Permissions required for the AD account configured in ADManager Plus
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management</td>
<td>1</td>
</tr>
<tr>
<td>i  Create Users</td>
<td>1</td>
</tr>
<tr>
<td>ii Modify Users</td>
<td>3</td>
</tr>
<tr>
<td>iii Delete Users</td>
<td>4</td>
</tr>
<tr>
<td>Contact Management</td>
<td>6</td>
</tr>
<tr>
<td>i  Create Contacts</td>
<td>6</td>
</tr>
<tr>
<td>ii Modify Contacts</td>
<td>7</td>
</tr>
<tr>
<td>iii Delete Contacts</td>
<td>8</td>
</tr>
<tr>
<td>Computer Management</td>
<td>9</td>
</tr>
<tr>
<td>i  Create Computers</td>
<td>9</td>
</tr>
<tr>
<td>ii Modify Computers</td>
<td>10</td>
</tr>
<tr>
<td>iii Delete Computers</td>
<td>11</td>
</tr>
<tr>
<td>Group Management</td>
<td>12</td>
</tr>
<tr>
<td>i  Create Groups</td>
<td>12</td>
</tr>
<tr>
<td>ii Modify Groups</td>
<td>13</td>
</tr>
<tr>
<td>iii Delete Groups</td>
<td>14</td>
</tr>
<tr>
<td>GPO Management and Reporting</td>
<td>15</td>
</tr>
<tr>
<td>AD Reporting</td>
<td>16</td>
</tr>
<tr>
<td>File Permission Management</td>
<td>16</td>
</tr>
<tr>
<td>Exchange Management and Reporting</td>
<td>16</td>
</tr>
<tr>
<td>Office 365 Management and Reporting</td>
<td>17</td>
</tr>
<tr>
<td>G-Suite Management and Reporting</td>
<td>17</td>
</tr>
<tr>
<td>High Availability</td>
<td>18</td>
</tr>
</tbody>
</table>
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.

![Delegation of Control Wizard](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.
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.

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.
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 objects* permission and click on *Next*.

8. Click *Finish*. 
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.
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.
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 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.
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.*
13

**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.
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.
<table>
<thead>
<tr>
<th>Operation</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create GPOs</td>
<td>Must be a member of the Group Policy Creator Owners group</td>
</tr>
<tr>
<td>Enable/Disable GPOs</td>
<td>Must have the Write permission on the ‘flags’ attribute of the GPO object to be managed.</td>
</tr>
<tr>
<td>Enable/Disable user configuration settings</td>
<td>Must have the Write permission on the ‘flags’ attribute of the GPO object to be managed.</td>
</tr>
<tr>
<td>Enable/Disable computer configuration settings</td>
<td>Must be a member of the Group Policy Creator Owners group</td>
</tr>
<tr>
<td>Enable/Disable/Remove GPO links</td>
<td>Must have the Write permission on the gPLink attribute of the Site/Domain/OU object to add or remove links to them</td>
</tr>
<tr>
<td></td>
<td>Must have the Write permission on the gPOptions attribute of the Site/Domain/OU object to Block/Unblock GPO Inheritance in them</td>
</tr>
<tr>
<td>Edit GPO settings</td>
<td>Must be a member of the Group Policy Creator Owners group</td>
</tr>
<tr>
<td>Enforce GPO links</td>
<td>Must have the Write permission on the gPLink attribute of the Site/Domain/OU object to enforce GPO links to them</td>
</tr>
<tr>
<td>Reporting</td>
<td>Must have the Read permission on the Site/Domain/OU objects (on gPLink attribute)</td>
</tr>
<tr>
<td></td>
<td>Must have the Read permission on the Site/Domain/OU objects (on gPOptions attribute)</td>
</tr>
<tr>
<td></td>
<td>Must have the Read permission on the GPO objects (on flags, versionNumber, modifyTimeStam, createTimeStamp attributes).</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Operations</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate all AD reports</td>
<td>- Must have the View permission in the desired OUs/domains.</td>
</tr>
<tr>
<td>Generate all NTFS reports</td>
<td>- Must have the Read permission on the relevant folders</td>
</tr>
</tbody>
</table>

### File Permission Management

<table>
<thead>
<tr>
<th>Operations</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify/Remove NTFS permissions</td>
<td>- Must have the Read and Write permissions on the relevant folders</td>
</tr>
<tr>
<td>Modify/Remove Share permissions</td>
<td>- The share must be reachable from the machine where ADManager Plus is installed</td>
</tr>
</tbody>
</table>

### Exchange Management

<table>
<thead>
<tr>
<th>Operations</th>
<th>Exchange versions</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Exchange mailboxes...</td>
<td>Exchange 2007</td>
<td>- Must have Exchange Recipient Administrator role and Account Operator role.</td>
</tr>
<tr>
<td>for existing Active Directory...</td>
<td>Exchange 2010</td>
<td>- Must be a part of the Organization Management group</td>
</tr>
<tr>
<td>users</td>
<td>Exchange 2013</td>
<td>- Must be a part of the Organization Management group</td>
</tr>
<tr>
<td>Setting mailbox rights</td>
<td>Exchange 2007</td>
<td>- Must have the Exchange view only administrator role, Administer information store permission and write permissions on the mailbox store where the mailbox is located.</td>
</tr>
</tbody>
</table>
### Exchange reporting

<table>
<thead>
<tr>
<th>Platform</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2010</td>
<td>- Must be a part of the Organization Management group</td>
</tr>
<tr>
<td>Exchange 2013</td>
<td>- Must be a part of the Organization Management group</td>
</tr>
<tr>
<td>All versions</td>
<td>- Must have the Exchange View Only Administrator role</td>
</tr>
</tbody>
</table>

### Office 365 Management and Reporting

<table>
<thead>
<tr>
<th>Operations</th>
<th>Platform</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Office 365</td>
<td>- Must have the User Management Admin role</td>
</tr>
<tr>
<td>(Recommended: Use an account that has the Global Admin role)</td>
<td>Exchange Online</td>
<td>- Must have the Exchange Administrator role</td>
</tr>
<tr>
<td>Reporting</td>
<td>Office 365</td>
<td>- Must have the View Only Administrator role</td>
</tr>
<tr>
<td></td>
<td>Exchange Online</td>
<td>- Must have the User Management Admin role</td>
</tr>
</tbody>
</table>

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

### G Suite (Google Apps) Management and Reporting

<table>
<thead>
<tr>
<th>Operations</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>API scopes:</td>
</tr>
<tr>
<td></td>
<td><a href="https://www.googleapis.com/auth/admin.directory.user">https://www.googleapis.com/auth/admin.directory.user</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.googleapis.com/auth/admin.directory.group">https://www.googleapis.com/auth/admin.directory.group</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.googleapis.com/auth/admin.directory.orgunit">https://www.googleapis.com/auth/admin.directory.orgunit</a></td>
</tr>
<tr>
<td>Reporting</td>
<td>API scopes:</td>
</tr>
<tr>
<td></td>
<td><a href="https://www.googleapis.com/auth/admin.directory.user">https://www.googleapis.com/auth/admin.directory.user</a></td>
</tr>
</tbody>
</table>

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.