicroLink
810-02532-04 Rev 02	4.20.xx	• Support for hardware RAID controller and dedicated Disk Buffer Solid State Drive (SSD) • Background recall feature • Replication of owner, owner group and ACLs • Alarm control on status page

Document revision number	System software version	Major Features
810-102532-05	5.00.xx	• Cloud Integrated Storage (CiS) • Data Encryption & Encryption Key Management • Backup to SSD • Update UI pages to support CiS and Encryption • New Recovery process for Encryption • New Feature License key
810-102532-06	5.00.xx	• Adding support for the Archive Appliance Express • Provide an integrated AA and AAE Administrators Guide

Revision history

Contents

Chapter 1

Introduction

Appliance concept

Alliance's Plasmon UDO Archive Appliance (hereafter referred to as the Archive Appliance) and Archive Appliance Express 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 Archive Appliance is a NAS (Network Attached Storage) archive storage solutions that consist of an automated optical library that provides near-line media storage and automated media handling. The Archive Appliance Express, also a NAS archive storage solution requires manual offline media handling, as no library automation is provided.

The web interface is common across both the Archive Appliance family allowing operators to easily transfer their knowledge as archive storage requirements change.

Archive Management Software (AMS)

The Appliance is controlled by the Archive Management Software which includes a customised Operating System, a web-based user interface and an Hierarchical Storage Management package called SSM (Storage Space Manager). SSM can be broadly divided into four separate functional components. Optical Media migration/recall, Cloud migration/recall, media management and Encryption Key Management.

Optical Media Migration

SSM migrates files from RAID to optical media allowing more than one copy to be created. Migration rules are configurable and once migrated files can be purged (released) from the RAID thereby freeing up storage space. When a file is retrieved it either already resides on the RAID or it will be automatically and transparently '*recalled*' from optical.

Cloud Migration

Cloud migration utilizes the same migration rules and procedures as optical migration except in the area of copies. With Cloud integrated Storage, only 1 copy of the data is created and migrated to the cloud. Once migrated to the cloud, the cloud provider, such as Amazon Web

Services, will create multiple replicated copies of the migrated data and store this data across multiple (typically four) datacenters located in that particular region.

Media Management

Optical media can be manged through the web interface by specifying offline rules or selecting specific media to be offlined. Media that are available for offlining can be remove from the library through the keypad. The keypad can also be used to return new or existing media. It is common to have one offline copy outside for extra protection while one copy remains in the library for fast retrieval. Request for offline media are emailed to the administrator who can retrieve the media using the barcode for identification and return it to the library.

Encryption Key Management

A key management system exists which is tightly integrated into SSM. It generates random 256-bit keys (used for AES encryption) and protects them on a second storage device (cloud or network share). A disaster recovery mechanism exists for data as does for keys. All externally stored keys are in turn encrypted using s split-key encryption strategy (system wide Masterkey and archive specific Archive key).

> *Note: Archive Management Software (AMS) uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1747) running on a Linux 3.2 platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.*

UDO technology

UDO™ (Ultra Density Optical), based on blue laser technology, is the underlying foundation to Alliance's archive solution portfolio, including the Appliance. As 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 more than 50 years of media life.

Blue lasers achieve far greater data densities, resulting in dramatically higher media capacities. First and second generation UDO products (UDO30 and UDO60) have a storage capacity of 30GB and 60 GB respectively, with capacity expected to reach 120GB by the third generation.

Archive 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/AA80A12 (Gx-80)
- AA174/AA174A12 (Gx-174)
- AA234/AA438/AA638 (G-238/438/638)

Library components

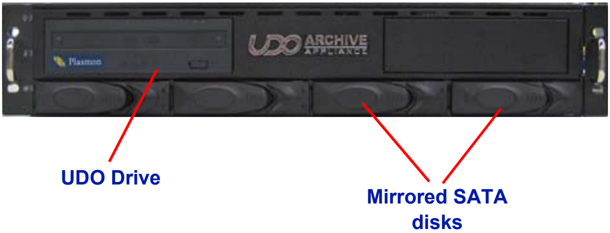
Component	Description
Dual Picker	Transfers UDO media between drives, media slots and Mailslot (IEE).

Component	Description
UDO Drive(s)	The number of UDO drives available for reading/writing media is model-dependent: - 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	House the media inside the Archive Appliance.
Mailslot (IEE)	UDO media is introduced to the Appliance via the mail slot or via direct slot loading. See “Adding UDO media” on page 196.
Server	A server is housed within the Appliance. This manages the Appliance hardware, configuration, and network connectivity. In the AA238,AA438, AA638, AA80A12 and AA174A12 models the server is mounted above the library enclosure.

Archive Appliance Express hardware

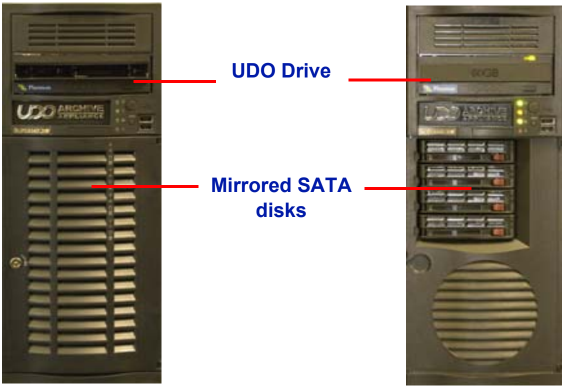
The AAE Rackmount model consists of:

- A server housed in a 2U rack mountable enclosure.
- A rackmount kit.
- 2-4 SATA disks (see below for supported RAID configurations).
- Integrated UDO drive.



The AAE Desktop model consists of:

- A server housed in a desktop form factor enclosure.
- 2-4 SATA disks (see below for supported RAID configurations).
- Integrated UDO drive



Archive Appliance Express supported RAID configurations

The AAE can be configured with 2, 3 or 4 SATA disks in the following configurations:

- 2 SATA disks in a RAID 1 (mirrored pair) configuration.
- 2 SATA disks in a RAID 1 (mirrored pair) configuration with a third SATA disk configured as a Hot Spare.
- 4 SATA Disks in a RAID 5 configuration.

IP Network port usage

In the Network-Configuration section of the web interface the port usage can be blocked from access. The network ports used by the Archive Appliance software are listed below:

Port	Name	Comments
21	**FTP**	**Only active if FTP service is turned on**
22	**Secure Shell - SSH**	
80	**HTTP**	
111	**Portmapper, rpcbind**	
139	**netbios-ssn NETBIOS Session Service**	
443	HTTPS	Can be blocked via port usage page
445	**microsoft-ds Microsoft-DS**	**Required for CIFS access, can be blocked via usage page**
873	**Rsync replication service**	**Only active if replication is turned on**
2809	Corba Name service	Blocked by default
3050	Firebird	Blocked by default
4000	**Rpcstatd (status)**	
4001	**Nlockmgr (NFS)**	**Only active if NFS service is turned on**
4002	**Mountd (NFS)**	**Only active if NFS service is turned on**

4003	**Rquotad (NFS)**	**Only active if NFS service is turned on**
8000	Java Debug	Blocked by default
30000	**System manager service**	**Required for replication**
UDP		
111	**Rpcbind**	
137	**Netbios-ns**	
138	Netbios-dgm	Filtered, no service
177	Xdmcp	Filtered, no service
502	Asa-appl-proto	Filtered, no service
623	Asf-rmcp	Filtered, no service
664	Secure-aux-bus	Filtered, no service
998	Puparp	Filtered, no service
2049	**NFS**	
3664	UPS Engine	Filtered, no service
4000	**Network Status Monitor, rpcstatd**	used by NFS

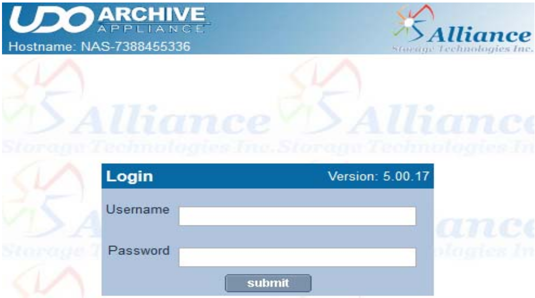
Chapter 2

The Archive Appliance

Starting the Web interface

1. On a LAN-attached client, start a web browser (e.g. Microsoft Internet Explorer, Mozilla Firefox).
2. In the URL field, enter the IP address or hostname of the Appliance to be configured. For example:

   `http://192.168.0.1`



Hostname: NAS-7388455336

Login Version: 5.00.17

Username

Password

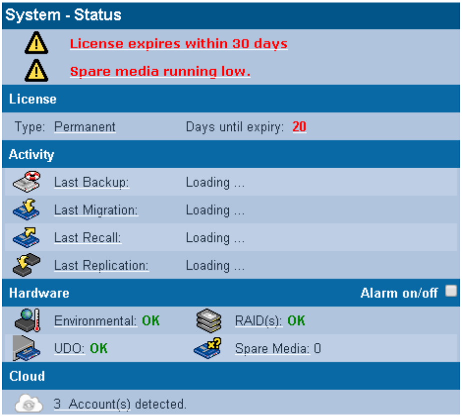
3. In the Web Interface login page, enter a valid Appliance Administrator User Name and Password.

Note: This is not the same as a Windows Domain Administrator.

- The default administrator username and password is **admin**. It is recommended that this is changed on first login. See “Modifying a User’s details” on page 57.
- 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

⚠ License expires within 30 days

⚠ Spare media running low.

License

Type: Permanent   Days until expiry: 20

Activity

Last Backup:	Loading ...
Last Migration:	Loading ...
Last Recall:	Loading ...
Last Replication:	Loading ...

Hardware   Alarm on/off □

Environmental: OK	RAID(s): OK
UDO: OK	Spare Media: 0

Cloud

3 Account(s) detected.

System - Status page features

The **System - Status** page displays an overview of current system status (“System - Status” on page 20), 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

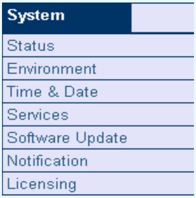
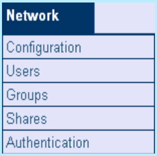
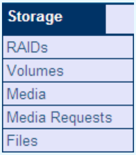
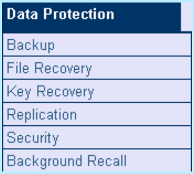
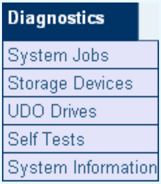
Menu/icon	Use to
 System Status Environment Time & Date Services Software Update Notification Licensing	Monitor the Appliance’s status, set the time & date, monitor and configure the services, update the system software, configure alert notifications and review/ apply licenses (Product and Feature License)
 Network Configuration Users Groups Shares Authentication	Define the network configuration, users, groups and shares
 Storage RAIDs Volumes Media Media Requests Files	Configure RAIDs and volumes, search and browse the media, and monitor offline media requests

Table 2-1: Web interface menus

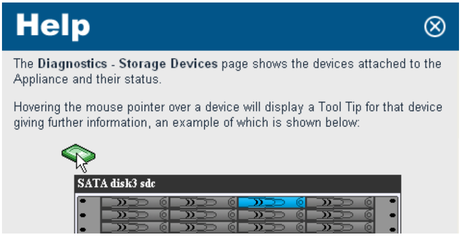
Menu/icon	Use to
 Data Protection Backup File Recovery Key Recovery Replication Security Background Recall	Perform a system configuration backup, recovery of archive(s), recovery of the encryption key database, configure archives for replication, manage security keys including the AA Master Encryption Wrapping Key, Archive Encryption Wrapping Key(s), as well as the UDOGuard key, and background recall of files from optical media onto RAID.
 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.:

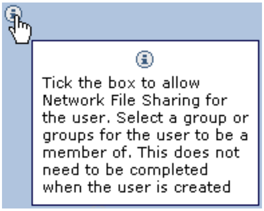


The **Diagnostics - Storage Devices** page shows the devices attached to the Appliance and their status.

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.:

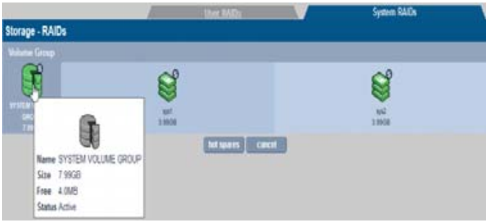


Tick the box to allow Network File Sharing for the user. Select a group or groups for the user to be a member of. This does not need to be completed when the user is created

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

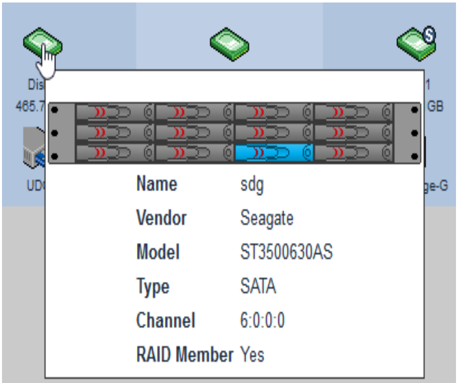
- Volumes and Volume Groups
- SATA Drives
- RAIDs
- Controllers
- Flash Media
- Attached Libraries

Hovering mouse over the device icons will display the device details



Name SYSTEM VOLUME GROUP
Size 7.99GB
Free 4.0MB
Status Active

Note: Occasionally the popup windows may either appear in the wrong color or be positioned incorrectly. Simply refresh the page (i.e. press F5). This should reset the page styles and correct any display issues.
On Internet Explorer pop ups may not appear at all. This can be rectified by switching the browser into “Compatibility View” mode (see page settings).

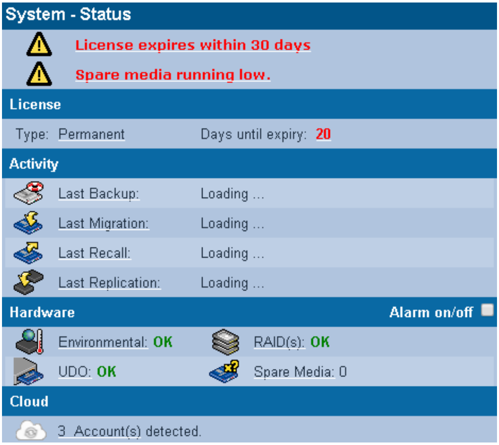


Name	sdg
Vendor	Seagate
Model	ST3500630AS
Type	SATA
Channel	6:0:0:0
RAID Member	Yes

Chapter 3
System menu

System - Status

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



System - Status

⚠ License expires within 30 days

⚠ Spare media running low.

License

Type: Permanent   Days until expiry: 20

Activity

Last Backup:	Loading ...
Last Migration:	Loading ...
Last Recall:	Loading ...
Last Replication:	Loading ...

Hardware   Alarm on/off □

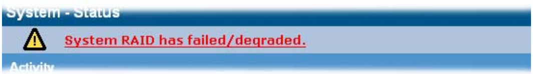
Environmental:	OK	RAID(s):	OK
UDO:	OK	Spare Media:	0

Cloud

3 Account(s) detected.

The page is split into five 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.:



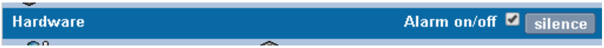
System - Status

⚠ System RAID has failed/degraded.

Activity

- The **License** area displays the license **Type** and **Days until expiry**.
- 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.The **RAID controller alarm** can be enabled/disabled

checking/unckecking the Alarm checkbox..

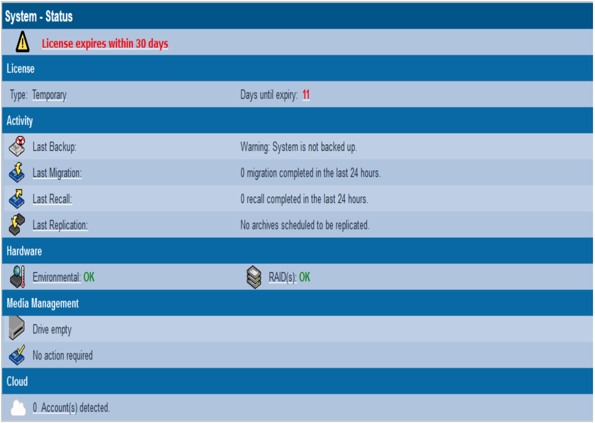


Hardware

Alarm on/off ☑ silence

'Silence' will also mute the enclosure but NOT the PSU alarm.

- At the bottom the of status page the Cloud agent status is displayed. The Cloud agent can assume four states: "Not started", "Not configured", "Not connected" and "Connected". Note that the cloud agent configuration can be accessed by clicking the hyperlink.
- AAE only, the **Media Management** area as displayed below is included on the Status page and displays information about the currently loaded media and indicates what, if any, operator action is required.



System - Status

⚠ License expires within 30 days

License

Type: Temporary — Days until expiry: 11

Activity

Last Backup: Warning: System is not backed up.

Last Migration: 0 migration completed in the last 24 hours.

Last Recall: 0 recall completed in the last 24 hours.

Last Replication: No archives scheduled to be replicated.

Hardware

Environmental: OK — RAID(s): OK

Media Management

Drive empty

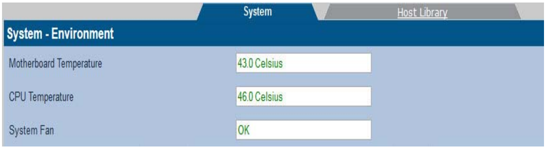
No action required

Cloud

0 Account(s) detected.

Environmental status

The environmental status of the Appliance can be viewed by clicking the “Environmental” hyperlink on the status page. *You can navigate to **System - Environment** page by clicking **Environment** option in the **System** menu.*. The information shown includes the library (and attached library, if present) and the server environmental such as **Motherboard Temperature**, **CPU Temperature** and **System Fan** in the **System** tab. If the server includes a RAID controller, the RAID environmental information is also displayed. The Host Library tab displays all the host environment details such as Temperature, Front Fan Status, and Rear Fan Status.



System - Environment

Motherboard Temperature	43.0 Celsius
CPU Temperature	46.0 Celsius
System Fan	OK

*Note: Only **System** tab is displayed in the AAE Web interface after clicking the **Environmental** hyperlink in the **Status** page, as the AAE has no attached host or extension library.*

A value shown in green indicates that the environmental value is within operational range and acceptable. “N/A “ indicates that a value is not given by the hardware, but it is within range. “Not monitored” means the metric cannot be obtained.

Important: The Battery Backup Unit (BBU) is required in order to maintain good performance. If the BBU fails, the RAID controller will not use the cache which in turn will significantly affect the IO performance. It is strongly recommended to review the BBU status once per month.

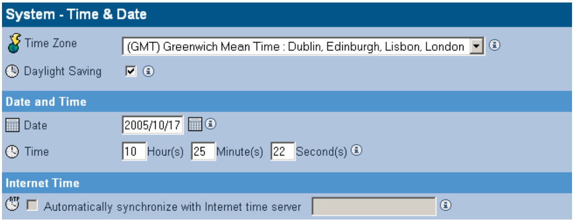
Finally, the “**silence**” button mutes the RAID controller alarm and server enclosure alarm. Some alarms cannot be muted as they are activated by the hardware (e.g. Power supply alarm, environmental failure alert).

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	☑

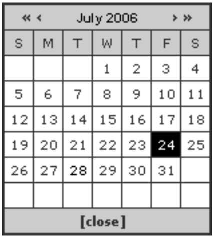
Date and Time

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	

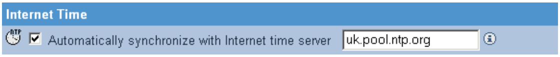
[close]

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, date, or timezone is changed, the Appliance will reboot. Ensure that no users are connected before proceeding.

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. Alliance strongly recommends the use of an NTP server.

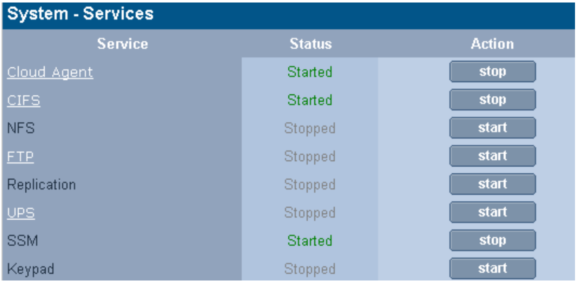
3. The connection to the NTP server may be tested by clicking the **test ntp** button.

Note: When connecting to the Active Directory time is automatically synchronised with the Domain controller and the NTP setting are ignored.

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

Note: When the status of the NTP checkbox is changed, the Appliance will reboot. Ensure that no users are connected before proceeding.

Managing services



System - Services

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

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

- **Cloud Agent** - Manages the connections from the AMS to the Cloud provider account(s). Also performs the upload and download of all data and metadata objects being migrated and recalled from the cloud. The Agent is started with SSM. Select the hyperlink to access and manage the Cloud provider account details.
- **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 26
- **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 63
- **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 31
- **Replication** - This service controls replication between the Appliance and a partnered Appliance - see page 130.
- **UPS (Uninterruptible Power Supply)** -Displays the status of an attached APC SmartUPS if one is present - see page 33

- **RAID Integrity Checker** - Monitors the data integrity of the RAIDs by reading / writing sectors and verifying them in the process. This process will begin once the service is started, and continues to operate in the background during times of low usage.
- **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.

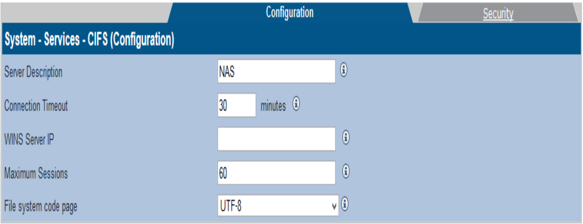
> *Note: In AAE Web interface, **Keypad** is not available as there is no host or extension library attached.*

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

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

> *Note: When using Windows Active Directory, it is essential that the primary DNS address entered when following the network configuration procedure (see “Configuration” on page 48) is set to that of the Active Directory Primary Domain Controller. To determine the IP address of the Domain Controller, see “DNS configuration for Windows Active Directory” on page 51.*

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



System - Services - CIFS (Configuration)

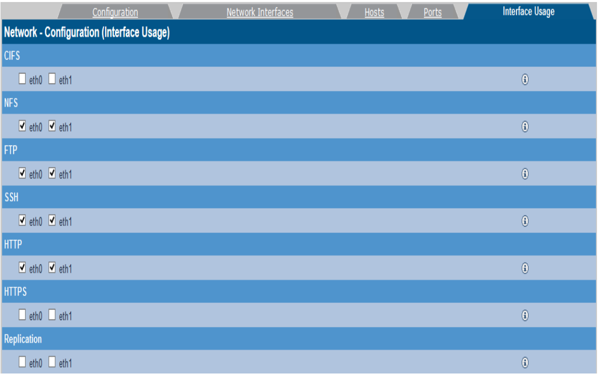
Server Description	NAS
Connection Timeout	30 minutes
WINS Server IP	
Maximum Sessions	60
File system code page	UTF-8

2. Enter a **Server Description**.

   This is the name by which the Archive Appliance advertises itself on the Windows network.
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 maximum number of sessions in the **Maximum Sessions** field.

   This is the maximum number of concurrent CIFS sessions that the Archive Appliance will accept. The default is 60 sessions.
6. The **File system code page** option allows for a specific character encoding table to be used for all CIFS communications. The default is UTF-8, and should not be changed unless strictly necessary on the Appliance’s host network.



Network - Configuration (Interface Usage)

CIFS

☐ eth0 ☐ eth1

NFS

☑ eth0 ☑ eth1

FTP

☑ eth0 ☑ eth1

SSH

☑ eth0 ☑ eth1

HTTP

☑ eth0 ☑ eth1

HTTPS

☐ eth0 ☐ eth1

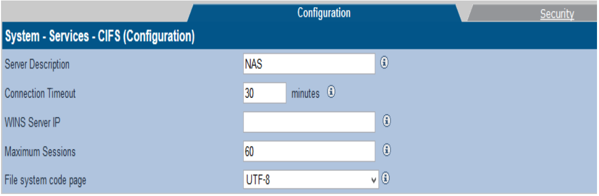
Replication

☐ eth0 ☐ eth1

Configuring CIFS (Windows Networking)

The Common Internet File System (or SMB - Server Message Block) protocol allows file access through a Windows Network share. To configure a share follow the procedure below:

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



System - Services - CIFS (Configuration)

Server Description	NAS
Connection Timeout	30 minutes
WINS Server IP	
Maximum Sessions	60
File system code page	UTF-8

2. Enter a **Server Description**.
   This is the name by which the AAE advertises itself on the Windows network.
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 maximum number of sessions in the **Maximum Sessions** field.

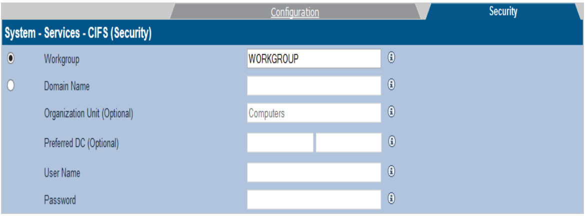
   This is the maximum number of concurrent CIFS sessions that the Archive Appliance will accept. The default is 60 sessions.

6. The **File System Code Page** option allows for a specific character encoding table to be used for all CIFS communications. The default is UTF-8, and should not be changed unless strictly necessary on the AAE host network.

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.



● Workgroup: WORKGROUP

○ Domain Name:

Organization Unit (Optional): Computers

Preferred DC (Optional):

User Name:

Password:

2. Enter either:

   A **Workgroup** - To authenticate against the local user database provided by the Archive 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 Archive Appliance to a Domain, additional details may be required:

- Up to two **Preferred DC**'s may be specified if desired, and the Archive Appliance will attempt to connect to them in order *(NT Compatible mode only)*
- The **Organizational Unit** (OU) within the Active Directory structure in which the Appliance will appear, (by default, the Archive Appliance will appear in the *Computers* OU).
- A Windows **User Name** with the correct access rights to add objects to the Domain, and the user's **Password**. The password must be repeated in the **Confirm Password** field.

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

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

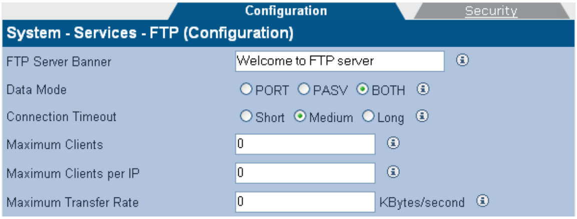
3. Click **save** to save the changes, **stop** to stop the CIFS service, or **diagnose** to diagnose connectivity problems.

Configuring NFS

The NFS networking service is configured via the **Network - Shares** page - see page 61.

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 FTP server
Data Mode	○ PORT ○ PASV ● BOTH
Connection Timeout	○ Short ● Medium ○ Long
Maximum Clients	0
Maximum Clients per IP	0
Maximum Transfer Rate	0 KBytes/second

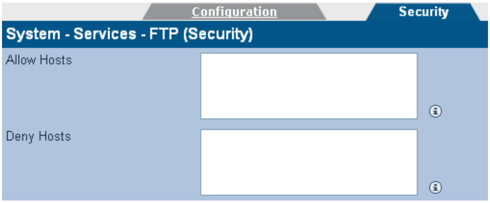
2. If required, enter an **FTP Server Banner**. This is a message which will be displayed to users when they access the Archive Appliance via FTP.
3. Enter a **Data Mode**. The data mode can be:
   - **PORT** - Also known as Active mode.
   - **PASV** - Passive mode FTP.
   - **BOTH** - The FTP client defines the connection method (PORT or PASV) and the server responds accordingly.
4. Enter a **Connection Timeout**. This defines how long the Archive 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 KB/s, 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. Click **Start** or **Stop** to start or stop the services whenever appropriate.

UPS

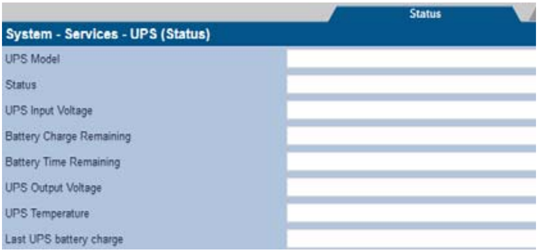
The information in the **System - Services - UPS** page is derived from the Uninterruptible Power Supply (UPS) itself.

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

> *Note: The Appliance only supports APC brand Smart UPS devices with a legacy serial connection.An adapter (AP9620 Legacy Interface) is required from APC to provide the serial connection (DB9 connector) for AA software support of the Smart UPS.*

> *Note: The Appliance does NOT support the MicroLink communication interface.*

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



System - Services - UPS (Status)

UPS Model

Status

UPS Input Voltage

Battery Charge Remaining

Battery Time Remaining

UPS Output Voltage

UPS Temperature

Last UPS battery charge

Th

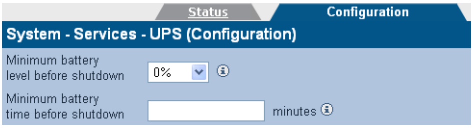
e following information is displayed:

- **UPS Model** - The model code of the UPS attached to the Appliance
- **Status** - The UPS's status
  (e.g ONLINE, LOW BATTERY, etc.)
- **UPS Input Voltage** - Mains line voltage
- **Battery Charge Remaining** - The amount of battery charge, in percent, remaining
- **Battery Time Remaining** - The amount of battery charge, in minutes, remaining

- **UPS Output Voltage** - The UPS's output voltage (to the Appliance)
- **UPS Temperature** - The temperature of the UPS enclosure
- **Last UPS battery charge** - 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:



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 any changes.

Update the System Software

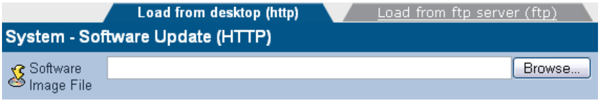
The **System - Software Update** page enables updates to the system software to be performed using:

- **Load from desktop (HTTP)** - from a local computer.
- **Load from ftp server (FTP)** - from the Alliance FTP server.

Load from desktop (HTTP)

1. Reboot the Appliance into maintenance mode via the **Shutdown** menu.
2. From the menu bar, select **System - Software Update**.

   The **System - Software Update (http)** page opens:



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

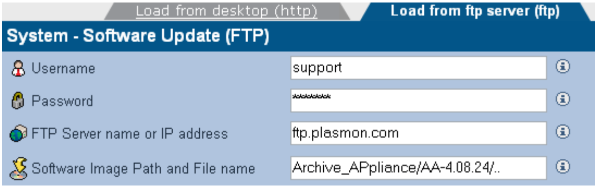
> *Note: The file transfer is controlled entirely by the web browser. There may be no visual indication of transfer progress.*

Follow the on-screen instructions to complete the installation.

Load from ftp server (FTP)

1. Reboot the Appliance into maintenance mode via the **Shutdown** menu.
2. From the menu bar, select **System - Software Update**.
3. Click on the **FTP** tab.

   The **System - Software Update (ftp)** page opens:



System - Software Update (FTP)

Username	support
Password	********
FTP Server name or IP address	ftp.plasmon.com
Software Image Path and File name	Archive_APpliance/AA-4.08.24/..

4. Contact Alliance technical support for the FTP server and login details. Enter them into the **Username**, **Password**, **Server name or IP** and **Software Image Path and File name** fields.
5. Click **transfer** to begin the software update.
   Follow the on-screen instructions to complete the installation.

Notification

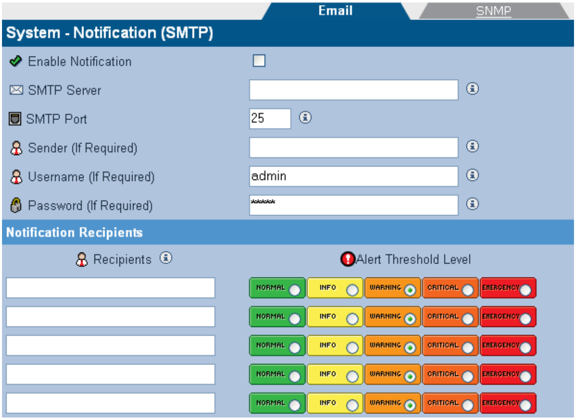
The Archive Appliance can notify system administrators of system events and errors by:

- Email (Simple Mail Transfer Protocol - SMTP) Notification - see below
- Simple Network Management Protocol (SNMP) Notification - see page 38.
- A history of the notifications can be viewed via the Web interface, and should be regularly reviewed and its contents cleared (see page 40).

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 Notification	□
SMTP Server	
SMTP Port	25
Sender (If Required)	
Username (If Required)	admin
Password (If Required)	*****

Notification Recipients

Recipients	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 ○

2. Select 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 default 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 1:* .

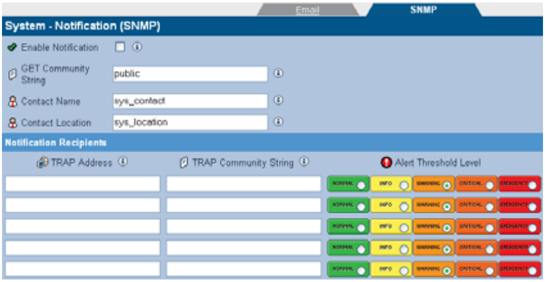
> *Note: For "call home" registered systems, please use the email monitoring service: tech.support@astiusa.com. This will allow Alliance to monitor the Appliance remotely. If you have any questions, please contact Alliance Technical Support.*

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 Notification □

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. Select 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@alliance.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, Alliance 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 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.

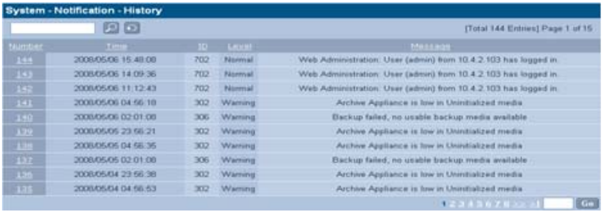
Table 1: . Notification Alert Threshold Levels

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 strongly recommended 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 144 Entries] Page 1 of 15

Number	Time	ID	Level	Message
144	2008/05/06 15:48:08	702	Normal	Web Administration: User (admin) from 10.4.2.103 has logged in
143	2008/05/06 14:09:36	702	Normal	Web Administration: User (admin) from 10.4.2.103 has logged in
142	2008/05/06 11:12:43	702	Normal	Web Administration: User (admin) from 10.4.2.103 has logged in
141	2008/05/06 04:56:18	302	Warning	Archive Appliance is low in Uninitialized media
140	2008/05/06 02:01:08	306	Warning	Backup failed, no usable backup media available
139	2008/05/05 23:56:21	302	Warning	Archive Appliance is low in Uninitialized media
138	2008/05/05 04:56:35	302	Warning	Archive Appliance is low in Uninitialized media
137	2008/05/05 02:01:08	306	Warning	Backup failed, no usable backup media available
136	2008/05/04 23:56:38	302	Warning	Archive Appliance is low in Uninitialized media
135	2008/05/04 04:56:53	302	Warning	Archive Appliance is low in Uninitialized media

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** 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.

Licensing

The Archive Appliance contains proprietary software which provides the unique capabilities and functionality of Alliance's Archive Appliance. With the Archive Appliance software, at release level 4.12 or higher, licensing of the software for usage on only authorized hardware has now been introduced.

Types of Archive Appliance License Keys

There are three unique types of License Keys which authorize the usage of the Archive Appliance software. Each license key, which is uniquely tied to the specific Archive Appliance that it authorizes, facilitates Archive Appliance functionality as outlined below:

Permanent License Key

Allows for permanent usage of Archive Appliance software

Has a time limit regarding access to upgrades and software patches, which typically expires at the end of the Warranty or Service Agreement period.

Temporary License Key

Allows for temporary usage of Archive Appliance software, disabling new migrations to media once the license has expired. Temporary License Keys are typically issued for a period of 30 to 90 days.

Has a time limit regarding access to upgrades and software patches, which typically expires at the end of the Warranty or Service Agreement period.

Grace License Key

Default key, instantiated when first activating the Archive Appliance software.

Allows for the temporary usage of Archive Appliance software, disabling new migrations to media after 30 days.

Feature License

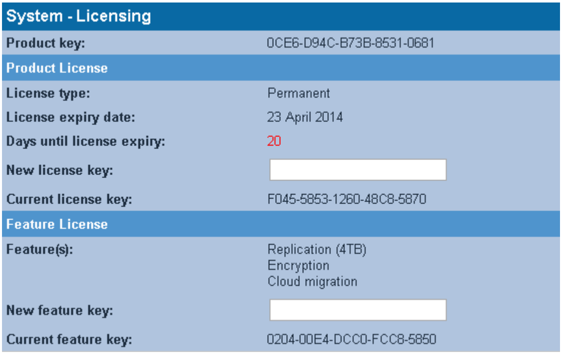
As well as a licensing the base product, specific feature can be enabled by setting the Feature License. Licensable features include Replication, Cloud integration and file encryption.

How the Archive Appliance's Licensing works?

The Archive Appliance at initialization time and on a daily basis validates licensing.

License Status	Key Type	Actions
Active	Permanent Temporay Grace	• AA fully functional • Can install all available Software
Active expiring within 30 days	Permanent Temporay Grace	• AA fully functional • Can install all available AA software released before License Key expired • Warning message issued daily: License Key expiring in xx days
License Expired	Permanent	• AA fully functional • Can install AA software released before License Key expires • Informational message monthly: *License expired, software upgrades disabled*
License Expired	Temporary Grace	• AA disables migrating and recall of data to/from media • Cannot install any AA Software • Warning message issued daily: *Invalid license key, system disabled*

Applying New License Keys.



System - Licensing	
Product key:	0CE6-D94C-B73B-8531-0681
Product License	
License type:	Permanent
License expiry date:	23 April 2014
Days until license expiry:	20
New license key:	
Current license key:	F045-5853-1260-48C8-5870
Feature License	
Feature(s):	Replication (4TB) Encryption Cloud migration
New feature key:	
Current feature key:	0204-00E4-DCC0-FCC8-5850

1. Enter or cut and paste the license key provide by Alliance Storage Technologies into the "New license key" textbox. If your key is not available, contact Alliance Technical Support.

   Note: Note: The License Key must contain 20 alpha-numeric characters (not including the dashes).

2. Once the License Key has been entered, press the save button. The Archive Appliance will process the license key and, if valid, will store the new license key as the active key and the newly applied License Key will be displayed in the Current License Key field along with the License Type (Permanent or Temporary), the date when the license expires and the number of days left before the license expires.

   Note: A newly installed Archive Appliance will automatically have a "Grace" license installed. Grace Keys can only be applied automatically by the Archive Appliance.

   Note: The Feature license is handled in the same way as the Product License, however, it does not expire. Feature include replication, encryption and cloud migration.

Cloud Service Configuration

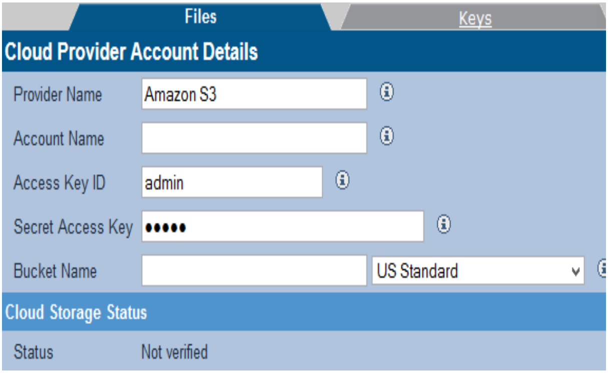
Before the cloud service can be started, it is necessary to define at least one cloud account. The cloud account contains the configuration settings required to establish an authenticated connection to a cloud provider. It is possible to have many accounts to the same provider, each account may have different access points or credentials.

There are two unique types of cloud account definitions:

Files – Can define 1 or more cloud accounts for the purpose of archiving files. A single cloud account can be used to store all your cloud enabled archives, or, for example, a unique cloud account could be defined for each unique cloud enabled archive volume.

Keys – Can define only 1 cloud account for the storage of encryption keys.

.



Cloud Provider Account Details

Provider Name	Amazon S3	
Account Name		
Access Key ID	admin	
Secret Access Key	●●●●●	
Bucket Name		US Standard

Cloud Storage Status

Status	Not verified

In order to create an account enter all the required fields and click “*save*”. If the information entered is correct and the network connection can be established, the account details will validate and the account will be locked. Once the account is validated and locked it cannot be removed.

If the account fails to be locked the information can be corrected or the account can be removed.

Some format and validation rules apply. Space character ‘ ‘ and underscore ‘_’ may not be used for the bucket name and the bucket name it needs to be unique to that provider.

Both “Files” and “Keys” accounts are managed in the same way.

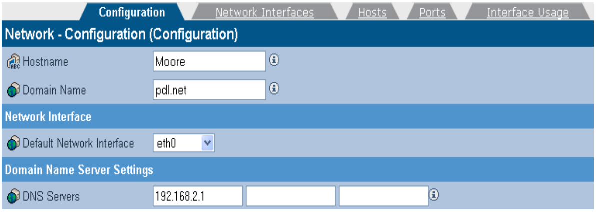
Chapter 4

Network menu

Network Settings

Configuration

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

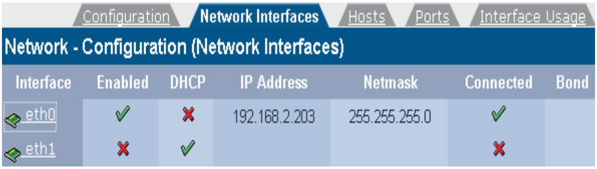


Network - Configuration (Configuration)

Hostname	Moore
Domain Name	pdl.net
Network Interface	
Default Network Interface	eth0
Domain Name Server Settings	
DNS Servers	192.168.2.1

2. Enter a **Hostname** for the Archive Appliance
3. Enter the **Domain Name** which the Archive Appliance belongs to.
4. Select the **Default Network Interface** from the drop-down list.
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 51 for details of configuring the Archive Appliance for use with Windows Active directory.

Click on the **Network Interfaces** tab. The Archive Appliance's network (Ethernet) interfaces are listed:



Network - Configuration (Network Interfaces)

Interface	Enabled	DHCP	IP Address	Netmask	Connected	Bond
eth0	✓	✗	192.168.2.203	255.255.255.0	✓	
eth1	✗	✓			✗	

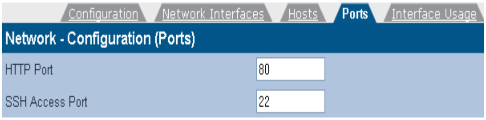
The following information is also displayed:

- **Name** - The Ethernet port name, *eth0* (the Archive 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
- **Connected** - Indicates whether or not the network connection is operational.
- **Bond** - On the Archive Appliance 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 52.

6. Click on the **Ports** tab. The Archive Appliance's administration TCP/IP ports are listed:



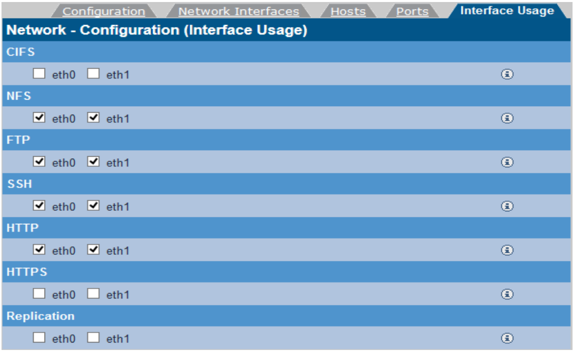
Network - Configuration (Ports)

HTTP Port 80

SSH Access Port 22

- **HTTP Port** - The port number for access via the Web Interface. The default HTTP port is 80.The HTTP Port will also be used by Alliance support engineers when accessing the web interface remotely. See "Update the System Software" on page 35.
- **SSH Access Port** - The port number for local and remote access via SSH. The default SSH port is 22.The SSH Port will also be used by Alliance support engineers when accessing the command-line interface remotely. See "Update the System Software" on page 35.

7. Click on the **Interface Usage** tab. This will list the protocols available, with checkboxes for all of the available interfaces:



Network - Configuration (Interface Usage)

CIFS
□ eth0 □ eth1

NFS
☑ eth0 ☑ eth1

FTP
☑ eth0 ☑ eth1

SSH
☑ eth0 ☑ eth1

HTTP
☑ eth0 ☑ eth1

HTTPS
□ eth0 □ eth1

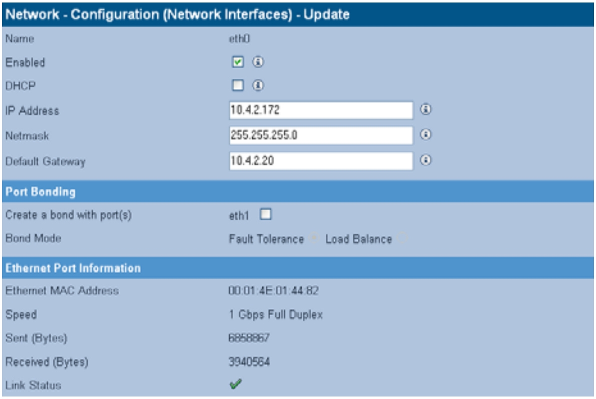
Replication
□ eth0 □ eth1

If the Archive Appliance has multiple network interfaces, it is possible to select which interface to use on a per-protocol basis. By default, all protocols use all interfaces.

8. Click **save** to save the changes.

Setting a static IP address

1. From within the **Network - Configuration (Network Interfaces)** page, click on a network interface’s name:



Network - Configuration (Network Interfaces) - Update

Name	eth0
Enabled	☑
DHCP	□
IP Address	10.4.2.172
Netmask	255.255.255.0
Default Gateway	10.4.2.20
Port Bonding	
Create a bond with port(s)	eth1 □
Bond Mode	Fault Tolerance ○ Load Balance ○
Ethernet Port Information	
Ethernet MAC Address	00:01:4E:01:44:82
Speed	1 Gbps Full Duplex
Sent (Bytes)	6858867
Received (Bytes)	3940564
Link Status	✓

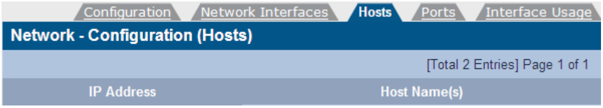
2. Clear the DHCP check-box.

3. Enter the **IP Address**, **Netmask** and **Default Gateway**. The network administrator can provide these details.
4. Click the **save** button.

Creating a static hosts table

Static host name configuration is generally not required. In some rare situations it may be beneficial to configure a host name for notification and ftp software installation when the host name is not available via DNS.

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



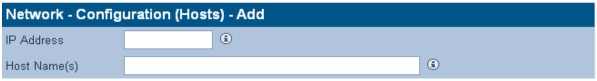
Network - Configuration (Hosts)

[Total 2 Entries] Page 1 of 1

IP Address	Host Name(s)

This page can be used to specify network hosts which are known to the Appliance so that the Appliance may communicate with them if the DNS service is not available or in the event of a DNS failure.

2. Click **add** to add a new host:



Network - Configuration (Hosts) - Add

IP Address

Host Name(s)

3. Enter the IP address and Host name, and click **add**.

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 48) 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 Archive 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 (Network Interfaces)** 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.

Note: Fault tolerance failover will cause a change in MAC address, which may have implications when the Appliance is connected to a switch with port security enabled. Refer to the switch documentation for further information on port security.

Users

The **Network - Users** page lists all the users defined on the Archive Appliance, whether defined locally or sourced from an Active Directory domain or LDAP server.

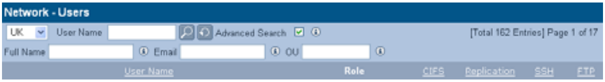
By default the locally defined users are listed. If the Archive Appliance has been configured to include users from an external directory, the drop-down box will become active, and any configured external directory may be selected.

> *Note: External Directory users may not be added, modified or deleted via the Archive Appliance.*

The local user list may be searched for by User Name. The asterisk may be used as a wildcard, and the search is case-sensitive.

> *Note: The wildcard character cannot be used as the first character in the search term.*

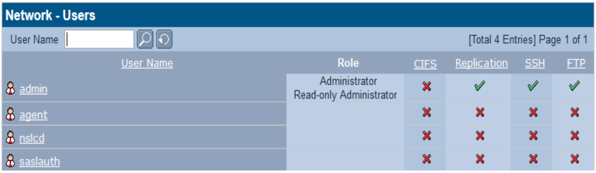
Active Directory user lists may use the Advanced Search function. To enable, tick the **Advanced Search** checkbox:


Network - Users
UK User Name Advanced Search ☑ [Total 162 Entries] Page 1 of 17
Full Name Email OU

It is possible to search using a user's **User Name**, **Full Name**, **Email** or **OU** (Organizational Unit), and the asterisk may be used as a wild card. This search is not case-sensitive.

Adding a User

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

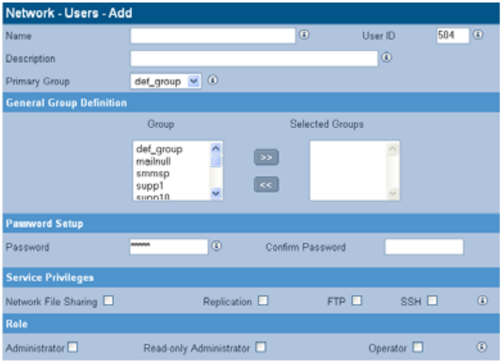


Network - Users

User Name [Total 4 Entries] Page 1 of 1

User Name	Role	CIFS	Replication	SSH	FTP
admin	Administrator Read-only Administrator	✗	✓	✓	✓
agent		✗	✗	✗	✗
nslcd		✗	✗	✗	✗
saslauth		✗	✗	✗	✗

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



Network - Users - Add

Name □ User ID 504

Description

Primary Group def_group

General Group Definition

Group: def_group, mailnull, smmsp, supp1, supp10

Selected Groups

Password Setup

Password ****** Confirm Password

Service Privileges

Network File Sharing □ Replication □ FTP □ SSH □

Role

Administrator □ Read-only Administrator □ Operator □

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. Select a **Primary Group** for the user to be a member of. The default group is `def_group`.

6. In the **General Group Definition** area, additional groups may be selected for the user to be a member of. Click any required group(s) in the **Group** list (CTRL-click to select more than one group at a time) and click the **>>** button to add the selected group(s) to the **Selected Groups** list.
7. Enter and confirm the user's **Password** (required).
8. Tick the **Network File Sharing** checkbox to enable CIFS for the User and select a Group from the **Network Sharing Group Privileges** list.
9. If the User is to have replication privileges, tick the **Replication** box.
10. If the User is to have FTP access privileges, tick the **FTP** box.
11. 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.
12. The user may have a Role defined. Roles control the level of access a user has to the Archive Appliance's Web Interface. A user with no Role selected cannot access the Web Interface.

    An **Administrator** can log on to the Web Interface and has full control over the Archive Appliance, including making changes to system configuration, volumes, archives and other settings.

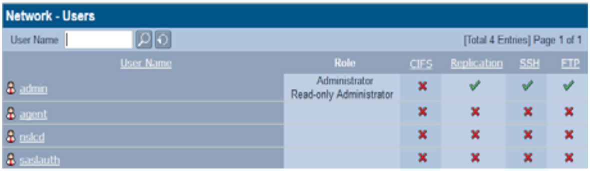
    A **Read-Only Administrator** may log on to the Web Interface and view all pages, but cannot make any changes.

    An **Operator** has read-only access to the Web Interface, limited to the **System - Status**, **Storage - Online Media** and **Storage - Offline Media** pages.

13. Click add to add the User.

Deleting a User

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



Network - Users

User Name

[Total 4 Entries] Page 1 of 1

User Name	Role	CIFS	Replication	SSH	FTP
admin	Administrator Read-only Administrator	✗	✓	✓	✓
agent		✗	✗	✗	✗
nslcd		✗	✗	✗	✗
saslauth		✗	✗	✗	✗

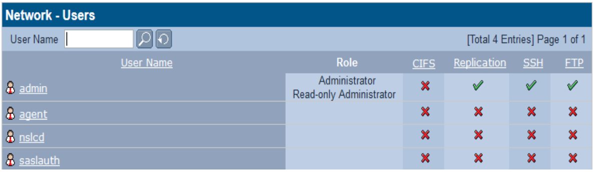
2. Click the User Name of the User to be deleted.
   The **Network - Users - Update** page is displayed.

3. Click delete. A warning message is displayed.

4. Click delete to confirm deletion of the user.

Modifying a User’s details

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

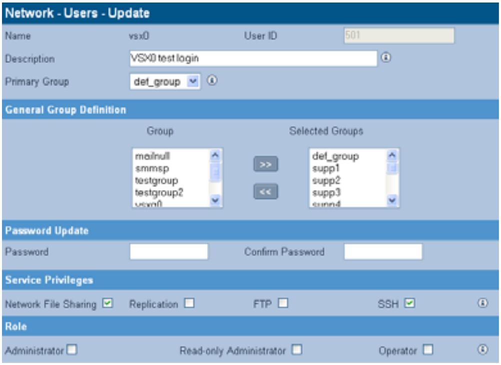


Network - Users

User Name [ ] [Total 4 Entries] Page 1 of 1

User Name	Role	CIFS	Replication	SSH	FTP
admin	Administrator Read-only Administrator	✗	✓	✓	✓
agent		✗	✗	✗	✗
nslcd		✗	✗	✗	✗
saslauth		✗	✗	✗	✗

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 vsx0 User ID 501

Description VSX0 test login

Primary Group def_group

General Group Definition

Group		Selected Groups
mailnull smmsp testgroup testgroup2 vsxg0	>> <<	def_group supp1 supp2 supp3 supp4

Password Update

Password [ ] Confirm Password [ ]

Service Privileges

Network File Sharing ☑ Replication □ FTP □ SSH ☑

Role

Administrator □ Read-only Administrator □ Operator □

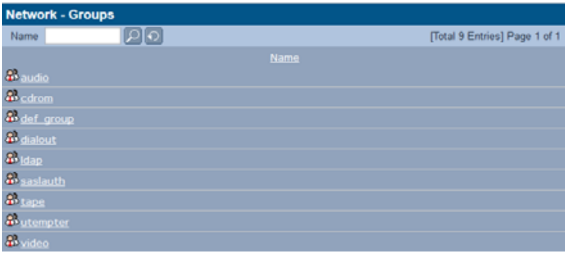
3. The user’s **Description**, **Primary Group**, **General Group Definition**, **Password** or **Role** can be updated.
4. Click **save** to save the changes.

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**:

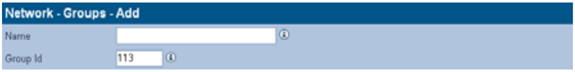


Network - Groups

Name [Total 9 Entries] Page 1 of 1

Name
audio
cdrom
def_group
dialout
ldap
saslauth
tape
utempter
video

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



Network - Groups - Add

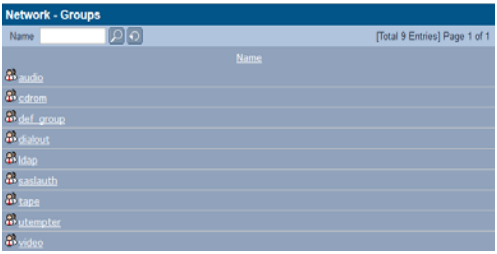
Name	
Group Id	113

3. Enter a **Name** for the Group. The **Group ID** is automatically assigned.
4. Click **add** to add the Group.

Editing a Group

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

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



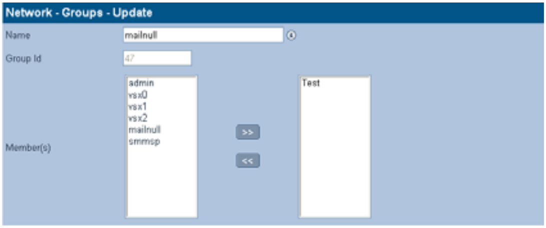
Network - Groups

Name [Total 9 Entries] Page 1 of 1

Name

- audio
- cdrom
- def_group
- dialout
- ldap
- saslauth
- tape
- utempter
- video

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



Network - Groups - Update

Name: mailnull

Group Id: 47

Member(s):

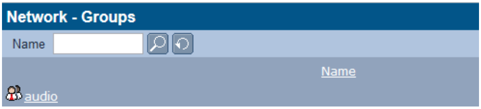
admin
vsx0
vsx1
vsx2
mailnull
smmsp

Test

3. Change the group’s **Name** and **Member(s)** as required.
4. Click **save** to save the changes.

Deleting a Group

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



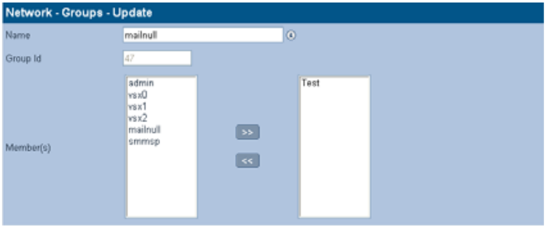
Network - Groups

Name

Name

audio

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



Network - Groups - Update

Name: mailnull

Group Id: 47

Member(s):

admin
vsx0
vsx1
vsx2
mailnull
smmsp

Test

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

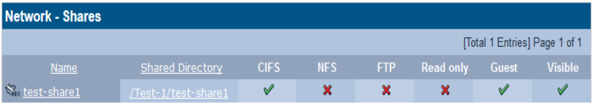
Shares

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**.

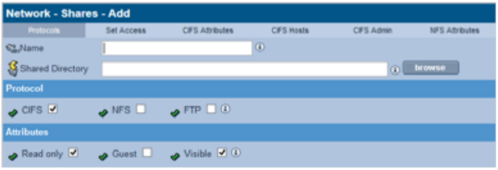


Network - Shares

[Total 1 Entries] Page 1 of 1

Name	Shared Directory	CIFS	NFS	FTP	Read only	Guest	Visible
test-share1	/Test-1/test-share1	✓	✗	✗	✗	✓	✓

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



Network - Shares - Add

Name

Shared Directory

Protocol

CIFS ☑ NFS ☐ FTP ☐

Attributes

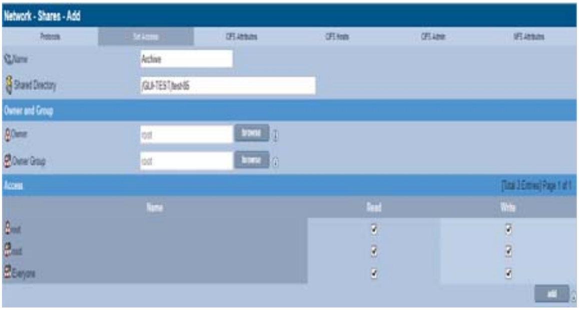
Read only ☑ Guest ☐ Visible ☑

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

Shared Directory: /GUI-TEST/test85

Owner and Group

Owner: root

Owner Group: root

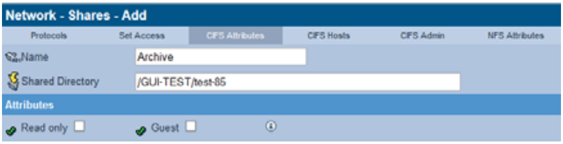
Access [Total 3 Entries] Page 1 of 1

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

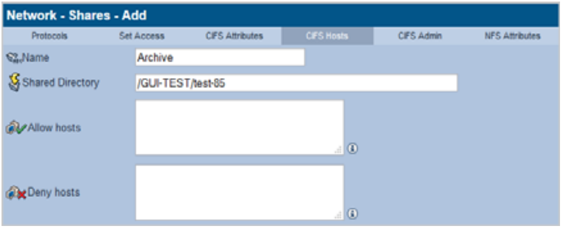
Shared Directory: /GUI-TEST/test-85

Attributes

Read only □ Guest □

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

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



Network - Shares - Add

Protocols | Set Access | CIFS Attributes | CIFS Hosts | CIFS Admin | NFS Attributes

Name: Archive

Shared Directory: /GUI-TEST/test-85

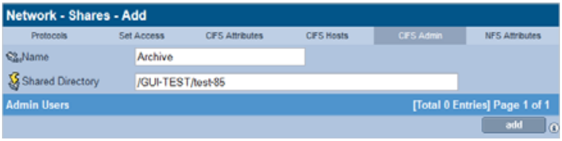
Allow hosts:

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:



Network - Shares - Add

Protocols | Set Access | CIFS Attributes | CIFS Hosts | CIFS Admin | NFS Attributes

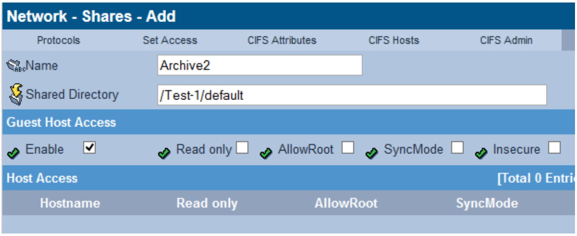
Name: Archive

Shared Directory: /GUI-TEST/test-85

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:



Network - Shares - Add

Protocols | Set Access | CIFS Attributes | CIFS Hosts | CIFS Admin

Name: Archive2

Shared Directory: /Test-1/default

Guest Host Access

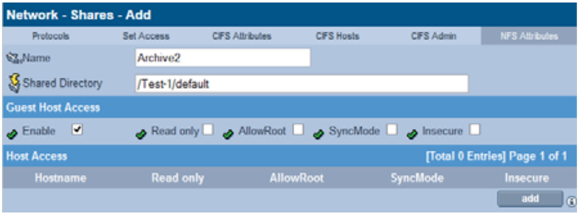
Enable ☑ Read only □ AllowRoot □ SyncMode □ Insecure □

Host Access [Total 0 Entri

Hostname	Read only	AllowRoot	SyncMode

16. Click add to add NFS Hosts to the Share.

The **NFS Host Entry Details** page opens:



Network - Shares - Add

Name: Archive2

Shared Directory: /Test-1/default

Guest Host Access

Enable ☑ Read only □ AllowRoot □ SyncMode □ Insecure □

Host Access [Total 0 Entries] Page 1 of 1

Hostname	Read only	AllowRoot	SyncMode	Insecure

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** - (disabled by default) can improve performance at the risk of filesystem fragmentation when reading or writing large amounts of small files.

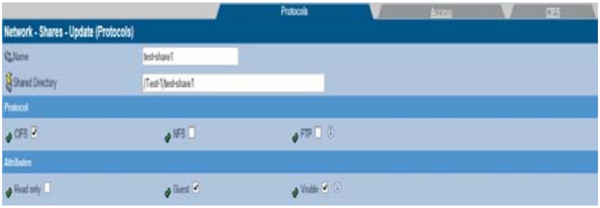
Click ok to continue.

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: test-share1

Shared Directory: /Test-1/test-share1

Protocol

CIFS ☑ NFS □ FTP □

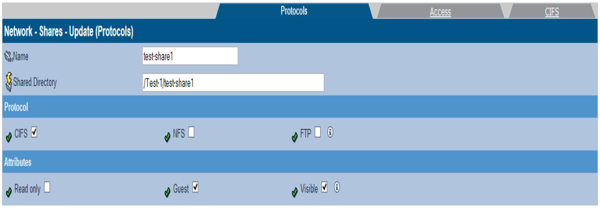
Attributes

Read only □ Guest ☑ Visible ☑

4. Click **delete**.
   The Archive 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 modified.
3. The **Network - Shares - Update (Protocols)** page opens:



Network - Shares - Update (Protocols)

Name: test-share1

Shared Directory: /Test-1/test-share1

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**.

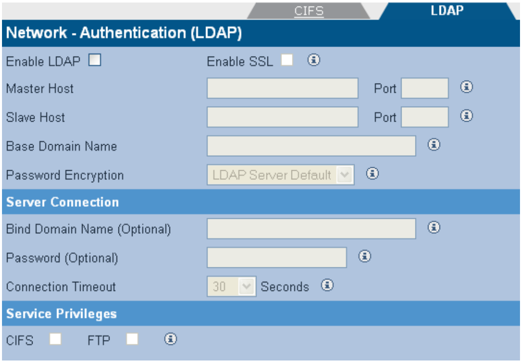
Note: For in-depth detail on the options available in each tab, see Adding a Share on page 61.

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**.



CIFS | LDAP

Network - Authentication (LDAP)

Enable LDAP □ Enable SSL □

Master Host ____ Port ____

Slave Host ____ Port ____

Base Domain Name ____

Password Encryption LDAP Server Default

Server Connection

Bind Domain Name (Optional) ____

Password (Optional) ____

Connection Timeout 30 Seconds

Service Privileges

CIFS □ FTP □

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

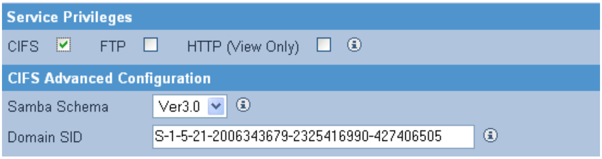
> *Note: Note that the user password cannot be set via an anonymous connection.*

9. Enter a **Password** (Optional). The password used when binding the LDAP server with the Bind Domain Name.
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 and FTP users to be authenticated against the LDAP directory.

1. If required, tick the **CIFS** or **FTP** boxes.
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 Archive 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

eDirectory can be administered using a number of tools. ConsoleOne and iManager are two popular administration consoles. The method of performing some of the setup tasks will vary depending on the administration tools used; however, the principles remain the same.

1. **Import schema definitions**

In order for Linux/Unix system to interoperate with a directory the "user" and "group" schema needs to be POSIX compliant.

Novell provide a command line tool called "ice" that can be used to import auxiliary schema definition into the directory:

```
    ice -SLDIF -fd:\export.ldif -DLDAP -s<SERVER> -
    p389 -dcn=<...> -w<PASSWORD>
```

In order for the any authentication to be successful the POSIX auxiliary classes (posixAccount and posixGroup) are required. However, for CIFS authentication to work an additional schema needs to be imported (sambaSamAccount). Note that sambaSamAccount depends on the POSIX schemas. The POSIX rfc2307 schema definitions are available from Novell and the Samba LDIF file is attached to this document. LDIF and schema files can be imported as shown below:

```
ice -SLDIF -f samba.ldif -D LDAP -s
192.168.2.22 -d cn=admin,o=asti.net -w mypasswd

ice -SSCH -f rfc2307-usergroup.sch -D LDAP -s
192.168.2.22 -d cn=admin,o=pdl.net -w mypasswd
```

Note: The schema import command may vary depending on the underlying Operating System. For example, the Linux NDS distribution also has "ndssch" available for schema import.

2. Create/Modify POSIX users

When creating new users for accessing the AA it is necessary to add the following posixAccount attributes:

- **Name** - keep same as object name
- **uidNumber** - user id of user (> 501)
- **gidNumber** - group ID of user (> 501)
- **Common Name** - same as Other Name
- **Unique ID** - this will already exist as it corresponds to the object name.

Note that the AA administration interface will setup all necessary objects and attributes required for CIFS authentication.

Important: If existing users need to access the AA then it is necessary to extend the existing user object.

Important: In order for the authentication to be successful it is essential that only one Unique ID exists even though the Unique ID attribute is multi-valued.

3. Set/Synchronize passwords

NDS/eDirectory maintains its own passwords and password policy which cannot be shared with Samba. For this reason it is necessary to maintain a separate password for CIFS authentication. However, the AA provides an interface to synchronize the Linux/Unix/Samba password. Simply access the user details "Network - Users - Update" and set the user password. Note also that Novell have been working towards a Universal password scheme and the reader is advised to consult with Novell regarding password synchronisation and Universal passwords.

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

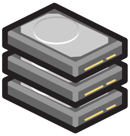
CIFS

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 26.

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: The Archive Appliances with an internal archive controller, the RAID configuration is limited to a single RAID-1 (mirrored pair hard drive). The Archive Appliances with an external archive controller, the system RAID configuration is made up of one RAID-1/Mirror system volume and a RAID 5/6 data volume. The System RAID is predefined and cannot be altered as it is maintained by the system automatically.

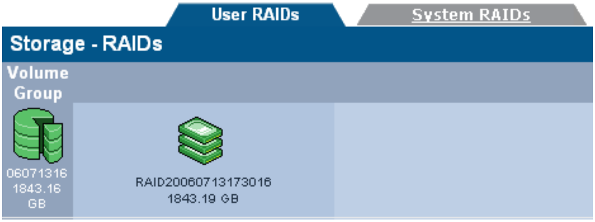
There are two types of RAID systems available in the Archive Appliance product line: SoftRAID, using a RAID software driver and HardRAID, using a RAID controller HBA.

Both solutions provide the same functionality, however, the HardRAID solution offers superior IO performance over the SoftRAID solution. Also, the HardRAID solution include a BBU (Battery Backup Unit) which eliminates the need to rebuild the RAID after a power failure. It also protects against the rare event of RAID corruption.

The only way to identify the presence of a RAID controller is to refer to the Devices page (*Storage Devices* on page 151). Note the “LSI SAS” controller icon at the left-hand edge of the page.

Viewing RAIDs

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



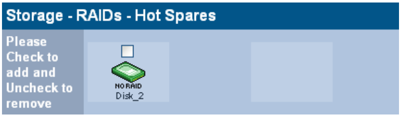
2. Hover over any Volume Group or RAID for a Tool Tip containing status information.

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
□
NO RAID
Disk_2

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.

Volumes

The **Storage - Volumes** page can view and add volumes to the volume group.

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.

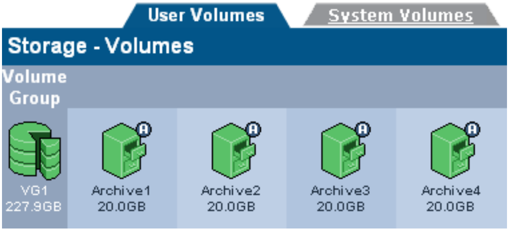
> *Note: On the AAE you can define up to 12 archives (managed volumes) that are cloud archive with only 1 of these archives that is optical archive. However, on the AA you can define as many archives (managed volumes) that are either Cloud Optical or cloud or optical.*

On the Archive Appliance, two types of volume are available:

- An archive - where data is written to the Archive Appliance's RAID(s) and when defined criteria have been met, the data is migrated onto UDO media - see *Creating an archive* on page 76.
- An unmanaged volume - where data is written to the Archive Appliance's RAID cache only - see *Creating an unmanaged volume* on page 89

Creating an archive

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



User Volumes | System Volumes

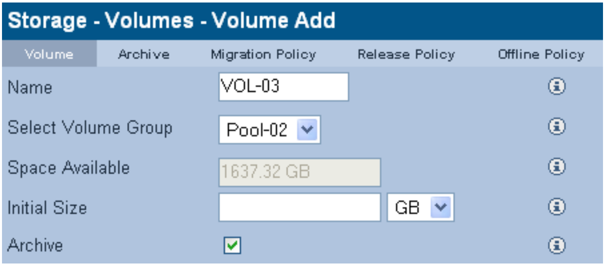
Storage - Volumes

Volume Group

VG1 227.9GB	Archive1 20.0GB	Archive2 20.0GB	Archive3 20.0GB	Archive4 20.0GB

2. Click add.

   The **Storage -Volumes - Volume Add** page opens:



Storage - Volumes - Volume Add

Volume | Archive | Migration Policy | Release Policy | Offline Policy

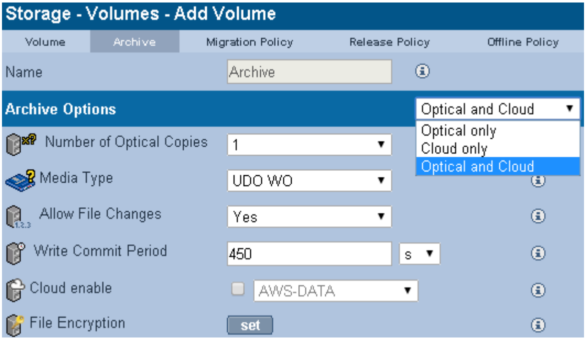
Name	VOL-03
Select Volume Group	Pool-02
Space Available	1637.32 GB
Initial Size	GB
Archive	☑

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.

   Note: Volume size may be increased at a later date, but may never be decreased.

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 - Add Volume

Name: Archive

Archive Options: Optical and Cloud (Optical only / Cloud only / Optical and Cloud)

Number of Optical Copies: 1

Media Type: UDO WO

Allow File Changes: Yes

Write Commit Period: 450 s

Cloud enable: □ AWS-DATA

File Encryption

8. When specifying your Archive Volume, you can choose between three types of Archive Volume storage options, which include:

    Optical Only All data will be migrated to Optical Media only

    Cloud Only All data will be migrated to Cloud Storage only

    Optical and Cloud All data will be migrated to both Optical Media and Cloud Storage

    Depending on your selection, the fields you will be presented with and subsequently required to complete will change.

Note: On the AAE you can define up to 12 archives (managed volumes) that are cloud archive with only 1 of these archives that is optical archive. However, on the AA you can define as many archives (managed volumes) that are either Cloud Optical or cloud or optical.

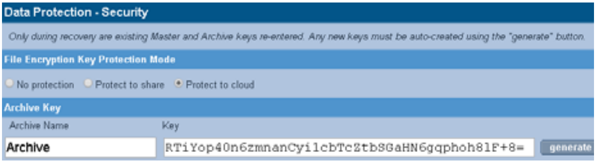
9. Select the **Number of Copies** of the file to make. Copies are made on separate UDO media and can be offlined to provide an additional level of data protection.
10. Select the **Media Type** the archive will use:
    - **UDO WO** - UDO WORM media
    - **UDO CWO** - Compliant UDO WORM media.
11. 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 file system is created. After the write commit period has expired, no further file changes are permitted.

12. . 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.
13. If a cloud account has been successfully configured, the options to enable cloud migration will be available. To enable migrations to the cloud, check the box and select the cloud provider account you wish the archive data to be migrated to.
14. Select the File Encryption ‘Set’ button if files are to be encrypted.

File Encryption configuration

In order to enable File encryption is necessary to ‘set’ the configuration parameters for the Key Manager. This includes the system wide Masterkey (if it has not already been set), the archive specific key and the key protection mode (if it has not already been set).



Data Protection - Security

Only during recovery are existing Master and Archive keys re-entered. Any new keys must be auto-created using the "generate" button.

File Encryption Key Protection Mode

○ No protection ○ Protect to share ● Protect to cloud

Archive Key

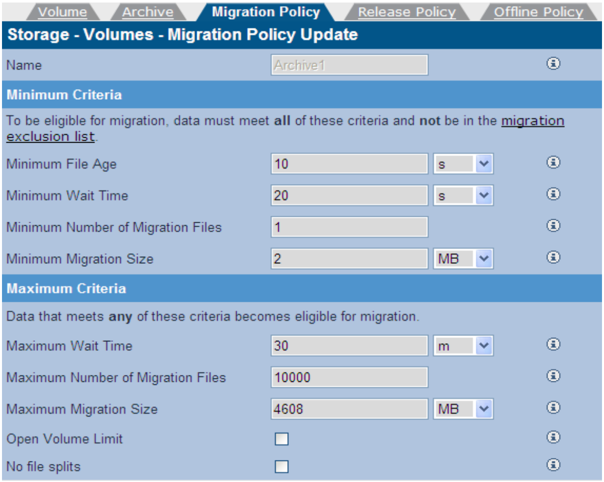
Archive Name	Key	
Archive	RTiYop40n6zmnanCyilcbTcZtbSGaHN6gqphoh8lF+8=	generate

In the picture above the masterkey has already been set but the archive key has not. Press the ‘*generate*’ button and it will create a valid and compliant key. Keys cannot be entered manually but must be generated using the ‘generate’ button.
Note that in the above example the keys will be saved to the cloud.

Important: It is critical that the generate key is copied and saved by the archive owner. Use Cut n’ Paste to create a hard copy and an electronic copy of the all generate keys.

Note: For more details on configuring File Encryption, see Security on page 137.

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



Storage - Volumes - Migration Policy Update

Name	Archive1	
Minimum Criteria		
To be eligible for migration, data must meet **all** of these criteria and **not** be in the migration exclusion list.		
Minimum File Age	10	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

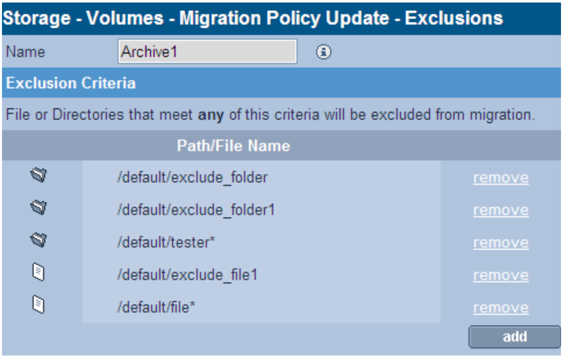
16. Enter the following **Minimum Criteria**:
    - **Minimum File Age** - The amount of time a file must remain unchanged to become a candidate for migration
    - **Minimum Wait Time** - Migration will NOT be started if new files are added to migration candidate list during the Minimum Wait Time
    - **Minimum Number of Migration Files** - Migration will NOT be started if there are less than the Minimum Number of Migration Files to be migrated
    - **Minimum Migration Size** - Migration will NOT be started if the total size is less than the Minimum Migration Size.
17. 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 the Maximum Wait Time
  - **Maximum Number of Migration Files** - Migration will be started if there are more than Maximum Number of the Migration Files waiting to be migrated
  - **Maximum Migration Size** - Migration will be started if the total size exceeds the Maximum Migration Size.

18. 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 utilize all of the available drives, and files from the same directory are less likely to be split across different media.
19. 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.
20. Files listed in the **Exclude** list will not be migrated to media. Click **migration exclusion list** to add or remove files and file types from this list.

Migration Exclusion List

When clicking the “migration exclusion list” hyperlink, the following page is displayed:



Storage - Volumes - Migration Policy Update - Exclusions

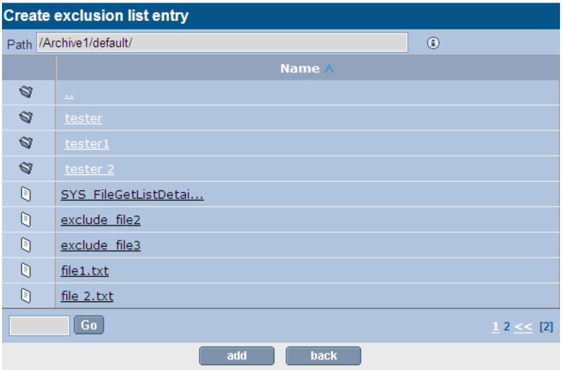
Name: Archive1

Exclusion Criteria

File or Directories that meet **any** of this criteria will be excluded from migration.

	Path/File Name	
	/default/exclude_folder	remove
	/default/exclude_folder1	remove
	/default/tester*	remove
	/default/exclude_file1	remove
	/default/file*	remove

To add a specific file or folder to the exclusion list, click the add button at the bottom right of the display area:



Create exclusion list entry

Path: /Archive1/default/

	Name
	..
	tester
	tester1
	tester 2
	SYS_FileGetListDetai...
	exclude_file2
	exclude_file3
	file1.txt
	file 2.txt

There are two options available for specifying an exclusion entry. Either select an existing item from the display list or enter the full file/folder path into the top edit control. Wildcard entries are permitted e.g. `*.tdb.` The entry will be accepted once the add button has been clicked and saved with the save button.

> *Note: Folders are identified by the trailing slash '/' character. So "/Archive1/default/folder/ identifies a folder while "/Archive1/default/folder" identifies a file called "folder".*

If an excluded file or folder is renamed (such that it is no longer excluded) it will be immediately scheduled for migration.

Archive Configuration Examples

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

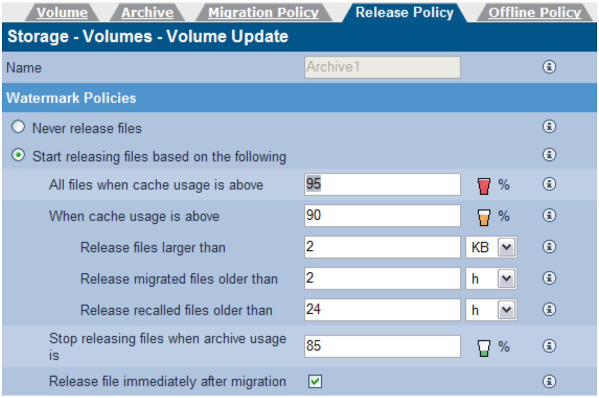
  Migration will occur as soon as at least 1000 files, larger than 100 MB in total become eligible for migration (by remaining unchanged for 10 seconds or more) and no other files have become eligible for migration within the last hour. Even if not all of the minimum criteria are met, a migration will 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 1: 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

21. 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.

22. To set release policies for the archive, select:

    - **Never release files** - Files are never released from the RAID cache.

- or -

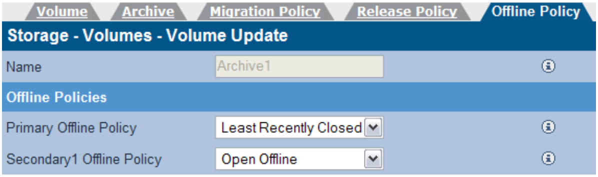
- **Start releasing files based on the following:**
    - **All files when cache usage is above:** When the specified percentage of storage space on the RAID cache is used, the system will start releasing all migrated and recalled files.
    - **When cache usage is above:** When the specified percentage 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.

23. Click next >> to continue.

    The **Storage -Volumes - Volume Add** page, **Offline Policy** tab opens:

    > *Note: For AA Only: Offline Policy tab is only available for AA.*



Storage - Volumes - Volume Update

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

24. Select a **Primary** and **Secondary Offline Policy** from the drop down lists:
    - **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.
    - **Least Recently Used** - Media are offlined in order of media closure. The oldest closed media is offlined first.
    - **Prohibit offline** - Media in the pool cannot be offlined.
    - **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*.

25. Click add.

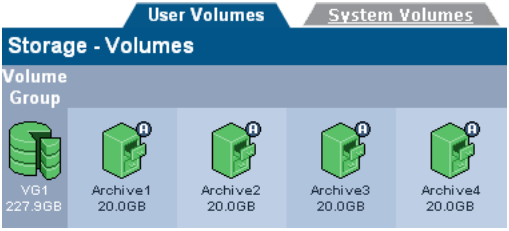
Once the volume has been created, the Archive Appliance will return to the **Storage - Volumes** page.

Creating an unmanaged volume

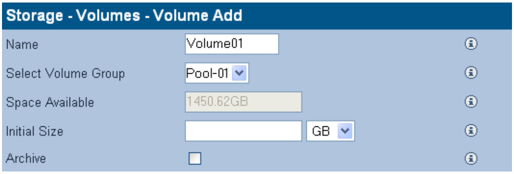
Once a RAID has been created, the associated volume group can be divided into volumes.

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	☐	

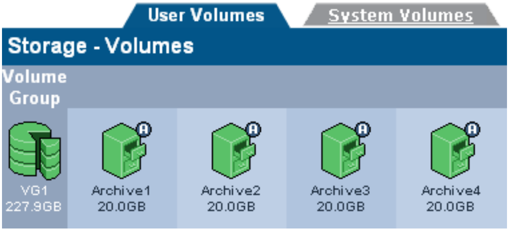
3. A **Volume Name** is automatically generated, or can be entered (up to 32 characters; a-z, A-Z, 0-9, - (hyphen e.g. Volume-01) and _ (underscore e.g. Volume_1).
4. Select a Pool that the volume should be in from the **Select Volume Group** drop-down list.
5. The **Space Available** is shown.

   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.

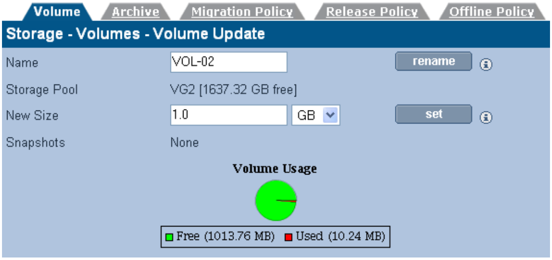
   Enter an **Initial Size** for the volume.
6. Click add. Once the volume has been created, the Archive Appliance will return to the **Storage - Volumes** page.

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	

Volume Usage

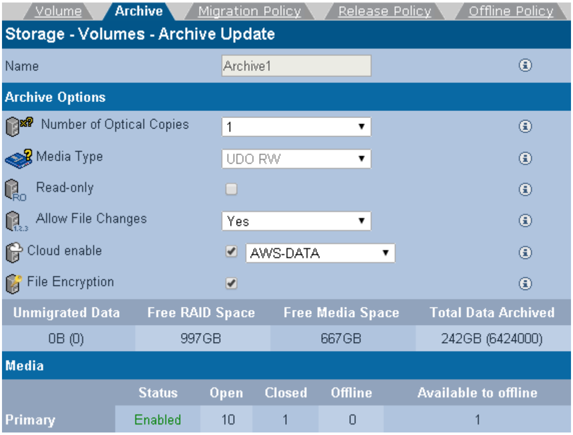
🟩 Free (1013.76 MB) 🟥 Used (10.24 MB)

Items that may be edited are:

- **Volume 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 a volume is a replica it is strongly recommended to match the size of each replica volume.

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



Storage - Volumes - Archive Update

Name: Archive1

Archive Options

Number of Optical Copies	1
Media Type	UDO RW
Read-only	☐
Allow File Changes	Yes
Cloud enable	☑ AWS-DATA
File Encryption	☑

Unmigrated Data	Free RAID Space	Free Media Space	Total Data Archived
0B (0)	997GB	667GB	242GB (6424000)

Media

	Status	Open	Closed	Offline	Available to offline
Primary	Enabled	10	1	0	1

Items that may be edited are:

- **Number of copies** - number of media pools. One pool per copy.
- **Read-only -** disable write to archive
- **Allow File Changes**. - disable to simulate WORM behaviour
- **Write commit period -** period after which file cannot be modified
- **Cloud enable -** enable migration to cloud. If more than one validated provider account exists, the required account can be selected.
- **File Encryption -** enable/disable encryption once all precondition have been satisfied (see note below)

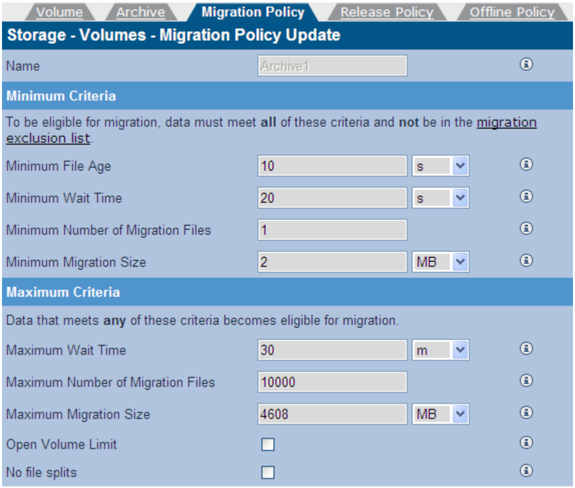
Note: In order to enable encryption the following preconditions need to be met. Encryption needs to be licensed, a Master key needs to exist, the associated archive key needs to exist and the key backup storage needs to be configured.

Note: Once a volume has been created, the Number of Copies option may only be changed to 1 or 2.

Information-only fields are:

- **Unmigrated Data** - Shows the cumulative size of the files awaiting migration to optical media and/or the cloud. 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 optical media and/or the cloud. The approximate number of files on the archive is show in brackets.
- **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 - Migration Policy Update

Name	Archive1	

Minimum Criteria

To be eligible for migration, data must meet **all** of these criteria and **not** be in the migration exclusion list.

Minimum File Age	10	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	□	

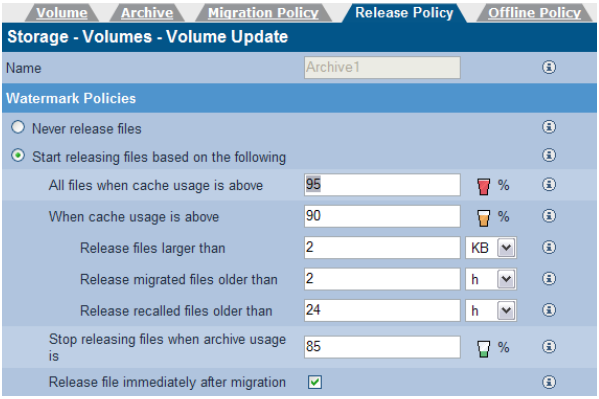
Items that may be edited are:

- **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**

Read-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	☑	

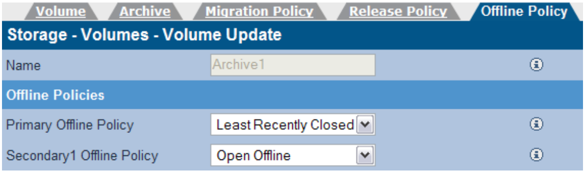
Items that may be edited are:

- **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.

Closing media

In some situations it is necessary to close all media associated with an archive volume at a specific point in time. To support this requirement the Archive Appliance provides a close media button at the bottom of the "Archive" tab (Storage>Volujme>select Archive).

> *Note: Media should only be closed when the archive is not active. As the close media process will force the archive into read-only mode for the duration of the close media process, any active write operations will be terminated. Furthermore, for the closing action to complete quickly it requires the maximum number of UDO drives.*

The close media process is made up of five steps:

1. Make archive read-only
2. Check that all files on the RAID have been migrated and that the correct number of copies exist for each file
3. Close all open media
4. Make the archive writable again
5. Backup the new media state

Step 1: Once the close media button has been pressed, the system will immediately make the archive read-only. This is to ensure that only files that already exist on the RAID cache at the time of the close media action will be saved to any open media.

Step 2: Check that all files for the archive volume in question have the correct number of copies. If an archive has two media pools then each file must exist on two pieces of media.

Step 3: Once all the files have been written to UDO, any open media are closed.

Step 4: Once all media have been closed the archive volume is reverted to writable.

Step 5: The backup is started to ensure that all media status information is protected, so that all closed media can be removed from the library if required.

Note: The media close process can be cancelled during step 1, 2 and 3 pressing the cancel close media *button. However, once a piece of media has been closed it cannot be reverted.*

The close media process may take some time to complete during which time the archive is not writable. Also the process will continue after a appliance restart until all media are closed.

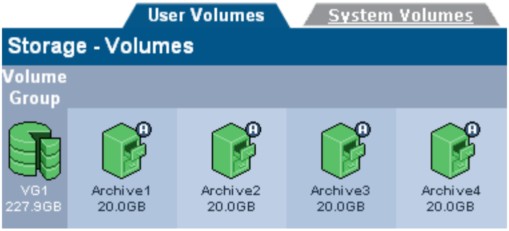
Note: If the close media process fails for any reason the archive remains read-only to avoid unwanted files to be written to the media set. Select 'cancel' close media' to cancel the closing process and make the archive writable.

Removing a Volume

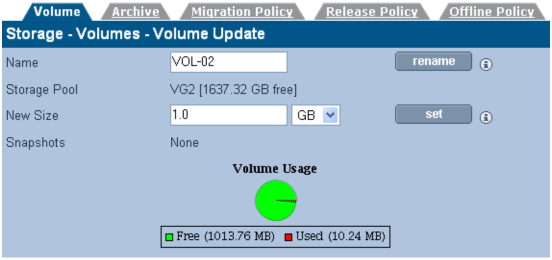
> *Warning: The Archive Appliance enforces strict rules regarding the removal of an archive, as it is a permanent repository of files. These rules affect media management, audit information and system information backup.*
>
> *To cleaning and successfully remove an archive please contact the Appliance support team.*

To remove a volume:

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



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



Storage - Volumes - Volume Update

Name	VOL-02
Storage Pool	VG2 [1637.32 GB free]
New Size	1.0 GB
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.

Special consideration for “Bulk migration”

Migration of legacy data to the Archive Appliance typically involves a large number of files (> 1million files) and large data volumes (> 1TB). In order to ensure an efficient and reliable migration we strongly recommend that a resume copy process is used and that the guidelines below are followed.

Release after migration

Files can be optionally release from the RAID cache after they have been successfully migrated to optical media. This is recommended if the customer does not require legacy files to be kept online. By releasing immediately the file system will never fill-up causing potential disruption during bulk migration.

At least 2 UDO drives for writing

In order to minimize the migration time it is strongly recommend to make at least two UDO drives available for migration (i.e. do not reserve UDO drive for recall in a two drive configuration).

Separate archives for legacy and current files

In order to facilitate the media management process we strongly recommend that the legacy data is migrated to a separate archive from the more recently created file sets. This facilitates media management and also allows the configuration of the appropriate migration policy.

Large number of archives (> 3)

When the number of total archive pools (i.e. total number of copies) exceeds the number available UDO drives for writing, minimising media swapping because the primary tuning consideration. We strongly recommend that the migration jobs are increased to a minimum migration size to 4608 MB for the duration of the legacy data migration process.

Migration throughput

Migration performance is heavily dependent on the size of the files to be migrated. For small files (< 50k) the migration performance between 2-5MB/sec. For large files (> 1MB) the expected migration speed is between 10-15MB/sec.

Providing the RAID cache is larger than the amount of data to be migrated or the "Release immediately" is set the RAID should always have free space. However, in some rare circumstances the cache file system will fill up, causing an " disk full" error. This will occur under the following circumstances:

1. RAID is very small (< 40GB free space)
2 Migration is running out of spare media
3 Too many library or drive errors
4 Files are large (> 500kB)
5 < 3 UDO drives available for writing

Note that the average write speed across 3 UDO drives is approximately 12MB/sec. For small to medium size files the RAID write speed is approximately the same. So providing a reasonable cache (> 100GB) is available for migration, the RAID cache should never fill.

To avoid any issue it is strongly recommended to utilize migration software that can recover from write errors and can deal with the disk full condition.

Migration configuration parameters

For the purpose of bulk migration the migration configuration parameters should be set in such a way to optimize the migration job size to approximately 4 GB.

For minimum constraints to trigger migration ALL minimum constraints must be true.

For maximum constraints to trigger migration ONLY ONE maximum constraint must be true.

Minimum migration constraints

In the case of bulk migration the minimum migration constraints will not all take effect as the "Minimum Wait Time" is not likely to be exceeded.

Minimum File Age (10 seconds)

Files will age once they are copied onto the archive but

Minimum Wait Time (20 seconds)

In the case of bulk migration the file system is constantly updated, so elapsed time since last file system update is not relevant.

Minimum Number of Migration Files (1 file)

This value should only be increased if the customer wants to force a "Maximum Wait Time" to be triggered for < n number of files. Not relevant for bulk migration.

Minimum Migration Size (2 MB)

Small migration jobs are not efficient to process, so the default value should not be decreased. Increase this value to force a minimum migration size.

Maximum migration constraints

Maximum Wait Time (30 minutes)

This parameter does not require changing when considering bulk migration, because within a 30 minute period the amount of data written will always exceed 1GB.

Maximum Number of Migration Files (10,000 files)

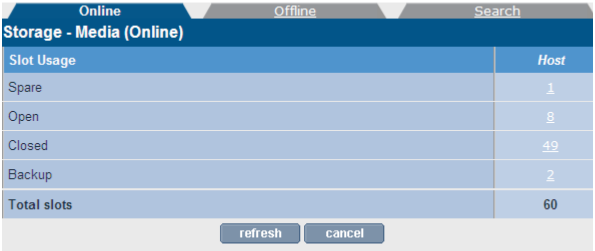
If the average file size is small (i.e. < 50kB) it would make sense to increase this migration parameter to allow a migration job size of 1GB. So in the case of 50k files the "Maximum Number of Migration Files" should be set to at least 20,000.

Max Migration Size (4608 MB)

This parameter does not require changing. The recommended range is between 1 and 5GB.

Media

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



Storage - Media (Online)

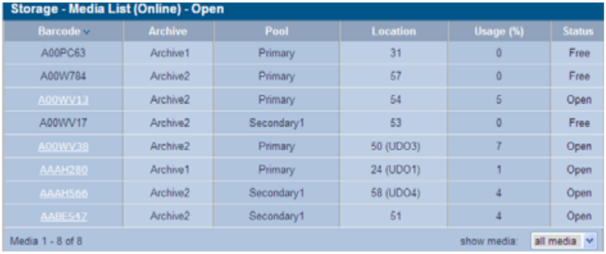
Slot Usage	Host
Spare	1
Open	8
Closed	49
Backup	2
Total slots	60

- **Slot Usage** will always display Spare, Open, Closed and Backup media, as well as the Total Slots count. Other options will be displayed if there is an error. Slot Usage may be one of:
  - **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. Alliance recommends that two pieces of backup media are kept in the Archive Appliance at all times.
  - **Suspected Dirty** - Media with errors that are suspected of being dirty by the system. Media suspected as dirty should be cleaned. To remove dirty media select all affected for offline and remove from library (*Cleaning Media* on page 202)
  - **Has Errors** - If the Archive Appliance scans the media and encounters a volume that was unexpected (i.e. media has been manually moved from it's original slot within the Archive Appliance or media from another Archive Appliance

is
introduced into the library) the media will have the **Has Errors**.

  - **Needs recovery** - Media is in this state prior to being re-synchronized during a system recovery.
  - **Failed to initialize** - Media in the Archive Appliance that have failed to initialize. Media in this state does not contain any useful file information and can be safely removed from the Archive Appliance using the keypad interface.
  - **Failed to unlock** - Media in the Archive Appliance which are protected by UDO Guard and cannot be unlocked.
  - **Unreadable barcode** - Media barcode could not be read due to missing/damaged barcode or barcode reader is faulty/misaligned.
  - **Initializing -** Media is being assigned from the spare pool to a partition pool.
  - **Read-only -** A write error has been detected on a medium. Media can only be used for reading and recovery and should be replaced.
  - **In wrong library -** If media has been added to the wrong library when the system is in a “Pool-per-library” configuration mode.
- **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 List (Online) - Open

Barcode ⌄	Archive	Pool	Location	Usage (%)	Status
A00PC63	Archive1	Primary	31	0	Free
A00W784	Archive2	Primary	57	0	Free
A00WV13	Archive2	Primary	54	5	Open
A00WV17	Archive2	Secondary1	53	0	Free
A00WV38	Archive2	Primary	50 (UDO3)	7	Open
AAAH280	Archive1	Primary	24 (UDO1)	1	Open
AAAH566	Archive2	Secondary1	58 (UDO4)	4	Open
AABE547	Archive2	Secondary1	51	4	Open

Media 1 - 8 of 8

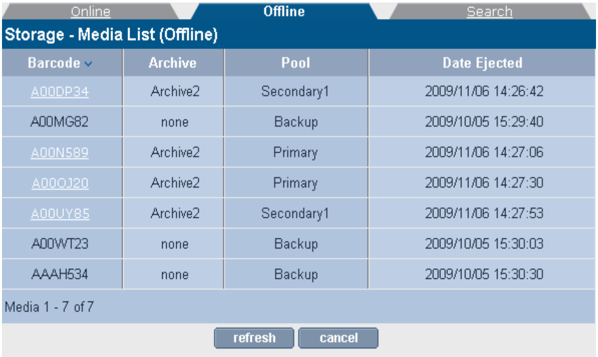
Not all the fields listed below are relevant to all media types and therefore may not be displayed on all online media inventory pages:

- **Barcode** - The media barcode
- **Archive** - The Archive which the media is assigned to

- **Pool** - The media pool that the media belongs to
- **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
- **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
  - **Read-only** - Media has suffered a read/write failure in two or more drives
  - **Not available** - Media identity cannot be verified
  - **Dirty** - media requires cleaning (*Cleaning Media* on page 202)
  - **Recovery** - Media is marked recovery prior to being re-synchronized during a system recovery
  - **Unknown** - Media has not yet been scanned and identified by the Archive Appliance (usually following insertion)
  - **Duplicated** - Media bears a duplicate barcode sticker to another media in the Archive Appliance's inventory.

Offline Media

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



Storage - Media List (Offline)

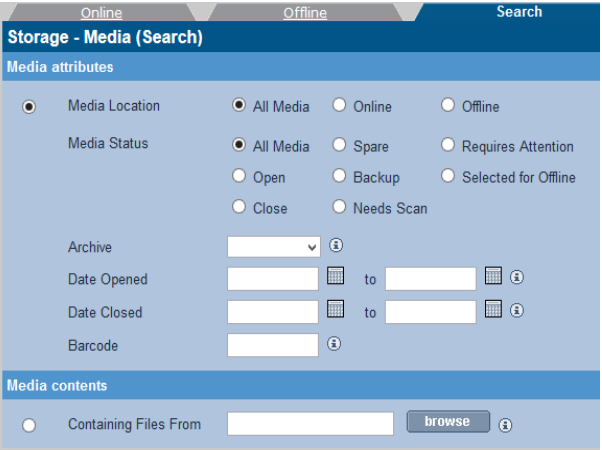
Barcode	Archive	Pool	Date Ejected
A00DP34	Archive2	Secondary1	2009/11/06 14:26:42
A00MG82	none	Backup	2009/10/05 15:29:40
A00N589	Archive2	Primary	2009/11/06 14:27:06
A00OJ20	Archive2	Primary	2009/11/06 14:27:30
A00UY85	Archive2	Secondary1	2009/11/06 14:27:53
A00WT23	none	Backup	2009/10/05 15:30:03
AAAH534	none	Backup	2009/10/05 15:30:30

Media 1 - 7 of 7

- **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.
- **Date 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.

Search Media

The **Storage - Media (Search)** page provide a search interface for locating media using media attributes. Broadly speaking, media can be located using media status information or media content.



Storage - Media (Search)

Media attributes

●	Media Location	● All Media	○ Online	○ Offline
	Media Status	● All Media	○ Spare	○ Requires Attention
		○ Open	○ Backup	○ Selected for Offline
		○ Close	○ Needs Scan	
	Archive			
	Date Opened		to	
	Date Closed		to	
	Barcode			

Media contents

○ Containing Files From [browse]

Media Attributes - criteria associated with media

- **Media Location**
  - **All Media** - media inside (online) and outside (offline) the library.
  - **Offline -** media that have been taken out of the library.
  - **Online -** media that is still in the library.
- **Media status**
  - **All Media -** do not filter on status.
  - **Spare -** unformatted media not assigned to any media pool.
  - **Requires attention -** something is wrong with this media e.g. media is dirty and needs to be cleaned (*Cleaning Media* on page 202).
  - **Open -** has files migrated to them.
  - **Backup -** Re-writable backup media.
  - **Selected for Offline -** this will show media selected for offline, but have not been removed from the library yet.

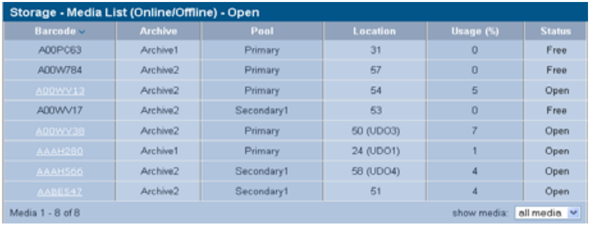
  - **Closed -** media that has been filled and can no longer be written to.
  - **Needs scan -** Media that has not been successfully scanned. Media can always be scanned.
- **Archive -** in the case of multiple archives the media specific to a given archive can be searched.
- **Date opened -**
  - **From date -** start date of open media date range. Empty from date will mean the “beginning of time”.
  - **To date -** end date of open media date range. Empty to date means “today”.
- **Date closed**
  - **From date -** start date of close media date range. Empty “from date” will mean the “beginning of time”
  - **To date -** end date of close media date range. Empty “to date” means “today”
- **Barcode -** enter barcode or wildcard expression of the required barcoded media. For example, “*a*” will locate all media which have the letter ‘a’ in the barcode.

Containing files from - Search for media containing files which are located below the specified folder.

  - **browse** - this button allows existing (i.e. not deleted) file/ folder to be located.

All search criteria can be cleared by clicking the reset button.

Once the criteria has been specified, the search can be started by clicking the search button..



Storage - Media List (Online/Offline) - Open

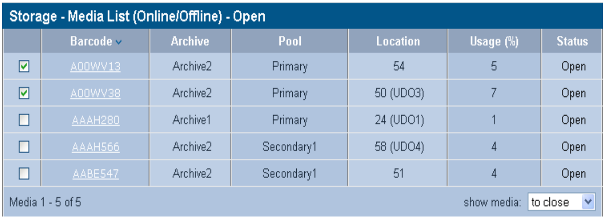
Barcode	Archive	Pool	Location	Usage (%)	Status
A00PC63	Archive1	Primary	31	0	Free
A00W784	Archive2	Primary	57	0	Free
A00WV13	Archive2	Primary	54	5	Open
A00WV17	Archive2	Secondary1	53	0	Free
A00WV38	Archive2	Primary	50 (UDO3)	7	Open
AAAH280	Archive1	Primary	24 (UDO1)	1	Open
AAAH566	Archive2	Secondary1	58 (UDO4)	4	Open
AABE547	Archive2	Secondary1	51	4	Open

Media 1 - 8 of 8

The “show media” drop down control subsets the search result list into available media that the actions can be applied to. When selecting the actions only the media are listed which apply to the action. The following actions are available:

- **to close** - show media that are currently open and are available to be closed.
- **to scan** - show all media that can be rescanned.
- **to select for offline** - show all media that are candidates for offline.
- **to deselect for offline** - show all media that have been selected for offline.

Once one of the above actions has been picked, the relevant media are then available for selection.



Storage - Media List (Online/Offline) - Open

	Barcode	Archive	Pool	Location	Usage (%)	Status
☑	A00WV13	Archive2	Primary	54	5	Open
☑	A00WV38	Archive2	Primary	50 (UDO3)	7	Open
□	AAAH280	Archive1	Primary	24 (UDO1)	1	Open
□	AAAH566	Archive2	Secondary1	58 (UDO4)	4	Open
□	AABE547	Archive2	Secondary1	51	4	Open

Media 1 - 5 of 5 show media: to close

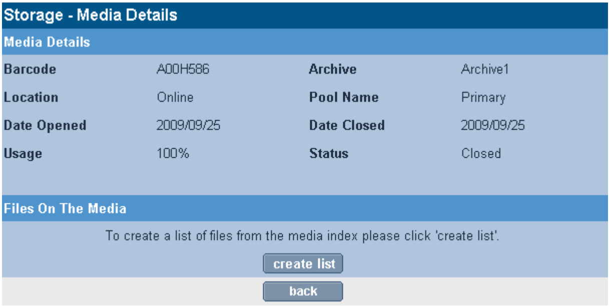
In the example above media available for closing are displayed and the first two media have be selected for closing (indicated by the checkbox).

Note: Media selected for offline can be removed through the keypad interface (see Offlining open media using the Keypad interface on page 227.)

Note: Media cannot be offlined if a system backup has not been successfully complete since it was closed. This is to ensure that system recovery from backup includes all the correct media information and does not miss offline media.

Storage - Media Details

Barcode labels are linked to the Media details page.



Storage - Media Details

Media Details

Barcode	A00H586	**Archive**	Archive1
Location	Online	**Pool Name**	Primary
Date Opened	2009/09/25	**Date Closed**	2009/09/25
Usage	100%	**Status**	Closed

Files On The Media

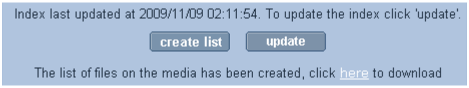
To create a list of files from the media index please click 'create list'.

Media details are available for open and closed media but not for backup or spare media. The details provided are:

- **Barcode** - The barcode of the media shared by A and B side.
- **Archive** - The Archive which the media is assigned to.
- **Location** - Online/Offline
- **Pool Name** - The media pool that the media belongs to.
- **Date Opened** - The date the media was initialised into the pool.
- **Date Closed** - The date the media was closed.
- **Usage** - Percentage of storage on media used by file or meta data.
- **Status** - Media's open/closed status.

Note: It may be to have a percent utilization greater than zero without any data files appearing on the media. This would be due to meta data migration e.g. file rename, ACL changes and file delete events being archived without any file data.

The media detail page also provides the interface for extracting a file inventory for a that media (side A and B). By pressing create list the media inventory list will be generated and prepared for download. Once the media list is available for download a hyperlink will appear:



Index last updated at 2009/11/09 02:11:54. To update the index click 'update'.

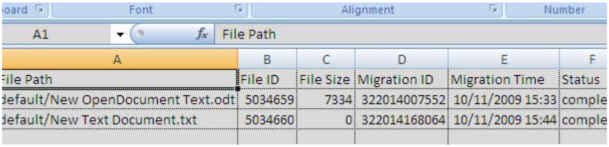
The list of files on the media has been created, click here to download

When selecting the hyperlink the .csv (Comma Separated Value) file will be automatically downloaded. This file can be loaded into any spreadsheet application for further analysis.

The inventory details are updated every night and do not need to be updated for closed media as the content no longer changes. However, the media contents may change for open media since the last update was performed. Note that the last update time is shown above the update button. If the inventory is believed to be out of date, press this button and the inventory will be regenerated as a background task, otherwise press the “create list” to generate the CSV file.

Note: .Only one list can be created at any given time. Attempts to create lists concurrently will simple be blocked until the previous “create list” operation has been completed.

A sample media inventory file is shown below.:



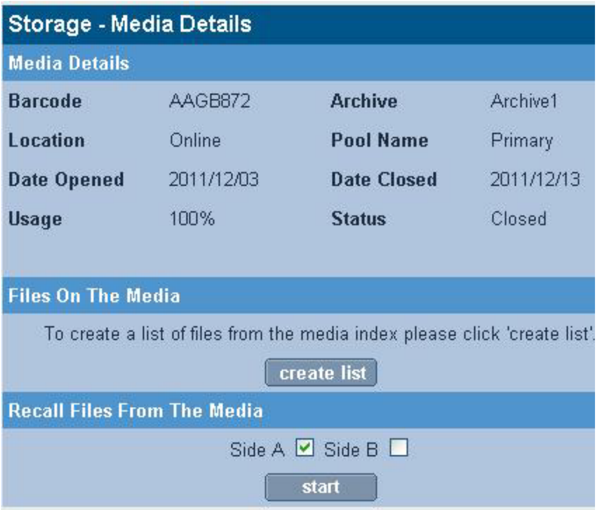
A1 File Path

	A	B	C	D	E	F
	ile Path	File ID	File Size	Migration ID	Migration Time	Status
	default/New OpenDocument Text.odt	5034659	7334	322014007552	10/11/2009 15:33	comple
	default/New Text Document.txt	5034660	0	322014168064	10/11/2009 15:44	comple

Recall all files from a single media (or single media side)

If it is necessary to return all the files of a specific medium to the RAID cache it is possible to do so using the recall interface on the media details page.

The media side(s) to be recalled can be selected.



Storage - Media Details

Media Details

Barcode	AAGB872	Archive	Archive1
Location	Online	Pool Name	Primary
Date Opened	2011/12/03	Date Closed	2011/12/13
Usage	100%	Status	Closed

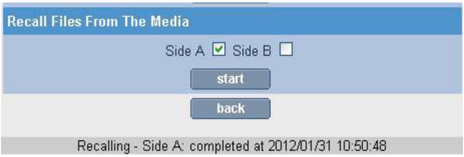
Files On The Media

To create a list of files from the media index please click 'create list'.

Recall Files From The Media

Side A ☑ Side B □

Once the side(s) has/have been selected the recall is started by pressing the start button. When the recall is completed a message will be displayed as shown above,



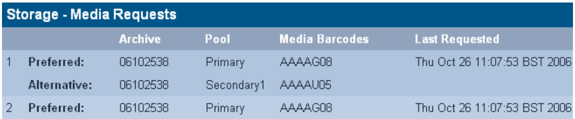
Recall Files From The Media

Side A ☑ Side B □

Recalling - Side A: completed at 2012/01/31 10:50:48

Warning: Split files (i.e. files that are split across two pieces of media) will be excluded from recall.Media Request

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

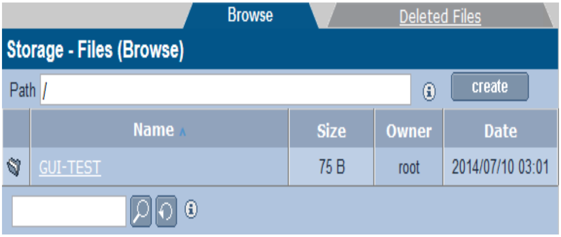
- **Preferred** and/or **Alternative** - indicates the preferred copy to be returned and if that is not available, an alternative copy.
- **Archive** - The archive the media is part of
- **Pool** - The pool (within the archive) which the media is part of
- **Media Barcode** - The barcode of the offline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

Files

The **Storage - Files** page enables searching or browsing through the archive directory structure and view all file/folder details.

Browsing files

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



Storage - Files (Browse)

Path /

	Name	Size	Owner	Date
	GUI-TEST	75 B	root	2014/07/10 03:01

2. Enter a search string in the text box and click 🔍. Partial string match are valid and will be matched. For example, when entering the search string “15” a valid match would be “minutes-version15.doc”

> *Note: This function only searches the currently visible folder.*

3. Click ↺ to clear the content of the text box.
   Alternatively, manually browse the directory tree for a file.

Navigate the RAID cache file system by clicking the folders on the browse tab or entering the required path into the “Path” edit control.

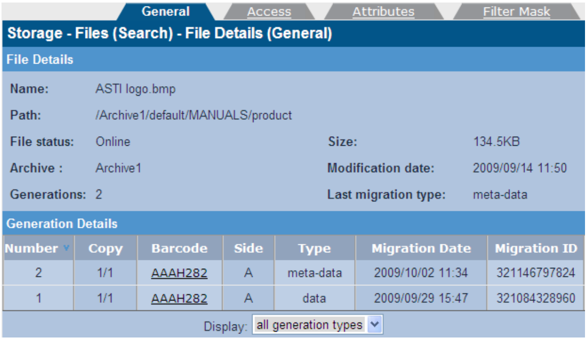
Folders can be created from the interface by entering the desired path and folder name and selecting the create button.

Displaying file/folder details

Files and folders are file system objects which have descriptive information associated with them. Some information are generic file/folder information but there are also archive specific information available.

General

Meta information relating to file migration status and history are available in the General tab:.



Storage - Files (Search) - File Details (General)

File Details

Name:	ASTI logo.bmp		
Path:	/Archive1/default/MANUALS/product		
File status:	Online	**Size:**	134.5KB
Archive :	Archive1	**Modification date:**	2009/09/14 11:50
Generations:	2	**Last migration type:**	meta-data

Generation Details

Number	Copy	Barcode	Side	Type	Migration Date	Migration ID
2	1/1	AAAH282	A	meta-data	2009/10/02 11:34	321146797824
1	1/1	AAAH282	A	data	2009/09/29 15:47	321084328960

Display: all generation types

File Details

File details represent all the file information relevant to the archiving status of the file.

- **File status** - Access status of file: Online/Offline/Nearline/Dirty/ Excluded status.
  - **Online -** File is on the RAID given fast read performance
  - **Offline -** Media of file has been removed from library
  - **Nearline -** File is not on RAID but is located on media which is still in the library
  - **Dirty -** File has not been migrated yet. Not to be confused with physical dirty/dust.
  - **Excluded -** File or parent folder has been explicitly excluded via migration exclusion list.
- **Archive -** Name of archive this file/folder is stored in.
- **Generations** - Number of modifications. The first generation is the initial file create. A generation may not always be a file content change but could be a meta-data modification (e.g. rename or permission change).
- **Size** - Size of the data
- **Modification Date** - Last time this file was modified.
- **Last Migration Type** - Last migration type: *metadata* or *data*. Metadata changes include file rename and ACL changes.

Generation Details

Each file system modification migrated to UDO is recorded in the Generation details table.

- **Generation Details -** Migration detail table which is ordered by migration number. The most recent migration is shown first with the highest generation number.

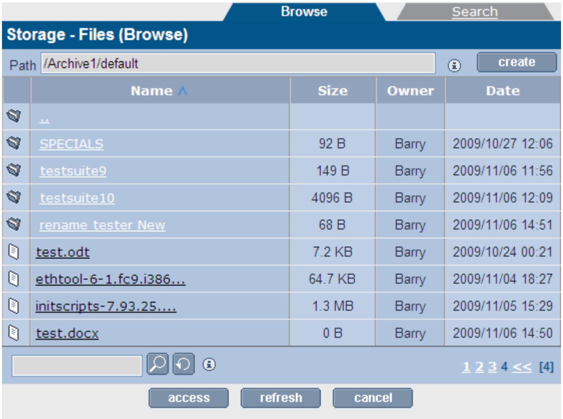
  - **Number** - Sequence number of this migration event. Number "1" is the first migration event.
  - **Copy** - Copy identifier. "1/1" is copy one of a total of one copy while "1/2" is the first copy of a total of two copies.
  - **Barcode** - The barcode label of the media which contains this copy of the file.
  - **Side** - The media side which contains this copy of the file
  - **Type** - *Metadata* or *Data*. Metadata changes include file rename and ACL changes.
  - **Migration Date** - The date this change was migrated to UDO media.
  - **Migration ID** - The migration ID identifies the migration job which wrote the file to UDO. Migration IDs are useful for auditing the the archive process.

Setting or modifying an ACL

Clicking on a file or folder will open the **Storage - Files - Access (Access)** page. From there the access privileges, known as Access Control Lists or ACLs, Groups and Users 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 - Files**.



Browse | Search

Storage - Files (Browse)

Path /Archive1/default create

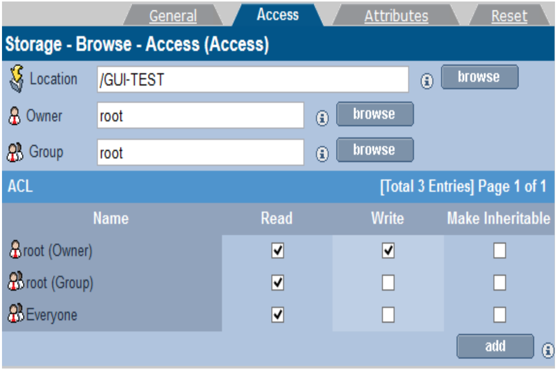
	Name ^	Size	Owner	Date
	..			
	SPECIALS	92 B	Barry	2009/10/27 12:06
	testsuite9	149 B	Barry	2009/11/06 11:56
	testsuite10	4096 B	Barry	2009/11/06 12:09
	rename tester New	68 B	Barry	2009/11/06 14:51
	test.odt	7.2 KB	Barry	2009/10/24 00:21
	ethtool-6-1.fc9.i386...	64.7 KB	Barry	2009/11/04 18:27
	initscripts-7.93.25....	1.3 MB	Barry	2009/11/05 15:29
	test.docx	0 B	Barry	2009/11/06 14:50

1 2 3 4 << [4]

access refresh cancel

2. Search or browse to a folder or file.

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



General | Access | Attributes | Reset

Storage - Browse - Access (Access)

Location /GUI-TEST browse

Owner root browse

Group root browse

ACL [Total 3 Entries] Page 1 of 1

Name	Read	Write	Make Inheritable
root (Owner)	☑	☑	□
root (Group)	☑	□	□
Everyone	☑	□	□

add

From this page:

- View the current **Location**.

  Click browse to browse to another directory

- View the folders's **Owner** and **Owner Group**.

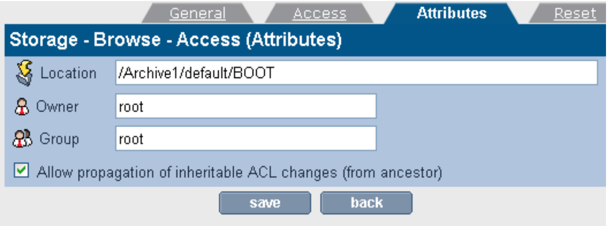
  Click browse to browse for another owner or owner group
- Set or view **ACL** - This section lists the users and groups who have access to the directory and their access privileges.

3. Click add to add more users or groups.

File/Folder Attributes

The file folder attributes include: full path, owner and owner group of file system object, option of allow/disallow propagation of ACLs from parent folder and DOS file system attributes.

1. Click the **Attributes** tab



Storage - Browse - Access (Attributes)

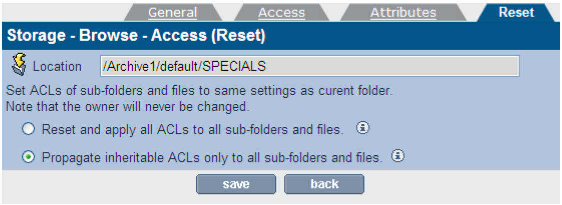
Location	/Archive1/default/BOOT
Owner	root
Group	root

☑ Allow propagation of inheritable ACL changes (from ancestor)

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

2. Click the **Reset** tab (applicable for folders only).



Storage - Browse - Access (Reset)

Location: /Archive1/default/SPECIALS

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 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. It will NOT reset existing ACLs.

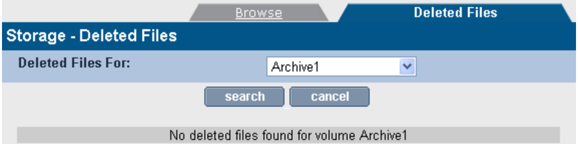
Note: On systems with large numbers of files, this operation may take an extended period of time to complete.

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

Searching files

At present the only criteria for searching files is the deleted status. However, in the future enhancements are planned to search the File System Catalog (FSC) using other attributes.

A selected archive can be searched to produce a downloadable file containing all deleted files. Once the search button has been clicked a progress bar will appear to indicated the status of the search. The user may want to return to the interface as a later date to download the result, as the search may take some time. The duration of the search will depend on the number of files in the File System Catalog (FSC).



Storage - Deleted Files

Deleted Files For: Archive1

No deleted files found for volume Archive1

Once the search has completed the search results file is available for download.

Chapter 6

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

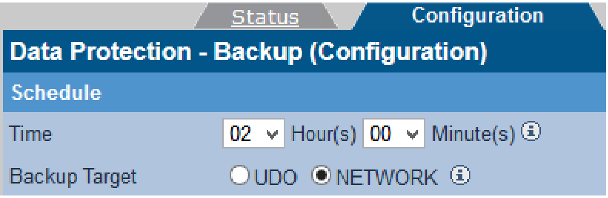
System and configuration data may be backed up either to RW UDO media stored in the Archive Appliance, or across the network to a remote location.

Backups significantly increase the speed of a data recovery in the event that the system fails. Even without a backup the data can still be recovered but will take significantly longer.

> *Note: Key protection and system backup share the network backup target. Only CIFS network shares can be used if the encryption keys are to be protected locally. The alternative is to protect the keys in the cloud.*

Creating a Backup schedule

1. From the menu bar, select **Data Protection - Backup**.
2. The **Data Protection - Backup (Status)** page is displayed.
3. Click the **Configuration** tab. The **Data Protection - Backup (Configuration)** page is displayed:



Data Protection - Backup (Configuration)

Schedule

Time 02 Hour(s) 00 Minute(s)

Backup Target ○ UDO ● NETWORK

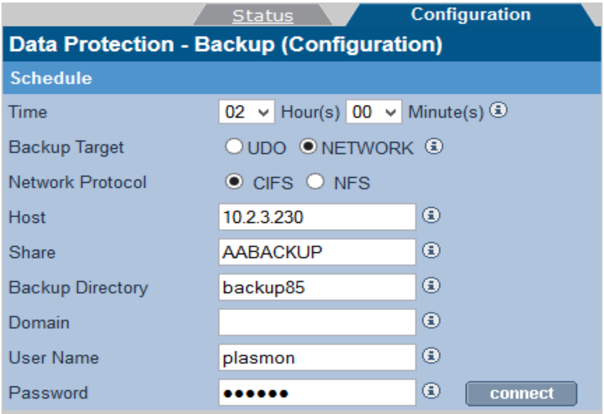
4. Select a time using the drop-down boxes. The backup will take place at this time every day.
5. To back up the RW UDO Media, click the **UDO** radio button and ensure that a piece of RW UDO Media is loaded into the Archive

Appliance as backup media - see *Adding Backup UDO media via the mailslot* - page 197.

6. To back up across the network, click the **NETWORK** radio button.
7. The Archive Appliance is capable of backing up across either CIFS or NFS Select the radio button appropriate to the protocol that is to be used.

Network Backup using CIFS

Click the CIFS radio button if the remote location is a Windows Share or a network device configured to appear as a Windows Share (e.g. a Linux server using Samba). The CIFS configuration page appears:



Data Protection - Backup (Configuration)

Schedule

Time	02 Hour(s) 00 Minute(s)
Backup Target	○ UDO ● NETWORK
Network Protocol	● CIFS ○ NFS
Host	10.2.3.230
Share	AABACKUP
Backup Directory	backup85
Domain	
User Name	plasmon
Password	●●●●●●

1. Enter the IP address or hostname of the remote backup location in the **Host** field. This must be a location which is accessible to the Archive Appliance across the network, and which has been configured to accept the connection (such as setting up a share, creating a user for the Archive Appliance to connect as, and configuring the correct permissions).
   The hostname may be the Fully Qualified Domain Name, or simply the hostname if the remote host is in the same Domain as the Archive Appliance.
2. Enter the name of the **Share** to which the backup is to be written.
3. Supply the **Backup Directory** within the Share. When using multiple Archive Appliances, each Archive Appliance should be

assigned a dedicated backup directory to ensure that backup files from one Archive Appliance are not overwritten by the backup files of another.

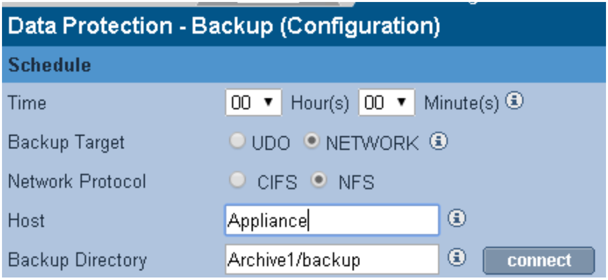
4. If the authenticated user is a domain user, the fully qualified domain name needs to be specified (e.g. eng.astiusa.com)
5. Provide a **User Name** with Read, Write, Delete and Rename permissions. This should be a user local to the server hosting the share, not to the Archive Appliance.

Note: Usernames should be entered in the format <domain-name>/<username> e.g. **UK/phill**

6. Enter that user's **Password**.
7. Click the **connect** button to test the connection to the remote network location and ensure the supplied details are correct.
8. Click **save**.

Network Backup using NFS

Click the NFS radio button if the remote location is an NFS share, such as a Novell server. The NFS configuration page appears:



Data Protection - Backup (Configuration)

Schedule

Time	00 ▼ Hour(s) 00 ▼ Minute(s) ⓘ
Backup Target	○ UDO ● NETWORK ⓘ
Network Protocol	○ CIFS ● NFS
Host	Appliance ⓘ
Backup Directory	Archive1/backup ⓘ connect

1. Enter the IP address or hostname of the remote backup location in the **Host** field. This must be a location which is accessible to the Archive Appliance across the network, and which has been configured to accept the connection (such as setting up a share, creating a user for the Archive Appliance to connect as, and configuring Read, Write, Delete and Rename permissions).

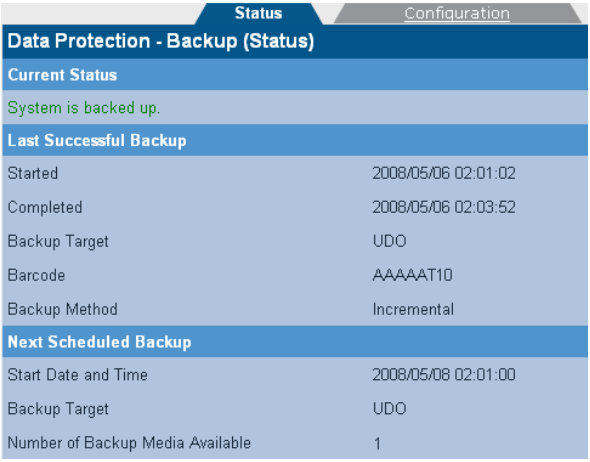
Note: Ensure that the **no_root_squash** *attribute is set on the NFS server.*

2. Supply the path to the **Backup Directory**. When using multiple Archive Appliances, each Archive Appliance should be assigned a dedicated backup directory to ensure that backup files from one Appliance are not overwritten by the backup files of another.
3. Click the **connect** button to ensure the supplied details are correct.
4. Click **save**.

Note: Clicking the ***connect*** *button does not establish a permanent connection to the remote backup location.*

Monitor the backups

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



Data Protection - Backup (Status)

Current Status	
System is backed up.	
Last Successful Backup	
Started	2008/05/06 02:01:02
Completed	2008/05/06 02:03:52
Backup Target	UDO
Barcode	AAAAAT10
Backup Method	Incremental
Next Scheduled Backup	
Start Date and Time	2008/05/08 02:01:00
Backup Target	UDO
Number of Backup Media Available	1

2. The following information is displayed:
   - **Current Status** - The backup status of the Archive Appliance. If there is an error preventing backup, it will be presented here.
   - **Last Successful Backup** - The time and date that the last successful backup started and completed, along with the target (UDO or Network) and information relevant to the target (Barcode for UDO media, remote target for Network backups, Incremental or Full backup).
   - **Next Scheduled Backup** - The date, time and target for the next scheduled backup. This section also displays the number of backup media available.

Note: The number of backup media is not displayed if Network Backup is configured.

Perform an unscheduled backup

1. From the menu bar, select **Data Protection - Backup**.
2. Click **start**. A backup will begin immediately.

File Recovery

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

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

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

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

In the rare event that a full recovery from media is required, be sure to configure any cloud provider account which may have existed prior to the disaster.

> *Warning: If encryption was previously used it will be necessary to configure the key backup storage and perform a full key recovery.*

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

- **Full 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 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 90*

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
- Re-synchronize the FSC database to reflect changes on media since the backup was made
- Delete existing file systems then rebuild them using the re-synchronised 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 Archive 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 necessary to reconfigure the list of local users on the Archive Appliance. (see *page 53*).

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 Archive Appliance performs the following steps:

- Restore archive's FSC from backup or media
- If restored from backup, re-synchronize 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 Alliance 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 Alliance Technical Support for further information on how to check an archive's FSC.*

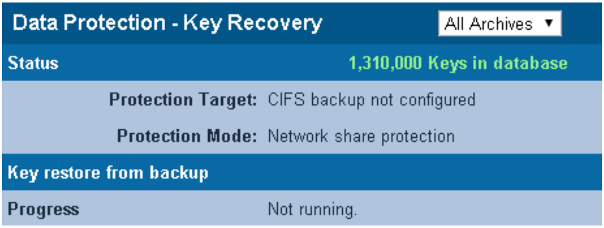
RMDB only

Recover only the Resource Manager Database (RMDB). For AAE, there is no RMDB recovery option available.

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

Key Recovery

Key recovery may be required if the keystore has been corrupted as a result of a power failure or some other system failure. The Key Management system has been designed to detect and automatically repair many corruption scenarios. Key recovery is the last fall back recovery method.



Data Protection - Key Recovery

All Archives ▼

Status	1,310,000 Keys in database
Protection Target:	CIFS backup not configured
Protection Mode:	Network share protection
Key restore from backup	
Progress	Not running.

Before the recovery process is started all the pre-conditions are checked to ensure a successful recovery. The pre-conditions are:

1. Encryption is licensed
2. Protection Mode is selected
3. Protection storage is configured
4. Existing keystore is consistent or empty

A message will usually appear to indicate that a recovery is required or that the key database is not consistent. This means a recovery needs to be performed.

In the example above the “Protection Mode” has been set to Network protection, however, the network backup target has not been configured yet. So, in this case, to perform the key recovery it is necessary to configure the CIFS backup to the correct share.

The option is available to restore all keystore database or just the keys for one specific archive.

Note: Key recovery only recovers missing keys. If keys already exist in the key database, these existing keys will not be recovered.

Replication

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

Before beginning, ensure that available volumes are present on both the source and target Archive Appliances. Alliance recommends that the source and target volumes are the same size.

For information on creating volumes, see *Creating an archive* on page 76.

Ensure that the target Archive Appliance has a user with Replication rights. See *Adding a User* on page 54.

Note: Files that are moved or deleted on the source volume after replication has occurred are not moved on or deleted from the target volume. Thus it is possible to utilize more space on the Passive volume than is in use on the Active 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.

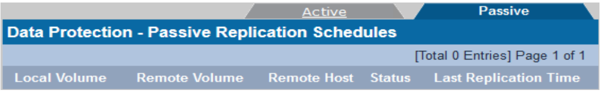
> *Important: It is necessary to configure the replication target (Passive) volume before attempting to configure the source (Active) volume.*

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

Creating the Passive schedule

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

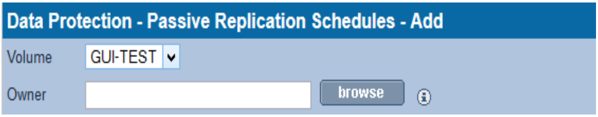


Data Protection - Passive Replication Schedules

[Total 0 Entries] Page 1 of 1

Local Volume	Remote Volume	Remote Host	Status	Last Replication Time

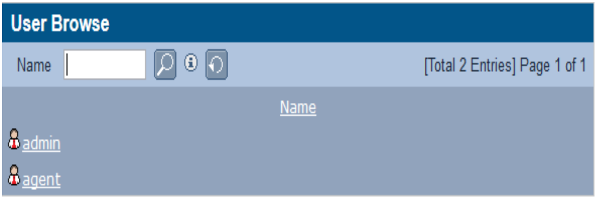
2. Click **add** to open the **Data Protection - Passive Replication Schedules - Add** page:



Data Protection - Passive Replication Schedules - Add

Volume	GUI-TEST
Owner	

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



User Browse

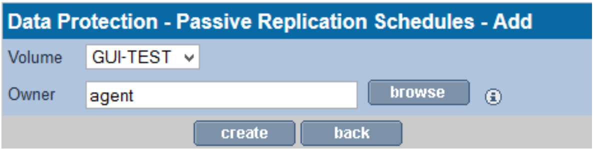
Name [Total 2 Entries] Page 1 of 1

Name

admin

agent

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



Data Protection - Passive Replication Schedules - Add

Volume: GUI-TEST

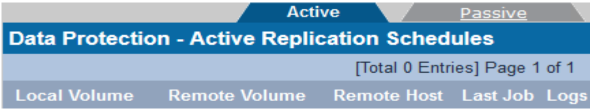
Owner: agent

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.

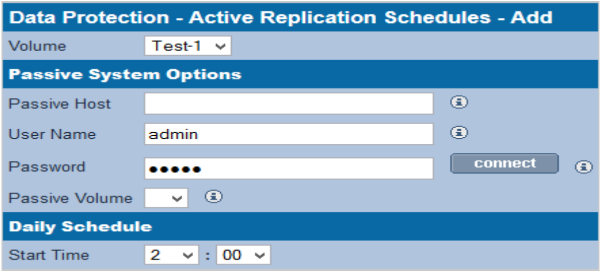


Data Protection - Active Replication Schedules

[Total 0 Entries] Page 1 of 1

Local Volume	Remote Volume	Remote Host	Last Job	Logs

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



Data Protection - Active Replication Schedules - Add

Volume: Test-1

Passive System Options

Passive Host:

User Name: admin

Password: ●●●●●

Passive Volume:

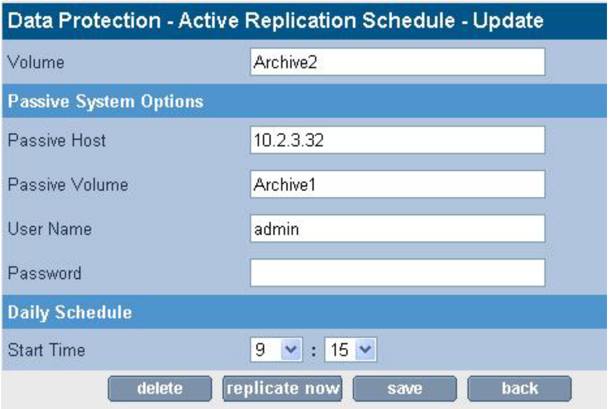
Daily Schedule

Start Time: 2 : 00

3. Select the source volume from the **Volume** drop-down box.
4. Enter the IP address or the Hostname of the target Appliance in the **Passive Host** field.
5. Enter the user name and password for the replication selected in Step 4 on *page 131.*
6. Click **connect**.
7. Select the **Passive Archive** from the drop-down box (which needs to be configured prior to this procedure).
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 Archive Appliance, open the **Data Protection - Replication** page.
2. Click on the Active Replication schedule to be edited:



Data Protection - Active Replication Schedule - Update

Volume	Archive2
Passive System Options	
Passive Host	10.2.3.32
Passive Volume	Archive1
User Name	admin
Password	
Daily Schedule	
Start Time	9 : 15

3. Edit details as required.

> *Note: In previous versions of the AMS software all files created on the passive replica were created by a user specified in the replication details; this is no longer the case and the user name is now only used for authentication. In version 4.20 and higher the owner, owner group and ACLs of each file system object are replicated and preserved.*

4. Click **save**.

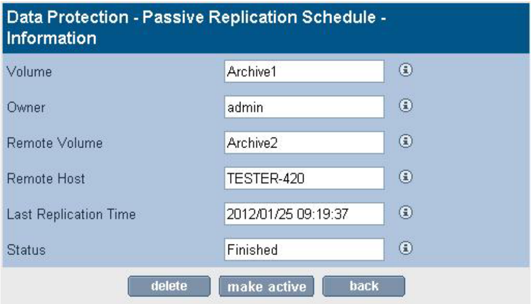
From this page it is also possible to start the replication process immediately instead of waiting for the schedule to run. Simply press *"replicate now"* button to start the replication job. The replication service will also be started if it is not already.

> *Note: Once the 'replicate now' button has been selected the option to perform a full file system scan will be given. For file system with many files (> 10 million) this may take a long time.*

Making the Passive replica active

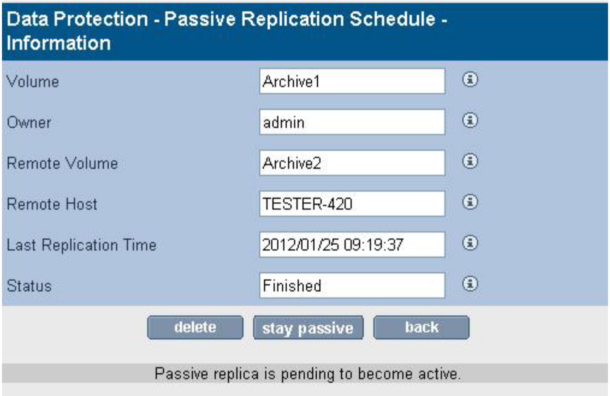
If in the unlikely event the active (primary) Archive Appliance should fail and not be recoverable in an acceptable time frame, it is possible to switch the passive replica into the active (i.e. writable) state.

Select the “Passive” tab and the relevant passive replication schedule. Then simply click the “make active” button and click a second time to confirm the action. The system will now proceed to activate the passive archive and changing it from read-only to writable.



Data Protection - Passive Replication Schedule - Information

Volume	Archive1
Owner	admin
Remote Volume	Archive2
Remote Host	TESTER-420
Last Replication Time	2012/01/25 09:19:37
Status	Finished



Data Protection - Passive Replication Schedule - Information

Volume	Archive1
Owner	admin
Remote Volume	Archive2
Remote Host	TESTER-420
Last Replication Time	2012/01/25 09:19:37
Status	Finished

Passive replica is pending to become active.

Note how the “make active” button changes to “stay passive” allowing the user to reverse the action. The success of the action is also confirmed and the replica is “pending active”. Now the replica is writable and once the failed replica returns, the pending active replica will attempt to synchronize any outstanding files that may have been written before the failure. Once this is completed the “pending active” state will change to “active”.

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

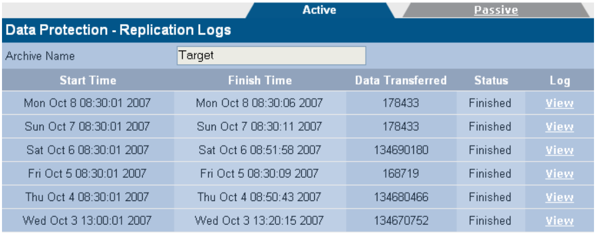
1. On the target Appliance, open the **Data Protection - Replication** page.
2. Select the **Passive** tab.
3. Click on the name of the local archive to be deleted.
4. Click **delete**. A message is displayed warning that the schedule is about to be deleted.
5. Click **delete** again to confirm deletion.

Note: Deleting a replication schedule does not delete the archive. For further information on deleting archives, see Removing a Volume on page 97.

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:

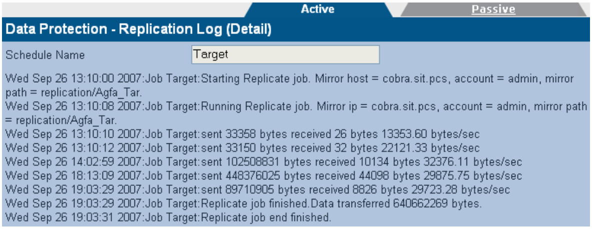


Data Protection - Replication Logs

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

   Start Time indicates the time the replication began.
   Finish Time indicates the time the replication ended.**Data Transferred** is in bytes.
   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.
```

Security

The AMS provides two levels of data protection security to ensure the safe keeping of your data assets.

Encryption – File level data encryption, providing AES-256 bit level data encryption with resilient key management protection. This UI page to used to set the library Master Key and Archive Volume(s) wrapping key for the protection of all file level encryption keys protecting data.

UDOGuard – Disk level protection to ensure that media cannot be read outside of it's host Appliance. UDO Guard is a low-level drive function that protects user data by preventing the drive from spinning up, and therefore reading, the media unless the correct security key is provided in advance.

All security keys are managed through this security interface.

Encryption

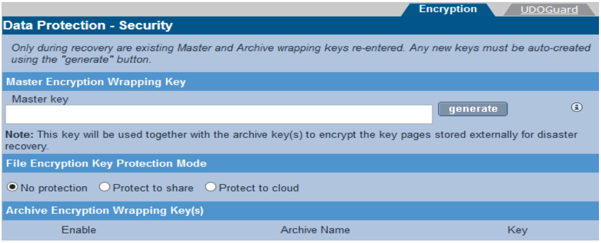
To ensure the protection of file level symmetrical encryption keys, the AMS utilizes symmetrical encryption wrapping keys as recommended by NIST SP 800-57 as well as FIPS 140-2.

The Master key is a system wide key which is used to encrypt using AES-256 bit algorithms, security sensitive information such as file level symmetrical encryption keys. AMS further utilizes a split key approach, where an additional per archive volume encryption key is utilized to further protect data. By utilizing this split key approach, multiple security officers can set specific keys (1 for library, another for each archive), where no one security officer has knowledge of the keys. This technique ensures that no one person could, with the correct knowledge and technical capabilities, decrypt sensitive data assets.

The Encryption tab contains three security parameters:

1. **Master key** - also known as Master Encryption Wrapping Key is a system wide encryption key
2. **Protection mode** - location of per file keys
3. **Archive key** - separate key for each archive

.



Data Protection - Security

Only during recovery are existing Master and Archive wrapping keys re-entered. Any new keys must be auto-created using the "generate" button.

Master Encryption Wrapping Key

Master key

Note: This key will be used together with the archive key(s) to encrypt the key pages stored externally for disaster recovery.

File Encryption Key Protection Mode

● No protection ○ Protect to share ○ Protect to cloud

Archive Encryption Wrapping Key(s)

Enable	Archive Name	Key

To create a Master Key

1. Compliant and valid keys must be created using the **generate** button.

2 Once a key is created, you should “save” the key. Click the **Save** button.

3 You will be presented with a file save dialog, where you should save the key to a secure location to avoid any transcription errors.

Warning: In the event of a DR event, you may be required to re-enter this key. If you do not save this key, or have it available, you will NOT BE ABLE TO ACCESS ANY ENCRYPTED DATA THAT HAS BEEN WRITTEN TO THE ARCHIVE APPLIANCE. IT IS ABSOLUTELY IMPARATIVE THAT YOU SAVE THIS KEY. IT IS RECOMMENDED THAT YOU KEEP AN ELECTRONIC COPY AND A PAPER COPY IN SAFE LOCATIONS THAT ARE RESILIENT IN NATURE.

Warning: Remember that the Master Key is not protected by the system as per NIST Special Publication 800-57 Guidelines and that it is not backed up. It is imperative that you retain a copy for Disaster Recovery events.

4 Confirm the key after setting it. The key is now set.

Setting the Protection Mode

All file level encryption keys are themselves encrypted and written to backup. The backup location can be one of the following locations:

*Note: You must select **Protect to share,** or **Protect to cloud** to enable the encryption.*

1. **Protect to share** – keys written to the FSC backup location network share
2. **Protect to cloud** – keys written to the key cloud provider account (refer to *Cloud Service Configuration* on page 44).

To create Archive Key(s)

1. Compliant and valid keys must be created using the ‘generate’ button.
2. Once a key is created, you should “save” the key. Click the Save button.
3. You will be presented with a file save dialog, where you should save the key to a secure location to avoid any transcription errors.

Warning: In the event of a DR event, you may be required to re-enter this key. If you do not save this key, or have it available, you will NOT BE ABLE TO ACCESS ANY ENCRYPTED DATA THAT HAS BEEN WRITTEN TO THE ARCHIVE APPLIANCE. IT IS ABSOLUTELY IMPARATIVE THAT YOU SAVE THIS KEY. IT IS RECOMMENDED THAT YOU KEEP AN ELECTRONIC COPY AND A PAPER COPY IN SAFE LOCATIONS THAT ARE RESILIENT IN NATURE.

4 Confirm the key after setting it. The key is now set.

5 To enable encryption for that archive, must now click the enable box to the left of the archive name.

Remember that the Master key is not protected by the system and only one copy exists on the appliance. It is NOT backed up!

Important: Make sure your keys are secured and protected!

UDO Guard

The **Data Protection - UDO Guard** page provides access to the configuration of UDO Guard.

The Archive Appliance employs the optional UDO Guard protection to ensure that media cannot be read outside of it's host Appliance. UDO Guard is a low-level drive function that protects user data by preventing the drive from spinning up, and therefore reading, the media unless the correct security key is provided in advance.

When UDO Guard is enabled, the user must provide, in the form of alphanumeric passwords:

- **An Administration Key:** The Administration key is unique to the Appliance and forms one half of the key pair required to lock and unlock the media for any UDO Guard-protected archives in the Appliance.
- **An Archive Key:** The Archive Key must be provided for each protected archive within the Appliance. An Archive Key is unique to an individual archive and forms the second half of the key pair required to lock and unlock the UDO media associated with it.

Once entered, the Administration and Archive Keys may be only changed as long as no media is locked using the key-pair.

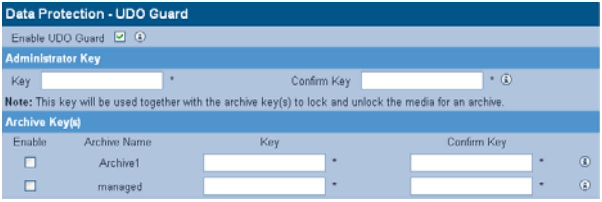
For each archive, the system uses the key pair (Administration Key and Archive Key) to calculate a UDO Guard Key that is unique to that Archive and that Appliance. Once media has been protected using the key-pair, neither the Administration nor Archive Key can be changed. The keys are stored in an encrypted format; the Administration Key in the SSM configuration file and the Archive Keys in the Resource Management Database (RMDB).

> *Warning: Once defined, keys must be noted and retained in a safe place. Loss of either key may prevent access to the media in the event of a recovery from media being required.*

Enabling UDO Guard

1. Open the **Data Protection - UDO Guard** page.

2. If not already enabled, tick the **Enable UDO Guard** checkbox. This displays the UDO Guard options:



Data Protection - UDO Guard

Enable UDO Guard ☑

Administrator Key

Key ________ * Confirm Key ________ *

Note: This key will be used together with the archive key(s) to lock and unlock the media for an archive.

Archive Key(s)

Enable	Archive Name	Key	Confirm Key
☐	Archive1	*	*
☐	managed	*	*

3. To begin using UDO Guard, an **Administrator Key** must be entered. This forms part of the key pair that is required to lock and unlock each Archive, and is unique to the Appliance.

   The key may consist of any characters, up to a maximum of 16. Confirm the key by re-entering it in the **Confirm Key** field.

   Note: Alliance strongly recommend that all keys be human-readable.

4. To enable UDO Guard on an Archive, tick the check box by the Archive's name, and enter a key in the **Key** and **Confirm Key** fields.

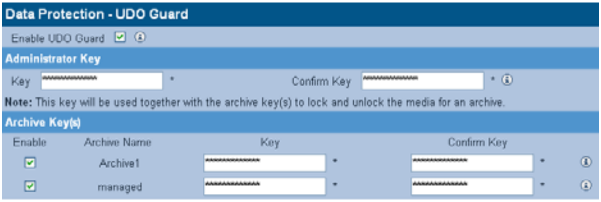
   As with the Administrator Key, the Archive Key may consist of any characters, up to a maximum of 16.

   Important: Each Archive's key must be unique, and cannot match the Administrator Key.

5. Make a note of all supplied keys and store in a safe, secure location.
6. Click **save** to save the keys and enable UDO Guard.

Disabling UDO Guard

1. Open the **Data Protection - UDO Guard** page:



Data Protection - UDO Guard

Enable UDO Guard ☑

Administrator Key

Key ************** * Confirm Key ************** *

Note: This key will be used together with the archive key(s) to lock and unlock the media for an archive.

Archive Key(s)

Enable	Archive Name	Key	Confirm Key
☑	Archive1	************** *	************** *
☑	managed	************** *	************** *

2. Un-tick the checkbox beside the name of the Archive which is to cease using UDO Guard.

Click **save**.

Background recall

The **Data Protection - Background recall** feature allows the configuration and execution of a background recall process which returns file content to the RAID cache from optical media.

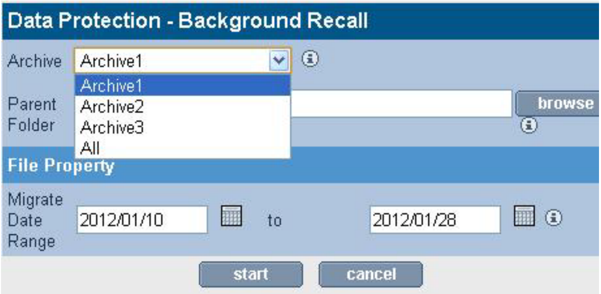
File content is released from the RAID under two circumstances. Firstly, if the RAID is nearly full the Archive Appliance will “release” file content from the cache to free up storage space. Once a file is released it has to be recalled onto the RAID from optical media. Secondly, files will also be released if the RAID file system has been rebuilt.

It is possible to define the files to be recalled by selecting a migration date range and/or a folder hierarchy. Once the recall is started it can be paused or aborted.

The background recall is performed in four stages:

Stage 0: Setup

The background initialization process is configured through the setup page. It is possible to specify the following recall criteria:



Data Protection - Background Recall

Archive: Archive1

Parent Folder:

File Property

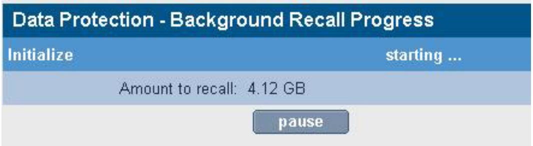
Migrate Date Range: 2012/01/10 to 2012/01/28

- One Archive or all Archives. **Archive** drop down list is not available for AAE.
- Root folder location of files to be recalled
- Date range when files were written to optical

Once the configuration has been completed the background recall (phase 1) can be started by pressing the “start” button.

Stage 1: Initialization

When the background recall starts, it first has to locate all the files that match the criteria specified in the configuration. It has to calculate the total amount of data to recall and the required list of media. Depending on the number of files in the archive this process may take several minutes.



Data Protection - Background Recall Progress

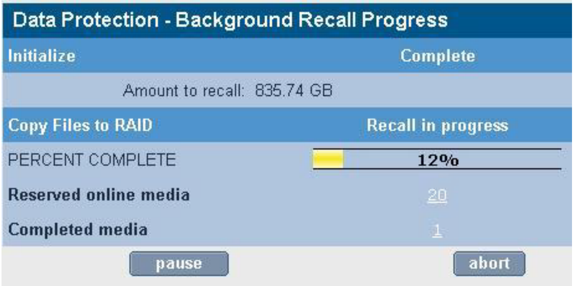
Initialize	starting ...
Amount to recall: 4.12 GB	

The progress is indicated by the “Amount to recall” value.

Stage 2: Recall progress

Once the initialization is complete the background recall may pause if the amount to recall exceeds the total volume size. The user has to acknowledge by pressing the ***“continue”*** button.

If the amount to recall fits into the free space, the recall will automatically continue by first recalling from online media.



Data Protection - Background Recall Progress

Initialize	Complete
Amount to recall: 835.74 GB	
Copy Files to RAID	Recall in progress
PERCENT COMPLETE	12%
Reserved online media	20
Completed media	1

As far as the background recall process is concerned media can be in one of three states:

- **Reserved Online** - Online media required to complete the background recall request.
- **Required Offline -** Offline media which needs to be returned to the library in order to complete the background recall request.
- **Completed Media -** no longer required by the background recall and can be offlined if necessary.

Note that offline media can be returned to the library at any time during the background recall. If all online media have been processed the job will wait until required offline media have been returned to the library. It will then automatically continue the recall. Note that background recall will also automatically continue after a system restart. It can be stopped by pressing the ***"abort"*** button. It can also be paused by pressing the ***"pause"*** button, however, a pause recall does not persist across restarts.

Any errors during the recall will be counted and a list of failed files can be viewed by selecting the error counter.

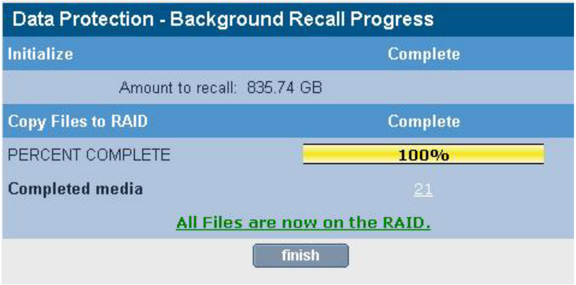
The background recall will try to use as many drives as possible but always exclude the "recall drive" from its selection. As the background recall job is a low priority it will not interfere with other migration and recall jobs.

If the archive has very large files it may be necessary to increase the disk buffer volume to ensure that concurrently executing background recalls and migration jobs have sufficient resource to successfully complete.

Important: Ensure that sufficient disk buffer space is available to recall the largest files in the archive. For example, if the largest files are 5GB then the disk buffer should be the total number of optical drives times 5GB. So for four drives the required disk buffer size should be (4 drives x 5GB) 20GB.

Stage 3: Background completion

The completion marks the end of the background recall and shows all the summary information to the user. This will include access to the error report should any files have failed to be recalled. It is important that the user acknowledges this stage by pressing the ***"finish"*** button.



Data Protection - Background Recall Progress

Initialize	Complete
Amount to recall: 835.74 GB	
Copy Files to RAID	Complete
PERCENT COMPLETE	100%
Completed media	21

All Files are now on the RAID.

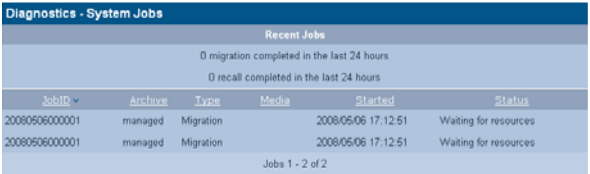
Once the "finish" button is pressed the error log will be archived, the media selection state will be cleared and the "Background recall in progress" message is removed from the status page.

Chapter 7

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	Media	Started	Status
20080506000001	managed	Migration		2008/05/06 17:12:51	Waiting for resources
20080506000001	managed	Migration		2008/05/06 17:12:51	Waiting for resources

Jobs 1 - 2 of 2

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.
- **Started** - The time the job was started
- **Status** - The job’s status.

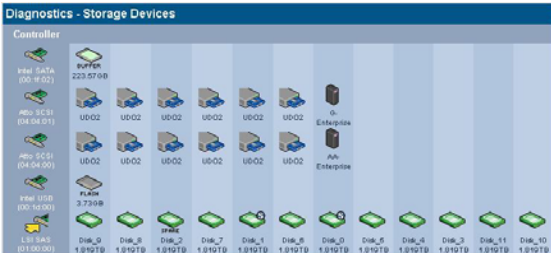
Click the **refresh** button to update the information displayed on this page.

Storage Devices

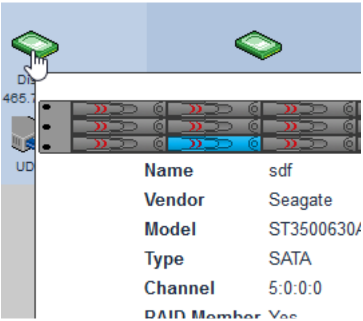
The **Diagnostics - Storage Devices** page shows all interface buses (SATA, SCSI, SAS, USB and IDE) and their associated devices and their status (see screen shot below).

Viewing the Storage Devices

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



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:

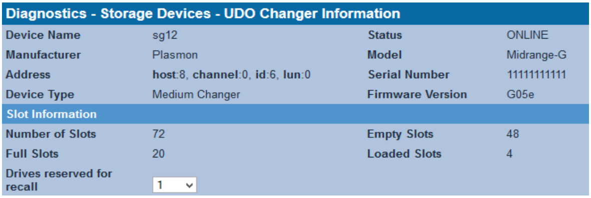


Name sdf
Vendor Seagate
Model ST3500630/
Type SATA
Channel 5:0:0:0
RAID Member Yes

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 Information

Device Name	sg12	**Status**	ONLINE
Manufacturer	Plasmon	**Model**	Midrange-G
Address	**host**:8, **channel**:0, **id**:6, **lun**:0	**Serial Number**	11111111111
Device Type	Medium Changer	**Firmware Version**	G05e
Slot Information			
Number of Slots	72	**Empty Slots**	48
Full Slots	20	**Loaded Slots**	4
Drives reserved for recall	1		

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**.

Note: The host or extension library can be disabled to prevent migrations from occurring without taking the archive offline. This is achieved by clicking the ‘disable’ button.

Apply Slot License

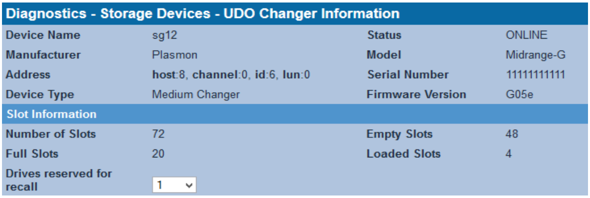
The Appliance library accepts a slot license to enable the usage of media storage slots. Depending on the license the number of license slots can be adjusted upto the maximum number of physical slots.

The slot license is nine characters long.

> *Note: If the firmware version does not support slot licensing, the associated Slot License text box will not be displayed.*

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 Information

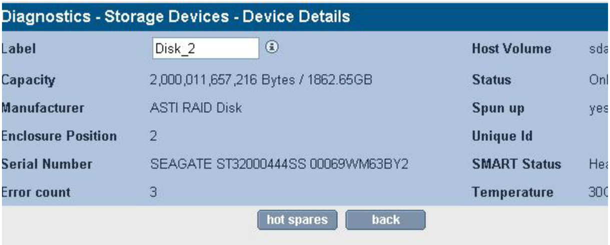
Device Name	sg12	**Status**	ONLINE
Manufacturer	Plasmon	**Model**	Midrange-G
Address	**host**:8, **channel**:0, **id**:6, **lun**:0	**Serial Number**	11111111111
Device Type	Medium Changer	**Firmware Version**	G05e
Slot Information			
Number of Slots	72	**Empty Slots**	48
Full Slots	20	**Loaded Slots**	4
Drives reserved for recall	1		

3. Enter the slot license key into the **Slot license**. The key is split into three triple alphabetic character codes (e.g. DIB-SAP-DOB).
4. Click **save**.

Designate drive as hotspare

If a hard drive is not part of a RAID it can be designated to be a global hotspare. Doing this will make it available to all RAIDs as a replacement drive in case a RAID drive fails or is rejected.

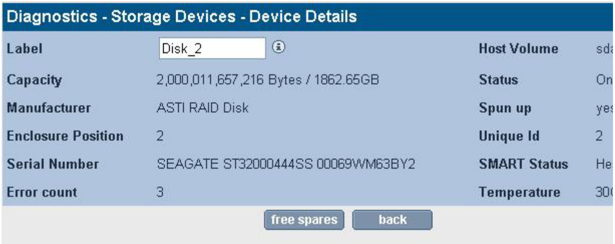
A drive can be added to the hotspare drive group by simply pressing the *“hot spares”* button, which is located at the bottom of the “Diagnostics - Storage Devices - Device Details” page (see below).



Diagnostics - Storage Devices - Device Details

Label	Disk_2	Host Volume	sda
Capacity	2,000,011,657,216 Bytes / 1862.65GB	Status	Onl
Manufacturer	ASTI RAID Disk	Spun up	yes
Enclosure Position	2	Unique Id	
Serial Number	SEAGATE ST32000444SS 00069WM63BY2	SMART Status	Hea
Error count	3	Temperature	30

Note that in the above example the “Error count” is ‘3’ suggesting that this drive already had some minor failures. If the error count becomes much higher (> 5) a drive may not be suitable as a hot spare and should be replaced.



Diagnostics - Storage Devices - Device Details

Label	Disk_2	Host Volume	sda
Capacity	2,000,011,657,216 Bytes / 1862.65GB	Status	On
Manufacturer	ASTI RAID Disk	Spun up	yes
Enclosure Position	2	Unique Id	2
Serial Number	SEAGATE ST32000444SS 00069WM63BY2	SMART Status	He
Error count	3	Temperature	30

Once the “hot spares” button has been pressed it becomes available as a replacement drive to all RAIDs. Note that the hotspare can be removed at any time by pressing the *“free spares”* button.

Disk status icons

Table 7-1 describes the disk status icons and their meaning.

- Disks which are marked with:

  S

  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 re-synchronised. The system, at all times, has to ensure that all mirrored RAID disks contain exactly the same data. If a difference is found, re-synchronization is performed to bring all the RAID disks back to identical mirrors of one another.

Table 7-1: Disk status icons

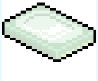
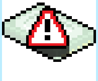
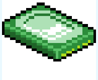
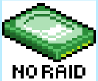
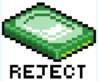
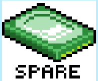
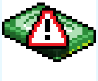
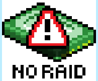
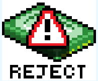
Icon	Meaning
	The disk is online and unformatted
	The disk is online, unformatted and the system has detected the disk is about to fail
	The disk is online
	The disk is online and the disk is not part of a RAID
	The disk is online and has been rejected by the system
	The disk is online and has been marked 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 7-1: Disk status icons

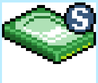
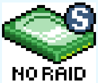
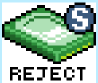
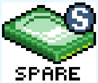
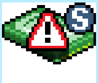
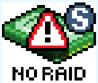
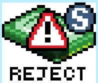
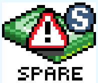
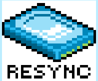
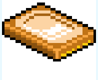
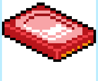
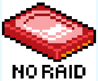
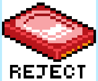
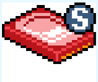
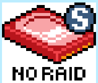
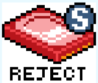
Icon	Meaning
	The disk is online and is a system disk
	The disk is online, is a system disk and is not part of a RAID
	The disk is online, is a system disk and has been rejected by the system
	The disk is online, is a system disk and has been marked as a spare disk
	The disk is online, is a system disk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

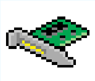
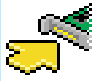
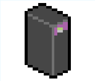
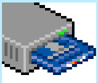
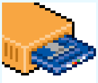
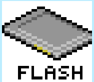
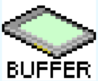
Table 7-1: Disk status icons

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

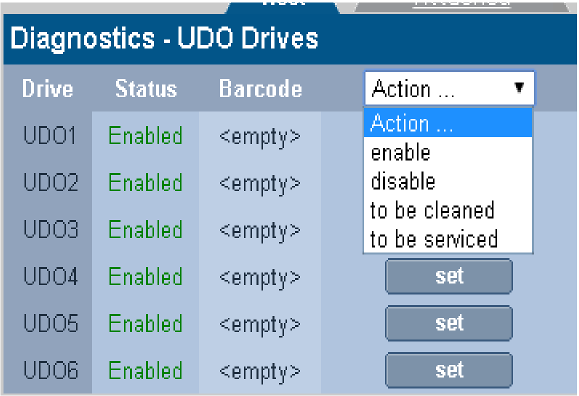
Table 7-1 describes the other status icons and their meaning.

Table 7-2:

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
	Flash drive which contains boot information and Vital Product Data (VPD)
	Dediciated Sold State Drive (SSD) disk buffer, used for packing files into a single migration job.

UDO Drives

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



Diagnostics - UDO Drives

Drive	Status	Barcode	Action ...
UDO1	Enabled	<empty>	
UDO2	Enabled	<empty>	
UDO3	Enabled	<empty>	
UDO4	Enabled	<empty>	set
UDO5	Enabled	<empty>	set
UDO6	Enabled	<empty>	set

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 and requires cleaning
- **error-dirty** - The drive has an error and has been taken offline by the system, but the drive requires cleaning.
- **to be cleaned** - Will be cleaned when cleaning cartridge is added to library.
- **to be serviced** - Drive is powered (Ent-G library only)

Managing a UDO drive

Note: AA only. Drop down options are not available in the AAE.

To enable or disable a UDO drive:

1. From the menu bar, select **Diagnostics - UDO Drives**.
2. Select the ‘*disable*’ action from the dropdown menu
3. Click the ‘set’ button to apply the disable action against the drive to be disabled.

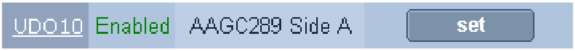
Other actions that may be performed are:

- **‘enable’** - to re-enable a drive
- **‘to be cleaned’** - mark the drive to be cleaned.
- **‘to be serviced’** - power down the drive module (Ent-G only)

Note: Once a drive is marked for cleaning the cleaning is performed by simply adding a cleaning cartridge into the library using the keypad ‘Add Disk’ option. The cleaning cartridge will be return when the cleaning process has completed.

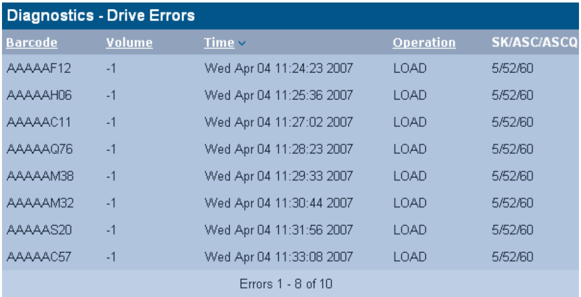
Drive Errors

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.



UDO10 Enabled AAGC289 Side A

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

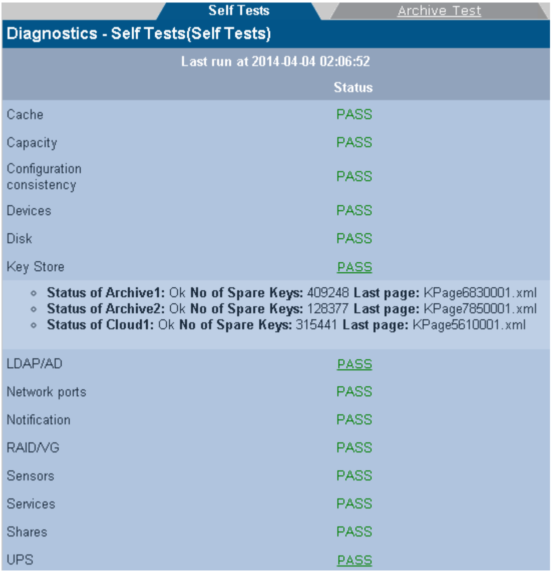
Errors 1 - 8 of 10

- **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 Tests

The **Diagnostics - Self Tests** pages allow the performance of tests which check either the hardware of the Appliance, or the archival process.

Self Test



Diagnostics - Self Tests(Self Tests)

Last run at 2014-04-04 02:06:52

	Status
Cache	PASS
Capacity	PASS
Configuration consistency	PASS
Devices	PASS
Disk	PASS
Key Store	PASS

- **Status of Archive1:** Ok **No of Spare Keys:** 409248 **Last page:** KPage6830001.xml
- **Status of Archive2:** Ok **No of Spare Keys:** 128377 **Last page:** KPage7850001.xml
- **Status of Cloud1:** Ok **No of Spare Keys:** 315441 **Last page:** KPage5610001.xml

LDAP/AD	PASS
Network ports	PASS
Notification	PASS
RAID/VG	PASS
Sensors	PASS
Services	PASS
Shares	PASS
UPS	PASS

The self test displays the time and date of the last self test.

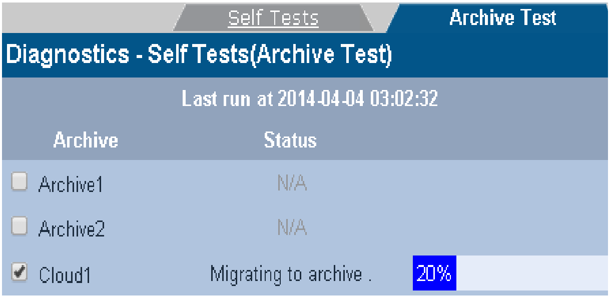
Clicking **start** will check:

- **Cache** - The status of the RAID, including SATA (disk) drives. Normally, the system will perform a re-synchronisation to fix any problems with the cache. However, if the problem persists, contact Alliance Technical Support for further assistance.
- **Capacity** - The status of the Appliance's total data capacity. A failure may indicate that closed media should be taken offline and replaced with new media.

- **Configuration consistency** - This test checks that the configuration of the Appliance is in line with the operation of the Appliance.
- **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.
- **Disk** - The status of all SMART disks. Contact Alliance Technical Support if this test fails.
- **Key Store** - The status of key store associated with each archive. As well as the status, the total number of spare keys and the latest key page name is displayed.
- **LDAP/AD** - The status of LDAP and Active Directory connectivity. If this fails, ensure the relevant service is correctly configured and that there are no network problems.
- **Network Ports** - The status of the physical network ports, as well as network connectivity.
- **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).
- **RAID/VG** - The status of all RAIDs, Volume Groups and Logical Volumes. Contact Alliance Technical Support should this test fail.
- **Sensors** - The status of all attached sensors - board temperature, fan sensors, etc. Sensors alarms should be reported to ASTI support.
- **Services** - The status of the processes, including configurable services, running on the appliance. If any services fail, verify the System - Services page is correctly configured. If this is correct, then contact Technical Support for further assistance.
- **Shares** - The status of any Shares on the Appliance. If this test fails, check the **Network - Shares** page and ensure the failed shares are correctly configured.
- **UPS** - The status of any connected UPS. If this test fails, ensure the UPS is connected correctly and that the UPS Service is running.

If any test fails, **FAIL** will appear in the **Status** column. Click **FAIL** to view the reason for the failure.

Archive Test



Diagnostics - Self Tests(Archive Test)

Last run at 2014-04-04 03:02:32

Archive	Status	
□ Archive1	N/A	
□ Archive2	N/A	
☑ Cloud1	Migrating to archive .	20%

An **Archive Test** creates a small test file, migrates it to media, releases the file from the cache, and then recalls the file from media to check the archive system from end-to-end.

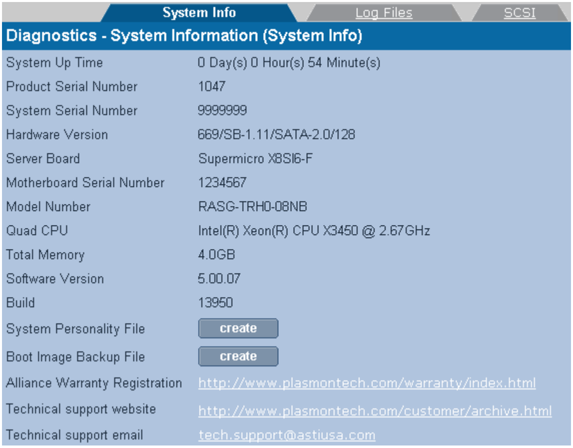
In the above example only the ‘Cloud1’ archive was selected for an archive test.

Click **start** to begin an archive test, and **stop** to abort a test in progress.

System Information

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

System Info



Diagnostics - System Information (System Info)

System Up Time	0 Day(s) 0 Hour(s) 54 Minute(s)
Product Serial Number	1047
System Serial Number	9999999
Hardware Version	669/SB-1.11/SATA-2.0/128
Server Board	Supermicro X8SI6-F
Motherboard Serial Number	1234567
Model Number	RASG-TRH0-08NB
Quad CPU	Intel(R) Xeon(R) CPU X3450 @ 2.67GHz
Total Memory	4.0GB
Software Version	5.00.07
Build	13950
System Personality File	create
Boot Image Backup File	create
Alliance Warranty Registration	http://www.plasmontech.com/warranty/index.html
Technical support website	http://www.plasmontech.com/customer/archive.html
Technical support email	tech.support@astiusa.com

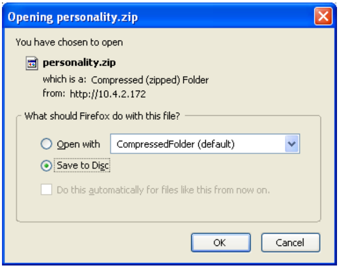
The **Diagnostics - System Information (System Info)** page lists:

- **System Up Time** - since last reboot
- **Product Serial Number** - same as Host Library serial number
- **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

- **System Personality File** - To create an XML based description of the system configuration.The XML file is zipped an can be downloaded to the client desktop.
- **Boot Image Backup File** - create a copy of the boot device file file system content. All the files on the boot device file system are compressed into a zip container and available for download.
- **Alliance Warranty Registration** - Hyperlink to the Alliance warranty registration web page (requires an external internet connection)
- **Technical Support Website** - Hyperlink to the Alliance technical support web page (requires an external internet connection)
- **Technical Support Email** - Alliance Technical Support email address.

Also present is the facility to create a copy of the current System Personality File should it be required by Alliance Technical Support. To do so click the **create** button.

The Appliance will generate a downloadable copy of the personality file, then pop-up the browser's Download dialog:



Opening personality.zip

You have chosen to open

personality.zip

which is a: Compressed (zipped) Folder

from: http://10.4.2.172

What should Firefox do with this file?

○ Open with CompressedFolder (default)

● Save to Disc

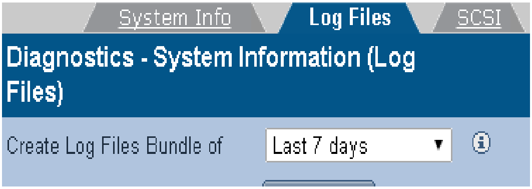
□ Do this automatically for files like this from now on.

OK Cancel

Select **Save to disk** (Firefox) or **Save** (Internet Explorer).

Personality.zip may then be emailed to Alliance Technical Support.

Log Files



Diagnostics - System Information (Log Files)

Create Log Files Bundle of: Last 7 days

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:

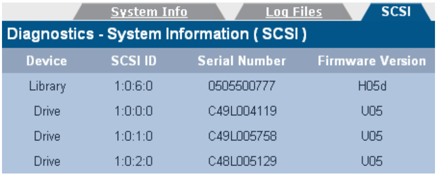
  - **Last 7 days**
  - **All days**
  - **From custom date**
  - **UDO Logs -** This option extracts a logging information from the UDO drives.

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

- This tab also allows SCSI logs to be purge. This is useful if a hardware fault has generated an excessive number of hardware errors. Once the required logs have been extracted the SCSI logs should be removed.

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**.

Page left intentionally blank

Chapter 8

Shutdown

Shutdown the Appliance using the Web Interface

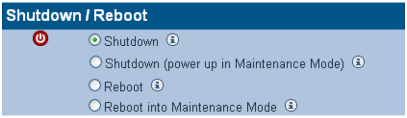
The **Shutdown/Reboot** page allows:

- **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

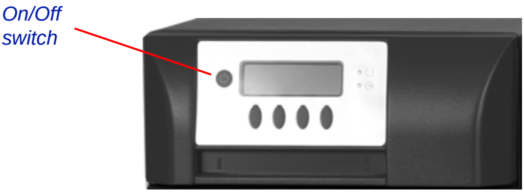
● Shutdown
○ Shutdown (power up in Maintenance Mode)
○ Reboot
○ Reboot into Maintenance Mode

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:



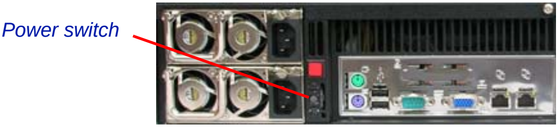
Press the power button and confirm shut down via the keypad.

> *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

Page left intentionally blank

Chapter 9

Troubleshooting

Troubleshooting

Table 9-1: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.
Question marks appear on keypad display for IP address	Cannot get IP address from DHCP server OR network connection cannot be established OR static IP address could not be applied	Try other network port (it needs to be eth0 and re-apply the network settings (gateway, mask and IP address)
Faulty Ethernet cable.	Test with a known working Ethernet cable.	

Table 9-1:Archive Appliance Troubleshooting checklist

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.	
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 Alliance 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 Alliance support.	
The Appliance fails its self-test.		
Possible cause	*Suggested action*	*Comments*

Table 9-1:Archive Appliance Troubleshooting checklist

A UDO drive is unavailable.	Reboot the Appliance. If this does not resolve the issue contact Alliance support.	
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.	Check service configuration in System - Services
Hardware failure.	Contact Alliance 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 Alliance support.	

Table 9-1: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 Alliance support if problem is not resolved.	
Dirty media.	Clean the media using a Alliance UDO media cleaning kit and retry.	(*Cleaning Media* on page 202)
Hardware failure.	Contact Alliance 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 (**Diagnostics - Storage Devices - Library**)	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 9-1: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 Alliance support if problem is not resolved.	
SSM fault.	Reboot the Appliance. Contact Alliance support if the problem is not resolved.	
Dirty media.	Clean the media using a Alliance UDO media cleaning kit and retry.	Refer to the Operator’s Guide for media storage and care information.
Hardware failure.	Contact Alliance support.	

Media fails to close.

Possible cause	*Suggested action*	*Comments*
"RMDB corruption, no partition found"	recover RMDB from backup	

Table 9-1:Archive Appliance Troubleshooting checklist

"Partition is not mounted"	Ensure that archive is mounted and active, run self-test	run migration selft test to confirm archive is healthy
"Failed to set the archive to read-only"	restart SSM and run self test	
"Failed to migrate all active files"	run migration selftest and check hardware status - run self-test	problem with hardware or resources
"Failed to close media"	check hardware status and archive resource	review media inventory and UDO drive status
"Failed to set the archive to read-write"	restart SSM and run self test	

Table 9-1: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 recommended.
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 Alliance support.	

Table 9-1:Archive Appliance Troubleshooting checklist

SATA drive missing.		
Possible cause	*Suggested action*	*Comments*
SATA drive not inserted correctly.	Shutdown the Appliance. Remove then re-insert the drive fully in its drive bay. Power on the Appliance. Contact Alliance 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 9-1: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 54.	
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 65.	
Host has been denied access.	If the host should have access, see *Modifying a share* on page 65.	

Table 9-1: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 65.	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 writable, open the **Network - Shares** page and click on the share. Ensure the **Read only** option is not selected.	

Table 9-1: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 Alliance 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 Alliance 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 65.	The connected users can be determined by going to the **Network - Shares** page and clicking on **connections**.

Table 9-1: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 Alliance 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 Alliance 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 65.	
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 90 and set the **Allow File Changes** option to YES.	
No Free Space reported when writing to the share.		
Possible cause	*Suggested action*	*Comments*

Table 9-1:Archive Appliance Troubleshooting checklist

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 90. Reconfigure release policy as required.	
Email Notifications 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.	
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.	

Table 9-1:Archive Appliance Troubleshooting checklist

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.	
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.	
Administrator notified that the UDO drive is dirty.		
Possible cause	*Suggested action*	*Comments*

Table 9-1:Archive Appliance Troubleshooting checklist

Dirty drive.	insert the cleaning cartridge to perform a cleaning cycle. The dirty status should be reset after the next recall or migration.	
Hardware failure.	Contact Alliance support.	
Appliance will only boot into MAINTENANCE mode.		
Possible cause	*Suggested action*	*Comments*
Hardware failure.	Contact Alliance 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 synchronized 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 51.	
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 9-1: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 replication 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.	
Files on the Active volume were offlined before replication took place.	Return offline media to Appliance.	

Table 9-1:Archive Appliance Troubleshooting checklist

Cloud connection failure

Possible cause	*Suggested action*	*Comments*
DNS or gateway not configured	Ensure that network configuration is correct. Gateway and DNS must be configured.	
Firewall disallows outbouind HTTPS connections	Ensure that AMS can make HTTPS outbound connections	
Account credentials are incorrect	Make sure that “Access key ID” and “Secret key” are valid and correct length.	Access key is typicallly 20 characters long. Secret key has 40 characters.
Hardware failure.	Contact Alliance support.	

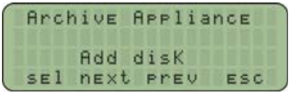
Chapter 10

Using the Keypad interface on the Archive Appliance

Configuration

Setting the IP address

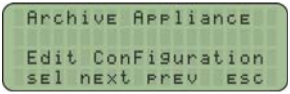
1. With the Appliance switched on and connected to the host LAN / Network, press any key to display the first item in the top-level menu on the LCD panel:



```
 Archive Appliance

    Add disk
 sel next prev  esc
```

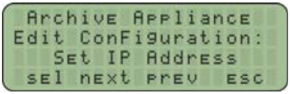
If already in a submenu, press **esc** a number of times until the Add disK menu is displayed.

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



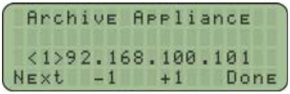
```
 Archive Appliance

 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
```

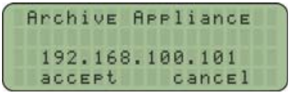
4. Press **sel** to display the IP address. Initially, the current IP address is displayed (in standard dotted-decimal format), with the first digit selected, ready for editing:



```
 Archive Appliance

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

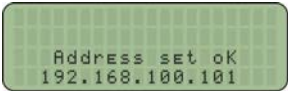
5. Press **-1** and **+1** to change the value inside the brackets (the first digit in any group of three can only be set to 0, 1 or 2).
6. Press **next** to highlight the next digit:
7. Press **-1** and **+1** to change the value inside the brackets (the maximum value for each 3-digit group is 255).
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 194. 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 194. In step 3, select the Set Gateway submenu. The remaining system configuration can be performed via the web interface.

Adding UDO media

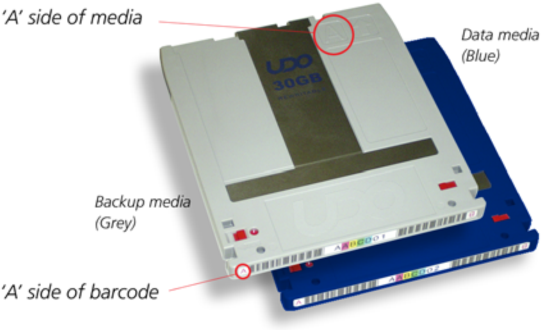
UDO media may be added to the Appliance via the Mailslot or via Direct slot access.

- 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.
- 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.

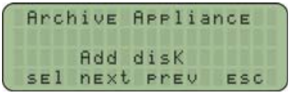
Pieces of UDO media must have a unique barcode of the approved format centered on the spine of the disk, ensuring the ‘A’ side of media and barcode label are oriented as shown below.



Adding Backup UDO media via the mailslot

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

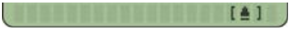
1. Press any key to display the top-level Add disk menu.



```
Archive Appliance

    Add disk
sel next prev  esc
```

2. Press **sel**.
3. 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.



```
                 [⏏]
```

4. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see *page 201*).

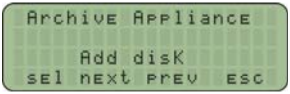
   If all is well, a Disk added OK message is be displayed.
5. Repeat the above steps until all required backup UDO media has been added.

*Note: At least one piece of backup UDO media **MUST** be added to the system. Alliance 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:

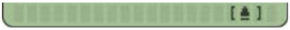
1. Press any key to display the top-level Add disk menu.



```
Archive Appliance

     Add 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.



```
[⏏]
```

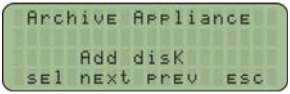
4. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see *page 201*).

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

Adding UDO cleaning cartridge via the mailslot

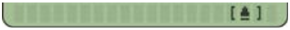
To load cleaning cartridges via the mailslot:

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



```
Archive Appliance

     Add disk
sel next prev  esc
```

2. Press **sel**.
3. Mark the usage tracker on the cartridge. A tick for each drive to be cleaned. The drives will have been previously marked for cleaning you the Web UI.
4. Insert the cartidge into the mailslot.



```
                  [⏏]
```

5. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see *page 201*).
6. The library will proceed to clean all the marked drive and when complete return the cleaning cartridge via he mailslot.

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 172 or *Shutdown the Appliance using the library power switch* on page 173.
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 237*, add media to the lowest numbered available slots.

Important: Do not place media in the Utility Slots.see Library slot maps on page 237

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 243*, 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 Alliance Technical Support.
- Move Failed - Hardware problem with the library picker. Contact Alliance Technical Support.

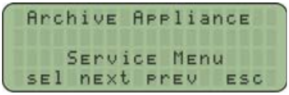
Removing UDO media

If any disks have failed, an administrator will receive an alert via the configured method (see *page 37*) 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 223*.

Removing UDO media with unreadable barcode

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



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

4. Press **next** or **prev** to display the required option (Bad Barcode Disk).
5. Press **sel**.
   The library picker will automatically select the first disk to be removed.
6. Remove the cartridge from the Mailslot.
   The “Bad Barcode Disk” submenu will be displayed once more.
7. Repeat the above steps until all failed media are removed.

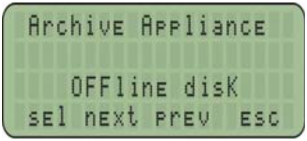
Cleaning Media

A UDO cleaning service is available from Alliance.

To remove dirty media navigate to the web GUI “Storage Media” menu item and select the search tab. This interface will allow the selection of all media that “Require attention” including dirty media (see *Search Media* on page 105)

Once the media has been identified select “show media: to select for offline” and select all media.

Media that have been selected for offline can be removed from the library with the keypad option 'Offline media - User selected' from the 'Offline Media’ Menu.



To re-introduce the cleaned media, see*Adding Backup UDO media via the mailslot* on page 197 or *Adding Data UDO media via the mailslot* on page 198.

Chapter 11

The Archive Appliance with an Additional Library Attached

Additional Library

An additional library can be purchased and attached to a host Archive Appliance to increase the total number of media slots available, providing either significantly expanded data storage capacity and data migration throughput or providing fail-over data protection.

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

The attached library can operate in one of two modes:

Slot Overflow

In Slot Overflow mode, the attached library is used to extend the available number of slots and drives.

Library operations are load-balanced between the host Appliance and the attached library to increase data throughput and, increase total storage capacity by using any available UDO drive and media in either library.

When an additional library is attached, it will operate in Slot Overflow mode by default.

Pool-per-Library

In Pool-per-library mode media entered into the host library is always allocated to the primary media pool, and media entered into the attached library is allocated to the secondary media pool. Data is migrated to both copies as with normal multiple copy media operations ensuring that, should the primary media pool be unavailable data can be read from the secondary media pool in the attached library.

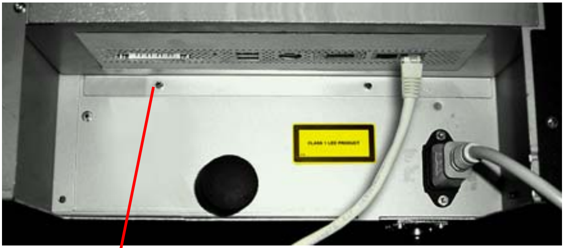
Note: Pool-per-library mode is only available to archives with two media pools.

Attaching an additional library

Alliance recommends that the additional 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 172*.
2. Connect the additional library to the host Appliance using the SCSI cable provided:

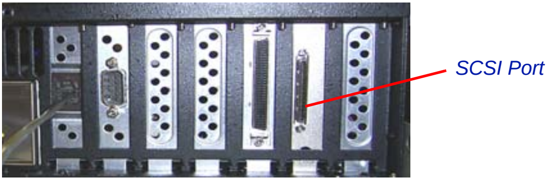
   AA16 to AA174 models only: SCSI port is located on the lower rear side of the Appliance:



SCSI Port

AA238 to AA638 models only:

The SCSI Card must be installed by a Alliance Support Engineer in order to connect an additional Library.

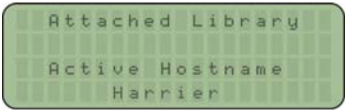


3. Connect the power cord to the additional library.
4. Power on the attached library.

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

5. Power on the Appliance.

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



```
  Attached Library

  Active Hostname
      Harrier
```

Attached library keypad interface

The attached library keypad interface offers differing options depending on what mode the attached library is operating in.

In Slot Overflow with Load Balancing mode, the keypad 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:

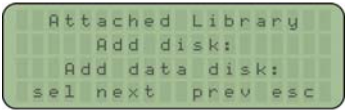
- Removing failed media - see *page 201*
- Offline Media Management - see *page 223*

In Pool Per Library mode the keypad may be used to:

- Add media to the library
- Offline media
- Offline open media
- Remove misplaced media

Adding UDO media to the attached library via the mailslot.

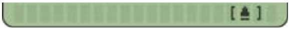
1. Press any key on the overflow library keypad to display (Add Data Disk).



```
 Attached 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 201*).

   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 attached library via direct slot access see page 199

Removing UDO media via the mailslot

> *Note: The library must be operating in Pool Per Library mode to access these options.*

1. Press any key to display the top-level Add disk menu.
2. Press **next** until Service Menu is displayed.
3. Press **sel** to display the Service Menu sub-menu.
4. Press **next** or **prev** to display the required option (Remove dirty disk, Failed data disk, or Misplaced 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.

Repeat the above steps until all failed media are removed.

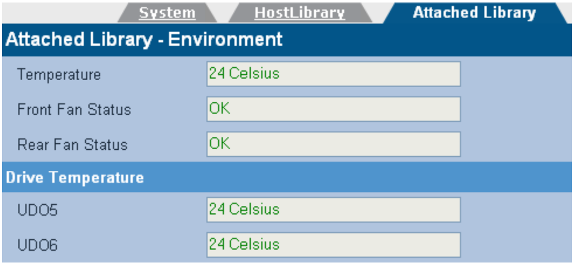
Attached library Web interface

The attached library can be monitored via the Web interface, and the operating mode may be changed.

Viewing attached library information

Information relating to the attached library are added as additional pages to the following sections of the Web interface:

- System - Status - Environment



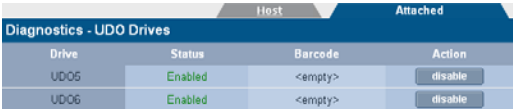
Attached Library - Environment

Temperature	24 Celsius
Front Fan Status	OK
Rear Fan Status	OK

Drive Temperature

UDO5	24 Celsius
UDO6	24 Celsius

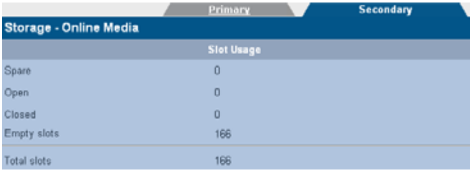
- Diagnostics - UDO Drives



Diagnostics - UDO Drives

Drive	Status	Barcode	Action
UDO5	Enabled	<empty>	disable
UDO6	Enabled	<empty>	disable

- Storage - Online Media

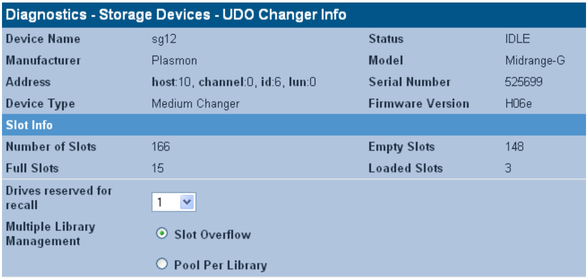


Storage - Online Media

	Slot Usage
Spare	0
Open	0
Closed	0
Empty slots	166
Total slots	166

Configuring mode of operation

1. In the **Diagnostics** menu, select **Storage Devices**.
2. Click on the library icon to open the configuration page.
3. Select the required mode of operation using the correct radio button:



Diagnostics - Storage Devices - UDO Changer Info

Device Name	sg12	**Status**	IDLE
Manufacturer	Plasmon	**Model**	Midrange-G
Address	host:10, channel:0, id:6, lun:0	**Serial Number**	525699
Device Type	Medium Changer	**Firmware Version**	H06e
Slot Info			
Number of Slots	166	**Empty Slots**	148
Full Slots	15	**Loaded Slots**	3
Drives reserved for recall	1		
Multiple Library Management	● Slot Overflow ○ Pool Per Library		

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

UDO ARCHIVE APPLIANCE

Chapter 12

Using the Archive Appliance Express

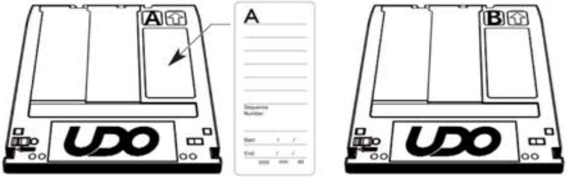
Media labelling

Each piece of UDO Media used in the AA Express is identified by a sequence number. Media must be labeled and numbered prior to use.

When new media is requested by the AA Express:

1. Remove the UDO media from the packaging.
2. Attach the supplied label to side A of the media.

> *Note: Sides A and B of the media are identified by the letters embossed on the casing.*



3. Write the sequence number indicated by the media request (See “Action requests” on page 218.) on the media label.

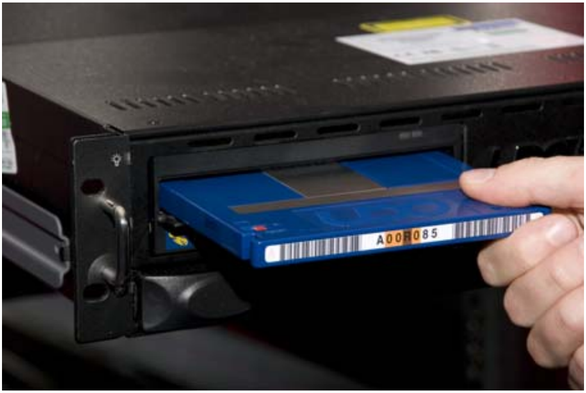
> *Note: When not in use, UDO media should be kept in the protective sleeve supplied.*

Media handling

Inserting media

Note: AA Express *models equipped with a UDO 2 drive feature a drive door to protect against dust ingress. Press the drive button to open the door before inserting media into UDO 2 drives.*

Hold the media at the rear of the cartridge and insert in the direction of the arrow (media shutter forward) as shown:



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

Correct media side

To load side A of the media for reading or writing, insert the media with the embossed “A” on the casing facing upwards and the “A” mark on the barcode label to the left.

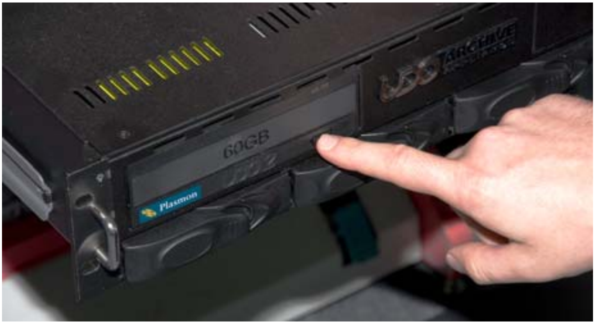
To load side B, insert the media with the embossed “B” on the casing facing upwards with the “B” mark on the barcode label to the left.

Ejecting media

Media is ejected automatically from the UDO drive only when a side or the complete media is full. For all other operations, media must be ejected manually.

> *Note: Media cannot be ejected during read/write operations.*

To eject media from the UDO drive, press the drive button as shown:



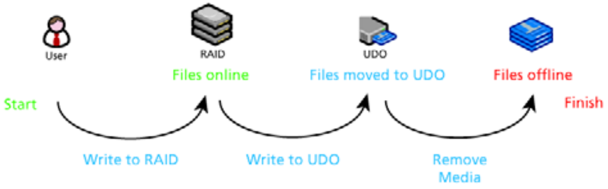
Cleaning media

During normal operation, dust and other particles may contaminate the surface of the media causing read/write failure. In this case, the media should be cleaned - See “Storage of offline media” on page 224.

Basic Operation

Writing to UDO media

Files written to the AA Express via network shares are initially stored on the RAID storage volume. Files are then moved to UDO media. The AA Express records the sequence number of the UDO media containing the file so that it can be located when requested for reading.



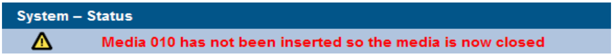
Writing files to the AA Express

The AA Express tracks only one piece of UDO media that is open for file writing at any one time. Under normal operation, once media is full the AA Express marks the media as closed. The media can then be stored appropriately until requested for file reading.

Blank media insertion

If a new blank piece of media is inserted into the UDO drive when a piece of open media already exists, the AA Express will mark the currently open media as closed even though it may not be full. Any remaining storage space on that media will be lost.

The AA Express issues an alert notification and displays the following in the **System - Status** section of the status page:



System – Status

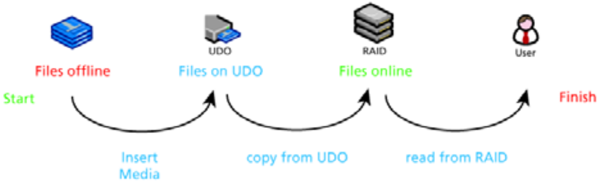
⚠ Media 010 has not been inserted so the media is now closed

The AA Express will mark the inserted blank media as being the currently open one, assign it a new sequence number and begin writing files to it.

Important: Insert blank media into the AA Express *only when requested.*

Reading from UDO media

When users attempt to read files, the AA Express determines the sequence number of the UDO media that the file has been written to. If the media is not in the drive, the AA Express will issue a request to the operator that it be inserted. Once the media has been inserted into the drive, the files are copied back to the RAID storage volume and can be read by the user.



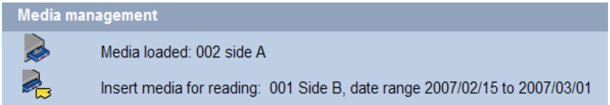
Reading files from the AA Express

Media request queuing

If the appropriate media is not loaded into the UDO drive, the AA Express “queues” read/write operations and their associated media requests. Queued operations are completed and their associated requests cleared automatically when the correct media and media side is loaded into the UDO drive.

Action request notification

If the AA Express requires the operator to perform an action, it is displayed on the status page in the **Media Management** section.



Media management

Media loaded: 002 side A

Insert media for reading: 001 Side B, date range 2007/02/15 to 2007/03/01

The upper line of the Media Management section displays the media identification information. It indicates if the drive is empty or, if there is media in the drive, displays the sequence number and which side of the media is currently loaded. The lower line displays operator action requests - See “Action requests” on page 218..

The AA Express can also be configured to send action requests by email. If an action request is received, it should be performed promptly to ensure that the AA Express continues to operate correctly.

Status icons

The drive and media status icons used in the web interface are detailed below.

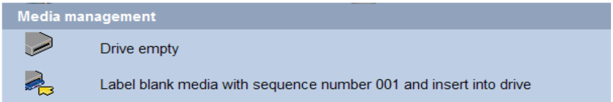
Drive Empty.	Insert media.
Media OK.	Media loaded.
Media write.	Media read.
Turn media over.	Remove media.
Find media.	Incorrect or unrecognised media.

Action requests

Please refer to this section to determine the action that must be taken by the operator in order for the AA Express to successfully write to or read from UDO media.

New blank media required

If the status page displays:



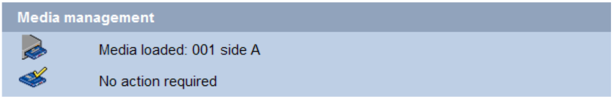
Media management

Drive empty

Label blank media with sequence number 001 and insert into drive

the AA Express requires blank media in order to write files.

1. Label a piece of blank UDO media with the sequence number indicated (See “Media labelling” on page 212.) and insert into the UDO drive ensuring side A is loaded (See “Inserting media” on page 213.).
2. The AA Express initializes the media and displays:



Media management

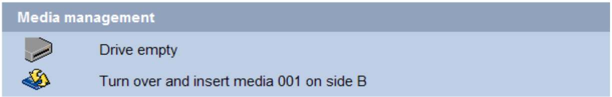
Media loaded: 001 side A

No action required

3. Files can now be written to the media.

Side A full

If the status page displays:



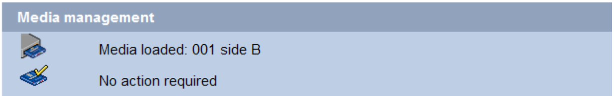
Media management

Drive empty

Turn over and insert media 001 on side B

side A of the media is full and the media has been ejected.

1. Turn the media over and re-insert so that side B is loaded (See “Inserting media” on page 213.).
2. The AA Express checks the media and displays:

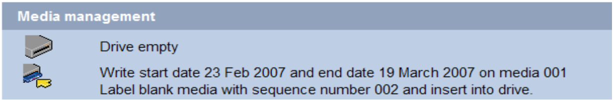


Media management

Media loaded: 001 side B

No action required

3. Files can now be written to the media.



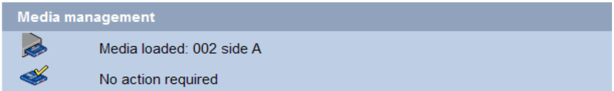
Media management

Drive empty

Write start date 23 Feb 2007 and end date 19 March 2007 on media 001
Label blank media with sequence number 002 and insert into drive.

both sides of the currently loaded media are full and the media has been ejected. The AA Express requires blank media in order to write files.

1. Remove the full media from the drive and enter the indicated date range on the media label. The media should then be stored appropriately - See “Storage of offline media” on page 224..
2. Label a piece of blank UDO media with the indicated new sequence number (See “Media labelling” on page 212.) and insert into the UDO drive ensuring side A is loaded.
3. The AA Express checks the media and displays:



Media management

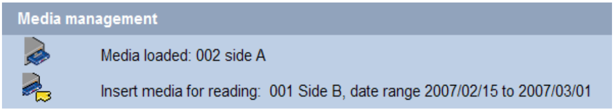
Media loaded: 002 side A

No action required

4. Files can now be written to the media.

Media required for reading files

If the status page displays:



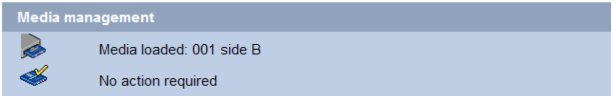
Media management

Media loaded: 002 side A

Insert media for reading: 001 Side B, date range 2007/02/15 to 2007/03/01

the AA Express requires the insertion of a closed media to read files requested by a user.

1. Eject and remove the currently loaded media (See “Ejecting media” on page 214.) noting which side (A or B) is facing upwards, to ensure correct orientation during re-insertion.
2. Locate the media with the requested sequence number and date range and insert into the UDO drive ensuring the correct media side is loaded.
3. The status page displays:



Media management

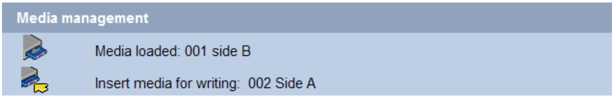
Media loaded: 001 side B

No action required

4. Files can now be read from the media

Media required for writing files

If the **System - Status** displays:



Media management

Media loaded: 001 side B

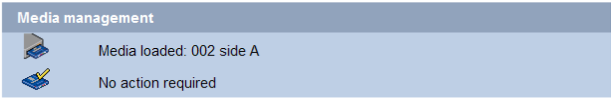
Insert media for writing: 002 Side A

the currently open media is required for writing files.

1. Insert the indicated currently open media ensuring the correct side is loaded.

   Important: Insert the already open media only. Inserting blank media into the AA Express *when open media exists will result in wasted storage space.*

2. The AA Express checks the media and displays:



Media management

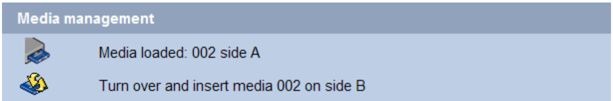
Media loaded: 002 side A

No action required

3. The AA Express can continue writing files to the media.

Turn media over

If the **System - Status** page displays:



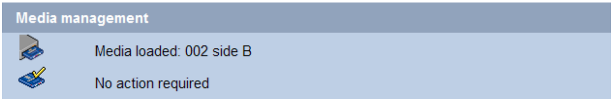
Media management

Media loaded: 002 side A

Turn over and insert media 002 on side B

the AA Express requires the media to be turned over in order to write or read files.

1. If required, eject and remove the media - See “Ejecting media” on page 214..
2. Turn media over and re-insert so that the requested media side is loaded.
3. The AA Express checks the media and displays:



Media management

Media loaded: 002 side B

No action required

Page left intentionally blank

UDO ARCHIVE APPLIANCE

Chapter 13

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 Alliance.

Alliance 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: Alliance 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 90.

or

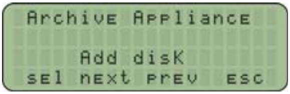
- The media has been selected for offline via the media management user interface (*to select for offline - show all media that are candidates for offline.* on page 107) .

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

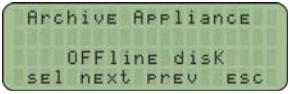
When the Web interface advises that media is eligible for OMM:

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

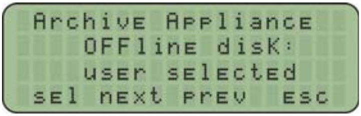
   ```
   Archive Appliance

       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.

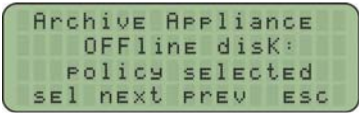
   ```
   Archive Appliance

     OFFline disk
   sel next prev  esc
   ```

3. Press **sel**.
4. Press **next** or **prev** to select the offline strategy: user or policy selection.



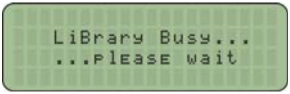
```
Archive Appliance
  OFFline disk:
  user selected
sel next prev  esc
```

or



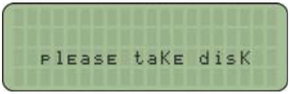
```
Archive Appliance
  OFFline disk:
 policy selected
sel next prev  esc
```

5. When using the Policy selection press **next** or **prev** to select which volume to offline the media from, as required, then press **sel**.
6. The library keypad will display:



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

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



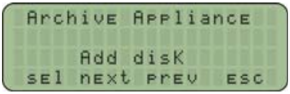
```
please take disk
```

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:

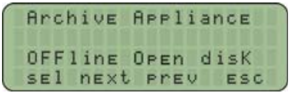
1. Press any key to display the first item in the top-level menu on the LCD panel:



```
Archive Appliance

    Add disk
sel next prev  esc
```

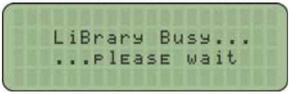
If already in a submenu, press **esc** (key **4** on the Keypad) a number of times until the `Add Disk` menu is displayed.

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



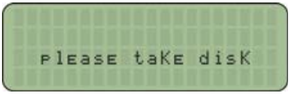
```
Archive Appliance

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:

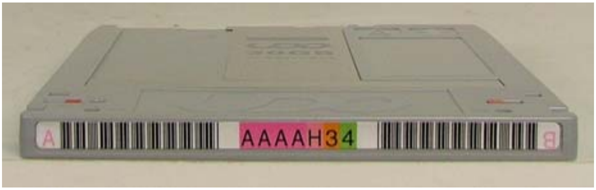


please take disk

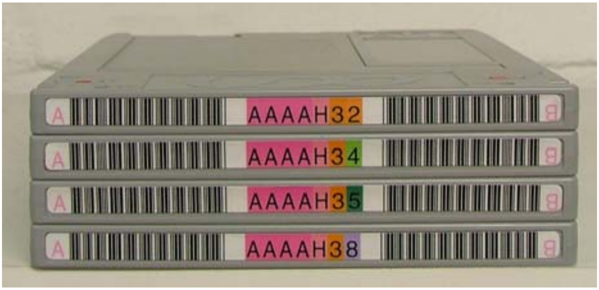
Remove the disk and store in accordance with *Storage of offline media* on page 224.

Organizing offline media

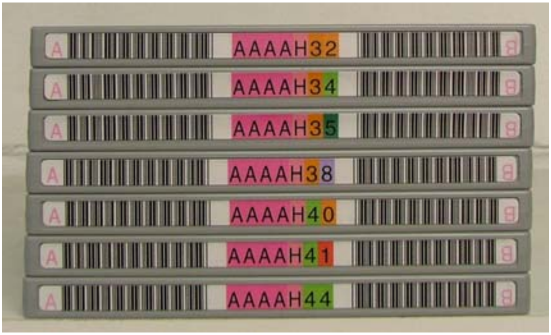
To aid location following *Offline media return requests*, media barcode labels feature a unique 7-digit alphanumeric coding scheme to aid the logical organization of offline media. This numbering scheme is also colour coded to aid in the visual location of barcodes.



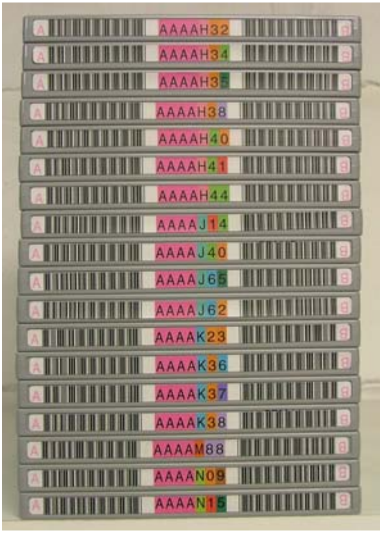
1. All media bearing the same sixth digit (**3** in the illustrated example) should be grouped together and arranged in numerical order according to the seventh digit.



2. The media should then be grouped according to the fifth digit (**H** in this example).



3. This should be continued until all media are organized for easy referencing.



To locate a piece of offline media (for example: media barcode **DGFGH71)**:

1. Read the first digit on each of the media barcodes until the required first digit (**D** in this example) is located.
2. Switch to the second digit and continue reading each of the media until the required second digit (**G** in this example) is located.
3. Continue this process for all seven digits to locate the required media.

Open Offline Media

The open offline media functionality is provided to allow open media to be stored offsite, providing an additional level of data protection in low-frequency migration usage scenarios.

It is important however, that open offline media be regularly returned to the Appliance to allow any files migrated since the media was offlined to be added, ensuring that the open offline media is kept as up-to-date as possible.

The regularity with which open offline media is returned is dependent on the frequency of migrations during normal usage and the allowable time for the data to exist in a single location. Alliance recommends that a regular schedule for returning open offline media is established and is based on these considerations.

Open offline media should be stored separately from closed offline media at the offsite storage location to ensure that closed media is not incorrectly returned to the Appliance instead of the open offline media. Open offline media can be identified on the **Storage - Offline Media** page of the web interface by a tick in the **Open** field for the media. The barcode can then be obtained and the correct media selected at the offsite storage location.

Open offline media is returned to the Appliance using the same procedure as for closed offline media (see “Returning offline media” on page 234).

When open offline media is returned to the Appliance, it should remain in the library for sufficient time to allow the Appliance to complete the migration operations required. This ensures that the open offline media is synchronized with the primary media pool.

The web interface **Diagnostics - System Jobs** page indicates any migration jobs associated with the open offline media (identified by the job type **CopyMig**) that are incomplete. Once all migrations have completed, the open offline media can once again be removed from the Appliance and stored offsite.

Note: During the course of updating, the open offline media may become full. In this case, the media is closed and can be offlined according to the normal offline media procedure. A spare piece of media is then assigned as the open offline media. It is possible therefore, that the media to be removed following an update may bear a different barcode to that inserted into the Appliance. This can be confirmed by viewing the ***Storage - Media - Offline*** *tab of the web interface.*

The sequence of operations for updating open offline media is as follows:

1. Return the open offline media to the Appliance (see “Returning offline media” on page 234).
2. Add any blank media if no spare media are available.
3. Return any closed offline media for recall.
4. Check that all **CopyMig** system jobs have completed.
5. Offline any closed media (see “Offlining media using the Keypad interface” on page 225).
6. Offline the open media (see “Offlining open media using the Keypad interface” on page 227).
7. Return the open offline media to the remote storage location ensuring it is stored separately from any closed offline media.

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 (**Storage - Media Requests**).

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

Returning offline media

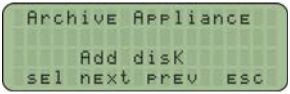
Offline media can be returned to the Appliance in two ways:

- *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

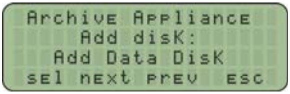
To return one or more offlined media cartridges via the mailslot:

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



```
Archive Appliance

    Add disk
sel next prev  esc
```

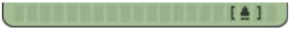
2. Press **sel** to display the first sub-menu (Add Data Disk):



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

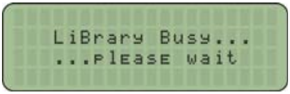
3. Press **sel**.
4. Insert the media, ‘A’ side facing up, into the Mailslot.

   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: 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 237*, 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:

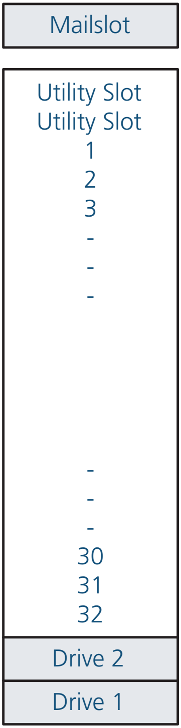
1. Using the Web interface, shut down the Appliance.
2. Open the library rear door.
3. Referring to the slot map on *page 243*, return the offlined media to the lowest numbered available and unassigned slots.
4. Restart the Appliance. The Appliance will rescan the contents of the library and update its 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



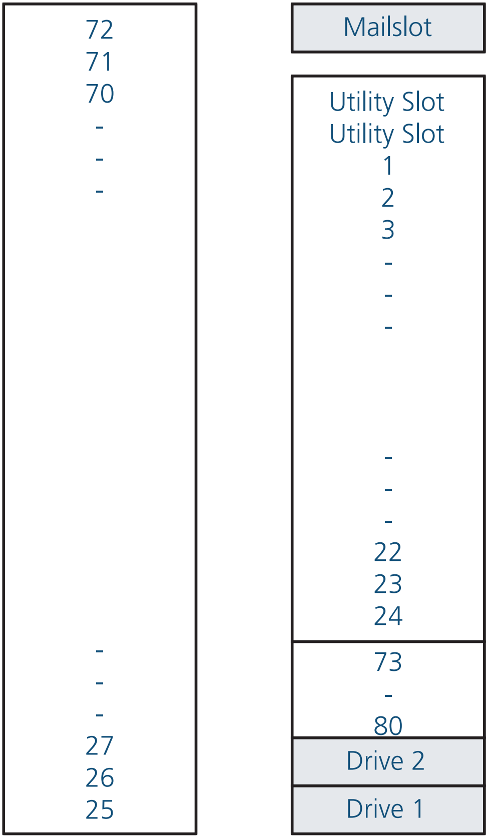
Mailslot

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

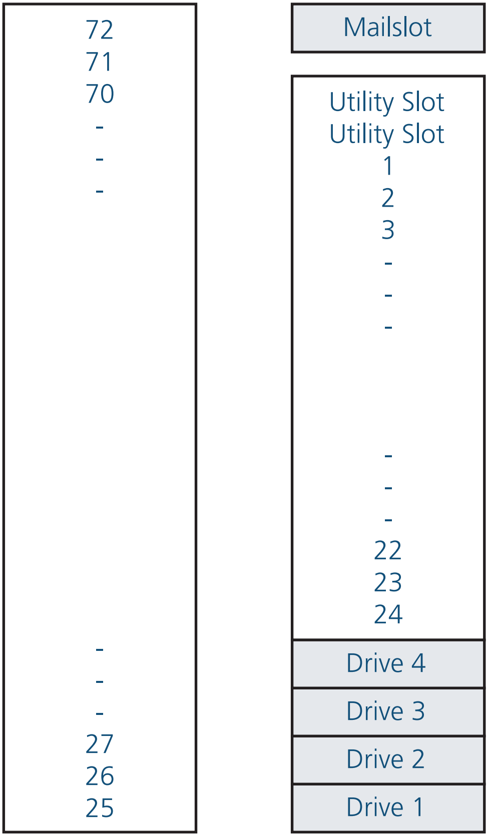
Drive 2

Drive 1

AA80 (2 drive) Appliance



AA80 (4 drive) Appliance



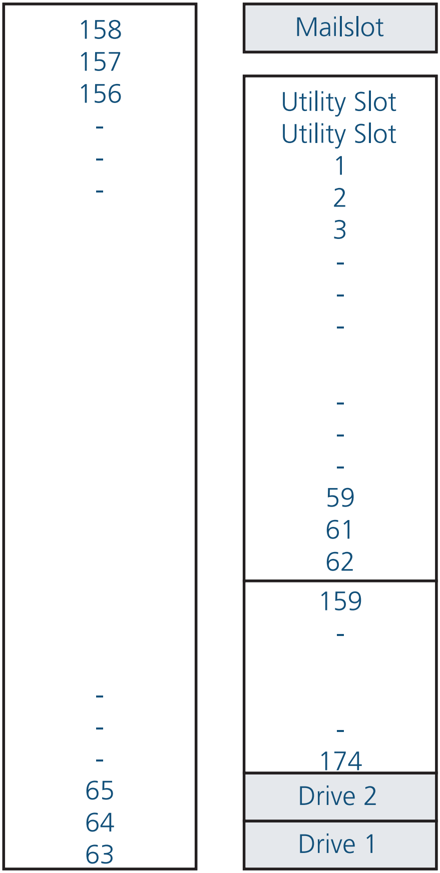
72
71
70
-
-
-
-
-
-
27
26
25

Mailslot

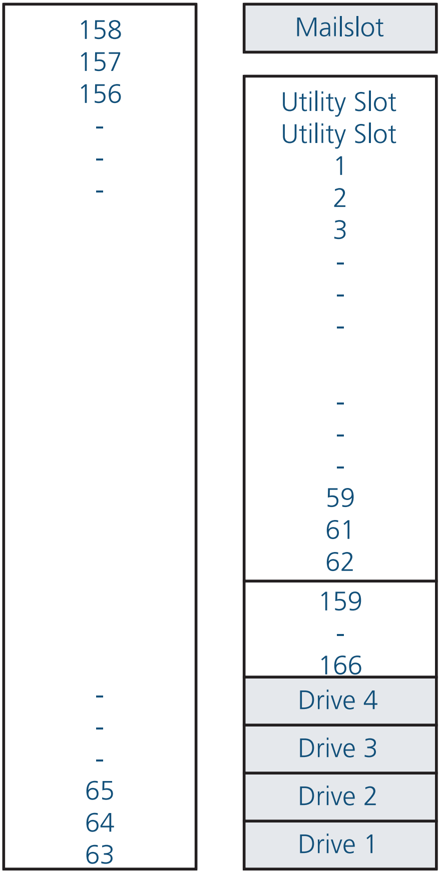
Utility Slot
Utility Slot
1
2
3
-
-
-
-
-
-
22
23
24

Drive 4
Drive 3
Drive 2
Drive 1

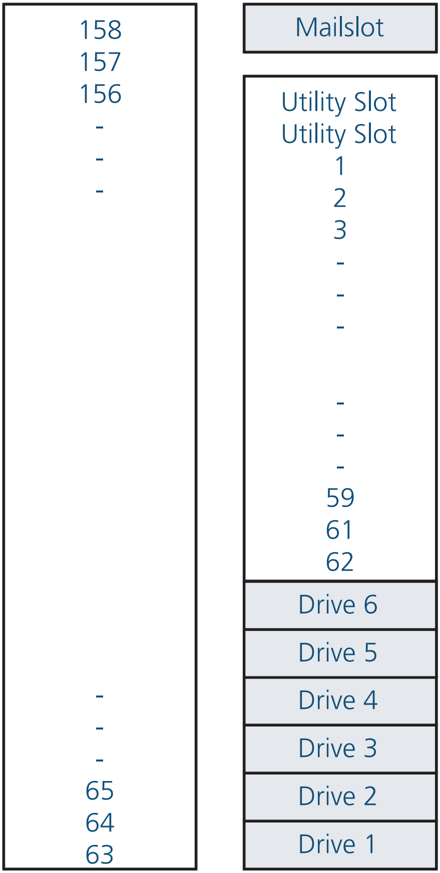
AA174 (2 drive) Appliance



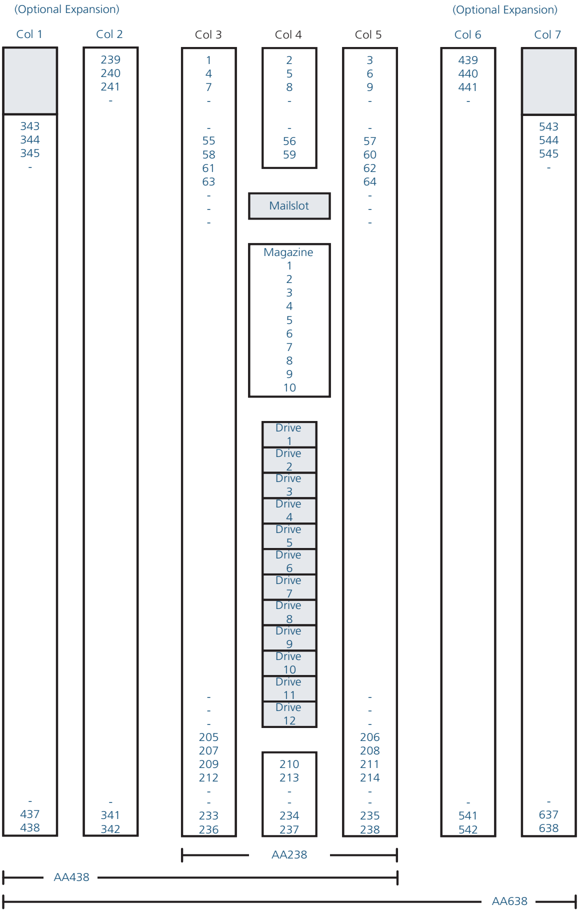
AA174 (4 drive) Appliance



AA174 (6 drive) Appliance



AA238, AA438 and AA638 Appliances



Page left intentionally blank

Chapter 14

Offline Media Management with the AAE

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.*

Organisation of offline media

UDO Media used by the AA Express are identified by the media sequence number. Cataloging of offline media can be achieved by one of the three methods detailed below:

By sequence number

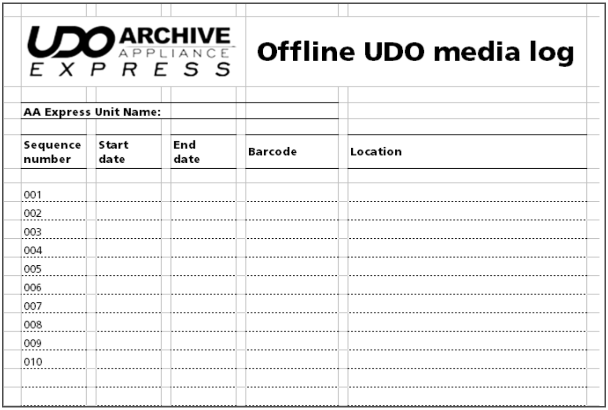
Offline media is stored by sequence number. If required, the correct media can be further verified by referencing the date range requested by the AA Express with that entered on the media label.

By date range

Offline media is stored chronologically by end date (date media was closed). If required, the media can be then further verified by referencing the sequence number requested by the AA Express with that entered on the media label.

By barcode

Offline media is organised according to barcode. In order to determine which media is required, it is necessary to create a spreadsheet or table similar to the example below to reference the sequence number of the media and/or the date range of the media against the barcode. A template is provided (in Microsoft Excel format) on the Resource CD supplied with the AA Express.



UDO ARCHIVE APPLIANCE EXPRESS

Offline UDO media log

AA Express Unit Name:

Sequence number	Start date	End date	Barcode	Location
001				
002				
003				
004				
005				
006				
007				
008				
009				
010				

At the storage location, media should be organized using the last three characters of the barcode label in ascending alphanumeric order.

Note: Barcode labels use an additional colour coding system to act as a visual aid in locating media. The Plasmon AA Express *barcode label number associated with a piece of media is unique.*

Chapter 15

Glossary of terms

Glossary of terms

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

Table 15-1:

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.
FTP	File Transfer Protocol - a protocol used for transferring data files across a TCP/IP network.

Table 15-1:

Term	Meaning
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.
Migration	Moving files from the Appliance's RAID storage volume to UDO media.

Table 15-1:

Term	Meaning
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.
Resync	Following a single disk RAID failure, data on the remaining operational disk(s) is used to rebuild the data set on a replacement disk.

Table 15-1:

Term	Meaning
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 de-facto 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.
SSH	Secure SHell, a protocol that allows data to be transferred securely between two hosts.

Table 15-1:

Term	Meaning
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 - Alliance’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.

Page left intentionally blank

Contact details

Alliance Storage Technologies Inc.
10045 Federal Drive
Colorado Springs, CO 80908 USA

Sales

email: sales@astiusa.com
web: www.astiusa.com /
www.plasmon.com

Tel: 719.593.7900
Fax: 719.593.4164

Support

email: tech.support@astiusa.com

Tel: 877.585.6793 / 719.593.4437
Fax: 719.593.4164

Alliance
Storage Technologies Inc.

Plasmon