



File Archiving software

Frequently Asked Questions (FAQ)

I. Product Overview	4
What is File Archiving software?	4
Does HP develop File Archiving software?.....	5
Where can I find current datasheets, QuickSpecs and sales collateral for FAs 2.5?	5
How is File Archiving software licensed?	5
What are the advantages of using File Archiving software?	5
What are the major features of File Archiving software?.....	5
What do we mean by File Archiving software “releasing” a file?	6
What types of user interfaces does File Archiving software provide?	7
II. System Requirements	8
What are the hardware platforms that are supported by File Archiving software?	8
What is the minimum hardware system requirements for File Archiving software?	8
What is the recommended hardware system requirement for File Archiving software?.....	8
What operating systems are supported by File Archiving software?	8
What type of archives are supported by File Archive Software?	9
What are the third party tools supported by File Archiving software?.....	9
Where can I find the current supportability matrix for File Archiving software?	9
What are some of File Archiving software limitations?	10
III. Installation.....	11
What is the File Archiving software installation wizard based on?.....	11
What are the requirements for upgrading to File Archiving 2.5?.....	11
What are some of the configurations supported by File Archiving software?	11
What is a major File Archiving software release?	11
What is a File Archiving software maintenance or minor release?	12
What is a File Archiving software hotfix?	12
What user account should I use to install File Archiving software?.....	12
What are the services that will be created during an installation?	13
What should I use as a Technical User?	13
Is File Archiving software customer installable?.....	13
Where can I find the installation instructions?	13
How are NFS shares supported?.....	14
IV. Licensing.....	16
What is File Archiving software license based on?	16
What type of licenses are available in File Archiving software?.....	17
What type of license do you have?	18

What type of license do I choose during license registration?.....	18
What IP address do I choose during license registration?	20
Where do I add my license key?.....	20
How do I install a File Archiving software license?.....	21
Why isn't my license being detected by File Archiving software?	22
V. Configuration.....	24
What are the different archive scenarios supported by File Archiving software?	24
Does File Archiving software perform replications?.....	25
Is there a way to maintain folder structure between source and archive target?	25
Is there a way to simulate a policy before executing it?.....	25
What are the files with extension *.000 and *.001 in the archive target?	26
Is there a way to limit the amount of revision history of a file in the archive?	26
What do the "Ignore Security" & "Data Stream Only" options mean?	26
What is the "Ignore system name or serial for storage descriptor creation" option?	27
How does File Archiving software work in a cluster configuration?	28
How do I install File Archiving software in a Microsoft Cluster Server?	31
How do I upgrade File Archiving software in a Microsoft Cluster Server?.....	32
How do I uninstall File Archiving software on a Microsoft Cluster configuration?.....	32
How do I configure an archive in a Cluster environment?.....	32
How do I configure my File Archive software managed volumes in a cluster?.....	33
How do I migrate a FAs cluster from Windows 2003 to Windows 2008?.....	33
VI. Active File Management	34
What happens if more archived data exists than there is available free space on a managed volume?.....	34
Are files searchable from the users' PC as well as by administrator on the source?.....	35
Is there a way to maintain folder structure between source and archive target?	35
Can I set granular schedules for when archiving take place?.....	35
How does File Archiving software policy work?	36
What happens at each volume watermarks?	37
What happens to the FAs column properties in Window Explorer?	37
VII. Backup and Restore	39
What are the requirements for a backup application to work with FAs?.....	39
What are some backup strategies for managed volume(s) and archive(s)?	39
What is the best practice when using FAs and Data Protector?	42
What is the best practice when using FAs and HP Storage Mirroring?.....	42
VIII. Downgrading.....	46
Can File Archiving software be downgraded to any version?.....	46
How do I check the Extended Attributes of a file?.....	47
How do I check the reparse tag information of a file?.....	47
What do I do when I receive an error code 0x00010019?	47
IX. Data Relocation	49
How do I relocate my managed data from one FAs server to another?.....	49
X. Window Registry Settings	52
Where can I find the File Archiving software registry settings?	52
How do I change the log settings to debug using the registry?	52
How do I control the number of threads used by FAs?	55

XI. File Archiving software Terminology	56
What is an Archive?	56
What is a managed file?	56
What is file policy?	56
What is volume policy?	56
What is metadata?	57
What is inactive data?	57
What is a managed volume?	57
What is migration?	57
What is releasing a file?	57
What is recalling a file?	58
What is a stub file?	58
What is remote storage adapter (RSA)?	58
What is activation of metadata?	58

I. Product Overview

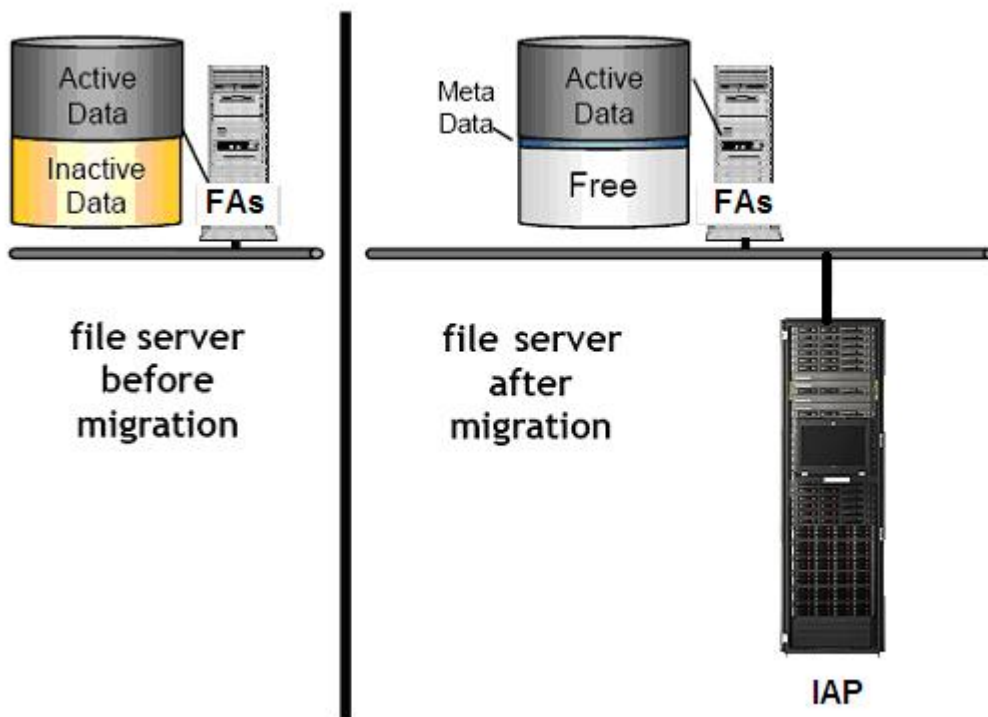
NOTE: Please be aware that although HP refers to this product as HP File Archiving software, the product itself, its documentation, SKUs and product descriptions are branded HP File Migration Agent.

NOTE: Reference the latest copy of the FAs Administration Guide that is posted on SSO (<http://h71028.www7.hp.com/enterprise/us/en/software/information-management-governance-ediscovery-file-archiving.html>)

What is File Archiving software?

In September 2005, HP launched HP File Migration Agent, or FMA, as a key new product within the Information Management business unit. In October 2007, FMA was re-branded as “HP File Archiving software” or “FAs”.

File Archiving software helps businesses manage growth and complexity of Windows File Servers by migrating inactive or rarely used data to a target archive. When using the HP Integrated Archive Platform (IAP) as the target archive, File Archiving software provides a compelling solution for customer with requirements for long-term file retention (compliance) and content search and retrieval (e-Discovery).



[Back to Top](#)

Does HP develop File Archiving software?

No, HP OEM's File Archiving software from a company named Crossroads. However, File Archiving software is a HP-branded product that is supported directly by HP.

[Back to Top](#)

Where can I find current datasheets, QuickSpecs and sales collateral for FAs 2.5?

Please follow this link: www.hp.com/go/filearchive

[Back to Top](#)

How is File Archiving software licensed?

As a general rule, File Archiving software is licensed per server. When used within a Microsoft cluster, File Archiving software must be licensed for all nodes, both active and passive. There is a special "cluster" license that should be ordered for each server on a cluster node. Capacity-based licensing only applies when migrating files to a non-HP archive (for example, EMC disk). Refer to the FAs QuickSpecs for more information.

[Back to Top](#)

What are the advantages of using File Archiving software?

There are many advantages to using File Archiving software:

- Frees up file servers for storage of active data
- Reduces investment costs for server & storage
- Smaller backup window & shorter restore time
- Improves data protection & access through multiple copies of archived data
- Automatic Online Failover

[Back to Top](#)

What are the major features of File Archiving software?

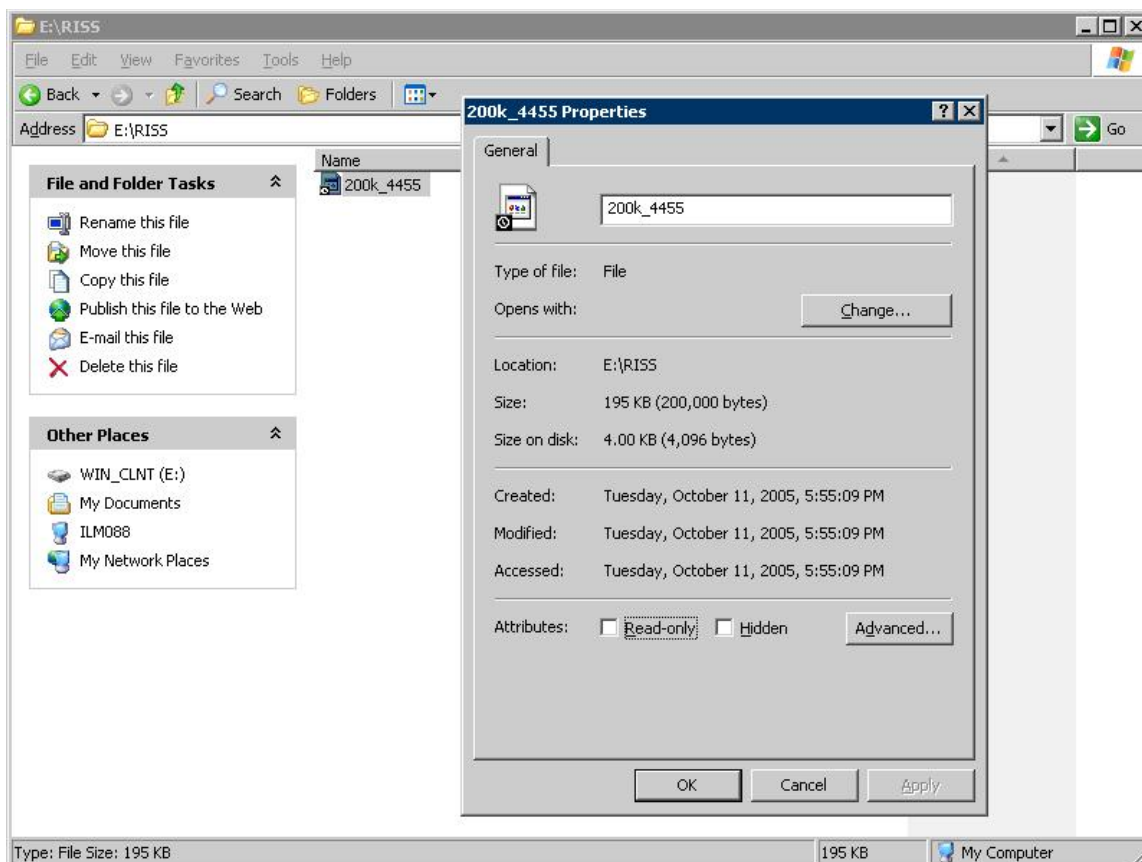
The major features of File Archiving software are:

- Policy-based automated migration of files based on file timestamps, file size, file name or other attributes.
- Policy-based automated release of files based on retention periods.
- High, critical, & low watermark functionality to help control how files are released.
- Automatic & transparent retrieval of files from archive(s).
- Supports migrating multiple copies in parallel to different archiving systems.
- Supports disaster recovery configurations with online failover.
- Microsoft Cluster Server support.

[Back to Top](#)

What do we mean by File Archiving software “releasing” a file?

Releasing a particular file means that File Archiving software deletes and replace the original file (that has been successfully migrated into an archive(s) in the managed volume) with a file-stub. Please refer to [XI. Terminology](#) for more details on a file-stub. To the user, the stub-file appears local. When viewing the properties of a stub-file, however, it is seen that the file size remains intact, but the size of the file on disk has been reduced to 4kbyte as shown below.



Although the release process enhances primary storage efficiency through the creation of stub-files, it does not change the file system structure as a result. A read access on any released file triggers an automatic and transparent retrieval from the archive.

[Back to Top](#)

What types of user interfaces does File Archiving software provide?

File Archiving software can be configured through the following interfaces:

- File Archiving Configuration Utility (Policy Manager)
- Command Line Interface
- File Archiving Windows Explorer

[Back to Top](#)

II. System Requirements

What are the hardware platforms that are supported by File Archiving software?

Please refer to the compatibility matrix for all supportability related questions. This document can be found using the following links:

http://spock.corp.hp.com/Pages.internal/spock2Html.aspx?htmlFile=sw_ilm.internal.html#fas
<http://www.hp.com/storage/spock>

[Back to Top](#)

What is the minimum hardware system requirements for File Archiving software?

Please refer to the compatibility matrix for all supportability related questions. This document can be found using the following links:

http://spock.corp.hp.com/Pages.internal/spock2Html.aspx?htmlFile=sw_ilm.internal.html#fas
<http://www.hp.com/storage/spock>

[Back to Top](#)

What is the recommended hardware system requirement for File Archiving software?

Please refer to the compatibility matrix for all supportability related questions. This document can be found using the following links:

http://spock.corp.hp.com/Pages.internal/spock2Html.aspx?htmlFile=sw_ilm.internal.html#fas
<http://www.hp.com/storage/spock>

[Back to Top](#)

What operating systems are supported by File Archiving software?

Please refer to the compatibility matrix for all supportability related questions. This document can be found using the following links:

http://spock.corp.hp.com/Pages.internal/spock2Html.aspx?htmlFile=sw_ilm.internal.html#fas
<http://www.hp.com/storage/spock>

[Back to Top](#)

What type of archives are supported by File Archive Software?

File Archiving software currently supports only the following archive devices:

- HP Integrated Archive Platform (formerly known as RISS)
 - IAP version 1.6.0 & 1.6.1
 - IAP version 2.0
- CIFS-Based NAS Appliance
 - FAs 2.5 supports any CIFS based NAS Appliance that can run in FAs supported Operating Systems.
- HP File System Extender
 - FAs 2.5 supports archiving into HP FSE

Note: FSE is an obsolete product. The support listed here is for the installed base customers of FSE who use FAs as a data mover tool.

[Back to Top](#)

What are the third party tools supported by File Archiving software?

Currently, File Archiving software supports a limited number of Backup and Anti-Virus tools. The list of third party tools support by File Archiving software can be found using the links below:

http://spock.corp.hp.com/Pages.internal/spock2Html.aspx?htmlFile=sw_ilm.internal.html#fas

<http://www.hp.com/storage/spock>

[Back to Top](#)

Where can I find the current supportability matrix for File Archiving software?

http://spock.corp.hp.com/Pages.internal/spock2Html.aspx?htmlFile=sw_ilm.internal.html#fas

<http://www.hp.com/storage/spock>

[Back to Top](#)

What are some of File Archiving software limitations?

Maximum number of volumes (display)	128
Maximum number of FAs-managed volumes	80
Maximum number of archives	255
Maximum path length (characters)	1024
Maximum file size (NTFS)	~16 terabytes
Maximum volume size (NTFS)	~256 terabytes
Files/Directories per volume (NTFS)	4,294,967,295
Maximum number of FAs policies	Unlimited (Less than 1000 active policies recommended)
Maximum number of nodes per cluster	8 homogeneous nodes per cluster configuration

[Back to Top](#)

III. Installation

What is the File Archiving software installation wizard based on?

File Archiving software installation is based on InstallShield (Version 10.5), which acts like a Framework Microsoft Installer (MSI).

[Back to Top](#)

What are the requirements for upgrading to File Archiving 2.5?

The following upgrade path is supported when upgrading to FAs 2.5:

- 2.1.x→2.5 - To upgrade from 2.1.x, you must first upgrade to 2.1.11, then upgrade to 2.2.7, and then upgrade to 2.5.
- 2.2.x→2.5 - To upgrade from 2.2.x, you must first upgrade to 2.2.7 and then upgrade to 2.5.

[Back to Top](#)

What are some of the configurations supported by File Archiving software?

File Archiving software only support two configurations:

- Stand alone server
- Microsoft Cluster Server configuration

Note: File Archiving software cannot manage volumes that contain the operating system (normally C:\ Drive) and quorum disks.

[Back to Top](#)

What is a major File Archiving software release?

A major File Archiving software release contains new features and functionality that

did not exist in previous versions. It contains a complete installation image that can normally be upgraded from previous versions. A major release occurs when one or more of the below items apply:

- Major new functionality
- Product structure changes
- Architectural changes

[Back to Top](#)

What is a File Archiving software maintenance or minor release?

A maintenance release may contain bug fixes or new supportability. It does not contain any new features or new functionality. It also comes with a complete installation image that can be upgraded from previous versions. The criteria of a minor release is as follows:

- New supportability
- Software brought up to current patch level (bug fixes)
- Compatibility with lower versions of the same major release and is a superset of the major release functionality

[Back to Top](#)

What is a File Archiving software hotfix?

A hotfix is a software fix for a specific problem that was encountered in the field. It is normally based on a defect ticket number and contains dedicated files that need to be manually replaced. Hotfixes always come with installation instructions. Hotfixes are customer-specific and should not be installed unless specified by HP support.

[Back to Top](#)

What user account should I use to install File Archiving software?

HP recommends that you install File Archiving software on a server using an Administrator or a domain Administrator account. If this is not possible, please use a user that is in the Administrative or Domain Administrative group. This eliminates manual interventions to grant read and write access to the selected CIFS storage.

[Back to Top](#)

What are the services created during an installation?

There are three services created during FAs installation:

- “HP File Migration Agent AFM service”
- “HP File Agent config service”
- “HP File Migration Agent service”

In a stand alone FAs server, all services are configured to startup “Automatic” and in a “Started” status. In a cluster configuration, after running the cluster wizard, the HP File Migration Agent config service is set to “Manual” mode, and is only in “Started” status on the Active node. If you have several active FAs nodes, you must start the HP File Migration Agent config service manually. Upon a failover, this service is started on the failover node automatically.

[Back to Top](#)

What should I use as a Technical User?

If you install the File Archiving software using an Administrator or Domain Administrator, you can select local system account. You can also use an account that has read and write privileges to the CIFS archive that you wish to access.

[Back to Top](#)

Is File Archiving software customer installable?

This product is customer installable; However, HP Professional Services Organization (PSO) services offers a suite of scalable, clearly defined service engagements that provide product and solution deployments consistent with HP’s quality standards. If you need or would prefer HP to handle this implementation, providing you with improved speed and confidence in IT infrastructure deployments while preparing your IT staff and processes for operational success, please contact the HP Professional Services Organization (PSO) via one of the following three email addresses depending on your region: IMServices.EMEA@hp.com, IMServices.Americas@hp.com, or IMServices.APJ@hp.com.

[Back to Top](#)

Where can I find the installation instructions?

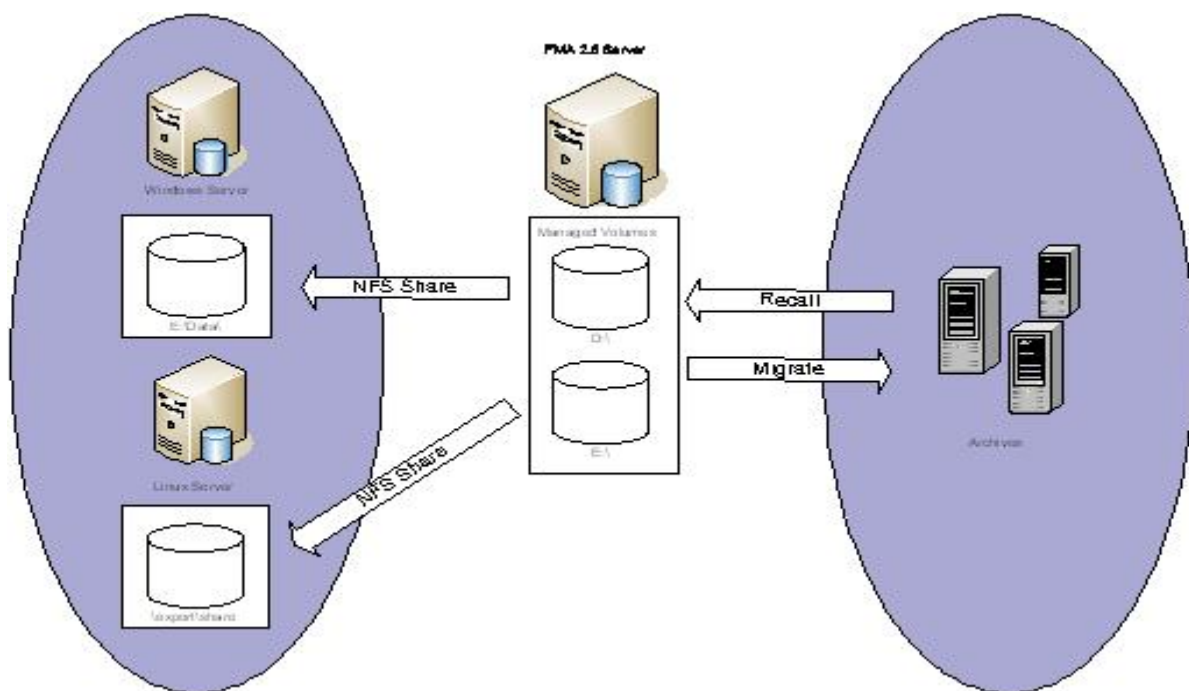
The step-by-step installation instructions can be found in the *File Archiving software*

Administration Guide that comes with your installation image. It contains steps on how to install standalone and cluster configurations.

[Back to Top](#)

How are NFS shares supported?

Managed volumes can be shared out through NFS in order to extend the value proposition of FAs to Unix applications. The following explains the recommended configuration:



File Archiving software supports the sharing of managed volume(s) to Windows and UNIX operating systems.

When sharing with Windows operating systems, the FAs system needs to have the NFS client installed. The system that uses the NFS share will need the NFS server installed and running. Both systems require the TCP/IP package installed.

When sharing with UNIX operating system, the following services need to be installed on the FAs system (depending on the Windows operating system):

For Windows 2003, the Services for UNIX 2.5 must be installed. You can download the package from the following Microsoft website:

<http://www.microsoft.com/downloads/details.aspx?familyid=896c9688-601b-44f1-81a4-02878ff11778&displaylang=en>

Ensure that the following services are installed and running:

- NFS Client for Windows
- User Name Mapping
- Password Synchronization
- TCP/IP
- File and Printer Sharing for Microsoft Networks
- NWLink NetBios
- NWLink IPX/SPX/NetBIOS Compatible Transport Protocol

After all the services are running, copy the “password” and “group” file from the UNIX system to the FAs system. This is required for the User Name Mapping. When performing User Name Mapping, ensure that the Administrator Group is matched with the root group. Map a super user on the UNIX system to the technical user of the FAs system.

For Windows 2008, the following services need to be installed and running:

- Services for NFS
- Client for NFS
- Subsystem for UNIX-based Application

As Windows 2008 does not have User Name Mapping service available, you must perform the translation using the following options:

- An Active Directory Domain Service that includes UNIX identity to Windows identities.
- Use an existing User Name Mapping server, which is a Windows 2003 server with SFU installed and configured.

To use a User Name Mapping server, enter the IP address of the server in the Service for NFS configuration window. Add the IP address of the Windows 2008 server to the .maphosts file on the User Name Mapping server. The .maphosts file can be found under the directory, C:\WINDOWS\msnfs. After editing the file, perform the mapping as you would in a Windows 2003 environment.

The following limitations applies when using NFS sharing:

- Windows can only handle paths with a maximum length of 260 characters.
- UNIX and Windows systems use different user and group IDs. Therefore, there needs to be a corresponding set of user and group IDs on the UNIX system to the Windows system.

- Windows files with the same name but different capitalization (such as tmp, Tmp, and TMP) are saved in the same directory. The Win32 subsystem recognizes only one of these versions, and it is not possible to determine which version is retrieved.
- The basic naming convention of all files and directory must comply with the Windows standards defined by Microsoft. For more details, please visit the following link:

[http://msdn.microsoft.com/en-us/library/aa365247\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa365247(VS.85).aspx)

- When an NFS volume is shared to a server, FAs does not have control over read access on this volume. FAs is not responsible for any unexpected mass recalls caused by the OS or any third party application installed.

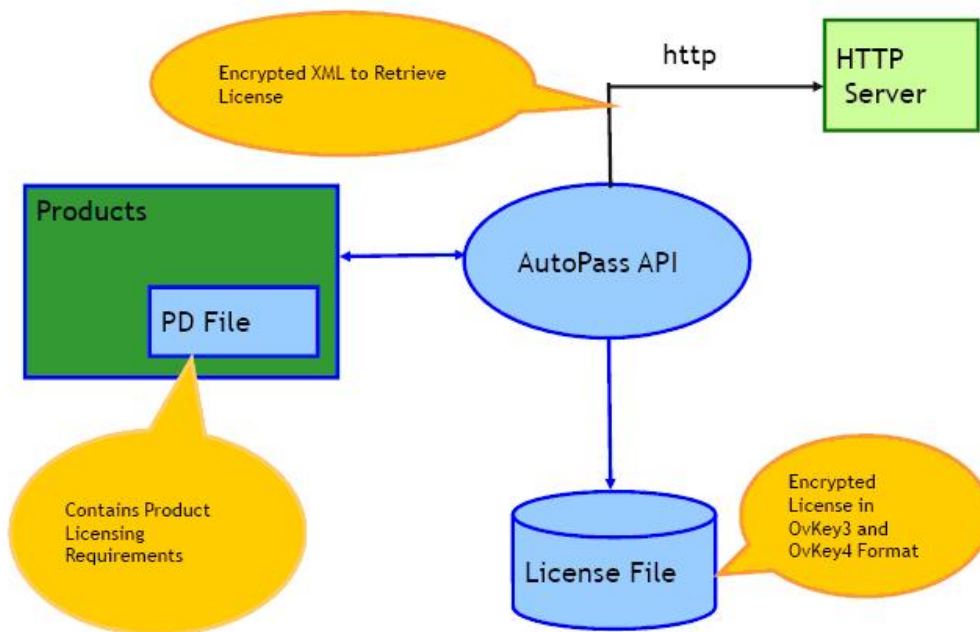
[Back to Top](#)

IV. Licensing

What is File Archiving software license based on?

File Archiving software (version 2.5.2) licensing is based on HP AutoPass version HPOvLic-05.51.066-WinNT4.0-release. The license on the server is checked at 09:00 am system time. Violations of the license are logged and displayed in hsm.log and event viewer logs. There are no functional restrictions for expired licenses.

The high level architecture of AutoPass is shown below:



[Back to Top](#)

What type of licenses are available in File Archiving software?

There are two types of licenses:

1. Instant ON License:
 - Used by the customers while evaluating the product.
 - Installed from the PD File
 - Creates some secret entries in the system to control the License expiration date.
 - After expiration backdating does not enable the license.
 - Valid for 60 days.

2. Permanent License:
 - Retrieved by AutoPass through the Web.
 - Imported to AutoPass
 - Does not expire
 - Can have multiple passwords for FAs and AutoPass aggregates the capacity

[Back to Top](#)

What type of license do you have?

If you just installed the license from the File Archiving software CD, you would have an Instant ON License. In order to obtain a permanent license, use the order number from HP to register your license through <http://www.webware.hp.com>. After registering your license, you immediately get a license key that needs to be installed onto your FAs server.

[Back to Top](#)

What type of license do I choose during license registration?

There are 14 licenses to choose from during registration, and you can only register one license at a time. The licenses with the suffix "A" apply if you ordered the FAs Media Kit, licenses with suffix "AE" apply if you ordered the electronic download version of the software. Please see below:

Select product	Product number	Product name	Product version	Quantity available
<input type="checkbox"/>	Product family: File Migration Agent			
<input type="checkbox"/>	T4275A	HP File Migration Agent LTU HP HW Windows 1 Server	any	473
<input type="checkbox"/>	T4275AAE	HP File Mig Agt E-LTU HP HW Win 1 Server	any	500
<input type="checkbox"/>	T4276A	HP File Migration Agent LTU HP HW Windows Cluster	any	487
<input type="checkbox"/>	T4276AAE	HP File Migr Agt E-LTU HP HW Win Cluster	any	500
<input type="checkbox"/>	T4277A	HP File Migration Agent LTU non-HP HW Win 1 Server	any	496
<input type="checkbox"/>	T4277AAE	HP File Mig Ag E-LTU non-HP HW Win 1 Svr	any	500
<input type="checkbox"/>	T4278A	HP File Migration Agent LTU non-HP HW Win Cluster	any	495
<input type="checkbox"/>	T4278AAE	HP File Mig Ag E-LTU non-HP HW Win Clstr	any	500
<input type="checkbox"/>	T4279A	HP File Migration Agent LTU 100GB to 1TB non-HP HW	any	488
<input type="checkbox"/>	T4279AAE	HP File Mig Ag E-LTU 100GB 1TB non-HP HW	any	499
<input type="checkbox"/>	T4280A	HP File Migration Agent LTU 1TB to 20TB non-HP HW	any	453
<input type="checkbox"/>	T4280AAE	HP File Mig Ag E-LTU 1TB-20TB non-HP HW	any	500
<input type="checkbox"/>	T4281A	HP File Migration Agent LTU 20TB+ non-HP HW	any	490
<input type="checkbox"/>	T4281AAE	HP File Mig Ag E-LTU 20TB+ non-HP HW	any	500
<input type="checkbox"/>	TB114AA	HP File Migration Agent HP Storage Windows Single Server LTU	2.5	500
<input type="checkbox"/>	TB114AAE	HP File Migration Agent HP Storage Windows Single Server E-LTU	2.5	500
<input type="checkbox"/>	TB115AA	HP File Migration Agent HP Storage Windows Cluster LTU	2.5	500
<input type="checkbox"/>	TB115AAE	HP File Migration Agent HP Storage Windows Cluster E-LTU	2.5	500
<input type="checkbox"/>	TB116AA	HP File Migration Agent non-HP Storage Windows Single Server LTU	2.5	500
<input type="checkbox"/>	TB116AAE	HP File Migration Agent non-HP Storage Windows Single Server E-LTU	2.5	500
<input type="checkbox"/>	TB117AA	HP File Migration Agent non-HP Storage Windows Cluster LTU	2.5	500
<input type="checkbox"/>	TB117AAE	HP File Migration Agent non-HP Storage Windows Cluster E-LTU	2.5	500
<input type="checkbox"/>	TB118AA	HP File Migration Agent 100GB Incremental (100GB-1TB) non-HP Storage LTU	2.5	500
<input type="checkbox"/>	TB118AAE	HP File Migration Agent 100GB Incremental (100GB-1TB) non-HP Storage E-LTU	2.5	500
<input type="checkbox"/>	TB119AA	HP File Migration Agent 1TB Incremental (1TB-20TB) non-HP Storage LTU	2.5	500
<input type="checkbox"/>	TB119AAE	HP File Migration Agent 1TB Incremental (1TB-20TB) non-HP Storage E-LTU	2.5	500
<input type="checkbox"/>	TB120AA	HP File Migration Agent 1TB Incremental (20TB+) non-HP Storage LTU	2.5	500
<input type="checkbox"/>	TB120AAE	HP File Migration Agent 1TB Incremental (20TB+) non-HP Storage E-LTU	2.5	500

These licenses consist of different types of licenses, configuration and storage license. Configuration licenses are: TB114AA, TB115AA, TB116AA, TB117AA, TB114AAE, TB115AAE, TB116AAE, and TB117AAE. Storage licenses are: TB118AA, TB119AA, TB120AA, TB118AAE, TB119AAE, TB120AAE.

You can have only one type of configuration license per server, but you can have

multiple storage licenses per server. You can only register one license at a time, which means you have to return to the website once you obtain a license (if you have more than one license).

For the configuration license:

- When using HP hardware, choose between TB114AA or TB114AAE (Stand alone configuration)
-Or-
TB115AA or TB115AAE (Cluster configuration).
- When using non HP hardware, choose between TB116AA or TB116AAE (Stand alone configuration)
-Or-
TB117AA or TB117AAE (Cluster configuration). For a cluster configuration, you would need a different license per node.

For the storage license, you would only select these if you are using non-HP storage for your manage volumes. The different types of storage licenses are fairly trivial and can stack with one another in the license file.

[Back to Top](#)

What IP address do I choose during license registration?

Each File Archiving software license generated is IP address bonded. If you have multiple network connections within your server, the IP address you would use is the primary network port. This applies to both the stand alone and cluster configurations. If you have a cluster configuration, use the primary IP address of each node during registration. File Archiving software does not recognize virtual IP address of a cluster configuration.

[Back to Top](#)

Where do I add my license key?

After you register choose the type of license you want and the IP address, a license key is immediately generated for you. The key needs to be placed in the *LicFile.txt* file as shown below:

```
C:\Program Files\Common Files\Hewlett-Packard\HPOvLic\data  
LicFile.txt
```

You can add the license key below the existing evaluation license. This file should never be left blank, or else FAs will not function at all.

[Back to Top](#)

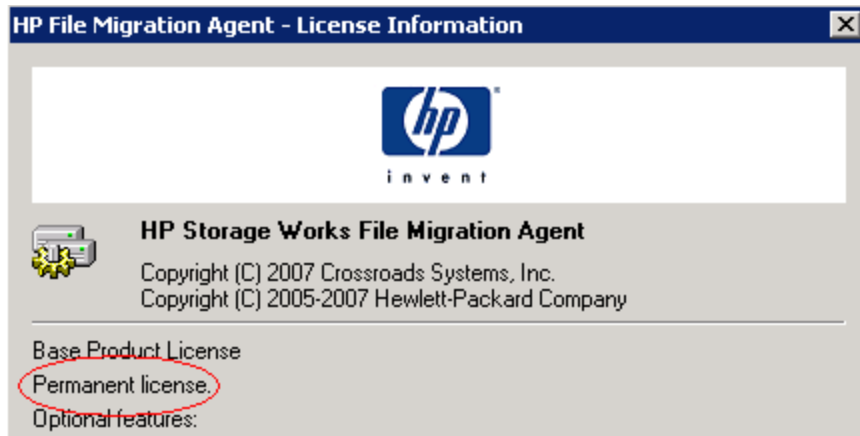
How do I install a File Archiving software license?

To install an FAs license, please follow these instructions:

1. Open a web browser, and enter <http://www.webware.hp.com> to access the HP Password delivery service website.
2. Click the Generate password(s) link in the navigation panel.
3. Enter the order number from the Entitlement Certificate that you received with the product, and click Next.
4. Select the correct license to generate appropriately to your system configuration.
Example #1: For a standalone configuration using HP Hardware, you will select TB114AA or TB114AAE.
Example #2: For a cluster configuration using HP Hardware, you will select TB115AA or TB115AAE.
5. Enter the IP address of the FAs server. Ensure that the IP address you use is the primary IP address of the FAs server. If you have a cluster configuration, using the virtual IP address will not work. You must generate a license for each node in your cluster using the primary IP address of each node. Click Next when you have entered the correct IP address. Repeat this process for each node in your system.
6. Enter your e-mail address and password, and click Sign-In.
NOTE: If this is the first time you are signing in to this website, you must create a password at this time.
7. Enter the appropriate contact information, and click Next.
The Password Certificate appears.
8. Scroll down and copy the license key that appears near the bottom of the certificate.
9. Open the *C:\Program Files\Common Files\Hewlett-Packard\HPOvLic\data\LicFile.txt* file in a text editing application, such as Notepad.
10. On a new line, paste the license key that you copied from the Password Certificate.
Note: It is important to note that you should never delete the license from LicFile.txt. Make backup of this file when you are adding the license.
11. Save and close the LicFile.txt file.
12. Restart the File Migration Agent service.

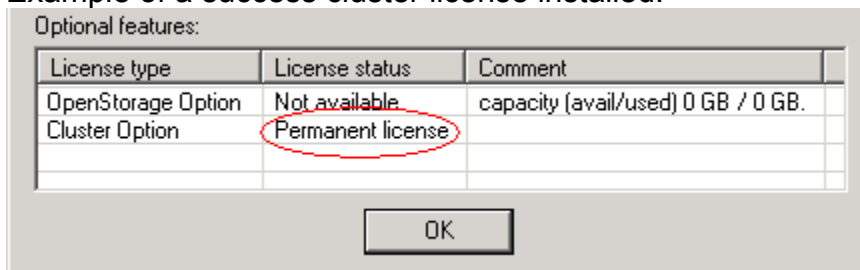
13. Start FAs by selecting Start > Programs > HP StorageWorks File Migration Agent > FMA Configuration.

14. Bring up the HP File Archiving software Configuration Utility, and select License information to verify that your permanent license was entered successfully.



If you have a Cluster license or OpenStorage license, “Permanent license” appears in the Optional features box. Otherwise, “Not available” is shown in the status.

Example of a success cluster license installed.



[Back to Top](#)

Why isn't my license being detected by File Archiving software?

Does “Permanent license” appear in license status after you install your license? If not, you have not successfully installed your File Archiving software license. Remember that the license generated during registration is bound to two elements: The type of configuration you have and the IP address that you used.

Did you choose the correct configuration license when you registered? A stand-alone (single server) license will not work in a cluster configuration and vice versa.

Did you use the primary IP address of the server during registration? If you have multiple network connections, you need to verify that the IP address you are using is the primary address. To do this, you need to go to the Network Connections-> Advanced Settings. This window displays the connections you have available in your system. Make sure that the port you are using is at the very top of the connection. Normally, if you use the command "ipconfig", the primary port is the first IP address that is shown.

If both the IP address and the configuration license type are correct, but the license is still not detected, open the LicFile.txt and make sure there is no extra carriage returns (line breaks) below your last license. An extra carriage return below your license can cause FAs not to detect the license.

If all these items check out okay and your license still doesn't come up under FAs license information, then please contact HP support for further assistance.

[Back to Top](#)

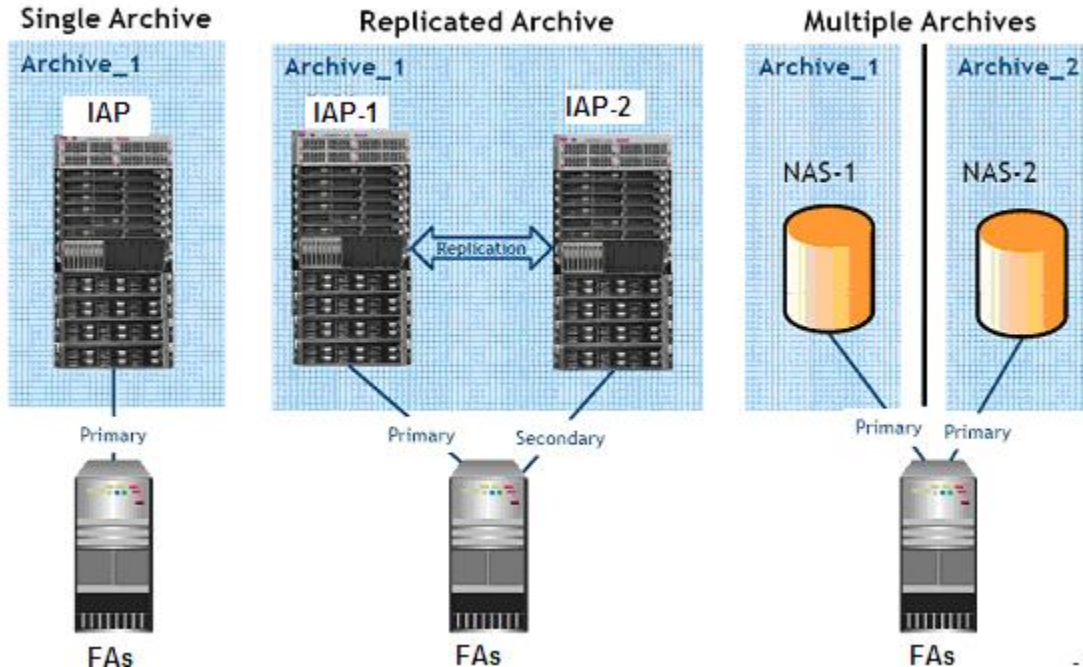
V. Configuration

What are the different archive scenarios supported by File Archiving software?

File Archiving software supports the following archive scenarios:

- Single Archive
 - No Archive Failover
- Replicated Archive
 - Archive Device supports replication
 - Single FAs Archive Configuration
 - Configure secondary Archive
 - Failover on Recall only
- Multiple independent Archives
 - Define multiple Archives in FAs
 - Failover in FAs

Example:



[Back to Top](#)

Does File Archiving software perform replications?

No, File Archiving software does not perform any replication or mirroring. FAs 2.5 is compatible with HP Storage Mirroring 5.1. In addition, you can backup your archive data by performing a migration of the same data to multiple archives. The process of migration is actually copying your data from the file server onto the archive. When release occurs, a file stub is created in replacement of your original file, and you free up the disk space on your file server. The file stub contains metadata that tells File Archiving software where your data are located. If one archive fails, File Archiving software will look for your data on the next available archive that contains the data.

[Back to Top](#)

Is there a way to maintain folder structure between source and archive target?

Yes, you can maintain folder structure exactly as it was on the source using CIFS & FTP archiving. To do this, select the following two options when creating an archive:

- Ignore system name for storage descriptor creation
- Ignore volume serial for storage descriptor creation

The limitation of this is as follows:

- You cannot have more than one FAs server using the same archive.
- Changing existing folder names and moving existing folders around will cause the folder structure in the archive to go out of sync. Only manual intervention will re-synchronize the two. It is not recommended to manually “tamper” with the archive volumes.

[Back to Top](#)

Is there a way to simulate a policy before executing it?

No, there is no way to simulate a policy in the current version of File Archiving software.

[Back to Top](#)

What are the files with extension *.000 and *.001 in the archive target?

Files with extension .000 and .001 are used for garbage collection to keep track of differences in files. FAs 2.5 only keeps track of the most current version of a file.

[Back to Top](#)

Is there a way to limit the amount of revision history of a file in the archive?

No, currently there is no way to limit the number of revision history of a file in the target archive.

[Back to Top](#)

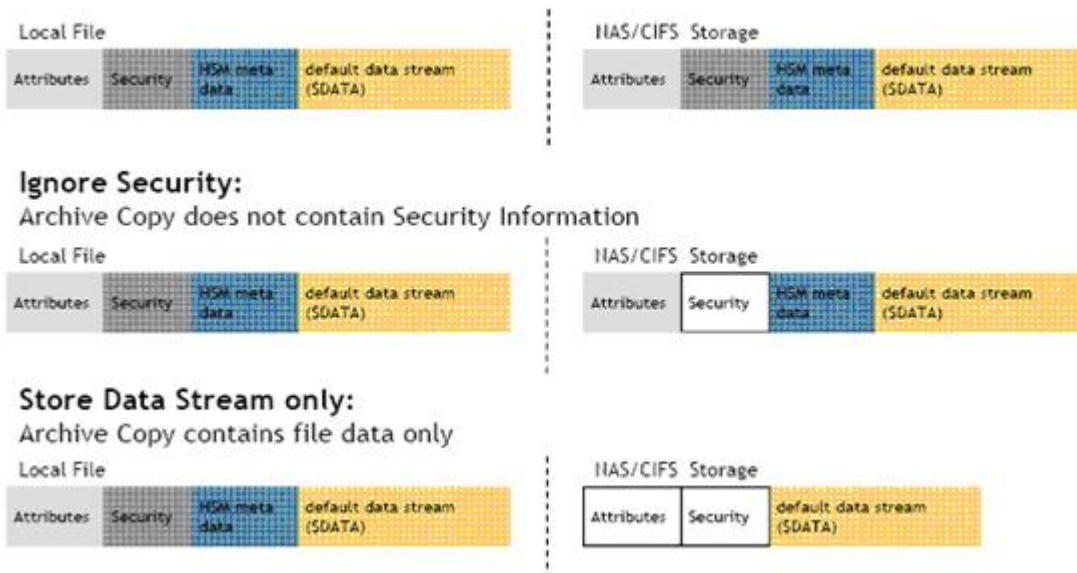
What do the “Ignore Security” & “Data Stream Only” options mean?

The process of migration is copying data from File Archiving software managed volumes onto the selected archive target. When these option(s) are selected, the particular information of the file is not stored into the archive. By default, a file contains these elements:

- File Attributes
- File Security
- HSM metadata
- Data

If the “Ignore security” option is selected, the security information is removed and stored onto the archive. Similarly, with “Data Stream Only”, only the data of the file is stored in the archive.

Example:



What is the “Ignore system name or serial for storage descriptor creation” option?

When storing your data onto the archive, by default, FAs keeps track of the following information regarding your data:

`<Arc_path>\<Sys_key>\<Vol_SN>\<Path>\<File_Name>.<Gen>`

`\\vm-archive\cifs01\VM-FMA-R2\B03A32B0\test-data\99_corner-cases\Many-Files\file.dat.0001`

- `<Arc_path>` - Archive Storage Path
- `<Sys_key>` - Name of the local system. Default is the name of the System when the archive was created. This will not change when System Name changes.
- `<Vol_SN>` - Serial Number of Volume the file belongs to
- `<Path>` - Local path of the file at time of migration
- `<File_Name>` - Local file name at time of migration
- `<Gen>` - Incremented each time a file with the same name exists

The “Ignore system name” option will remove the file server system name when creating the archive storage path. Similarly, the “Ignore volume serial” option will remove the volume serial number of the managed volume on the serial path.

Default:

System Name and Volume Serial Number are part of the Storage Path

<Arc_path>\<Sys_key>\<Vol_SN>\<Path>\<File_Name>.<Gen>

\\vm-archive\cifs01\VM-FMA-R2\B03A32E0\test-data\99_corner-cases\Many-Files\file.dat.0001

Ignore System Name:

System Key is not part of the Storage Path

<Arc_path>\<Vol_SN>\<Path>\<File_Name>.<Gen>

\\vm-archive\cifs01\B03A32E0\test-data\99_corner-cases\Many-Files\file.dat.0001

Ignore Volume Serial:

Volume Serial Number is not part of the Storage Path

<Arc_path>\<Sys_key>\<Path>\<File_Name>.<Gen>

\\vm-archive\cifs01\VM-FMA-R2\test-data\99_corner-cases\Many-Files\file.dat.0001

[Back to Top](#)

How does File Archiving software work in a cluster configuration?

FAs 2.5 supports clusters based on Windows Server 2003 and 2008. Consult Microsoft documentation for help in determining the best cluster configuration for the application. The following quorum modes are supported by FAs and installation instructions are the same for all cases:

- Windows 2003:

Standard Quorum – All nodes use a common disk to store the cluster information

Majority Node Set – All nodes store a copy of the cluster information and there is no shared disk quorum resources

- Windows 2008:

Node Majority - This is similar to Majority Node Set for Windows 2003

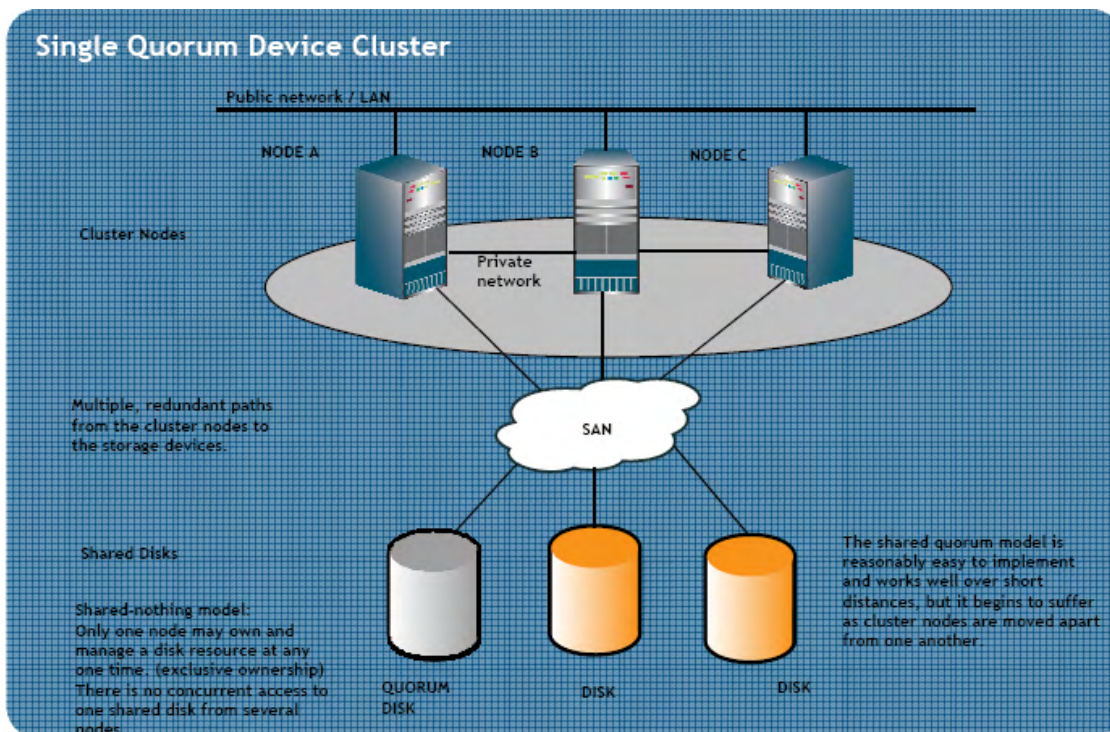
Node and Disk Majority – This is used when there are an even number of nodes for a single site cluster and there is a single shared disk resource

Node and File Share Majority – This is used when there are an even number of nodes and the shared disk resources is a file share that enables nodes from remote site to access the quorum data

No Majority – This is similar to Standard Quorum for Windows 2003

When you work with a cluster environment, consider the following:

- FAs must be installed on every node.
- All cluster nodes must be running and the cluster system must be fully operational before installing and configuring FAs. For a Windows Server 2008 cluster, run the “Validate a Configuration” Wizard before installing FAs. All issues must be resolved before installation of FAs.
- When deploying FAs on an MNS multi-site cluster, ensure that the replication tool maintains exact duplicates of production disks at the recovery location.



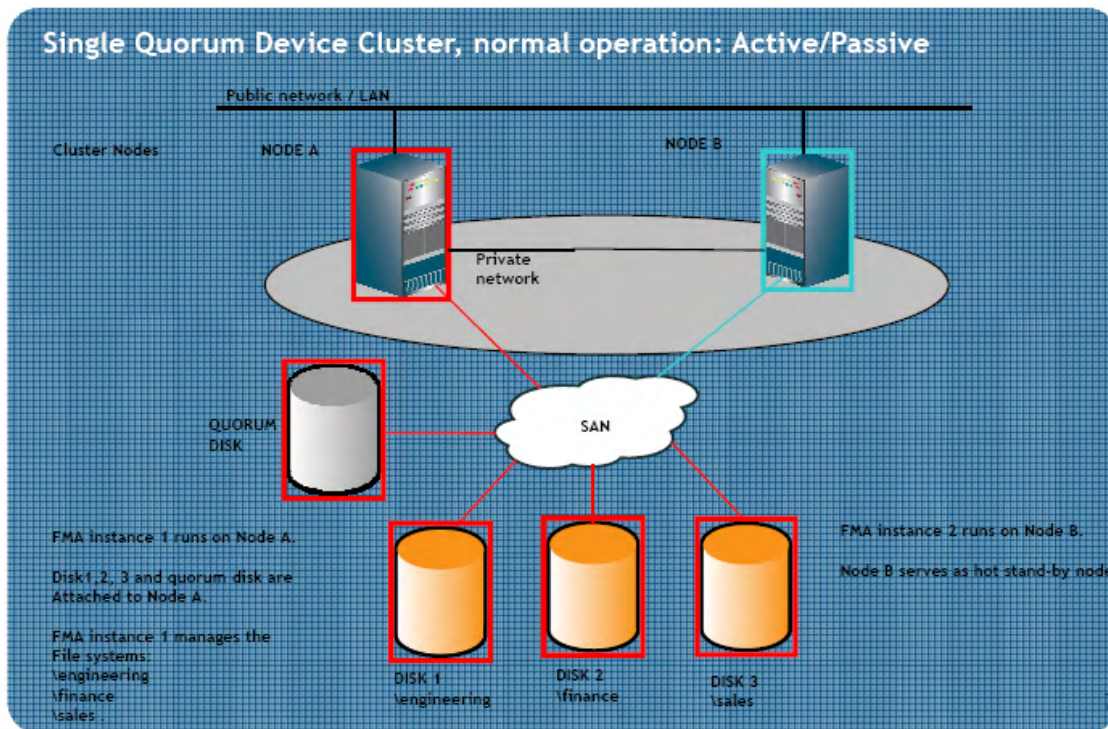
File Archiving software supports an Active/Passive, and an Active/Active cluster configuration. Note that you need to install File Archiving software and its license(s) individually on all nodes, and all managed volumes need to be manually activated in each node during configuration. This means you need to manually failover your resources to all your nodes during configuration and manually start the managed volume. If this is not done, your managed volume will not be managed by File Archiving software when a failover occurs.

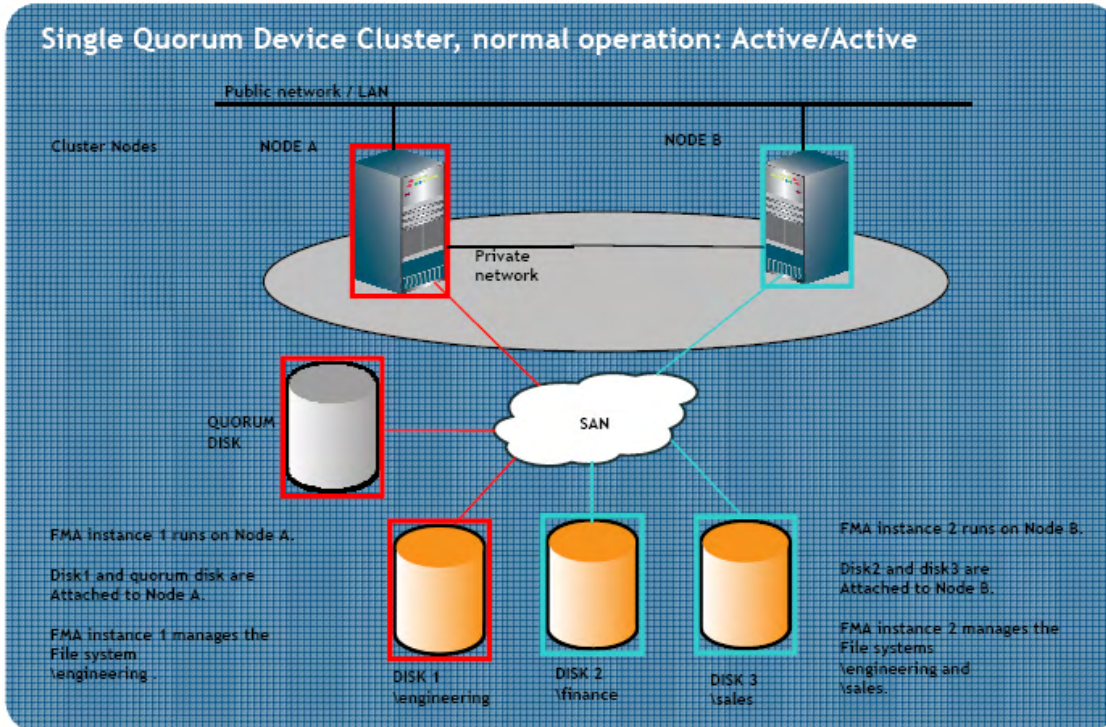
In an Active/Passive cluster configuration, you have one active node and one or more passive node(s) in your cluster. Only one instance of File Archiving software is running at a time in an Active/Passive environment. The active node runs the

instance of File Archiving software, while all passive node(s) are dormant. When a hardware failure occurs on the Active node, the resources of the cluster failover to an available passive node. Note that all resources such as quorum disk, and manage disk(s) are all shared by every node in the cluster. The passive node becomes active, and all other nodes become dormant. When the hardware failure is repaired, a failback of resources can be performed to the primary node. Note that the entire cluster is represented by a Virtual IP address. Regardless of which node is active, a user can access the managed volume(s) in a cluster through the Virtual IP address. The advantage of a cluster configuration is that it prevents multiple hardware failures from negatively impacting the FAs file server.

In an Active/Active cluster configuration, two or more nodes are running FAs. Only one instance of FAs is being run on a single node, but you can have two or more nodes running FAs simultaneously. In this configuration, you would have one or more passive node(s) waiting for hardware failure. A maximum of 8 nodes is supported by Microsoft Cluster Server. When an active node encounters hardware failure, all the resources allocated to this node can either be moved to another active node or to a passive node. The advantage of an Active/Active configuration is that it allows users to balance the workload. The disadvantage of an Active/Active configuration is the complexity of the configuration. Note that all FAs archive configurations are shared by all nodes. Each managed volume configuration such as policy configuration and scheduler will still be persistent after a failover.

Example of Active/Passive and Active/Active cluster configuration:





[Back to Top](#)

How do I install File Archiving software in a Microsoft Cluster Server?

After you have created the cluster in Microsoft Clustering, follow the preceding steps:

1) Log on with a Domain Administrator and run setup.exe on each node of the cluster:

- Select custom setup type
- Do not select the HSM Explorer yet, it can be installed after the FAs configuration has been finished.
- Wait for the installation to complete and click “Finish”

2) Run the FAs cluster configuration wizard on one node of the cluster system:

- Select “Yes” on the 1st page of the wizard.
- Select “LocalSystem Account” on the “Technical User” page.
- Assign the “FMA config service” to the default cluster group.
- Enter the resource name FMACfs and a description.
- Check if the new cluster resource gets “ONLINE” using cluadmin.

[Back to Top](#)

How do I upgrade File Archiving software in a Microsoft Cluster Server?

- 1) Failover the cluster groups containing the managed volumes and resources of the default cluster group to another node.
- 2) Run the setup.exe program and click “Update”.
- 3) Wait for installation to complete and click “Finish”.
- 4) If you are updating from FAs 2.1 click “Yes” and reboot the server. Wait until the node is active. Updating from FAs 2.2 does not require a reboot.
- 5) Repeat the previous steps on any additional nodes of the cluster system.
- 6) Check if the “FMA config service” cluster resource is online.
- 7) Check if the FileMigration Agent service and FileMigration Agent AFM service are running on all nodes.

[Back to Top](#)

How do I uninstall File Archiving software on a Microsoft Cluster configuration?

- 1) Before File Archiving software can be un-installed from any cluster node, stop the “FileMigration Agent service” and “FileMigration Agent AFM service” on all cluster nodes.
- 2) Remove the “FMA config server” cluster resource from the default cluster group to prevent the cluster group from failure using <cluadmin>.
- 3) Run FAs uninstall on all nodes.

[Back to Top](#)

How do I configure an archive in a Cluster environment?

- 1) Start the “FAs configuration” GUI on one node of the cluster system and add a new archive.
- 2) Verify SystemKey contains Cluster Name
- 3) Verify that the newly created archive is displayed on each node of the cluster.

[Back to Top](#)

How do I configure my File Archive software managed volumes in a cluster?

- 1) File Archiving software managed volumes must be explicitly configured on each node of the cluster. Therefore the cluster group, which contains the physical disk resource for the respective File Archiving software managed volume, must be moved to each cluster node and marked as “NEW” in the FAs configuration GUI. Only move a volume to the next node when the status is “Active”. Use the cluster administrator to move your volume between nodes.
- 2) Verify that all managed volumes become “Active” on all nodes of a single quorum device cluster.

[Back to Top](#)

How do I migrate a FAs cluster from Windows 2003 to Windows 2008?

1. Uninstall FAs 2.2 on each node of the 2003 cluster.
2. Migrate the cluster configuration to the Microsoft Server 2008 cluster by following the recommended Microsoft process, <http://technet.microsoft.com/en-us/library/cc754506.aspx>.

Note the following:

- The storage must be migrated to the same drive letters.
- To prevent recalling all the managed files in the process, the storage must be moved as-is to the new cluster.

3. Install FAs 2.5 on each node of the 2008 cluster and configure it as described in [the Administration Guide](#).
4. Manage the volumes that were moved during the migration process. For more information on adding a volume to management, see [the Administration Guide](#).
5. Recreate the archives as follows:
 - Create archives in the same order in which they were created on the original cluster, to ensure that the archive IDs are created properly. Use the list of archives that was generated by the `fmacli arc` command before beginning this procedure.
 - When complete, run the `fmacli arc` command again. The output should be identical to the output of the command for the 2003 cluster.

VI. Active File Management

What happens if more archived data exists than there is available free space on a managed volume?

Full disk space should never occur when File Archiving software is used correctly, but there are two ways FAs controls migration of files:

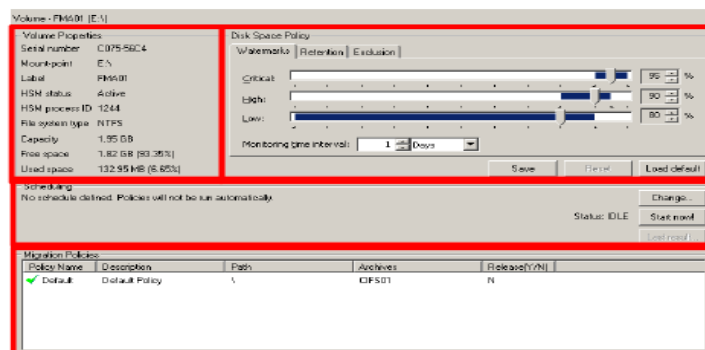
- 1) Volume watermarks
- 2) Folder Policies

For Volume watermarks, there are low, high, and critical watermarks that you define on the managed volume. At the low watermark, a system warning will be generated. At the high watermark, FAs attempts to release files based on established policy that has been defined. At the critical watermark, FAs attempts to release all existing files that have been migrated, ignoring folder policies.

Folder policies are specific details regarding the content of the folder you want to archive your data to. The FAs schedulers control when folder policies are triggered. File details such as File Age, File Size, File type, and Inclusion and Exclusion policies, are considered when folder policies are triggered.

A managed volume would reach “disk full” only if a large amount of data has been stored onto the managed volume filling it up to critical watermark, and this data has not been migrated to an archive. In this case, if someone attempts to recall data that exceeds free disk space, FAs will generate an error stating disk that the “disk is full”.

- Volume Properties
 - File System
 - HSM Status
- Disk Space Policy
 - Watermarks
 - Retention
 - Exclusion
 - Schedule
- Scheduling
 - File Policy Schedule
 - Control/Monitor Policy Process
- Migration Policies
 - List of Policies



[Back to Top](#)

Are files searchable from the users' PC as well as by administrator on the source?

Yes and No.

Online files can be searched, but Offline files are excluded from the search. To get search results in combination with offline files, set the Advanced Options of Microsoft's Internet Explorer to "Search tape backup".

This setup has the following behavior:

- 1) If you only search for "All or part of a file name", you get search results and files are not recalled.
- 2) If you search for "A word or phrase in the file", all files matching your search criteria (all or part of a file name) are recalled.

[Back to Top](#)

Is there a way to maintain folder structure between source and archive target?

Yes, you can maintain folder structure exactly as it was on the source using CIFS & FTP archiving. To do this, select the following two options when creating an archive:

- Ignore system name for storage descriptor creation
- Ignore volume serial for storage descriptor creation

The limitation of this is as follows:

- You cannot have more than one FAs server using the same archive.
- Changing existing folder names and moving existing folders around will cause the folder structure in the archive to go out of sync. Only manual intervention will re-synchronize the two. It is not recommended to manually "tamper" with the archive volumes.

[Back to Top](#)

Can I set granular schedules for when archiving take place?

Yes, scheduling is based at the FAs system level, not at the folder or managed volume level. You can set one schedule with multiple trigger times and run-time durations. You can use the following fields to set your schedules:

- Start time
- Day of the month

- Months
- Days of the week
- Duration in minutes

Example: You can set a schedule to run archiving every weekday at 6pm and 12 Noon for the duration of 1 hour. This schedule will not run on the 31st of each month, and will not run on the month of December.

[Back to Top](#)

How does File Archiving software policy work?

File Archiving software policies are based on “Directories”. By default, all subdirectories will be included in the policy. For example: If you create a policy on C:\, this policy will be enforced on all files in the C: drive and all folders and sub-folders. A single directory can have multiple policies, and subdirectories which have their own policy will be excluded.

For example:

Directories	Policies
\	
\A	Pol1
\A1	
\A2	Pol2
\A3	Pol3
\B	Pol4 Pol5
\B1	
\B2	
\B3	

Example:

Pol1 applies to \A and \A\A1
 Pol2 applies to \A\A2;
 Pol3 applies to \A\A3;
 Pol4 applies to \B, \B\B1, \B\B2 and \B\B3;
 Pol5 applies to \B, \B\B1, \B\B2 and \B\B3;

User can set migration policy filters folders to control the movement of files to the archive. The parameters of the files that can be used to control the movements are as follows:

- Minimum File Age – Last Access time, Last Modification Date, Create Date of the file.
- Minimum File Size – The smallest file size that FAs will release is 4k file size (about the size of a file stub)
- Inclusion Field – You can set what type of files to be migrated, such as *.doc, *.pdf, etc.
- Exclusion Field – Do not migrate any files that have Hidden, Archive, or System attributes. Or you can enter the field where you exclude all “*. exe”

which will exclude migration of files that are executable. Note that if there is a conflict between Inclusion and Exclusion, Exclusion policy will always supersede Inclusion field.

- Release immediately option – Checking this option will automatically release a file creating a file stub in replacement after migration is complete. This option will not release a file that has been recalled, but not modified.

If the Inclusion and Exclusion field is left blank, all files within the folder meeting the Minimum File Age and Minimum File Size parameter will be migrated to the archive.

[Back to Top](#)

What happens at each volume watermarks?

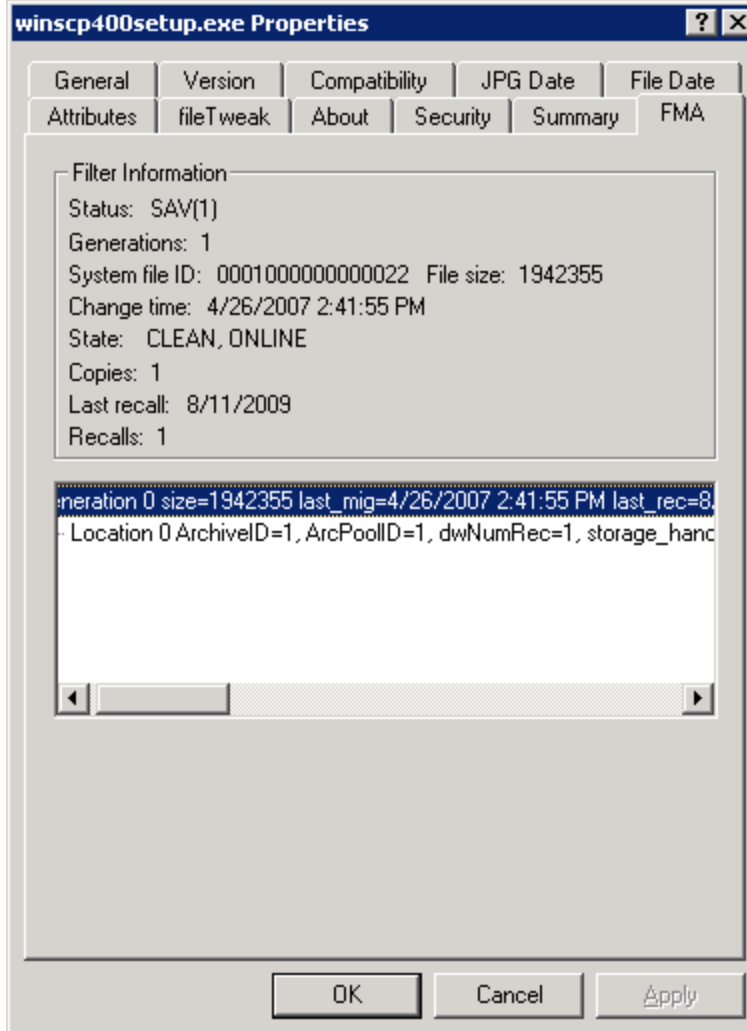
There are three volume watermarks, low, high, and critical watermarks which are user defined on the managed volume. At the low watermark, a system warning will be generated. At the high watermark, FAs attempts to release files based on established policy that has been defined. At the critical watermark, FAs attempts to release all existing files that have been migrated, ignoring folder policies.

[Back to Top](#)

What happens to the FAs column properties in Window Explorer?

The following FAs column properties under Window Explorer have been moved to File Properties under the FMA tab:

- State
- Copies
- Last recall
- Recalls



[Back to Top](#)

VII. Backup and Restore

What are the requirements for a backup application to work with FAs?

Backup applications must be capable of backing up and restoring the following file information in order to ensure proper interoperability with FAs:

- Unnamed data stream (actual file data)
- Proper sparse-file handling
- Access Control List (file security)
- ADS (alternate data streams)
- EAs (extended attributes, only FAs version <= 2.1)
- Reparse point information
- NTFS object ID
- File Attributes (for example, offline, sparse attributes)

In addition, the backup application must meet the following criteria:

- Open files using the options:
 - FILE_FLAG_OPEN_NO_RECALLS
 - FILE_FLAG_BACKUP_SEMANTICS
- Using WIN32 functions, BackupRead and BackupWrite
- Last access timestamp of scanned and/or backed up files may not be changed.

[Back to Top](#)

What are some backup strategies for managed volume(s) and archive(s)?

File Archiving software is not a replacement for backup applications and requires regular backups on the managed volumes and backend archives. Backup applications use different criteria when selecting file candidates during incremental backup. Basic changes of the following parameters may trigger a backup of a file:

- File Size
- Date or time of last modification
- Extended Attributes
- Access Control List
- File attributes like sparse, offline or reparse point flag
- NTFS file security descriptors (SID, Group SID)

There are two basic strategies for backing up managed volume(s).

- 1) Incremental forever backups
- 2) Weekly full backup and daily increments

“Incremental forever backups” is only suitable for backup applications which select a file for backup, and when the reparse attribute has been changed since the last backup. If the reparse attributes is not checked by the backup application, only “ONLINE” files will be backup and therefore the backed up data capacity of a volume could exceed the physical volume size. This strategy slows down disaster recovery since release jobs must be run in parallel to perform a full restore.

“Weekly full backup and daily increments backup” is a better approach compared to “increment forever backups”. The backup applications (for example, HP Data Protector, EMC NetWorker, Symantec BackupExec), which only check the modification timestamp and file size, should be configured for running weekly full backup with daily incremental backups. The periodic full backups will remove the actual content of released files from the backup pools which reduces the backup data capacity.

Some of the backup limitations with FAs are as follows:

- Backing up files on managed volumes via network shares triggers recalls.
- Qualified backup applications have only been tested for local file backup. Archiving features, volume image creation, etc. have not been subject of interoperability testing.
- File restore operations are not supported to alternate locations.
- TSM snapshot technology is not supported.
- VSS client is not supported.
- HP Storage Mirroring or Double-Take is not supported

When doing backup, the following rules needs to be applied:

- Run weekly full backups and daily incremental backups on the managed volumes and CIFS archive(s) at the same time. For performance reasons it’s suitable to run “incremental forever” backups on the CIFS archive(s).
- Do not run migration and release operations during the backup windows to ensure that backups of the managed volume and CIFS archives are synchronized.
- Ensure that the archive copy of a file is backed up before the file is released on the managed volume. This condition simplifies the disaster recovery in case the CIFS archive is lost, but if a file has been released before a backup of the archive copy has been taken, there is still no data loss as long as the file is still included in the backup of the managed volume. Data loss will

occur when the file content is dropped out due to subsequent full backup runs. This case could happen, when an archive copy is lost and an administrator does not become aware of this problem. Regular consistency checks (***fmacli verify -o remote -r <managed_volume>*** can avoid this problem.

Please follow the following step-by-step instruction examples, when releasing files based on the last access timestamp (release all files, which have not been accessed since the last n days)

1. FAs jobs are scheduled daily

- Run the FAs job

```
fmacli migrate -a <archive> -A (n-1)d -r <directory> -F <filelist.lst>  
fmacli release -n1 -A (n)d -f <filelist.lst>
```

- Run the backup job on the managed volume and CIFS archive in parallel after the FAs jobs has been finished.

2. FAs migration and release jobs are alternately scheduled

- Run the following FAs job on Monday, Wednesday, Friday

```
fmacli migrate - a <archive> -A n d -r <directory> -F <filelist.lst>
```

- Run the following FAs job on Tuesday, Thursday, Saturday

```
fmacli release -n 1 -f <filelist.lst>
```

- Run the daily incremental backup jobs on the managed volume and CIFS archive in parallel after the FAs migrate or FAs release has finished.

- Run the weekly full backup job on Sunday on the managed volume and CIFS archive.

- Ensure that the FAs retention time used by the FMA cleanup command is equal to HP Data Protector's protection period. The protection period of the managed volume(s) must also be equal to the protection period of the CIFS archive(s).

[Back to Top](#)

What is the best practice when using FAs and Data Protector?

Here are some of the basic fundamentals you should know about File Archiving software (FAs) and Data Protector (DP) Interoperability:

- If a valid backup version of a file exists, HP DP does not create a new backup version of the file during an incremental backup, when the file status (migrated, released, recalled) has been changed since the last backup. This means, that FAs file operations (migrate, release, recall) are invisible for HP DP.
- When running full backups on released files (stub files) no recalls are triggered. The backup version of a released file contains all NTFS streams (security, attributes, extended attributes, alternate data streams, unnamed stream), but the unnamed stream is completely converted to a sparse zero area. As a result less backup storage is needed for a managed volume since HP DP is a sparse-aware application.
- Since HP DP does not re-back up a file, when the file has been released since the last backup, HP recommends running a combination of weekly full backups and daily incremental backups. The “incremental forever” approach has disadvantages in case of a disaster recovery, because it is very likely that the backed up data capacity will exceed the capacity of the managed volume.
- When running periodic full backups the data of the released files will be dropped out after the n^{th} full backup run, when n^{th} backup versions of a file are configured. In this case only the links to the archive copies are contained in the backed up versions of a file. Therefore it is mandatory to run regular backups on the CIFS archives.
- Since FAs provides an archive cleanup function, which deletes the archive copies of already deleted files after a configurable retention time, this retention time must be equal to the HP DP protection period of the managed volume and CIFS archive file systems as well.

[Back to Top](#)

What is the best practice when using FAs and HP Storage Mirroring?

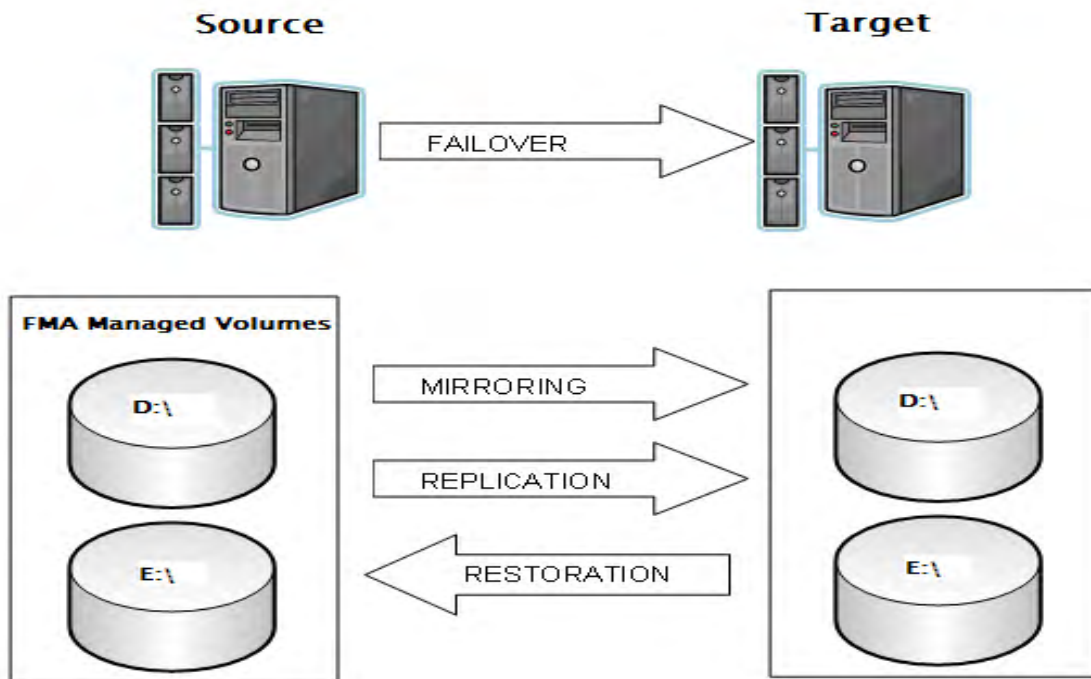
FAs 2.5 supports the following HP Storage Mirroring features:

- Mirroring – The initial copy and subsequent resynchronization of selected data.
- Replication – The on-going capture of byte-level file changes.
- Restoration – A mirror of selected data from the target back to the source.

- Failure monitoring and failover – The ability to monitor and stand-in for server in the event of a failure.

These features are supported in the following two configurations:

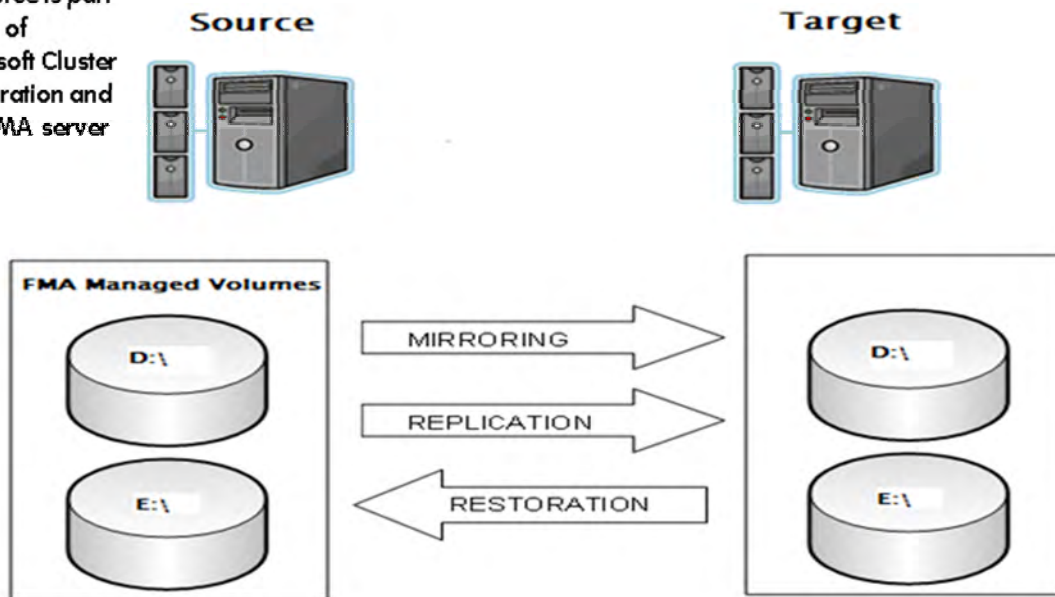
Configuration #1



This configuration shows two stand-alone servers with both FAs 2.5 and Storage Mirroring 5.1 installed on both servers. They are identically configured, but in an active (Source)/passive (Target) configuration. FAs does not support an active/active configuration at this time. Both source and target could be located at the same site. This configuration is best used when there is no Microsoft clustering. The Target is mainly used as backup and standby server for the Source server.

Configuration #2

The Source is part of a Microsoft Cluster configuration and is the FMA server



Note: FMA 2.5 and HP Storage Mirroring 5.1 is installed on all nodes and servers.

The second supported configuration is where the source server is part of a Microsoft cluster configuration. The failover feature is not supported in this configuration. The target server is still mainly used as the backup for the FAs managed volumes. Since HP Storage Mirroring does not allow Virtual IP to be used for mirroring and replication, all nodes in the cluster need to be configured with FAs and HP Storage Mirroring.

FAs 2.5 has been qualified with HP Storage Mirroring version 5.1 (Build 5.1.1.867). HP Storage Mirroring documentation can be found on the HP website:

<http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=115&prodTypeId=12169&prodSeriesId=3185478>

Limitations:

- HP Storage Mirroring Management Console cannot detect “Offline” or “AO” files. The file stub icon can be seen, but the state of the file will show “A” or “Online”.
- Only the two configurations described above are supported at this time.
- After a restoration and failover, FAs file stubs must be reactivated by using the command “fmacli act” (example is in failover.bat). For restoration, this reactivation needs to be performed manually.

- Only active (source)/passive (target) is supported.

[Back to Top](#)

VIII. Downgrading

Can File Archiving software be downgraded to any version?

No, If you are using FAs 2.5, you can downgrade only to FAs 2.2.7. Use the following steps to downgrade:

1. Uninstall FAs 2.5 as described in “[Uninstalling FAs](#)” section of the Administration Guide.
2. When prompted to save configuration settings, select **Yes**.
3. Insert the FAs 2.5 CD.
4. Change directories to the CD drive.
5. Run the following command:
instmod RISS "\SOFTWARE\Hewlett-Packard\HP FMA\Archives"
6. Reinstall 2.2.7 as described in “[Installing FAs on file servers](#)” section of the Administration Guide. (You can ignore the Autopass warning about the higher version.) FAs 2.5 provides a new version of Autopass which is backward compatible with 2.2.

If you are using File Archiving software version 2.2, you can not downgrade to version 2.1. The major differences between FAs 2.2 and FAs 2.1.x versions are shown below:

	FMA Version 2.1	FMA Version 22.2
Filter Driver Technology	Windows Legacy File System Filter Driver	Windows File System Mini-Filter
Binary Driver File	Hsmfs.sys	Hsmfilter.sys
Offline File Flagging	Extended Attribute Controlled by Filter Driver “_IVD_WIN”	Reparse Point: IO_REPARSE_TAG_GRAU_DATASTORAGE_HSM (0x0000001CL)
HSM Meta Data Storage Technology	Extended Attributes “_IFE_FILEINFO”	Alternate Data Stream “:_IFE_FILEINFO”
User Space Communication	Inverted Call Model using IOCTL Commands	Windows Local Procedure Calls (LPC)
Lines of Code		
Supported Platforms	IA32	IA32, EMT64, AMD64
Support for Upcoming Windows Versions (Windows 2008)	No	Yes

4

File Archiving software 2.2 uses reparse point technology whereas version 2.1 uses extended attributes to store HSM metadata. They are mutually exclusive, and cannot exist together. During the 2.1 upgrade, the File Archiving Extended Attributes of file stubs are deleted and replaced with reparse point information during release process. Note that if you have other third party tools that have extended attributes on this file, it will not be deleted by File Archiving software. This needs to be deleted manually using eautil.exe. See question: [“What do I do when I receive an error code 0x00010019?”](#) for details on how to use eautil.exe.

[Back to Top](#)

How do I check the Extended Attributes of a file?

There is a command line interface that will allow you to check the extended attributes of a file, and it's called “eautil”. The following is the syntax for “eautil”:

```
eautil <filename>
```

Note that this command does not work with OFFLINE files. An error appears if you attempt to read the Extended Attributes of an offline file.

[Back to Top](#)

How do I check the reparse tag information of a file?

Use the command line interface “fsutil” to check the reparse tag of a file. The following is the syntax for “fsutil”:

```
fsutil <filename>
```

Note that this command does not work with OFFLINE files. An error appears if you attempt to read the reparse information of an offline file.

[Back to Top](#)

What do I do when I receive an error code 0x00010019?

First, upgrade your system to the latest version of File Archiving software (FAs). Version 2.5 contains corrections and improvements for handling files with 3rd party extended attributes attached. An administrator is now able to detect files with the 3rd party Extended Attributes and additionally, FAs version 2.5 checks for 3rd party Extended Attributes on a file before starting the release operation on that file.

However, FAs does not automatically remove 3rd party Extended Attributes in order to release the file. This must be done manually by the administrator using the following steps:

1. If the error 0x00010019 occurs when releasing a file, an administrator has to check which EAs are attached to the file by using the tool eutil.exe.

syntax: eutil <filename>

2. The administrator has to decide if a specific 3rd party EA can be removed. For removing 3rd party EAs the following options are available:

2.1. remove a specific EA on a single file
eutil <filename> <EA_Name> -d

2.2. remove a specific EA on all files in a directory (recursively)
eutil -r <path> <EA_Name> -d

NOTE:

The command eutil -r <path> -d without specifying the EA_Name deletes all EAs of a file and may break FAs functionality in case the EA "IVD_WIN" was attached to files. The EA "IVD_WIN" must not be deleted!

"IVD_WIN" was used by hsmfs (legacy file system filter of FAs 2.0 and 2.1) and is interpreted and removed by FAs 2.2 or higher when a file is released or recalled.

[Back to Top](#)

IX. Data Relocation

How do I relocate my managed data from one FAs server to another?

The pre-requisites of moving your data from one FAs server to another are the following:

- 1) Shared Archive Configuration – When moving FAs managed files to other server system, ensure that the FAs archive configuration is identical on all server systems.
- 2) Use the command line tool robocopy.exe version XP010 from Microsoft Resource Kit.

Below are some use cases for why you would relocate your data:

- Reassigning managed volumes to other servers in a SAN environment
- Moving a complete managed file system to a new managed volume either local or remote
- Moving a single directory to another managed volume either local or remote

The steps that you would follow in moving your data highly depend on the hardware configuration of your File Archiving server. Particularly, what type of storage are you using as your managed volume? If you are using SAN storage in for your managed volume(s), the steps in reallocating your data are short and straight forward. Whereas, if you are using local hard drive(s) as your managed volume, reallocating your data may take much longer.

In the case where you have your managed volume(s) in a SAN environment, all you need to do is meeting the following prerequisite, and reassign your LUNs to the new file server:

- 1) The FAs archive configuration must be identical on the server systems. This includes the archive number and information.
- 2) The FAs version of the target server must be equal or higher than the FAs version of the source server.
- 3) The managed volume(s) assignment must be identical on the server systems. This mean if you are moving drive E:\ from the source server, the target server must also recognizes that same LUN as drive E:\.

In the case where your managed volume(s) is not located in a SAN environment, you need to perform the following steps:

Pre-requisites:

- Identical FAs archive configuration on all servers.
- FAs Version of target server >= FAs Version of source server.
- Revoke user and application access from the source and target volume until the relocation procedure is finished successfully.
- Ensure that you have a valid backup of the source volume.
- Do not run any migration/release operations during the relocation procedure. Stop the FileMigration Agent AFM service on the source and target server.

Steps for moving a complete managed file system to a new managed volume either local or remote:

1. Disable all files on the source volume by using the following command:
 - `fmacli act --off -r <source_drive_letter> --ignore-files="\System Volume Information" --ignore-files="\HSM Volume Information"`
2. Copy the files using robocopy Version XP010:
 - `robocopy <source_drive_letter> <root_share_target_volume> /E /SEC /COPYALL /B /XD "<source_drive_letter>\System Volume Information"`
3. Synchronize FAs meta data on the target server to the new system fileID:
 - `fmacli act -r <target_drive_letter> --ignore-files="\System Volume Information" -ignore-files="\HSM System Information"`
4. Verify the FAs links on the target server:
 - `fmacli verify -o remote -r <target_drive_letter>`
5. `--ignore-files="\System Volume Information"`
6. `--ignore-files="\HSM System Information"`
7. Restart the FMA AFM service on the target server.
8. Set the source volume to "NOT MANAGED" mode.
9. Delete source Volume (Format).
10. Restart the FMA AFM service on the source server.

Steps for moving a single directory to another managed volume either local or remote:**Pre-requisites:**

- Identical FAs archive configuration on all servers.
- FAs Version of target server >= FAs Version of source server.
- Revoke user and application access from the source directory until the relocation procedure is finished successfully.
- Ensure that you have a valid backup of the source directory.
- Do not run any migration/release operations during the relocation procedure on the source directory. Stop the FileMigration Agent AFM service on the

source and target server.

1. Disable all files on the source directory.
 - fmacli act -off -r <source_directory>
2. Copy the files using robocopy Version XP010
 - robocopy <source_directory> <share_of_target_directory> /E /SEC /COPYALL /B
3. Synchronize FAs meta data on the target server to the new system fileID
 - fmacli act -r <target_directory>
4. Verify the FAs links on the target server:
 - fmacli verify -o remote -r <target_directory>
5. Restart the FMA AFM service on the target server.
6. Remove the files from source directory.
7. Restart the FMA AFM service on the source server.

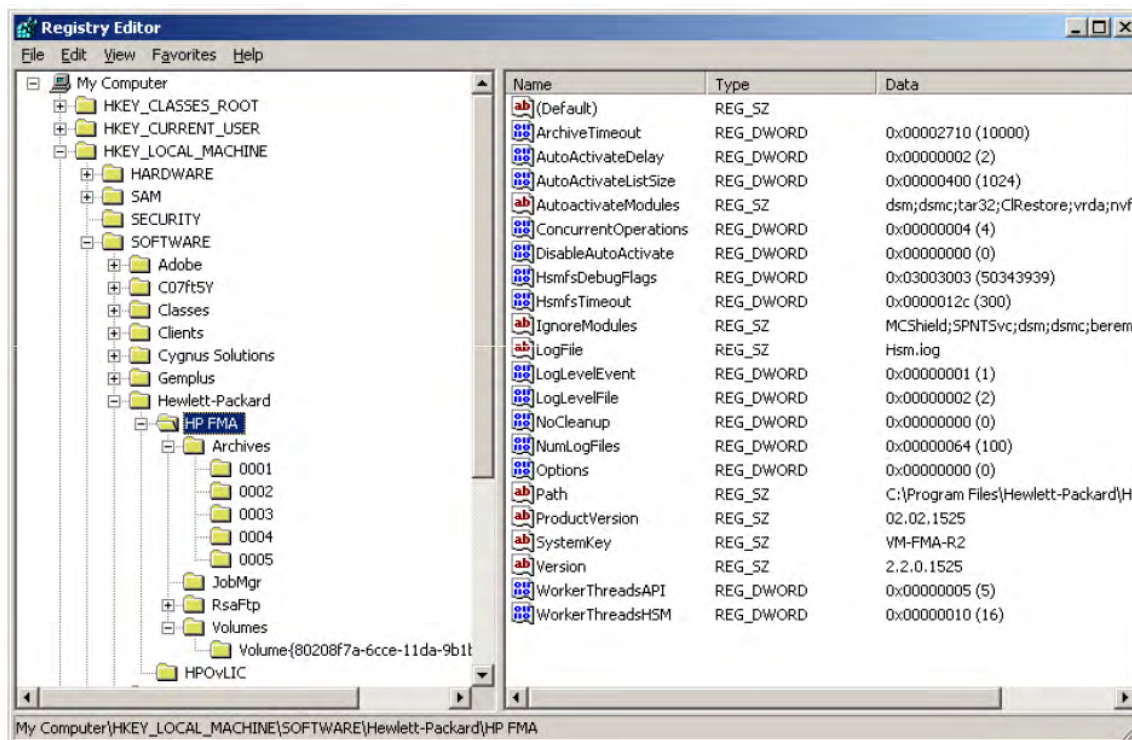
[Back to Top](#)

X. Window Registry Settings

Where can I find the File Archiving software registry settings?

The most important thing about FAs registry is to *never* edit the values unless specifically instructed by an HP support engineer. Reading the registry value is harmless, but when you are editing or changing the Registry you should know exactly what you are doing. You can bring up the FAs registry settings by running the command “regedit” under Windows. The FAs registry path is as follows: \HKLM\SOFTWARE\Hewlett-Packard\HP FMA\ in a 32-bit machine.

The path between 32-bit and 64-bit Windows operating system is different. For a 64-bit machine, you can find the settings under \HKLM\Software\WOW6432Node\Hewelett-Packard\HP FMA.



[Back to Top](#)

How do I change the log settings to debug using the registry?

The most common registry edit for FAs is changing the log settings to debug level when you are encountering a problem with your system. When debug log level is turned on, additional information will be printed and display in the logs to allow

engineers to help troubleshoot your issue. The value you want to look at can be found under the “HP FMA” home registry directory, as shown in the above picture. The registry value is called “LogLevelFiles”. This registry value controls the level of message written to the FAs file log.

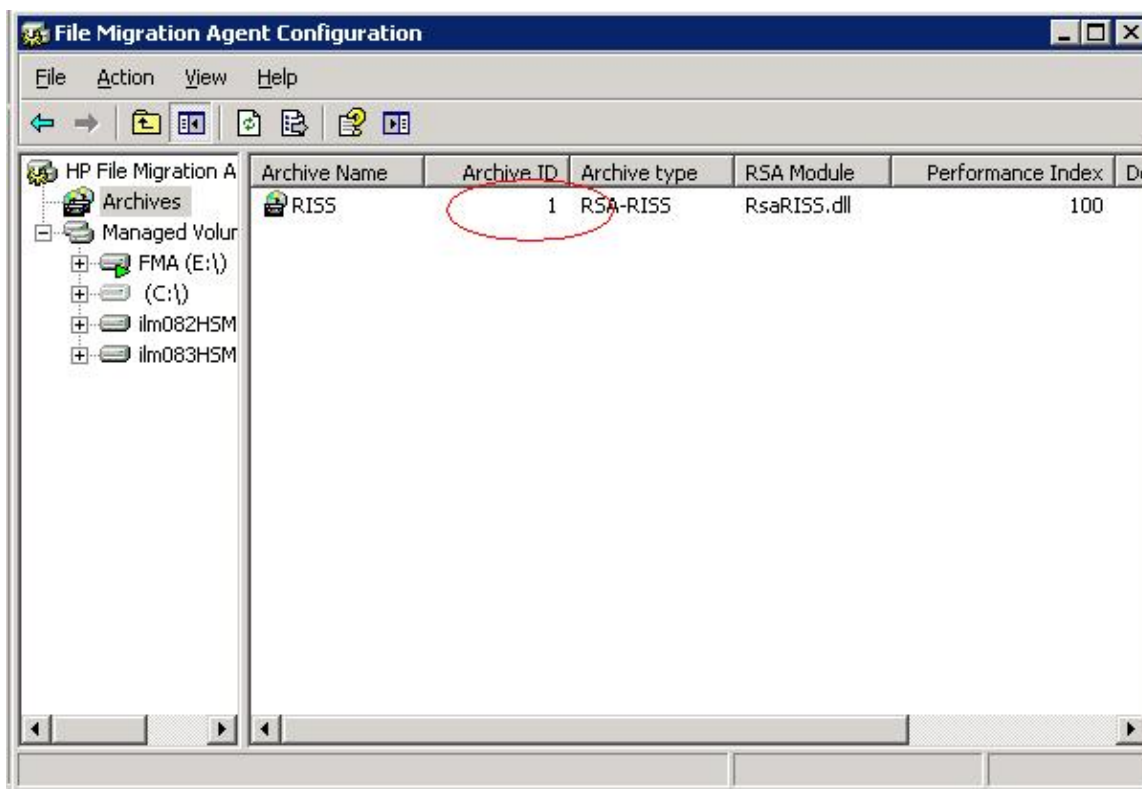
Value 0 – Error Message Only

Value 1 – Warning and Error Message Only

Value 2 – Default value that shows Information, Warning and Errors.

Value 3 – Debug Level

To change the log settings to debug level, edit the LogLevelFile value under the FAs path. Change the value from 2 to 3. Afterwards, open up the File Archiving software Configuration, and note the Archive ID of the archive you wish to debug.



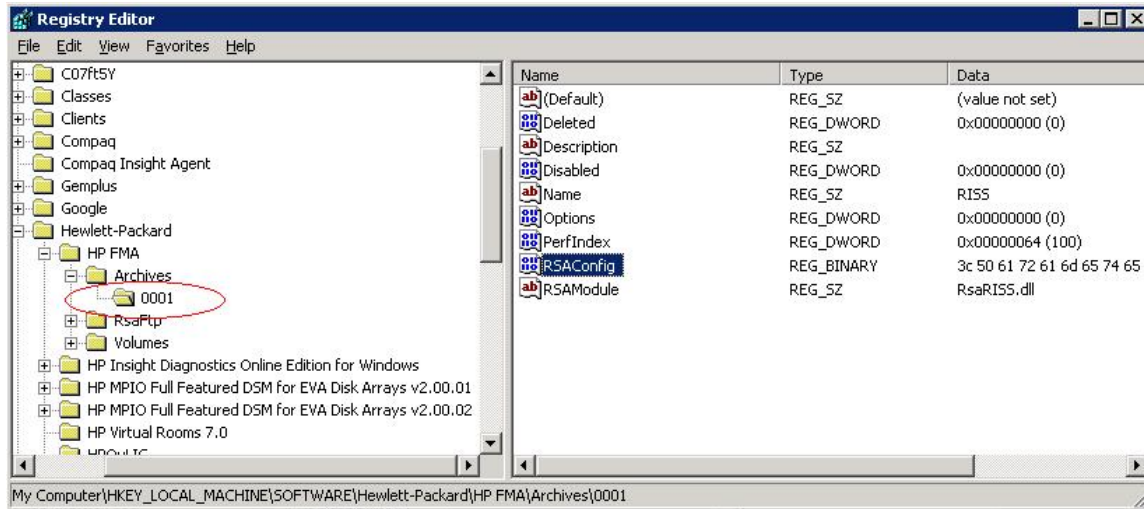
Enter the registry edit and go to

\HKLM\Software\Hewlett-Packard\HP FMA\Archives\ directory (This is for 32-bit machine.

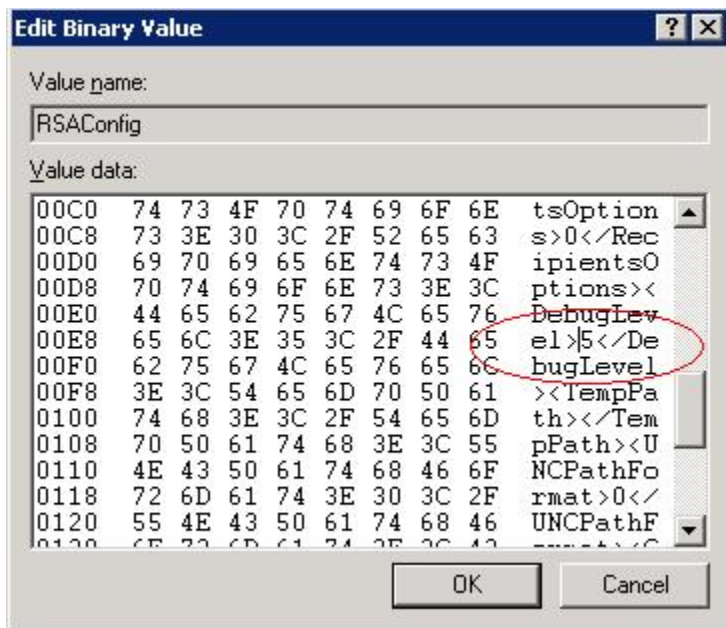
For 64-bit machine, you need to go to

\HKLM\Software\WOW6432Node\Hewlett-Packard\HP FMA\Archives\).

Find and select the corresponding folder number that matches with your Archive ID.



Open up the RSAConfig value contained in this folder and scroll down until you find DebugLevel. Change the value from 0 to 5 and exit. See picture below for more details.



Once you have changed the log level value, try to reproduce the problem or issue that you are encountering. You will see additional statements being printed in the hsm.log.

REMEMBER to change the DebugLevel value back to "0" when you are finished. Debug level log generates a lot of data and fills up your log quotas very quickly.

[Back to Top](#)

How do I control the number of threads used by FAs?

There is no direct way to control the number of threads used by File Archiving software, but you can control the maximum number of threads it uses in your file server. The two registry values of interest are “ConcurrentOperations” and “WorkerThreadHSM”. The ConcurrentOperations value controls the maximum number of threads used by FAs. The default value is 4, but it supports value from 1 to 10. The equation that controls this value is equal to $\text{WorkerThreadHSM}/2$. Depending on which value is smaller. The WorkerThreadHSM value controls the number of HSM worker threads per volume. This value provides the basis for concurrent operations and release operations. The default value for WorkerThreadHSM is 8 and support value from 8 to 20.

Note, the maximum number of threads supported per operation is 10 ($\text{WorkThreadHSM}/2$). This value controls the maximum number of threads open by FAs per operation. Be careful when increasing the value and ensure that your hardware is able to keep up to the number of operations. To optimize your FAs file server, change the ConcurrentOperations to 10 and WorkerThreadHSM to 20.

[Back to Top](#)

XI. File Archiving software Terminology

What is an Archive?

An archive is defined as the backend storage device that stores the data which has been moved from the local systems. File Archiving software supports three types of archives:

- CIFS archive
- NAS archive
- HP IAP or HP RISS

[Back to Top](#)

What is a managed file?

A managed file is a file under the control of the File Archiving software. Managed files typically have metadata attached which points to a number of archive locations.

[Back to Top](#)

What is file policy?

File Policy is a set of rules that determine which files are to be migrated whenever the policy process runs. The rules can be any combination of file age, file size, and file name or types. Rules can be inclusive or exclusive from migration by name or attributes. Wild cards may be used to represent a group of files. File policies maybe defined per directory and are applied to all files of that directory and its sub-directories.

[Back to Top](#)

What is volume policy?

A Volume Policy is a set of watermarks and retention periods that determine the automatic release of files in a manage volume. This is very different from the File Policy. At the high watermark, the volume policy releases files that confirm to the retention period and policy set. At the critical watermark, the volume policy ignores the retention and begins releasing files can be migrated.

[Back to Top](#)

What is metadata?

Metadata is information needed by the File Archiving software to manage files and data. Basically, metadata is data about your data.

[Back to Top](#)

What is inactive data?

Files that have not been touched for a specified period of time and therefore are considered outdated. Do not confuse this with INACTIVE file status of managed files. It is not the same.

[Back to Top](#)

What is a managed volume?

A managed volume is a disk drive that is handled by the File Archiving software (FAs). The file system of these drives must be NTFS. System drives and Quorum drives can not be managed by FAs.

[Back to Top](#)

What is migration?

The process of migration is creating a copy of the local file into an archive(s). This operation does not include the release.

[Back to Top](#)

What is releasing a file?

The process of releasing a file consists of deleting the local file content and freeing up disk space. This step can only be performed after a successful migration of the file. When a file is successfully released, only a stub file remains and the file is marked OFFLINE.

[Back to Top](#)

What is recalling a file?

The process of recalling a file is to retrieve the data of a file from the archive. You can only recall an offline file or stub file. After a successful recall of your file, the file will be ONLINE.

[Back to Top](#)

What is a stub file?

The stub file is the local proxy for a file that has been released; also called a “shortcut”. The stub file is marked as sparse file and the file’s data contains zero-bytes. The link to the file’s data in the archive is kept in the metadata of the file. Stub files are marked “OFFLINE”.

[Back to Top](#)

What is remote storage adapter (RSA)?

The Remote Storage Adapter implements the FAs Storage interface and acts like a “driver” for different types of archive storages.

[Back to Top](#)

What is activation of metadata?

When managed files are restored or relocated, they are set to status inactive by default. Those files need to be activated explicitly. This can be done manually through a browser, or through the command line interface, or by the system itself.

[Back to Top](#)