ManageEngine
ADAudit Plus

Windows workstation auditing guide

www.adauditplus.com

Table of Contents

1. Introduction

1.1 Overview

Auditing Windows workstations helps monitor and report on a user's logon and logoff information, their most productive hours, logon history details, and more. It helps monitor the usage of removable storage devices, instances of scheduled tasks, and process creation as well as termination. Monitor critical system, configuration, and program files for anomalous change events to ensure their integrity. Detect and respond to anomalous login activities that are indicative of malicious insiders by closely monitoring user login trends.

1.2 Benefits of Windows workstation auditing with ADAudit Plus

- Audit, monitor, and report on all users' local logon and logoff instances across Windows workstations.
- Measure your employees' productivity by monitoring their average work hours, idle time, and more.
- Monitor user actions across terminal services to analyze remote login activities.
- Track critical process creation and termination events with details on who initiated the action and when.
- Track, record, and maintain an audit trail of all users' login history details.
- Audit and report on the usage of removable storage such as USB devices.
- Monitor and report on Windows startup time, shutdown time, and the duration of each user's session on the workstation.
- Ensure file integrity by keeping track of changes made to system files, program files, and more.
- Gain instant visibility into changes made to your local administrator groups and user accounts, including creation, deletion, and account lockout activities.

1.3 Supported Windows workstation OS versions

ADAudit Plus can audit workstations running Windows 10, 8, 7, Vista and XP.

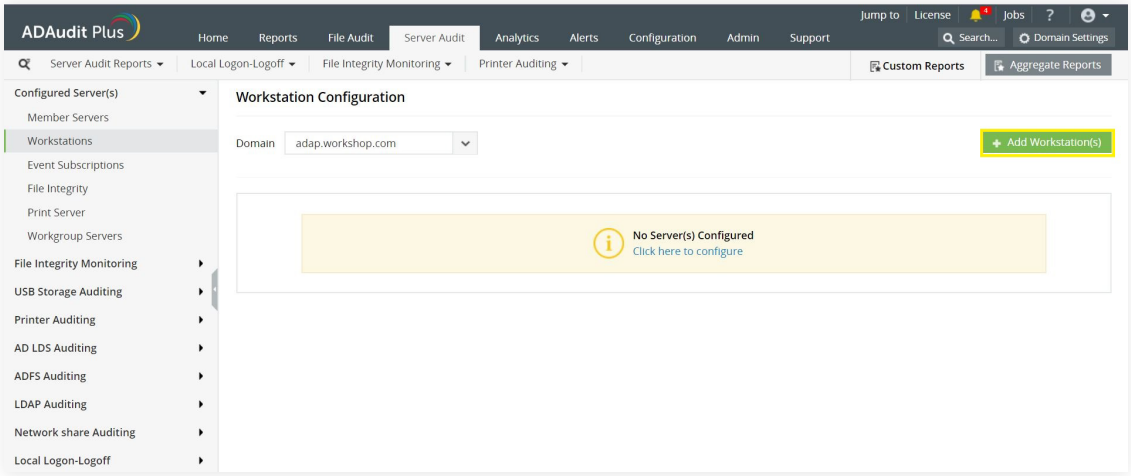
2. Configuring Windows workstations

ADAudit Plus workstation auditing uses a client-side agent for real-time data collection. The agent helps to easily scale across hundreds of workstations. Check out this guide for detailed instructions on how to install and configure the ADAudit Plus agent.

2.1 Using product console

Configure the desired workstations using the following steps:

1. Open ADAudit Plus.
2. Click **Server Audit** from the top menu.
3. Under **Configured Server(s)** in the left-hand menu, choose **Workstations**.
4. Choose the desired **domain** in the Domain drop-down.



5. Select **+ Add Workstation(s)** in the top-right corner.
6. Select the list of workstations to be monitored, then click **OK**.

2.2 Using command line arguments

Configure the desired workstations with command scripts using the following steps:

1. Log in to the system ADAudit Plus is installed.
2. Create a file in **<Installation dir>\ManageEngine\ADAudit Plus\bin\servers.csv**. Use the encoding tab and save the document in UTF-8 format.

3. Enter the workstation names separated by a comma in a newline and save the list as a .csv file.

   E.g. Test-WS1,

   Test-WS2,

   Test-WS3...,

4. Go to Start and type in "Command Prompt". Right-click Command Prompt, then select Run as administrator.

5. Navigate to the folder <Installation dir>\ManageEngine\ADAudit Plus\bin.

6. Open Command Prompt and type in "cmdUtil.bat".

7. Enter the ADAudit Plus default admin username and password.

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

8. Enter "server usage".

9. Type in "config server add -machinetype ws -isauditpolicy true".

Note: Here are the descriptions for the above arguments:

machinetype: The type of machine that's going to be added i.e., ws=workstations.

isauditpolicy: The audit policy will be enabled for the chosen machine via Group Policy Object (GPO).

true: Automatically configures the required object access policy.

false: Manually configure the required object access policy.

3. Configuring audit policies

3.1 Automatic process

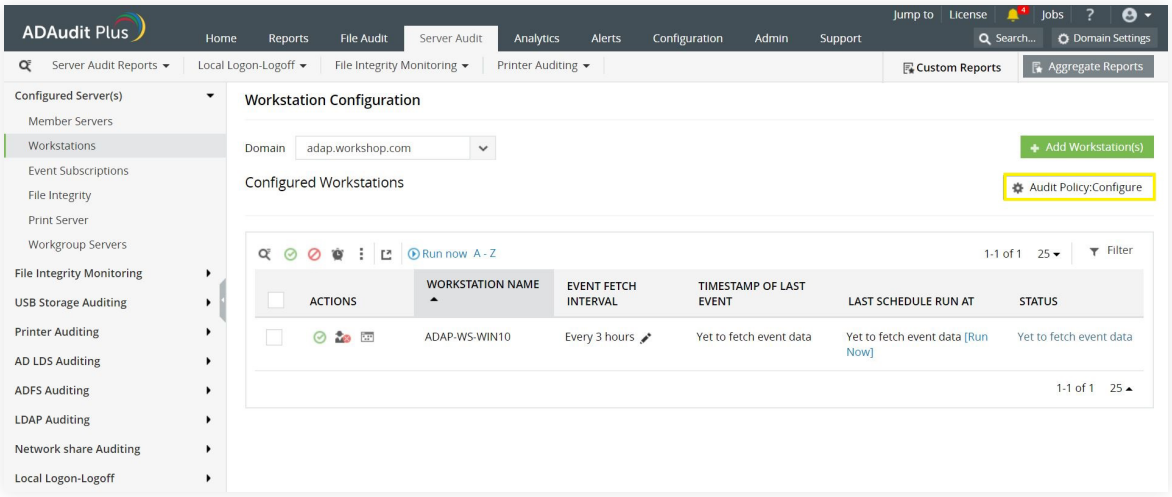
Configure the audit policies automatically using the steps below:

1. Open ADAudit Plus.

2. Click Server Audit from the top menu.

3. Under Configured Server(s) in the left-hand menu, choose Workstations.

4. Choose the desired domain in the Domain drop-down.



5. Click **Audit Policy: Configure** in the top-right corner.

Note: ADAudit Plus can automatically configure the required audit policies for workstation auditing. Clicking **Audit Policy: Configure** in the step above will create a GPO named <domain name>_ADAudit PlusWSPolicy with the audit policies required for workstation auditing.

3.2 Manual process

3.2.1 Configure list of Windows workstations to be audited

Configure the list of Windows workstations to be audited using the steps below:

1. Open **Active Directory Users and Computers**.
2. Right-click on the domain and select **New** > **Group**.
3. In the **New object - Group** window that opens, type in **"ADAuditPlusWS"** 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 workstations 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.

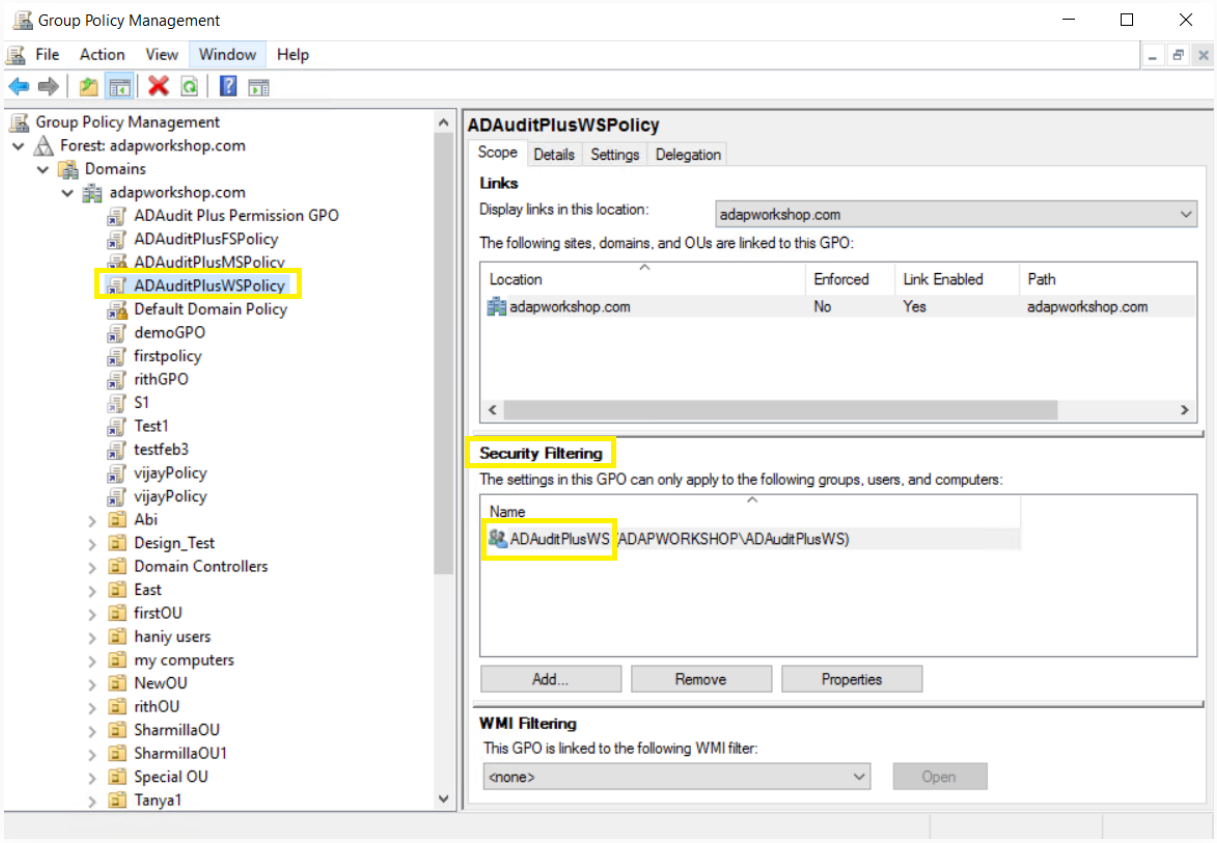
Note: The GPMC will not be installed on workstations and/or enabled on member servers by default, so we recommend configuring audit policies on Windows domain controllers. Otherwise follow the steps in this page to install GPMC on your desired member server or workstation.

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 "ADAuditPlusWSPolicy" and click **OK.**

8. Select the <domain name>_ADAuditPlusWSPolicy GPO. Under **Security Filtering,** select **Authenticated Users.** Click **Remove.** In the **Group Policy Management** window that opens, select **OK.**

9. Select the <domain name>_ADAuditPlusWSPolicy GPO. Under **Security Filtering,** click **Add** and choose the security group **ADAuditPlusWS** created previously. Click **OK.**



3.2.2 Configure advanced audit policies

Configure the audit policies manually using the steps below:

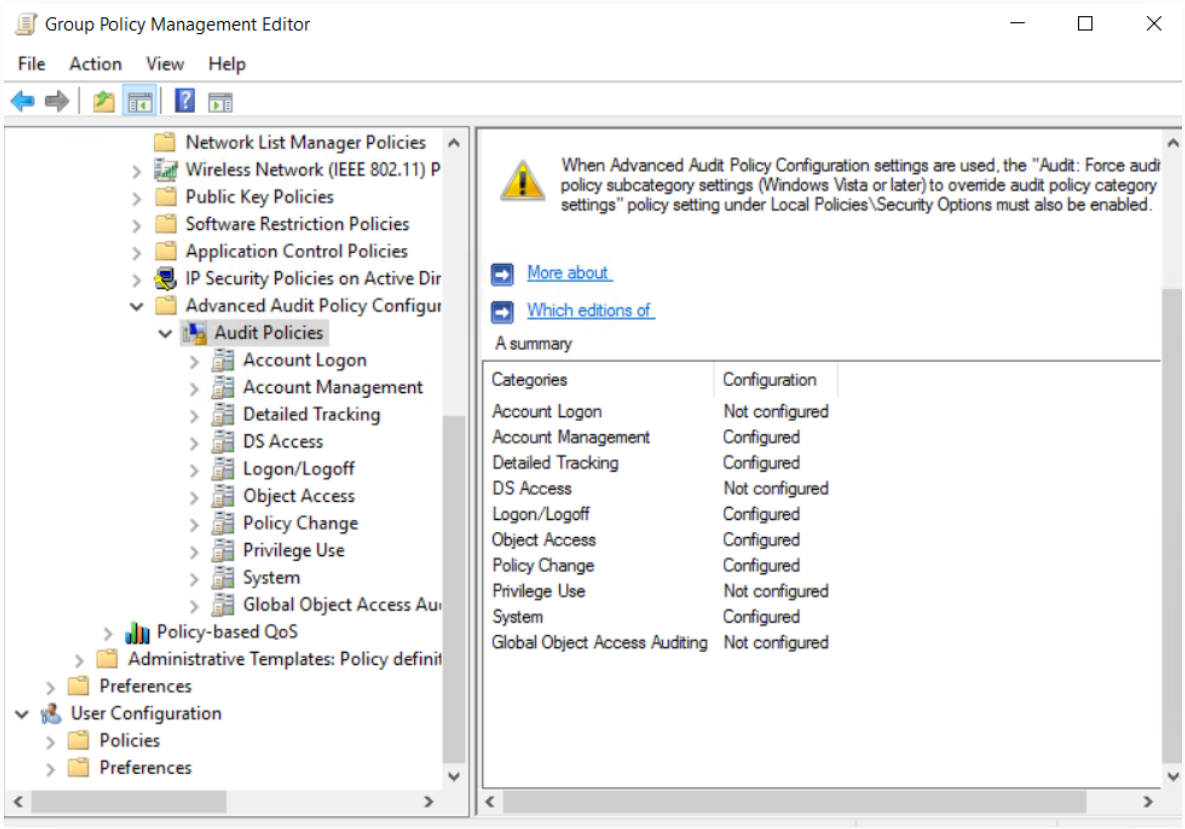
1. Using domain admin credentials, log in to any computer that has the GPMC on it.
2. Go to Start > Windows Administrative Tools > Group Policy Management.
3. Right-click the GPO <domain name>_ADAuditPlusWSPolicy and select Edit.
4. In the Group Policy Management Editor, follow the steps below:

Note: Advanced audit policy configuration is only available in Windows Server 2008 or later. If you have an older version of Windows, configure legacy audit policies. It is recommended that you configure advanced audit policies instead of legacy audit policies to prevent storing needless event data logs, as the legacy policies contain more unwanted events.

5. Choose Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies.
6. Click, enable, and save the audit policies as shown below:

Advanced audit policy		Audit events
Category	**Subcategory**	
Account Management	Audit Computer Account Management	Success
	Audit Distribution Group Management	Success
	Audit Security Group Management	Success
	Audit User Account Management	Success and failure
Detailed Tracking	Audit PNP Activity	Success and failure
Logon/Logoff	Audit Logoff	Success
	Audit Logon	Success and failure
	Audit Network Policy Server	Success and failure
	Audit Other Logon/Logoff Events	Success and failure
Object Access	Audit File Share	Success and failure
	Audit File System	Success and failure
	Audit Handle Manipulation	Success

	Audit Other Object Access Events	Success
	Audit Removable Storage	Success and failure
Policy Change	Audit Authentication Policy Change	Success
	Audit Authorization Policy Change	Success
System	Audit Security State Change	Success

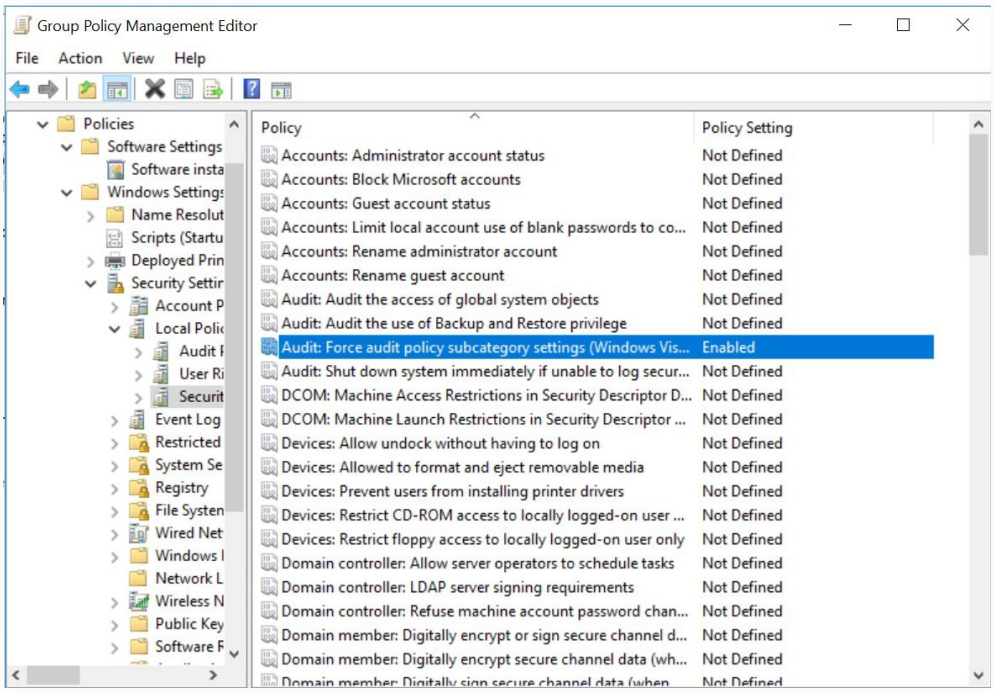


3.2.3 Force advanced audit policies

Force the advanced audit policies manually using the steps below:

1. Right-click the <domain name>_ADAuditPlusWSPolicy from GPMC.
2. In the Group Policy Management Editor, follow the steps below:
3. Choose Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.

4. Enable the policy and click OK.



3.2.4 Configure legacy audit policies

Configure the legacy audit policies manually using the steps below:

1. Go to **Start** > **Windows Administrative Tools** > **Group Policy Management**.

2. Right-click the GPO **<domain name>_ADAuditPlusWSPolicy** and select **Edit**.

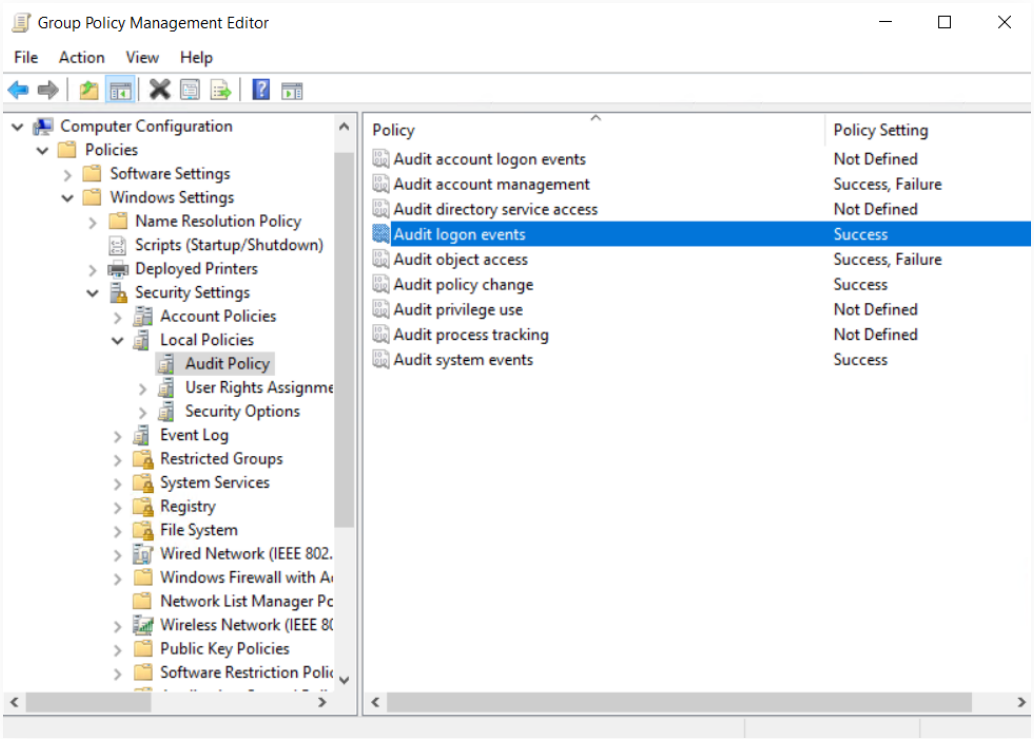
3. In the **Group Policy Management Editor**, follow the steps below:

Note: Advanced audit policy configuration is only available in Windows Server 2008 or later.
If you have an older version of Windows, configure legacy audit policies. It is recommended that you configure advanced audit policies instead of legacy audit policies to prevent storing needless event data logs, as the legacy policies contain more unwanted events.

4. Choose **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Audit Policies**.

5. Click, enable, and save the audit policies as shown below:

Local audit policy	Audit events
Category	
Audit account management	Success and failure
Audit logon events	Success
Audit object access	Success and failure
Audit policy change	Success
Audit system events	Success



4. Configuring security log size and retention settings

4.1 Configuring security log size

Configure security log size for Windows workstation audit data using the steps below:

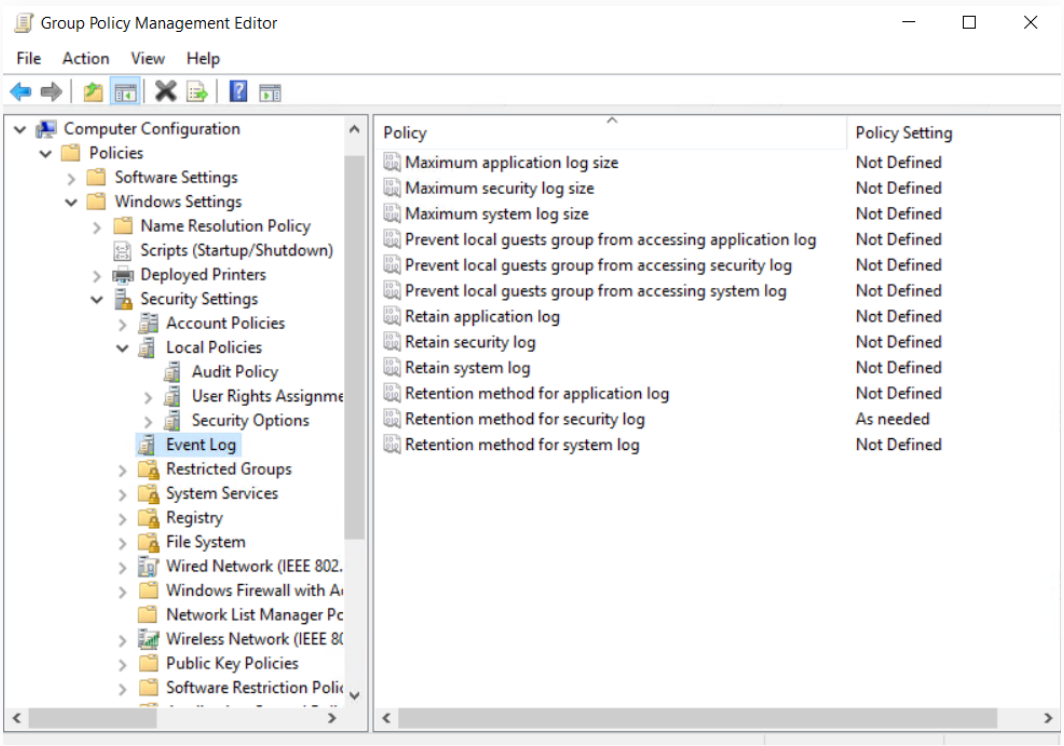
1. Go to Start > Windows Administrative Tools > Group Policy Management.
2. In GPMC, right-click the GPO <domain name>_ADAuditPlusWSPolicy and select Edit.
3. In the Group Policy Management Editor, choose Computer Configuration > Policies > Windows Settings > Security Settings > Event Log > Retention method for security log.

4. Check **Define these policy settings**, and select **Overwrite events as needed**.

5. Click **OK**.

6. Select **Maximum security log size** and configure the values as shown below. Make sure that the security log can hold a minimum of 12 hours of data.

Role	Operating system	Size
Windows workstation	Windows 10, 8, 7, Vista, and XP	512MB



5. Troubleshooting

5.1 How do you check to confirm the audit policies have been applied to the monitored workstations?

1. Log in to any computer with domain admin credentials.

2. Go to **Start** and type in "**Command Prompt**". Right-click **Command Prompt**, and select **Run as administrator**.

3. Type in "**gpresult /S <monitored computer> /F /H a.html**".

4. Ensure that all the audit policy settings and security log settings are in place.

5.2 How to check if the monitored events are being logged in workstations

1. Log in to any computer with domain admin credentials.
2. Go to **Start** > **Run**. Type in "**eventvwr.msc**".
3. In the **Event Viewer** window, right-click on the event viewer in the top-left corner and select **Connect to Another Computer**. In the **Select Computer** window that opens, check **Another computer** and type in the machine name whose events you want to verify. Click **Browse**, type in the machine name, and click **OK**.
4. Click **Windows Logs** > **Security**.
5. Right-click **Security**, then select **Filter Current Log...**
6. Monitor the desired event ID by entering details such as event logged time or the exact event ID under the **<All event ID>** text box.
7. Close the window once you've verified that events are being logged in your workstations.

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.

$ Get Quote Download