ManageEngine
ADAudit Plus

Windows file server auditing guide

www.adauditplus.com

Table of Contents

Overview

A file server is a computer attached to a network that provides a location for shared storage of computer files.

ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Windows servers secure and compliant. With ADAudit Plus, you can:

- Track accesses and changes to shares, files, and folders
- Identify the username, workstation, and IP address of each user file activity
- Receive email alerts upon suspicious activity
- Audit Windows failover clusters for a secure and compliant network environment that experiences no downtime
- Automate the tracking of changes through scheduled reports
- Meet SOX, HIPAA, PCI DSS, and GLBA compliance requirements

1. Supported systems

Windows Server versions:

- 2008/2008 R2
- 2012/2012 R2
- 2016/2016 R2
- 2019
- 2022

Share types

- SMB
- CIFS
- DFS
- DFSR

Volume types

- Mounted volume
- SAN volume
- Junction path

File and folder activity

- Created
- Deleted
- Modified
- Read
- Copied and pasted
- Moved
- Renamed
- Owner changes
- Permission changes
- Audit settings changes
- Failed read attempts
- Failed write attempts
- Failed delete attempts

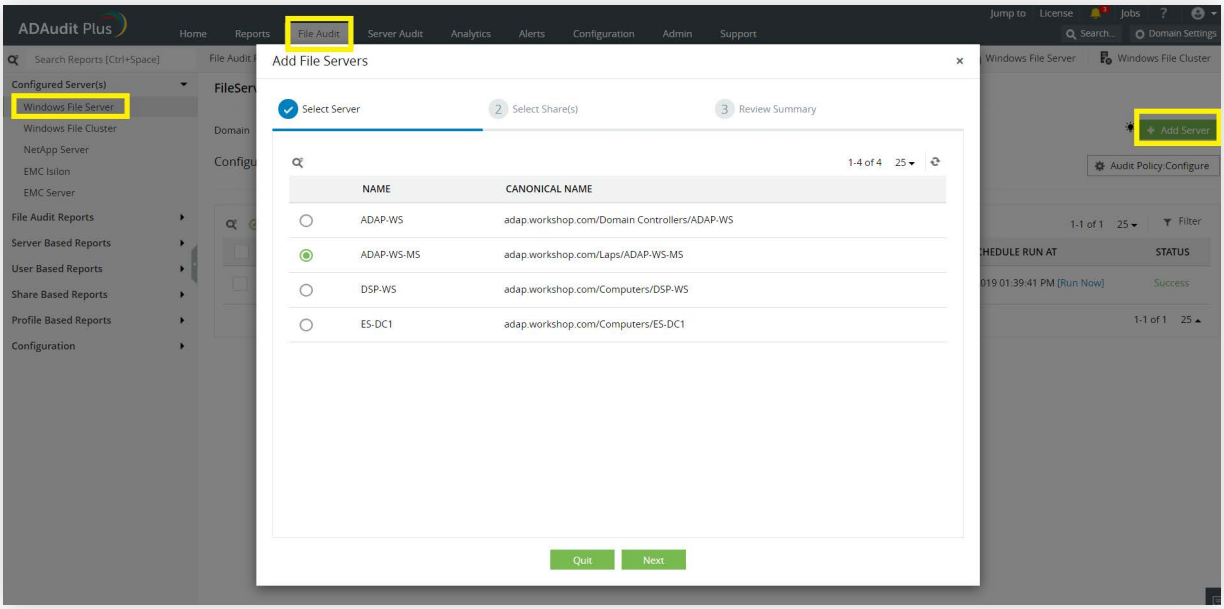
2. Configure Windows file servers in ADAudit Plus

2.1 One server at a time

To configure Windows file servers one by one:

Log in to ADAudit Plus' web console. → Click on the **File Audit tab** → Select **Windows File Server** from under the **Configured Server(s)** drop-down list → Click on **Add Server** → Follow the instructions from the wizard to add the desired file server.

Note: ADAudit Plus can automatically configure the required audit policies and object-level auditing for Windows file server auditing. In the final step, you can either choose **Yes** to let ADAudit Plus automatically configure the required audit policies and object-level auditing, or choose **No** to manually configure the required audit policies and object-level auditing.



2.2 In bulk

To configure Windows file servers in bulk:

1. Create a CSV file by the name 'servers.csv' in the location <installation dir>\ManageEngine\ ADAudit Plus\bin. From the Encoding tab, save the document in UTF-8 format. → Open the file, enter the names of all file servers (that you want to audit) in adjacent lines, and separate them using commas.

   For example, to add the file servers Test-FS1, Test-FS2, and Test-FS3; open the servers.csv file and enter:

   Test-FS1,

   Test-FS2,

   Test-FS3

2. Create a CSV file by the name 'shares.csv' in the location <installation dir>\ManageEngine\ ADAudit Plus\bin. From the Encoding tab, save the document in UTF-8 format → Open the file, enter the names of all file shares (that you want to audit) in adjacent lines, and separate them using commas.

   For example, to add the shares \\SERVERNAME\testfolder1, \\SERVERNAME\testfolder2, \\SERVERNAME\testfolder3; open the shares.csv file and enter: \\SERVERNAME\testfolder1, \\SERVERNAME\testfolder2, \\SERVERNAME\testfolder3

3. Navigate to <installation dir>\ManageEngine\ADAudit Plus\bin. → Open command prompt and execute 'cmdUtil.bat'. → Enter ADAudit Plus' default admin credentials.→

   Note: ADAudit Plus' default username and password are both 'admin'.

   And execute the following command:

   config server add -machinetype fs -shares **all (or) single (or) shares.csv** -issacl **true (or) false** -isauditpolicy **true (or) false**

   After -shares, enter **'all'** to audit all shares, **'single'** to audit one random share, and **'shares.csv'** to audit the selected shares.

   After -issacl, enter **'true'** to automatically configure the required object level auditing settings and **'false'** to manually configure the required object level auditing settings.

   After -isauditpolicy, enter **'true'** to automatically configure the required object access audit policy and **'false'** to manually configure the required object access audit policy.

   For example, if you want to audit selected shares in all file servers and configure the required object access audit policy and object level auditing settings automatically; execute the following command:

   config server add -machinetype fs -shares **shares.csv** -issacl **true** -isauditpolicy **true**

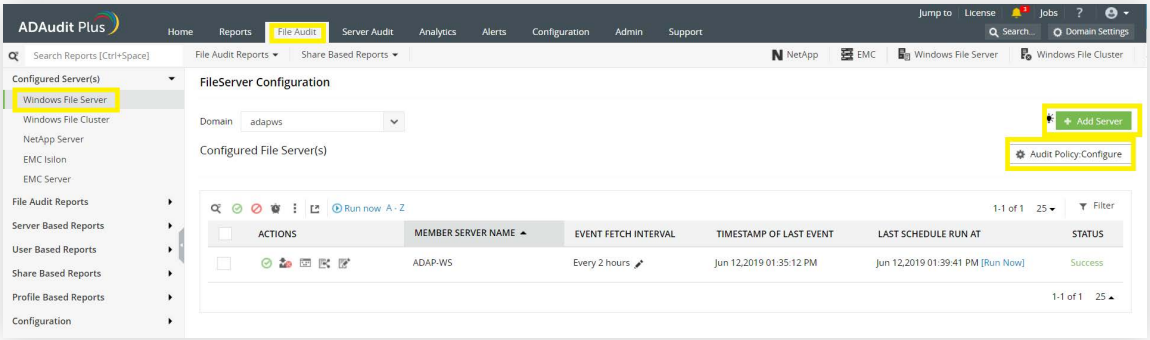
3. Configure audit policies in your domain

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

3.1 Automatic configuration

Log in to **ADAudit Plus' web console** → Click on the **File Audit** tab → Select **Windows File Server** from under the Configured Server(s) drop-down list → Click on **Configure Audit Policy** in the right corner above the table view.

This will create a Group Policy object (GPO) [domainname_ADAuditPlusPolicy] and set the required audit policies for Windows file server auditing.



3.2 Manual configuration

3.2.1 Configure list of Windows file servers to be audited

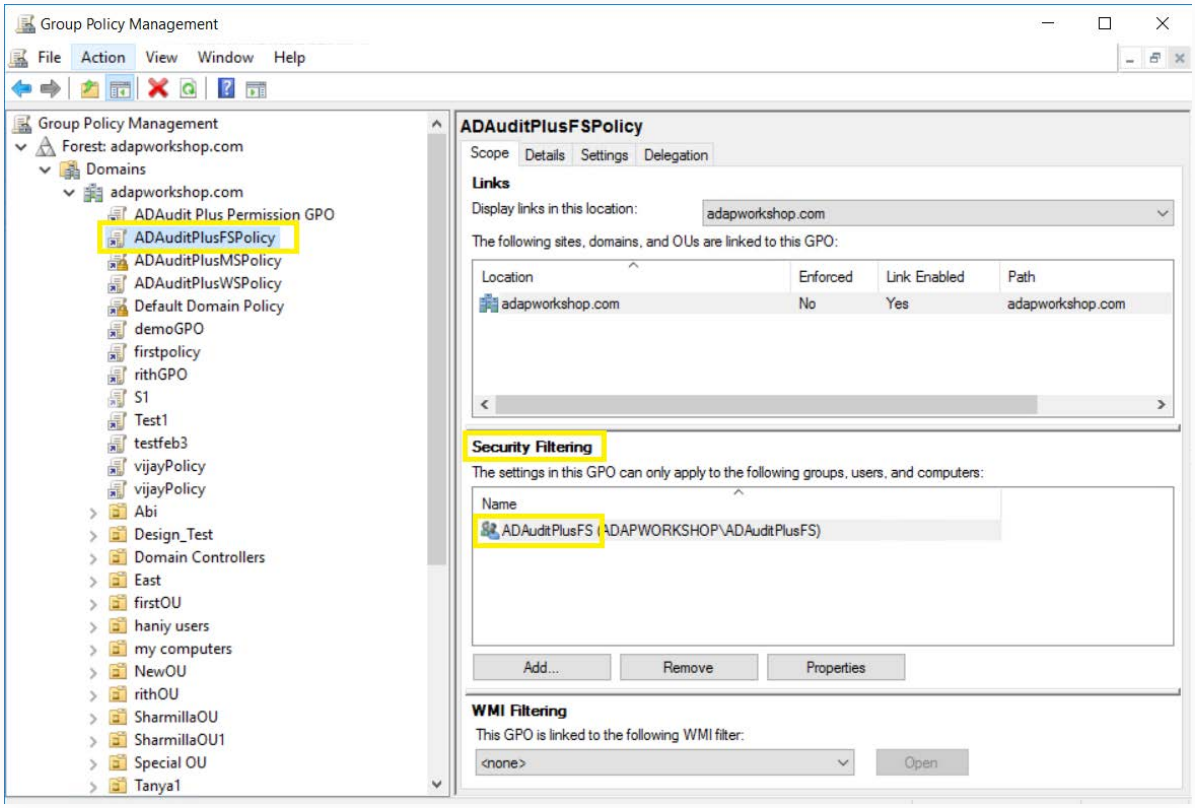
1. Open **Active Directory Users and Computers.**
2. Right-click the domain and select **New > Group.**
3. In the **New object - Group** window that opens, type in **"ADAuditPlusFS"** as the **Group name,** check **Group scope: Domain Local** and **Group type: Security.** Click **OK.**
4. Right-click the newly created group, then select **Properties > Members > Add.** Add all the Windows file servers that you want to audit as a member of this group. Click **OK.**
5. Using domain admin credentials, log in to any computer that has the **Group Policy Management Console (GPMC)** on it.

   Note: The GPMC will not be installed on workstations and/or enabled on member servers by default, so we recommend configuring audit policies on Windows domain controllers. Otherwise follow the steps in this page to install GPMC on your desired member server or workstation.
6. Go to **Start > Windows Administrative Tools > Group Policy Management.**

7. In the **GPMC,** right-click the domain in which you want to configure the Group Policy. Select **Create a GPO and Link it here.** In the **New GPO** window that opens, type in **"ADAuditPlusFSPolicy"** and click **OK.**

8. Select the **ADAuditPlusFSPolicy** GPO. Under **Security Filtering,** select **Authenticated Users.** Click **Remove.** In the **Group Policy Management** window that opens, select **OK.**

9. Select the **ADAuditPlusFSPolicy GPO.** Under **Security Filtering,** click **Add** and choose the security group **ADAuditPlusFS** created previously. Click **OK.**



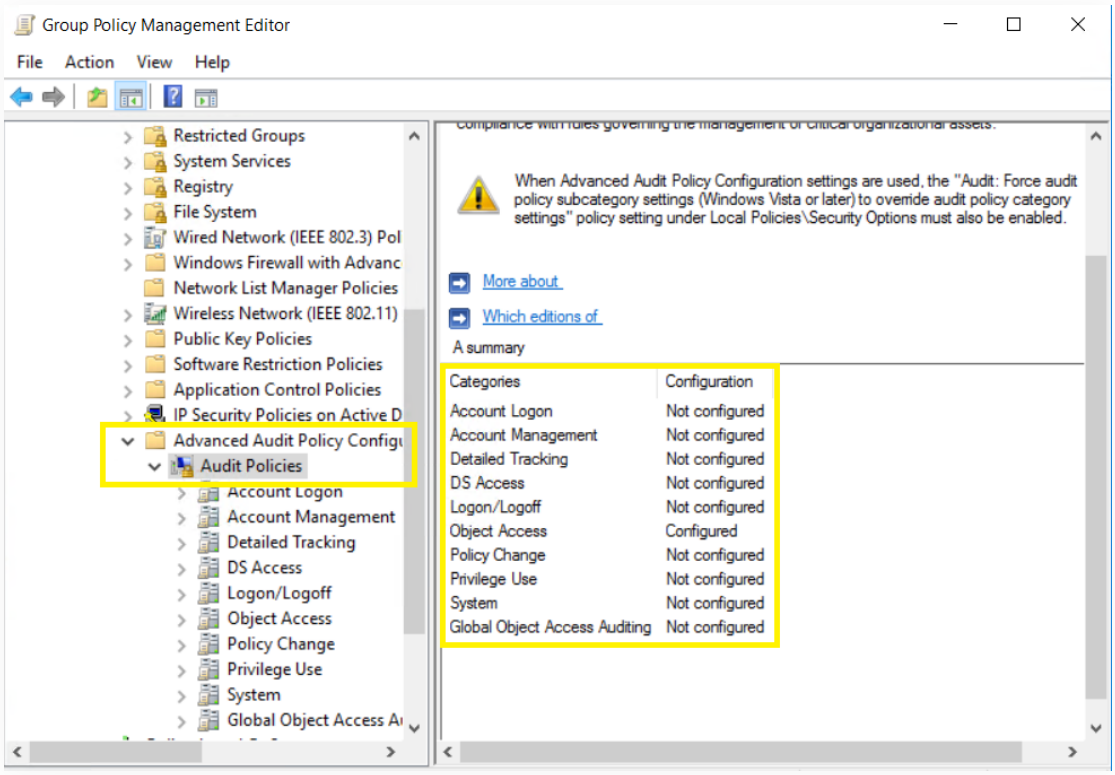
3.2.2 Configure advanced audit policies

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

1. To set this up, edit **<ADAuditPlusFSPolicy>** by right-clicking on the policy and selecting **Edit.**

2. Navigate to **Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration,** and configure the following settings.

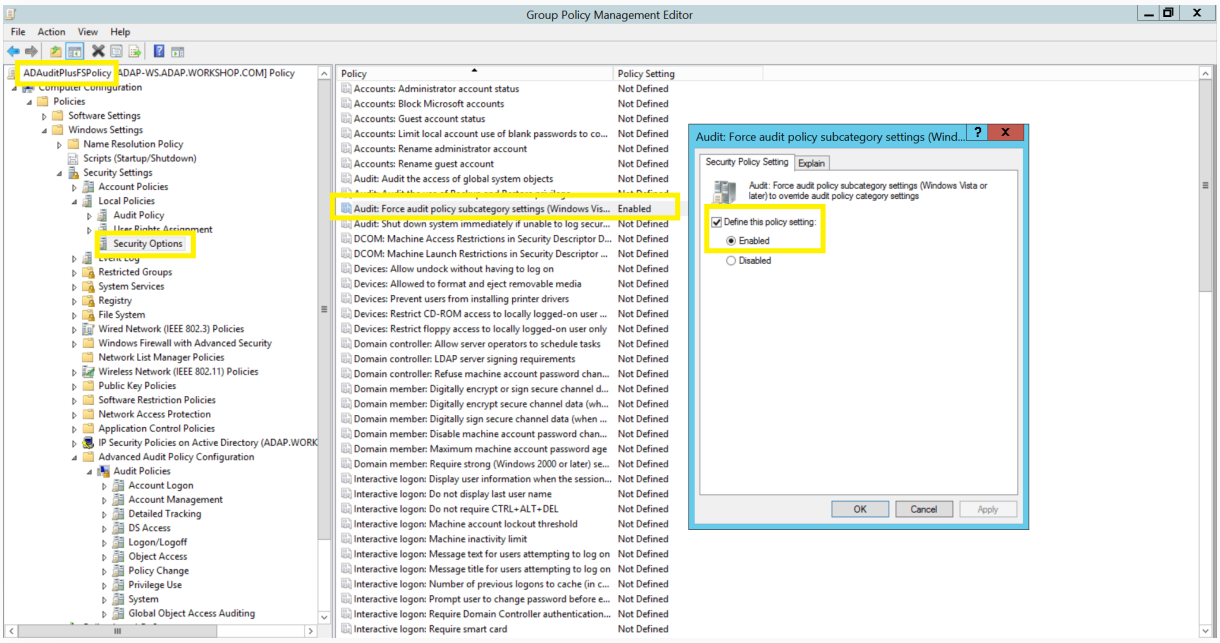
Cateogory	Sub Category	Audit Events	Purpose
Object Access	✓ Audit File System ✓ Audit File Share ✓ Audit Handle Manipulation	Success, Failure Success Success, Failure	✓ File share auditing
Policy Change	✓ Audit Policy Change ✓ Authorization Policy Change	Success, Failure Success	✓ File permission change auditing



3.2.3 Force advanced audit policies

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

1. Enable Force audit policy subcategory settings in **<ADAuditPlusFSPolicy>.**
2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Polices > Security Options > Audit: Force audit policy subcategory settings** (Windows Vista or later) to override the audit policy category settings.

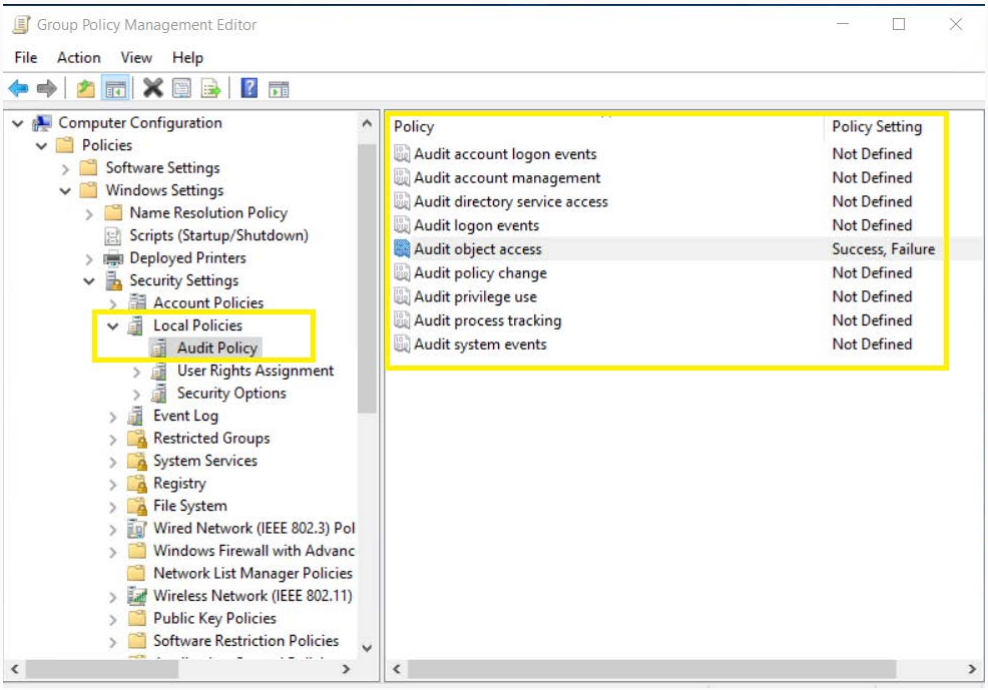


3.2.4 Configure legacy audit policies

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. To set this up, edit **<ADAuditPlusFSPolicy>** by right-clicking on the policy and selecting **Edit.**
2. Navigate to **Configuration > Windows Settings > Security Settings > Audit Policy Configuration,** and configure the following settings.

Cateogory	Audit events	Purpose
Object Access	✓ Success, Failure	✓ File share auditing ✓ File integrity monitoring ✓ File permission change auditing



4. Configure object-level auditing

To audit file and folder access, corresponding object-level auditing must be applied to shared folders. This can be achieved in two ways:

1. Automatic configuration
2. Manual configuration

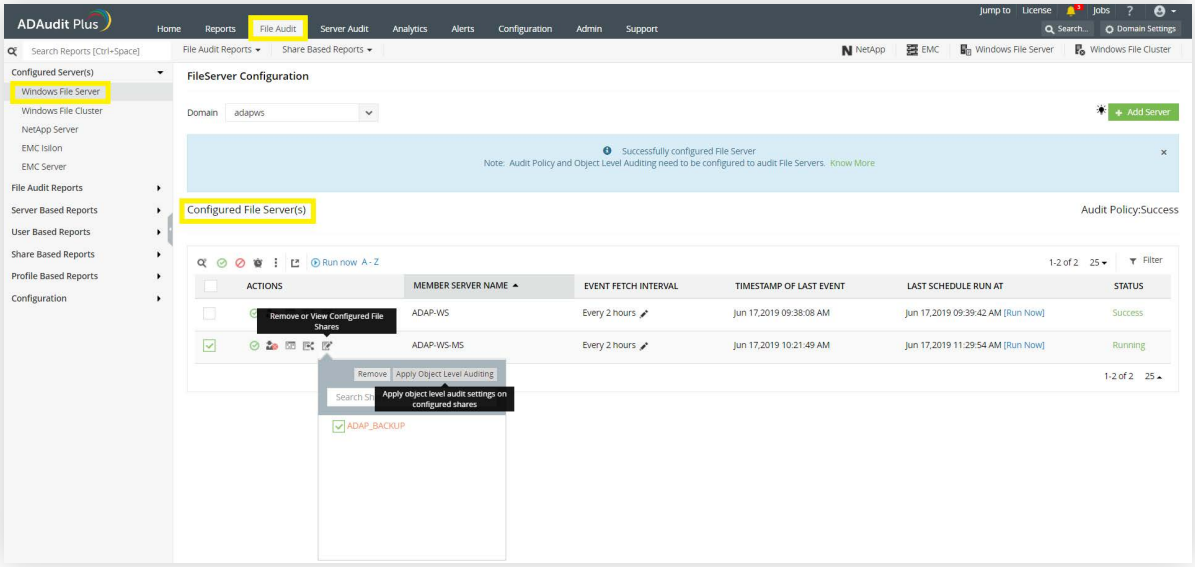
4.1 Automatic configuration

1. Log in to ADAudit Plus' web console → Go to the **File Audit** tab in the top menu → Click on **Windows File Server** under Configured Server(s) in the left pane.
2. Click on the **Remove or View Configured File Shares** icon corresponding to the file server you're looking to configure object-level auditing for in the list of servers → Select the respectiv shares, and click **Apply object-level audit settings on configured shares** (found at the top right corner).

Color codes:

Hover the cursor over the share to see the error code.

- Green—Object-level auditing is set correctly.
- Red—Object-level auditing is not set correctly or an error occurred during the configuration.
- Orange—Object-level auditing configuration is in progress.



4.2 Manual configuration

4.2.1 Using Windows shares

Right-click on the **share folder** that you want to audit, select **Properties,** and then click on the **Security** tab → Select **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 sub folders and files • Delete	This Folder, sub folders, and files
Folder permission and owner changes	Everyone	Success, Failure	• Take ownership • Change permissions	This folder and sub folders
File read	Everyone	Success, Failure	• List folder / Read data	Files only
Folder read failure	Everyone	Failure	• List folder / Read data	This folder and sub folders

4.2.2 Using PowerShell cmdlets

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

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

   Example:

   \\SERVERNAME\folder,FA

   C:\test folder,FA

Nots: 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	**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 sub-folder 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
-username	**DOMAIN_NAME\username** of the user with privilege over the file or folder to set the object-level auditing settings. (No cross-domain support)	no

Note:

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

For example:

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

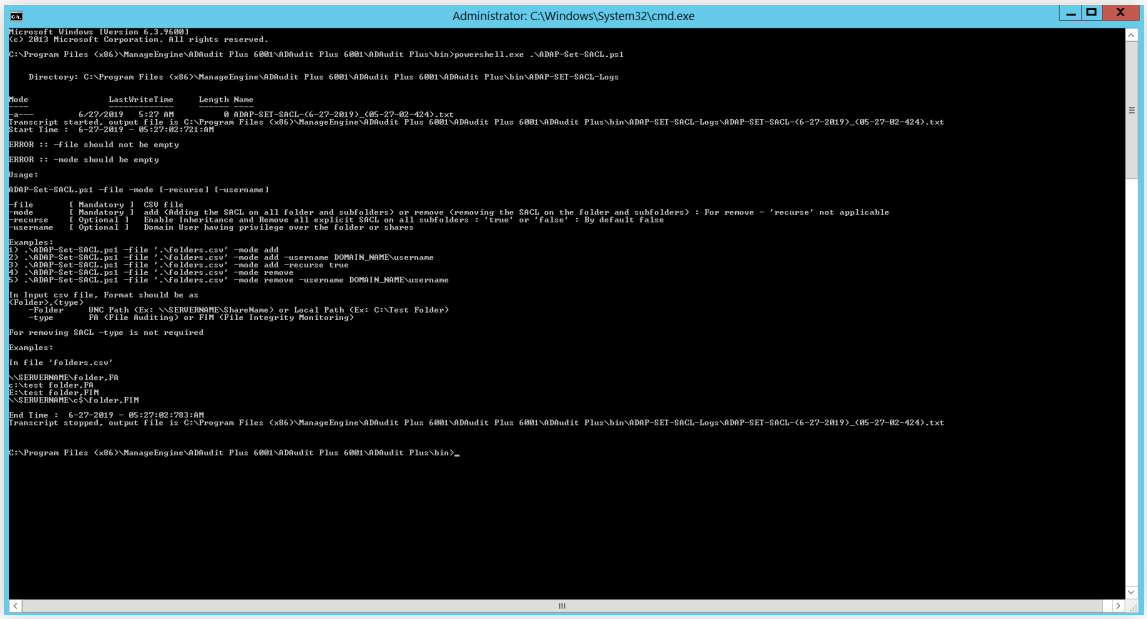
  .\ADAP-Set-SACL.ps1 -file '.\shared_folders_list.CSV' -mode add

- To replace all sub-folder object-level auditing settings with inheritable auditing settings applied to the shared_folders_list.CSV file, use:

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

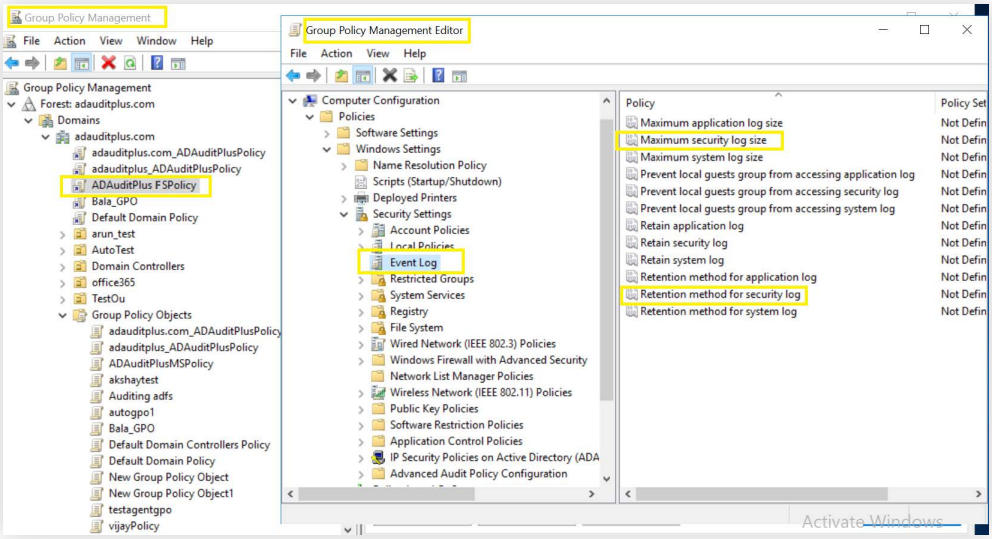
- To remove object-level auditing for the list of folders in the shared_folders_list.CSV file, use:

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



5. Configure security log size and retention settings

1. Open **GPMC** → Edit the **<ADAuditPlusFSPolicy>** GPO → Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Event Log.**
2. Configure **Retention method for security log** to **Overwrite Events As Needed.**
3. Configure the **Maximum security log** size as defined below. Ensure that the security log can hold a minimum of **12 hours** worth of data.

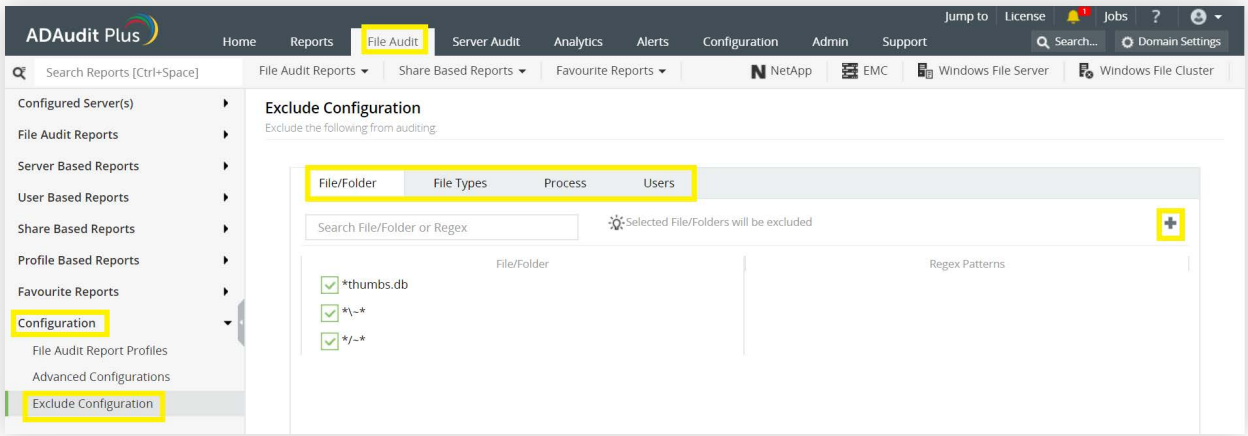


Role	Operating System	Size
Windows File Server	Windows Server 2003	512MB
Windows File Server	Windows Server 2008 and above	4096MB

6. Exclude configuration

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

Log in to ADAudit Plus' web console → Go to the **File Audit** tab, navigate to the left pane, click on **Configuration** and then on **Excude Configuration** → Choose to exclude by **File/Folder** local path, **File Type, Process Name,** or Users → Click on '+', and configure the necessary settings.



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

Objective	To exclude a folder and all of its subfolders and files	
Objective	**Share path**	**Local path**
	\\SERVER_NAME\share_name	c:\sharefolder
Path of folder that is to be excluded	c:\sharefolder\excludefolder	
File/Folder or Regex Patterns	File/Folder Patterns	
Syntax	• c:\sharefolder\excludefolder • c:\sharefolder\excludefolder*	
What will get excluded	• c:\sharefolder\excludefolder • c:\sharefolder\excludefolder\folder • c:\sharefolder\excludefolder\files.txt • c:\sharefolder\excludefolder\folder\files.txt	
What won"t get excluded		

Objective	To exclude "AppData" folder for every user profile
Share and folder path	\\SERVER_NAME\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 get excluded	• C:\Users\user1\AppData • C:\Users\user2\AppData • C:\Users\user1\AppData\subfolder • C:\Users\user2\AppData\subfolder
What won"t get excluded	• C:\Users\user1\subfolder\AppData • C:\Users\user2\subfolder\AppData

Objective	To exclude files from a specific folder but audit all subfolders and its contents
Share and folder path	\\SERVER_NAME\share_name c:\sharefolder
Path of folder that is to be excluded	c:\sharefolder\excludefolder
File/Folder or Regex Patterns	Regex Patterns
Syntax	^c:\\sharefolder\\excludefolder\\[^\\]*\.[^\\]*$
What will get excluded	• c:\sharefolder\excludefolder\file.txt • c:\sharefolder\excludefolder\folder.withDot
What won"t get excluded	• c:\sharefolder\excludefolder • c:\sharefolder\excludefolder\folderWithoutDot • c:\sharefolder\excludefolder\folderWithoutDot\subfolder • c:\sharefolder\excludefolder\folderWithoutDot\testfile.txt • c:\sharefolder\excludefolder\folder.withDot\subfolder • c:\sharefolder\excludefolder\folder.withDot\testfile.txt

7. File Analysis in ADAudit Plus

Overview

File Analysis uses metadata and disk space scans to provide critical insights into file server security and storage aspects. It is a component of ManageEngine's data visibility and security platform, DataSecurity Plus. The File Analysis module within ADAudit Plus lets you scan up to 200,000 files to gain file storage insights.To try out all File Analysis features, you can download a free, fully functional, 30-day trial here.

Supported Windows server versions

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

Reports available for preview in ADAudit Plus

- All Files
- Old Files
- Stale Files
- Unmodified Files
- Hidden Files

How to set up File Analysis in ADAudit Plus

The preview version of File Analysis will automatically scan up to 200, 000 files configured in ADAudit Plus for file server auditing. Scan data for these files will be retained and processed to be presented in reports. To scan more files and try all File Analysis features, you can download a fully functional, 30-day trial here.

You can specify the files you want File Analysis to scan by editing the file shares configured at **File Analysis > Configuration > Windows File Server.** Specify the number of days that indicate the age or the last access time of the files you wish to report by navigating to **File Analysis > Configuration > Report Configuration.**

8. Troubleshooting

1. **How to check if the audit polices and the security log settings have been applied on the monitored computers:**

   Log in to **any computer with domain IT admin privileges** → Run **Command Prompt** as an administrator → Type **gpresult /S <monitored computer> /F /H <file name>.HTML** → Navigate to **C:\Users\<logged in user>\<file name.HTML>** to check if all the audit policy settings and security logs settings are in place.

2. **How to check if object-level auditing settings are in place:**

   Refer to section four (4) found in this document.

3. **How to verify that the events are present in the monitored computers:**

   Log in to **any computer with domain admin privileges** → Go to **Run,** and type **eventvwr.msc** → Right-click on **Event Viewer,** and connect to the target computer → Check if the corresponding event numbers are present.