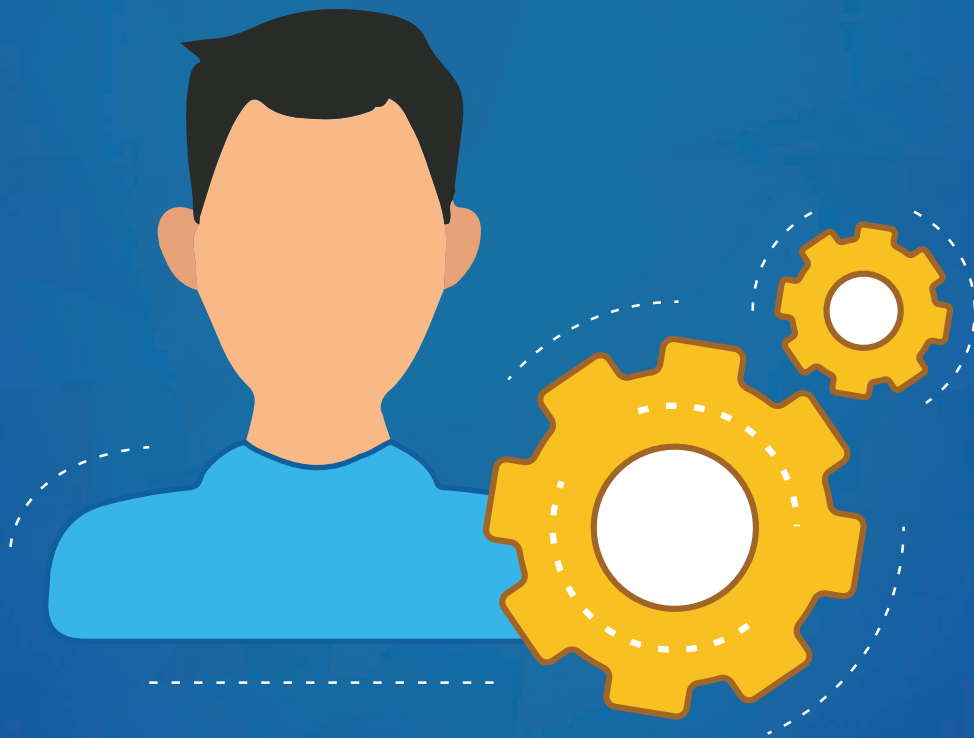


# AD Audit Plus

## Service Account Configuration



# Table of Contents

<b>1. New user, group, and GPO creation</b>	<b>1</b>
1.1 Create a new user	1
1.2 Create a new group	1
1.3 Create a new domain level GPO and link it to all the audited computers	1
<b>2. Privileges/permissions required for event log collection</b>	<b>2</b>
2.1 Grant the user the Manage auditing and security log right	2
2.2 Make the user a member of the Event Log Readers group	3
<b>3. Privileges/permissions required for automatic audit policy and object level auditing configuration</b>	<b>4</b>
3.1 Privileges/permissions required for Domain Controller auditing configuration	4
3.2 Privileges/permissions required for member server, workstation, and file server auditing configuration	5
3.2.1 Make the user a member of the Group Policy Creator Owners group	5
3.2.2 Grant the user, group management permissions	5
<b>4. Privileges/permissions required for file server auditing</b>	<b>7</b>
4.1 Make the user a member of the Power Users group	7
4.2 Grant the user Read permission on all audited shares	8
4.3 Grant the user DCOM and WMI permissions	9
<b>5. Other privileges/permissions required</b>	<b>10</b>



# 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.

## 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.

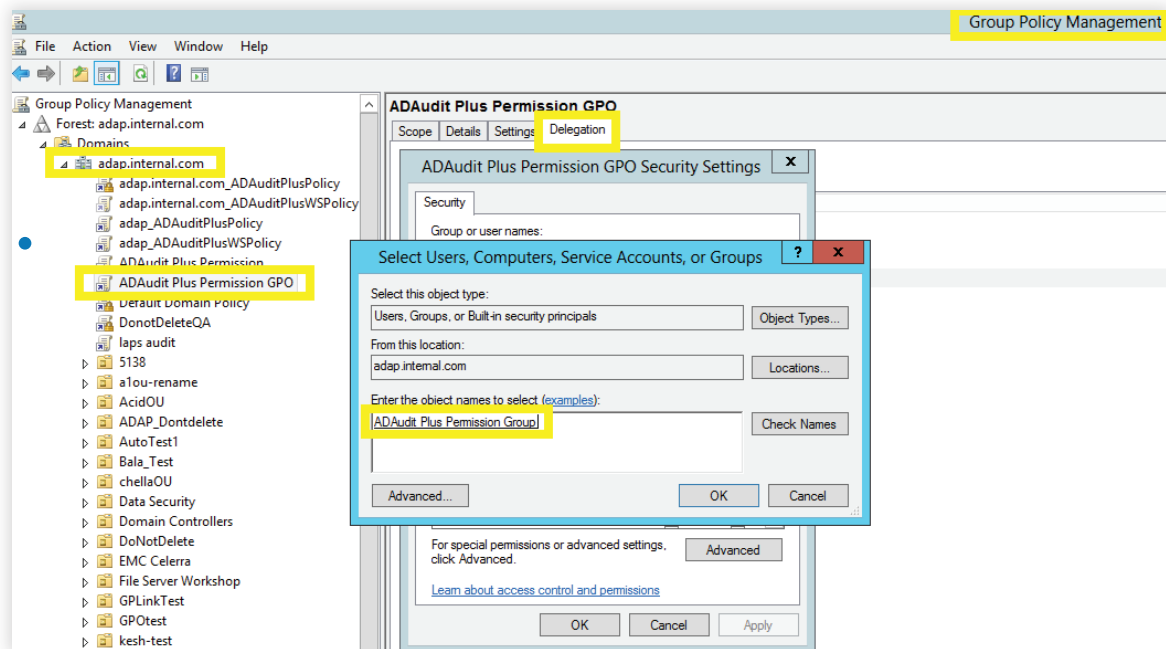
### 1.3 Create a new domain level GPO and link it to all the audited computers

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".

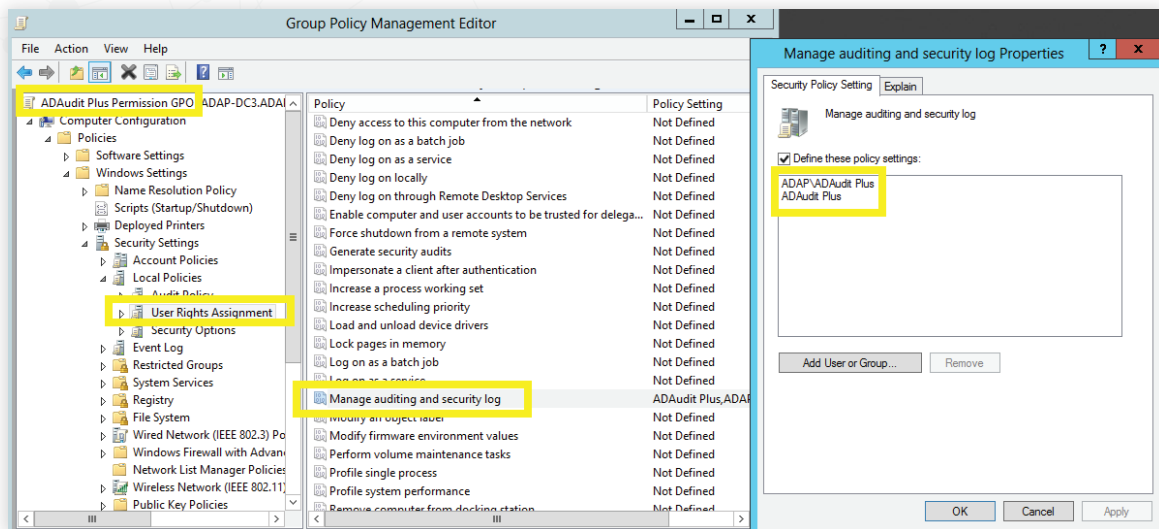


## 2. Privileges/permissions required for event log collection

### 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.

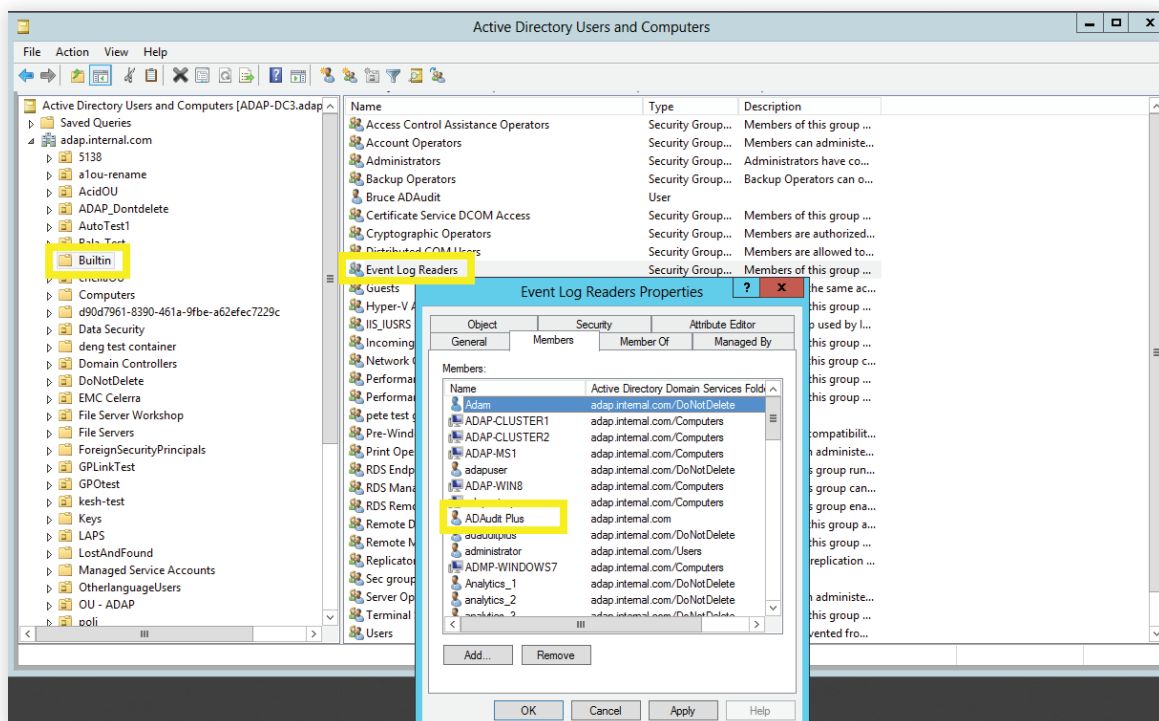


## 2.2 Make the user a member of the Event Log Readers group

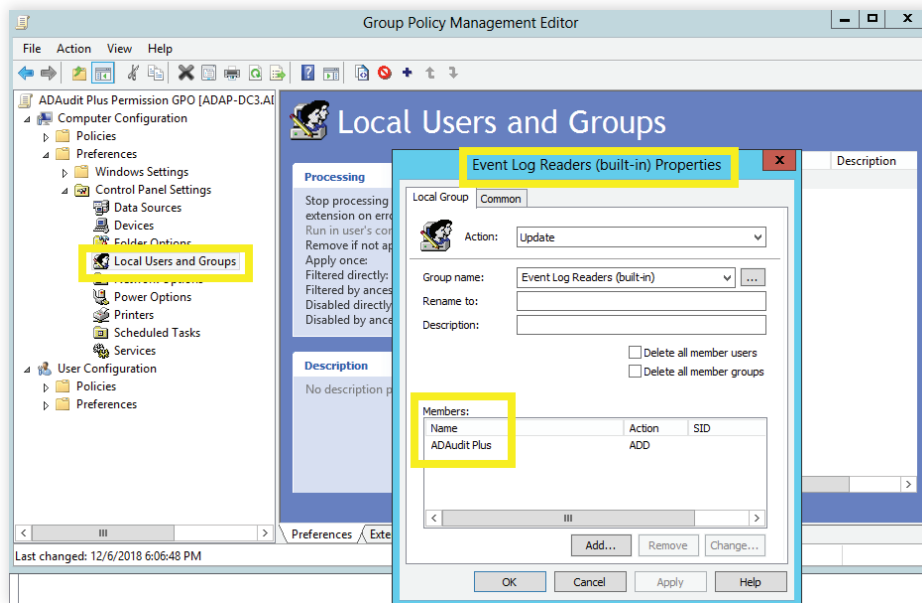
Members of the event log readers group will be able to read the event logs of all the audited computers.

- **For Domain Controllers:**

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



- **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.

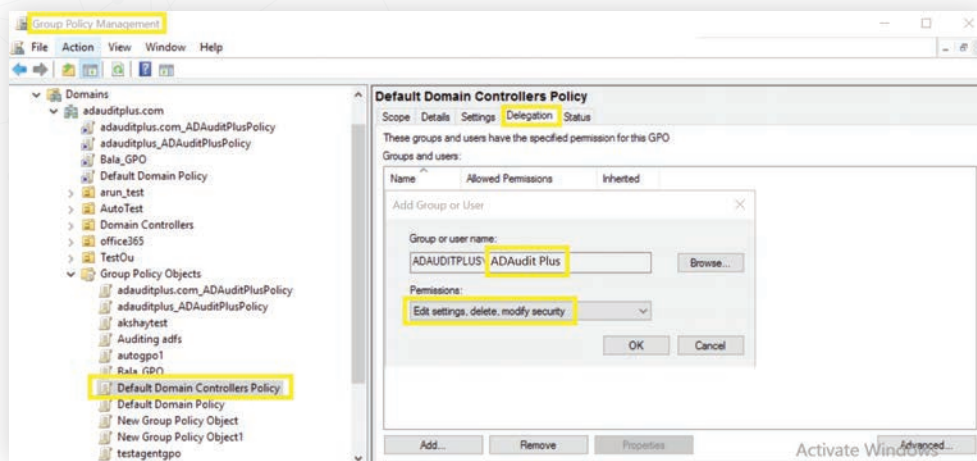


### 3. Privileges/permissions required for automatic audit policy and object level auditing configuration

#### 3.1 Privileges/permissions required for Domain Controller auditing configuration

Granting the service account the following privileges/permissions, allows ADAudit Plus to 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.

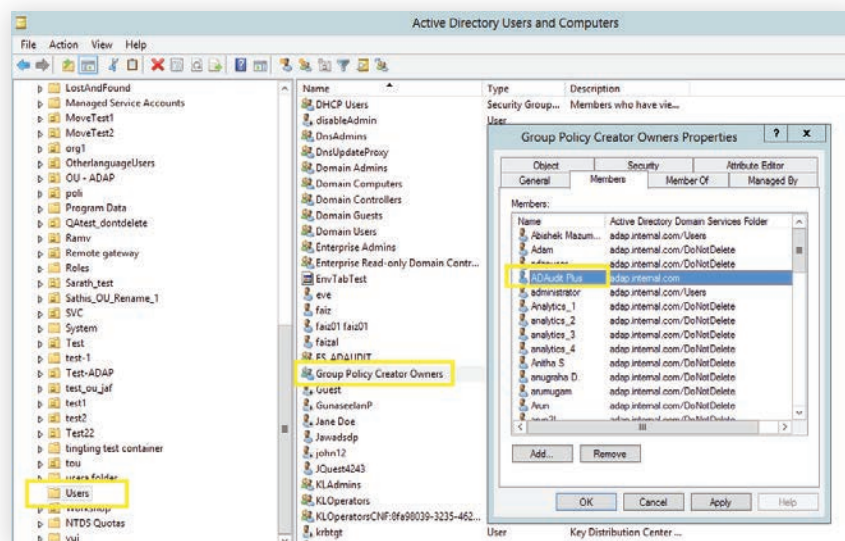
- **Log in to your Domain Controller with Domain Admin privileges** → Open the Group Policy Management Console → click on Default Domain Controllers Policy → Navigate to the right panel, click on the Delegation tab → Add the ADAudit Plus User → Provide permission to Edit settings, delete, modify security.



## 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.



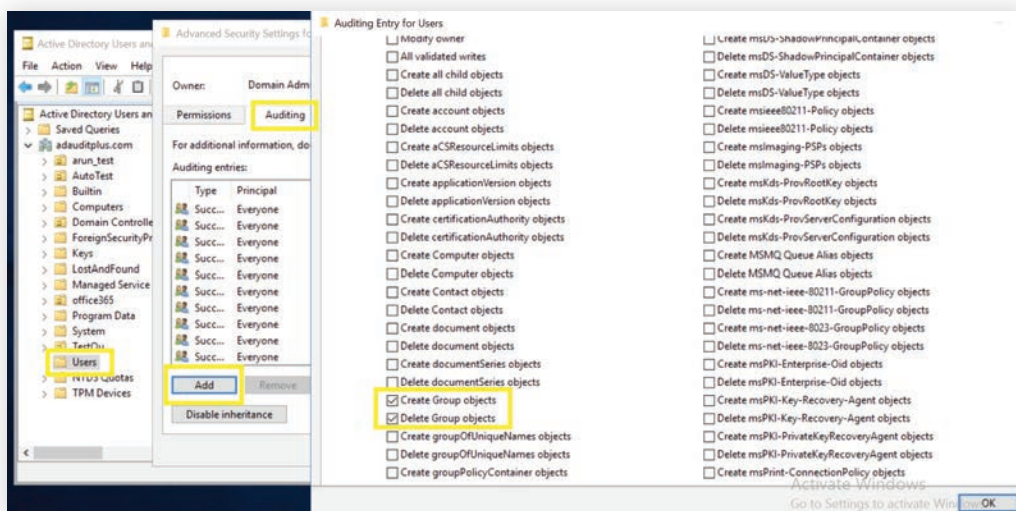
### 3.2.2 Grant the user, group management permissions

- 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.



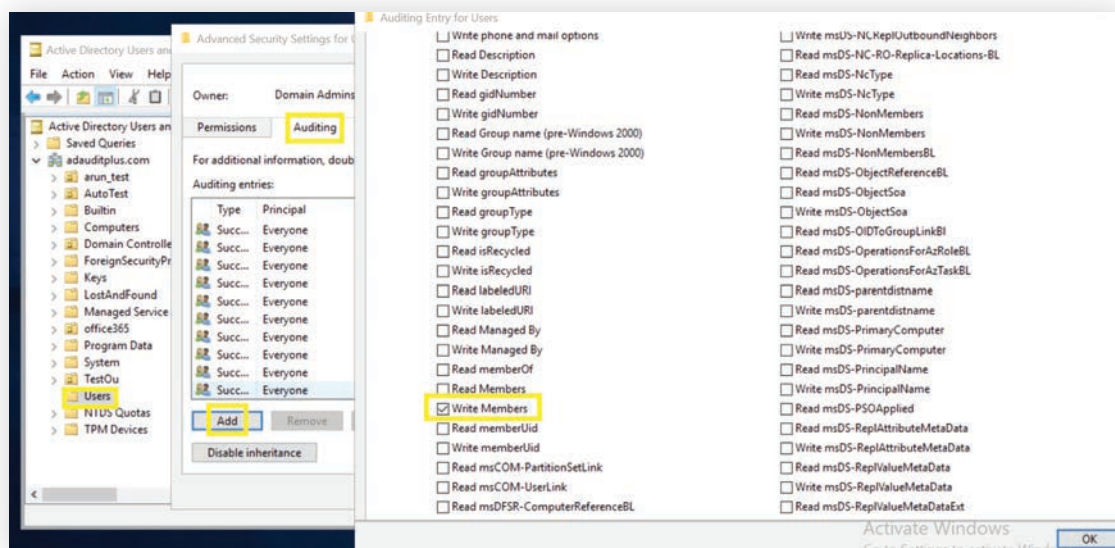
- Right click on Users → Properties → Security → Advanced → Auditing → Add → In the Auditing Entry window, Select a principal: ADAudit Plus user → Type: Success → Applies to: This object and all descendant objects → Select permissions: Create group objects and Delete group objects.

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



- From the Active Directory User and Computers console → Right click on Users → Properties → Security → Advanced → Auditing → Add → In the Auditing Entry window → Select a principal: ADAudit Plus user → Type: Success → Applies to: Descendant group objects → Select property: Write members.

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



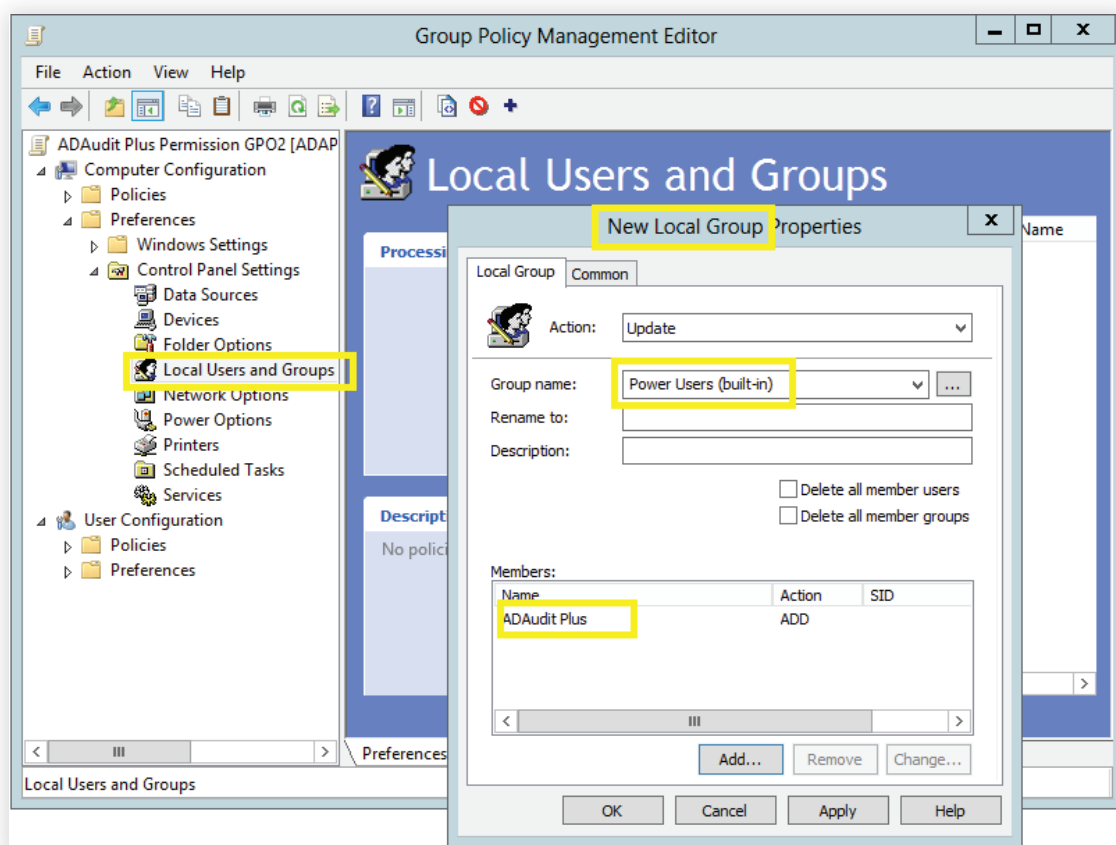


## 4. Privileges/permissions required for file server auditing

### 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.

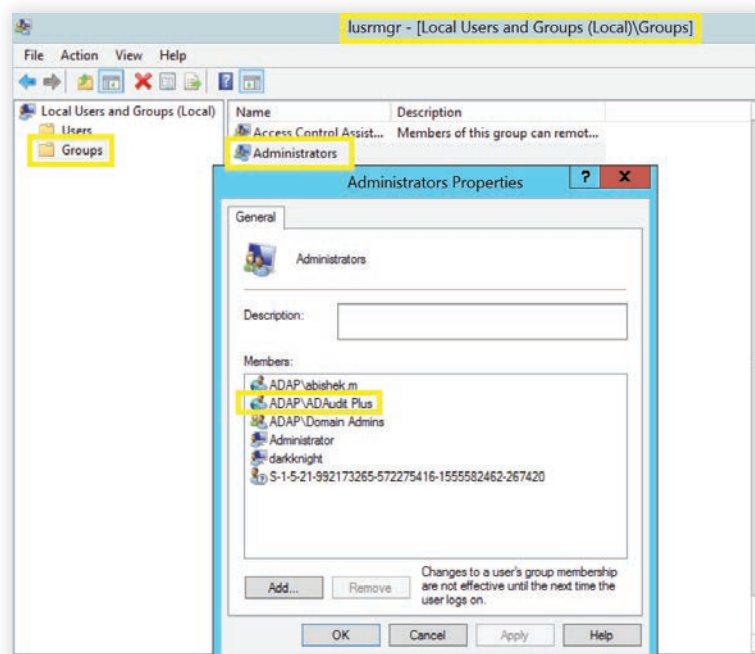
- Log in to your Domain Controller with Domain Admin privileges → Open the Group Policy Management Console → Right click on the "ADAudit Plus Permission GPO" → Edit.
- In the Group Policy Management Editor → Computer Configuration → Preferences Control Panel Settings → Right click on Local Users and 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.



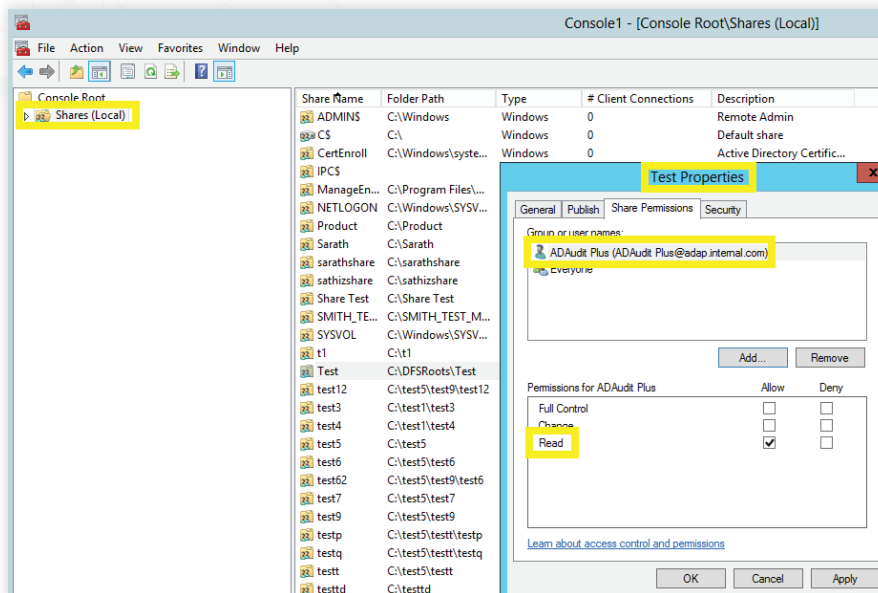
## 4.2 Grant the user Read permission on all audited shares

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.



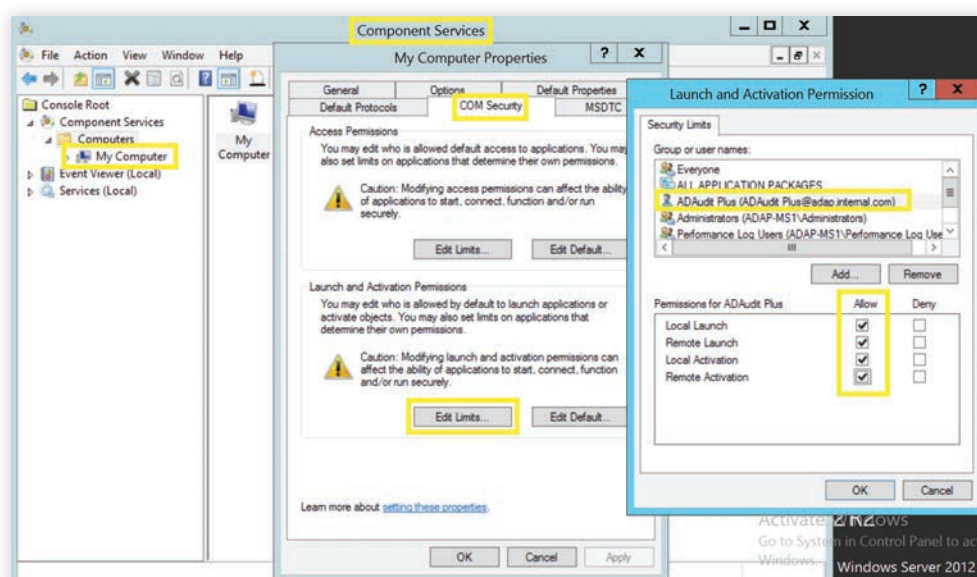
- **Grant the user both Share and NTFS, Read permission on every audited share.**
  - a. Login to any computer with Domain Admin privileges → Open MMC console → File → Add/Remove Snap-in → Select Shared Folders → Add → Another computer → Add target computer
  - b. Select target computer → Select share → 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.



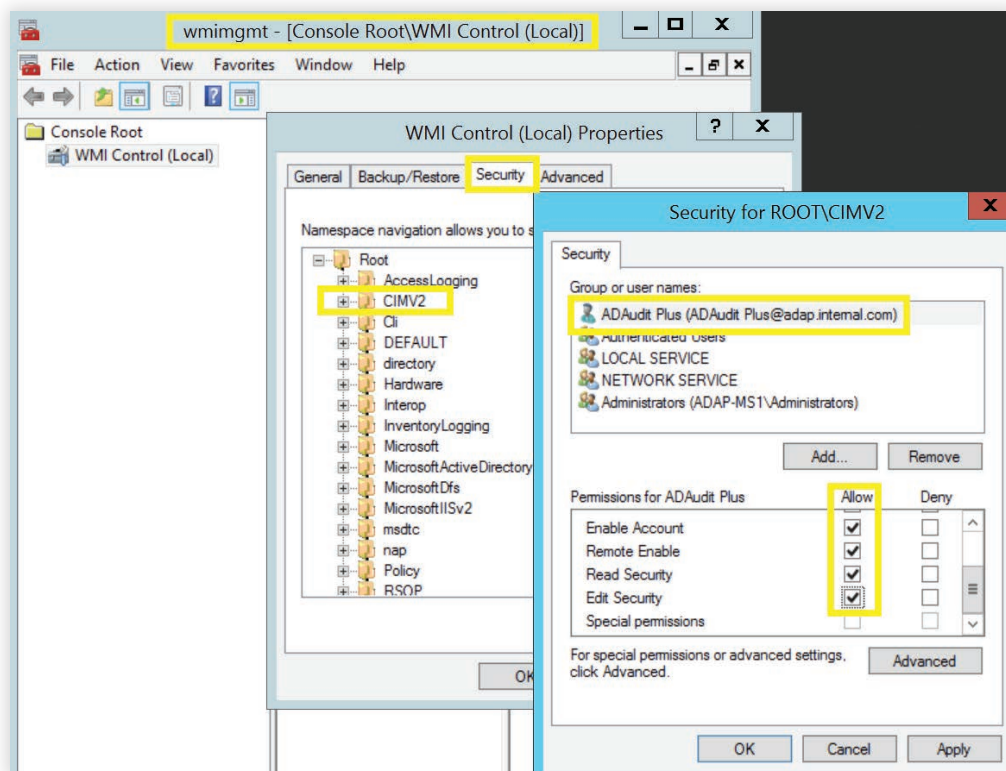
### 4.3 Grant the user DCOM and WMI permissions

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

- Granting DCOM permission:
  - Log in to any computer with Domain Admin privileges → Open Component Services → Connect to target computer → Right click on target computer → Properties → COM Security.
  - Navigate to Launch and Activation Permissions → Edit Limits → Security Limits → Add the "ADAudit Plus" user and grant all permissions.
  - Repeat the steps for every audited computer.



- **Granting WMI permission:**
  - a. **Log in to any computer with a Domain Admin privileges** → Run `wmimgmt.msc` → Right click on WMI Control → Connect to target computer.
  - b. Right click on WMI Control (target computer) → Properties → Security → CIMV2 → Security → Add the "ADAudit Plus" user and grant all permissions.
  - c. Repeat the steps for every audited computer.

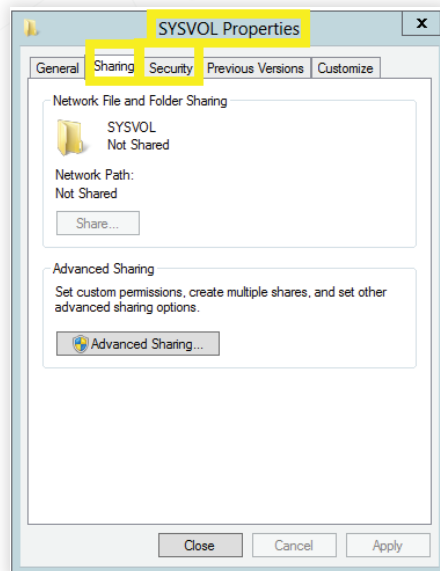


## 5. Other privileges/permissions required

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

Full control over the SYSVOL folder is needed for GPO Settings change auditing.

**Log in to your Domain Controller with Domain Admin privileges** → Locate the SYSVOL folder → Right click → Properties → Security → Edit → Add the "ADAudit Plus" user → Provide both Share and NTFS, Read permission.



- **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.

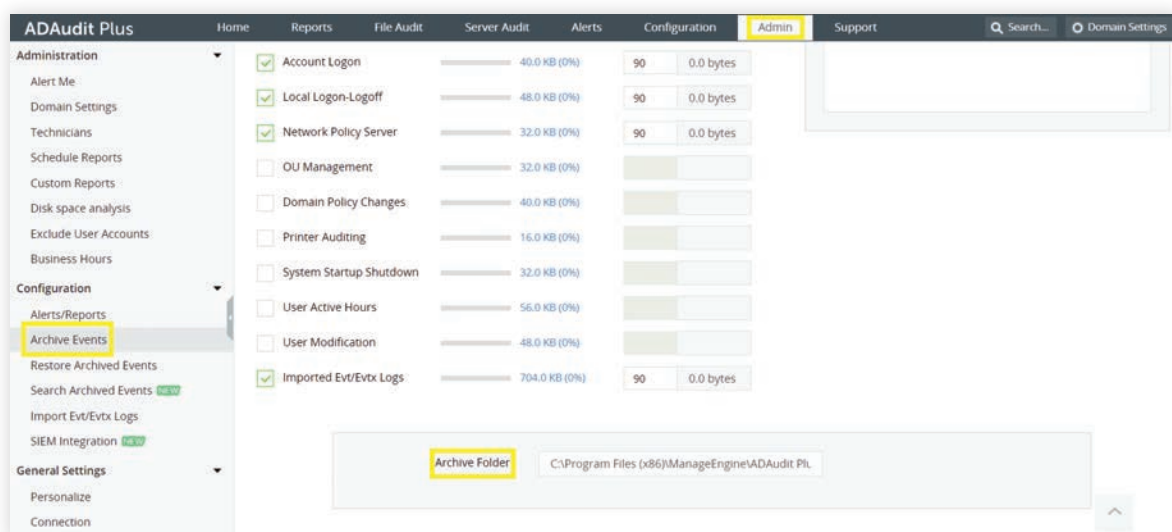
**Log in to the computer where ADAudit Plus is installed with Domain Admin privileges**

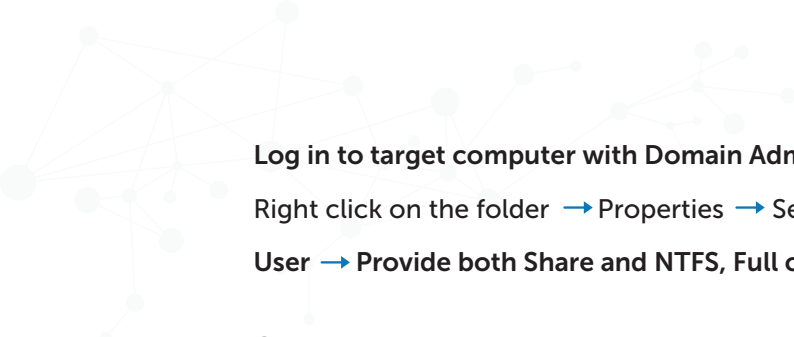
Locate the product installation folder → Right click → Properties → Security → Edit → Add the "ADAudit Plus" user and provide full control.

- **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.

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





**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 both Share and 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.

**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.

**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 both Share and NTFS, Full control permission.**

**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.

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

**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 both share and NTFS, Read and Execute permissions.**

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

## 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