ManageEngine
ADAudit Plus

Windows server auditing guide

www.adauditplus.com

Table of Contents

Document summary

A Windows member server is a computer that runs on Windows Server, belongs to a domain, and is not a domain controller. Windows member servers typically run different services and can act like a file server, print server, etc. For the sake of convenience, Windows member servers will be referred to as Windows servers in this guide.

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:

- Monitor file integrity.
- Audit local logon and account management.
- Track printer, removable storage, AD FS, AD LDS, and LAPS activities.
- Keep tabs on scheduled tasks and processes.

ADAudit Plus enables you to audit the following versions of Windows Server:

- Windows Server 2003/2003 R2
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019

This guide takes you through the process of setting up ADAudit Plus and your Windows servers for real-time change auditing and user behavior analytics.

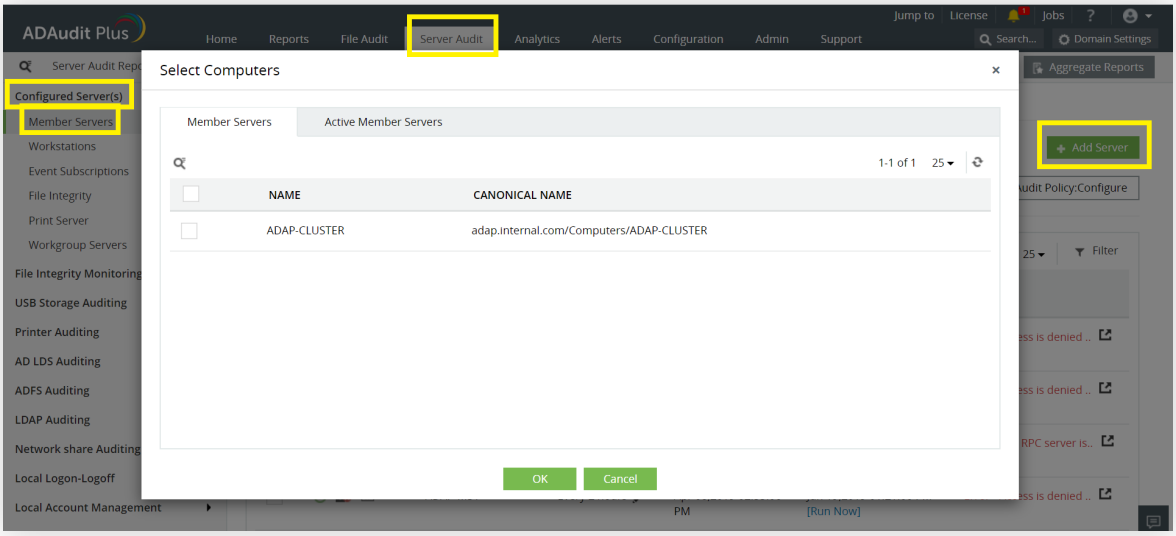
1. Configure Windows servers in ADAudit Plus

1.1 Using product console

From the product console up to a 100 windows servers can be configured at a time, to do this:

Log in to the ADAudit Plus web console. Go to the **Server Audit** tab → **Configured Servers** → **Member Servers** → **Add Server.** Enter the details needed to complete the configuration.

Note: ADAudit Plus can automatically configure the required audit policies for Windows server auditing. In the final step, you can either choose **Yes** to let ADAudit Plus automatically configure the required audit policies, or choose **No** to manually configure the required audit policies.



1.2 Using command line arguments

Using command line arguments all Windows servers in your environment can be configured at a time, to do this:

1. 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 Windows servers (that you want to audit) in adjacent lines, and separate them using commas.

   For example, to add the file servers Test-MS1, Test-MS2, and Test-MS3; open the servers.csv file and enter:

   Test-MS1,

   Test-MS2,

   Test-MS3

2. 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 ms -isauditpolicy **true (or) false**

   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 all Windows servers and configure the required audit policies automatically; execute the following command:

   config server add -machinetype ms -isauditpolicy **true**

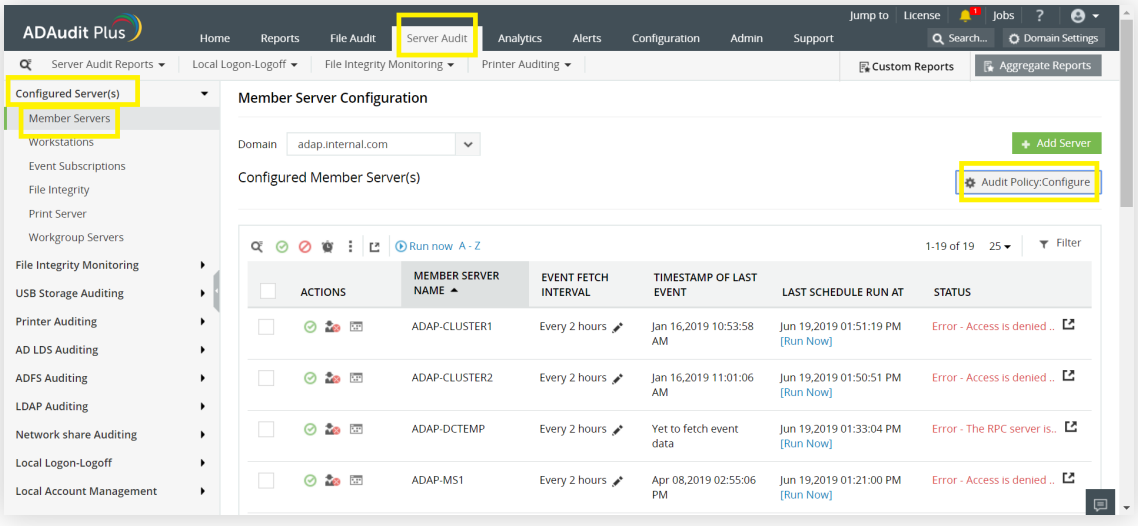
2. Configure audit policies in your domain

Audit policies must be configured to ensure that events are logged whenever any activity occurs.

2.1 Automatic configuration

Log in to the ADAudit Plus web console. Go to the **Server Audit** tab → **Configured Servers** → **Member Servers** → **Audit Policy: Configure.**

Note: ADAudit Plus can automatically configure the required audit policies for Windows server 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 the required audit policies.

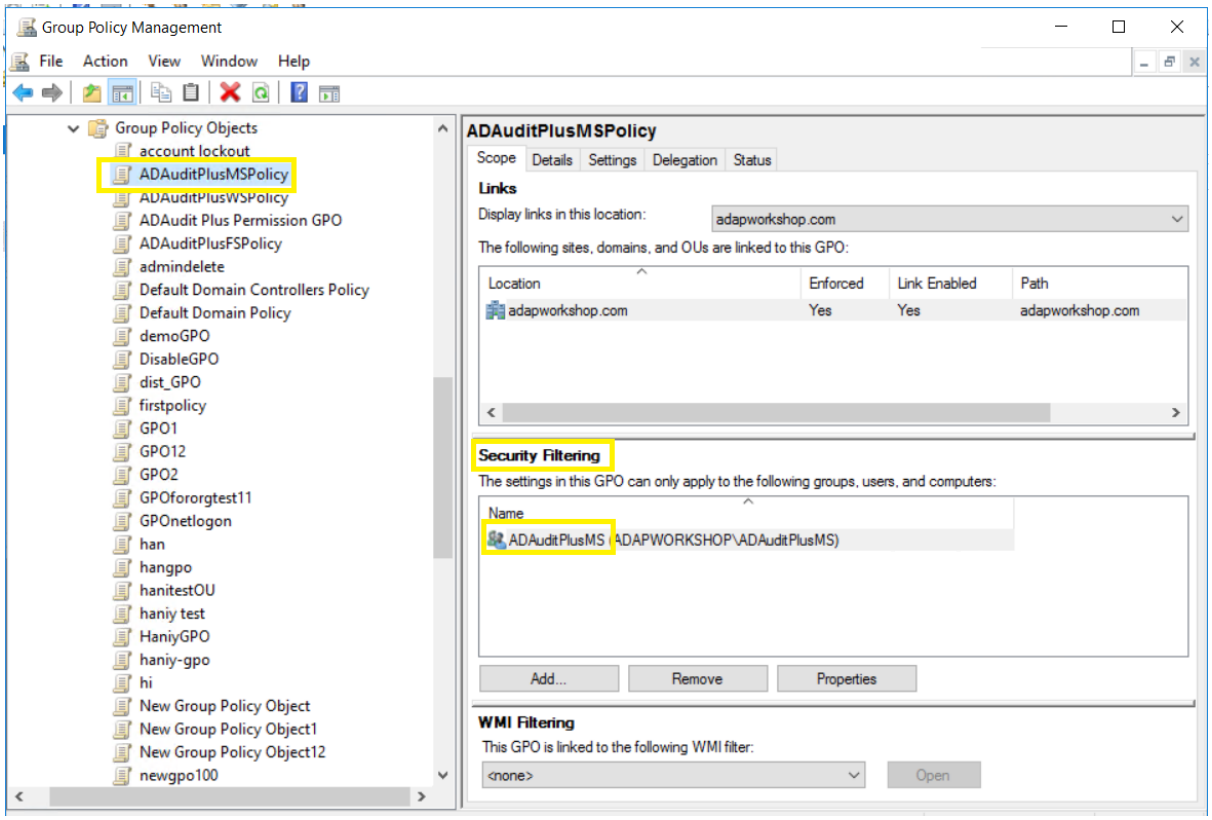


2.2 Manual configuration

2.2.1 Configure list of Windows 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 **"ADAuditPlusMS"** as the **Group name,** check **Group scope: Domain Local** and **Group type: Security.** Click **OK.**
4. Right-click the newly created group and select **Properties > Members > Add.** Add all the Windows servers 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 **"ADAuditPlusMSPolicy"** and click **OK.**
8. Select the **ADAuditPlusMSPolicy** GPO. Under **Security Filtering,** select **Authenticated Users.** Click **Remove.** In the **Group Policy Management** window that opens, select **OK.**
9. Select the **ADAuditPlusMSPolicy GPO.** Under **Security Filtering,** click **Add** and choose the security group **ADAuditPlusMS** created previously. Click **OK.**

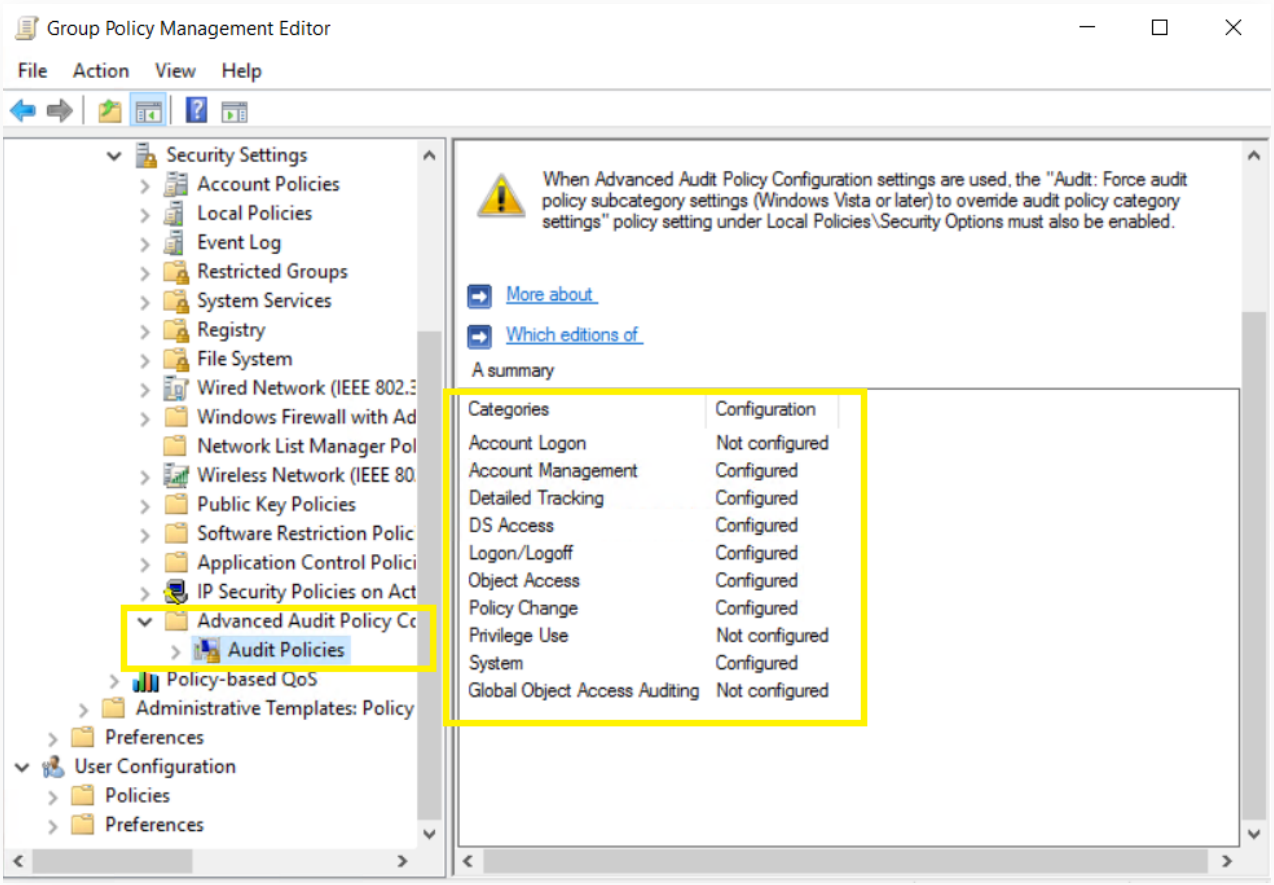


2.2.2 Configure advanced audit policies

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. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, then right-click **ADAuditPlusMSPolicy** and select **Edit.**
2. In the Group Policy Management Editor, go to Computer **Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policy.** Double-click on the relevant policy setting.
3. Navigate to the right pane and right-click on the relevant Subcategory. Select **Properties,** then **choose Success,** Failure, or both, as directed in the table below.

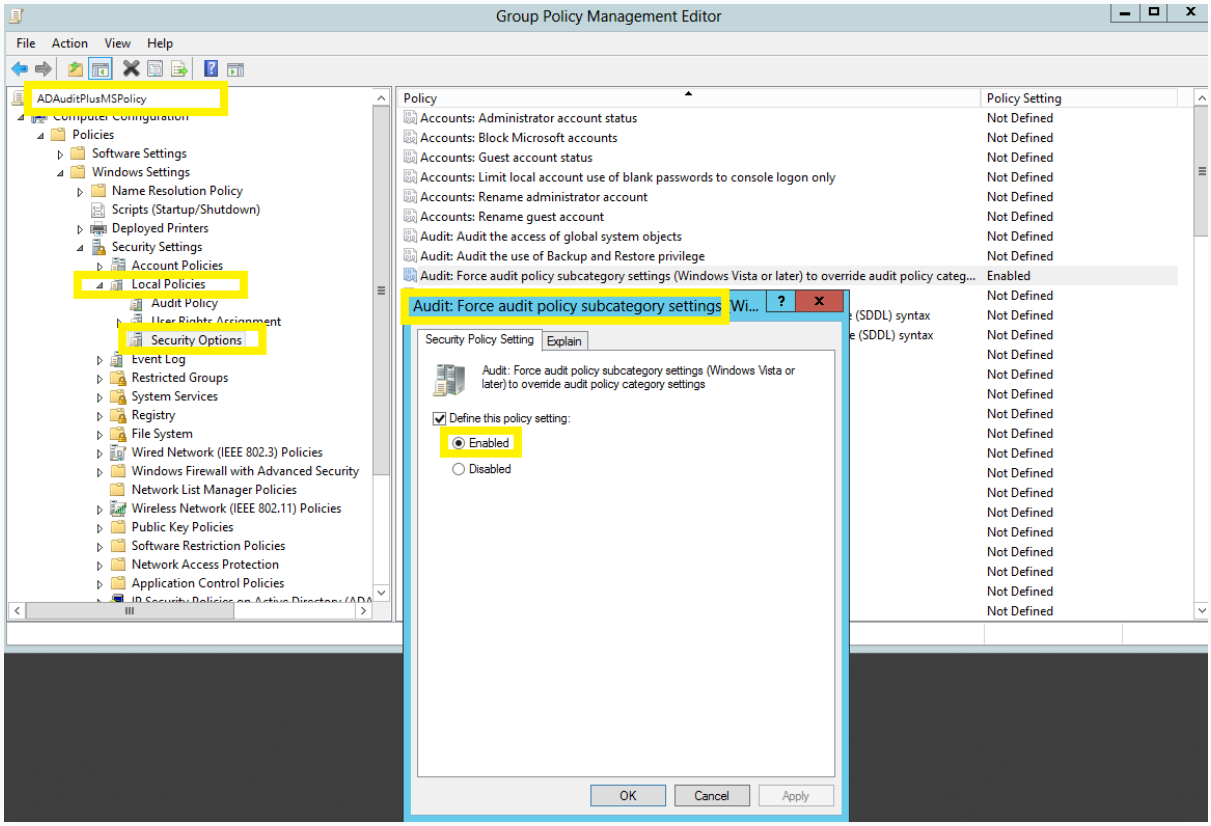
Category	Subcategory	Audit Events
Account Management	• Audit Computer Account Management • Audit Distribution Group Management • Audit Security Group Management	✓ Success
	• Audit User Account Management	✓ Success and Failure
Detailed Tracking	• Audit Process Creation Audit Process Termination	✓ Success
DS Access	• Audit Directory Service Changes • Audit Directory Service Access	✓ Success
Logon/Logoff	• Audit Logon • Audit Network Policy Server	✓ Success and Failure
	• Audit Other Logon/Logoff Events • Audit Logoff	✓ Success
Object Access	• Audit File System • Audit Handle Manipulation • Audit File Share	✓ Success and Failure
Policy Change	• Audit Authentication Policy Change • Audit Authorization Policy Change	✓ Success
System	• Audit Security State Change	✓ Success



2.2.3 Force advanced audit policies

When using advanced audit policies, ensure that they are forced over legacy audit policies.

1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click **ADAuditPlusMSPolicy,** then select **Edit.**
2. In the Group Policy Management Editor, go to **Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options.**
3. Navigate to the right pane, then right-click **Audit: Force audit policy subcategory settings.** Select **Properties,** then **Enable.**

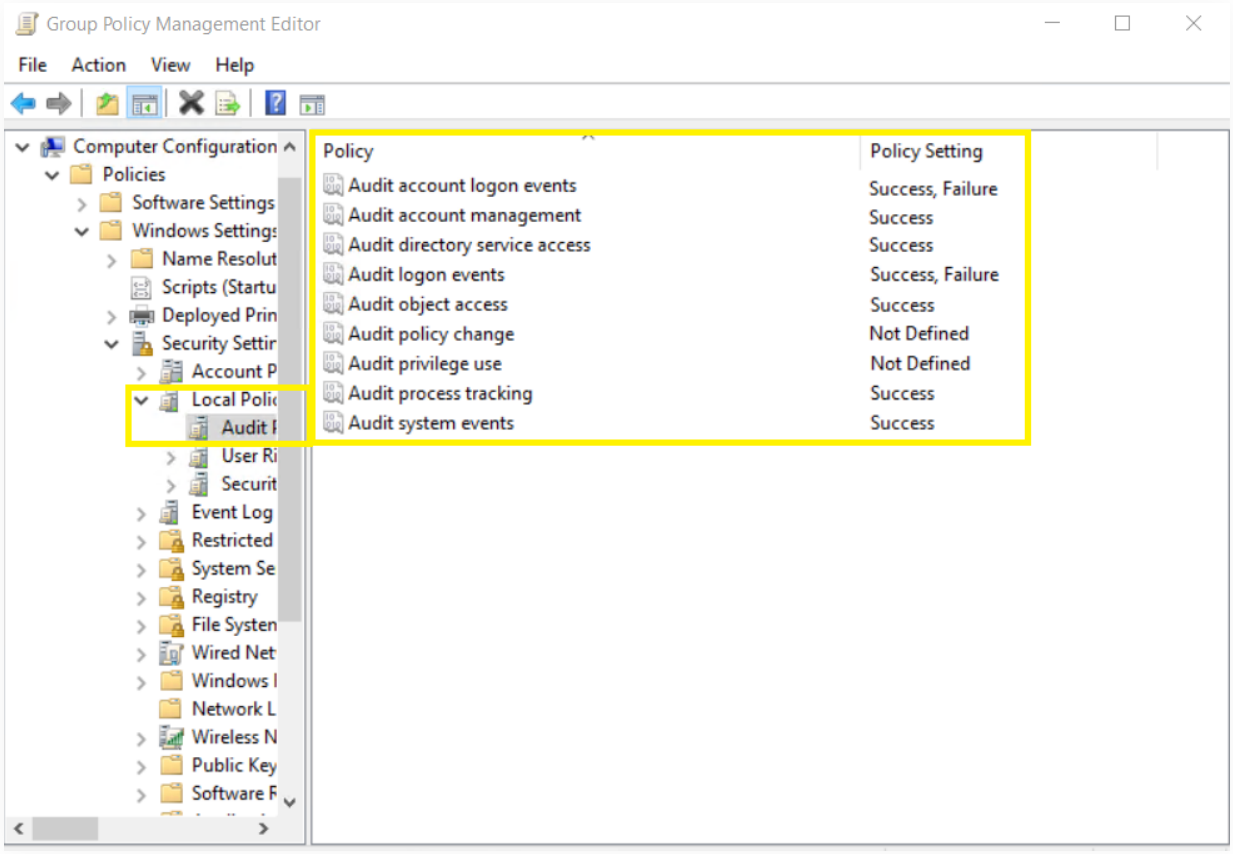


2.2.4 Configure legacy audit policies

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. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click **ADAuditPlusMSPolicy,** then select **Edit.**
2. In the Group Policy Management Editor, go to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies**, and double-click **Audit Policy.**
3. Navigate to the right pane and right-click on the relevant policy. Select **Properties,** then choose **Success, Failure,** or both, as directed in the table below:

Category	Audit Events
Account Logon	✓ Success and Failure
Audit Logon/Logoff	✓ Success and Failure
Account Management	✓ Success
Directory Service Access	✓ Success
Process Tracking	✓ Success
Object Access	✓ Success
System Events	✓ Success



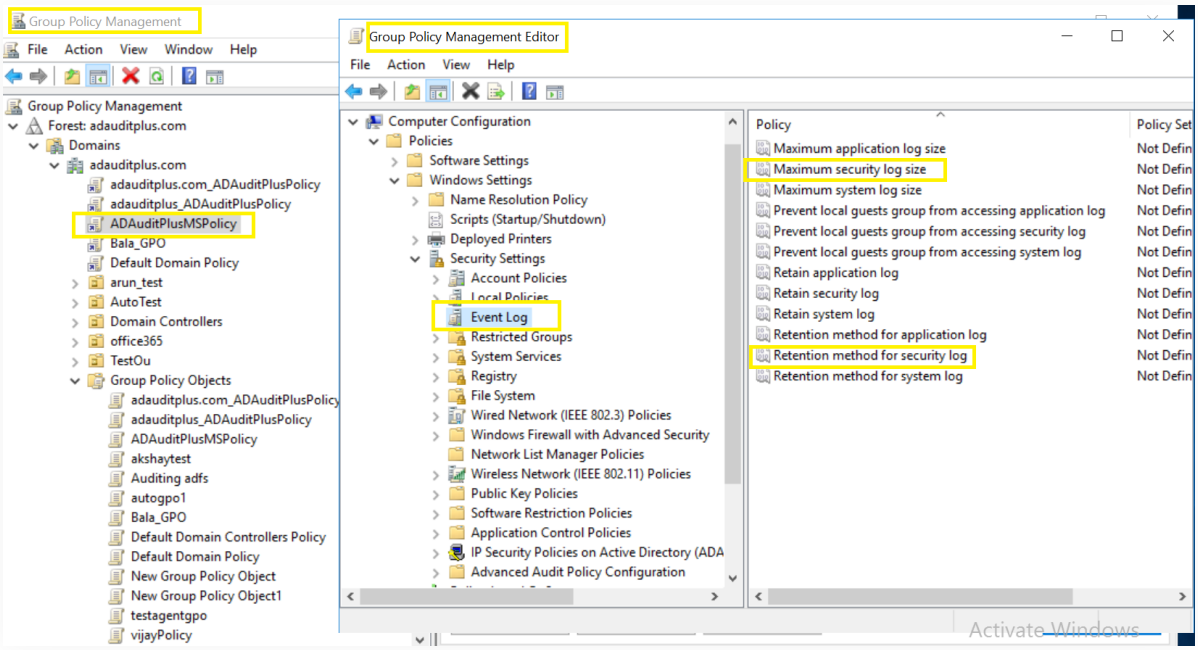
3. Configure event log settings in your domain

Event log size needs to be defined to prevent loss of audit data due to overwriting of events.

To configure event log size and retention settings, follow the steps outlined below:

1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click **ADAuditPlusMSPolicy,** then select **Edit.**
2. In the Group Policy Management Editor, select **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Event Log.**
3. Navigate to the right pane and right-click on **Retention method for security log.** Select **Properties** → **Overwrite events as needed.**
4. Navigate to the right pane, then right-click **Maximum security log size** and define the size as directed in the table below.

Role	Operating System	Operating System
Windows file server	Windows Server 2003	512MB
Windows file server	Windows Server 2008 and above	4,096MB



4. FAQs

1. **To verify if the desired audit policies and security log settings are configured:**

   Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click **Group Policy Results,** and open the Group Policy Results Wizard. Select the computer and user (current user), then verify if the desired settings as defined in step 2.2 are configured.

2. **To verify if the desired events are getting logged:**

   Log in to any computer with Domain Admin credentials. Open **Run,** then type “eventvwr.msc”. Right-click on Event Viewer. Connect to the target computer, then verify if events corresponding to the configured audit policies are getting logged.

   For example, event ID 4768 should get logged when Success audit events is configured under the Audit Kerberos Authentication Service Subcategory, under the Account Logon Category (refer to step 2.2.1).