UDO ARCHIVE APPLIANCE EXPRESS

ADMINISTRATOR'S GUIDE

Plasmon

Preliminaries

Copyright statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative, such as translation, transformation, or adaptation, without permission from Plasmon PLC.

Trademarks

Plasmon, **UDO**, **Archive Appliance**, **Archive Appliance Express**, **Discover Appliance**, **NetArchive**, **DiskArchive**, **Archive File Manager**, **Enterprise Active** and **Business Archive Maturity Model**. are registered trademarks of Plasmon PLC Copyright 2008.

Other names and/or trademarks belong to their respective proprietors.

Limited warranty

Plasmon PLC makes no representation or warranties with respect to the contents or use of this user's guide, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Plasmon PLC reserves the right to make revisions on this documentation without obligation to notify any person or entity of such changes.

Changes

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

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

Additional information may be obtained from your supplier, or from the addresses on page iv.

Safety

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

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

FCC note

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

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

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

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

Contact details

Europe, Middle East and Africa

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

Email: emea.sales@plasmon.com

Web: www.plasmon.com

Tel +44 (0) 1763 264 400
Fax +44 (0) 1763 264 444

North America, South America and Asia Pacific

Plasmon Inc.
370 Interlocken Blvd,

Suite 600
Broomfield
CO 80021
United States of America

Email: emea.sales@plasmon.com

Web: www.plasmon.com

Tel: +1-720-873-2500

Fax: +1-720-873-2501

How to use this guide

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

Related documentation

Please refer to the following document for further information:

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

Revision history

Document revision number	System software version	Author	Major Features
860-102721-01 Rev A	4.08.xx	Christian McCormack	- Replication.
860-102721-02 Rev A	4.11.xx	Trudi Topham	- UDO Guard - Remote Management - Network Backup

Contents

Page left intentionally blank

UDO ARCHIVE APPLIANCE EXPRESS

Chapter 1

Introduction

Appliance concept

The Plasmon UDO Archive Appliance Express (hereafter referred to as the AA 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 AA Express over a TCP/IP connection. As the low cost offering in the Archive Appliance family, the AA Express utilizes manual off-line management of UDO media. The web interface is common across the Archive Appliance family allowing operators to easily transfer their knowledge as archive storage requirements change.

UDO technology

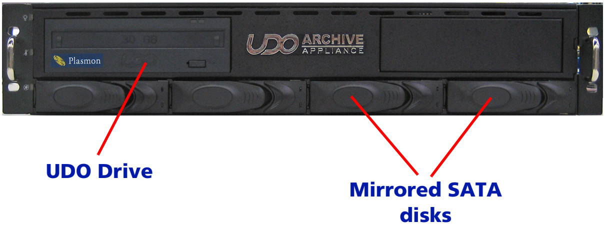
UDO™ (Ultra Density Optical), based on blue laser technology, is the underlying foundation to Plasmon's archive solution portfolio, including the AA Express. It’s the first storage technology specifically designed for long-term professional data archive requirements. UDO provides absolute data authenticity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

Blue lasers achieve far greater data densities, resulting in dramatically higher media capacities. First and second generation UDO products (UDO and UDO 2) have a storage capacity of 30GB and 60 GB respectively, with capacity expected to reach 120GB by the third generation.

AA Express hardware

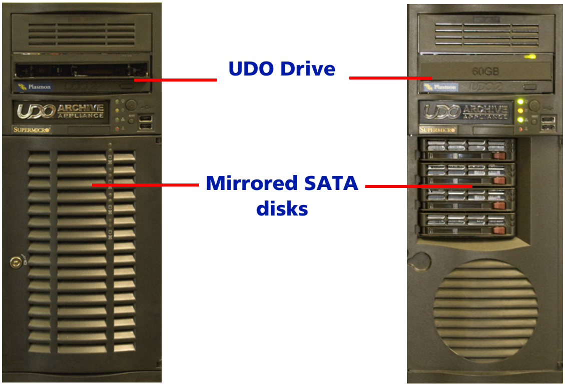
The AA Express consists of:

- 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 consists of:

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



AA Express supported RAID configurations

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

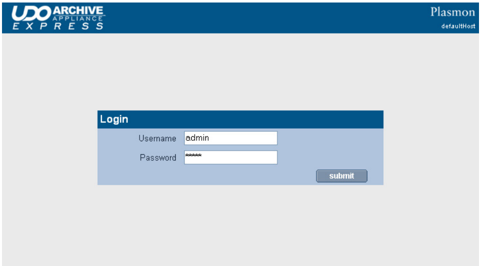
- 2 SATA disks in a RAID 1 (mirrored pair) configuration.
- 2 SATA disks in a RAID 1 (mirrored pair) configuration with a third SATA disk configured as a Hot Spare.
- 4 SATA Disks in a RAID 5 configuration.

Chapter 2

The Archive Appliance Express

Starting the Web Interface

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



Username admin

Password ******

3. Enter a valid AA Express Administrator User Name and Password.
   - This is not the same as a Windows Domain Administrator.
   - The default administrator username and password is **admin**. It is reccommended that this is changed on first login (“Modifying a User’s details” on page 40).
   - The default administrator can be used to add or remove additional administrator accounts.
4. Click **OK**.
   The Web Interface **System - Status** page is displayed.

System - Status page features

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

Menu bar

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

Table 1: Web interface menu bar

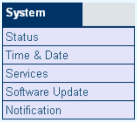
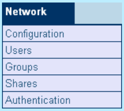
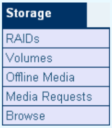
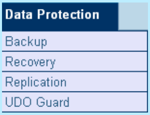
Menu/icon	Use to
 System Status Time & Date Services Software Update Notification	Monitor the AA Express’ status, set the time & date, monitor and configure the services, update the system software and configure alert notifications
 Network Configuration Users Groups Shares Authentication	Define the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

Table 1: Web interface menu bar

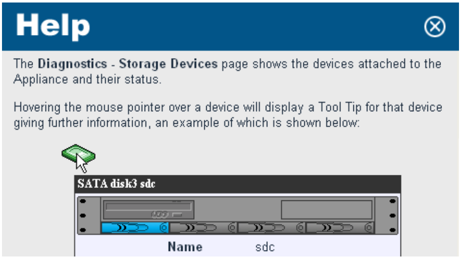
Menu/icon	Use to
Diagnostics System Jobs Storage Devices UDO Drives Self Tests System Information	Monitor system jobs and devices (disks, libraries, etc.), perform self tests, view system information (software version, serial numbers, hardware revisions, etc.) and create a log file bundle
Shutdown	Reboot or shut down the AA Express.
?	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 AA Express Help page will open in a pop-up browser Window, e.g.:



Help

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

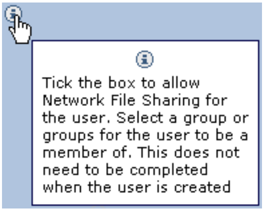
Hovering the mouse pointer over a device will display a Tool Tip for that device giving further information, an example of which is shown below:

SATA disk3 sdc

Name sdc

Tool Tips

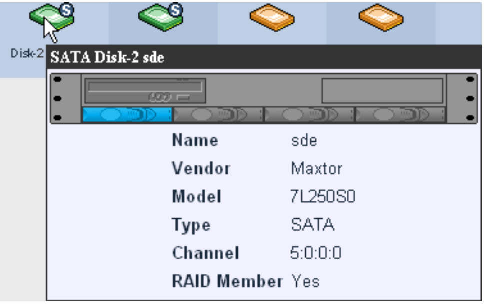
Hovering the mouse pointer over the tool tip icon icon displays a text box detailing key features of that field or function, e.g.:



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 attached that provide diagnostic information. These are:

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



SATA Disk-2 sde

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

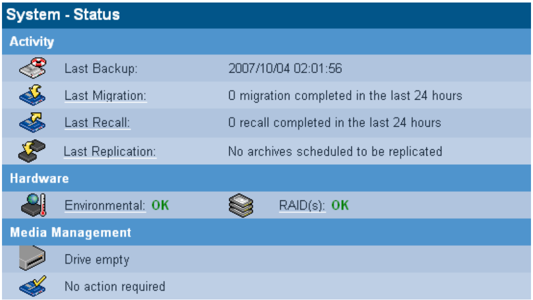
Page left intentionally blank

Chapter 3

System menu

System Status

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



System - Status

Activity

Last Backup:	2007/10/04 02:01:56
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

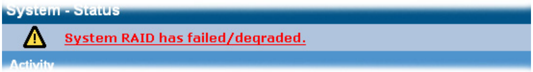
Media Management

Drive empty

No action required

The page is divided into four areas:

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



System - Status

⚠ System RAID has failed/degraded.

Activity

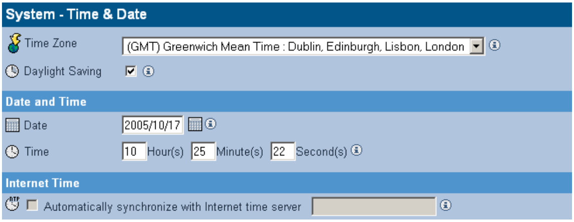
- The **Activity** area displays the time of the **Last Backup**, **Last Migration**, **Last Recall** and **Last Replication**.
- The **Hardware** area indicates the **Environmental** status of the hardware and the status of the **RAID(s)**.
- The **Media Management** area displays information about the currently loaded media and indicates what, if any, operator action is required.

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

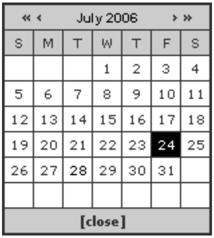
Date: 2005/10/17

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	

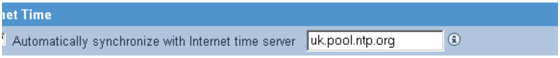
[close]

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 AA Express will reboot. Ensure that no users are connected before proceeding.

Synchronising the time and date with an NTP server

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



et Time

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

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

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

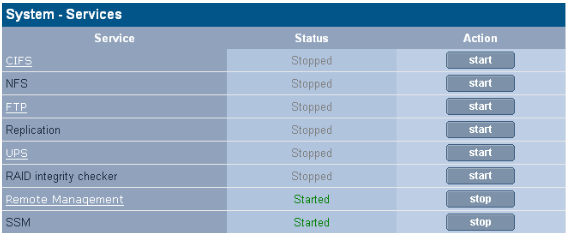
3. The connection to the NTP server may be tested by clicking the **test ntp** button.

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

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

Note: If 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
CIFS	Stopped	start
NFS	Stopped	start
FTP	Stopped	start
Replication	Stopped	start
UPS	Stopped	start
RAID integrity checker	Stopped	start
Remote Management	Started	stop
SSM	Started	stop

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

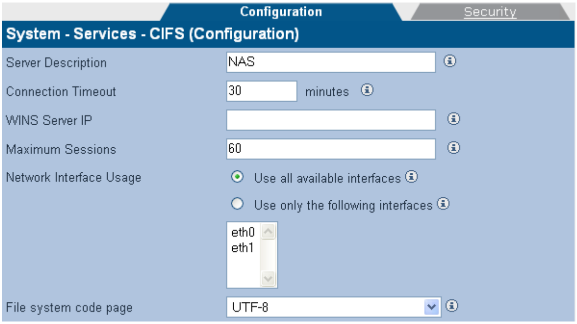
- **CIFS (Common Internet File System)** - also known as SMB (Server Message Block), is the communications protocol used by Windows-based operating systems to support sharing of resources across a network - see page 16
- **NFS (Network File System)** - is a method of making a remote filesystem accessible on the local system. From a user's perspective, an NFS-mounted filesystem is indistinguishable from a filesystem on a directly-attached disk drive. There are no configurable options for the NFS service; however when creating shares using NFS, Host Entry attributes must be configured - see page 47.
- **FTP (File Transfer Protocol)** - FTP is a protocol which allows a user on one host to access, and transfer files to and from, another host over a network - see page 18
- **Replication** - This service controls replication between the AA Express and a partnered AA Express - see page 92.
- **UPS (Uninterruptible Power Supply)** - Displays the status of an attached APC SmartUPS if one is present - see page 20
- **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.
- **Remote Management** - If included in your service contract, the Remote Management service allows Plasmon Technical Support to monitor and troubleshoot the Appliance securely across the Internet - see page 22.

- **SSM (Storage Space Manager)** - Start or stop the HSM (Hierarchical Storage Management) software on the AA Express. 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.

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

Configuring CIFS (Windows Networking)

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
Network Interface Usage	● Use all available interfaces ○ Use only the following interfaces eth0 eth1
File system code page	UTF-8

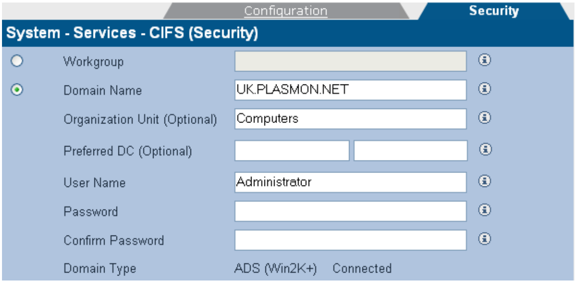
2. Enter a **Server Description**.
   This is the name by which the AA Express advertises itself on the Windows network.
3. If required, enter a **Connection Timeout** in minutes.
   This is the amount of time that connections may remain idle, with no open files, before disconnecting them from the share. 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 Appliance will accept. The default is 60 sessions.

6. **Network Interface Usage**, offers the following options:
   - **Using all available interfaces** - to use any and all available network ports
   - **Using the following interfaces** - to the network port(s) specified from the list.
   - 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 AA Express' 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 AA Express to authenticate share users against a Windows domain and create file permissions for them. By configuring the Windows Domain security, the AA Express has access to all domain users. These users can then be added to the access control list (ACL) from the **Network - Shares - Update (Access)** and the **Storage - Browse - Access (Access)** pages of the Web interface.



System - Services - CIFS (Security)

○	Workgroup	
●	Domain Name	UK.PLASMON.NET
	Organization Unit (Optional)	Computers
	Preferred DC (Optional)	
	User Name	Administrator
	Password	
	Confirm Password	
	Domain Type	ADS (Win2K+) Connected

2. Enter either:

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

   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 AA Express to a Domain, additional details may be required:

- Up to two **Preferred DC**'s may be specified if desired, and the Appliance will attempt to connect to them in order.
- The **Organizational Unit** (OU) within the Active Directory structure in which the AA Express will appear, (by default, the AA Express will appear in the *Computers* OU).
- A Windows **User Name** with the right 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**.

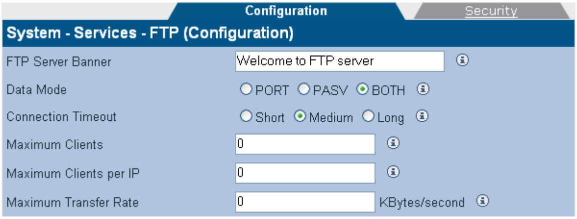
Click **save** to save the changes, **stop** to stop the CIFS service, or **diagnose** to diagnose connectivity problems.

NFS

The NFS networking service is configured via the **Network - Shares** page - see page 44.

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

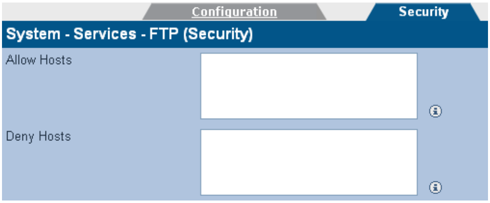
2. If required, enter an **FTP Server Banner**. This is a message which will be displayed to users when they access the AA Express via FTP.
3. Enter a **Data Mode**. The data mode can be:
   - **PORT** - Also known as Active mode.
   - **PASV** - Passive mode.
   - **BOTH** - The FTP client defines the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

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.



System - Services - FTP (Security)

Allow Hosts	
Deny Hosts	

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

UPS

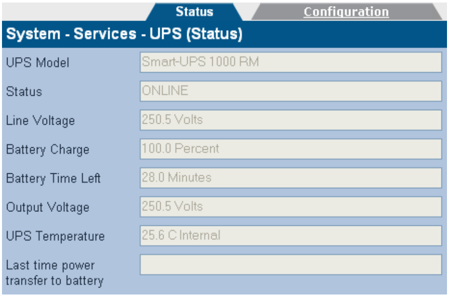
The information in the **System - Services - UPS** page is derived from the Uninterruptable Power Supply (UPS) itself.

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

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

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

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



System - Services - UPS (Status)

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

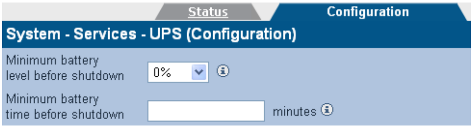
   The following information is displayed:

   - **UPS Model** - The model code of the UPS attached to the Appliance

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

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

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

   System - Services - UPS (Configuration)

   Minimum battery level before shutdown: 0%

   Minimum battery time before shutdown: minutes

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

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

3. Click **save** to save any changes.

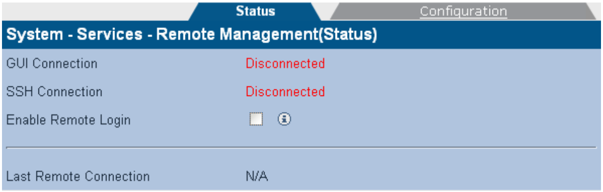
Remote Management

The Remote Management service allows Plasmon technical support to monitor the Appliance and perform selected maintenance and support tasks on a customer’s Appliance securely over the internet.

> *Note: Remote management is only available if included as part of the service contract.*

The **System - Services - Remote Management** page displays the current status of any Remote Management sessions, and enables configuration of the Remote Management service.

1. From the **System - Services** page click on **Remote Management**.
2. The **Remote Management (Status)** page opens:



System - Services - Remote Management(Status)

GUI Connection	Disconnected
SSH Connection	Disconnected
Enable Remote Login	□ ⓘ
Last Remote Connection	N/A

- **GUI Connection** - Indicates whether the Appliance is ready to allow Plasmon support remote access to the web interface.
- **SSH Connection** - Indicates whether the Appliance is ready to allow Plasmon support remote access to the command-line interface (SSH).

For both connection types the status will display:

Connected - if Remote Access is enabled and the Appliance is ready to allow connections from plasmon support.

Disconnected - If Remote Access is disabled.

- **Enable Remote Login** - Click the checkbox to enable GUI and SSH connections, or clear the checkbox to disable. The default state is disabled.

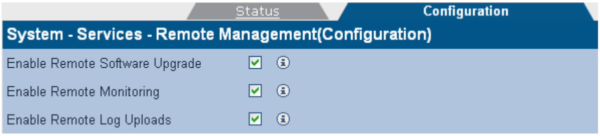
> *Note: It is recommended that remote login be enabled only when requested by Plasmon Support.*

- **Last Remote Connection** - Displays the time and date of the last successful remote management connection.

Click **save** to save any changes.

3. Click the **Configuration** tab.

   The **Remote Management (Configuration)** page opens:



System - Services - Remote Management(Configuration)

Enable Remote Software Upgrade ☑ ⓘ

Enable Remote Monitoring ☑ ⓘ

Enable Remote Log Uploads ☑ ⓘ

- **Enable Remote Software Upgrade** - Allows Plasmon technical support to apply software upgrades to the Appliance remotely.
- **Enable Remote Monitoring** - Allows Plasmon technical support to monitor the Appliance remotely.
- **Enable Remote Log Uploads** - Allows the Appliance to upload it’s log files directly to Plasmon.

By default these options are enabled. If required, clear the relevant checkbox to disable a service.

Click on **save** to save any changes.

4. Click **back** to return to the **System - Services** page.

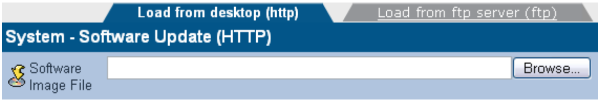
Update the System Software

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 Plasmon 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:



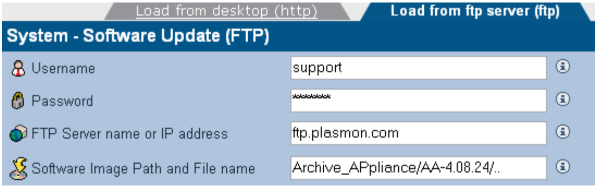
3. Enter the **Software Image File** path to a local copy of the Appliance software image or click **browse** to locate the image file.
4. Click **transfer** to begin the software update.

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 Plasmon 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.
6. Follow the on-screen instructions to complete the installation.

Notification

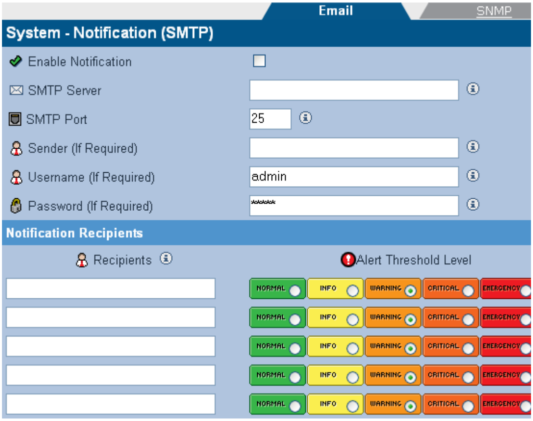
The AA Express can notify system administrators of system events and errors by:

- Email (Simple Mail Transfer Protocol - SMTP) Notification - see below
- Simple Network Management Protocol (SNMP) Notification - see page 27.
- A history of the notifications can be viewed via the Web interface, and should be regularly reviewed and its contents cleared (see page 29).

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

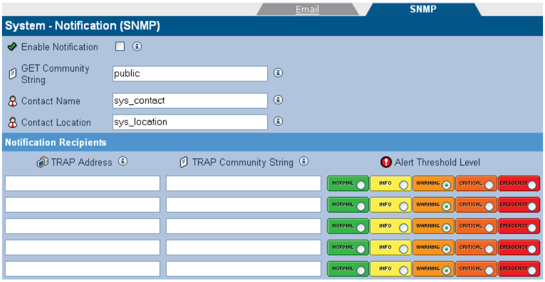
6. If required, add a **Username** to the notifications. If a username is added, that user's **Password** must also be entered.
7. Enter the email address(es) of up to five email notification **Recipients**.
8. Select an **Alert Threshold Level** for each recipient. These are described in *Table 3-1*.

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

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

Configure SNMP Notification

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



System - Notification (SNMP)

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

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

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

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

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

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

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

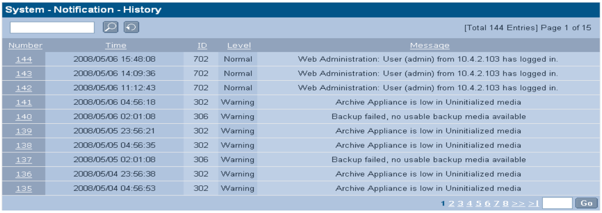
Table 3-1. Notification Alert Threshold Levels

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

Notification history

The AA Express maintains a log of all notifications that have been 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 any required actions have been performed, click **delete all**.
6. A warning that all event logs will be deleted is displayed. Click **delete all** again to confirm.

Page left intentionally blank

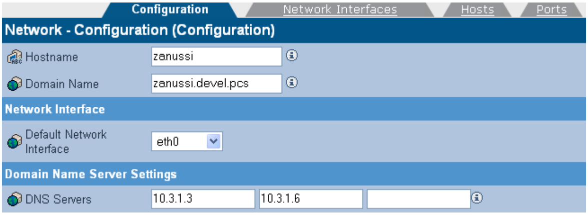
Chapter 4

Network menu

Network Settings

Configuration

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



Network - Configuration (Configuration)

Hostname	zanussi
Domain Name	zanussi.devel.pcs

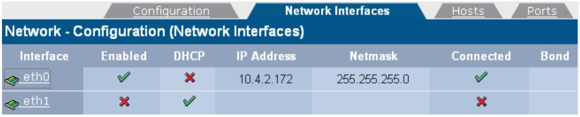
Network Interface

Default Network Interface	eth0

Domain Name Server Settings

DNS Servers	10.3.1.3	10.3.1.6	

2. Enter a **Hostname** for the AA Express
3. Enter the **Domain Name** which the AA Express 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.
6. Click on the **Network Interfaces** tab. The AA Express's network (Ethernet) ports are listed:



Network - Configuration (Network Interfaces)

Interface	Enabled	DHCP	IP Address	Netmask	Connected	Bond
eth0	✓	✗	10.4.2.172	255.255.255.0	✓	
eth1	✗	✓			✗	

The following information is also displayed:

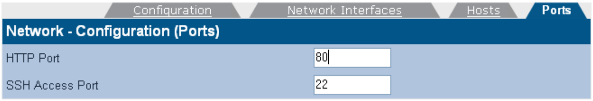
- **Name** - The Ethernet port name, *eth0* or *eth1*. Clicking on the port name displays the network port's configuration.
- **Enabled** - Indicates whether the Ethernet port is enabled
- **DHCP** - Indicates whether Dynamic Host Configuration Protocol (DHCP) is enabled.

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** - Whether or not the ports are bonded. This is used to provide load balancing (where the two ethernet cards share network activity to prevent overloading) or fault tolerance (where one ethernet card is used, the other being kept as a backup in case of failure of the first).

7. Click on the **Ports** tab. The AA Express' TCP/IP ports are listed:



Network - Configuration (Ports)

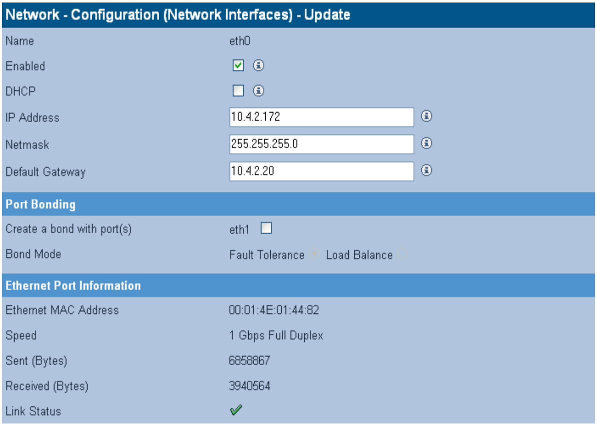
HTTP Port	80
SSH Access Port	22

- **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 Plasmon support engineers when accessing the web interface remotely. See "Remote Archive Manager" on page 24.
- **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 Plasmon support engineers when accessing the command-line interface remotely. See "Remote Archive Manager" on page 24.

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:

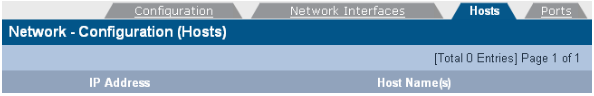


Network - Configuration (Network Interfaces) - Update	
Name	eth0
Enabled	☑
DHCP	□
IP Address	10.4.2.172
Netmask	255.255.255.0
Default Gateway	10.4.2.20
Port Bonding	
Create a bond with port(s)	eth1 □
Bond Mode	Fault Tolerance ○ Load Balance ○
Ethernet Port Information	
Ethernet MAC Address	00:01:4E:01:44:82
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

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



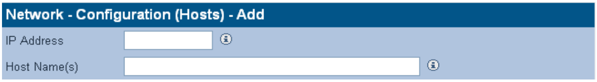
Network - Configuration (Hosts)

[Total 0 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 Hostname, 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 32) 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 AA Express 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 Appliance, whether defined locally or sourced from an Active Directory domain or LDAP server.

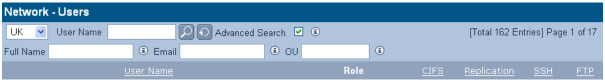
By default the locally defined users are listed. If the Appliance has been configured to include users from an external directory, the drop-down box will become active, and any configured external directory may be selected.

Note: 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

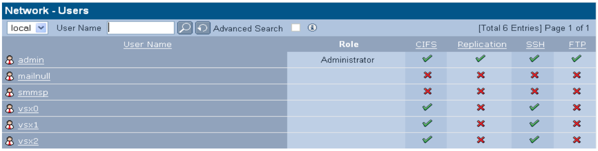
Full Name | Email | OU

User Name	Role	CIFS	Replication	SSH	FTP

It is possible to search using a user's **User Name**, **Full Name**, **Email** or **OU** (Organisational 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**.

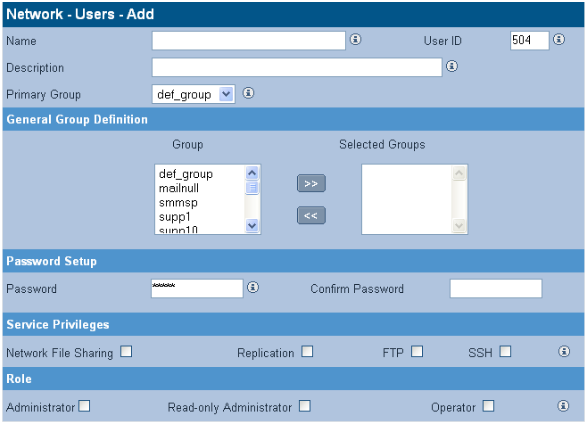


Network - Users

local ▾ User Name [ ] Advanced Search □ [Total 6 Entries] Page 1 of 1

User Name	Role	CIFS	Replication	SSH	FTP
admin	Administrator	✓	✓	✓	✓
mailnull		✗	✗	✗	✗
smmsp		✗	✗	✗	✗
vsx0		✓	✗	✓	✗
vsx1		✓	✗	✓	✗
vsx2		✓	✗	✓	✗

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: (empty)

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.*

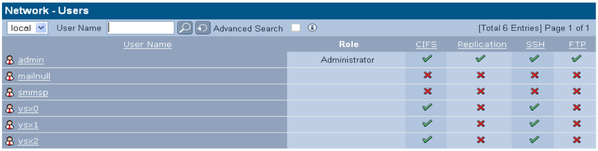
4. Enter a **Description** for the User.
5. Select a **Primary Group** for the user to be a member of. The default group is `def_group`.
6. In the **General Group Definition** area, additional groups may be selected for the user to be a member of. Click any required group(s) in the **Group** list (CTRL-click 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** (this is mandatory).
8. Tick the **Network File Sharing** box 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 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 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.
13. An **Operator** has read-only access to the Web Interface, limited to the **System - Status**, **Storage - Online Media** and **Storage - Offline Media** pages. required, select the **Full Control** radio button.
14. Click **add** to add the User.

Deleting a User

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



Network - Users

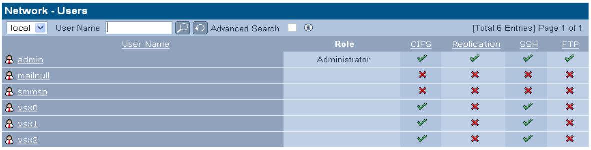
local User Name Advanced Search [Total 6 Entries] Page 1 of 1

User Name	Role	CIFS	Replication	SSH	FTP
admin	Administrator	✓	✓	✓	✓
mailnull		✗	✗	✗	✗
smmsp		✗	✗	✗	✗
vsx0		✓	✗	✓	✗
vsx1		✓	✗	✓	✗
vsx2		✓	✗	✓	✗

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

Modifying a User's details

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

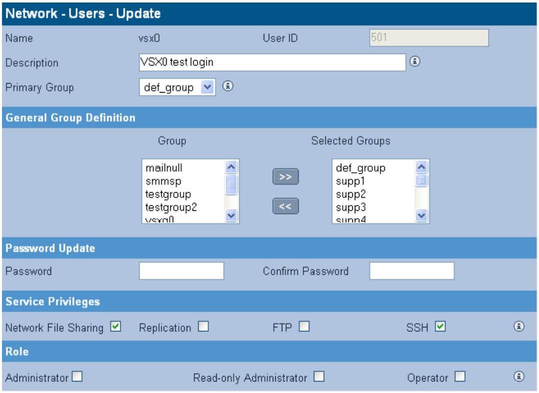


Network - Users

local ▾ User Name [ ] Advanced Search □ [Total 6 Entries] Page 1 of 1

User Name	Role	CIFS	Replication	SSH	FTP
admin	Administrator	✓	✓	✓	✓
mailnull		✗	✗	✗	✗
smmsp		✗	✗	✗	✗
vsx0		✓	✗	✓	✗
vsx1		✓	✗	✓	✗
vsx2		✓	✗	✓	✗

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

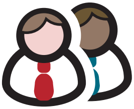
Network File Sharing ☑ Replication □ FTP □ SSH ☑

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.

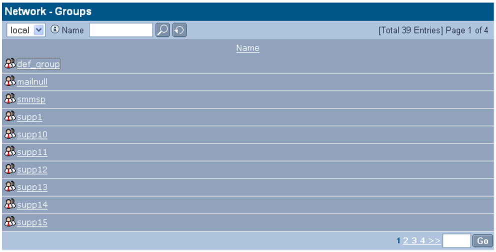
Groups



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

Adding a Group

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



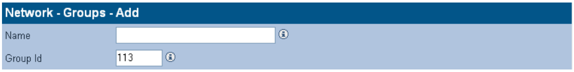
Network - Groups

local Name [Total 39 Entries] Page 1 of 4

Name
def_group
mailnull
smmsp
supp1
supp10
supp11
supp12
supp13
supp14
supp15

1 2 3 4 >> Go

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



Network - Groups - Add

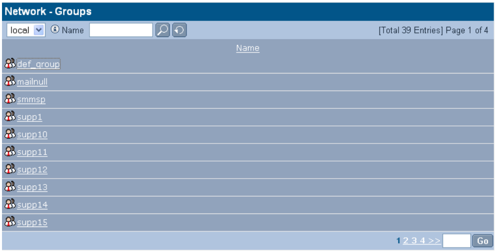
Name	
Group Id	113

3. Enter a **Name** for the Group.
4. Click **add** to add the Group.

Editing a Group

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

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

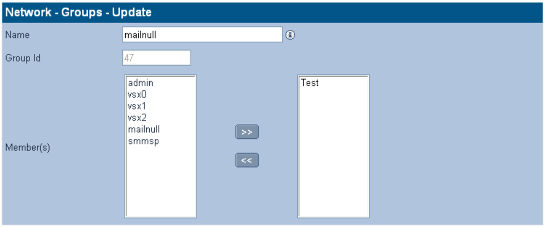


Network - Groups

local Name [Total 39 Entries] Page 1 of 4

Name
def_group
mailnull
smmsp
supp1
supp10
supp11
supp12
supp13
supp14
supp15

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



Network - Groups - Update

Name: mailnull

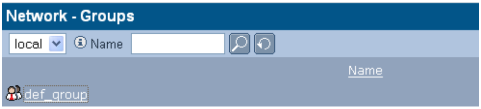
Group Id: 47

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

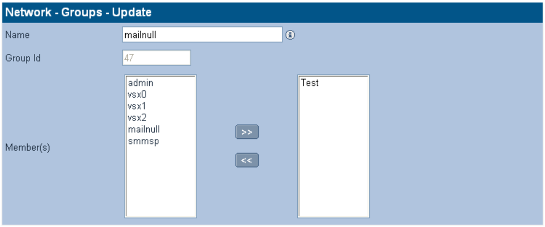
1. From the menu bar, select **Network - Groups**.



Network - Groups

local ▾ Name

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.

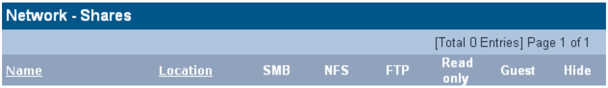
Shares

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

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

Adding a Share

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

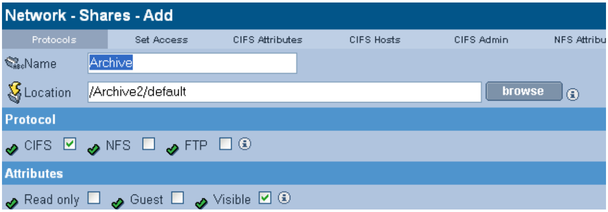


Network - Shares

[Total 0 Entries] Page 1 of 1

Name	Location	SMB	NFS	FTP	Read only	Guest	Hide

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



Network - Shares - Add

Name: Archive

Location: /Archive2/default

Protocol

CIFS ☑ NFS ☐ FTP ☐

Attributes

Read only ☐ Guest ☐ Visible ☑

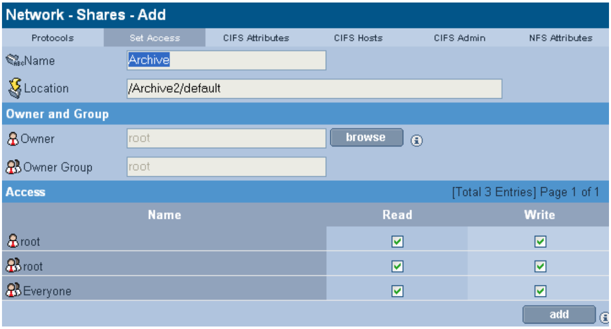
3. Enter a **Name** for the Share.
4. Enter a **Location** for the Share or click **browse** to browse for a location.
5. Tick the relevant **Protocol** box(es). This defines how the Users may access the Share. The Appliance can share files via Common Internet File System (**CIFS**), Network File System (**NFS**) and File Transfer Protocol (**FTP**).

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

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

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

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



Network - Shares - Add

Name: Archive

Location: /Archive2/default

Owner and Group

Owner: root

Owner Group: root

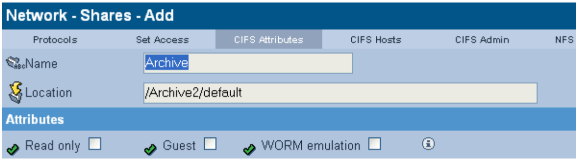
Access [Total 3 Entries] Page 1 of 1

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

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

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

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



Network - Shares - Add

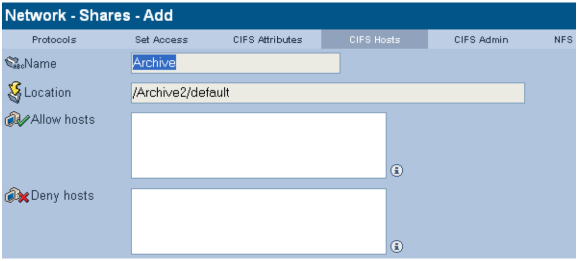
Name: Archive

Location: /Archive2/default

Attributes

Read only □ Guest □ WORM emulation □

11. Enter the **Attributes** for Windows (SMB) access to the Share.
12. Click **next >>**. The **CIFS Hosts** tab is displayed:



Network - Shares - Add

Name: Archive

Location: /Archive2/default

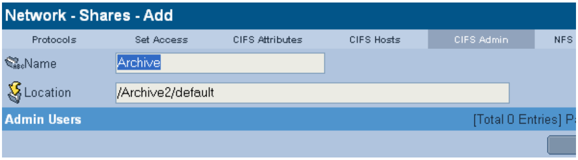
Allow hosts:

Deny hosts:

Enter the hostnames or IP addresses of Hosts that are to be specifically allowed or denied access to the Share.

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

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



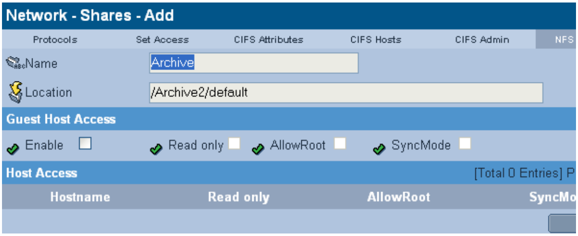
Network - Shares - Add

Name: Archive

Location: /Archive2/default

Admin Users [Total 0 Entries] P

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

Name: Archive

Location: /Archive2/default

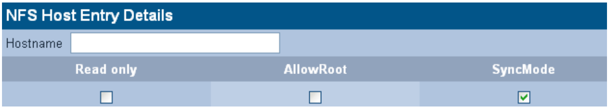
Guest Host Access

Enable □ Read only □ AllowRoot □ SyncMode □

Host Access [Total 0 Entries] P

Hostname	Read only	AllowRoot	SyncMo

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



NFS Host Entry Details

Hostname

Read only	AllowRoot	SyncMode
☐	☐	☑

Enter the Hostname, then tick the boxes as required:

- **Read only** - Allow Read Only access to the share.
- **AllowRoot** - allows root user access to the share.
- **SyncMode** - (disabled by default) can improve performance at the risk of filesystem fragmentation when reading or writing large amounts of small files.

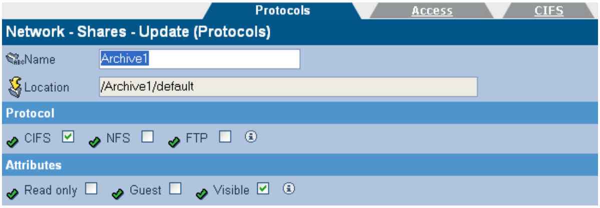
Click **ok** to continue.

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: Archive1

Location: /Archive1/default

Protocol

CIFS ☑ NFS ☐ FTP ☐

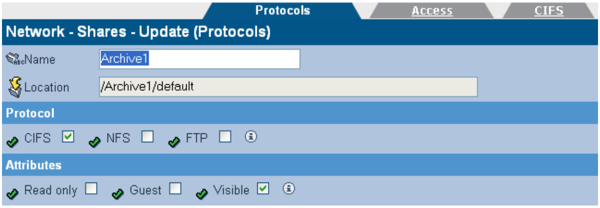
Attributes

Read only ☐ Guest ☐ Visible ☑

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

Modifying a share

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



Network - Shares - Update (Protocols)

Name: Archive1

Location: /Archive1/default

Protocol

CIFS ☑ NFS □ FTP □

Attributes

Read only □ Guest □ Visible ☑

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

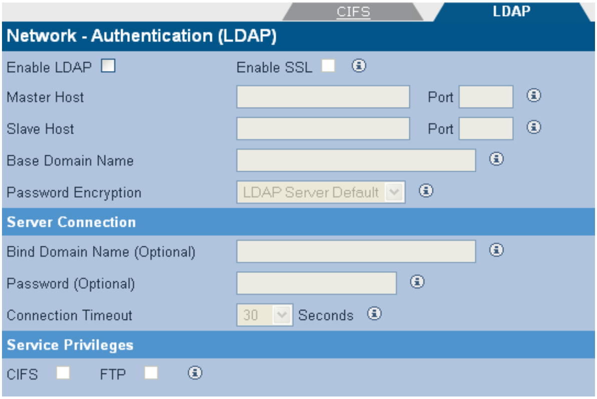
Note: For in-depth detail on the options available in each tab, see See “Adding a Share” on page 44.

Authentication

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

LDAP configuration

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



Network - Authentication (LDAP)

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

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

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

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

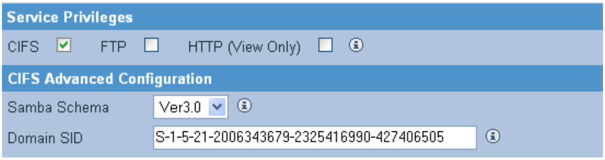
Service Privileges

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

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

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

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



Service Privileges

CIFS ☑ FTP □ HTTP (View Only) □

CIFS Advanced Configuration

Samba Schema: Ver3.0

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

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

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

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

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

LDAP Service authentication configuration

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

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

OpenLDAP

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

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

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

iPlanet

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

Novell eDirectory

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

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

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

Most commonly used Samba schema attributes

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

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

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

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

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

2 Set the following attributes:

For Samba Schema 2.2

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

For example, `4097804623`

lmPassword - LanManager hashed password

ntPassword - Windows NT hashed password

For Samba Schema 3.3

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

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

sambaLMPassword
sambaNTPassword

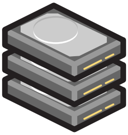
CIFS

1. The information in this tab is derived from, the **System - Services (CIFS)** page. Refer to "Configuring CIFS (Windows Networking)" on page 16.

Chapter 5

Storage menu

RAIDs

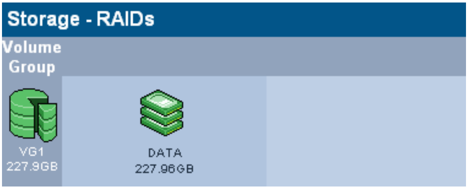


The **Storage - RAIDs** page allows viewing of RAIDs (Redundant Array of Independent Disks) on the system. Global hot spare disks can also be defined.

> *Note: Depending on the number of SATA disks in the enclosure, the AA Express RAID configuration is limited to a single RAID 1 (mirrored pair) or a single RAID 5 (parity stripe). Either RAID configuration may utilize a hot spare disk.*

Viewing the RAID

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



Storage - RAIDs

Volume Group

VG1 227.9GB

DATA 227.96GB

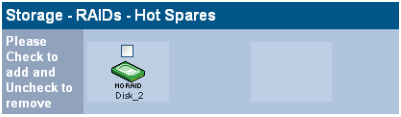
2. Hover over a Volume Group or RAID for a Tool Tip containing status information.

Assigning a global hot spare disk to the RAID

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

> *Note: A hot spare disk can only be defined if the system has a free disk available.*

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



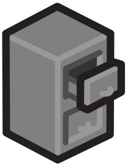
Storage - RAIDs - Hot Spares

Please Check to add and Uncheck to remove

□ NO RAID Disk_2

3. Tick the box of the disk to mark as hot spare.

   Click set to set the hot spare.
4. Click save to save the changes and return to the **Storage - RAIDs** page.



The **Storage - Volumes** page can view or change volumes

About volumes

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

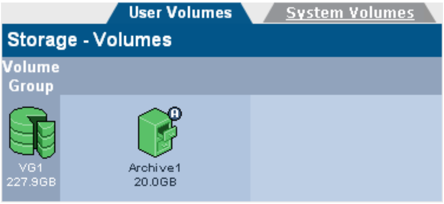
On the AA Express, two types of volume are available:

- An archive - where data is written to the Appliance's RAID(s) and, when defined criteria have been met, the data is migrated onto UDO media - see *Creating an archive* on page 55.
- An unmanaged volume - where data is written to the Appliance's RAID cache only - see *Creating an unmanaged volume* on page 64.

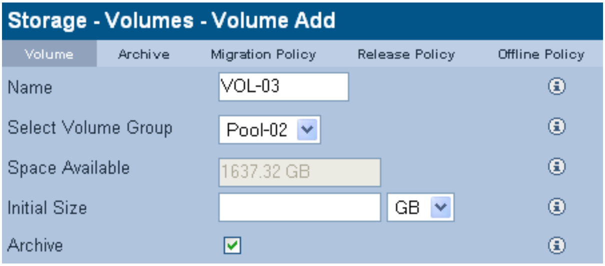
Note: The AA Express may only have one archive. Multiple unmanaged volumes can be configured.

Creating an archive

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

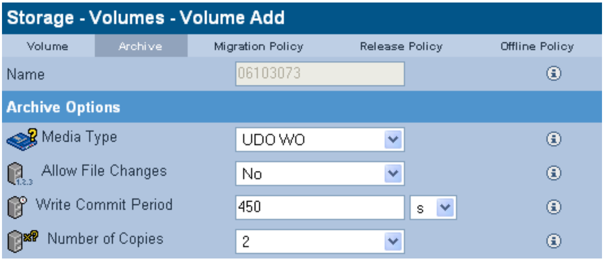


2. Click add.
   The **Storage -Volumes - Volume Add** page opens:



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

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



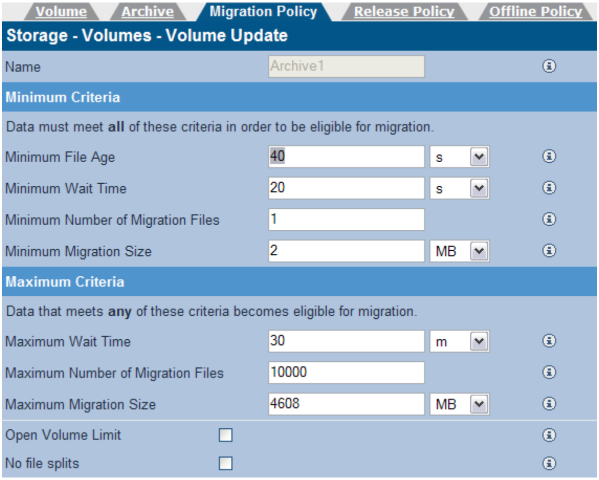
Storage - Volumes - Volume Add

Name	06103073

Archive Options

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

8. The **Media Type** the archive will use is **UDO WO** - UDO WORM media.
9. Select whether to **Allow File Changes**:
   - If **Yes** is selected then changes to the file are permitted at any time after the file is written and multiple versions of the file are stored.
   - If **No** is selected, a WORM filesystem is created. After the write commit period has expired, no further file changes are permitted.
10. Enter a **Write Commit Period** in **s**econds, **m**inutes or **h**ours. This sets the time period after the file is closed during which file updates can be made. After this time period has passed no further changes are permitted.
11. The **Number of Copies** is set to one and cannot be changed.
12. Click next >> to continue.
    The **Storage -Volumes - Volume Add** page, **Migration Policy** tab opens:



Storage - Volumes - Volume Update

Name	Archive1		

Minimum Criteria

Data must meet **all** of these criteria in order to be eligible for migration.

Minimum File Age	40	s
Minimum Wait Time	20	s
Minimum Number of Migration Files	1	
Minimum Migration Size	2	MB

Maximum Criteria

Data that meets **any** of these criteria becomes eligible for migration.

Maximum Wait Time	30	m
Maximum Number of Migration Files	10000	
Maximum Migration Size	4608	MB

Open Volume Limit ☐

No file splits ☐

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

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

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

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

Example 1 - Migration default settings

With the following minimum settings:

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

and the following maximum settings:

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

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

Example 2 - Frequent, low data volume

With the following minimum settings:

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

and the following maximum settings:

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

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

Example 3 - Less frequent, greater data volume

With the following minimum settings:

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

and the following maximum settings:

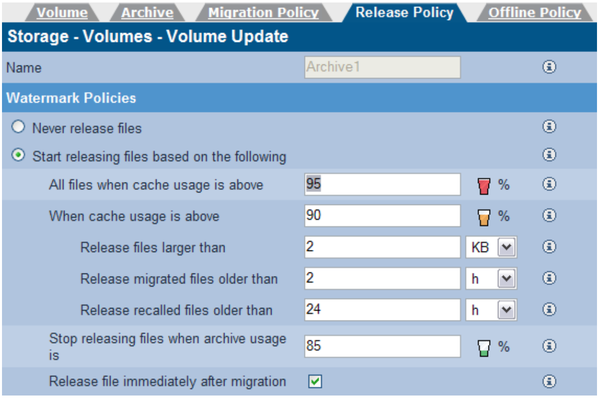
- **Maximum Wait Time:** 4 Hours
- **Maximum Number of Migration files:** 10000
- **Maximum migration size:** 4.5 GB

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

Table 5-1: 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

15. 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.

16. 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.

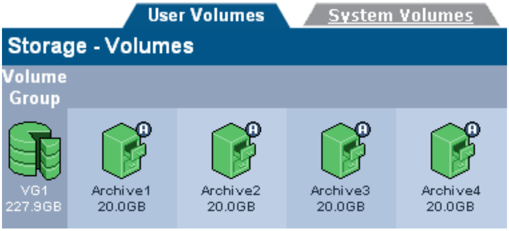
    - **Release recalled files older than:** Only files that have been recalled longer than the specified time will be released.
  - **Stop releasing files when archive usage is**: When RAID cache usage reaches the specified percentage, files stop being released.
  - **Release files immediately after migration:**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

17. Click add.

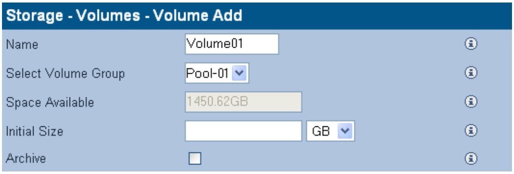
    Once the volume has been created, the Appliance will return to the **Storage - Volumes** page.

Creating an unmanaged volume

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



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



Storage - Volumes - Volume Add

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

3. A **Name** is automatically generated, or can 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 Volume Group** displays the Volume Group that the new volume will be a member of.
5. The **Space Available** is shown.

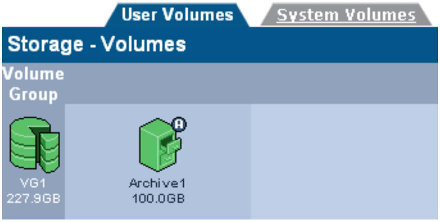
Caution: Volume size can be increased after creation. However, the size of a volume can only be reduced by removing the volume from the volume group and restoring from backup (we recommend that this only be performed by a Service Engineer). We recommend that during creation, the volume size is set to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

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

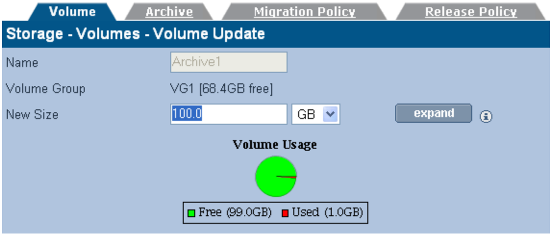
Click add. Once the volume has been created, the Appliance will return to the **Storage - Volumes** page.

Viewing and editing a volume’s properties

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



2. Click on the volume to be displayed.
   The **Storage -Volumes - Volume Update** page opens:



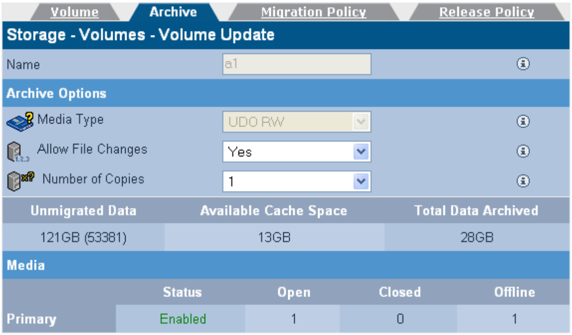
Name	Archive1
Volume Group	VG1 [68.4GB free]
New Size	100.0 GB

🟩 Free (99.0GB) 🟥 Used (1.0GB)

New Size - To change the size of the volume, enter a new size and click **expand.**

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

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



Storage - Volumes - Volume Update

Name: a1

Archive Options

Media Type	UDO RW
Allow File Changes	Yes
Number of Copies	1

Unmigrated Data	Available Cache Space	Total Data Archived
121GB (53381)	13GB	28GB

Media

	Status	Open	Closed	Offline
Primary	Enabled	1	0	1

Items that may be edited are:

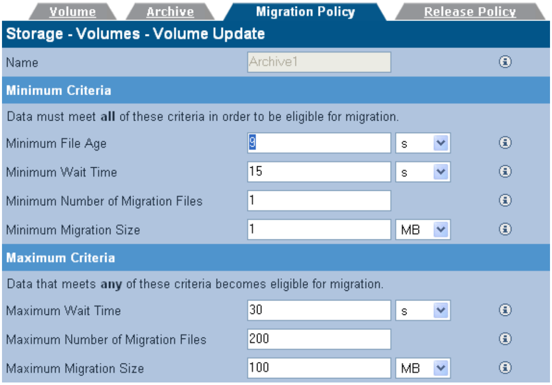
- **Allow File Changes**.
- **Write commit period**

Information-only fields are:

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

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



Storage - Volumes - Volume Update

Name	Archive1	
Minimum Criteria		
Data must meet **all** of these criteria in order to be eligible for migration.		
Minimum File Age	9	s
Minimum Wait Time	15	s
Minimum Number of Migration Files	1	
Minimum Migration Size	1	MB
Maximum Criteria		
Data that meets **any** of these criteria becomes eligible for migration.		
Maximum Wait Time	30	s
Maximum Number of Migration Files	200	
Maximum Migration Size	100	MB

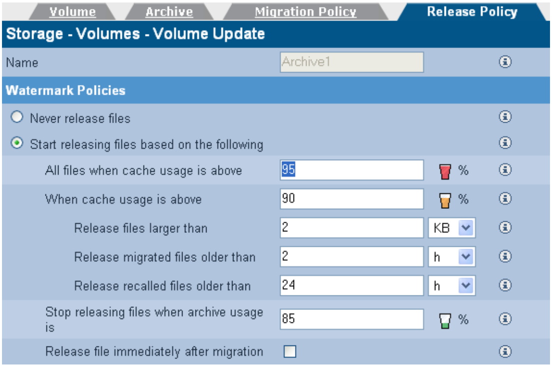
Items that may be edited are:

- **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**

Information-only fields are:

- **Name**

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



Storage - Volumes - Volume Update

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

Items that may be edited are:

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

Information-only fields are:

- **Name**

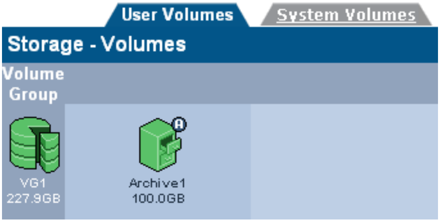
6. When any changes are complete, click **save** to save the changes.

Volume quotas

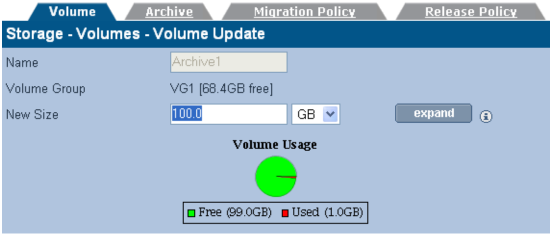
Users can be allocated a specific amount of the volume which they can use. This amount is called their quota.

Defining a user's quota

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

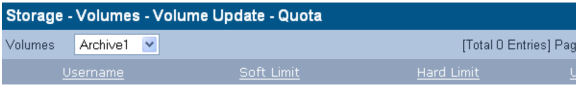


2. Click on the **Archive1** volume.
   The **Storage -Volumes - Volume Update** page opens:



Name: Archive1
Volume Group: VG1 [68.4GB free]
New Size: 100.0 GB
🟩 Free (99.0GB) 🟥 Used (1.0GB)

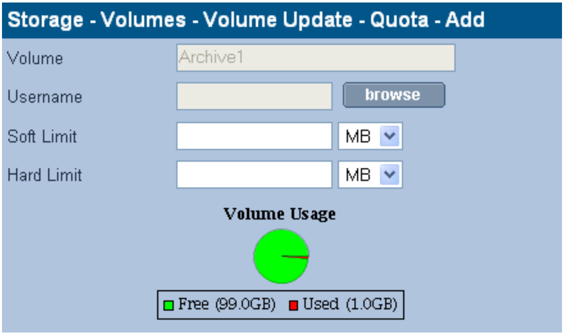
3. Click **quota**.
   The **Storage - Volumes - Volume Update - Quota** page opens:



Volumes: Archive1
[Total 0 Entries] Pag

4. Click **add**.

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



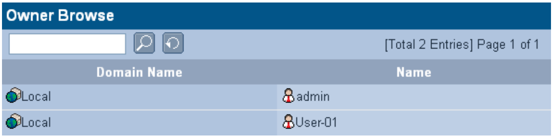
Storage - Volumes - Volume Update - Quota - Add

Volume	Archive1
Username	
Soft Limit	MB
Hard Limit	MB

Volume Usage

🟩 Free (99.0GB) 🟥 Used (1.0GB)

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

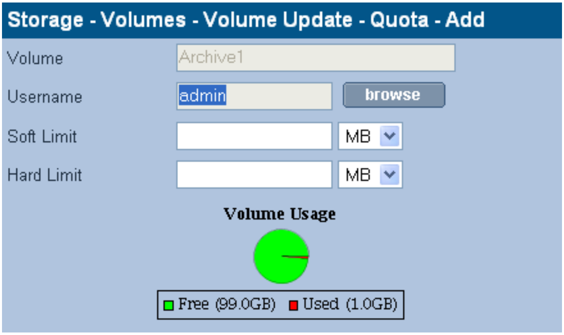


Owner Browse

[Total 2 Entries] Page 1 of 1

Domain Name	Name
Local	admin
Local	User-01

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



Storage - Volumes - Volume Update - Quota - Add

Volume	Archive1
Username	admin
Soft Limit	MB
Hard Limit	MB

Volume Usage

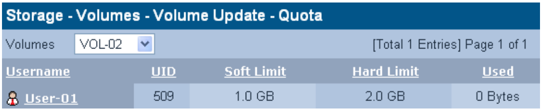
🟩 Free (99.0GB) 🟥 Used (1.0GB)

For that user, enter:

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

7. Click **add**.

   The **Storage - Volumes - Volume Update - Quota** page opens, displaying the user’s new quota:



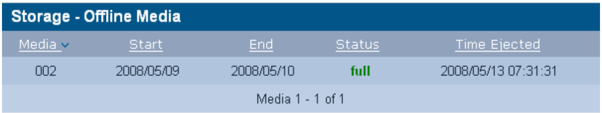
Storage - Volumes - Volume Update - Quota

Volumes VOL-02 [Total 1 Entries] Page 1 of 1

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

Offline Media

The **Storage - Offline Media** page tracks the status of media which is in use or has been used by the AA Express, as follows:



Storage - Offline Media

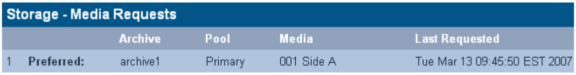
Media	Start	End	Status	Time Ejected
002	2008/05/09	2008/05/10	full	2008/05/13 07:31:31

Media 1 - 1 of 1

- **Media** - The sequence number of the media.
- **Start** - The date the media was opened.
- **End** - The date the media was closed. If the media is still open, **N/A** is displayed.
- **Status** - The media’s status, e.g. **open.**
- **Time Ejected** - The time and date the media was last ejected from the AA Express.

Media Requests

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



Storage - Media Requests

		Archive	Pool	Media	Last Requested
1	**Preferred:**	archive1	Primary	001 Side A	Tue Mar 13 09:45:50 EST 2007

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

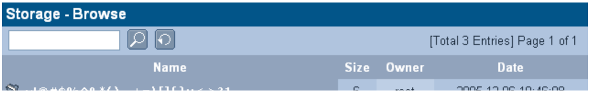
Browse

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

Finding files

To search for a file:

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



Storage - Browse

🔍 ⟲ [Total 3 Entries] Page 1 of 1

Name	Size	Owner	Date

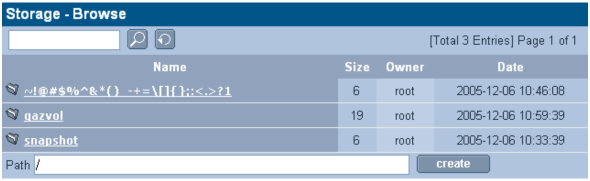
2. Enter a search string in the text box and click 🔍.
3. Click ⟲ to clear the content of the text box.
   Alternatively, manually browse the directory tree for a file.

Setting or modifying an ACL

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

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

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



Storage - Browse

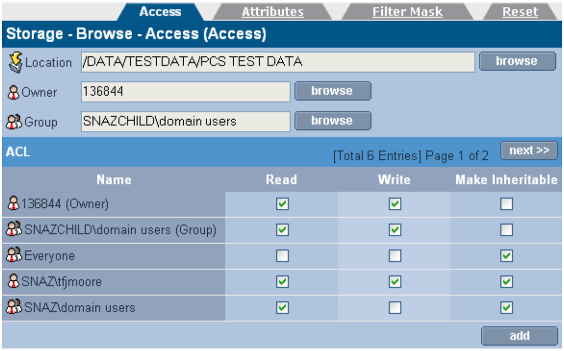
🔍 ⟲ [Total 3 Entries] Page 1 of 1

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

Path /

2. Search or browse to a directory or file.
   Click on **access**.

The **Storage - Browse - Access** page opens.



Storage - Browse - Access (Access)

Location /DATA/TESTDATA/PCS TEST DATA browse

Owner 136844 browse

Group SNAZCHILD\domain users browse

ACL [Total 6 Entries] Page 1 of 2 next >>

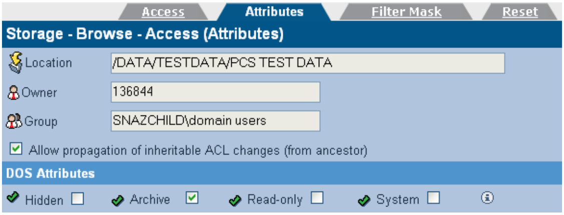
Name	Read	Write	Make Inheritable
136844 (Owner)	☑	☑	□
SNAZCHILD\domain users (Group)	☑	☑	□
Everyone	□	□	☑
SNAZ\tfjmoore	☑	☑	☑
SNAZ\domain users	☑	□	☑

add

From this page:

- View the current **Location**.
  Click **browse** to browse to another directory
- View the directory's **Owner** and **Owner Group**.
  Click **browse** to browse for another owner or owner group
- Set or view **ACL** - This section lists the users and groups who have access to the directory and their access privileges.

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



Storage - Browse - Access (Attributes)

Location /DATA/TESTDATA/PCS TEST DATA

Owner 136844

Group SNAZCHILD\domain users

☑ Allow propagation of inheritable ACL changes (from ancestor)

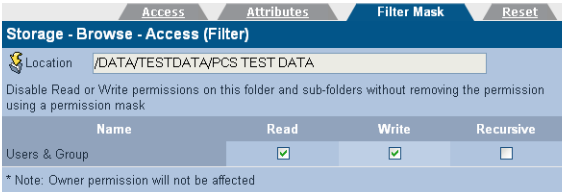
DOS Attributes

Hidden □ Archive ☑ Read-only □ System □

From this tab:

- **Allow propagation of inheritable ACL changes (from ancestor)** - This can be used to pass access privileges from the current directory to its sub-directories. In this way, a single ACL can be placed high up in the directory tree to control access. The **DOS Attributes** for the directory can also be set.

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



Storage - Browse - Access (Filter)

Location /DATA/TESTDATA/PCS TEST DATA

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

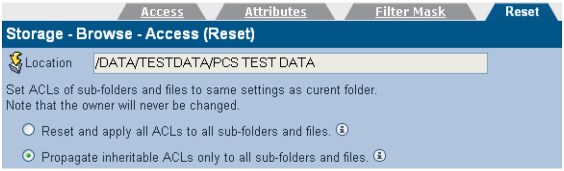
Name	Read	Write	Recursive
Users & Group	☑	☑	☐

* Note: Owner permission will not be affected

In this tab:

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

6. Click the **Reset** tab.



Storage - Browse - Access (Reset)

Location /DATA/TESTDATA/PCS TEST DATA

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

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

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

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

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

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

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

Chapter 6

Data Protection menu

Data Protection

Note: Data protection in this context refers to the protection of AA Express 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 inserted into the AA Express, 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.

Backup to media is initiated automatically when RW UDO media is inserted into the drive and protects system and file information for all closed media.

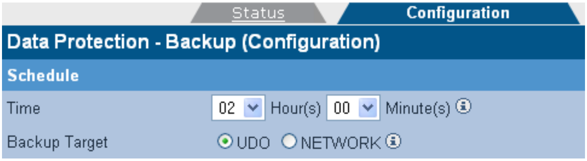
Note: A backup accelerates recovery . Plasmon recommends a backup is performed each time media is closed.

1. Insert RW UDO Media side A.
2. The AA Express will eject the media once the backup is complete, or when side A is full. If side B is required the administrator is notified via the **System - Status** page and E-mail (if configured).
   Media cannot be manually ejected during a backup.
3. Store the backup media appropriately.

Note: The AA Express does not provide Offline Media Management for backup media, and only the details of the most recent backup are retained and displayed to the administrator.

Creating a Network 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)

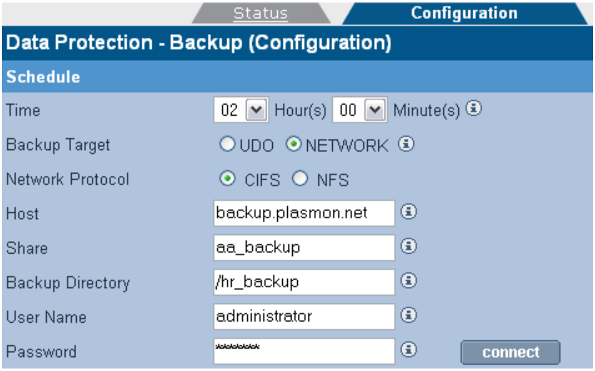
Schedule

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. Click the **NETWORK** radio button.
6. The AA Express is capable of backing up across either CIFS, NFS or FTP. 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	backup.plasmon.net
Share	aa_backup
Backup Directory	/hr_backup
User Name	administrator
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 AA Express across the network, and which has been configured to accept the connection (such as setting up a share, creating a user for the AA Express to connect as, and configuring the correct permissions).

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 AA Express units, each AA Express should be assigned a dedicated backup directory to ensure that backup files from one AA Express are not overwritten by the backup files of another.
4. Provide the **User Name** with Read, Write, Delete and Rename permissions. This is a user local to the server hosting the share, not to the AA Express.

Note: Usernames should be entered in the format <domainname>/<username> e.g. ***UK/psogani***

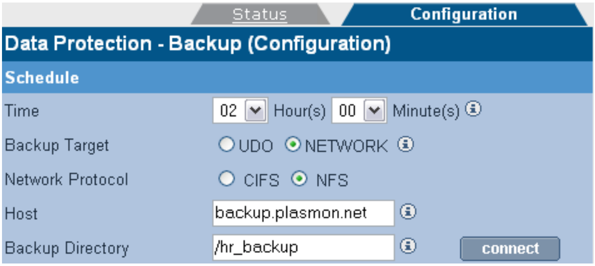
5. Enter that user's **Password**.
6. Click the **connect** button to test the connection to the remote network location and ensure the supplied details are correct.

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

7. 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	02 Hour(s) 00 Minute(s)
Backup Target	○ UDO ● NETWORK
Network Protocol	○ CIFS ● NFS
Host	backup.plasmon.net
Backup Directory	/hr_backup

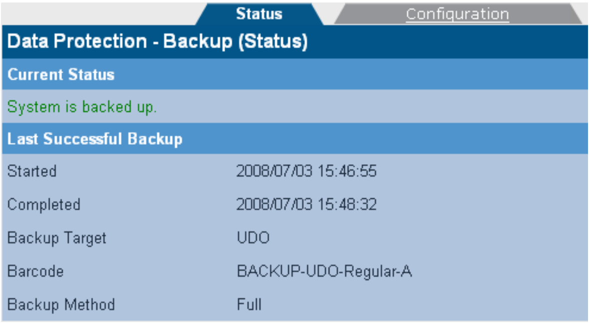
1. Enter the IP address or hostname of the remote backup location in the **Host** field. This must be a location which is accessible to the AA Express across the network, and which has been configured to accept the connection (such as setting up a share, creating a user for the Appliance to connect as, 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 AA Express units, each AA Express should be assigned a dedicated backup directory to ensure that backup files from one AA Express are not overwritten by the backup files of another.
3. Click the **connect** button to ensure the supplied details are correct.
4. Click **save**.

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	2008/07/03 15:46:55
Completed	2008/07/03 15:48:32
Backup Target	UDO
Barcode	BACKUP-UDO-Regular-A
Backup Method	Full

2. The following information is displayed:
   - **Current Status** - The backup status of the AA Express. 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).

Perform an unscheduled backup

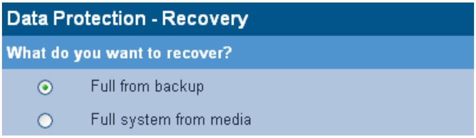
1. From the menu bar, select **Data Protection - Backup**.
2. Click **start**. A backup will begin immediately.

Recovery

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

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

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



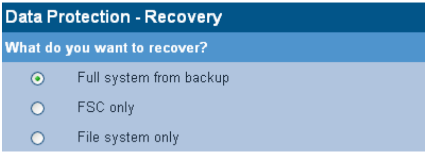
Data Protection - Recovery

What do you want to recover?

● Full from backup

○ Full system from media

If the system already has archives, the AA Express offers these options:



Data Protection - Recovery

What do you want to recover?

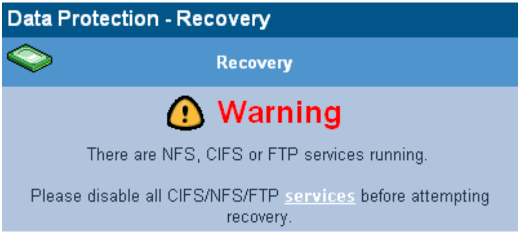
● Full system from backup

○ FSC only

○ File system only

Full system from backup

1. Select the **Full system from backup** radio button and click **recover**.
2. The AA Express ascertains whether there are services running which will interfere with the recovery. If either NFS, CIFS or FTP services are started, the web interface displays a warning:



Data Protection - Recovery

Recovery

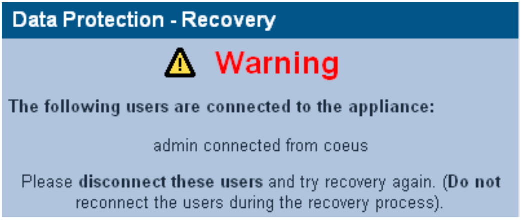
Warning

There are NFS, CIFS or FTP services running.

Please disable all CIFS/NFS/FTP services before attempting recovery.

Click the **services** link and stop these services, then return to step 1.

3. If users are connected to the AA Express, the following warning is displayed:



Data Protection - Recovery

⚠ Warning

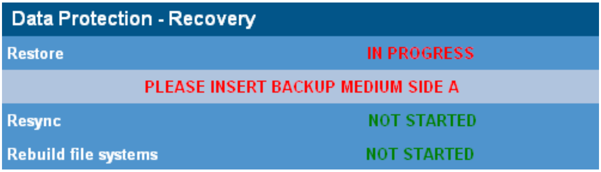
The following users are connected to the appliance:

admin connected from coeus

Please **disconnect these users** and try recovery again. (**Do not** reconnect the users during the recovery process).

Disconnect these users and click **OK**.

4. The AA Express checks for unmigrated data, and will issue a warning if any is detected.
   Click **yes** to proceed.
5. The web interface displays a progress page throughout the recovery process. A request for side A of the backup medium is displayed:



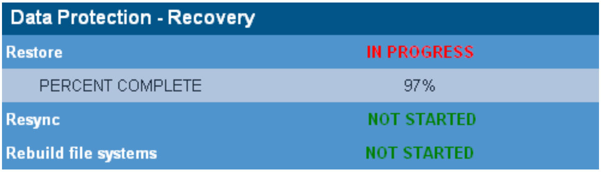
Data Protection - Recovery

Restore	IN PROGRESS
PLEASE INSERT BACKUP MEDIUM SIDE A	
Resync	NOT STARTED
Rebuild file systems	NOT STARTED

6. Insert side A of the backup media.

Note: Should the wrong media or side be inserted, the AA Express will eject the disk and prompt for the correct media.

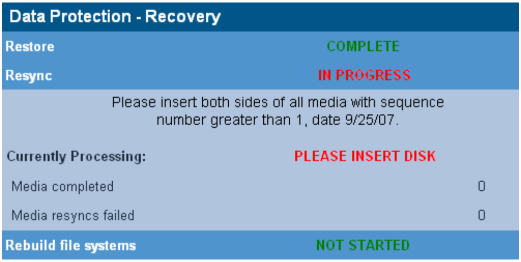
7. Once the backup media is detected the web interface displays a progress indicator:



Data Protection - Recovery

Restore	IN PROGRESS
PERCENT COMPLETE	97%
Resync	NOT STARTED
Rebuild file systems	NOT STARTED

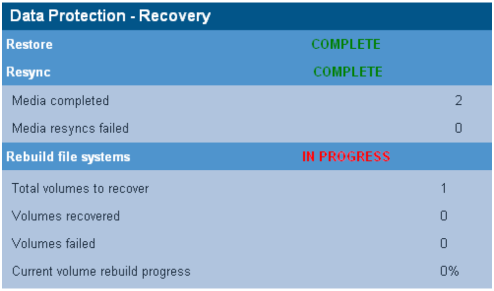
8. If side B of the media is required, the AA Express will eject the disk, and the web interface will request side B.
9. Once the file system restore has been performed the AA Express proceeds to resynchronise data. The web interface will request the necessary media:



Data Protection - Recovery

Restore	COMPLETE	
Resync	IN PROGRESS	
Please insert both sides of all media with sequence number greater than 1, date 9/25/07.		
Currently Processing:	PLEASE INSERT DISK	
Media completed		0
Media resyncs failed		0
Rebuild file systems	NOT STARTED	

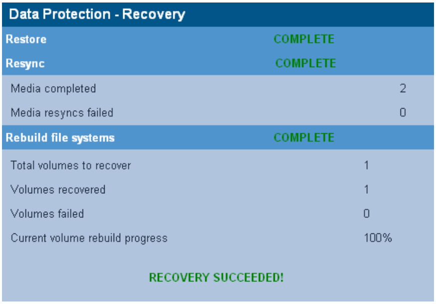
10. Insert or turn over media as requested during the resync process. The web interface will display a progress indicator throughout.
11. When resync is complete, the AA Express rebuilds the file system and restores the FSC:



Data Protection - Recovery

Restore	COMPLETE	
Resync	COMPLETE	
Media completed		2
Media resyncs failed		0
Rebuild file systems	IN PROGRESS	
Total volumes to recover		1
Volumes recovered		0
Volumes failed		0
Current volume rebuild progress		0%

12. When the rebuild is finished, the recovery is complete:



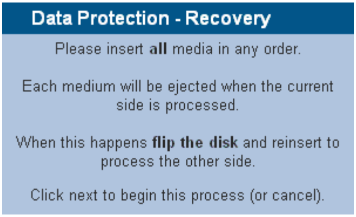
Data Protection - Recovery

Restore	COMPLETE
Resync	COMPLETE
Media completed	2
Media resyncs failed	0
Rebuild file systems	COMPLETE
Total volumes to recover	1
Volumes recovered	1
Volumes failed	0
Current volume rebuild progress	100%

RECOVERY SUCCEEDED!

Full system from media

1. Select **Full system from media** radio button and click **recover**.
2. The AA Express will prompt as follows:



Data Protection - Recovery

Please insert **all** media in any order.

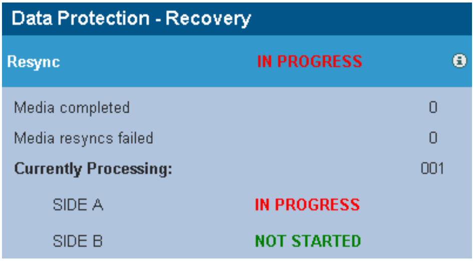
Each medium will be ejected when the current side is processed.

When this happens **flip the disk** and reinsert to process the other side.

Click next to begin this process (or cancel).

Insert the first piece of media and click **next**.

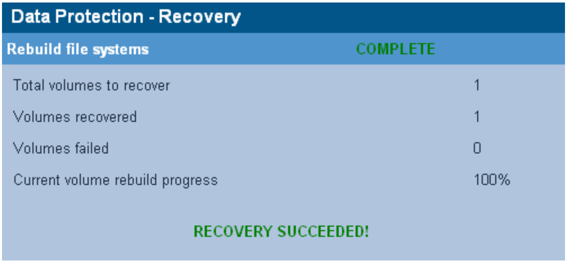
3. The AA Express will indicate it's progress:



Data Protection - Recovery

Resync	IN PROGRESS
Media completed	0
Media resyncs failed	0
Currently Processing:	001
SIDE A	IN PROGRESS
SIDE B	NOT STARTED

4. Continue to insert or turn over media until all sides of all media have been read.
5. Once complete, the AA Express displays:



Data Protection - Recovery

Rebuild file systems	COMPLETE
Total volumes to recover	1
Volumes recovered	1
Volumes failed	0
Current volume rebuild progress	100%

RECOVERY SUCCEEDED!

Click **finish**.

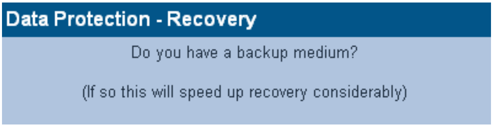
Following a recovery from media it is neccessary to reconfigure the list of local users on the Appliance. (see *page 36*).

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.

Recover FSC only

1. Select the **FSC only** radio button and click **recover**.
2. The web interface prompts for backup media:



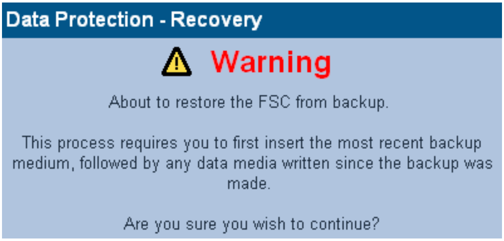
Data Protection - Recovery

Do you have a backup medium?

(If so this will speed up recovery considerably)

3. Click **yes** if backup media is available, and **no** to proceed without it. If no backup media is available, go to step 8 below.

4. A warning advises that the FSC is about to be restored from backup:



Data Protection - Recovery

⚠ Warning

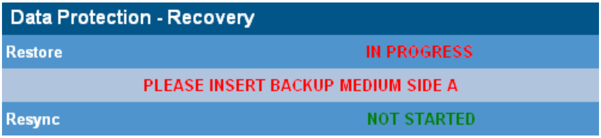
About to restore the FSC from backup.

This process requires you to first insert the most recent backup medium, followed by any data media written since the backup was made.

Are you sure you wish to continue?

Click **yes** to continue.

5. The web interface prompts for the backup media:



Data Protection - Recovery

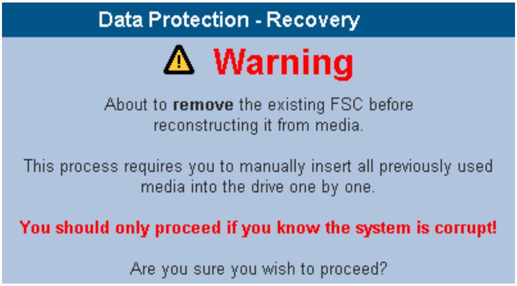
Restore	IN PROGRESS
PLEASE INSERT BACKUP MEDIUM SIDE A	
Resync	NOT STARTED

Insert side A of the backup media.

6. Turn the backup media over if requested to by the web interface.

   Go to step 9.

7. If no backup media are available, a warning advises that the existing FSC will be removed:



Data Protection - Recovery

⚠ Warning

About to **remove** the existing FSC before reconstructing it from media.

This process requires you to manually insert all previously used media into the drive one by one.

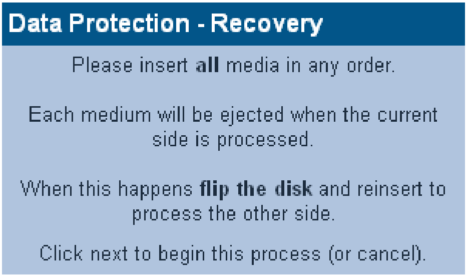
You should only proceed if you know the system is corrupt!

Are you sure you wish to proceed?

Click **yes** to continue or **no** to cancel.

8. Without backup media, the FSC must be restored from data media. This may take an extended period of time.

The AA Express will prompt as follows:



Data Protection - Recovery

Please insert **all** media in any order.

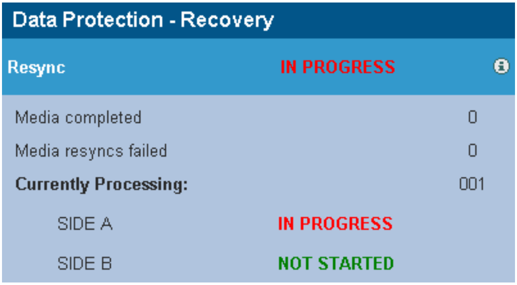
Each medium will be ejected when the current side is processed.

When this happens **flip the disk** and reinsert to process the other side.

Click next to begin this process (or cancel).

Insert the first piece of media and click **next**.

9. The AA Express will display the recovery process progress:



Data Protection - Recovery

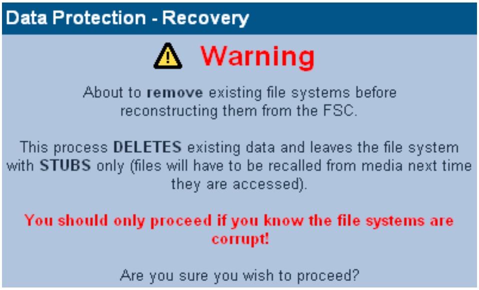
Resync	**IN PROGRESS**	
Media completed		0
Media resyncs failed		0
Currently Processing:		001
SIDE A	**IN PROGRESS**	
SIDE B	**NOT STARTED**	

10. When all media has been processed, click **finish**.

Recover File system only

1. Select the **File system only** radio button and click **recover**.

2. The AA Express displays the warning:



Data Protection - Recovery

⚠ Warning

About to **remove** existing file systems before reconstructing them from the FSC.

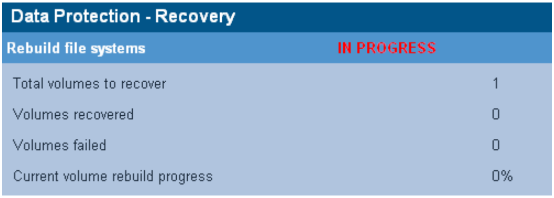
This process **DELETES** existing data and leaves the file system with **STUBS** only (files will have to be recalled from media next time they are accessed).

You should only proceed if you know the file systems are corrupt!

Are you sure you wish to proceed?

Click **yes** to proceed.

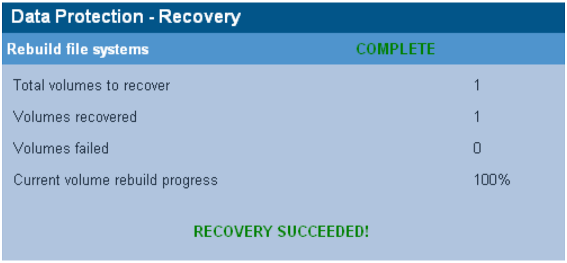
3. The process is automatic and requires little administrator activity. During the recovery, the web interface displays a progress monitor:



Data Protection - Recovery

Rebuild file systems	IN PROGRESS
Total volumes to recover	1
Volumes recovered	0
Volumes failed	0
Current volume rebuild progress	0%

4. Once complete, the AA Express displays:



Data Protection - Recovery

Rebuild file systems	COMPLETE
Total volumes to recover	1
Volumes recovered	1
Volumes failed	0
Current volume rebuild progress	100%

RECOVERY SUCCEEDED!

Click **OK**.

Replication

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

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

Ensure that the target AA Express has a user with Replication rights. See *Adding a User* on page 37.

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

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

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

Configuring Replication

Replication is unidirectional, from the source volume to the target volume.

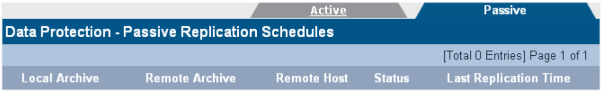
> *Important: It is necessary to configure the replication target (Passive) volume before attempting to configure the source (Active) volume.*

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. The Passive schedule validates incoming Active connections and routes the data to the correct volume.

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

Creating the Passive schedule

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

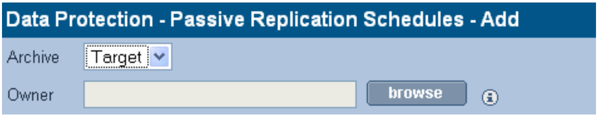


Data Protection - Passive Replication Schedules

[Total 0 Entries] Page 1 of 1

Local Archive	Remote Archive	Remote Host	Status	Last Replication Time

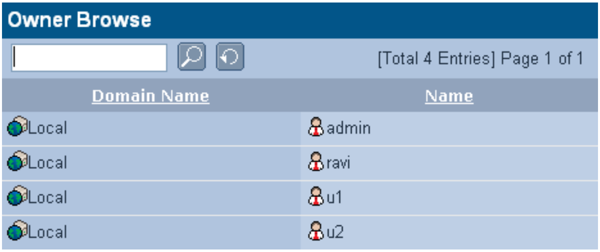
2. Click **add** to open the **Data Protection - Passive Replication Schedules - Add** page:



Data Protection - Passive Replication Schedules - Add

Archive	Target
Owner	

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

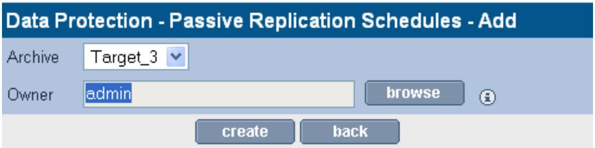


Owner Browse

[Total 4 Entries] Page 1 of 1

Domain Name	Name
Local	admin
Local	ravi
Local	u1
Local	u2

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



Data Protection - Passive Replication Schedules - Add

Archive	Target_3
Owner	admin

5. Click **create**.

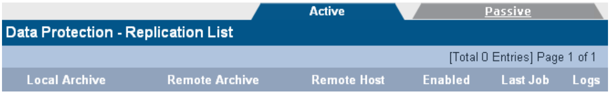
6. A warning may be displayed that the volume contains data. Click **create** again to confirm only if absolutely certain that the volume is available for use, as any existing data may be deleted.

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 AA Express, open the **Data Protection - Replication** page. The **Active** tab is displayed by default.

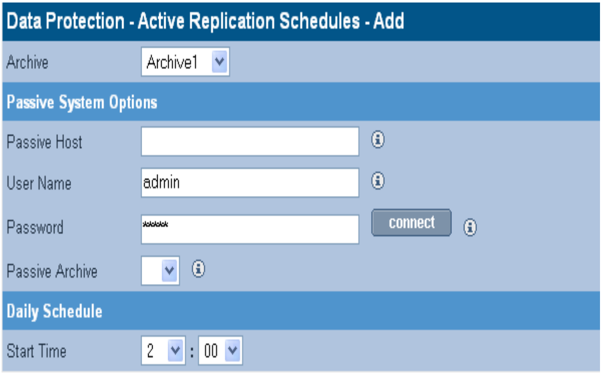


Data Protection - Replication List

[Total 0 Entries] Page 1 of 1

Local Archive	Remote Archive	Remote Host	Enabled	Last Job	Logs

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



Data Protection - Active Replication Schedules - Add

Archive: Archive1

Passive System Options

Passive Host:

User Name: admin

Password: *****

Passive Archive:

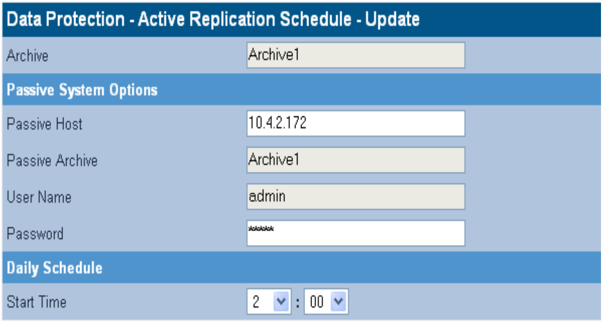
Daily Schedule

Start Time: 2 : 00

3. Select the source volume from the **Archive** drop-down box.
4. Enter the IP address or the Hostname of the target AA Express in the **Passive Host** field.
5. Enter the username and password of the Passive Replication owner.
6. Click **connect**.
7. Select the **Passive Archive** from the drop-down box.
8. Set a **Start Time** using the drop-down boxes.
9. Click **add**.
10. Go to the **System - Services** page and **enable** the Replication service.

Editing Active Replication Schedule Details

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



Data Protection - Active Replication Schedule - Update

Archive	Archive1
Passive System Options	
Passive Host	10.4.2.172
Passive Archive	Archive1
User Name	admin
Password	*****
Daily Schedule	
Start Time	2 : 00

3. Edit details as required.

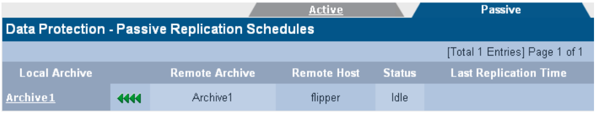
Note: Passive Archive and User Name cannot be changed.

4. Click **save**.

Changing the Passive Replication Schedule Owner

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

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

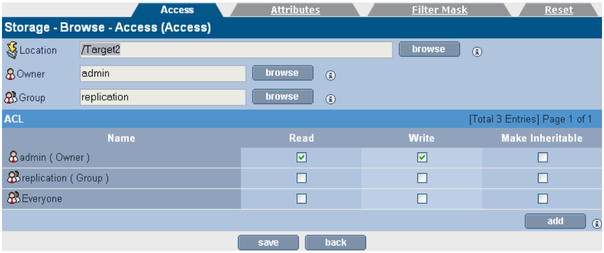


Data Protection - Passive Replication Schedules

[Total 1 Entries] Page 1 of 1

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

3. Click **Delete**. At the system's request, click **Delete** a second time to confirm deletion of the Passive Replication Schedule.
4. Recreate the Passive replication schedule as described on *page 92* specifying the new user to be assigned as the Schedule owner.
5. Open the **Storage** - **Browse** page and click the name of the replication target archive.
6. Click **Access**.



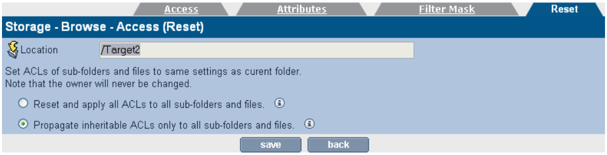
Storage - Browse - Access (Access)

Location	/Target2
Owner	admin
Group	replication

ACL [Total 3 Entries] Page 1 of 1

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

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



Storage - Browse - Access (Reset)

Location /Target2

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

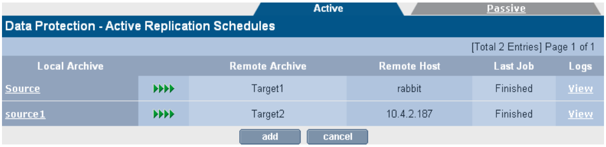
○ Reset and apply all ACLs to all sub-folders and files.

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

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

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

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



Data Protection - Active Replication Schedules

[Total 2 Entries] Page 1 of 1

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

13. Select the Active Replication Schedule that corresponds to the Passive Replication Schedule changed above by clicking on the name of the source archive.
14. Click **delete**. At the system's request, click **Delete** a second time to confirm deletion of the Active Replication Schedule.
15. Recreate the Active Replication Schedule as described on *page 94*. Ensure that the newly configured Passive Schedule owner is entered in the **User** field.

Deleting a Replication Schedule - Source Appliance

1. On the source AA Express, 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 Replication Schedule - Target Appliance

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

Note: Deleting a replication schedule does not delete the archive.

Note: If a passive replication schedule is accidentally deleted or requires reconfiguration following a system recovery, see Recovering the passive replication schedule on page 98.

Recovering the passive replication schedule

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

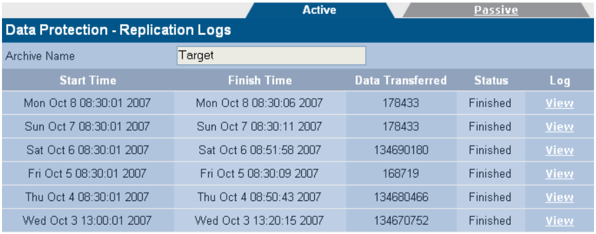
If a different user is to be specified as the Passive Replication Schedule owner, follow the procedure for changing the owner described on *page 96*.

Viewing Replication logs

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

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

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



Data Protection - Replication Logs

Archive Name: Target

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

Data Transferred is in bytes.

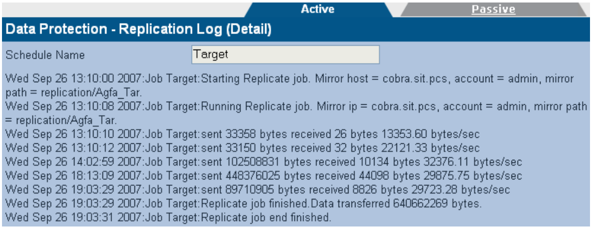
Start Time indicates the time the replication began.

Finish Time indicates the time the replication ended.

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

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

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



Data Protection - Replication Log (Detail)

Schedule Name: Target

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

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

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.

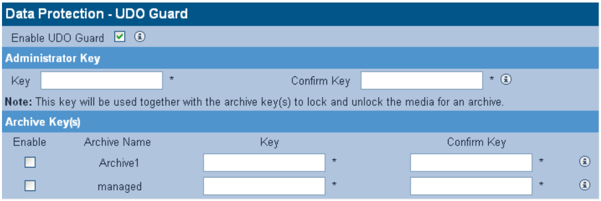
Once entered, the Administration and Archive Keys may be only changed as long as no media is locked using the key-pair.

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: Plasmon strongly reccommend 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.

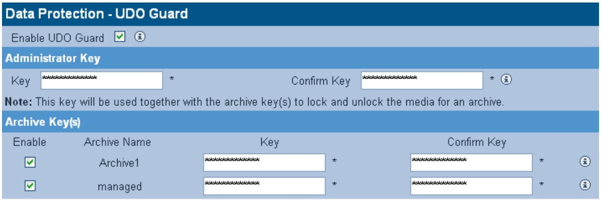
   As with the Administrator Key, the Archive Key may consist of any characters, up to a maximum of 16.

   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	************** *	************** *

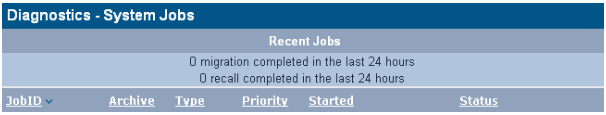
2. Uncheck the box beside the name of the Archive which is to cease using UDO Guard.
3. Click **save**.

Chapter 7

Diagnostics menu

System Jobs

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



Diagnostics - System Jobs

Recent Jobs

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

JobID	Archive	Type	Priority	Started	Status

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.
- **Priority** - Jobs are given one of three priorities; recall jobs have the highest priority, migration medium priority and backup the lowest priority
- **Media** - The media being used for the specified Job ID by the AA Express
- **Started** - The time the job was started
- **Status** - The job’s status.

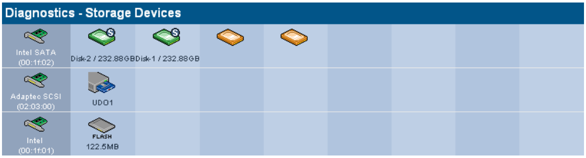
Click the **refresh** button to update the information displayed on this page.

Storage Devices

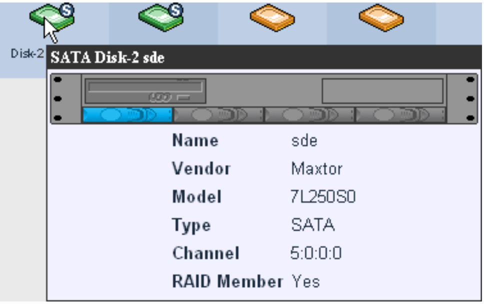
The **Diagnostics - Storage Devices** page shows all interface buses (SATA, SCSI and IDE) and their associated devices and their status.

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:



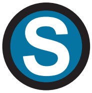
SATA Disk-2 sde

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

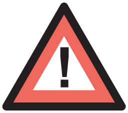
Disk status icons

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

- Disks which are marked with:

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

  have been detected by the system as being in a prefail state. This means that certain types of errors have been found on them and they are likely to become faulty as a result. The system uses Self-Monitoring Analysis And Reporting Technology (SMART) parameters to track these errors
- Disks which are marked with:

  SPARE

  have been assigned as hot spare disks. These are used should one of the other disks fail
- Disks which are marked with:

  NO RAID

  are not currently members of a RAID
- Disks which are marked with:

  REJECT

  have been rejected by the RAID they were a member of
- Disks which are marked with

  RESYNC

  are currently being resynchronised. The system, at all times, has to ensure that all mirrored RAID disks contain exactly the same data. If a difference is found, resynchronisation is performed to bring all the RAID disks back to identical mirrors of one another.

Table 7-1: Disk status icons

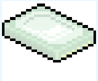
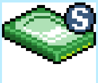
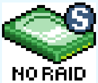
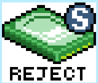
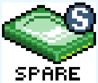
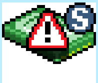
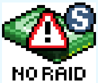
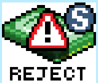
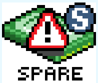
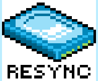
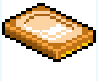
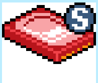
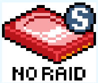
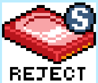
Icon	Meaning
	The disk is online and unformatted
	The disk is online and is a system disk
	The disk is online, is a system disk and is not part of a RAID
	The disk is online, is a system disk and has been rejected by the system
	The disk is online, is a system disk and has been marked as a spare disk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

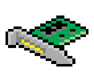
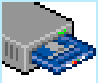
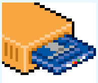
Table 7-1: Disk status icons

Icon	Meaning
	The disk is resynchronising
	The disk is offline or is missing from the AA Express. This icon is also used to represent a dummy shuttle
	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

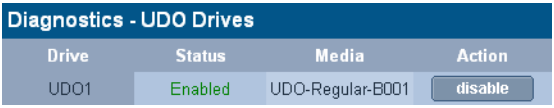
Table 7-1 describes the other status icons and their meaning.

Table 7-2:

Icon	Meaning
	This icon represents an internal controller card
	This icon represents an online UDO drive
	This icon represents an offline or faulty UDO drive

UDO Drives

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



Diagnostics - UDO Drives

Drive	Status	Media	Action
UDO1	Enabled	UDO-Regular-B001	disable

- Drive **Status** can be:
  - **Enabled** - The drive has been enabled
  - **Disabled** - The drive has been disabled
  - **Error** - The drive has an error and has been taken offline by the system
  - **Enabled-dirty** - The drive has been enabled, but the drive requires cleaning
  - **Disabled-dirty** - The drive has been disabled, but the drive requires cleaning. If the Appliance uses UDO30 Media, insert the supplied cleaning cartridge.

  Note: If the Appliance uses UDO60 Media, contact Plasmon Support.

  - **Error-dirty** - The drive has an error and has been taken offline by the system, but the drive requires cleaning. If the Appliance uses UDO30 Media, insert the supplied cleaning cartridge.

  Note: If the Appliance uses UDO60 Media, contact Plasmon Support.

- **Media** - The type and sequence number of the currently loaded media.

Enabling or disabling a UDO drive

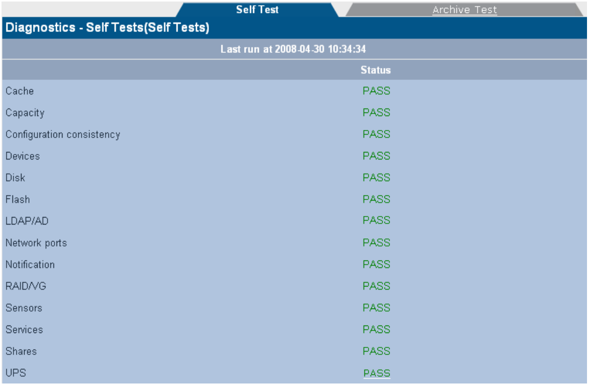
To enable or disable a UDO drive:

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

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 2008-04-30 10:34:34

	Status
Cache	PASS
Capacity	PASS
Configuration consistency	PASS
Devices	PASS
Disk	PASS
Flash	PASS
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.

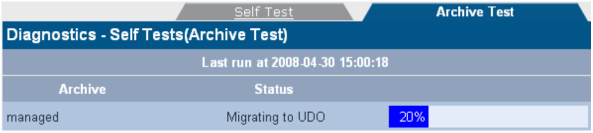
Clicking **start** will check:

- **Cache** - The status of the RAID, including SATA (disk) drives. Normally, the system will perform a resynchronisation to fix any problems with the cache. However, if the problem persists, contact Plasmon 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 Plasmon Technical Support if this test fails.
- **Flash** - The status of the Appliance's Flash disk. The Flash disk stores data vital to the operation of the Appliance. If this test fails, contact Plasmon Technical Support.
- **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 Plasmon Technical Support should this test fail.
- **Sensors** - The status of all attached sensors - board temperature, fan sensors, etc.
- **Services** - The status of the processes, including Services, running on the system. If any services fail, initially check the System - Services page is correctly configured. If this is correct, then contact Technical Support for further assistance.
- **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 2008-04-30 15:00:18

Archive	Status	
managed	Migrating to UDO	20%

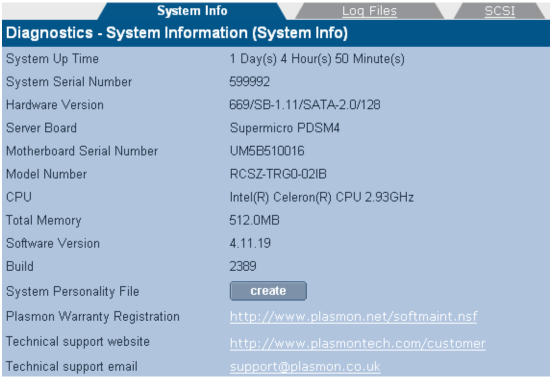
An **Archive Test** creates a small test file, migrates it to media, releases the file from the cache, and then recalls the file from media to check the archive system from end-to-end.

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	1 Day(s) 4 Hour(s) 50 Minute(s)
System Serial Number	599992
Hardware Version	669/SB-1.11/SATA-2.0/128
Server Board	Supermicro PDSM4
Motherboard Serial Number	UM5B510016
Model Number	RCSZ-TRG0-02IB
CPU	Intel(R) Celeron(R) CPU 2.93GHz
Total Memory	512.0MB
Software Version	4.11.19
Build	2389
System Personality File	create
Plasmon Warranty Registration	http://www.plasmon.net/softmaint.nsf
Technical support website	http://www.plasmontech.com/customer
Technical support email	support@plasmon.co.uk

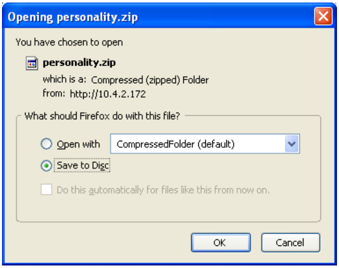
The **Diagnostics - System Information (System Info)** page lists:

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

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

Also present is the facility to create a copy of the System Personality File should it be required by Plasmon 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)

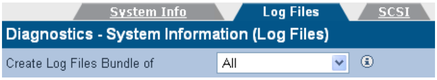
● Save to Disc

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

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

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

Log Files



Diagnostics - System Information (Log Files)

Create Log Files Bundle of: All

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

- **Create Log Files Bundle of** - Log file bundles are used by Technical Support to perform diagnostics on the Appliance.

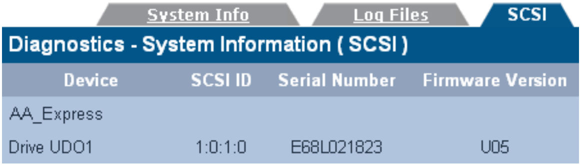
  Specify a time period, using the drop down list, to create a log file bundle of as follows:
  - **Today**
  - **Last 7 days**
  - **All**
  - **All and config.** - This option produces an **All** type log file bundle with the addition of a text file listing the current system configuration settings.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

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

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

Note: The AA Express does not store previous log bundles.

SCSI



Diagnostics - System Information (SCSI)

Device	SCSI ID	Serial Number	Firmware Version
AA_Express			
Drive UDO1	1:0:1:0	E68L021823	U05

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

Chapter 8
Troubleshooting

Troubleshooting

Warning: Shutting down and rebooting the AA Express must be performed using the Web Interface unless specified otherwise. Ensure that no users or applications are accessing the AA Express before rebooting or shutting down.

Table 1: Troubleshooting checklist

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

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

Table 1: Troubleshooting checklist

System Crash.	Reboot or power-cycle.	If the Web Interface is inaccessible, attempt to reboot via serial console. As a last resort press and hold the power button to switch off.
Incorrect Web browser settings.	If a proxy server is being used ensure it is bypassed for local addresses.	
Hardware failure	Contact Plasmon support.	
The AA Express will not power on (no LED or fan activity).		
Possible cause	*Suggested action*	*Comments*
Faulty power cable.	Test with a known working power cable.	
Hardware failure.	Contact Plasmon support.	
The AA Express fails its self-test.		
Possible cause	*Suggested action*	*Comments*
The UDO drive is unavailable.	Reboot the AA Express. If this does not resolve the issue contact Plasmon support.	

Table 1: Troubleshooting checklist

Notification ping failure to either SMTP or SNMP server	Ensure relevant server is available. Check Notification configuration.	
One or more key services are not running.	Check running services and enable any which have stopped. If a service fails to start, reboot the AA Express.	
Hardware failure	Contact Plasmon support	
Data is not migrating to media.		
Possible cause	*Suggested action*	*Comments*
Incorrect or no media loaded.	View the **System - Status** page to determine which media to load. Open the **Storage - Media Requests** page to see other outstanding media requests.	
SSM Service not started.	Open the **System - Services** page and start SSM. If this fails reboot the AA Express, then attempt to start SSM. Contact Plasmon support if problem is not resolved.	

Table 1: Troubleshooting checklist

SSM fault.	Go to the **Diagnostics - Self test** page and run the Archive Test. If this fails, reboot the AA Express then retest. Contact Plasmon support if problem is not resolved.	
Media fault.	See “Troubleshooting media” on page 137.	
Hardware failure.	Contact Plasmon support	
Data cannot be recalled from media.		
Possible cause	*Suggested action*	*Comments*
A migration job is in progress.	Wait for the migration job to complete. Select the **Diagnostics - System Jobs** page to view the status of current jobs.	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.
Incorrect or no media loaded.	View the system status page to determine which media to load. Refer to the **Storage - Media Requests** page to see other outstanding media requests.	

Table 1: Troubleshooting checklist

SSM service not started.	Go to the **System - Services** page and start SSM. If this fails reboot the AA Express then attempt to start SSM. Contact Plasmon support if problem is not resolved.	
SSM fault.	Reboot the AA Express. Contact Plasmon support if the problem is not resolved.	
Dirty media	Clean the media using a Plasmon UDO media cleaning kit and retry.	Refer to the Operator's Guide for media storage and care information.
Hardware failure	Contact Plasmon support	

Table 1: Troubleshooting checklist

Backup failure.		
Possible cause	*Suggested action*	*Comments*
Backup media dirty / damaged.	Replace media.	
Backup media at end of life.	Replace media.	Media can be re-written approximately 5,000 times.
Administrator Notified that a dirty shutdown was performed.		
Possible cause	*Suggested action*	*Comments*
Power failure.	Connect to a UPS.	A UPS is reccommended.
Connected to a UPS but did not shutdown before UPS battery discharged.	Check the serial link to the UPS.	
UPS service not started.	Select **System - Services** and start the UPS service.	
Administrator notified that the RAID has degraded.		
Possible cause	*Suggested action*	*Comments*
Hardware failure	Contact Plasmon support	

Table 1: Troubleshooting checklist

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

Table 1: Troubleshooting checklist

Network service not started	Select **Network - Services**. Ensure the correct network services have been started on the AA Express. Also refer to the Administrator Guide to do this.	
Incorrect hostname or IP used	Use the correct hostname or IP address. Check that it is possible to ping the AA Express 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 AA Express.	See “Adding a User” on page 37.	
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 48.	
Host has been denied access	If the host should have access, see “Modifying a share” on page 48.	

Table 1: 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 48.	The connected users can be determined by going to the **Network - Shares** page and clicking on **connections**. If the access problem only occurs for a specific path or file in the share use the **Storage - Browse** option to check the access permissions for the file or directory
The share has been set read-only	Should the share be writeable, open the **Network - Shares** page and click on the share. Ensure the **Read only** option is not selected.	

Table 1: Troubleshooting checklist

SSM service not started	Open the **System - Services** page and start SSM. If this fails reboot the AA Express then attempt to start SSM. Contact Plasmon support if problem is not resolved.	
SSM fault	Go to the **Diagnostics - Self test** page and run the **Archive Test**. If this fails, reboot the AA Express, then retest. Contact Plasmon support if problem is not resolved.	
Successfully connect to network share but permission denied when reading.		
Possible cause	*Suggested action*	*Comments*
File or directory does not have read access permissions for the connected user	If the user should have read permissions, see “Modifying a share” on page 48.	The connected users can be determined by going to the **Network - Shares** page and clicking on **connections**.

Table 1: Troubleshooting checklist

SSM service not started	Open the **System - Services** page and start SSM. If this fails reboot the AA Express then attempt to start SSM. Contact Plasmon support if problem is not resolved.	
SSM fault	Open the **Diagnostics - Self test** page and run the **Archive Test**. If this fails, reboot the AA Express, then retest. Contact Plasmon support if problem is not resolved.	
Media is under-utilised.		
Possible cause	*Suggested action*	*Comments*
Blank media insert in place of media requested for migration	Ensure requested media is inserted in future.	If a blank media is loaded when the AA Express is requesting an existing open media, the open media will be closed and writing will continue on the blank media.

Table 1: Troubleshooting checklist

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 48.	
Allow File Changes has been set to NO for the Archive Volume	If file changes should be allowed, see “Viewing and editing a volume’s properties” on page 65 and set the **Allow File Changes** option to YES.	
No Free Space reported when writing to the share.		
Possible cause	*Suggested action*	*Comments*
The RAID cache is full.	See the causes and actions for *Data is not migrating to media.*	
The Archive Volume option **Never Release Files** has been set.	See “Viewing and editing a volume’s properties” on page 65. Reconfigure release policy as required.	

Table 1: Troubleshooting checklist

Email Noficiations not being received.

Possible cause	*Suggested action*	*Comments*
SMTP server IP address incorrect.	Enter a valid SMTP service IP address.	
SMTP server hostname not being resolved.	Enter a valid DNS server IP address into the network configuration. Alternatively use the IP address of the SMTP server instead.	
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 AA Express.	
SMTP server port number incorrect.	Enter the correct port number.	
Sender not defined.	Enter a sender address.	This is required by some SMTP servers.
Username and password not defined.	Enter a valid username and password.	These are required by some SMTP servers.

Table 1: Troubleshooting checklist

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.	

Table 1: Troubleshooting checklist

Media marked "dirty".		
Possible cause	*Suggested action*	*Comments*
Dirty media	If this occurs during migration the AA Express will prompt for a new media to be inserted. If this occurs during recall the recall will continue as normal. Clean the media using a Plasmon UDO media cleaning kit and retry. If further media are marked unreliable, contact Plasmon support	Refer to the Operator's Guide for media storage and care information.
Administrator notified that the UDO drive is dirty.		
Possible cause	*Suggested action*	*Comments*
Dirty drive.	If it is a UDO1 drive, insert the cleaning cartridge to perform a cleaning cycle. The dirty status should be reset after the next recall or migration. If it is a UDO2 drive, contact Plasmon support as UDO2 drives are self cleaning.	
Hardware failure.	Contact Plasmon support.	
AA Express will only boot into MAINTENANCE mode.		

Table 1: Troubleshooting checklist

Possible cause	*Suggested action*	*Comments*
Hardware failure.	Contact Plasmon support.	
Unable to join Active Directory or NT4 domain.		
Possible cause	*Suggested action*	*Comments*
Incorrect time on AA Express.	Go to the **System - Time & Date** and correct the time.	When the AA Express joins the domain its time will be synchronised with the domain.
DNS is not / incorrectly configured.	The AA Express must have DNS configured to be able to join a domain. See “DNS configuration for Windows Active Directory” on page 35.	
Unable to connect to LDAP server		
Possible cause	*Suggested action*	*Comments*
Incorrect time on AA Express	Go to the **System - Time & Date** and correct the time.	

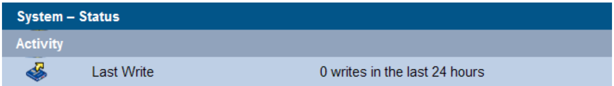
Table 1: Troubleshooting checklist

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

Troubleshooting media

Files cannot be written to UDO media

If files are not being written or the **Activity - Last write** section on the **System - Status** page displays:



System – Status

Activity

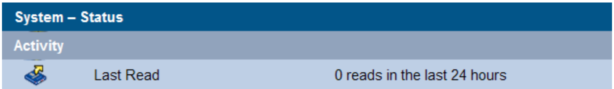
	Last Write	0 writes in the last 24 hours

consult **Media Management** on the status page. File write failure may be caused by one or more of the following:

- Incorrect media or media side loaded, see:
  - “Media required for writing files” on page 155,
  - “New blank media required” on page 152,
  - “Media full” on page 153,
  - “Turn media over” on page 155.
- Media initialization failure - see:
  - “Initialization failure” on page 138.
- Drive or media failure - see:
  - “Open media read/write failure” on page 139.

Files cannot be read from UDO media

If files cannot be read by a user or the **Activity - Last read** section on the status page displays:



System – Status

Activity

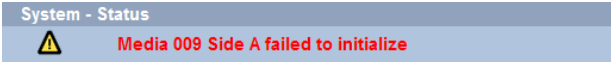
	Last Read	0 reads in the last 24 hours

consult **Media Management** on the status page. File read failure may be caused by one or more of the following:

- Incorrect media or media side loaded, see:
  - “Media required for writing files” on page 155.
  - “Turn media over” on page 155.
- Drive or media failure - see:
  - “Open media read/write failure” on page 139
  - “Closed media read failure” on page 140

Initialization failure

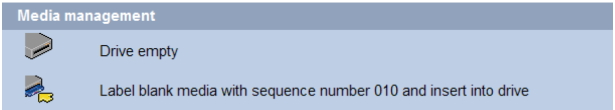
If the status page displays:



System - Status

⚠ Media 009 Side A failed to initialize

and



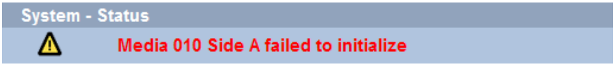
Media management

Drive empty

Label blank media with sequence number 010 and insert into drive

the inserted blank media has failed to initialize, the sequence number (009) is no longer usable.

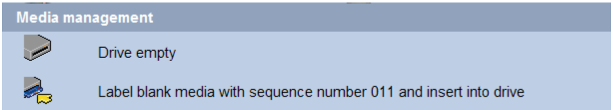
1. Eject and remove the media from the drive.
2. Clean the media (see page 158) and place a blank media label over the existing one and write the indicated new sequence number (010) on to the label.
3. Re-insert the media in to the UDO drive.
4. If the media fails to initialise again, the status page displays:



System - Status

⚠ Media 010 Side A failed to initialize

and



Media management

Drive empty

Label blank media with sequence number 011 and insert into drive

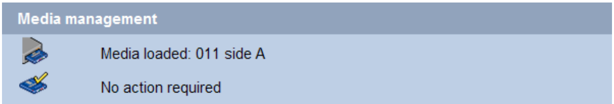
5. Determine the cause of the initialization failure by inserting a different piece of media labeled with the indicated new sequence number (011). If this media fails then it can be assumed that the failure is caused by a drive error. Contact technical support. Both media can be retained for future use.

   Note: The sequence numbers (009 and 010 and 011) are now unusable. Blank media labels should be attached to both media to ensure that the sequence numbers are not used in the future.

6. If the second media (011) initializes correctly, it can be assumed that the original media is damaged. Damaged

media should be retained to indicate that the sequence number is unusable.

7. The AA Express checks the new media and displays:



Media management

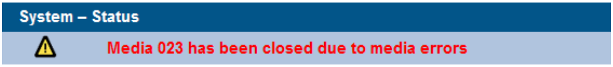
Media loaded: 011 side A

No action required

8. The media is now initialized and is open for writing.

Open media read/write failure

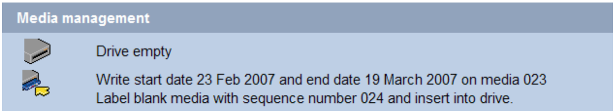
If the status page displays:



System – Status

⚠ Media 023 has been closed due to media errors

and



Media management

Drive empty

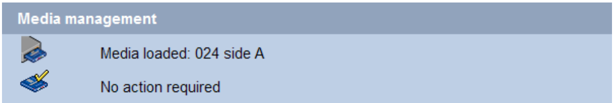
Write start date 23 Feb 2007 and end date 19 March 2007 on media 023
Label blank media with sequence number 024 and insert into drive.

the Appliance has failed to read data from, or write data to, the currently open media. The media has been closed automatically and no further files will be written to it.

1. Eject and remove the media from the drive and enter the indicated date range on the media label.
2. Determine the cause of the read/write failure by inserting a different piece of media labeled with the indicated new sequence number (024). If a subsequent read/write failure occurs with the new media then it can be assumed that the failure is caused by a drive error. Contact technical support. The new media can be retained for future use.

   Note: The sequence number of the media (024) is now unusable. A blank media label should be attached to the media to ensure that the sequence number is not used in the future.

3. If no subsequent read/write error occurs, it can be assumed that the original media is damaged. The media may still be used for file reading and should be stored appropriately.
4. The AA Express checks the new media and displays:



Media management

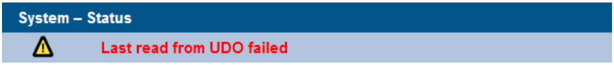
Media loaded: 024 side A

No action required

5. The media is now initialized and is open for writing.

Closed media read failure

If the status page displays:



System – Status

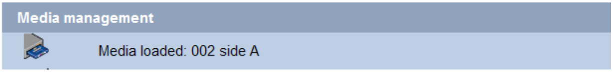
⚠ Last read from UDO failed

The AA Express has failed to read from the UDO media. This may indicate a media or drive error. Contact technical support. The AA Express will continue to attempt to complete any queued reading tasks. If a subsequent read is successful the alert status message will be cleared.

Media label missing

UDO media with missing labels can be identified by inserting the media into the UDO drive and consulting the web interface.

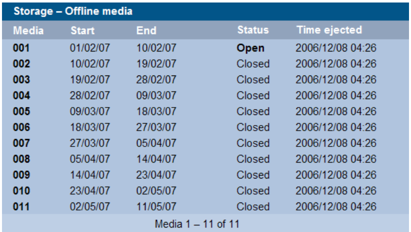
1. Insert media with side A loaded.
2. The AA Express checks the media and displays:



Media management

Media loaded: 002 side A

3. Navigate to the **Storage - Offline Media** page of the web interface:



Storage – Offline media

Media	Start	End	Status	Time ejected
001	01/02/07	10/02/07	**Open**	2006/12/08 04:26
002	10/02/07	19/02/07	Closed	2006/12/08 04:26
003	19/02/07	28/02/07	Closed	2006/12/08 04:26
004	28/02/07	09/03/07	Closed	2006/12/08 04:26
005	09/03/07	18/03/07	Closed	2006/12/08 04:26
006	18/03/07	27/03/07	Closed	2006/12/08 04:26
007	27/03/07	05/04/07	Closed	2006/12/08 04:26
008	05/04/07	14/04/07	Closed	2006/12/08 04:26
009	14/04/07	23/04/07	Closed	2006/12/08 04:26
010	23/04/07	02/05/07	Closed	2006/12/08 04:26
011	02/05/07	11/05/07	Closed	2006/12/08 04:26

Media 1 – 11 of 11

4. Note the date range for the media (002)
5. Eject and remove the media.

6. Attach a new UDO media label (See “Media labelling” on page 146.) and enter the sequence number and date range from the web interface.
7. The media should be stored appropriately.

Warning: Inserting blank media into the AA Express *when open media exists will result in wasted storage space.*

Page left intentionally blank

Chapter 9

Shutdown menu

Shutdown or reboot the AA Express

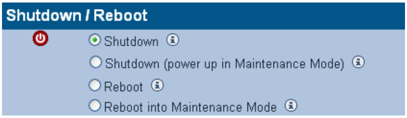
The **Shutdown/Reboot** page allows:

- **Shutdown**
- **Shutdown (power up in Maintenance Mode)** - Used to power down the AA Express, 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** - Maintenance Mode is normally only used by Service personnel.

> *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 AA Express 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.

Chapter 10

Using the AA Express

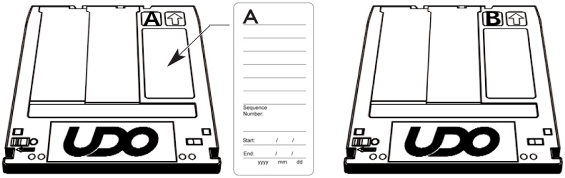
Media labelling

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 152) on the media label.

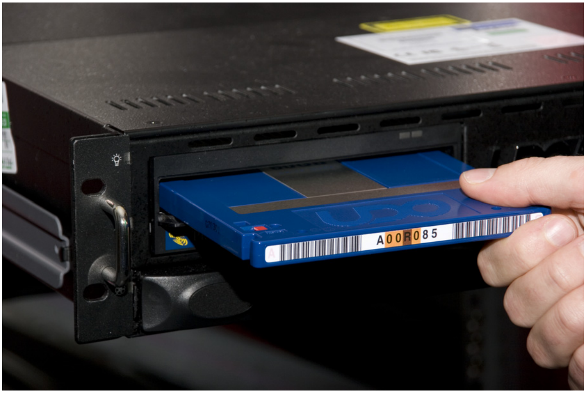
Note: When not in use, UDO media should be kept in the protective sleeve supplied.

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.

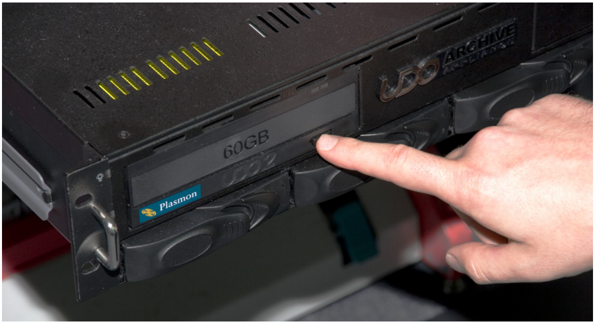
To load side B, insert the media with the embossed “B” on the casing facing upwards with the “B” mark on the barcode label to the left.

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:



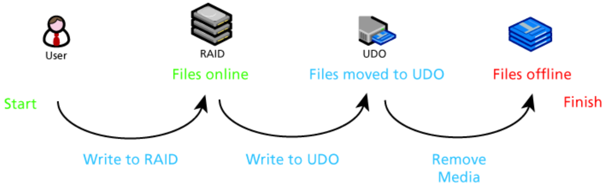
Cleaning media

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 158

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.



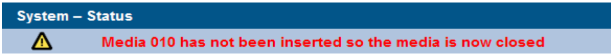
Writing files to the AA Express

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

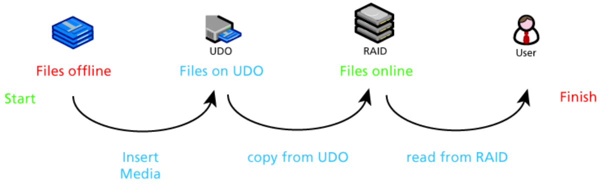
⚠ **Media 010 has not been inserted so the media is now closed**

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.



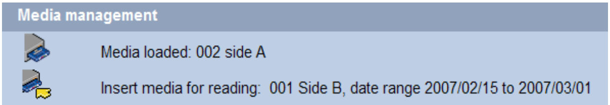
Reading files from the AA Express

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 152.

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.

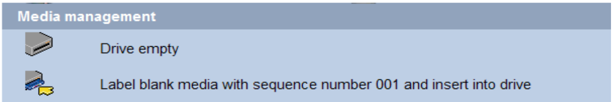
Drive Empty.	Insert media.
Media OK.	Media loaded.
Media write.	Media read.
Turn media over.	Remove media.
Find media.	Incorrect or unrecognised media.

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:



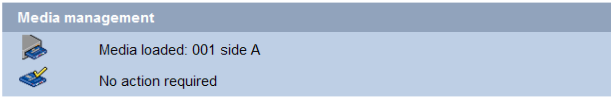
Media management

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 146) and insert into the UDO drive ensuring side A is loaded (see *Inserting media* on page 147).
2. The AA Express initializes the media and displays:



Media management

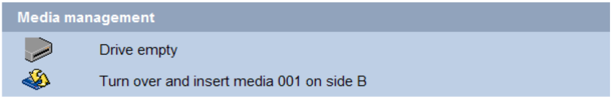
Media loaded: 001 side A

No action required

3. Files can now be written to the media.

Side A full

If the status page displays:



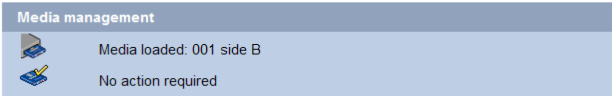
Media management

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 147).
2. The AA Express checks the media and displays:

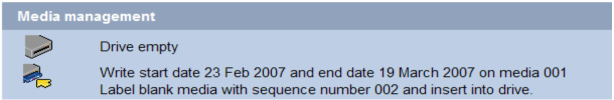


Media management

Media loaded: 001 side B

No action required

3. Files can now be written to the media.



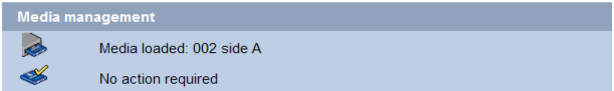
Media management

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 158.
2. Label a piece of blank UDO media with the indicated new sequence number (see *Media labelling* on page 146) and insert into the UDO drive ensuring side A is loaded.
3. The AA Express checks the media and displays:



Media management

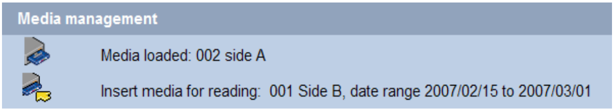
Media loaded: 002 side A

No action required

4. Files can now be written to the media.

Media required for reading files

If the status page displays:



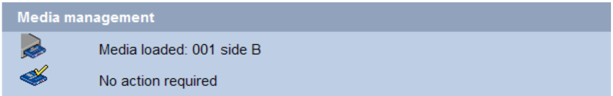
Media management

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 148) 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

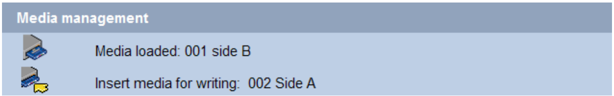
Media loaded: 001 side B

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

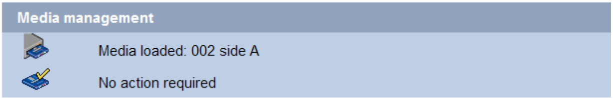
Insert media for writing: 002 Side A

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

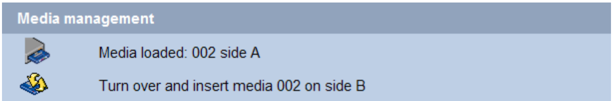
Media loaded: 002 side A

No action required

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

Turn media over

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



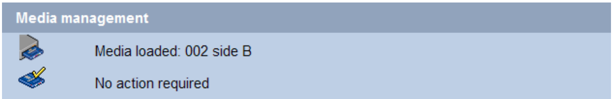
Media management

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 148.
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

Chapter 11

Offline Media Management

Storage of offline media

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

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

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

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

Table 1: . UDO operating and storage conditions

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

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

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

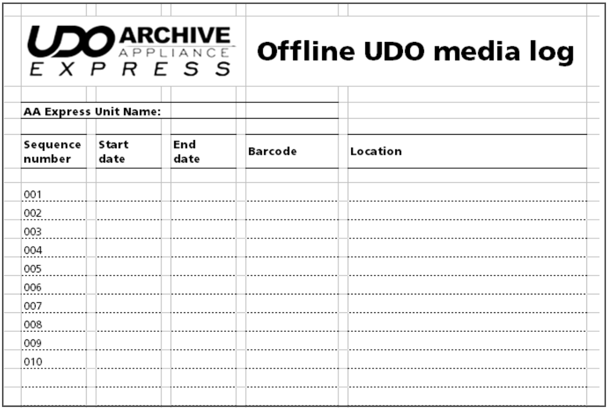
Offline media is stored by sequence number. If required, the correct media can be further verified by referencing the date range requested by the AA Express with that entered on the media label.

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 12

Glossary of terms

Glossary of terms

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

Table 12-1: Glossary

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

Table 12-1: Glossary

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

Table 12-1: Glossary

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

Table 12-1: Glossary

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

Table 12-1: Glossary

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

Worldwide Technical Support

Europe, Africa and Middle East

Tel: +44 (0)1763 262963
Fax: +44 (0)1763 264407
Web: http://www.plasmontech.com
Email: emea.support@plasmon.com

North America, South America and Asia/Pacific

Tel: +1-877-585-6793 or +1-719-593-4437
Fax: +1-719-593-4192
Web: http://www.plasmontech.com
Email: tech.support@plasmon.com

Sales

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

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

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

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

Plasmon