ManageEngine
ADAudit Plus

Removable storage auditing configuration guide

www.adauditplus.com

Document summary

ADAudit Plus monitors and reports on the use of removable storage devices in a network, including USB flash drives, external hard drives, mobile phones, CDs, DVDs, micro-SD cards, WPD devices, etc.

With ADAudit Plus' removable storage auditing feature, you can:

- Detect when USB devices are plugged in to devices in your network
- Track file accesses and modifications in USB devices
- Monitor and report on files that were copied and pasted to and from USBs
- Ensure compliance with IT regulations like HIPAA and GDPR

Depending on the Windows OS version, the following events pertaining to removable storage devices can be audited and reported on by ADAudit Plus:

- File Read
- File Modified
- File Copy and Paste
- Removable Device Plug In

Note: The first three events can be audited on Windows 8 and above, and Windows Server 2012 and above. Auditing for Removable Device Plug In is only available for Windows 10/Windows server 2016 and above.

Difference between agent-based and agentless mode of removable device auditing.

It is strongly recommended to opt for agent-based removable storage device auditing over the agentless mode. The table below highlights the difference between the modes and elucidates why the agent-based mode is preferable.

	Agent-based	Agentless
The *USB name* value is displayed in the reports generated.	✓ The agent keeps track of all external storage devices plugged in and correlates USB details with the event data collected to display the *USB name* value.	✗
Auditing events when the object name includes the drive letter.	✓	✗

This guide takes you through the process of setting up USB Storage Auditing in ADAudit Plus and configuring your audit policies for complete visibility into file actions in removable storage devices.

1. Configuring ADAudit Plus to audit removable storage devices

Audit all USB plugins and file activities in removable storage devices for all configured Windows domain controllers, servers, and workstations using the supported OS versions.

1.1 Configuring Windows domain controllers

To add and set up audit policies for Windows domain controller auditing, follow the steps in this guide.

Note: While configuring the advanced audit policies for Windows domain controllers, ensure that the below audit category is enabled:

Category	Subcategory	Audit events
Object Access	• Audit Removable Storage	✓ Success and Failure

1.2 Configuring Windows servers

To add and set up audit policies for real-time Windows server auditing and change analytics, follow the steps in this guide.

Note: While configuring the advanced audit policies for Windows servers, ensure that the below audit category is enabled:

Category	Subcategory	Audit events
Object Access	• Audit Removable Storage	✓ Success and Failure

1.3 Configuring workstations

To add and configure audit policies for workstation auditing, follow the steps in this guide.

Note: While configuring the audit policies for workstations, ensure that the below audit category is enabled:

Category	Subcategory	Audit events
Object Access	• Audit Removable Storage	✓ Success and Failure

2. Tips for troubleshooting when events are not reported

2.1 Verify whether the desired audit policies and security log settings are configured

1. Using domain admin credentials, log in to any computer that has the Group Policy Management Console (GPMC) on it.
2. Open the **GPMC**, right-click on **Group Policy Results**, then select **Group Policy Results Wizard.** Select the **computer,** and then the **user** (current user).
3. Verify that the desired settings are configured.

2.2 Verify whether the desired object-level auditing settings are configured

1. Run through steps 1.1, 1.2, and 1.3 of this guide.

2.3 Verify whether the registry value of the HotplugSecureOpen is configured

1. Open **Registry Editor** in the target machine.
2. Ensure that the registry value of the *HotplugSecureOpen* is "1" (DWORD) in the below registry path.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Storage\HotplugSecureOpen

   Note: In case the *HotplugSecureOpen* key is not present, create a key (DWORD) and set it's value to "1".

2.4 Verify whether the desired events are getting logged

1. Log in to any **computer** with domain admin credentials.
2. Open **Run**, then type **eventvwr.msc**. Right-click on **Event Viewer.**
3. Connect to the **target computer**, then verify whether the below event IDs are getting logged under the Removable storage device category.

   a. **Event ID 4663:** Logs successful attempts to write to or read from a removable storage device.

   b. **Event ID 6416:** Logs removable device plugins.

3. View/edit audit actions for Removable Storage Audit

1. Log in to **ADAudit Plus' web console > Configuration tab > Configuration > Advanced Configurations.**
2. In the Category drop-down, select **Removable Storage Audit** and select the audit action you want to view/edit.

4. View/edit report profiles for Removable Storage Audit

1. Log in to **ADAudit Plus' web console > Configuration tab > Report Profiles > View/Modify Report Profiles.**
2. Choose your **domain** in the Domain drop-down.
3. In the *Category* drop-down, select **Removable Storage Audit**, then select the report profile you want to view/edit.