ManageEngine
ADAudit Plus

Configuring Synology NAS auditing in ADAudit Plus

www.adauditplus.com

Overview

A Synology DiskStation is a network-attached storage (NAS) drive running the DiskStation Manager (DSM) OS. ADAudit Plus, real-time change auditing and user behavior analytics software, audits file accesses and modifications in Synology NAS devices to ensure IT compliance with regulations like HIPAA, FISMA, GDPR, and SOX.

Benefits of auditing your Synology DiskStation NAS with ADAudit Plus

To ensure the safety of business-critical files and folders, ADAudit Plus provides comprehensive reports on every file create, read, write, modify, move, rename, and delete event, with details such as:

- Who made the change
- Which file was changed
- When the change was made
- Where the change was made

With ADAudit Plus, you can:

- Track accesses and changes to shares, files, and folders.
- View information on the user and origin IP address of every file action.
- Receive periodic access audit reports in your inbox.
- Meet the requirements of HIPAA, GLBA, SOX, PCI DSS, ISO 27001, FISMA, GDPR, and other IT regulations.

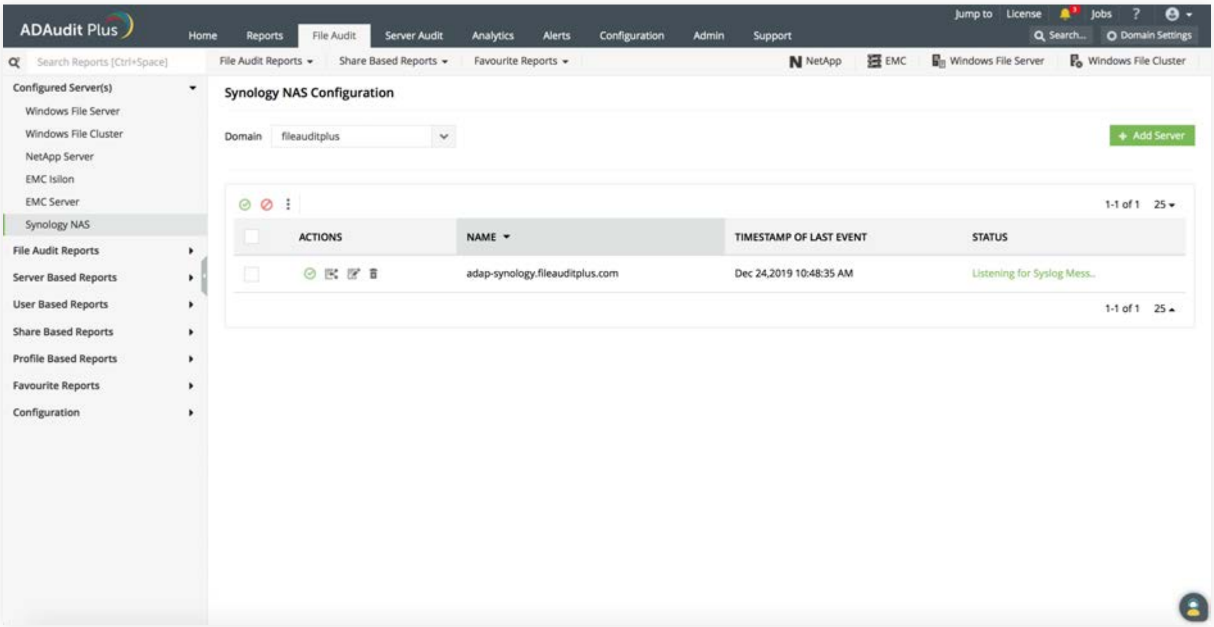
Supported DSM versions: DSM 5.0 and above

Configuring Synology NAS auditing

This article describes the steps to add a Synology NAS device and configure it to send logs to ADAudit Plus.

Adding DiskStation servers

1. Log in to the ADAudit Plus web console. Navigate to the **File Audit** tab > **Configured Server(s)** > **Synology NAS**. Click **Add Server** in the top-right corner.



Synology NAS Configuration

Domain: fileauditplus

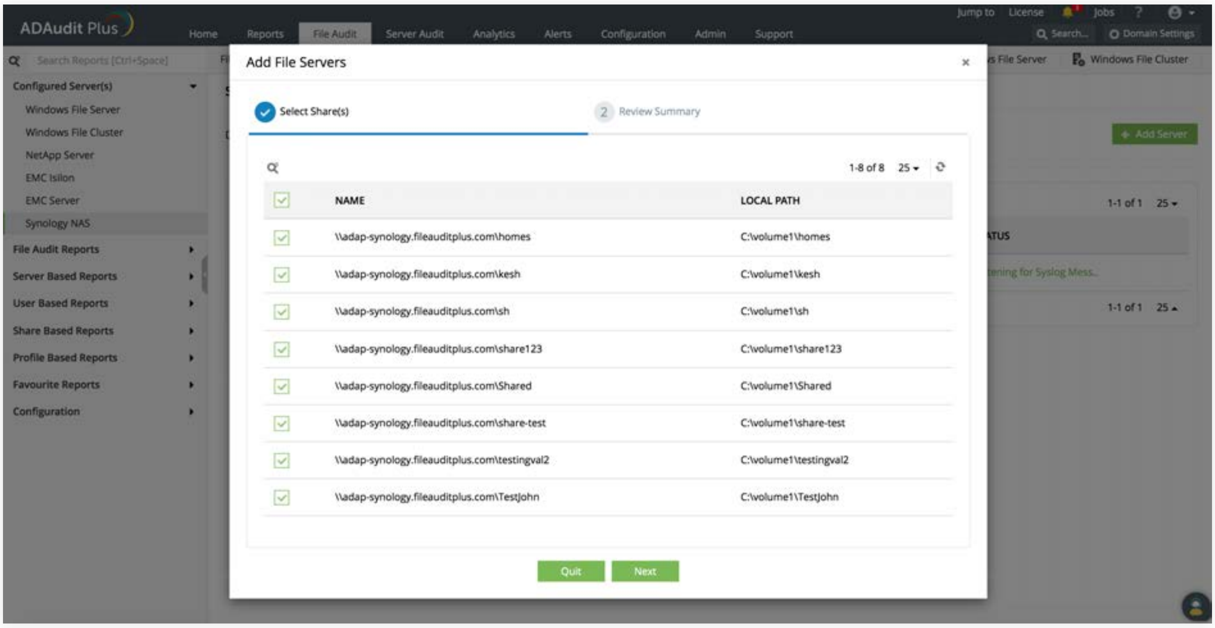
1-1 of 1 25

ACTIONS	NAME	TIMESTAMP OF LAST EVENT	STATUS
	adap-synology.fileauditplus.com	Dec 24,2019 10:48:35 AM	Listening for Syslog Mess...

1-1 of 1 25

2. Enter the name of the Synology device to be configured, and click **Next.**

3. Select the shares to be monitored with ADAudit Plus, and click **Next.**



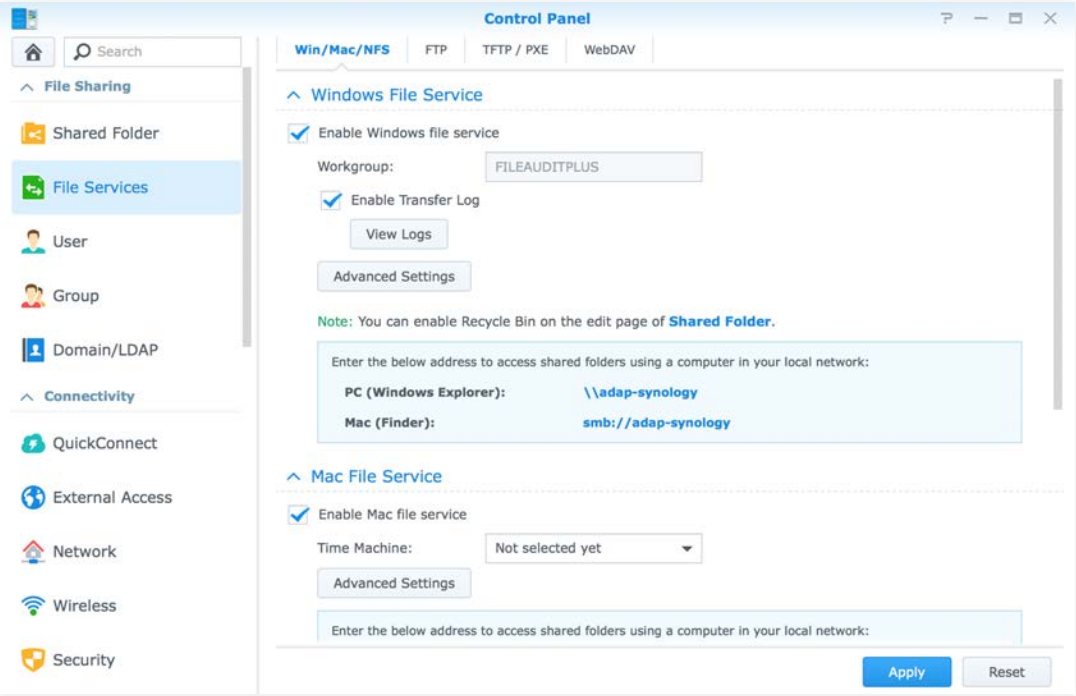
Add File Servers

1-8 of 8 25

☑	NAME	LOCAL PATH
☑	\\adap-synology.fileauditplus.com\homes	C:\volume1\homes
☑	\\adap-synology.fileauditplus.com\kesh	C:\volume1\kesh
☑	\\adap-synology.fileauditplus.com\sh	C:\volume1\sh
☑	\\adap-synology.fileauditplus.com\share123	C:\volume1\share123
☑	\\adap-synology.fileauditplus.com\Shared	C:\volume1\Shared
☑	\\adap-synology.fileauditplus.com\share-test	C:\volume1\share-test
☑	\\adap-synology.fileauditplus.com\testingval2	C:\volume1\testingval2
☑	\\adap-synology.fileauditplus.com\TestJohn	C:\volume1\TestJohn

Setting up log forwarding

1. In the **Synology DiskStation Manager,** open the **Control Panel,** navigate to **File Services,** and select **Enable Transfer Log.**



☑ Enable Windows file service

Workgroup: FILEAUDITPLUS

☑ Enable Transfer Log

Note: You can enable Recycle Bin on the edit page of Shared Folder.

Enter the below address to access shared folders using a computer in your local network:

PC (Windows Explorer): \\adap-synology

Mac (Finder): smb://adap-synology

☑ Enable Mac file service

Time Machine: Not selected yet

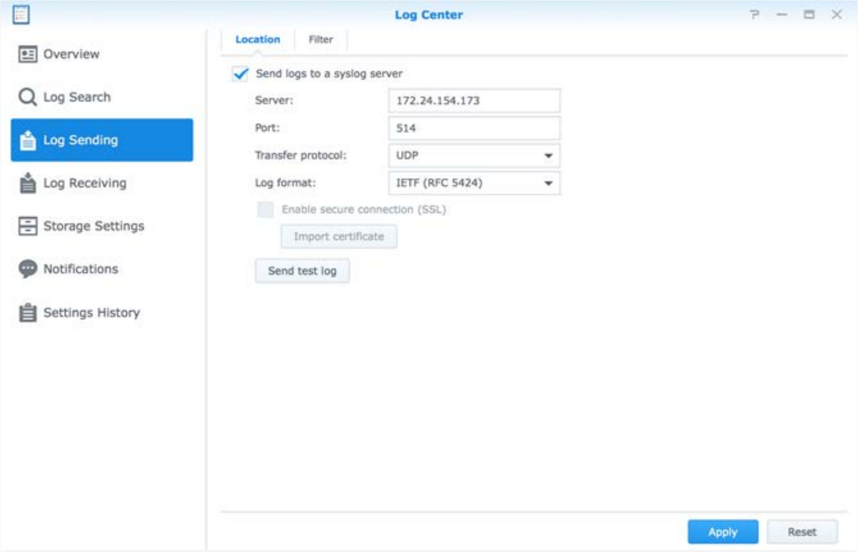
Enter the below address to access shared folders using a computer in your local network:

2. Open the **Log Center** and navigate to **Log Sending.** Select **Send logs to a syslog server.**

3. Provide the name of the target server and the syslog port number that ADAudit Plus is listening to.

4. Set the log format to **IETF (RFC 5424).**

5. Click **Apply.**



☑ Send logs to a syslog server

Server: 172.24.154.173

Port: 514

Transfer protocol: UDP

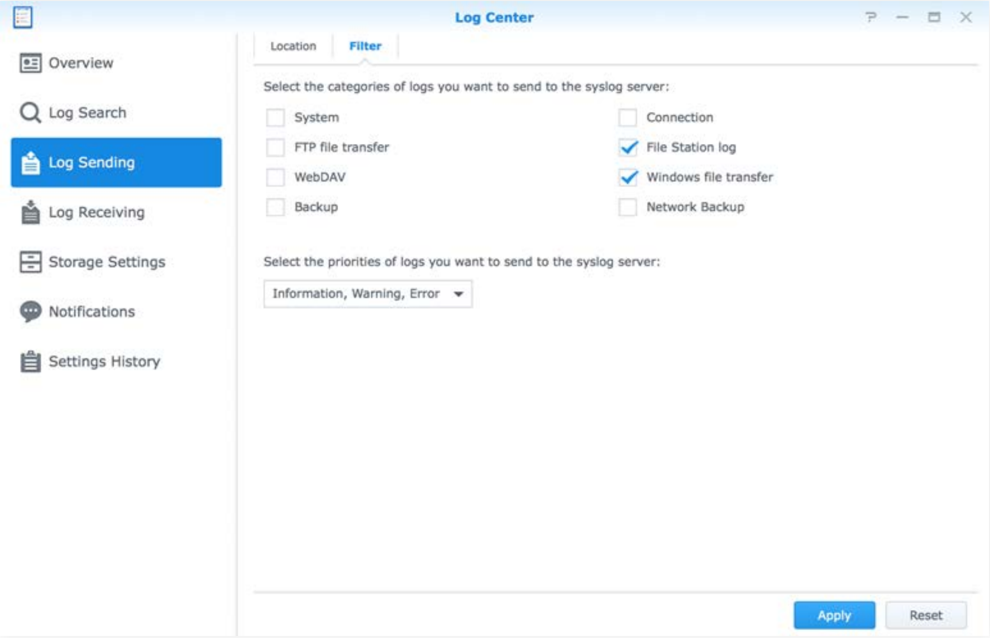
Log format: IETF (RFC 5424)

□ Enable secure connection (SSL)

Note: By default, port 514 is configured as ADAudit Plus' Syslog Listening Port. This can be changed under **Admin > General Settings > Connection.**

6. Under the **Filter** tab, ensure that the following filters are selected:

- File Station log
- Windows file transfer



Select the categories of logs you want to send to the syslog server:

□ System
□ FTP file transfer
□ WebDAV
□ Backup
□ Connection
☑ File Station log
☑ Windows file transfer
□ Network Backup

Select the priorities of logs you want to send to the syslog server:

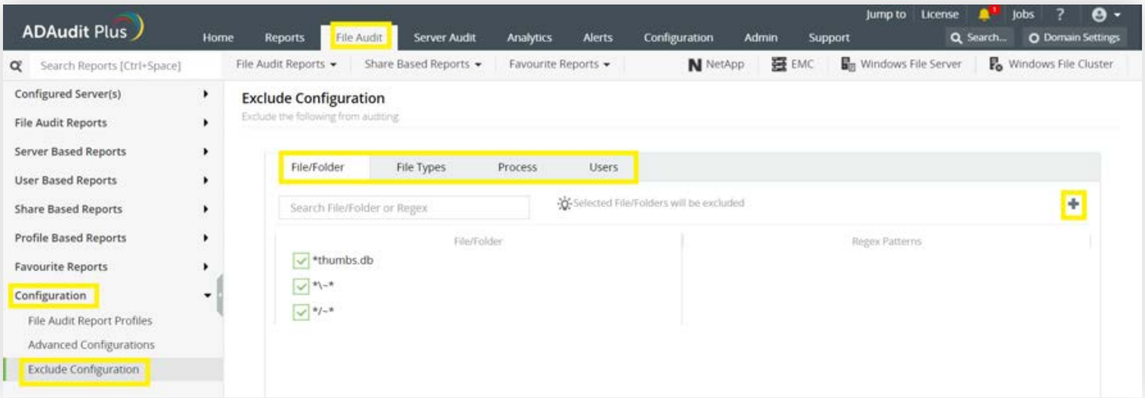
Information, Warning, Error

Excluding files and folders from auditing

Learn more about ADAudit Plus' Exclude Configuration feature.

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.



Exclude Configuration

Exclude the following from auditing

Selected File/Folders will be excluded

File/Folder	Regex Patterns
☑ *thumbs.db	
☑ *\~*	
☑ */~*	

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

Troubleshooting

How to verify if the port number configured for Log Sending and ADAudit Plus' Syslog Listening Port are the same:

1. In ADAudit Plus' web console, navigate to **Admin > General Settings > Connection** to view the port number being used by ADAudit Plus.

2. In Synology DSM, navigate to **Log Center > Log Sending** and verify if the same port number is provided.