ManageEngine
ADManager Plus

Permissions required for the AD account configured in **ADManager Plus**

www.admanagerplus.com

Table of contents

To carry out the desired Active Directory (AD) management and reporting operations,
ADManager Plus must be provided with the necessary permissions. This can be done by entering the credentials of a user account which has been granted the necessary permissions in the Domain Settings section ADManager Plus' Admin tab.

The user account that you provide can have the credentials of a Domain Admin account. If you do not want to use a Domain Admin account, you can use a user account that has been granted sufficient privileges to carry out the necessary operations.

The following sections contain the least privileges that have to be assigned to a user account for performing the required operation.

User Management

This section provides a detailed explanation on the permissions required to create, modify and delete user accounts.

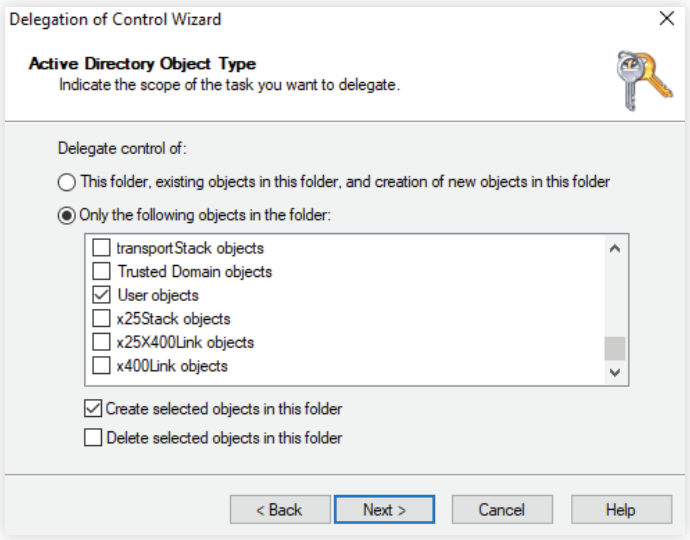
Operation: Create users

Permissions needed:

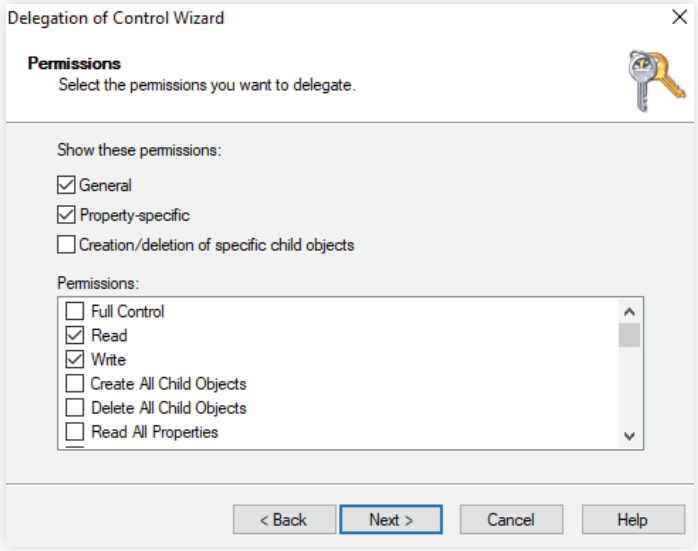
- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all user objects of the required OU.

Steps to grant the permissions to create a user account.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select Delegate Control. The **Delegation of Control** wizard will pop-up
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **User objects** checkbox. Also select the **Create selected objects in this folder** option as indicated in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.
7. Under the permissions section, select the **Read** and **Write** permissions and click on **Next** as indicated in the following image.



8. Click **Finish.**

Operation: Modify users

Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Read, Write, Read All Properties permissions on all user objects of the required OU.

Steps to grant the permissions to modify a user account.

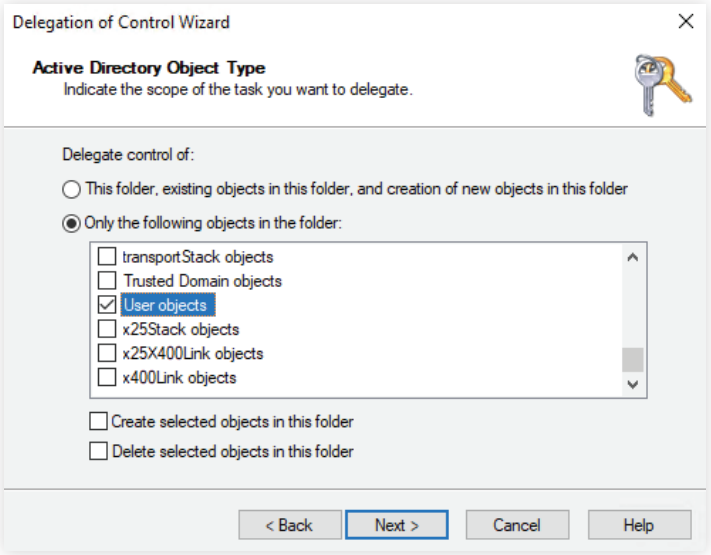
1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**

2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.

3. Click **Next** , add the required user account and click **Next.**

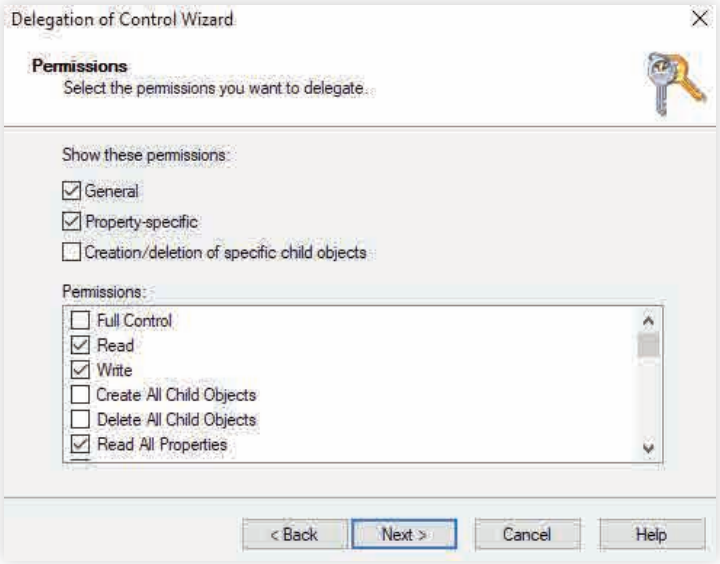
4. Select the **Create a custom task to delegate** option

5. Select the **Only objects in this folder** option and select the **User objects** option as indicated in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.

7. Under the permissions section, select the **Read, Write** and **Read all properties** permissions and click on **Next** as indicated in the following image.



8. Click **Finish.**

Operation: Delete users

Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Delete All Child Objects permission on all user objects of the required OU.

Steps to grant the permissions to delete a user account.

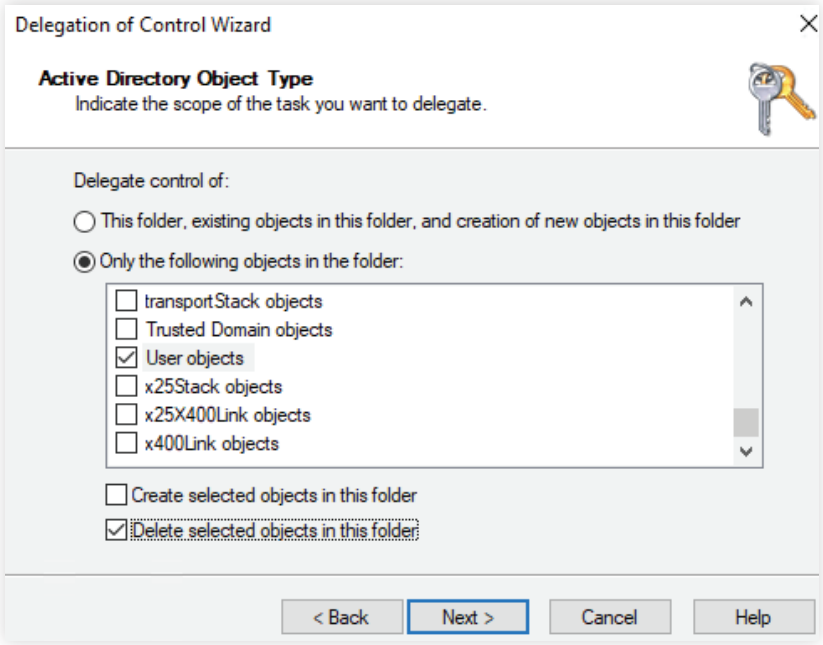
1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**

2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.

3. Click **Next** , add the required user account and click **Next.**

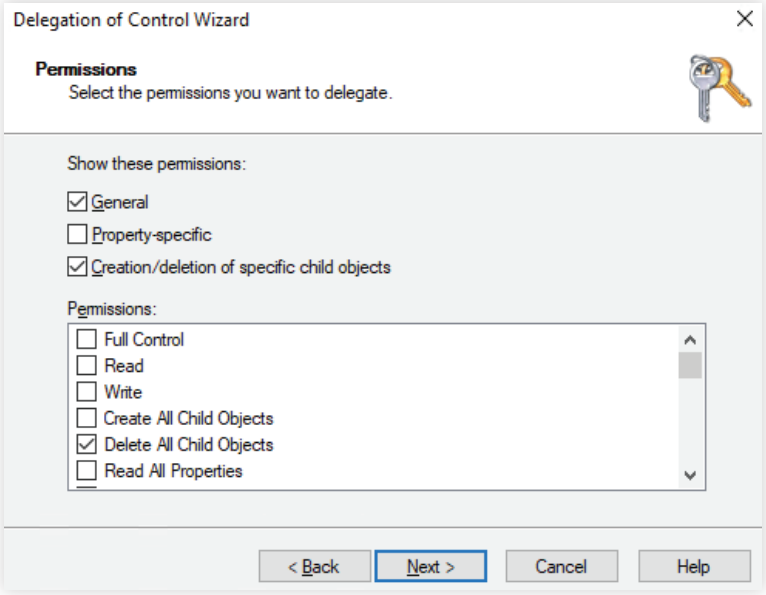
4. Select the **Create a custom task to delegate** option

5. Select the **Only objects in this folder** option and select the **User objects** checkbox.
   Also select the **Delete selected objects in this folder** option as indicated in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Creation/Deletion of specific child objects** options.

7. Under the permissions section, select the **Delete all child objects** permission and click on **Next** as indicated in the following image.



8. Click **Finish.**

Contact Management

This section provides a detailed explanation on the permissions required to create, modify and delete contacts in AD.

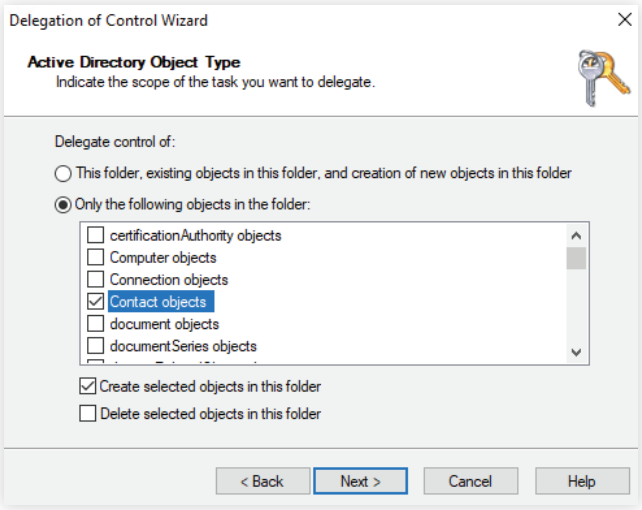
Operation: Create contacts

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all contact objects of the required OU.

Steps to grant the permissions to create a contact account.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **Contact objects** checkbox. Also select the **Create selected objects in this folder** option as indicated in the image below:



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.
7. Under the permissions section, select the **Read** and **Write** permissions and click on **Next.**
8. Click **Finish.**

Operation: Modify contacts

Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Read, Write, Read All Properties permissions on all user objects of the required OU.

Steps to grant the permissions to modify a contact account.

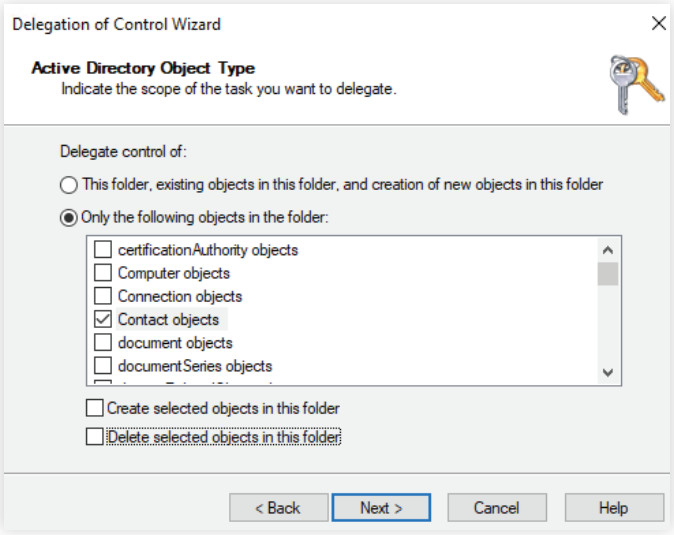
1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**

2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.

3. Click **Next** , add the required user account and click **Next.**

4. Select the **Create a custom task to delegate** option

5. Select the **Only objects in this folder** option and select the **Contact objects** option as indicated in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.

7. Under the permissions section, select the **Read, Write** and **Read all properties** permissions and click on **Next.**

8. Click **Finish.**

Operation: Delete contacts

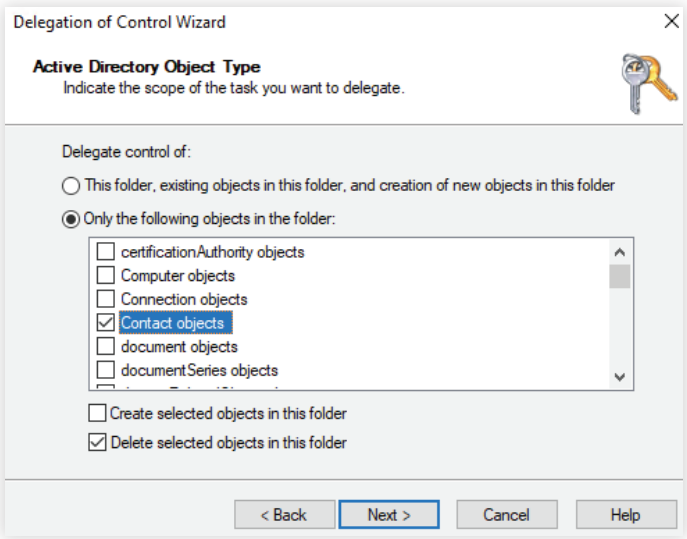
Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Delete All Child objects permission on all contact objects of the required OU.

Steps to grant the permissions to delete a contact account.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option.
5. Select the **Only objects in this folder** option and select the **Contact objects** checkbox. Also select the **Delete selected objects in this folder** option as depicted in the image below:



6. Click on **Next.** Under the Show these permissions section, select **General** and **Creation/Deletion of specific child objects** options.
7. Under the permissions section, select the **Delete all child object**s permission and click on **Next.**
8. Click **Finish.**

Computer Management

This section provides a detailed explanation on the permissions required to create, modify and delete computers in AD.

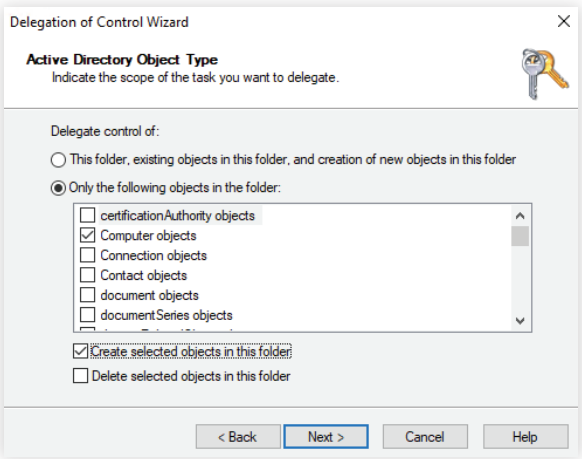
Operation: Create computers

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all computer objects of the required OU.

Steps to grant the permissions to create a computer account.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **Computer objects** checkbox. Also select the **Create selected objects in this folder** option as indicated in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.
7. Under the permissions section, select the **Read** and **Write** permissions and click on **Next.**
8. Click **Finish.**

Operation: Modify computers

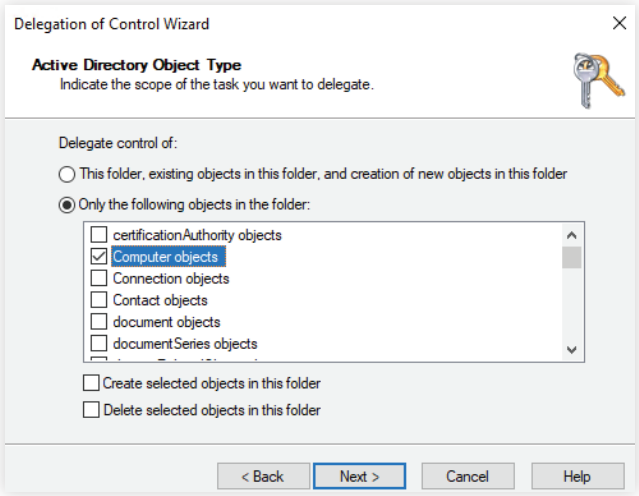
Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Read, Write, Read All Properties permissions on all computer objects of the required OU.

Steps to grant the permissions to modify a computer account.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **Computer objects** checkbox as depicted in the image below:



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.
7. Under the permissions section, select the **Read, Write** and **Read all properties** permissions and click on **Next.**
8. Click **Finish.**

Operation: Delete computers

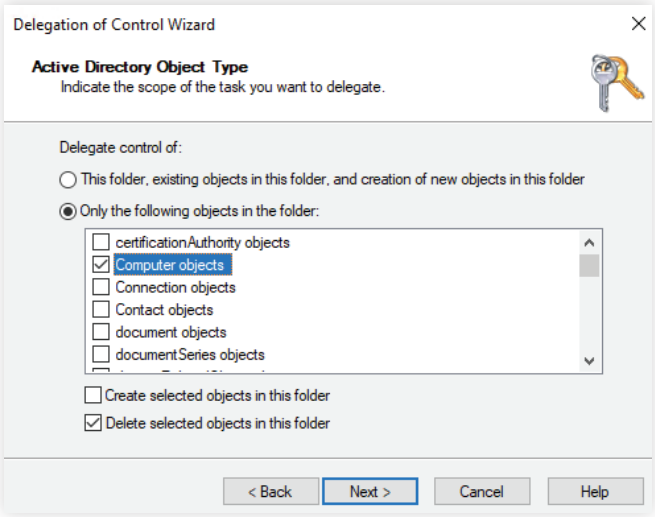
Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Delete All Child objects permission on all computer objects of the required OU.

Steps to grant the permissions to delete a computer account.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **Computer objects** checkbox as depicted in the image below:



6. Click on **Next**. Under the **Show these permission**s section, select **General** and **Creation/Deletion of specific child objects** options.
7. Under the permissions section, select the **Delete all child objects** permission and click on **Next.**
8. Click **Finish.**

Group Management

This section provides a detailed explanation on the permissions required to create, modify and delete groups in AD.

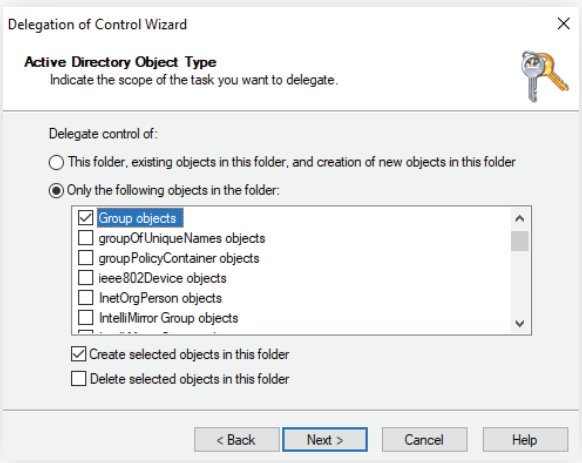
Operation: Create Groups

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Read and Write permissions on all the group objects of the required OU.

Steps to grant the permissions to create groups.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **Group objects** checkbox. Also select the **Create selected objects in this folder** option as depicted in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.
7. Under the permissions section, select the **Read** and **Write** permissions and click on **Next.**
8. Click **Finish.**

Operation: Modify Groups

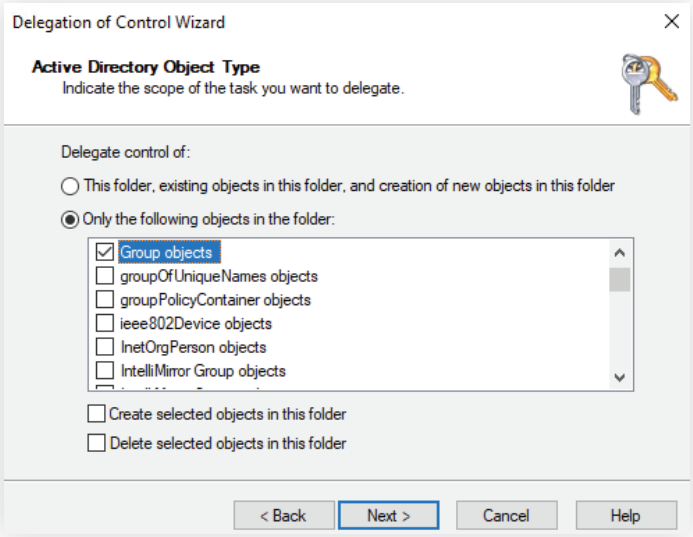
Permissions needed:

- Must be a member of the Account Operators Group

- Must have the Read, Write, Read All Properties permissions on all the group objects of the required OU.

Steps to grant the permissions to modify groups.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option
5. Select the **Only objects in this folder** option and select the **Group objects** checkbox as indicated in the following image.



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Property-specific** options.
7. Under the permissions section, select the **Read, Write** and **Read all properties** permissions and click on **Next.**
8. Click **Finish.**

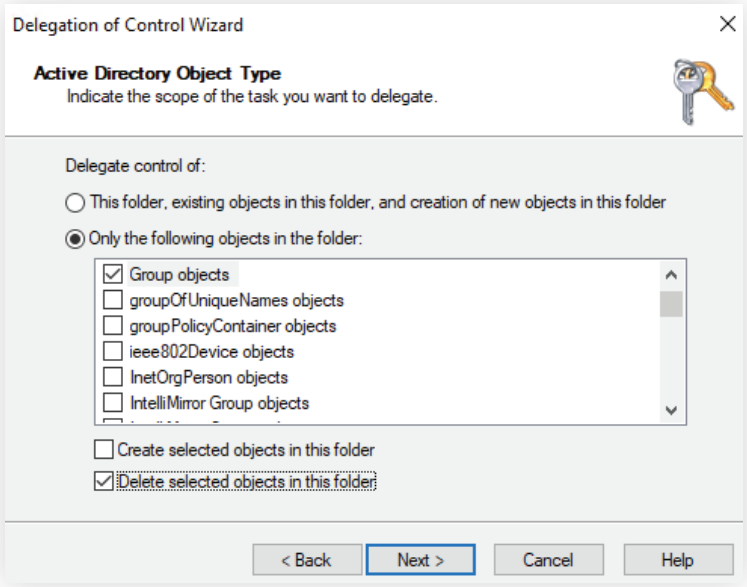
Operation: Delete Groups

Permissions needed:

- Must be a member of the Account Operators Group
- Must have the Delete All Child Objects permission on all the group objects of the required OU.

Steps to grant the permissions to delete groups.

1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**
2. Locate and right click the domain/OU for which you wish to grant the required permissions and select **Delegate Control.** The Delegation of Control wizard will pop-up.
3. Click **Next** , add the required user account and click **Next.**
4. Select the **Create a custom task to delegate** option.
5. Select the **Only objects in this folder** option and select the **Group objects** checkbox. Also select the **Delete selected objects in this folder** option as depicted in the image below:



6. Click on **Next.** Under the **Show these permissions** section, select **General** and **Creation/Deletion of specific child objects** options.
7. Under the permissions section, select the **Delete all child objects** permission and click on **Next.**
8. Click **Finish.**

GPO Management and Reporting

Operation	Permissions needed
Create GPOs	- Must be a member of the Group Policy Creator Owners group
Enable/Disable GPOs	- Must have the Write permission on the 'flags' attribute of the GPO object to be managed.
Enable/Disable user configuration settings	- Must have the Write permission on the 'flags' attribute of the GPO object to be managed.
Enable/Disable computer configuration settings	- Must be a member of the Group Policy Creator Owners group
Enable/Disable/Remove GPO links	- Must have the Write permission on the gPLink attribute of the Site/Domain/OU object to add or remove links to them - Must have the Write permission on the gPOptions attribute of the Site/Domain/OU object to Block/Unblock GPO Inheritance in them
Edit GPO settings	- Must be a member of the Group Policy Creator Owners group
Enforce GPO links	- Must have the Write permission on the gPLink attribute of the Site/Domain/OU object to enforce GPO links to them
Reporting	- Must have the Read permission on the Site/ Domain/OU objects (on gPlink attribute) - Must have the Read permission on the Site/ Domain/OU objects (on gPOptions attribute) - Must have the Read permission on the GPO objects (on flags, versionNumber, modifyTimeStamp, createTimeStamp attributes). **Note:** By default, Domain Users group will have these rights to generate reports. Domain admins and Enterprise admins will have all the above mentioned rights to perform all management/ reporting operations.

AD Reporting

Operations	Permissions needed
Generate all AD reports	- Must have the View permission in the desired OUs/domains.
Generate all NTFS reports	- Must have the Read permission on the relevant folders

File Permission Management

Operations	Permissions needed
Modify/Remove NTFS permissions	- Must have the Read and Write permissions on the relevant folders
Modify/Remove Share permissions	- The share must be reachable from the machine where ADManager Plus is installed

Exchange Management

Operations	Exchange versions	Permissions needed
Creating Exchange mailboxes while creating a corresponding user account in AD	Exchange 2007	- Must have Exchange Recipient Administrator role and Account Operator role.
	Exchange 2010	- Must be a part of the Organization Management group
	Exchange 2013	- Must be a part of the Organization Management group.
Creating Exchange mailboxes for existing Active Directory users	Exchange 2007	- Must have the Exchange Recipient Administrator role and Account Operator role.
	Exchange 2010	- Must be a part of the Organization Management group.
	Exchange 2013	- Must be a part of the Organization Management group.
Setting mailbox rights	Exchange 2007	- Must have the Exchange view only administrator role, Administer information store permission and write permissions on the mailbox store where the mailbox is located.

	Exchange 2010	- Must be a part of the Organization Management group
	Exchange 2013	- Must be a part of the Organization Management group.
Exchange reporting	All versions	- Must have the Exchange View Only Administrator role.

Office 365 Management and Reporting

Operations	Platform	Permissions needed
Management (Recommended: Use an account that has the Global Admin role)	Office 365	- Must have the User Management Admin role.
	Exchange Online	- Must have the Exchange Administrator role.
Reporting	Office 365	- Must have the View Only Administrator role
	Exchange Online	- Must have the User Management Admin role.

To know about the pre-requisites for configuring an Office 365 account in ADManager Plus, click here.

G Suite (Google Apps) Management and Reporting

Operations	Permissions needed
Management	API scopes: https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.orgunit
Reporting	API scopes: https://www.googleapis.com/auth/admin.directory.user

To know about the pre-requisites for configuring a G Suite (Google Apps) account in ADManager Plus, click here.

High Availability

High availability refers to a system or component which aims to ensure an agreed level of operational performance for a higher than normal period. ADManager Plus helps administrators maintain high availability for a server in case of failure of the primary server.

ADManager Plus achieves this by employing a high availability architecture which designates a backup server to act as a shield to the primary server.

- The same database is used for both the servers and at any given time, a single server will cater to user requests and the other will be inactive.
- Whenever the primary server runs encounters unplanned downtime, the standby server becomes operational and takes control of components.

Prerequisites:

- Both the primary and the secondary server must be in the same subnet.

- The user account configured in both the services must be a member of the Domain Admins group while configuring high availability in ADManager Plus.

Note:

Later on, you can remove this user account from the Domain Admins group. However, ensure that this user account has the NTFS and share permissions on both the primary and the secondary servers along with C$(admin share).

If you need any further assistance or information, please write to support@admanagerplus.com or call us at +1 844 245 1108.