

Archive Management Software

# AMS

PROFESSIONAL

## Administration Guide



**Alliance**  
Storage Technologies Inc.

## 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 Alliance Storage Technologies Inc.

### Trademarks

**Plasmon, UDO, Archive Appliance, Archive Appliance Express, and NETArchive** are registered trademarks of Alliance Storage Technologies Inc. Copyright 2017.

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

### Limited Warranty

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

### Changes

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

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

Additional information may be obtained from your supplier, or from the addresses on the [Contact Details](#) 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 Alliance could void the user's authority to operate equipment.

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

## Contact Details

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

Email: [sales@astiusa.com](mailto:sales@astiusa.com)

Web: [www.astiusa.com](http://www.astiusa.com)

Tel: 719.593.7900

Fax: 719.592.4164

## Support

Email: [support@astiusa.com](mailto:support@astiusa.com)

Tel: 877.585.6793/719.593.4437

Fax: 719.593.4164

## How to Use This Guide

This guide describes in detail the Archive Management Software and the operation of the NETArchive and Archive Appliance. It is aimed at system administrators.

## Related Documentation

Please refer to the following document for further information:

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

## Revision History

Document Revision Number	System Software Version	Major Features
10-104334-00	6.00.xx	<ul style="list-style-type: none"><li>• First Release supporting NETArchive</li></ul>
810-104334-02	6.01.xx	<ul style="list-style-type: none"><li>• Changes supporting enhancements including support for the Archive Appliance, Licensing, NETArchive ODA2 libraries and drives, new 6TB SAS RAID drives, and Windows Azure Cloud Provider support.</li></ul>

# *Archive Management Software*

*Contents*

Preliminaries .....	ii
<i>Copyright Statement</i>	ii
<i>Trademarks</i>	ii
<i>Limited Warranty</i>	ii
<i>Changes</i>	ii
<i>Safety</i>	iii
<i>FCC Note</i>	iii
<i>Contact Details</i>	iv
How to Use This Guide .....	v
Related Documentation.....	v
Revision History .....	vi
<i>Contents .....</i>	<i>vii</i>
<i>Introduction.....</i>	<i>1</i>
Archive Management Software .....	2
<i>Optical Media Migration</i>	2
<i>Media Management</i>	2
<i>Cloud Migration</i>	3
<i>Data Encryption and Key Management</i>	3
Archive Management Software Archive Solutions .....	4
<i>NETArchive</i>	4
<i>Plasmon UDO Archive Appliance</i>	11
<i>Getting Started - The AMS Quick Start Guide..</i>	<i>19</i>
Getting Started with Archive Management Software.....	20
Prerequisites: Determine the AMS Configuration to support Your Archiving Needs.....	20
<i>What Data Archives Will You Define?</i>	20
Configuring the AMS: Quick Start Common AMS Setup...	26
<i>How to Access the AMS Web Interface</i>	26
<i>Please refer to <a href="#">Managing Services</a> on page 63 for more details.</i>	43



<i>The AMS User Interface</i> .....	47
Starting the Web Interface .....	48
System - Status Page Features .....	51
<i>Menu Bar</i>	51
<i>Online Help</i>	52
<i>Tool Tips</i>	53
<i>System Menu</i> .....	55
System - Status.....	56
<i>Environmental Status</i>	58
Setting the Time and Date .....	61
<i>Setting Time and Date Manually</i>	61
<i>Synchronising Time and Date with an NTP Server</i>	62
Managing Services .....	63
Updating the System Software .....	73
<i>Load from Desktop (HTTP)</i>	73
Notification .....	74
<i>Configuring email (SMTP) Notification</i>	74
<i>Configuring SNMP Notification</i>	76
<i>Notification History</i>	77
Licensing.....	79
<i>Types of AMS License Keys</i>	79
<i>How the AMS's Licensing Works?</i>	80
<i>Applying New License Keys</i>	81
<i>Defining Cloud Accounts</i>	83
<i>Network Menu</i> .....	87
Network Settings.....	88
<i>Configuring Network</i>	88
<i>Users</i>	93
<i>Groups</i>	97
<i>Shares</i>	100
Authentication .....	106

**Storage Menu ..... 113**

**RAIDs ..... 114**

*Viewing RAIDs* 115

*Assigning Global Hot Spare Disks to a RAID* 116

*Adding Storage RAID* 116

**Volumes ..... 118**

*About Volumes* 118

*Creating an Archive* 118

*Creating an Unmanaged Volume* 129

*Viewing and Editing Volume Properties* 130

*Special Consideration for "Bulk migration"* 139

**Media ..... 143**

*Adding Media to the NETArchive* 143

*Removing Media from the NETArchive* 144

*Adding and Removing Media with the AA* 145

*Online Media* 146

*Offline Media* 149

*Search Media* 150

*Storage - Media Details* 152

*Recall All Files from a Single Media (or single media side)* 155

**Files ..... 158**

*Browsing Files* 158

*Displaying File/Folder Details* 158

*Searching Files* 163

**Data Protection Menu ..... 165**

**Data Protection ..... 166**

*Backup* 166

*File Recovery* 171

*Key Recovery* 180

**Replication ..... 182**

*Configuring Replication* 182

**Security ..... 189**

<i>Encryption</i>	189
<i>UDO Guard (Archive Appliance only)</i>	192
<b>Background Recall.....</b>	<b>195</b>
<i>Stage 0: Setup</i>	195
<i>Stage 1: Initialization</i>	196
<i>Stage 2: Recall Progress</i>	196
<i>Stage 3: Background Completion</i>	197
 <i>Diagnostics Menu .....</i>	 <i>199</i>
<b>System Jobs .....</b>	<b>200</b>
<b>Storage Devices.....</b>	<b>201</b>
<i>Disk Status Icons</i>	205
<i>Other Status Icons</i>	208
<b>Optical Drives .....</b>	<b>210</b>
<b>Self Tests .....</b>	<b>213</b>
<i>Self Test</i>	213
<i>Archive Test</i>	215
<b>System Information.....</b>	<b>216</b>
 <i>Shutdown.....</i>	 <i>221</i>
<b>Shutdown the AMS using the Web Interface .....</b>	<b>222</b>
<b>Shutdown the Archive Appliance Using the Library Power Switch .....</b>	<b>223</b>
<i>AA16, AA32, AA80 and AA174 Models only</i>	223
<i>AA238, AA438 and AA638 Models only</i>	223
<i>NETArchive S-Series Library only</i>	224
 <i>Troubleshooting.....</i>	 <i>225</i>
<b>Troubleshooting .....</b>	<b>226</b>
 <i>Using the Archive Appliance Keypad Interface for Media Operations &amp; Setting IP Address ...</i>	 <i>243</i>
<b>Configuration .....</b>	<b>244</b>

<i>Setting the IP Address</i>	244
<i>Setting the Netmask</i>	245
<i>Setting the Gateway IP Address</i>	245
<b>Adding UDO Media .....</b>	<b>246</b>
<i>Adding Backup UDO Media via the Mailslot</i>	246
<i>Adding Data UDO Media via the Mailslot</i>	247
<i>Adding UDO Cleaning Cartridge via the Mailslot</i>	247
<i>Adding Data UDO Media via Direct Slot Access</i>	248
<i>Possible Problems</i>	250
<b>Removing UDO Media .....</b>	<b>251</b>
<b><i>Using the NETArchive Keypad Interface for Setting Library IP Addresses .....</i></b>	<b><i>253</i></b>
<b>Configuring the NETArchive NA-S10 IP Address.....</b>	<b>254</b>
<i>Setting Library IP Address via NETArchive NA-S10 Keypad Interface</i>	254
<i>Setting IP Address via AMS User Interface</i>	256
<b>Configuring the NETArchive NA-S30 Maintenance IP Address.....</b>	<b>258</b>
<i>Setting Library Maintenance IP Address via NA-S30 Keypad Interface</i>	258
<i>Setting Maintenance IP Address via AMS User Interface</i>	261
<b>Starting and Stopping the NETArchive NA-S10 and NA-S30 Libraries.....</b>	<b>263</b>
<i>Starting the NA-S10 Library</i>	263
<i>Stopping the NA-S10 Library</i>	263
<b><i>The Archive Appliance with an Additional Library Attached .....</i></b>	<b><i>265</i></b>
<b>Additional Library .....</b>	<b>266</b>
<i>Attaching an Additional Library</i>	267
<i>Attached Library Keypad Interface</i>	268
<i>Attached Library Web Interface</i>	269
<b><i>Using the NETArchive Express (NAE) or the Archive Appliance Express (AA Express).....</i></b>	<b><i>273</i></b>

Media Labelling.....	274
Media Handling.....	275
<i>Inserting Media in the NAE</i>	275
<i>Inserting Media in the AA Express</i>	275
<i>Ejecting Media from the NAE</i>	276
<i>Ejecting Media from the AA Express</i>	276
<i>Cleaning Media</i>	276
Basic Operation .....	278
<i>Writing to ODA and UDO Media</i>	278
<i>Reading from UDO Media</i>	279
<i>Media Request Queuing</i>	279
Action Request Notification.....	280
<i>Status Icons</i>	280
Action Requests.....	281
<i>Offline Media Management .....</i>	<i>285</i>
Storage of Offline Media .....	286
<i>NETArchive and UDO Media</i>	286
<i>When to Offline Media</i>	287
<i>How to Offline Closed Media</i>	288
<i>How to Offline Closed Media</i>	289
Open Offline Media.....	291
Offline Media Return Requests.....	293
<i>Returning Offline Media</i>	293
Library Slot Maps.....	296
<i>AA16/32 Appliance</i>	297
<i>AA80 (2 drive) Appliance</i>	298
<i>AA80 (4 drive) Appliance</i>	299
<i>AA174 (2 drive) Appliance</i>	300
<i>AA174 (4 drive) Appliance</i>	301
<i>AA174 (6 drive) Appliance</i>	302
<i>AA238, AA438 and AA638 Appliances</i>	303
<i>Offline Media Management with the AAE .....</i>	<i>305</i>

Storage of Offline Media.....	306
Organisation of Offline Media.....	307
<i>By Sequence Number</i>	307
<i>By Date Range</i>	307
<i>By Barcode</i>	307
<i>Glossary of Terms .....</i>	<i>309</i>
Glossary of Terms .....	310

# *Archive Management Software*

## *Chapter 1* *Introduction*

## Archive Management Software

The Archive Management Software (AMS) provides a complete Archive Management Solution when combined with Alliance's NETArchive and Archive Appliance solutions. The AMS includes a customised Linux Operating System providing support for NETArchive and Plasmon Archive Appliance Optical libraries and drives, a web-based administrator's user interface, and a Hierarchical Storage Management package called SSM (Storage Space Manager).

SSM, the heart of ASTI's Archive Management Solution, can be broadly divided into four separate functional components:

- Optical Media Migration and Recall
- Media Management
- Cloud Migration and Recall
- Data Encryption and Key Management

The AMS presents the integrated archiving solution as a NAS (Network Attached Storage) storage device, supporting both Windows and Unix/Linux connectivity via the CIFS and NFS protocols (FTP is supported as well). Users, once authenticated via the on-board support for Windows Active Directory, LDAP or local users, through standard Ethernet connectivity, then transfer data to the optical libraries and drives for archiving or for accessing previously archived data.

### Optical Media Migration

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

### Media Management

Optical media can be managed through the web interface by specifying offline rules or selecting specific media to be offlined. Media that are available for offlining can then be removed from the library through the keypad or AMS user interface, or be used to return new or existing media to the library.



It is common practice to have one offline copy of last resort outside the library for disaster recovery protection while one copy remains in the library for fast retrieval. Request for offline media request to satisfy user request for data recalls are raised by sending alerts via email and/or SNMP to the administrator(s) (which is configurable) who can retrieve the media using the barcode for identification and return it to the library.

## Cloud Migration

Cloud migration utilizes the same migration rules and procedures as optical migration except in the area of copies. With Cloud integrated Storage, only 1 copy of the data is created and migrated to the cloud. Once migrated to the cloud, the cloud provider, such as Amazon Web Services, or Windows Azure, will create multiple replicated copies of the migrated data and store this data across multiple (typically four) datacenters located in that particular region.

## Data Encryption and Key Management

For Archives where data encryption is enabled, the AMS Software will encrypt all data to be migrated to the cloud or media. This encryption is certified to FIPS 140-2 standards, meeting strict compliance rules set forth by the USA and Canadian governments. Encryption is performed using AES-256 bit strength required for data to be archived past the year 2035. Additionally, as part of any robust encryption system, a key management system exists which is tightly integrated into SSM. It generates random 256-bit keys (used for AES encryption) and protects them on a second storage device (cloud or network share).

Following NIST (National Institute of Science and Technology) standards for key management, all externally stored keys are in turn encrypted using a split-key encryption strategy (system wide Masterkey and archive specific Archive key). A full suite of disaster recovery mechanism exists for data and for keys.

---

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

---

## Archive Management Software Archive Solutions

The AMS supports and is packaged with several optical archiving solutions, including:

- NETArchive
- NETArchive Express
- Plasmon UDO Archive Appliance
- Plasmon UDO Archive Appliance Express

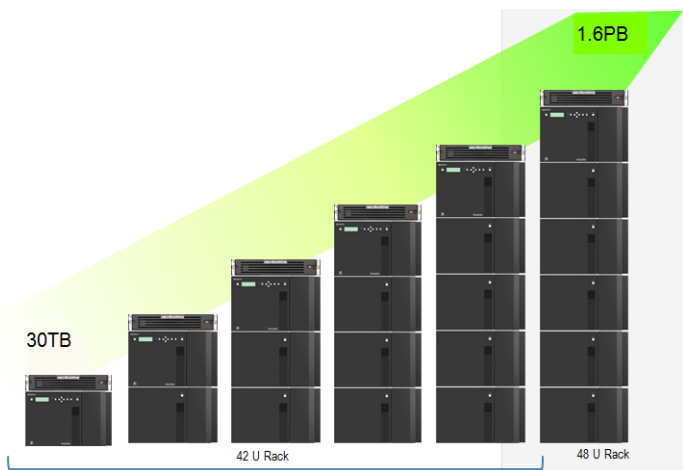
### NETArchive

NETArchive is the convergence of industry-leading technological developments that together establish the new paradigm in data archiving. Specifically architected to address the pain points associated with storing critical data assets, this revolutionary new solution reduces business risks, secures data unaltered, enables regulatory compliance, and simplifies operations. Designed to extend your investments in technology and data, this all-inclusive, high-capacity solution delivers up to 1.6PB of archival storage within a single rack-mount footprint, with ground breaking performance. With a flexible, modular system architecture, the NAS solution delivers enterprise-level capability to all archiving environments whether small or large via elastic scalability.

The NETArchive is a game-changer offering the perfect fusion of professional archiving features and progressive true WORM media technology. The solution changes the way archiving is accomplished with increased performance, higher capacities, fibre channel communication to drives, and increased reliability over tape and disk.

### NETArchive S-Series Libraries Scales from 30TB to 1.6TB

Extensibility and investment protection are fundamental features of the NETArchive solution. Designed to meet the archiving requirements of any size, solutions start with near line capacities of up to 30TB in a single unit, with enterprise systems scaling up to 1.6PB within a standard rack mount footprint. To balance performance and storage capacity, enterprise systems can accommodate up to 18 drives.



NETArchive S Series Libraries

### NETArchive S-Series Enterprise Libraries

NETArchive Enterprise Libraries have high capacity storage ranging from 30TB up to 1.6PB of near line data in a single rack.

The libraries are available in scalable configurations and suitable for any sized business or organization.

NETArchive Enterprise Libraries provide the following features:

- High capacity & performance
- Scalable configuration adapt to any sized business or organization
  - NA-S30 Master Unit (required) provides foundation
  - NA-S60 & NA-S100 Optional Extension Libraries upto 5 optional libraries
  - 11 Standard configurations available
- Modular rack mount components
  - All library components are 7U High
  - Rack mounting required
- Optional redundant power supplies for high availability

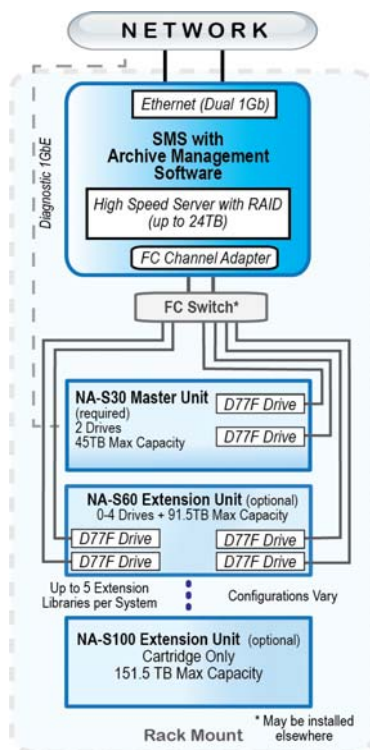
- Convenient space efficient rack mount options that conserves IT floor space, 268TB per Square Foot (based on 24" x 36" rack footprint)



NETArchive S Series Library

Scalable Network Attached Storage (NAS) Solution for Enterprise Archives

- Dual 1Gb Ethernet NAS Connectivity
- Storage Management System (SMS)
- Archive Management Software (AMS)
- NETArchive S Series Libraries
  - 1 master & up to 5 optional extensions
  - 8Gbps FC Optical Drives, FC Switch may be rack installed with other components or elsewhere or rack mount only
  - Secure Write-Once-Read-Many (WORM) optical media, multi-media 1.5TB to 3.0TB Media Cartridge design



### NETArchive S-Series Small to Medium Libraries

NETArchive Entry-Midrange NA-S10 Library provide the following features:

- Convenient pullout media drawer for fast loading and media exchanges
- Highly reliable robotics provide fully automated Media Transport Assembly
- Supports upto 2 Optical S Series D77U Drives
- Supports upto 10 Nearline Cartridges, providing upto 15TB nearline capacity

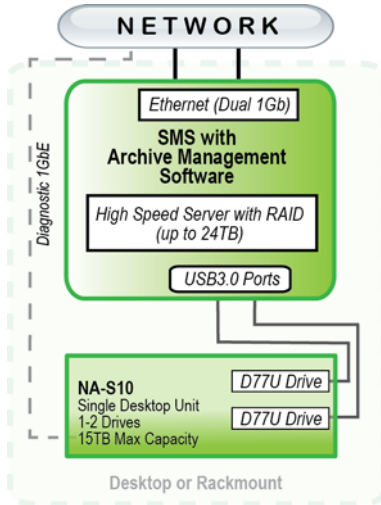
- Desktop or rack mountable options (5U)
- Optional redundant power supply for high availability
- Connectivity to NETArchive SMS
  - Super speed USB 3.0 interface to optical drives
  - Ethernet connectivity to library for library control



NETArchive S Series Small Library

Scalable NAS Solution for Small to Medium Archives

- Dual 1Gb Ethernet NAS Connectivity
- Storage Management System (SMS) with up to 72TB RAID
- USB 3.0 Connectivity to Optical Drives
- Desktop or rack mount
- Secure Write-Once-Read-Many (WORM) 1.5TB optical media
- Upto 15TB nearline capacity
- Operates within a standard office or IT environment
- No special environmental conditions required



NAS Solution for Small to Medium Archives

### NETArchive Express

The NETArchive Express (NAE), offering the lowest profile Network Attached Storage (NAS) device, is a large archiving solution within a small package. The NAE is functionally similar to the standard NETArchive only without the automated library robotics, and includes RAID, archive management software, and a single NETArchive Optical ODA drive for writing to archiving media. The NAE is specifically designed for those organizations that require a smaller optical archive or require cloud based archives of any size.

*NETArchive Express provide the following features:*

- Excellent solution for small to medium archives
- Provides a high-speed, high-capacity foundation for archiving large amounts of unstructured data
- Excellent archiving solution for cloud-based archives, with high speed access to the most recent data

- An optical ODA drive (provides immutable compliant archive storage)
- Compact size optimized for an office environment



### NETArchive Media

Archiving with optical storage is the most secure method of archiving data. NETArchive Media technology, based on Sony ODA technology, is at the core of ASTI's NETArchive archiving solutions. ISO Certified NETArchive Media meets today's diverse requirements for storing static data over the long-term. This archiving media is available in Write-Once-Read-Many (WORM) format, offered in 1.5TB to 3.0TB capacity.

#### Multi-Media 1.5TB Cartridge Design

- Compliant WORM preserves data unaltered for > 100 years
- High-capacity, low-cost
- Provides unquestioned record authenticity, withstanding chain of evidence scrutiny in court proceedings
- Cartridge prevents human contact and secures media
- Phase Change Technology providing 100+ year life guarantee
- Small profile lends itself to off site storage as needed
- Improved media reliability with special protective hard coating
- Does not require special environmental conditions while stored
- UDF Multi-volume format



- Cartridges are equipped with an RFID chip



Multimedia Cartridge

## Plasmon UDO Archive Appliance

The Archive Appliance (AA) product line features modular architecture and design in order to provide customers with an optimized data archiving solution. Each NAS archiving solution can be configured specifically for the needs of the organization according to capacity, scalability, performance, features, and budget. ASTI's Archive Appliance line of NAS storage devices combine all of the resources necessary for managing and storing data effectively over the long-term. NAS storage devices consist of:

- Storage Management System (SMS) Server
- One or more fully automated optical archiving libraries
- Archive Management Software (AMS) (preconfigured) with optional features.

## Enterprise Libraries

Designed to support the data capacity requirements of the largest corporations, Enterprise libraries feature state-of-the-art automation and robotics. Libraries include dual media transport assemblies, barcode scanners, 10 disk bulk magazine load, hot swappable UDO drives, redundant power supplies, and modular scalability. Four models are available that scale from 9.8TB to 38.3TB. The Enterprise Archive Appliance is available with the Elite SMS only.

- Increase storage capacity incrementally with designed-in scalability. Choose from four different models that scale to meet future data archiving requirements and can be field upgraded as required. Add UDO drives and media slots to scale the 164 base model to the AA238 within the same cabinet; add expansion bays to scale from the AA238 to the AA438, or the AA438 to the AA638.
- Additionally, an extension cabinet can be added doubling capacity to 76.6 TB.



Plasmon UDO library

### Entry-Midrange Scalable Models

Two models of fully automated robotic Archive Appliance midrange libraries are available with scalable capacities that feature dual media transport assemblies, barcode scanners and UDO drives. Available with a Standard or Elite SMS, RAID configurations will vary based on selection (raw capacity from 2 to 24 TB. Standard libraries are equipped with SATA drives and Elite with SAS drives.

Models are as follows:

- AA80 can be configured with two or four UDO drives and scales from 1.2TB (20 slots) to 4.8TB (80 slots). Available as stand alone or with 19" rack mount kit.
- AA174 can be configured with 2, 4, or 6 UDO drives and scales from 6TB (100 slots) to 10.4TB (174 slots).
- Additionally, an extension library can be added increasing capacity to up to 638 additional media slots.



## Ultra Density Optical (UDO) Media for the Archive Appliance

Archiving with optical storage is the most secure method of archiving data. Ultra Density Optical® (UDO) technology is the core of many of ASTI's Plasmon UDO Archive Appliance archiving solutions. ISO Certified UDO® digital storage media meets today's diverse requirements for storing static data over the long-term. This archiving media is available in Rewritable and WORM formats, with both formats offered in 30GB UDO1 and 60GB UDO2 capacities.



UDO Media

## Library Components

Component	Description
<b>Dual Picker</b>	Transfers UDO media between drives, media slots and Mailslot (IEE).
<b>UDO Drive(s)</b>	The number of UDO drives available for reading/writing media is model-dependent: <ul style="list-style-type: none"> <li>- AA80 = 2 or 4</li> <li>- AA174 = 2, 4 or 6</li> <li>- AA238/AA438/AA638 = 2, 4 or 6</li> </ul>
<b>Barcode Reader</b>	Reads the unique identifier on each UDO disk.
<b>Media Slots</b>	House the media inside the Archive Appliance.
<b>Mailslot (IEE)</b>	UDO media is introduced to the Appliance via the mail slot or via direct slot loading. See <a href="#">Adding UDO Media</a> on page 246.
<b>Server</b>	A server is housed within the Appliance. This manages the Appliance hardware, configuration, and network connectivity. In the AA238, AA438, AA638, AA80A12 and AA174A12 models the server is mounted above the library enclosure.

## Archive Appliance Express Hardware

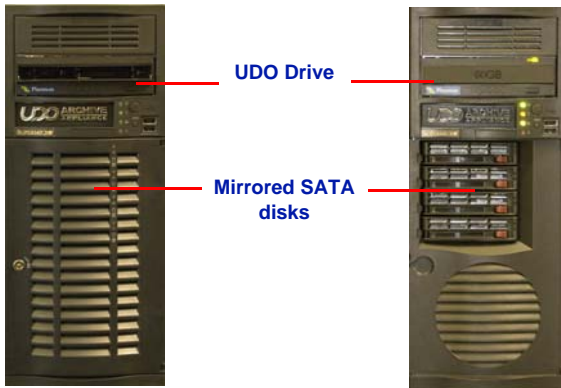
The Archive Appliance Express (AAE) Rackmount model consists of:

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



The AAE Desktop model consists of:

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



### Archive Appliance Express Supported RAID Configurations

The AAE can be configured with two, three or four SATA disks in the following configurations:

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

## IP Network Port Usage

In the Network-Configuration section of the web interface, the port usage can be blocked from access. The AMS software uses the following network ports.

*Table 1-1: Network port details*

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

Table 1-1: Network port details

Port	Name	Comments
4003	Rquotad (NFS)	Only active if NFS service is turned on
8000	Java Debug	Blocked by default
30000	System manager service	Required for replication service

Table 1-2: Network port details: UDP

Port	Name	Comments
111	Rpcbind	
137	Netbios-ns	
138	Netbios-dgm	Filtered, no service
177	Xdmcp	Filtered, no service
502	Asa-appl-proto	Filtered, no service
623	Asf-rmcp	Filtered, no service
664	Secure-aux-bus	Filtered, no service
998	Puparp	Filtered, no service
2049	NFS	
3664	UPS Engine	Filtered, no service
4000	Network Status Monitor, rpcstatd	used by NFS



# *Archive Management Software*

## *Chapter 2*

### *Getting Started - The AMS Quick Start Guide*



The following should be considered within your archiving strategy:

1. **Archive Volumes – Determine Archive Volume requirements**  
Archiving storage and segregation of archive data will have to be determined. For example:
  - Do you have healthcare data for different modalities such as Oncology or Radiology, or legal data such as court proceedings or residential data that must be segregated or have restricted access to certain users or groups?
  - Do you have Content Management Systems (healthcare, financial, legal, and corporate, etc.) whose data will be stored?
  - Will the Archive Data need to be segregated due to users authorized for access or due to data management requirements?
2. **Storage Tiers – Determine what archive data storage tiers will be utilized and how this supports your DR contingency plans.**  
Archive data can be stored on Optical media, in the cloud, or on both. In determining the storage tiers to be utilized for your Archives, it is important to consider primary and secondary DR copies.
  - It is highly recommended to have 2 copies of data stored on the Archive Storage Tiers.
  - A primary copy should be stored onsite, with a secondary copy being stored offsite.
  - The recommendation is to store the primary copy on optical, with the secondary copy being stored:
    - o On Optical media and shipped offsite to a DR location.
    - o In the cloud being remote to your primary installation (a hybrid strategy).
    - o Replicated to a secondary NETArchive or Archive-Appliance system providing high availability failover in the event of a DR situation.
3. **RAID Cache Size – Determine your RAID Cache sizing for each Archive**  
“Active Archives” can be defined as archives where data is not only being added, but is constantly being accessed. In this case, you will want to try and keep this active data on the RAID cache. Therefore, a larger amount of RAID storage should be dedicated to the Archive to provide high performance.

"Inactive Archives" can be defined as archives where data is being added, but the data is rarely being accessed. In this case, use a smaller amount of RAID storage, as infrequent access needs does not justify the expense of added RAID storage.

Considerations for sizing your RAID cache for the Archive include:

- Consider access patterns. If data is accessed frequently in its first year, but not in subsequent years, you will want to size your RAID cache to facilitate storing 1 years worth of archive data.
- Consider migration speed. If you will be constantly migration data at a rate of 1TB per week, you may wish to have at least a 1 TB buffer added to your Archive Volumes RAID Cache size.

---

*Important: It is important to not initially oversize an Archive Volume's RAID Cache size. Archive Volume RAID Cache sizes can be expanded, but not reduced.*

---

#### 4. Authentication – Data must be secured from unauthorized access

Data is always vulnerable to unauthorized access. For this reason it is important to plan how you will protect the access to archive data. Techniques to be considered for implementation include:

- User authentication can be implemented in multiple ways:
  - o Utilize Windows Active Directory to extend your existing user policies to your Archives. In this way, security administration is implemented via existing corporate standards. **This is the most common user authentication technique deployed.**
  - o Utilizing LDAP for Unix / Linux environments, extending your existing user policies to your Archives.
  - o AMS Named Users, where a User Names and Passwords can be configured. This is typically utilized where a specific application such as a content management system will be the only system access the archive data.

---

*Critical: The usage of user groups is highly recommended (such as Windows Active Directory). This allows the access authorization to be associated with the groups, where modification of users to be easily added or removed without having to update ACLs (Access Control List) for every file within the AMS system. Alternatively, if groups are not used, every time users are added or removed from access authorization you will have to modify all ACL's on potentially millions of files.*

---

5. Network Shares – Consider utilizing multiple Network Shares rather than many Archive Volumes

In almost every organization, data is segregated and access authority is authorized by groupings. An example of groupings might be departments such as Sales, Marketing, HR or by function such as executive corporate information.

If the archive data will be managed in the same way (archive storage tiers, copies, encryption, and replication) then one Archive Volume can be created. Data segregation can then be implemented by having multiple shares that map to unique directories, one for each unique group. This facilitates creating many unique shares for individual groups with access control implemented through Windows Active Directory for example.

This greatly improves the efficiency and scalability of the system, lowering requirements such as total optical drives required, more efficient usage of RAID cache space for logical volumes associated with each Archive Volume's partition, and reduces concurrent open media operations (swapping) reducing media operations and hardware cycles.

6. System Backups – Determine your AMS system backup location.

The backup location is where the AMS will backup key system information for restoration of the system should a disaster recovery be required. By having a backup of the system, restoration of the AMS control structures and archive file systems can be accelerated rather than doing a restore from the actual archive media (which is always possible but has much longer business continuity Recovery Time Objectives).

By default, backups are written to the on board SSD's installed in the SMS Server. This provides a basic backup, but it is always possible that these hardware images could be compromised.

**Optionally and highly recommended, you can also have a copy of these backups (full and incremental) written to a backup network share.** This provides the highest level of protection in the event of a physical disaster of your equipment.

---

*Important: It is highly recommended that a backup network share location be implemented to ensure the highest level of protection of system backup information and to accelerate system restores should they be required.*

---

### Other Required AMS Infrastructure Decisions to be Considered

Other key decisions to be formulated into your archiving strategy include the following:

1. Replication feature – Replication can be enabled to meet stringent high availability and business continuity needs  
The AMS Replication feature keeps a replicated Archive Volume ready for failover should a DR event occur. If you will be utilizing the Replication feature for high availability business continuity, you will have to define your replication configuration and replication schedule. This will consist of an Active Archive Volume on your primary NETArchive or AA system, and a Passive Archive Volume on your secondary NETArchive or AA system.
2. Data Encryption feature – Data encryption can be enabled for additional data security  
To protect important corporate and private information, whether secured within the physical hardware or possibly removed and offsite, data encryption ensures the data is protected even if it falls into unauthorized hands or is inadvertently placed in the public domain where stiff penalties under mandates such as HIPAA exist.  
Data encryption can easily be added to any Archive to provide this much needed level of protection and is FIPS 140-2 certified and meets NIST standards for encryption key management.
3. Location of the File Level Encryption Key Vault  
If you will be encrypting your data, you will have to determine where your file level encryption keys will be stored. The AMS ensures unique symmetrical encryption keys are created for each unique file. The Encryption Key Vault must be located outside of the physical NETArchive or Archive Appliance system. Your options include:

- Utilizing the backup network share location.
  - Utilizing the Cloud (AWS or Windows Azure).
4. You must establish AWS and/or Windows Azure Cloud Accounts if archiving to the cloud
- If you will be archiving to the Cloud or encrypting data and placing your Encryption Key Vault in the Cloud, you will need to establish a Cloud Account(s). Once defined, you will need to create a storage account and have the access key details when defining your cloud account to the AMS.

## Configuring the AMS: Quick Start Common AMS Setup

### How to Access the AMS Web Interface

To access the AMS for the NETArchive or Archive Appliance, you will utilize the AMS Web Interface. Via a web browser, enter the network name or IP address of the system in the URL field. For example, enter <http://192.168.0.1> in your browser. The default username and password is admin/admin.

Please refer to [Starting the Web Interface](#) on page 48 for more details. In this section you will also find instructions on how to change your default username and/or password which is highly recommended to secure system access.

The quick start process is divided into the following key steps. Most customer environments can be configured in minutes. The only steps required are dependent on your configuration and the features you will be utilizing. This is indicated in the setup matrix below

Step	Action	Step Required For
1	Configure your Product License and Feature Key	All
2	Configure your AMS Backup Strategy	All
3	Configure your Masterkey	Encryption, Cloud
4	Configure Cloud Accounts for Cloud Archiving	Cloud
5	Configure the Encryption Key Storage Vault	Encryption
6	Configure Archive Volumes for long-term data retention	All
7	Configure User Access and Authentication	All
8	Configure your Network Shares for access to Archiving Volumes	All
9	Ensure the appropriate AMS Services are started	All
10	Configure Replication Pairs	Replication

### STEP 1: Configure Product Licensing

Initially, your AMS will be configured with a temporary License Key and if you have purchased Cloud, Encryption or Replication features, a Feature Key. Once you receive your permanent License Key, you will need to install the key. If you have already received it, you should install it now.



To install the License Key and / or Feature Key:

1. Select SYSTEM – LICENSING menu item.
2. Cut and paste your License Key and your Feature Key into the appropriate fields.
3. Click Save. The new Keys should be accepted and you should see the license and feature details change.

System - Licensing			
Product key:	4000-A070-7808-4858-7838		
Product License			
License type:	Permanent		
License expiry date:	08 February 2019		
Days until license expiry:	395		
New license key:	F028-5D5C-1230-6E41-76AB		
Current license key:	F028-5D5C-1230-6E41-76AB		
Feature License			
Feature(s):		Total Quota	Used Quota
	Replication	5120 GB	0 GB
	Encryption	5120 GB	0 GB
	Cloud migration	5120 GB	0 GB
Storage Slot Limit:	30		
New feature key:	0305-0051-E005-0005-002E		
Current feature key:	0305-0051-E005-0005-002E		
<input type="button" value="save"/> <input type="button" value="cancel"/>			
New license key created New feature key created, please restart the SSM service for the change to take effect.			

Please refer to [Licensing](#) on page 79 for more details.

## STEP 2: Configure Your AMS Backup Strategy

By default, the backup of the AMS System information and archive files is written to the onboard SSD's within the SMS Server. But, to ensure the protection of your system and faster recovery should a DR event occur, we highly recommend a NETWORK SHARE be defined as a backup location.

To define a network backup share, do the following:

1. Define a network share within your existing storage infrastructure. This storage location should be on a tier 1 storage location which is backed up on a regular basis. The space required is not excessive. As an example, an installation

where 300 million files are archived might take 50GB of backup space for the full and incremental copies.

2. Select Data Protection – Backup menu item.
3. Select the Configuration tab and fill in the configuration screen. As you can see below, you will need to specify the NETWORK option, Protocol, Host location of the network share, the share name, the backup directory (which must exist and be empty), and Domain / User name / Password.

- a. Click connect and look for the connection successful message. Make sure to click Save.
- b. If you click then on the status tab, you can either start the backup or it will actually start itself after a few seconds.

Please refer to [Backup](#) on page 166 for more details on the backup process, configuring and monitoring.

### STEP 3: Configure Your Master Key

#### GO TO STEP 4 IF NOT UTILIZING CLOUD STORAGE OR DATA ENCRYPTION FEATURES

The Master Key is utilized to encrypt all file level encryption keys and the information associated with your AWS or Microsoft Azure accounts.

**Critical:** It is imperative that you retain the Master Key. The Master Key is not stored outside the system. If a DR event occurs, you may have to re-enter the Master Key. If you do not have the Master Key, YOU WILL LOSE ALL ACCESS TO ALL ENCRYPTED DATA.

### To set the Master Key:

1. Select Data Protection - Security menu item. The following page will be displayed.

**Data Protection - Security** Masterkey UDOGuard

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

**Master Key**

Key  generate ⓘ

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

**File Encryption Key Protection Mode**

No protection
  Protect to share
  Protect to cloud

**Archive Key(s)**

Enable	Archive Name	Key

save cancel

2. In the Master Key section, click on the generate button. This will generate a master wrapping key (32 bytes long).
3. Click the Save button. You will be prompted to save this key in a safe location for usage during a DR event.

**Important:** Ensure this Master Key is retained in a secure location, such as a fire safe vault. The key may be require in the event of a disaster situation.

4. YOU MUST CLICK THE SAVE BUTTON AGAIN. This will confirm that you have saved your key and will set the key.

**Warning:** Once the Master Key is set, you will no longer be able to retrieve it from the system. You must ensure you retain the Master Key. This ensures security of your archive data.

Please refer to [Creating a Master Key](#) on page 190 for more details.

#### STEP 4: Configure Your Cloud Accounts for Archiving

##### GO TO STEP 5 IF NOT UTILIZING CLOUD STORAGE

If you are utilizing the cloud for the long-term retention of Archive Data or as a Encryption Key vault, you must define your cloud account details.

1. Select System - Services menu item.
2. Click on the Cloud Agent link and the "Cloud Provider Account Details" page will be displayed.
3. If archiving data to the cloud, fill in the Files tab.

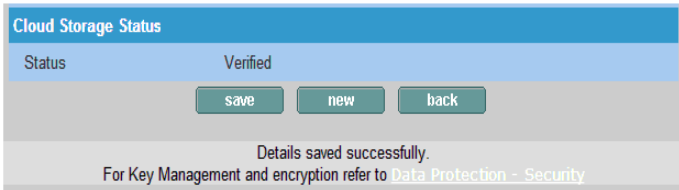
The screenshot shows a web interface for configuring cloud provider details. It features two tabs: 'Files' and 'Keys'. The 'Files' tab is selected. The main section is titled 'Cloud Provider Account Details' and contains the following fields:

- Provider Name: Amazon S3 (dropdown menu)
- Account Name: (empty text input)
- Access Key ID: admin (text input)
- Secret Access Key: (masked with asterisks)
- Bucket Name: (empty text input)
- Region: US Standard (dropdown menu)

Below these fields is a 'Cloud Storage Status' section with a 'Status' field showing '--'. At the bottom of the form are two buttons: 'save' and 'back'.

You must first create a [masterkey](#) to secure your provider details.

- a. For details on completing this page, see [Defining Cloud Accounts](#) on page 83
- b. Click "SAVE". This will result in the appliance connecting to the cloud and validating the account. Once completed, you should now see VERIFIED instead of NOT VERIFIED under status.



**Cloud Storage Status**

Status: Verified

Buttons: save, new, back

Details saved successfully.  
For Key Management and encryption refer to [Data Protection - Security](#)

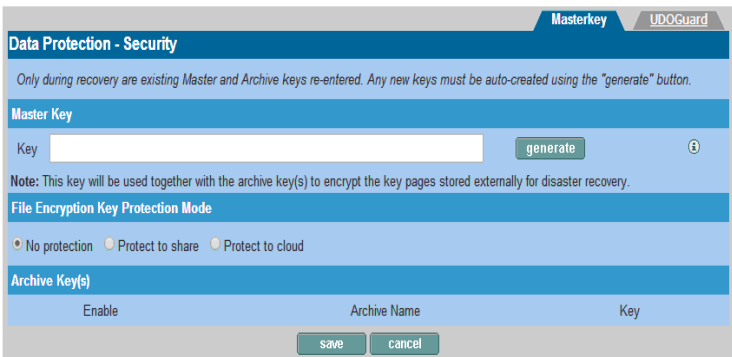
4. If you plan on using the Encryption option to Encrypt Archive Data, and you plan on placing the Encryption Key Vault in the cloud, you will have to click on the files tab and save access details using the same process. See STEP 5: Configure Your Encryption Key Storage Vault below.

## STEP 5: Configure Your Encryption Key Storage Vault

### GO TO STEP 6 IF NOT UTILIZING DATA ENCRYPTION

If you are utilizing the Encryption feature, you will have to select the location that will be used to store all your file level encryption keys.

1. Select the Data Protection - Security menu item. The following page will be displayed.



**Data Protection - Security** Masterkey UDGuard

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

**Master Key**

Key:  generate ⓘ

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

**File Encryption Key Protection Mode**

No protection  Protect to share  Protect to cloud

**Archive Key(s)**

Enable	Archive Name	Key

Buttons: save, cancel

2. In the File Encryption Key Protection Mode section, click on either "Protect to share" or "Protect to cloud" based on your storage location decision.
3. Click the Save button. The "No protection" option will disappear and your new selection should remain.

Please refer to [Setting the Protection Mode](#) on page 191 for more details.

## STEP 6: Configure Your Archive Volumes for Long-Term Data Retention

It is now time to set up your Archive Volumes. You will set these up based on archiving strategy that you determined as part of prerequisite planning.

The following process will be repeated for each Archive Volume that you are defining. For additional details on defining Archive Volumes, please refer to [Creating an Archive](#) on page 118 for more details.

1. Select the STORAGE – VOLUMES menu item
2. Click “add” a volume. The following page will be displayed.

Storage - Volumes - Add Volume			
Volume	Archive	Migration Policy	Release Policy
Volume Name		<input type="text" value="TIMTEST1"/>	
Select Volume Group		<input type="text" value="VG2"/>	
Space Available		<input type="text" value="1598.18GB"/>	
Volume Size		<input type="text" value="25"/> <input type="text" value="GB"/>	
Archive		<input checked="" type="checkbox"/>	
		<input type="button" value="next &gt;&gt;"/>	<input type="button" value="back"/>

- a. Define the “Volume Name”.
- b. Specify the RAID Cache Volume Size, then click next.

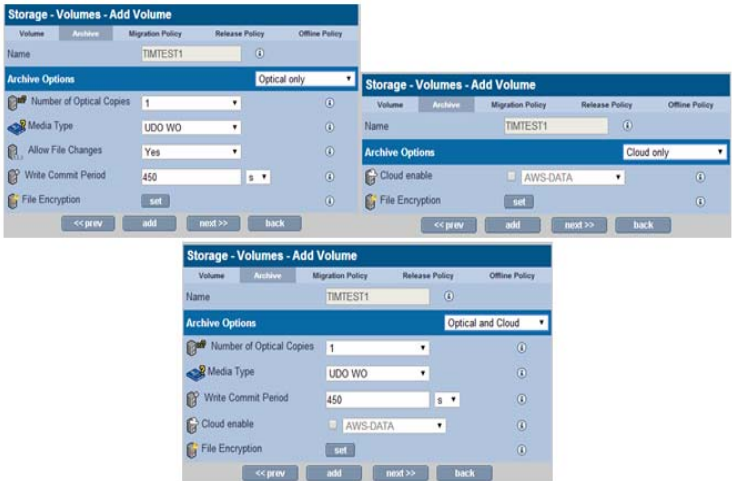
---

*Important: Remember to consider whether this will be an “Active Archive” or an “Inactive Archive” and that you can always increase the Volume Size but you cannot reduce the Volume Size later as discussed in prerequisite considerations.*

---

- c. You can now choose to create a Cloud only, Cloud and Optical, or Optical Only Archive Volume based on

your archive strategy. Please refer to [Creating an Archive](#) on page 118 for more details.



- d. Choose your Archive Volume type and then fill in the fields as appropriate. In the following examples, these are just examples of selections. You can configure each archive based on your specific needs as discussed above in prerequisite considerations.
  - i. For Optical only archives, you may wish to have 2 copies of media (1 for offsite DR)
  - ii. For Cloud, select the checkbox next to Cloud enable.
  - iii. For Optical and Cloud, select the checkbox next to Cloud enable and select 1 copy of media
- e. Do you want to enable Encryption? If not, proceed to the next step.
  - i. Click the SET button. This will take you to the Data

Protection – Security page where you need to establish the Archive Volume level Encryption Wrapping Key!

**Data Protection - Security**

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

**File Encryption Key Protection Mode**

No protection  Protect to share  Protect to cloud

**Archive Key**

Archive Name	Key	
<input type="text" value="TIMTEST1"/>	<input type="text"/>	<input type="button" value="generate"/>
<input type="button" value="save"/> <input type="button" value="back"/>		

- ii. Click the "Generate" button to have a 32 character symmetrical encryption wrapping key generated.
- iii. Click Save. AMS will prompt you to now print the screen and save this key for DR usage later, just like the AA Master Key before.

**Data Protection - Security**

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

**File Encryption Key Protection Mode**

No protection  Protect to share  Protect to cloud

**Archive Key**

Archive Name	Key	
<input type="text" value="TIMTEST1"/>	<input "="" type="text" value="wKeLyzWar9fMosm5oFUchV7uHKDxG1zxMFOkXw3/Fxo="/>	<input type="button" value="generate"/>
<input type="button" value="save"/> <input type="button" value="back"/>		

**NOW copy and paste all generated keys into a secure document!**  
Click again to save keys. Archive keys will then disappear from view.



- iv. Now click Save again, and you will return to the Add Volume page. The File Encryption option check-box will be checked.

### Storage - Volumes - Add Volume

Volume **Archive** Migration Policy Release Policy Offline Policy

Name  ⓘ

**Archive Options** Optical and Cloud ▾

Number of Optical Copies	<input type="text" value="1"/> ▾	ⓘ
Media Type	<input type="text" value="ODA WO"/> ▾	ⓘ
Allow File Changes	<input type="text" value="Yes"/> ▾	ⓘ
Write Commit Period	<input type="text" value="450"/> <input type="text" value="S"/> ▾	ⓘ
Cloud enable	<input checked="" type="checkbox"/> <input type="text" value="azure-data"/> ▾	ⓘ
File Encryption	<input checked="" type="checkbox"/>	ⓘ

- f. Now click “next”. The Migration Policy tab will now be displayed.

**Storage - Volumes - Add Volume**

Volume	Archive	Migration Policy	Release Policy	Offline Policy
Name	<input style="width: 100%;" type="text" value="TIMTEST1"/>			
<b>Minimum Criteria</b>				
Data must meet <b>all</b> of these criteria in order to be eligible for migration.				
Minimum File Age	<input style="width: 100%;" type="text" value="10"/>	s		
Minimum Wait Time	<input style="width: 100%;" type="text" value="20"/>	s		
Minimum Number of Migration Files	<input style="width: 100%;" type="text" value="1"/>			
Minimum Migration Size	<input style="width: 100%;" type="text" value="2"/>	MB		
<b>Maximum Criteria</b>				
Data that meets <b>any</b> of these criteria becomes eligible for migration.				
Maximum Wait Time	<input style="width: 100%;" type="text" value="30"/>	m		
Maximum Number of Migration Files	<input style="width: 100%;" type="text" value="10000"/>			
Maximum Migration Size	<input style="width: 100%;" type="text" value="2048"/>	MB		
Open Volume Limit	<input checked="" type="checkbox"/>			

<< prev
add
next >>
back

This defines the minimum and maximum time periods before new data written to the archive volume RAID Cache will be “migrated” to the archive storage tiers (optical and/or cloud).

**Typically users will utilize the default settings except for the “Open Volume Limit”.**

---

*Important:* Checking the Open Volume Limit will ensure that the AMS fills one media at a time before placing data on the next media

---



---

*Important:* Consider how many total Archive Volumes you will have. I.E. If you have 4 Archive Volumes and 4 optical drives, you could have up to 16 open media at 1 time which could result in heaving media exchanges, excessive amounts of open media, and reduced overall performance.

---

If you do not check this box, then the AMS will open multiple media cartridge and write data to them simultaneously, spreading data out across the media. This facilitates writing data much faster, but it also spreads data across media where time order of data is not preserved. Most users select to write to one media at a time until filled and closed.

Please refer to [Creating an Archive](#) on page 118 for more details.

- g. Click “next” and the Release Policy tab will now be displayed. This policy defines when archive data will be released from the RAID cache. File entries and

**Storage - Volumes - Add Volume**

Volume	Archive	Migration Policy	Release Policy	Offline Policy
Name			TIMTEST1	
<b>Watermark Policies</b>				
<input type="radio"/>	Never release files			
<input checked="" type="radio"/>	Start releasing files based on the following			
	All files when cache usage is above	<input type="text" value="95"/>	%	
	When cache usage is above	<input type="text" value="90"/>	%	
	Release files larger than	<input type="text" value="2"/>	KB	
	Release migrated files older than	<input type="text" value="2"/>	h	
	Release recalled files older than	<input type="text" value="24"/>	h	
	Stop releasing files when archive usage is	<input type="text" value="85"/>	%	
	Release file immediately after migration	<input type="checkbox"/>		

<< prev
add
next >>
back

Archive data will always remain on the RAID Cache after it is migrated to the Archive Storage Tiers. Once migrated, the release policy will determine how long the data will remain on the RAID based on the policy you set. **Most users will utilize the default values, where files will be released when a space shortage is encountered (based on the thresholds set).**

*Note: If this is an “inactive/deep archive”, where data is rarely accessed, you could consider making the RAID space small and checking “Release files immediately after migration”. When a read is requested, it will always be recalled from media.*

*Note: Note: If you desire to have all archive data always online, never to be released from the RAID Cache, then select “never release files”. It should be noted, once you utilize up all the RAID Cache for this archive, there will be no space to store additional data and future migrations will be denied unless you increase the Archive Volume RAID Size.*

Please refer to [Creating an Archive](#) on page 118 for more details.

- h. Click “next” and the Offline Policy tab will now be displayed.

This defines how the AMS will export media cartridges from the library when media needs to be imported to the library and no empty media slots exist. **Most users select the default option of “Least Recently Closed”** (oldest media).

Please refer to [Creating an Archive](#) on page 118 for more details.

- i. Click “add”. The AMS will now create the Archive Volume’s Partition on the RAID Cache (a logical volume) and define all internal policies for automated archive management. You will now be returned to the primary Storage – Volumes page.

## STEP 7: Configure User Access and Authentication

An important step to facilitating user and application access to the Archive Volumes is configuring how you will authenticate users. **The most common practice for authentication is the usage of Windows Active Directory.** By using Windows Active Directory, if present, you can then utilize the same authentication system for defining access to your archive data as with the rest of your storage resources.

1. Select the NETWORK – Authentication menu item. The following page will be displayed.

The screenshot shows a configuration window titled "Network - Authentication (CIFS)". It features two tabs: "CIFS" (active) and "LDAP". The form contains the following fields:

- Workgroup:** A radio button is selected, and the text "WORKGROUP" is entered in the adjacent text box.
- Domain Name:** An empty text box.
- Organization Unit (Optional):** The text "Computers" is entered in the text box.
- Preferred DC (Optional):** Two empty text boxes for entering IP addresses.
- User Name:** An empty text box.
- Password:** An empty text box.

Each text box has a small information icon (i) to its right. At the bottom of the window are four buttons: "save", "start", "diagnose", and "cancel".

2. This is where you will point to your Windows Active Directory Domain Controller. Complete the required information. It is likely that your network administrator may need to provide this information.
  - a. Click on "Domain Name" and fill in the Domain Name field.
  - b. Type in the Preferred DC (Domain Controller) and secondary DC IP addresses.
  - c. Provide the User Name and Password with access authority.

**CIFS** LDAP

### Network - Authentication (CIFS)

<input type="radio"/> Workgroup	<input type="text" value="WORKGROUP"/>	
<input checked="" type="radio"/> Domain Name	<input type="text" value="ENG"/>	
Organization Unit (Optional)	<input type="text" value="Computers"/>	
Preferred DC (Optional)	<input type="text" value="10.2.2.211"/> <input type="text" value="10.2.2.42"/>	
User Name	<input type="text" value="admin"/>	
Password	<input type="password" value="....."/>	

- d. Click on “Save”. You should now be connected to your domain controller.
3. To validate the connection to the Domain Controller, select menu option Network – Users and the following page will be displayed. You should now see the details associated with users defined within your environment.

**Network - Users**

ENG User Name  Advanced Search

[Total 203 Entries] Page 1 of 21

User Name	Role	CIFS	Replication	SSH	FTP
ENG\la1west		✓	✗	✗	✗
ENG\la2central		✓	✗	✗	✗
ENG\la3east		✓	✗	✗	✗
ENG\la4mailbox		✓	✗	✗	✗
ENG\laa		✓	✗	✗	✗
ENG\laasenk		✓	✗	✗	✗
ENG\laaccountingmailbox		✓	✗	✗	✗
ENG\ladmin		✓	✗	✗	✗
ENG\laandersonc		✓	✗	✗	✗
ENG\laaspen		✓	✗	✗	✗

1 2 3 4 5 6 7 8 9 10 >>> | Go

## STEP 8: Configure Your Network Shares for Access to Volumes

Access to the Archive Volumes that you have defined in the previous step is accomplished by creating a Network Share, making it accessible via SMB/CIFS or NFS. To define a Network Share:

1. Select the NETWORK – SHARES menu item.
2. Click the “ADD” button, the Network – Shares – Add page will be displayed

The screenshot shows the 'Network - Shares - Add' configuration interface. It features a top navigation bar with tabs for 'Protocols', 'Set Access', 'CIFS Attributes', 'CIFS Hosts', 'CIFS Admin', and 'NFS Attributes'. The 'Protocols' tab is selected. Below the tabs, there are several sections:
 

- Name:** A text input field containing 'HRarchive'.
- Shared Directory:** A text input field containing '/test1/HR' and a 'browse' button.
- Protocol:** A section with three options: 'CIFS' (checked), 'NFS' (unchecked), and 'FTP' (unchecked).
- Attributes:** A section with three options: 'Read only' (checked), 'Guest' (unchecked), and 'Visible' (checked).

 At the bottom of the form, there are two buttons: 'next >>' and 'back'.

3. Define the share as is exemplified in the illustration above:
  - a. Give the Network Share a name which will be made available on the network (visible option). In the example we have used “HRarchive”.
  - b. Select the directory that will be shared. This path will map to a specific Archive Volume you have created, along with a specific directory within that Archive Volume where data will be archived. In our example, “/test1/HR”, test1 is the Archive Volume and HR is the directory.
  - c. Select CIFS (access from windows) or NFS (access from Unix/Linux)

- Click next and the following page will be displayed. Click “create” to create this Network Share.

**Network - Shares - Add**

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

Name:

Shared Directory:

**Owner and Group**

Owner:   ⓘ

Owner Group:   ⓘ

**Access** [Total 3 Entries] Page 1 of 1

Name	Read	Write
root	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
root	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Everyone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ⓘ

<< prev | next >> |  |

Please refer to [Adding a Share](#) on page 100 for more details on customizing the share.

## STEP 9: Ensure Appropriate AMS Services Are Started

Finally, before users and applications can map to the share and start accessing the Archive volumes you have created, you need to ensure that the “Services” (system processes) are started. By default, the AMS services are typically turned off to minimize external access points to the system.

- Click the STORAGE – VOLUMES menu item. The System – Services page will be displayed. Ensure the appropriate services are started. These will include as illustrated below.

**System - Services**

Service	Status	Action
Cloud Agent	Started	<input type="button" value="stop"/>
CIFS	Started	<input type="button" value="stop"/>
NFS	Started	<input type="button" value="stop"/>
FTP	Stopped	<input type="button" value="start"/>
Replication	Stopped	<input type="button" value="start"/>
UPS	Stopped	<input type="button" value="start"/>
SSM	Started	<input type="button" value="stop"/>



Please refer to [Managing Services](#) on page 63 for more details.

### Start Accessing Shares

At this point, you are ready to start accessing your Network Shares. To accomplish this, you must simply map a network drive to a network share that you have created.

## STEP 10: Configuring Replication Pairs

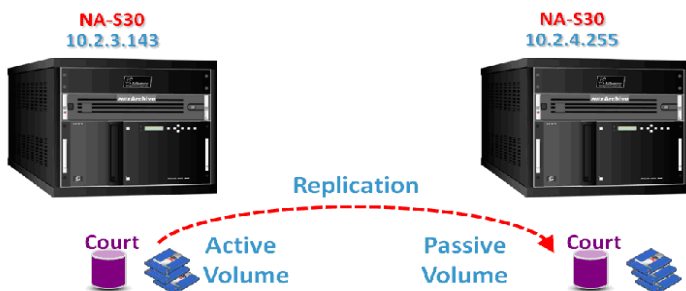
### **SKIP THIS STEP IF NOT UTILIZING REPLICATION**

If you will be utilizing the Replication feature for high availability business continuity, you will have to define your replication configuration and replication schedule.

The following diagram illustrates a replication configuration. The Court archive on the primary system is being replicated to the Court archive on the secondary (failover) system. The “Active Volume” is enabled for reading and writing data, while the “Passive Volume” is read-only.

The following procedure provides an outline on how to create a replication configuration:

1. On your primary system, create an Archive Volume. This will



be the “Active Archive Volume”. This can be an existing Archive Volume and can have existing data archived to the volume.

2. On your secondary system create an Archive Volume. This will be the “Passive Archive Volume”. This should be a new Archive Volume.
3. On your secondary system, click on the Data Protection – Replication menu item. The Data Protection – Active Replication Schedules page will appear. Click on the Passive tab.

Active Passive

Data Protection - Passive Replication Schedules

[Total 0 Entries] Page 1 of 1

Local Volume	Remote Volume	Remote Host	Status	Last Replication Time
--------------	---------------	-------------	--------	-----------------------

add cancel

- a. Click the “add” button. The Data Protection – Passive Replication Schedules – Add page will be displayed.
- b. Select the Archive Volume which is the passive target.

Data Protection - Passive Replication Schedules - Add

Volume COURT ▾

Owner admin browse ⓘ

create back

- c. Click the browse button and select the User Name to be used to connect from the Primary Replication system to this Passive Replication system.
- d. Click Create. Your passive volume is ready for usage.
4. On your primary system, click on the Data Protection – Replication menu item. The Data Protection – Active Replication Schedules page will appear.
  - a. On the Active tab, click the “add” button. The Data Protection – Active Replication Schedules – Add page will be displayed.

**Data Protection - Active Replication Schedules - Add**

Volume

**Passive System Options**

Passive Host  ⓘ

User Name  ⓘ

Password   ⓘ

Passive Volume  ⓘ

**Daily Schedule**

Start Time  :

- Select the Volume that will be your Active Archive Volume.
- Fill in the Passive Host IP Address or Host name.
- Type in the User Name and Password (what was selected when setting up the Passive schedule above).
- Click connect. All unused available Passive Volumes will be displayed in the drop down list. Select the appropriate Passive Volume.
- Select your daily scheduled Start Time for replication to occur.
- Click "add". The replication pairing has now been completed. The replication will occur as per the replication schedule. Please refer to [Replication](#) on page 182 for more details.

Active		Passive		
<b>Data Protection - Active Replication Schedules</b>				
[Total 1 Entries] Page 1 of 1				
Local Volume	Remote Volume	Remote Host	Last Job	Logs
<a href="#">COURT</a>	▶▶▶ COURT	10.2.3.69	Not Run	<a href="#">View</a>
<input type="button" value="add"/> <input type="button" value="cancel"/>				

**Important:** You must ensure that the Replication Service is started on the Primary and Secondary systems.

---

*Important: IMPORTANT: Both your primary and secondary system must be set to automatically synchronize with an Internet time service. This can be set by selecting the System – Time & Date menu item. See Synchronizing Time and Date with an NTP Server on page 34 for additional details.*

---

# *Archive Management Software*

## *Chapter 3*

### *The AMS User Interface*

## Starting the Web Interface

This section describes the details to start the AMS web interface.

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

`http://192.168.0.1`



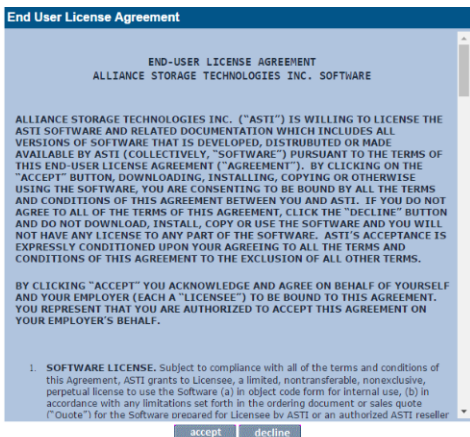
3. In the Web Interface login page, enter a valid AMS Administrator **Username** and **Password**.

---

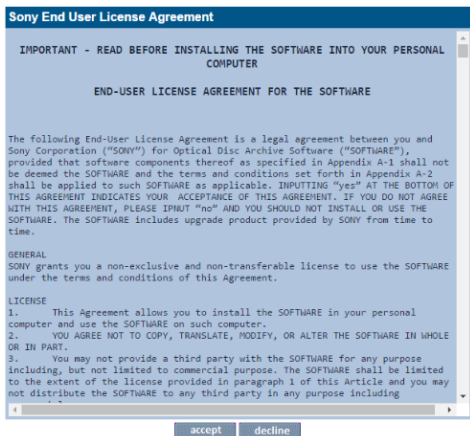
*Note: This is not the same as a Windows Domain Administrator.*

---

- The default administrator username and password is **admin**. It is recommended to change the password on first login. See [Modifying a User's Details](#) on page 96.
  - The default administrator can be used to add or remove additional administrator accounts.
4. Click **submit**. If this is the first time you are logging into the system, you will need to accept the ASTI End User License Agreement before continuing. If you have already accepted the EULA, it will not be displayed. Continue with Step 6. The ASTI EULA is displayed. Read the license agreement and click **accept**. The Sony EULA displays.



- If this is a NETArchive system and it is the first time you are logging into the system, you will need to accept the Sony End User License Agreement before continuing. If you have already accepted the EULA, it will not be displayed. Continue with the Step 6. The Sony EULA is displayed.



- Read the license agreement and click **accept**.  
The following Web Interface **System - Status** UI page is displayed. The **System - Status** page displays the current status of the appliance. For more details, see *System - Status* on page 56.

### System - Status




 **License expires within 30 days**

 **Spare media running low.**

#### License



Type: Grace      Days until expiry: **25**

#### Activity

	Last Backup:	2016/09/14 02:02:06
	Last Migration:	2016/09/14 03:25:36
	Last Recall:	0 recall completed in the last 24 hours.
	Last Replication:	No archives scheduled to be replicated.

#### Hardware

RAID(s) alarm on/off  **silence**

	Environmental: <b>OK</b>		Library: <b>10.2.2.74</b>
	RAID(s): <b>OK</b>		Optical Drive: <b>OK</b>
	Spare Media: 0		

#### Cloud

 0 Account(s) detected.



## System - Status Page Features

The **System - Status** page displays an overview of current system status and the menu bar.


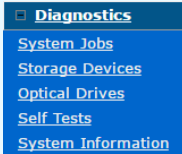




### Menu Bar

The menu bar provides access to the AMS's configuration and monitoring options, as well as to the online help.

*Table 3-1: Web interface menus*


Menu/icon	Use to
<div style="border: 1px solid black; background-color: #0056b3; color: white; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px 5px;"> <input type="checkbox"/> <b>System</b> </div> <ul style="list-style-type: none"> <li><a href="#" style="color: white; text-decoration: none;">Status</a></li> <li><a href="#" style="color: white; text-decoration: none;">Environment</a></li> <li><a href="#" style="color: white; text-decoration: none;">Time &amp; Date</a></li> <li><a href="#" style="color: white; text-decoration: none;">Services</a></li> <li><a href="#" style="color: white; text-decoration: none;">Software Update</a></li> <li><a href="#" style="color: white; text-decoration: none;">Notification</a></li> <li><a href="#" style="color: white; text-decoration: none;">Licensing</a></li> </ul> </div>	<p>Monitor the AMS's status, set the time &amp; date, monitor and configure the services, update the system software, configure alert notifications and review/apply licenses (Product and Feature License)</p> <p><i>With the AAE, the Environment option is not available in the System menu.</i></p>
<div style="border: 1px solid black; background-color: #0056b3; color: white; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px 5px;"> <input type="checkbox"/> <b>Network</b> </div> <ul style="list-style-type: none"> <li><a href="#" style="color: white; text-decoration: none;">Configuration</a></li> <li><a href="#" style="color: white; text-decoration: none;">Users</a></li> <li><a href="#" style="color: white; text-decoration: none;">Groups</a></li> <li><a href="#" style="color: white; text-decoration: none;">Shares</a></li> <li><a href="#" style="color: white; text-decoration: none;">Authentication</a></li> </ul> </div>	<p>Define the network configuration, users, groups, shares and authentication details.</p>
<div style="border: 1px solid black; background-color: #0056b3; color: white; padding: 5px;"> <div style="background-color: #003366; color: white; padding: 2px 5px;"> <input type="checkbox"/> <b>Storage</b> </div> <ul style="list-style-type: none"> <li><a href="#" style="color: white; text-decoration: none;">RAIDs</a></li> <li><a href="#" style="color: white; text-decoration: none;">Volumes</a></li> <li><a href="#" style="color: white; text-decoration: none;">Media</a></li> <li><a href="#" style="color: white; text-decoration: none;">Media Requests</a></li> <li><a href="#" style="color: white; text-decoration: none;">Files</a></li> </ul> </div>	<p>Configure RAID's and volumes, search and browse the media, and monitor offline media requests.</p>

Table 3-1: Web interface menus

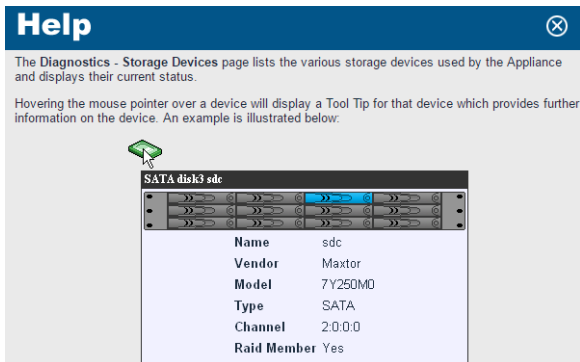
Menu/icon	Use to
 <ul style="list-style-type: none"> <li><a href="#">Data Protection</a></li> <li><a href="#">Backup</a></li> <li><a href="#">File Recovery</a></li> <li><a href="#">Key Recovery</a></li> <li><a href="#">Replication</a></li> <li><a href="#">Security</a></li> <li><a href="#">Background Recall</a></li> </ul>	Perform a system configuration backup, recovery of archive(s), recovery of the encryption key database, configure archives for replication, manage security keys including the Master Encryption Wrapping Key, Archive Encryption Wrapping Key(s), and background recall of files from optical media onto RAID.
 <ul style="list-style-type: none"> <li><a href="#">Diagnostics</a></li> <li><a href="#">System Jobs</a></li> <li><a href="#">Storage Devices</a></li> <li><a href="#">Optical Drives</a></li> <li><a href="#">Self Tests</a></li> <li><a href="#">System Information</a></li> </ul>	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.
	Reboot or shutdown the system.
	Display context-sensitive online help.
	Return to the Web interface <b>System - Status</b> 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 AMS's Help page will open in a pop-up browser Window, example:



**Help** ✕

The Diagnostics - Storage Devices page lists the various storage devices used by the Appliance and displays their current status.


Hovering the mouse pointer over a device will display a Tool Tip for that device which provides further information on the device. An example is illustrated below.

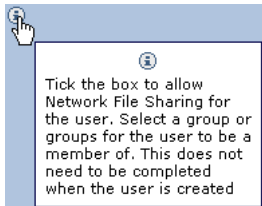



**SATA disk3 sdc**


<b>Name</b>	sdc
<b>Vendor</b>	Maxtor
<b>Model</b>	7Y250MO
<b>Type</b>	SATA
<b>Channel</b>	2:0:0:0
<b>Raid Member</b>	Yes

## Tool Tips

Wherever the  icon is present, hovering the mouse pointer over, it will display a relevant Tool Tip, example:







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

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

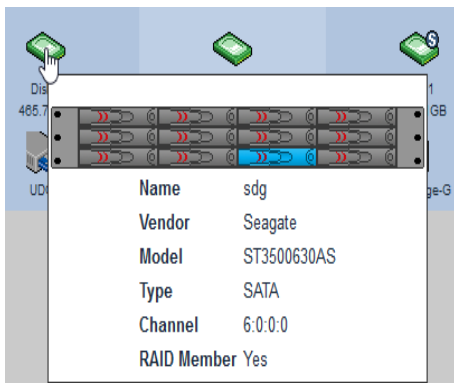
- Volumes and Volume Groups
- SATA/SAS Drives
- RAIDs
- Controllers
- Flash Media
- Attached Libraries

Hovering mouse over the device icons will display the device details.



*Note: Occasionally the popup windows may either appear in the wrong color or be positioned incorrectly. Simply refresh the page (press F5). This should reset the page styles and correct any display issues.*

*On Internet Explorer, pop ups may not appear at all. This can be rectified by switching the browser into "Compatibility View" mode.*



# *Archive Management Software*

## *Chapter 4* *System Menu*

## System - Status

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

**System - Status**

- License expires within 30 days**
- Spare media running low.**

**License**

Type: Grace      Days until expiry: **25**

**Activity**

	Last Backup:	2016/09/14 02:02:06
	Last Migration:	2016/09/14 03:25:36
	Last Recall:	0 recall completed in the last 24 hours.
	Last Replication:	No archives scheduled to be replicated.

**Hardware**      RAID(s) alarm on/off  **silence**

	Environmental: <b>OK</b>		Library: <b>10.2.2.74</b>
	RAID(s): <b>OK</b>		Optical Drive: <b>OK</b>
	Spare Media: 0		

**Cloud**

0 Account(s) detected.

The page is split into five areas:

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

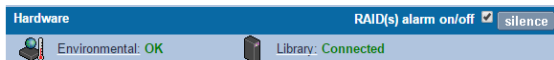
**System - Status**

**System RAID has failed/degraded.**

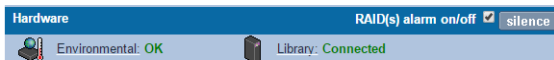
**Activity**

- The **License** area displays the license **Type** and **Days until expiry**.
- The **Activity** area displays the time of the **Last Backup**, **Last Migration**, **Last Recall** and **Last Replication**.
- The **Hardware** area displays the **Environmental** status of the SMS enclosure, the status of the **RAID(s)** and the optical drives. It also displays the quantity of **Spare Media** in the library. For

NA-S10 library, the IP of the library is displayed. For all other libraries, the status (“*Connected/Not Connected*”) is displayed.



- The **RAID alarm** can be enabled/disabled by checking/unchecking the **RAID(s) alarm on/off** check box.



‘**Silence**’ will also mute the enclosure but NOT the PSU alarm.

- At the bottom of the Status page, the Cloud agent status is displayed. The Cloud agent can assume four states:
  - Not started
  - Not configured
  - Not connected
  - Connected

Note that the Cloud agent configuration can be accessed by clicking the hyperlink.

- For the AAE only, the **Media Management** area as displayed below is included on the **Status** page and displays information about the currently loaded media and indicates what, if any, operator action is required.

**System - Status**

License expires within 30 days

**License**

Type: Temporary Days until expiry: 11

**Activity**

Last Backup:	Warning: System is not backed up.
Last Migration:	0 migration completed in the last 24 hours.
Last Recall:	0 recall completed in the last 24 hours.
Last Replication:	No archives scheduled to be replicated.

**Hardware**

Environmental: OK	RAID(s): OK
-------------------	-------------

**Media Management**

Dive empty
No action required

**Cloud**

0 Account(s) detected.
------------------------

## Environmental Status

The environmental status of the SMS can be viewed by clicking the “Environmental” hyperlink on the **System - Status** page. You can also navigate to the **System - Environment** page by clicking the **Environment** option in the **System** menu.

For the Archive Appliance, the following screen displays:

**System - Environment**

	System	Host Library
Motherboard Temperature	N/A	
CPU Temperature	N/A	
RAID Controller Temperature	34 Celsius	
RAID Slot Status	OK	
RAID BBU Status	OK	
System Fan	N/A	

cancel silence



For NETArchive, the following screen displays:

System - Environment (System)		System	
	Status	Value	
RAID Slot Status	Faulty	2 empty slot(s)	
RAID Battery Status	OK	Not Applicable	
Fan 1	OK	2900 RPM	
Fan 2	OK	2900 RPM	
Fan A	OK	3100 RPM	
CPU Temperature	OK	47 Celsius	
PCH Temperature	OK	44 Celsius	
Motherboard Temperature	OK	29 Celsius	
ROC Temperature	OK	68 Celsius	
Power supply 1	Present	Not Applicable	
Power supply 2	Present	Not Applicable	

The information shown includes the server environmental value such as **Motherboard Temperature**, **CPU Temperature**, **Power supply status** and **Fan** in the **System** tab. If the server includes a RAID controller, the RAID environmental information is also displayed.

For Archive Appliance, the **Host Library** tab displays all the host environment details such as Temperature, Front Fan Status, and Rear Fan Status. The attributes will vary depending on the connected library.

---

*Note: The Host Library tab is not displayed for NETArchive.*

---

System		Host Library
<b>Host Library - Environment</b>		
Temperature	25 Celsius	
Front Fan Status	OK	
Rear Fan Status	OK	
<b>Drive Temperature</b>		
UDO1	Temperature unavailable	
UDO2	32 Celsius	
UDO3	30 Celsius	
UDO4	31 Celsius	
cancel		silence

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

A value shown in green indicates that the environmental value is within operational range and acceptable.

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

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

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

## Setting the Time and Date

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

### Setting Time and Date Manually

- 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:  ⓘ

- Use the drop-down menu to select the correct **Time Zone** from the list.
- If appropriate, tick the box for **Daylight Saving** time.
- Set the **Date**: Either type in the date in the format YYYY/MM/DD (for example: 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]						

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

*Note: If the time, date, or timezone is changed, the system will reboot. Ensure that no users are connected before proceeding.*

## Synchronising Time and Date with an NTP Server

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



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

---

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

---

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

---

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

---

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

---

*Note: When the status of the NTP check box is changed, the system will reboot. Ensure that no users are connected before proceeding.*

---

## Managing Services

You can start or stop the services by navigating to **System - Services** page by clicking the **Services** option in the **System** menu.

For NETArchive

System - Services		
Service	Status	Action
<a href="#">Cloud Agent</a>	Stopped	<input type="button" value="start"/>
<a href="#">CIFS</a>	Stopped	<input type="button" value="start"/>
NFS	Stopped	<input type="button" value="start"/>
FTP	Stopped	<input type="button" value="start"/>
Replication	Stopped	<input type="button" value="start"/>
<a href="#">UPS</a>	Stopped	<input type="button" value="start"/>
SSM	Started	<input type="button" value="stop"/>

For Archive Appliance

System - Services		
Service	Status	Action
<a href="#">Cloud Agent</a>	Started	<input type="button" value="stop"/>
<a href="#">CIFS</a>	Started	<input type="button" value="stop"/>
NFS	Stopped	<input type="button" value="start"/>
FTP	Stopped	<input type="button" value="start"/>
Replication	Stopped	<input type="button" value="start"/>
<a href="#">UPS</a>	Stopped	<input type="button" value="start"/>
SSM	Started	<input type="button" value="stop"/>
Keypad	Stopped	<input type="button" value="start"/>

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

- Cloud Agent** - Manages the connections from the AMS to the Cloud provider account(s). Also, uploads and downloads data and metadata objects being migrated and recalled from the cloud. The Agent is started with SSM. Select the hyperlink to access and manage the Cloud provider account details - see [You must create a masterkey prior to configuring the cloud provider account details. For more details, refer Creating a Master Key on page 190 section. Configuring Cloud Service on page 82.](#)
- 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 - [Configuring CIFS \(Including Active Directory Server / NT Domain Server\)](#) on page 65.

- **NFS (Network File System)** - is a method of making a remote filesystem accessible on the local system. From a user's perspective, a 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 103](#).
- **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 68](#).
- **Replication** - This service controls replication between the Appliance and a partnered Appliance - [see page 182](#).
- **UPS (Uninterruptible Power Supply)** - Displays the status of an attached APC Smart UPS if one is present - [see page 71](#).
- **RAID Integrity Checker** - Monitors the data integrity of the RAIDs by reading / writing sectors and verifying them in the process. This process will begin after the service is started, and continues to operate in the background during times of low usage.
- **SSM (Storage Space Manager)** - Start or stop the HSM (Hierarchical Storage Management) software on the system. Stopping the SSM service halts communication between the RAID cache and the library. If SSM is stopped, all archive volumes are taken offline and no migration will be performed by the system.
- **Keypad** - Enable or disable the Library Keypad (applicable to the Archive Appliance library only).

---

*Note: In AAE Web interface, as there is no optical library attached, no keypad is present. For NETArchive libraries, the Keypad is not controlled by the AMS. For loading and unloading media from the library, see [Media](#) on page 143.*

---

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

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

*Note: When using Windows Active Directory, it is essential that the primary DNS address entered when following the network configuration procedure (see [Configuring Network](#) on page 88) is set to that of the Active Directory Primary Domain Controller. To determine the IP address of the Domain Controller, see [DNS Configuration for Windows Active Directory](#) on page 92.*

- From the menu bar, select **System - Services**, and click on **CIFS**.  
The **CIFS (Configuration)** page opens.
- Enter a **Server Description**.

The screenshot shows the 'System - Services - CIFS (Configuration)' page. At the top, there are two tabs: 'Configuration' (selected) and 'Security'. Below the tabs, the page title is 'System - Services - CIFS (Configuration)'. The main area contains several configuration fields, each with an information icon (i) to its right:

- Server Description:** A text input field containing 'NAS'.
- Connection Timeout:** A text input field containing '30' followed by the unit 'minutes'.
- WINS Server IP:** An empty text input field.
- Maximum Sessions:** A text input field containing '60'.
- File system code page:** A dropdown menu currently set to 'UTF-8'.

At the bottom of the form, there are three buttons: 'save', 'stop', and 'back'.

This is the name by which AMS advertises itself on the Windows network.

- 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.
- If required, enter a **WINS Server IP**. This is the IP address of the Windows Internet Naming Service (WINS) server.
- If required, enter the maximum number of sessions in the **Maximum Sessions** field.  
This is the maximum number of concurrent CIFS sessions that the Archive Appliance will accept. The default is 60 sessions.
- The **File system code page** option allows for a specific character encoding table to be used for all CIFS communications.

**CAUTION**

*Caution: The default is UTF-8, and should not be changed unless strictly necessary on the system's host network.*

### Configuring CIFS (Windows Networking)

The Common Internet File System (or SMB - Server Message Block) protocol allows file access through a Windows Network share.

Following is the procedure to configure a share:

1. From the menu bar, select **System - Services** page.
2. Click **CIFS**. The **CIFS (Configuration)** page opens.

Configuration		Security
<b>System - Services - CIFS (Security)</b>		
<input checked="" type="radio"/>	Workgroup	WORKGROUP ⓘ
<input type="radio"/>	Domain Name	ⓘ
	Organization Unit (Optional)	Computers ⓘ
	Preferred DC (Optional)	ⓘ
	User Name	ⓘ
	Password	ⓘ
<input type="button" value="save"/> <input type="button" value="stop"/> <input type="button" value="diagnose"/> <input type="button" value="back"/>		

3. Enter a **Server Description**.  
This is the name by which the AMS advertises itself on the Windows network.
4. 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.
5. If required, enter a **WINS Server IP**.  
This is the IP address of the Windows Internet Naming Service (WINS) server.
6. If required, enter the maximum number of sessions in the **Maximum Sessions** field.



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

- The **File System Code Page** option allows for a specific character encoding table to be used for all CIFS communications.

### CAUTION



*Caution: The default is UTF-8, and should not be changed unless strictly necessary on the AMS's host network.*

## Configuring CIFS Security

- From the menu bar, select **System - Services** and click **CIFS**. The **CIFS (Configuration)** page opens.
- 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 AMS to authenticate share users against a Windows domain and create file permissions for them. By configuring the Windows Domain security, the AMS 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)		Configuration	Security
<input checked="" type="radio"/>	Workgroup	WORKGROUP	ⓘ
<input type="radio"/>	Domain Name		ⓘ
	Organization Unit (Optional)	Computers	ⓘ
	Preferred DC (Optional)		ⓘ
	User Name		ⓘ
	Password		ⓘ

- Enter either:
  - A **Workgroup** - To authenticate against the local user database provided by the AMS.
 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 AMS to a Domain, additional details may be required:
  - Up to two **Preferred DC's** may be specified if desired, and the AMS will attempt to connect to them in order (*NT Compatible mode only*)
  - The **Organizational Unit** (OU) within the Active Directory structure in which the AMS will appear, (by default, the AMS will appear in the *Computers* OU).
  - A Windows **User Name** with the correct access rights to add objects to the Domain, and the user's **Password**. The password must be repeated in the **Confirm Password** field.
  - The **Domain Type** is derived from the connection to the Active Directory Server. The two types of domain controller are:
    - **ADS (Win2K+)**
    - **NT Compatible** (legacy)
- 4. Click **save** to save the changes, **stop** to stop the CIFS service, or **diagnose** to diagnose connectivity problems.

### Configuring NFS

The NFS networking service is configured via the **Network - Shares** page - [see page 100](#).

### Configuring FTP

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

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

The timeout settings for connections are:

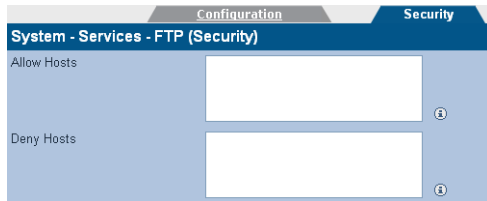
  - **Short**: 30 seconds
  - **Medium**: 60 seconds
  - **Long**: 300 seconds

The timeout settings for data transfers are:

  - **Short**: 150 seconds
  - **Medium**: 300 seconds
  - **Long**: 1500 seconds
5. Enter the maximum number of allowable concurrent FTP client connections (**Max Clients**).
6. Enter the maximum number of allowable concurrent FTP connections from the same IP address (**Max Clients per IP**).
7. Enter the maximum rate, in KB/s, of FTP data transfer (**Max Transfer Rate**).
8. Click on the **Security** tab.

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

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



Click **save** to save the changes.

9. Click **start** or **stop** to start or stop the services whenever appropriate.

## UPS

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

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

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

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

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

	Status	Configuration
<b>System - Services - UPS (Status)</b>		
UPS Model		
Status		
UPS Input Voltage		
Battery Charge Remaining		
Battery Time Remaining		
UPS Output Voltage		
UPS Temperature		
Last UPS battery charge		

The following information is displayed:

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

- **UPS Temperature** - The temperature of the UPS enclosure
  - **Last UPS battery charge** - The last time the power was transferred from the mains supply to the UPS.
2. Click on the **Configuration** tab.  
The **UPS (Configuration)** page opens. This allows configuration of the following.

Status	Configuration
<b>System - Services - UPS (Configuration)</b>	
Minimum battery level before shutdown	<input type="text" value="0%"/>
Minimum battery time remaining before shutdown	<input type="text"/> minutes

- **Minimum battery level before shutdown** - Select the percentage at or below which the UPS will shut down the system.
  - **Minimum battery time remaining before shutdown** - Enter the minimum UPS battery time remaining, in minutes, prior to the system shutting down.
- The UPS will initiate a shutdown of the system when either of these conditions are met.
3. Click **save** to save any changes.

## Updating 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 Desktop (HTTP)

1. Reboot the system into maintenance mode via the **Shutdown** menu.
2. From the menu bar, select **System - Software Update**.  
The **System - Software Update (HTTP)** page opens.



3. Click **Choose File** to locate the **Software Image File**.
4. Click **upload** 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.

## Notification

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

- Email (Simple Mail Transfer Protocol - SMTP) Notification - [Configuring email \(SMTP\) Notification](#) on page 74
- Simple Network Management Protocol (SNMP) Notification - [Configuring SNMP Notification](#) on page 76.
- A history of the notifications can be viewed via the Web interface, and should be regularly reviewed and its contents cleared ([Notification History](#) on page 77).

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

### Configuring email (SMTP) Notification

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



Email
SNMP

**System - Notification (SMTP)**

Enable Notification

ⓘ

SMTP Port ⓘ

ⓘ

ⓘ

ⓘ

**Notification Recipients**

Recipients ⓘ
Alert Threshold Level ⓘ

	<input checked="" type="radio"/> NORMAL <input type="radio"/> INFO <input type="radio"/> WARNING <input type="radio"/> CRITICAL <input type="radio"/> EMERGENCY
	<input checked="" type="radio"/> NORMAL <input type="radio"/> INFO <input type="radio"/> WARNING <input type="radio"/> CRITICAL <input type="radio"/> EMERGENCY
	<input checked="" type="radio"/> NORMAL <input type="radio"/> INFO <input type="radio"/> WARNING <input type="radio"/> CRITICAL <input type="radio"/> EMERGENCY
	<input checked="" type="radio"/> NORMAL <input type="radio"/> INFO <input type="radio"/> WARNING <input type="radio"/> CRITICAL <input type="radio"/> EMERGENCY
	<input checked="" type="radio"/> NORMAL <input type="radio"/> INFO <input type="radio"/> WARNING <input type="radio"/> CRITICAL <input type="radio"/> EMERGENCY

save history test alert cancel

2. Select the **Enable** box to enable, or untick to disable, the email notification service.
3. Enter the **SMTP Server** (email server) name or IP address.
4. Enter the **SMTP Port**. The default port used for email is 25.
5. If required, add a **Sender** to the notifications.
6. If required, add a **Username** to the notifications. If a username is added, that user's **Password** must also be entered.
7. Enter the email address(es) of up to five email notification **Recipients**.
8. Select an **Alert Threshold Level** for each recipient. These are described in [Table 1, "Notification Alert Threshold Levels," on page 77](#).

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

- 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.






## Configuring SNMP Notification

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

- Select the **Enable** box to enable the SNMP notification service.
- Enter a **GET Community String**. By default, the AMS does not use Community Strings to authenticate sent notifications. However, if required, a Community String can be entered here to enable this function.
- Enter a **Contact Name** for SNMP notifications.  
The Contact Name specifies the person to contact for the host, and how they may be contacted, for example: John Smith, X 1234, smith@alliance.com.
- Enter a **Contact Location** for SNMP notifications.  
The Contact Location lists the geographical location of the system, for example: Appliance-1, Server Room 2, Alliance HQ, UK.
- Enter the **TRAP Address** (IP address) and **TRAP Community String** of up to five SNMP notification Recipients.
- Select an **Alert Threshold Level** for each recipient. These are described in [Table 1, "Notification Alert Threshold Levels," on page 77](#).

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

*Table 1: Notification Alert Threshold Levels*

Level	Meaning
	Emergency alerts require immediate action. Setting the Alert Threshold Level to this level will only send notifications of Emergency alerts.
	Critical events require that action must be taken urgently. This level of notification includes notification of both Critical and Emergency events.
	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 alerts may require some action to be taken. This level of notification includes Info, Warning, Critical and Emergency events.
	Normal events require no action. This notification level includes all events.

## Notification History

The AMS keeps a log of all notifications that it has sent, and it is strongly recommended that this log be reviewed and cleared regularly.

- From the menu bar, select **System - Notification**.

- Click the **history** button.

System - Notification - History				
<input type="text"/>				[Total 75 Entries] Page 1 of 8
Number	Time	ID	Level	Message
75	2016/08/30 01:56:55	702	Normal	Web Administration: User (admin) from 172.17.102.64 has logged in.
74	2016/08/30 01:08:54	702	Normal	Web Administration: User (admin) from 172.17.102.64 has logged in.
73	2016/08/30 00:56:51	702	Normal	Web Administration: User (admin) from 172.17.102.64 has logged in.
72	2016/08/29 23:15:01	900	Critical	The system volume is nearly full, 84 percent space is used.
71	2016/08/29 15:15:01	900	Critical	The system volume is nearly full, 84 percent space is used.
70	2016/08/29 09:54:28	702	Normal	Web Administration: User (admin) from 10.2.2.30 has logged in.
69	2016/08/29 07:41:20	702	Normal	Web Administration: User (admin) from 172.17.102.57 has logged in.
68	2016/08/29 07:15:01	900	Critical	The system volume is nearly full, 84 percent space is used.
67	2016/08/29 07:13:54	702	Normal	Web Administration: User (admin) from 172.17.102.57 has logged in.
66	2016/08/29 07:11:46	3	Normal	Server running

1 2 3 4 5 6 7 8 >>  Go

- Click the **next** and **back** buttons to navigate through a log that spans multiple pages.
- Click any column header to order the list by that column (such as **Number**, **Time**, **ID**, **Level** or **Message**).
- Once satisfied that all alerts are sufficiently attended to, click **delete all**.
- A message appears advising that this will delete all event logs. Click **delete all** again to confirm.

## Licensing

The AMS is a proprietary software which provides the unique capabilities and functionality of Alliance's NETArchive and Archive Appliance.

### Types of AMS License Keys

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

#### Permanent License Key

Allows for permanent usage of AMS.

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

#### Temporary License Key

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

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

#### Grace License Key

Default key, instantiated when first activating the AMS.

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

#### Feature License

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

## How the AMS's Licensing Works?

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

License Status	Key Type	Actions
Active	Permanent Temporary Grace	<ul style="list-style-type: none"> <li>AMS fully functional</li> <li>Can install all available Software</li> </ul>
Active expiring within 30 days	Permanent Temporary Grace	<ul style="list-style-type: none"> <li>AMS fully functional</li> <li>Can install all available AMS software released before License Key expired</li> <li>Warning message issued daily: License Key expiring in xx days</li> </ul>
License Expired	Permanent	<ul style="list-style-type: none"> <li>AMS fully functional</li> <li>Can install AMS software released before License Key expires</li> <li>Informational message monthly: <i>License expired, software upgrades disabled</i></li> </ul>
License Expired	Temporary Grace	<ul style="list-style-type: none"> <li>AMS disables migrating and recall of data to/from media</li> <li>Cannot install any AMS Software</li> <li>Warning message issued daily: <i>Invalid license key, system disabled</i></li> </ul>

## Applying New License Keys

System - Licensing			
Product key:	584F-A923-C92B-EB26-B014		
<b>Product License</b>			
License type:	Grace		
License expiry date:	27 August 2017		
Days until license expiry:	29		
New license key:	<input type="text"/>		
Current license key:	FF51-A259-1069-3E6F-EACA		
<b>Feature License</b>			
Feature(s):		Total Quota	Used Quota
	Replication	1024 GB	0 GB
	Encryption	1024 GB	0 GB
	Cloud migration	1024 GB	0 GB
Storage Slot Limit:	30		
New feature key:	<input type="text" value="0301-0069-2401-0001-000E"/>		
Current feature key:	0301-0069-2401-0001-000E		
<input type="button" value="save"/> <input type="button" value="cancel"/>			
New feature key created, please restart the SSM service for the change to take effect.			

1. Enter or cut and paste the license key provided by Alliance Storage Technologies into the **New license key** text box. If your key is not available, contact Alliance Technical Support.

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

2. Enter the **New feature key** that defines the slots used in the system, replication, encryption and cloud migration quota details (contact Alliance Technical Support for details). When detecting a FC connected library (NA-S30 or higher), the AMS validates authorized slots. If no feature key is specified, the system will default to 10 slots for usage, from 1 to 10 and I/E station slots 28 to 30. Slots=30+ enables slot usage from 1 to 27 and I/E Station slots 28 to 30.

*Note: If no feature key is specified, the system will default to Slots=10 slots operationally.*

3. After the License Key is entered, click the **save** button. The AMS will process the license key and, if valid, will store the new license key as the active key. The newly applied License Key will be displayed in the **Current license key** field along with the **License type** (Permanent or Temporary), the date when the license expires and the number of days left before the license expires.

For NETArchive system, if the feature key is entered, *SSM service restart* is required for the slot licensing changes to take effect. If the slots value is set to 10 and if media are detected in the unlicensed slot, then media in the unlicensed slot will not be used and following error message displays. A newly installed AMS will automatically have a "Grace" license installed. Grace Keys can only be applied automatically by the AMS. If the slots value is set to 10 and if media are detected in the unlicensed slot, then media in the unlicensed slot will not be used and following error message displays.

The screenshot shows the 'System - Status' window with the following sections:

- System - Status:** Contains three warning icons and messages:
  - License expires within 30 days.
  - Slot usage limited to 10. Medias in unlicensed slots will not be used.
  - Spare media running low.
- License:**
  - Type: Grace
  - Days until expiry: 29
- Activity:**
  - Last Backup: 2017/07/28 02:01:18
  - 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:**
  - RAID(s) alarm on/off
  - Environmental: OK
  - Library: Connected
  - RAID(s): OK
  - Optical Drive: OK
  - Spare Media: 0
- Cloud:**
  - 0 Account(s) detected

The Feature license is handled in the same way as the Product License, however, it does not expire. Feature includes slot licensing, replication quota, encryption quota and cloud migration quota details.

*Note: You must create a masterkey prior to configuring the cloud provider account details. For more details, refer [Creating a Master Key](#) on page 190 section. [Configuring Cloud Service](#)*

Before you start the cloud service, it is necessary to define at least one cloud account. The cloud account contains the configuration settings required to establish an authenticated connection to a cloud provider.

You may define both AWS (Amazon Web Services) S3 storage accounts and Windows Azure storage accounts. It is possible to have many accounts to the same provider or multiple providers. Each account may have different access points or credentials providing flexibility.

There are two unique types of cloud account definitions:



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

**Keys** – Can define only 1 cloud account for the storage of encryption keys for this instance of the AMS. All encryption keys for all encrypted archive volumes are stored within this encryption key vault.

## Defining Cloud Accounts

*Note: You must create a masterkey prior to configuring the cloud provider account details. For more details, refer [Creating a Master Key](#) on page 190 section.*

1. From the **System - Services** page, click on **Cloud Agent**. The **Cloud Provider Account Details** page opens and will change based on the cloud provider you select.

The screenshot shows the 'Cloud Provider Account Details' configuration page. It features two tabs: 'Files' and 'Keys'. The 'Files' tab is selected. The form contains the following fields:

- Provider Name:** A dropdown menu set to 'Windows Azure'.
- Cloud Instance:** An empty text input field.
- Storage Account Name:** An empty text input field.
- Primary/Secondary Account Key:** A long text input field.
- Container Name:** An empty text input field.

Below the form is a section titled 'Cloud Storage Status' with a 'Status' field containing '--'. At the bottom of the page are two buttons: 'save' and 'back'.

The screenshot shows a web interface for configuring a cloud provider account. The main heading is 'Cloud Provider Account Details'. Below this, there are two tabs: 'Files' and 'Keys'. The 'Files' tab is active and contains several input fields: 'Provider Name' (a dropdown menu currently showing 'Amazon S3'), 'Cloud Instance' (a text input field), 'Access Key ID' (a text input field), 'Secret Access Key' (a text input field), and 'Bucket Name' (a text input field with a dropdown menu set to 'US Standard'). The 'Keys' tab is currently inactive. Below the input fields, there is a section titled 'Cloud Storage Status' with a 'Status' field that currently displays '--'. At the bottom of the form, there are two buttons: 'save' and 'back'.

2. In order to create an account, enter all the required fields.
  - **Cloud Instance:** This is the reference name which you will later apply to Archive Volumes when enabling it for the cloud. An example would be "AZURE-DATA".
  - **Access Key ID** or **Storage Account Name:** For AWS, the cloud account is identified by its Access Key ID. For Azure, the Storage Account Name is utilized.
  - **Secret Access Key** or **Primary/Secondary Account Key:** For AWS, the Secret Access Key provides access to the cloud account. For Azure, the Primary or Secondary Account Key is required.
  - **Bucket Name / Container Name:** For AWS and Azure respectively, this defines the name of the AWS Bucket or Azure Container that will be created to contain your archive data migrated to this cloud instance.
3. Click "Save". If the information entered is correct and the network connection can be established, the account details will validate and the account will be defined and locked in. After the account is validated and locked, it cannot be removed. This will be indicated with a "verified" status message. If any issues validating the account are encountered, this information can be corrected or the account can be removed.

---

*Note: If the account fails to be locked, the information can be corrected or the account can be removed.*

---



---

*Note: Some format and validation rules apply depending on the Cloud Provider. Space character ' ' and underscore '\_' may not be used for the bucket name. The bucket name needs to be*

---

*unique to that provider. Consult the Cloud Provider for restrictions on bucket names.*

---

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

---

*Note: You must create a masterkey prior to configuring the cloud provider account details. For more details about creating master key, see [Encryption](#) on page 189.*

---



# *Archive Management Software*

## *Chapter 5* *Network Menu*

## Network Settings

In the Network menu, you can configure the network settings that includes configuring the network, adding users, groups, and shares. You can define access authentication to the AMS using local users, LDAP or CIFS.

### Configuring Network

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



The screenshot shows the 'Network - Configuration (Configuration)' window. At the top, there are tabs: 'Configuration', 'Network Interfaces', 'Hosts', 'Ports', and 'Interface Usage'. The 'Configuration' tab is selected. Below the tabs, the window title is 'Network - Configuration (Configuration)'. There are four main sections:

- Hostname:** A text input field containing 'NAS-6737495512' with an information icon to its right.
- Domain Name:** An empty text input field with an information icon to its right.
- Network Interface:** A section header.
- Default Network Interface:** A dropdown menu currently showing 'eth0'.
- Domain Name Server Settings:** A section header.
- DNS Servers:** Three empty text input fields with an information icon to the right of the last one.

At the bottom of the window, there are two buttons: 'save' and 'cancel'.

2. Enter a **Hostname** for the Archive Appliance.
3. Enter the **Domain Name** which the Archive Appliance belongs to.
4. Select the **Default Network Interface** from the drop-down list.
5. Enter the IP address(es) of up to three **DNS Servers**. Multiple DNS Servers are usually used to offer continuity of Domain Name resolution if the primary server fails. For more details to configure the Archive Appliance to use with Windows Active directory, see [DNS Configuration for Windows Active Directory](#) on page 92.

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

Network - Configuration (Network Interfaces)						
Interface	Enabled	DHCP	IP Address	Netmask	Connected	Bond
 eth0	✓	✓	<input type="text" value=""/>	255.255.0.0	✓	
 eth1	✗	✓			✗	

The following information is displayed:

- **Interface** - The Ethernet port name, *eth0* (the AMS has a second port, *eth1*). Clicking on the interface name shows the network port's configuration. For details, see [Setting a Static IP Address](#) on page 90.
- **Enabled** - Indicates whether the Ethernet port is enabled.
- **DHCP** - Indicates whether Dynamic Host Configuration Protocol (DHCP) is enabled.

---

*Note: By default, DHCP is enabled.*

---

- **IP Address** - Displays the IP address of the port.
  - **Netmask** - Displays the Network mask of the port.
  - **Connected** - Indicates whether or not the network connection is operational.
  - **Bond** - On the AMS indicates whether or not the two Ethernet ports are bonded. This is used to provide load balancing or fault tolerance. For details on how to configure bonding, see [page 92](#).
7. Click on the **Ports** tab. The AMS's administration TCP/IP ports are listed.

Network - Configuration (Ports)	
HTTP Port	<input type="text" value="80"/>
SSH Access Port	<input type="text" value="22"/>

- **HTTP Port** - The port number for access via the Web Interface. The default HTTP port is 80. The HTTP Port will

also be used by Alliance support engineers when accessing the web interface remotely. See [Updating the System Software](#) on page 73.

- **SSH Access Port** - The port number for local and remote access via SSH. The default SSH port is 22. The SSH Port will also be used by Alliance support engineers when accessing the command-line interface remotely. See [Updating the System Software](#) on page 73.
8. Click on the **Interface Usage** tab. This will list the protocols available, with check boxes for all of the available interfaces.

Protocol	eth0	eth1	Info
<b>CIFS</b>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">i</a>
<b>NFS</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>
<b>FTP</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>
<b>SSH</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>
<b>HTTP</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>
<b>HTTPS</b>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">i</a>
<b>Replication</b>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">i</a>

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

9. Click **save** to save the changes.

### Setting a Static IP Address

1. From the menu bar, select **Network - Configuration (Network Interfaces)**, and click on a network interface's name. Following page displays.



**Network - Configuration (Network Interfaces) - Update**

Name	eth0
Enabled	<input checked="" type="checkbox"/>
DHCP	<input checked="" type="checkbox"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/> ⓘ

**Port Bonding**

Create a bond with port(s)	eth3 <input checked="" type="checkbox"/> eth2 <input type="checkbox"/> eth1 <input type="checkbox"/>
Bond Mode	Fault Tolerance <input type="radio"/> Load Balance <input checked="" type="radio"/>

**Ethernet Port Information**

Ethernet MAC Address	0C:C4:7A:32:10:AC
Speed	1 Gbps Full Duplex
Sent (Bytes)	56394398
Received (Bytes)	69396414
Link Status	<input checked="" type="checkbox"/>

2. Clear the DHCP check box to change the IP Address, Netmask and Default Gateway.
3. Enter the **IP Address**, **Netmask** and **Default Gateway**. The network administrator can provide these details.
4. Select the required eth port to create a bond with the port. For more details, see [Bonding Network Ports](#) on page 92.
5. Click the **save** button.

### Creating a Static Hosts Table

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

1. From the menu bar, select **Network - Configuration**, and then click on the **Hosts** tab.

Network - Configuration (Hosts)	
IP Address	Host Name(s)
[Total 2 Entries] Page 1 of 1	

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

- Click **add** to add a new host.

The screenshot shows a web form titled "Network - Configuration (Hosts) - Add". It contains two input fields: "IP Address" and "Host Name(s)". Each field has a small circular icon with an 'i' next to it, likely representing an information or help tooltip.

- Enter the **IP Address** and **Host Name(s)**, 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 88](#)) is one of the AD domain's specified nameservers. To determine the IP address of the nameserver:

- Using a Windows PC on the same AD domain as the Appliance, select **Start menu > Run...**
- Type **cmd** and press **Enter** to open a Windows Shell.
- At the command line, enter **nslookup** followed by the domain name entered in step 3 of the network configuration procedure (see [page 88](#)). Press **Enter**.
- Consult the Network Administrator to determine which of the displayed IP addresses should be used as the primary DNS address.

### Bonding Network Ports

The system 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).

- From within the **Network - Configuration (Network Interfaces)** page, click on a network interface name.
- Check the **Create a bond with port(s)** tick box.
- The radio buttons for **Fault Tolerance** and **Load Balance** are enabled. **Fault Tolerance** is selected by default.
- 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 system 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 AMS, whether defined locally or sourced from an Active Directory domain or LDAP server.

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

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

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 **Search** function.

**Network - Users**

User Name

It is possible to search using a user's **User Name** and the asterisk may be used as a wild card. This search is not case-sensitive.

### Adding a User

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

Network - Users						
User Name <input style="width: 100px;" type="text"/>						[Total 4 Entries] Page 1 of 1
User Name	Role	CIES	Replication	SSH	FTP	
admin	Administrator	✗	✓	✓	✓	
agent	Read-only Administrator	✗	✗	✗	✗	
nslcd		✗	✗	✗	✗	
saslauth		✗	✗	✗	✗	

- 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 Selected Groups

def\_group  
mailnull  
srmmsp  
supp1  
sunrpc

>> <<

**Password Setup**

Password  ⓘ Confirm Password

**Service Privileges**

Network File Sharing  Replication  FTP  SSH  ⓘ

**Role**

Administrator  Read-only Administrator  Operator  ⓘ

- 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.*

- Enter a **Description** for the User.
- Select a **Primary Group** for the user to be a member of. The default group is `def_group`.
- 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.
- Enter and confirm the user's **Password** (required).
- Tick the **Network File Sharing** check box to enable CIFS for the User and select a Group from the **Network Sharing Group Privileges** list.
- 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 AMS'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 AMS, including making changes to system configuration, volumes, archives and other settings.
  - A **Read-Only Administrator** may log on to the Web Interface and view all pages, but cannot make any changes.
  - An **Operator** has read-only access to the Web Interface, limited to the **System - Status**, **Storage - Online Media** and **Storage - Offline Media** pages.
13. Click  to add the User.

## Deleting a User

*Note: You must have the privilege to delete a user, else the following **delete** button is not displayed.*

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

Network - Users						
User Name <input type="text"/>				[Total 4 Entries] Page 1 of 1		
User Name	Role	CIFS	Replication	SSH	FTP	
admin	Administrator	✗	✓	✓	✓	
agent	Read-only Administrator	✗	✗	✗	✗	
nslcd		✗	✗	✗	✗	
saslauthd		✗	✗	✗	✗	

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

## Modifying a User's Details

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

Network - Users						
User Name <input type="text"/>				[Total 4 Entries] Page 1 of 1		
User Name	Role	CIFS	Replication	SSH	FTP	
admin	Administrator	✗	✓	✓	✓	
agent	Read-only Administrator	✗	✗	✗	✗	
nslcd		✗	✗	✗	✗	
saslauthd		✗	✗	✗	✗	

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 testlogin

Primary Group: del\_group

**General Group Definition**

Group	Selected Groups
mainnull	del_group
smmsp	supp1
testgroup	supp2
testgroup2	supp3
vsxentf	vsxentf

**Password Update**

Password:  Confirm Password:

**Service Privileges**

Network File Sharing  Replication  FTP  SSH

**Role**

Administrator  Read-only Administrator  Operator

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

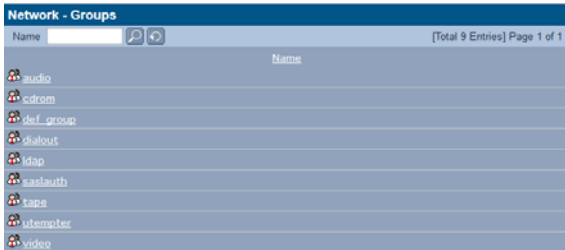
## Groups



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

## Adding a Group

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



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

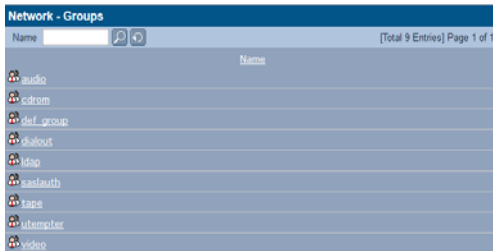


3. Enter a **Name** for the Group. The **Group ID** is automatically assigned.
4. Click **add** to add the Group.

## Modifying a Group Details

After a group is created, its name and members may be edited.

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



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



**Network - Groups - Update**

Name  ⓘ

Group Id

Member(s)

agent

admin

>>

<<

save delete back

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

### Deleting a Group

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

**Network - Groups**

Name  🔍 ↻

audio

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

**Network - Groups - Update**

Name  ⓘ

Group Id

Member(s)

agent      admin

>>      <<<

save      delete      back

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

## Shares



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

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

### Adding a Share

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

Network - Shares							
							[Total 1 Entries] Page 1 of 1
Name	Shared Directory	CIFS	NFS	FTP	Read only	Guest	Visible
test-share1	/Test-1/test-share1	✓	✗	✗	✗	✓	✓

- Click **add**. The **Network - Shares - Add** page is displayed.

**Network - Shares - Add**

Protocols    Set Access    CIFS Attributes    CIFS Hosts    CIFS Admin    NFS Attributes

Name

Shared Directory  **browse**

**Protocol**

CIFS     NFS     FTP

**Attributes**

Read only     Guest     Visible

- Enter a **Name** for the Share.
- Enter the **Shared Directory** location for the Share or click **browse** to browse for a location.
- Tick the relevant **Protocol** box(es). This defines how the Users may access the Share. The AMS can share files via Common Internet File System (**CIFS**), Network File System (**NFS**) and File Transfer Protocol (**FTP**).
- 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 AMS 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.
- Click **next >>**. The **Set Access** tab is displayed.

**Network - Shares - Add**

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

Name

Shared Directory

**Owner and Group**

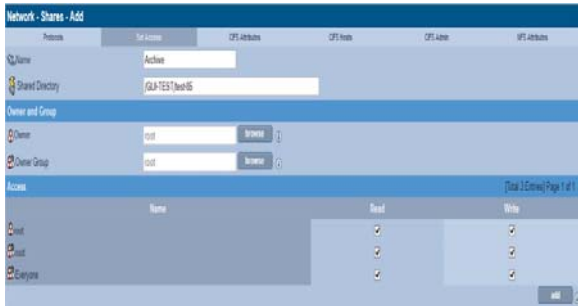
Owner  **browse**

Owner Group  **browse**

**Access**

Account	Share	Read	Write
root	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
guest	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

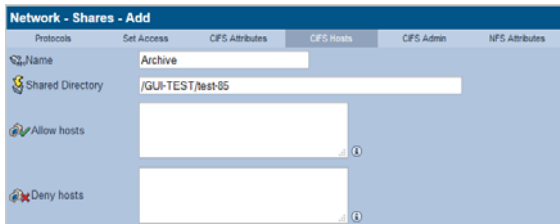
(Next 2 Entries) Page 1 of 1



8. The currently logged in user and group are displayed as the default **Owner** and **Owner Group**. Click **browse** to browse for a specific user.
9. To give specific users access to the share, click **add** and select from the user list (all local, Active Directory, and LDAP users are displayed).
10. Click **next >>**. If CIFS was selected in step 5, the **CIFS Attributes** tab is displayed.



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



- 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.*

- Click **next >>**. The **CIFS Admin** tab is displayed.

Network - Shares - Add

Protocols Set Access CIFS Attributes CIFS Hosts CIFS Admin NFS Attributes

Name Archive

Shared Directory /GUI-TEST/test85

Admin Users [Total 0 Entries] Page 1 of 1

add

- Click **add** to add an Administrator User for this Share. The **next >>** button is only available if NFS was selected in step 5. Clicking it will display the **NFS Attributes** tab.

Network - Shares - Add

Protocols Set Access CIFS Attributes CIFS Hosts CIFS Admin NFS Attributes

Name Archive2

Shared Directory /Test-1/default

Guest Host Access

Enable  Read only  AllowRoot  SyncMode  Insecure

Host Access [Total 0 Entries] Page 1 of 1

Hostname	Read only	AllowRoot	SyncMode	Insecure
add				

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

Network - Shares - Add

Protocols Set Access CIFS Attributes CIFS Hosts CIFS Admin NFS Attributes

Name Archive2

Shared Directory /Test-1/default

Guest Host Access

Enable  Read only  AllowRoot  SyncMode  Insecure

Host Access [Total 0 Entries] Page 1 of 1

Hostname	Read only	AllowRoot	SyncMode	Insecure
add				

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  to continue.

16. Click  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.

The screenshot shows the 'Network - Shares - Update (Protocols)' configuration page. It features three tabs: 'Protocols', 'Access', and 'CIFS'. The 'Protocols' tab is selected. The form contains the following fields and options:

- Name:** kaz2
- Shared Directory:** /kaz2/default
- Protocol:** CIFS (checked), NFS (unchecked), FTP (unchecked)
- Attributes:** Read only (unchecked), Guest (checked), Visible (checked)

At the bottom of the form are three buttons: 'save', 'delete', and 'back'.

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

## Modifying a Share

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

**Network - Shares - Update (Protocols)**

Name

Shared Directory

**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 are made, click **save**.

---

*Note: For in-depth detail on the options available in each tab, see [Adding a Share on page 100](#).*

---

## Authentication

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

### LDAP Configuration

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

The screenshot shows the 'Network - Authentication (LDAP)' configuration page. It features a top navigation bar with 'CIFS' and 'LDAP' tabs, where 'LDAP' is active. The main content area is divided into three sections:

- Network - Authentication (LDAP):** Contains checkboxes for 'Enable LDAP' and 'Enable SSL'. Below are input fields for 'Master Host' and 'Slave Host', each with a 'Port' field. There is also a 'Base Domain Name' field and a 'Password Encryption' dropdown menu set to 'LDAP Server Default'.
- Server Connection:** Contains optional fields for 'Bind Domain Name (Optional)', 'Password (Optional)', and a 'Connection Timeout' dropdown set to '30' seconds.
- Service Privileges:** Contains checkboxes for 'CIFS' and 'FTP'.

3. Tick **Enable LDAP** to enable LDAP authentication.
4. If required, tick **Enable SSL** to enable SSL encryption on the connection to the LDAP server.
5. Enter the **Master Host** hostname (or IP address) and TCP **Port** of the master LDAP server.
6. 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.*

---

7. Enter the **Base Domain Name**. The DN (Domain/Distinguished Name) of the base object from which to start the search.
8. 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).



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

*Note: The user password cannot be set via an anonymous connection.*

- Enter a **Password** (Optional). The password used when binding to the LDAP server with the Bind Domain Name.
- Enter a **Connection Timeout**. Select the LDAP request timeout (in seconds). For details about setting service privileges, refer [Service Privileges](#) on page 107.
- Click  to save the changes or click  to test the connection to the LDAP server.

### Service Privileges

The AMS can be configured to enable CIFS and FTP users to be authenticated against the LDAP directory.

- If required, tick the **CIFS** or **FTP** boxes.
- If **CIFS** is selected, the **CIFS Advanced Configuration** options become available.

The screenshot shows a configuration window with two main sections. The top section, 'Service Privileges', has three checkboxes: 'CIFS' (checked), 'FTP' (unchecked), and 'HTTP (View Only)' (unchecked). The bottom section, 'CIFS Advanced Configuration', has two fields: 'Samba Schema' with a dropdown menu set to 'Ver3.0', and 'Domain SID' with a text input field containing a long alphanumeric string.

- 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 AMS also supports version 2.2 release.
- Enter the **Domain SID**. The Windows Security ID of the LDAP users. The SID defined in the directory is used if it is available.
- 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 AMS.

The Schema files referred in this section can be found on the AMS 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-netscaped5.x** to the `.\iPlanet\servers\slapd-plz\config\schema` directory and rename it to **99user.ldif**
2. Restart the iPlanet service.

### Novell eDirectory

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

#### 1. Import schema definitions

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

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

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

For successful authentication, the POSIX auxiliary classes (posixAccount and posixGroup) are required. However, for

successful CIFS authentication, an additional schema needs to be imported (sambaSamAccount).

Note that sambaSamAccount depends on the POSIX schemas. The [POSIX rfc2307](#) schema definitions are available from Novell and the Samba LDIF file is attached to this document. LDIF and schema files can be imported as follows:

```
ice -SLDIF -f samba.ldif -D LDAP -s <SERVER> -d
cn=admin,o=asti.net -w <PASSWORD>
```

```
ice -SSCH -f rfc2307-usergroup.sch -D LDAP -s
<SERVER> -d cn=admin,o=pdl.net -w <PASSWORD>
```

---

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

---

## 2. Create/Modify POSIX users

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

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

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

---

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

---



---

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

---

## 3. Set/Synchronize passwords

NDS/eDirectory maintains its own passwords and password policy which cannot be shared with Samba. For this reason, it is necessary to maintain a separate password for CIFS authentication. However, the AMS provides an interface to synchronize the Linux/Unix/Samba

password. Simply access the user details "Network - Users - Update" and set the user password.

---

*Note: Novell have been working towards a Universal password scheme and you are advised to consult with Novell regarding password synchronisation and Universal passwords.*

---

### Most Commonly used Samba Schema Attributes

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

**username:uid:LM\_HASH:NT\_HASH:account flags:timestamp**

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

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

- 1 Add the object class `sambaAccount` / `SambaSAMAccount` to the user.
- 2 Set the following attributes:

For Samba Schema 2.2

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

For example, `4097804623`

**lmPassword** - LanManager hashed password

**ntPassword** - Windows NT hashed password

For Samba Schema 3.3

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

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

**sambaLMPassword**

**sambaNTPassword**

### CIFS

The **Network - Authentication (CIFS)** page allows authentication settings for CIFS connections to the Appliance to be defined.

The screenshot shows the 'Network - Authentication (CIFS)' configuration interface. The title bar indicates 'CIFS'. The form contains the following fields and values:

- Workgroup: WORKGROUP
- Domain Name: (empty)
- Organization Unit (Optional): Computers
- Preferred DC (Optional): (empty)
- User Name: (empty)
- Password: (empty)

At the bottom of the form are four buttons: Save, Stop, Diagnose, and Cancel.

1. Enter the **Windows Workgroup** name.

OR

1. Enter the **Domain Name** (this is not the same as the DNS Domain Name) the CIFS service will use.
2. Enter the name of the **Organization Unit** (OU) within the Active Directory tree in which the Appliance will appear. By default, the server will appear within the OU named Computers.
3. If required, enter the IP address or hostname of the **Preferred DC** (Domain Controller).
4. Enter the **User Name** of a Domain user with rights to create an object in Active Directory.
5. Enter the user's **Password**.
6. Re-enter the user's password.

---

*Note: If the Appliance's authentication method is changed or the system software re-installed, the Appliance's user and group lists will be cleared of all imported entries. Entries will need to be re-imported manually.*

---

Domain Type - The system automatically detects and displays the domain type from the connection to the Domain Controller. ADS (Win2K+) and NT Compatible domains are supported.

7. Click **save** to save the changes.
  - Click **start** to start or stop to stop the service.
  - Click **diagnose** to diagnose a connection problem.
  - Click **back** to return to the **System - Services** page.



# *Archive Management Software*

*Chapter 6*  
*Storage Menu*

## RAIDs



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

---

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

---

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

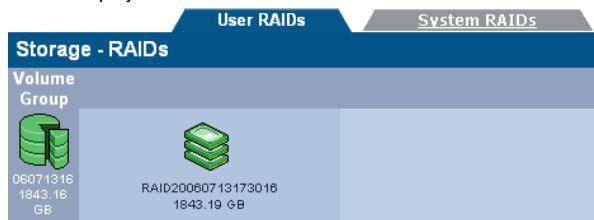
Both solutions provide the same functionality, however, the HardRAID solution offers superior IO performance over the SoftRAID solution. Also, the HardRAID solution includes a BBU (Battery Backup Unit) or a NAND SuperCap backup capability which eliminates the need to rebuild the RAID after a power failure.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

The only way to identify the presence of a RAID controller is to refer to the Devices page ([Storage Devices](#) on page 201). Note the “LSI SAS” controller icon at the left-hand edge of the page.

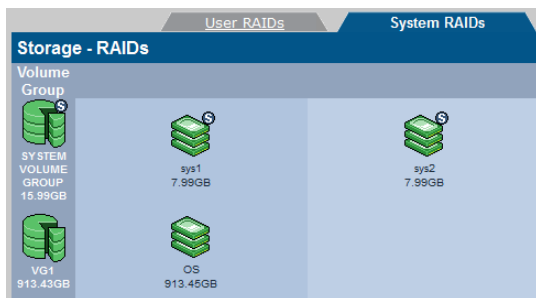


## Viewing RAIDs

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



- Hover over any Volume Group or RAID for a Tool Tip containing status information.
- Click the **System RAIDs** tab to view the list of system RAIDs as follows.

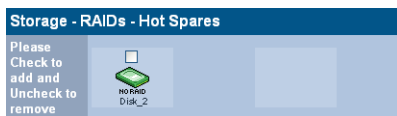


## Assigning Global Hot Spare Disks to a RAID

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

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

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



3. Tick the box(es) of disk(s) to mark as hot spare(s).  
Click **set** to set the hot spare(s).  
Click **save** to save the changes and return to the **Storage - RAIDs** page.

## Adding Storage RAID

In the event that you have had additional drives to the RAID, you will need to add a new RAID group to the RAID.

1. From the menu bar, select **Storage - RAIDs**.
2. Click **add**. The **Storage - RAIDs - Add** page displays.



3. A name is automatically generated, which can be edited in the **Volume Group Name** and **RAID Name** field.

4. Select the **RAID Level** from the drop-down list.
5. Select the chunking size from the **Chunk Size** list.
6. A list of disks available for creating the new RAID are listed. You can remove the default selected disk by clicking the **remove** button.
7. Click **create** to add a new RAID.

You can update the following details of the added Storage RAID:

- **Raid Name** - The name of the RAID.
- **Raid Level** - The level of the RAID (i.e. RAID 1, RAID 5, etc).
- **Status** - The status of the RAID.
- **Size** - The size of the RAID.
- **Device Name** - The device name of the RAID.
- **Number of Disks** - The number of disks the RAID uses.

## Volumes



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

### About Volumes

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

---

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

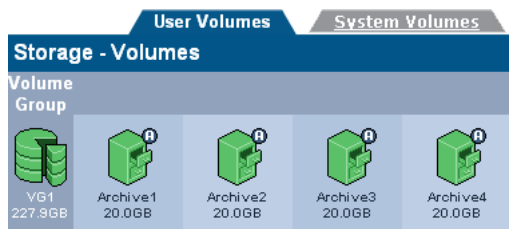
---

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

- An archive - where data is written to the Archive Appliance's RAID(s) and when defined criteria have been met, the data is migrated onto optical media - see [Creating an Archive](#) on page 118.
- An unmanaged volume - where data is written to the Archive Appliance's RAID cache only - see [Creating an Unmanaged Volume](#) on page 129.

### Creating an Archive

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



2. Click **add**.

The **Storage -Volumes - Add Volume** page displays.

Storage - Volumes - Add Volume				
Volume	Archive	Migration Policy	Release Policy	Offline Policy
Volume Name		15092923		
Select Volume Group		VG2		
Space Available		3653.81GB		
Volume Size		2923.05	GB	
Archive	<input checked="" type="checkbox"/>			

3. A **Volume 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 where you want to create the volume from the **Select Volume Group** drop-down list.
5. The **Space Available** is shown. Enter an initial **Volume Size** for the volume.

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

6. If the Volume is to be an archive, tick the **Archive** box.
7. Click **next >>** to continue.

The **Storage -Volumes - Add Volume** page, **Archive** tab opens.

Storage - Volumes - Add Volume				
Volume	Archive	Migration Policy	Release Policy	Offline Policy
Name	16081764			
Archive Options				
	Number of Optical Copies	1		
	Media Type	ODA WO		
	Allow File Changes	Yes		
	Write Commit Period	450	S	
	File Encryption	set		
<< prev		add	next >>	back

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

- Optical Only** All data will be migrated to Optical Media only
- Cloud Only** All data will be migrated to Cloud Storage only
- Optical and Cloud** All data will be migrated to both Optical Media and Cloud Storage

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

---

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

---

9. Select the **Number of Optical Copies** of the file to make. Copies are made on separate optical media and can be offlined to provide an additional level of data protection.
10. Select the **Media Type** the archive will use:
- ODA WO - NETArchive WORM Media
  - UDO WO - Archive Appliance UDO WORM Media
  - UDO CWO - Archive Appliance UDO Compliant WORM Media

11. Select whether to **Allow File Changes**:
  - If **Yes** is selected then changes to the file are permitted at any time after the file is written and multiple versions of the file are stored.
  - If **No** is selected, a WORM file system is created. After the write commit period has expired, no further file changes are permitted.
12. Enter a **Write Commit Period** in **seconds**, **minutes** or **hours**. This sets the time period after the file is closed during which file updates can be made. After this time period has passed, no further changes are permitted.
13. If a cloud account has been successfully configured, the options to enable cloud migration will be available. To enable migrations to the cloud, check the box and select the cloud provider account you wish the archive data to be migrated to.
14. Select the **File Encryption 'set'** button, if files are to be encrypted.

### File Encryption Configuration

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

In the picture above, the masterkey has already been set but the archive key has not. Click the **'generate'** button and it will create a valid and compliant key. Keys cannot be entered manually but must be generated using the **'generate'** button.

Note that in the above example, the keys will be saved to the cloud.

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

*Note: For more details on configuring File Encryption, see Security on page 189.*

15. Click **next >>** to continue.

The **Storage -Volumes - Volume Add** page, **Migration Policy** tab opens.

Storage - Volumes - Add Volume				
Volume	Archive	Migration Policy	Release Policy	Offline Policy
Name	16081764			
Minimum Criteria				
Data must meet <b>all</b> of these criteria in order to be eligible for migration.				
Minimum File Age	10	s		
Minimum Wait Time	20	s		
Minimum Number of Migration Files	1			
Minimum Migration Size	2	MB		
Maximum Criteria				
Data that meets <b>any</b> of these criteria becomes eligible for migration.				
Maximum Wait Time	30	m		
Maximum Number of Migration Files	10000			
Maximum Migration Size	2048	MB		
Open Volume Limit	<input type="checkbox"/>			
<div style="display: flex; justify-content: space-around;"> <span>&lt;&lt; prev</span> <span>add</span> <span>next &gt;&gt;</span> <span>back</span> </div>				

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

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

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



- **Minimum Migration Size** - Migration will NOT be started if the total size is less than the Minimum Migration Size.
17. Enter the following **Maximum Criteria**:
- **Maximum Wait Time** - Migration will be started if the elapsed time since the first file was added to migration candidate list is more than the Maximum Wait Time
  - **Maximum Number of Migration Files** - Migration will be started if there are more than Maximum Number of the Migration Files waiting to be migrated
  - **Maximum Migration Size** - Migration will be started if the total data exceeds the Maximum Migration Size. When setting the maximum migration size, there are considerations to be made.
    - If the archive volume is Optical only, a larger migration package size such as 4GB is preferable. This allows the Optical drive to stream a larger amount of data, facilitating maximum performance.
    - If the archive volume is enabled for cloud archiving, the maximum migration size is limited to 512MB. If a larger value is specified, it will default to the 512MB maximum size.
    - For Cloud only Archive Volumes, a smaller Maximum Migration Size is recommended, such as 50MB or 100MB. A smaller size can be preferable if a higher number of recalls is expected. When a recall is performed on the cloud, the entire migration package may have to be recalled even when only a small portion is required, which extends the recall time and increases cloud download cost.
18. Select whether there should be an **Open Volume Limit**.  
Selecting this option will limit the number of open volumes in a media pool to one. This can result in lower migration throughput as multiple volumes are not opened to utilize all of the available drives, and files from the same directory are less likely to be split across different media.
19. In the event that the media becomes full during a migration task, files may be split between different media cartridges. Setting the **No file splits with max. file size limit** option prevents this.
20. Files listed in the **Exclude** list will not be migrated to media. Click **migration exclusion list** to add or remove files and file types from this list.

## Migration Exclusion List

1. When clicking the “**migration exclusion list**” hyperlink, the following page is displayed.

**Storage - Volumes - Migration Policy Update - Exclusions**

Name  ⓘ

**Exclusion Criteria**

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

Path/File Name		
	/default/exclude_folder	<a href="#">remove</a>
	/default/exclude_folder1	<a href="#">remove</a>
	/default/tester*	<a href="#">remove</a>
	/default/exclude_file1	<a href="#">remove</a>
	/default/file*	<a href="#">remove</a>

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

**Create exclusion list entry**

Path  ⓘ

Name ^	
	..
	tester
	tester1
	tester_2
	SYS_FileGetListDetail...
	exclude_file2
	exclude_file3
	file1.txt
	file_2.txt

1 2 << [2]

3. There are two options available for specifying an exclusion entry. Either select an existing item from the display list.  
or  
Enter the full file/folder path into the top edit control.  
Wildcard entries are permitted e.g. \*.t.db. Click the **add** button and then the **save** button.

---

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

---

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

#### *Archive Configuration Examples*

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

- **EXAMPLE 1** - Migration default settings

With the following minimum settings:

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

and the following maximum settings:

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

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

- **EXAMPLE 2** - Frequent, low data volume

With the following minimum settings:

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

and the following maximum settings:

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

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

- **EXAMPLE 3** - Less frequent, greater data volume

With the following minimum settings:

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

and the following maximum settings:

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

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

*Table 1: Migration policy setting ranges*

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

4. Click  to continue.

The **Storage -Volumes - Volume Add** page, **Release Policy** tab opens.

Volume	Archive	Migration Policy	Release Policy	Offline Policy
<b>Storage - Volumes - Volume Update</b>				
Name	Archive1			
<b>Watermark Policies</b>				
<input type="radio"/> Never release files				
<input checked="" type="radio"/> Start releasing files based on the following				
All files when cache usage is above	95	<input type="text"/>	%	
When cache usage is above	90	<input type="text"/>	%	
Release files larger than	2	<input type="text"/>	KB	
Release migrated files older than	2	<input type="text"/>	h	
Release recalled files older than	24	<input type="text"/>	h	
Stop releasing files when archive usage is	85	<input type="text"/>	%	
Release file immediately after migration	<input checked="" type="checkbox"/>			

Releasing is the process of truncating files on the RAID cache following migration to optical 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.

- 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.
6. Click  to continue.  
The **Storage - Volumes - Volume Add** page, **Offline Policy** tab opens.

*Note: For the AA Express, no Offline Policy tab is made available as there is no library management involved.*

Volume	Archive	Migration Policy	Release Policy	Offline Policy
<b>Storage - Volumes - Volume Update</b>				
Name	<input type="text" value="Archive1"/>			
<b>Offline Policies</b>				
Primary Offline Policy	<input type="text" value="Least Recently Closed"/>			
Secondary1 Offline Policy	<input type="text" value="Open Offline"/>			

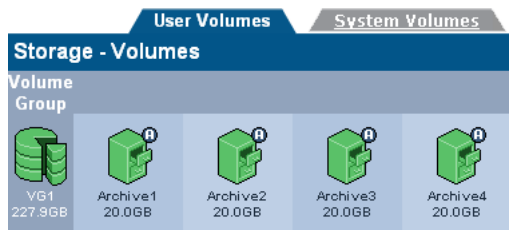
7. Select a **Primary** and **Secondary Offline Policy** from the drop down lists:
- **Least Recently Closed** - Media are offlined in order of last read/write operation. The closed media with the oldest read/write request is offlined first.
  - **Least Recently Used** - Media are offlined in order of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

## Creating an Unmanaged Volume

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

To create a standard volume:

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



- Click **add**.

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

Storage - Volumes - Volume Add		
Name	<input type="text" value="Volume01"/>	
Select Volume Group	<input type="text" value="Pool-01"/>	
Space Available	<input type="text" value="1450.62GB"/>	
Initial Size	<input type="text"/> <input type="text" value="GB"/>	
Archive	<input type="checkbox"/>	

- A **Volume Name** is automatically generated, or can be entered (up to 32 characters; a-z, A-Z, 0-9, - (hyphen e.g. Volume-01) and \_ (underscore for example: Volume\_1).
- Select a Pool where you want to create the volume from the **Select Volume Group** drop-down list. The **Space Available** is shown.

### CAUTION



*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).*

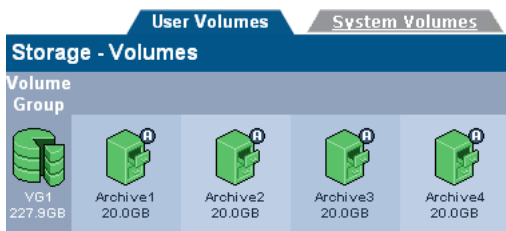
*We recommend that during creation, the volume size is set to the minimum size that is likely to be required.*

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

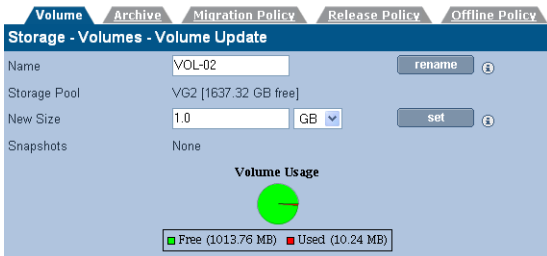
- Click **add**. Once the volume has been created, the AMS will return to the **Storage - Volumes** page.

## Viewing and Editing Volume Properties

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



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



Items that may be edited are:

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



*Note: If a volume is a replica it is strongly recommended to match the size of each replica volume.*

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

**Storage - Volumes - Archive Update**

Name

**Archive Options**

- Number of Optical Copies:
- Media Type:
- Read-only:
- Allow File Changes:
- Cloud enable:
- File Encryption:

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

**Media**

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

Items that may be edited are:

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

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

---

*Note: After a volume is created, the Number of Copies option may only be changed to 1 or 2.*

---

Information-only fields are:

- **Unmigrated Data** - Shows the cumulative size of the files awaiting migration to optical media and/or the cloud. The value in brackets is the number of files awaiting migration. This value includes directories, files and file attribute changes.
- **Available Cache Space** - This value is the summation of the actual free space on the cache (shown on the Volume tab) plus the space currently taken up by releasable files which will be made available when the release watermarks are met (see Release Policy tab).
- **Maximum Available Media Space** - Is the amount of media space available for migration assuming that all available media gets assigned to this archive. If there are multiple archives configured, then in practise this available media space will be smaller.
- **Total Data Archived** - Is the total amount of data from this archive that has been migrated to optical media and/or the cloud. The approximate number of files on the archive is show in brackets.
- **Media** - Totals are for each pool (Primary, Secondary1, Secondary2 as appropriate):
  - **Status**
    - **Enabled** - data will be migrated to media in this pool
    - **Disabled** - data will not be migrated to media in this pool.
    - **Open** - The number of open media in this pool. Open media already have data written to them
    - **Closed** - The number of closed media in this pool. Closed media will have no further data migrated to them
    - **Offline** - The number of offline media from this pool
    - **Available to offline** - The number of media now available to be offlined from this pool. Media can be offlined by using the 'Offline media' option on the keypad.

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

Volume	Archive	Migration Policy	Release Policy	Offline Policy
<b>Storage - Volumes - Migration Policy Update</b>				
Name	Archive1			ⓘ
<b>Minimum Criteria</b>				
To be eligible for migration, data must meet <b>all</b> of these criteria and <b>not</b> be in the <a href="#">migration exclusion list</a> .				
Minimum File Age	10	s	▼	ⓘ
Minimum Wait Time	20	s	▼	ⓘ
Minimum Number of Migration Files	1			ⓘ
Minimum Migration Size	2	MB	▼	ⓘ
<b>Maximum Criteria</b>				
Data that meets <b>any</b> 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	<input type="checkbox"/>			ⓘ
No file splits	<input type="checkbox"/>			ⓘ

Items that may be edited are:

- **Minimum File Age**
- **Minimum Wait Time**
- **Minimum Number of Migration Files**
- **Minimum Migration Size**
- **Maximum Wait Time**
- **Maximum Number of Migration Files**
- **Maximum Migration Size**
- **Open Volume Limit**
- **No file splits**

Read-only fields are:

- **Name**

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

Volume	Archive	Migration Policy	Release Policy	Offline Policy
<b>Storage - Volumes - Volume Update</b>				
Name	Archive1			
<b>Watermark Policies</b>				
<input type="radio"/> Never release files				
<input checked="" type="radio"/> 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	<input checked="" type="checkbox"/>			

Items that may be edited are:

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

Information-only fields are:

- **Name**

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

Volume	Archive	Migration Policy	Release Policy	Offline Policy
<b>Storage - Volumes - Volume Update</b>				
Name	Archive1			
<b>Offline Policies</b>				
Primary Offline Policy	Least Recently Closed			
Secondary1 Offline Policy	Open Offline			

Items that may be edited are:

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

Information-only fields are:

- **Name**

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

## Closing Media

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

Unmigrated Data	Free RAID Space	Free Media Space	Total Data Archived
0B (0)	20GB	3TB	10GB (56)

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

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

The close media process is made up of five steps:

- Make archive read-only
- Check that all files on the RAID have been migrated and that the correct number of copies exist for each file
- Close all open media
- Make the archive writeable again
- Backup the new media state

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

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

**Step 3:** After all the files have been written to optical media, any open media are closed.

**Step 4:** After all media have been closed the archive volume is reverted to writeable.

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

---

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

---

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

---

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

---



---

**Warning: Removing a Volume** The AMS enforces strict rules re-

**WARNING**



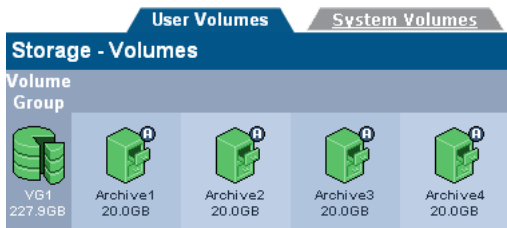
*garding the removal of an archive, as it is a permanent repository of files. These rules affect media management, audit information and system information backup.*

*To clean and successfully remove an archive, please contact the Alliance support team.*

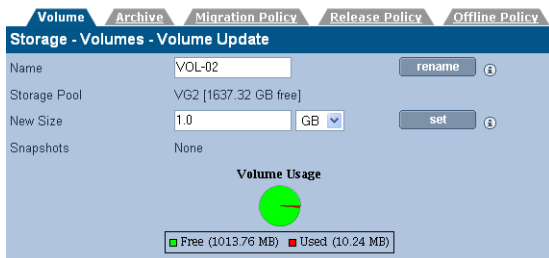
---

To remove a volume:

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



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



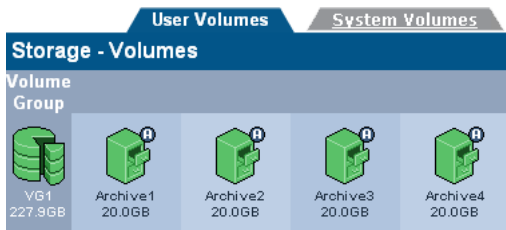
4. Click **remove**. The system will offer a prompt to confirm deletion of the volume.
5. Click **remove** again to confirm or click **cancel** to cancel.

### Diagnosing a Volume

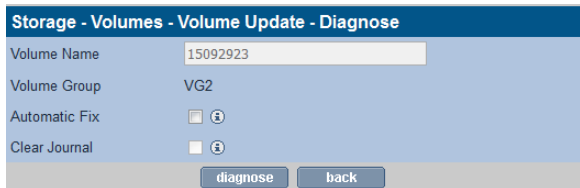
For volumes where file system corruption has been detected, the volume can be diagnosed and the issue possible corrected.

To perform diagnostics on a volume:

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

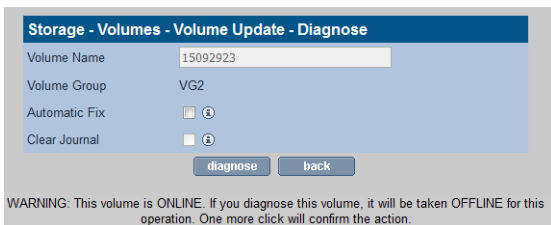


- Click on the volume that is to be diagnosed and click **Diagnose**. The **Volume Update - Diagnose** page opens displaying the Volume Name and Volume Group.
- The diagnostics can be run with or without fixes being automatically applied. To automatically take corrective action when issues are encountered, check the **Automatic Fix** check box.

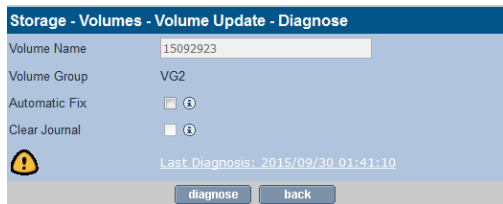


- Check the **Clear Journal** check box to delete the file system journal or logs before you repair the volume. To have the journal or logs, do not tick this option.
- Click **diagnose**. The following warning displays to confirm that if the volume is online, it will be made offline to start the diagnose.





- Click **diagnose** again to continue. An information message displays with the last diagnosis details.



*Note: When Diagnose is run, the volume will be taken offline and then brought back online when completed. For this reason, access by users and applications to the volume will not be available. If the volume is enabled through a fileshare, CIFS or NFS may have to be disabled before the Diagnose can be run.*

- To review the Diagnose results, click on the hyperlink ([Last Diagnosis: <Date> <Timestamp>](#)) to retrieve the Diagnose output.

## Special Consideration for “Bulk migration”

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

### Release After Migration

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

### At least 2 Optical Drives for Writing

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

### Separate Archives for Legacy and Current Files

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

### Large Number of Archives (> 3)

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

### Migration Throughput

Migration performance can vary based on the average file size of data being migrated, especially with the Archive Appliance with UDO drives. For small files (< 50k) the migration performance is between 2-5MB/sec. For large files (> 1MB) the expected migration speed is between 10-15MB/sec.

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

1. RAID is very small (< 40GB free space)
2. Migration is running out of spare media

- 3 Too many library or drive errors
- 4 Files are large (> 500kB)
- 5 < 3 optical drives available for writing

For the Archive Appliance, the average write speed across 3 UDO drives is approximately 12MB/sec.

For the NETArchive, the average write speed across 3 NETArchive optical drives is over 200MB/sec, providing a much faster migration process. So providing a reasonable cache (>100GB) is available for migration, especially with the Archive Appliance, the RIAD cache should never fill.

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

### Migration Configuration Parameters

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

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

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

#### *Minimum Migration Constraints*

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

#### **Minimum File Age (10 seconds)**

Files will age once they are copied onto the archive

#### **Minimum Wait Time (20 seconds)**

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

#### **Minimum Number of Migration Files (1 file)**

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

#### **Minimum Migration Size (2 MB)**

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

*Maximum Migration Constraints*

**Maximum Wait Time (30 minutes)**

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

**Maximum Number of Migration Files (10,000 files)**

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

**Max Migration Size (4608 MB)**

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

## Media

The following section describes the **Storage - Media** page. You can add and remove media, view online and offline media, search media for various attributes, and recall files from a single media.

For details about NETArchive media, see [NETArchive Media](#) on page 10 and for Archive Alliance, see [Ultra Density Optical \(UDO\) Media for the Archive Appliance](#) on page 14.

### Adding Media to the NETArchive

NETArchive media can be added to the NETArchive library using the I/E Tray Door. The I/E Tray Door is used to access the cartridge slots within the library that facilitates adding media cartridges.

If there are no empty slots in the library, then a message is displayed informing you to first remove existing media and then add new media.

To open and close the I/E tray door to add media, use the AMS web interface as follows.

1. From the menu bar, select **Storage - Media**. The **Storage - Media (Online)** page displays.

Storage - Media (Online)	
Slot Usage	Host
Unreadable Barcodes	1
Needs Recovery	2
Empty slots	7
<b>Total slots</b>	<b>10</b>

refresh   cancel   add   remove

2. Click **add** to add media. On clicking **add**, the IE drawer is unlocked.
3. Add the media, close the drawer, and then click **add**.

Online		Offline	Search
<b>Storage - Media (Online)</b>			
<b>Slot Usage</b>			<b>Host</b>
Unreadable Barcodes			1
Needs Recovery			2
Empty slots			7
Total slots			10
<input type="button" value="refresh"/> <input type="button" value="cancel"/> <input type="button" value="add"/> <input type="button" value="remove"/>			
IE drawer unlocked. Please close it after adding media.			

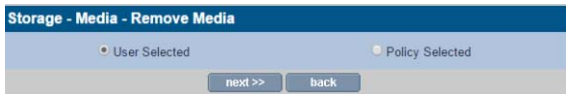
*Note: If no slot is empty, a message displays to first remove the existing media and then add new media.*

## Removing Media from the NETArchive

NETArchive media can be removed from the NETArchive library using the I/E Tray Door. The I/E Tray Door is used to access the cartridge slots within the library that facilitates removing media cartridges.

To open and close the I/E tray door to remove media, use the AMS web interface as follows.

1. From the menu bar, select **Storage - Media**. The **Storage - Media (Online)** page displays.
2. Click **remove** to remove media.

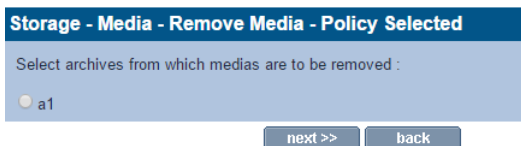


3. Select **User Selection** to remove media that are selected in the **Offline** page. For details, see [Offline Media](#) on page 149.  
OR  
Select **Policy Selected** to remove the media that is set in the **Offline Policy** tab while Creating an Archive. For details, see [page 128](#).
4. Click **next**. A list of media that will be removed are displayed.

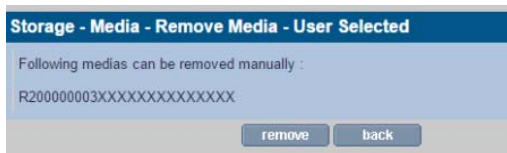
## For User Selected



## For Policy Selected



- Review the listed media names and click **remove** to remove the listed media.



- Click **remove** again to remove the listed media.

## Adding and Removing Media with the AA

With the AA, you can utilize the library keypad to add and remove media to and from the AA library. UDO media can be added to the Archive Appliance via the Mailslot or via Direct slot access.

For details to add or remove media with the AA library, see [Adding UDO Media](#) on page 246 and [Removing UDO Media](#) on page 251.

## Online Media

You can view the slot usage details of the storage media that are online. Also, you can view the detailed inventory page of a particular online media by clicking the particular category hyperlinks on the summary page as follows.

- From the menu bar, select **Storage** and then **Media**. The **Storage - Media (Online)** page displays.

Storage - Media (Online)	
Slot Usage	Host
Unreadable Barcodes	1
Needs Recovery	2
Empty slots	7
<b>Total slots</b>	<b>10</b>

refresh   cancel   add   remove

- Slot Usage** will always display Spare, Open, Closed and Backup media, as well as the Total Slots count. Slot Usage may be one of:
  - Needs Scan** - Media which has been added to the Appliance but has not yet been scanned.
  - Scanning** - Media which is in the process of being scanned.
  - Scan failed** - Media that cannot be scanned by the AMS, indicating a media error.
  - Spare** - Unused and available pieces of media in the spare pool (i.e. not assigned to any archive).
  - Open** - Media assigned to an archive and with data still being written to it.
  - Closed** - Full media. Media that has been closed due to being filled or has been manually closed by the user. Closed media can be taken offline once it has been included in the system backup.
  - Backup** - The number of pieces of backup media in the system. Alliance recommends that two pieces of backup media are kept in the Archive Appliance at all times, where as the NETArchive does not backup to media.
  - Suspected Dirty** - Media with errors that are suspected of being dirty by the system. Media suspected as dirty should be cleaned. To remove dirty media select all affected for



offline and remove from library (*Cleaning Media* on page 251).

- **Has Errors** - If the AMS scans the media and encounters a volume that was unexpected (i.e. media has been manually moved from its original slot within the library or media from another library is introduced into the library) the media will have the **Has Errors**.
  - **Needs recovery** - Media is in this state prior to being re-synchronized during a system recovery.
  - **Failed to initialize** - Media in the library that have failed to initialize. Media in this state does not contain any useful file information and can be safely removed from the library using the keypad interface.
  - **Failed to unlock** - Media in the Archive Appliance which are protected by UDO Guard and cannot be unlocked.
  - **Unreadable barcode** - Media barcode could not be read due to missing/damaged barcode or barcode reader is faulty/misaligned.
  - **Initializing** - Media is being assigned from the spare pool to a partition pool.
  - **Read-only** - A write error has been detected on a medium. Media can only be used for reading and recovery and should be replaced.
  - **In wrong library** - If media has been added to the wrong library when the system is in a "Pool-per-library" configuration mode.
  - **Empty slots** - Slots that are available/empty and can add new media to the library.
  - **Total slots** - The total number of storage slots available in the library.
2. By clicking the category hyperlinks on the summary page, a detailed inventory page for that type of online media is displayed.

Storage - Media List (Online) - Open					
Barcode	Archive	Pool	Location	Usage (%)	Status
A00PC63	Archive1	Primary	31	0	Free
A00W784	Archive2	Primary	57	0	Free
A00WV13	Archive2	Primary	54	5	Open
A00WV17	Archive2	Secondary1	53	0	Free
A00WV38	Archive2	Primary	50 (JDO3)	7	Open
AAAH260	Archive1	Primary	24 (JDO1)	1	Open
AAAH566	Archive2	Secondary1	58 (JDO4)	4	Open
AARE547	Archive2	Secondary1	51	4	Open

Media 1 - 8 of 8 show media:

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

- **Barcode** - The media barcode
- **Archive** - The Archive which the media is assigned to
- **Pool** - The media pool that the media belongs to
- **Library** - Indicates if the media resides in the host or the overflow library (Archive Appliance only)
- **Location** - The slot or drive number where the media is currently located
- **Usage (%)** - The percentage of storage space used on the media
- **Status** - Current status of the media:
  - **Free** - Media is assigned to an Archive but is not being used for migration
  - **Good** - Backup media which is not in use and has no errors.
  - **Needs Scan** - Media has been inserted into the library but has yet to be scanned.
  - **Scanning** - Media is currently being read after being inserted into the library.
  - **Scan Failed** - Media cannot be scanned by the AMS.
  - **Uninitialized** - Media has not yet been initialized or assigned to a spare media pool
  - **Open** - Media is open for writing
  - **Full** - All storage space on the media is used
  - **In use** - Media is currently being used for a migration or recall operation
  - **Read-only** - Media has suffered a read/write failure in two or more drives

- **Not available** - Media identity cannot be verified
- **Dirty** - media requires cleaning (*Cleaning Media* on page 251)
- **Recovery** - Media is marked recovery prior to being re-synchronized during a system recovery
- **Unknown** - Media has not yet been scanned and identified by the AMS (usually following insertion)
- **Duplicated** - Media bears a duplicate barcode sticker to another media in the AMS's inventory.

## Offline Media

The **Storage - Media (Offline)** page allows tracking of media that has been offlined by the system.

1. From the menu bar, select **Storage - Media**.
2. Click the link of the required host and click **Offline**.

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

Barcode	Archive	Pool	Date Ejected
A000P34	Archive2	Secondary1	2009/11/06 14:26:42
A00MG82	none	Backup	2009/10/05 15:29:40
A00N589	Archive2	Primary	2009/11/06 14:27:06
A00OJ20	Archive2	Primary	2009/11/06 14:27:30
A00UY85	Archive2	Secondary1	2009/11/06 14:27:53
A00WT23	none	Backup	2009/10/05 15:30:03
AAAH534	none	Backup	2009/10/05 15:30:30

Media 1 - 7 of 7

refresh cancel

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

## Search Media

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

The screenshot shows the 'Storage - Media (Search)' interface with three tabs: 'Online', 'Offline', and 'Search'. The 'Search' tab is active. The interface is divided into two main sections: 'Media attributes' and 'Media contents'.

**Media attributes:**

- Media Location:** Radio buttons for 'All Media' (selected), 'Online', and 'Offline'.
- Media Status:** Radio buttons for 'All Media' (selected), 'Spare', 'Requires Attention', 'Open', 'Backup', 'Selected for Offline', 'Close', and 'Needs Scan'.
- Archive:** A dropdown menu.
- Date Opened:** Two date input fields with calendar icons and a 'to' separator.
- Date Closed:** Two date input fields with calendar icons and a 'to' separator.
- Barcode:** A text input field.

**Media contents:**

- Containing Files From:** A text input field with a 'browse' button and an information icon.

At the bottom, there are three buttons: 'search', 'reset', and 'cancel'.

**Media Attributes** - criteria associated with media

- **Media Location**
  - **All Media** - media inside (online) and outside (offline) the library.
  - **Offline** - media that have been taken out of the library.
  - **Online** - media that is still in the library.
- **Media Status**
  - **All Media** - do not filter on status.
  - **Spare** - unformatted media not assigned to any media pool.
  - **Requires Attention** - something is wrong with this media e.g. media is dirty and needs to be cleaned (*Cleaning Media* on page 251).
  - **Open** - has files migrated to them.
  - **Backup** - Re-writeable backup media.
  - **Selected for Offline** - this will show media selected for offline, but have not been removed from the library yet.
  - **Close** - media that has been filled and can no longer be written to.

- **Needs Scan** - Media that has not been successfully scanned. Media can always be scanned.
- **Archive** - in the case of multiple archives the media specific to a given archive can be searched.
- **Date Opened** -
  - **From date** - start date of open media date range. Empty from date will mean the "beginning of time".
  - **To date** - end date of open media date range. Empty to date means "today".
- **Date Closed**
  - **From date** - start date of close media date range. Empty "from date" will mean the "beginning of time"
  - **To date** - end date of close media date range. Empty "to date" means "today"
- **Barcode** - enter barcode or wildcard expression of the required barcoded media. For example, "\*a\*" will locate all media which have the letter 'a' in the barcode.
- **Containing Files From** - Search for media containing files which are located below the specified folder.
  - **browse** - this button allows existing (i.e. not deleted) file/folder to be located.

All search criteria can be cleared by clicking the  button.

After the criteria is specified, the search can be started by clicking the  button.

Storage - Media List (Online/Offline) - Open					
Barcode	Archive	Pool	Location	Usage (%)	Status
A00P063	Archive1	Primary	31	0	Free
A00W784	Archive2	Primary	67	0	Free
A00WY13	Archive2	Primary	54	5	Open
A00WV17	Archive2	Secondary1	53	0	Free
A00WV38	Archive2	Primary	50 (UDO3)	7	Open
AAAH280	Archive1	Primary	24 (UDO1)	1	Open
AAAH566	Archive2	Secondary1	58 (UDO4)	4	Open
AAEL347	Archive2	Secondary1	51	4	Open

Media 1 - 8 of 8 show media:

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

- **to close** - show media that are currently open and are available to be closed.
- **to scan** - show all media that can be rescanned.

- **to select for offline** - show all media that are candidates for offline.
- **to deselect for offline** - show all media that have been selected for offline.

After one of the above actions are picked, the relevant media are then available for selection.

Storage - Media List (Online/Offline) - Open						
	Barcode	Archive	Pool	Location	Usage (%)	Status
<input checked="" type="checkbox"/>	A00WV13	Archive2	Primary	54	5	Open
<input checked="" type="checkbox"/>	A00WV38	Archive2	Primary	50 (UD03)	7	Open
<input type="checkbox"/>	AAAH280	Archive1	Primary	24 (UD01)	1	Open
<input type="checkbox"/>	AAAH566	Archive2	Secondary1	58 (UD04)	4	Open
<input type="checkbox"/>	AABE547	Archive2	Secondary1	51	4	Open

Media 1 - 5 of 5 show media: to close

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

---

*Note: Media selected for offline can be removed through the keypad interface for the Archive Appliance (see [How to Offline Closed Media](#) on page 289) or the **Storage - Media** page remove option for the NETArchive (see [Removing Media from the NETArchive](#) on page 144).*

---



---

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

---

## Storage - Media Details

Barcode labels are linked to the **Media Details** page.

1. From the menu page, click **Storage - Media**.

Storage - Media (Online)	
Slot Usage	Host
Open	8
Has Errors	4
Empty slots	15
Total slots	27

refresh cancel add remove

- Click the required host link you want to view. The following page displays.

Storage - Media List (Online) - Open					
Barcode	Archive	Pool	Location	Usage (%)	Status
10000019	test3	Secondary1	3	39.9	Open
1000001A	test3	Secondary2	4	39.9	Open
1000001B	test2	Primary	5	39.9	Open
10000021	test2	Secondary2	27	39.8	Open
10000022	test1	Secondary1	10	35.9	Open
1000002B	test2	Secondary1	6	40.0	Open
419RE10028	test1	Secondary2	11 (ODS1)	34.3	In Use
419RE10033	test1	Primary	12 (ODS2)	33.9	In Use

Media 1 - 8 of 8 show media: all media

refresh back

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

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

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

The **Media Details** page also provides the interface for extracting a file inventory for that media (for Archive Appliance, side A and B).

Storage - Media Details			
<b>Media Details</b>			
Barcode	10000019	Archive	test3
Location	Online	Pool Name	Secondary1
Date Opened	2016/09/28	Date Closed	N/A
Usage	39.9%	Status	Open
<b>Files On The Media</b>			
To create a list of files from the media index please click 'create list'.			
Index last updated at 2016/09/29 02:03:39. To update the index click 'update'.			
<a href="#">create list</a>		<a href="#">update</a>	
<b>Recall Files From The Media</b>			
To start recalling from the current loaded media please click 'start'.			
<a href="#">start</a>			
<a href="#">back</a>			

By clicking **create list**, the media inventory list will be generated and prepared for download. After the media list is available for download, a hyperlink will appear:

Index last updated at 2009/11/09 02:11:54. To update the index click 'update'.
<a href="#">create list</a> <a href="#">update</a>
The list of files on the media has been created, click <a href="#">here</a> to download

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

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

---

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

---



Following is a sample media inventory file:

File Path	File ID	File Size	Migration ID	Migration Time	Status
default/New OpenDocument Text.odt	5034659	7334	322014007552	10/11/2009 15:33	complete
default/New Text Document.txt	5034660	0	322014168064	10/11/2009 15:44	complete

## Recall All Files from a Single Media (or single media side)

You can return all the files of a specific medium to the RAID cache using the recall interface on the **Media Details** page.

*Note: NETArchive media is single sided. Side selection is therefore ignored.*

**Storage - Media Details**

**Media Details**

Barcode	1000019	Archive	test3
Location	Online	Pool Name	Secondary1
Date Opened	2016/09/28	Date Closed	N/A
Usage	39.9%	Status	Open

**Files On The Media**

To create a list of files from the media index please click 'create list'.  
Index last updated at 2016/09/29 02:03:39. To update the index click 'update'.

**Recall Files From The Media**

To start recalling from the current loaded media please click 'start'.

### Media Details for NETArchive System

For Archive Appliance, the media side(s) to be recalled can be selected.

Storage - Media Details			
<b>Media Details</b>			
<b>Barcode</b>	AAGB872	<b>Archive</b>	Archive1
<b>Location</b>	Online	<b>Pool Name</b>	Primary
<b>Date Opened</b>	2011/12/03	<b>Date Closed</b>	2011/12/13
<b>Usage</b>	100%	<b>Status</b>	Closed
<b>Files On The Media</b>			
To create a list of files from the media index please click 'create list'.			
<input type="button" value="create list"/>			
<b>Recall Files From The Media</b>			
Side A <input checked="" type="checkbox"/> Side B <input type="checkbox"/>			
<input type="button" value="start"/>			
<input type="button" value="back"/>			

## Media Details for Archive Appliance

After the side(s) are selected, the recall is started by clicking the **start** button. When the recall is completed, following message is displayed.

Recall Files From The Media	
Side A <input checked="" type="checkbox"/> Side B <input type="checkbox"/>	
<input type="button" value="start"/>	
<input type="button" value="back"/>	
Recalling - Side A: completed at 2012/01/31 10:50:48	

**WARNING**

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

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

Storage - Media Requests					
		Archive	Pool	Media Barcodes	Last Requested
1	<b>Preferred:</b>	06102538	Primary	AAAAAG08	Thu Oct 26 11:07:53 BST 2006
	<b>Alternative:</b>	06102538	Secondary1	AAAAAU05	
2	<b>Preferred:</b>	06102538	Primary	AAAAAG08	Thu Oct 26 11:07:53 BST 2006

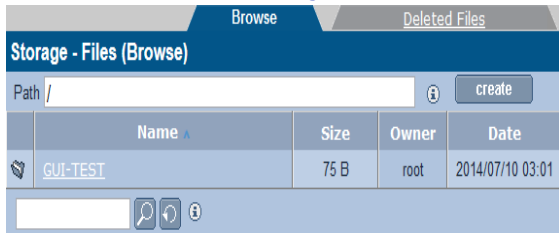
- **Preferred** and/or **Alternative** - indicates the preferred copy to be returned and if that is not available, an alternative copy.
- **Archive** - The archive the media is part of
- **Pool** - The pool (within the archive) which the media is part of
- **Media Barcode** - The barcode of the offline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

## Files

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

### Browsing Files

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



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

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

3. Click to clear the content of the text box.

Alternatively, manually browse the directory tree for a file.

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

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

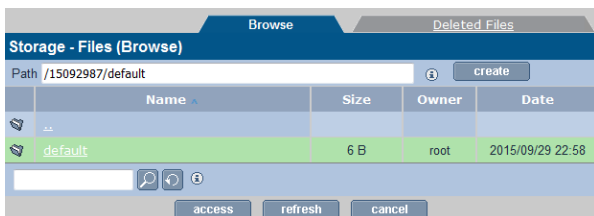
### Displaying File/Folder Details

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

## General

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

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



- Select the required path and click **access**.
- Click **General**. The following screen displays.

**File Details**

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

**Generation Details**

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

Display: all generation types

### File Details

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

- File status** - Access status of file: Online/Offline/Nearline/Dirty/Excluded status.
  - Online** - File is on the RAID given fast read performance
  - Offline** - Media of file has been removed from library
  - Nearline** - File is not on RAID but is located on media which is still in the library

- **Dirty** - File has not been migrated yet. Not to be confused with physical dirty/dust.
- **Excluded** - File or parent folder has been explicitly excluded via migration exclusion list.
- **Archive** - Name of archive this file/folder is stored in.
- **Generations** - Number of modifications. The first generation is the initial file create. A generation may not always be a file content change but could be a meta-data modification (for example: rename or permission change).
- **Size** - Size of the data
- **Modification Date** - Last time this file was modified.
- **Last Migration Type** - Last migration type: *metadata* or *data*. Metadata changes include file rename and ACL changes.

#### Generation Details

Each file system modification migrated to optical media is recorded in the Generation Details table.

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

#### Setting or Modifying an ACL

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

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

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

**Storage - Files (Browse)**

Path: /Archive1/default

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

Buttons: access, refresh, cancel

2. Search or browse to a folder or file.

Click on **access**.

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

**Storage - Browse - Access (Access)**

Location: /GUI-TEST

Owner: root

Group: root

ACL [Total 3 Entries] Page 1 of 1

Name	Read	Write	Make Inheritable
root (Owner)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
root (Group)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: add, browse

From this page:

- View the current **Location**.  
Click  to browse to another directory.
  - View the folder's **Owner** and **Owner Group**.  
Click  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  to add more users or groups.

### File/Folder Attributes

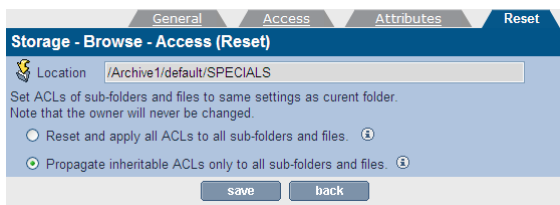
The file/folder attributes include: full path, owner and owner group of file system object, option of allow/disallow propagation of ACLs from parent folder and DOS file system attributes.

1. Click the **Attributes** tab.

From this tab:

- **Allow propagation of inheritable ACL changes (from ancestor)** - This can be used to pass access privileges from the current directory to its sub-directories. In this way, a single ACL can be placed high up in the directory tree to control access.
2. Click the **Reset** tab (applicable for folders only).





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

- **Reset and apply all ACLs to all sub-folders and files** - This option will reset and then apply the current folder's access properties to all sub-folders and files
- **Propagate inheritable ACLs only to all sub-folders and files** - This option will apply the current folder's access properties, which are marked as Propagate Inheritable, to all sub-folders and files. It will NOT reset existing ACLs.

---

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

---

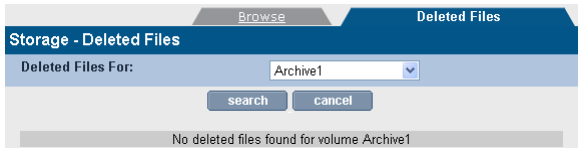
When the ACLs are satisfactorily set, click **save** to save the changes.

## Searching Files

The only criteria for searching files is currently the deleted status. A selected archive can be searched to produce a downloadable file containing all deleted files.

After the **search** button is clicked, a progress bar appears to indicate the status of the search.

The user may want to return to the interface at a later date to download the result, as the search may take some time. The duration of the search will depend on the number of files in the File System Catalog (FSC).



After the search has completed, the search results file is available for download.

# *Archive Management Software*

## *Chapter 7*

### *Data Protection Menu*

## Data Protection

*Note: Data protection in this context refers to the protection of AMS system and configuration data. It does not refer to the protection of user data files which are inherently protected by migration to optical media.*

### Backup

Backups significantly increase the speed of a data recovery in the event that the system fails. System and configuration data should be backed up on a regular basis. This enables closed media to be offlined as well as restoring the system in a much shorter time frame should the RAID be lost due to hardware issues.

- With the NETArchive, backups are written to the SSD devices and to the network based location.
- With the Archive Appliance, the backups are either written to RW UDO media stored in the Archive Appliance or to the network based backup location.

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

### Creating a Backup Schedule

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

The screenshot shows the configuration interface for backup schedules. It features a dark blue header with 'Status' and 'Configuration' tabs. The main content area is titled 'Data Protection - Backup (Configuration)'. Underneath, there's a 'Schedule' section. The 'Time' field is set to 02 hours and 00 minutes. The 'Backup Target' section has two options: 'SSD' (checked) and 'NETWORK (Required)' (unchecked). At the bottom, there are 'save' and 'cancel' buttons.

- Select a time using the drop-down boxes. The backup will take place at this time every day.
- Select backup location(s).
  - For NETArchive, by default the backup is placed on the SSD. For added security, it is highly recommended that the **NETWORK** location is selected for backup as well. For more details, see *Network Backup using CIFS* on page 167 and *Network Backup using NFS* on page 168.
  - For the Archive Appliance, select either the UDO RW Media or NETWORK as your backup location. If the selection is UDO RW media, ensure that UDO RW Media is in the library (two pieces recommended).

---

*Note: The AMS is capable of backing up across either CIFS or NFS. Select the radio button appropriate to the protocol that is to be used.*

---

#### Network Backup using CIFS

- Click the **CIFS** radio button if the remote location is a Windows Share or a network device configured to appear as a Windows Share (for example: a Linux server using Samba). The **CIFS Configuration** page displays.

Status      Configuration

**Data Protection - Backup (Configuration)**

**Schedule**

Time	02 ▾ Hour(s)	00 ▾ Minute(s) ⓘ	
Backup Target	<input checked="" type="checkbox"/> SSD <input checked="" type="checkbox"/> NETWORK (Required) ⓘ		
Network Protocol	<input type="radio"/> CIFS <input type="radio"/> NFS		
Host	<input type="text"/>		ⓘ
Share	<input type="text"/>		ⓘ
Backup Directory	<input type="text"/>		ⓘ
Domain	<input type="text"/>		ⓘ
User Name	<input type="text"/>		ⓘ
Password	<input type="password"/>		ⓘ

2. 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 AMS across the network, and which has been configured to accept the connection (such as setting up a share, creating a user for the AMS to connect as, and configuring the correct permissions).  
The hostname may be the Fully Qualified Domain Name, or simply the hostname if the remote host is in the same Domain as the AMS.
3. Enter the name of the **Share** to which the backup is to be written.
4. Supply the **Backup Directory** within the Share. When using multiple system, each system should be assigned a dedicated backup directory to ensure that backup files from one systems are not overwritten by the backup files of another.
5. If the authenticated user is a domain user, the fully qualified domain name needs to be specified (for example: eng.asti-usa.com).
6. Provide a **User Name** with Read, Write, Delete and Rename permissions. This should be a user local to the server hosting the share, not to the AMS.

---

*Note: Usernames should be entered in the format <domain-name>/<username> for example: UK/phill*

---

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

#### *Network Backup using NFS*

1. Click the **NFS** radio button if the remote location is a NFS share, such as a Novell server. The NFS configuration page displays.

**Data Protection - Backup (Configuration)**

**Schedule**

Time: 02 Hour(s) 00 Minute(s)

Backup Target:  SSD  NETWORK (Required)

Network Protocol:  CIFS  NFS

Host:

Backup Directory:

Buttons: save, cancel, connect

- 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 AMS across the network, and which has been configured to accept the connection (such as setting up a share, creating a user for the AMS 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.*

- Provide the path to the **Backup Directory**. When using multiple AMS, each AMS should be assigned a dedicated backup directory to ensure that backup files from one Appliance are not overwritten by the backup files of another.

*Note: Please ensure that you do not provide the Backup Directory path starting with a "/" (slash).*

- Click the **connect** button to ensure the supplied details are correct.
- Click **save**.

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

## Monitor the Backups

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

Status		Configuration
<b>Data Protection - Backup (Status)</b>		
<b>Current Status</b>		
System is backed up.		
<b>Last Successful Backup</b>		
Started	2017/04/20 02:00:19	
Completed	2017/04/20 02:00:45	
Backup Target	NETWORK	
Backup Directory	//10.2.3.230/aabackup2//backup193	
Backup Method	Incremental	
Backup Summary	Successfully copied backup to Primary SSD	
<b>Next Scheduled Backup</b>		
Start Date and Time	2017/04/21 02:00:00	
Backup Target	NETWORK	
Backup Directory	//10.2.3.230/aabackup2//backup193	
<input type="button" value="start"/>		<input type="button" value="cancel"/>

- The following information is displayed:
  - Current Status** - The backup status of the AMS. 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/ SSD and/or Network) and information relevant to the target (Barcode for UDO media, SSD and/or remote target for Network backups, Incremental or Full backup).
  - Next Scheduled Backup** - The date, time and target for the next scheduled backup. This section also displays the number of backup media available.

---

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

---



When the Cloud Quota is full, following message displays:



*Note: After the cloud quota reaches 100%, the backup activity continues but migration tasks stops until free space is made available.*

### Perform an Unscheduled Backup

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

### File Recovery

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

**WARNING**



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

**Data Protection - File Recovery**

**What do you want to recover?**

Full system from backup ⓘ

Full system from media ⓘ

recover
cancel

If Cloud storage was previously used, the `cloud_provider(s)` must be configured first.

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

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

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

---

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

---

If the system already has archives, the AMS offers following recovery options:

### Data Protection - File Recovery

#### What do you want to recover?

- Full from backup ⓘ
- Single Archive FSC only ⓘ
- Single Archive FS only ⓘ
- RMDB only ⓘ

recover

cancel

If Cloud storage was previously used, the [cloud provider\(s\)](#) must be configured first.

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

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

The different recovery processes are described in detail below.

#### Full from Backup

**WARNING**



*Warning: This option will delete UNMIGRATED data and leave all files in the offline state. Check for unmigrated data in the Storage - Volumes page for each archive - see [Viewing and Editing Volume Properties](#) on page 130.*

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

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

The steps that the system performs are:

- Restore databases and system settings from the backup
- Re-synchronize the FSC database to reflect changes on media since the backup was made
- Delete existing file systems then rebuild them using the re-synchronised FSC. Note: this deletes unmigrated data and leaves all files on each file system in the offline state.

Following is the procedure to perform recovery from full backup.

### Perform file recovery from SSD

1. From the menu bar, select **Data Protection - File Recovery**. The **Data Protection - File Recovery** page displays.

**Data Protection - File Recovery**

**What do you want to recover?**

- Full from backup ⓘ
- Single Archive FSC only ⓘ
- Single Archive FS only ⓘ
- RMDB only ⓘ

If Cloud storage was previously used, the [cloud provider\(s\)](#) must be configured first.

- Click **recover**. Select the location from where you want to backup.

**Data Protection - File Recovery**

Backup Location  SSD  NETWORK ⓘ

recover
cancel

Please provide details of the location of your most recent backup  
 SSM problem (please see ssm.log and error.log)

- Select **SSD**.  
For backup from Network location, the following page displays.

**Data Protection - File Recovery**

Backup Location  SSD  NETWORK ⓘ  
 Network Protocol  CIFS  NFS  
 Host  ⓘ  
 Share  ⓘ  
 Backup Directory  ⓘ  
 Domain .com ⓘ  
 User Name  ⓘ  
 Password  ⓘ

recover
cancel

Please provide details of the location of your most recent backup

- Click **recover**. The **File Recovery** progress displays.

**Data Protection - File Recovery**

Restore	PREPARING
Resync	NOT STARTED
Rebuild file systems	NOT STARTED

*Note: If you have any unmigrated data on any of the archives, then a warning displays. The data will be lost if you continue the recovery.*

**Data Protection - File Recovery**

**Warning**

Unmigrated data exists on the following archive(s):

Enc	mounted on /exports/Enc
16082987	mounted on /exports/16082987
16082910	mounted on /exports/16082910

This data will be lost if you proceed with the recovery

recover cancel

5. The recovery will begin immediately.

To recover from Network

### Perform file recovery from SSD

- From the menu bar, select **Data Protection - File Recovery**. The **Data Protection - File Recovery** page displays.

**Data Protection - File Recovery**

What do you want to recover?

- Full from backup ⓘ
- Single Archive FSC only ⓘ
- Single Archive FS only ⓘ
- RMDB only ⓘ

recover cancel

If Cloud storage was previously used, the [cloud provider\(s\)](#) must be configured first.

- Click **recover**. Select the location from where you want to backup.

**Data Protection - File Recovery**

Backup Location  SSD  NETWORK ⓘ

recover cancel

Please provide details of the location of your most recent backup SSM problem (please see ssm.log and error.log)

3. Select **Network**. The following page displays.

**Data Protection - File Recovery**

Backup Location	<input type="radio"/> SSD <input checked="" type="radio"/> NETWORK ⓘ
Network Protocol	<input checked="" type="radio"/> CIFS <input type="radio"/> NFS
Host	<input type="text" value=""/> ⓘ
Share	<input type="text" value="backup"/> ⓘ
Backup Directory	<input type="text" value="tmp-227"/> ⓘ
Domain	<input type="text" value=""/> .com ⓘ
User Name	<input type="text" value=""/> ⓘ
Password	<input type="password" value="*****"/> ⓘ

Please provide details of the location of your most recent backup

4. Select the **CIFS** option if the network location is a Windows Share, or a device advertising itself as such (for example: a Linux server using Samba).
- Host - The hostname, Fully Qualified Domain Name or IP address of the remote server.
  - Share - The share name on the remote host.
  - Backup Directory - The full path to the directory in which the backup is located. If the backup is on the root of the share, then the path is / (forward slash).
  - Domain - Provide the domain name.
  - User Name - This must be a user specified on the remote server which has write access to the backup location.
  - Password - That user's password.

Else,

Select **NFS** option if the network location is an NFS share (for example: a Novell server).


- Host - The hostname or Fully Qualified Domain Name of the remote server.
- Path - The full path to the directory in which the backup is located.

5. Click **recover**. The **File Recovery** progress displays.

Data Protection - File Recovery	
Restore	PREPARING
Resync	NOT STARTED
Rebuild file systems	NOT STARTED

*Note: If you have any unmigrated data on any of the archives, then a warning displays. The data will be lost if you continue the recovery.*

**Data Protection - File Recovery**

 **Warning**

Unmigrated data exists on the following archive(s):

Enc	mounted on /exports/Enc
16082987	mounted on /exports/16082987
16082910	mounted on /exports/16082910

This data will be lost if you proceed with the recovery

6. The recovery will begin immediately.

### Full System from Media



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

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

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

---

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

---

In addition, following a recovery from media it is necessary to reconfigure the list of local users on the AMS (see [page 93](#)).

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

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

### Single Archive FSC only

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

- Restore archive's FSC from backup or media
- If restored from backup, re-synchronize the archive's FSC database to reflect changes on media since the backup was made

---

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

---

### Perform file recovery from single archive FSC

1. From the menu bar, select **Data Protection - File Recovery**. The **Data Protection - File Recovery** page displays.



**Data Protection - File Recovery**

What do you want to recover?

- Full from backup ⓘ
- Single Archive FSC only ⓘ
- Single Archive FS only ⓘ
- RMDB only ⓘ

If Cloud storage was previously used, the [cloud provider\(s\)](#) must be configured first.

- Select **Single Archive FSC only**. A list of archives available are displayed.

**Data Protection - File Recovery**

Which archive do you want to recover?

- Enc
- a1
- 16082987
- 16082910

- Select the archive you want to recover and click **recover**.

### Single Archive FS only

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

#### WARNING



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

---

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

---

---

*Warning:* You must disable all CIFS/NFS/FTP/Replication services before attempting recovery.

---

### RMDB only

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

#### WARNING



---

*Warning:* You must disable all CIFS/NFS/FTP/Replication services before attempting recovery.

---

---

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

---

### Key Recovery

Key recovery may be required if the keystore has been corrupted as a result of a power failure or some other system failure. The Key Management system has been designed to detect and automatically

repair many corruption scenarios. Key recovery is the last fall back recovery method.

Data Protection - Key Recovery		All Archives ▼
<b>Key store Status</b>		
<b>Configuration</b>		
Protection Mode	Not set	
Master Key	Key not set	
Archive Key(s)	No archive encryption configured	
<b>Key restore from backup</b>		
Progress	Not running.	
start		cancel

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

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

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

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

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

---

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

---

## Replication

The **Data Protection - Replication** page enables configuration of replication services between two AMS systems, via TCP/IP. The AMS Systems can be any combination of Archive Appliance or NETArchive systems. The AMS supports and facilitates replication between disparate technologies.

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

For information on creating volumes, see [Creating an Archive](#) on page 118.

Ensure that the target AMS system has a user with Replication rights. See [Adding a User](#) on page 93.

---

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

---

---

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

---

### Configuring Replication

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

---

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

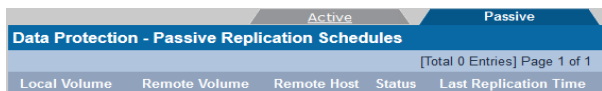
---

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

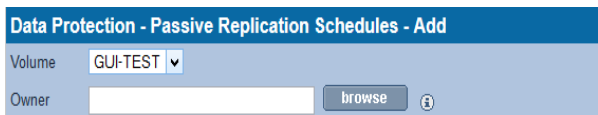
The Active schedule resides on the AMS system that holds the source volume, and the Passive schedule resides on the AMS system containing the target volume.

### Creating a Passive Schedule

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



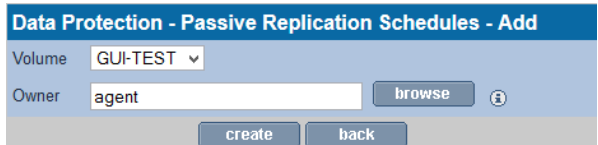
2. Click **add** to open the **Data Protection - Passive Replication Schedules - Add** page.



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



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



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

- 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 an Active Schedule

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

Active		Passive	
<b>Data Protection - Active Replication Schedules</b>			
[Total 0 Entries] Page 1 of 1			
Local Volume	Remote Volume	Remote Host	Last Job Logs

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

<b>Data Protection - Active Replication Schedules - Add</b>	
Volume	Test-1 <input type="button" value="v"/>
<b>Passive System Options</b>	
Passive Host	<input type="text"/> <input type="button" value="i"/>
User Name	admin <input type="button" value="i"/>
Password	••••• <input type="button" value="connect"/> <input type="button" value="i"/>
Passive Volume	<input type="button" value="v"/> <input type="button" value="i"/>
<b>Daily Schedule</b>	
Start Time	2 : 00 <input type="button" value="v"/>

- Select the source volume from the **Volume** drop-down box.
- Enter the IP address or the Hostname of the target AMS system in the **Passive Host** field.
- Enter the user name and password for the replication selected in Step 4 on [page 183](#).
- Click **connect**.
- Select the **Passive Archive** from the drop-down box (that needs to be configured prior to this procedure).
- Set a **Start Time** using the drop-down boxes.
- Click **add**.
- Go to the **System - Services** page and **enable** the Replication service.

## Modifying Replication Details

1. On the source AMS system, open the **Data Protection - Replication** page.
2. Click on the Active Replication schedule to be modified.

Data Protection - Active Replication Schedule - Update	
Volume	<input type="text" value="Archive2"/>
<b>Passive System Options</b>	
Passive Host	<input type="text"/>
Passive Volume	<input type="text" value="Archive1"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password"/>
<b>Daily Schedule</b>	
Start Time	9 : 15
<input type="button" value="delete"/> <input type="button" value="replicate now"/> <input type="button" value="save"/> <input type="button" value="back"/>	

3. Modify details as required.

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

4. Click **save**.

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

*Note: After the ‘replicate now’ button is selected, the option to perform a full file system scan will be given. For file system with many files (> 10 million) this may take a long time.*

## Making the Passive Replica Active

If in the unlikely event the active (primary) AMS system should fail and not be recoverable in an acceptable time frame, it is possible to switch the passive replica into the active (writeable) state.

1. Select the “**Passive**” tab and the relevant passive replication schedule.

Data Protection - Passive Replication Schedule - Information	
Volume	Archive1 ⓘ
Owner	admin ⓘ
Remote Volume	Archive2 ⓘ
Remote Host	TESTER-420 ⓘ
Last Replication Time	2012/01/25 09:19:37 ⓘ
Status	Finished ⓘ

2. Click the “**make active**” button and click to confirm the action. The system will now proceed to activate the passive archive and changing it from read-only to writeable.

Data Protection - Passive Replication Schedule - Information	
Volume	Archive1 ⓘ
Owner	admin ⓘ
Remote Volume	Archive2 ⓘ
Remote Host	TESTER-420 ⓘ
Last Replication Time	2012/01/25 09:19:37 ⓘ
Status	Finished ⓘ

Passive replica is pending to become active.



---

*Note: Note how the “make active” button changes to “stay passive” allowing the user to reverse the action. The success of the action is also confirmed and the replica is “pending active”.*

---

3. The replica is writeable and after the failed replica returns, the pending active replica will attempt to synchronize any outstanding files that may have been written before the failure.
4. After this is completed, the “**pending active**” state will change to “**active**”.

### Deleting an Active Replication Schedule

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

### Deleting a Passive Replication Schedule

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

---

*Note: Deleting a replication schedule does not delete the archive. For further information on deleting archives, see [Removing a Volume](#). The AMS enforces strict rules regarding the removal of an archive, as it is a permanent repository of files. These rules affect media management, audit information and system information backup. To clean and successfully remove an archive, please contact the Alliance support team. on page 136.*

---

### Viewing Replication Logs

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

1. On the source AMS system, 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		Active	Passive	
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	<a href="#">View</a>
Sun Oct 7 08:30:01 2007	Sun Oct 7 08:30:11 2007	178433	Finished	<a href="#">View</a>
Sat Oct 6 08:30:01 2007	Sat Oct 6 08:51:58 2007	134690180	Finished	<a href="#">View</a>
Fri Oct 5 08:30:01 2007	Fri Oct 5 08:30:09 2007	168719	Finished	<a href="#">View</a>
Thu Oct 4 08:30:01 2007	Thu Oct 4 08:50:43 2007	134680466	Finished	<a href="#">View</a>
Wed Oct 3 13:00:01 2007	Wed Oct 3 13:20:15 2007	134670752	Finished	<a href="#">View</a>

**Start Time** indicates the time the replication began.

**Finish Time** indicates the time the replication ended.

**Data Transferred** is in bytes.

**Status** indicates the overall status of each replication attempt.

This will be one of:

- **Running** - A replication is currently in progress.
- **Failed** - The last replication failed (for example: 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)		Active	Passive
Schedule Name	Target		
Wed Sep 26 13:10:00 2007:Job Target:Starting Replicate job. Mirror host = cobra.sit.pcs, account = admin, mirror path = replication/Agfa_Tar.			
Wed Sep 26 13:10:08 2007:Job Target:Running Replicate job. Mirror ip = cobra.sit.pcs, account = admin, mirror path = replication/Agfa_Tar.			
Wed Sep 26 13:10:10 2007:Job Target:sent 33358 bytes received 26 bytes 13353.60 bytes/sec			
Wed Sep 26 13:10:12 2007:Job Target:sent 33150 bytes received 32 bytes 22121.33 bytes/sec			
Wed Sep 26 14:02:59 2007:Job Target:sent 102508831 bytes received 10134 bytes 32376.11 bytes/sec			
Wed Sep 26 18:13:09 2007:Job Target:sent 448376025 bytes received 44098 bytes 29875.75 bytes/sec			
Wed Sep 26 19:03:29 2007:Job Target:sent 89710905 bytes received 8826 bytes 29723.28 bytes/sec			
Wed Sep 26 19:03:29 2007:Job Target:Replicate job finished.Data transferred 640662269 bytes.			
Wed Sep 26 19:03:31 2007:Job Target:Replicate job end finished.			

## Security

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

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

All security keys are managed through this security interface.

### Encryption

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

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

The **Encryption** tab contains three security parameters:

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

Encryption

**Data Protection - Security**

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

**Master Encryption Wrapping Key**

Master key  generate ⓘ

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

**File Encryption Key Protection Mode**

No protection
  Protect to share
  Protect to cloud

**Archive Encryption Wrapping Key(s)**

Enable	Archive Name	Key
<input type="checkbox"/>		

save
cancel

### Creating a Master Key

1. From the menu, click **Data Protection -Security**.
2. Compliant and valid keys must be created using the **generate** button.
3. After a key is created, you should "**save**" the key. Click the **save** button.
4. You will be presented with a file save dialog, where you should save the key to a secure location to avoid any transcription errors.

#### WARNING



*In the event of a DR, you may be required to re-enter this key. If you do not save this key, or do not have it available, you will NOT BE ABLE TO ACCESS ANY ENCRYPTED DATA THAT HAS BEEN WRITTEN TO THE AMS. IT IS ABSOLUTELY IMPARATIVE THAT YOU SAVE THIS KEY. IT IS RECOMMENDED THAT YOU KEEP AN*

ELECTRONIC COPY AND A PAPER COPY IN SAFE LOCATIONS THAT ARE RESILIENT IN NATURE.

**WARNING**



---

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

---

- 5 Confirm the key after setting it. The key is now set.

### Setting the Protection Mode

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

1. **No protection** – keys are not protected.
2. **Protect to share** – keys written to the FSC backup location network share.
3. **Protect to cloud** – keys written to the key cloud provider account (refer to *You must create a masterkey prior to configuring the cloud provider account details. For more details, refer Creating a Master Key on page 190 section. Configuring Cloud Service on page 82*).

---

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

---

### Creating Archive Key(s)

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

**WARNING**


---

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

---

- 4 Confirm the key after setting it. The key is now set.
- 5 To enable encryption for that archive, click the **enable** box to the left of the archive name.

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

---

*Important: Make sure your keys are secured and protected!*

---

## UDO Guard (Archive Appliance only)

The **Data Protection -Security UDO Guard** tab will be available if this is an Archive Appliance or an Archive Appliance Express. This 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.

After the key is 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. After the 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



*Warning:* After the keys are defined, the 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** check box. This displays the UDO Guard options.

Data Protection - UDO Guard			
Enable UDO Guard <input checked="" type="checkbox"/> ⓘ			
Administrator Key			
Key	<input type="text"/>	*	Confirm Key <input type="text"/>
* ⓘ			
<b>Note:</b> 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
<input type="checkbox"/>	Archive1	<input type="text"/>	<input type="text"/>
		*	* ⓘ
<input type="checkbox"/>	managed	<input type="text"/>	<input type="text"/>
		*	* ⓘ

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

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

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

- 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.*

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

### Disabling UDO Guard

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

Enable	Archive Name	Key	Confirm Key
<input checked="" type="checkbox"/>	Archive1	*****	*****
<input checked="" type="checkbox"/>	managed	*****	*****

- Un-tick the check box beside the name of the Archive which is to cease using UDO Guard.
- Click **save**.



## Background Recall

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

File content is released from the RAID under two circumstances.

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

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

The background recall is performed in four stages:

### Stage 0: Setup

The background initialization process is configured through the setup

**Data Protection - Background Recall**

Archive: test1

Parent Folder: /test1

Download from cloud if media offline:

**File Property**

Migrate Date Range: 2017/06/01 to 2018/08/01

start cancel

page. It is possible to specify the following recall criteria:

- One Archive or all Archives. **Archive** drop-down list is not available for AAE.
- Root folder location of files to be recalled.
- For Archives that have data written to Optical and Cloud storage, when media is offline (removed from the library), by default data will Not be recalled from the cloud. This is to avoid data download charges from the cloud vendor being utilized. If you check the box, data will be recalled from the cloud during the background recall should the media not be available.

After the configuration is completed, the background recall (phase 1) can be started by clicking the **“start”** button.

## Stage 1: Initialization

When the background recall starts:

- It first locates all the files that match the criteria specified in the configuration.
- It calculates the total amount of data to recall and the required list of media.
- Depending on the number of files in the archive, this process may take several minutes.

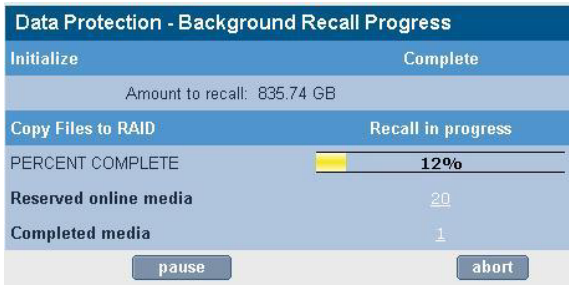


The progress is indicated by the **“Amount to recall”** value.

## Stage 2: Recall Progress

After the initialization is complete:

- The background recall may pause if the amount to recall exceeds the total volume size.
- The user has to acknowledge by clicking the **“continue”** button.
- If the amount to recall fits into the free space, the recall will automatically continue by first recalling from online media.



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

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

Note that offline media can be returned to the library at any time during the background recall. If all online media are processed, the job will wait until required offline media is returned to the library. It will then automatically continue the recall. Note that background recall will also automatically continue after a system restart.

- It can be stopped by clicking the “**abort**” button.
- It can also be paused by clicking the “**pause**” button. However, a pause recall does not persist across restarts.
- Any errors during the recall will be counted and a list of failed files can be viewed by selecting the error counter.

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

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

---

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

---

### Stage 3: Background Completion

The completion marks the end of the background recall and displays the summary information. This includes access to the error report if

any files have failed to be recalled. It is important that you acknowledge at this stage by clicking the “**finish**” button.



After clicking the “**finish**” button, following events are followed:

- The error log will be archived
- The media selection state will be cleared
- The “Background recall in progress” message is removed from the status page.

# *Archive Management Software*

## *Chapter 8* *Diagnostics Menu*

## System Jobs

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

Diagnostics - System Jobs					
Recent Jobs					
0 migration completed in the last 24 hours					
0 recall completed in the last 24 hours					
JobID	Archive	Type	Media	Started	Status
20080506000001	managed	Migration		2008.05.06 17:12:51	Waiting for resources
20080506000001	managed	Migration		2008.05.06 17:12:51	Waiting for resources
Jobs 1 - 2 of 2					

The following information is presented:

- **Job ID** - The unique identifying number assigned to the job.
- **Archive** - The archive which the migration job is a part of.
- **Type** - Whether the job is a migration, recall, backup, etc.
- **Media** - The Barcode of the media being used by the system job.
- **Started** - The time the job was started.
- **Status** - The job's status.

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

## Storage Devices

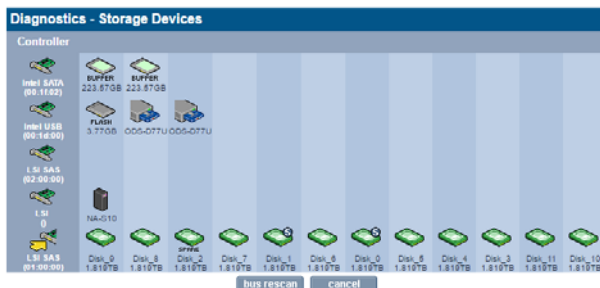
The **Diagnostics - Storage Devices** page shows all interface buses (SATA, SCSI, SAS, USB, FC, and IDE) and their associated devices and their status (see following screen shot).

### Viewing the Storage Devices

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

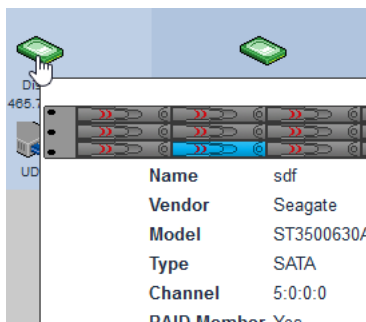


For UDO Archive Appliance



For NA-S10

- Hovering the mouse pointer over a device displays a Tool Tip for that device giving further information. Following is an example:



### Reserving Optical Drives for Recall

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

- From the menu bar, select **Diagnostics - Storage Devices**, and click on the library (or attached Library) icon:



- The **Optical Drive Changer Information** page is displayed.

#### Diagnostics - Storage Devices - Optical Drive Changer Information

Device Name	sg1	Status	ONLINE
Manufacturer	SONY	Model	NA-S30
Address	host:0 channel:0 id:0 lun:1	Serial Number	N/A
Device Type	Medium Changer	Firmware Version	0120

#### Slot Information

Number of Slots	27	Empty Slots	17
Full Slots	9	Loaded Slots	1

Drives reserved for recall




- For the Archive Appliance mid-range libraries, slot licensing may apply. Provide the slot license details. For more details, refer [Apply Slot License](#) on page 203.



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

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

### Apply Slot License

The Archive Appliance mid-range libraries accepts a slot license to enable the usage of media storage slots. Depending on the license, the number of license slots can be adjusted up to the maximum number of physical slots.

The slot license is nine characters long.

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

- From the menu bar, select **Diagnostics - Storage Devices**, and click on the library (or attached Library) icon.



- The **Optical Drive Changer Information** page is displayed.

Device Name	sg10	Status	ONLINE
Manufacturer	Alliance	Model	Midrange-XB
Address	host 9, channel 0, id 6, lun 0	Serial Number	0314000005
Device Type	Medium Changer	Firmware Version	T110
<b>Slot Information</b>			
Number of Slots	48	Empty Slots	0
Full Slots	44	Loaded Slots	4
Slot license	KGG OEN NEJ		
Drives reserved for recall	1		
<input type="button" value="save"/> <input type="button" value="back"/> <input type="button" value="disable"/>			

- Enter the slot license key into the **Slot license**. The key is split into three triple alphabetic character codes (for example: DIB-SAP-DOB).
- Click **save**.

## Designating Drive as Hotspare

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

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

1. From the menu bar, select **Diagnostics - Storage Devices**.
2. Click on the drive icon that can be added to the hotspare drive group.
3. The **Diagnostics - Storage Devices - Devices Details** page is displayed. Click the **hot spares** button.

Diagnostics - Storage Devices - Device Details			
Label	Disk_2 ⓘ	Host Volume	sda
Capacity	2,000,011,657,216 Bytes / 1862.65GB	Status	Online
Manufacturer	ASTI RAID Disk	Spun up	yes
Enclosure Position	2	Unique Id	
Serial Number	SEAGATE ST32000444SS 00069WM63BY2	SMART Status	Healthy
Error count	3	Temperature	30C (86.00 F)
<input type="button" value="hot spares"/> <input type="button" value="back"/>			

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

Diagnostics - Storage Devices - Device Details			
Label	Disk_2 ⓘ	Host Volume	sda
Capacity	2,000,011,657,216 Bytes / 1862.65GB	Status	Online
Manufacturer	ASTI RAID Disk	Spun up	yes
Enclosure Position	2	Unique Id	2
Serial Number	SEAGATE ST32000444SS 00069WM63BY2	SMART Status	Healthy
Error count	3	Temperature	30C (86.00 F)
<input type="button" value="free spares"/> <input type="button" value="back"/>			

After clicking the **“hot spares”** button, it becomes available as a replacement drive to all RAIDs. Note that the hotspare can be removed at any time by clicking the **“free spares”** button.

## Disk Status Icons

Table 8-1 Disk status icons 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 AMS. 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 when one of the other disks fail.

- Disks which are marked with:

**NO RAID**

are not currently members of a RAID.

- Disks which are marked with:

**REJECT**

have been rejected by the RAID they were a member of.

- Disks which are marked with

**RESYNC**

are currently being re-synchronised. The system, at all times, has to ensure that all RAID disks contain the appropriate current

data. If a difference is found, re-synchronization is performed to ensure all the RAID disks are synchronized.

Table 8-1: Disk status icons










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

Table 8-1: Disk status icons

















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

Table 8-1: Disk status icons

Icon	Meaning
	The disk is faulty
	The disk is faulty and is not part of a RAID
	The disk is faulty and has been rejected by the system
	The disk is faulty and is a system disk
	The disk is faulty, is a system disk and is not part of a RAID
	The disk is faulty, is a system disk and has been rejected by the system

## Other Status Icons

Table 8-2 Status icon describes the other status icons and their meaning.

Table 8-2: Status icon








Icon	Meaning
	This icon represents an internal controller card
	This icon represents an external controller card, i.e. the interface to an external device attached to the system

Table 8-2: Status icon

Icon	Meaning
	This icon represents the Archive Appliance or NETArchive optical library
	This icon represents an online optical drive
	This icon represents an offline or faulty optical drive
	Flash drive which contains boot information and Vital Product Data (VPD)
	Dedicated Solid State Drive (SSD) disk(s) that are used for efficiencies in packaging files into a single migration job, for efficient encryption key management, as well as with the NETArchive the default system backup location.

## Optical Drives

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

Diagnostics - Optical Drives			
Drive	Status	Barcode	Action ...
ODS1	Enabled	<empty>	set
ODS2	Enabled	<empty>	set

cancel

Drive status can be:

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

### Managing an Optical Drive

---

*Note: This option is applicable to the Archive Appliance and the NETArchive only. Drop-down options are not applicable to the Archive Appliance Express.*

---

To enable or disable an optical drive:



- From the menu bar, select **Diagnostics - Optical Drives**.

Diagnostics - Optical Drives			
Drive	Status	Barcode	Action ... ▾
ODS1	Enabled	<empty>	set
ODS2	Enabled	123QE20277	set

cancel

- Select the 'disable' action from the **Action** drop-down menu. By default, the 'disable' action is selected.
- Click the 'set' button to apply the disable action against the drive to be disabled.

Other actions that may be performed are:

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

*Note: When a drive is marked for cleaning, cleaning is performed by simply adding a cleaning cartridge into the library using the keypad 'Add Disk' option. The cleaning cartridge will be returned when the cleaning process has completed.*

## Drive Errors

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

Diagnostics - Optical Drives			
Drive	Status	Barcode	Action ... ▾
ODS1	Enabled	419RE10024	set
ODS2	Enabled	419RE10040	set

cancel

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

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

- **ASC** - Additional Sense Code
- **ASCQ** - Additional Sense Code Qualifier.

## Self Tests

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

### Self Test

	Status
Cache	N/A
Capacity	N/A
Configuration consistency	N/A
Devices	N/A
Disk	N/A
Key Store	PASS
LDAP/AD	N/A
Network ports	N/A
Notification	N/A
RAID/VG	N/A
Sensors	N/A
Services	N/A
Shares	N/A
UPS	N/A

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

Clicking **start** will check:

- **Cache** - The status of the RAID, including SATA (disk) drives. Normally, the system will perform a re-synchronisation to fix any problems with the cache. However, if the problem persists, contact Alliance Technical Support for further assistance.
- **Capacity** - The status of the AMS'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 system is in line with the operation of the AMS.

- **Devices** - The status of the devices attached to the SCSI bus (i.e. optical library and optical drives). If any of the devices are faulty, contact Technical Support for further assistance.
- **Disk** - The status of all SMART disks. Contact Alliance Technical Support if this test fails.
- **Key Store** - The status of key store associated with each archive. As well as the status, the total number of spare keys and the latest key page name is displayed.
- **LDAP/AD** - The status of LDAP and Active Directory connectivity. If this fails, ensure the relevant service is correctly configured and that there are no network problems.
- **Network Ports** - The status of the physical network ports, as well as network connectivity.
- **Notification** - Validates the notification system by pinging the email/SNMP address(es) listed for notification. If this fails, a valid email/SNMP address was not found. Check the **System - Notification** page to confirm the validity of the email/SNMP address(es).
- **RAID/VG** - The status of all RAIDs, Volume Groups and Logical Volumes. Contact Alliance Technical Support should this test fail.
- **Sensors** - The status of all attached sensors - board temperature, fan sensors, etc. Sensors alarms should be reported to ASTI support.
- **Services** - The status of the processes, including configurable services, running on the AMS. If any services fail, verify the **System - Services** page is correctly configured. If this is correct, then contact Technical Support for further assistance.
- **Shares** - The status of any Shares on the AMS. 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

Self Tests		Archive Test
<b>Diagnostics - Self Tests(Archive Test)</b>		
Last run at 2014-04-04 03:02:32		
Archive	Status	
<input type="checkbox"/> Archive1	N/A	
<input type="checkbox"/> Archive2	N/A	
<input checked="" type="checkbox"/> Cloud1	Migrating to archive .	20%

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

In the above example, only the 'Cloud1' archive was selected for an archive test.

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

## System Information

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

- System Information
- Log Files
- SCSI

### System Info

System Info		Log Files	SCSI
<b>Diagnostics - System Information (System Info)</b>			
System Up Time	0 Day(s) 16 Hour(s) 7 Minute(s)		
Product Serial Number	00006001		
System Serial Number	default		
Hardware Version	default		
Server Board	Supermicro X10SRH-CLN4F		
Motherboard Serial Number	default		
Model Number	default		
Quad CPU	Intel(R) Xeon(R) CPU E5-1620 v3 @ 3.50GHz		
Total Memory	31.37GB		
Software Version	6.00.12		
Build	14851		
System Personality File	<input type="button" value="create"/>		
Boot Image Backup File	<input type="button" value="create"/>		
Alliance Warranty Registration	<a href="http://www.plasmontech.com/warranty/index.html">http://www.plasmontech.com/warranty/index.html</a>		
Technical support website	<a href="http://www.plasmontech.com/customer/archive.html">http://www.plasmontech.com/customer/archive.html</a>		
Technical support email	<a href="mailto:tech.support@astiusa.com">tech.support@astiusa.com</a>		
<input type="button" value="cancel"/>			

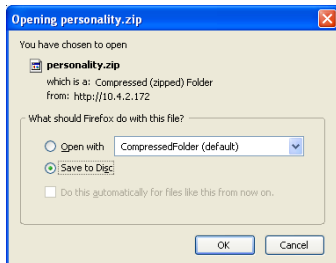
The **Diagnostics - System Information (System Info)** page lists:

- **System Up Time** - since last reboot
- **Product Serial Number** - same as optical Library serial number
- **System Serial Number** - The SMS (server) serial number
- **Hardware Version** - The current hardware version
- **Server Board** - Server board information

- **Motherboard Serial Number** - The SMS (server) motherboard serial number
- **Model Number** - The model number details the product configuration of the system, describing information such as the enclosure type, the memory capacity and many others
- **QUAD CPU** - Processor information
- **Total Memory** - The amount of memory (RAM) on the system
- **Software Version** - The currently installed software version
- **Build** - The currently installed software version's build number
- **System Personality File** - To create an XML based description of the system configuration. The XML file is zipped and can be downloaded to the client desktop.
- **Boot Image Backup File** - create a copy of the boot device file system content. All the files on the boot device file system are compressed into a zip container and available for download.
- **Alliance Warranty Registration** - Hyperlink to the Alliance warranty registration web page (requires an external internet connection)
- **Technical Support Website** - Hyperlink to the Alliance technical support web page (requires an external internet connection)
- **Technical Support Email** - Alliance Technical Support email address.

You can create a copy of the current System Personality File if it is required by Alliance Technical Support. To do so:

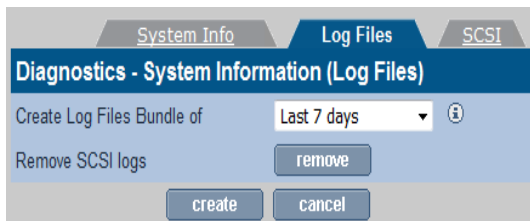
1. Click the **create** button.
2. The AMS will generate a downloadable copy of the personality file, then pop-up the browser's Download dialog:



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

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

## Log Files



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 AMS. Specify a time period, using the drop-down list, to create a log file bundle of the following:
    - **Last 7 days**
    - **All days**
    - **From custom date**
    - **Secure**
    - **Drive Logs** - This option extracts a logging information from the optical drives.
- The log bundle can be downloaded to the local PC and then emailed to Alliance Technical support.
- This tab also allows SCSI logs to be purged. This is useful if a hardware fault has generated an excessive number of hardware errors. After the required logs have been extracted, the SCSI logs should be removed.

---

*Note: The AMS does not store previous log bundles.*

---

## SCSI

---

*Note: This section is not applicable for NETArchive.*

---



System Info			Log Files			SCSI		
Diagnostics - System Information ( SCSI )								
Device		SCSI ID		Firmware Version				
Library Host		0:0:0:1		0120				
Drive ODS1		0:0:0:0		1570				
Drive ODS2		1:0:0:0		1570				

cancel

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

- **Devices** on the SCSI bus (i.e. optical Drives and Libraries)
- **SCSI ID** (in the format Host, Bus, ID and LUN for example: 1:0:2:0) **Serial Number**
- Currently installed **Firmware Version**.



# *Archive Management Software*

## *Chapter 9* *Shutdown*

## Shutdown the AMS using the Web Interface

### Shutdown

The **Shutdown/Reboot** page allows:

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

---

*Note: The AMS powers down both the SMS server and Optical Library.*

---



---

*Note: NETArchive powers down only the SMS Server. Optical Library can only be powered down via front panel.*

---



---

*Important: 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 system from the Web interface:

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

The **Shutdown/Reboot** page opens:



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

## Shutdown the Archive Appliance Using the Library Power Switch

### AA16, AA32, AA80 and AA174 Models only

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

On/Off  
switch



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

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

### AA238, AA438 and AA638 Models only

To shut down the Archive Appliance:

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

Power switch



3. Power off the library.

## NETArchive S-Series Library only

The NETArchive NA-S10 library starting and stopping is not controlled by the AMS software. To start and stop the library, see [Starting and Stopping the NETArchive NA-S10 and NA-S30 Libraries](#) on page 263.

# *Archive Management Software*

## *Chapter 10* *Troubleshooting*

# Troubleshooting

Table 10-1:AMS Troubleshooting Checklist

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

Possible cause	Suggested action	Comments
The system is still booting.	Wait for boot to complete - approximately six minutes.	
The IP address is invalid.	For Archive Appliance, use the keypad to check that the IP address is configured correctly.	
Incorrect Ethernet port used (on dual port Appliance).	Test using other Ethernet port.	<i>eth0</i> is the port enabled by default.
Question marks appear on keypad display for IP address	Cannot get IP address from DHCP server OR network connection cannot be established OR static IP address could not be applied	Try other network port (it needs to be <i>eth0</i> and re-apply the network settings (gateway, mask and IP address)
Faulty Ethernet cable.	Test with a known working Ethernet cable.	



Table 10-1:AMS Troubleshooting Checklist

Faulty network Switch / configuration.	Verify the Switch is receiving power, the port is enabled and set to Auto Negotiate. Test the system using another Switch port.	
System Crash.	Reboot or power-cycle.	If the Web Interface is inaccessible, attempt to reboot via the keypad or serial console. As a last resort press and hold the power button to switch off.
Incorrect Web browser settings.	If a proxy server is being used ensure it is bypassed for local addresses.	
Hardware failure.	Contact Alliance support.	
<b>The system does not power ON (no LED or fan activity).</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Faulty power cable.	Test with a known working power cable.	
Hardware failure.	Contact Alliance support.	
<b>The system fails its self-test.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>

Table 10-1:AMS Troubleshooting Checklist

An optical drive is unavailable.	Reboot the system. If this does not resolve the issue contact Alliance support.	
Notification ping failure to either SMTP or SNMP server.	Ensure relevant server is available. Check Notification configuration.	
One or more key services are not running.	Check running services and enable any which have stopped. If a service fails to start, reboot the system.	Check service configuration in <b>System - Services</b>
Hardware failure.	Contact Alliance support.	
<b>Data is not migrating to media.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Library media full.	Offline closed media and add blank spares.	
SSM Service not started.	Open the <b>System - Services</b> page and start SSM. If this fails reboot the system, then attempt to start SSM. If this also fails contact Alliance support.	

Table 10-1:AMS Troubleshooting Checklist

SSM fault.	Go to the <b>Diagnostics - Self test</b> page and run the Archive Test. If this fails, reboot the system, then retest. Contact Alliance support if problem is not resolved.	
Dirty media.	Clean the media using an Alliance UDO media cleaning kit and retry.	<i>Cleaning Media</i> on page 251
Hardware failure.	Contact Alliance support.	
<b>Data cannot be recalled from media.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
A migration job is using all optical drives.	Wait for the migration job to complete. Select the <b>Diagnostics - System Jobs</b> page to view the status of current jobs. Reserve at least one optical drive for recall operations ( <b>Diagnostics - Storage Devices - Library</b> )	Recalls take priority over migration, but any migrations for the loaded disk must be completed before the media can be ejected to load a different media for recall.

Table 10-1:AMS Troubleshooting Checklist

Required media is offline.	View the <b>System - Status</b> page to determine which media to load. Refer to the <b>Storage - Media Requests</b> page to see other outstanding media requests.	
SSM service not started.	Go to the <b>System - Services</b> page and start SSM. If this fails reboot the system then attempt to start SSM. Contact Alliance support if problem is not resolved.	
SSM fault.	Reboot the system. Contact Alliance support if the problem is not resolved.	
Dirty media.	Clean the media using an Alliance UDO media cleaning kit and retry.	Refer to the Operator Guide for media storage and care information.
Hardware failure.	Contact Alliance support.	
<b>Media fails to close.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
"RMDB corruption, no partition found"	Recover RMDB from backup	

Table 10-1:AMS Troubleshooting Checklist

"Partition is not mounted"	Ensure that archive is mounted and active, and run self-test	Run migration self-test to confirm archive is healthy
"Failed to set the archive to read-only"	Restart SSM and run self-test	
"Failed to migrate all active files"	Run migration self-test and check hardware status - run self-test	Problem with hardware or resources
"Failed to close media"	Check hardware status and archive resource	Review media inventory and optical drive status
"Failed to set the archive to read-write"	Restart SSM and run self test	

Table 10-1:AMS Troubleshooting Checklist

**Backup failure.**

<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
No backup media in Appliance.	Add backup media.	
Backup media dirty / damaged.	Replace media.	
Backup media at end of life.	Replace media.	Media can be re-written approximately 5,000 times.

**Administrator Notified that a dirty shutdown was performed.**

<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Power failure.	Connect to a UPS.	A UPS is recommended.
Connected to a UPS but did not shutdown before UPS battery discharged.	Check the serial link to the UPS.	
UPS service not started.	Select <b>System - Services</b> and start the UPS service.	

**Administrator notified that the RAID has degraded.**

<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Hardware failure.	Contact Alliance support.	

Table 10-1:AMS Troubleshooting Checklist

<b>SATA/SAS drive missing.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
SATA/SAS drive not inserted correctly.	Shutdown the system. Remove then re-insert the drive fully in its drive bay. Power ON the system. Contact Alliance support if the problem is not resolved.	A missing SATA/SAS drive can be determined from the <b>Diagnostics - Storage Devices</b> page of the web browser interface.
<b>Unable to add a user.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
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)
<b>Unable to connect to network share.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Incorrect username or password.	Ensure the correct username and password is used to connect to the AMS.	

Table 10-1:AMS Troubleshooting Checklist

Network service not started.	Select <b>Network - Services</b> . Ensure the correct network services have been started on the AMS.	
Incorrect hostname or IP used.	Use the correct hostname or IP address. Check that it is possible to ping the system 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 AMS.	<i>See "Adding a User" on page 93.</i>	
The client username does not have permissions to access the share.	If the user should have the required permissions, see <i>Modifying a Share</i> on page 104.	
Host has been denied access.	If the host should have access, see <i>Modifying a Share</i> on page 104.	



Table 10-1:AMS Troubleshooting Checklist

**Successfully connect to network share but permission denied when writing.**

<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
File or directory does not have write access permissions for the connected user.	If the user should have the required permissions, see <a href="#">Modifying a Share</a> on page 104.	The connected users can be determined by opening the <b>Network - Shares</b> page and clicking on <b>connections</b> . If the access problem only occurs for a specific path or file in the share, use the <b>Storage - Browse</b> option to check the access permissions for the file or directory.
The share has been set read-only.	If the share is writeable, open the <b>Network - Shares</b> page and click on the share. Ensure the <b>Read only</b> option is not selected.	

Table 10-1:AMS Troubleshooting Checklist

SSM service not started.	Open the <b>System - Services</b> page and start SSM. If this fails, reboot the system then attempt to start SSM. Contact Alliance support if problem is not resolved.
--------------------------	--

SSM fault.	Go to the <b>Diagnostics - Self test</b> page and run the <b>Archive Test</b> . If this fails, reboot the system, then retest. Contact Alliance support if problem is not resolved.
------------	---

**Successfully connect to network share but permission denied when reading.**

<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
File or directory does not have read access permissions for the connected user.	If the user should have read permissions, see <a href="#">Modifying a Share</a> on page 104.	The connected users can be determined by going to the <b>Network - Shares</b> page and clicking on <b>connections</b> .

Table 10-1:AMS Troubleshooting Checklist

SSM service not started.	Open the <b>System - Services</b> page and start SSM. If this fails reboot the system then attempt to start SSM. Contact Alliance support if problem is not resolved.	
SSM fault.	Open the <b>Diagnostics - Self test</b> page and run the <b>Archive Test</b> . If this fails, reboot the system, then retest. Contact Alliance support if problem is not resolved.	
<b>Unable to overwrite or modify files.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
The <b>WORM emulation</b> option has been set for the CIFS share.	Deselect <b>WORM emulation</b> on the <b>CIFS</b> tab of the share, see <a href="#">Modifying a Share</a> on page 104.	
<b>Allow File Changes</b> has been set to NO for the Archive Volume.	If file changes should be allowed, see <a href="#">Viewing and Editing Volume Properties</a> on page 130 and set the <b>Allow File Changes</b> option to YES.	
<b>No Free Space reported when writing to the share.</b>		

Table 10-1:AMS Troubleshooting Checklist

Possible cause	Suggested action	Comments
The RAID cache is full.	See the causes and actions for <i>Data is not migrating to media.</i> on page 228.	
The Archive Volume option <b>Never Release Files</b> has been set.	See “ <i>Viewing and Editing Volume Properties</i> ” on page 130. Reconfigure release policy as required.	
<b>Email Notifications not being received.</b>		
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 if it is possible to ping the SMTP server from another server on the same subnet as the system.	

Table 10-1:AMS Troubleshooting Checklist

SMTP server port number incorrect.	Enter the correct port number.	
Sender not defined.	Enter a sender address.	This is required by some SMTP servers.
Username and password not defined.	Enter a valid username and password.	These are required by some SMTP servers.
Incorrect recipient email address entered.	Check the recipient email address is entered correctly.	
SMTP not enabled.	Ensure the <b>enable</b> check box is checked.	
<b>SNMP traps not being received.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
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 <b>enable</b> check box is checked.	
<b>Administer notified that the UDO drive is dirty.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>

Table 10-1:AMS Troubleshooting Checklist

Dirty drive.	Insert the cleaning cartridge to perform a cleaning cycle. The dirty status should be reset after the next recall or migration.	
Hardware failure.	Contact Alliance support.	
<b>Appliance will only boot into MAINTENANCE mode.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Hardware failure.	Contact Alliance support.	
<b>Unable to join Active Directory or NT4 domain.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Incorrect time on Appliance.	Go to the <b>System - Time &amp; Date</b> page and correct the time.	When the system joins the domain its time will be synchronized with the domain.
DNS is not / incorrectly configured.	The system must have DNS configured to be able to join a domain. See <a href="#">DNS Configuration for Windows Active Directory</a> on page 92.	
<b>Unable to connect to LDAP server.</b>		
<i>Possible cause</i>	<i>Suggested action</i>	<i>Comments</i>
Incorrect time on Appliance.	Go to the <b>System - Time &amp; Date</b> and correct the time.	

Table 10-1:AMS Troubleshooting Checklist

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

Table 10-1:AMS Troubleshooting Checklist

**Cloud connection failure**

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



# *Archive Management Software*

## *Chapter 11*

### *Using the Archive Appliance Keypad Interface for Media Operations & Setting IP Address*

## Configuration

### Setting the IP Address

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

```
Archive Appliance
      Add disK
SEL next PREV ESC
```

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

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

```
Archive Appliance
      Edit ConFiguRation
SEL next PREV ESC
```

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

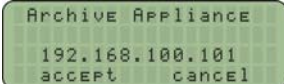
```
Archive Appliance
Edit ConFiguRation:
      Set IP Address
SEL next PREV ESC
```

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

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

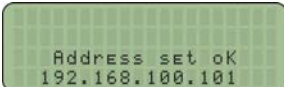
5. Press **-1** and **+1** to change the value inside the brackets (the first digit in any group of three can only be set to 0, 1 or 2).
6. Press **next** to highlight the next digit.
7. Press **-1** and **+1** to change the value inside the brackets (the maximum value for each 3-digit group is 255).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

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



```
Archive Appliance
192.168.100.101
accept  cancel
```

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



```
Address set ok
192.168.100.101
```

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

## Setting the Netmask

To edit the netmask, follow the method in [Setting the IP Address](#) on page 244. In step 3, make sure the **Set Netmask** submenu is selected.

## Setting the Gateway IP Address

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

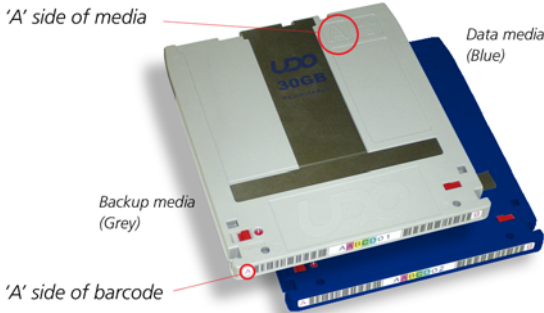
To edit the gateway IP address, follow the method in [Setting the IP Address](#) on page 244. In step 3, select the **Set Gateway** submenu. The remaining system configuration can be performed via the web interface.

## Adding UDO Media

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

- Add new disks (UDO RW only) for backup purposes (can only be added via the mailslot).  
UDO RW media can be identified by its **Grey** cartridge case.
- Add new data disks (UDO WORM or Compliant UDO WORM only) for migration (can be added via the mailslot or direct slot access).  
UDO WORM media can be identified by its **Blue** cartridge case.

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



### Adding Backup UDO Media via the Mailslot

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

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

```

Archive Appliance
Add disk
SEL next PREV ESC
  
```

2. Press **sel**.

3. Insert the backup UDO media, 'A' side facing up, into the Mailslot.  
AA238, AA438 and AA638 models only: Press the eject button, shown below. The library will then take the media and close the mailslot.



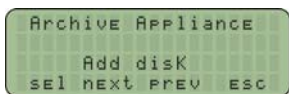
4. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see [page 250](#)).  
If all is well, a **Disk added OK** message is displayed.
5. Repeat the above steps until all required backup UDO media has been added.

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

## Adding Data UDO Media via the Mailslot

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

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



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

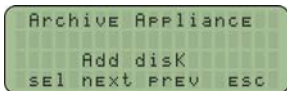


4. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see [page 250](#)).  
If all is well, a **Disk added OK** message is displayed.
5. Repeat the above steps until all media have been added.

## Adding UDO Cleaning Cartridge via the Mailslot

To load cleaning cartridges via the mailslot:

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



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



5. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see [page 250](#)).
6. The library will proceed to clean all the marked drive and when complete, return the cleaning cartridge via the mailslot.

## Adding Data UDO Media via Direct Slot Access

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

### AA16/32, AA80 and AA174 Models

#### Removing the Library Side Panel

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

1. Shut down the Archive Appliance: see [Shutdown the AMS using the Web Interface](#) on page 222 or [Shutdown the Archive Appliance Using the Library Power Switch](#) on page 223.
2. Remove the power cord from the supply.
3. Open the library front door.
4. Remove and retain the panel securing screws from the front and rear of the library side panel.
5. Lift the panel up to remove it.

**WARNING**

---

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

---

---

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

---

### Adding Media

Referring to the slot map appropriate for the Archive Appliance library model, see [page 296](#), add media to the lowest numbered available slots.

---

*Important:* Do not place media in the Utility Slots, see [Library Slot Maps on page 296](#).

---

### Refitting the Library Side Panel

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

### AA238, AA438 and AA638 Models

To return offline media via direct slot access:

1. Shut down the Archive Appliance.
2. Open the library rear door.
3. Referring to the slot map on [page 303](#), add media to the lowest numbered available and unassigned slots.
4. Restart the Archive Appliance. The Archive Appliance will rescan the contents of the library and update its inventory.

## Possible Problems

### Disk Errors

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

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

Remove the cartridge. Another may be inserted.

### Other Errors

Other error messages are:

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



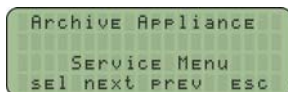
## Removing UDO Media

If any disks have failed, an administrator will receive an alert via the configured method (see [Notification](#) on page 74) informing which media need to be removed. When this happens, remove UDO media from the Archive Appliance via the Mailslot.

Media can also be removed for Offline Media Management - see [page 285](#).

### Removing UDO Media with Unreadable Barcode

1. Press any key to display the top-level **Add disk** menu.
2. Press **next** three times to display **SERVICE MENU**.



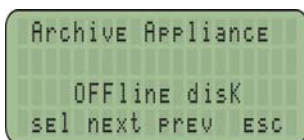
3. Press **sel** to display the **SERVICE MENU** sub-menu.
4. Press **next** or **prev** to display the required option (Bad Barcode Disk).
5. Press **sel**.  
The library picker will automatically select the first disk to be removed.
6. Remove the cartridge from the Mailslot.  
The "**Bad Barcode Disk**" submenu will be again displayed.
7. Repeat the above steps until all failed media are removed.

### Cleaning Media

A UDO cleaning service is available from Archive Alliance.

To remove dirty media, perform the following steps:

1. Navigate to the web GUI "**Storage Media**" menu item and select the **Search** tab. This interface will allow the selection of all media that "**Requires attention**" including dirty media (see [Search Media](#) on page 150).
2. After the media has been identified, select "**show media: to select for offline**" and select all media.
3. Media that have been selected for offline can be removed from the library with the keypad option '**Offline media - User selected**' from the '**Offline Media**' Menu.



To re-introduce the cleaned media, see [Adding Backup UDO Media via the Mailslot](#) on page 246 or [Adding Data UDO Media via the Mailslot](#) on page 247.

# *Archive Management Software*

## *Chapter 12*

### *Using the NETArchive Keypad Interface for Setting Library IP Addresses*

## Configuring the NETArchive NA-S10 IP Address

For the Archive Management Software (AMS) to access the NA-S10 optical library, an IP address must be specified. This IP Address must be specified in two locations:

1. On the physical optical library via the NA-S10 Keypad interface
2. Via the AMS User Interface

### Setting Library IP Address via NETArchive NA-S10 Keypad Interface

The IP address, subnet mask, and default gateway settings must first be set on the physical library to facilitate connecting the AMS software for initialization and control of the library.

The following values are the factory default values.

- IP address: 192.168.1.10
- Subnet mask: 255.255.255.0
- Default gateway: 0.0.0.0

To modify these factory default settings, you must utilize the keypad on the front panel, utilizing the following procedure:

1. Press the MENU button.  
The display changes to a menu display.



IP SETTING

2. Scroll using the ↑ ↓ buttons to select IP SETTING, then press the ENTER button.  
The IP ADDRESS screen appears.



IP ADDRESS  
192.168.001.010

3. Press the ENTER button.  
The first digit in the IP address starts flashing to indicate the address is in edit mode.



IP ADDRESS  
192.168.001.010

4. Enter the IP address. Move between digits using the → ← buttons, and change the value using the ↑ ↓ buttons.
5. When finished, press the ENTER button. Validate that the address is correct.

```
IP ADDRESS
192.168.001.010
```

6. Display the SUBNET MASK screen using the ↑ ↓ buttons, then press the ENTER button.

```
SUBNET MASK
255.255.255.000
```

7. Enter the subnet mask using the same technique as with the IP address, and press the ENTER button when finished.
8. Display the DEFAULT GATEWAY screen using the Jj buttons, then press the ENTER button.

```
DEFAULT GATEWAY
000.000.000.000
```

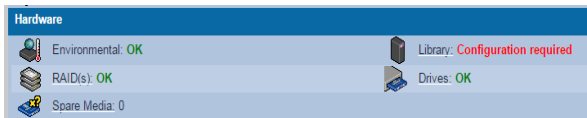
9. Enter the default gateway using the same technique as with the IP address, then press the ENTER button when finished.
10. Press the **MENU** button or the **ESC** button twice to exit the menu.
11. Reboot the library. The updated IP address takes effect only after the library is rebooted. See section [Starting and Stopping the NETArchive NA-S10 and NA-S30 Libraries](#) on page 263 for details on rebooting the library.
12. The library is now back online.

## Setting IP Address via AMS User Interface

To facilitate the AMS connection to the NETArchive NA-S10 library, you must now specify the IP address of the library. After the IP address is specified, the AMS will connect to the library and perform the initial configuration of the library, including discovery, scanning and inventorying NETArchive media loaded into the library.

To set the IP address of the library, perform the following procedure:

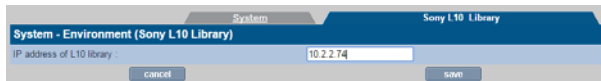
1. Log into the AMS system.
2. On the **System – Status** page, in the **Hardware** section, click on **Library**.



You will now be taken to the **System – Environment** (NETArchive NA-S10 Library) configuration page.



3. Specify the IP address of the NETArchive NA-S10 Library.



4. Click the **save** button.
5. The AMS software will now connect to the NETArchive NA-S10 library and perform discovery of installed hardware. Next it will initialize the library, discovering all NETArchive Media installed in the library and populate all internal data structures.

After initialization has completed, you will be returned to the **System – Status** page. As depicted in the following display, the IP address of the library is displayed.

Hardware	
 Environmental: <b>OK</b>	 Library: <b>10.2.2.74</b>
 RAID(s): <b>OK</b>	 Drives: <b>OK</b>
 Spare Media: 0	

## Configuring the NETArchive NA-S30 Maintenance IP Address

For the Archive Management Software (AMS) to access the NA-S30 optical library maintenance interface, an IP address must be specified. Typically, only Alliance's Service Representatives will need to access this maintenance interface. They can do this by directly connecting a service laptop using a cross-over cable to the library. But in instances where remote access may be required, and IP address must be configured for network based access.

To setup for remote access to the NA-S30 library, the IP Address must be specified in two locations:

1. On the physical optical library via the NA-S30 Keypad interface.
2. Via the AMS User Interface

### Setting Library Maintenance IP Address via NA-S30 Keypad Interface

The IPv4 address, subnet mask, and default gateway settings must first be set on the physical library to facilitate connecting the AMS software for library maintenance operations.

The following values are the factory default values.

- IP address: 192.168.1.10
- Subnet mask: 255.255.255.0
- Default gateway: 0.0.0.0

To modify these factory default settings, you must utilize the keypad on the front panel, utilizing the following procedure:

1. Press the MENU button.  
The menu appears in the display.

```
Menu
> 1.Information
  2.Setup
  3.Maintenance
```

2. Use the  $\uparrow$   $\downarrow$  buttons to select Setup, and press the ENTER button. The Setup screen will appear.

```
Setup
> 1.Network
  2.Control Panel
```



- Use the  $\uparrow$   $\downarrow$  buttons to select Network, then press the ENTER button. The Network screen will appear.

```
Network
> 1.Network 1
  2.Network 2
```

- Use the  $\uparrow$   $\downarrow$  buttons to select Network 1, and press the ENTER button. The Network1 screen will appear.

```
Network1
> 1.IPv4 Settings
  2.IPv6 Settings
```

- Use the  $\uparrow$   $\downarrow$  buttons to select [IPv4 Setting], and press the ENTER button.

The following screen appears. An asterisk (\*) shows the current setting. To configure the IPv4 address, this setting must be set to Enabled. If the setting is already set to Enabled, then proceed directly to step 8.

```
IPv4 Setting
IPv4 Enabled
  Enabled
*Disabled
```

- Press the ENTER button to change the setting. The selection screen will appear (i.e. screen with the cursor (>)). You can now change the setting on this screen.

```
IPv4 Setting
IPv4 Enabled
> Enabled
  *Disabled
```

- Use the  $\uparrow$   $\downarrow$  buttons to select [Enabled], and press the ENTER button. The confirmation screen (i.e. screen without the cursor (>)) appears.

```
IPv4 Setting
IPv4 Enabled
*Enabled
  Disabled
```

- Check that [Enabled] is selected, and press the  $\downarrow$  button.
- Press the ENTER button to display the selection screen.
- To use a static IP address, use the  $\uparrow$   $\downarrow$  buttons to select [Static], and press the ENTER button.

---

*Note: To use DHCP, use the  $\uparrow$   $\downarrow$  buttons to select [Auto], press the ENTER button, and then proceed to step 17.*

---

11. Press the ↓ button. The following screen appears.

```
IPv4 Setting
IPv4 Address
000.000.000.000
```

12. Press the ENTER button. The first digit of the IP address blinks, indicating that it can be changed.

```
IPv4 Setting
IPv4 Address
000.000.000.000
```

13. Enter the IP address. Use the → ← buttons to move the cursor, and use the ↑ ↓ buttons to change the values.
14. Press the ENTER button after entering the address to confirm it.
15. Press the ↓ button to display [IPv4 Netmask], and configure the subnet mask using the same technique as when setting the IP address.

```
IPv4 Setting
IPv4 Netmask
000.000.000.000
```

16. Press the ↓ button to display [IPv4 Gateway], and configure the default gateway using the same technique.

```
IPv4 Setting
IPv4 Gateway
000.000.000.000
```

17. Press the ↓ button. [IPv4 DNS] appears.

```
IPv4 Setting
IPv4 DNS
Auto
*Static
```

18. To configure the DNS address, select Static.
- If the current setting is Auto, display the selection screen using the ENTER button, use the ↑ ↓ buttons to select [Static], and then press the ENTER button to confirm.

---

*Note: To obtain the DNS address automatically, select Auto. Confirm the setting using the same technique as you would with Static, and proceed to step 24.*

---

- Press the ENTER button. The IPv4 Primary DNS screen appears.

```
IPv4 Settings
IPv4 Primary DNS
000.000.000.000
```

- Press the ENTER button. The first digit of the IP address blinks, indicating that it can be changed.
- Use the →, ←, ↓ and ↑ buttons to enter the primary DNS address, and press the ENTER button.
- Press the ↓ button. The IPv4 Secondary DNS screen appears.
- Enter the secondary DNS address using the same method as step 20, and press the ENTER button.
- Press the ↓ button. The following confirmation screen appears.

```
Network1
IPv4 Settings
> Save
Cancel
```

- Check that Save is selected, and press the ENTER button. The changed IP address is enabled. The [Network1] screen appears again.

```
Network1
> 1. IPv4 Settings
2. IPv6 Settings
```

- Press the BACK button three times to end menu operation.

## Setting Maintenance IP Address via AMS User Interface

To facilitate the AMS connection to the NETArchive NA-S30 library maintenance interface, you must now specify the IP address to the AMS. Once the IP address is specified, the AMS will be able to connect to the library for maintenance operations.

To set the maintenance IP address, perform the following procedure:

- Log into the AMS system.
- On the **Diagnostics – Storage Devices** page, click on the NETArchive Library. The **Diagnostics – Storage Devices – NETArchive Changer Information** page will be displayed.
- Click on the **Maintenance** UI button. The NA-S30 Maintenance UI page will be displayed.
- Enter the IP address for the NA-S30 Maintenance IP Address.

5. Click **Save**. If you have previously filled this IP address information in, you can proceed to the next step.
6. Click the **Launch** button. This will launch the NA-S30 Maintenance UI.
7. After connected, enter the user name and password.

## Starting and Stopping the NETArchive NA-S10 and NA-S30 Libraries

The NETArchive NA-S10 library starting and stopping is not controlled by the AMS software. To start and stop the library, you must interface directly with the library component.

---

*Note: The I/E drawer must always be closed when starting and stopping the NETArchive NA-S10 library.*

---

### Starting the NA-S10 Library

1. Check that the power supply cord is connected.
2. Turn on the main power switch on the rear panel of the library.
3. Press the On/Standby switch on the front panel.
  - When the button is pressed, the On/Standby button indicator will turn green.
  - When initialization ends, the library is ready for use. The text on the library display will stop flashing.

### Stopping the NA-S10 Library

1. Press the On/Standby switch for two seconds or longer.
2. A shutdown confirmation message appears on the display. Use the arrow buttons to select [Y], then press the [ENTER] button.
3. Wait until the On/Standby button indicator changes from flashing green to red.
4. Turn off the main power switch on the rear panel.



# *Archive Management Software*

## *Chapter 13*

### *The Archive Appliance with an Additional Library Attached*

## Additional Library

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

---

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

---

The attached library can operate in one of two modes:

### Slot Overflow

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

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

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

### Pool-per-Library

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

---

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

---



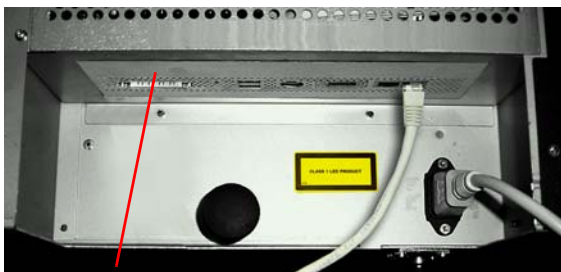
## Attaching an Additional Library

Alliance recommends that the additional library is situated as close as possible to the host Appliance for convenience of operation.

1. Ensure that the host Archive Appliance is properly shut down - see [Shutdown the AMS using the Web Interface](#) on page 222.
2. Connect the additional library to the host Appliance using the SCSI cable provided.

### AA16 to AA174 models only

SCSI port is located on the lower rear side of the Appliance.



SCSI Port

### AA238 to AA638 Models Only

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



SCSI Port

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

---

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

---

5. Power on the Appliance.

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

```
Attached Library
Active Hostname
Harrier
```

## Attached Library Keypad Interface

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

In Slot Overflow with Load Balancing mode, the keypad can only be used to add media to the library. All other functions are controlled using the host Appliance keypad interface; refer to the appropriate sections of the Administrator's Guide for:

- Removing failed media - see [page 250](#)
- Offline Media Management - see [page 285](#)

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

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

### Adding UDO Media to the Attached Library via the Mailslot.

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

```
Attached Library
Add disk:
Add data disk:
sel next prev esc
```

2. Press **sel**.

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



4. The cartridge will be checked for valid UDO format and barcode (if there is a problem, see [page 250](#)).  
If all is well, a **Disk added OK** message is displayed.
5. Repeat the above steps until all media have been added.

---

*Note:* To add media to the attached library via direct slot access, see [page 248](#).

---

### Removing UDO Media via the Mailslot

---

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

---

1. Press any key to display the top-level **Add disk** menu.
2. Press **next** until **SERVICE MENU** is displayed.
3. Press **sel** to display the **SERVICE MENU** sub-menu.
4. Press **next** or **prev** to display the required option (Remove dirty disk, Failed data disk, or Misplaced disk).
5. Press **sel**.  
The library picker will automatically select the first disk to be removed.
6. Remove the cartridge from the Mailslot.  
The **REMOVE Disk** submenu will be displayed once more.

Repeat the above steps until all failed media are removed.

### Attached Library Web Interface

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

#### Viewing Attached Library Information

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

- System - Status - Environment

System	HostLibrary	Attached Library
<b>Attached Library - Environment</b>		
Temperature	24 Celsius	
Front Fan Status	OK	
Rear Fan Status	OK	
<b>Drive Temperature</b>		
UD05	24 Celsius	
UD06	24 Celsius	

- Diagnostics - UDO Drives

Host	Attached		
<b>Diagnostics - UDO Drives</b>			
Drive	Status	Barcode	Action
UD05	Enabled	<empty>	<input type="button" value="disable"/>
UD06	Enabled	<empty>	<input type="button" value="disable"/>

- Storage - Online Media

Primary	Secondary
<b>Storage - Online Media</b>	
Slot Usage	
Spare	0
Open	0
Closed	0
Empty slots	166
Total slots	166

## Configuring Mode of Operation

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

Diagnostics - Storage Devices - UDO Changer Info			
Device Name	sg12	Status	IDLE
Manufacturer	Plasmon	Model	Midrange-G
Address	host10, channel:0, id:6, lun:0	Serial Number	525699
Device Type	Medium Changer	Firmware Version	H06e
Slot Info			
Number of Slots	166	Empty Slots	148
Full Slots	15	Loaded Slots	3
Drives reserved for recall	1 <input type="button" value="v"/>		
Multiple Library Management	<input checked="" type="radio"/> Slot Overflow <input type="radio"/> Pool Per Library		

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



# *Archive Management Software*

## *Chapter 14*

*Using the NETArchive Express (NAE) or the Archive Appliance Express (AA Express)*

## Media Labelling

For the NETArchive Express (NAE), all media is barcoded. The NAE dynamically identifies all media by its barcode and all data that is migrated to it as well as its status. Any media utilized by the NAE will be identified and tracked using its barcode.

For the Archive Appliance Express (AA Express), each unique piece of UDO Media used in the AA Express is identified with a dynamically incremented sequence number. It is the administrator's responsibility to label and number each media cartridge prior to usage.

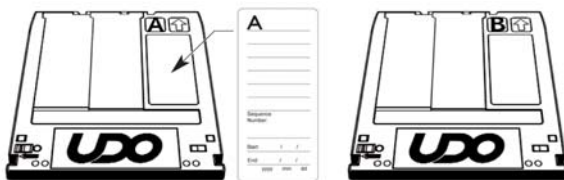
When new media is requested by the AA Express:

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 ([Action Requests](#) on page 281) on the media label.

---

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

---



## Media Handling

### Inserting Media in the NAE

Hold the NETArchive ODA media at the rear of the cartridge and insert in the direction of the arrow (media shutter forward) until it clicks into place. The ODA drive will then move the cartridge into the drive for usage.

### Inserting Media in the AA Express

---

*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

The NAE media is single sided.

For AA Express, 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 from the NAE

NETArchive ODA Media is automatically ejected from drive when it has been closed or during a background recall or data recovery processing. To manually remove media from the ODA Drive, simply click on the remove button on the Storage - Media UI page display as described in section [Removing Media from the NETArchive](#) on page 144

## Ejecting Media from the AA Express

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 - [Storage of Offline Media](#) on page 286.

## Basic Operation

### Writing to ODA and UDO Media

Files written to either the NAE or the AA Express via network shares are initially stored on the RAID storage volume. Files are then migrated to the optical media. The NAE records what media the data was written to (NAE ODA Media Barcode or AA Express UDO Media sequence number).



#### Writing files to the AA Express

The NAE and AA Express track only one piece of 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.

### NAE Blank Media Insertion

If a new blank piece of media is inserted into the NETArchive ODA drive when a piece of open media already exists, the NAE will request that the open media be returned to the ODA Drive. The NAE will not utilize a new media until the current open media has been closed.

The NAE issues an alert notification and displays requesting the media be reinserted into the drive.

### AA Express 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 NAE and AA Express only when requested.*

## Reading from UDO Media

When users attempt to read files, the NAE and AA Express determines the media that the file has been written to. If the media is not in the drive, a media request will be issued to the operator for it to 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.

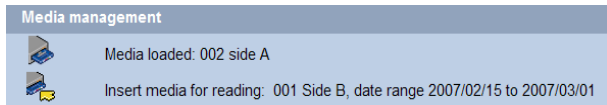


## Media Request Queuing

If the appropriate media is not loaded into the optical drive, read/write operations and associated media requests will be "queue". Queued operations are completed and their associated requests cleared automatically when the correct media and/or media side is loaded into the drive.

## Action Request Notification

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



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 barcode or sequence number and which side of the media is currently loaded. The lower line displays operator action requests - *Action Requests* on page 281.

The NAE and 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 system 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 NAE or AA Express to successfully write to or read from media.

*Note: In the sections below, examples are provided for the AA Express. The NAE will differ only in displaying specific barcodes rather than sequence numbers and sides.*

### 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 system requires blank media in order to write files.



1. For the NAE, insert a new barcoded ODA cartridge. For the AA Express, Label a piece of blank UDO media with the sequence number indicated (see [Media Labelling](#) on page 274) and insert into the UDO drive ensuring side A is loaded (see [Inserting Media in the NAE](#) on page 275).
2. The system 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 (AA Express Only)

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 in the NAE](#) on page 275).
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 286.
2. Label a piece of blank UDO media with the indicated new sequence number (see [Media Labelling](#) on page 274) 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 system 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 248) 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 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.*

---

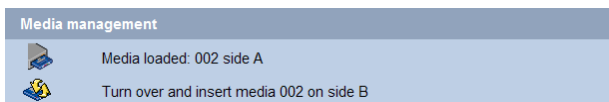
2. The system checks the media and displays:

Media management	
	Media loaded: 002 side A
	No action required

3. The system can continue writing files to the media.

### Turn Media Over (AA Express Only)

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



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 - [Ejecting Media](#) on page 248.
2. Turn media over and re-insert so that the requested media side is loaded.
3. The AA Express checks the media and displays:



Page left intentionally blank

# *Archive Management Software*

## *Chapter 15* *Offline Media Management*

## Storage of Offline Media

### Optical Media Care and Handling

To maintain maximum reliability, the operator should take time to inspect each media cartridge before use, and whenever it is removed from the library.

#### CAUTION



---

*Caution: The media should be in normal room temperature before using. Improper handling or an inappropriate environment can damage the media.*

---

To ensure continued reliability:

- Do not carry media loosely (for example, in a box or basket). Media should be carefully and securely packed for transport.
- Do not load damaged magazines into a drive or a library. Damaged magazines can interfere with load/unload reliability.
- Never remove a tray from a magazine or touch the disk. Removing trays from the protective magazine could cause damage to both the tray and media.
- Do not expose the magazines to moisture.
- Do not expose the magazines to excessive heat (permissible temperature range is 5 to 55°C).

### NETArchive and UDO Media

When media is not in the Library 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 cartridge should not be opened manually as this exposes the media to potential contaminants.*

---

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

Alliance recommends that the cartridge be stored in the plastic sleeve in which it was supplied and in accordance with the following temperature and humidity limits.

*Table 1: Optical media operating and storage conditions*

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

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

## When to Offline Media

For media to be eligible for Offline Media Management (OMM):

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

or

- The media must be in a secondary media pool that is designated as an **Open Offline** media pool - see [Viewing and Editing Volume Properties](#) on page 130.

or

- The media has been selected for offline via the media management user interface ([to select for offline - show all media that are candidates for offline](#). on page 152).

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

## How to Offline Closed Media

### Offlining NETArchive Closed Media with the NETArchive AMS Web Interface

When the Web Interface advises that media is eligible for OMM (Storage- Media closed medial category), see [Removing Media from the NETArchive](#) on page 144 for instructions on how to remove media from the NETArchive library.

### Offlining Closed UDO Media with the Archive Appliance Keypad Interface

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

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

```
Archive Appliance
      Add disk
SEL NEXT PREV ESC
```

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

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

```
Archive Appliance
      OFFline disk
SEL NEXT PREV ESC
```

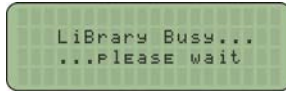
3. Press **sel**.
4. Press **next** or **prev** to select the offline strategy: user or policy selection.

```
Archive Appliance
      OFFline disk:
      user selected
SEL NEXT PREV ESC
```

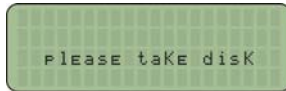
or

```
Archive Appliance
      OFFline disk:
      Policy selected
SEL NEXT PREV ESC
```

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



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



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

## How to Offline Closed Media

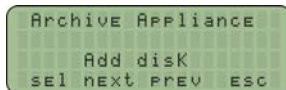
### Offlining NETArchive Open Media with the NETArchive AMS Web Interface

When the Web Interface advises that media is eligible for OMM (Storage - Media closed media category), see [Removing Media from the NETArchive](#) on page 144 for instructions on how to remove media from the NETArchive library.

### Offlining Open UDO Media with the Archive Appliance Keypad Interface

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

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



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

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

```
Archive Appliance
Offline Open disk
SEL next PREV ESC
```

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

```
LiBrary Busy...
...Please wait
```

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

```
PLEASE taKE disk
```

Remove the disk and store in accordance with [Storage of Offline Media](#) on page 286.



## Open Offline Media

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

---

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

---

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

### Storing Open Offline Media

Open offline media should be stored separately from closed offline media at the offsite storage location to ensure that closed media is not incorrectly returned to the library instead of the open offline media.

### Identifying Open Offline Media

Open offline media can be identified on the **Storage - Offline Media** page of the web interface by a tick in the **Open** field for the media. The barcode can then be obtained and the correct media selected at the offsite storage location.

### Returning Open Offline Media

Open offline media is returned to the library using the same procedure as for closed offline media (see ["Returning Offline Media" on page 293](#)).

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

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

---

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

---

#### Updating Open Offline Media

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

1. Return the open offline media to the library (see [“Returning Offline Media” on page 293](#)).
2. Add any blank media if no spare media are available.
3. Return any closed offline media for recall.
4. Check that all **CopyMig** system jobs have completed.
5. Offline any closed media (see [How to Offline Closed Media](#) on page 288).
6. Offline the open media (see [“How to Offline Closed Media” on page 289](#)).
7. Return the open offline media to the remote storage location ensuring it is stored separately from any closed offline media.

## Offline Media Return Requests

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

When a request is received, it will detail the barcode of the required piece of media (**Storage - Media Requests**).

---

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

---

### Returning Offline Media

#### Returning Offline Media to the NETArchive

To return media to the NETArchive library, see section [Adding Media to the NETArchive](#) for instructions on how to add media to the NETArchive library.

#### Returning Offline Media to the Archive Appliance

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

- [Via the Mailslot](#) - if a small amount of media is to be returned
- [Via Direct Slot Access](#) - if a large amount of media is to be returned.

##### [Via the Mailslot](#)

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

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

```
Archive Appliance
  Add disk
sel next PREV ESC
```

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

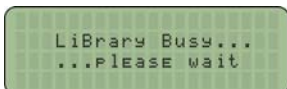
```
Archive Appliance
  Add disk:
  Add Data Disk
sel next PREV ESC
```

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

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



- The library keypad will display:



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

#### Via Direct Slot Access

#### WARNING



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

### AA16, AA32, AA80 and AA174 Models

#### Removing the Library Side Panel

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

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

#### Returning Media

Referring to the slot map appropriate for the Archive Appliance model, see [page 296](#), return the offlined media to the lowest numbered available and unassigned slots.

### *Refitting the Library Side Panel*

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

### **AA238, AA438 and AA638 Models**

To return offlined media via direct slot access:

1. Using the Web interface, shut down the Archive Appliance.
2. Open the library rear door.
3. Referring to the slot map on [page 303](#), return the offlined media to the lowest numbered available and unassigned slots.
4. Restart the Archive Appliance. The Archive Appliance will rescan the contents of the library and update its inventory.

## Library Slot Maps

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

**WARNING**



---

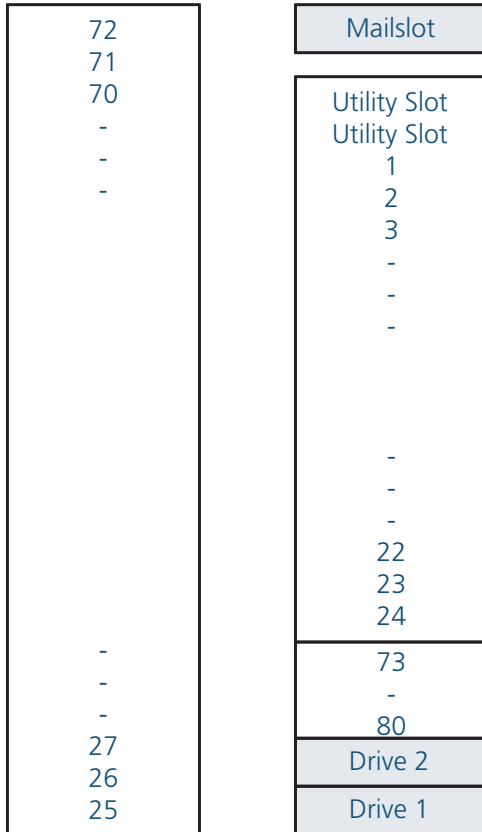
*Warning: Media must not be inserted into the utility slots, as these are used by the Appliance to rotate media.*

---

## AA16/32 Appliance

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

## AA80 (2 drive) Appliance





## AA80 (4 drive) Appliance

72	Mailslot
71	Utility Slot
70	Utility Slot
-	1
-	2
-	3
	-
	-
	-
	22
	23
	24
-	Drive 4
-	Drive 3
-	Drive 2
27	Drive 1
26	
25	

## AA174 (2 drive) Appliance

158	Mailslot
157	
156	Utility Slot
-	Utility Slot
-	1
-	2
	3
	-
	-
	-
	-
	59
	61
	62
	159
	-
	-
	174
	Drive 2
65	Drive 1
64	
63	

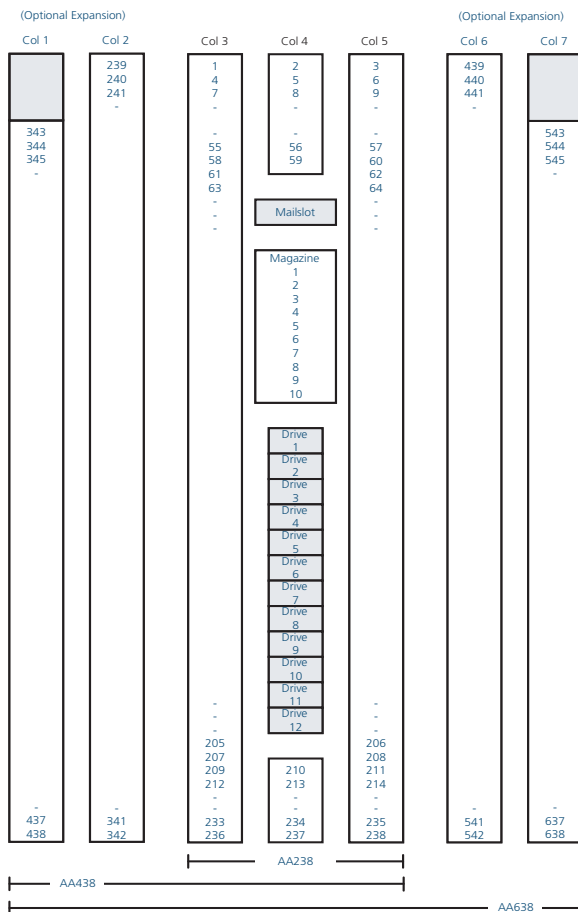
## AA174 (4 drive) Appliance

158	Mailslot
157	
156	Utility Slot
-	Utility Slot
-	1
-	2
	3
	-
	-
	-
	-
	59
	61
	62
	159
	-
	166
-	Drive 4
-	Drive 3
-	Drive 2
65	Drive 1
64	
63	

## AA174 (6 drive) Appliance

158	Mailslot
157	
156	Utility Slot
-	Utility Slot
-	1
-	2
	3
	-
	-
	-
	-
	59
	61
	62
	Drive 6
	Drive 5
-	Drive 4
-	Drive 3
-	Drive 2
65	Drive 1
64	
63	

## AA238, AA438 and AA638 Appliances





# *Archive Management Software*

## *Chapter 16*

### *Offline Media Management with the AAE*

## Storage of Offline Media

When media is not in the Archive Appliance Express, 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 it exposes the media to potential contaminants.*

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

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

*Table 1: UDO operating and storage conditions*

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

*Note: Alliance recommend the use of a media rack, such as those produced by Engineered Data Products ([www.edp-usa.com](http://www.edp-usa.com) or [www.edpeurope.com](http://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 (the 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.

			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 AA Express barcode label number associated with a piece of media is unique.*

---

# *Archive Management Software*

## *Chapter 17*

### *Glossary of Terms*

## Glossary of Terms

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

*Table 17-1: Term and their meaning*

<b>Term</b>	<b>Meaning</b>
ACL	Access Control Lists
Archive	An archive is a set of system resources allocated for the storage of data.
AA	Archive Appliance
AAE	Archive Appliance Express
AMS	Archive Management Software
BBU	Battery backup unit
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.
DN	Domain/Distinguished Name

Table 17-1: Term and their meaning

Term	Meaning
DNS	Domain Name Service - Translates meaningful domain names into IP addresses for network communication.
Fibre Channel	Utilized with the NETArchive Enterprise solution for high speed communications with library and drives from the server.
Ethernet	A standard for sending data packets across networks.
FSC	File System Catalog.
FTP	File Transfer Protocol - a protocol used for transferring data files across a TCP/IP network.
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.
HSM	Hierarchical Storage Management

Table 17-1: Term and their meaning

Term	Meaning
HTML	HyperText Markup Language - The text-based language used to transmit web pages for interpretation by browser programs.
IP	Internet protocol - a data-oriented protocol used for communicating data across a network.
IP Address	Internet Protocol Address uniquely identifies the Appliance on the TCP/IP network.
LAN	A Local Area Network is a computer network covering a small geographic area.
Migration	Moving files from the Appliance's RAID storage volume to optical media.
MTA	Media Transport Assembly
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.

Table 17-1: Term and their meaning

Term	Meaning
Operating system	A program that manages system resources and provides a user interface and an application interface, making it possible for programs to run.
OMM	Offline Media Management
OU	Organization unit
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 optical media back to the RAID storage volume.
Resync	Following a single disk RAID failure, data on the remaining operational disk(s) is used to rebuild the data set on a replacement disk.
RMDB	Resource management database
SATA	Serial Advanced Technology Attachment - a computer bus technology designed for transfer of data to and from hard disks and optical drives.

Table 17-1: Term and their meaning

Term	Meaning
SCSI	Small Computer System Interface - a set of standards for physically connecting and transferring data between computers and peripheral devices.
Server	A program which responds to clients requests, which are generally transmitted over a network.
Sequence Number	The Appliance assigns a unique sequence number to each piece of optical media during initialization.
Shutter	Spring-loaded door protecting the surface of the optical media.
SMB	Server Message Block
SMS	Storage Management System
SMTP	Simple mail transfer protocol - The de-facto standard for e-mail transmissions across the Internet.
SNMP	Simple Network Management Protocol - Used by network management systems to monitor network-attached devices for conditions that warrant administrative attention.
SSH	Secure Shell, a protocol that allows data to be transferred securely between two hosts.
SSD	Solid State Drive
SSM	Storage Space Manager



Table 17-1: Term and their meaning

Term	Meaning
Storage Volume	Dedicated storage area on the Appliance RAID where user files are stored before being moved to optical 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	Uninterrupted Power Supply - A device which maintains a continuous supply of electric power to the Archive Appliance by supplying power from a separate source (usually a battery) when mains power is not available.
UDO	Ultra Density Optical - Alliance's optical disk format designed for high-density data storage.
VPD	Vital Product Data
WINS	Windows Internet Naming Service
WORM	Write-once, read many - storage media that can only be written to once, but read from multiple times.



Page left intentionally blank

## **Contact details**

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

### **Sales**

email: [sales@astiusa.com](mailto:sales@astiusa.com)  
web: [www.astiusa.com](http://www.astiusa.com) /  
[www.plasmon.com](http://www.plasmon.com)

Tel: 719.593.7900  
Fax: 719.593.4164

### **Support**

email: [support@astiusa.com](mailto:support@astiusa.com)

Tel: 877.585.6793 / 719.593.4437  
Fax: 719.593.4164