ManageEngine ADAudit Plus

## Active Directory Auditing Guide



www.adauditplus.com

## **Table of Contents**

Document summary	1
1. Configuring Active Directory domains and domain controllers	
in ADAudit Plus	2
1.1 Automatic configuration	2
1.2 Manual configuration	2
2. Configuring audit policies	2
2.1 Automatic configuration	2
2.2 Manual configuration	3
2.2.1 Configuring advanced audit policies	3
2.2.2 Enforcing advanced audit policies	5
2.2.3 Configuring legacy audit policies	6
3. Configuring object level auditing	7
3.1 Automatic configuration	7
3.2 Manual configuration	8
3.2.1 Configuring auditing for OU, GPO, user, group,	
computer, and contact objects	8
3.2.2 Configuring auditing for container objects	11
3.2.3 Configuring auditing for password setting objects	12
3.2.4 Configuring auditing for configuration objects	13
3.2.5 Configuring auditing for schema objects	15
3.2.6 Configuring auditing for DNS objects	16
4. Configuring event log settings	20
5. Troubleshooting FAQ	21

### **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 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

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  $\rightarrow$  Domain Settings  $\rightarrow$  Select the necessary domain controllers by clicking on the respective check boxes.

ADAudit Plus	Home	Reports	File Audit	Server Audit	Alerts	Configuration	Admin	Support		Purchase Now Jump to License Control Licens	Search. O Domen Set
Configured Domain(s	2										+ Aits Dire
adauditplus com	-1										0
Available Domain	Controllers					1	Authenticat	den: Error - The user/system has no admin privil	ese		Audit Policy:Configure
q 😔 🥝 📽 🗉	Ľ										1-6 of 6 23 • T Filter
ACTION	es	DOMAIN CO	NTROLLER NAME	•		EVENT FETCH INTER	VAL	TIMESTAMP OF LAST EVENT	LAST EVENT READ TIME	STATUS	
0 12	010	adap-dc2 ad	auditplus.com			Every 2 hours 🌶		Yet to fetch event data	Feb 05,2019 02:45:07 PM [Run Now]	Error - A required privil.	2
0 0		adap-dc3.ad	auditpluc.com			Every 2 hours /		Yet to fetch event data	Feb 05,2019 02:24:42 PM [Run Now]	Error - Access is denied	C

#### 1.2 Manual configuration

To add a domain: Log in to the ADAudit Plus web console  $\rightarrow$  Domain Settings  $\rightarrow$  Add Domain

 $\rightarrow$  Enter the necessary details.

ADAudit Plus	Reports File Audit	Server Audit	Alerts Co	onfiguration	Purchase N Admin	ow jump to Support	Literse 斗 . Q Search	Jobn ? 🔮 -
Add Domain Details							⇒∳ Ad	d Workgroup Server
	Domain Name a	sdap internal com						
	Authentication Anonymous legin is used when	n no authentication is g	were a					
	Domain User Name:	administrator		Ø				
	Domain Password:							
	Domain Controller Name: Add	I More DCs						
	NAME		EVENT FETC	H MODE				
	adap-dc3		RealTime					
	adap-dc2		RealTime					
		Sove Can	cel					

## 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: If you do not want to provide Domain Admin credentials, you can set-up a service account having only the least privileges required to configure audit policies automatically, following these steps.

								Jump to Lice	nse 📮 J	obs ?
	Home	Reports	File Audit	Server Audit	Alerts	Configuration	Admin	Support	Q Search	O Domain S
nfigured Domain(s)										+ Add Do
adapws 🗸 adaud	itplus.com <del>-</del>									
wailable Domain Cor	ntrollers		× Auth	entication: Error - The	user/system	has no admin privilege			Audit P	ollcy :Configu
Q 🔗 🚫 🕸 🖬 🖸									1-1 of 1	25 <b>▼</b> Filt
ACTIONS	DOMAIN CO	ONTROLLER NA	AME 🔺	EVENT FETCH INTERVA	L TIM	ESTAMP OF LAST EVEN	r la	ST EVENT READ TIME	STATUS	
0 🖬 🕯	adap-ws				Nov	09,2018 01:16:22 PM	No	v 09,2018 01:01:45 PM	Listenin	g for events
									1	-1 of 1 25 🔺

#### 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  $\rightarrow$  Right-click on the relevant Subcategory, and then click Properties  $\rightarrow$  Select Success, Failure, or both; as directed in the table below.

Cateogory	Sub Category	Audit Events
Account Logon	<ul> <li>Audit Kerberos</li> <li>Authentication Service</li> </ul>	<ul> <li>Success and Failure</li> </ul>
Account Management	<ul> <li>Audit Computer Account Management</li> <li>Audit Distribution Group Management</li> <li>Audit Security Group Management</li> </ul>	✓ Success
	<ul> <li>Audit User Account</li> <li>Management</li> </ul>	<ul> <li>Success and Failure</li> </ul>
Detailed Tracking	<ul> <li>Audit Process Creation</li> <li>Audit Process Termination</li> </ul>	<ul> <li>✓ Success</li> </ul>
DS Access	<ul> <li>Audit Directory Services</li> <li>Changes</li> <li>Audit Directory Service Access</li> </ul>	<ul> <li>✓ Success</li> </ul>
Logon /Logoff	<ul><li>Audit Logon</li><li>Audit Network Policy Server</li></ul>	<ul> <li>Success and Failure</li> </ul>
	<ul> <li>Audit Other Logon/Logoff</li> <li>Events</li> <li>Audit Logoff</li> </ul>	<ul> <li>✓ Success</li> </ul>
Object Access	<ul> <li>Audit Other Object</li> <li>Access Events</li> </ul>	✓ Success
Policy Change	<ul> <li>Audit Authentication</li> <li>Policy Change</li> <li>Audit Authorization Policy</li> <li>Change</li> </ul>	<ul> <li>✓ Success</li> </ul>
System	<ul> <li>Audit Security State Change</li> </ul>	✓ Success



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

Note: To enable auditing of NTLM events, log in to ADAudit Plus' web console  $\rightarrow$  Click on the Support tab > Under Support Info, click on More > Under Configuration, click on Enable/Disable Configuration settings > Enable NTLM Auditing.

#### 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  $\rightarrow$  Computer Configuration  $\rightarrow$  Policies
  - $\rightarrow$  Windows Settings  $\rightarrow$  Security Settings  $\rightarrow$  Local Policies  $\rightarrow$  Security Options.
- iii Navigate to the right pane → Right-click on Audit: Force audit policy subcategory settings → Properties → Enable.

<u>a</u>	Group Policy Management Editor		- 0 X
File Action View Help			
Default Domain Controllers Policy     Default Domain Controllers Policy     Compared Compared     Default Domain Controllers Policy     Default Domain Controllers     Default Domain Controllers     Default Policies     Default Policies	Petry Accounts Bick Microsoft account status Accounts Bick Microsoft accounts Accounts Bick Microsoft accounts Accounts Bick Microsoft accounts Accounts Rename administrator account Accounts Rename guest account Audit: Audit the access of global system objects Audit: Audit the access of global system objects Audit: Force audit policy subcategory settings Microsoft Force audit policy subcategory settings Audit: Force audit policy subcategory settings Audit: Force audit policy subcategory settings Audit: Addit forces audit policy subcategory settings Audit: Force audit policy subcategory settings Audit: Addit forces audit policy subcategory settings Audit: Addit forces audit policy subcategory settings Audit: Destated Audit: Destated Audit: Destated Audit: Addit forces Audit: Addit: Addit forces Audit: Addit: Addit forces Audit: Addit: Addit	Policy Setting Not Defined Not Defined	
	OK Cancel Acoly		

#### 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  $\rightarrow$  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	<ul> <li>Success and Failure</li> </ul>
Audit Logon / Logoff	✓ Success and Failure
Account Management	✓ Success
<ul> <li>Directory Service Access</li> </ul>	✓ Success
Process Tracking	✓ Success
<ul> <li>Object Access</li> </ul>	✓ Success
System Events	<ul> <li>✓ Success</li> </ul>



Image showing: Audit account logon events category  $\rightarrow$  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  $\rightarrow$  Reports  $\rightarrow$  GPO Management  $\rightarrow$  GPO History  $\rightarrow$  Object level auditing needs to be configured for getting proper reports: Configure.

ADAudit Plus	ne Reports	File Audit	Server Audit	Alerts	Configuration	Admin Su	pport	Q Search	jobs : Ö Dom	o v ain Settings
🍳 Logon Audit 🗸 🛛 AD Changes 🗸	GPO Changes 👻	Compliance 👻	1		@Analytics	Custom Reports	😧 Sch	edule Reports	强 Aggreg	gate Reports
Active Directory	GPO History (From Oct 10,2018 03)	:41:13 PM to Nov 09,2	018 03:41:13 PM)			Dom	ain adaa	auditplus.com		*
User Logon Reports			Object level aud	iting needs	to be configured for	getting proper reports	. Configure			×
ADFS Auditing	Period 🛗 La	ist 30 Days	Hours	All		✓ Select Objects	All		<b>2</b> + /	Add
Account Management								🖸 Export As	Add to	E: More
User Management ) Group Management ) Computer Management )	GPO History									
OU Management   GPO Management  Recently Created GPOs  Recently Deleted GPOs  Devent Medical CPOs				(i	No Data Availabl	e bleshoot				
GPO Link changes										
GPO History										Ę

#### 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  $\rightarrow$  Properties  $\rightarrow$  Security  $\rightarrow$  Advanced  $\rightarrow$  Auditing  $\rightarrow$  Add.
- iii In the Auditing Entry window  $\rightarrow$  Select a principal: Everyone  $\rightarrow$  Type: Success  $\rightarrow$  Select the appropriate permissions, as directed in the table below.

Auditing Entry	Auditing Entry for	Access	Apply onto			
number			Windows Server 2003	Windows Server 2008 and above		
182	OU	<ul> <li>Create Organizational Unit objects</li> <li>Delete Organizational Unit objects</li> </ul>	This object and all child objects	This object and all descendant objects		
		<ul><li>Write All Properties</li><li>Delete Modify Permissions</li></ul>	Organizational Unit objects	Descendant Organizational Unit objects		
3&4	GPO	<ul> <li>Create groupPolicy Container Objects</li> <li>Delete groupPolicy Container Objects</li> </ul>	This object and all child objects	This object and all descendant objects		
		<ul><li>Write All Properties</li><li>Delete</li><li>Modify Permissions</li></ul>	groupPolicy Container objects	Descendant groupPolicy Container objects		
586	User	<ul><li>Create User Objects</li><li>Delete User Objects</li></ul>	This object and all child objects	This object and all descendant objects		
		<ul> <li>Write All Properties</li> <li>Delete</li> <li>Modify Permissions</li> <li>All Extended Rights</li> </ul>	User objects	Descendant User objects		
788	Group	<ul><li>Create Group Objects</li><li>Delete Group Objects</li></ul>	This object and all child objects	This object and all descendant objects		
		<ul> <li>Write All Properties</li> <li>Delete</li> <li>Modify Permissions</li> <li>All Extended Rights</li> </ul>	Group objects	Descendant Group objects		

9&10	Computer	<ul> <li>Create Computer Objects</li> <li>Delete Computer Objects</li> </ul>	This object and all child objects	This object and all descendant objects
		<ul> <li>Write All Properties</li> <li>Delete</li> <li>Modify Permissions</li> <li>All Extended Rights</li> </ul>	Computer objects	Descendant Computer objects
11812	Contact	<ul> <li>Create Contact Objects</li> <li>Delete Contact Objects</li> </ul>	This object and all child objects	This object and all descendant objects
		<ul><li>Write All Properties</li><li>Delete</li><li>Modify Permissions</li></ul>	Contact objects	Descendant Contact objects

Action View Help		
+ 2 📷 ¥ 🗆 🗙 🖬 📾 📾 🔧	a 🔻 🖬 🛰	
Active Directory Users and Computers (ADAP-DC3-adap A Saved Queries adsp.internal.com	Advanced Security Settings for adap	
adap.internal.com Properties ?	Owner: Administrators (ADAP-Administrators) Change	
eneral   Managed By   Object   Security   Entbute Editor	Permissions Auditing Effective Access	
Sroup or user names:	Auditing Entry for a	
Bereynone     Scretz FOR OWNER     Scretz FOR OWNER     Scretz     Screz	Principal: Everyone select a principal     Type: Success     V     Applies to: This object and all descendent objects     V	
Pemiasions for Everyone Allow Deny		
Full control	Pull control     Delete     List contents     Read all properties     Write all properties     Create	45MQ Queue Alias objects nsPKI-Key-Recovery-Agent objects nsPKI-Key-Recovery-Agent objects nsPU3Mai/Aliases objects
For special permissions or advanced settings, click Advanced Volvenced.	Delete     Delete     Delete     Delete     Delete     Delete     Create     Read permissions     Delete     Delete     Delete     Create     Delete	nsFFU3OMaitAliases objects nsSFU3ONetid objects nsSFU3ONetid objects nsSFU3ONetid objects
OK Cancel Apply He	Modify owner Delete	ns\$FU30NetworkUser objects
0.0 ADAP         0.0 ADAP	ever      All validated writes     eremin     All autoridated writes     eremin     All extended rights     Delete     Create All bild objects     Create All bild objects     Create Computer objects     Delete     Create Consult objects     Delete     Delete friendly Country objects     Delete     Delete	nsTPAI-InformationObjectsContainer objects wiTPAI-InformationObjectsContainer objects isMap objects isMap objects isMapsopup objects isMapsopup objects isObject objects isObject objects ncRac objects ncRac objects Typanizational Unit objects Typanizational Unit 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  $\rightarrow$  Click on Default naming context  $\rightarrow$  Right click on domains distinguished name  $\rightarrow$  Select properties  $\rightarrow$  Security  $\rightarrow$  Advanced  $\rightarrow$  Auditing  $\rightarrow$  Add.
- iv In the Auditing Entry window  $\rightarrow$  Select a principal: Everyone  $\rightarrow$  Type: Success  $\rightarrow$  Select the appropriate permissions, as directed in the table below.

Auditing Entry	Access	Apply onto				
		Windows Server 2003	Windows Server 2008 and above			
Container	<ul><li>Write All Properties</li><li>Delete</li><li>Modify Permissions</li></ul>	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  $\rightarrow$  Click on Default naming context  $\rightarrow$  Expand the domain  $\rightarrow$ Expand the System container  $\rightarrow$  Right click on the Password Settings Container  $\rightarrow$  Properties  $\rightarrow$  Security  $\rightarrow$  Advanced  $\rightarrow$  Auditing  $\rightarrow$  Add.
- iv In the Auditing Entry window  $\rightarrow$  Select a principal: Everyone  $\rightarrow$  Type: Success  $\rightarrow$  Select the appropriate permissions, as directed in the table below.

Auditing Entry number	Auditing Entry for	Access	Apply onto		
			Windows Server 2003	Windows Server 2008 and above	
182	Password Settings Container	<ul> <li>Create msDS-Password Settings objects</li> <li>Delete msDS-Password Setting objects</li> </ul>	Not Applicable	This object and all descendant objects	
		<ul><li>Write All Propertie</li><li>Delete</li><li>Modify Permissions</li></ul>	Not Applicable	Descendant msDS- PasswordSettings objects	

2		ADSI Edit		= <b>D</b> X		
File Action View Help						
◆ ⇒ 2 00 × 0 2 2 00						
OU=GPOtest	1	CN=Password Settings Container Propertie	AL :	Auditing Entry for	Password Settings Container	
OU=kesh-test		In the second seco				
OU=LAPS		Atribute Editor Security	Principal: Everyone Select a principal			
CN=LestAndFound		Advanced Securit	Type: Success	~		
CN=Mahi		1	Applies to: This object and all descendant	objects v		
CN=NTDS Quotes		Owner: Domain Admins (ADAP\Domain Adv				
OU=OtherlanguageUsers		Providence Development Development				
OU=OU - ADAP		Permissions Auditing Effective Access	Permissions:			
CN=Program Data		For additional information, double-click an audit entr	E Full control		Modify permissions	
OU=QAtest_dontdelete		Auditing entries:	List contents		Modify owner	
OU=Ramy		Type Principal Acces	Read all properties		All validated writes	
CN_Rolet		& Succ Everyone Speci-	Write all properties		Create all child objects	
OU=Sarath_test		Succ Everyone Speci	Delete		Delete all child objects	
OU=Sathis_OU_Rename_1		Succ Everyone Speci	Delete subtree		Create msDS-PasswordSettings objects	
OIL-SUC		Se Succ Everyone Speci.	Read permissions		Delete msDS-PasswordSettings objects	
a CN=System		A Surr Everyone Speci	Properties			
CN=ComPartitions		Succ. Everyone Specia	Read all properties		Write msDS-NeTupe	
CN= ComPartitionSets		& Succ Everyone Speci	Write all properties		Read mcDS-NonMembersBL	
CN=Default Domain Policy	-	💐 Succ Everyone Speci	Read adminDescription		Write msDS-NonMembersBL	
CN=Dfc-Configuration	-	A Fail Everyone Full o	Write adminDescription		Read msDS-ObjectReferenceBL	
CN=DrmainUndates			Read adminDisplayName		Write msDS-ObjectReferenceBL	
CN=File Replication Service		Add Nemove View	Write adminDisplayName		Read mcDS-ObjectSoa	
CNu FileLinks		Disable inheritance	Read allowedAttributes		Write msDS-ObjectSoa	
CNuIP Security			17140.5 # 046.5 F		Fig. 1 sc. sist c 11.16	
Chi-MicrosoftChis						OK Cance
CN=Password Settings Container				E		
LINE POICIES						
CN=PSPs	e 🗌					
Charlos and IAS Servers Access Chec	ð.					
CNuWinsockServices						
CN=WMIPolicy						

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  $\rightarrow$  Click on Configuration  $\rightarrow$  Right click on Configuration naming context  $\rightarrow$  Select properties  $\rightarrow$  Security  $\rightarrow$  Advanced  $\rightarrow$  Auditing  $\rightarrow$  Add.
- iv In the Auditing Entry window  $\rightarrow$  Select a principal: Everyone  $\rightarrow$  Type: Success  $\rightarrow$  Select the appropriate permissions, as directed in the table below.

Auditing Entry for	Access	Apply onto		
		Windows Server 2003	Windows Server 2008 and above	
Configur ation	<ul> <li>Create All Child objects</li> <li>Write All Properties</li> <li>Delete All child objects</li> <li>Delete</li> <li>Modify Permissions</li> <li>All Extended Rights</li> </ul>	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.
- In the Connection Settings window → Under Select a Well-Known Naming Context →
   Select Schema
- iii Navigate to the left panel  $\rightarrow$  Click on Schema  $\rightarrow$  Right click on Schema naming context  $\rightarrow$  Select properties  $\rightarrow$  Security  $\rightarrow$  Advanced  $\rightarrow$  Auditing  $\rightarrow$  Add.
- iv In the Auditing Entry window  $\rightarrow$  Select a principal: Everyone  $\rightarrow$  OK  $\rightarrow$  Type: Success  $\rightarrow$  Select the appropriate permissions, as directed in the table below.

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

2	ADSI Edit	_ <b>_</b> X	
File Action View Help			
🗢 🔿 📶 🖬 🖬 📓 🖬			
ADSI Edit			
Default naming context [ADAP-DC3.adap.internal.com]	CN=Schema,CN=Configuration,DC=adap,DC=i		
Configuration [ADAP-DC3.adap.internal.com]	Advanced Security	Settings for Schema	
Schema [ADAP-DC3.adap.internal.com]			
RootDSE [ADAP-DC3.adap.internal.com]			
Default naming context [ADAP-DC3.adap.internal.com]	Owner: Schema Admins (ADAP\Schema Admins) Change	1	
Default naming context [ADAP-DC3.adap.internal.com] Default naming context [ADAP-DC3.adap.internal.com]	Permissions Auditing Effective Access		
Configuration (ADAP-DC3.adap.internal.com)	A A	uditing Entry for Schema	_ <b>□</b> X
Schema (ADAP-DC3.adap.internal.com)	Type: Success	1	<u>^</u>
	Applies to: This object and all descendant objects 🗸 🗸		=
	Permissions:		
	Full control	✓ Create classSchema objects	
	List contents	Delete classSchema objects	
	Read all properties	Create lostAndFound objects	
	Write all properties	✓ Delete lostAndFound objects	
	✓ Delete	✓ Change schema master	
	Delete subtree	Manage replication topology	
		Read only replication secret synchronization	
	Modify owner	Reanimate tombstones	
	☐ All validated writes	Replicating Directory Changes	
	All extended rights	Replicating Directory Changes All	
	Create all child objects	Replicating Directory Changes In Filtered Set	
	Delete all child objects	Replication synchronization	
	Create attributeSchema objects	✓ Update schema cache	
	Delete attributeSchema objects		
	Properties		
	Read all properties	Read mcDS-ObjectReferenceBI	
	Write all properties	Write mrDS-ObjectReferenceBl	~
	L		OK Cancel

#### **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.
- 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.

Connection Settings				
Name: Default naming context				
Path: LDAP://ADAP-DC3.adap.internal.com/DC=DomainDNSZones,DC=				
Connection Point				
Select or type a Distinguished Name or Naming Context:				
DC=DomainDNSZones,DC=adap,DC=internal,DC=com 🗸				
O Select a well known Naming Context:				
Default naming context 🗸 🗸				
Computer				
○ Select or type a domain or server: (Server   Domain [:port])				
✓				
Default (Domain or server that you logged in to)				
Use SSL-based Encryption				
Advanced OK Cancel				

📝 ADSI Edit			
File Action View Help			
🗢 🔿 🛅 🐹 📷 🖄	?		
ADSI Edit	Name CN=AdminSDHolder CN=ComPartitions CN=ComPartitionSets CN=Default Domain Policy CN=Dfs-Configuration CN=DFSR-GlobalSettings CN=File Replication Service CN=File Replication Service CN=FileLinks CN=IP Security CN=Meetings CN=MicrosoftDNS CN=Password Settings Con CN=Policies CN=PSPs CN=RAS and IAS Servers Ac CN=RpcServices CN=WMIPolicy CN=BCKUPKEY_B7f03459-a CN=BCKUPKEY_PSecret CN=BCKUPKEY_PSecret CN=RDD ManagerS CN=RD ManagerS	Class container container domainPolicy dfsConfigura msDFSR-Glo container nTFRSSettings fileLinkTracki container container container msDS-Passw container msImaging container rpcContainer container container secret secret secret secret secret rIDManager camSenver	Distinguished Name CN=AdminSDHolder, C CN=ComPartitions, CN CN=ComPartitionSets, CN=Default Domain P CN=Dfs-Configuratior CN=DFSR-GlobalSettir CN=DFSR-GlobalSettir CN=DFSR-GlobalSettir CN=DFSR-GlobalSettir CN=FileLinks, CN=Syst CN=FileLinks, CN=Syst CN=IP Security, CN=Sy CN=Meetings, CN=Syst CN=Policies, CN=Syste CN=PSPs, CN=Syste CN=PSPs, CN=Syste CN=RAS and IAS Serve CN=RpCServices, CN=S CN=WINPOLicy, CN=S CN=BCKUPKEY_B7034 CN=BCKUPKEY_PSecr CN=BCKUPKEY_PSecr CN=RID ManagerS, CN
< >	<		>

- iii Navigate to the left panel  $\rightarrow$  Click on Default naming context  $\rightarrow$  Right click on MicrosoftDNS  $\rightarrow$  Select properties  $\rightarrow$  Security  $\rightarrow$  Advanced  $\rightarrow$  Auditing  $\rightarrow$  Add.
- iv In the Auditing Entry window  $\rightarrow$  Select a principal  $\rightarrow$  Everyone  $\rightarrow$  OK  $\rightarrow$  Type: Success  $\rightarrow$  Select the appropriate permissions, as directed in the table below.

	A	uditing Entry for MicrosoftDNS		
L M	- Available only seconds for a	Create Container objects	Delete msPKI-Key-Recovery-Agent objects	
N=MicrosoftDNS Proper		Delete Container objects	Create msPKI-PrivateKeyRecoveryAgent objects	
thrbute Editor Security	Owner: SYSTEM Chang	Create controlAccessRight objects	Delete msPKI-PrivateKeyRecoveryAgent objects	
Group or user names:		Delete controlAccessRight objects	Create msPrint-ConnectionPolicy objects	
A CREATOR OWNER	Permissions Auditing	Create cRLDistributionPoint objects	Delete msPrint-ConnectionPolicy objects	
SELF	For additional information, doubt	Delete cRLDistributionPoint objects	Create msSFU30DomainInfo objects	
SYSTEM	Per additional information, doubl	Create device objects	Delete msSFU30DomainInfo objects	
DrsAdmins (FILEAUD	Auditing entries:	Delete device objects	Create msSFU30MailAliases objects	
R Enternine Admins (FILE)	Type Principal	Create dfsConfiguration objects	Delete msSFU30MailAliases objects	
	88. Succ Everyone	Delete dfsConfiguration objects	Create msSFU30NetId objects	
	🚨 Succ Everyone	Create dHCPClass objects	Delete msSFU30NetId objects	
emissions for CREATOR	Succ Everyone	Delete dHCPClass objects	Create msSFU30NetworkUser objects	
Full control	Succ Everyone	Create displaySpecifier objects	Delete msSFU30NetworkUser objects	
Read	Succ Everyone	Delete displaySpecifier objects	Create msSFU30NISMapConfig objects	
Wite	Ma Succ Everyone	Create displayTemplate objects	Delete msSFU30NISMapConfig objects	
Create all child objects		Delete displayTemplate objects	Create msSPP-ActivationObjectsContainer objects	
Control de Cristo Collecto		Create dnsZone objects	Delete msSPP-ActivationObjectsContainer objects	
or special permissions or a		Delete dnsZone objects	Create mS-SQL-OLAPServer objects	
		Create document objects	Delete mS-SQL-OLAPServer objects	
	Add Remove	Delete document objects	Create mS-SQL-SQLServer objects	
OF	Disable inheritance	Create documentSeries objects	Delete mS-SQL-SQLServer objects	
OK	Crocket and Charles	Delete documentSeries objects	Create msWMI-MergeablePolicyTemplate objects	
		Create Domain Policy objects	Delete msWMI-MergeablePolicyTemplate objects	
6		Delete Domain Policy objects	Create msWMI-ObjectEncoding objects	
		Create dSA objects	Delete msWMI-ObjectEncoding objects	

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

Auditing Entry	Auditing Entry for	Access	Apply onto		
number			Windows Server 2003	Windows Server 2008 and above	
182	DNS Zones	<ul> <li>Create DNS Zones objects</li> <li>Delete DNS Zones objects</li> </ul>	This object and all child objects	This object and all descendant objects	
		<ul><li>Write All Properties</li><li>Delete</li><li>Modify Permissions</li></ul>	DNS Zone objects	Descendant DNS Zone objects	
3&4 Permissions	DNS Nodes	<ul> <li>Create DNS Nodes objects</li> <li>Delete DNS Nodes objects</li> </ul>	This object and all child objects	Descendant DNS Zone objects	
		<ul><li>Write All Properties</li><li>Delete</li><li>Modify Permissions</li></ul>	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.

Class container container container lomainPolicy	Distinguished Name CN=AdminSDHolder, ( CN=ComPartitions, CN
Class container container container domainPolicy	Distinguished Name CN=AdminSDHolder, CN=ComPartitions, CN
Class container container container lomainPolicy	Distinguished Name CN=AdminSDHolder, ( CN=ComPartitions, CN
IfsConfigura nsDFSR-Glo iontainer nTFRSSettings ileLinkTracki container container nsDS-Passw container nsImaging container pcContainer container ecret ecret ecret ecret ecret ecret ecret ecret ecret ecret ecret	CN=ComPartitionSets, CN=Default Domain P CN=Dfs-Configuration CN=DfSR-GlobalSettir CN=DomainUpdates, C CN=File Replication Se CN=FileLinks, CN=Syst CN=IP Security, CN=Sy CN=Meetings, CN=Syst CN=Meetings, CN=Syst CN=Password Settings CN=Policies, CN=Syste CN=PSPs, CN=System, CN=RAS and IAS Serve CN=RpcServices, CN=S CN=WinsockServices, C CN=WinsockServices, C CN=WMIPolicy, CN=S CN=BCKUPKEY_B703- CN=BCKUPKEY_PSeci CN=BCKUPKEY_PSeci CN=BCKUPKEY_PSeci CN=RID Manager\$, CN CN=Server CN-System
	simaging ontainer occontainer ontainer ontainer ortai

## 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  $\rightarrow$  Open Run  $\rightarrow$  Type eventvwr.ms  $\rightarrow$  Right click on Event Viewer  $\rightarrow$  Connect to the target computer  $\rightarrow$  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.

#### 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.

🛨 Download