

# Archive Management Software

## Product Release Notes

Release Details	
Release Name	Archive Management Software (AMS)
Release Note Number	17
Release Version	5.00.17 (MD5: 6383d52219faf96a5321cbaba009f64d)
Software Release Date	June 10 <sup>th</sup> , 2014
License Release Date	June 10 <sup>th</sup> , 2014, 12:00:00 UTC
Release Type	Feature Release
UDO Drive Firmware Version	UDO1 U06C and UDO2 W06D H07 and G07 (Midrange-Gx) G05e/H06e/6.40
Documentation Version	Software Upgrade Guide - 810-103029-05 Administration Guide - 810-102532-06 Service Manual - 800-103405-02
Supported Platforms	SuperMicro PDSM4, PDSM4+ and SuperMicro X8SI6-F

AMS 5.0 - Product Enhancements	
New Feature/Enhancement	Description/Benefit
Archive to Cloud (Amazon S3)	AMS now offers Cloud Integrated Storage Support. Archive data may be migrated to Cloud storage, optical media, or both. The user interface has been enhanced to manage Cloud provider accounts (initially Amazon only), show cloud status and link a cloud provider to specific archives defined by the user. Each archive can be linked to only one cloud provider. Full recovery support is provided in which the AMS will automatically synchronize with the cloud account.
Encryption key management	Archive Data (files) can now be encrypted using a FIPS compliant key generation and encryption software library. Keys are generated when required and are protected to either a special cloud account or on the CIFS backup share. For the protection of cloud account passwords and file encryption keys, symmetrical encryption wrapping keys at the Appliance and Archive Volume levels are employed to encrypt this data, providing compliant key management and the ultimate level of protection.
FIPS compliancy	The Archive Management Software (AMS) uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1747) running on a Linux 3.2 platform per FIPS 140-2 Implementation as per Guidance section G.5 guidelines.
Backup option to internal SSD	With select library models, a second SSD is now available in the E12 which can be configured as a backup device.
Boot image backup	A boot image can be created from either 'Normal' or 'Maintenance mode'.
Mechanism for preventing backup from running.	Creating the <code>'/var/opt/ssm/lock/prohibit_backup'</code> file will prevent the backup from running. This option should be utilized only after consulting ASTI Technical Support.

<b>Cloud integration support tool</b>	A new ssmcloud command utility has been provided to assist in troubleshooting cloud integration issues, including encryption key backups.
<b>Key management support tool</b>	New ssmkey and ssmrestorekeypages command utilities have been provided to assist in viewing the key database status and troubleshooting encryption key database or encryption key cache related issues.
<b>EDAC support</b>	Error Detection And Correction has been added to prevent hardware/memory errors from causing data corruption.
<b>Trigger logs for specific UDO drive errors</b>	UDO drive error logs are now written out when specific SCSI errors are encountered before any power off/ power on cycle is required.
<b>Upgrade of OS to latest level</b>	The AMS Linux kernel has been upgraded to level 3.2.54 with SMP support, along with CentOS 6.2 and Samba 3.6.19
<b>Feature License</b>	Product licensing support has been added for Replication capacity, Cloud and encryption license. Replication quota is enforced by tracking the amount of data replicated. All information is tracked in a secured data store.
<b>In SCP in maintenance mode</b>	Allow files to be copied onto the AA RAID in maintenance mode.
<b>Most Recently Closed OMM policy</b>	Added new offline media management policy option to offline the most recently closed media. This facilitates working in conjunction with applications that retain a copy of the most recently utilized archive data on tier-1 storage to minimize recall times.
<b>Drive cleaning function</b>	UDO drive can be marked for cleaning. When the cleaning cartridge is added through the library mail slot using the 'Add media' key pad option, the cleaning process is automated. Once completed, the cleaning cartridge is then ejected from the library.
<b>ssmcheck progress</b>	File progress count is now periodically written to ssm.log (after each 100,000 files).
<b>Set drive module into service mode on Ent-G library</b>	A drive and its module can be switched into and out of service mode from the Drive UI page.
<b>Show approximate number of files on volume page</b>	The approximate number of files written to the archive volume is now shown on the Volume page under the 'Archive' tab. It is located next to "Total Data Archived" and displayed in brackets. When migrating data to the cloud, this is useful to see that all data has been migrated.
<b>NFS 4.0 support</b>	NFS service for Linux has been upgraded to the last level.
<b>Always assign RW media to backup pool</b>	RW media can only be used as a backup medium. It requires manual intervention to assign RW media to an archive. A new command has been provided to create a RW test archive - create_production_archive.
<b>New log to track SMART errors for SATA drives</b>	Separate log file /var/log/disk_error.csv will be created if significant SATA drive errors occur.
<b>Add option to create secure log bundle</b>	Log bundles are created without any information that could compromise security.
<b>Notification if file (inode) limit is exceeded</b>	As the archive approaches 100 million files an email notification is sent to alert the customer that the archive has reach its scalability limits. Archives that contain more than 100 million files can suffer degraded performance.
<b>Full replication scan option</b>	When replication is started from the UI an option is presented to scan the entire archive. This is to allow user driven verification of the replication status of every file.

<b>Self-test per archive</b>	Allow selected archives to be self-tested for migration/recall.
<b>Add file system option to repair without deleting journal/log</b>	If a file system cannot be mounted or repaired it is now possible, as a final resort, to delete the file system journal. However, taking this action will result in some loss of files recently written.
<b>Add "Remove SCSI log" action button to UI</b>	SCSI logs can now be purged from the "Diagnostics - System Information (Log Files)" page (with the most recent log being retained).
<b>Allow library to be enabled/disabled through UI</b>	Action button is now available to disable the library.
<b>UI rebrand</b>	Color scheme and minor look and feel changes have been made to the UI in line with ASTI product branding.
<b>Confirmation prompt if volumes exceed 12 instances</b>	A warning message will appear if the user attempts to create more than 12 archives. This exceeds the general recommended scalability limit. To note, the total number of archives is very much dependent on a number of factors which include the total number of files and total activity levels.
<b>Create archive checks for matching media type in library</b>	If the media in the library does not match the media type specified, the user cannot create archives that utilize that media. This is to ensure that archives are not added that cannot be migrated.
<b>Multi-archive support on AAE platform</b>	The AAE will now support one optical-based archive along with multiple cloud based archives.

## AMS 5.0 – Software Changes

	Change ID	Category	Descriptive Notes
1	1100	Backup/ Recovery	Significant scalability and performance improvements to ssm_fsc -c have been made. Previously, the checker could run out of memory and/or could take hours to run. Additionally, some additional data integrity checks have been added.
2	1183	Cloud	Updated self test to add verification of the encryption keystore integrity and functionality.
3	1182		Update status page to reflect cloud agent status.
4	1179		Include cloud enable option in Archive configuration page
5	1176		Added cloud service to service page.
6	1249	Encryption & Keys	Key Restore can be started from "Key Recovery" menu option
7	939	Install/Startup	Data partitions on a system must be of same size even if the disk sizes are different.
8	1188	Media Management	To handle RMDB growth as it can become very large over time; a database cleanup/compaction is performed on SSM restarts.
9	1364	Migration/Recall	SSM could previous not handle very large UID. This has now been resolved.

10	1122		Occasionally entries in the HSM active list did not get removed causing the active list table to grow very large. If a file cannot be located on the file system, any associated file events are now removed and the administrator is notified.
11	965		Associative recall default has been change to off. After analysis, there appears to be no benefit in running associative recall.
12	1320	Network	NTPD security vulnerability has been fixed and NTPD service has been upgraded.
13	1378		Gateway was not set if AMS is running with as a DHCP client.
14	911	Notification and Logging	A link to ASTI website has been added to the dirty media message.
15	847		The default log bundle size has been changed to 7 days.
16	1321	OS/Kernel	ACL propagation now resumes after reboot and power failure rather than restarting from the beginning.
17	1044		Remove support for filesystem quotas.
18	1142	Replication	System folders are excluded from replication.
19	1207	Security	Enhanced UDOGuard interface to include Master/Archive key management. The UI menu under Data Protection has been renamed to "Security".
20	1116		Added progress indication in ACL propagation in "/dev/shm/acl_propagate"
21	1382		An Openssl library vulnerable related to the Heartbleed bug has been addressed. The heartbeat has been disabled. AMS was never exposed to this bug, but the heart beat feature has been disabled anyway to ensure security.
22	1231	Support and manufacturing	License keys recovery has been added to RestoreFlashContents.
23	1229		Add script to determine SNAZ OS version on system volume (check_os_version). This is to be run from maintenance mode and determines the OS version in the least intrusive way possible.
24	967	UI Look n' Feel	Internet Explorer version 8 tooltip issues such as clipped by edge of page have been addressed
25	983	Wizard	Minor improvements to Wizard interface including automatic reconnection after reboot.

## Known issues

1. **Recalls from cloud storage may time out if the network bandwidth is not sufficient** to download the migration container file. This is a current limitation but will be addressed in a future release.
2. While recalls from the cloud are occurring, depending on the available network bandwidth, the CIFS connection will block for longer than from optical media,. This in turn can result in a timeout **of concurrent write operations** from the same client.
3. If the Master Wrapping Key has been restored, it is necessary to restart SSM as the cloud service needs to be re-initialised and validated.
4. When the backup target is changed (UDO / Network Share), it is necessary to restart the SSM service for the change to take effect.
5. In the highly unlikely event that imported key pages are missing from the key page cache **WITHIN** the range of key pages (i.e. not the first or last key page), the key recovery will report this and stop. In this event, the key recovery needs to be restarted. If it fails again, the key recovery should be restarted again and the cycle should continue until the recovery completes.

## Installation Note

New users should refer to the “Archive Appliance Installation Guide” (810-103403-00 Rev B) for setup instructions.

Users who are upgrading from an earlier release should refer to the “Archive Appliance System Upgrade Guide” (810-103029-05) for upgrade instructions.

### Supported Upgrade Paths

Users can upgrade to AA 5.0 from these earlier releases:

- 4.11.39 (All Patches) – see note below
- 4.12.43 (All Patches) – see note below
- 4.20.23 (All Patches) – see note below
- 4.20.31 (All Patches) – will automatically reboot after initial install for second phase

**Note:** The 5.0 upgrade is performed in two phases. After the first phase is completed the system **MUST be rebooted into maintenance mode manually**. Failing to reboot into maintenance mode will break the ‘Normal’ boot mode.