

Release Notes

HP Software File Migration Agent (FMA[®])

Product Version: 2.5
Software release date: September 2009
Document release date: February 2010
second edition



© 2004—2010 Hewlett-Packard
All rights reserved

No part of this document may be copied in any form or by any means without prior written consent of HP.

All drawings, schematics and artwork used in the manufacture of the products described herein are copyrighted. Reproduction of said drawings, schematics and artwork or manufacture of said products without written consent of HP is absolutely prohibited.

Contents

- Introduction 1**
 - Related documentation 1
 - Technical Support 1

- Installation and Configuration 2**
 - Installation 2
 - Upgrades 2
 - System requirements 2
 - Hardware platforms 2
 - Operating systems 3
 - User interface and Explorer plug-in 3
 - File systems 3
 - Archive devices 4
 - FMA size limitations 4
 - End of Life feature 5
 - Tested third-party software 5
 - Backup management software 5
 - Virtualization software 5
 - Antivirus software 6
 - Defragmentation software 6
 - Multipathing software 6
 - Quota management software 7
 - Mirroring software 7

- Resolved Issues and Enhancements 8**

- Known Issues 12**

- Troubleshooting 14**

- Issue Index 16**

Introduction

These release notes apply to HP Software File Migration Agent (FMA[®]), version 2.5. This section describes how to use this document, related documentation, and technical support information.

Throughout this document, the issue tracking number is designated by a number in parentheses. Refer to this number if making inquiries to Technical Support. Note that the issue tracking number is merely a unique identifier, not a counter.

Related documentation

For more information about FMA, refer to the *File Migration Agent Installation and Administration Guide*. This guide provides the deployment team with information about installation, configuration, administration, and use of FMA.

Technical Support

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

- For 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.

Installation and Configuration

This section describes how to access information about installing and configuring HP Software File Migration Agent (FMA) 2.5. It also provides system requirements and tested applications.

Installation

For complete information about installing and configuring FMA, refer to the *File Migration Agent Installation and Administration Guide*.

Upgrades

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.

For complete information about upgrading FMA, refer to the *File Migration Agent Installation and Administration Guide*.

System requirements

This section lists hardware platforms and operating systems supported for managed file servers and supported archive devices.

Hardware platforms

The following table lists system requirements for the supported 32 and 64-bit systems:

System	System Requirements	
	Minimum	Recommended
32-bit	<ul style="list-style-type: none">• Intel® Xeon® 3.60 GHz 32-bit processor (or) AMD Athlon™ 1000 32-bit processor• 1GB of Total RAM• At least 10% free hard drive disk space	<ul style="list-style-type: none">• Dual Core Intel Xeon 5000 sequence 32-bit processor (or) AMD-K6® 2E+ series 32-bit processor• 4GB of Total RAM• At least 10% free hard drive disk space
64-bit	<ul style="list-style-type: none">• Intel Xeon processor 5000 sequence (or) AMD-Athlon 64 processors• 1GB of Total RAM• At least 10% free hard drive disk space	<ul style="list-style-type: none">• Dual-Core Intel Xeon 5140 2.33 GHz 64-bit Processor (or) AMD Opteron™ model 2214 HE 2.2 GHz — 2MB L2 dual-core — 64-bit processor• 4GB of Total RAM• At least 10% free hard drive disk space

Operating systems

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
- 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.
 - 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.
- HP Windows Unified Data Storage Server (WUDSS) 2003 32-bit only

User interface and Explorer plug-in

The FMA user interface requires Microsoft Management Console (MMC) 3.0. If you must update MMC on your system, the update is available from the following location:

<http://support.microsoft.com/kb/907265>

FMA does not support the 64-bit version of Server Manager or Computer Management. The FMA user interface is not integrated into the Microsoft Management Console and the Explorer plug-in is not available. To configure FMA on this operating system, select **Start→All Programs→HP StorageWorks File Migration Agent→FMA Configuration**. You can also create a 32-bit instance of the Microsoft Management Console (MMC) and add the FMA configuration snap-in. Finally, Explorer functionality is available by running the 32-bit version of Windows Explorer, which is provided with 64-bit Windows.

Also, for Server 2008, Microsoft has removed the Windows Explorer column management utility that allowed FMA to create new columns for the file detail view. The information presented in the FMA columns is now presented on the FMA File Properties tab. (Right-click a file and select Properties, and then click the FMA tab.) In addition, to be uniform across platforms, the column feature has also been removed from Server 2003 systems.

File systems

FMA supports managed files on Windows NTFS file systems. FMA can only manage locally attached NTFS volumes. Volumes mapped on the file server cannot be managed by FMA.

Local FMA-managed NTFS drives can be shared using CIFS protocol for Windows clients and NFS for non-Windows clients. Sharing non-Windows CIFS clients is not supported. FMA cannot manage remote file systems, such as CIFS shares or NFS mounts. FMA only supports NFS with Microsoft NFS server. In addition, FMA does not support Single Instance Storage service (SIS).

FMA supports the Microsoft Volume Shadow Copy Service (VSS) on volumes managed by FMA. VSS allows taking manual or automatic backup copies (or “snapshots”) of a volume at specific points in time. Volume snapshots can be taken on FMA managed volumes; there is no negative interference between VSS and FMA. Taking volume shadow copies will not initiate recalls of already released files.

When using VSS and FMA, the following restrictions should be considered:

- VSS shadow copies are read only and it is not possible for FMA to recall a file using a stub file in a shadow copy. Users are encouraged to consider this limitation when deploying both VSS and FMA. A file can only be recalled to a stub file if the entire volume is reverted to the snapshot. This will of course remove all file changes and new files that occurred after the time the snapshot was taken. There are no restrictions to copying managed online and unmanaged files from shadow copies.
- Windows provides the “Shadow Copies of Shared Folders” feature, which enables a VSS client to restore a file from a shadow copy on a remote file share. Because shadow copies are read-only, FMA cannot recall a file using a stub file in a shadow copy of a shared folder. There are no restrictions to copying managed online and unmanaged files from shadow copies.
- FMA applies metadata to files in order to reference the archive where the file was migrated. After a file is released, the file contents reside only in the archive(s). Thus, if a file is modified, migrated, and garbage collected over a period of time while snapshots are taken, older snapshot versions of the stub file may reference archived files that no longer exist. Be sure to establish a garbage collection expiration period that is longer than the age of the oldest retained snapshot.
- FMA does not support file activation for files that have been restored to a new location. Restoring files from a snapshot is only supported to their original location.
- Viewing previous versions of files that were offline during the volume snapshot is not supported.
- There are no restrictions for copying or viewing of online unmanaged files.

FMA also supports VSS when used by a qualified backup application. In this scenario, the snapshot may contain stub files which are then backed up by the backup application as a stub file. See the Backing up Managed Volumes and Restoring Data sections of the *Administration Guide*.

FMA is compatible with Microsoft Distributed File System (DFS) under the following restrictions.

- DFS Replication (one-way or two-way) is not supported by FMA.
- The DFS private directory (DfsrPrivate) must be excluded from FMA management. Add the path to hidden system directory DfsrPrivate to the Exclusion section of the Filtering tab in the FMA migration policy. If DFS-R is not installed, the directory is not present.

Archive devices

The following devices are supported for FMA archives:

- Any CIFS-based NAS appliance that runs on one of the supported hardware platforms and operating systems
- Any FTP server with SuSE Linux or Red Hat that uses the Very Secure FTP Daemon (VSFTPD)

FMA size limitations

The following are the maximum limitations supported for a single FMA server or a cluster configuration:

Description	Limit
Maximum number of volumes (display)	128
Maximum number of FMA-managed volumes	80
Maximum number of archives	255
Maximum path length (characters)	1024
Maximum file size (NTFS)	16TB

Description	Limit
Maximum volume size (NTFS)	256TB
Files/Directories per volume (NTFS)	4,294,967,295
Maximum number of migration policies	Unlimited (fewer than 1000 active policies recommended)
Maximum number of nodes per cluster	8 homogeneous nodes per cluster configuration

End of Life feature

File Migration Agent version 2.5 no longer includes the Job Manager feature. This feature was replaced by the FMA file policies and scheduling features. For configuration of these features, please refer to the *HP Software File Migration Agent Installation and Administration Guide*.

Tested third-party software

The following third-party software was tested with FMA.

Backup management software

The following backup management software is supported with FMA:

- BakBone NetVault 7.1.1, 8.1
- CA ArcServe Backup 11.5, 12
- CommVault Galaxy Backup & Recovery 6.1, 7.0
- EMC NetWorker 7.2, 7.4
- HP Data Protector 6.0, 6.1
- IBM Tivoli Storage Manager 5.5
- Symantec Backup Exec 11d, 12.0
- Symantec NetBackup Enterprise Server 6.0, 6.5.x

In addition, FMA supports the following:

- Microsoft Windows Server 2003 Resource Kit Tools – Robocopy.exe (Robust File Copy Utility)
- Hard quotas on Veritas Storage Exec 5.5

FMA does not support the following:

- Restoring an FMA-managed volume to an alternate location
- IBM Tivoli Storage Manager snapshot technology

Virtualization software

FMA supports VMware Server 1.4 and 1.5 (formerly known as GSX Server) virtualization software running one of the supported operating systems.

Antivirus software

The following antivirus and backup applications were tested with FMA:

Note Running FMA and antivirus software on the same file server is not recommended unless necessary, such as when the file server is attached to the Internet.

- CA eTrust 8.0, 8.1
- McAfee VirusScan Enterprise 8.0i, 8.5
- Sophos Anti-Virus 6.5, 7.x
- Symantec AntiVirus Corporate Edition 10.1
- Symantec EndPoint Protection 11.0
- TrendMicro ServerProtect 5.58, 5.7
- TrendMicro OfficeScan 7.0, 8.0

The following settings must be modified in Symantec AntiVirus when it is used with FMA:

- Select **Symantec AntiVirus**→**Configure**→**File System Auto-Protect**→**Advanced** to access the Auto-Protect Advanced Options dialog box.

Change the following settings in the Scan files when area:

- Select **Modified (scan on create)**.
- Clear the **Opened for backup (not applicable to Windows 9x or NetWare)** option.
- In the Scan Advanced Options dialog box, change the following settings in the Storage migration options area:
 - Select **Skip offline files**.
 - Select **Open file using backup semantics**.

If TrendMicro OfficeScan is installed and active, be aware that a released file will be recalled if you attempt to rename or move it. To avoid a file recall, disable the OfficeScan first.

Defragmentation software

The following defragmentation software was tested with FMA:

- Microsoft Disk Defragmenter 1.0
- O&O Defragmenter 8.0

Multipathing software

The following multipathing software was tested with FMA:

- HP MPIO DSM (Device Specific Module) Manager v2.00.2
- HP StorageWorks Secure Path 4.0c

Note FMA can manage disk volumes that have been assigned to it by external disk arrays. These disk arrays may utilize multipathing software that allows backend features such as load balancing and failover/failback. FMA only supports multipathing software associated with HP StorageWorks EVA, MSA, and XP disk arrays.

Quota management software

The following quota management software was tested with FMA:

- Symantec Storage Exec 5.5
- Microsoft Windows 2003 R2, File Server Resource Manager, Quota Management

Note FMA can exist with these quota management tools. Folder or volume quotas can be set on FMA managed volumes. When setting hard quotas on your folder or managed volumes, be careful not to allow the managed resources to reach 100% capacity. Disk quota space of 5% is needed to perform basic FMA operations such as migration, release, and recall.

Mirroring software

HP StorageWorks Storage Mirroring software, version 5.1, was tested with FMA.

Resolved Issues and Enhancements

The following changes have been incorporated into the FMA 2.5 release and are applicable to all platforms unless noted otherwise.

- **Changing Windows configuration to place pagefile.sys on an FMA managed volume caused a system fault (blue screen) during boot up.** You can now configure Windows paging such that the pagefile is stored on an FMA managed volume. (FMA-1844)
- **Recall to a full managed volume may have corrupted the stub file's size.** If the managed volume overflowed during recall operations, the file size of the stub files may have been reset to a wrong value resulting in a failed recall unless manual repair operations were taken. This issue is resolved in this release. (FMA-1777)
- **The FMA filter driver did not start on some cluster servers.** The FMA filter driver would not start on systems that did not have a registry entry for HKLM\System\ControlSet001. This issue has been resolved. (FMA-1745)
- **Explorer on Server 2008 does not show FMA column headings.** For Server 2008, Microsoft has removed the Windows Explorer column management utility that allowed FMA to create new columns for the file detail view. The information presented in the FMA columns is now presented on the FMA File Properties tab. (Right-click a file and select Properties, and then click the FMA tab.) In addition, to be uniform across platforms, the column feature has also been removed from Server 2003 systems. (FMA-1830)
- **FMA could not recall files from the FTP Secondary server.** When the primary archive was not available, FMA should have attempted to recall the file from the secondary definition if it existed. Now, FMA attempts to recall files from the secondary server if the primary is not reachable. (FMA-680)
- **FMA configuration service remained in a Stopping state after reconnection in a cluster.** In a cluster environment, when network communications were lost between cluster nodes, the FMA configuration service running as a cluster resource may have been left in a “stopping” state. To get it out of this state, the cluster node had to be rebooted. This issue is now resolved. (FMA-2089)
- **Invalid entries in fields were not checked by the user interface.** The user interface has been improved to check for invalid entries. (FMA-1958, FMA-1979, FMA-2068, FMA-2085, FMA-2087, FMA-2088)
- **Migration to locally mounted network share failed.** In previous versions, FMA archive configuration could not use a network share that was mounted to a local drive letter. This is now possible but FMA will offer to convert the path to its universal naming convention (UNC) equivalent. This is done because Microsoft does not recommend that processes reference network shares using local drive letters. (FMA-2051)
- **Volume status of Not Mounted is shown when a managed volume was stopped.** In previous versions of FMA, when a managed volume was stopped by a user request, the volume status in the FMA UI would show “Not Mounted”. This has been changed to show a status of “Stopped”. Now, the “Not Mounted” status is displayed only if the volume is not physically mounted, such as in a cluster environment when the volume is moved to another node. (FMA-2049)
- **“RISS” has been changed to “IAP”.** HP StorageWorks Reference Information Storage System (RISS) has been renamed to HP Integrated Archive Platform (IAP). Therefore, all occurrences of “RISS” have been changed to “IAP” in the FMA UI. Note that log entries may still reference RISS. (FMA-2026)
- **Volume manager restarted when migrating PowerPoint file with blank Company attribute.** In previous versions of FMA, migration of Microsoft PowerPoint files that contained a blank “Company” attribute sometimes caused the FMA volume manager process to restart. This resulted in all active migrations to be interrupted. This issue is now resolved. (FMA-2015)

- **fmacli and afmsvc ignored files dated in the future.** In previous versions of FMA, files that had dates that were in the future were ignored by FMA policy management. This issue has been resolved and files with future dates are now checked against the defined policy criteria. (FMA-2013)
- **Deleting a policy did not prompt for confirmation.** In previous versions of FMA, when the user deleted a policy, the operation occurred without any prompting. This behavior has been changed to provide a confirmation dialog to give the user the option to cancel the operation. (FMA-1943)
- **Configuration service stopped and restarted.** In previous versions of FMA running in a cluster environment, the configuration service sometimes stopped and restarted. The issue is not always noticeable because the service is automatically restarted. The issue has been resolved in this release. (FMA-1916)
- **Browsing when setting up a CIFS archive did not show shares on the archive.** In previous versions of FMA, it was not always possible to browse to network share names when configuring a CIFS archive destination. With this release, this is now possible. Note that access rights for the share and the FMA technical user must be set up to match. See the Administration Guide for details. (FMA-1915)
- **New and Delete menu options changed.** In previous versions of FMA, when the user added or removed a volume from FMA management, “New” or “Delete” was selected from the menu. These terms have been changed to “Add to Management” and “Remove from Management” respectively because the volumes are not actually being created or deleted. (FMA-1827)
- **New -> Archive menu option was removed.** In previous version of FMA, there were two menu items for creating a new archive definition. These were “New Archive” and “New -> Archive”. Both options performed the same action. The “New->Archive” option was removed in this release for simplification. (FMA-1824)
- **Migrated column was not removed from the “fmacli arc” command output.** The number of bytes migrated was previously visible using the “fmacli archive” command. Starting with this release, migrated data is counted on a per volume basis and not on a per archive basis. The total bytes migrated column for the “fmacli archive” command has been removed. A similar column is now available for the “fmacli volume” command. See the Administration Guide for more information on these commands. This change is also reflected in the FMA UI for the Archive and Volume displays. (FMA-1781, FMA-1687)
- **File released more than once when “Release Immediately” is selected and Archive Copies is set to “All”.** When the “Release Immediately” checkbox is selected in the Migration Policy, the file should be released only after the first time it is migrated. It should not be released for subsequent migrations, such as after a recall. However, with earlier releases, when the “Release Immediately” checkbox was selected and the Archive Copies option was set to “All” in the Archive section of the migration policy, the file was released on migrations after the first occurrence. With this release, the file will only be released after the first time it is migrated when the “Release Immediately” checkbox is selected. (FMA-1778)
- **Troubleshooting package is now available.** A Troubleshooting package can now be generated. See the Administration Guide for details. (FMA-1767)
- **Naming scheme for change revisions now uses timestamp instead of index number.** When FMA migrates files to archives and the file already exists in the archive, it adds a suffix to the filename to differentiate the new copy from the old copy. In previous releases, FMA added a four-digit number (“nnnn”) to the end of the filename in the archive. Beginning with this release, the suffix will be a timestamp in this format: “YYYYMMDDhhmmssuuu”. This makes it easier to determine which archive copies are newer when viewing files in the archive. (FMA-1688)
- **recall command returned incorrect message when managed disk was full.** In previous versions, when the managed volume filled up during a recall, it was possible to get an error (0x00060103) “verification failed file does not exist”. This was an incorrect error. This release provides the proper message: “Error writing data” (FMA-1300)

- **The “Ignore system” setting for CIFS archives did not take effect until restart, but user was not notified.** When changing settings on Archive definitions, the changes did not take effect until after the FMA services are restarted. With this release, the change confirmation dialog reminds the user that the FMA services must be restarted for the changes to take effect. (FMA-863)
- **“Ignore security on backend archive” option now available for CIFS archives.** In previous releases, the “Ignore security on backend archive” option had no effect when selecting it in the CIFS RSA Configuration dialog. This feature is now implemented and has the effect of not storing migrated files' security settings with the archive copy of the file. (FMA-853)
- **Can now remove an unmounted volume from management.** In previous releases of FMA, a volume could not be removed from management if it was no longer mounted to the server. The volume can now be removed from the FMA volumes view even if it is physically removed. (FMA-814)
- **Policy application terminated when trying to migrate files from a deleted directory.** In previous versions of FMA, when a policy ran that tried to migrate files from a directory that was deleted, the policy application was terminated and did not continue to search for other files that should be migrated. Now, the missing files and directory are logged and the policy service continues to run. (FMA-784)
- **Files were not expired if expiration period was set to 0.** In previous versions, when an expiration period of zero was specified for the fmacli cleanup command, the command would not clean up any files. With this release, an expiration period of 0 is handled correctly and the files are immediately expired. (FMA-774)
- **Apply button now enabled for Exclusion list.** In previous versions of FMA, when the user entered a new path in the Exclusion list, the Apply button did not activate. Now, the Apply button is enabled when changes are made to the Exclusion list. (FMA-767)
- **FMA terminated if an unprivileged user attempted to use context menus.** In previous versions of FMA, if an unprivileged user attempted to use the FMA context menus in Windows Explorer, the application would terminate abnormally. This issue has been resolved and the unprivileged user will not see the FMA context menu items. To use FMA Explorer menu functions, the user must have Administrator rights. (FMA-765)
- **IAP archive limit not checked until limit was exceeded.** In previous versions of FMA, the IAP archive file size was not checked prior to migrating the file. The error would be reported when the limit was encountered during the migration, which wasted time. In this release, the file size is proactively checked before the file is migrated. The exact number of bytes that can be migrated to an HP IAP archive is 1,579,024,383. (FMA-718)
- **Policy command now reports all fields.** Previously, the fmacli policy command did not report all fields of the named policy. These issues have been corrected. See the Administration Guide for more information on the fmacli policy command. (FMA-717)
- **Undefined policy start time error logged an error.** In previous versions, when a policy start time was not defined, FMA always logged an error that no start time was defined. Now, a log entry is made at a warning level to be less obtrusive. (FMA-450)
- **File policy would not start if days of the week were not specified.** Previously, the “Days of week” option on the file policy could be left with all days unchecked. This resulted in the policy not starting as expected with no warning. With this release, FMA will force the user to check the desired days of week before saving the policy. (FMA-9)
- **RSA Config button did not enable when configuring a new archive.** When configuring a new archive, the RSA Config button did not enable. This has been fixed. (FMA-1977)

- **Start and stop icons were incorrectly displayed if you started or stopped volume management while viewing archives.** In FMA configuration, if you selected the Archives view in the left pane and then started or stopped volume management by right-clicking a volume below that, the red or green stop and start icons were incorrectly displayed on an archive listed in the right pane. This has been fixed. (FMA-1993)
- **Archive was saved even with unspecified storage path.** It was possible to save an RSA-CIFS archive without specifying an archive path, which caused migrations to fail. This has been fixed. (FMA-1988)
- **cleanup of inaccessible archive removed garbage collection list, stranding files.** If the cleanup command was run and the archive containing files that needed to be deleted was not accessible, the garbage collection list was removed as if the files had been removed from the archive. This resulted in stranded files in the archive. This has been resolved in this release. (FMA-78)
- **cleanup did not work for overwritten or superseded files.** The cleanup command did not work for overwritten or superseded Microsoft Office files. This has been resolved. (FMA-451)

Known Issues

The following known issues (or errata) apply to FMA 2.5. The issue tracking number is provided in parentheses. Refer to this number if making inquiries to Technical Support.

There is a table of tracking numbers and their summaries listed in ascending order in the [Issue Index](#) on page 16.

- **HSM status of the quorum disk may indicate Inactive instead of Unknown.** In the FMA user interface, the HSM status of the quorum disk may indicate Inactive instead of Unknown. While the listed status is incorrect, no bad consequences are known to occur as a result. (FMA-2131)
- **Volume does not start after it is added to management.** If a volume is added to FMA management immediately after its partition is created, FMA may not be able to manage the volume. It will appear in the user interface as managed but stopped. Attempts to start FMA on the volume result in the “Error to start volume: The handle is invalid” error. (FMA-2122)

WORKAROUND: Stop then start the HsmSvc service. After the service is restarted, the volume will appear in a running state.

- **Test button must be clicked twice to change password on FTP archive page.** If you change the password when entering the FTP archive information, a popup dialog is displayed that prompts you to confirm the password. After clicking OK, you are returned to the page. Note that the test is not run until Test is selected a second time. If the password was not changed, the popup dialog is not displayed and the test is run immediately. (FMA-2121)
- **Up to 99 archives are supported with the Explorer plugin.** The FMA Explorer plugin has not been tested with more than 99 archives defined. It is not recommended to exceed this limit when using the Explorer plugin. (FMA-66)
- **“Access Denied on FMA Metadata Erase” errors may be logged for Firefox.** If a Firefox profile directory is located on an FMA managed volume and the Firefox user clears their website cache, “Access Denied on FMA Metadata Erase” errors may be logged in the FMA logs. In this case, the errors can be ignored because the metadata has been erased. (FMA-1706)
- **Back button is displayed but cannot be used if installation is run more than once.** When you run FMA setup after FMA is installed and select the Modify or Repair operations, the installer will show a Back button, but it will not function correctly and should not be used. (FMA-1822)
- **Uninstall may fail if FMA is uninstalled before cluster configuration is completed.** In a cluster environment, if FMA is uninstalled prior to completing its cluster configuration, the uninstall may fail because the FMASVC service will fail to stop. (FMA-1911)

WORKAROUND: If the FMASVC service is now in the “Stopping” state, you can manually start the FMA Configuration Service on that server node, which will allow the FMASVC service to complete its stopping operation. You can also wait for the FMASVC service to stop on its own, which could take up to seven minutes. After the FMASVC service is stopped, you can start the uninstall procedure again.

- **Stopped managed volume may start after server is rebooted.** If a managed volume is set to Stopped state and the server is rebooted, it may enter the active state when the server starts back up. (FMA-2057)

WORKAROUND: Correct the management state of the volume using the FMA UI after the server is running.

- **Errors are logged if System and HSM Volume Information directories are removed from exclusion lists.** In the Disk Space and Migration policies, FMA populates the Exclusion lists with the “System Volume Information” and “Hsm Volume Information” directories. If these are deleted, errors will appear in the FMA logs when FMA tries to manage these directories. To avoid the errors, do not remove these from the exclusion lists and, if they are removed, replace them. (FMA-1940)

- **Incorrect version number listed in the Add/Remove Programs list on Windows 2008.** For Server 2008, the FMA version number should be obtained from the FMA software Version dialog. All other reports of the FMA version number, such as in Add/Remove Programs, should be ignored. (FMA-2064)
- **Unknown Error displayed when deleting an unmounted volume.** When a volume is being removed from FMA management and the physical volume is no longer mounted to the server, an error may be shown stating that an “Unknown Error Occurred” when deleting the volume. This error can be ignored because the volume is actually removed correctly from FMA. (FMA-2107)
- **Entering 0 for the Disk Space Policy monitoring time interval disables disk space monitoring.** The user interface allows you to enter 0 for the Disk Space Policy monitoring time interval. This will have the effect of disabling disk space monitoring instead of providing continuous monitoring. (FMA-1963)
- **Uninstalling FMA closes any open My Computer windows.** If any My Computer instances are running when FMA is uninstalled, the instances are closed and the user is not warned. (FMA-1722)
- **Explorer plugin shows recall option for files that were not migrated.** The Explorer plugin adds FMA file operation commands for migration, release, and recall to the Windows Explorer context menu for files. When a single file is selected, the Explorer plugin determines the available options for the selected file based on its status and disables unavailable options. When multiple files or directories are selected, the menu displays all FMA file operation commands, including those that are not available for some files. If an unavailable option is selected, FMA will reject the operation and display an appropriate result code. (FMA-703)
- **Deleted files may not be garbage-collected if the HsmSvc service is stopped.** When the FMA volume manager service (HsmSvc.exe) is stopped, it is possible that deleted files are not garbage-collected from their respective archive(s). This only occurs for files that are managed (migrated) and currently online in the managed volume. (FMA-4)

WORKAROUND: To avoid this issue, do not perform file operations while this service is in a stopped state. If this situation does occur, manually delete the files from the archive.

- **Files are not migrated to second IAP archive if the second archive is added after files are initially migrated and released from first archive.** When files are initially migrated and released to a single IAP archive and then a second IAP archive is added to the policy at a later date, the original files are not migrated to the second archive. This procedure is only needed for IAP archives and is not needed when the two archives are CIFS type. (FMA-819)

WORKAROUND: To create two copies of the migrated files, recall them and then remigrate them with number of copies specified as “2” or “All”.

- **Limitation when archiving to IAP.** While FMA allows non-ASCII repository names to be created, Integrated Archive Platform (IAP) does not support non-ASCII repository names. To efficiently archive data into IAP using FMA ensure all repository names use ASCII characters. (FMA-5105)

Troubleshooting

This section includes information about how to troubleshoot problems and notes about special steps that need to be taken with specified applications.

- **Executable files are automatically recalled when viewing properties or manually releasing them using Explorer.** When viewing the properties of or manually releasing an executable file using Windows Explorer, FMA automatically recalls the file. This is because Explorer reads the file content in order to populate the file's property sheet. Executable files can be released using FMA policies, the Fmacli utility, or by having Explorer release all files from the directory level. (FMA-725)

- **Windows Explorer may not show status of offline files correctly.** The 64-bit version of Windows Explorer may not correctly show the status of offline files in some situations. (FMA-1986)

WORKAROUND: Run the 32-bit of Explorer at least once before running the 64-bit version.

- **Problem with “Veritas AOFO” option in Backup Exec application.** When using the Advanced Open File Option (AOFO) in Backup Exec, you must select the Microsoft Volume Shadow Copy Service (VSS) as the snapshot provider service. FMA only supports Microsoft VSS. (FMA-2081)

- **Back button on FMA Technical User Wizard is disabled.** If a mistake is made, the wizard can be cancelled and rerun to correct the mistake. In addition, a user's settings can be modified using standard Windows user management utilities if, for example, the wrong user is selected. (FMA-1913)

- **Managed volumes not active after cluster node failover.** Managed volumes may not be active after a cluster node failover when SCSI-3 compliant persistent reservations in the Device Specific Module (DSM) component on Windows 2003 SP1 are used. (FMA-462)

WORKAROUND: Refer to <http://support.microsoft.com/kb/911030/en-us>

- **FMA user interface opens slowly when configuration service unavailable.** If the configuration server is not available, the FMA user interface may take a long time to open. (FMA-457)
- **File objects blocked when hard quota limits exceeded.** When hard quota limits are exceeded on a volume or folder, migration, release, and recall are blocked on the corresponding file objects. (FMA-869)

WORKAROUND: Extend the quota limit temporarily or reduce the disk space consumption by compressing or deleting files.

- **Icons of msg, htm, and html files disappear on Explorer view pane after release.** With older versions of Windows 2003 Server, there may be situations where the icon for file types msg, htm, and html may disappear when the file is released. If this situation occurs, refer to the following Microsoft Knowledge Base articles for resolution to these issues. (FMA-10)

- <http://support.microsoft.com/kb/895115/en-us>
- <http://support.microsoft.com/kb/935774/en-us>

- **Antivirus software should scan on writes, not reads.** For any antivirus software, make sure that the antivirus software scans only on writes, not on reads. Otherwise, the performance of a backup will be affected. (FMA-6)

- **IBM Tivoli Storage Manager will not overwrite a managed file that has a stub file.** When restoring files using TSM, TSM will not overwrite an HSM managed or recalled file with a stub file. (FMA-6)

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 will 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. See the Administration Guide for more information on this command.

- **NetVault will skip 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 “Check for files being modified during backup?” option can be disabled to eliminate the warning messages. (FMA-2104)
- **CA ArcServe will not overwrite a migrated file that has a stub file.** During backup restore, CA ArcServe will not overwrite a migrated file with a stub file. This will appear in the CA activity log as “Skip file - Migrated”. CA ArcServe will, however, overwrite a stub file with a stub file from tape. (FMA-2065)

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 will 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. See the Administration Guide for more information on this command.

- **hsmfilter.sys file is reported as missing when FMA is installed on 64-bit platforms.** The "fmacli version -v" command and the VerInfo.txt content in the TroubleShooting package will report that the hsmfilter.sys file is missing when FMA is installed on 64-bit platforms. The report for this file is not valid on 64-bit platforms. (FMA-2017)

WORKAROUND: To confirm the existence of the file, use the 64-bit version of Windows Explorer and look for the hsmfilter.sys file in the C:\Windows\system32\drivers directory.

Issue Index

FMA-0004	Deleted files may not be garbage-collected if the HsmSvc service is stopped..	13
FMA-0006	Antivirus software should scan on writes, not reads..	14
FMA-0006	IBM Tivoli Storage Manager will not overwrite a managed file that has a stub file.	14
FMA-0009	File policy would not start if days of the week were not specified..	10
FMA-0010	Icons of msg, htm, and html files disappear on Explorer view pane after release.	14
FMA-0066	Up to 99 archives are supported with the Explorer plugin.	12
FMA-0078	cleanup of inaccessible archive removes garbage collection list, stranding files.	11
FMA-0450	Undefined policy start time error logged an error.	10
FMA-0451	cleanup did not work for overwritten or superseded files	11
FMA-0457	FMA user interface opens slowly when configuration service unavailable.	14
FMA-0462	Managed volumes not active after cluster node failover.	14
FMA-0680	FMA could not recall files from the FTP Secondary server.	8
FMA-0703	Explorer plugin shows recall option for files that were not migrated	13
FMA-0717	Policy command now reports all fields..	10
FMA-0718	IAP archive limit not checked until limit was exceeded..	10
FMA-0725	Executable files are automatically recalled when viewing properties or manually releasing them using Explorer.	14
FMA-0765	FMA terminated if an unprivileged user attempted to use context menus.	10
FMA-0767	Apply button now enabled for Exclusion list.	10
FMA-0774	Files were not expired if expiration period was set to 0.	10
FMA-0784	Policy application terminated when trying to migrate files from a deleted directory.	10
FMA-0814	Can now remove an unmounted volume from management.	10
FMA-0819	Files are not migrated to second IAP archive if the second archive is added after files are initially migrated and released from first archive.	13
FMA-0853	“Ignore security on backend archive” option now available for CIFS archives.	10
FMA-0863	The “Ignore system” setting for CIFS archives did not take effect until restart, but user was not notified..	10
FMA-0869	File objects blocked when hard quota limits exceeded..	14
FMA-1300	recall command returned incorrect message when managed disk was full.	9
FMA-1687	Migrated column was not removed from the “fmacli arc” command output.	9
FMA-1688	Naming scheme for change revisions now uses timestamp instead of index number.	9
FMA-1706	“Access Denied on FMA Metadata Erase” errors may be logged for Firefox.	12
FMA-1722	Uninstalling FMA closes any open My Computer windows.	13
FMA-1745	The FMA filter driver did not start on some cluster servers.	8
FMA-1767	Troubleshooting package is now available.	9
FMA-1777	Recall to a full managed volume may have corrupted the stub file’s size.	8
FMA-1778	File released more than once when “Release Immediately” is selected and Archive Copies is set to “All”	9
FMA-1781	Migrated column was not removed from the “fmacli arc” command output.	9
FMA-1822	Back button is displayed but cannot be used if installation is run more than once.	12
FMA-1824	New -> Archive menu option was removed.	9
FMA-1827	New and Delete menu options changed.	9
FMA-1830	Explorer on Server 2008 does not show FMA column headings.	8
FMA-1844	Changing Windows configuration to place pagefile.sys on an FMA managed volume caused a system fault (blue screen) during boot up.	8
FMA-1911	Uninstall may fail if FMA is uninstalled before cluster configuration is completed.	12
FMA-1913	Back button on FMA Technical User Wizard is disabled.	14
FMA-1915	Browsing when setting up a CIFS archive did not show shares on the archive.	9

FMA-1916	Configuration service stopped and restarted.	9
FMA-1940	Errors are logged if System and HSM Volume Information directories are removed from exclusion lists.	12
FMA-1943	Deleting a policy did not prompt for confirmation.	9
FMA-1958	Invalid entries in fields were not checked by the user interface.	8
FMA-1963	Entering 0 for the Disk Space Policy monitoring time interval disables disk space monitoring.	13
FMA-1977	RSA Config button did not enable when configuring a new archive.	10
FMA-1979	Invalid entries in fields were not checked by the user interface.	8
FMA-1986	Windows Explorer may not show status of offline files correctly.	14
FMA-1988	Archive was saved even with unspecified storage path.	11
FMA-1993	Start and stop icons were incorrectly displayed if you started or stopped volume management while viewing archives.	11
FMA-2013	fmacli and afmsvc ignored files dated in the future.	9
FMA-2015	Volume manager restarted when migrating PowerPoint file with blank Company attribute.	8
FMA-2017	hsmfilter.sys file is reported as missing when FMA is installed on 64-bit platforms.	15
FMA-2026	"RISS" has been changed to "IAP".	8
FMA-2049	Volume status of Not Mounted is shown when a managed volume was stopped.	8
FMA-2051	Migration to locally mounted network share failed.	8
FMA-2057	Stopped managed volume may start after server is rebooted.	12
FMA-2064	Incorrect version number listed in the Add/Remove Programs list on Windows 2008.	13
FMA-2065	CA ArcServe will not overwrite a migrated file that has a stub file.	15
FMA-2068	Invalid entries in fields were not checked by the user interface.	8
FMA-2081	Problem with "Veritas AOFO" option in Backup Exec application.	14
FMA-2085	Invalid entries in fields were not checked by the user interface.	8
FMA-2087	Invalid entries in fields were not checked by the user interface.	8
FMA-2088	Invalid entries in fields were not checked by the user interface.	8
FMA-2089	FMA configuration service remained in a Stopping state after reconnection in a cluster.	8
FMA-2104	NetVault will skip files that FMA is in the process of migrating.	15
FMA-2107	Unknown Error displayed when deleting an unmounted volume.	13
FMA-2121	Test button must be clicked twice to change password on FTP archive page.	12
FMA-2122	Volume does not start after it is added to management.	12
FMA-2131	HSM status of the quorum disk may indicate Inactive instead of Unknown.	12
FMA-5105	Limitation when archiving to IAP.	13