ManageEngine
ADAudit Plus

File Integrity Monitoring

www.adauditplus.com

Table of Contents

Overview

Tracking changes to system files can help ensure normal functioning of an operating system and its applications. While, tracking creation of new program files can help detect malware. For these reasons, file integrity monitoring (FIM) which involves monitoring changes across program and system files is important.

ADAudit Plus helps monitor file integrity across your Windows network.

Supported systems:

Windows Server versions:

- 2003/2003 R2
- 2008/2008 R2
- 2012/2012 R2
- 2016/2016 R2
- 2019

Workstation versions:

- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows XP

File and folder activity monitored:

- Create
- Modify
- Delete
- Move
- Rename
- Permission changes
- Audit setting changes (SACL)
- Owner changes
- Copy and paste
- Failed attempt to write
- Failed attempt to delete

This guide takes you through the process of setting up ADAudit Plus for FIM.

1. Configure FIM in ADAudit Plus

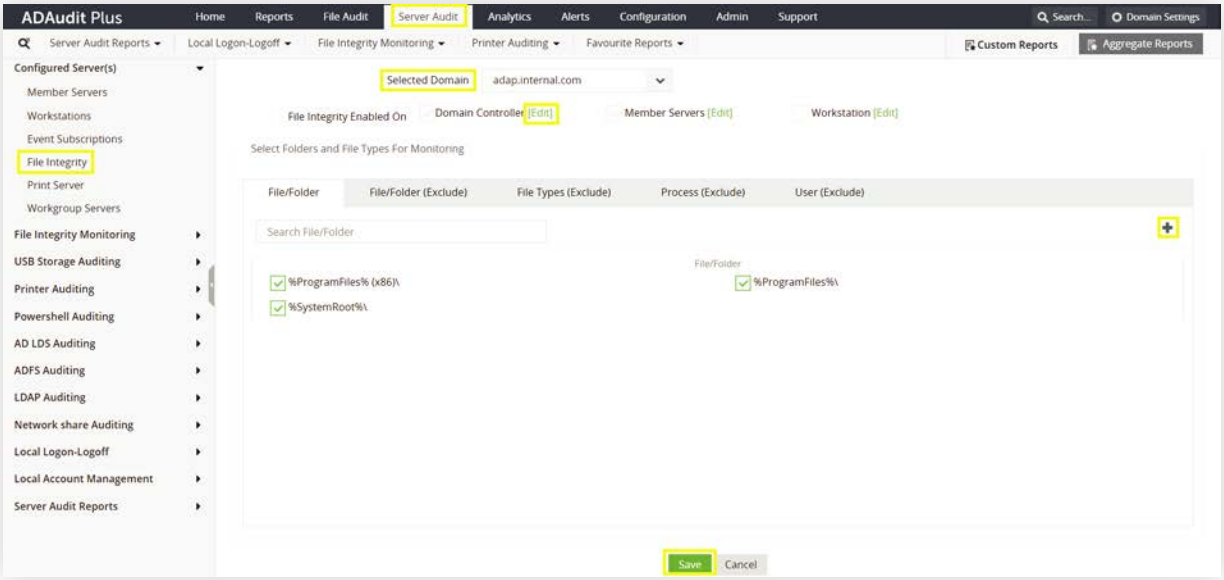
1. Log in to the ADAudit Plus web console.

2. Go to the **Server Audit** tab > **Configured Servers** > **File Integrity** > **Add Domain** > **Select Domain.**

3. Choose a domain from the drop-down. Click on **Edit** next to **Domain Controller, Member Servers**, and **Workstation** to select computers for FIM.

4. Click on + to add more files and folders for FIM, in addition to the preconfigured list of files and folders that will be configured for FIM by default.

5. Click **Save.**



2. Configure audit policies in your domain

Audit policies must be configured to ensure that events are logged whenever any activity occurs.

2.1 Automatic configuration

ADAudit Plus can automatically configure the required audit policies for FIM.

Click here to learn how to enable audit policies automatically for FIM on domain controllers.

Click here to learn how to enable audit policies automatically for FIM on Windows servers.

Click here to learn how to enable audit policies automatically for FIM on workstations.

2.2 Manual configuration

2.2.1 Configure advanced audit policies

Advanced audit policies help administrators exercise granular control over which activities get recorded in the logs, helping reduce event noise. We recommend configuring advanced audit policies on Windows Server 2008 and above.

1. Log in to any computer that has the Group Policy Management Console (GPMC) with Domain Admin credentials.

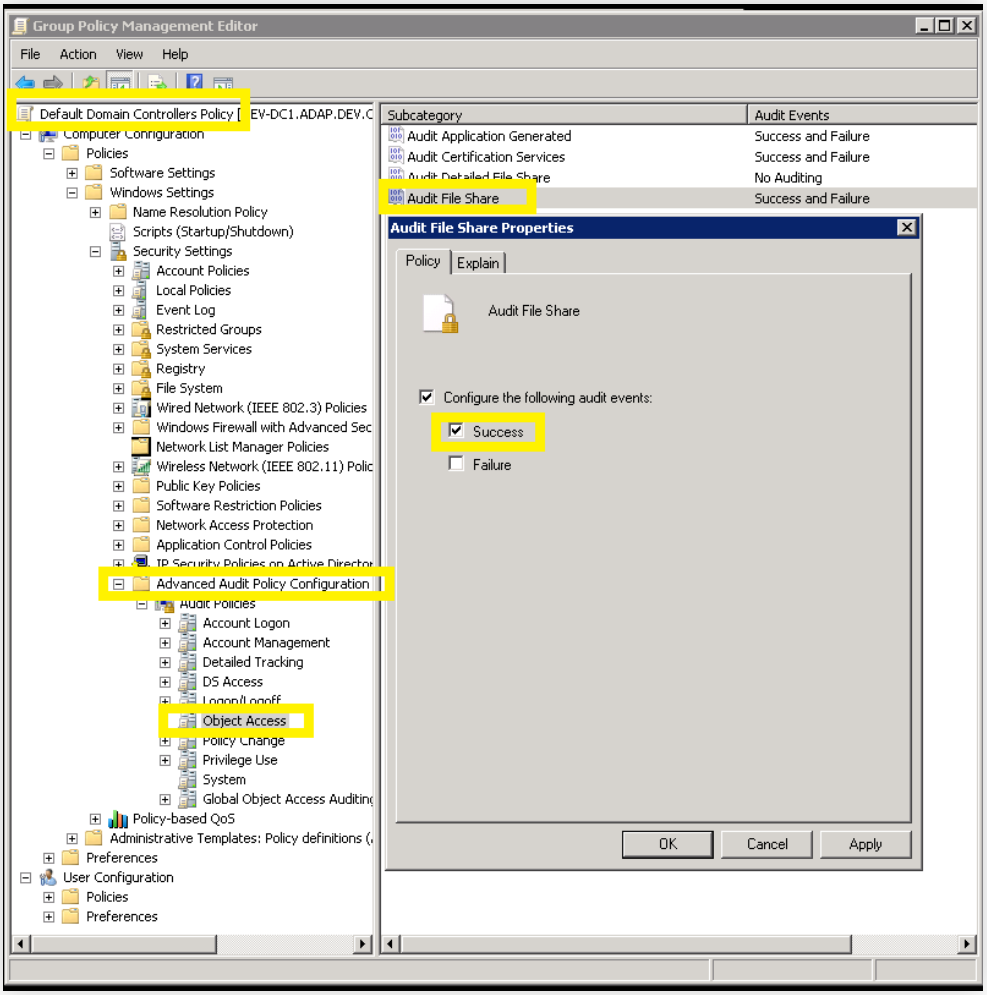
2. Open the GPMC and, based on your setup, right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy** or **ADAuditPlusWSPolicy,** and select **Edit.**

Note:

To enable FIM on	Operating System
Domain controller	Default Domain Controllers Policy GPO
Windows server	ADAuditPlusMSPolicy GPO
Workstation	ADAuditPlusWSPolicy GPO

3. In the *Group Policy Management Editor*, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration,** and configure the following settings:

Category	Subcategory	Audit events
Object Access	✓ Audit File System	Success, Failure
	✓ Audit File Share	Success
	✓ Audit Handle Manipulation	Success, Failure



2.2.2 Force advanced audit policies

When using advanced audit policies, ensure they are forced over legacy audit policies.

1. Log in to any computer that has the GPMC with Domain Admin credentials.

2. Open the **GPMC** and, based on your setup, right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy** or **ADAuditPlusWSPolicy**, then select **Edit.**

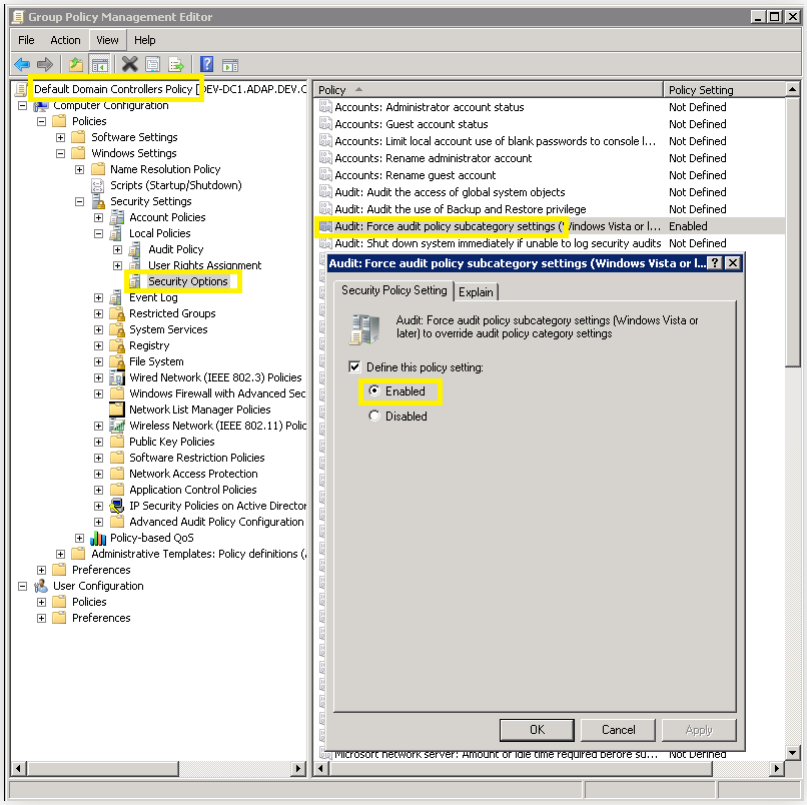
Note:

To enable FIM on	Right-click
Domain controller	Default Domain Controllers Policy GPO
Windows server	ADAuditPlusMSPolicy GPO
Workstation	ADAuditPlusWSPolicy GPO

3. In the *Group Policy Management Editor*, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.**

4. Right-click **Audit: Force audit policy subcategory settings** from the right pane.

5. Select **Properties,** then choose **Enabled.**



2.2.3 Configure legacy audit policies

Due to the unavailability of advanced audit policies in Windows Server 2003 and earlier versions, legacy audit policies need to be configured for these types of servers.

1. Log in to any computer that has the GPMC with Domain Admin credentials.

2. Open the **GPMC** and, based on your setup, right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy** or **ADAuditPlusWSPolicy**, then select **Edit.**

Note:

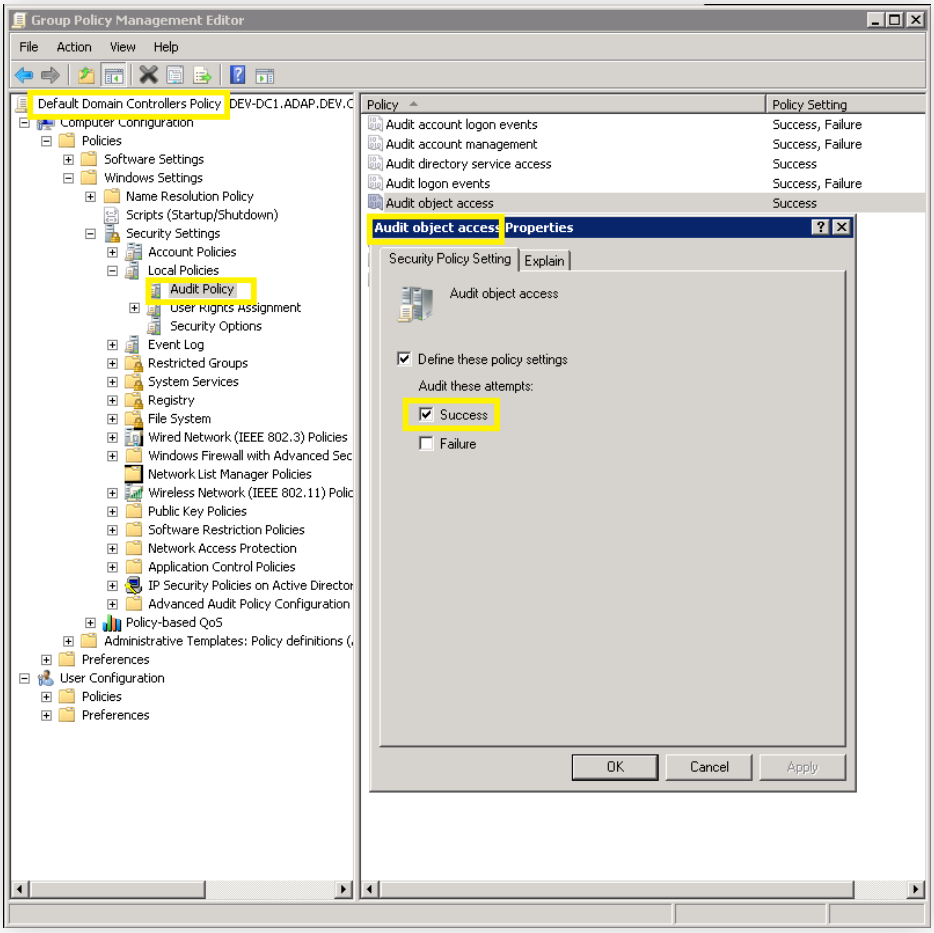
To enable FIM on	Right-click
Domain controller	Default Domain Controllers Policy GPO
Windows server	ADAuditPlusMSPolicy GPO
Workstation	ADAuditPlusWSPolicy GPO

3. In the *Group Policy Management Editor*, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies**

4. Double-click **Audit Policy.**

5. Right-click on the **Object Access** policy in the right pane.

6. Select **Properties,** then check the box next to **Success.**



3. Configure object-level auditing

To audit file and folder access, object-level auditing must be enabled. This can be achieved in three ways:

1. Using Windows shares

2. Using PowerShell cmdlets

3. Using Global Object Access Auditing

3.1 Using Windows shares

1. Right-click on the **share folder** that you want to audit, and select **Properties.**

2. Click on the **Security** tab > **Advanced,** and then click on the **Auditing** tab. For the **Everyone** group, add the following entries:

	Principal	Type	Access	Applies To
File/folder changes	Everyone	Success, Failure	• Create files / Write data • Create folders / Append data • Write attributes • Write extended attributes • Delete subfolders and files • Delete	This folder, subfolders, and files
Folder permission and owner changes	Everyone	Success, Failure	• Take ownership • Change permissions	This folder and subfolders

3.2 Using PowerShell cmdlets

1. Create a CSV file containing the Universal Naming Convention (UNC) path or local path and the type of auditing (FIM) of all the folders that you want to enable auditing for.

2. The CSV file should contain the list of folders in the following format: <folder>,<type>

For example:

E:\test folder,FIM

\\SERVERNAME\c$\folder,FIM

Note:

When removing object-level auditing for a set of folders, the **<type>** parameter is **not mandatory.**

Once you have the CSV file that lists all the servers and the type of auditing required, go to the **<Installation Directory>\bin** folder within the PowerShell command prompt and type in:

.\ADAP-Set-SACL.ps1 -file **'.\file name'** -mode **add (or) remove** -recurse **true (or) false** -username **DOMAIN_NAME\username**

Where:

Parameter	Input variable	Mandatory
-file	The name of the CSV file containing the list of shared folders.	Yes
-mode	**Add:** Sets the object-level auditing settings. (or) **Remove:** Removes the object-level auditing settings.	Yes
-recurse	**True:** Replace all subfolder object-level auditing settings with inheritable auditing settings applied to the chosen folder. (or) **False:** Apply object-level auditing settings only to the chosen folder. **Note:** By default, the **-recurse** parameter is set to **false.**	No

For example:

- To set object-level auditing for the list of folders in a CSV file named *folders.CSV*, use:

  .\ADAP-Set-SACL.ps1 -file '.\folders.CSV' -mode add

- To replace all subfolder object-level auditing settings with inheritable auditing settings applied to a CSV file named *folders.CSV*, use:

  .\ADAP-Set-SACL.ps1 -file '.\folders.CSV' -mode add -recurse true

- To remove object-level auditing for the list of folders in a CSV file named *folders.CSV*, use:

  .\ADAP-Set-SACL.ps1 -file '.\folders.CSV' -mode remove

3.3 Using Global Object Access Auditing

1. Log in to any computer that has the GPMC with Domain Admin credentials.

2. Open the **GPMC** and, based on your setup, right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy** or **ADAuditPlusWSPolicy**, then select **Edit.**

Note:

To enable FIM on	Right-click
Domain controller	Default Domain Controllers Policy GPO
Windows server	ADAuditPlusMSPolicy GPO
Workstation	ADAuditPlusWSPolicy GPO

3. In the *Group Policy Management Editor*, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Global Object Access Auditing > File system > Define this policy setting > Configure.**

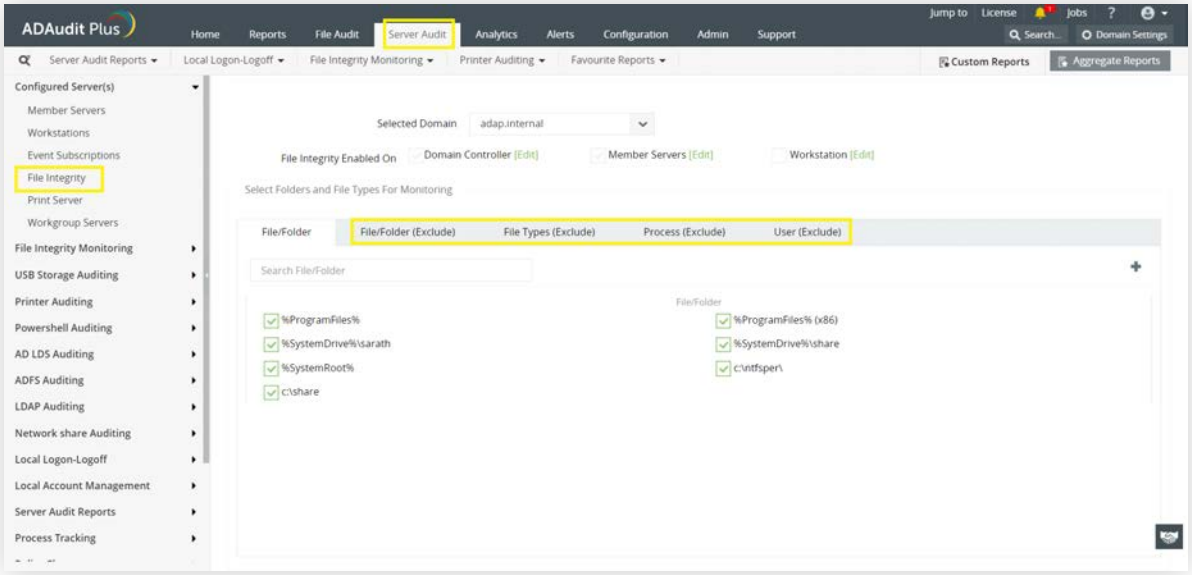
   For the **Everyone** group, add the following entries:

	Principal	Type	Access	Applies To
File/folder changes	Everyone	Success, Failure	• Create files / Write data • Create folders / Append data • Write attributes • Write extended attributes • Delete subfolders and files • Delete	This folder, subfolders, and files
Folder permission and owner changes	Everyone	Success, Failure	• Take ownership • Change permissions	This folder and subfolders

4. Exclude configuration

Files and folders can be excluded based on file/folder local path, file type, process name, and username by using the **Exclude Configuration** setting.

1. Log in to the ADAudit Plus web console.
2. Go to the **Server Audit** tab > **Configured Servers > File Integrity > Add Domain > Select Domain.**
3. Choose a domain from the drop-down. Choose to exclude by **File/Folder** local path, **File Type, Process Name**, or **Users.**
4. Click on **+** and configure the necessary settings.



Example scenarios to exclude by **File/Folder** path:

Objective	**To exclude a folder and all of its subfolders and files**	
Share configured	**Share path**	**Local path**
	\\SERVERNAME\c$\fimfolder	c:\fimfolder
Path of folder that is to be excluded	c:\fimfolder\excludefolder	
File/Folder or regex patterns	File/Folder patterns	
Syntax	c:\fimfolder\excludefolder c:\fimfolder\excludefolder*	
What will be excluded	c:\fimfolder\excludefolder c:\fimfolder\excludefolder\folder c:\fimfolder\excludefolder\files.txt c:\fimfolder\excludefolder\folder\files.txt	
What won't be excluded		

Objective	To exclude the "AppData" folder for every user profile
Share and folder path	\\SERVER_NAME\c$\Users c:\Users
Path of folder that is to be excluded	C:\Users\user1\AppData
File/Folder or regex patterns	Regex Patterns
Syntax	C:\\Users\\[^\\]*\\AppData
What will be excluded	C:\Users\user1\AppData C:\Users\user2\AppData C:\Users\user1\AppData\subfolder C:\Users\user2\AppData\subfolder
What won't be excluded	C:\Users\user1\subfolder\AppData C:\Users\user2\subfolder\AppData

Objective	To exclude files from a specific folder but audit all subfolders and their contents
Share and folder path	\\SERVERNAME\c$\fimfolder c:\fimfolder
Path of folder that is to be excluded	c:\fimfolder\excludefolder
File/Folder or regex patterns	Regex Patterns
Syntax	^c:\\fimfolder\\excludefolder\\[^\\]*\.[^\\]*$
What will be excluded	c:\fimfolder\excludefolder\file.txt c:\fimfolder\excludefolder\folder.withDot
What won't be excluded	c:\fimfolder\excludefolder c:\fimfolder\excludefolder\folderWithoutDot c:\fimfolder\excludefolder\folderWithoutDot\subfolder c:\fimfolder\excludefolder\folderWithoutDot\testfile.txt c:\fimfolder\excludefolder\folder.withDot\subfolder c:\fimfolder\excludefolder\folder.withDot\testfile.txt

5. Configure security log size and retention settings

Event log size needs to be defined to prevent loss of audit data due to overwriting of events.

1. Open the **GPMC** and, based on your setup, right-click **Default Domain Controllers Policy** or **ADAuditPlusMSPolicy** or **ADAuditPlusWSPolicy**, then select **Edit.**

Note:

To enable FIM on	Right-click
Domain controller	Default Domain Controllers Policy GPO
Windows server	ADAuditPlusMSPolicy GPO
Workstation	ADAuditPlusWSPolicy GPO

2. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Event Log.**

3. Set **Retention method for security log** to **Overwrite events as needed.**

4. Configure the **Maximum security log** size as defined below. Ensure that the security log can hold a minimum of **12 hours'** worth of data.

Role	Operating system	Size
Domain controller	Windows Server 2003	512 MB
Domain controller	Windows Server 2008 and above	1,024 MB
Member server	Windows Server 2003	512 MB
Member server	Windows Server 2008 and above	4,096 MB
Workstation	Windows 10, 8, 7, Vista, and XP	512 MB