ManageEngine
ADAudit Plus

Active Directory Auditing Guide

www.adauditplus.com

Table of Contents

Document summary

Securing Active Directory protects user accounts, company systems, software applications, and other critical components of an organization's IT infrastructure from unauthorized access.

ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps secure Active Directory.

With ADAudit Plus you can audit all three major contexts of Active Directory, namely-

- Domain Naming Context, which comprises of users, computers, groups, OUs, and other objects,
- Schema Context, which comprises of all schema objects,
- Configuration Context, which comprises of sites, subnets, AD DNS, and other objects.

ADAudit Plus allows you to audit the following domain controller OS versions.

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

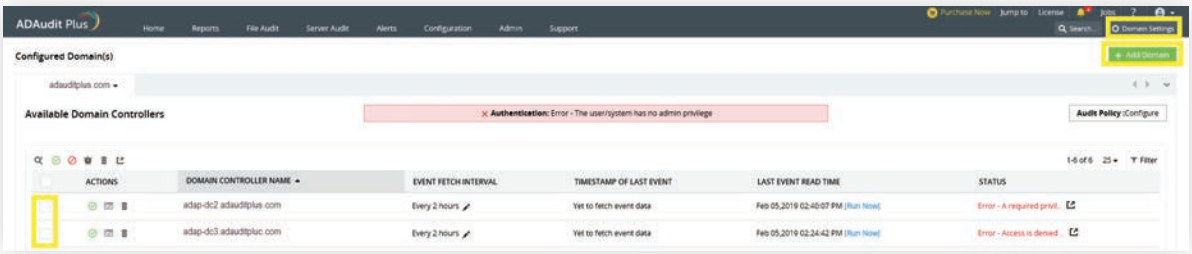
This guide takes you through the process of setting-up ADAudit Plus and your Active Directory environment for real-time auditing.

1. Configuring Active Directory domains and domain controllers in ADAudit Plus

1.1 Automatic configuration

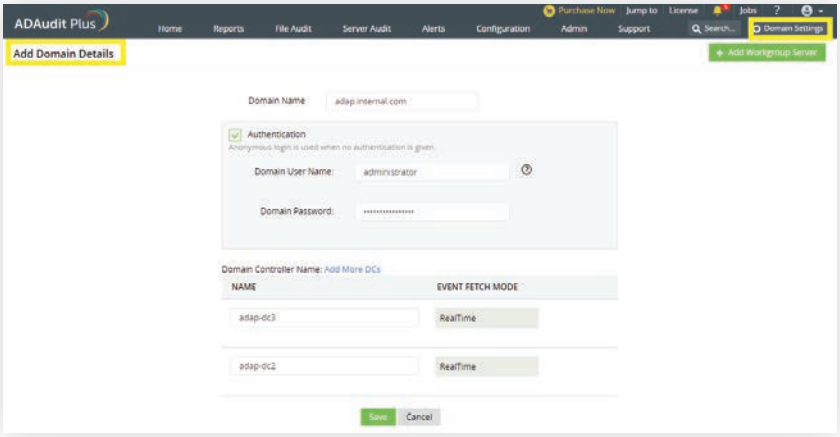
Post installation, ADAudit Plus automatically discovers the local domain and the domain controllers running in it.

Log in to the ADAudit Plus web console → Domain Settings → Select the necessary domain controllers by clicking on the respective check boxes.



1.2 Manual configuration

To add a domain: Log in to the ADAudit Plus web console → Domain Settings → Add Domain → Enter the necessary details.



2. Configuring audit policies

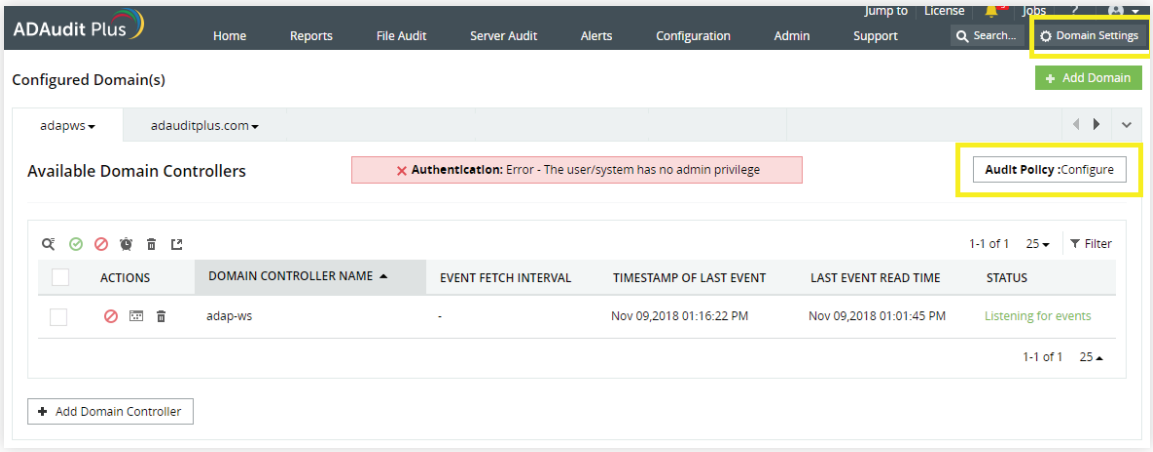
Audit policies must be configured to ensure that events are logged whenever any activity occurs.

2.1 Automatic configuration

ADAudit Plus can automatically configure the required audit policies for Active Directory auditing.

Note: Automatic audit policy configuration is not done without the users consent.

Steps for automatic audit policy configuration: Log in to the ADAudit Plus web console → Domain Settings → Audit Policy: Configure.



2.2 Manual configuration

2.2.1 Configuring 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. It is recommended that advanced audit policies are configured on domain controllers running on Windows Server 2008 and above.

i Log in to any computer that has the Group Policy Management Console (GPMC), with Domain Admin credentials → Open GPMC → **Right click on Default Domain Controllers Policy** → **Edit.**

ii In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policy, Double-click on the relevant policy setting.

iii Navigate to the right pane → Right-click on the relevant Subcategory, and then click Properties → Select Success, Failure, or both; as directed in the table below.

Cateogory	Sub Category	Audit Events
Account Logon	◦ Audit Kerberos Authentication Service	✓ Success and Failure
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 Services 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 Other Object Access Events	✓ Success
Policy Change	◦ Audit Authentication Policy Change ◦ Audit Authorization Policy Change	✓ Success
System	◦ Audit Security State Change	✓ Success

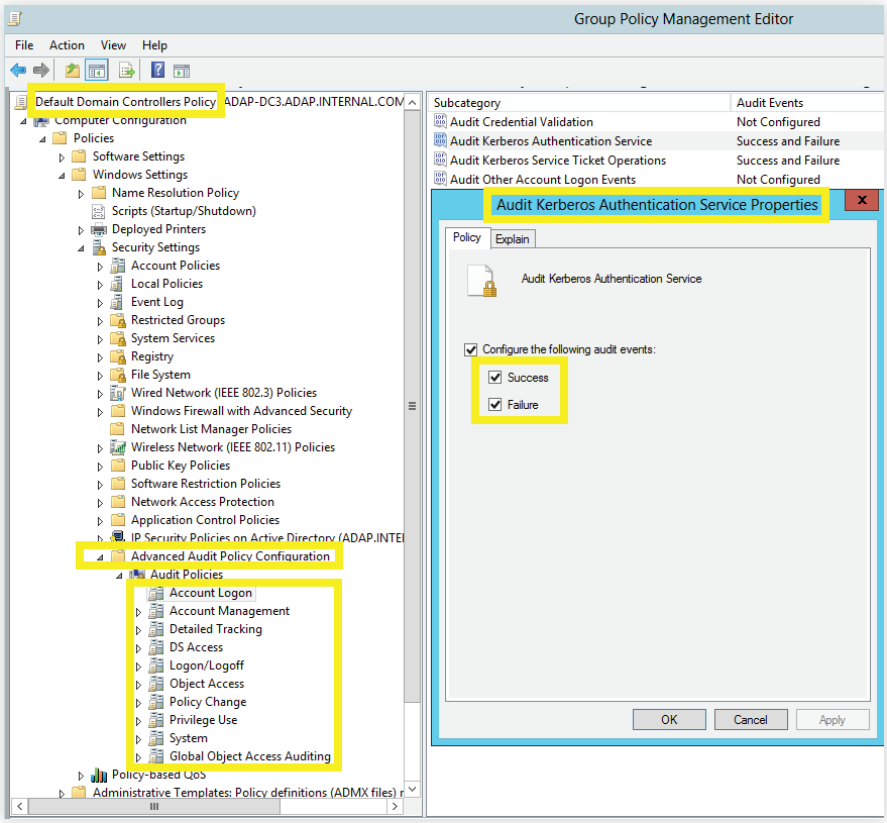


Image showing: Account Logon category → Audit Kerberos Authentication Service subcategory → Both Success and Failure configured.

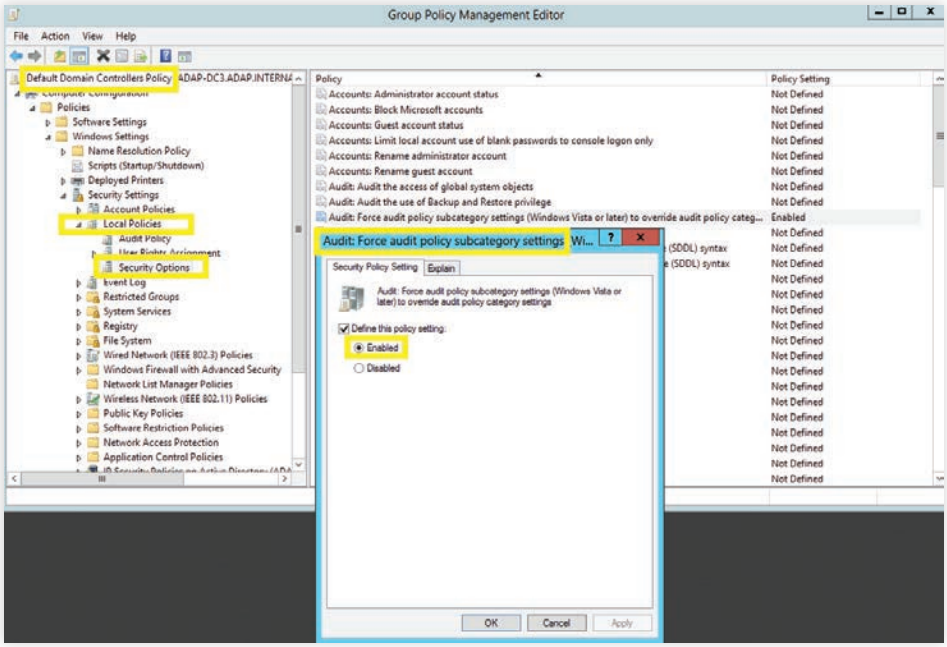
2.2.2 Enforcing advanced audit policies

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

i Log in to any computer that has the Group Policy Management Console (GPMC), with Domain Admin credentials → Open GPMC → **Right click on Default Domain Controllers Policy** → **Edit.**

ii In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options.

iii Navigate to the right pane → Right-click on Audit: Force audit policy subcategory settings → Properties → Enable.



2.2.3 Configuring legacy audit policies

The option to configure advanced audit policies is not available in Windows Server 2003 and below. Therefore for these systems, you need to configure the legacy audit policies.

i Log in to any computer that has the Group Policy Management Console (GPMC), with Domain Admin credentials → Open GPMC → **Right click on Default Domain Controllers Policy** → **Edit.**

ii In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Double click on Audit Policy.

iii Navigate to the right pane → Right-click on the relevant policy, and then click Properties → Select 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

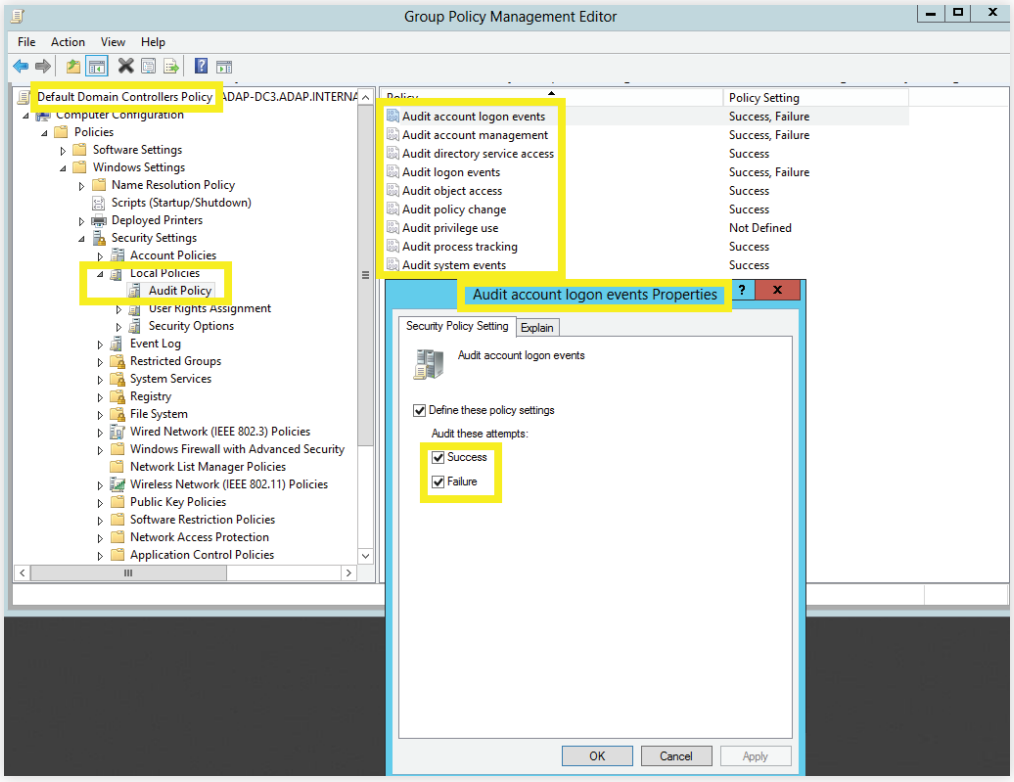


Image showing: Audit account logon events category → Both Success and Failure configured.

3. Configuring object level auditing

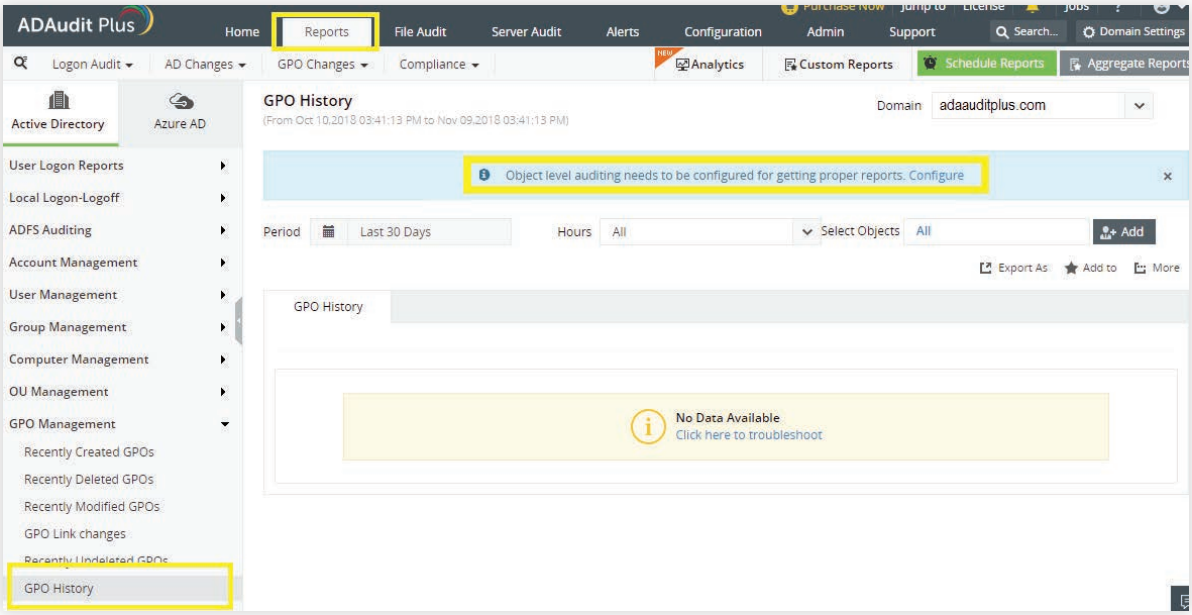
Setting up object level auditing ensures that events are logged whenever any Active Directory object related activity occurs.

3.1 Automatic configuration

ADAudit Plus can automatically configure the required object level auditing.

Note: Automatic object level auditing configuration is not done without the users consent.

To initiate the configuration of object level auditing automatically, log in to the ADAudit Plus web console → Reports → GPO Management → GPO History → Object level auditing needs to be configured for getting proper reports: Configure.



3.2 Manual configuration

3.2.1 Configuring auditing for OU, GPO, user, group, computer, and contact objects

i Log in to any computer that has the Active Directory Users and Computers, with Domain Admin credentials → Open ADUC.

Click on View and ensure that Advanced Features is enabled. This will display the advanced security settings for selected objects in Active Directory Users and Computers.

ii Right click on domain → Properties → Security → Advanced → Auditing → Add.

iii In the Auditing Entry window → Select a principal: Everyone → Type: Success → Select the appropriate permissions, as directed in the table below.

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

Auditing Entry number	Auditing Entry for	Access	Apply onto	
			Windows Server 2003	Windows Server 2008 and above
1&2	OU	• Create Organizational Unit objects • Delete Organizational Unit objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete Modify Permissions	Organizational Unit objects	Descendant Organizational Unit objects
3&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	groupPolicy Container objects	Descendant groupPolicy Container objects
5&6	User	• Create User Objects • Delete User Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions • All Extended Rights	User objects	Descendant User objects
7&8	Group	• Create Group Objects • Delete Group Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions • All Extended Rights	Group objects	Descendant Group objects

9&10	Computer	• Create Computer Objects • Delete Computer Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions • All Extended Rights	Computer objects	Descendant Computer objects
11&12	Contact	• Create Contact Objects • Delete Contact Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions	Contact objects	Descendant Contact objects

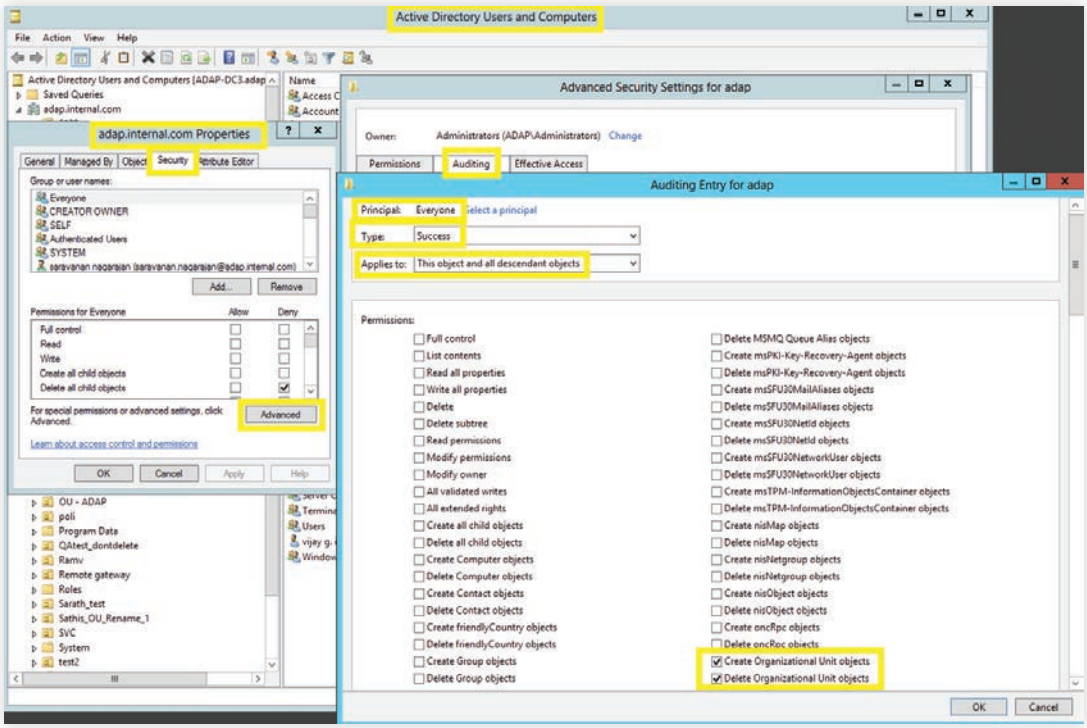


Image displaying: Auditing Entry number 1.

Note: All 12 Auditing Entries must be enabled.

3.2.2 To audit container objects

i Log in to any computer that has the Active Directory Service Interfaces snap-in → Open the ADSI Edit console → Right click on ADSI Edit → Connect to.

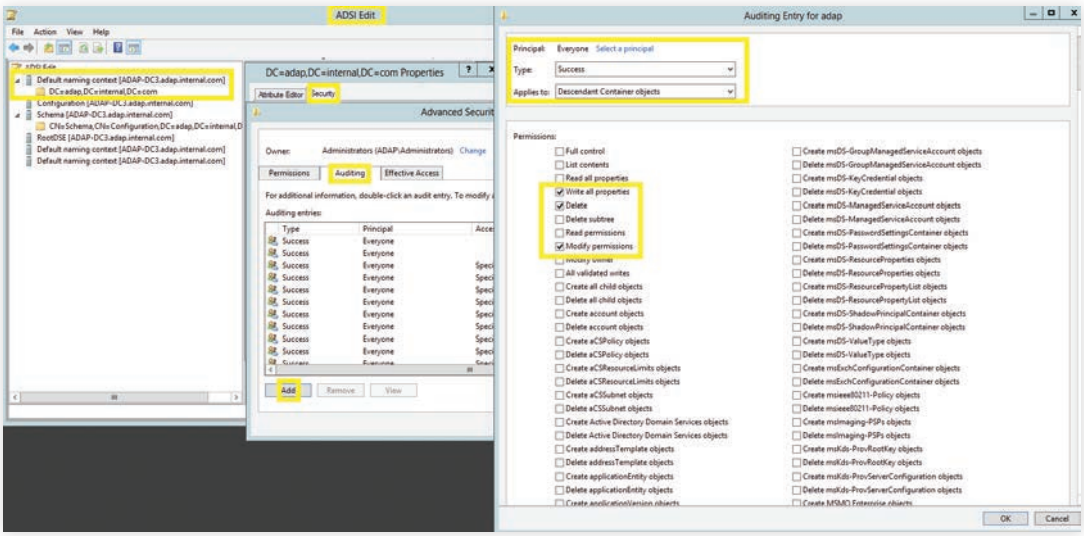
ii In the Connection Settings window → Under Select a Well-Known Naming Context → Select 'Default Naming Context'.

iii Navigate to the left panel → Click on Default naming context → Right click on domains distinguished name → Select properties → Security → Advanced → Auditing → Add.

iv In the Auditing Entry window → Select a principal: Everyone → Type: Success → Select the appropriate permissions, as directed in the table below.

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

Auditing Entry	Access	Apply onto	
		Windows Server 2003	Windows Server 2008 and above
Container	• Write All Properties • Delete • Modify Permissions	Container objects	Descendant Container objects



3.2.3 Configuring auditing for password setting objects

i Log in to any computer that has the Active Directory Service Interfaces snap-in → Open the ADSI Edit console → Right click on ADSI Edit Connect to.

ii In the Connection Settings window → Under Select a Well-Known Naming Context → Select 'Default Naming Context'.

iii Navigate to the left panel → Click on Default naming context → Expand the domain → Expand the System container → Right click on the Password Settings Container → Properties → Security → Advanced → Auditing → Add.

iv In the Auditing Entry window → Select a principal: Everyone → Type: Success → Select the appropriate permissions, as directed in the table below.

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

Auditing Entry number	Auditing Entry for	Access	Apply onto	
			Windows Server 2003	Windows Server 2008 and above
1&2	Password Settings Container	◦ Create msDS-Password Settings objects ◦ Delete msDS-Password Setting objects	Not Applicable	This object and all descendant objects
		◦ Write All Propertie ◦ Delete ◦ Modify Permissions	Not Applicable	Descendant msDS-PasswordSettings objects

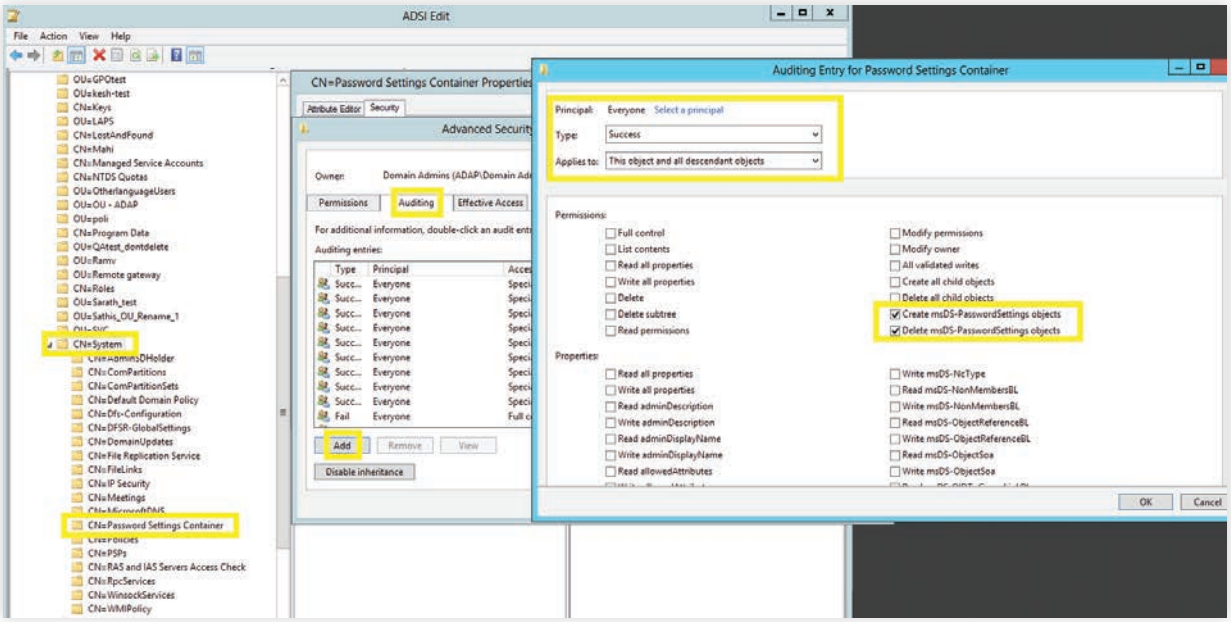


Image showing: Auditing Entry number 1.

Note: Both Auditing Entries must be enabled.

3.2.4 Configuring auditing for configuration objects

i Log in to any computer that has the Active Directory Service Interfaces snap-in → Open the ADSI Edit console → Right click on ADSI Edit → Connect to.

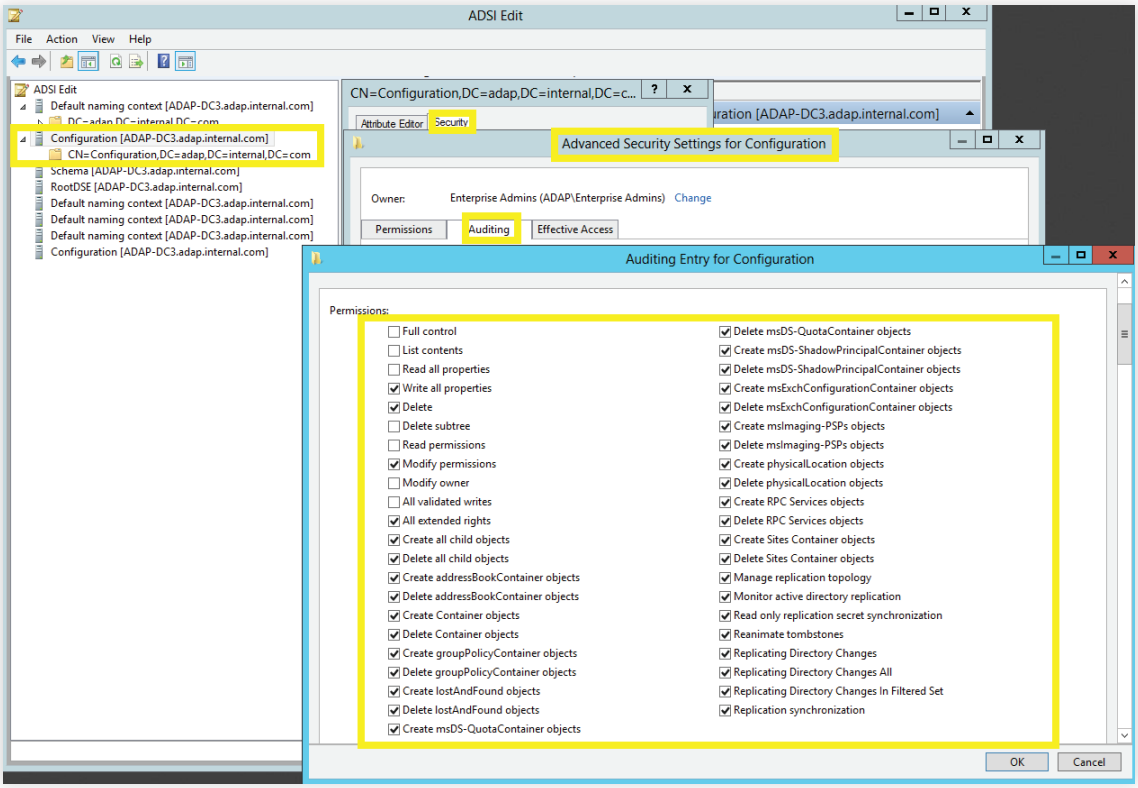
ii In the Connection Settings window → Under Select a Well-Known Naming Context → Select Configuration.

iii Navigate to the left panel → Click on Configuration → Right click on Configuration naming context → Select properties → Security → Advanced → Auditing → Add.

iv In the Auditing Entry window → Select a principal: Everyone → Type: Success → Select the appropriate permissions, as directed in the table below.

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

Auditing Entry for	Access	Apply onto	
		Windows Server 2003	Windows Server 2008 and above
Configuration	• Create All Child objects • Write All Properties • Delete All child objects • Delete • Modify Permissions • All Extended Rights	This object and all child objects	This object and all



3.2.5 Configuring auditing for schema objects

i Log in to any computer that has the Active Directory Service Interfaces snap-in → Open the ADSI Edit console → Right click on ADSI Edit → Connect to.

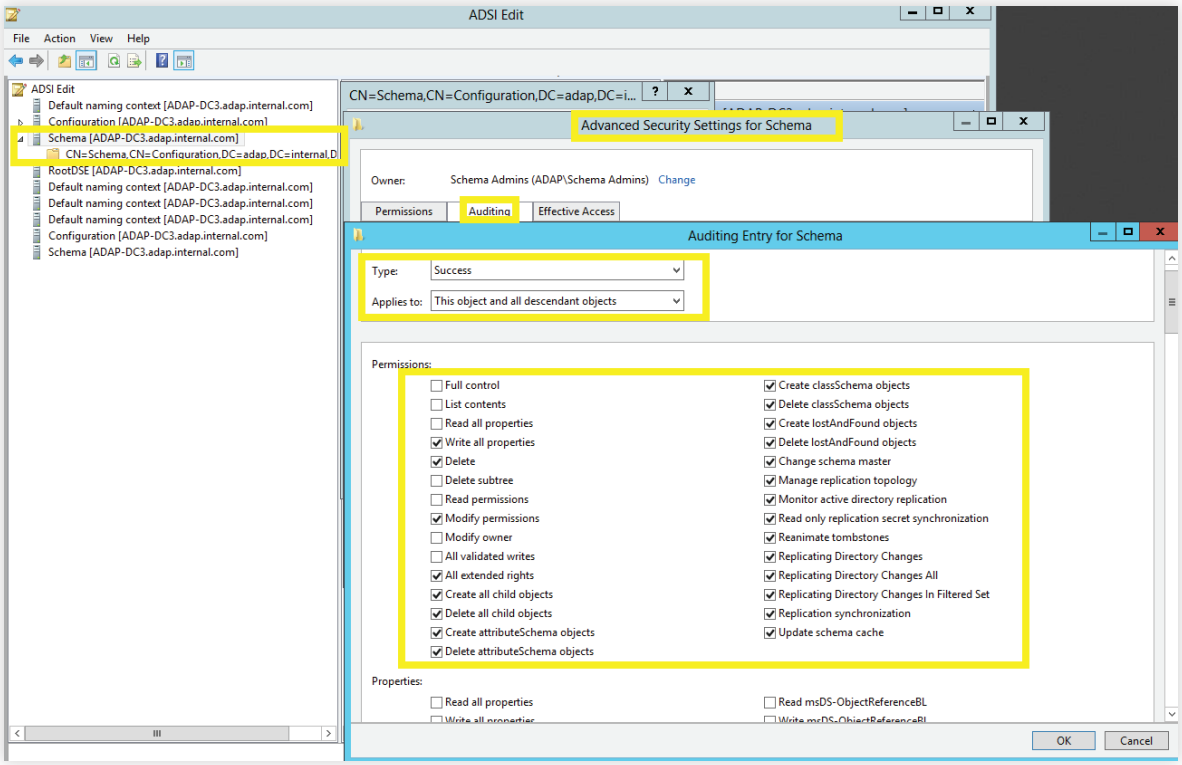
ii In the Connection Settings window → Under Select a Well-Known Naming Context → Select Schema

iii Navigate to the left panel → Click on Schema → Right click on Schema naming context → Select properties → Security → Advanced → Auditing → Add.

iv In the Auditing Entry window → Select a principal: Everyone → OK → Type: Success → Select the appropriate permissions, as directed in the table below.

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

Auditing Entry for	Access	Apply onto	
		Windows Server 2003	Windows Server 2008 and above
Schema	◦ Create All Child objects ◦ Write All Properties ◦ Delete All child objects ◦ Delete ◦ Modify Permissions ◦ All Extended Rights	This object and all child objects	This object and all descendant objects

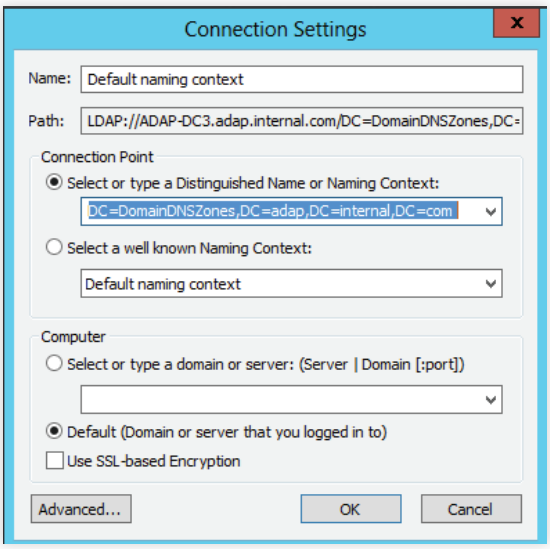


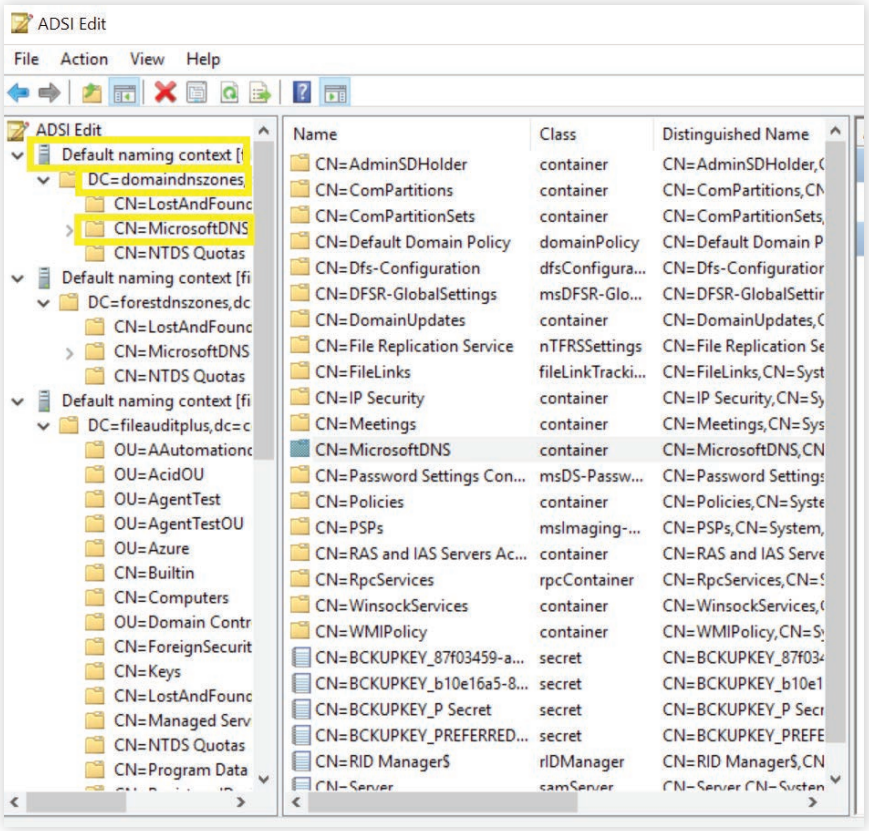
3.2.6 Configuring auditing for DNS objects

i Login to any computer that has the Active Directory Service Interfaces snap-in → Open Run Type adsiedit.msc → OK → Right click on ADSI Edit → Connect to.

ii In the Connection Settings window → Under Select or type a Distinguished Name or Naming Context.

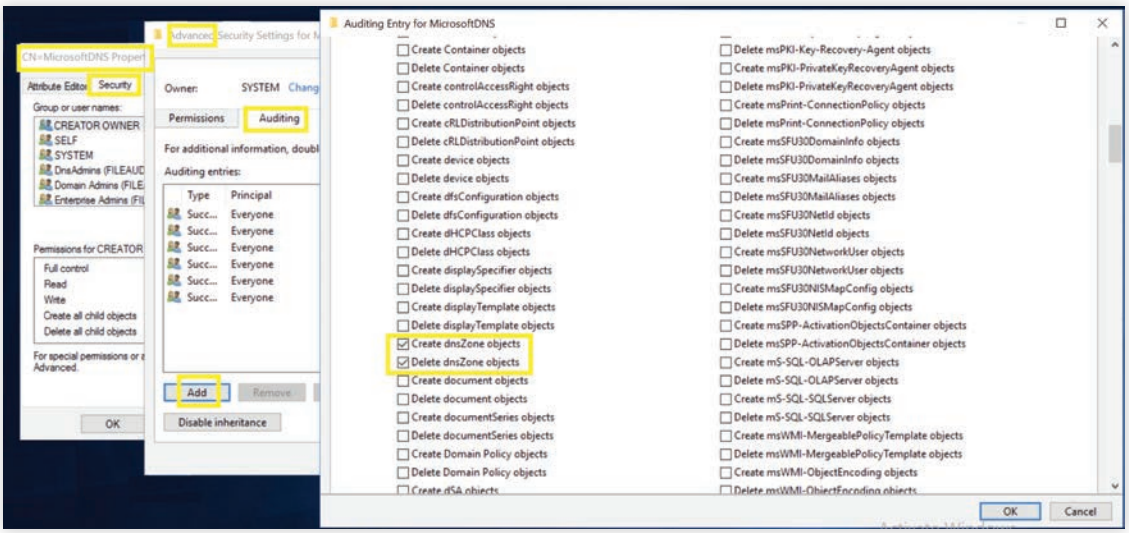
- Type DC=adap, DC=internal,DC=com as the Distinguished Name. (This partition is generally loaded in Adsiedit by default)
- Type DC=DomainDNSZones,DC=adap,DC=internal,DC=com as the Distinguished Name.
- Type DC=ForestDNSZones,DC=adap,DC=internal,DC=com as the Distinguished Name.





iii Navigate to the left panel → Click on Default naming context → Right click on MicrosoftDNS → Select properties → Security → Advanced → Auditing → Add.

iv In the Auditing Entry window → Select a principal → Everyone → OK → Type: Success → Select the appropriate permissions, as directed in the table below.

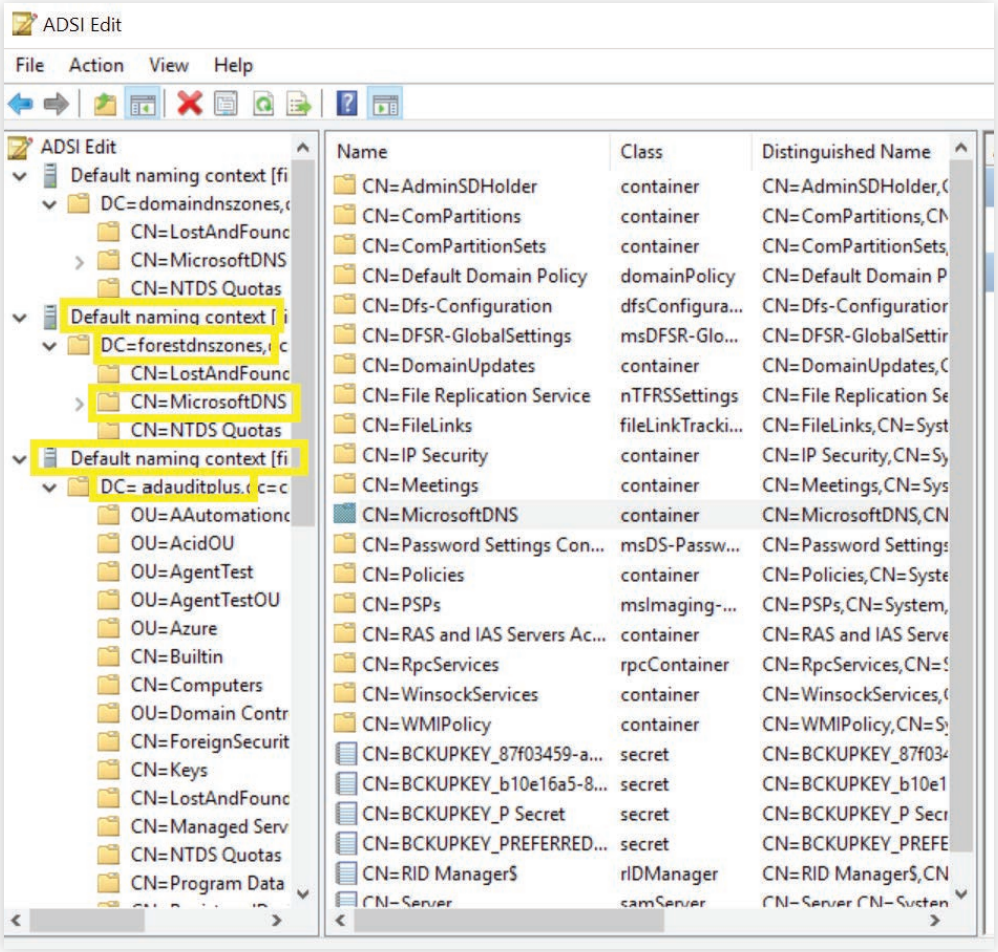


Note: Use Clear all to clear all permissions and properties before selecting appropriate permissions.

Auditing Entry number	Auditing Entry for	Access	Apply onto	
			Windows Server 2003	Windows Server 2008 and above
1&2	DNS Zones	• Create DNS Zones objects • Delete DNS Zones objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions	DNS Zone objects	Descendant DNS Zone objects
3&4 Permissions	DNS Nodes	• Create DNS Nodes objects • Delete DNS Nodes objects	This object and all child objects	Descendant DNS Zone objects
		• Write All Properties • Delete • Modify Permissions	DNS Node objects	Descendant DNS Node objects

Note: All Auditing Entries must be completed.

Note: Repeat steps iii. and iv. for the remaining 2 default naming contexts.



4. Configuring event log settings

Setting a threshold value for the event log size helps prevent the loss of audit data. If you've not specified the event log size in your system, older events will be overwritten.

i Log in to any computer that has the Group Policy Management Console (GPMC), with Domain Admin credentials → Open GPMC → **Right click on Default Domain Controllers Policy** → **Edit.**

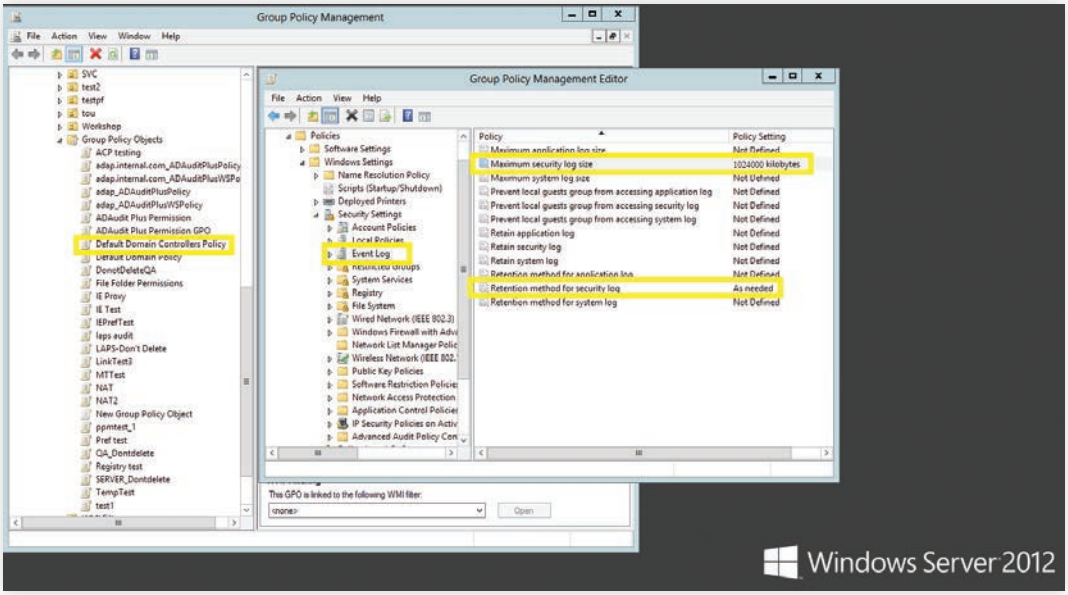
ii In the Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Event Log.

iii Navigate to the right pane → Right click on Retention method for security log → Properties → Overwrite events as needed.

iv Navigate to the right pane → Right click on Maximum security log size → Define size as directed in the table below.

Note: Ensure security event log holds minimum of 12hrs of data.

Role	Operating System	Size
Domain Controller	Windows Server 2003	512 MB
Domain Controller	Windows Server 2008 and above	1024 MB



5. Troubleshooting FAQ

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

Log in to any computer that has the Group Policy Management Console (GPMC), with Domain Admin credentials → Open GPMC → Right click on Group Policy Results → Group Policy Results Wizard → Select the computer, user (current user) → Verify if the desired settings are configured.

ii **To verify if the desired object level auditing settings are configured:**

Run through step 3.2 found in this document.

iii **To verify if the desired events are getting logged:**

Log in to any computer with Domain Admin credentials → Open Run → Type eventvwr.ms → Right click on Event Viewer → Connect to the target computer → Verify if events corresponding to the audit policies configured are getting logged.

For example: Kerberos Authentication Service Success advanced audit policy configuration should result in event ID 4768 getting logged.