

HP Software

File Migration Agent (FMA[®])

Installation and Administration Guide



© Copyright 2009 Hewlett-Packard Development Company, L.P.

Legal Notice

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Export of the information contained in this publication may require authorization from the U.S. Department of Commerce.

Microsoft, Windows, Internet Explorer, Notepad, and all Windows-based trademarks are either trademarks or registered trademarks of Microsoft Corporation.

Mozilla and Firefox are registered trademarks of the Mozilla Corporation.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc.

Other product and company names may be the trademarks of their respective owners.

Contents

Preface	vii
About this guide	vii
Audience	vii
Typographical conventions	viii
Related documentation	viii
Support	viii
Subscription service	viii
Support	ix
1 Overview	1
Migration	2
Release	2
Recall	2
Cluster operation	3
FMA components	3
2 Installation	5
Creating a technical user account	5
Configuring backup management applications to work with FMA	6
Ensuring interoperability with FMA	6
Backing up managed volumes	6
Backing up archives	6
Restoring data	7
Installing FMA on file servers	7
Prerequisites	7
Minimum requirements	7
Technical user	7
Operating system version	7
Compatibility issues	8
Restrictions	8
First steps	8
Installing FMA in a cluster configuration	14
Evicting a node from a cluster	17
Adding a new node to a cluster	17
Configuring FMA	17
Upgrading FMA	17
Migrating a Windows 2003 cluster	18
Downgrading FMA	19
Uninstalling FMA	20
Removing the Explorer plugin	20
3 Licensing	21
Enter FMA license keys	21
FMA licensing problems	23

4	Archives	25
	Primary and secondary configuration	25
	Storage descriptors	25
	Ignore Security and Data Stream Only	26
	Ignore System Name and Ignore Volume Serial	26
	Viewing archives	27
	Adding archives to FMA in a cluster environment	28
	Creating CIFS archives	28
	Preparing CIFS archives for FMA	28
	Configuring CIFS archives	29
	Creating FTP archives	31
	Preparing FTP archives for FMA	31
	Configuring FTP archives	35
	Using FmaFileUtil to work with FTP archives	37
	Creating HP Integrated Archive Platform archives	39
	Preparing IAP archives for FMA	40
	Configuring IAP archives	40
	Editing archive properties	43
	Deleting archives	44
	Removing deleted files from archives	44
5	Managed Volumes	45
	Viewing managed volumes	45
	Creating managed volumes	47
	Releasing files using disk space policies	48
	Setting disk space watermarks	48
	Setting retention periods	49
	Excluding files from release based on disk space	50
	Migrating and releasing files using file policies	51
	Creating file policies	51
	Scheduling file policies	54
	Editing file policies	55
	Enabling and disabling file policies	55
	Deleting file policies	55
	Migrating and releasing files with the Explorer plugin	56
	Recalling files	58
	Moving files to another managed volume	58
	Moving a small number of files	58
	Moving a large number of files	59
	Stopping volume management	59
	Restarting volume management	60
	Removing volume management	60

6	Best Practices	61
	Create a new HP StorageWorks File Migration Agent (FMA) archive	61
	FMA archive configuration for a Windows FTP archive	61
	FMA archive configuration for an Linux FTP archive	64
	FMA archive configuration for a CIFS-based NAS device	68
	FMA archive configuration for IAP	70
	Create a new managed volume	72
	Create file policies	72
	Create disk usage monitoring	74
	Determine FMA software version	75
	Migrate files	76
	Release files	76
	Recall files	77
	Set a high-watermark for migration or releases	77
	Verify data files	77
	Schedule FMA commands	77
	Schedule FMA jobs	78
	Backup/restore concept for FMA managed volumes	78
	Relocating data to another FMA managed volume	79
	Relocating data procedure	79
	Relocating a large number of files	80
A	Command Line Interface Reference	81
	FMA commands	81
	activate	83
	archive	86
	cleanup	88
	erase	89
	info	92
	migrate	97
	policy	101
	recall	103
	release	106
	rsa	110
	system	112
	verify	114
	version	117
	volume	119
	Result codes	121
B	Troubleshooting	123
	Accessing FMA log files	124
	FMA log	124
	FMACLI log	125
	Windows event log	126
	Troubleshooting installation	126
	Troubleshooting configuration issues	126
	Troubleshooting connectivity	127
	Troubleshooting common issues	129
	Troubleshooting third-party application issues	132
	Troubleshooting cluster systems	133

C	Third-party Product Compatibility List	135
	Anti-virus	135
	Symantec AntiVirus	135
	McAfee VirusScan	135
	Sophos Anti-Virus	136
	ServerProtect	136
	eTrust AntiVirus	136
	TrendMicro OfficeScan	137
	Backup/restore	137
	BackupExec	137
	BrightStor ArcServe	137
	Data Protector	138
	NetBackup	138
	Networker	139
	NetVault	139
	MS VSS	139
	Tivoli Storage Manager	140
	Galaxy Backup & Recovery	140
	Quota/encryption	141
	StorageExec	141
	Defragmentation	141
	O & O Defrag	141
	MS Defragmentation	142
	IndexServer	142
	MS IndexServer	142
	HP Storage Mirroring Interoperability	143
	Mirroring and Replication	143
	Failure monitoring and failover	144
	Restoration	144
	Supported Configuration	145
	Script creation	147
D	Error Codes and Messages	149
	Index	175

Preface

Welcome to the *File Migration Agent Installation and Administration Guide*. This guide provides the information required to install and work with File Migration Agent (FMA[®]).

FMA enables systematic migration of inactive and rarely used data on Windows file servers to Hierarchical Storage Management (HSM) systems or other Network Attached Storage (NAS) devices. Before migration is enabled, an FMA user must define the volumes to be managed and the archives where data will be stored.

About this guide

The *File Migration Agent Installation and Administration Guide* is designed to help you install, configure, and work with FMA. The chapters include information about product functionality and use, planning and performing installation, creating and managing archives, managing volumes and moving files between managed volumes and archives, using the Command Line Interface (CLI), and troubleshooting.

Audience

This guide is designed for use by anyone deploying FMA. Users should be familiar with the file servers that will be managed in order to effectively create migration policies. Familiarity with system and network configuration is highly recommended.

Typographical conventions

This guide uses the following typographical conventions:

Convention	Description
Bold	Used for file names, field names, URLs, interface elements that are clicked/selected, and information that must be used literally.
<i>Bold Italic</i>	Represents variables within file names, command syntax, URLs, or other literal text.
<i>Italics</i>	Used for emphasis, book titles, and variables.
Monospace	Used for output text, command names and arguments (syntax), code, file content (such as parameters), and command-line text.
<i>Monospace Italic</i>	Represents variables within command syntax, code, or command-line text.
Blue Text	Used for cross-references.

Related documentation

In addition to this guide, you can reference the *HP File Migration Agent Release Notes*. This document provides information about system requirements, known issues, and other information about the current release.

These and other HP documents can be found on the HP documents web site. In the Software section, select Software and go to the Information Management section to find FMA:

<http://www.hp.com/support/>.

Support

For service and support assistance, contact your authorized service and support representative directly.

- For technical assistance with an evaluation version of FMA, contact your sales representative.
- For technical assistance with a registered version of FMA, contact HP Support for support of this product.
- ****ADD standard HP support contact****

Subscription service

HP strongly recommends that customers sign up online using the Subscriber's choice web site:

<http://www.hp.com/go/e-updates>

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

Support

You can visit the HP Software Support web site at:

<http://www.hp.com/go/hpsoftwaresupport>

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

For more information about HP Passport, go to:

<http://h20229.www2.hp.com/passport-registration.html>

When calling support:

Collect the following information before calling:

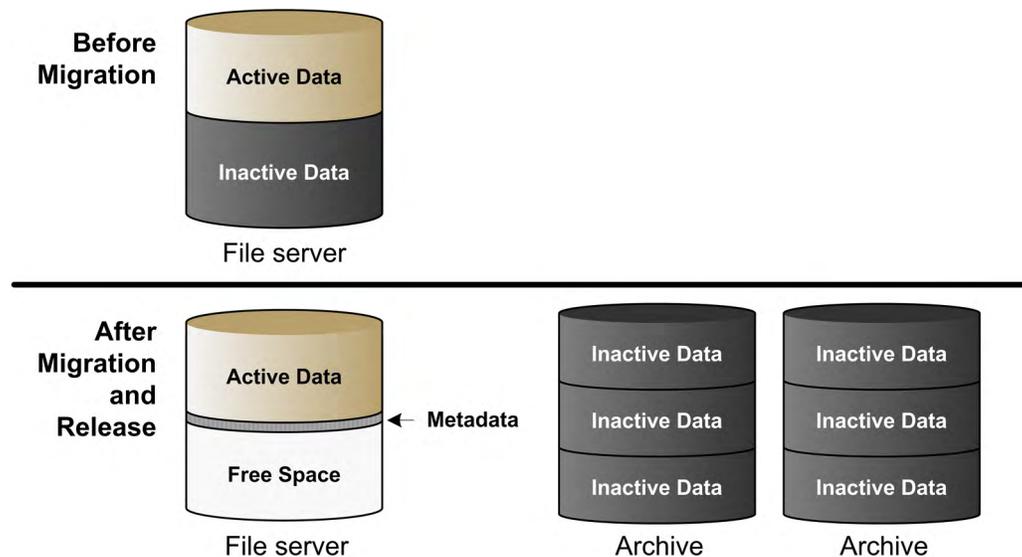
- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Error messages
- Troubleshooting package (If further investigation is needed to resolve an issue. Please provide the troubleshooting package to support. See [Troubleshooting](#) on page 123 on how to obtain this package from your system.)

Overview

File Migration Agent (FMA) offers a technologically innovative approach to data management by maintaining active files on high-performance primary storage while archiving inactive files on cost-effective secondary storage. FMA does not require changes to the current directory structure and integrates seamlessly into the existing IT infrastructure. FMA only manages files on specified volumes on the file server defined as *managed volumes*.

FMA is a Windows-based solution that copies, or *migrates*, inactive or rarely used data to archive storage systems such as Content Addressed Storage (CAS) systems, Hierarchical Storage Management (HSM) systems, or Network Attached Storage (NAS) devices. Migrated files can subsequently be *released* so that only a stub file (a data file that stands in for the original file) remains on the file server while the full file resides on the archive storage system. FMA *recalls* the file from the archive whenever it is needed on the file server.

Migration, release, and recall processes are transparent to Windows users and applications, which can continue to access files as if the files were still on the file server. Migrating and releasing files manages the growth and complexity of Windows file servers, freeing space for active data.



FMA administrators define the conditions under which files on managed volumes are migrated or released. The administrator can create policies to migrate and release files based on properties such as the file extension or timestamp. The administrator can monitor the space on a managed volume and automatically release migrated files based on a retention time period when a configurable watermark is reached.

Migration

During the migration process, FMA adds FMA-specific metadata to a managed file on a file server and copies the managed file to one or more archives. FMA supports the following:

- Common Internet File System (CIFS), for Windows-based archives
- File Transfer Protocol (FTP), for Linux-based archives
- HP Integrated Archive Platform (IAP), for IAP archives

Although files can be migrated manually, FMA administrators typically create *policies* to define the conditions under which files are migrated. Policies can migrate files based on file name; file age in relation to creation, modification, or last access time; or a minimum file size. They can exclude files from migration based on file name or file attributes, such as hidden files. Policies can be run manually or scheduled to run at regular intervals.

Administrators can apply any number of policies to each managed volume. Policies set in the root folder apply to all files in the entire volume. Policies set at the folder level are valid for the files in that folder and its subfolders.

After migration, FMA verifies that the file size and timestamp of a file on the file server and the file on the archive are identical.

For information about migrating files, see [Managed Volumes](#) on page 45.

Release

During the release process, FMA replaces a migrated file on a file server with a stub file. FMA marks this stub file as offline, which designates files that have remote data.

Although files can be released manually, FMA administrators typically set disk space policies, which are watermark levels that monitor available disk space on managed volumes. When a managed volume reaches its high watermark, FMA evaluates the retention policies for the volume and begins releasing files that match the policy criteria. FMA stops releasing files when it reaches its low watermark. If the critical watermark is reached, files are released independently of the retention policies. Retention policies are related to elapsed time since last access or modification to a file. For information about these watermarks, see [Releasing files using disk space policies](#) on page 48.

Before a file can be released, it must be migrated with at least one valid copy in an archive and it must be larger than 1024 bytes. Because releasing locks files exclusively, files that cannot be opened exclusively cannot be released and remain on the file server. Files can also be released according to user-set policies regarding the number of archived copies existing for each file.

For information about releasing files, see [Managed Volumes](#) on page 45.

Recall

When a user or application accesses a released file to read it or write to it, FMA intercepts the read or write request and retrieves the file data from the archive. If one archive is not available, FMA attempts to find the file in other archives where the file was also migrated. If FMA cannot recall a file from any of the archives, it returns an error.

Files can also be manually recalled explicitly by using the FMA command line interface, or by using the Window Explorer plug-in.

For information about recalling files, see [Managed Volumes](#) on page 45.

Cluster operation

When running on a Microsoft Cluster Server, an instance of FMA is installed and running on each node. Two of the FMA services are concurrently active on all nodes. The Active File Management (AFMSvc) and the Volume Manager (HsmSvc) run concurrently on each node to handle file migrations and recalls on any managed volumes that might be active on those nodes. A third service, the Configuration service (HsmCfgSvc), runs only on the node currently hosting the cluster group resources. Its activation is tied to and controlled by the cluster group.

For a given volume, the policy information is stored at the root level of the volume in the “HSM Volume Information” system directory. Because this information is stored on the volume, policy information for the volume is available when the volume is moved or fails over to another node in the cluster. When this volume appears on the new node where FMA is running, a new file system filter instance is attached to the volume and an instance of the volume manager is started for this volume. The volume manager is then able to read the policy information and carry on management of the volume on the new node.

Archive configuration is considered a global resource and is controlled by the Configuration service. Although archive configuration is accessible from all nodes, the policy referencing the archive must be edited from the node where the volume is currently active. When installing or managing FMA in a Microsoft Cluster Server, be aware of the cluster-specific instructions in chapters 2-5.

FMA components

The following FMA interfaces and utilities are available:

User interface

Use the FMA user interface to perform most tasks related to managed files or volumes. The user interface is seamlessly integrated into Microsoft’s Management Console (MMC) and its use is documented throughout this guide. To access the FMA user interface, select **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.

You can also access the FMA user interface from the Computer Management window or the Server Management window, depending on the operating system. For the 32-bit version of Server 2003, the File Migration Agent section is listed in the Storage section of Computer Management. For the 32-bit version of Server 2008, the File Migration Agent section is listed in the Storage section of Server Manager.

Explorer plugin

Use the Explorer plugin on the file server to manually migrate, release, and recall managed files from Windows Explorer. To view the FMA properties of a file using the Explorer plugin, right-click on a file (in a managed volume) in Windows Explorer, select **Properties**, and then select the **FMA** tab. For more information about using the Explorer plugin, see [Migrating and releasing files with the Explorer plugin](#) on page 56.

Command line interface

Use the FMA command line interface (FMACLI) to work with managed files. While most functions are available from the FMACLI, tasks such as creating managed volumes must be performed in the user interface.

When running HP FMA on a 64-bit Windows Operating System, the Explorer plug-in is only available for the 32-bit MS Explorer version. In order to use the FMA plug-in on a 64-bit OS, the following command must be manually run:

```
%windir%\syswow64\explorer /separate
```

For details about the FMACLI, see [Command Line Interface Reference](#) on page 81.

FMAFileUtil

Use FMAFileUtil to manually retrieve and store data on FTP-based archives. For details about this utility, see [Using FmaFileUtil to work with FTP archives](#) on page 37.

Installation

This chapter describes the tasks you must perform to install File Migration Agent (FMA). These tasks include the following:

1. Create the technical user required by the FMA service.
2. Configure backup management applications to ensure that data on file servers continues to be backed up as expected.
3. Install FMA on each file server with files that you want to manage.
4. If you are installing in a Windows cluster environment, run the FMA cluster configuration wizard.

In addition, this chapter contains information about FMA license keys, upgrading FMA, downgrading FMA, uninstalling FMA, and removing the Explorer plugin.

Note To install, use the FMA components, or uninstall FMA, the login user account must have Administrator privileges.

Note Ensure there is no unsupported third-party applications installed on the file server.

Creating a technical user account

FMA can run processes using a technical user account. Before you begin, create a Windows user account with **Full Control** permissions, including permissions to start, stop, and pause services. Specifically, FMA uses the technical user to migrate data to Common Internet File System (CIFS) archives. To maintain FMA access to the files it manages, the password for this technical user account should never change or expire. If a password change is required, the password must be updated on every archive accessed by FMA.

In a cluster environment, a domain user is typically used to run FMA processes.

Configuring backup management applications to work with FMA

Managed volumes and archives must be backed up regularly. FMA is an archiving solution and does not replace the current backup solution.

Refer to the *File Migration Release Notes* for a list of supported backup management applications and their limitations with FMA.

Ensuring interoperability with FMA

To ensure proper interoperability with FMA, the backup management application must back up and restore the following file information:

- Unnamed data stream (actual file data)
- Proper sparse-file handling
- Access control list (file security)
- Alternate data streams
- Reparse point information
- NTFS object-id
- File attributes, such as offline and sparse

In addition, keep the following in mind when performing backups:

- The backup management application must open files using the `FILE_FLAG_OPEN_NO_RECALLS` and `FILE_FLAG_BACKUP_SEMANTICS` options.
- The backup management application must use the `WIN32 BackupRead` and `BackupWrite` functions.
- The backup management application must not make changes to the last access timestamp of scanned or backed up files.
- Backing up files on managed volumes using network shares triggers recalls.

Backing up managed volumes

Backup management applications use different criteria when selecting candidates for incremental backup. Changes to parameters such as file size, modification date, or file attributes can trigger a backup.

Some applications monitor the reparse attribute for a file. If this attribute has changed since the last backup, the application backs up the file again. These applications should back up files incrementally. Currently, IBM Tivoli Storage Manager is the only supported backup management application that should use only incremental backups.

Other applications monitor the modification timestamp and file size. For these applications, FMA operations are transparent. Configure these backup management applications to run a weekly full backup with daily incremental backups. As files are released, periodic full backups include stub files rather than full files. This reduces the size of backups but requires that the archive be backed up reliably.

Backing up archives

Archive files must be backed up as well. Because these are always full files, they do not have the same restrictions as the managed volume backups. However, for CIFS backups, use the following guidelines:

- Run weekly full and daily incremental backups on the managed volumes and CIFS archives at the same time.
- For performance reasons, run **incremental forever** backups on the CIFS archives.

- Do not migrate or release files during the backup window to ensure that the backups of the managed volumes and CIFS archives are synchronized and consistent.
- As a best practice, create two archive copies when using CIFS archives.
- FMA archive cleanup expiration time must be greater than the backup retention time. For information about cleanup, see [Removing deleted files from archives](#) on page 44.
- Ensure that a replica of a file is backed up before that file is released from the managed volume.

Restoring data

If you must restore a backup of a file or folder, you should copy and paste the current file or folder to a new location and then restore the file or folder to the original location. FMA does not support file activation for files that have been restored to a new location. Restoring files is only supported to their original location.

Installing FMA on file servers

Prerequisites

Minimum requirements

- A server that meets the minimum hardware requirements shown in the HP FMA 2.5 Release Notes document.
- An additional hard disk drive(s).

Technical user

The FMA service needs to run under a user account (for example, FMAUser) with the following privileges:

- Backup files and directories.
- Restore files and directories.
- Take ownership of files or other objects.
- Network access.
- Other things to consider about technical users:
 - Password must not expire.
 - Password should not be changeable by the user.

Note The user must have the appropriate access rights (“FULL CONTROL”) on the NAS devices, which are used as backend data stores. Create the FMA technical user account before starting the installation procedure. A wizard is launched during the installation for setting up the technical user.

Operating system version

The 32 and 64-bit versions of the following operating systems are supported for file servers and for CIFS-based NAS archives:

- Microsoft Windows Server 2008 Standard, Enterprise, and Datacenter Editions
- Microsoft Windows Server 2003 SP2 Standard and Enterprise Edition
- Microsoft Windows Server 2003 R2 SP2 Standard and Enterprise Edition
- Microsoft Windows Storage Server 2003 Standard and Enterprise Edition

- Microsoft Windows Storage Server 2003 R2 SP2 Standard and Enterprise Edition
- HP Windows Unified Data Storage Server (WUDSS) 2003
- Microsoft Windows Server 2003 R2 NFS server with the following restrictions:
 - 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.
 - Window components “Services for Unix” and “User mapping” components is required for NFS sharing of the source volume(s)
 - When files with the same name but different capitalization (such as temp1, Temp1, and TEMP1) are saved in the same directory, the Win32 subsystem recognizes only one of them. FMA and other Windows applications can only access one of these versions, and it is not possible to determine which version will be retrieved.

Compatibility issues

Before installation, please review [Third-party Product Compatibility List](#) on page 135. Software which is not on the list is not supported and needs to be removed from the FMA server before installation.

Restrictions

The following features are not part of this FMA version:

- No continuous migration and release.
- No event-driven migration and release.
- No built-in disaster recovery function. Regular backups of the managed file system are required. (See [Third-party Product Compatibility List](#) on page 135.)
- The system volume cannot be managed by FMA.
- No support for multiple generations of files.
- No load balancing for recall between different archives.
- A monitor resolution of at least 1024 x 768 pixels is required.
- FMA can not manage a cluster quorum disks.
- For restrictions on third-party applications see [Third-party Product Compatibility List](#) on page 135.

First steps

When using the FMA for the first time, the following procedures must be executed:

1. Install the backend archive (CIFS, IAP, or FTP).
2. Create a technical user for the File Migration Agent service. Collect information about the data storage (user ID, IP address, and so on).
3. Install FMA. For further information about the FMA installation, see [Installing FMA on file servers](#) on page 7, [Installing FMA in a cluster configuration](#) on page 14, and [Upgrading FMA](#) on page 17.
4. Configure at least one FMA archive using the FMA MMC Snap-In. For further information about the FMA archive management, see [Archives](#) on page 25.
5. Configure the managed volumes using the FMA MMC Snap-In. For further information about the FMA volume management, see [Managed Volumes](#) on page 45.

6. Configure file policies and schedules on the managed volumes using the FMA Policy Manager (see [Migrating and releasing files using file policies](#) on page 51).
7. Configure the watermarks and retention periods for disk space monitoring of the managed volumes using the FMA Policy Manager (see [Releasing files using disk space policies](#) on page 48).

You must install FMA on each file server to be managed. During this installation process, the following folders are created the FMA installation folder, which by default is C:\Program Files\Hewlett-Packard\HP FMA\.

- bin—Program files and binaries
- doc—Documentation
- log—FMA log files
- templates—Policy templates

If you are working in a cluster environment, see [Installing FMA in a cluster configuration](#) on page 14.

To install FMA

1. Close all applications running on the file server.
2. Run **setup.exe** to start the installation wizard. This file is available on the installation CD.

The Welcome dialog box is displayed:



3. On the Welcome dialog box, click **Next**. The License Agreement dialog box is displayed:



4. On the License Agreement dialog box, read the agreement, select whether to accept it, and click **Next**. You cannot continue with installation unless you accept the license agreement.

The Destination Folder dialog box is displayed:



5. On the Destination Folder dialog box, choose the location where to install FMA.
 - To install in the default location, click **Next**. This is recommended.
 - To install in a different location, click **Change**, select a new location in the dialog box, and then click **Next** in the wizard.

The Setup Type dialog box is displayed:



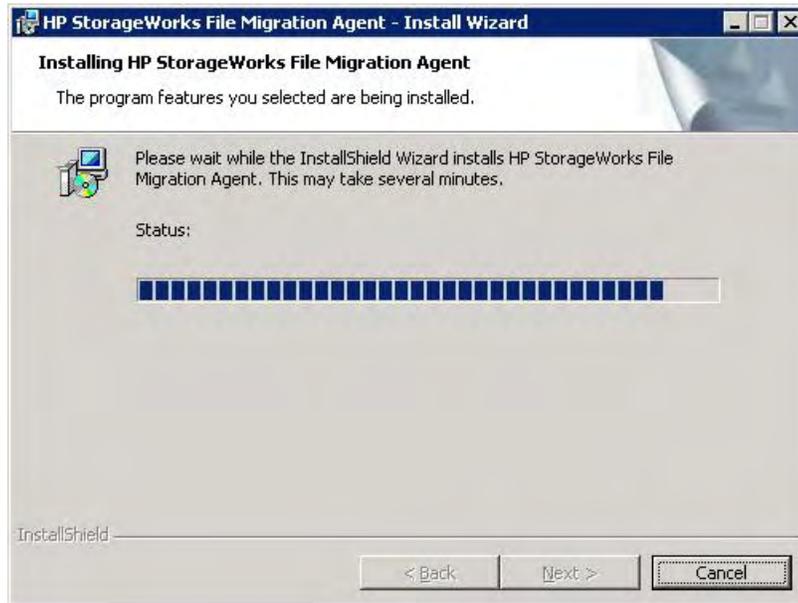
6. On the Setup Type dialog box, choose whether to install all features or select features.
 - To install all features, which is recommended, click **Next**.
 - To install select features or if you are installing in a Windows cluster environment, select **Custom** and then click **Next**. The Custom Setup dialog box is displayed:



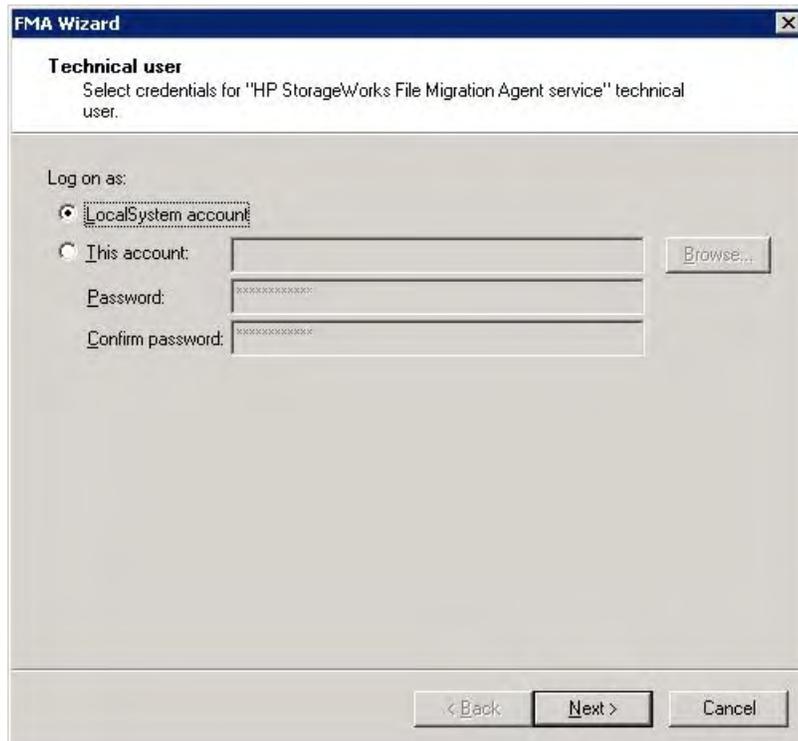
Click the icon on the Custom Setup dialog box next to the files you do not want to install. To install these files in a location other than the default location, click **Change** and select a new location in the dialog box. Then, click **Next**.

Note If you are installing in a Windows cluster environment, do not select **HSM Explorer Extension**. This feature (the Windows Explorer plugin) can be installed after FMA configuration is complete.

The wizard installs FMA.



Then, the Technical user dialog box is displayed:

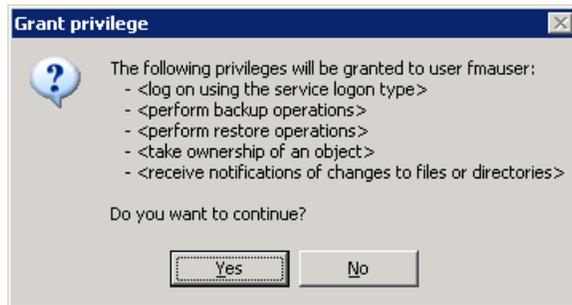


7. On the Technical user dialog box, provide information about the technical user you set up for the FMA service. For more information about this account, see [Creating a technical user account](#) on page 5.
If you select **LocalSystem account**, FMA uses the local ID named `system` to run processes.

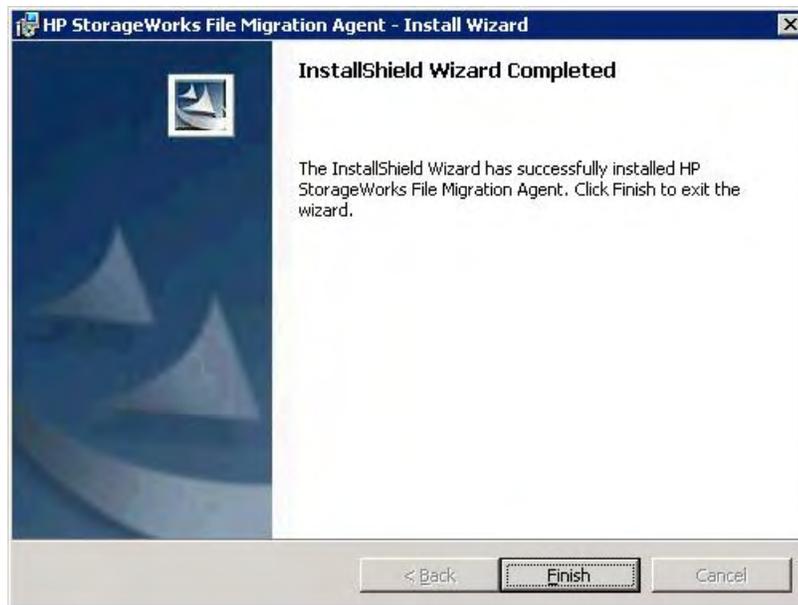
To specify a technical user, complete these steps:

- a. Select **This account** and type the name of the account.
- b. In the **Password** and **Confirm** password fields, type the account password.
- c. Click **Next**.

The Grant Permissions dialog box is displayed:



8. Click **Yes** to confirm you want to grant permissions to the technical user.
9. Click **Next** on the Wizard Summary dialog. The completion dialog box is displayed.



10. Click **Finish**.

Installing FMA in a cluster configuration

If you are installing FMA on a Microsoft cluster system, you must perform additional configuration steps.

FMA 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 FMA and the installation instructions are the same for all cases:

- Server 2003

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

Majority Node Set (MNS)—All nodes store a copy of the cluster information and there is no shared disk quorum resource.

- Server 2008

Node Majority—This is similar to MNS for Server 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 resource is a file share that enables nodes from remote sites to access the quorum data.

No Majority—This is similar to Standard Quorum for Server 2003.

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

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

If you want to migrate a Windows 2003 cluster that includes FMA to a Windows 2008 cluster, see [Migrating a Windows 2003 cluster](#) on page 18.

To configure FMA in a cluster environment

The Active/Active and Active/Passive configuration have different configuration steps in the cluster environment, refer to [To create an Active/Active Cluster configuration](#) on page 15 for more information.

The following steps are for the Active/Passive cluster configuration:

1. Install FMA on each cluster node, following the steps in [Installing FMA on file servers](#) on page 7.

Note In cluster environments, the FMA configuration service runs on one node only. This service is not started until all steps in this procedure are completed. The FMA migrator service should only run for seven minutes when the configuration service is not running. Therefore, if step 1 takes longer than seven minutes to complete for ALL nodes, HP recommends rebooting all nodes prior to completing step 2.

2. Launch the FMA cluster wizard on any cluster node to configure the FMA configuration service as a cluster resource in the default cluster group.

From the Start menu, select **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Cluster Setup**.

3. On the Cluster Setup dialog box, click **Next**.

4. On the Cluster Setup dialog box, select the account to use to run processes and click **Next**. In a cluster environment, a domain user is typically used to run the FMA Configuration process. If you do not want to create a new user for this process, you can select **Localsystem account**.
5. On the Cluster Setup dialog box, select **Cluster Group** and click **Next**.
6. On the next Cluster Setup dialog box, enter a resource name and brief description and click **Next**.
7. On the Wizard Summary dialog box, click **Finish**.
8. Use the Windows cluster administration tools to view the status of the cluster group and the FMA service that was just created. The cluster group should be online and contain the FMA configuration service that was just created.
9. Move the cluster group to all nodes of the cluster and verify that it comes online in each case. Manually Start the management of managed volume(s) on each node after verifying the cluster group is online. Moving the cluster group is different depending on whether the system is based on Server 2003 or 2008.
 - Server 2003
 - In the cluadmin application, right-click the default cluster group and select **Move**.
 - Server 2008
 - Enter the following command at a command line prompt:
 - ```
cluster . group "Cluster Group" /move:Node
```
    - where *Node* is the destination for the move.

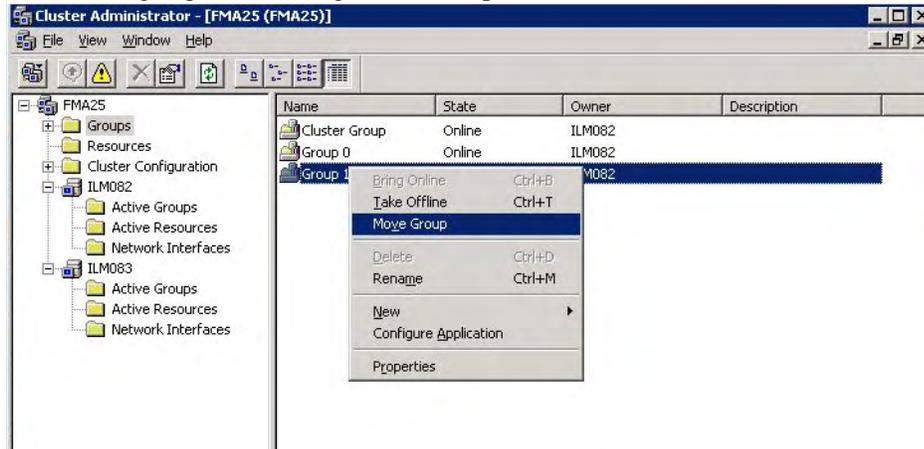
For information about adding archives in a cluster environment, see [Adding archives to FMA in a cluster environment](#) on page 28. See [Creating managed volumes](#) on page 47 for information about adding volumes in a cluster environment.

### To create an Active/Active Cluster configuration

The Active/Active configuration requires a few additional steps to configure compare to the Active/Passive configuration.

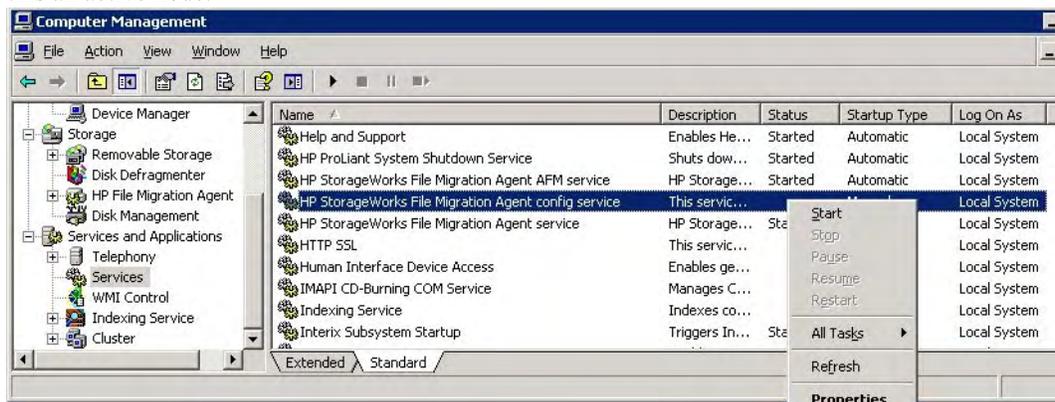
1. Create an Active/Passive configuration using the steps provided in [To configure FMA in a cluster environment](#) on page 14.
2. Open the **Cluster Administrator**. The Cluster Administrator is a tool to enable creating and controlling cluster configurations. To open the Cluster Administrator:
  - Open a new command window by clicking **Start** → **Run**. Enter `cluadmin`.
  - or
  - Open the control panel by clicking **Start** → **Settings** → **Control Panel**. Open **Administrative Tools** and then **Cluster Administrator**.

3. Create a new Cluster Group for the resources to be allocated to the secondary Active node.
  - a. Click **Add New Resources**. Add the new Physical Disk to the new Cluster Group you have created.
  - b. Move the Cluster Group with all its resources to the appropriate active node by right clicking over the selected group and selecting **Move Group**.



**Note** All drive letters or resource names in the cluster resources must be unique. Drive letters or resource names cannot be used more than once. If you have identical drive letters or resources, they will not failover to the another node because it already contains the same drive letter. If the disk drive does not failover to another node during failure, it will not be managed by FMA.

4. Log on to the secondary active node and verify the resources have come online.
  - a. Open the control panel by clicking **Start → Settings → Control Panel**.
  - b. Open **Administrative Tools** and then **Computer Management**.
  - c. Expand **Service and Applications**, and select **Services**.
  - d. Examine the list for **HP StorageWorks File Migration Agent config service**. The startup type should be **Manual**, and the two other FMA services should already be in **Started** status.
  - e. Right click the **HP StorageWorks File Migration Agent config service** and select **Start** to make this an active node.



5. Bring up the FMA configuration, and manage your new volumes as described in Chapter 5, [Managed Volumes](#). You can now configure your archives and file policies.

**Note** During failover, your cluster resources failover to the other active node, or to a passive node depending on configuration.

## Evicting a node from a cluster

To uninstall FMA from a node that has been evicted from a cluster, follow these steps:

1. Evict the node using Windows cluster administration tools.
2. Uninstall FMA from the evicted node. Follow the instructions ([To uninstall FMA from a single file server](#) on page 20) for uninstalling FMA from a single server.
3. Return to a node that is still a member of the cluster and run the FMA Cluster Setup wizard. Select **Yes** on the first dialog to allow the wizard to reconfigure the cluster and then click **Next** for the remainder of the dialogs.

## Adding a new node to a cluster

If you want to add a new node to a cluster that is already running FMA, follow these steps.

1. Ensure the new node has access to all cluster disks.
2. Add the new node using Windows cluster administration tools.
3. Install FMA on the new node. The new node must already be a member of the cluster before installing FMA so that the installer completes the necessary cluster based configurations.
4. Go back to one of the other nodes in the cluster and run the FMA Cluster Setup wizard (select **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Cluster Setup**). Select **Yes** on the first dialog and then click **Next** on the remaining dialogs. Verify that the wizard shows all nodes that are expected to be in the cluster on the final dialog.
5. Move the cluster group to the new node and verify that the FMA Configuration service comes online. Refer to the information ([Evicting a node from a cluster](#) on page 17) on moving cluster groups.
6. Move all disk resources that are managed by FMA on this cluster to the new node.
7. Open the FMA configuration user interface and add the managed volumes to FMA management on the new node. Refer to [Managed Volumes](#) on page 45 for instructions on adding volumes.

## Configuring FMA

After you install FMA on file servers, you must set up the archives to store data and the managed volumes that FMA will manage. For information about archives, see [Archives](#) on page 25. For information about managed volumes, see [Managed Volumes](#) on page 45.

To view the user interface for configuring FMA, select **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu. Also, FMA configuration information is available in the Storage section of Computer Management on Server 2003 (32 bit) and in the Server Manager section on Server 2008 (32 bit).

## Upgrading FMA

The following upgrade paths are supported:

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

If you want to migrate a Windows 2003 cluster that includes FMA to a Windows 2008 cluster, see [Migrating a Windows 2003 cluster](#) on page 18.

### To upgrade FMA on a file server

1. Run **setup.exe**. This file is available on the installation CD.
2. In the confirmation dialog box, click **Yes**.
3. Follow the instructions in the installation wizard.

### To update a cluster

**WARNING** Window 2003 clusters cannot be upgraded to Windows 2008 clusters directly with this method. This is because of the differing requirements of the Windows 2003 server clusters and Windows 2008 failover clusters. See [Migrating a Windows 2003 cluster](#) on page 18 to prevent data loss.

1. Failover the cluster groups containing the managed volumes and resources of the default cluster group to another node.
2. Update the nodes in the cluster.
  - a. Run **setup.exe**. This file is available on the installation CD.
  - b. When prompted, confirm to install the new version.
  - c. After the installation is complete, click **Finish**.
  - d. If you are upgrading from FMA 2.1, click **Yes** to reboot the server. Wait until the node is active before continuing with the step 3.

If you are updating from FMA 2.2, a reboot is not required.

3. Repeat steps 1 and 2 on each node of the cluster.

Use the Windows cluster administration tools to view the status of the cluster group and the FMA service that was just updated. The cluster group should be online and it should contain the FMA configuration service. Viewing the cluster group is different depending on whether the system is based on Server 2003 or 2008:

- Server 2003:  
Run the `cluadmin` application. The default cluster group can be found under the Groups section.
- Server 2008:  
Run the `cluadmin.msc` application. Select the cluster name and then in the center pane expand the Cluster Core Resources section.

To verify that the File Migration Agent service and File Migration Agent AFM service are running on all nodes, run **services.msc** from the Windows Run menu and check the status of both services. The FMA configuration service only runs on the node that is hosting the Cluster Group.

## Migrating a Windows 2003 cluster

This section describes how to migrate a Windows 2003 cluster to a 2008 cluster configuration and FMA is installed in the cluster.

Before beginning this upgrade process, perform the following:

- Record the drive letter that is listed in FMA volume management.

- Use the `fmacli arc` command to record the list of archives with their IDs. The IDs are listed in the first column of the output of the command.

### To migrate an FMA cluster to 2008

1. Uninstall FMA 2.2 on each node of the 2003 cluster. Refer to [Uninstalling FMA](#) on page 20 for more information.
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 FMA 2.5 on each node of the 2008 cluster and configure it as described in [Installing FMA in a cluster configuration](#) on page 14.
4. Manage the volumes that were moved during the migration process. For more information on adding a volume to management, see [Creating managed volumes](#) on page 47.
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.

## Downgrading FMA

If you must downgrade from version 2.5 and 2.2.7 was previously installed, you must complete the following steps.

### To downgrade from 2.5 to 2.2.7

1. Uninstall 2.5 as described in [Uninstalling FMA](#) on page 20.
2. When prompted to save configuration settings, select **Yes**.
3. Insert the 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 FMA on file servers](#) on page 7. (You can ignore the Autopass warning about the higher version.) FMA 2.5 provides a new version of Autopass which is backward compatible with 2.2.

## Uninstalling FMA

Use the following steps to uninstall FMA.

### To uninstall FMA from a single file server

1. In the Windows Start menu, select **HP StorageWorks File Migration Agent→FMA Uninstall**.
2. After starting the uninstallation process, you are asked if you want to keep the current FMA configuration or if you want to completely uninstall the FMA software.

HP recommends selecting **Yes** to keep the current FMA configuration. If you select **No**, ensure that all migrated data from each managed volume have been successfully recalled. Otherwise, you will not be able to access released files.

3. If you are uninstalling version 2.1.x or older, you must reboot after uninstalling.

### To uninstall FMA from a cluster

1. Stop the File Migration Agent and File Migration Agent AFM services on every cluster node.
2. To remove the FMA configuration server cluster resource from the default cluster group, use the Windows cluster administration user interface, right-click the FMA resource (located in the Cluster Group by default) and click **Delete**. Removing this resource prevents the cluster group from failing.
3. Run the FMA uninstallation on all nodes. For more information, see [To uninstall FMA from a single file server](#) on page 20.
4. If you are uninstalling version 2.1.x or older, you must reboot after uninstalling.

**Note** If you are permanently uninstalling FMA as a single file server or as a cluster, examine the managed volumes carefully to ensure all metadata is removed. If necessary, run `fmacli erase` on the managed volumes to remove any remaining FMA metadata from the files.

## Removing the Explorer plugin

The FMA Explorer plugin is automatically registered during the installation process.

### To remove the plugin from Windows Explorer

On the command line, enter the following:

```
regsvr32 /u hsmext.dll
```

### To add the plugin to Windows Explorer

On the command line, enter the following:

```
regsvr32 hsmext.dll
```

# Licensing

---



## Enter FMA license keys

FMA includes a temporary license that allows use of the product for 60 days. Use this procedure to enter your permanent license keys.

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 pane.
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 appropriate to your system configuration.

Example #1: For a standalone configuration using HP Hardware, you will select T4275A.

Example #2: For a cluster configuration using HP Hardware, you will select T4276A.

5. Enter the IP address of the FMA server. Ensure that the IP address you use is the primary IP address of the FMA server. If you have a cluster configuration, using the virtual IP address does 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. You need to repeat this process for each node in your system.
6. Enter your e-mail address and password, and click **Sign-In**.

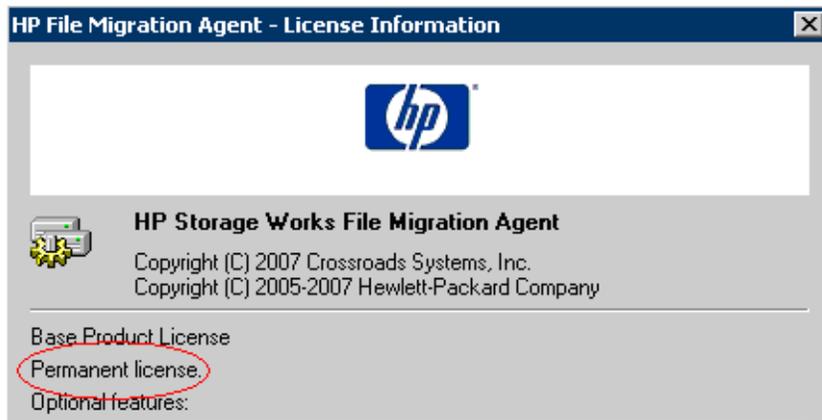
**Note** If this is the first time you are signing in to this website, you must create a password at this time.

7. Enter the appropriate contact information, and click **Next**, and 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\ directory
10. Open LicFile.txt in a text editing application, for example, Notepad.
11. On a new line, paste the license key that you copied from the Password Certificate.
12. Save and close the LicFile.txt file.

**Note** It is important that you do not delete the license from LicFile.txt. Make backup of this file after adding the license information.

13. Restart the File Migration Agent service.

14. Start FMA by selecting **Start → Programs → HP StorageWorks File Migration Agent→ FMA Configuration**.
15. Bring up the HP File Archiving software Configuration Utility, and select License information to verify that your permanent license was entered successfully.



*FMA License Information – Stand-alone Permanent License*

If you have a Cluster license or OpenStorage license, you will see Permanent license in the Optional features box. Otherwise, Not available will be shown in the status.

Here is an example of a success cluster license installed:



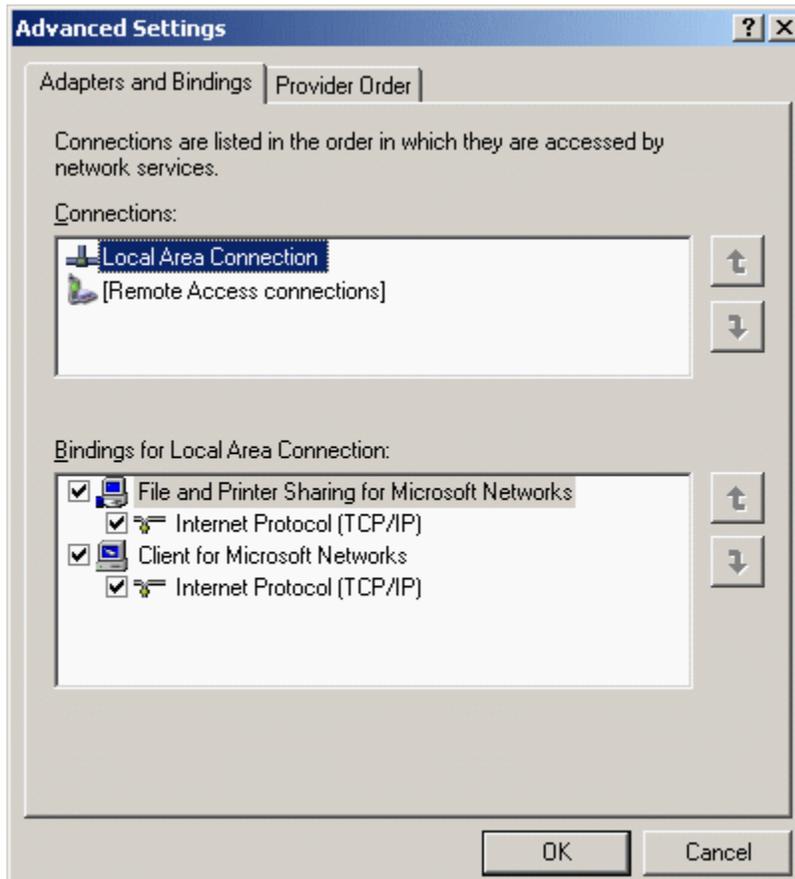
*FMA License Information – Cluster License*

**Note** There is a defect that currently does not display the values and status of the capacity license(s) in the License Information screen shown above. If you have a capacity license installed, rest assure that the capacity is being track by the FMA application.

## FMA licensing problems

If your permanent license keys are not active, verify that the connection for which you have requested the License keys is on top of the connections list. The order of the connections can be configured by right-clicking **My Network Places** and selecting:

**Properties** → **Network Connections** → **Advanced** → **Advanced Settings** → **Adapters and Bindings**



### *Advanced Settings dialog*

Use the up and down arrow keys to move the connection of the registered IP address to top of the connections list.

If you have a Cluster license or OpenStorage license, **Permanent license** is listed in the Optional features box. Otherwise, **Not available** is displayed as the status.



## Archives

---



Archives store data that FMA has migrated or released from managed volumes. FMA supports the following types of archives:

- Common Internet File System (CIFS), for Windows-based archives
- File Transfer Protocol (FTP), for Linux-based archives
- HP Integrated Archive Platform (IAP), for IAP archives

When you create an archive, you configure an FMA remote storage adapter (RSA) so that the archive can communicate with FMA. You must create the archive in the FMA user interface, but you can perform other archive operations using the FMA command line interface (FMACLI). For more information about the FMACLI, see [Command Line Interface Reference](#) on page 81.

### Primary and secondary configuration

When creating an archive, you are given the option of entering a primary and secondary archive path. The primary archive path is mandatory, and the secondary archive path is optional. When entering the primary archive path, you must choose the location of the archive where data is stored. You must choose the locations of the archives where data is stored. A *primary archive* is the location where FMA migrates data and the location from which it recalls data. You can choose to archive information from a managed volume to one or more primary archives. Using multiple independent archives provides failover security; if FMA cannot access one archive, it tries to access the other archives. When you use multiple archives, you should set a performance index for each. Performance index prioritizes the lowest number as the highest priority. For example, the performance index number 1 has a higher priority than index number 100. FMA attempts to recall a file from the archive with the smallest index number first.

An optional *secondary archive* replicates the primary archive and must be created outside of FMA using a replication mechanism. If the primary archive location becomes inaccessible, FMA retrieves data from the secondary archive. FMA does not migrate data to the secondary archive.

### Storage descriptors

A storage descriptor defines where a file is stored in the archive. The following is the default structure of the storage descriptor:

*ArchivePath\SystemName\VolumeSerial\LocalPath\FileName.Generation*

The following is an example of a storage descriptor:

D:\archives\system03\00471100\dir1\dir2\file1.dat.timestamp

When you create a CIFS or FTP archive, the system name and volume serial number in the storage descriptor are optional. HP recommends using the default structure unless you can ensure that the storage descriptor is unique without the system name or volume serial number.

During the creation of a CIFS or FTP archive, you are given the option to remove some of these descriptors:

- Ignore system Name
- Ignore Volume Serial
- Ignore Security
- Data Stream Only

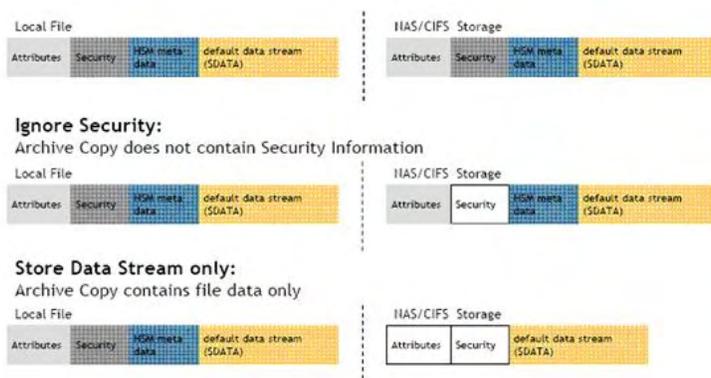
## Ignore Security and Data Stream Only

The process of migration is copying data from the File Migration Agent managed volume onto the selected archive target. When the **Ignore Security** and **Data Stream Only** options are selected, the 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.

For example:



## Ignore System Name and Ignore Volume Serial

When storing your data onto the archive, the default setting allows the FMA to track the following information regarding your data:

**<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**

- <Arc\_path> is the archive storage path.
- <Sys\_key> is the name of the local system. The default value is the name of the system when the archive was created. This does not change when System Name changes.
- <Vol\_SN> is the volume serial number the file belongs to.
- <Path> is the local path of the file at time of migration.
- <File\_Name> is the local file name at time of migration.
- <Gen> the new number incrementally generated each time a file with the same name exists.

The **Ignore system name** option removes the file server system name when creating the archive storage path. Similarly, **Ignoring volume serial** removes 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
```

## Viewing archives

You can view a list of archives and information about each archive.

### To view the list of archives

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Archives**.

In the right pane, the following information is displayed about each archive:

- Archive Name—The name of the archive, which identifies this archive for migration and recall operations.
- Archive ID—The unique, internal reference number for the archive, which is generated automatically and cannot be modified.
- Archive type—The type of archive:
  - RSA-CIFS for Windows-based archives
  - RSA-FTP for Linux-based archives
- RSA module—The module required for FMA to communicate with the archive.
- Performance Index—The order in which FMA recalls files from this archive. The range is 0-100, and the default is 100. If a file is stored on multiple archives, FMA attempts to recall it from the archive with the smallest index number first.
- Description—A description of the archive.
- Configuration—The primary and secondary hosts
- State—Whether the archive is accessible

## Adding archives to FMA in a cluster environment

If FMA is installed in a cluster environment, you must move all cluster resources, including the default cluster group, to a single node. Then, complete the steps in the following sections to create archives. After you have created the archives, redistribute the cluster resources.

## Creating CIFS archives

On a managed volume, a managed file contains file attributes, security information, Hierarchical Storage Management (HSM) metadata, and the default data stream. In CIFS archives, an exact copy of the managed file is archived by default.

**Note** To have exact copy of the managed file in the archive, the option "Ignore Security" and "Data Stream Only" options must NOT be selected during archive creation.

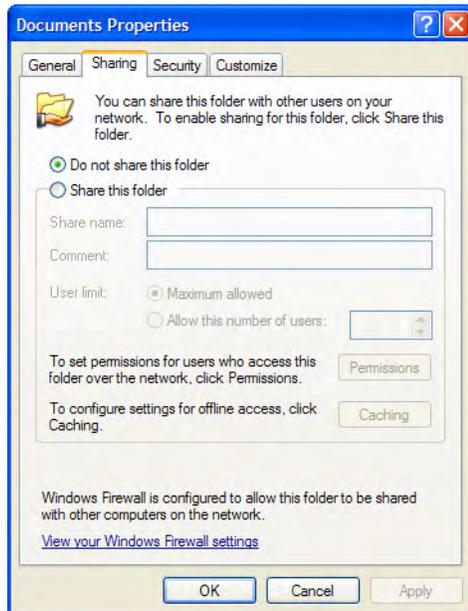
## Preparing CIFS archives for FMA

Before files can be saved to a CIFS-based Network Attached Storage (NAS) device, the archive folder on the NAS device needs to be shared on the network. By default, FMA only supports NTFS filesystems on Windows-based CIFS archives.

After sharing the appropriate folder on the NAS device, the NTFS permissions on the folder must be set to Full Control for the FMA technical user account. It is recommended that you restrict access to the share and allow only the FMA technical user and administrators access to the archive.

### To configure the NTFS permissions on the archive share

1. Right-click the CIFS share and select **Sharing and Security**.
2. In the Properties dialog box, click the **Sharing** tab.



3. Click **Share this folder**.
4. Click **Permissions**.

5. Add the technical user account that you established during installation. Give this user Full Control permissions.

For more information about the technical user account, see [Creating a technical user account](#) on page 5.

6. Click the **Security** tab.
7. Add the same technical user account with Full Control permissions.
8. Click **OK**.

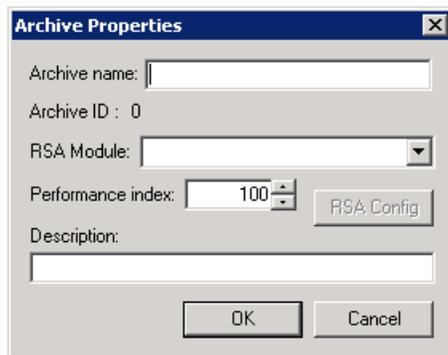
## Configuring CIFS archives

After you set up the archive share, you can configure the archive.

**Note** You can create an archive even if it is currently unavailable. This enables you to create definitions for archives that may be offline.

### To configure a CIFS archive

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Archives**.
3. In the right pane, right-click and select **New archive** from the context menu. The Archive Properties dialog box is displayed.



4. In the Archive Properties dialog box, enter the following information:
  - **Archive name**—The name of the archive, which identifies this archive for migration and recall operations and is used to refer to the archive for command line operations. You cannot include a space or semi-colon character in the name.
  - **RSA Module**—The module required for FMA to communicate with the archive. Select **RSA-CIFS**, which is required for CIFS archives.
  - **Performance Index**—The order in which FMA recalls from this archive. The range is 0-100, and the default is 100. If a file is stored on multiple archives, FMA attempts to recall it from the archive with the smallest index number first.
  - **Description**—A description of the archive.

In addition, this dialog box displays the Archive ID, which is the unique, internal reference number for this archive. It is generated automatically and cannot be modified.

5. Click **RSA Config**. The RSA Configuration dialog box is displayed.

**Rsa Configuration**

RSA - Adapter information

Name: RSA-CIFS

Description: Storage on local or remote (CIFS) file systems using UNC path specifications

Systemname: FILESERVER

Version: 2.5.0.10

Archive storage path

Primary Archive

Secondary Archive

Options

Ignore security on backend archive

Store data stream only

Ignore system name for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths across all systems that use this archive are unique.

Ignore volume serial for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths of ALL managed volumes are unique. A good example for such a case are home directories.

Test Save Cancel

6. In the Archive storage path area, enter the following information:
  - Primary Archive—The fully qualified NAS path to the location to which data is migrated and from which it is recalled. The specified path must exist and be specified using Universal Naming Convention (UNC) notation. Using a mapped drive is not recommended due to the limited visibility of the mapped drive for the service.
  - Secondary Archive—The fully qualified NAS path to the location from which data is recalled when the primary archive is not accessible. The specified path must exist and be specified using UNC notation. Using a mapped drive is not recommended due to the limited visibility of the mapped drive for the service. FMA does not replicate files to the secondary archive; you must perform this operation yourself.
7. In the Options area, select any of the following options if applicable:
  - Ignore security on backend archive—Select this option if you have a multi-domain environment in which security information should not be stored on the archive.
  - Store data stream only—Select this option to only store the default data stream on the archive. The default data stream refers to the file content and does not include any NTFS file metadata. This option is not recommended for normal Windows NAS devices.

- Ignore system name—Select this option if you do not want the storage descriptors for this archive to include the system name. This option is required for cluster systems. If you use this option, you must ensure that the storage descriptor is unique without the system name.
  - Ignore volume serial—Select this option if you do not want the storage descriptors for this archive to include the serial number of the local managed file system. If you use this option, you must ensure that the storage descriptor is unique without the volume serial number.
8. Click **Save**.
  9. In the Archive Properties dialog box, click **OK**.

## Creating FTP archives

On a managed volume, a managed file contains file attributes, security information, HSM metadata, and the default data stream. In FTP archives, the managed file is stored in an envelope.

Because of how the managed file is stored, no direct file access is available except through a packing and unpacking utility. For more information, see [Using FmaFileUtil to work with FTP archives](#) on page 37.

## Preparing FTP archives for FMA

FTP archives require additional configuration before they can be used with FMA. The RSA-FTP module uses FTP commands including the following, which are not supported on all servers:

- STOR (Defined in RFC765)
- RETR (Defined in RFC765)
- MDTM (Extension)
- SIZE (Extension)

The steps to make these commands available and to configure FTP archives to work with FMA vary depending on the FTP server and operating system, as described in the following sections. You must perform one of the following procedures.

## Configuring VSFTPD on SuSE Linux

Perform the following steps to enable an FMA-compatible FTP configuration with Very Secure FTP Daemon (VSFTPD) on SuSE Linux.

### To set up a new group and user

1. At the system prompt, enter the following to add a new user group with restricted rights to the system:

```
groupadd fma
```

2. Enter the following to add a user with minimal rights:

```
useradd -m -k /bin/false -d PartitionRoot -g fma -s /bin/false fma
```

where **-d *PartitionRoot*** is the root directory of the archive location, **-s /bin/false** prevents a login using telnet, and **-g fma** is the primary group of the FMA user.

3. Enter the following to change the password and activate the account:

```
passwd fma
```

4. Enter a new password.

### To take ownership of the PartitionRoot

At the system prompt, enter the following:

```
chown -R fma:fma PartitionRoot
```

### To activate inetd, the UNIX daemon that manages Internet services

1. Enter the following to start the YaST operating system setup and configuration tool with the corresponding parameter:

```
yast inetd
```

2. Enter the following to check whether inetd is already active:

```
ps ax | fgrep -i inetd
```

3. If inetd does not appear in the output of grep, enter the following to start inetd:

```
/etc/init.d/inetd start
```

### To configure VSFTPD

1. Activate the FTP server vsftpd in /etc/inetd.conf file. The entry is commented out by default.
2. Create a file named /etc/vsftpd.userlist.
3. Open the file and add all users that are allowed to access the FTP server.
4. Open the /etc/vsftpd.conf file for the FTP server and modify it to match the following:

```
/etc/vsftpd.conf
#----- Configuration used for FTPAccess of FMA
anonymous_enable=NO
local_enable=YES
write_enable=YES
dirmessage_enable=YES
xferlog_enable=YES
chroot_local_user=YES
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd.userlist
local_umask=027
```

5. At the system prompt, enter the following to trigger inetd to reread its configuration file:
 

```
killall -HUP inetd
```
6. Enter the following to convert all files with the **dos2unix** utility. This prevents problems caused by transferring these configuration files from a DOS filesystem to a UNIX filesystem.
 

```
dos2unix vsftpd.conf
dos2unix vsftpd.userlist
```

### To prevent uncontrolled growth of the vsftpd.log file using LogRotate

1. Create the /etc/cron.daily/logrotate file and use a text editor to add the following lines:
 

```
#!/bin/sh
/usr/sbin/logrotate /etc/logrotate.conf
```
2. Enter the following to make the file executable:
 

```
chmod +x /etc/cron.daily/logrotate
```
3. Create the /etc/cron.daily/logrotate.d/ivd file and use a text editor to add the following lines:
 

```
/etc/logrotate.d/ivd
Configuration for logrotate
/var/log/vsftpd.log
{
 compress
 size=500M
 rotate=5
}
```

where

- **compress** ensures that old versions of log files are compressed with gzip by default.
- **size=size** ensures that log files are rotated as they grow larger than the specified size. This size can be specified in bytes, kilobytes (k) or megabytes (M).
- **rotate=count** ensures that log files are rotated the specified number of times before being removed. If **count** is 0, old versions are removed rather than rotated.

## Configuring VSFTPD on Red Hat

Perform the following steps to enable an FMA-compatible FTP configuration with VSFTPD on Red Hat.

### To configure VSFTPD on Red Hat

1. Verify the /usr/sbin/vsftpd directory exists. If it does, continue with the step 2. If not, install it with the following steps:
  - a. Mount Red Hat Installation CD #1.
  - b. Change to the RedHat/RPMS directory.
  - c. Enter the following to add the package vsftpd-1.2.1-3.i386.rpm to the system:
 

```
rpm -ivh vsftpd-1.2.1-3.i386.rpm
```
2. Enter the following to create the fma user group:
 

```
groupadd fma
```
3. Enter the following to create the fma\_user FTP user:
 

```
useradd -d path -g fma fma_user
```

where **path** is the mount point of the archive.

4. Enter the following to change the password and activate the account:

```
passwd fma_user
```

5. Enter a new password.

6. Enter the following to change the user and group assignment of the archive:

```
chown -R fma_user:fma
```

This enables the `fma_user` user to write to the archive.

7. Add the `fma_user` user to the `/etc/vsftpd.user_list`, which contains all users that are allowed to access the archive using FTP.

8. In the `/etc/vsftpd/vsftpd.conf` file, modify or add the following parameters:

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
dirmessage_enable=YES
xferlog_enable=YES
chroot_local_user=YES
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd.user_list
local_umask=027
```

9. If parameter `xferlog_enable` is set to **YES**, remove the comment from the `xferlog_file=/var/log/vsftpd.log` parameter.

10. Enter the following to restart `inetd`:

```
/etc/init.d/xinetd restart
```

11. Enter the following to start `vsftpd`:

```
/etc/init.d/vsftpd start
```

The start/stop script is installed in `/etc/init.d/vsftpd`. The installation also creates symbolic links into different directories for different run levels, for example, `/etc/rc2.d/K50vsftpd`.

Because `vsftpd` is dependent on module `xinetd` (`K50xinetd`), the standard installation runs `vsftpd start` before `xinetd start` at next boot time, which will fail. Therefore, you must delete all symbolic links and add them properly by creating an appropriate symbolic link in the different run level directories.

For example, you would perform the following steps:

1. Change to the `/etc/rc2.d` directory.
2. Delete `K50vsftpd`.
3. Enter the following to create a new link:

```
ln -s ../init.d/vsftpd S99vsftpd
```

## To prevent uncontrolled growth of the `vsftpd.log` file using LogRotator

1. Create the `/etc/cron.daily/logrotate` file and use a text editor to add the following lines:

```
#!/bin/sh
/usr/sbin/logrotate /etc/logrotate.conf
```

2. Enter the following to make the file executable:

```
chmod +x /etc/cron.daily/logrotate
```

3. Create the /etc/cron.daily/logrotate.d/ivd file and use a text editor to add the following lines:

```
/etc/logrotate.d/ivd
Configuration for logrotate
/var/log/vsftpd.log
{
 compress
 size=500M
 rotate=5
}
```

where

- **compress** ensures that old versions of log files are compressed with gzip by default.
- **size=size** ensures that log files are rotated as they grow larger than the specified size. This size can be specified in bytes, kilobytes (k) or megabytes (M).
- **rotate=count** ensures that log files are rotated the specified number of times before being removed. If **count** is 0, old versions are removed rather than rotated.

## Configuring FTP archives

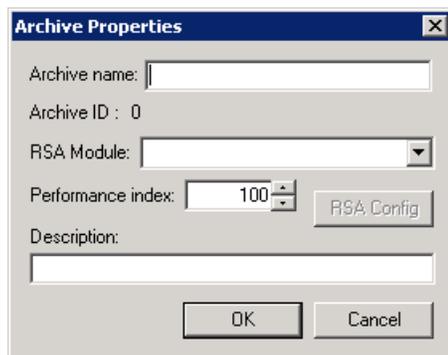
Use the following steps to create an FTP archive using GDSFTPserver for Windows.

**Note** You can create an archive even if it is currently unavailable. This enables you to create definitions for archives that may be offline.

### To configure an FTP archive

Ensure a GDSFTPserver has been installed and configured on the FTP archive before configuring the FMA server.

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Archives**.
3. In the right pane, right-click and select **New archive** from the context menu. The Archive Properties dialog box is displayed.



4. In the Archive Properties dialog box, enter the following information:
  - **Archive name**—The name of the archive, which identifies this archive for migration and recall operations. You cannot include a space or semi-colon character in the name.

- **RSA Module**—The module required for FMA to communicate with the archive. Select **RSA-FTP**, which is required for FTP archives.
- **Performance Index**—The order in which FMA recalls from this archive. The range is 0-100, and the default is 100. If a file is stored on multiple archives, FMA attempts to recall it from the archive with the smallest index number first.
- **Description**—A description of the archive.

In addition, this dialog box displays the Archive ID, which is the unique, internal reference number for this archive. It is generated automatically and cannot be modified. If you move a stub file between file servers, you must ensure that the archive ID remains unique.

5. Click **RSA Config**. The RSA Configuration dialog box is displayed.

**Rsa Configuration**

**Rsa information**

Name: RSA-FTP  
 Description: Storage on ftp server  
 Systemname: FILESERVER  
 Version: 2.5.0.10

**Ftp configuration parameters**

Host/IP:  Port:   
 Secondary Host/IP:   
 User:   
 Password:   
 Root path:   
 Connection timeout [ms]:  Data read timeout [ms]:

**Options**

Ignore system name for storage descriptor creation.  
 NOTE:  
 Choose this option only in case you can ensure that paths across all systems that use this archive are unique.

Ignore volume serial for storage descriptor creation.  
 NOTE:  
 Choose this option only in case you can ensure that paths of ALL managed volumes are unique. A good example for such a case are home directories.

6. In the FTP configuration parameters area, enter the following information:
  - **Host/IP**—The hostname or IP address of the FTP server to which data is migrated and from which it is recalled.
  - **Secondary Host/IP**—The hostname or IP address of the FTP server from which data is recalled when the primary archive is not accessible. FMA does not replicate files to the secondary archive; you must perform this operation.

- Port—The FTP port. The default port is 21.
  - User—The FTP user required to access the FTP server.
  - Password—The password used to access the FTP server.
  - Root path—The root path on the specified FTP server.
  - Connection timeout (ms)—The number of milliseconds after which the connection to the FTP server times out. The default value is 500 ms.
  - Data read timeout (ms)—The number of milliseconds after which reads on FTP data times out. The default value of 0 results in no timeout. Do not modify this setting except at the request of Technical Support.
7. Enter the following information in the Options area:
    - Ignore system name—Select this option if you do not want the storage descriptors for this archive to include the system name. This option is required for cluster systems. If you use this option, you must ensure that the storage descriptor is unique without the system name.
    - Ignore volume serial—Select this option if you do not want to the storage descriptors for this archive to include the serial number of the local managed file system. If you use this option, you must ensure that the storage descriptor is unique without the volume serial number.
  8. Click **Save**.
  9. In the Archive Properties dialog box, click **OK**.

## Using FmaFileUtil to work with FTP archives

FMA stores data in the archive in its own internal archive format. This prevents metadata from being lost as files are transferred from the NTFS-based Windows file server to the Linux archive. FmaFileUtil is a command line utility used for unpacking the envelope and restoring the local NTFS file.

The syntax for FmaFileUtil commands is as follows:

```
FmaFileUtil [options] command [command-options] arguments
```

The following options are available for FmaFileUtil:

| Option | Description                                                      |
|--------|------------------------------------------------------------------|
| -v     | Writes verbose ERROR, WARNING, or INFO messages to stdout.       |
| -L     | Writes ERROR messages to the log file.                           |
| -V     | Writes verbose ERROR, WARNING, or INFO messages to the log file. |
| -H     | Displays usage information for the command.                      |

If none of these options are used, all ERROR messages are written to stdout.

The FmaFileUtil pack and unpack commands are both available.

### pack

Creates a packed file based on an NTFS file.

#### Syntax

```
FmaFileUtil p[ack]
```

## Description

Creates a packed file based on an NTFS file. Its input is an NTFS file and its output is a file in the FMA storage format. All NTFS file information is included.

## Options

| Option             | Description                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>-f Filelist</i> | Converts all files listed in ( <i>Filelist</i> ).                                                                                                                                                                                                                                                                       |
| <i>-o</i>          | Overwrites existing destination files. By default, no files are overwritten.                                                                                                                                                                                                                                            |
| <i>-r</i>          | Recurse into directories.                                                                                                                                                                                                                                                                                               |
| <i>-p</i>          | Preserves timestamps. When unpacking a file, the original creation and modification timestamp is restored.<br><br>If this option is used without the <i>-o</i> option, FmaFileUtil only resets the timestamps of the destination file ( <i>dFile</i> ) to the timestamps preserved in the source file ( <i>sFile</i> ). |
| <i>sFile dFile</i> | Packs the source file ( <i>sFile</i> ) to destination file ( <i>dFile</i> ).                                                                                                                                                                                                                                            |
| <i>sDir dDir</i>   | Packs all files in the source directory ( <i>sDir</i> ) to the destination directory ( <i>dDir</i> ). The new files have the same name.                                                                                                                                                                                 |

## unpack

Creates an NTFS file based on a packed file.

## Syntax

```
FmaFileUtil u[npack]
```

Creates an NTFS file based on a packed file. Its input is a packed file and its output is an NTFS file. All NTFS streams saved in the packed file are written into the created NTFS file.

## Options

| Option             | Description                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>-f Filelist</i> | Converts all files listed in ( <i>Filelist</i> ).                                                                                                                                                                                                                                                                       |
| <i>-o</i>          | Overwrites existing destination files. By default, no files are overwritten.                                                                                                                                                                                                                                            |
| <i>-r</i>          | Recurse into directories.                                                                                                                                                                                                                                                                                               |
| <i>-p</i>          | Preserves timestamps. When unpacking a file, the original creation and modification timestamp is restored.<br><br>If this option is used without the <i>-o</i> option, FmaFileUtil only resets the timestamps of the destination file ( <i>dFile</i> ) to the timestamps preserved in the source file ( <i>sFile</i> ). |
| <i>sFile dFile</i> | Unpacks the source file ( <i>sFile</i> ) to destination file ( <i>dFile</i> ).                                                                                                                                                                                                                                          |
| <i>sDir dDir</i>   | Unpacks all files in the source directory ( <i>sDir</i> ) to the destination directory ( <i>dDir</i> ). The new files have the same name.                                                                                                                                                                               |

## Examples

```
FmaFileUtil pack File001.dat File001.dat.p
```

Packs the File001.dat file into the File001.dat.p file.

```
FmaFileUtil pack d:\Dir001 d:\tmp\Dir001.p
```

Packs all files in the d:\Dir001 directory into the d:\tmp\Dir001.p directory.

```
FmaFileUtil pack -r d:\Dir001 d:\tmp\Dir001.p
```

Packs all files in the d:\Dir001 directory and its subdirectories into the d:\tmp\Dir001.p directory.

```
FmaFileUtil unpack -p -oFile001.dat.p File001.dat
```

Unpacks the File001.dat.p file into the File001.dat file and restores the original timestamps. If the File001.dat file already exists, the File001.dat file are overwritten.

```
FmaFileUtil unpack -p File001.dat.p File001.dat
```

Resets the timestamps of the File001.dat destination file to the timestamps preserved in the File001.dat.p source file.

```
FmaFileUtil pack -o d:\Dir001 d:\tmp\Dir001.p
```

Packs all files in the d:\Dir001 directory into the d:\tmp\Dir001.p directory. If a destination file exists, it are overwritten.

```
FmaFileUtil unpack File001.dat.p File001.dat
```

Unpacks the File001.dat.p file into the File001.dat file.

```
FmaFileUtil unpack d:\Dir001.p d:\tmp\Dir001
```

Unpacks all files in the d:\Dir001.p directory into the d:\tmp\Dir001 directory.

```
FmaFileUtil unpack -r d:\Dir001.p d:\tmp\Dir001
```

Unpacks all files in the d:\Dir001.p directory and its subdirectories into the d:\tmp\Dir001 directory.

```
FmaFileUtil unpack -o d:\Dir001.p d:\tmp\Dir001
```

Unpacks all files in the d:\Dir001.p directory into the d:\tmp\Dir001 directory. If a destination file exists, it are overwritten.

## Creating HP Integrated Archive Platform archives

Any documents with a size of up to 1.47 GB (1,470,581,054 bytes) can be sent from a managed volume to the Integrated Archive Platform (IAP). On the managed volume, a managed file contains file attributes, security information, HSM metadata, and the default data stream. In IAP archives, managed file information is stored as a BLOB in the IAP object store.

Depending on FMA's RSA-IAP configuration, a specific set of metadata about the document can be attached to the binary object. FMA attaches the following metadata:

- File modification date
- MIME type of the file
- Full path name in UNC notation
- File security depending on FMA's recipients options
- Subject (filename without path and file extension)

The following additional metadata is attached for OLE compound documents, such as those generated with Microsoft Office 97 and later: title, subject, author, company, keywords, comments, last author, revision, created, last saved, name of application used, type, and extension.

FMA's recipients options and the Recipients field entries determine which IAP repositories are granted access to the binary object. The access information is retrieved from the document's Access Control List (ACL).

## Preparing IAP archives for FMA

FMA uses the ILM Object Storage API interface to access IAP archives. Before you create an IAP archive, you must configure the IAP system.

### Enabling integration

Applications integrating with HP IAP must have TCP/IP access to port 25 and port 80. To store email, the application requires the virtual IP addresses for each storage domain. To use the ILM Object Storage API, the application can use any HTTP IP address. These attributes are defined when the IAP device is initially configured and installed in the environment.

### Configuring IAP devices

An application requires an IAP repository and user to view BLOBs through the API. The application might require additional separate repositories and users if end users are using the IAP web interface to search for documents stored through the ILM Object Storage API. At a minimum, all BLOBs should be stored in the repository for the application. Applications can make information available to the individual users who own files if those users also have accounts automatically populated on IAP from the installation's user management LDAP server.

See the *HP StorageWorks Reference Information Storage System Administrator Guide* for instructions on adding users, data repositories, and ACLs between users and repositories. The administrator guide is available on the documentation CD and on the HP Business Support Center.

### Configuring computers on which FMA is installed

If data is stored with Windows Security Descriptor information, the computers on which FMA is installed must be configured with access to the active-directory server on the network.

### Enabling secondary sites

If the primary IAP site cannot accept any incoming traffic, FMA does not redirect the data traffic to the secondary replica site. FMA only supports one replica site, which is built by one-way (Active/Passive) IAP remote replication services.

## Configuring IAP archives

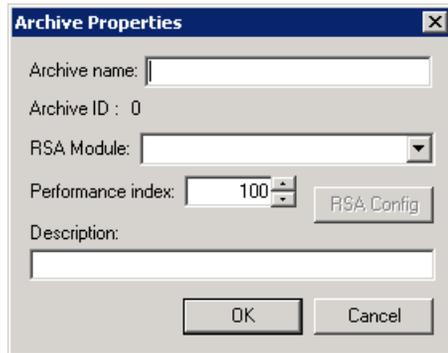
Use the following steps to create an IAP archive.

**Note** You can create an archive even if it is currently unavailable. This enables you to create definitions for archives that may be offline.

### To configure an IAP archive

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Archives**.

3. In the right pane, right-click and select **New archive** from the context menu.



4. In the Archive Properties dialog box, enter the following information:
  - Archive name—The name of the archive. You cannot include a space or semi-colon character in the name. This name identifies this archive for migration and recall operations.
  - RSA Module—The module required for FMA to communicate with the archive. Select **RSA-IAP**, which is required for IAP archives.
  - Performance Index—The priority in which FMA recalls from this archive. The default is 100. If a file is stored on multiple archives, FMA attempts to recall it from the archive with the smallest index number first.
  - Description—A description of the archive.

In addition, this dialog box displays the Archive ID—the unique, internal reference number for this archive. It is generated automatically and cannot be modified. If you move a stub file between systems, you must ensure that the archive ID remains unique.

5. Click **RSA Config**. The Rsa Configuration dialog is displayed:

**Rsa Configuration**

Rsa information

Name: RSA-IAP

Description: archive

Parameters

Primary IAP Host name:

Secondary IAP Host name:

Domain:

Default repository:

Recipients:

Recipients options

- The addresses of users contained in the ACL should not be added to the recipients list. This is the default.
- The addresses of users and groups defined in the "top" level of the ACL should be added to the recipients. Groups will not be expanded to include their users.
- The addresses of users and groups defined in the ACL, including those contained in any groups defined, are to be included in the recipients list.

Test Save Cancel

6. In the Rsa Configuration dialog box, enter the following in the Parameters area:
  - Primary IAP Host name—The hostname or IP address of the IAP system to which data is migrated and from which it is recalled
  - Secondary IAP Host name—The hostname or IP address of the IAP system from which data is recalled when the primary archive is not accessible  
You must replicate files to the secondary archive outside of FMA.
  - Domain—The IAP domain where data is stored
  - Default repository—The default repository where data is stored
  - Recipients—The default recipients for FMA data
  - Recipients options—Select one of the following:
    - The addresses of users contained in the access control list (ACL) should not be added to the recipients list. (Default)
    - The addresses of users and groups defined in the **top** level of the ACL should be added to the recipients. Groups are not expanded to include their users.
    - The addresses of users and groups defined in the ACL, including those contained in any groups defined, are to be included in the recipients list.

7. Click **Save**.
8. In the Archive Properties dialog box, click **OK**.

## Editing archive properties

You can edit archive properties to change the archive name, performance index, or description. You cannot change the archive ID or RSA module. While you can change the RSA configuration, you should do so with caution to ensure continued access to archive.

### To edit archive properties

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Archives**.
3. In the right pane, right-click the archive and select **Properties** from the context menu.
4. In the Archive Properties dialog box, edit the following as necessary:
  - **Archive name**—The name of the archive, which identifies this archive for migration and recall operations.
  - **Performance Index**—The order in which FMA recalls from this archive. The default is 100. If a file is stored on multiple archives, FMA attempts to recall it from the archive with the smallest index number first.
  - **Description**—A description of the archive.
5. To modify RSA-specific information, click **RSA Config** and modify the primary and secondary archive path and the options, as necessary.

**Note** Editing the RSA configuration is not recommended because it can prevent you from accessing data saved with the old configuration.

For information about the CIFS configuration, see [Configuring CIFS archives](#) on page 29. For information about the FTP configuration, see [Configuring FTP archives](#) on page 35. For information about the IAP configuration, see [Creating HP Integrated Archive Platform archives](#) on page 39.

Then, click **Save**.

6. In the Archive Properties dialog box, click **OK**.
7. If you changed the RSA configuration, restart the File Migration Agent service.

## Deleting archives

You can delete an archive and remove all of its data.

**WARNING** Prior to deleting an archive, be sure to recall any released files to prevent loss of access to data.

### To delete an archive

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Archives**.
3. In the right pane, right-click the archive and select **Delete** from the context menu.
4. In the confirmation dialog box, click **Yes**.

## Removing deleted files from archives

If deletion is supported by your archives, routinely run the `cleanup` command to remove archive entries that have been deleted from the file server. This command removes expired files and cleans up the archive. The `cleanup` command can only be run through the FMA CLI command line. Use the `cleanup` command carefully, as any files in the archive that does not have a file or a file stub associated with it will be deleted.

When a managed file is deleted on the file server, FMA moves metadata to the following garbage collection log: `\HSM Volume Information\SHsmGC.log`. When you run the `cleanup` command, you specify an expiration time for deleted files. FMA only deletes files from the archive if they were deleted prior to that expiration period. For example, if you run the `cleanup` command with an expiration time of 15 days, only files deleted from the file server more than 15 days ago are removed from the archive. The `cleanup` command cleans-up the garbage collection associated with multiple copies of a file, for example `file.001` and `file.002`.

For information about using the `cleanup` command, see [cleanup](#) on page 88.

## Managed Volumes

When you designate a volume as managed by FMA, its data can be migrated and released to one or more archives. You can manage any locally attached NTFS volumes with the exception of network drives, system volumes, and Microsoft cluster quorum disks.

You must designate managed volumes using the FMA user interface, but you can perform other operations related to the managed volume using the FMA command line interface (FMACLI). For more information about the FMACLI, see [Command Line Interface Reference](#) on page 81.

When FMA migrates a managed file, it saves a copy to one or more archives associated with the managed volume. Files can be migrated manually or through the user of policies that define the conditions under which files are migrated and released.

When FMA releases a file, it replaces the file on the file server with a stub file that points to the copies on the archives. FMA marks the file as offline using the Windows `FILE_ATTRIBUTE_OFFLINE` flag, which designates files with remote data. Windows 2008 Offline files can look different compared to [Figure 1: The Windows `FILE\_ATTRIBUTE\_OFFLINE` flag](#). Offline files typically take up to 4k in file sizes on the local drive.



*Figure 1: The Windows `FILE_ATTRIBUTE_OFFLINE` flag*

After files are migrated or released, users can continue to work with them on the file server. FMA automatically recalls released files when they are accessed.

## Viewing managed volumes

This section describes how to view a list of managed volumes and information about each volume using the FMA user interface. You can also view managed volume information from the FMA command line interface (FMACLI). FMA can support up to 80 managed volumes and display up to 128 drives on the FMA Configuration pane. Refer to [volume](#) on page 119 for more information.

### To view the list of volumes on the file server

1. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
2. In the left pane, select **Managed Volumes**.

In the right pane, the following information is displayed for each volume:

- Volume—The name of the volume and an icon that represents its current status

| Icon                                                                              | Status                 | Description                                                                                                                      |
|-----------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|  | Not managed            | Available but not managed by FMA                                                                                                 |
|  | Active                 | Managed by FMA                                                                                                                   |
|  | Stopped or Not Mounted | Managed by FMA but was stopped by a user, or the volume is not mounted. In a cluster, the volume can be mounted on another node. |
|  | Restricted             | System volume that cannot be managed                                                                                             |
|  | Error                  | A problem must be resolved to return the status to Active                                                                        |
|  | Reboot required        | The file server must be rebooted to return the status to Active                                                                  |

- Status—The current status
- File system—The file system
- Capacity—The amount of disk space in gigabytes
- Free Space—The amount of free disk space in megabytes
- % Free—The percentage of free disk space
- HSM Status—The volume status
  - Active—Managed by FMA
  - Inactive—Available but not managed by FMA, or management was stopped
  - Unknown—Cannot be managed by FMA
- PID—The process ID of the volume manager process
- Migrated bytes—The number of bytes migrated from this volume

### To view information about a particular volume

In the right pane, double-click the volume.

The following information is displayed in the Volume Properties area:

- Serial number—The volume serial number
- Mount point—The drive on which this volume is mounted
- Label—The volume label
- HSM status—The volume status
  - Active—Managed by FMA
  - Inactive—Available but not managed by FMA, or management was stopped
  - Unknown—Cannot be managed by FMA

- HSM process ID—The process ID of the FMA volume manager process
- File system type—The type of file system (FMA only supports NTFS volumes)
- Capacity—The amount of space available on the volume
- Free space—The amount of free space in gigabytes and as a percentage of total space
- Used space—The amount of used space in gigabytes and as a percentage of total space

In addition, you can view the following information for this volume:

- Disk space policies  
For information about setting disk space policies, see [Releasing files using disk space policies](#) on page 48.
- Scheduling information for policies  
For information about scheduling file policies, see [Scheduling file policies](#) on page 54.
- Migration policies  
For information about creating file policies, see [Creating file policies](#) on page 51.

## Creating managed volumes

Before you begin, ensure that the volume is a locally attached NTFS volume. FMA does not support network drives, system volumes, or Microsoft cluster quorum disks.

If FMA is installed in a cluster environment, you must perform additional steps, which are described in [To create a managed volume in a cluster environment](#) on page 47.

### To create a managed volume

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, right-click the volume you want to manage and select **Add to Management** from the context menu. (Note that the status of the volume changed to **Active**.)

Repeat this step for each volume you want to manage.

### To create a managed volume in a cluster environment

1. Move all cluster resources, including the default cluster group, to a single node.
2. Launch the FMA user interface by selecting **All Programs**→**HP StorageWorks File Migration Agent**→**FMA Configuration** from the Windows Start menu.
3. In the left pane, select **Managed Volumes**.
4. In the right pane, right-click the volume you want to manage and select **Add to Management** from the context menu. (Note that the status of the volume changed to **Active**.)

Repeat this step for each volume you want to manage.

5. Move the volume resources to the next node, and then repeat steps 2-4. Because FMA configuration information is stored on the volume, it is only necessary to add the volume to management. All other volume-based FMA settings configured in these steps are configured automatically.

**Note** For both Server 2003 and 2008 clusters, the resources can be moved to other nodes by right-clicking and selecting the Move operation in the cluster administration tool.

6. Repeat steps 2-5 until all volumes have been added to FMA management on all nodes.

## Releasing files using disk space policies

You can set disk space policies, which are watermarks and retention periods that define when files are released from a managed volume. You can also set an exclusion list of files that are not released, even if they meet the criteria in these disk space policies.

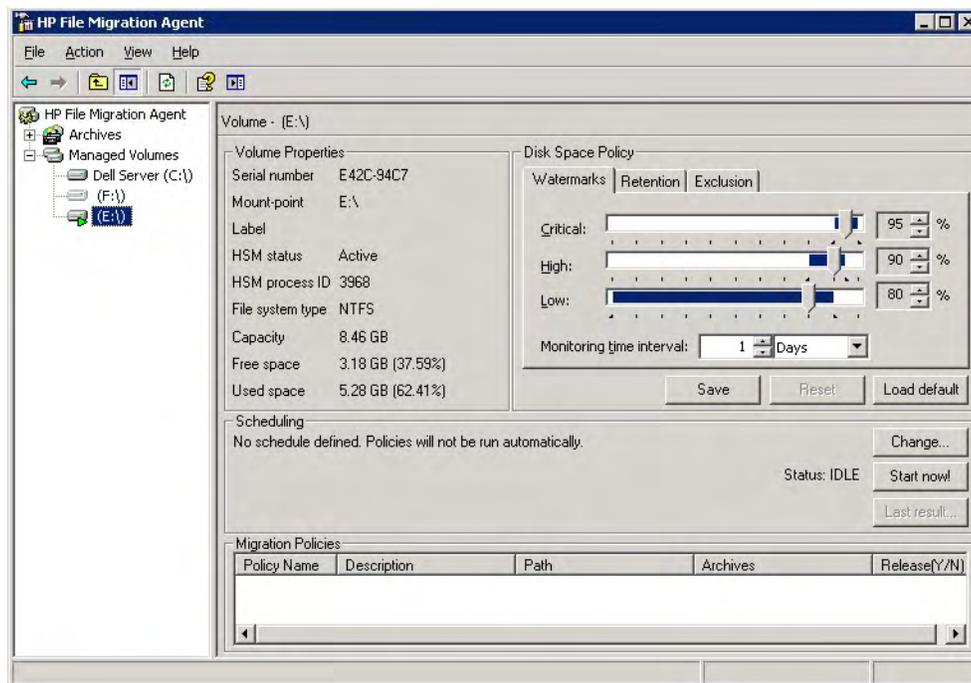
FMA monitors the disk space on each managed volume and releases files when the high watermark is reached. This release process continues until the low watermark is met or until no more files meet the retention criteria you define for the volume. When disk space reaches the critical watermark, all migrated files are released, regardless of the retention periods you have set.

### Setting disk space watermarks

Use these steps to create watermarks that define the files to be released as disk space fills.

#### To set watermarks for disk use

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume for which you want to set disk space watermarks. FMA displays information about that volume.



3. In the Disk Space Policy area, set the percentage of disk space that corresponds to the following watermarks:
  - Critical—When disk space reaches this watermark, FMA releases migrated files until the disk space reaches the low watermark.
  - High—When disk space reaches this watermark, FMA releases migrated files that meet the retention criteria you set. It stops releasing files when disk space reaches the low watermark.
  - Low—When disk space reaches this watermark, FMA stops releasing files.
4. From the Monitoring time interval drop-down lists, set the amount of time FMA waits before it checks disk space use.

**Note** The disk space policy interval counter starts running when the server is started. If the server is rebooted, the counter restarts.

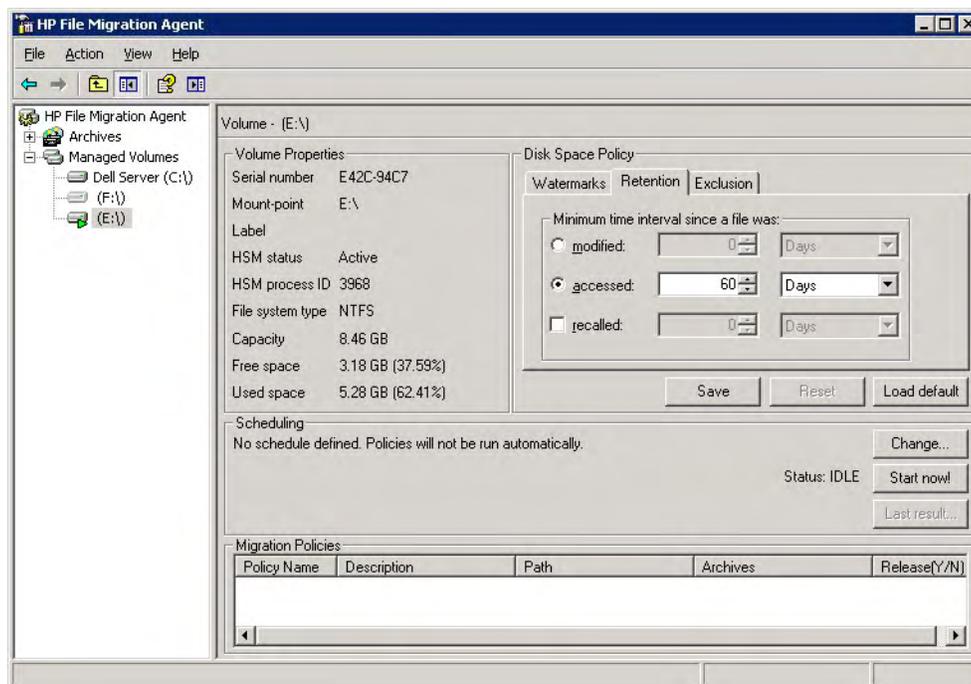
5. Click **Save**.

## Setting retention periods

Use the following steps to establish retention periods during which files are not released based on the high watermark.

### To set retention periods

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume on which you want to set retention periods. FMA displays information about that volume.
3. In the Disk Space Policy area, click the **Retention** tab.



4. Set the time interval for each of the following retention periods:
  - **modified**—When the high watermark is reached, migrated files that have been modified more than this number of days ago can be released. You cannot enable **accessed** if you enable **modified**.
  - **accessed**—When the high watermark is reached, migrated files that have been accessed more than this number of days ago can be released. You cannot enable **modified** if you enable **accessed**.
  - **recalled**—When the high watermark is reached, released files that were recalled more than this number of days ago can be released again.
5. Click **Save**.

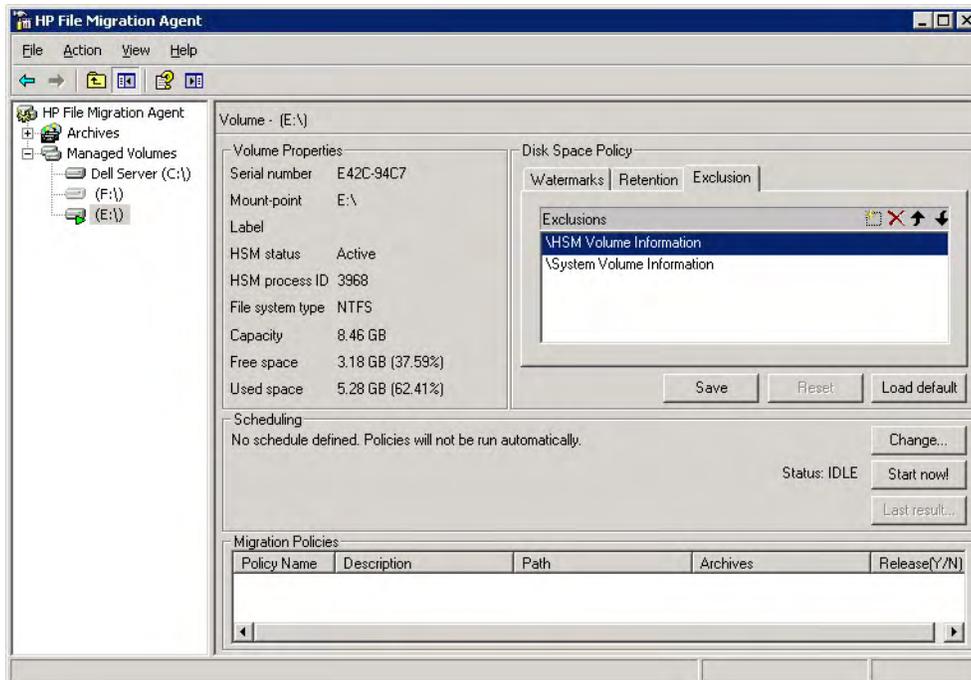
## Excluding files from release based on disk space

Use the following steps to specify a list of files that FMA must not release, regardless of whether they meet the criteria in the disk space policies.

**Note** Excluded files are also excluded from statistical summaries.

### To exclude files from release based on disk space

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume on which you want to exclude files from disk space policies. FMA displays information about that volume.
3. In the Disk Space Policy area, click the **Exclusion** tab.



By default the Exclusions list contains \HSM Volume Information and \System Volume Information.

4. Click  and then enter the absolute path to the folder or file you want to exclude from the release process. Do not enter the mount point (drive letter, such as "D:") or the mount path if the volume is mounted to another volume's directory ("D:\MountPoint"). The path should begin with "\".

You can use the asterisk (\*) wildcard to specify any number of characters of any value or the question mark (?) wildcard to specify exactly one character of any value.

Repeat this step for each folder or file you want to exclude.

5. Click **Save**.

## Migrating and releasing files using file policies

File policies define the conditions under which files are migrated to an archive or set of archives. You can define a file policy to migrate files in a managed volume based on any combination of file age, size, or name. Files are migrated to archives according to the order specified in the policy's archive list.

By default, a file policy applies to all files in the specified folder and its subfolders, but you can include or exclude specific files. Policies that are defined for a subfolder override the policies set at a higher level. Each folder can have multiple policies. In the event that two policies conflict with one another when using inclusion and exclusions, exclusion always takes precedence over inclusion policies.

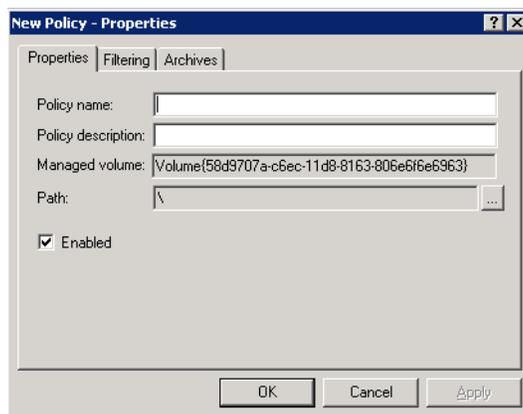
### Creating file policies

You can create a file policy for a single volume or a folder within a volume.

#### To create a file policy

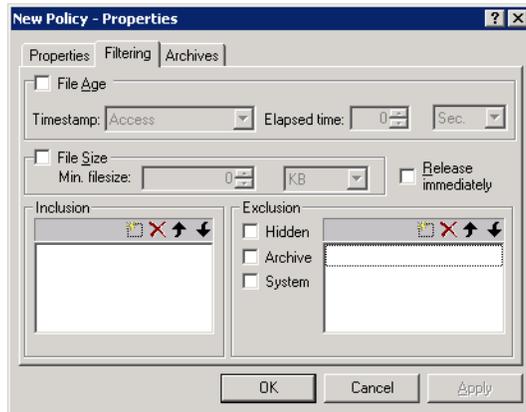
1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume on which you want to create a file policy.
3. In the right pane, right-click in the Migration Policies area and select **New**.

The New Policy dialog box is displayed.



4. On the Properties tab, enter the policy name and description.  
FMA automatically enters managed volume information.
5. To apply this policy to a folder rather than to the entire volume, perform the following steps:
  - a. Click **Browse (...)** next to the Path field.
  - b. In the Browse for Folder dialog box, select a folder and click **OK**.
6. To activate this policy, select **Enabled**.

7. Click the **Filtering** tab.



8. To migrate based on the age of a file, perform the following steps:
  - a. Select **File Age**.
  - b. Select one of the following from the **Timestamp** list:
    - Access—Files that have been accessed more than this number of days ago are migrated.
    - Modification—Files that have been modified more than this number of days ago are migrated.
    - Creation—Files that were created more than this number of days ago are migrated.
  - c. From the **Elapsed** time drop-down lists, set the number of seconds, minutes, hours, or days that FMA waits before it migrates files.
9. To migrate based on the size of a file, perform the following steps:
  - a. Select **File Size**.
  - b. From the **Min Filesize** drop-down lists, set number of kilobytes, megabytes, or gigabytes that the file must reach before it can be migrated.
10. If you want to release files as soon as they have been successfully migrated to all archives configured for the policy, select **Release immediately**.
11. To include specific files in this policy, perform the following steps in the **Inclusion** area:
  - a. Click .
  - b. Type the name of the file. You can use the asterisk (\*) wildcard to specify none or any number of characters of any value or the question mark (?) wildcard to specify exactly one character of any value.
12. To exclude hidden, archive, or system files, select the corresponding checkbox.

**Note** If you select the **Archive** checkbox, files that are ready to be archived (files for which the archive, or “A”, attribute is set) are excluded.  
Also, note that excluded files are excluded from statistical summaries.

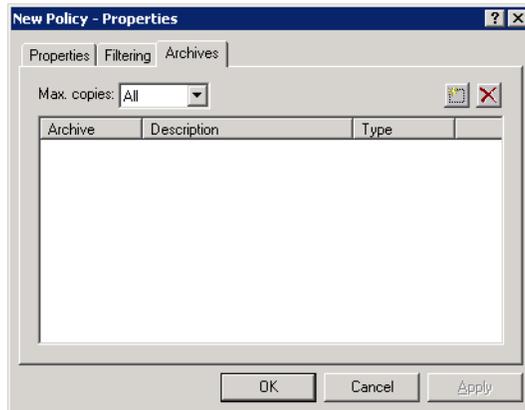
To exclude specific files, perform the following steps:

- a. Click .
- b. Type the name of the file. Do not enter the mount point (drive letter, such as “D:”) or the mount path if the volume is mounted to another volume's directory (“D:\MountPoint”). The path should

begin with “\”. You can use the asterisk (\*) wildcard to specify none or any number of characters of any value or the question mark (?) wildcard to specify exactly one character of any value.

**Note** The exclusion list takes precedence over inclusion list. If multiple criteria are specified, all of them must be met in order for a file to be excluded.

13. Click the **Archives** tab.



14. Use the following steps to set up to four archive locations where FMA migrates data. Using the following steps to setup the archive(s) location to which FMA migrates data. A maximum of four archive locations are recommended for migration of data.
  - a. Click .
  - b. In the Select archive dialog box, select up to four archives where files are migrated and click **OK**.
  - c. From the **Max copies** list, select the number of archives to which this file must be saved before it can be considered for release.
15. Click **OK**.

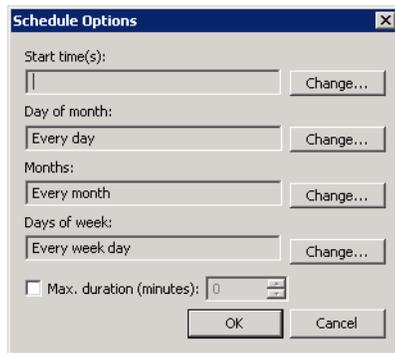
## Scheduling file policies

You can schedule a time when FMA runs all file policies for a specific volume.

**Note** If the server is offline when a policy is scheduled to start, the policy does not run again until the next scheduled time after the server is started.

### To schedule file policies

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume on which you want to schedule file policies.
3. In the Scheduling area, click **Change**.



4. In the Schedule Options dialog box, change the following information as necessary:
  - Start times—The time (in 24-hour notation) when FMA starts migrating files based on policies. If no start time is set, file policies are not processed for this volume unless they are run manually.
  - Day of month—The days of the month when FMA runs policies.
  - Months—The months when FMA runs policies.
  - Days of week—The days of the week when FMA runs policies.
5. To limit the duration of the policy run, select **Max duration (minutes)** and set the number of minutes that FMA spends running policies.
6. Click **OK**.

### To run policies manually

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume on which you want to run policies.
3. In the Scheduling area, click **Start now**.

## Editing file policies

You can modify file policies and define the files that they affect, but you cannot change the volume that they affect.

### To edit a file policy

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume that contains the policy.
3. In the right pane, right-click the policy in the Migration Policies area and select **Properties**.

For information about fields in the Policy dialog box, see [Creating file policies](#) on page 51.

## Enabling and disabling file policies

After you disable a policy, FMA does not apply it to the managed volume until you enable it again.

### To enable a file policy

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume that contains the policy.
3. In the right pane, right-click the policy in the Migration Policies area and select **Enable**.

### To disable a file policy

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume that contains the policy.
3. In the right pane, right-click the policy in the Migration Policies area and select **Disable**.

## Deleting file policies

### To delete a file policy

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. In the right pane, double-click the volume that contains the policy.
3. In the right pane, right-click the policy in the Migration Policies area and select **Delete**.
4. Select **Yes** to confirm the deletion.

## Migrating and releasing files with the Explorer plugin

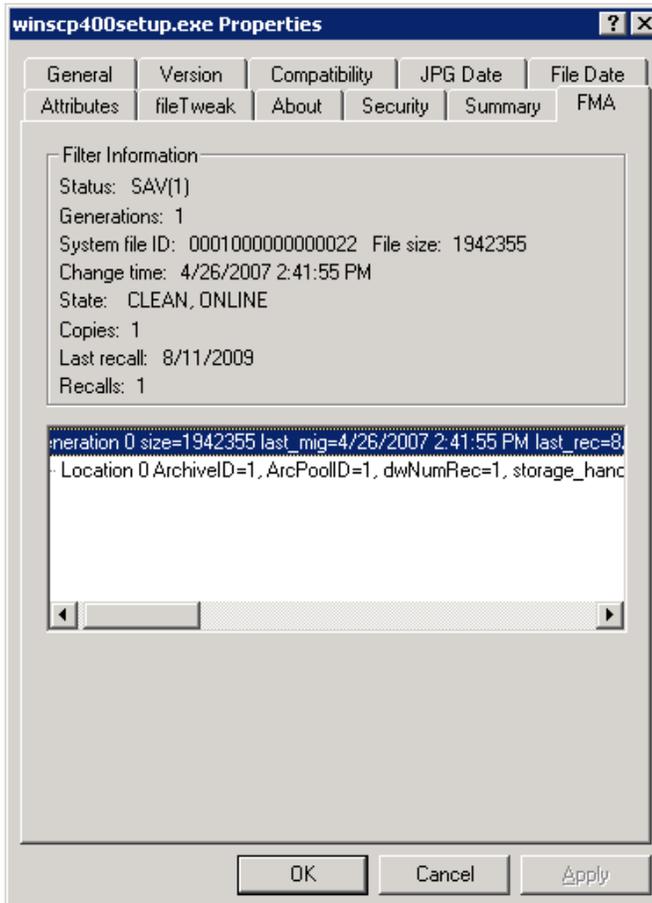
The Explorer plugin enables you to manually migrate, release, or recall files or folders from a managed volume on the local system. To access these commands in Windows Explorer, right-click a file or folder in a managed volume.

**Note** The 64-bit version of Explorer is not supported. You can run the 32-bit version of Windows Explorer, which is provided with 64-bit Windows, by entering the following from the Command Prompt window:

```
%systemroot%\SysWOW64\explorer.exe /separate
```

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

- State
- Copies
- Last recall
- Recalls



### **To view FMA file properties**

1. In Windows Explorer, select one or more files or a folder
2. Right-click to display the context menu and select **Properties**.
3. Click the **FMA** tab.

FMA displays the following information:

- **Status**—The current status of the file
    - OFF(n)—Offline
    - MOD(n)—Modified
    - SAV(n)—Migrated
    - INA(n)—Inactive
    - DIS(n)—Disabled
- (n) indicates the number of valid copies.
- **Generations**—The number of versions of this file that are archived
  - **System file ID**—The operating system ID number for the file
  - **File size**—The file size in bytes
  - **Change time**—The date and time when this file was last modified
  - **State**—The current status of the file
  - **Copies**—The number of copies of this file that are archived
  - **Last recall**—The last date and time when this file was recalled
  - **Recalls**—The number of times this file has been recalled

### **To migrate one or more files or a folder**

1. In Windows Explorer, select one or more files or a folder
2. Right-click to display the context menu and select **Migrate**.
3. Select the archive to which FMA should copy the data. If a command takes more than a few seconds, the Explorer plugin displays a progress bar.
4. In the Processing results dialog box, select **OK**.

### **To release one or more files or a folder**

1. In Windows Explorer, select one or more files or a folder.
2. Right-click to display the context menu and select **Release**.
3. If you are releasing a folder, set the following options in the Release options dialog box, as necessary:
  - **Min number of archive copies**—The minimum number of copies that must be migrated to the archive before the files can be released.
  - **Modified retention Time**—Files that have been modified more than this number of days ago can be released.
  - **Accessed retention time**—Files that have been accessed more than this number of days ago can be released.
4. Click **OK**.

## Recalling files

When users select a released file on the file server, FMA automatically recalls the file. Specifically, FMA must recall files when the “system” process reads the file contents. In addition, you can recall the file manually using the Explorer plugin.

If a file is migrated to multiple archives and FMA releases the file, the file is recalled from the last location to which it was migrated. The last location contains the most recent version of the file contents.

### To recall files or folders using the Explorer plugin

1. In Windows Explorer, select the objects you want to recall and right-click the selection.
2. In the context menu, select **Recall**.
3. In the Processing results dialog box, click **OK**.

## Moving files to another managed volume

You can move data from one managed volume to another using the `robocopy` command line tool, which is available from the Microsoft Resource Kit.

### Moving a small number of files

Moving files from one volume to another can be time-consuming. Use this procedure if you are moving a small number of files or if you have a large production downtime available.

### To move files to another managed volume

1. Ensure that the FMA archive configuration is identical on both file servers.
2. Obtain the **robocopy.exe** utility Version XP010 or higher by installing the Microsoft Resource Kit.
3. Add the NoRecRobocopy process name to the FMA registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Hewlett-Packard\HP FMA\IgnoreModules
4. Restart the File Migration Agent configuration service and File Migration Agent service.
5. Stop sharing the subfolder you want to move to avoid user access during relocation.
6. Ensure that all data is backed up.
7. Stop the File Migration Agent AFM service. This ensures that no migration jobs are running during the relocation process. If the target location is another FMA file server, stop the File Migration Agent AFM service on the other file server as well.
8. Disable the files in the source folder. Here is an example:  
FMACLI act --off -r e:\homedir  
To check whether the files are set to DIS (DISABLED), use the following command:  
FMACLI info -r e:\homedir
9. Copy the files using the `robocopy` command. Here is an example:  
robocopy e:\homedir f:\homedir /E /SEC /COPYALL /B
10. Ensure that all files have been copied successfully to the target location.
11. Activate the files in the target folder.

Activating a file means that the FMA metadata is synchronized to the new system file ID. This step enables the link to the archive copy and is performed from the FMACLI. For more information about the FMACLI, see [Command Line Interface Reference](#) on page 81.

```
FMACLI act -r f:\homedir
```

12. Delete the source folder.
13. Restart the File Migration Agent AFM service.

## Moving a large number of files

Use this procedure if you are relocating a large number of files and only a short production downtime is available. You run the command for disabling the files after the target folder has been enabled for user access and before the source folder is deleted. This decreases downtime by the processing time of the command for disabling the files.

This procedure is feasible under the following conditions:

- User and application access to the source folder must be permanently revoked before starting the relocation procedure.
- Do not allow user and application access to the target folder until all files have been activated using the FMACLI `act` command.
- You must ensure that the command for disabling the files in the source folder has been run before deleting them.

### To move a large number of files

1. Revoke access to the filesystems of the source and target folders.
2. Ensure that all data is backed up.
3. Stop the File Migration Agent AFM service. This ensures that no migration jobs are running during the relocation process. If the target location is on a remote FMA file server, stop the File Migration Agent AFM service on the remote file server as well.
4. Copy the data from the source folder using the `robocopy` command and check that all files have been copied successfully.

Example:

```
robocopy e:\homedir f:\homedir /E /SEC /COPYALL /B
```

5. Activate the files in the target location.  
FMACLI `act -r f:\homedir`
6. Grant access to the target location.
7. Deactivate the files in the source location.  
FMACLI `act --off -r e:\homedir`
8. Delete the files in the source location.
9. Restart the File Migration Agent AFM service.

## Stopping volume management

When you stop volume management, FMA cannot access the released files stored in the archive until you restart volume management. Stopping volume management is rarely required unless you want to prevent

FMA from managing it (remove volume management) or you want to address an issue on the volume, as directed by Technical Support.

### **To stop managing a volume**

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. Right-click on the volume you want to stop managing and select **Stop** from the context menu. The status for this volume has changed to **Stopped**.

## **Restarting volume management**

After you stop volume management, you can restart it to restore access to the files stored on the archive.

### **To start managing a volume**

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. Right-click on the volume you want to start managing and select **Start** from the context menu. The status for this volume changed to **Active**.

## **Removing volume management**

**WARNING** Before you discontinue FMA management of a volume, be sure to recall all migrated files to ensure against data loss. After you remove volume management, you can no longer access the files stored on the archive.

### **To stop FMA management of a volume**

1. In the left pane of the FMA user interface, select **Managed Volumes**.
2. Right-click on the volume you want to stop managing and select **Stop** from the context menu. The status for this volume changed to **Stopped**.
3. Right-click on the volume again and select **Remove from Management** from the context menu. The status for this volume changed to **Not managed**.

## Best Practices

---

# 6

### Create a new HP StorageWorks File Migration Agent (FMA) archive

#### FMA archive configuration for a Windows FTP archive

##### Prerequisites

For archiving data to a Windows-based HP StorageWorks File System Extender (FSE) Archive, the GDS FTP-Server needs to be set up on the FSE Archive.

The GDS FTP-Server comes with its own user management facilities. Therefore, the FTP authentication process is completely controlled by the GDS FTP-Server and no Windows domain user account needs to be created for the FTP client access.

Because the GDS FTP-Server runs as a Windows service, user access to the FTP server's home directory can be restricted to designated administrators of the domain.

The absolute path to the archive directory is composed of the root directory, which is specified in the configuration file `ftp_server.cfg` of the GDS FTP-Server, and the root path set up in the FMA's RSA-FTP configuration dialog. If a root path is defined on the client side (FMA), the administrator needs to create this subdirectory during the GDS FTP-Server configuration.

The absolute path to the archive directory in the following example should be:

```
c:\fsefs1\data\fma
```

##### Example of the GDS FTP-Server configuration file `ftp_server.cfg` file

```
[default]
RootDirectory = c:\fsefs1
Port = 21
UserFile = C:\program files\Hewlett-Packard\FTPServer\GDSftpServerUsers
LogFile = C:\program files\Hewlett-Packard\FTPServer\GDSftpServer.log
```

## FMA RSA-FTP Configuration dialog

**Rsa Configuration**

**Rsa information**

Name: RSA-FTP  
Description: Storage on ftp server  
Systemname: W2K3R2  
Version: 2.1.0.1076 ALPHA-1

**Ftp configuration parameters**

Host/IP: IAF1 Port: 21  
Secondary Host/IP:   
User: fma  
Password:   
Root path: /data1/fma  
Connection timeout (ms): 500 Data read timeout (ms): 0

**Options**

Ignore system name for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths across all systems that use this archive are unique.

Ignore volume serial for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths of ALL managed volumes are unique. A good example for such a case are home directories.

Save Cancel

For archiving data directly to c:\fsefs1, the root path of the FMA RSA-FTP configuration menu needs to be left blank.

Verification of the GDS FTP-Server configuration can be done with any FTP client software.

After the FTP server side has been tested successfully, the next step is to attach FMA as an FTP client to the new archive storage location. For this, the following actions are necessary:

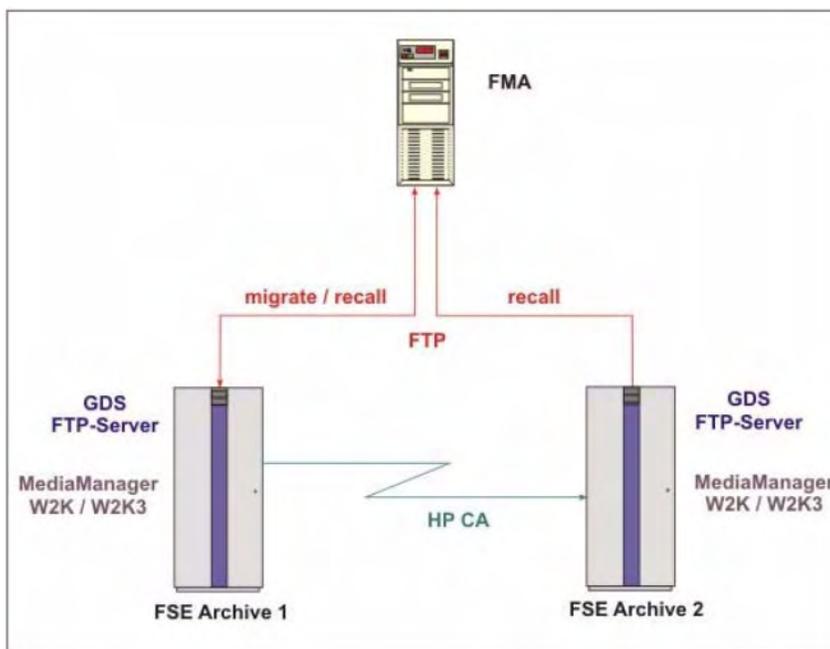
1. Start FMA MMC Snap-In from Windows Start menu. (**Start** → **Programs** → **HP StorageWorks File Migration Agent** → **FMA Configuration**)
2. Select the **Archives** item.
3. Start the context menu and select the item **New**. A new dialog is displayed.
4. Enter the name for the new archive. The archive name must be unique.
5. Select **RSA-FTP** as RSA module.
6. Enter the performance index. Typically, smaller the index, the higher the priority.
7. Enter an archive description.
8. Click **OK**. A new dialog is displayed.
9. Enter the following settings corresponding to the requirements:
  - Host or IP address (primary and secondary host)
  - Port (default: 21)

- User
- Password
- Root path
- FTP server
- Connection timeout in ms
- Data read timeout in ms
- Select various options

10. Click **Save**. The new FMA archive is shown in the FMA MMC Snap-In list.

The creation of a new FMA archive is finished.

If the backend archive is replicated outside of FMA via some replication mechanism such as the HP Continuous Access (HP CA) for the FSE Archive, the host name or IP address of the secondary system needs to be added to the entry field Secondary Host/IP.



In this case recall requests are switched to the secondary system, when the primary archive is not accessible.

Note that the primary and secondary archive configuration (FTP user ID, FTP server configuration and archive directory structure) must be identical.

**Rsa Configuration**

Rsa information

Name: RSA-FTP  
Description: Storage on ftp server  
Systemname: W2K3R2  
Version: 2.1.0.1076 ALPHA-1

Ftp configuration parameters

Host/IP: IAF1 Port: 21  
Secondary Host/IP: IAF2  
User: fma  
Password: \*\*\*\*\*  
Root path: /data1/fma  
Connection timeout [ms]: 500 Data read timeout [ms]: 0

Options

Ignore system name for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths across all systems that use this archive are unique.

Ignore volume serial for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths of ALL managed volumes are unique. A good example for such a case are home directories.

Save Cancel

**Note** For further information about managing FMA archives, see [Archives](#) on page 25.

## FMA archive configuration for an Linux FTP archive

For archiving data to a Linux-based FSE Archive, the VSFTPD needs to be set up on the FSE Archive.

The absolute path to the archive directory is composed of the FTP user's home directory and the relative path, which is configured in the FMA RSA-FTP configuration dialog.

The first part of the absolute path to the archive is specified during the creation of the FTP user on the Linux system. The command

```
useradd -m -k /bin/false -d /fma/hmsfs1 -g fma -s /bin/false fma
```

defines the directory `/fma/hmsfs1` as the home directory for the FTP user `fma`. The second part of the absolute path to the archive directory is set up in the FMA RSA-FTP configuration dialog.

In this example, the complete path to the archive directory is /fma/hsmfs1/data1/fma.

**Rsa Configuration**

Rsa information  
Name: RSA-FTP  
Description: Storage on ftp server  
Systemname: W2K3R2  
Version: 2.1.0.1076 ALPHA-1

Ftp configuration parameters  
Host/IP: IAF1 Port: 21  
Secondary Host/IP:   
User: fma  
Password:   
Root path: /data1/fma  
Connection timeout [ms]: 500 Data read timeout [ms]: 0

Options  
 Ignore system name for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths across all systems that use this archive are unique.  
 Ignore volume serial for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths of ALL managed volumes are unique. A good example for such a case are home directories.

Save Cancel

After the FTP server side has been tested successfully, the next step is to attach FMA as an FTP client to the new archive storage location. For this, the following actions are necessary:

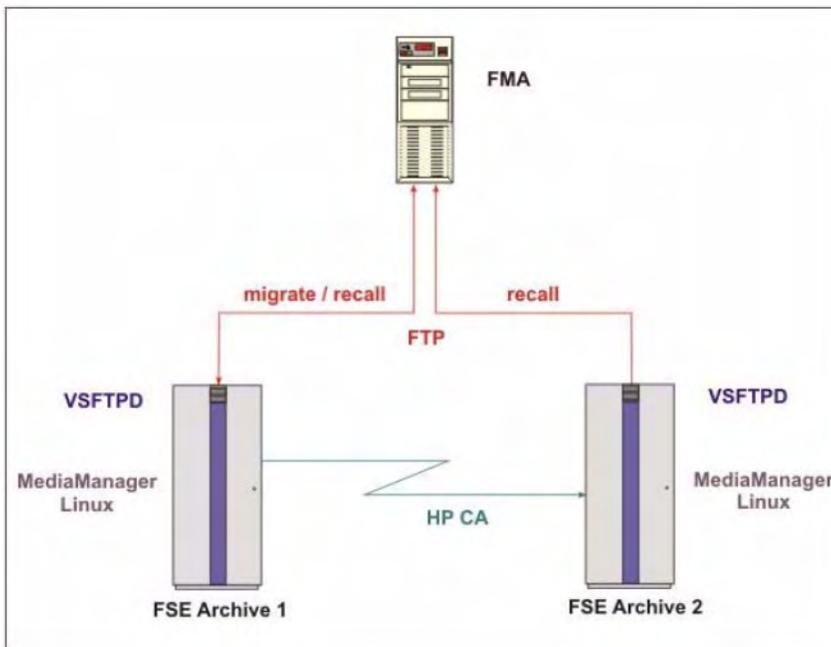
1. Start FMA MMC Snap-In from Windows Start menu. (Start → Programs → HP StorageWorks File Migration Agent → FMA Configuration)
2. Select the **Archives** item.
3. Start the context menu and select the item **New**. A new dialog is displayed.
4. Enter the name for the new archive. The archive name must be unique.
5. Select **RSA-FTP** as RSA module.
6. Enter the performance index. Typically, the smaller the index, the higher the priority.
7. Enter an archive description.
8. Click **OK**. A new dialog is displayed.
9. Enter the following settings corresponding to the requirements:
  - Host or IP address (primary and secondary host)
  - Port (default: 21)
  - User
  - Password
  - Root path

- FTP server
- Connection timeout in ms
- Data read timeout in ms
- Select various options

10. Click **Save**. The new FMA archive is shown in the FMA MMC Snap-In list.

The creation of a new FMA archive is finished.

If the backend archive is replicated outside of FMA via some replication mechanism such as the HP CA for the FSE Archive, the host name or IP address of the secondary system needs to be added to the entry field Secondary Host/IP.



In this case recall requests are switched to the secondary system, when the primary archive is not accessible.

Note that the primary and secondary archive configuration (FTP user ID, FTP server configuration and archive directory structure) must be identical.

**Rsa Configuration**

Rsa information

Name: RSA-FTP  
Description: Storage on ftp server  
Systemname: W2K3R2  
Version: 2.1.0.1076 ALPHA-1

Ftp configuration parameters

Host/IP: |AF1 Port: 21  
Secondary Host/IP: |AF2  
User: |ma  
Password: [masked]  
Root path: /data1/|ma  
Connection timeout [ms]: 500 Data read timeout [ms]: 0

Options

Ignore system name for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths across all systems that use this archive are unique.

Ignore volume serial for storage descriptor creation.  
NOTE:  
Choose this option only in case you can ensure that paths of ALL managed volumes are unique. A good example for such a case are home directories.

Save Cancel

**Note** For further information about managing FMA archives, see [Archives](#) on page 25.

## FMA archive configuration for a CIFS-based NAS device

For archiving data to a CIFS-based NAS device, the archive folder on the NAS device needs to be shared on the network. FMA only supports NTFS file systems on CIFS archives.

After sharing the appropriate folder on the NAS device, the NTFS permissions on the folder must be set to FULL Control for the FMA technical user account (see [Creating a technical user account](#) on page 5) or the corresponding group.

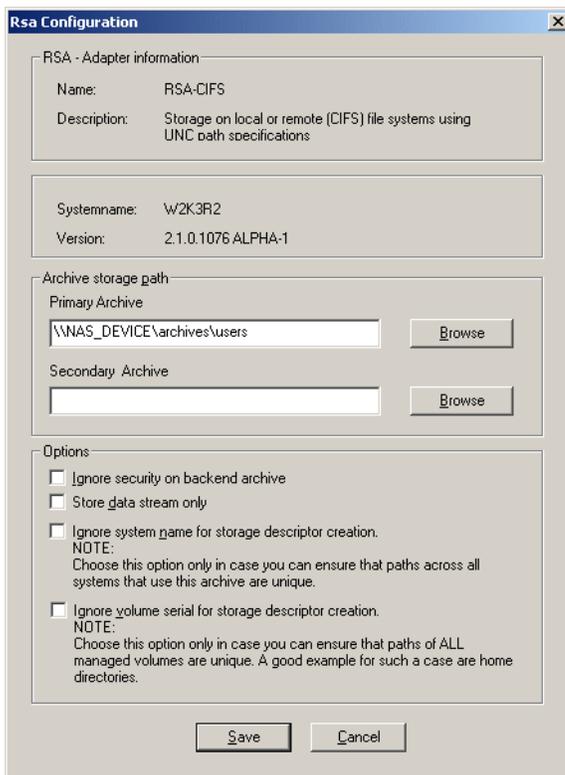
The absolute path to the archive location can be configured in FMA's RSA-CIFS dialog.

Example:

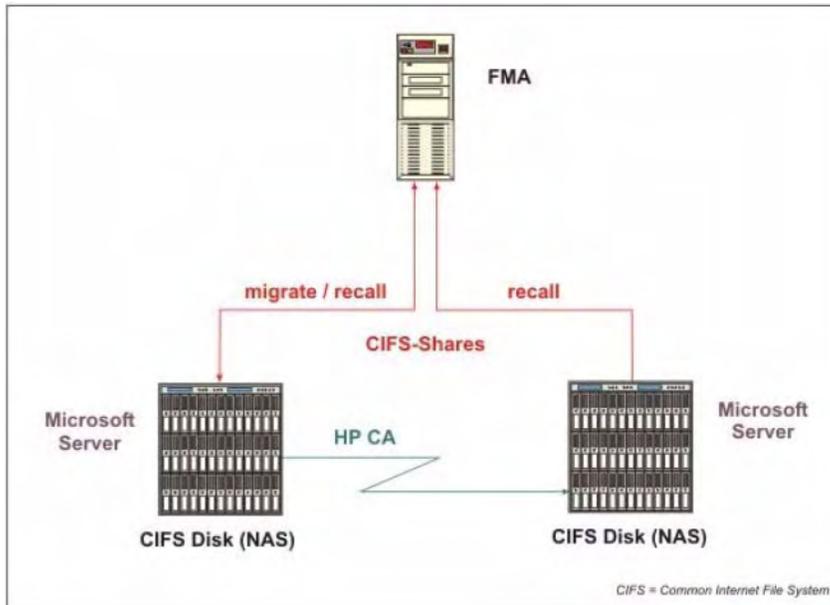
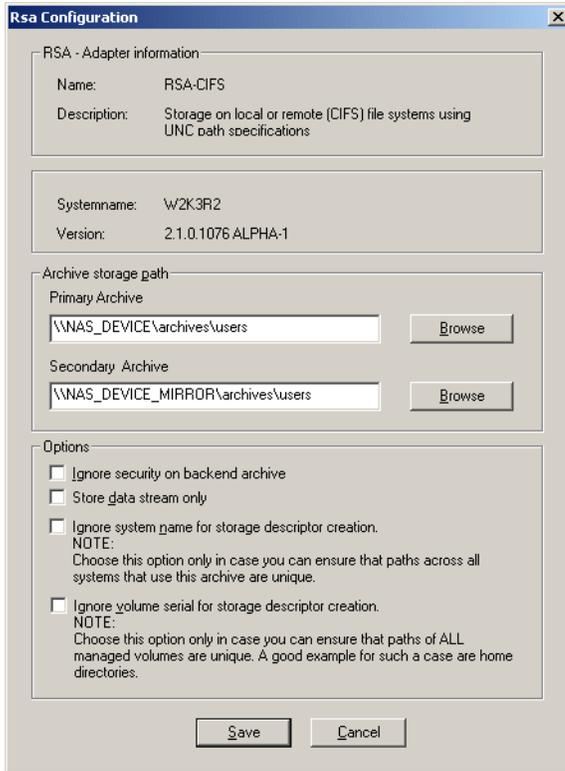
If the share *archives* has been created on the NAS device *NAS\_DEVICE*, subsequent archives can be set up through FMA RSA-CIFS configuration:

```
\\NAS_DEVICE\archives\users
```

```
\\NAS_DEVICE\archives\projects
```



If the backend archive is replicated outside of FMA via some replication mechanism the UNC path of the target location needs to be added to the entry field Secondary Archive. In this case recall requests are switched to the secondary archive location, when the primary archive is not accessible.



## FMA archive configuration for IAP

FMA is using the ILM Object Storage API interface for accessing the HP Integrated Archive Platform (IAP) as a backend archive.

Any documents with a size of up to 1.58 GB can be sent from an FMA managed volume to the IAP. Depending on FMA's RSA-IAP configuration, a specific set of metadata about the document can be attached to the binary object. The following metadata is attached by FMA:

- File modification date
- MIME type of the file
- Full path name in UNC notation
- File security depending on FMA's recipients options
- Subject (file name without path and file extension)

FMA's recipients options and the Recipients field entries determine which IAP repositories are granted access to the binary object. The access information is retrieved from the document's Access Control List (ACL).

**Rsa Configuration**

Rsa information

Name: aaa

Description: qqq

Parameters

Primary IAP

Host name: IAP1

Secondary IAP

Host name:

Domain: mydomain

Default repository: fma01@mydomain

Recipients:

Recipients options

The addresses of users contained in the ACL should not be added to the recipients list. This is the default.

The addresses of users and groups defined in the "top" level of the ACL should be added to the recipients. Groups will not be expanded to include their users.

The addresses of users and groups defined in the ACL, including those contained in any groups defined, are to be included in the recipients list.

Test Save Cancel

Documents are automatically retrieved from the IAP, when a user or application accesses the document on the FMA managed volume. To search for documents, users can use the IAP Web Interface embedded in a standard IAP solution.

If a IAP is mirrored on a remote location using the IAP Replication Manager, the host name or IP address of the replica site needs to be entered to the input field Secondary IAP. In this case FMA retrieves data from the

replica site, when the primary IAP is not available. If the primary IAP site can not accept any incoming traffic, FMA does not redirect the data traffic to the replica site.

**Rsa Configuration**

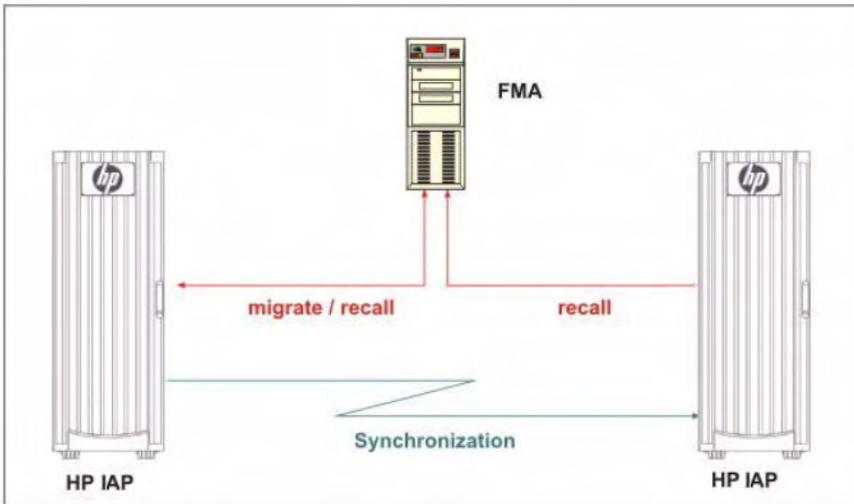
Rsa information  
Name: aaa  
Description: qqq

Parameters  
Primary IAP Host name: IAP1  
Secondary IAP Host name: IAP2  
Domain: mydomain  
Default repository: fma01@mydomain  
Recipients:

Recipients options  
 The addresses of users contained in the ACL should not be added to the recipients list. This is the default.  
 The addresses of users and groups defined in the "top" level of the ACL should be added to the recipients. Groups will not be expanded to include their users.  
 The addresses of users and groups defined in the ACL, including those contained in any groups defined, are to be included in the recipients list.

Test Save Cancel

FMA only supports one replica site, which is built by one-way (Active/Passive) IAP remote replication services.



## Create a new managed volume

To create a new managed volume:

1. Start FMA MMC Snap-In from Windows Start menu. (Start → Programs → HP StorageWorks File Migration Agent → FMA Configuration)
2. Select the Managed Volumes item. All NTFS volumes are displayed.
3. Right-click the corresponding volume entry to display the context menu.
4. Select the New item in the context menu.
5. Reboot the FMA system now.
6. The creation of a new managed volume is finished.

**Note** For further information about managing volumes, see [Managed Volumes](#) on page 45.

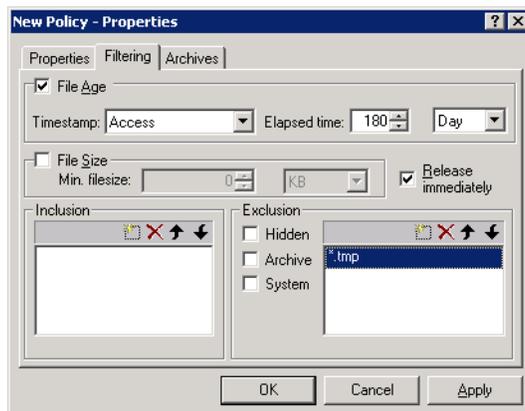
## Create file policies

To create and schedule migration rules on a managed volume:

1. Start FMA MMC Snap-In from Windows Start menu. (Start → Programs → HP StorageWorks File Migration Agent → FMA Configuration)
2. Select the Managed Volumes item.
3. Double-click the corresponding volume entry to display the Policy Configuration window.
4. Right-click the Policies pane to display the context menu and select New.
5. Enter a policy name and policy description, and select the path, for which the policy should be applied.
6. Set up the migration rules on the Filtering tab.

Example:

- Migrate all files that have not been accessed for 180 days and release the files immediately.
- Files with the extension \*.tmp are excluded from migration.



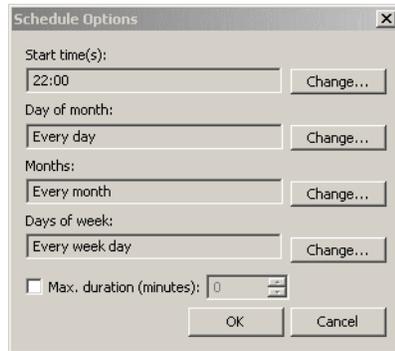
7. Select the archives, where data needs to be stored, and click **OK**.
8. After all policies are configured for the managed volume, set up the schedule for policy processing by clicking **Change** in the Scheduling pane.



9. Policy processing can be scheduled to be run hourly, daily, weekly or monthly and at any point in time to suit your business needs.

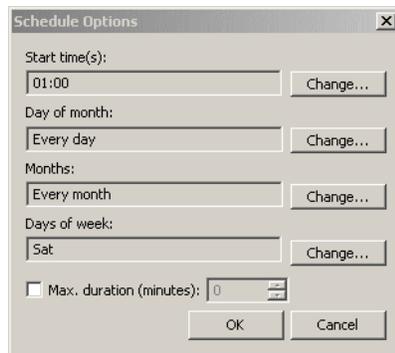
Examples:

- Start policies every day at 10:00 p.m.



- Start policies every Saturday at 01:00 a.m.

(Select Every day on Day of month, if policies should run on certain days of week.)



- Start policies on the 1st of every month.

(Select Every week day, if policies should run on certain days of month.)



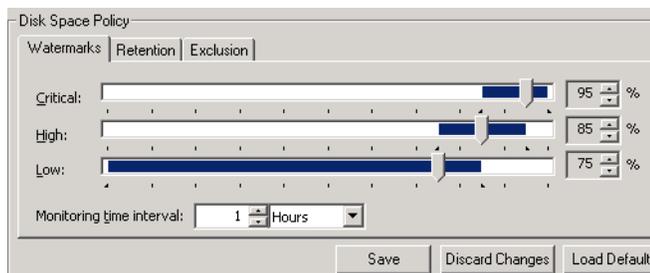
## Create disk usage monitoring

To set up the disk space monitor on a managed volume:

1. Start FMA MMC Snap-In from Windows Start menu. (Start → Programs → HP StorageWorks File Migration Agent → FMA Configuration)
2. Select the Managed Volumes item.
3. Double-click the corresponding volume entry to display the Policy Configuration window.
4. Files are released when the high or critical watermark threshold is reached. The policy ensures that the monitored managed volume never causes a DISK FULL error. The release operation is based on the configured retention times and the configuration for excluded files and directories.

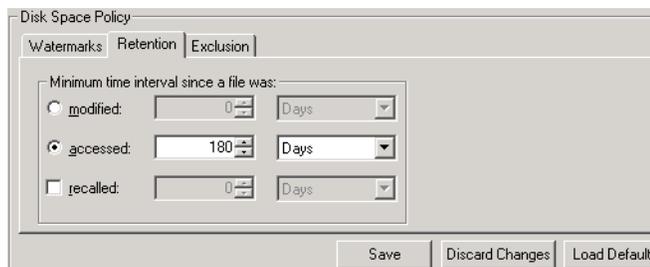
Example:

For an optimal usage of the managed volume, the following watermarks are defined:

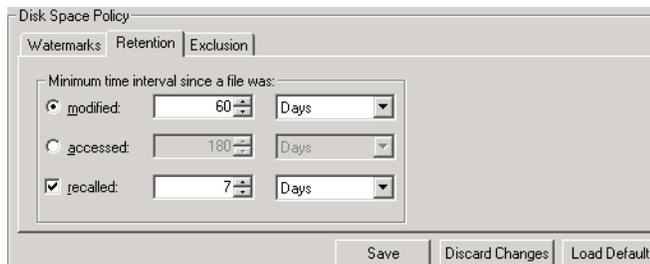


The disk space is monitored every hour and when the disk utilization reaches 85%, files which have not been accessed for 180 days are not released until the low watermark is reached.

If the critical watermark is hit, the release process is no longer limited by the defined retention criteria until the high watermark is reached.



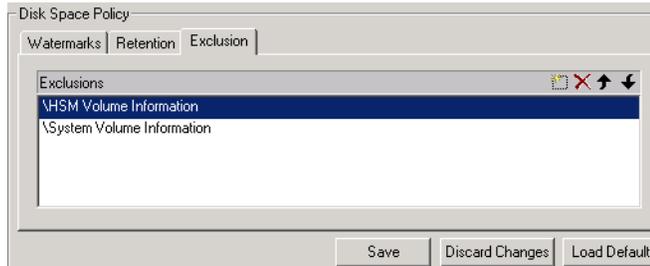
If the retention time period is based on the modification timestamp of a file, HP recommends specifying a retention time for recalled files to avoid unnecessary recalls.



In this example recalled files are kept online for a minimum of 7 days, although the files have not been modified for 60 days.

This configuration guarantees a fast access to files for a certain time period since the files have been recalled.

Files which should always be online, can be excluded.



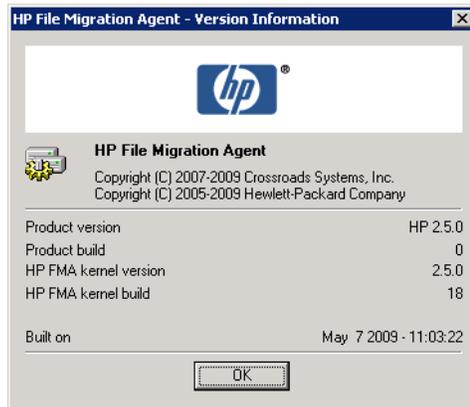
## Determine FMA software version

To display the current version of FMA software components:

- Enter `FMACLI sys` in the command line. On top of the output, the current version is displayed:

```
HP Storage Works File Migration Agent
Version 2.5.1.0
HP File Migration Agent command line interface
Copyright (C) 2007-2009 Crossroads Systems, Inc.
Copyright (C) 2005-2009 Hewlett-Packard Company
Version of HP File Migration Agent kernel 2. 5. 0. 17
System status = 0, installPath=[C:\Program Files\Hewlett-Packard\HP
FMA]
HSM API Version = 2.5.0-0017 ""
License Information:
=====
+ Serial number S-
+ Base Product License Evaluation license expiration in 59 days
+ OpenStorage Option Evaluation license, capacity (avail/used) 1000
GB / 0 GB.
+ Cluster Option Evaluation license.
Config:
Loglevel for eventlog: LOG_WARNING
Loglevel for logfile: LOG_INFO
Number of log files: 100
Options:=00000000
```

- Or view the version information for (almost) each FMA file by looking at the files in the Windows File Explorer. Right-click the file, click **Properties**, and click the **Version** tab.
- Or click **About HP FMA** in the menu of the FMA MMC Snap-In.



- For further information, see the Readme.txt file. To read the Readme.txt file, use the shortcut: **Start** → **Programs** → **HP StorageWorks File Migration Agent** → **FMA Readme**.

## Migrate files

To migrate files:

- Use the FMA CLI command-line utility to migrate files.

```
FMA CLI migrate f:\testdir\test.* -a myArchive
```

In the following example, the testdir directory is migrated into the myArchive archive:

```
FMA CLI migrate -r f:\testdir -a myArchive
```

- To migrate a directory to more than one archive (max. 4), apply:

```
FMA CLI migrate -r f:\testdir -a myArchive, myArchive02
```

- To migrate a directory with immediately release operation after successfully migrating of the directory, apply:

```
FMA CLI migrate -r f:\testdir -a myArchive -n1 --release
```

You can also migrate files using the FMA Explorer plug-in.

## Release files

- To release files:

Use the FMA CLI command-line utility to release files.

```
FMA CLI release f:\testdir\test.* -n 1
```

In the following example, the testdir directory is released:

```
FMA CLI release -r f:\testdir -n 1
```

You can also migrate files using the FMA Explorer plug-in.

## Recall files

- To recall files:  
Use the FMACLI command-line utility to recall files.  

```
FMACLI recall f:\testdir\test.*
```

  
In the following example, the testdir directory is recalled:  

```
FMACLI recall -r f:\testdir
```

  
You can also migrate files using the FMA Explorer plug-in.

## Set a high-watermark for migration or releases

- To set a high-watermark for migration or release:  
Use the FMACLI command-line utility. In the following example, the testdir directory is released when the fill level of the file system (85 percent) is reached.  

```
FMACLI release -r f:\testdir -u 85
```

## Verify data files

- To verify FMA metadata information:  
Use the FMACLI command-line utility to check whether the FMA metadata of a file object is consistent.  

```
FMACLI verify f:\testdir\test.dat -o local
```
- To check all files of a directory, apply:  

```
FMACLI verify -r f:\testdir -o local
```
- To check if the link to the archive copy of a file is valid, apply:  

```
FMACLI verify f:\testdir\test.dat -o remote
```

## Schedule FMA commands

- To schedule an FMA command:  
Use the AT command-line utility of Windows. In the following example, the FMA release command starts at 10 a.m.:  

```
at 10:00 "FMACLI release -r f:\testdir -n 2"
```

**Note** For further information about the AT command-line utility, see the documentation for Microsoft Windows.

You can use the Scheduled Task Wizard in the Windows Control Panel (**Start** → **Control Panel** → **Scheduled Tasks**) for these tasks also.

## Schedule FMA jobs

- To schedule FMA jobs, use the Scheduled Task Wizard in the Windows Control Panel (**Start** → **Control Panel** → **Planned/Scheduled Tasks**) for scheduling the FMA job.
- Or, you can use the following command-line tools for scheduling an FMA job.

In this example, the FMA job starts every Sunday (Su) at 03:00 a.m.

```
schtasks /create /ST 03:00 /D Su /TN "C:\Progr..\MyJob.cmd"
```

**Note** For further information about the AT or SCHTasks command-line utility, see the documentation for Microsoft Windows.

## Backup/restore concept for FMA managed volumes

FMA is a hierarchical storage management (HSM) solution and, therefore, not a replacement for data backup. The major purpose for backup is to ensure recovery of data on the server if a disaster occurs. The main goal of HSM is to better manage data storage costs.

FMA migrates files to other forms of storage and creates copies of files, but does not back up files on the server. When FMA releases files, only stubs are left on the managed file system, which point FMA to the exact location in the backend storage, enabling file retrieval and user access.

To provide data protection, third-party backup applications are absolutely essential for disaster recovery. The qualified third-party backup applications are HSM-aware, which means that stubfiles are backed up without causing recalls from backend storage. Because FMA stubfiles are created as Windows sparse files, a further requirement for backup applications is the appropriate processing of sparse files to avoid heavy network traffic and to minimize the backup window.

Concepts for organizing the back up of FMA managed volumes:

- Protect all data on the server—To accomplish this, the backup process needs to be set up to the *incremental forever* mode and the release of FMA jobs needs to be scheduled after the backup process to ensure that files are backed up before becoming a stubfile. In this case it is most likely that the capacity of the saved data exceeds the capacity of the original locations on the managed volumes. Therefore, release operations trigger during a disaster recovery or massive restore of saved data. HP recommends adjusting the monitoring time interval (for example, 10 minutes) and watermarks accordingly.
- Speedy backup/restore processing—In this scenario, data backup needs to be configured to periodically run full backups with subsequent incremental backups. This approach reduces the backup data volume and backup/restore time period compared to a non-HSM managed filesystem with the same data capacity and number of files.

**CAUTION:** When backing up stubfiles, it is very important that FMA's cleanup expiration time must be set equal to the expiration time that is configured for the backed up files. The FMA cleanup function removes the archive copies of deleted files depending on the specified cleanup expiration time. In this context, the expiration time, which is specified for the backend storage, also needs to be configured appropriately.

FMA does not support multiple references to one archive file copy. Only one stubfile can be linked to one archive copy. As a result of this restriction, restore operations of files to an alternate location are not permitted by FMA. Backed up files from FMA managed volumes can only be restored to their original location.

## Relocating data to another FMA managed volume

Copying data to another FMA managed volume needs to be run by the **robocopy.exe** command-line tool, which is available from Microsoft's Resource Kit.

To avoid recall operations during copying of the data, HP recommends creating a duplicate of the robocopy utility. Name the duplicate **NoRecRobocopy.exe**. Add the process name NoRecRobocopy to the list of modules for which FMA enables a physical view to the file system.

Therefore, the following steps are necessary:

1. Install the **robocopy.exe** utility Version XP010 or higher by installing Microsoft's Resource Kit.

```

ROBOCOPY :: Robust File Copy for Windows :: Version XP010

```

2. Create the NoRecRobocopy command:

```
copy <InstPath>\robocopy.exe %SYSTEMROOT%\system32\NoRecRobocopy.exe
```

3. Add the process name NoRecRobocopy to FMA's registry key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP FMA\IgnoreModules
```

4. Restart the FMA services:

- File Migration Agent config service
- File Migration Agent service

**Note** When moving data to other server systems, ensure that the FMA archive configuration is identical on all systems.

## Relocating data procedure

This section describes the steps that are needed to copy a subdirectory from an FMA managed volume to another FMA managed volume either local or remote. Assume that you want to relocate a subdirectory named e:\homedir to f:\homedir.

1. Stop sharing the subdirectory to avoid user access during the relocation process.
2. Ensure that the data has been backed up.
3. Disable the files in the source directory.

Description:

When a *disabled* file is deleted, no entry is written to the *garbage collection* container and, therefore, the corresponding archive copy is not deleted during an FMA cleanup run. Additionally, recall operations are rejected on *disabled* files.

```
FMACLI act --off -r e:\homedir
```

(Check whether the files are set to DIS (DISABLED), use the command FMACLI info -r e:\homedir.)

4. Use the appropriate NoRecRobocopy command now.

Example:

```
NoRecRobocopy e:\homedir f:\homedir /E /SEC /COPYALL
```

(Check that all files have been copied successfully to our target location.)

5. Activate the files in the target directory.

Description:

Activating a file means that FMA's metadata is synchronized to the new system file ID. This step enables the link to the archive copy.

```
FMACLI act -r f:\homedir
```

6. Delete the source directory

## Relocating a large number of files

If the relocation process is required for a large number of files and only a short production downtime is available, the command for disabling the files can also be run after the target directory has been enabled for user access and before deleting the source directory. In this case, the downtime is decreased by the processing time of the command for disabling the files.

This procedure is feasible under the following conditions:

- User and/or application access to the source directory must be permanently revoked before starting the relocation procedure.
- User and/or access to the target directory must be avoided until all files have been activated using the command **fmacti act**.
- The administrator must guarantee that the command for disabling the files in the source directory has been run before deleting them.

Steps for relocating a large number of files:

1. Revoke access to the file systems of the source and target directories.
2. Ensure that the data has been backed up.
3. Copy the data using the NoRecRobocopy command and check that all files have been copied successfully.

Example:

```
NoRecRobocopy e:\homedir f:\homedir /E /SEC /COPYALL
```

4. Activate the files in the target location.

```
FMACLI act -r f:\homedir
```

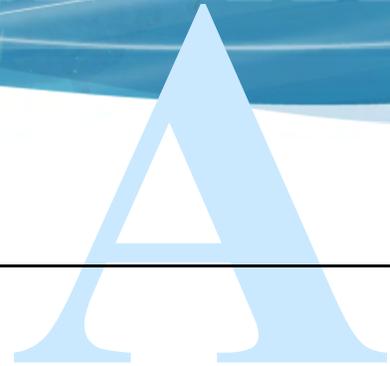
5. Grant access to the target location.
6. Deactivate the files in the source location.

```
FMACLI act --off -r e:\homedir
```

7. Delete the files in the source location.

## Command Line Interface Reference

---



The FMA command line interface (FMACLI) provides access to most FMA functions and can be used instead of the user interface to manage data. The FMACLI is implemented in the FMACLI.exe module. It writes informational output to stdout and errors to stderr. Keep this in mind when redirecting output for logging purposes.

This section uses the following typographical conventions:

- **Bold** is used for command names and arguments in text.
- Monospace is used for command names and arguments in syntax and for code.
- *Monospace italic* is used for variables within command syntax, code, or command-line text.
- Brackets [ ] and braces { } are used for optional information.

### FMA commands

The syntax for FMACLI commands is as follows: `FMACLI [command] [command-options]`.

Use `FMACLI` or `FMACLI --help` to list the available commands, which include the following:

| Command                 | Description                                                             | CLI only |
|-------------------------|-------------------------------------------------------------------------|----------|
| <code>act[ivate]</code> | Repairs metadata file IDs after restore                                 | X        |
| <code>arc[hive]</code>  | Displays a list of defined archives                                     |          |
| <code>cle[anup]</code>  | Removes the archived replicas of deleted files and reorganizes archives | X        |
| <code>era[se]</code>    | Deletes FMA metadata                                                    | X        |
| <code>inf[o]</code>     | Displays FMA metadata                                                   |          |
| <code>mig[rate]</code>  | Migrates files to specified archives                                    |          |
| <code>pol[icy]</code>   | Displays or runs a file policy                                          |          |
| <code>rec[all]</code>   | Recalls data for released file                                          |          |
| <code>rel[ease]</code>  | Releases data for files                                                 |          |
| <code>rsa</code>        | Displays a list of storage adapters and their status                    |          |
| <code>sys[tem]</code>   | Displays FMA-related information and settings                           |          |

| Command   | Description                                     | CLI only |
|-----------|-------------------------------------------------|----------|
| ver[ify]  | Displays the result of the verification process | X        |
| vers[ion] | Displays FMA version and build information      |          |
| vol[ume]  | Displays information about available volumes    |          |

Most commands can be shortened on the first three letters (for example, **mig** instead of **migrate**). Only the **version** command needs four letters (**vers**) to define the short form. There is no short form for the **find** command. In addition, many command parameters have a short form. For example, **--help** and **-h** are interchangeable.

All commands return 0 on successful completion and a non-zero value in failure situations.

## activate

Sets the file ID in the metadata to the current ID of the file.

### Syntax

```
FMACLI act[ivate]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
 [file] | [{--filelist} | -f} filelist]
 [{--recursive | -r} path]
 [--oem-file-format | --unicode-file-format | --ansi-file-format |
 --utf8-file-format]
 [{--minimum-file-size | -S} nb|k|m|g]
 [{--minimum-access-time | -A} nd|h|m|s]
 [{--minimum-write-time | -W} nd|h|m|s]
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [--off]
 [-F outlist]
```

### Description

The **activate** command sets the file ID in the metadata to the current ID of the file. Use this function under the following conditions:

- When the file ID of the file changes.
- After metadata is restored.
- When moving FMA metadata from one computer to another.
- When file has been restored from a backup application. File stubs must be activated after a restore from backup for it to operate correctly.

Do not try to activate files that have an unknown status.

Files must be active in order to be recalled.

Disabling files ensures that no entry is written to the FMA garbage collection container when files are deleted. As a result, the corresponding archive copy is not deleted during an FMA cleanup run.

**Note** Excluded files are excluded from statistical summaries.

## Options

| Option                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                              | Displays Online Help for the <b>activate</b> command.                                                                                                                                                                                                                                                                                                                                                                                                  |
| --logfile <i>logfile</i><br>-L <i>logfile</i>             | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"> <li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li> <li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li> </ul> |
| --log-info-message<br>-V                                  | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                   |
| --verbose<br>-v                                           | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                    |
| <i>file</i>                                               | Specifies a file name. Wildcards like * or ? can be used.                                                                                                                                                                                                                                                                                                                                                                                              |
| --filelist <i>filelist</i><br>-f <i>filelist</i>          | Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts use fully qualified names only.                                                                                                                                                                                                                                              |
| --recursive <i>path</i><br>-r <i>path</i>                 | Applies this command to subfolders starting at <i>path</i> .                                                                                                                                                                                                                                                                                                                                                                                           |
| --oem-file-format                                         | Indicates that the input file list is in OEM format.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --unicode-file-format                                     | Indicates that the input file list is in unicode format.                                                                                                                                                                                                                                                                                                                                                                                               |
| --ansi-file-format                                        | Indicates that the input file list is in ANSI format.                                                                                                                                                                                                                                                                                                                                                                                                  |
| --utf8-file-format                                        | Indicates that the input file list is in UTF8 format (default).                                                                                                                                                                                                                                                                                                                                                                                        |
| --minimum-file-size <i>nb k m g</i><br>-S <i>nb k m g</i> | Defines a minimum file size ( <i>n</i> ) for the specified operation.<br>The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).                                                                                                                                                                                                                                                                                      |

| Option                                                      | Description                                                                                                                                                                        |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --minimum-access-time <i>nd h m s</i><br>-A <i>nd h m s</i> | Defines the minimum time ( <i>n</i> ) since file was last accessed for the specified operation.<br>The value can be specified in seconds (s), minutes (m), hours (h), or days (d). |
| --minimum-write-time <i>nd h m s</i><br>-W <i>nd h m s</i>  | Defines the minimum time ( <i>n</i> ) since file was last modified for the specified operation.<br>The value can be specified in seconds (s), minutes (m), hours (h), or days (d). |
| --exclude-system                                            | Excludes system files.                                                                                                                                                             |
| --exclude-hidden                                            | Excludes hidden files.                                                                                                                                                             |
| --exclude-read-only                                         | Excludes read-only files.                                                                                                                                                          |
| --exclude-archive                                           | Excludes files with an active archive bit.                                                                                                                                         |
| --exclude-compressed                                        | Excludes files with an active compressed bit.                                                                                                                                      |
| --ignore-files <i>ignorefile</i>                            | Excludes file <i>ignorefile</i> . Wildcards like * or ? can be used.                                                                                                               |
| --off                                                       | Deactivates files.<br>This is required when files need to be relocated on FMA managed volumes.                                                                                     |
| -F <i>outlist</i>                                           | Creates a file list ( <i>outlist</i> ) as output.                                                                                                                                  |

To define an operation, specify an explicit file name or a file list that contains file names. If neither is specified, the FMA CLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

### Example

```
FMA CLI activate D:\ASC\MyFile.doc
 Activates the D:\ASC\MyFile.doc file.
```

## archive

Lists the status of the FMA archives.

### Syntax

```
FMACLI arc[hive]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
```

### Description

The **archive** command displays list of all archives.

### Options

| Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                    | Displays Online Help for the <b>archive</b> command.                                                                                                                                                                                                                                                                                                                                                                                         |
| --logfile logfile<br>-L logfile | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger then 10MB, the file is switched.</li><li>• Old log files are named logfile.nnn, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V        | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                         |
| --verbose<br>-v                 | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                          |

## Example

FMACLI arc

Lists the archives. Output of the **archive** command is as follows:

Id—The unique, internal reference number for the archive, which is generated automatically and cannot be modified.

Status—The status of the archive (currently not used).

State—Whether the archive is online or offline.

Archive type—Type of Remote Storage Adapter (RSA-FTP for Linux archives, RSA-CIFS for Windows archives, RSA\_IAP for IAP archives).

pI—The order in which FMA recalls files from this archive. The range is 0-100. and the default is 100. If a file is stored on multiple archives, FMA attempts to recall it from the archive with the smallest index number first.

Name—The name of the archive, which identifies this archive for migration and recall operations.

Location—Path of primary and secondary archives.

Description—A description of the FMA archive.

Here is an example:

| Id   | Status | State  | Archive type | pI  | Name   | Location                              | Description       |
|------|--------|--------|--------------|-----|--------|---------------------------------------|-------------------|
| 0001 | OK     | online | RSA-IAP      | 100 | IAP-1  | P.: 192.168.40.163,<br>S.:            | "HP IAP #12"      |
| 0002 | OK     | online | RSA-FTP      | 100 | FTP-1  | P.: 192.168.100.8:21,<br>S.: :21      | "FTP Archive"     |
| 0003 | OK     | online | RSA-CIFS     | 100 | CIFS-1 | P.: \\w2003r2vm-arch1\Arch1-2,<br>S.: | "CIFS<br>Archive" |

## cleanup

Reorganizes FMA archives after files are deleted on the file server.

### Synopsis

```
FMACLI cle[anup]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]]
 [--verbose | -v]
 [--expiration nd|h|m|s]
```

### Description

Use the **cleanup** command after files have been deleted on the file server to remove copies from the archive and reorganize the archive.

### Options

| Option                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                  | Displays Online Help for the <b>cleanup</b> command.                                                                                                                                                                                                                                                                                                                                                                                                |
| --logfile <i>logfile</i><br>-L <i>logfile</i> | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V                      | Writes informational and debug messages to the log file (and the console). This option must be specified in combination with the <b>--logfile   -L</b> option. By default, only errors are written to the log.                                                                                                                                                                                                                                      |
| --verbose<br>-v                               | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                 |
| --expiration <i>nd h m s</i>                  | Deletes all files in all archives that have been deleted more than an expiration value ( <i>n</i> ) ago.<br>The value ( <i>n</i> ) can be specified in seconds (s), minutes (m), hours (h), or days (d).<br>This option is mandatory if the <b>-h --help</b> option is not used.                                                                                                                                                                    |

### Example

```
FMACLI cleanup --expiration 30d
 Removes archive files that were deleted more than 30 days ago on the file server.
```

## erase

Deletes FMA metadata from a file.

### Syntax

```
FMACLI era[se]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]]
 [--verbose | -v]
 [file] | [{--filelist} | -f} filelist]
 [{--recursive | -r} path]
 [--oem-file-format | --unicode-file-format |
 --ansi-file-format | --utf8-file-format]
 [{--minimum-file-size | -S} nb|k|m|g]
 [{--minimum-access-time | -A} nd|h|m|s]
 [{--minimum-write-time | -W} nd|h|m|s]
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [--primary-metadata | -Mp] |
 [--secondary-metadata | -Ma] |
 [--all-metadata | -Mb]]
 [--force]
 [-F outlist]
```

### Description

The **erase** command deletes FMA metadata from a file system.

**Note** **erase** deletes metadata without confirmation. Before erasing the file metadata, recall the file to avoid data loss. Metadata from offline files are erased unless the `--force` option is used.

Excluded files are excluded from statistical summaries.

## Options

| Option                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                              | Displays Online Help for the <b>erase</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| --logfile <i>logfile</i><br>-L <i>logfile</i>             | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"> <li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li> <li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>               logfile.log<br/>               logfile.000<br/>               logfile.001<br/>               ...</li> </ul> |
| --log-info-message<br>-V                                  | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                                                                               |
| --verbose<br>-v                                           | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>file</i>                                               | Specifies a file name. Wildcards like * or ? can be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --filelist <i>filelist</i><br>-f <i>filelist</i>          | Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts, use fully qualified names only.                                                                                                                                                                                                                                                                                                         |
| --recursive <i>path</i><br>-r <i>path</i>                 | Applies this command to subfolders starting at <i>path</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| --oem-file-format                                         | Indicates that the input file list is in OEM format.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| --unicode-file-format                                     | Indicates that the input file list is in unicode format.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| --ansi-file-format                                        | Indicates that the input file list is in ANSI format.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| --utf8-file-format                                        | Indicates that the input file list is in UTF8 format (default).                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --minimum-file-size <i>nb k m g</i><br>-S <i>nb k m g</i> | Defines a minimum file size ( <i>n</i> ) for the specified operation.<br>The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).                                                                                                                                                                                                                                                                                                                                                  |

| Option                                                | Description                                                                                                                                                                                 |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>--minimum-access-time nd h m s -A nd h m s</pre> | <p>Defines the minimum time (<i>n</i>) since file was last accessed for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p> |
| <pre>--minimum-write-time nd h m s -W nd h m s</pre>  | <p>Defines the minimum time (<i>n</i>) since file was last modified for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p> |
| <pre>--exclude-system</pre>                           | Excludes system files.                                                                                                                                                                      |
| <pre>--exclude-hidden</pre>                           | Excludes hidden files.                                                                                                                                                                      |
| <pre>--exclude-read-only</pre>                        | Excludes read-only files.                                                                                                                                                                   |
| <pre>--exclude-archive</pre>                          | Excludes files with an active archive bit.                                                                                                                                                  |
| <pre>--exclude-compressed</pre>                       | Excludes files with an active compressed bit.                                                                                                                                               |
| <pre>--ignore-files ignorefile</pre>                  | Excludes file <i>ignorefile</i> . Wildcards like * or ? can be used.                                                                                                                        |
| <pre>--primary-metadata -Mp</pre>                     | Deletes primary metadata (alternate data stream).                                                                                                                                           |
| <pre>--secondary-metadata -Ma</pre>                   | Deletes secondary metadata (alternate data stream).                                                                                                                                         |
| <pre>--all-metadata -Mb</pre>                         | Deletes all metadata (default).                                                                                                                                                             |
| <pre>--force</pre>                                    | Enables the deletion of offline files.                                                                                                                                                      |
| <pre>-F outlist</pre>                                 | Creates a file list ( <i>outlist</i> ) as output.                                                                                                                                           |

To define an operation, specify either an explicit file name or a file list that contains file names. If neither is specified, the FMA CLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

## Example

```
FMA CLI erase D:\ASC\MyFile.doc
Removes FMA metadata from the D:\ASC\MyFile.doc file.
```

## info

Displays FMA metadata.

### Syntax

```
FMACLI inf[o]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
 [file] | [{--filelist} | -f} filelist]
 [{--recursive | -r} path]
 [--oem-file-format | --unicode-file-format | --ansi-file-format |
 --utf8-file-format]
 [{--minimum-file-size | -S} nb|k|m|g]
 [{--minimum-access-time | -A} nd|h|m|s]
 [{--minimum-write-time | -W} nd|h|m|s]
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [--long | -l]
 [-F outlist]
```

### Description

This command displays HSM metadata. This information corresponds to the information available in the Properties tab for a file when the Explorer plugin is installed.

**Note** Excluded files are excluded from statistical summaries.

### Options

| Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                    | Displays Online Help for the <b>info</b> command.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --logfile logfile<br>-L logfile | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named logfile.<i>nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --verbose<br>-v                 | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                 |

| Option                                                | Description                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>--log-info-message -V</pre>                      | <p>Writes informational and debug messages to the log file (and the console).</p> <p>This option must be specified in combination with the <b>--logfile</b>   <b>-L</b> option.</p> <p>By default, only errors are written to the log.</p> |
| <pre>file</pre>                                       | <p>Specifies a file name. Wildcards like * or ? can be used.</p>                                                                                                                                                                           |
| <pre>--filelist filelist -f filelist</pre>            | <p>Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts use fully qualified names only.</p>                           |
| <pre>--recursive path -r path</pre>                   | <p>Applies this command to subfolders starting at <i>path</i>.</p>                                                                                                                                                                         |
| <pre>--oem-file-format</pre>                          | <p>Indicates that the input file list is in OEM format.</p>                                                                                                                                                                                |
| <pre>--unicode-file-format</pre>                      | <p>Indicates that the input file list is in unicode format.</p>                                                                                                                                                                            |
| <pre>--ansi-file-format</pre>                         | <p>Indicates that the input file list is in ANSI format.</p>                                                                                                                                                                               |
| <pre>--utf8-file-format</pre>                         | <p>Indicates that the input file list is in UTF8 format (default).</p>                                                                                                                                                                     |
| <pre>--minimum-file-size nb k m g -S nb k m g</pre>   | <p>Defines a minimum file size (<i>n</i>) for the specified operation.</p> <p>The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).</p>                                                                 |
| <pre>--minimum-access-time nd h m s -A nd h m s</pre> | <p>Defines the minimum time (<i>n</i>) since file was last accessed for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p>                                                |
| <pre>--minimum-write-time nd h m s -W nd h m s</pre>  | <p>Defines the minimum time (<i>n</i>) since file was last modified for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p>                                                |
| <pre>--exclude-system</pre>                           | <p>Excludes system files.</p>                                                                                                                                                                                                              |
| <pre>--exclude-hidden</pre>                           | <p>Excludes hidden files.</p>                                                                                                                                                                                                              |
| <pre>--exclude-read-only</pre>                        | <p>Excludes read-only files.</p>                                                                                                                                                                                                           |
| <pre>--exclude-archive</pre>                          | <p>Excludes files with an active archive bit.</p>                                                                                                                                                                                          |
| <pre>--exclude-compressed</pre>                       | <p>Excludes files with an active compressed bit.</p>                                                                                                                                                                                       |
| <pre>--ignore-files ignorefile</pre>                  | <p>Excludes file <i>ignorefile</i>. Wildcards like * or ? can be used.</p>                                                                                                                                                                 |

| Option            | Description                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------|
| --long<br>-l      | Displays all available information (long output). In the short version (default), only one line per file is displayed. |
| -F <i>outlist</i> | Creates a file list ( <i>outlist</i> ) as output.                                                                      |

To define an operation, specify either an explicit file name or a file list that contains file names. If neither is specified, the FMACLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

## Example

```
FMACLI info -r D:*.*
```

Displays FMA metadata for the files in the D:\\*.\* folder, as follows:

```

Last Modification Size Attributes Status Name

2008-02-02 17:09:28 18755 -A---O---PF OFF(1) D:\ASC\EULA.rtf
2006-04-21 16:00:14 1088 -A-----MOD D:\ASC\Fma.txt
2005-07-27 15:42:54 4344083 -A-----SAV(1) D:\ASC\FMAAdmGd.pdf
2007-04-07 13:56:38 5482 -A-----D:\ASC\Readme.txt
2006-05-04 06:49:36 102400 -A-----SAV(3) D:\ASC\MyFile.doc
.
.
12 files succeeded
0 files failed
0 files were processed earlier
22579118080 bytes processed

```

Output of the **info** command is as follows:

- Last Modification—The last modification date and time.
- Size—The size of the file.
- Attributes—File attributes including the following:
  - A—Archived
  - F—Sparse
  - H—Hidden
  - O—Offline
  - P—Reparse point
  - R—Read-only
  - S—System
  - T—Temporary
- Status—A blank status shows that a file is not managed. The following states are available:
  - OFF—Offline
  - MOD—Modified
  - SAV—Migrated
  - INA—Inactive
  - DIS—Disabled
  - (n)—Number of valid copies

- Name—The fully qualified file name.

## Example

```
FMACLI info -r D:*.* -l
```

Displays all available information for the files in the D:\\*.\* folder, as follows:

```

:
:
File: D:\ASC\MyFile.doc
File info:
state=SAV(1), attr=-A-----F, size=102400, generations=0001
Filter file info:
SysFileID=0001000000000038, AppFileID=0000000000000000, ChgTime=2006-02-01
13:49:36,766, FileSize=104965100, CLEAN, ONLINE
File generation info:
size=104965100, last_mig=2006-02-01 13:49:36,766, last_rec=2006-05-03
15:11:04,268, attr=-A-----, locations=1
File location info:
ArchiveID=1, ArcPoolID=1, dwNumRec=1, storage_handle_descr=Id: 2 Version: 2
Filesize: 104965444 Last Write Time: 20060503130432 File name: MyFile.doc

12 files succeeded
0 files failed
0 files were processed earlier
22579118080 bytes processed

```

Output of the **info** command with the **-l** option is as follows:

|                      | Field                  | Output                                                                                               |
|----------------------|------------------------|------------------------------------------------------------------------------------------------------|
| File info            | state                  | FMA status                                                                                           |
|                      | attr                   | File attributes                                                                                      |
|                      | size                   | File size                                                                                            |
|                      | generations            | Number of versions stored in the archive<br>(Only the latest version of a file object is supported.) |
| Filter file info     | SysFileID              | NTFS file identifier                                                                                 |
|                      | AppFileID              | Not used (always zero)                                                                               |
|                      | ChgTime                | Modification timestamp                                                                               |
|                      | FileSize               | File size                                                                                            |
|                      | Filter status          | Status of filter, such as CLEAN                                                                      |
|                      | Offline file attribute | Whether file is ONLINE or OFFLINE                                                                    |
| File generation info | Size                   | File size of replica                                                                                 |
|                      | last_mig               | Modification timestamp of replica                                                                    |
|                      | last_rec               | Timestamp of last recall operation                                                                   |
|                      | attr                   | Attributes of replica                                                                                |
|                      | locations              | Number of replicas                                                                                   |

|                    | <b>Field</b>         | <b>Output</b>                              |
|--------------------|----------------------|--------------------------------------------|
| File location info | ArchiveID            | Internal reference number for the archive  |
|                    | ArchPoolID           | Not used (reserved for future use)         |
|                    | dwNumRec             | Total number of recalls from this location |
|                    | storage_handle_descr | Archive link descriptor                    |

## migrate

Explicitly migrates a file to the specified archive.

### Syntax

```
FMACLI mig[rate]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
 [file] | [--filelist] | -f} filelist]
 [--recursive | -r} path]
 [--oem-file-format | --unicode-file-format | --ansi-file-format |
 --utf8-file-format]
 [--minimum-file-size | -S} nb|k|m|g]
 [--minimum-access-time | -A} nd|h|m|s]
 [--minimum-write-time | -W} nd|h|m|s]
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [--archive | -a} arc] | [--archives arc1,...]
 [--maximum-copies | -n} copies]
 [--release]
 [-F outlist]
```

### Description

This command copies files from a file server to one or more archives. The original files remain on the file server.

**Note** Excluded files are excluded from statistical summaries.

Also, if a file is migrated to multiple archives and FMA releases the file, the file is recalled from the last location to which it was migrated. The last location contains the most recent version of the file contents.

## Options

| Option                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                              | Displays Online Help for the <b>migrate</b> command.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --logfile <i>logfile</i><br>-L <i>logfile</i>             | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"> <li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li> <li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li> </ul> |
| --log-info-message<br>-V                                  | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                   |
| --verbose<br>-v                                           | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                    |
| <i>file</i>                                               | Specifies a file name. Wildcards like * or ? can be used.                                                                                                                                                                                                                                                                                                                                                                                              |
| --filelist <i>filelist</i><br>-f <i>filelist</i>          | Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts use fully qualified names only.                                                                                                                                                                                                                                              |
| --recursive <i>path</i><br>-r <i>path</i>                 | Applies this command to subfolders starting at <i>path</i> .                                                                                                                                                                                                                                                                                                                                                                                           |
| --oem-file-format                                         | Indicates that the input file list is in OEM format.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --unicode-file-format                                     | Indicates that the input file list is in unicode format.                                                                                                                                                                                                                                                                                                                                                                                               |
| --ansi-file-format                                        | Indicates that the input file list is in ANSI format.                                                                                                                                                                                                                                                                                                                                                                                                  |
| --utf8-file-format                                        | Indicates that the input file list is in UTF8 format (default).                                                                                                                                                                                                                                                                                                                                                                                        |
| --minimum-file-size <i>nb k m g</i><br>-S <i>nb k m g</i> | Defines a minimum file size ( <i>n</i> ) for the specified operation.<br>The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).                                                                                                                                                                                                                                                                                      |

| Option                                                      | Description                                                                                                                                                                                                    |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --minimum-access-time <i>nd h m s</i><br>-A <i>nd h m s</i> | Defines the minimum time ( <i>n</i> ) since file was last accessed for the specified operation.<br>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).                             |
| --minimum-write-time <i>nd h m s</i><br>-W <i>nd h m s</i>  | Defines the minimum time ( <i>n</i> ) since file was last modified for the specified operation.<br>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).                             |
| --exclude-system                                            | Excludes system files.                                                                                                                                                                                         |
| --exclude-hidden                                            | Excludes hidden files.                                                                                                                                                                                         |
| --exclude-read-only                                         | Excludes read-only files.<br>Note: The read-only attribute does not affect the behavior of policies or the Explorer plug-in. FMA will migrate, release, and recall read-only files and preserve the attribute. |
| --exclude-archive                                           | Excludes files with an active archive bit.                                                                                                                                                                     |
| --exclude-compressed                                        | Excludes files with an active compressed bit.                                                                                                                                                                  |
| --ignore-files <i>ignorefile</i>                            | Excludes file <i>ignorefile</i> . Wildcards like * or ? can be used.                                                                                                                                           |
| --archive <i>arc</i><br>-a <i>arc</i>                       | Specifies the name of the archive where the file is stored. This parameter is mandatory for the migration command.                                                                                             |
| --archives <i>arc1, ...</i>                                 | Specifies a list of archives with maximum 4 archives (“arc1, arc2, ... arc <i>n</i> ”)                                                                                                                         |
| --maximum-copies <i>copies</i><br>-n <i>copies</i>          | Sets the maximum number of archive copies of a file.                                                                                                                                                           |
| --release                                                   | Releases the files after a successfully migration.                                                                                                                                                             |
| -F <i>outlist</i>                                           | Creates a file list ( <i>outlist</i> ) as output.                                                                                                                                                              |

To define an operation, specify either an explicit file name or a file list that contains file names. If neither is specified, the FMA CLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

## Examples

FMACLI migrate D:\Test\file.dat -a arc01  
Migrates the file D:\Test\file.dat to the archive arc01.

FMACLI migrate -f c:\temp\miglist.dat -a arc01  
Migrates the filelist c:\temp\miglist.dat to the archive arc01.

FMACLI migrate D:\Data -A 4d --archive arc01  
Migrates the file D:\Data to the archive arc01 if the file has not been accessed in the last four days.

FMACLI migrate D:\Data --archives "arc01, arc02, arc03 "  
Migrates the file D:\Data to the archives arc01, arc02, and arc03.

FMACLI migrate D:\Data --archive arc01 --release  
Migrates the file D:\Data to the archive arc01 and then releases the file.

## policy

Displays or runs file policies.

### Syntax

```
FMACLI pol[icy]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
 [--name polname | --all | --run polname]
```

### Description

This command displays or runs file policies. A policy defines the conditions under which files on a managed volume are migrated and released. For more information about policies, see [Migrating and releasing files using file policies](#) on page 51.

### Options

| Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                    | Displays Online Help for the <b>policy</b> command.                                                                                                                                                                                                                                                                                                                                                                                                 |
| --logfile logfile<br>-L logfile | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named logfile.<i>nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V        | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                |
| --verbose<br>-v                 | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                 |
| --name polname                  | Displays a specific policy.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| --all                           | Displays all policies.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| --run polname                   | Runs a specific policy.                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Example

FMACLI POL --name Reports

Displays information about the policy named Reports, with output as follows:

```
GUID: volume{78a17197-d505-11da-a579-806e6f6e6963}
Policy name: Reports
(Enabled)
Description: weekly Reports
Path: \Reports2006\
List of archives: IAF01;NAS01
Filtering:
Size: 1024
Time stamp:
Release flag = TRUE
List of excludes: \System volume Information*; \Hsm volume Information*;
```

## recall

Explicitly recalls data for a released file.

### Syntax

```
FMACLI rec[all]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
 [file] | [{--filelist} | -f} filelist]
 [{--recursive | -r} path]
 [--oem-file-format | --unicode-file-format |
 --ansi-file-format | --utf8-file-format]
 [{--minimum-file-size | -S} nb|k|m|g]
 [{--minimum-access-time | -A} nd|h|m|s]
 [{--minimum-write-time | -W} nd|h|m|s]
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [-F outlist]
```

### Description

This command recalls a released file.

**Note** Excluded files are excluded from statistical summaries.

Also, if a file is migrated to multiple archives and FMA releases the file, the file is recalled from the last location to which it was migrated. The last location contains the most recent version of the file contents.

### Options

| Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                    | Displays Online Help for the <b>recall</b> command.                                                                                                                                                                                                                                                                                                                                                                                          |
| --logfile logfile<br>-L logfile | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named logfile.nnn, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |

| Option                                                | Description                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>--log-info-message -v</pre>                      | <p>Writes informational and debug messages to the log file (and the console).</p> <p>This option must be specified in combination with the <b>--logfile</b>   <b>-L</b> option.</p> <p>By default, only errors are written to the log.</p> |
| <pre>--verbose -v</pre>                               | <p>Display debug information on the console (std_out).</p>                                                                                                                                                                                 |
| <pre>file</pre>                                       | <p>Specifies a file name. Wildcards like * or ? can be used.</p>                                                                                                                                                                           |
| <pre>--filelist filelist -f filelist</pre>            | <p>Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts use fully qualified names only.</p>                           |
| <pre>--recursive path -r path</pre>                   | <p>Applies this command to subfolders starting at path.</p>                                                                                                                                                                                |
| <pre>--oem-file-format</pre>                          | <p>Indicates that the input file list is in OEM format.</p>                                                                                                                                                                                |
| <pre>--unicode-file-format</pre>                      | <p>Indicates that the input file list is in unicode format.</p>                                                                                                                                                                            |
| <pre>--ansi-file-format</pre>                         | <p>Indicates that the input file list is in ANSI format.</p>                                                                                                                                                                               |
| <pre>--utf8-file-format</pre>                         | <p>Indicates that the input file list is in UTF8 format (default).</p>                                                                                                                                                                     |
| <pre>--minimum-file-size nb k m g -S nb k m g</pre>   | <p>Defines a minimum file size (<i>n</i>) for the specified operation.</p> <p>The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).</p>                                                                 |
| <pre>--minimum-access-time nd h m s -A nd h m s</pre> | <p>Defines the minimum time (<i>n</i>) since file was last accessed for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p>                                                |
| <pre>--minimum-write-time nd h m s -W nd h m s</pre>  | <p>Defines the minimum time (<i>n</i>) since file was last modified for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p>                                                |
| <pre>--exclude-system</pre>                           | <p>Excludes system files.</p>                                                                                                                                                                                                              |
| <pre>--exclude-hidden</pre>                           | <p>Excludes hidden files.</p>                                                                                                                                                                                                              |

| Option                           | Description                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --exclude-read-only              | Excludes read-only files.<br>Note: The read-only attribute does not affect the behavior of policies or the Explorer plug-in. FMA will migrate, release, and recall read-only files and preserve the attribute. |
| --exclude-archive                | Excludes files with an active archive bit.                                                                                                                                                                     |
| --exclude-compressed             | Excludes files with an active compressed bit.                                                                                                                                                                  |
| --ignore-files <i>ignorefile</i> | Excludes file <i>ignorefile</i> . Wildcards like * or ? can be used.                                                                                                                                           |
| -F <i>outlist</i>                | Creates a file list ( <i>outlist</i> ) as output.                                                                                                                                                              |

To define an operation, specify either an explicit file name or a file list that contains file names. If neither is specified, the FMA CLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

## Example

```
FMA CLI rec myfile.doc
```

Recalls the myfile.doc file. If this file is saved on multiple archives, FMA pulls it from the archive with the lowest performance index number.

## release

Explicitly releases a migrated file, leaving a stub file on the file server.

### Synopsis

```
FMACLI rel[ease]
 [--help | -h]
 [--logfile | -L] logfile
 [--log-info-messages | -V]
 [--verbose | -v]
 [file] | [--filelist] | -f} filelist
 [--recursive | -r] path
 [--oem-file-format | --unicode-file-format | --ansi-file-format |
 --utf8-file-format]
 [--minimum-file-size | -S] nb|k|m|g
 [--minimum-access-time | -A] nd|h|m|s
 [--minimum-write-time | -W] nd|h|m|s
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [--minimum-copies | -n} mc]
 [--changed-retention-time | -t} crtd|h|m|s]
 [--read-retention-time | -T} rrtd|h|m|s]
 [--low-watermark | -U} nn]
 [--high-watermark | -u} nn]
 [-F outlist]
```

### Description

The **release** command gains space on a managed volume by converting already migrated files to stub files. If the command detects that not enough archived copies exist, the release operation is not performed. For releasing a file both retention times (*crt* and *rrt*) and the number of copies (*mc*) must be fulfilled.

A file smaller than 1024 bytes are not released because replacing it with a stub file does not increase available space on the file server.

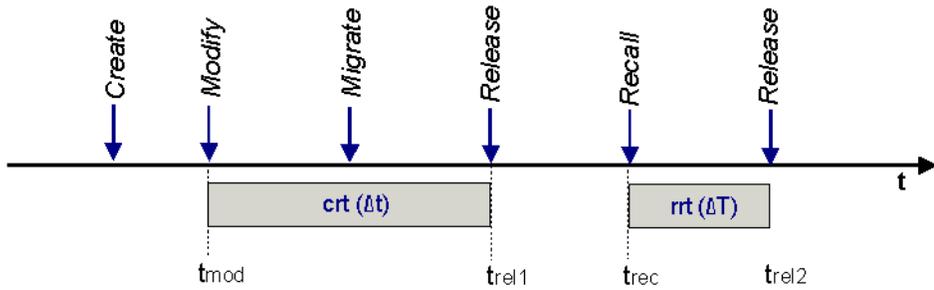
**Note** Excluded files are excluded from statistical summaries.

Also, if a file was released and migrated to multiple archives, it is restored from the last archive to which it was migrated when recalled.

## Options

| Option                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                              | Displays Online Help for the <b>release</b> command.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --logfile <i>logfile</i><br>-L <i>logfile</i>             | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"> <li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li> <li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li> </ul> |
| --log-info-message<br>-V                                  | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                   |
| --verbose<br>-v                                           | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                    |
| <i>file</i>                                               | Specifies a file name. Wildcards like * or ? can be used.                                                                                                                                                                                                                                                                                                                                                                                              |
| --filelist <i>filelist</i><br>-f <i>filelist</i>          | Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts use fully qualified names only.                                                                                                                                                                                                                                              |
| --recursive <i>path</i><br>-r <i>path</i>                 | Applies this command to subfolders starting at <i>path</i> .                                                                                                                                                                                                                                                                                                                                                                                           |
| --oem-file-format                                         | Indicates that the input file list is in OEM format.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --unicode-file-format                                     | Indicates that the input file list is in unicode format.                                                                                                                                                                                                                                                                                                                                                                                               |
| --ansi-file-format                                        | Indicates that the input file list is in ANSI format.                                                                                                                                                                                                                                                                                                                                                                                                  |
| --utf8-file-format                                        | Indicates that the input file list is in UTF8 format (default).                                                                                                                                                                                                                                                                                                                                                                                        |
| --minimum-file-size <i>nb k m g</i><br>-S <i>nb k m g</i> | Defines a minimum file size ( <i>n</i> ) for the specified operation.<br>The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).                                                                                                                                                                                                                                                                                      |

| Option                                                   | Description                                                                                                                                                                                                                                      |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>--minimum-access-time nd h m s -A nd h m s</pre>    | <p>Defines the minimum time (<i>n</i>) since file was last accessed for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p>                                                      |
| <pre>--minimum-write-time nd h m s -W nd h m s</pre>     | <p>Defines the minimum time (<i>n</i>) since file was last modified for the specified operation.</p> <p>The value can be specified in seconds (s), minutes (m), hours (h), or days (d).</p>                                                      |
| <pre>--exclude-system</pre>                              | Excludes system files.                                                                                                                                                                                                                           |
| <pre>--exclude-hidden</pre>                              | Excludes hidden files.                                                                                                                                                                                                                           |
| <pre>--exclude-read-only</pre>                           | <p>Excludes read-only files.</p> <p>Note: The read-only attribute does not affect the behavior of policies or the Explorer plug-in. FMA will migrate, release, and recall read-only files and preserve the attribute.</p>                        |
| <pre>--exclude-archive</pre>                             | Excludes files with an active archive bit.                                                                                                                                                                                                       |
| <pre>--exclude-compressed</pre>                          | Excludes files with an active compressed bit.                                                                                                                                                                                                    |
| <pre>--ignore-files ignorefile</pre>                     | Excludes file ( <i>ignorefile</i> ). Wildcards like * or ? can be used.                                                                                                                                                                          |
| <pre>--changed-retention-time crtm h d -t crtm h d</pre> | <p>Defines the Changed Retention Time (<i>crt</i>). This is the time period in minutes (m), hours (h), or days (d) that changed files stay on disk before they are released.</p>                                                                 |
| <pre>--read-retention-time rrtm h d -T rrtm h d</pre>    | <p>Defines the Release Retention Time (<i>rrt</i>). This is the time period in minutes (m), hours (h), or days (d) that recalled and unchanged files stay on disk before they are released.</p>                                                  |
| <pre>--minimum-copies mc -n mc</pre>                     | <p>Defines the minimum number of copies in the archive before a file can be released.</p>                                                                                                                                                        |
| <pre>--high-watermark nn -u nn</pre>                     | <p>Defines the High-Watermark value (<i>nn</i>). The release process starts if the fill level (percentage) of the file system is reached. If the fill level is not reached the process is immediately terminated without releasing any data.</p> |
| <pre>--low-watermark nn -U nn</pre>                      | <p>Defines the Low-Watermark value (<i>nn</i>). The release process is stopped if the low-watermark (percentage) of the file system is reached.</p>                                                                                              |
| <pre>-F outlist</pre>                                    | Creates a file list ( <i>outlist</i> ) as output.                                                                                                                                                                                                |



|     |                                                                                                                                                                               |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crt | The time period for migrated and changed files. All files remain on disk for the specified time period before they become a release candidate.                                |
| rrt | The time period for recalled and unchanged files. All recalled and unchanged files remain on disk for the specified time period before they become again a release candidate. |

To define an operation, specify either an explicit file name or a file list that contains file names. If neither is specified, the FMACLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

**Examples**

FMACLI release D:\ASC\MyFile.doc -t 1d -T 10d -n 2  
 If the MyFile.doc file was modified, it stays one day on disk before it becomes a release candidate.

If the MyFile.doc file was not modified, it stays for another 10 days on disk before it becomes a release candidate.

FMACLI release D:\ASC\MyFile.doc --minimum-copies 3  
 In this case the MyFile.doc file is released when three copies are available on different archives.

## rsa

Lists the status of the remote storage adapter.

### Syntax

```
FMACLI rsa
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
```

### Description

The **rsa** command displays the remote storage adapter status.

### Options

| Option                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                  | Displays Online Help for the <b>rsa</b> command.                                                                                                                                                                                                                                                                                                                                                                                                    |
| --logfile <i>logfile</i><br>-L <i>logfile</i> | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V                      | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                |
| --verbose<br>-v                               | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                 |

## Example

FMACLI `rsa`

Lists information about the remote storage adapters, as follows:

| # | Type | Capabs   | Name     | RSA         | Description                  |
|---|------|----------|----------|-------------|------------------------------|
| 0 | 0    | 00000000 | RSA-CIFS | RsaCIFS.dll | "Storage ... specifications" |
| 1 | 0    | 00000000 | RSA-FTP  | RsaFtp.dll  | "Storage on ftp server"      |
| 2 | 0    | 00000000 | RSA-RISS | RsaRISS.dll | "Storage on HP RISS"         |

Output of the `rsa` command is as follows:

- #—Index number
- Type—Reserved for future use
- Capabs—Archive capabilities (reserved for future use)
- Name—RSA name
- RSA—Dynamic link library of the remote storage adapter
- Descr.—Description of the remote storage adapter

## system

Displays system information.

### Syntax

```
FMACLI sys[tem]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]]
 [--verbose | -v]
```

### Description

The **system** command displays system information such as version, license, and other FMA settings.

### Options

| Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                    | Displays Online Help for the <b>system</b> command.                                                                                                                                                                                                                                                                                                                                                                                          |
| --logfile logfile<br>-L logfile | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named logfile.nnn, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V        | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                         |
| --verbose<br>-v                 | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                          |

### Example

```
FMACLI sys
 Lists system information, as follows:
 HP Storage Works File Migration Agent
 Version 2.5.1.0
 HP File Migration Agent command line interface
 Copyright (C) 2007-2009 Crossroads Systems, Inc.
 Copyright (C) 2005-2009 Hewlett-Packard Company
```

```
Version of HP File Migration Agent kernel 2. 5. 0. 17
System status = 0, installPath=[C:\Program Files\Hewlett-Packard\HP FMA]
HSM API Version = 2.5.0-0017 ""
License Information:
=====
+ Serial number S-
+ Base Product License Evaluation license expiration in 59 days
+ OpenStorage Option Evaluation license, capacity (avail/used) 1000 GB
/ 0 GB.
+ Cluster Option Evaluation license.
Config:
Loglevel for eventlog: LOG_WARNING
Loglevel for logfile: LOG_INFO
Number of log files: 100
Options:=00000000
```

## verify

Displays the result of the verification process.

### Syntax

```
FMACLI ver[ify]
 [--help | -h]
 [--logfile | -L] logfile
 [--log-info-messages | -V]
 [--verbose | -v]
 [file] | [--filelist] | -f} filelist
 [--recursive | -r] path
 [--oem-file-format | --unicode-file-format | --ansi-file-format |
 --utf8-file-format]
 [--minimum-file-size | -S] nb|k|m|g
 [--minimum-access-time | -A] nd|h|m|s
 [--minimum-write-time | -W] nd|h|m|s
 [--exclude-system]
 [--exclude-hidden]
 [--exclude-read-only]
 [--exclude-archive]
 [--exclude-compressed]
 [--ignore-files ignorefile]
 [--repair]
 [--local-checks | -o local}]
 [--remote-checks | -o remote}]
 [-F outlist]
```

### Description

The **verify** command checks metadata for files on the file server or in the archive.

**Note** Excluded files are excluded from statistical summaries.

#### Local Check (Level 1)

If verification option `local` is specified, the following checks are performed:

- Load primary metadata (checks if the file-id matches with the metadata).
- Load secondary metadata and compare with local metadata.
- Check whether offline files have meta data.
- Check for offline files with non-zero file size.
- Check if the copies on the archives are up to date.

#### Remote Check (Level 2)

In case verification option `remote` is specified, the following checks are performed:

- Local verification.
- Each link to an archive is verified using the RSAVerify-Method. The validation algorithm is part of the remote storage adapter implementation. All copies for all available generations are checked. Locally modified files are processed the same way.

**Note** Verify does not report detailed results to the screen. It displays a list of failed files, but you must check the `hsm.log` file for details.

## Options

| Option                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                              | Displays Online Help for the <b>verify</b> command.                                                                                                                                                                                                                                                                                                                                                                                                    |
| --logfile <i>logfile</i><br>-L <i>logfile</i>             | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"> <li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li> <li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li> </ul> |
| --log-info-message<br>-V                                  | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                   |
| --verbose<br>-v                                           | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                    |
| <i>file</i>                                               | Specifies a file name. Wildcards like * or ? can be used.                                                                                                                                                                                                                                                                                                                                                                                              |
| --filelist <i>filelist</i><br>-f <i>filelist</i>          | Specifies an input file list (default is stdin). Files in the file list are separated by CR/LF. File names can be relative or fully qualified. If you plan to run scripts use fully qualified names only.                                                                                                                                                                                                                                              |
| --recursive <i>path</i><br>-r <i>path</i>                 | Applies this command to subfolders starting at <i>path</i> .                                                                                                                                                                                                                                                                                                                                                                                           |
| --oem-file-format                                         | Indicates that the input file list is in OEM format.                                                                                                                                                                                                                                                                                                                                                                                                   |
| --unicode-file-format                                     | Indicates that the input file list is in unicode format.                                                                                                                                                                                                                                                                                                                                                                                               |
| --ansi-file-format                                        | Indicates that the input file list is in ANSI format.                                                                                                                                                                                                                                                                                                                                                                                                  |
| --utf8-file-format                                        | Indicates that the input file list is in UTF8 format (default).                                                                                                                                                                                                                                                                                                                                                                                        |
| --minimum-file-size <i>nb k m g</i><br>-S <i>nb k m g</i> | Defines a minimum file size ( <i>n</i> ) for the specified operation. The value can be specified in bytes (b), kilobytes (k), megabytes (m), or gigabytes (g).                                                                                                                                                                                                                                                                                         |

| Option                                                      | Description                                                                                                                                                                        |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --minimum-access-time <i>nd h m s</i><br>-A <i>nd h m s</i> | Defines the minimum time ( <i>n</i> ) since file was last accessed for the specified operation.<br>The value can be specified in seconds (s), minutes (m), hours (h), or days (d). |
| --minimum-write-time <i>nd h m s</i><br>-W <i>nd h m s</i>  | Defines the minimum time ( <i>n</i> ) since file was last modified for the specified operation.<br>The value can be specified in seconds (s), minutes (m), hours (h), or days (d). |
| --exclude-system                                            | Excludes system files.                                                                                                                                                             |
| --exclude-hidden                                            | Excludes hidden files.                                                                                                                                                             |
| --exclude-read-only                                         | Excludes read-only files.                                                                                                                                                          |
| --exclude-archive                                           | Excludes files with an active archive bit.                                                                                                                                         |
| --exclude-compressed                                        | Excludes files with an active compressed bit.                                                                                                                                      |
| --ignore-files <i>ignorefile</i>                            | Excludes file <i>ignorefile</i> . Wildcards like * or ? can be used.                                                                                                               |
| --repair                                                    | Upgrades local metadata to the current FMA version and forces values to match those in the archive.                                                                                |
| --local-checks<br>-o local                                  | Verifies archive contents.<br>Operation level of verify operation is local (default).                                                                                              |
| --remote-checks<br>-o remote                                | Verifies archive contents.<br>Operation level of verify operation is remote.                                                                                                       |
| -F <i>outlist</i>                                           | Creates a file list ( <i>outlist</i> ) as output.                                                                                                                                  |

To define an operation, specify either an explicit file name or a file list that contains file names. If neither is specified, the FMA CLI tries to read the file list from stdin.

Use UNICODE or UTF8 formats whenever possible. The OEM and ANSI formats are for compatibility reasons only and cannot display all character sets.

### Example

```
FMA CLI verify D:\ASC\MyFile.doc -o remote
 Performs a remote check on the D:\ASC\MyFile.doc file.
```

## version

Displays version and build information about the installed FMA.

### Syntax

```
FMACLI vers[ion]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
```

### Description

The **version** command displays version and build information about the installed FMA.

### Options

| Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                    | Displays Online Help for the <b>version</b> command.                                                                                                                                                                                                                                                                                                                                                                                                |
| --logfile logfile<br>-L logfile | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named logfile.<i>nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V        | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                |
| --verbose<br>-v                 | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                 |

## Example

FMACLI vers

Displays FMA version information, as follows:

```
HP Storage Works File Migration Agent
Version HP 2.5.1.0
HP File Migration Agent command line interface
Copyright (C) 2007-2009 Crossroads Systems, Inc.
Copyright (C) 2005-2009 Hewlett-Packard Company
```

## volume

Displays a list of available volumes.

### Syntax

```
FMACLI vol[ume]
 [--help | -h]
 [{--logfile | -L} logfile]
 [--log-info-messages | -V]
 [--verbose | -v]
```

### Description

The **volume** command displays information about the available volumes.

### Options

| Option                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --help<br>-h                                  | Displays Online Help for the <b>volume</b> command.                                                                                                                                                                                                                                                                                                                                                                                                 |
| --logfile <i>logfile</i><br>-L <i>logfile</i> | Specifies a log file.<br>The log file must be specified with a fully qualified path. Log files are created with the following (fixed) policies: <ul style="list-style-type: none"><li>• Maximum size is 10MB. If the file grows larger than 10MB, the file is switched.</li><li>• Old log files are named <i>logfile.nnn</i>, where the lowest number contains the youngest file:<br/>logfile.log<br/>logfile.000<br/>logfile.001<br/>...</li></ul> |
| --log-info-message<br>-V                      | Writes informational and debug messages to the log file (and the console).<br>This option must be specified in combination with the <b>--logfile   -L</b> option.<br>By default, only errors are written to the log.                                                                                                                                                                                                                                |
| --verbose<br>-v                               | Display debug information on the console (std_out).                                                                                                                                                                                                                                                                                                                                                                                                 |

## Example

```
FMACLI vol
```

Displays a list of volumes in the following format:

| Volume List: |   |        |             |            |             |      |          |           |             |             |    |      |                    |
|--------------|---|--------|-------------|------------|-------------|------|----------|-----------|-------------|-------------|----|------|--------------------|
| Id           | M | Volume | Status      | HSM Status | Label       | FS   | Serial   | Migrated  | Capacity    | Free Space  | %  | PID  | GUID               |
| 0            | X |        | Active      | Active     | PARTITION02 | NTFS | 9AD85144 | 952595200 | 15734927360 | 4181913600  | 74 | 3096 | Volume(78AL...963) |
| 1            |   |        | Restricted  | Unknown    | PARTITION01 | NTFS | 64327E55 | 0         | 10487197696 | 6488842240  | 39 | 0    | Volume(78AL...963) |
| 2            |   |        | Not Managed | Unknown    | PARTITION03 | NTFS | DC66B6D9 | 0         | 41948893184 | 19570405376 | 54 | 0    | Volume(78AL...963) |
| 3            |   |        | Not Managed | Unknown    | PARTITION04 | NTFS | 6B614510 | 0         | 11852595200 | 10746290176 | 10 | 0    | Volume(78AL...963) |

Output of the **volume** command is as follows:

- Id—The volume index number.
- M—Designates which volumes are managed.
- Volume Status—The management status of the volume
  - Not managed
  - Stopped
  - Active
  - Not mounted
  - Error
  - Restricted
  - Cannot be managed
  - Need reboot
- HSM Status—The status of the volume
  - Active
  - Inactive
  - Unknown
- Label—The volume label.
- FS—The file system of this volume. (Only NTFS is supported for managed volumes.)
- Serial—The serial number of the volume.
- Migrated—The number of bytes migrated from this volume
- Capacity—The amount of disk space in gigabytes
- Free Space—The amount of free disk space in megabytes
- %—The percentage of free disk space
- PID—The HSM process ID of the volume manager process
- GUID—Global unique identifier (36 characters)

## Result codes

FMA CLI returns 0 if successful. Positive result codes show warning conditions. In the case of a fatal error condition, negative values are returned.

| Return Value | Description                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| (0)          | No error occurred.                                                                                                                              |
| (1)          | Watermark not reached.                                                                                                                          |
| (2)          | Error occurred during operation. The command started successfully but some errors occurred.<br>Example: Some of the files can not be processed. |
| (-1)         | A generic error occurred. Check error messages (stderr) for more information.                                                                   |
| (-2)         | An invalid parameter was specified. Check error messages to determine the bad parameter.                                                        |
| (-3)         | An invalid command was specified.                                                                                                               |
| (-4)         | FMA has found a bad configuration. This is caused by invalid archive configuration or duplicate archive IDs.                                    |



# Troubleshooting

---



This section documents the log files generated by FMA and provides steps for troubleshooting FMA. For information about contacting Support, see [Support](#) on page viii.

If you must contact Support, please have the following information ready when you report an FMA issue:

- Operating system version of the file server
- FMA version and license information

Use the **FMACLI system** command (page 112) to retrieve this information.

- List of third-party applications installed on your file server, including antivirus scanners, backup management applications, and so on
- Issue description
  - When did the issue occur?
  - Which activities have caused the issue?
- Logging information
  - Save all FMA log files in the *FMAInstallFolder*\log folder into a zip file. By default, the FMA installation folder is C:\Program Files\Hewlett-Packard\HP FMA\.
  - Send a Windows application and system event log. These logs are available in the Event Viewer section of the Windows Computer Management window. To save a log, right-click the log, select **Save File As**, and save it to the computer.
- Troubleshooting package

To generate a troubleshooting package, right-click **HP File Migration Agent** in the left navigation pane of the FMA user interface and select **Troubleshooting Package**. When prompted, specify a location for the ZIP file.

The package contains files that provided detailed information about FMA, including events, file information, log entries, policies, registry information, system information, and version information.

- FMA configuration
  - Use the **regedit** command to export the following registry keys:
    - 32-bit systems: KEY\_LOCAL\_MACHINE\Software\Hewlett-Packard\HP FMA
    - 64-bit systems: KEY\_LOCAL\_MACHINE\Software\WOW6432Node\Hewlett-Packard\HP FMA
    - HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\hsmfilter
  - For problems installing or uninstalling, provide the FMAInst.log and FMARemove.log files. By Default, these files are located in the %temp% directory.
  - If a file cannot be opened or processed, redirect the output of the **fmacli info -l filename** command to a file.

- If an FMA command line operation failed, provide the log file or a screenshot of the stdout/stderr output.
- If an FMA process has terminated abnormally, provide the Dr. Watson log file and the related user dump.

Run **drwtsn32** from a command window to find the Dr. Watson log file path and user dump location.

## Accessing FMA log files

FMA has several log files that you can reference when troubleshooting issues.

### FMA log

FMA writes all FMA-related messages in a log file named **hsm.log**. The log file is stored in the installation folder. The default location is C:\Program Files\Hewlett-Packard\HP FMA\log\hsm.log.

#### To access the FMA log

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Show Log**.

The FMA log is displayed in a separate window.

#### To set the logging level for messages written to the FMA log

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, select one of the following levels from the File list in the Logging level area:
  - **Error**—Events that are likely to cause problems
  - **Warning**—Events that can indicate a problem if they do not occur in the correct context
  - **Information**—Basic events
  - **Debug**—Detailed information, typically required only for troubleshooting
4. Click **OK**.

## Layout

The layout of the log file is as follows:

| Date and Time       | PID/TID     | Module | Severity: | Message Text                                      |
|---------------------|-------------|--------|-----------|---------------------------------------------------|
| 2005-02-21 13:28:17 | [07D0/07F0] | FMASVC | [I]:      | Setting log level 2 for file.                     |
| 2005-02-21 13:28:17 | [07D0/07F0] | FMASVC | [I]:      | Setting log level 1 for event log.                |
| 2005-02-21 13:28:17 | [07D0/07F0] | FMASVC | [I]:      | License OK. Capacity: UNLIMITED, used: 0 GB.      |
| 2005-02-21 13:28:17 | [07D0/07F0] | FMASVC | [I]:      | Hsmfs debug flags: 0x000000FF..                   |
| ...                 |             |        |           |                                                   |
| 2005-03-02 10:41:16 | [07F8/02A4] | FMAVmr | [E]:      | delete file 0005000000000040 failed, rc=00000006. |

**FMA / Windows Returncodes (>65536 = FMA)**

## Limits

The FMA log file is created with the following limits:

- Maximum size is 10MB. If the file size reaches 10MB, the file is switched.
- The current log file is **hsm.log**. Older log files are named **hsm.nnn**, where the lowest number contains the youngest file:

hsm.000

hsm.001

...

hsm.099

- By default, up to 100 log files (hsm.000 - hsm.099) are stored.

## To change the number of FMA log files saved

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, enter a number in the **Max files** field.
4. Click **OK**.

## FMACLI log

Optionally, you can log all actions taken in the FMA command line interface (FMACLI). This is highly recommended because the options in FMACLI are case-sensitive.

To configure the log file option of the FMACLI command, use the **--logfile logfile** global option. Use the **--log-info-messages** option to specify a verbose log.

For more information about FMACLI, see [Command Line Interface Reference](#) on page 81.

## Windows event log

By default, warning and error messages are recorded in the Windows application event log. By changing the log settings informational messages can also be logged into the event log, although this is not recommended.

### To set the logging level for messages written to the Windows event log

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, select one of the following levels from the System list in the Logging level area:
  - Error—Events that are likely to cause problems
  - Warning—Events that can indicate a problem if they do not occur in the correct context
  - Information—Basic events
  - Debug—Detailed information, typically required only for troubleshooting
4. Click **OK**.

## Troubleshooting installation

### If installation failed

- Ensure that the prerequisites defined in the *FMA Release Notes* were met. For example, if the operating system currently installed on this computer is not supported, you must upgrade it in order to use FMA.
- Ensure that the technical user has administrator privileges.
- Ensure there is sufficient local disk space.
- Check the last line of the **FMAInstall.log** file, which contains potential error codes.

### If the “Protocol error, eye-catcher not found or invalid length” error is displayed

- Check the versions of the installed file in a binary directory and ensure that the FMA installation is the only location in the “PATH” that contains FMA binaries.
- Use **Repair** from the Setup Maintenance to refresh a corrupted installation.

## Troubleshooting configuration issues

### If the license does not work

Ensure that the license key was entered correctly. HP Licenses are currently bound to the primary IP address. The IP address used must be the primary IP address of the server regardless of whether the standalone or clustering configurations are used. See [Licensing](#) on page 21 for more information.

### If FMA does not start

- Verify that the license is correct.
- Check the password for the technical user account.
- Verify that the technical user account has sufficient privileges.
- Verify that the file system filter is running by entering `fl tmc` on the command line.

### **If files are not migrated**

- Verify the migration policy.
  - Verify that the migration policy is enabled.
  - Check for the correct policy path.
  - Check include and exclude filters. Remember that the exclusion list takes precedence over the inclusion list.
- Verify that a schedule is defined on the managed volume.
- Verify that the archive is available. Check the FMA log files for any RSA errors.

### **If a "disk full" error is displayed for a managed volume**

- Decrease the high and critical watermark.
- Reduce the monitoring interval.
- Check the retention times.
- Check whether *hard* quotas are configured.

### **If migrated files are not released**

- Check retention times. Remember that the "recalled" timestamp takes precedence over the modification or access timestamp.
- Check the number of existing archive copies by entering `fmacli info`. Remember that a file that is not covered by a file policy must have at least two archive copies before it can be released.
- Verify that the file size is larger than 1KB. Smaller files are not released.
- Verify that the file is not excluded for release.
- Verify that the archive is available.

### **If IrpStackSize is too small for server to use a local device (EventID: 2011)**

This problem is caused by increasing the number of file system filters running on a system. To resolve it, follow the Microsoft instructions under KB198386.

### **If no more archives can be added because maximum number of archives reached**

Remove archive entries with the status "Deleted=1" from the following registry key:  
HKLM\Software\Hewlett-Packard\HP FMA\Archives

Note The maximum number of defined archives is 255.

## **Troubleshooting connectivity**

### **If files cannot be migrated to the FTP archive (RSA-error: 0x006000x)**

- Verify the RSA configuration settings.
- Ping the FTP server.
- Enter the following to connect and log in to the FTP server:  
`ftp hostname`
- Release and recall a test file.
- Increase the connect timeout parameter in the RSA configuration dialog from 500ms to 5000ms.

- Set the debug mode of the RSA-FTP module:
  - a. Open the following registry entry:
    - HKLM\Software\Hewlett-Packard\HP FMA\Archives\ArcID\RsaConfig
  - b. Change the debug level from 0 to 5:
    - <DebugLevel>5</DebugLevel>
    - <DebugLevelFtp>5</DebugLevelFtp>
  - c. Restart all FMA services.
  - d. Start DbgView to capture RSA debug information.

**If files cannot be migrated to the CIFS archive (RSA-error: 0x006000x)**

- Ensure that share permissions are configured correctly. Select the Sharing tab on the folder Properties dialog box and click **Permissions**. The technical user account must have Full Control.
- Check NTFS folder permissions. The technical user account must have Full Control.

**If files cannot be migrated to the IAP archive (RSA-error: 0x006000x)**

- Verify the RSA configuration settings.
- Verify that the applications integrated with IAP have TCP/IP access to ports 25, 80, and 81.
- Enter the following to test the IAP SMTP portal:
  - telnet <ip\_address\_of\_portal> 25
- Check for IAP error codes (E\_RISSSMTP\_xxx, E\_RISSHTTP\_xxxx) in the FMA log file.
- Set the debug mode of the RSA-IAP module:
  - a. Open the following registry entry:
    - HKLM\Software\Hewlett-Packard\HP FMA\Archives\<ArcID>\RsaConfig
  - b. Change the debug level from 0 to 5:
    - <DebugLevel>5</DebugLevel>
  - c. Restart all FMA services.
  - d. Start DbgView to capture RSA debug information.

## Troubleshooting common issues

### If a system fault (BSOD) occurs

A system fault (blue screen) occurs when Windows detects a problem or error from which it cannot recover. The contents of the memory are dumped to a file for later analysis. (By default, this file is %SystemRoot%\memory.dmp.) When this screen is displayed, deeper investigation with WinDBG and debugged version of file system filter must be initiated by Technical Support.

Have the following information ready when you report a system fault (blue screen):

- Windows operating system version and service pack level
- Name of installed file system filters (screenshot of fltmc command output)
- FMA log files
- Application and system event log
- Memory dump file

### If an application fault occurs

A crash dump analysis must be performed by Technical Support if the application fault was caused by one of the following processes:

- HsmSvc.exe
- HsmVolMgr.exe
- FMACfs.exe
- FMACli.exe

Have the following information ready when you report an application fault:

- FMA log files
- Application and system event log
- Full crash dump file
  - The crash dump location is displayed by drwtsn32.exe.
  - The crash dump type (Full, Mini, NT4 compatible Full) can be configured using drwtsn32.exe.

### If the system stalled

The user interface or Windows Explorer can take a long time to open if the system stalls.

- Check whether the computer on which FMA is installed is up and running
- Check the configuration of the computer on which FMA is installed.
  - Verify that port 9111 (default) is not used by any other application.
  - Check the following registry entry:  
HKLM\Software\Hewlett-Packard\HP FMA\ConfigServer
    - For a stand-alone system, the ConfigServer entry is not needed. If the entry exists, it must be set to localhost.
    - For a cluster system, the ConfigServer entry is mandatory and must be set to the virtual cluster IP address.
- Check FMA log files for FMACfs error messages.

## Tracing Archive Files

- Enter the following to retrieve the storage descriptors:

```
fmacli info -l filename
```

The following example shows the output from this command:

```
File: D:\ASC\MyFile.doc
File info:
state=SAV(1), attr=-A-----F, size=102400, generations=0001
Filter file info:
SysFileID=0001000000000038, AppFileID=0000000000000000, chgTime=2006-02-01
13:49:36,766, FileSize=104965100, CLEAN, ONLINE
File generation info:
size=104965100, last_mig=2006-02-01 13:49:36,766, last_rec=2006-05-03
15:11:04,268, attr=-A-----, locations=1
File location info:
ArchiveID=1, ArcPoolID=1, dwNumRec=1, storage_handle_descr=Id: 2 Version: 2
Filesize: 104965444 Last Write Time: 20060503130432 File name: MyFile.doc
12 files succeeded
0 files failed
0 files were processed earlier
22579118080 bytes processed
```

Gather the following file location information:

- Archive ID
- storage\_handle\_descr
- On the FMA user interface, look up the RSA configuration and determine the URI.
  - For CIFS, the URI is the primary archive + storage\_handle\_descr, for example:  
\\NAS\arc2\W2K3EE64BIT\9C162104\openbooks\uml\_tutorial.pdf
  - For FTP, the URI is Host/IP + ftp\_server\_RootDirectory + RSA\_root-path + Filename, for example:  
ftp://FSE/ftp\_server\_RootDirectory/fs1/openbooks/uml\_tutorial.pdf  
where ftp\_server\_RootDirectory is the home directory for the ftp user fma.

## If the “Duplicate Serial Number” error message is displayed

A snapshot of a managed volume has been mounted on the system. This is not supported by FMA.

### If offline files are not accessible (ACCESS\_DENIED)

- Verify that Hsmfilter is running. If it is not, enter `fltmc load hsmfilter` and start the FMA services.
- Check whether the file is inactive.
  - Enter the following to determine the file status: `fmacli info filename`
  - Enter the following to activate the file: `fmacli act filename`
- Check whether the filter recall timeout has been exceeded. Access the file again and then increase the filter timeout (HsmfsTimeout) in the registry.
- Check whether the archive read timeout has been exceeded. Increase the archive read timeout (ArchiveTimeout) in the registry.
- Check NTFS security.

### **If recall performance is poor**

- Check if disk caching is enabled.
- Check load and performance on the archive system.

### **If the managed volume status remains not mounted**

- Trigger a remount request:
  - For a stand-alone system, enter: `fsutil volume dismount drive`
  - For a cluster system, take the volume offline and online again.
- Check whether volume is accessible.
- Check for orphaned HsmVolMgr processes.
- If the file cannot be migrated and a SHARING\_VIOLATION error code is displayed, the file is in use by another application.

### **If archive device has high latency time that affects throughput**

If you are using an archive device that has a high latency time when storing files, you can increase the number of worker threads and the number of concurrent operations to optimize throughput. Increasing the number of parallel operations per volume improves the overall throughput when migrating to such systems.

**Note** In general you do not need to change the default settings. It is not recommended that you change these values unless directed to do so by Technical Support.

#### **To change the number of worker threads**

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, enter a higher number of threads in the **Worker Threads HSM** field in the Global Settings area.
4. Click **OK**.

#### **To change the number of concurrent operations**

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, enter a higher number of operations in the **Concurrent Operations** field in the Global Settings area.
4. Click **OK**.

### **If the "Overflow of the auto activation file cache. Increase 'Auto Activate List Size' setting." (Error: RC=0x00010350) error is displayed**

Auto Activation is the process that takes place when managed files (stub files) are restored from a backup. Each file must be activated by a dedicated thread in the system. This error indicates that the list size must be increased.

#### **To increase the size of the auto activate list**

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, enter a higher list size (in increments of 1024) in the **Auto Activate List Size** field in the Global Settings area.

4. Click **OK**.

**If the “<<< Auto-activate metadata file 0x0000000000000000 terminated, rc=00000020” (rc=0x0020 “Sharing Violation”)” error is displayed**

Auto Activation is the process that takes place when managed files (stub files) are restored from a backup. Each file must be activated by a dedicated thread in the system. This error indicates that the delay time for auto activation must be increased.

**To increase the delay time for auto activation**

1. In the left pane of the FMA user interface, right-click **File Migration Agent**.
2. Click **Properties**.
3. In the Properties dialog box, enter a higher delay time in the **Auto Activate Delay** field in the Global Settings area.
4. Click **OK**.

## **Troubleshooting third-party application issues**

**If unexpected recalls occur during backup**

- Check the FMA log file to see which process has triggered the recalls. For example:  
Event: data offline, fileID=0x000100000002971C, type=READ, process=[iexplore.exe], SID=[S-1-5-21-1507807297-445138137-1326596225-500]
- If recalls were triggered by the system process, configure AntiVirus real-time scanning mode to “on-write” access.
- Configure the backup management application for VSS.
- Verify that the managed volume is not backed up using a share.

**If unexpected recalls occur during AntiVirus manual scans**

- Check the *FMA Release Notes* to see whether the AntiVirus is supported for FMA.
- Determine the process name that triggered the recalls. Check whether this process name is listed in the FMA IgnoreModules registry entry.

**If unexpected recalls occur while searching for words or phrases using Windows Explorer**

Clear **Search tape backup** in Advanced options.

**If unexpected recalls occur while searching using Google Desktop**

This is not supported by FMA.

**If there are no search results for offline files**

- Windows Explorer skips files with the Offline attribute set.
- Microsoft Index Server removes the indexes for offline files.

**If thumbnails are not visible**

Windows Explorer removes the thumbnails for offline files.

**If poor backup performance occurs**

Configure the AntiVirus real-time scanner to “on-write” access.

## If Office files cannot be opened when working offline using offline folder replication

Update the Windows XP client system using the following:

<http://support.microsoft.com/kb/936071/en-us>

## Troubleshooting cluster systems

### If a managed volume cannot be activated

- Check whether the volume GUID is listed in the following registry key:

HKLM\System\CurrentControlSet\Services\hsmfilter\Volumes

The volume GUID can be determined by using the **mountvol** command. If the GUID is missing, delete and then add the volume as an FMA managed volume on the node.

- Check whether the volume can be accessed by writing a test file.
- Check whether a mount request for the volume has been sent to FMA by analyzing the hsm log file.
  - If no mount message for the volume can be found, analyze **cluster.log** located in the %windir%\cluster directory for any problems.
  - Check whether the Microsoft hotfix KB911030 is installed in case the customer is running Windows 2003 service pack 1.
- Enter the following command to check the number of file system filter instances:

fltmc

| Filter Name      | Num Instances | Frame |
|------------------|---------------|-------|
| FileScreenFilter | 5             | 1     |
| hsmfilter        | 2             | 1     |
| TmPreFilter      | <Legacy>      |       |
| DfsDriver        | <Legacy>      |       |
| QaFilter         | 5             | 0     |

The number of instances must be equal to the number of mounted FMA managed volumes on a particular node.

- Set the volume offline and online again using the Windows cluster administration user interface.
- If the problem cannot be resolved with these steps, provide the following information to the HP FMA support team:
  - Detailed problem description
  - FMA hsm log files
  - System and application event logs
  - **Cluster.log** files from all nodes
  - Output of the commands mountvol and fltmc from all cluster nodes

### If the FMA archive configuration is not displayed on one node

- Check whether the FMA configuration service is up and running in the default cluster group.
- Check whether the following registry entry contains the virtual IP address of the cluster system.

For 32-bit: HKM\Software\Hewlett-Packard\HP FMA\ConfigServer

For 64-bit: HKLM\Software\Wow6432Node\Hewlett-Packard\HP FMA\ConfigServer

- Enter the following command to check whether TCP/IP port 9111 is already used by any other instance:

```
netstat -a
```

The port can be changed in the %windir%\system32\drivers\etc\services file in the hsmconfsrv port/tcp entry.

## Third-party Product Compatibility List

---

### Anti-virus

FMA's interoperability with anti-virus scanners has been successfully tested for the following products.

#### Symantec AntiVirus

|                         |                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name:           | AntiVirus / EndPoint Protection                                                                                                                                                                                                                                                                                                      |
| Manufacturer:           | Symantec                                                                                                                                                                                                                                                                                                                             |
| Version:                | AntiVirus 10.1, EndPoint Protection 11.0                                                                                                                                                                                                                                                                                             |
| Supported FMA Versions: | 2.5                                                                                                                                                                                                                                                                                                                                  |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                                                                                                                                                                                                      |
| Restrictions:           | The feature "scan files opened for backup" is not supported. Therefore, the option "opened for backup" needs to be switched off in Symantec AntiVirus "Auto-Protect Advanced Options" menu.                                                                                                                                          |
| Remark:                 | To more efficiently scan files maintained by Hierarchical Storage Management (HSM), Symantec AntiVirus enables configuration options for on-demand or scheduled scans.<br>The appropriate settings for FMA are: <ul style="list-style-type: none"><li>• Skip offline and sparse</li><li>• Open files with Backup semantics</li></ul> |

#### McAfee VirusScan

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | VirusScan                                                       |
| Manufacturer:           | McAfee                                                          |
| Version:                | Enterprise 8.0i, Enterprise 8.5                                 |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |

|               |                                                                                                                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrictions: | None                                                                                                                                                                                                                                                                                                        |
| Remark:       | For proper interoperability, HP recommends not selecting the option:<br>Scan files that have been migrated to storage<br>The option is located in the menu: <ul style="list-style-type: none"> <li>• VirusScan On-Demand Scan Properties</li> <li>• Advanced properties</li> <li>• Miscellaneous</li> </ul> |

### Sophos Anti-Virus

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | Sophos Anti-Virus                                               |
| Manufacturer:           | Sophos                                                          |
| Version:                | 6.5, 7.x                                                        |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |
| Restrictions:           | None                                                            |
| Remark:                 | None                                                            |

### ServerProtect

|                         |                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------|
| Product Name:           | ServerProtect                                                                            |
| Manufacturer:           | TrendMicro                                                                               |
| Version:                | 5.58, 5.7                                                                                |
| Supported FMA Versions: | 2.5                                                                                      |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                          |
| Restrictions:           | None                                                                                     |
| Remark:                 | Opening the property page of an offline file triggers a file recall from remote storage. |

### eTrust AntiVirus

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | eTrust AntiVirus Scanner                                        |
| Manufacturer:           | Computer Associates International                               |
| Version:                | 8.0, 8.1                                                        |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |

|               |                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrictions: | None                                                                                                                                                      |
| Remark:       | Because eTrust changes the access timestamp of a file, the release operation should be based on the modification timestamp and the last recall timestamp. |

### **TrendMicro OfficeScan**

|                         |                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------|
| Product Name:           | OfficeScan                                                                               |
| Manufacturer:           | TrendMicro                                                                               |
| Version:                | 7.0, 8.0                                                                                 |
| Supported FMA Versions: | 2.5                                                                                      |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                          |
| Restrictions:           | None                                                                                     |
| Remark:                 | Opening the property page of an offline file triggers a file recall from remote storage. |

### **Backup/restore**

FMA's interoperability with backup/restore applications has been successfully tested for file system backup/restore operations with the following products.

Additional features, like data archiving or disk image creation, were not subject of interoperability tests.

### **BackupExec**

|                         |                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name:           | BackupExec                                                                                                                                                |
| Manufacturer:           | Veritas                                                                                                                                                   |
| Version:                | 11D, 12.0                                                                                                                                                 |
| Supported FMA Versions: | 2.5                                                                                                                                                       |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                           |
| Restrictions:           | FMA does not support "file activation" for files that have been restored to a new location. Restoring files is only supported to their original location. |
| Remark:                 | None                                                                                                                                                      |

### **BrightStor ArcServe**

|               |                            |
|---------------|----------------------------|
| Product Name: | BrightStor ArcServe Backup |
| Manufacturer: | Computer Associates        |
| Version:      | 11.5, 12                   |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported FMA Versions: | 2.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Restrictions:           | FMA does not support “file activation” for files that have been restored to a new location. Restoring files is only supported to their original location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Remark:                 | <p>During backup restore, CA ArcServe does not overwrite a migrated file with a stub file. This appears in the CA activity log as “Skip file - Migrated”. CA ArcServe does, however, overwrite a stub file with a stub file from tape.</p> <p>As a workaround, remove the old files first. To do this, right-click the volume in FMA management and select <b>Stop</b>. Delete the files from the restore destination. When Volume Management is stopped, deleted files are not placed in the garbage collection list, thus preserving the file copy in the archive. Then, right-click the volume again and select <b>Start</b>, and restore the stub files from tape. An alternative to stopping volume management is to use the <code>fmacli activate --off</code> command on specific files or directories.</p> |

### Data Protector

|                         |                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name:           | Data Protector                                                                                                                                            |
| Manufacturer:           | HP                                                                                                                                                        |
| Version:                | 6.0, 6.1                                                                                                                                                  |
| Supported FMA Versions: | 2.5                                                                                                                                                       |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                           |
| Restrictions:           | FMA does not support “file activation” for files that have been restored to a new location. Restoring files is only supported to their original location. |
| Remark:                 | None                                                                                                                                                      |

### NetBackup

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | NetBackup Enterprise Server                                     |
| Manufacturer:           | Veritas                                                         |
| Version:                | 6.0, 6.5.x                                                      |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |

|               |                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrictions: | FMA does not support “file activation” for files that have been restored to a new location. Restoring files is only supported to their original location. |
| Remark:       | When using the Veritas AOFO option, you must select the Microsoft VSS service.                                                                            |

## Networker

|                         |                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name:           | Networker                                                                                                                                                 |
| Manufacturer:           | EMC                                                                                                                                                       |
| Version:                | 7.2, 7.4                                                                                                                                                  |
| Supported FMA Versions: | 2.5                                                                                                                                                       |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                           |
| Restrictions:           | FMA does not support “file activation” for files that have been restored to a new location. Restoring files is only supported to their original location. |
| Remark:                 | None                                                                                                                                                      |

## NetVault

|                         |                                                                                                                                                                                                                                                                              |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name:           | NetVault                                                                                                                                                                                                                                                                     |
| Manufacturer:           | BakBone                                                                                                                                                                                                                                                                      |
| Version:                | 7.1.1, 8.1                                                                                                                                                                                                                                                                   |
| Supported FMA Versions: | 2.5                                                                                                                                                                                                                                                                          |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                                                                                                                                              |
| Restrictions:           | FMA does not support “file activation” for files that have been restored to a new location. Restoring files is only supported to their original location.                                                                                                                    |
| Remark:                 | NetVault skips files that FMA is in the process of migrating. Choose an FMA policy start time that does not overlap with disaster recovery backups. Also, the <b>Check for files being modified during backup?</b> option can be disabled to eliminate the warning messages. |

## MS VSS

|                         |                                         |
|-------------------------|-----------------------------------------|
| Product Name:           | Volume Shadow Copy Services (VSS)       |
| Manufacturer:           | Microsoft                               |
| Version:                | A component of Windows operating system |
| Supported FMA Versions: | 2.5                                     |

|                   |                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating System: | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                                                                  |
| Restrictions:     | See the FMA Readme.txt file for the latest updates. To access the Readme.txt file, select <b>All Programs</b> → <b>HP StorageWorks File Migration Agent</b> → <b>FMA Readme</b> .                |
| Remark:           | Volume snapshots can be taken on FMA managed volumes; there is no negative interference between VSS and FMA.<br>Taking volume shadow copies does not initiate recalls of already released files. |

### Tivoli Storage Manager

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name:           | Tivoli Storage Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Manufacturer:           | IBM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Version:                | 5.4.x, 5.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Supported FMA Versions: | 2.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Restrictions:           | <ul style="list-style-type: none"> <li>• FMA does not support “file activation” for files, which have been restored to a new location. Restoring files is only supported to their original location.</li> <li>• The TSM Logical Volume Snapshot Agent is not supported in combination with FMA.</li> <li>• FMA does not support TSM backup in combination with Sophos Anti-Virus realtime-scanning.</li> </ul>                                                                                                                                                                                                                                                    |
| Remark:                 | <p>When restoring files using TSM, TSM does not overwrite an HSM managed or recalled file with a stub file.</p> <p>As a workaround, remove the old files first. To do this, right-click the volume in FMA management and select Stop. Delete the files from the restore destination. When Volume Management is stopped, deleted files are not be placed in the garbage collection list, thus preserving the file copy in the archive. Then, right-click the volume again and select Start, and restore the stub files from tape. An alternative to stopping volume management is to use the “fmacli activate --off” command on specific files or directories.</p> |

### Galaxy Backup & Recovery

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | Galaxy Backup & Recovery                                        |
| Manufacturer:           | CommVault Systems                                               |
| Version:                | 6.1, 7.0                                                        |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrictions: | FMA does not support “file activation” for files, which have been restored to a new location. Restoring files is only supported to their original location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Remark:       | <p>VSS can be used on a server, with volumes managed by FMA.</p> <p><b>Note:</b> Volume snapshots can be taken on FMA managed volumes; there is no negative interference between VSS and FMA. Taking volume shadow copies does not initiate recalls of already released files.</p> <p>When using VSS and FMA, the following restrictions exist:</p> <ul style="list-style-type: none"> <li>• FMA supports VSS when used by a qualified backup application. It does not support the use of VSS-Client.</li> <li>• FMA does not support file activation for files that have been restored to a new location. Restoring files is only supported to their original location. <ul style="list-style-type: none"> <li>• Restoring previous versions from VSS to original location: No restrictions exist to the restore of online files.</li> <li>• Viewing previous snapshot from VSS: Viewing a previous snapshot of files that were offline during the volume snapshot is not supported.</li> <li>• Copying previous versions from VSS to a different location is not supported by FMA.</li> </ul> </li> </ul> <p>Since shadow copies are read only, it is not possible for FMA to recall a file using a stub file in a shadow copy. HP recommends giving careful consider this limitation when deploying both VSS and FMA.</p> |

## Quota/encryption

### StorageExec

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | StorageExec                                                     |
| Manufacturer:           | Veritas                                                         |
| Version:                | 5.0                                                             |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |
| Restrictions:           | Only passive limits on FMA managed volumes are supported.       |
| Remark:                 | None                                                            |

## Defragmentation

### O & O Defrag

|               |                |
|---------------|----------------|
| Product Name: | O & O Defrag   |
| Manufacturer: | O & O Software |

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Version:                | 8.0                                                             |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |
| Restrictions:           | None                                                            |
| Remark:                 | None                                                            |

### MS Defragmentation

|                         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| Product Name:           | Defragmentation                                                 |
| Manufacturer:           | Microsoft                                                       |
| Version:                | Windows 2003, Windows 2008, Windows Unified Data Storage Server |
| Supported FMA Versions: | 2.5                                                             |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server |
| Restrictions:           | None                                                            |
| Remark:                 | None                                                            |

## IndexServer

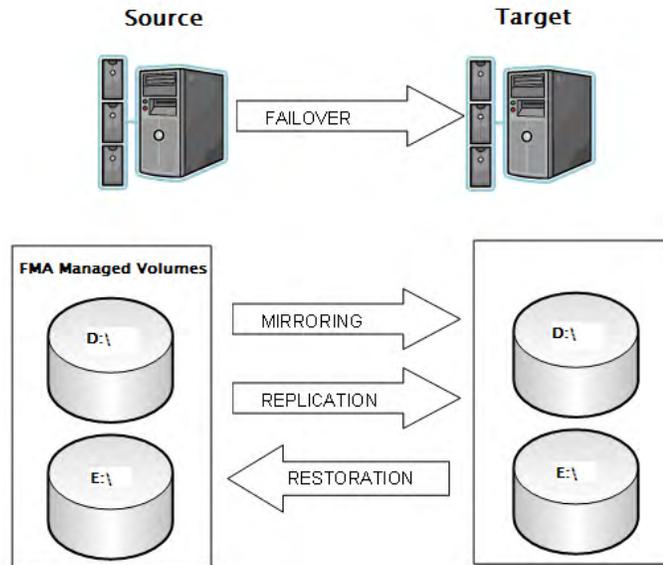
### MS IndexServer

|                         |                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------|
| Product Name:           | IndexServer                                                                                                    |
| Manufacturer:           | Microsoft                                                                                                      |
| Version:                | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                |
| Supported FMA Versions: | 2.5                                                                                                            |
| Operating System:       | Windows 2003, Windows 2008, Windows Unified Data Storage Server                                                |
| Restrictions:           | None (interoperable, no recalls)                                                                               |
| Remark:                 | The IndexServer only keeps index informations of online files. Index informations are lost by releasing files. |

## HP Storage Mirroring Interoperability

File Migration Agent 2.5 supports the following features of HP Storage Mirroring 5.1.1.867:

- **Mirroring**—The initial copy or subsequent resynchronization of selected data
- **Replication**—The on-going capture of byte-level file changes
- **Failure monitoring and failover**—The ability to monitor and stand-in for a server, in the event of a failure
- **Restoration**—A mirror of selected data from the target back to the source



There are some limitations and additional configuration requirements for FMA and HP Storage Mirroring interoperability. Refer to the HP Business Support Center below for technical manuals on HP StorageWorks Storage Mirroring Software. Individual manuals describe how each of the major features of Storage Mirroring are supported by FMA.

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

### Mirroring and Replication

Mirroring is the process of transmitting user-specified data from the source to the target so that an identical copy of data exists on the target. When Storage Mirroring initially performs mirroring, it copies all of the selected data, including file attributes and permissions. Replication is the real-time transmission of file changes. The Storage Mirroring replication process operates at the file system level and is able to track file changes independently from the file's related application. Replication keeps the target up-to-date and synchronized with the source.

HP Storage Mirroring is able to mirror and replicate files and file stubs from managed volume(s) to target storage on the target server. HP File Migration Agent supports one way (active source/passive target) mirroring and replication provided by HP Storage Mirroring. FMA can be installed on both source and target with the below restrictions in mind.

|               |                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrictions: | The same resources (files or file stubs) can not be managed concurrently by HP File Migration Agent on source and target server during mirroring and replication. |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Failure monitoring and failover

Failover is the process in which a target stands in for a failed source. As a result, user and application requests that are directed to the failed source are routed to the target. Storage Mirroring monitors the source status by tracking network requests and responses exchanged between the source and target. When a monitored source misses a user-defined number of requests, Storage Mirroring assumes that the server has failed. Storage Mirroring then prompts the network administrator to initiate failover, or, if configured, it occurs automatically.

HP Storage Mirroring provides different options to the users during failover configuration. These options include failing over the following items:

- IP address
- Hostname
- Shares (resources)

Depending on which options are selected, the user is limited to certain configurations. If the user decides to create a full failover including IP address, Hostname, and Shares, the user is limited to only a one-way mirroring and replication (active source/passive target) configuration. If the user wanted a two-way mirroring and replication, only the share resources can be selected during failover configuration.

**WARNING** Failover IP address and Hostname in an active source/active target configuration causes data loss on one of the servers. Follow the configuration instructions carefully when configuring an active/active configuration.

In the event of a failover, a script must be run to activate all the file stubs located in the volume(s) of the target server.

## Restoration

Restoration provides a method for copying replicated data from the target back to its original location on the source. When using HP Storage Mirroring with HP File Migration Agent, you have the ability to restore files and file stubs back to the original managed volume. When using this feature, an extra step is required to fully restore a file stub(s). Run the FMA CLI command **fmacli act** on the file stub(s) before recalling the file(s).

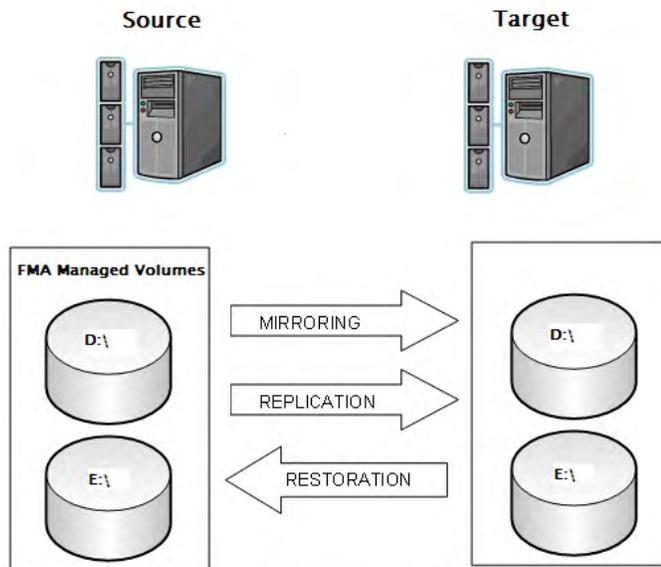
For example, if file stubs were restored on letter drive D:\ on the source server.

- a. Open up a command prompt on the source server.
- b. Run `fmacli act -r D:` to reactive the file stubs.

If this command is not executed, an error occurs when attempting to recall the files.

## Supported Configuration

### Configuration 1



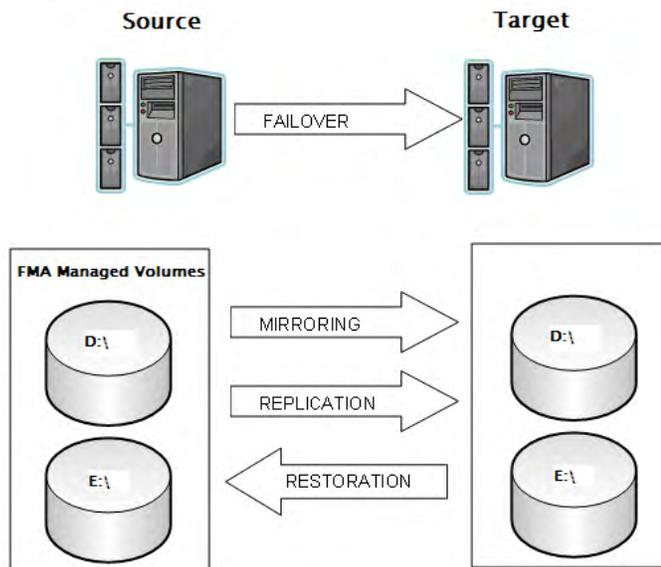
This configuration utilizes the HP Storage Mirroring features, but does not utilize the failover features of HP Storage Mirroring:

- Mirroring
- Replication
- Restoration

The failover feature is not used because the Source server is part of a Microsoft cluster configuration. In this case, only the Source server has the File Migration Agent installed, but HP Storage Mirroring is required for both source and target. There are no special procedures required to install and configure this configuration. Refer to the product manual for details.

**Note** In Configuration 1, the FMA command **fmacli act** must be run manually after a file stub has been restored onto the source volume(s) in order for recall to operate correctly. This can be done by running a script. Creation of this script is described in [Script creation](#) on page 147.

## Configuration 2



These are the types of failover that HP Storage Mirroring provides:

- Partial Failover
- Full Server Failover

This configuration is most likely to be used if no clustering is available. The HP Storage Mirroring failover wizard allows failover for the following elements:

- IP address
- Server Name
- Share(s)

When choosing the partial failover, only the share(s) are failover to the target server. The term *failover* is different than what is used in a cluster. When there is a replicated set of data on both source and target servers, the target server takes over the management of FMA volumes in the event a failover occurs. No physical resources are actually moved. When selecting the full server failover, the target server inherits the IP address, Server Name, and all the Shares of the source server. A reboot is required during a full server failover to enable the failover server to take over all the properties of the failed server. A partial failover does not require a reboot.

In this configuration, FMA and HP Storage Mirroring are installed on both servers. FMA configuration is only required on the source server. The replication set must be mirroring to identical drive letters between source and target volumes. The FMA configuration is stored in the **HSM Volume Information** which is required to be part of the replication set when configuring HP Storage Mirroring. There is a minimum download time for failover in this configuration.

A script needs to be run after failover and failback to reactivate the file stubs. Creation of this script is described in [Script creation](#) on page 147.

**Note** In Configuration 2, if you are archiving to a CIFS archive using the failover, the **Ignore system name** and **Ignore serial for storage descriptor** options must be used to enable the target server's access to the archive files.

## Script creation

It is necessary to create a script to reactivate the file stubs during restoration and failover/failback. To create a script open a text editor, such as Notepad, on your Windows server. The reactivation command is **fmacli act -r <drive letters>**. The drive letters are the managed volumes of your FMA server. For example:

If you have letter drive D:\ and E:\ managed on your FMA server, you would need two lines in your script:

```
fmacli act -r D:\
fmacli act -r E:\
```

The **-r** option is for recursive; it activates all files in folders and subfolders on a disk drive.

After entering the two lines with the correct drive letters, save the file as a .bat file. Make a note where you save the batch file and point to it during the HP Storage Mirroring failover configuration. You can also run this batch file if you restore some files from the target server.



## Error Codes and Messages

This appendix contains information about FMA-related messages and their descriptions. FMA returns a WIN32 defined error code or an FMA defined information or error code. For a description of system error codes (Code No. 0 - 6118), see the Microsoft error list or contact Technical Support.

| Error Code | Error Text            | Description                                                                                                   | Recommended Action                                                                                                                                                                                                       |
|------------|-----------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010001 | File is migrated.     | Informational: The file in question has been migrated.                                                        | The file must be overwritten or modified before it can be migrated again.                                                                                                                                                |
| 0x00010002 | File is not migrated. | Informational: The file was not migrated and cannot be released or recalled.                                  | The file must be migrated before it can be released or recalled.                                                                                                                                                         |
| 0x00010003 | File is released.     | Informational: The file was released and cannot be migrated.                                                  | The file must be recalled and modified or overwritten before it can be migrated again.                                                                                                                                   |
| 0x00010004 | File is online.       | Informational: The file is already online and cannot be recalled.                                             | Files must be released before they can be recalled.                                                                                                                                                                      |
| 0x00010005 | Metadata not found.   | Informational: The file does not contain FMA metadata; it is an unmanaged file.                               | FMA attaches metadata to a file when it is migrated. The file must be migrated.                                                                                                                                          |
| 0x00010006 | File is not expired.  | Warning: File cannot be released by the Disk Space policy because the retention time has not been reached.    | If this behavior is not desired, the retention times can be adjusted. See <a href="#">Releasing files using disk space policies</a> on page 48.                                                                          |
| 0x00010007 | Not enough copies.    | Warning: A file release was attempted by a user or policy but too few migration copies exist in the archives. | If there is more than one archive, ensure there is connectivity to each. The number of copies required is specified in the policy on the Archives tab. If there is no policy defined for a given file, the default is 2. |

| Error Code | Error Text                                                                | Description                                                                                                                                                                                                                         | Recommended Action                                                                                                                                               |
|------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x0001000A | FMA operation on internal control file was ignored                        | Warning: FMA operations on internal files are ignored when a user tries to manage a file that is in the HSM Volume Information directory. This directory is a hidden system folder located at the root level of the managed volume. | Files in the HSM Volume Information directory cannot be managed.                                                                                                 |
| 0x0001000B | Directory ignored.                                                        | Warning: When the user attempted to perform an FMA operation on a directory, it was ignored.                                                                                                                                        | Do not attempt FMA operations on directories.                                                                                                                    |
| 0x0001000C | File is active                                                            | Informational: The file is already active.                                                                                                                                                                                          | None.                                                                                                                                                            |
| 0x0001000D | File is inactive                                                          | Informational: The file is already deactivated.                                                                                                                                                                                     | None.                                                                                                                                                            |
| 0x0001000E | FMA metadata recovered.                                                   | Informational: An internal operation to acquire FMA metadata from a file was completed successfully.                                                                                                                                | None.                                                                                                                                                            |
| 0x0001000F | File metadata has been disabled                                           | Warning: The file was disabled from FMA management. This occurs when FMA tries to manage a file that has been disabled.                                                                                                             | If desired, the file must be enabled before it can be managed. See the <code>fmacli activate</code> command on page 83.                                          |
| 0x00010010 | File has outdated metadata. Run <code>verify</code> to update file format | Warning: The FMA metadata in the file cannot be used by the currently installed version of FMA.                                                                                                                                     | The FMA metadata needs to be updated using the <code>"fmacli verify --repair filename"</code> command. See <a href="#">verify</a> on page 114.                   |
| 0x00010011 | File is smaller than 1024 bytes. This is below the release limit.         | Warning: Files that are 1KB or smaller cannot be released. Based on NTFS overhead, there is no disk space savings when releasing files that are smaller than 1KB.                                                                   | None.                                                                                                                                                            |
| 0x00010012 | Maximum copies for migration has been reached. File was not migrated.     | Warning: The file has reached the maximum number of archive copies and no additional archive copy of the file has been created.                                                                                                     | If this is not the desired behavior, deselect archives from the policy or change the number of copies if the files are not archiving to the desired destination. |

| <b>Error Code</b> | <b>Error Text</b>                                                            | <b>Description</b>                                                                                                                                                                                                                                                                                               | <b>Recommended Action</b>                                                                                                 |
|-------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 0x00010013        | File has foreign reparse point attached. File cannot be released.            | Warning: Another application has attached a reparse point to the file; only one reparse point can be attached to a file. FMA attaches a reparse point when releasing a file that has been migrated. To avoid conflicts with other applications, FMA does not migrate files with unknown reparse points attached. | If this is not the desired behavior, identify the application attaching foreign reparse points and possibly uninstall it. |
| 0x00010014        | File has foreign reparse point attached. File is excluded from migration.    | Warning: FMA has encountered a file with foreign reparse points attached during normal FMA file management. Only one reparse point can be attached to a file. To avoid conflicts with other applications, FMA does not migrate files with unknown reparse points attached.                                       | If this is not the desired behavior, identify the application attaching foreign reparse points and possibly uninstall it. |
| 0x00010015        | File has foreign reparse point attached. File is excluded from verification. | Warning: FMA has encountered a file with foreign reparse points attached while trying to run the verify command. The verify function is not applied to files with unknown reparse points attached.                                                                                                               | If this is not the desired behavior, identify the application attaching foreign reparse points and possibly uninstall it. |
| 0x00010016        | Tried to remigrate an offline file to the same location                      | Warning: FMA cannot create two identical archive copies of a file in the same storage location. This can occur if the user adds another archive definition to a policy where the volume already contains released files. If the new archive has the same address as the old, the remigration of the file fails.  | Do not create identical archive definitions.                                                                              |

| Error Code | Error Text                                                     | Description                                                                                                                                                                               | Recommended Action                                                                                                                                                                                                                                     |
|------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010017 | Modification timestamp has been changed on offline file        | Error: During migration, processing an offline file has been encountered that has a modification date that is newer than the date of the file at the time that it was migrated.           | Identify the application that could change the modified date without causing a recall. Attempt a repair operation using <code>fmacli verify --repair filename</code> . See page 114. File content may need to be restored from an earlier backup copy. |
| 0x00010018 | File cannot be released since Extended Attributes are attached | Error: File cannot be released because Extended Attributes are attached. This occurs during file release operations.                                                                      | Contact HP Support for assistance in viewing and managing attached extended attributes. Do not delete foreign extended attributes until you are sure they are not needed.                                                                              |
| 0x00010019 | File has an unknown Extended Attribute attached                | Error: Files that contain unknown extended attributes cannot be managed by FMA. This occurs during file activation and in preparation for files to the volume manager for FMA processing. | Contact HP Support for assistance in viewing and managing attached extended attributes. Do not delete extended attributes until you are sure they are not needed.                                                                                      |
| 0x00010100 | General internal error occurred                                | Error: This is an internal error that occurs during FMA software processes management.                                                                                                    | Contact HP Support and report the error. Rebooting the server can help resolve the issue.                                                                                                                                                              |
| 0x00010101 | HsmApi protocol error.                                         | Error: This is an internal error that occurs during FMA message passing.                                                                                                                  | Contact HP Support and report the error. Rebooting the server can help resolve the issue.                                                                                                                                                              |
| 0x00010102 | HsmApi protocol version mismatch.                              | Error: This is an internal error that occurs during FMA message passing. It indicates that there is a version mismatch between FMA components.                                            | Contact HP Support and report the error. Rebooting the server can help resolve the issue.                                                                                                                                                              |
| 0x00010103 | Invalid function                                               | Error: This is an internal error that occurs during FMA message passing. It indicates that there is a programmatic mismatch between FMA components.                                       | Contact HP Support and report the error. Rebooting the server can help resolve the issue.                                                                                                                                                              |

| <b>Error Code</b> | <b>Error Text</b>                             | <b>Description</b>                                                                                                                                                                                                                                                  | <b>Recommended Action</b>                                                                                                                                                                                                                                                                     |
|-------------------|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010104        | Recall failed, no valid archive found.        | Error: FMA was not able to identify the archive referenced by the file's metadata. This occurs when trying to recall a file and the archive cannot be found.                                                                                                        | Check archive definitions. The FMA properties tab of the file indicates the ID of the archive that holds the file. Verify that the named ID is still present. If the archive no longer exists, the file cannot be recalled and must to be restored from a backup copy taken prior to release. |
| 0x00010112        | Archive unknown.                              | Error: The given archive name (specified by the FMA CLI option -a) is not defined in the registry. This occurs when the user tries to migrate a file and the archive name cannot be resolved. The name may be misspelled or the configuration may not be available. | Ensure the archive name is entered correctly.                                                                                                                                                                                                                                                 |
| 0x00010122        | Required entry point in RSA library not found | Error: A mandatory function was not found in the specified RSA Library. This can be due to an old version of the library file or a corrupted library file.                                                                                                          | Reinstall FMA.                                                                                                                                                                                                                                                                                |
| 0x00010131        | Metadata corrupt                              | Error: Archive filename cannot be recovered from metadata. This occurs during a file release or recall operation.                                                                                                                                                   | Erase metadata from the file or restore stub file from the disaster recovery backup.                                                                                                                                                                                                          |
| 0x00010132        | Metadata error                                | Error: Metadata of the file cannot be loaded because it does not match any of the FMA metadata types. This occurs during a file recall operation.                                                                                                                   | Erase metadata from the file or restore stub file from the disaster recovery backup.                                                                                                                                                                                                          |

| <b>Error Code</b> | <b>Error Text</b>                              | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Recommended Action</b>                                                                                                                                                                                      |
|-------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010135        | Unable to activate file, duplicate metadata    | Error: A file cannot be activated because another file already has a valid reference to the requested archive object. This error occurs if a stub file is restored to an alternate location and the original file still exists. This error can also occur if a file is deleted and it goes to the recycle bin. This occurs during automatic file activation, backup restore, or manually using the fmacli activate command. | Restore the stub-file to the original location using the overwrite option. Or, delete the file from the recycle bin.                                                                                           |
| 0x00010160        | Stub file is not empty, recall cancelled.      | During recall, a non-empty stub file was found. This occurs at the start of a file recall.                                                                                                                                                                                                                                                                                                                                  | Notify HP Support. The file may need to be restored from a disaster recovery backup.                                                                                                                           |
| 0x00010164        | File was not completely recalled from archive. | Error: File was not completely recalled from archive.                                                                                                                                                                                                                                                                                                                                                                       | Verify that the connection to the archive is stable and that the size of the stub file matches the size in the archive. The original file size at the time of migration is also available in the FMA metadata. |
| 0x00010171        | Maximum of parallel HSM operations is reached  | Warning: The maximum number of concurrent HSM operations is reached. Storage to process this request is not available. This occurs when a user tries to migrate, recall, release, erase, and so on.                                                                                                                                                                                                                         | Try the operation again after current operations are complete.                                                                                                                                                 |
| 0x00010190        | Verify created informational message           | Informational: The fmacli verify command was successful.                                                                                                                                                                                                                                                                                                                                                                    | None.                                                                                                                                                                                                          |
| 0x00010192        | Verify created error message                   | Error: The file reference entry for the current file generation can not be validated with the archive copy. This occurs during file activation, release, or recall.                                                                                                                                                                                                                                                         | Consult other log entries for more details.                                                                                                                                                                    |

| Error Code | Error Text                        | Description                                                                                                                                                                                                                                                                                   | Recommended Action                                                                                                                              |
|------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010201 | Stub file is not empty.           | Error: A stub file contained data. This occurs during recall or a deliberate verify operation and file is offline but contains data.                                                                                                                                                          | The file may need to be restored from the disaster recovery archive. Investigate third party applications that might modify stub file contents. |
| 0x00010203 | Metadata incomplete.              | Warning: The file generation information of the metadata could not be read. This occurs during a release, recall, or deliberate verify operation on a managed file.                                                                                                                           | The file is damaged and may need to be recovered from the disaster recovery archive. Contact HP Support.                                        |
| 0x00010204 | Stubfile is modified.             | Warning: A stub file's generation file size does not match the OS file size of the stub. This occurs during a release, recall, or deliberate verify operation on a managed file.                                                                                                              | See <a href="#">verify</a> on page 114 and error code 0x00010164. Consider use of "--repair" parameter to resolve the issue.                    |
| 0x00010207 | Offline attribute missing.        | Informational: The offline attribute is clear but the FMA metadata indicates that the file is offline. The offline attribute can be easily and accidentally toggled by many third party applications. This occurs during a release, recall, or deliberate verify operation on a managed file. | See the verify command. Consider use of "--repair" parameter to resolve the issue.                                                              |
| 0x00010208 | Offline attribute invalid.        | Informational: The offline attribute is set but the FMA metadata indicates that the file is online. The offline attribute can be easily and accidentally toggled by many third party applications. This occurs during a release, recall, or deliberate verify operation on a managed file.    | See the verify command on page 114. Consider use of "--repair" parameter to resolve the issue.                                                  |
| 0x00010301 | HsmSvc subsystem is not available | Error: Internal FMA component communications was not functioning correctly. This can occur during normal operations.                                                                                                                                                                          | Attempt to restart all FMA services or reboot the server. If the error persists, contact HP Support.                                            |

| Error Code | Error Text                                         | Description                                                                                                                                                                                                                                                                                              | Recommended Action                                                                                                                                                                         |
|------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010302 | Configuration is invalid.                          | Error: The install path defined in the FMA registry did not resolve to FMA binary or logging directories. This occurs when FMA tries to obtain the installation directory.                                                                                                                               | Check the FMA installation directory. Reinstallation can be necessary if the path is corrupt.                                                                                              |
| 0x00010303 | Volume serial not unique.                          | Warning: Two or more disk volumes attached to the system have the same volume serial number. This occurs during startup when a volume inventory is taken. This can happen if a snapshot of a managed volume is mounted.                                                                                  | Volumes with duplicate serial numbers cannot be managed.                                                                                                                                   |
| 0x00010304 | Volume is not managed.                             | Error: The volume on which the file resides was not managed. This condition is checked prior to all FMA file operations.                                                                                                                                                                                 | The volume must be added to FMA management. See <a href="#">Managed Volumes</a> on page 45.                                                                                                |
| 0x00010305 | Volume status is invalid for this operation status | Error: The current volume operational status for this operation is invalid. This error usually results when the user tries to start FMA volume management when it is already started, or when the user tries to stop an already stopped volume.                                                          | If action was accidental, no action is needed for resolution. If the volume status indication does not appear to be correct, refresh the configuration screen or restart all FMA services. |
| 0x00010306 | Volume ID does not match for file list             | Error: The volume referenced by a file in a list of files targeted for FMA processing does not match the managed volume. This can occur when a list of files is submitted to the volume manager for processing. Typically, the list comes from a <code>fmaccli</code> command or the AFM policy service. | Retry the operation. It is likely that the file was moved to another volume after it was placed on the processing list but before it was actually processed.                               |

| <b>Error Code</b> | <b>Error Text</b>                 | <b>Description</b>                                                                                                                                                                                                                                          | <b>Recommended Action</b>                                                                                                         |
|-------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 0x00010307        | File list is invalid.             | Error: The specified list was not valid, such as if it was not initialized. This can occur when a list of files is submitted to the volume manager for processing. Typically, the list comes from a <code>fmactli</code> command or the AFM policy service. | Retry the operation. If the problem persists, restart the FMA services. If this continues to be an issue, contact HP Support.     |
| 0x00010308        | File list is empty                | Error: The specified list contained no entries. This can occur when a list of files is submitted to the volume manager for processing. Typically, the list comes from a <code>fmactli</code> command or the AFM policy service.                             | Do not submit empty file lists for processing.                                                                                    |
| 0x00010310        | Generic error in licensing module | Error: The licensing subsystem could not function. This occurs during FMA startup or during any operation that requires license validation.                                                                                                                 | If all license codes have been applied correctly, attempt to restart the FMA services or reboot the server.                       |
| 0x00010311        | No license was found.             | Error: No permanent or evaluation license was found. The feature is not licensed or it is violated. This can occur during FMA startup or for any operation that requires license validation.                                                                | Recheck the application's permanent licenses. Restart FMA services or reboot the server. If failure persists, contact HP Support. |
| 0x00010312        | Evaluation license has expired.   | Warning: An evaluation license has expired. This occurs 60 days after installation of FMA if no permanent license has been installed. This message appears automatically every morning.                                                                     | Check license keys or purchase a permanent license.                                                                               |
| 0x00010315        | Licensed capacity exceeded        | Error: The licensed capacity for migrated files has been exceeded. The used capacity is checked at the beginning of each migration. If it exceeds the licensed capacity, migration fails.                                                                   | Delete unneeded files from the managed volumes or update the license key to migrate more capacity.                                |

| <b>Error Code</b> | <b>Error Text</b>                                                                       | <b>Description</b>                                                                                                                                                                                                | <b>Recommended Action</b>                                                                                                                          |
|-------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010316        | The HSM subsystem is busy and rejected the request.                                     | Error: An internal communication channel was busy and the file operation was rejected. A file processing request from the AFM policy service, the FMA command line utility, or the Explorer plug-in was rejected. | Wait and try again. If the error occurs often, contact HP Support.                                                                                 |
| 0x00010317        | Generic error connecting to hsm subsystem.                                              | Error: FMA was unable to make internal communication connections. A file processing request from the AFM policy service, the FMA command line utility, or the Explorer plug-in was rejected.                      | Retry the operation. If the problem persists, restart the FMA services or reboot the server. If this continues to be an issue, contact HP Support. |
| 0x00010318        | File cannot be activated due to a missing file object ID.                               | Warning: FMA metadata is found in the file, but no object ID for file exists. This occurs when there is a request to activate a file for FMA management.                                                          | The stub file is damaged and cannot be activated. It needs to be recovered from a disaster recovery archive.                                       |
| 0x00010350        | Overflow of the auto activation file cache. Increase 'Auto Activate List Size' setting. | Warning: An internal error has occurred during file auto-activation. This occurs when files are being automatically activated. The most common case is during a backup restore.                                   | Contact HP Support.                                                                                                                                |
| 0x00010401        | Duplicate archive name                                                                  | Error: An archive name is used more than once. This occurs when the user tries to create an archive with a name that already exists.                                                                              | Choose a new name for the archive.                                                                                                                 |
| 0x00010403        | Archive already exists                                                                  | Warning: Archive already exist. This occurs if the user tries to create an archive using the name of an existing archive.                                                                                         | Choose another name for the archive.                                                                                                               |
| 0x00010430        | Cleanup process is already active.                                                      | Warning: The cleanup process is active and cannot be started twice.                                                                                                                                               | Wait until the first process is finished.                                                                                                          |
| 0x00010432        | Garbage Collection: end of data reached                                                 | Informational: The end of garbage collection list was reached and all entries are completed.                                                                                                                      | None.                                                                                                                                              |

| <b>Error Code</b> | <b>Error Text</b>                                      | <b>Description</b>                                                                                                                                                                                                                                       | <b>Recommended Action</b>                                                                                                                                                                |
|-------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010433        | Garbage Collection: end of current logfile reached     | Informational: No entries exist in the current garbage collection file.                                                                                                                                                                                  | None.                                                                                                                                                                                    |
| 0x00010434        | An error occurred reading from garbage collection file | Error: The garbage collection file could not be read. This occurs during cleanup or when files are deleted or replaced in a managed volume.                                                                                                              | Restart FMA services and contact HP Support if the problem persists.                                                                                                                     |
| 0x00010435        | Storage descriptor data does not fit into buffer       | Error: The storage descriptor data does not fit into the processing buffer. This occurs during a cleanup operation and the file storage descriptor is too long to process.                                                                               | Restart FMA services and contact HP Support if the problem persists.                                                                                                                     |
| 0x00010436        | Garbage collection log is not in the expected format   | Error: An item in the garbage collection list is not in the expected format. This occurs during a cleanup operation and the file list entry cannot be determined.                                                                                        | FMA cleanup tries to resynchronize with the start of the next entry. Contact HP Support if the problem persists.                                                                         |
| 0x00010501        | Connection to configuration server failed              | Error: HSM service was unable to connect to the configuration service. This occurs during FMA startup when the hsmSvc waits for the configuration service to start or during initial cluster setup.                                                      | Check for errors to determine whether the configuration service is not running or failed. See the cluster configuration section for more information if the system is part of a cluster. |
| 0x00010502        | Remote-Request-Protocol violation                      | Error: An error in RRP protocol occurred. This can occur during internal message passing within FMA and the message received is not formatted correctly.                                                                                                 | Restart FMA services and contact HP Support if the problem persists.                                                                                                                     |
| 0x00010503        | Incompatible RRP protocol version                      | Error: An RRP message was received and its tagged protocol version does not match the receiving function's version. This can occur if internal FMA modules in the install directory are replaced with incompatible modules from another release version. | Check the FMA installation and perform a repair install if needed. If there is no reason for this to occur, contact HP Support.                                                          |

| <b>Error Code</b> | <b>Error Text</b>                              | <b>Description</b>                                                                                                                                                                                                                                                                                                | <b>Recommended Action</b>                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00010551        | Configuration server: unknown function         | Error: The FMA configuration service received a request that does not match an available operation. This can occur if internal FMA modules in the install directory are replaced with incompatible modules from another release version.                                                                          | Check the FMA installation and perform a repair install if needed. If there is no reason for this to occur, contact HP Support.                                                                                                                                                                                                                          |
| 0x00010552        | Configuration server: protocol violation error | Error: The configuration service received a request that cannot be processed due to lack of memory or a mismatch in the length of the request compared to what was expected. This can occur if internal FMA modules in the install directory are replaced with incompatible modules from another release version. | Check the FMA installation and perform a repair install if needed. If there is no reason for this to occur, contact HP Support.                                                                                                                                                                                                                          |
| 0x00020003        | An invalid archive entry was found             | Error: The system could not reference the contents of a given archive configuration.                                                                                                                                                                                                                              | Check archive configuration. Restart FMA services. Contact HP Support if the problem persists.                                                                                                                                                                                                                                                           |
| 0x00020004        | Unable to load RSA dynamic link library        | Error: FMA could not load a Remote Storage Adapter (RSA) dynamic link library (DLL) file. This occurs during FMA startup when installed RSA modules are discovered and loaded.                                                                                                                                    | The RSA DLL file may be damaged. Restart FMA services or reinstall FMA. Contact HP Support if the problem persists.                                                                                                                                                                                                                                      |
| 0x00020005        | Registry key for archive definitions not found | Error: The Archives registry key contains all archive definitions for FMA. If this error occurs, it is missing or not readable during FMA startup.                                                                                                                                                                | Restart FMA or reboot the server. Check registry values at HKLM\Software\Hewlett-Packard\HP FMA\Archives. Missing registry values can require reinstallation of FMA. If Archive definitions are recreated, they should be created in the same order as before to preserve IDs used.<br><br>Note: For IAP, the registry path is "Hewlett-Packard\HP FMA". |

| Error Code | Error Text                                         | Description                                                                                                                                                                                                                  | Recommended Action                                                                                                                                                                                                              |
|------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00020007 | Archive pool is empty                              | Warning: Activate archive error occurred. This occurs when system tries to activate the next archive in a sequence but the archive pool is empty.                                                                            | None.                                                                                                                                                                                                                           |
| 0x00020008 | Unable to write to registry                        | Error: FMA could not write to the Windows registry.                                                                                                                                                                          | Examine the log to find the reason of an error.                                                                                                                                                                                 |
| 0x0002000A | Maximum number of archives reached.                | Error: Maximum number of archives reached when a user tries to create an archive.                                                                                                                                            | Delete the unneeded archive(s).                                                                                                                                                                                                 |
| 0x0002000B | Archive name is invalid                            | Error: Archive name specified during creation was invalid.                                                                                                                                                                   | Check the archive name for the invalid character(s). See <a href="#">Archives</a> on page 25.                                                                                                                                   |
| 0x0002000D | Error contacting the configuration server service. | Error: FMA uses a configuration service to perform archive configuration operations such as create or delete archives. This error occurs when communication with this service is not successful. The service may be stopped. | Check the FMA configuration service status. If it is stopped, restart service or reboot the server. In a cluster environment, the configuration service is active on only one node. Contact HP Support if the problem persists. |
| 0x00030002 | Maximum number of volumes exceeded                 | Error: FMA can only see a maximum of 128 volumes. This occurs if a server has more than 128 volumes attached.                                                                                                                | Any volumes beyond this point cannot be seen by FMA and cannot be managed. Remove some or move some to another server.                                                                                                          |
| 0x00030003 | Volume not a fixed disk                            | Error: The volume was not recognized as a fixed disk. FMA can only manage fixed disk volumes. This occurs when FMA starts up and scans all attached volumes.                                                                 | If you believe the volume is type "fixed disk", it can be corrupt and cannot be recognized as a fixed disk. Run Windows check disk on it.                                                                                       |
| 0x00030004 | No message displayed                               | Error: A request to open the volume returned an invalid response. This occurs when the user tries to unmount a volume and the volume can not be opened.                                                                      | Restart FMA services or reboot the server. Contact HP Support if the problem persists.                                                                                                                                          |

| <b>Error Code</b> | <b>Error Text</b>                                                       | <b>Description</b>                                                                                                                                                                                         | <b>Recommended Action</b>                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00030007        | The volume manager process was started, but failed.                     | Error: The volume manager process was started but then stopped immediately. This can occur during FMA startup or HsmSvc service startup.                                                                   | Restart FMA services or reboot the server. Set management status for needed volumes. The FMA installation can be corrupt. Try to reinstall FMA. Contact HP Support if the problem persists. |
| 0x00030008        | The volume cannot be managed, maximum number of managed volumes reached | Error: FMA can only manage a maximum of 80 volumes. This occurs if a user tries to add more than 80 volumes to FMA management.                                                                             | Some volumes must be removed from management or moved to another server.                                                                                                                    |
| 0x00040001        | Target file cannot be opened                                            | Error: The file in the Archive Storage System cannot be opened. This error is produced by the FmaFileUtil application if it cannot open the file.                                                          | Check that the file exists or that you have the proper access rights.                                                                                                                       |
| 0x00040006        | Invalid access mode                                                     | Error: An Archive Storage System open request of an unrecognized type occurred. This error is produced by the FmaFileUtil application if it tries to open the file and it does not use read or write mode. | Contact HP Support.                                                                                                                                                                         |
| 0x00040007        | Shadow device cannot be opened                                          | Error: An Archive Storage System open request using the shadow device mode failed. This error is produced by the FmaFileUtil application if it tries to open the file using the shadow device option.      | Contact HP Support.                                                                                                                                                                         |
| 0x00040008        | Wrong number of bytes read                                              | Error: An Archive Storage System read request returned the wrong number of bytes. This error is produced by the FmaFileUtil application if it tries to read data and gets too many or too few bytes.       | Contact HP Support.                                                                                                                                                                         |

| <b>Error Code</b> | <b>Error Text</b>                                                  | <b>Description</b>                                                                                                                                                                                                                                                        | <b>Recommended Action</b>                                                                                                                                          |
|-------------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x0004000A        | Wrong number of bytes written                                      | Error: An Archive Storage System write request returned the wrong number of bytes written confirmation. This error is produced by the FmaFileUtil application if it tries to write data and the return confirmation does not match the request.                           | Contact HP Support.                                                                                                                                                |
| 0x0004000B        | Data is corrupt                                                    | Error: An Archive Storage System write or read request did not pass validation checks. The data may be corrupt. This error is produced by the FmaFileUtil application if it tries to write or read data and the operation validation did not pass.                        | Contact HP Support.                                                                                                                                                |
| 0x00050002        | Metadata was not found                                             | Error: There is no FMA metadata attached to the file. This occurs during recall and other metadata operations where an unmigrated file may be selected.                                                                                                                   | The file must be migrated before it contains FMA metadata.                                                                                                         |
| 0x00050003        | Version of HSM metadata is not supported.                          | Error: FMA automatically upgrades the metadata from older versions to the current version. In rare cases, the old version can be too old to support. This becomes an issue if legacy stub files are restored from a backup set or imported into a current managed volume. | Stub files with unsupported metadata cannot be recalled. Metadata can be deleted from managed online files. Most legacy metadata is supported. Contact HP Support. |
| 0x00050004        | Outdated HSM metadata format was detected. Conversion is required. | Error: Outdated FMA metadata format was detected and the current operation cannot be completed. The attached metadata must be updated to the current version. This error occurs during typical file management operations like recall and migrate.                        | This error is typically reported using code 0x00010010 (File is outdated). See that code for more information.                                                     |

| <b>Error Code</b> | <b>Error Text</b>                    | <b>Description</b>                                                                                                                                                                                                                                                               | <b>Recommended Action</b>                                                                                                                                                                   |
|-------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00050101        | File ID does not match with metadata | Error: The FMA metadata contains a copy of the file ID. If a file is restored from backup or copied into a managed volume, the system file ID may no longer match the ID in the metadata. This error occurs when a user tried to recall or migrate the file.                     | The file must be activated in order to resynchronize the file ID. Files are normally auto-activated when restored by a support backup application. See <a href="#">activate</a> on page 83. |
| 0x00050102        | Metadata is corrupt (CRC error)      | Error: The system checks the metadata prior to typical commands like migrate, release, and recall. The metadata did not pass a CRC check and is assumed to be corrupt and not usable.                                                                                            | The metadata must be erased from this file. See the <code>fmacli erase</code> command. If the file is a stub file, it must be restored from a disaster recovery backup.                     |
| 0x00050103        | Record not found in metadata         | Error: The system checks the metadata prior to typical commands like migrate, release, and recall. This error indicates that information can not be read from the metadata.                                                                                                      | The metadata must be erased from this file. See the <code>fmacli erase</code> command. If the file is a stub file, it must be restored from a disaster recovery backup.                     |
| 0x00050201        | Verify: metadata size differs.       | Error: The system compares the primary and secondary copies of the metadata as part of the activate and verify commands. The size of the primary copy of the metadata does not match the secondary copy. FMA keeps a secondary copy of the metadata in an Extended Attribute.    | The metadata must be erased from this file. See the <code>fmacli erase</code> command. If the file is a stub file, it must be restored from a disaster recovery backup.                     |
| 0x00050202        | Verify: metadata differs             | Error: The system compares the primary and secondary copies of the metadata as part of the activate and verify commands. The content of the primary copy of the metadata does not match the secondary copy. FMA keeps a secondary copy of the metadata in an Extended Attribute. | The metadata must be erased from this file. See the <code>fmacli erase</code> command. If the file is a stub file, it must be restored from a disaster recovery backup.                     |

| <b>Error Code</b> | <b>Error Text</b>                           | <b>Description</b>                                                                                                                                                                                                                                               | <b>Recommended Action</b>                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00050203        | Verify: primary metadata not found          | Error: The system compares the primary and secondary copies of the metadata as part of the activate and verify commands. The content of the primary copy of the metadata can not be read. FMA keeps a secondary copy of the metadata in an Extended Attribute.   | The metadata must be erased from this file. See the fmacli erase command. If the file is a stub file, it must be restored from a disaster recovery backup.                                                                                                                                                           |
| 0x00050204        | Verify: alternate metadata not found.       | Error: The system compares the primary and secondary copies of the metadata as part of the activate and verify commands. The content of the secondary copy of the metadata can not be read. FMA keeps a secondary copy of the metadata in an Extended Attribute. | The metadata must be erased from this file. See the fmacli erase command. If the file is a stub file, it must be restored from a disaster recovery backup.                                                                                                                                                           |
| 0x00050205        | Verify: Metadata not found.                 | Warning: The system read nothing from the primary and secondary copies of the metadata as part of the activate and verify commands. This file is not managed by FMA.                                                                                             | Metadata is added to the file if and when it is migrated.                                                                                                                                                                                                                                                            |
| 0x00060001        | RSA specific error.                         | Error: The Remote Storage Adapter interface reported an error. This can occur during most operations that require reading or writing to the remote archive.                                                                                                      | Examine the FMA logs around the time of this error. Contact HP Support if the issue cannot be resolved.                                                                                                                                                                                                              |
| 0x00060002        | Unable to connect to archive storage system | Error: The system can not connect to the selected remote archive system. This can occur during most operations that require reading or writing to the remote archive.                                                                                            | Check archive settings in the RSA configuration. Verify that the archive hostname or IP address is correct and that the remote system is online and available for browsing. Any change to the RSA configuration settings after its initial creation does not take effect until after the FMA services are restarted. |

| <b>Error Code</b> | <b>Error Text</b>                                                                    | <b>Description</b>                                                                                                                                                                                                                                | <b>Recommended Action</b>                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00060003        | Authentication at storage archive storage system failed. Check supported credentials | Error: The system can connect to the remote archive system, but the designated user did not have sufficient credentials to read from or write to it. This can occur during most operations that require reading or writing to the remote archive. | Check archive settings in the RSA configuration. Check that the archive user's credentials are set correctly locally and in the remote archive system. For CIFS archives, the FMA technical user needs to have full control privileges in the remote archive system. Any change to the RSA configuration settings after its initial creation does not take effect until after the FMA services are restarted. |
| 0x00060004        | File cannot be stored in archive system.                                             | Error: The file can not be written to the archive system during migration because it is out of storage space.                                                                                                                                     | Check archive for capacity availability.                                                                                                                                                                                                                                                                                                                                                                      |
| 0x00060005        | Configuration dialog cancelled                                                       | Warning: The RSA configuration dialog was cancelled by the user.                                                                                                                                                                                  | None.                                                                                                                                                                                                                                                                                                                                                                                                         |
| 0x00060006        | Configuration dialog error                                                           | Error: An unexpected error in RSA configuration occurred.                                                                                                                                                                                         | Try the operation again. Try to restart the FMA services or reboot the server. Contact HP Support if the problem persists.                                                                                                                                                                                                                                                                                    |
| 0x00060008        | No message displayed                                                                 | Warning: An alternate location for a given archive was not defined. This can occur during recalls if the secondary archive is omitted and the primary is not accessible.                                                                          | This is not an error if the secondary path to the archive is left blank on purpose. If not, check the secondary archive configuration and if it is online.                                                                                                                                                                                                                                                    |
| 0x00060009        | The archive does not support the requested function.                                 | Error: There are some advanced functions that are not supported by the remote archive system. These are typically not invoked by FMA. This error can occur during archive management.                                                             | If this issue is seen frequently, contact HP Support.                                                                                                                                                                                                                                                                                                                                                         |
| 0x00060010        | No message displayed                                                                 | Error: A retry of a previous command was requested.                                                                                                                                                                                               | None.                                                                                                                                                                                                                                                                                                                                                                                                         |

| <b>Error Code</b> | <b>Error Text</b>                                   | <b>Description</b>                                                                                                                                                                          | <b>Recommended Action</b>                                                                                                                                                                                                                              |
|-------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00060102        | Verification failed (file size)                     | Error: During fmacli verify or activate commands, some portions of the operation are RSA specific. This error occurs if the managed file has a different size from the copy in the archive. | If the managed file is currently a stub file, it must be repaired using the fmacli verify command. If it is not a stub file, analyze why the file sizes are different and whether the local copy or archive copy is the correct file.                  |
| 0x00060103        | Verification failed (file does not exist)           | Error: The file does not exist in the archive. This occurs during a recall or verify operation.                                                                                             | Check for file existence in the archive. If the local file is a stub file and the archive copy is missing, it must be restored from a disaster recovery backup. If the local file is not a stub file, it can be remigrated after erasing the metadata. |
| 0x00060121        | Stream format error                                 | Error: An unlikely internal error occurred relating to the data stream type during an archive write operation.                                                                              | If this issue is seen frequently, contact HP Support.                                                                                                                                                                                                  |
| 0x00060123        | Stream write failed                                 | Error: The number of bytes written to the archive does not match the expected bytes to write. This can occur during a file migration to an archive.                                         | Retry the operation. If the error persists, contact HP Support.                                                                                                                                                                                        |
| 0x00060124        | Unknown storage descriptor                          | Warning: A file to be removed from the archive can not be found in the archive. This can occur during the fmacli cleanup operation.                                                         | None.                                                                                                                                                                                                                                                  |
| 0x00060125        | Remote storage adapter does not match with metadata | Error: During an fmacli activate or verify operation, it was determined that the local copy of the metadata references an RSA type that is different from the RSA being addressed.          | This should not occur unless RSA configurations were changed without using the FMA configuration UI or the file was restored from a different managed volume from another server. FMA does not support restoring files to an alternate location.       |
| 0x00060126        | The archive status file is corrupt                  | Error: The system attempted to check the archive status but the archive status file is corrupted.                                                                                           | Check archive settings or restart FMA.                                                                                                                                                                                                                 |

| <b>Error Code</b> | <b>Error Text</b>                                 | <b>Description</b>                                                                                                                                                                                                               | <b>Recommended Action</b>                                                                                                                                                                        |
|-------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00060129        | Archive is inactive due to invalid configuration. | Error: During system startup, the archive configuration list is scanned and if an archive has an invalid name or IP address, it is marked as invalid. This error occurs when a file's metadata references one of these archives. | Check the archive configuration. If the archive path looks correct, restart the system and check again. If the problem persists, contact HP Support.                                             |
| 0x00060130        | No message displayed                              | Error: The managed file's metadata that is stored in the archive cannot be read. This can occur during a recall or verify operation. A verify operation attempts to fix the metadata in the archive.                             | Analyze the archive system and FMA logs regarding activity with this file. It may need to be migrated again to refresh the metadata in the archive. If the problem persists, contact HP Support. |
| 0x00060131        | No message displayed                              | Error: The managed file's metadata that is stored in the archive does not exist. This can occur during a recall or verify operation. A verify operation attempts to fix the metadata in the archive.                             | Analyze the archive system and FMA logs regarding activity with this file. It may need to be migrated again to refresh the metadata in the archive. If the problem persists, contact HP Support. |
| 0x00060132        | No message displayed                              | Error: An internal software error has occurred when trying to read the file's metadata in the archive during a recall or verify operation.                                                                                       | Retry the operation or restart the FMA services. If the error persists, contact HP Support.                                                                                                      |
| 0x00070002        | Ftp: access denied                                | Error: File access was denied in the FTP archive during a file create or open request.                                                                                                                                           | Check that the FTP user has been given the proper credentials in the FTP archive.                                                                                                                |
| 0x00070003        | Ftp: connection failed                            | Error: The configured FTP archive was not responding to a connect request. This can occur when FMA tries to connect or reconnect to the FTP archive.                                                                             | Check that the FTP archive is available and that the RSA FTP hostname configuration is correct in FMA.                                                                                           |
| 0x00070005        | Ftp: invalid archive file name                    | Error: The file name is invalid because it is formatted illegally. This occurs when the system tries to create a new file in the FTP archive.                                                                                    | Check the format of the file you are trying to migrate.                                                                                                                                          |

| <b>Error Code</b> | <b>Error Text</b>                           | <b>Description</b>                                                                                                                                                                                                                           | <b>Recommended Action</b>                                                                                                     |
|-------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 0x00070006        | Ftp: error modifying date                   | Error: Unable to read the date of the remote file. This occurs when the system tries to read the date of the file in the FTP archive.                                                                                                        | Check the configuration of the FTP archive.                                                                                   |
| 0x00070007        | Ftp: error size                             | Error: Unable to read the size of the remote file. This occurs when the system tries to read the size of the file in the FTP archive.                                                                                                        | Check the configuration of the FTP archive.                                                                                   |
| 0x00070008        | Ftp: invalid storage descriptor header size | Error: The Storage Descriptor header size is incorrect. This is an internal check during FTP operations that is not affected by external conditions.                                                                                         | Contact HP Support.                                                                                                           |
| 0x00070009        | Ftp: error creating path                    | Error: FMA can not create a directory in the archive. When a file is migrated, the local directory structure is mirrored in the archive and the hostname and volume ID of the managed machine can be set as part of the path in the archive. | Check the privileges of the defined FTP user in the archive and confirm that the FTP server is online.                        |
| 0x0007000B        | Ftp: server not supported                   | Error: FMA tested interoperability with only certain versions of FTP servers. This error occurs when FMA is configured to connect to an unsupported FTP server.                                                                              | Check the Release Notes for a current list of supported FTP servers.                                                          |
| 0x0007000C        | Ftp: wrong file size                        | Error: After a file is recalled or migrated to an FTP archive, the number of bytes read or written is compared to the reported size from the FTP server. This error indicates that the values do not match.                                  | Retry the operation. If the error persists, contact HP Support.                                                               |
| 0x0007000E        | FTP: write failure                          | Error: Preparation for or migration of a file to the FTP archive has failed.                                                                                                                                                                 | Retry the operation and check the stability of the FTP server and network connections between the FMA server and the archive. |

| <b>Error Code</b> | <b>Error Text</b>          | <b>Description</b>                                                                                                                                                                                       | <b>Recommended Action</b>                                                                                                                  |
|-------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 0x0007000F        | FTP: read failure          | Error: Preparation for or recall of a file from the FTP archive has failed.                                                                                                                              | Retry the operation and check the stability of the FTP server and network connections between the FMA server and the archive.              |
| 0x00070010        | Ftp: authentication failed | Error: While establishing a connection with the FTP server, the server returned an authentication error response. This occurs when FMA tries to establish a connection to the FTP server for any reason. | Check the FTP user settings in FMA and the FTP server. They should be identical.                                                           |
| 0x00070011        | No message displayed       | Error: FMA can not delete a file from the archive. This occurs when FMA attempts garbage collection cleanup in the archive.                                                                              | Ensure that the FTP user has file delete privileges in the archive.                                                                        |
| 0x00070012        | No message displayed       | Error: FMA can not delete a directory from the archive. This occurs when FMA attempts garbage collection cleanup in the archive.                                                                         | Ensure that the FTP user has directory delete privileges in the archive.                                                                   |
| 0x00070013        | No message displayed       | Warning: FMA can not convert a file or directory name in wide character format to a name in multi-byte format. This occurs when the system tries to convert the encoding of a file name.                 | Check the feasibility of converting the file names that do fail.                                                                           |
| 0x00070015        | No message displayed       | Error: FMA was unable to close a connection to the FTP server. This occurs when the system tries to close the FTP connection during a recall or migration.                                               | The connection can be closed by the FTP server due to a timeout or other condition. Check the stability of the network and the FTP server. |
| 0x000A0001        | No message displayed       | Error: This error is related to reading the RSA-IAP configuration settings from the registry. This occurs during system startup when the RSA-IAP configuration settings are processed.                   | Restart the system. Contact HP Support if the problem persists.                                                                            |

| <b>Error Code</b> | <b>Error Text</b>                                                             | <b>Description</b>                                                                                                                                                                                                                                                                 | <b>Recommended Action</b>                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x000A0002        | File not migrated because file size exceeds IAP limit of 1,579,024,383 bytes. | Error: The HP IAP archive has a maximum file size limitation of 1,579,024,383 bytes. This occurs if the system tries to migrate a file that is larger than the maximum allowed size.                                                                                               | Files larger than the limit cannot be managed using an IAP archive.                                                                                                                                                                   |
| 0x00090001        | Not enough memory to allocate buffer.                                         | Error: The FMA file system filter can not allocate memory for a given task.                                                                                                                                                                                                        | Check the available memory in the server. Reduce the memory usage or add more memory.                                                                                                                                                 |
| 0x00090002        | Parameter not a valid file.                                                   | Error: The FMA file system filter can not access the file based on the provided file handle.                                                                                                                                                                                       | The issue may not be an error if the file was deleted by another process or it is not accessible because it is already open.                                                                                                          |
| 0x00090003        | No such volume exists.                                                        | Error: The FMA file system filter can not find the referenced volume based on its unique ID (GUID). This occurs when an attempt to add a volume to FMA management was made using an invalid volume ID or initial file information access was attempted using an invalid volume ID. | Retry the operation. Check if there have been recent additions or deletions of volumes. In a cluster, volumes that failover to another node become unavailable on the current node, which can result in filter errors of this nature. |
| 0x00090004        | Wrong volume was specified.                                                   | Error: The volume ID format did not match the standard notation: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". This can occur when a volume is added or removed from FMA management.                                                                                                     | Restart the system. If the problem persists, contact HP Support.                                                                                                                                                                      |
| 0x00090005        | File System Filter Driver not loaded                                          | Error: The FMA file system filter driver was not loaded. This error occurs when any request to the driver is not loaded on a managed volume.                                                                                                                                       | Restart the system or try to remove and add the volume to FMA management again. If the problem persists, contact HP Support.                                                                                                          |
| 0x00090006        | Client is not allowed to connect.                                             | Error: The FMA file system driver refused the event.                                                                                                                                                                                                                               | Contact HP Support.                                                                                                                                                                                                                   |
| 0x00090007        | Client already registered with filter.                                        | Error: Some FMA components register with the file system filter driver. A given component can only register once.                                                                                                                                                                  | Contact HP Support.                                                                                                                                                                                                                   |

| <b>Error Code</b> | <b>Error Text</b>              | <b>Description</b>                                                                                                                                                                                                                                                                              | <b>Recommended Action</b>                                                                                                                                                                                                          |
|-------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x00090008        | Error accessing registry       | Error: The FMA filter driver components can not access the system registry when a volume was added or removed from FMA management.                                                                                                                                                              | Restart the system or try to remove and add the volume to FMA management again. If the problem persists, contact HP Support.                                                                                                       |
| 0x00090009        | Error accessing attributes.    | Error: A file system filter component can not access a file's attributes because the file's offline attribute was changed when the file was released or recalled.                                                                                                                               | Normally, the file is set to the state it was in prior to the operationally a file's offline attribute ends up in the wrong state, the "fmacli verify --repair" command can fix it. If this occurs frequently, contact HP Support. |
| 0x0009000A        | Error accessing Reparse Point. | Error: A reparse point is a tag that notifies the file system that the file contents cannot be accessed until another process is called first. This error indicates that the reparse point can not be read because a file's offline attribute is managed or other file information was queried. | Retry the operation. If the problem persists, contact HP Support.                                                                                                                                                                  |
| 0x0009000B        | Error setting sparse file.     | Error: When FMA creates a stub file, its contents are converted to a zero filled sparse file. This error indicates that this process has failed while setting the file offline after a release.                                                                                                 | Normally, the file is set to the state it was in prior to the operation. Retry the operation. If the problem persists, contact HP Support.                                                                                         |
| 0x0009000C        | Error writing zeros            | Error: When FMA creates a stub file, its contents are converted to a zero filled sparse file. This error indicates that part of this process has failed while setting the file offline after a release.                                                                                         | Normally, the file is set to the state it was in prior to the operation. Retry the operation. If the problem persists, contact HP Support.                                                                                         |
| 0x0009000D        | No connection with filter      | Error: The connection to the file system filter driver was lost during an FMA file management operation.                                                                                                                                                                                        | Restart the system or try to remove and add the volume to FMA management again. If the problem persists, contact HP Support.                                                                                                       |

| <b>Error Code</b> | <b>Error Text</b>                              | <b>Description</b>                                                                                                                                                                                                                                                                                    | <b>Recommended Action</b>                                                                                                                                        |
|-------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x0009000E        | Error writing data                             | Error: During a recall, the FMA filter driver can not write the file contents to the local managed file system.                                                                                                                                                                                       | Ensure the file system is not full and that no other application has the target file open. Retry the operation. If the problem persists, contact HP Support.     |
| 0x0009000F        | Error occurred while waiting for filter event. | Error: The system was waiting for the next event from the filter driver when a “wait abandoned” or “wait error” response was received.                                                                                                                                                                | Restart the system if this issue is occurring frequently. If the problem persists, contact HP Support.                                                           |
| 0x00090010        | Failed to create event handle.                 | Error: The FMA system creates objects call events that pass information to and from the filter driver. In this case, a new event can not be created.                                                                                                                                                  | Check that the server is not overloaded or out of memory. Restart the system if this issue is occurring frequently. If the problem persists, contact HP Support. |
| 0x00090011        | Connection port with filter is closed.         | Error: The FMA file system filter driver was unloaded unexpectedly. In a cluster environment, this can occur if there are active FMA events while the managed volume is failing over to another node. It is also possible that the filter encountered an unrecoverable error and was forced to close. | If there is not an obvious cause, restart the system or try to remove and add the volume to FMA management again. If the problem persists, contact HP Support.   |
| 0x00090013        | Unknown error occurred                         | Error: An unexpected return code was returned from the file system filter.                                                                                                                                                                                                                            | Contact HP Support for analysis.                                                                                                                                 |



# Index

---

## A

- accessing FMA Explorer plugin 3
- accessing FMA user interface 3
- activate command 83
- activating managed files 83
- Active/Active 15
- Active/Passive 14
- archive command 86
- archives
  - backing up 6
  - cleaning up 88
  - configuring
    - CIFS 29
    - FTP 35
    - RISS 40
  - creating
    - CIFS 28
    - FTP 31
    - RISS 39
  - deleting 44
  - editing 43
  - listing 86
  - overview 25
  - preparing
    - CIFS 28
    - Linux-based FTP 31
    - RISS 40
  - removing deleted files 44
  - types 25
  - viewing 27
- audience vii
- Auto Activate Delay 132
- Auto Activate List Size 131

## B

- backing up
  - archives 6
  - managed volumes 6
- backup management applications, configuring 6

## C

- CIFS archives
  - configuring for FMA 29
  - creating 28
  - data stored 28
  - preparing for FMA 28

- cleaning up archives
  - overview 44
  - syntax 88
- cleanup command
  - overview 44
  - syntax 88
- Cluster Administrator 15
- clusters
  - installing FMA 14
  - uninstalling FMA 20
  - updating FMA 18
- commands
  - activate 83
  - archive 86
  - cleanup 88
  - erase 89
  - info 92
  - migrate 97
  - policy 101
  - recall 103
  - release 106
  - rsa 110
  - system 112
  - verify 114
  - version 117
  - volume 119
- configuring
  - CIFS archives for FMA 29
  - FTP archives for FMA 35
  - RISS archives for FMA 40
  - VSFTPD
    - on Red Hat 33
    - on SuSE Linux 32
- Copies 56
- creating
  - CIFS archives 28
  - FTP archives 31
  - managed volumes 47
  - RISS archives 39
  - technical user account 5
- critical watermark 48

## D

- deactivating managed files 83
- deleting
  - archives 44
  - file policies 55
  - FMA metadata 89
- disabling file policies 55
- disk space policies 48
  - excluding files 50
  - setting
    - retention periods 49
    - watermarks 48
- documentation library viii

## E

- editing
  - archives 43
  - file policies 55
- enabling file policies 55
- erase command 89
- excluding files from disk space policies 50
- Explorer plugin
  - accessing 3
  - migrating files 57
  - overview 3
  - recalling 58
  - registering 20
  - releasing files 57

## F

- Failover 144
- file policies
  - about 51
  - deleting 55
  - disabling 55
  - editing 55
  - enabling 55
  - running
    - manually 54
    - on a schedule 54
  - scheduling 54
- File Properties 56

## FMA

- command line interface *See FMACLI*
  - Explorer plugin
    - accessing 3
  - log
    - about 124
    - accessing in user interface 124
    - setting
      - logging level 124
      - number of files 125
  - metadata, viewing 92
  - overview 1
  - user interface
    - accessing 3
    - overview 3
- FMA column properties 56

## FMACLI

- commands 81
- log 125
- overview 3
- result codes 121
- syntax 81

## FmaFileUtil

- commands 37
- options 37
- overview 4
- syntax 37

## FTP archives

- accessing files 37
- configuring for FMA 35
- creating 31
- data stored 31
- preparing Linux-based for FMA 31

## H

- high watermark 48
- HP
  - Subscriber's choice web site viii

## I

- info command 92
- installation folder 9
- installing
  - FMA
    - in cluster 14
    - on file servers 9
  - overview 5
  - steps 5

## L

- Last recall 56
- licensing 21
- logs
  - FMA log 124
  - FMACLI log 125
  - Windows event log 126
- low watermark 48

## M

- managed files
  - activating 83
  - contents 45
  - deactivating 83
  - deleting FMA metadata 89
  - moving 58
- managed volumes
  - backing up 6
  - creating 47
  - overview 45
  - removing management 60
  - restarting management 60
  - starting management 60
  - status 46
  - stopping management 59
  - viewing 45
  - viewing list 119
- migrate command 97
- migrating
  - overview 2
  - using
    - file policies 51
    - migrate command 97
    - the Explorer plugin 57
    - watermarks 48
- moving managed files 58

## P

- policy command 101
- preparing
  - CIFS archives for FMA 28
  - Linux-based FTP archives for FMA 31
  - RISS archives for FMA 40
- primary archive 25

## R

- recall command 103
- recalling
  - overview 2
  - using recall command 103
  - using the Explorer plugin 58
- Recalls 56
- registering the Explorer plugin 20
- release command 106
- Release Notes viii
- releasing
  - overview 2
  - using disk space policies 48
  - using file policies 51
  - using migrate command 97
  - using release command 106
  - using the Explorer plugin 57
  - using watermarks 48
- removing
  - deleted files from archives 44
  - volume management 60
- Restoration 144
- restoring backed up data 7
- result codes for FMACLI 121
- RISS archives
  - configuring for FMA 40
  - creating 39
  - data stored 39
  - preparing for FMA 40
- RSA
  - overview 25
  - viewing status 110
- rsa command 110
- running file policies 54

## S

- scheduling file policies 54
- secondary archive 25
- secondary RISS, enabling 40
- starting volume management 60
- State 56
- stopping volume management 59
- storage descriptor
  - overview 25
  - structure 25

- Subscriber's choice, HP viii
- support viii
- syntax for FmaFileUtil 37
- system command 112

## **T**

- technical support viii
- technical user account
  - creating 5
  - overview 5
- typographical conventions viii

## **U**

- uninstalling FMA
  - in cluster 20
  - on file servers 20
- updating FMA
  - in cluster 18
  - on file servers 18

## **V**

- verify command 114
- version command 117
- viewing
  - archives 27
  - FMA metadata 92
  - FMA version information 117
  - managed volume information 119
  - managed volumes 45
  - system information 112
- volume command 119
- VSFTPD, configuring
  - on Red Hat 33
  - on SuSE Linux 32

## **W**

- watermarks, setting for disk space use 48
- web sites
  - HP Subscriber's choice viii
- Windows event log
  - about 126
  - setting logging level 126



