ManageEngine
ADAudit Plus

Group Policy Object (GPO) auditing guide

Table of Contents

1. Introduction

1.1 Overview

Group Policy is a collection of settings used to add additional controls to the working environment of both user and computer accounts. Group Policy helps enforce password policies, deploy patches, disable USB drives, disable PST file creation, and more. Group Policy helps strengthen your organizations' IT security posture by closely regulating critical policies such as password change, account lockout, and more.

1.2 Benefits of auditing Group Policy Objects using ADAudit Plus

- Audit, alert, and report on Group Policy Object (GPO) creation, deletion, modification, history, and more.
- Monitor who made what setting changes to your GPOs and from where in real time.
- Generate granular reports on the new and old values of all GPO setting changes.
- Keep a close eye on critical policy changes like changes to account lockout policy and password change policy to detect and respond to malicious activities instantly.
- And much more.

2. Supported systems

2.1. Supported Windows Server versions

Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, 2016, 2016 R2, and 2019.

3. Configuring domain controllers

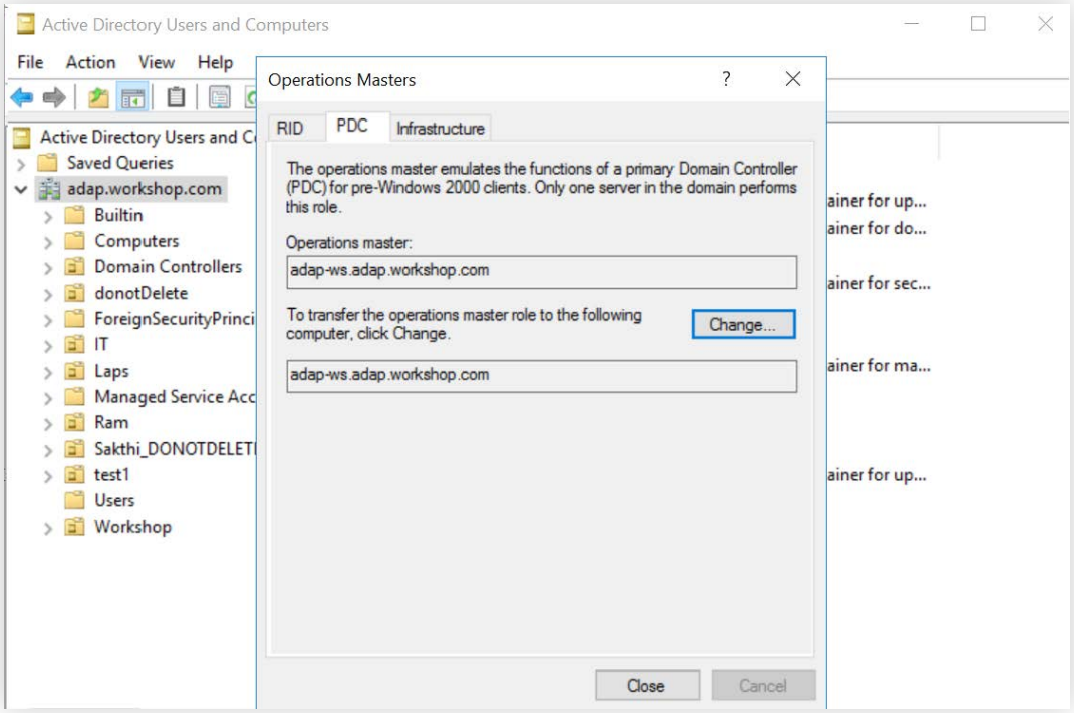
3.1 Automatic process

Check whether the configured domain controller is a primary domain controller (PDC) using the following steps.

1. Log in to any computer with **Active Directory Users and Computers.**
2. Go to **Start > Windows Administrative Tools > Active Directory Users and Computers.**
3. Right-click on the **domain** and select **Operations Masters.**
4. In the operations master window that opens, click the **PDC** tab at the top.

5. Under **Operations master** is the name of the server configured as the PDC.
6. Click **Close.**
7. Open **ADAudit Plus.**
8. Click **Domain Settings** in the top right corner.
9. Under **Available Domain Controllers,** ensure that the PDC has been configured.
10. If not, Select **+Add Domain Controllers,** and choose one.

    Note: If ADAudit Plus is unable to discover your domain controller, you can manually type it in.
11. Click **Save.**



Notes:

- Ensure that the share path **\\"machine_name"\sysvol** is accessible from the machine that has ADAudit Plus installed on it.
- To perform GPO setting change auditing, you only need to configure the PDC. GPO management auditing, on the other hand, requires configuring all the domain controllers that have been licensed.

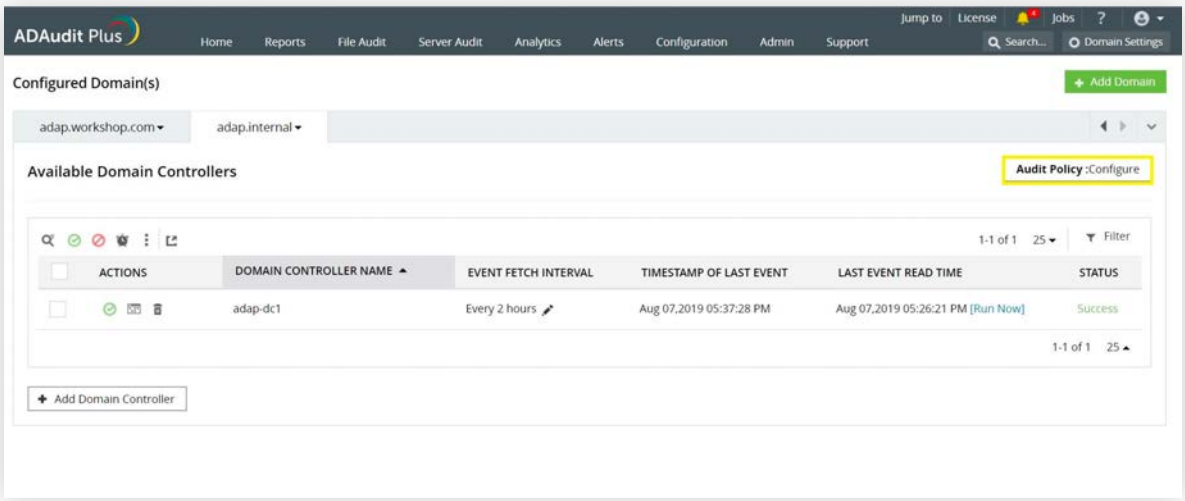
4. Configuring the audit policies

4.1 Automatic process

Configure the audit policies automatically using the steps below:

1. Open **ADAudit Plus.**
2. Go to **Admin > Domain Settings.** Click **Audit Policy: Configure** in the top-right corner.

Note: ADAudit Plus can automatically configure the required audit policies for GPO auditing.
After clicking **Audit Policy: Configure** in the above step, you can either choose **Yes** to let ADAudit Plus automatically configure the required audit policies, or choose **No** to manually configure them.



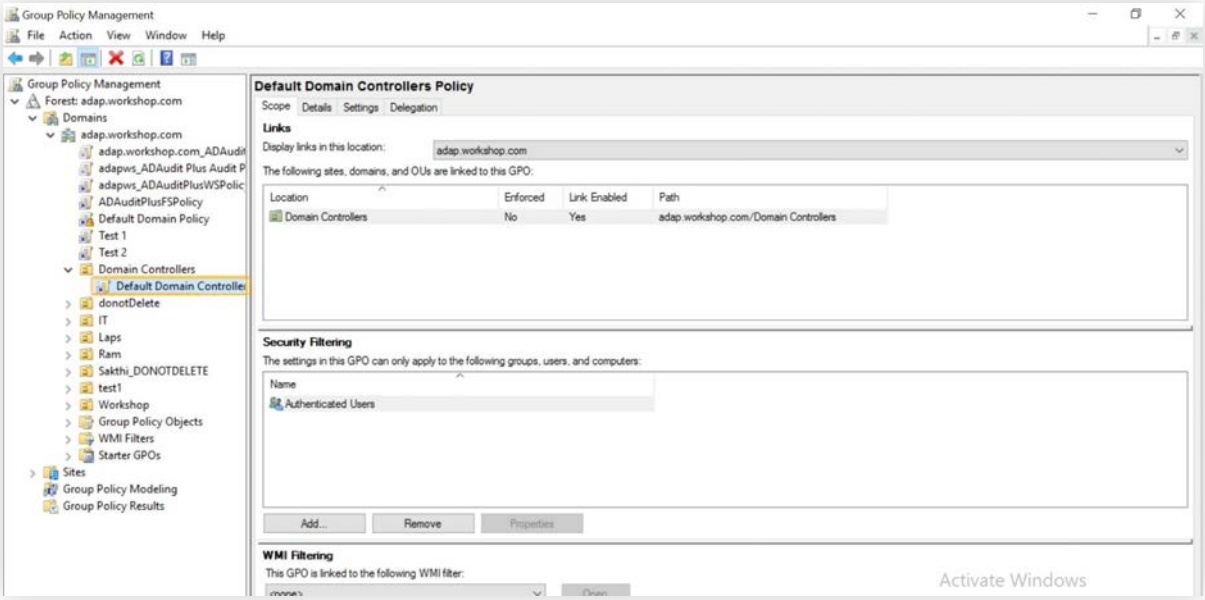
4.2 Manual process

Configure the audit policies manually using the steps below:

1. 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 in workstations and/or enabled in member servers by default. Hence, we recommend configuring audit policies in Windows domain controllers.

2. Go to **Start > Windows Administrative Tools > Group Policy Management.**
3. In the **GPMC,** select **Domains** and choose the domain you want to configure Group Policy for. Select **Domain Controller,** right-click the **Default Domain Controllers Policy,** and select **Edit.**



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

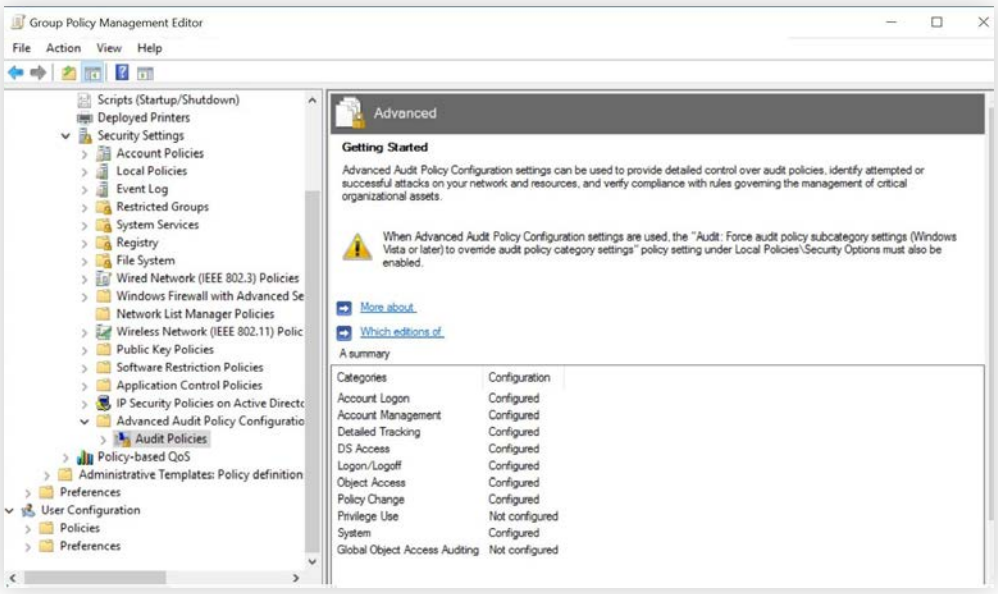
Note: Advanced audit policy configuration will only be available in Windows Server 2008 or later. If you have an older version of Windows, configure legacy audit policies.

Advanced audit policies

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**	
DS Access	Audit Directory Service Access	Success
	Audit Directory Service Changes	Success

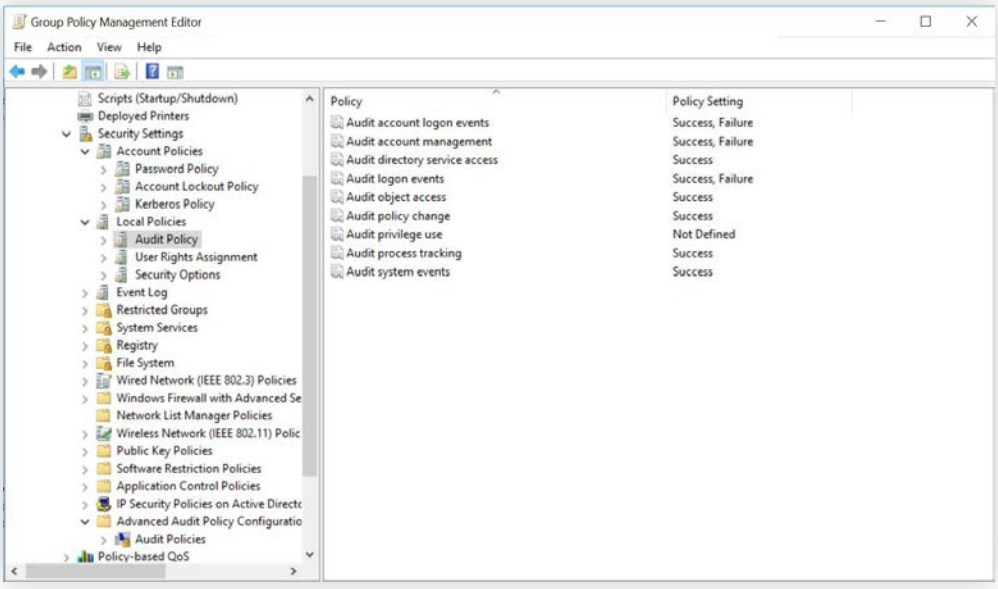


Local audit policies

7. Choose **Computer configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policies.**

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

Local audit policy	Audit events
Category	
Audit directory service access	Success



5. Configuring object-level auditing

5.1 Automatic process

Automatic configuration of object-level auditing requires the user's consent.

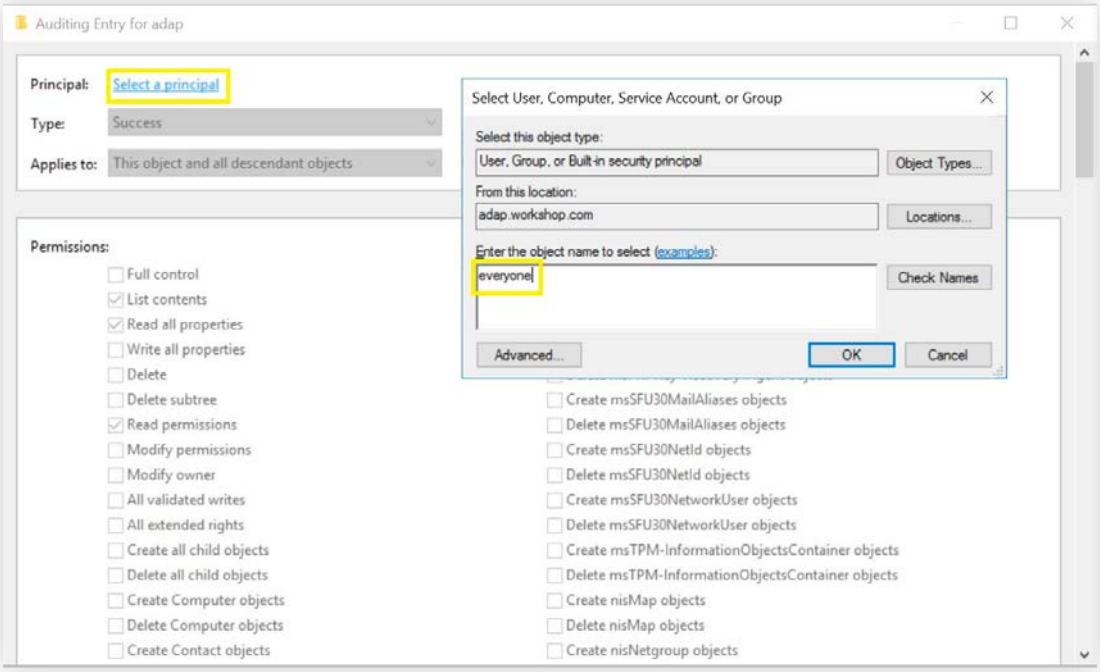
To configure object-level auditing automatically:

1. Open **ADAudit Plus.**
2. Go to **Reports > GPO Management > GPO History > Object-level auditing needs to be configured for getting proper reports: Configure.**

5.2 Manual process

Configure object-level auditing manually using the steps below:

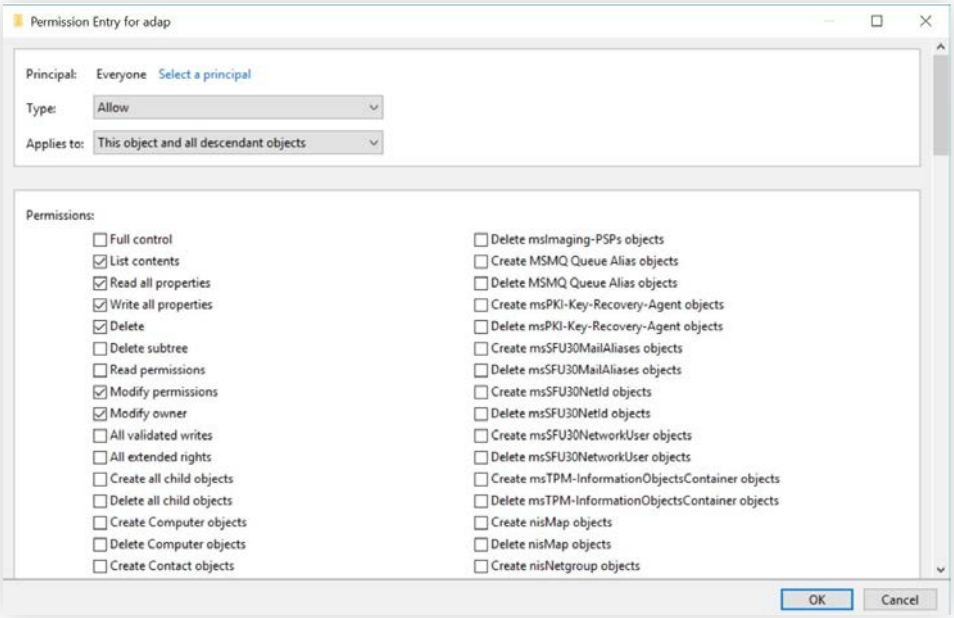
1. Using domain admin credentials, log in to any computer that has **Active Directory Users and Computers** on it.
2. Go to **Start > Windows Administrative Tools > Active Directory Users and Computers.**
3. Click **View > Advanced features.**
4. Right-click on the domain, and go to **Properties > Security > Advanced > Auditing > Add.**
5. In the **Auditing Entry** window, click **Select a principal.** Under **Enter the object name to select,** type in **Everyone,** and click **OK.**



6. Select **Type: Success.** Select the appropriate permissions as directed below.

Note: Use **Clear all** to remove all permissions and properties before selecting the appropriate permissions.

Auditing entry number	Auditing entry for	Access	Apply to Windows Server 2003	Apply to Windows Server 2008/Windows Server 2012
3 and 4	GPO	Create groupPolicy Container objects Delete groupPolicy Container objects	This object and all child objects	This object and all descendant objects
		Write all properties Delete Modify permissions	groupPolicyContainer objects	Descendant groupPolicy Container objects



6. Configuring security log size and retention settings

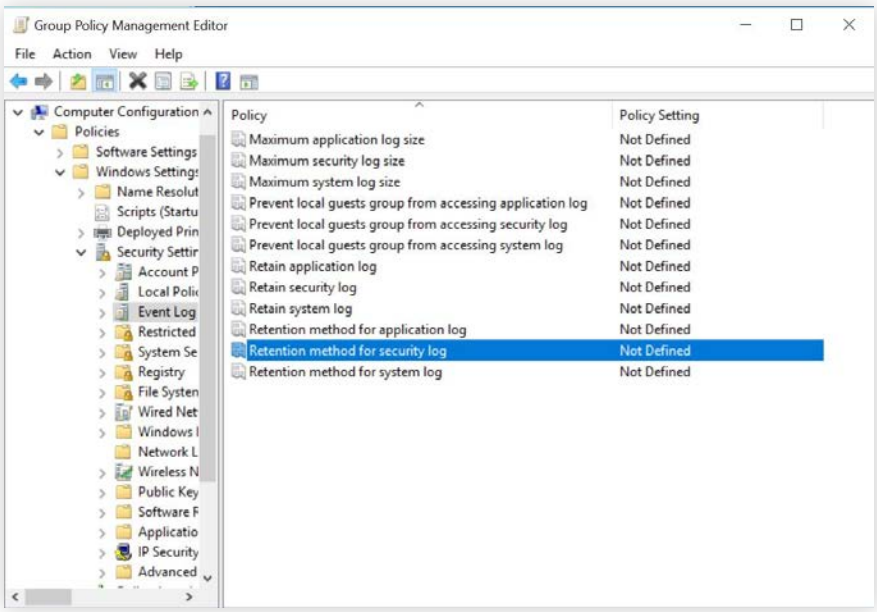
6.1 Configuring security log size

Configure security log size for Group Policy 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"_ADAudit Plus Audit policy,** 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.**



6.2 Configuring retention settings

Configure retention settings for Group Policy audit data using the steps below:

1. Open **ADAudit Plus.**

2. Go to **Admin > Configuration > Archive events** and check the **GPO Management** box. Then enter the number of **Days** and **Reclaimable space.**

3. Choose the **Archive folder.**

4. Click **Save.**

7. Installing the Group Policy Management Console (GPMC)

The GPMC must be installed on the machine used to run ADAudit Plus. Install GPMC in the machine running ADAudit Plus using the steps below:

For Windows Server 2012 and above

1. Go to **Start > Control Panel,** and select **Turn Windows features on and off** under *Programs.*

2. In the **Add Roles and Feature Wizard** window that opens, select **Features.**

3. Check **Group Policy Management,** and click **Next.**

4. Click **Install.**

For Windows Server 2008 and 2008 R2

1. Go to **Start > Control Panel,** and select **Turn Windows features on and off** under *Programs*.
2. In the **Server manager** window select **Features > Add features.**
3. Check **Group Policy Management,** and click **Next.**
4. Click **Install.**

Note: Once the GPMC is installed, open **ADAudit Plus console > Reports > GPO Settings Changes > Group Policy Settings Changes.** An error message will be displayed on top that says **"Please install GPMC in the computer where ADAudit Plus is installed. After you install GPMC please Click here."** Go ahead and click the **Click here** hyperlink to begin advanced GPO report generation in ADAudit Plus.