ManageEngine) ADAudit Plus

Windows file server auditing guide



www.adauditplus.com

Table of Contents

Overview	3
1. Supported systems	3
2. Configure Windows file servers in ADAudit Plus	4
2.1 One server at a time	4
2.2 In bulk	5
3. Configure audit policies in your domain	6
3.1 Automatic configuration	6
3.2 Manual configuration	6
3.2.1 Configure list of Windows file servers to be audited	6
3.2.2 Configure advanced audit policies	7
3.2.3 Force advanced audit policies	8
3.2.4 Configure legacy audit policies	9
4. Configure object-level auditing	10
4.1 Automatic configuration	10
4.2 Manual configuration	11
4.2.1 Using Windows shares	11
4.2.2 Using PowerShell cmdlets	12
5. Configure security log size and retention settings	13
6. Exclude configuration	14
7. File Analysis in ADAudit Plus	17
8. Troubleshooting	18

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. \rightarrow Click on the **File Audit tab** \rightarrow Select **Windows File Server** from under the **Configured Server(s)** drop-down list \rightarrow Click on **Add Server** \rightarrow 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.

Search Reports (Ctrl+Space)	Home	Reports	File Audit	Server Audit	Analytics Alerts Configuration	Admin Support	~	Q Search	O Domain Sett Windows File Clus
figured Server(s)	-	FileSen	Add File Ser	vers			^	in a second s	
Vindows File Server			Select Se	rver	2 Select Share(s)	3 Review Summary			
Vindows File Cluster		Domain							🐐 🕂 Add Sei
NetApp Server		Configu	q				1-4 of 4 25 🗸 🤨	🏟 Au	idit Policy Config
MC Server				NAME	CANONICAL NAME				
Audit Reports	•	a e	0	ADAP-WS	adap.workshop.com/Domain Conti	rollers/ADAP-WS		1-1 of 1	25 🗸 🕆 Filt
ver Based Reports	1		۲	ADAP-WS-MS	adap.workshop.com/Laps/ADAP-W	S-MS		HEDULE RUN AT	STATUS
r Based Reports	1		0	DSP-WS	adap.workshop.com/Computers/D	SP-WS		019 01:39:41 PM:[Run Now]	
file Based Reports			0	ES-DC1	adap workshop com/Computers/F	S-DC1			1-1 of 1 25
figuration	•		0						
					internet internet				
					Quit Nex	at .			

2.2 In bulk

To configure Windows file servers in bulk:

 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

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.cs**v -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 \rightarrow Click on the File Audit tab \rightarrow Select Windows File Server from under the Configured Server(s) drop-down list \rightarrow 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.

											Jump to License	: •	Jobs	? 🛛 -
	Home	Reports	File Audit	Server Audit	Analytics A	lerts Confi	iguration Admin	Support		-		λ Search.	- 01	bomain Settings
Search Reports [Ctrl+Space]	Fil	a Audit Repo	.rts ♥ Share E	3ased Reports 👻					N NetApp	EMC	Windows File Serve	r Fe	, Windov	/s File Cluster
Configured Server(s)		ileServer	Configuration											
Windows File Server														
Windows File Cluster	1	iomain a	dapws	×.									*	Add Server
NetApp Server	C	onfigured	l File Server(s)									ð	Audit Pol	ior:Configure
EMC Isilon												-		ey een myere
EMC Server														
ile Audit Reports	•	Q 0 0) 🕸 i 🗈	Run now A - Z								1.1 of 1	25 -	▼ Filter
erver Based Reports			ACTIONS		MEMBER SERVER	NAME +	EVENT FETCH INTER	RVAL	TIMESTAMP OF LAST EVENT	LAS	ST SCHEDULE RUN AT			STATUS
erver Based Reports Iser Based Reports				12	MEMBER SERVER	NAME 🔺	EVENT FETCH INTER	RVAL	TIMESTAMP OF LAST EVENT	LAS	ST SCHEDULE RUN AT	n Nowl		STATUS
erver Based Reports Iser Based Reports hare Based Reports			actions ightarrow 🙋 🔯 📧	2	MEMBER SERVER	NAME 🔺	EVENT FETCH INTER	RVAL	TIMESTAMP OF LAST EVENT Jun 12,2019 01:35:12 PM	LAS	5T SCHEDULE RUN AT 12,2019 01:39:41 PM [Ru	in Now]		STATUS Success
Server Based Reports Jser Based Reports ihare Based Reports 'rofile Based Reports	1		actions 🥝 🏜 📼 📧	B ,	MEMBER SERVER	NAME 🔺	EVENT FETCH INTER	RVAL	TIMESTAMP OF LAST EVENT	LAS Jun	5T SCHEDULE RUN AT 12,2019 01:39:41 PM [RL	in Now]	1-1	STATUS Success

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.**
- 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**.

Group Policy Management				- 🗆 X
File Action View Window Help				- 8 >
Group Policy Management A Forest: adapworkshop.com Commins A ADAudit Plus Permission GPO ADAudit Plus Permission GPO	ADAuditPlusFSPolicy Scope Details Settings Deleg Links Display links in this location: The full integration of the set of	adapworkshop.com		~
ADAuditPlusMSPolicy ADAuditPlusWSPolicy Default Domain Policy demoGPO	Location	Enforced No	Link Enabled Yes	Path adapworkshop.com
in rithGPO in S1 in Test1 in testfeb3 in testfeb3	<			>
in vijayPolicy if vijayPolicy if vijayPolicy if Abi if Design_Test if Domain Controllers if Fart	The settings in this GPO can only a Name	Apply to the following groups, us	ers, and computers	
 is firstOU is firstOU is haniy users is my computers is NewOU 	Add Re	ernove Properties		
> 🗃 rithOU > 🗃 SharmillaOU > 🗃 SharmillaOU1 > 🗃 Special OU	WMI Filtering This GPO is linked to the following <none></none>	j WMI filter: ∽	Open	

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.
- 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 	Success, Failure	 File share auditing
	 Audit File Share 	Success	
	 Audit Handle Manipulation 	Success, Failure	
Policy Change	 Audit Policy Change 	Success, Failure	 File permission
	 Authorization Policy Change 	Success	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>.
- 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.
- 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

Group Policy Management Editor	- <u> </u>	×	
File Action View Help			
	 Policy Audit account logon events Audit directory service a Audit logon events Audit object access Audit policy change Audit privilege use Audit process tracking Audit system events 	Policy Setting rents Not Defined access Not Defined Not Defined Success, Failure Not Defined Not Defined Not Defined Not Defined	
S	×		2

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

- 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.

ADAudit Plus	Home	Reports File Audit Server Audit Ar	alytics Alerts Configuration	Admin Support		Jump to License Q, Se	🐥 ³ Jobs ? 🙆 🗸 harch 🏠 Domain Settings
♥ Search Reports [Ctrl+Space]		File Audit Reports 👻 Share Based Reports 👻			N NetApp	🚟 EMC 🛛 🖥 Windows File Server	Nindows File Cluster
Configured Server(s)	-	FileServer Configuration					
Windows File Server							
Windows File Cluster NetApp Server		Domain adapws 🗸					🗰 🔸 Add Server
EMC Isilon EMC Server			Note: Audit Policy and	Successfully configured Fi d Object Level Auditing need to be confi	le Server gured to audit File Servers. Know More		×
File Audit Reports							
Server Based Reports	1	Configured File Server(s)					Audit Policy:Success
User Based Reports	1						
Share Based Reports	,	🔍 🥝 🖉 😧 🔝 🕲 Run now A - Z				1-2 :	of 2 25 - TFilter
Profile Based Reports	•	ACTIONS	MEMBER SERVER NAME	EVENT FETCH INTERVAL	TIMESTAMP OF LAST EVENT	LAST SCHEDULE RUN AT	STATUS
Configuration	•	Remove or View Configured File Shares	ADAP-WS	Every 2 hours 🖌	Jun 17,2019 09:38:08 AM	Jun 17,2019 09:39:42 AM [Run Now]	Success
		✓ Ø 20 K K	ADAP-WS-MS	Every 2 hours 🖌	Jun 17,2019 10:21:49 AM	Jun 17,2019 11:29:54 AM [Run Now]	Running
		Remove A	pply Object Level Auditing				1-2 of 2 25 🔺
		search Sn 1012	configured shares				
		ADAP_BACKU	P.II				

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 \rightarrow Select **Advanced**, and then click on the **Auditing** tab \rightarrow For the **Everyone** group, add the following entries:

	Principal	Туре	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

Administrator: C/Windows/System32/cmd.exe	_ 🗆 🗙
Hiersaft Window (Dersion 5.3.5400)	<u>^</u>
C:\Fregram Files (x86)\ManageEngine\MDMudit Plus 6001\MDMudit Plus 6001\MDMudit Plus\bin>powershell.exe .\MDMP-Set=8ACL.ps1	
birectory: C:Vrogram Files (s86)ManageEngineMDAudit Flus 6081MDAudit Flus 6081MDAudit Flus SchrMDAr-EET-SACE-Logs	
Mode LastWriteFine Length Name	
-a 6/27/2019 5:27 AM 8 ADAP-SET-SACL-(6-27-2019)_(05-27-02-024)_txt Transcript started, output file is C:VProgram Files (x06)ManageEnginxVADMudit Plus 6001/ADAudit Plus/bin/ADAP-SET-SACL-Logs/ADAP-SET-SACL-(6-27-2019)_(25-27-02-024)_txt Start fine : 6-27-2019 - 65:27:27:11AM	≡
ERROR :: -file should not be empty	
ERROR :: -mode should be empty	
Jage :	
MDRP-Set-SACL-ps1 -file -mode (-recurse) (-username)	
-file [Mandatory] GSU file recurse [Onclatory] add (ddsing the SACL on all folder and subfolders) or renove (renoving the SACL on the folder and subfolders) : For renove - 'recurse' not applicable recurse [Optional] bankle inheritance and Renove all explicit SACL on all subfolders : 'trum' or 'falss' : By default false username [Optional] banklin ber having privilege over the folder or have sets dders : 'trum' or 'falss' : By default false	
Examples: D xmBFS: D xMBFS:=CHCR:psi = file 'Xelafor:es' =made add D xMBFS:=CHCR:psi = file 'Xelafor:es' =made add =username DOWIN.MMFSusername D xMBFS:=CHCR:psi = file 'Xelafor:es' =made add =username DOWIN.MMFSusername D xMBFS:=CHCR:psi = file 'Xelafor:es' =made add =username DOWIN.MMFSusername	
h laput seu file. Format should be as Foldery. Luga UNC Reth (52: VSRUDRMMRS)anvName) op Lacal Path (52: C:Vest Folder) -Tolder UNC Teth (52: VSRUDRMRS)anvName) or STA (File Integrity Monitoring)	
For renoving SACL -type is not required	
Examples :	
In file 'folders.csu'	
N SEBUDINMENT of Iden - FM Extest Folder - FM Extest Folder - FIM	
End Time : 6-27-2819 - 05:27:08:783-6H Transcript stopped, output file is C:Vprogram Files (x86)/ManageEnginer/ADMudit Plus 6001/ADMudit Plus 6001/ADMudit Plus/bin/ADMP-SET-SACL-Logs/ADMP-SET-SACL-(6-27-2019)_(05-27-02-424).txt	
C:\Program Files (x86)\ManageEngime\DBMudit Plus 6001\DBMudit Plus\6001\DBMudit Plus\bin>_	
	~
	×

5. Configure security log size and retention settings

- 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 \rightarrow Go to the **File Audit** tab, navigate to the left pane, click on **Configuration** and then on **Excude Configuration** \rightarrow Choose to exclude by **File/Folder** local path, **File Type, Process Name,** or Users \rightarrow Click on '+', and configure the necessary settings.

ADAudit Plus	Home	Reports	File Audit	Server Audit	Analytics	Alerts	Configuration	Admin Suj	Jump to License	📮 Jobs ? 😔 ▾ Search Ŏ Domain Settings
Q Search Reports [Ctrl+Space]		File Audit Reports	Share	e Based Reports 👻	Favourite	e Reports 👻	NetA	op 🔄 🧱 EMC	Windows File Server	🐻 Windows File Cluster
Configured Server(s) File Audit Reports	•	Exclude Confi Exclude the followin	guration g from auditir	ıg.						
Server Based Reports User Based Reports Share Based Reports	* * *	File/Fold	ler File/Folder o	File Types	Process	Users	Folders will be exclud	ed		+
Profile Based Reports Favourite Reports	•	√ *th	umbs.db	File/Fo	lder				Regex Patterns	
Configuration File Audit Report Profiles	-	✓ *\-* ✓ */-*								
Advanced Configurations										

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.t; c:\sharefolder\excludefolder\folder 	xt \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	<pre>^c:\\sharefolder\\excludefolder\\[^\\]*\.[^\\]*\$</pre>
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, <u>DataSecurity Plus</u>. 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 <u>here</u>.

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 <u>here</u>.

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 \rightarrow Run Command Prompt as an administrator \rightarrow Type gpresult /S <monitored computer> /F /H <file name>.HTML \rightarrow 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.

- 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 \rightarrow Go to Run, and type eventvwr.msc \rightarrow Right-click on Event Viewer, and connect to the target computer \rightarrow Check if the corresponding event numbers are present.

ManageEngine) ADAudit Plus

ManageEngine ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Active Directory, Azure AD, Windows servers, and workstations secure and compliant.