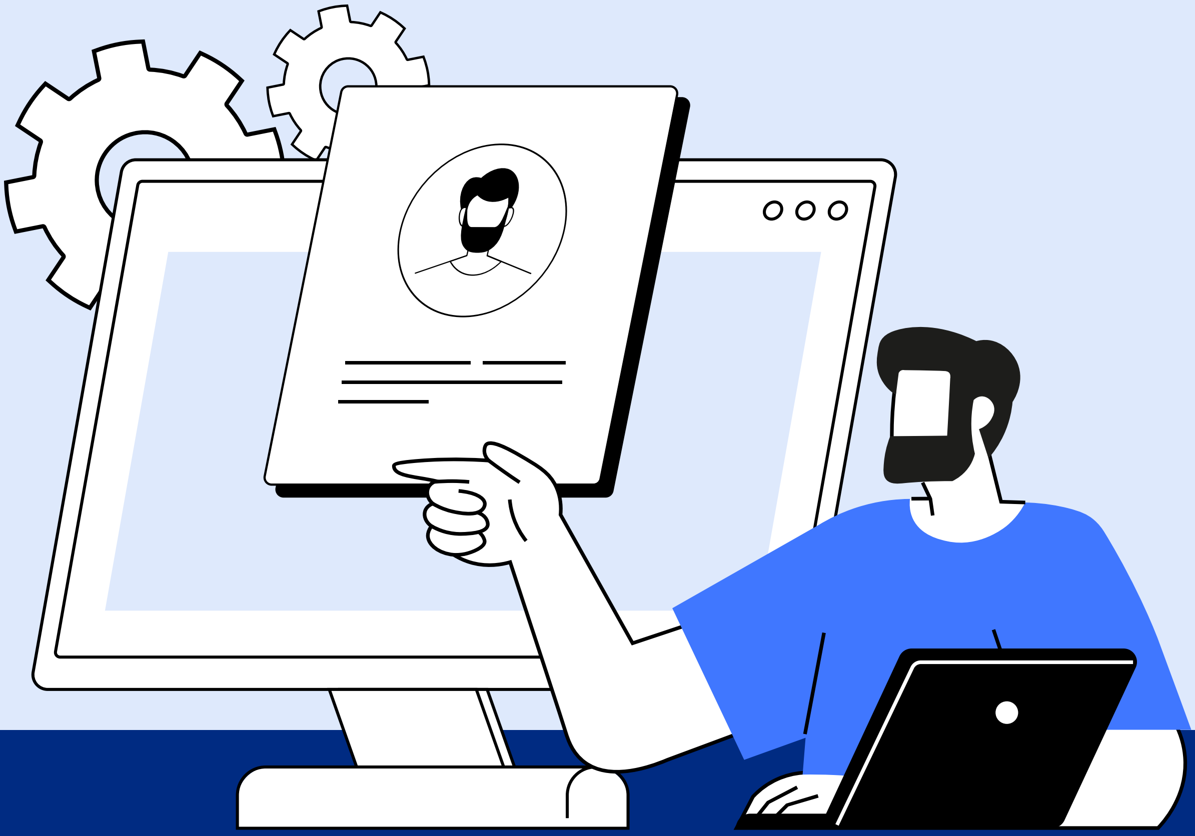
ManageEngine
ADAudit Plus

Minimum privileges



manageengine.com/products/active-directory-audit/

Table of Contents

Overview 1

1. For product start-up 1

1.1 Installation folder privileges (RHS) 1

1. 2 Using SecureDeployment.exe 1

1.3 Modifying the permissions manually 2

1.4 Exclude ADAudit Plus from antivirus and endpoint protection 3

2. For DataEngine 4

2.1 Introduction 4

2.2 Required permissions 5

2. 3 Troubleshooting 7

3. For AD, Windows Server, and Workstation auditing 8

3.1 Overview 8

3.2 New user, group, and GPO creation 8

3.3 Privileges/permissions required for event log collection 9

3.4 Privileges/permissions required for automatic audit policy and object level auditing configuration 11

4. For file server auditing 14

4.1 Make the user a member of the Power Users group 14

4.2 Grant the user Read permission on all audited shares 14

4.3 Grant the user DCOM and WMI permissions 16

4.4 Grant the user read permission over the c$ share 18

5. Other privileges 18

Overview

Certain minimum privileges are required to start ManageEngine ADAudit Plus and begin auditing your Active Directory (AD), Azure AD, Windows servers, file servers, workstations, and other network-attached storage (NAS) devices. This guide will walk you through these prerequisites and the process of setting up a service account with the required privileges.

1. For product start-up

1.1 Installation folder privileges

To enhance the security of your ADAudit Plus installation, starting from build 7251, default access to the ADAudit Plus folder is limited to the user account used for installation and the *SYSTEM, Administrators*, and *Domain Admins* groups. However, to allow other users to start ADAudit Plus, you can follow the steps under *Assign Modify permission to the ADAudit Plus folder for users starting the product*.

If you are using an earlier build of ADAudit Plus, or if you have upgraded to build 7251 recently, there are two ways to safeguard the ADAudit Plus folder from unauthorized modifications:

- Using SecureDeployment.exe
- Modifying the permissions manually

1. 2 Using SecureDeployment.exe

The SecureDeployment.exe file will strengthen the security of your ADAudit Plus installation by automatically:

- Preventing non-administrative groups from accessing the ADAudit Plus folder.
- Assigning the Modify permission to a selected user account.
- Configuring "Log On" account credentials if ADAudit Plus is installed as a service.

To run the SecureDeployment.exe file:

- Go to *<Installation_Directory>\ADAudit Plus\bin* folder (if you have upgraded to build 7251 recently) and locate *SecureDeployment.exe* file.

> **Note:** If you are using an earlier build, download the SecureDeployment zip file, unzip it and copy its contents to *<Installation_Directory>\ADAudit Plus\bin* folder.

- Right-click the **SecureDeployment.exe** file and select **Run as Administrator.**
- Enter "1" and proceed with removing the permissions for the non-administrative groups, namely *Authenticated Users, BUILTIN\Users, CREATOR OWNER, ALL RESTRICTED APPLICATION PACKAGES, ALL APPLICATION PACKAGES, TrustedInstaller, and Everyone.*
- Once the permissions are removed, press any key to open the **Select User or Group** dialog box.
- Enter the name of the user that you want to assign the permission to start ADAudit Plus, and click **Check Names** to confirm the selection.

> **Note:** If you have installed ADAudit Plus as a service with "Log On" account credentials, enter the username associated with that account.

- Click **OK.**

> **Note:** If you want to assign the permission to start ADAudit Plus to multiple users, follow the steps under *Assign Modify permission to the ADAudit Plus folder for users starting the product*.

1.3 Modifying the permissions manually

If you do not want to use the *SecureDeployment.exe* file, you can strengthen the security of your ADAudit Plus installation by ensuring the following:

Disable Inheritance for the ADAudit Plus folder.

- Go to <Installation_Directory>\ManageEngine.
- Right-click the **ADAudit Plus folder** and select **Properties.**
- Click the **Security** tab and then click **Advanced.**
- In the *Advanced Security Settings* window, click **Disable inheritance.**
- Click **OK.**

Remove non-administrative groups from ADAudit Plus folder's Access Control List.

- Go to <Installation_Directory>\ManageEngine.
- Right-click the **ADAudit Plus folder** and select **Properties.**
- Click the **Security** tab and then click **Advanced.**
- In the **Advanced Security Settings** window, under **Permission entries**, select the non-administrative users and groups, and click **Remove.**
- Click **OK.**

Assign Full control permission to the Domain Admins, Administrators, and SYSTEM groups.

- Go to <Installation_Directory>\ManageEngine.
- Right-click the ADAudit Plus folder and select **Properties.**
- Click the **Security** tab and then click **Advanced.**
- In the **Permissions** tab, click **Add.**
- Click the **Select a principal** link and add *Domain Admins, Administrators*, and *SYSTEM* groups.
- Click **OK**.
- Next to **Type**, select **Allow**, and next to **Applies to**, select **This folder, subfolders, and files.**
- Under **Basic Permissions**, check the **Full control** box.
- Click **OK.**

Assign Modify permission to the ADAudit Plus folder for users starting the product.

- Go to <Installation_Directory>\ManageEngine.
- Right-click the ADAudit Plus folder and select **Properties.**
- Click the **Security** tab and then click **Advanced**.
- In the **Permissions** tab, click **Add.**
- Click the **Select a principal** link, enter the name of the user that you want to assign the permission to start ADAudit Plus, and then click **Check Names** to confirm the selection.
- Click **OK.**
- Next to **Type**, select **Allow** and next to **Applies to**, select **This folder, subfolders, and files.**
- Under **Basic Permissions**, check the **Modify** box.
- Click **OK.**

> **Note:** If the product is installed as a service with "Log On" account credentials, ensure this account has *Modify* permission

1.4 Exclude ADAudit Plus from antivirus and endpoint protection

To prevent any performance issues and to avoid potential disruptions to the ADAudit Plus database's (PostgreSQL) operation, it is essential to exclude certain directories from antivirus and endpoint protection on the ADAudit Plus server. This exclusion is crucial, as antivirus and endpoint protection solutions can sometimes falsely tag the database and other files within ADAudit Plus' installation directory as a threat or vulnerability.

The performance issues that you might face in ADAudit Plus due to antivirus and endpoint protection software include high latency when processing events and alerts, low throughput when adding data to the database or DataEngine, and corruption of database files.

For optimal performance, it is recommended that you exclude the directories used by java.exe and postgres.exe from antivirus and endpoint protection on the ADAudit Plus server. The directories that need to be excluded are listed below:

<Installation_folder>\ManageEngine\ADAudit Plus\index
<Installation_folder>\ManageEngine\ADAudit Plus\eventdata
<Installation_folder>\ManageEngine\ADAudit Plus\alertdata
<Installation_folder>\ManageEngine\ADAudit Plus\ehcache
<Installation_folder>\ManageEngine\ADAudit Plus\apps\dataengine-xnode\data
<Installation_folder>\ManageEngine\ADAudit Plus\pgsql

> **Note:** The java.exe and postgres.exe processes are located, respectively, at:
> *<Installation_Directory>\ManageEngine\ADAudit Plus\jre\bin\java.exe*
> *<Installation_Directory>\ManageEngine\ADAudit Plus\pgsql\bin\postgres.exe*

2. For DataEngine

2.1 Introduction

The DataEngine component within ADAudit Plus stores and retrieves log data efficiently. It enhances scalability by enabling faster search and retrieval of data.

The DataEngine stores its data under C:\Program Files (x86)\ManageEngine\ADAudit Plus\apps by default. The size of this folder will depend on the volume of logs collected and stored. For example, approximately 15MB of space will be necessary for every 100,000 log entries. So be sure to allocate the space required on the disk for storing log data.

> **Note:** Any accidental deletion of the files within this folder could result in data loss, which is why it is strongly recommended not to delete any files in this folder.

The DataEngine runs as a separate service, i.e., *ManageEngine ADAudit Plus - DataEngine XNode*. This service uses port 29118 to communicate, and it needs to be kept running for the optimal functioning of ADAudit Plus.

You can change the port being used by modifying the value of the parameter *xnode.connector.port* in the below files. Make sure to use the same value in both the files listed below:

<Installation directory>\apps\dataengine-xnode\conf\dataengine-xnode.conf
<Installation directory>\conf\DataEngine\engines\xnode\dataengine-xnode.conf

2.2 Required permissions

The user or the service account that starts the ManageEngine ADAudit Plus service needs these privileges:

- Full control over the product installation folder.
- Privilege to start, install, and stop the ManageEngine ADAudit Plus - DataEngine XNode service.

Steps to provide full control privileges over the product installation folder:

- Log in to the **machine** where ADAudit Plus is installed with domain admin privileges.
- Navigate to the **product installation folder** (C:\Program Files (x86)\ManageEngine\ADAudit Plus). Right-click on it and select **Properties** > **Security** > **Edit.** Select the **user account** you want to provide full control access to and click **Add**. Check **Allow** under **Full control** access. Click **Ok.**

Steps to provide privileges required to start, install, and stop the DataEngine service
You can either add the user to the local administrator group or use Group Policy to provide the necessary privileges.

A. To add the user to the local administrator group:

- Log in to the **machine** where ADAudit Plus is installed.
- Go to **Start** > **Control Panel** > **Edit local users and groups** > **Groups**. Double-click **Administrators.**
- In the Administrators **Properties** window that opens, click **Add.**
- Select the **Entire Directory**. Select the desired user and click **Add.**
- Click **OK.**

B. To provide the necessary privileges using Group Policy:

- Log in with Domain Admin credentials to any of the domain controllers that has **Active Directory Users and Computers.**
- Go to **Start** > **Windows Administrative Tools** > **Active Directory Users and Computers.**
- Right-click the **domain** to which you want to add the organizational unit to. Click **New** > **Organizational Unit.**
- In the *New object - Organizational Unit* window that opens, type in the desired **OU name** and move the **computer** where ADAudit Plus service is running into the OU.
- Go to **Start** > **Windows Administrative Tools** > **Group Policy Management.**

> **Note:** The Group Policy Management Console (GPMC) will not be installed on all workstations and servers by default. You can follow the steps on this page to install the GPMC on the desired member servers and workstations.

- Navigate to the recently created **OU**. Right-click the **OU** and select **Create a GPO and Link it here**. In the *New GPO* window, type in the desired **name** and click **OK.**
- Select the newly created **GPO**, right-click it, and select **Edit**. In the *Group Policy Management Editor,* go to Computer **Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **System services.** Right-click **ManageEngine ADAudit Plus - DataEngine XNode** and select **Properties**. In the new window, check the **Define this policy setting** box. Click **Edit Security.**
- In the *Security* tab that opens, search and find the user account to which you want to provide the necessary privileges. Select the user account and give **Full access** to it.
- Click **OK.**
- This Group Policy needs to be enforced throughout the domain. To do this, go to **Start** > **Command Prompt**. Type in **gpupdate/force.**

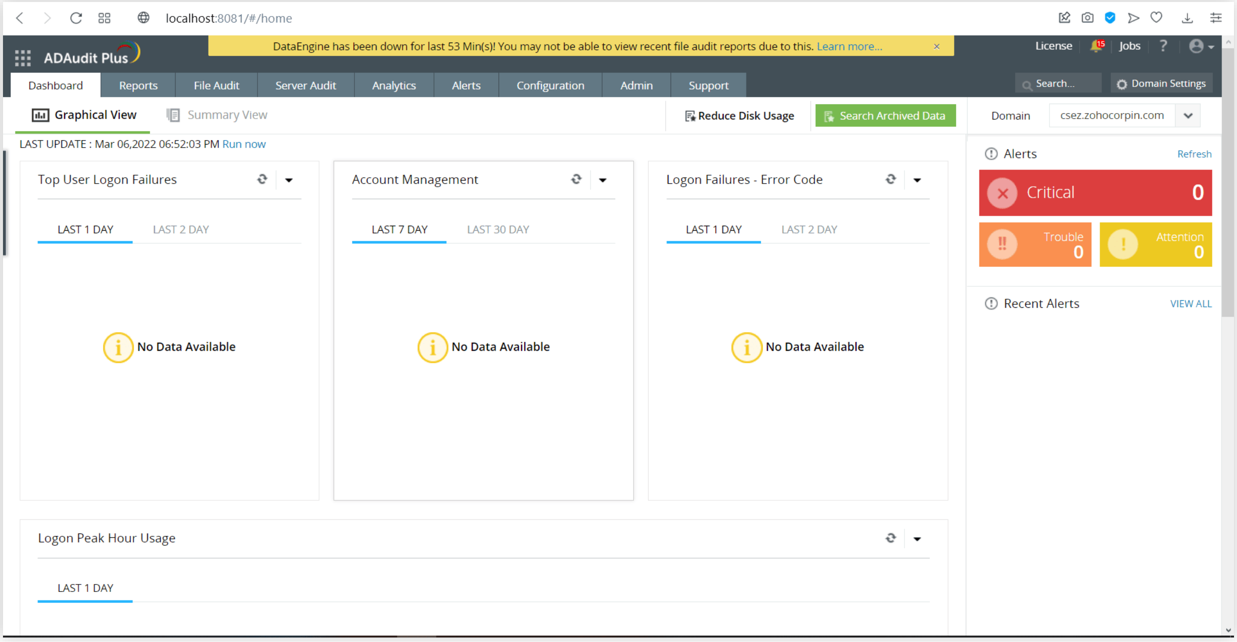
Steps to provide privileges to archive and restore the audit data

- **To find out the location of the Archive Folder: Open ADAudit Plus → Admin → Archive Events → Scroll down to see the location.**
- Log in to the **machine** where ADAudit Plus is installed with Domain Admin privileges. → Locate the archive folder → Right-click on it and select **Properties** > **Security** > **Edit.** Select the **user account** you want to provide full control access to and click **Add**. Check **Allow** under **Full control** access. Click **Ok.**
- If the archive folder is a shared folder, go to the **Sharing** tab → **Advanced Sharing...** → **Permissions** → Select the **user account** you want to provide full control access to and click **Add.** → Check **Allow** under **Full control** access. Click **Ok.**

> **Note:** If the archive folder is a shared folder it is important to ensure that the service account used to run the DataEngine service is the same as the service account used to run the ADAudit Plus service. that you've assigned the Full control permission to.

2.3 Troubleshooting

1. DataEngine has been down for last "x" mins(s). You may not be able to view recent file audit reports due to this.



DataEngine has been down for last 53 Min(s)! You may not be able to view recent file audit reports due to this. Learn more...

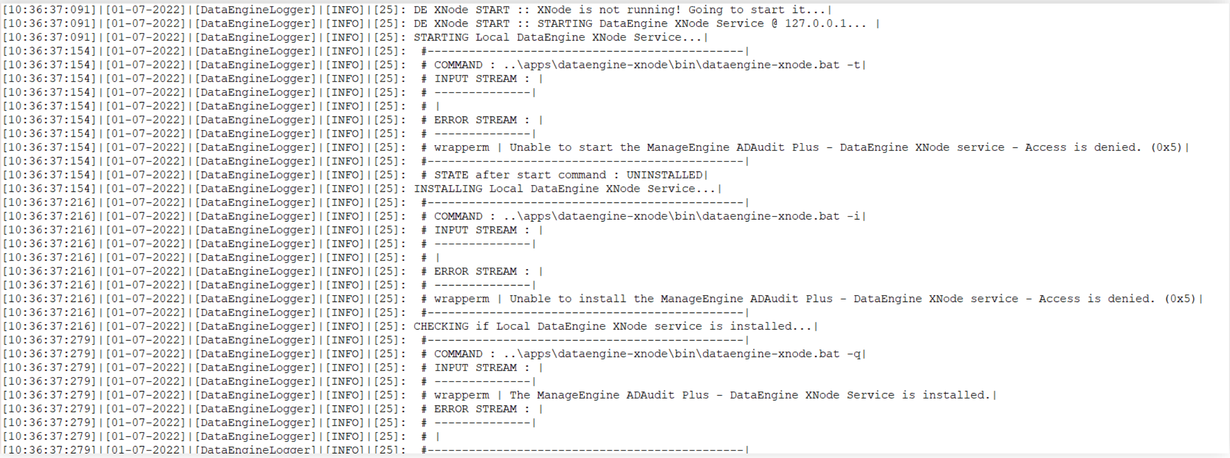
LAST UPDATE : Mar 06,2022 06:52:03 PM Run now

Solution:

1. Open the DataEngine.log file in the ADAudit Plus log folder, i.e., <installation_dir>\logs.

2. Check if the errors listed below are in the DataEngine.log file:

- Unable to install the ManageEngine ADAudit Plus - DataEngine XNode service - Access is denied.
- Unable to start the ManageEngine ADAudit Plus - DataEngine XNode service - Access is denied.



```
[10:36:37:091]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: DE XNode START :: XNode is not running! Going to start it...|
[10:36:37:091]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: DE XNode START :: STARTING DataEngine XNode Service @ 127.0.0.1... |
[10:36:37:091]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: STARTING Local DataEngine XNode Service...|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #---------------------------------------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # COMMAND : ..\apps\dataengine-xnode\bin\dataengine-xnode.bat -t|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # INPUT STREAM : |
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # -------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # |
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # ERROR STREAM : |
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # -------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # wrapperm | Unable to start the ManageEngine ADAudit Plus - DataEngine XNode service - Access is denied. (0x5)|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #---------------------------------------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # STATE after start command : UNINSTALLED|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: INSTALLING Local DataEngine XNode Service...|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #---------------------------------------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # COMMAND : ..\apps\dataengine-xnode\bin\dataengine-xnode.bat -i|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # INPUT STREAM : |
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # -------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # |
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # ERROR STREAM : |
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # -------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # wrapperm | Unable to install the ManageEngine ADAudit Plus - DataEngine XNode service - Access is denied. (0x5)|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #---------------------------------------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: CHECKING if Local DataEngine XNode service is installed...|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #---------------------------------------------|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # COMMAND : ..\apps\dataengine-xnode\bin\dataengine-xnode.bat -q|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # INPUT STREAM : |
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # -------------|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # wrapperm | The ManageEngine ADAudit Plus - DataEngine XNode Service is installed.|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # ERROR STREAM : |
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # -------------|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # |
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #---------------------------------------------|
```

2.1 If these appear in the file, DataEngine is unavailable due to insufficient privileges. To provide sufficient privileges required to start, install, and stop the DataEngine service, follow the steps listed here.

2.2 If these are not in the file, then contact our support team. They will assist you in debugging the issue with the DataEngine service.

3. For AD, Windows Server, and Workstation auditing

3.1 Overview

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.

3.2 New user, group, and GPO creation

1. Create a new user

i. 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*".

2. Create a new group

i. 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*".

ii. 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.

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

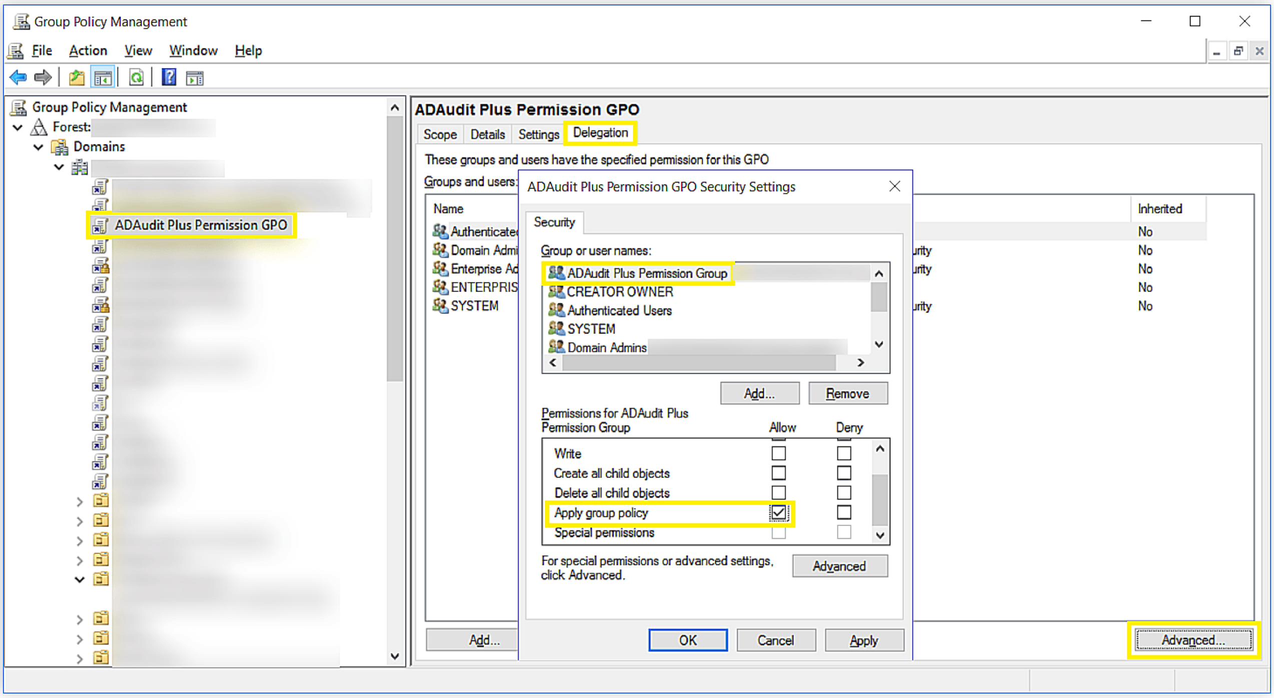
Since configuring permissions on individual computers is an elaborate process, a domain level GPO is created and applied on all monitored computers.

i. Log in to your Domain Controller with Domain Admin privileges.

ii. 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*"

iii. 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.

iv. 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" → Check Apply group policy.



Group Policy Management

File Action View Window Help

ADAudit Plus Permission GPO

Scope | Details | Settings | Delegation

These groups and users have the specified permission for this GPO

Groups and users:

Name	Inherited
Authenticate	No
Domain Admi	No
Enterprise Ad	No
ENTERPRIS	No
SYSTEM	No

ADAudit Plus Permission GPO Security Settings

Security

Group or user names:

- ADAudit Plus Permission Group
- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins

Add... Remove

Permissions for ADAudit Plus Permission Group	Allow	Deny
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Apply group policy	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply

Add... Advanced...

3.3 Privileges/permissions required for event log collection

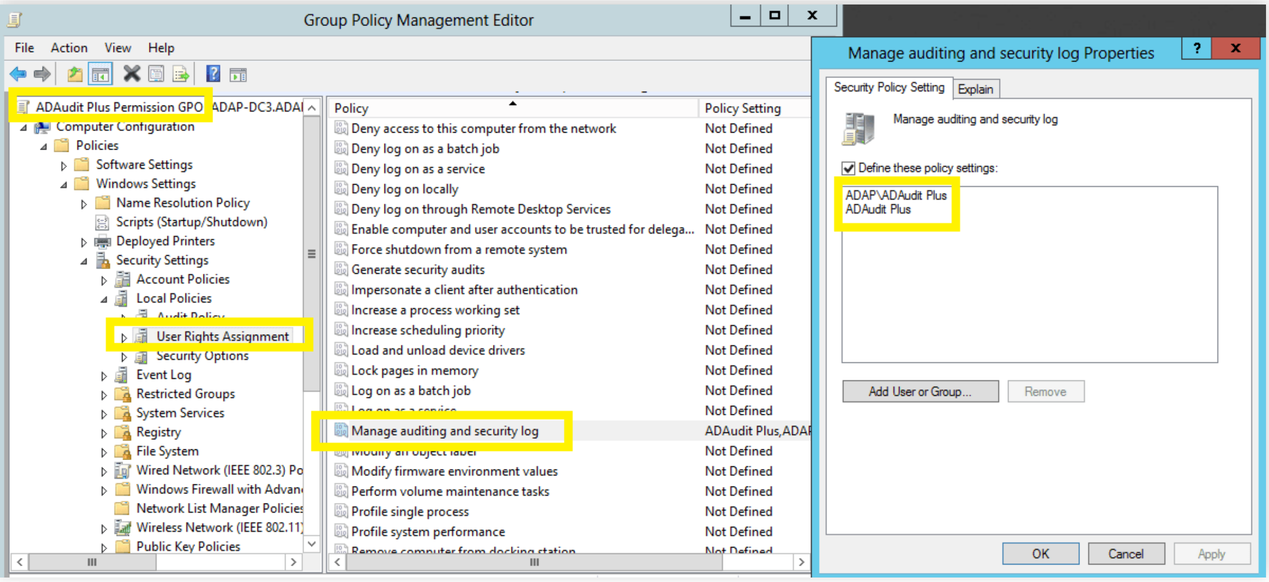
1. Grant the user the Manage auditing and security log right

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

i. **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.

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

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



Group Policy Management Editor

File Action View Help

ADAudit Plus Permission GPO [ADAP-DC3.ADAI

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Po
        - Windows Firewall with Advan
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11)
        - Public Key Policies

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,ADAI
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

Add User or Group... Remove

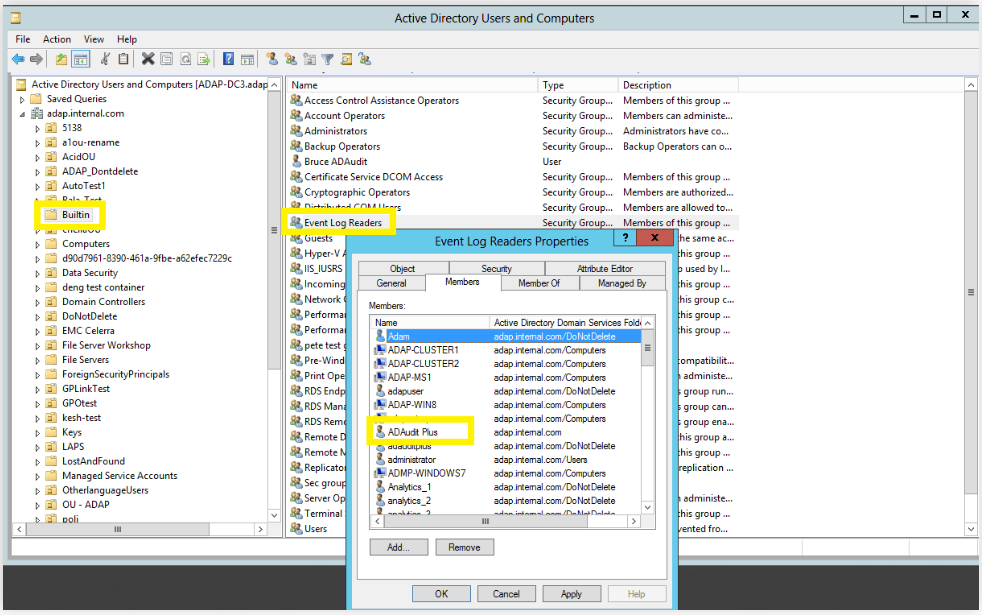
OK Cancel Apply

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.

i. 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 ...

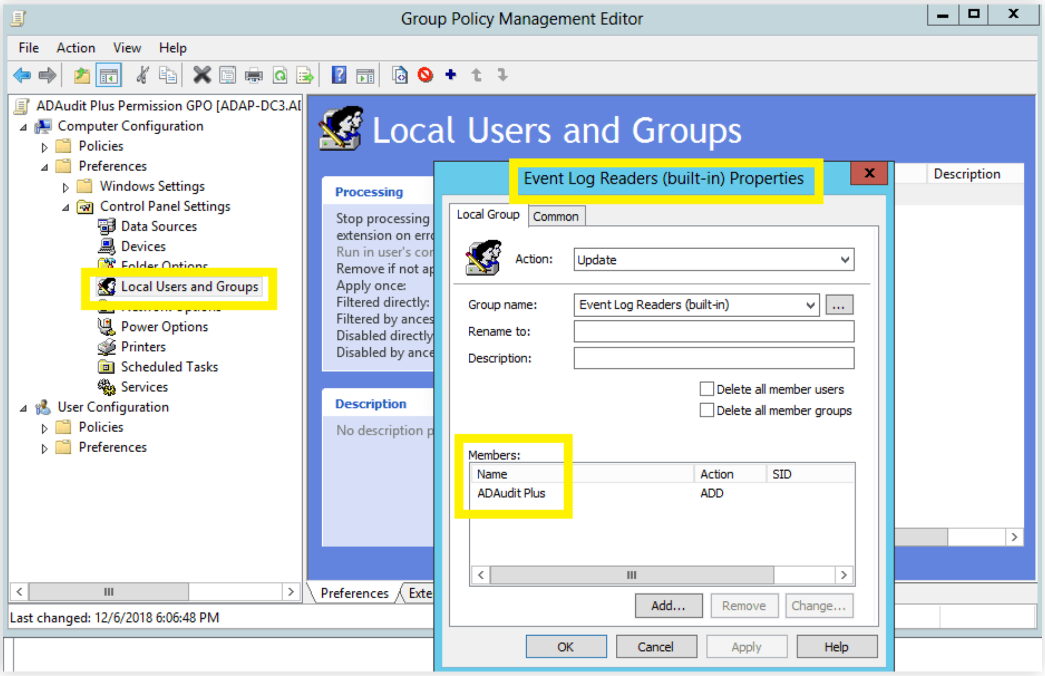
Members:

Name	Active Directory Domain Services Fold
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

ii. 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.**



Stop processing extension on err
Run in user's cor
Remove if not ap
Apply once:
Filtered directly:
Filtered by ances
Disabled directly
Disabled by ance

No description p

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

Note: To read the event logs, you also need to grant the "**ADAudit Plus**" user **Read** permission over **HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security.**

i. 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.

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

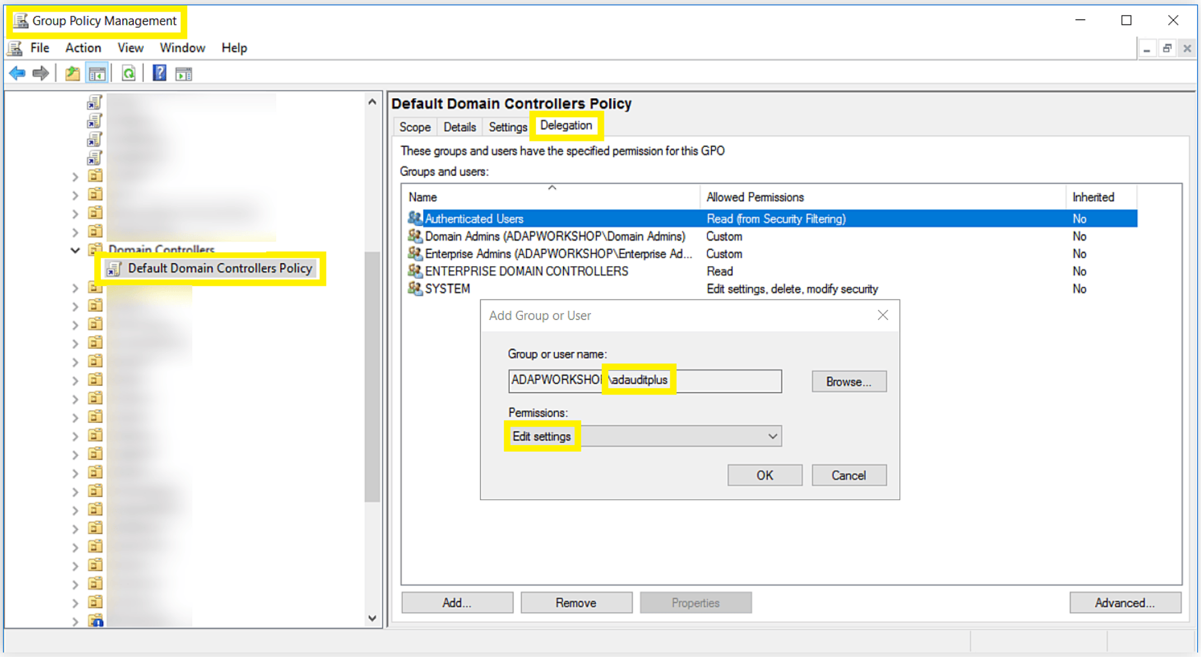
iii. In the Select Registry Key Window, navigate to MACHINE → SYSTEM → CurrentControlSet → Services → EventLog → Security → Click OK → Grant **Read** permission to "**ADAudit Plus**" user → Click Apply.

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

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

1. Privileges/permissions required for Domain Controller auditing configuration
Granting the service account the following privileges/permissions, allows ADAudit Plus to automatically 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.

i. 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

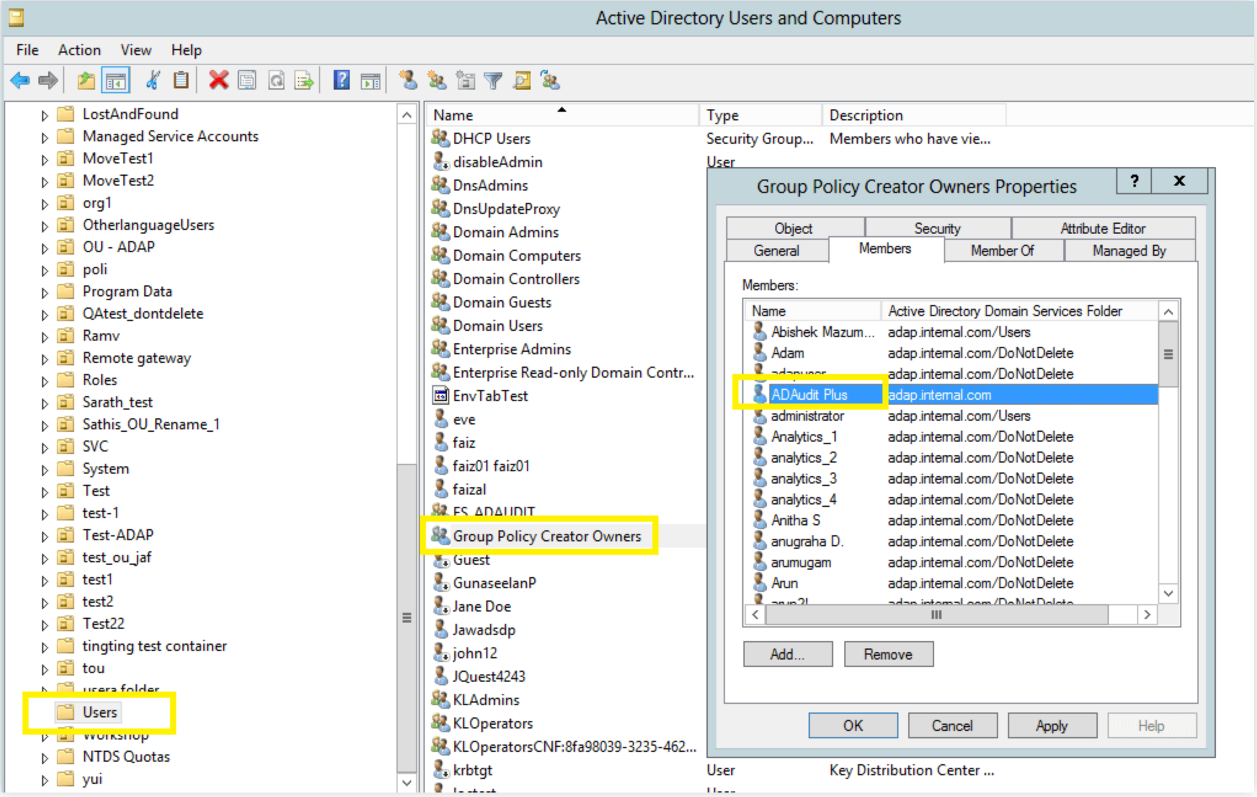
Group or user name: ADAPWORKSHOP\adauditplus

Permissions: Edit settings

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

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

i. **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.**



LostAndFound
Managed Service Accounts
MoveTest1
MoveTest2
org1
OtherlanguageUsers
OU - ADAP
poli
Program Data
QAtest_dontdelete
Ramv
Remote gateway
Roles
Sarath_test
Sathis_OU_Rename_1
SVC
System
Test
test-1
Test-ADAP
test_ou_jaf
test1
test2
Test22
tingting test container
tou
usera folder
Users
Workshop
NTDS Quotas
yui

Name	Type	Description
DHCP Users	Security Group...	Members who have vie...
disableAdmin	User	
DnsAdmins		
DnsUpdateProxy		
Domain Admins		
Domain Computers		
Domain Controllers		
Domain Guests		
Domain Users		
Enterprise Admins		
Enterprise Read-only Domain Contr...		
EnvTabTest		
eve		
faiz		
faiz01 faiz01		
faizal		
FS_ADAUDIT		
Group Policy Creator Owners		
Guest		
GunaseelanP		
Jane Doe		
Jawadsdp		
john12		
JQuest4243		
KLAdmins		
KLOperators		
KLOperatorsCNF:8fa98039-3235-462...		
krbtgt	User	Key Distribution Center ...

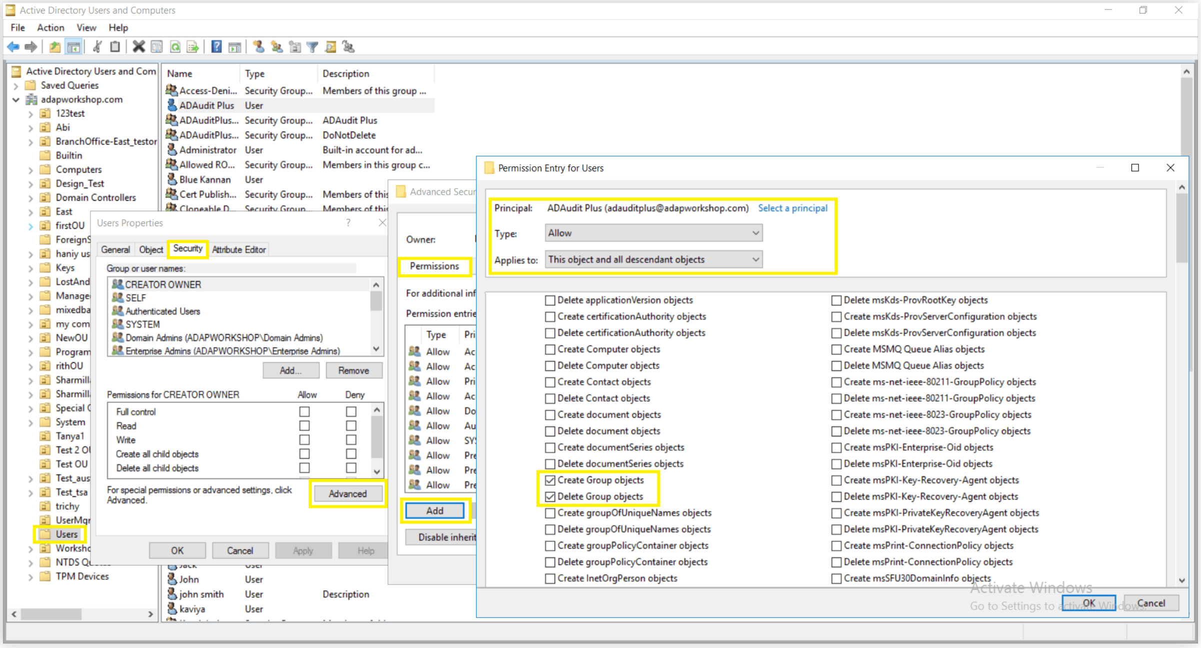
Name	Active Directory Domain Services Folder
Abishek Mazum...	adap.internal.com/Users
Adam	adap.internal.com/DoNotDelete
adapuser	adap.internal.com/DoNotDelete
ADAudit Plus	adap.internal.com
administrator	adap.internal.com/Users
Analytics_1	adap.internal.com/DoNotDelete
analytics_2	adap.internal.com/DoNotDelete
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
arun2l	adap.internal.com/DoNotDelete

2.2 Grant the user, group management permissions

i. **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.

ii. 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.


Permission Entry for Users

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

Type: Allow

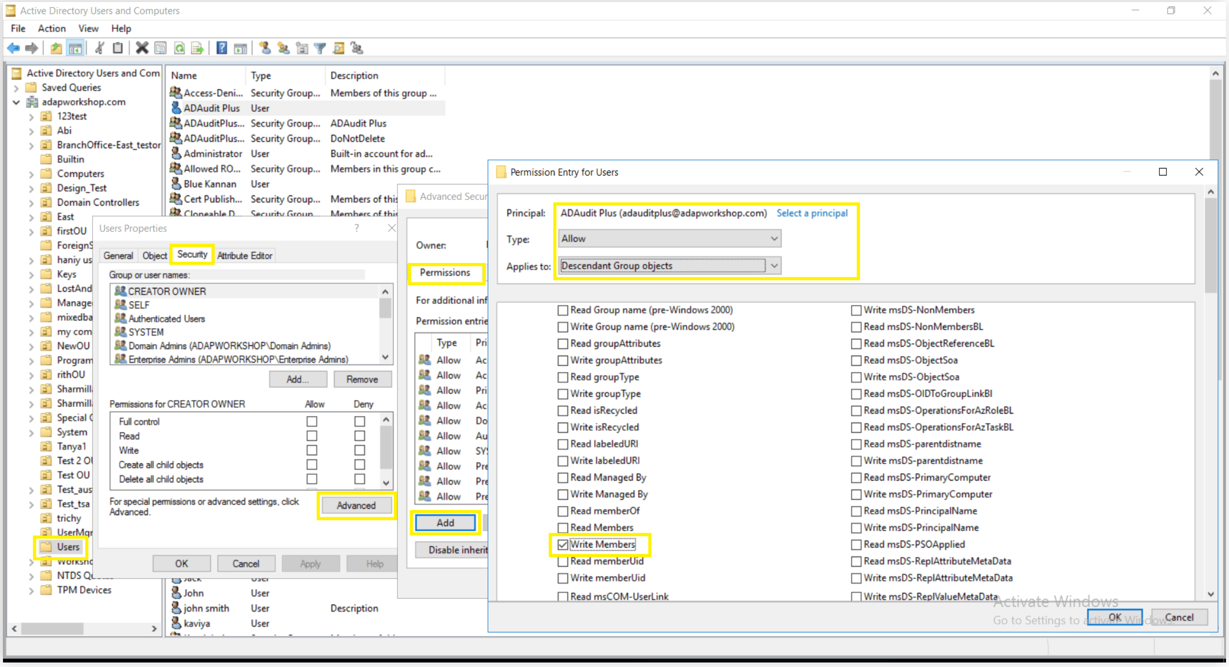
Applies to: This object and all descendant objects

☑ Create Group objects

☑ Delete Group objects

iii. 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.


Permission Entry for Users

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

Type: Allow

Applies to: Descendant Group objects

☑ Write Members

4. For file server auditing

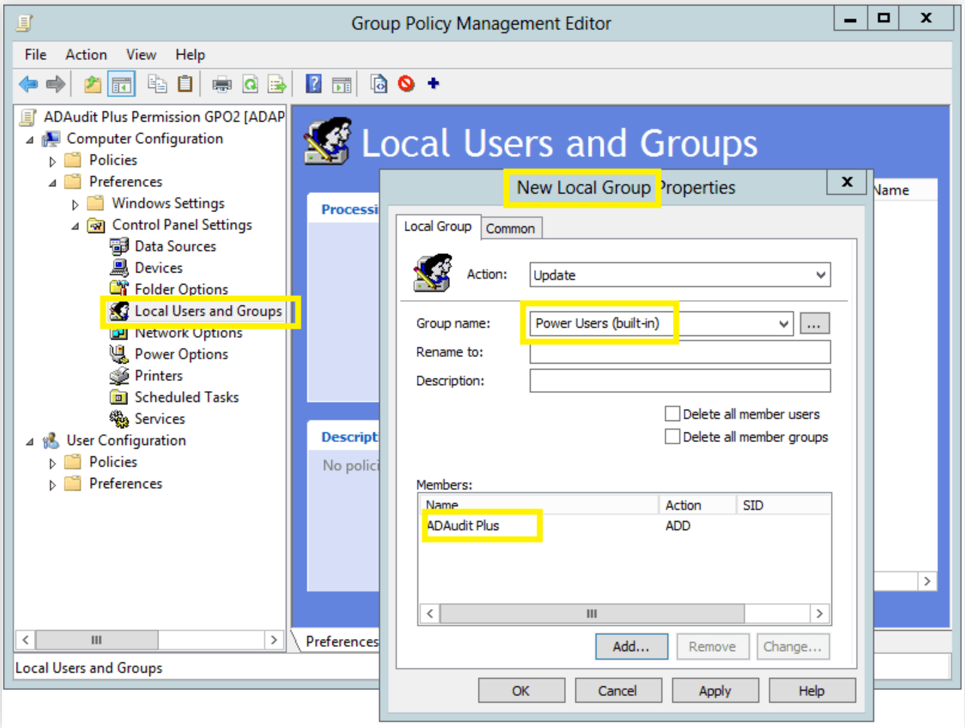
4.1 Make the user a member of the Power Users group

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

i. 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.

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

iii. 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

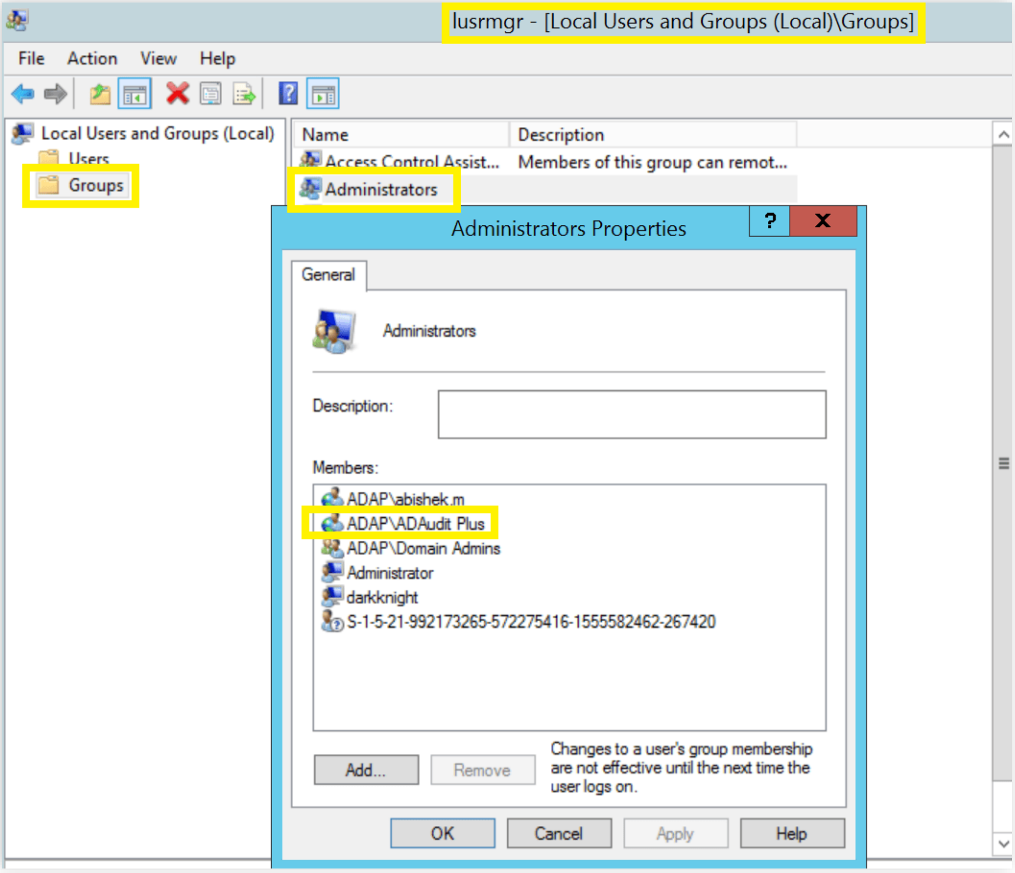
There are two ways to grant the user Read permission on all the audited shares-

i. 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]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Description
Access Control Assist...
Members of this group can remot...
Administrators
Administrators Properties
?
X
General
Add...
Remove
OK
Cancel
Apply
Help

Administrators

Description:

Members:

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

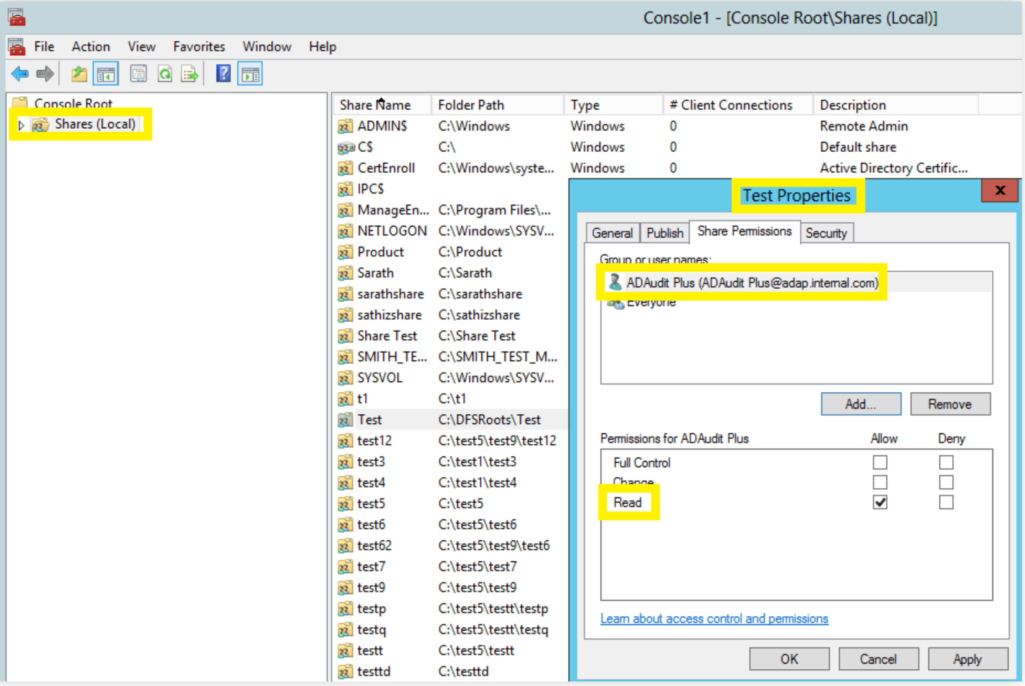
Changes to a user's group membership are not effective until the next time the user logs on.

ii. 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.



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			

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 also needed for file cluster auditing.

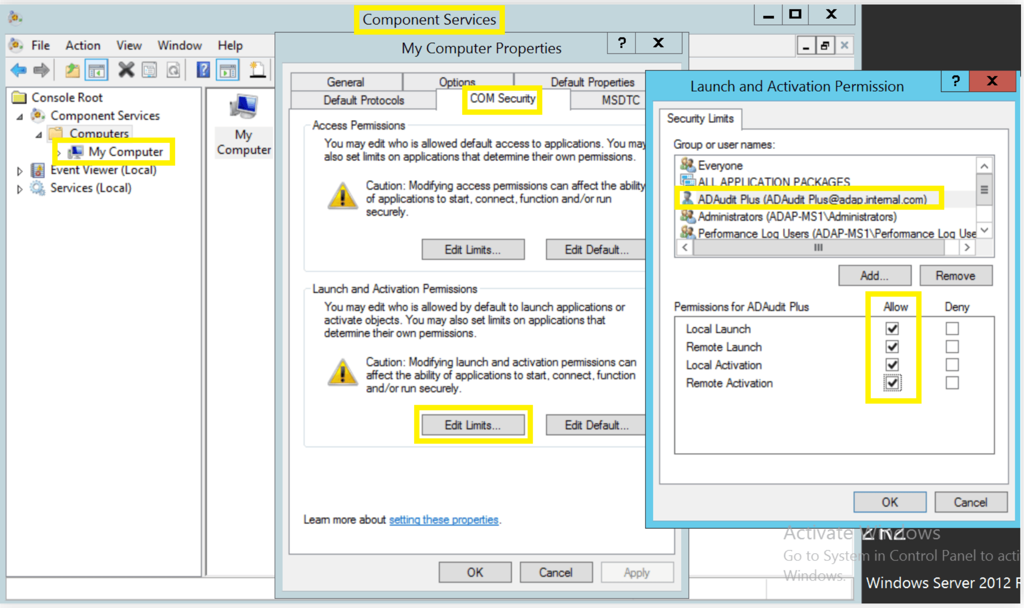
i. Granting DCOM permission:

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.



Access Permissions

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.

Launch and Activation Permissions

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	☑	□

Go to System in Control Panel to acti Windows.

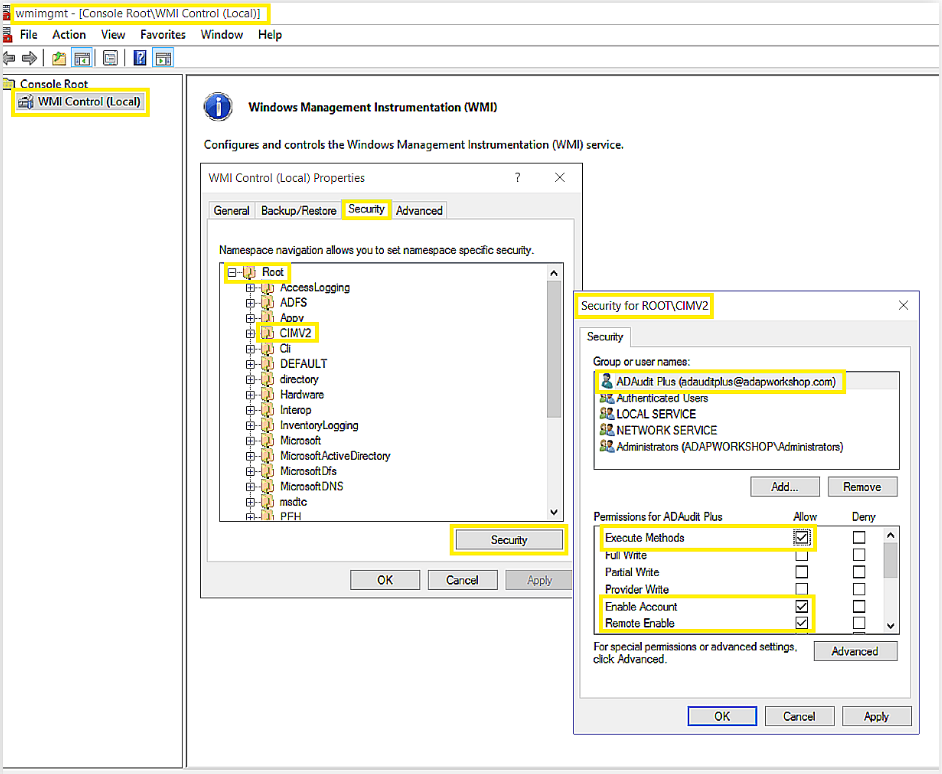
ii. Granting WMI permission:

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.


wmimgmt - [Console Root\WMI Control (Local)]
File Action View Favorites Window Help
Console Root
WMI Control (Local)
General Backup/Restore Security Advanced
Security
OK Cancel Apply
Add... Remove
Advanced
OK Cancel Apply

Windows Management Instrumentation (WMI)

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

WMI Control (Local) Properties

Namespace navigation allows you to set namespace specific security.

- Root
  - AccessLogging
  - ADFS
  - Appv
  - CIMV2
  - Cli
  - DEFAULT
  - directory
  - Hardware
  - Interop
  - InventoryLogging
  - Microsoft
  - MicrosoftActiveDirectory
  - MicrosoftDfs
  - MicrosoftDNS
  - msdtc
  - PEH

Security for ROOT\CIMV2

Group or user names:

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

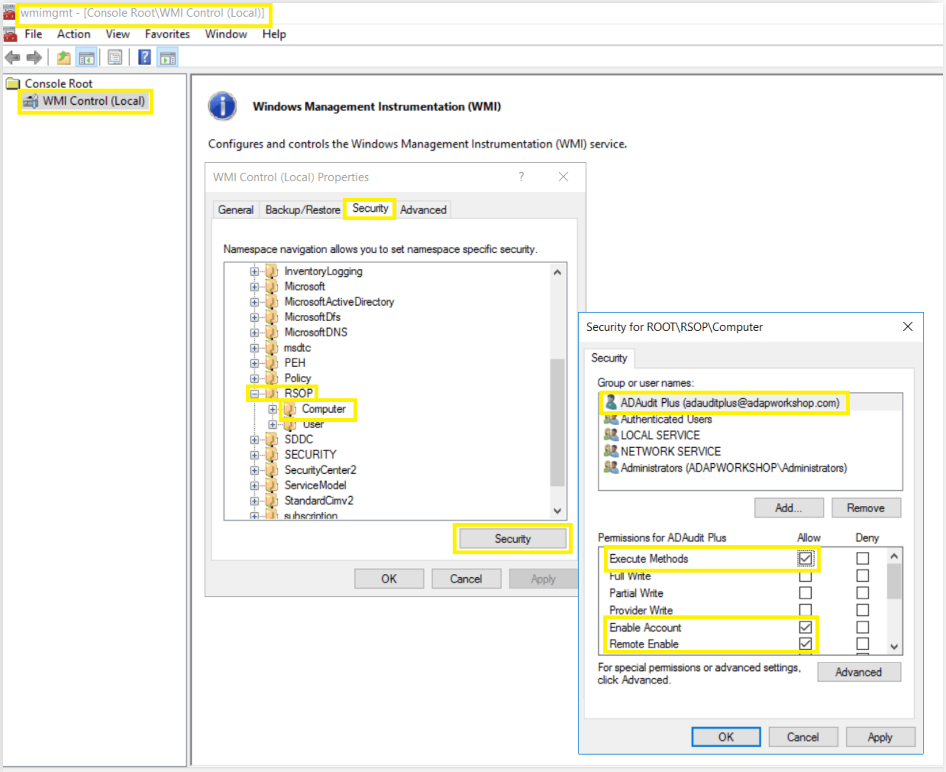
Permissions for ADAudit Plus	Allow	Deny
Execute Methods	☑	□
Full Write	□	□
Partial Write	□	□
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□

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.


wmimgmt - [Console Root\WMI Control (Local)]
File Action View Favorites Window Help
Console Root
WMI Control (Local)
General Backup/Restore Security Advanced
Security
OK Cancel Apply
Add... Remove
Advanced
OK Cancel Apply

Windows Management Instrumentation (WMI)

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

WMI Control (Local) Properties

Namespace navigation allows you to set namespace specific security.

- InventoryLogging
- Microsoft
- MicrosoftActiveDirectory
- MicrosoftDfs
- MicrosoftDNS
- msdtc
- PEH
- Policy
- RSOP
  - Computer
  - User
- SDDC
- SECURITY
- SecurityCenter2
- ServiceModel
- StandardCimv2
- subscription

Security for ROOT\RSOP\Computer

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.

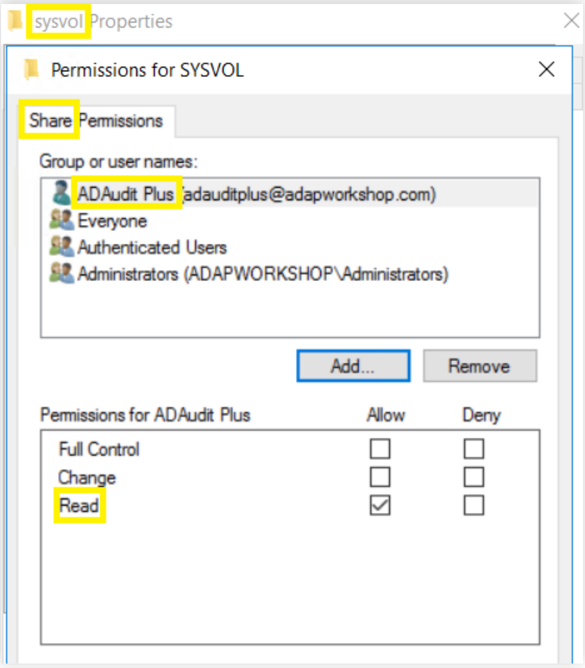
4.4 Grant the user read permission over the c$ share

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

5. Other privileges

i. 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	☑	□

ii. Grant the user Full control over the product installation folder:

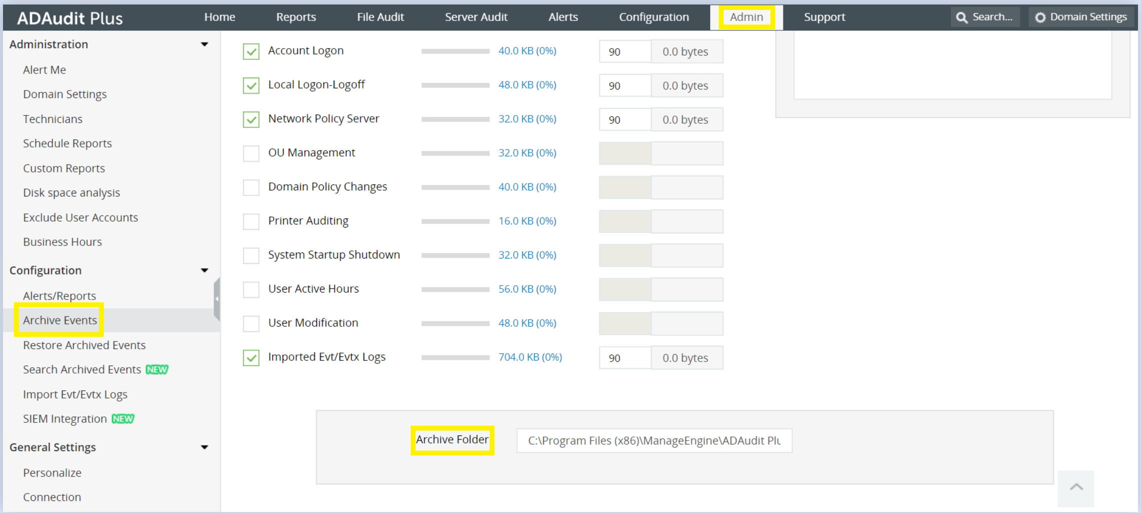
Full control over the product installation folder is needed for ADAudit Plus to write in the database.

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.**

iii. 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\archive). If the Archive folder is saved elsewhere, Full control permissions 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.**

c. If the archive folder is a shared folder, go to the Sharing tab → Advanced Sharing... → Permissions → **Add the ADAudit Plus User → Provide Full control permission.**

iv. 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.

ii. 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.**

iii. 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 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.**

v. 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.**

vi. 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.

ManageEngine
ADAudit Plus

Our Products

AD360 | Log360 | ADManager Plus | ADSelfService Plus

DataSecurity Plus | M365 Manager Plus

About ADAudit Plus

ADAudit Plus is a unified auditing solution that provides full visibility into activities across Active Directory (AD), Entra ID, file servers (Windows, NetApp, EMC and more), Windows servers and workstations—all in just a few clicks. ADAudit Plus helps organizations streamline auditing, demonstrate compliance and enhance their identity threat detection and response with capabilities like real-time change auditing, user logon tracking, account lockout analysis, privileged user monitoring, file auditing, compliance reporting, attack surface analysis (for AD, Azure, AWS, and GCP), UBA, response automation and AD backup and recovery.

For more information about ADAudit Plus, visit www.manageengine.com/products/active-directory-audit/.

$ Get Quote   ⤓ Download