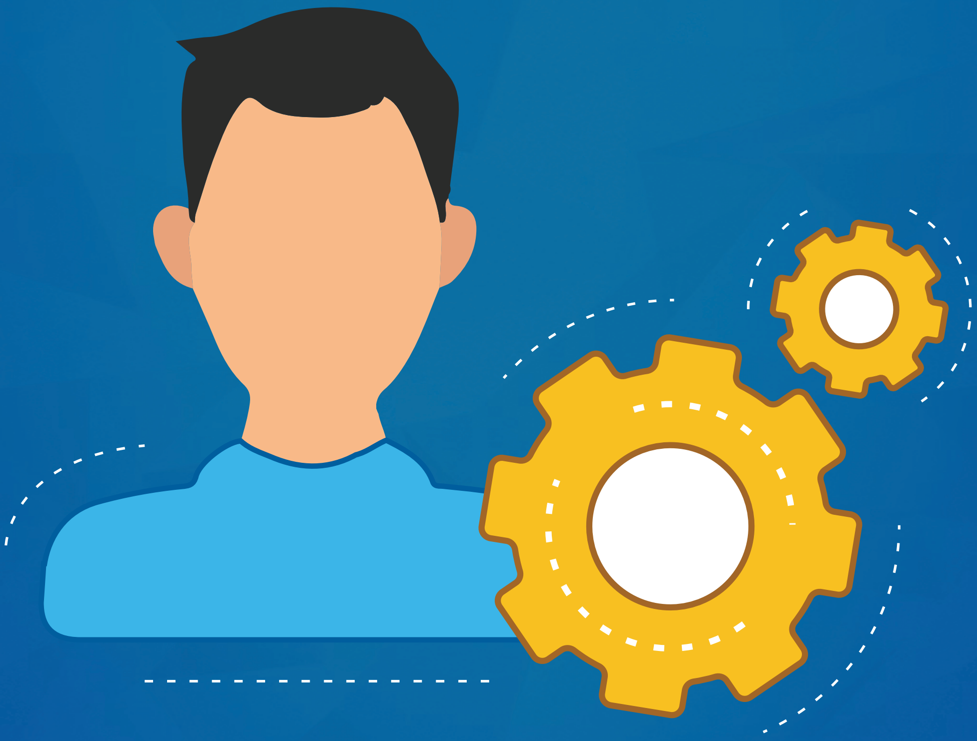
ManageEngine
ADAudit Plus

ADAudit Plus
Service Account Configuration



www.adauditplus.com

Table of Contents

Introduction

ADAudit Plus instantly starts to audit activities upon providing Domain Admin credentials. If you do not want to provide Domain Admin credentials, follow the steps laid out in this guide to set-up the service account to have only the least privileges required for auditing your environment.

Note: If you want to configure multiple domains in ADAudit Plus, we recommend creating separate service accounts for each individual domain.

1. New user, group, and GPO creation

1.1 Create a new user

- **Log in to your Domain Controller with Domain Admin privileges**→Open Active Directory Users and Computers→Right click on your domain→New→User→Name the user as "***ADAudit Plus***".

1.2 Create a new group

- **Log in to your Domain Controller with Domain Admin privileges**→Open Active Directory Users and Computers→Right click on your domain→New→Group→Name the group as "***ADAudit Plus Permission Group***".

- **Add all the audited computers as members of the "*ADAudit Plus Permission Group*":** Right click on the "***ADAudit Plus Permission Group***"→Properties→Members→Add all the Domain Controllers, Windows servers and workstations that you wish to audit.

1.3 Create a new domain level GPO and link it to all the audited computers

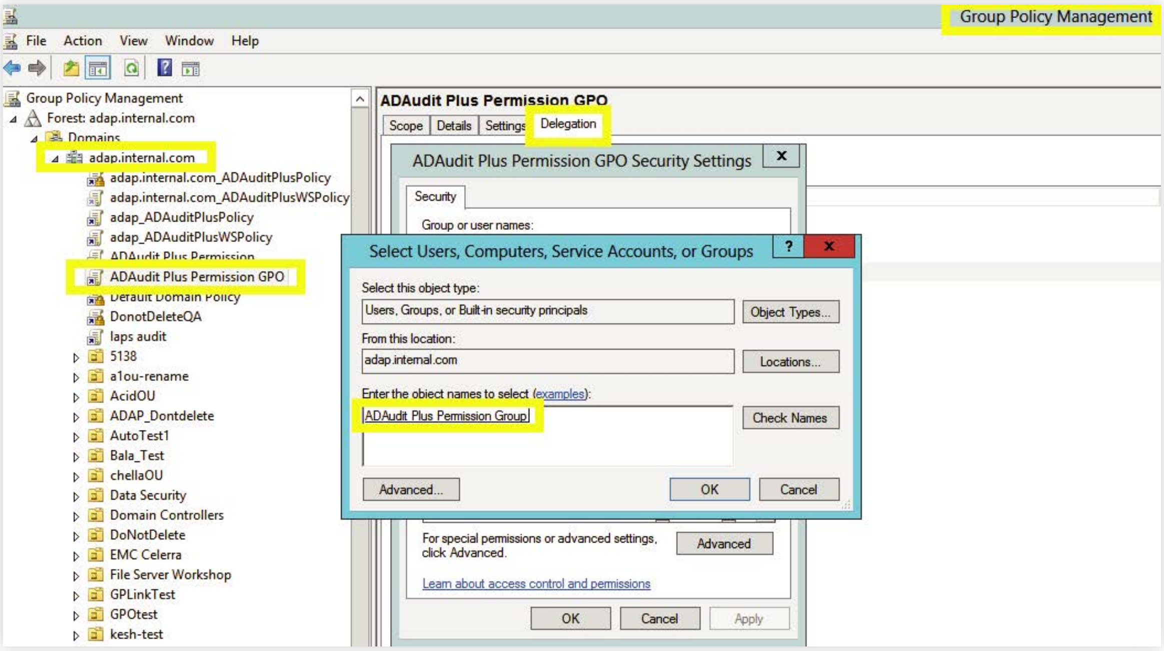
Since configuring permissions on individual computers is an elaborate process, a domain level GPO is created and applied on all monitored computers.

- **Log in to your Domain Controller with Domain Admin privileges.**

- **Create a new domain level GPO:** Open the Group Policy Management Console→Right click on your domain→Create a GPO in this domain and link it here→Name the GPO as **"ADAudit Plus Permission GPO"**

- **Remove Apply group policy permission for Authenticated Users group:** Click on the "ADAudit Plus Permission GPO"→Navigate to the right panel, click on the Delegation tab→Advanced→Click on Authenticated Users→Remove the Apply group policy permission.

- **Add the "ADAudit Plus Permission Group" to the security filter settings of the "ADAudit Plus Permission GPO":**
  Open the Group Policy Management Console ⟶ Domain ⟶ Select the "ADAudit Plus Permission GPO" ⟶ Navigate to the right panel, click on the Delegation tab ⟶ Advanced ⟶ Add "ADAudit Plus Permission Group".



Select this object type:
Users, Groups, or Built-in security principals

From this location:
adap.internal.com

Enter the object names to select (examples):
ADAudit Plus Permission Group

For special permissions or advanced settings, click Advanced.

2. Privileges/permissions required for event log collection

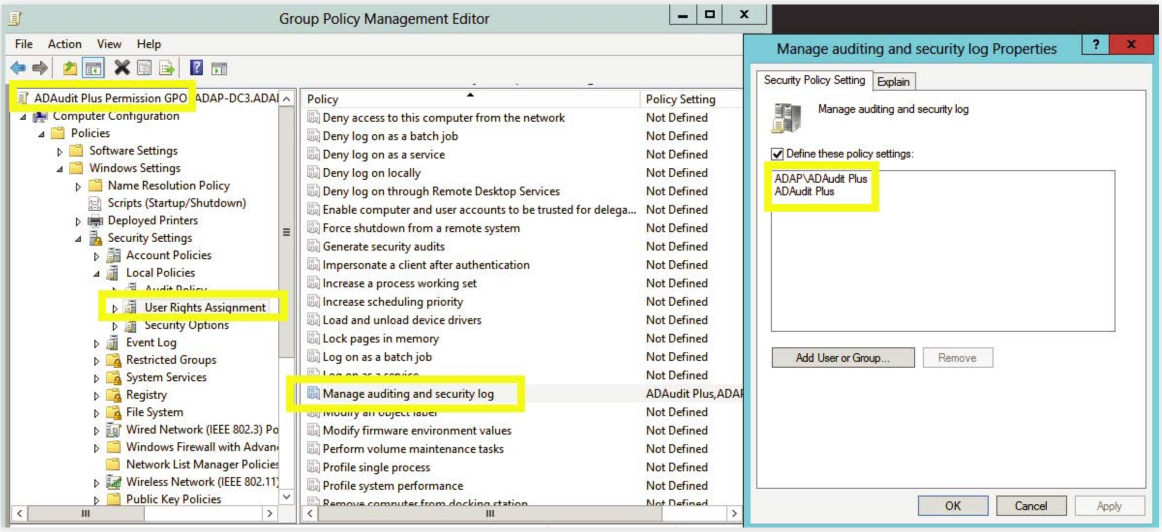
2.1 Grant the user the Manage auditing and security log right

The Manage auditing and security log right allows the user to define object level auditing.

- **Log in to your Domain Controller with Domain Admin privileges** ⟶ Open the Group Policy Management Console ⟶ Right click on the "ADAudit Plus Permission GPO" ⟶ Edit.

- In the Group Policy Management Editor ⟶ Computer Configuration ⟶ Policies ⟶ Windows Settings ⟶ Security Settings ⟶ Local Policies ⟶ User Rights Assignment.

- Navigate to the right panel, right click on Manage auditing and security log ⟶ Properties ⟶ **Add the "ADAudit Plus" user.**



Policy	Policy Setting
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Manage auditing and security log	ADAudit Plus,ADAP
Modify an object label	Not Defined
Modify firmware environment values	Not Defined
Perform volume maintenance tasks	Not Defined
Profile single process	Not Defined
Profile system performance	Not Defined
Remove computer from docking station	Not Defined

Manage auditing and security log Properties

Security Policy Setting | Explain

Manage auditing and security log

☑ Define these policy settings:

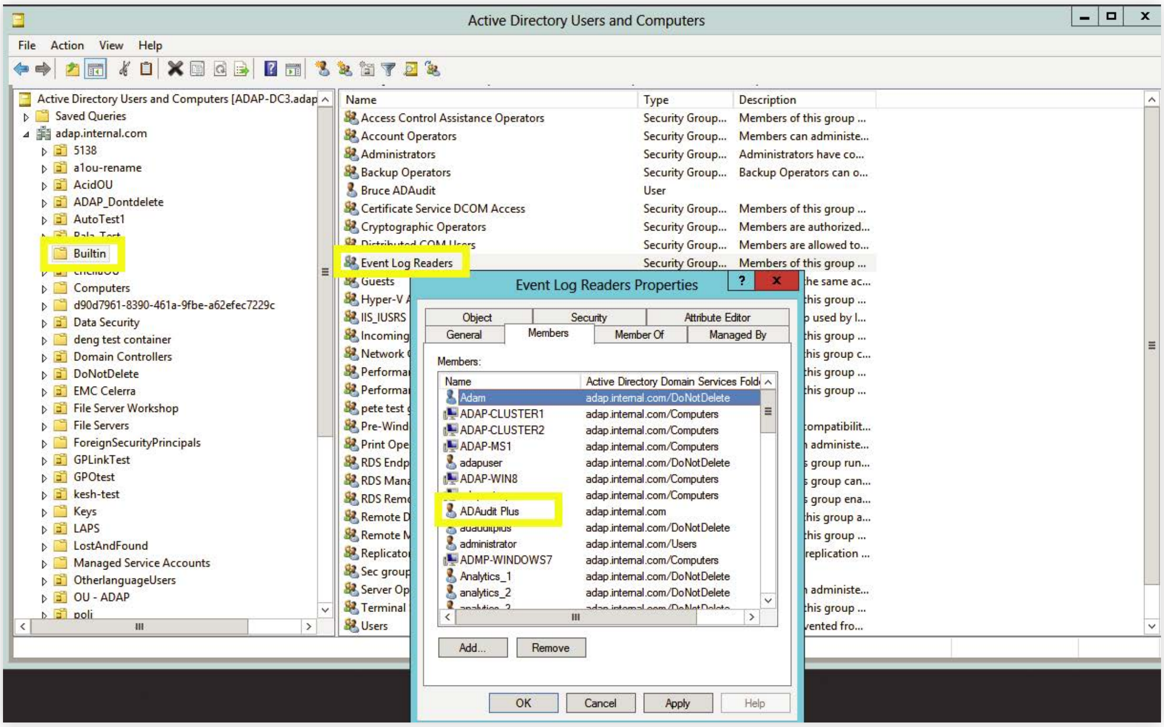
ADAP\ADAudit Plus
ADAudit Plus

2.2 Make the user a member of the Event Log Readers group

Members of the event log readers group will be able to read the event logs of all the audited computers.

- **For Domain Controllers:**

  Log in to your Domain Controller with Domain Admin privileges → Open Active Directory Users and Computers → Builtin Container → Navigate to the right panel, right click on Event Log Readers → Properties → Members → **Add the "ADAudit Plus" user.**



Name	Type	Description
Access Control Assistance Operators	Security Group...	Members of this group ...
Account Operators	Security Group...	Members can administe...
Administrators	Security Group...	Administrators have co...
Backup Operators	Security Group...	Backup Operators can o...
Bruce ADAudit	User	
Certificate Service DCOM Access	Security Group...	Members of this group ...
Cryptographic Operators	Security Group...	Members are authorized...
Distributed COM Users	Security Group...	Members are allowed to...
Event Log Readers	Security Group...	Members of this group ...
Guests		

Event Log Readers Properties

Object | Security | Attribute Editor
General | Members | Member Of | Managed By

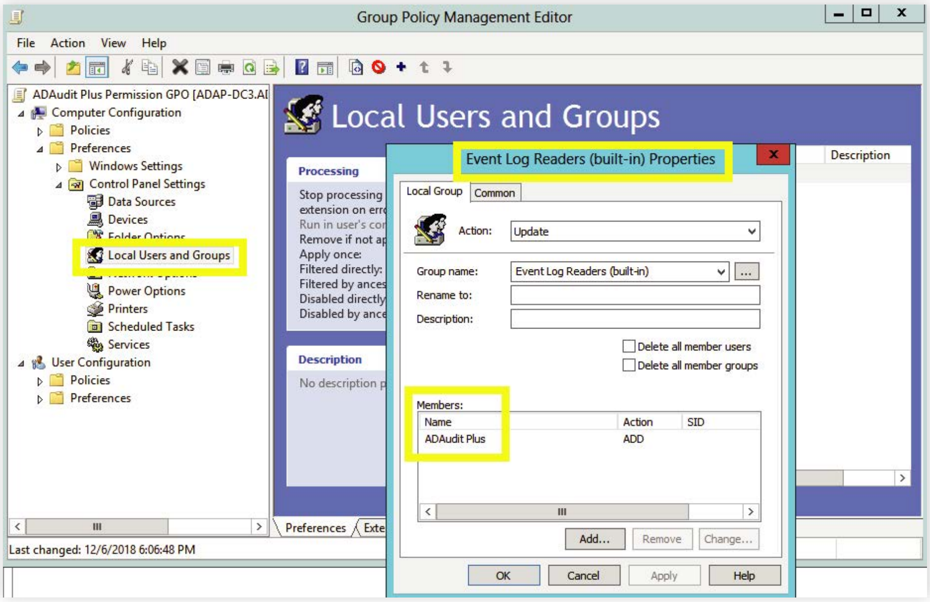
Members:

Name	Active Directory Domain Services Folder
Adam	adap.internal.com/DoNotDelete
ADAP-CLUSTER1	adap.internal.com/Computers
ADAP-CLUSTER2	adap.internal.com/Computers
ADAP-MS1	adap.internal.com/Computers
adapuser	adap.internal.com/DoNotDelete
ADAP-WIN8	adap.internal.com/Computers
	adap.internal.com/Computers
ADAudit Plus	adap.internal.com
adauditplus	adap.internal.com/DoNotDelete
administrator	adap.internal.com/Users
ADMP-WINDOWS7	adap.internal.com/Computers
Analytics_1	adap.internal.com/DoNotDelete
analytics_2	adap.internal.com/DoNotDelete

- **For other computers (Windows servers and workstations):**

  a. **Log in to your Domain Controller with Domain Admin privileges**→Open the Group Policy Management Console→Right click on the "ADAudit Plus Permission GPO"→Edit.

  b. In the Group Policy Management Editor→Computer Configuration→Preferences→ Control Panel Settings →Right click on Local Users and Groups →New →Local Group→ Select Event Log Readers group under group name→**Add the "ADAudit Plus" user.**



Group Policy Management Editor

Event Log Readers (built-in) Properties

Action: Update

Group name: Event Log Readers (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

Name	Action	SID
ADAudit Plus	ADD	

Last changed: 12/6/2018 6:06:48 PM

<span style="color:red">**Note:**</span> To read the event logs, you also need to grant the "**ADAudit Plus**" user **Read** permission over **HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security.**

- Log in to your Domain Controller with Domain Admin privileges →Open the Group Policy Management Console→ Right click on the "**ADAudit Plus Permission GPO**"→ Edit.

- In the Group Policy Management Editor →Computer Configuration →Policies →Windows Settings → Security Settings→ Right-click Registry → Add Key.

- In the Select Registry Key Window, navigate to MACHINE →SYSTEM →CurrentControlSet → Services →EventLog →Security→ Click OK → Grant **Read** permission to "**ADAudit Plus**" user → Click Apply.

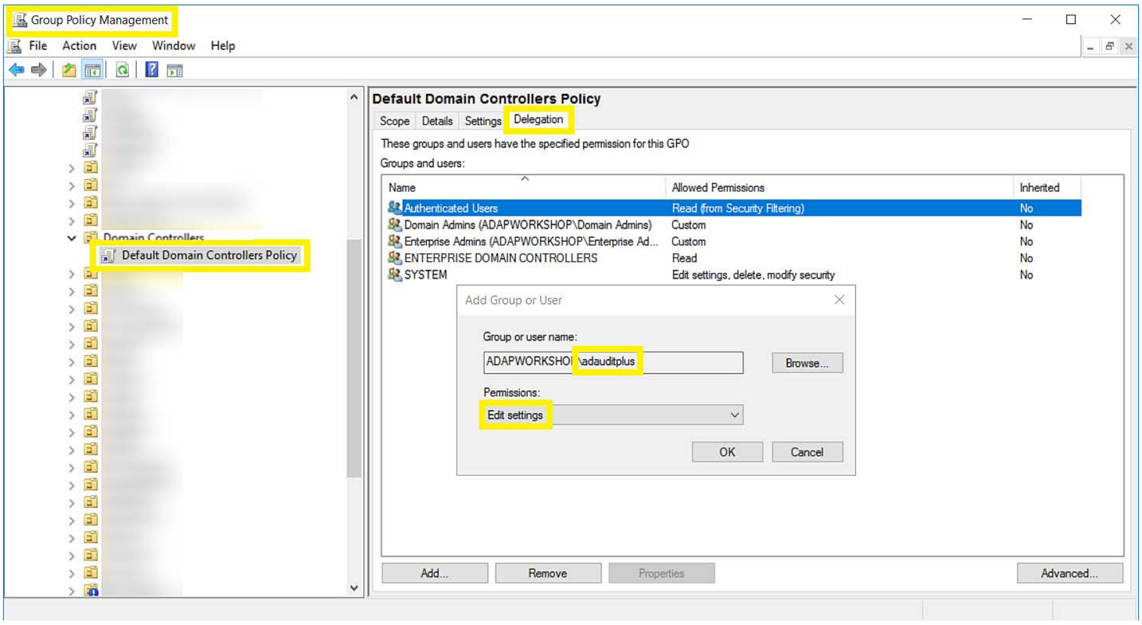
- In the Add Object window, select **Configure this key then**→ **Replace existing permissions on all subkeys with inheritable permissions**→ Click OK.

3. Privileges/permissions required for automatic audit policy and object level auditing configuration

3.1 Privileges/permissions required for Domain Controller auditing configuration

Granting the service account the following privileges/permissions, allows ADAudit Plus to automatially configure the required audit policy and object level auditing settings in your environment. ADAudit Plus does this by pushing the required settings via GPO, to the group which contains all the monitored computers.

- **Log in to your Domain Controller with Domain Admin privileges** → Open the Group Policy Management Console → click on Default Domain Controllers Policy → Navigate to the right panel, click on the Delegation tab → **Add the ADAudit Plus User** → Provide permission to Edit settings.



Default Domain Controllers Policy

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (ADAPWORKSHOP\Domain Admins)	Custom	No
Enterprise Admins (ADAPWORKSHOP\Enterprise Ad...	Custom	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

Add Group or User

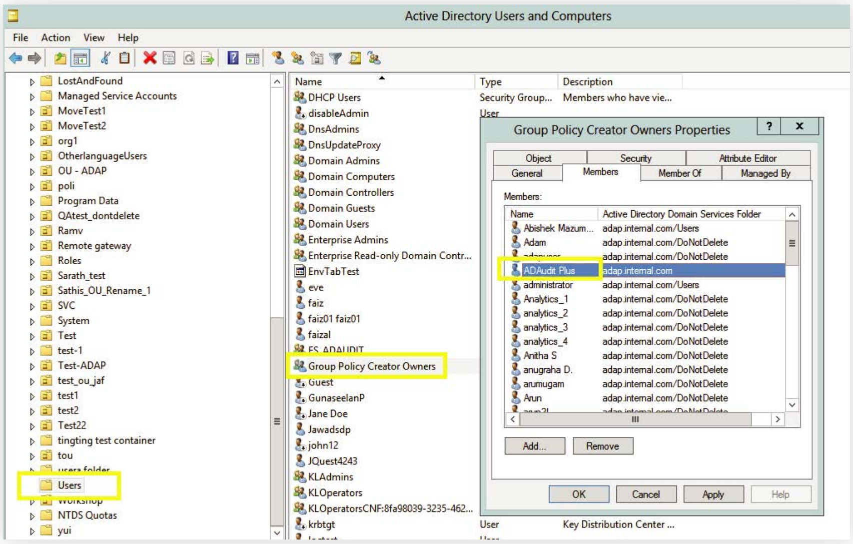
Group or user name: ADAPWORKSHOP\adauditplus

Permissions: Edit settings

3.2 Privileges/permissions required for member server, workstation, and file server auditing configuration

3.2.1 Make the user a member of the Group Policy Creator Owners group

- **Log in to your Domain Controller with Domain Admin privileges** → Open Active Directory Users and Computers → Click on Users → Navigate to the right panel, right click on Group Policy Creator Owners group → **Add the "ADAudit Plus" user as a member.**



Active Directory Users and Computers

Group Policy Creator Owners Properties

Members:

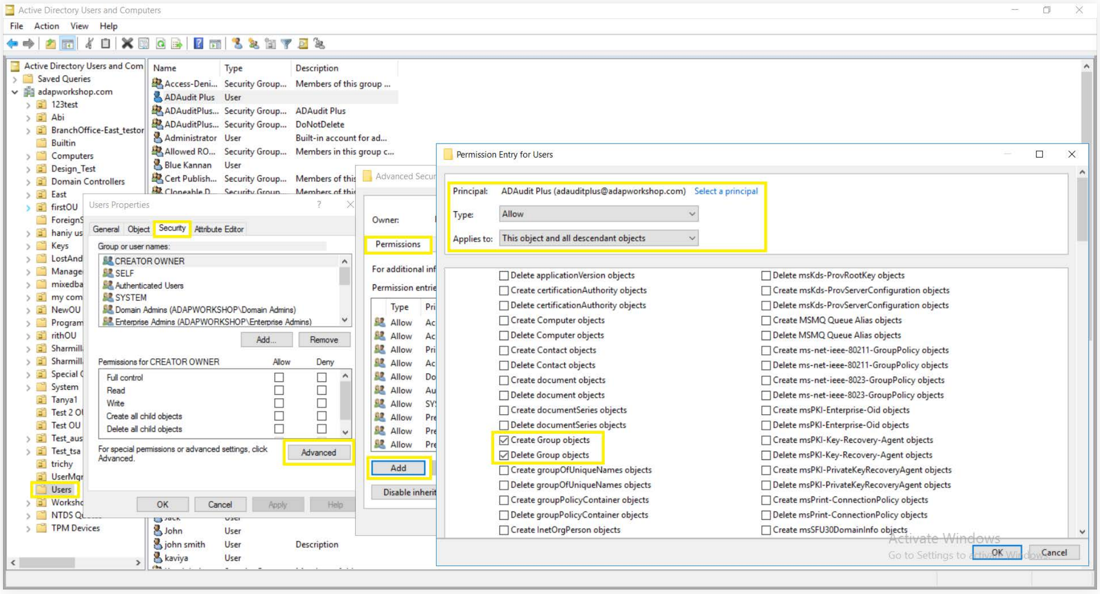
Name	Active Directory Domain Services Folder
Abishek Mazum...	adap.internal.com/Users
Adam	adap.internal.com/DoNotDelete
adapuser	adap.internal.com/DoNotDelete
ADAudit Plus	adap.internal.com
administrator	adap.internal.com/Users
Analytics_1	adap.internal.com/DoNotDelete
analytics_2	adap.internal.com/DoNotDelete
analytics_3	adap.internal.com/DoNotDelete
analytics_4	adap.internal.com/DoNotDelete
Anitha S	adap.internal.com/DoNotDelete
anugraha D.	adap.internal.com/DoNotDelete
arumugam	adap.internal.com/DoNotDelete
Arun	adap.internal.com/DoNotDelete

3.2.2 Grant the user, group management permissions

- **Log in to your Domain Controller with Domain Admin privileges** → Open Active Directory User and Computers. 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.

- Right-click Users → Properties → Security → Advanced → Permissions → Add → In the Permissions Entry for Users window, **Select a principal: ADAudit Plus user** → **Type: Allow** → **Applies to: This object and all descendant objects** → **Select permissions: Create Group objects and Delete Group objects.**

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



Active Directory Users and Computers

Users Properties

Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (ADAPWORKSHOP\Domain Admins)
- Enterprise Admins (ADAPWORKSHOP\Enterprise Admins)

Permissions for CREATOR OWNER	Allow	Deny
Full control	☐	☐
Read	☐	☐
Write	☐	☐
Create all child objects	☐	☐
Delete all child objects	☐	☐

For special permissions or advanced settings, click Advanced.

Permission Entry for Users

Principal: ADAudit Plus (adauditplus@adapworkshop.com) Select a principal

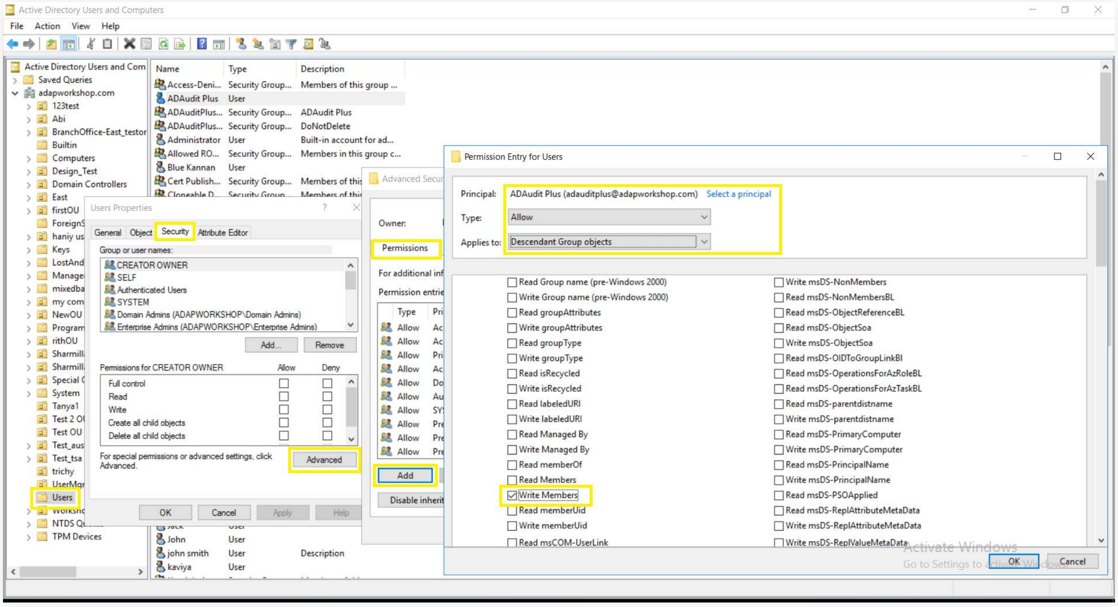
Type: Allow

Applies to: This object and all descendant objects

☐ Delete applicationVersion objects
☐ Create certificationAuthority objects
☐ Delete certificationAuthority objects
☐ Create Computer objects
☐ Delete Computer objects
☐ Create Contact objects
☐ Delete Contact objects
☐ Create document objects
☐ Delete document objects
☐ Create documentSeries objects
☐ Delete documentSeries objects
☑ Create Group objects
☑ Delete Group objects
☐ Create groupOfUniqueNames objects
☐ Delete groupOfUniqueNames objects
☐ Create groupPolicyContainer objects
☐ Delete groupPolicyContainer objects
☐ Create InetOrgPerson objects
☐ Delete msKds-ProvRootKey objects
☐ Create msKds-ProvServerConfiguration objects
☐ Delete msKds-ProvServerConfiguration objects
☐ Create MSMQ Queue Alias objects
☐ Delete MSMQ Queue Alias objects
☐ Create ms-net-ieee-80211-GroupPolicy objects
☐ Delete ms-net-ieee-80211-GroupPolicy objects
☐ Create ms-net-ieee-8023-GroupPolicy objects
☐ Delete ms-net-ieee-8023-GroupPolicy objects
☐ Create msPKI-Enterprise-Oid objects
☐ Delete msPKI-Enterprise-Oid objects
☐ Create msPKI-Key-Recovery-Agent objects
☐ Delete msPKI-Key-Recovery-Agent objects
☐ Create msPKI-PrivateKeyRecoveryAgent objects
☐ Delete msPKI-PrivateKeyRecoveryAgent objects
☐ Create msPrint-ConnectionPolicy objects
☐ Delete msPrint-ConnectionPolicy objects
☐ Create msSFU30DomainInfo objects

- From the Active Directory User and Computers console → Right-click Users → Properties → Security → Advanced → Permissions → Add → In the Permission Entry for Users window → **Select a principal: ADAudit Plus user → Type: Allow → Applies to: Descendant Group objects → Select property: Write Members.**

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



Principal: ADAudit Plus (adauditplus@adapworkshop.com) Select a principal

Type: Allow

Applies to: Descendant Group objects

☑ Write Members

4. Privileges/permissions required for file server auditing

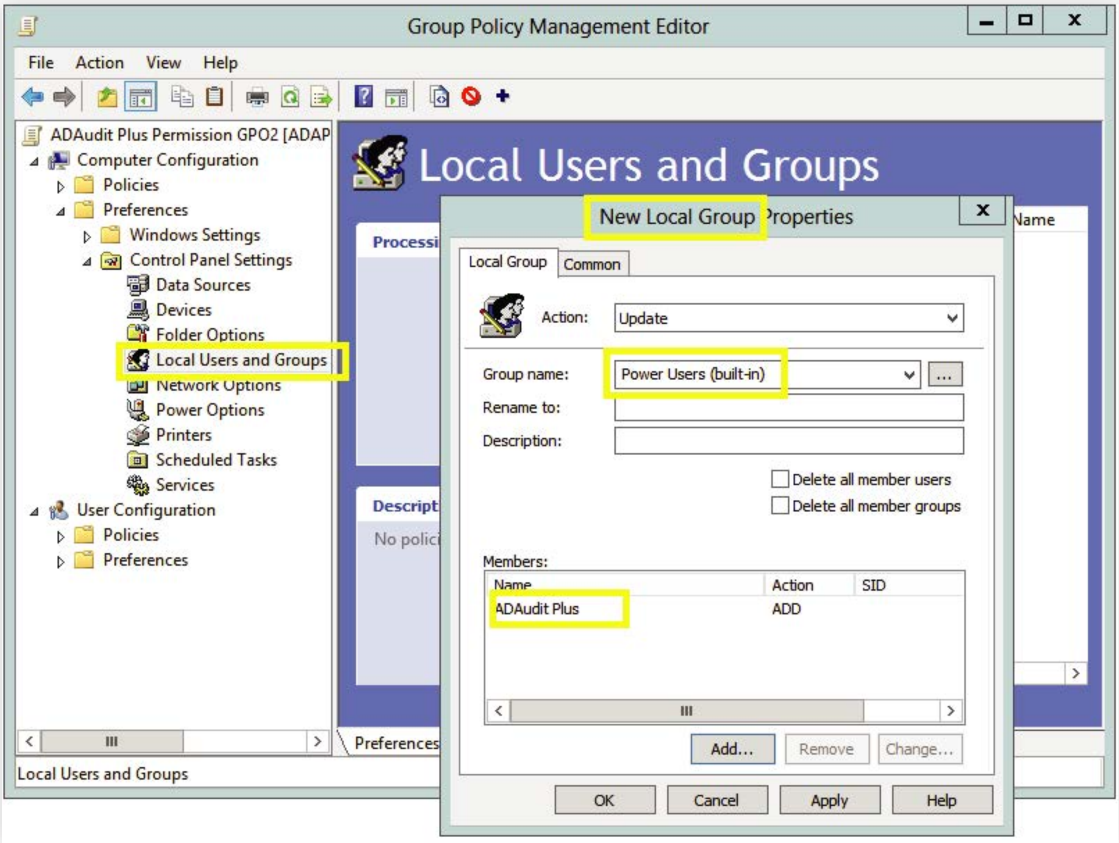
4.1 Make the user a member of the Power Users group

Members of the Power Users group will be able to discover shares residing on Windows file servers.

- Log in to your Domain Controller with Domain Admin privileges →Open the Group Policy Management Console→Right click on the "ADAudit Plus Permission GPO" →Edit.

- In the Group Policy Management Editor →Computer Configuration →Preferences Control Panel Settings →Right click on Local Users and Groups →Add Local Group.

- In the New Local Group Properties wizard, select Update under Action →Select Power Users group under group name →**Add the "ADAudit Plus" user.**



Action: Update

Group name: Power Users (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

Name	Action	SID
ADAudit Plus	ADD	

4.2 Grant the user Read permission on all audited shares

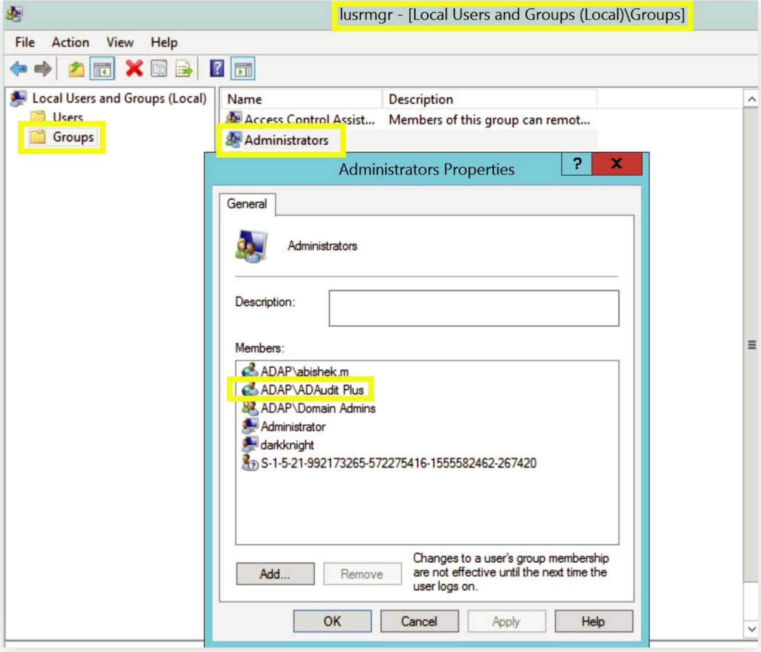
There are two ways to grant the user Read permission on all the audited shares-

- Make the user a Member of the Local Administrators group.

  a. **Login to any computer with Domain Admin privileges** → Open MMC console → File → Add/Remove Snap-in → Select Local Users and Groups → Add → Another computer → Add target computer

  b. Select target computer → Open Local Users and Groups → Select Groups → Right click on administrators → Properties → **Add "ADAudit Plus" user.**

  c. **Repeat the above steps for every audited Windows file server/cluster.**



lusrmgr - [Local Users and Groups (Local)\Groups]

Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	

Administrators Properties

Administrators

Description:

Members:

- ADAP\abishek.m
- ADAP\ADAudit Plus
- ADAP\Domain Admins
- Administrator
- darkknight
- S-1-5-21-992173265-572275416-1555582462-267420

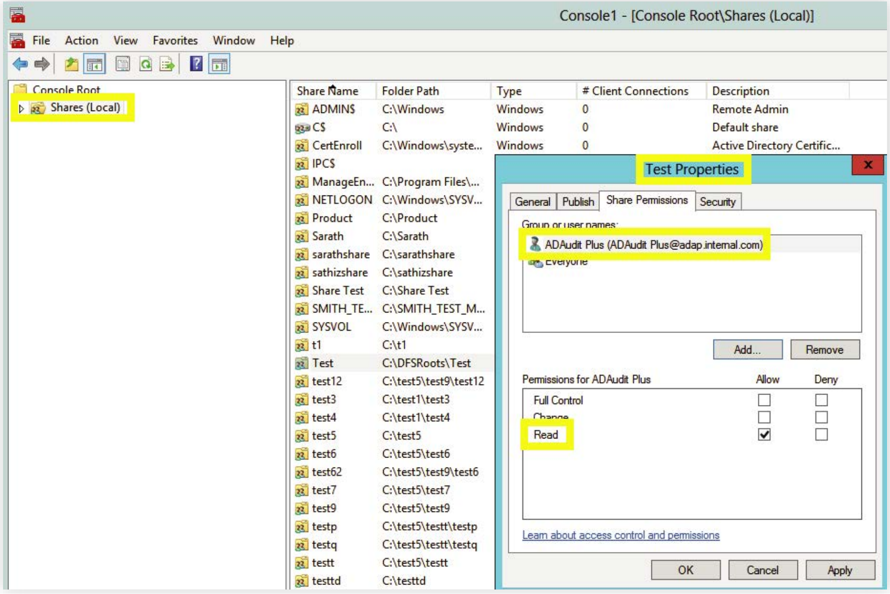
Changes to a user's group membership are not effective until the next time the user logs on.

- **Grant the user both Share and NTFS, Read permission on every audited share.**

  a. **Login to any computer with Domain Admin privileges** ⟶Open MMC console⟶File⟶ Add/Remove Snap-in ⟶Select Shared Folders⟶Add ⟶Another computer ⟶ Add target computer

  b. Select target computer ⟶Select share⟶Right click ⟶Properties ⟶Security⟶ Edit ⟶**Add the "ADAudit Plus" user** ⟶**Provide both Share and NTFS, Read permission.**

  c. **Repeat the above steps for every audited share.**



Console1 - [Console Root\Shares (Local)]

Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
CertEnroll	C:\Windows\syste...	Windows	0	Active Directory Certific...
IPC$				
ManageEn...	C:\Program Files\...			
NETLOGON	C:\Windows\SYSV...			
Product	C:\Product			
Sarath	C:\Sarath			
sarathshare	C:\sarathshare			
sathizshare	C:\sathizshare			
Share Test	C:\Share Test			
SMITH_TE...	C:\SMITH_TEST_M...			
SYSVOL	C:\Windows\SYSV...			
t1	C:\t1			
Test	C:\DFSRoots\Test			
test12	C:\test5\test9\test12			
test3	C:\test1\test3			
test4	C:\test1\test4			
test5	C:\test5			
test6	C:\test5\test6			
test62	C:\test5\test9\test6			
test7	C:\test5\test7			
test9	C:\test5\test9			
testp	C:\test5\testt\testp			
testq	C:\test5\testt\testq			
testt	C:\test5\testt			
testtd	C:\testtd			

Test Properties

Group or user names:

- ADAudit Plus (ADAudit Plus@adap.internal.com)
- Everyone

Permissions for ADAudit Plus	Allow	Deny
Full Control	☐	☐
Change	☐	☐
Read	☑	☐

4.3 Grant the user DCOM and WMI permissions

Note: DCOM and WMI permissions are needed for file cluster auditing and WMI mode of event collection, respectively.

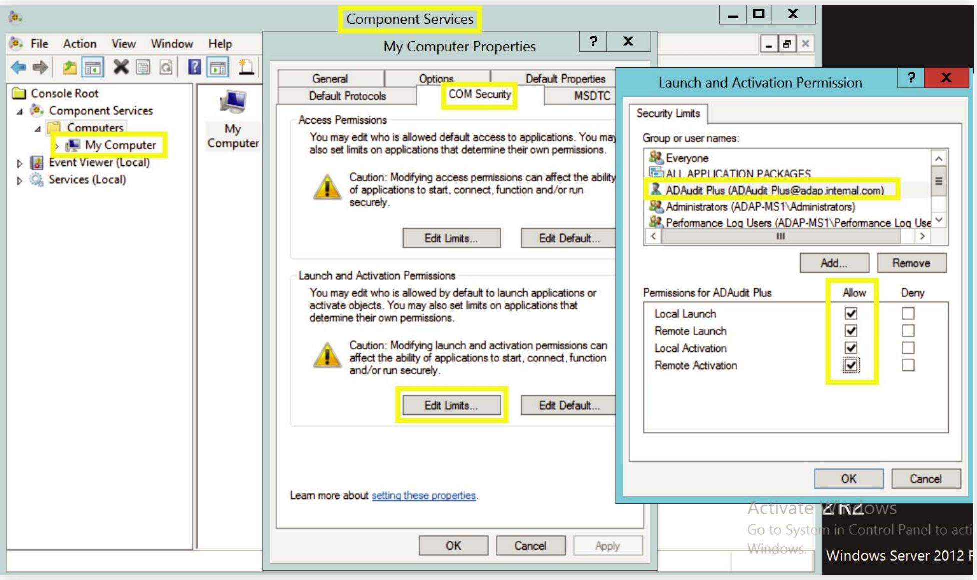
- **Granting DCOM permission:**

  a. **Log in to any computer with Domain Admin privileges** → Open Component Services → Connect to target computer → Right click on target computer → Properties → COM Security.

  b. Navigate to Launch and Activation Permissions → Edit Limits → Security Limits → Add the "ADAudit Plus" user and grant the following permissions:

  - Local Launch
  - Remote Launch
  - Local Activation
  - Remote Activation.

  c. **Repeat the steps for every audited computer.**



You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

Group or user names:

Everyone
ALL APPLICATION PACKAGES
ADAudit Plus (ADAudit Plus@adap.internal.com)
Administrators (ADAP-MS1\Administrators)
Performance Log Users (ADAP-MS1\Performance Log Use

Permissions for ADAudit Plus	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

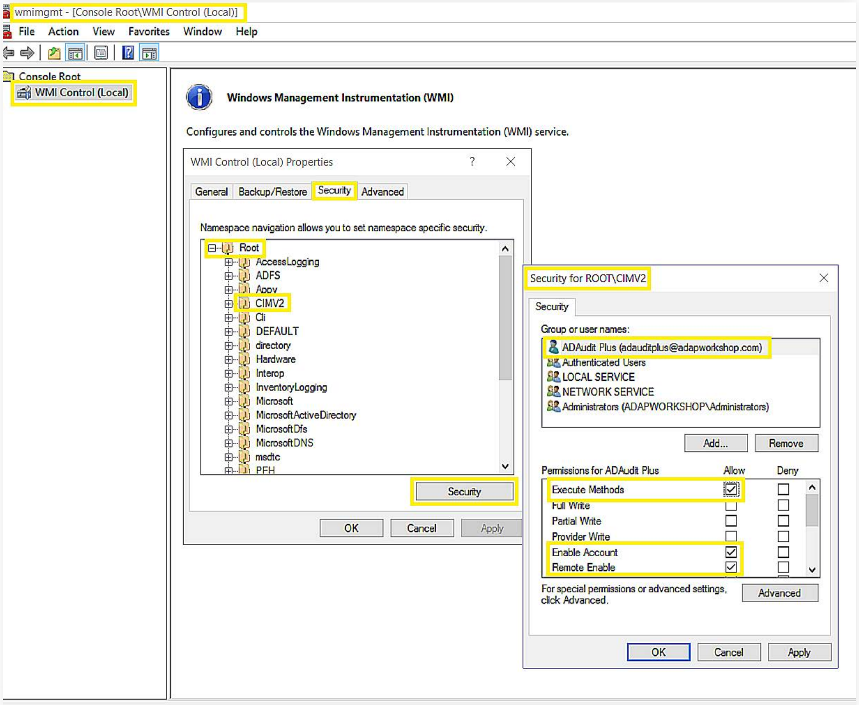
- **Granting WMI permission:**

  a. Log in to any computer with Domain Admin privileges → Run wmimgmt.msc → Right click on WMI Control (Local) → Connect to target computer.

  b. Right click on WMI Control (target computer) → Properties → Security →+Root → CIMV2 → Security → Add the "ADAudit Plus" user and grant the following permissions:

  - Execute Methods
  - Enable Account
  - Remote Enable

  c. Click OK.



Configures and controls the Windows Management Instrumentation (WMI) service.

Namespace navigation allows you to set namespace specific security.

Group or user names:

- ADAudit Plus (adauditplus@adapworkshop.com)
- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (ADAPWORKSHOP\Administrators)

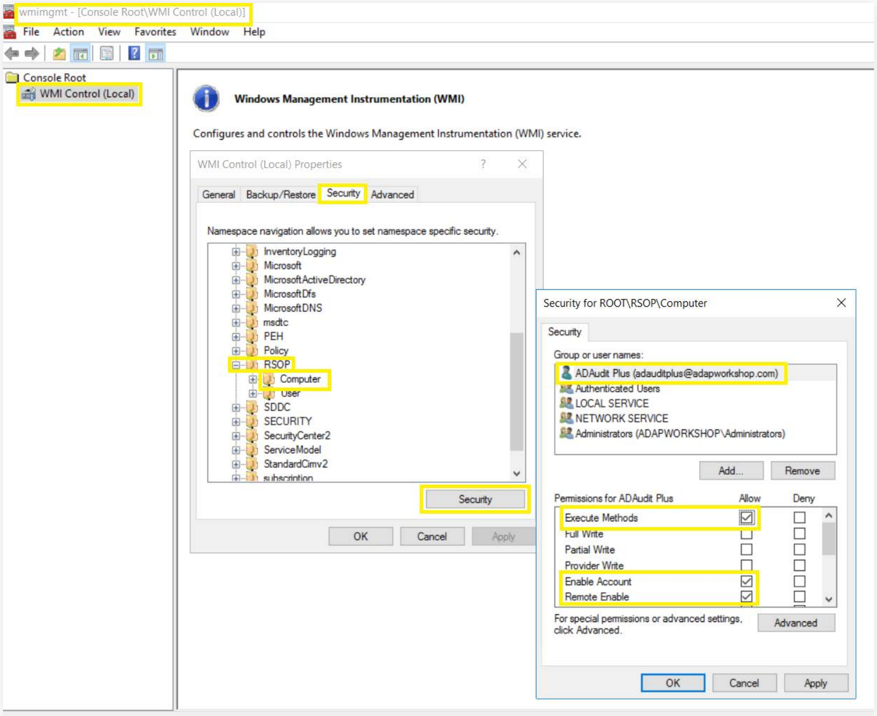
Permissions for ADAudit Plus	Allow	Deny
Execute Methods	☑	□
Full Write	□	□
Partial Write	□	□
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□

For special permissions or advanced settings, click Advanced.

d. Navigate to +Root→+RSOP→Computer→Security→Add the "ADAudit Plus" user and grant the following permissions:

- Execute Methods
- Enable Account
- Remote Enable

e. Click OK.



Configures and controls the Windows Management Instrumentation (WMI) service.

Namespace navigation allows you to set namespace specific security.

Group or user names:

- ADAudit Plus (adauditplus@adapworkshop.com)
- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (ADAPWORKSHOP\Administrators)

Permissions for ADAudit Plus	Allow	Deny
Execute Methods	☑	□
Full Write	□	□
Partial Write	□	□
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□

For special permissions or advanced settings, click Advanced.

f. Repeat the steps for every audited computer.

Note: If multiple computers are audited, you may prefer automating the above process by running a script through Group Policy. Please contact support@adauditplus.com for more details.

4.4 Grant the user read permission over the c$ share (\\server_name\C$):

Note: Read permission over C$ share (\\server_name\C$) is needed to access NetApp C-Mode log files.

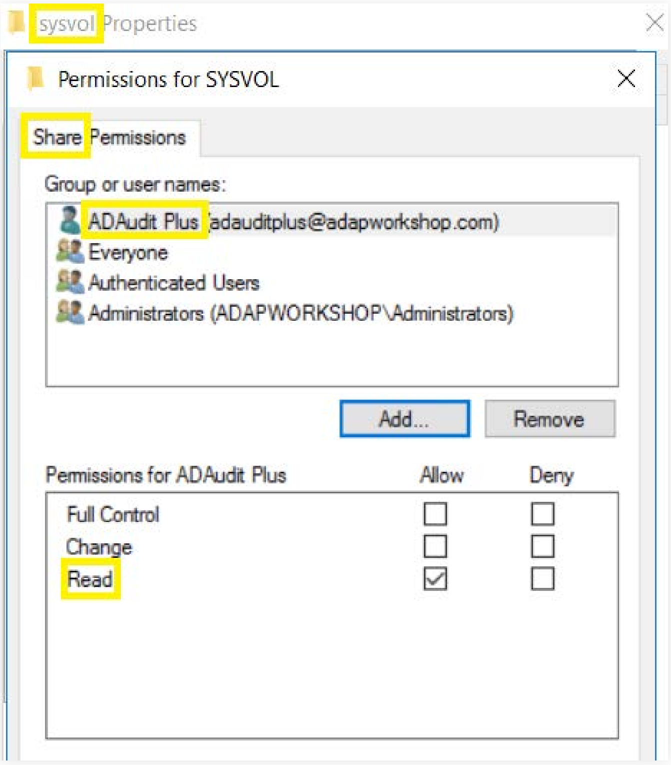
5. Other privileges/permissions required

- **Grant the user Read permission over the SYSVOL folder:**

  Read permission over the SYSVOL folder is needed for GPO Settings change auditing.

Note: By default, all Authenticated Users have read permission over the sysvol folder, if the "ADAudit Plus" user does not, the Read permission has to be provided by following the steps listed below.

Navigate to the sysvol folder (**C:\Windows\SYSVOL\sysvol**) → Right click → **Properties** → **Sharing** → **Advanced sharing** → **Permissions** → Add the "ADAudit Plus" user → Provide Share Read permission.



Group or user names:

- ADAudit Plus (adauditplus@adapworkshop.com)
- Everyone
- Authenticated Users
- Administrators (ADAPWORKSHOP\Administrators)

Permissions for ADAudit Plus	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

- **Grant the user Full control over the product installation folder:**

  Full control over the product installation folder is needed for ADAudit Plus to write in the database.

  a. **Log in to the computer where ADAudit Plus is installed with Domain Admin privileges**

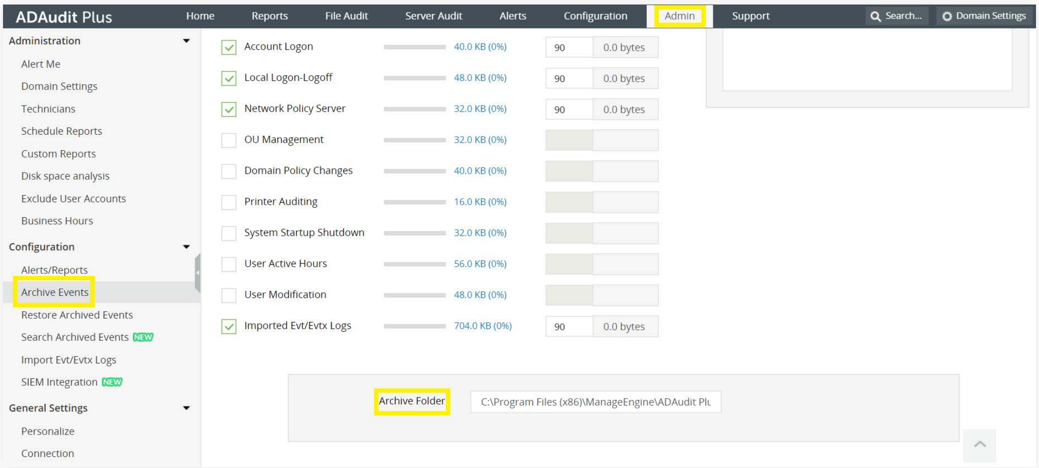
  Locate the product installation folder → Right click → Properties → Security → Edit → **Add the "ADAudit Plus" user and provide full control.**

- **Grant the user Full control over ADAudit Plus' archive folder:**

  Full control over the archive folder is needed for storing and retrieving archived data from the database.

Note: By default, the Archive folder is stored in the installation folder (<Installation_folder>\ManageEngine\ADAudit Plus\arhcive). If the Archive folder is saved elsewhere, NTFS Full control permission needs to be provided by following the steps listed below.

a. **To find out the location of the Archive Folder:** Open ADAudit Plus → Admin → Archive Events → Scroll down to see the location.



☑	Account Logon	40.0 KB (0%)	90	0.0 bytes
☑	Local Logon-Logoff	48.0 KB (0%)	90	0.0 bytes
☑	Network Policy Server	32.0 KB (0%)	90	0.0 bytes
□	OU Management	32.0 KB (0%)		
□	Domain Policy Changes	40.0 KB (0%)		
□	Printer Auditing	16.0 KB (0%)		
□	System Startup Shutdown	32.0 KB (0%)		
□	User Active Hours	56.0 KB (0%)		
□	User Modification	48.0 KB (0%)		
☑	Imported Evt/Evtx Logs	704.0 KB (0%)	90	0.0 bytes

Archive Folder: C:\Program Files (x86)\ManageEngine\ADAudit Plu

b. **Log in to target computer with Domain Admin privileges** → Locate the folder → Right click on the folder → Properties → Security → Edit → **Add the ADAudit Plus User → Provide NTFS Full control permission.**

- **Grant the user Full control over all ADAudit Plus Scheduled Reports folders:**

  Full control over a Scheduled Reports folder is needed for saving the scheduled report in the specified location.

Note: By default, the Schedule Reports folder is stored in the installation folder (<Installation_folder>\ManageEngine\ADAudit Plus). If the Schedule Reports folder is saved elsewhere, NTFS Full control permission needs to be provided by following the steps listed below.

a. **To find out the location of a Scheduled Reports Folder:** Open ADAudit Plus → Admin Schedule Reports → Modify Schedule Report → Scroll down to see the location.

b. **Log in to target computer with Domain Admin privileges** → Locate the folder → Right click on folder → Properties → Security → Edit → **Add the ADAudit Plus User** → **Provide NTFS Full control permission.**

c. **Repeat the steps on all Schedule Reports folders.**

- **Grant the user Read and Execute permission over all ADAudit Plus' Alert Script folders:** Read and Execute permissions on a alert script folder is needed for executing script files once an alert gets triggered.

Note: By default, the Alert Scripts folder is stored in the installation folder (<Installation_folder>\ManageEngine\ADAudit Plus). If the Alerts Script folder is saved elsewhere, NTFS Read and Execute permission needs to be provided by following the steps listed below.

a. **To find out the location of a Folder:** Open ADAudit Plus → Configuration → Modify Alert Profile → Scroll down to see the location.

b. **Log in to target computer with Domain Admin privileges** → Locate the folder → Right click on folder → Properties → Security → Edit → **Add the ADAudit Plus User** → **Provide NTFS Read and Execute permissions.**

c. **Repeat the steps on all Alert Script folders.**

- **Grant the user DCOM and WMI permissions:**
  DCOM and WMI permissions are needed for WMI mode of event collection and for RSoP data to be shown for Domain Controllers, Windows member servers and workstations.
  a. To grant the user DCOM and WMI permissions, follow these steps.

Our Products

AD360 | Log360 | ADManager Plus | ADSelfService Plus | DataSecurity Plus | M365 Manager Plus

ManageEngine
ADAudit Plus

ManageEngine ADAudit Plus is an IT security and compliance solution. With over 200 event-specific reports and real-time email alerts, it provides in-depth knowledge about changes effected to both the content and configuration of Active Directory, Azure AD and Windows servers. Additionally it also provides thorough access intelligence for workstations and file servers (including NetApp and EMC).

To learn more about how ADAudit Plus can help you with all your Active Directory auditing needs, please visit: https://www.manageengine.com/products/active-directory-audit/

$ Get Quote   ⤓ Download