ManageEngine
ADManager Plus

Permissions setup guide for ADManager Plus operations

www.admanagerplus.com

Table of contents

To carry out the desired Active Directory (AD) and Microsoft 365 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.

To modify Privileged Groups, you need to log in with a user account that is a member of the Administrators Group. If you do not want to use a domain admin account, you can log in with 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

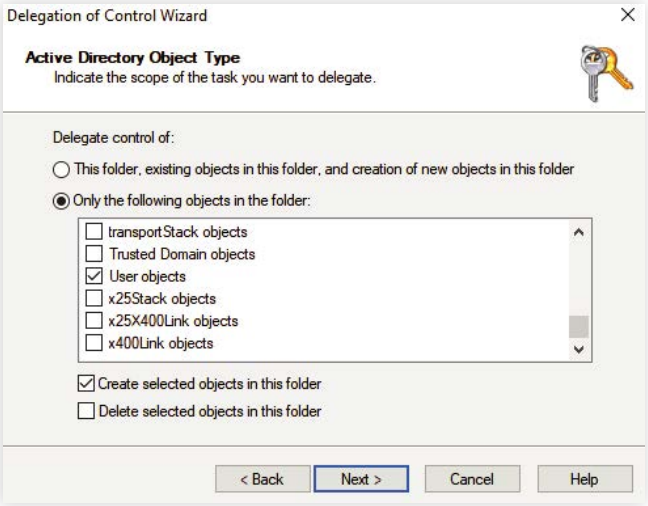
Permissions needed:

- Must be a member of the Account Operators Group, or

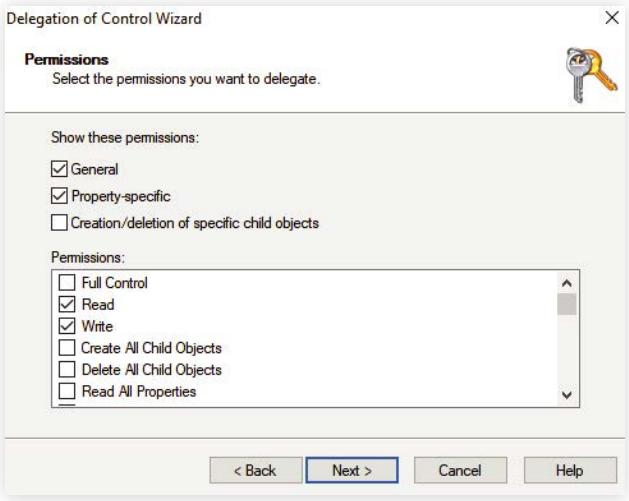
- Must have the Read and Write permissions on all user objects of the required OU.

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, or

- 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.

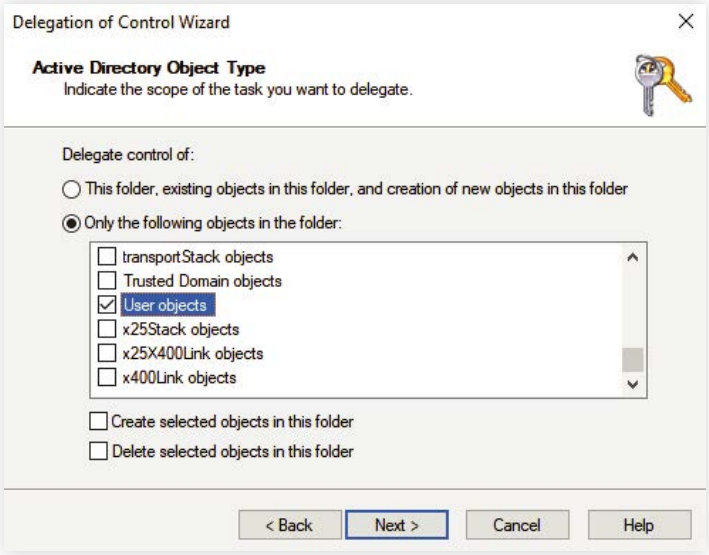
1. Logon to your Domain controller and launch the **Active Directory Users and Computers.**

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.**

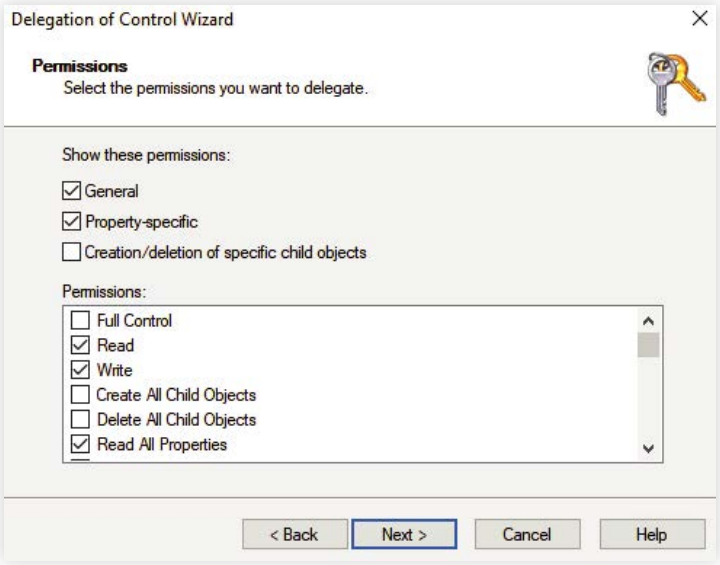
4. Select the **Create a custom task to delegate** option

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

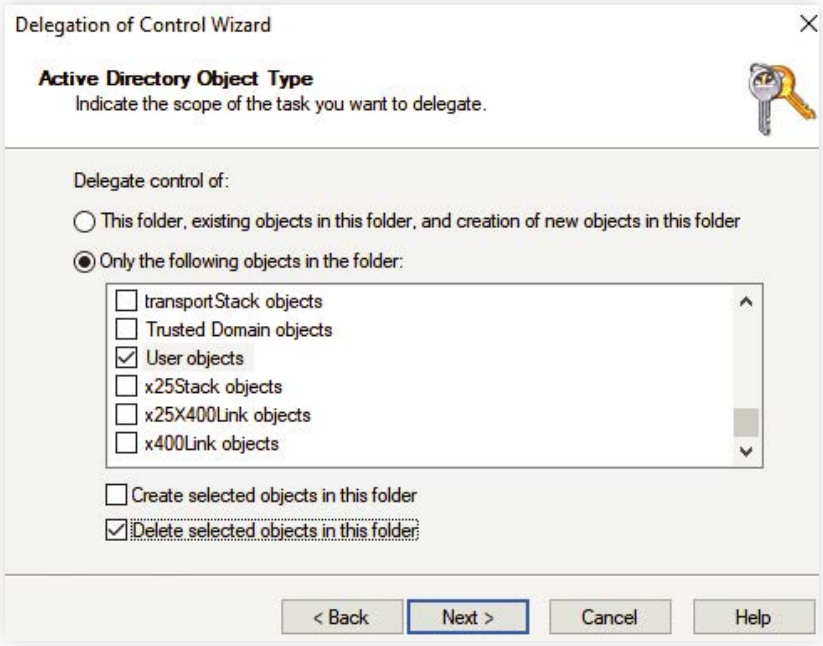
Permissions needed:

- Must be a member of the Account Operators Group, or

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

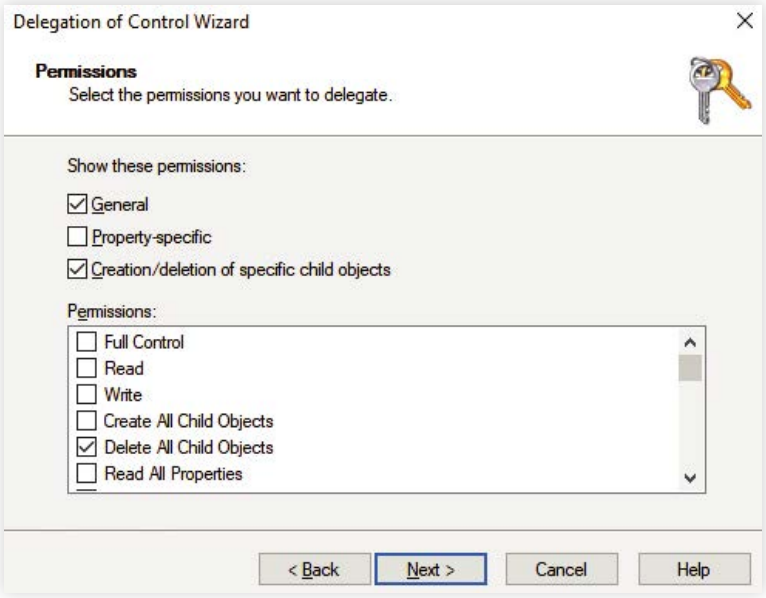
Steps to grant the permissions to delete a user account.

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.**

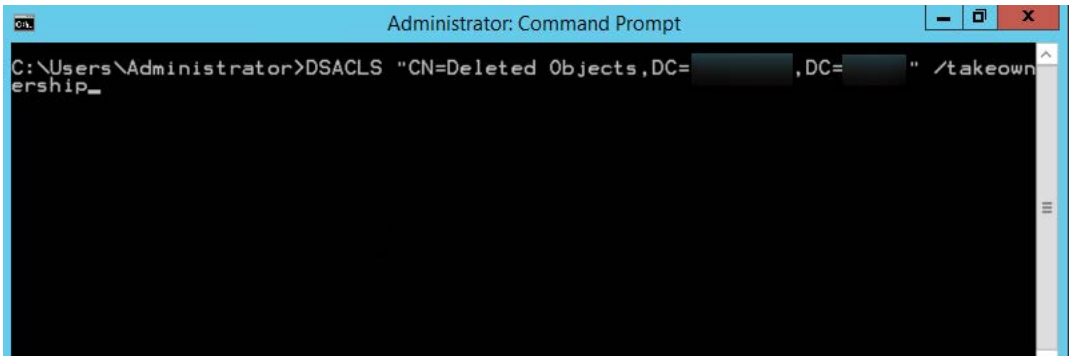
Operation: Restore users

Permissions needed:
- The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group, or
- Permissions to restore AD users must be manually given to the required security principles as shown in the below steps.

Steps to grant the permissions required to restore a deleted AD user

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container.
To grant the required permissions:

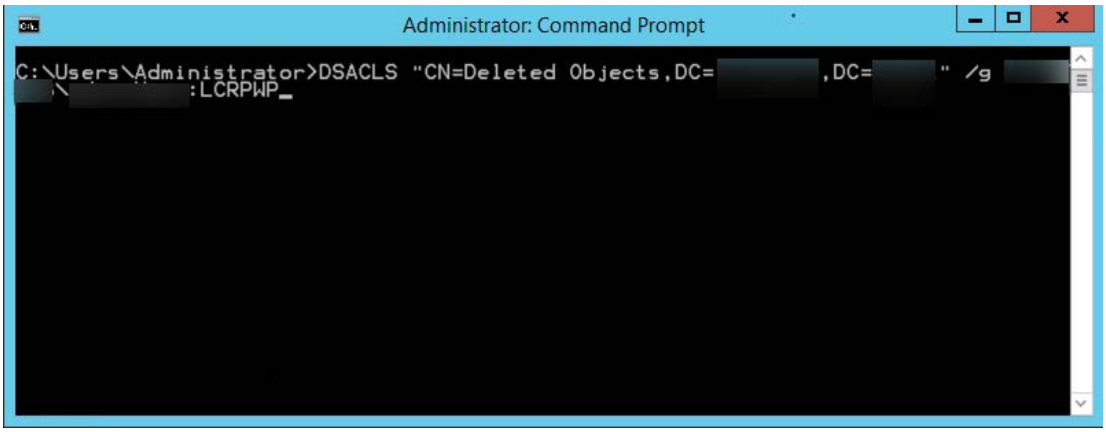
1. Log in to your domain controller and launch the command prompt as an administrator.
2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=**admanagerplus**, DC=**com**" /takeownership and run the command as an administrator.



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.

3. To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP

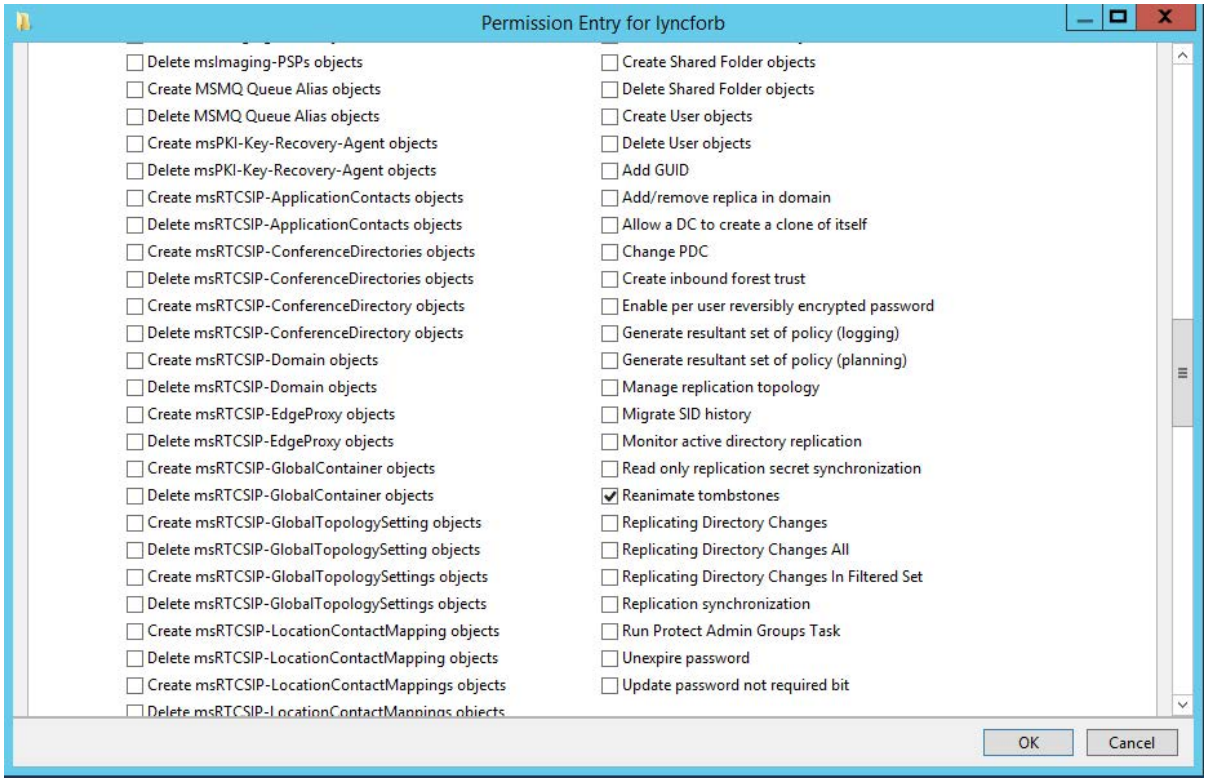


Note: Replace "LukeJohnson" with the security principal of your choice.

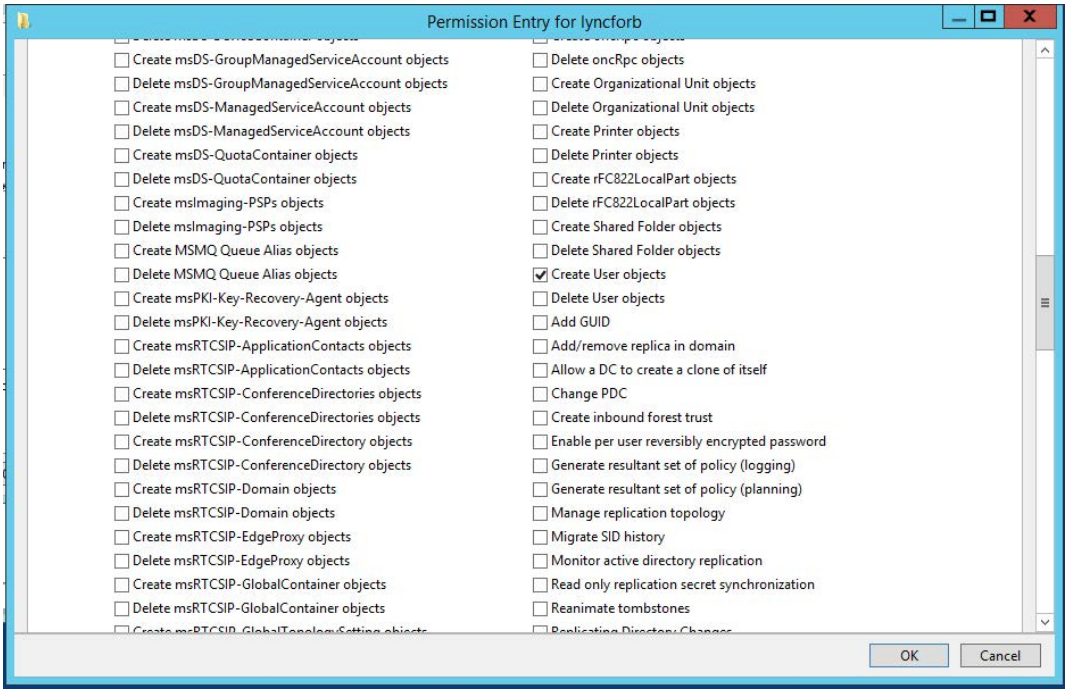
4. Next, connect to the default naming context, right-click on the domain root, and select **Properties.**

5. In the **Security** tab, click **Advanced.**

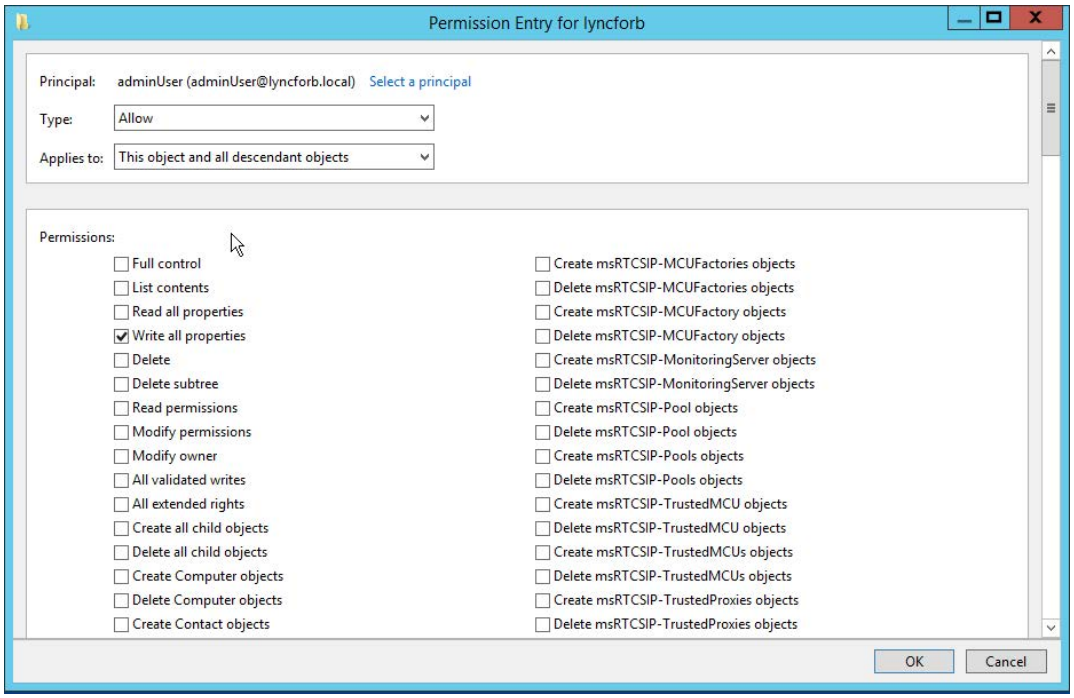
6. Add the user or group, and select the following rights:
   a. Reanimate tombstones



b. Create User objects



c. Write all properties



Note: Apply the **Reanimate tombstones rights** to the object being secured and its descendant objects.

7. Click **OK.**

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

Contact Management

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

Operation: Create contacts

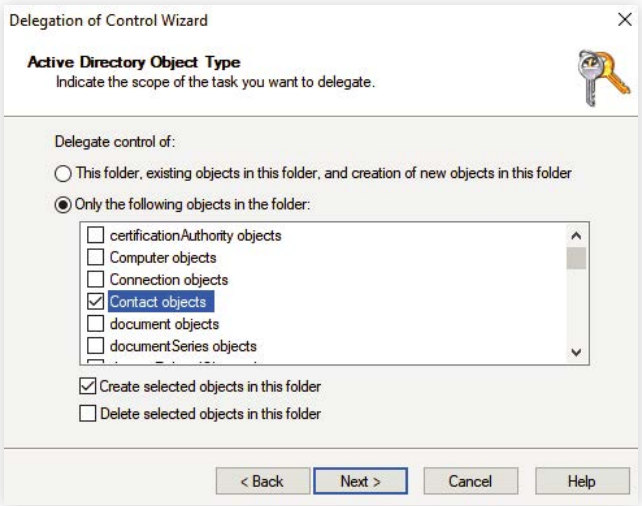
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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

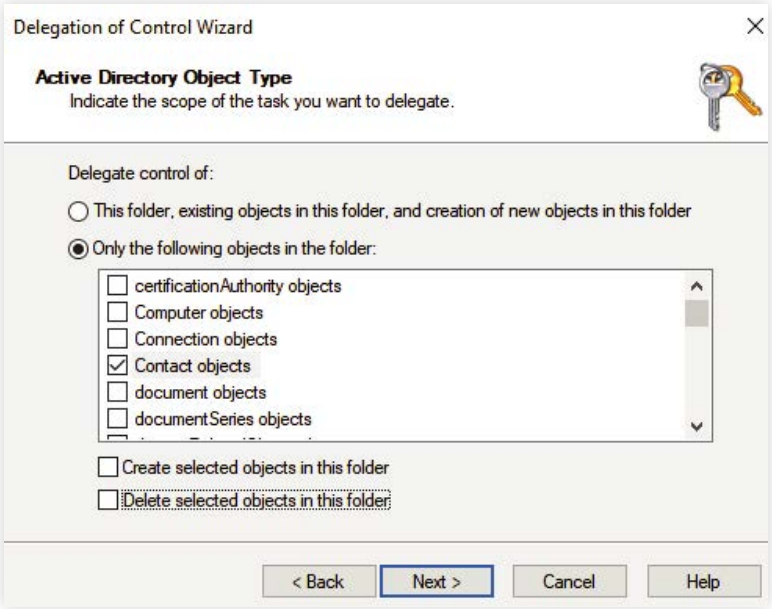
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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, or

- 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.**

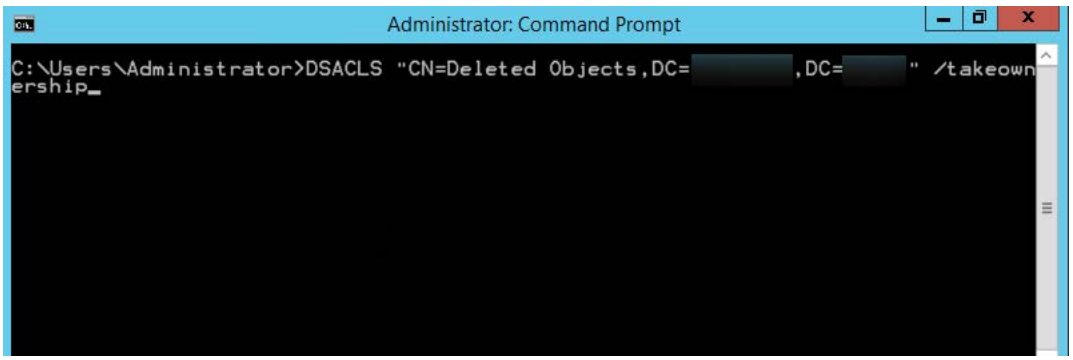
Operation: Restore contacts

Permissions needed:
-The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group, or
- Permissions to restore AD contacts must be manually given to the required security principles as shown in the below steps.

Steps to grant the permissions required to restore a deleted AD contact

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container.
To grant the required permissions:

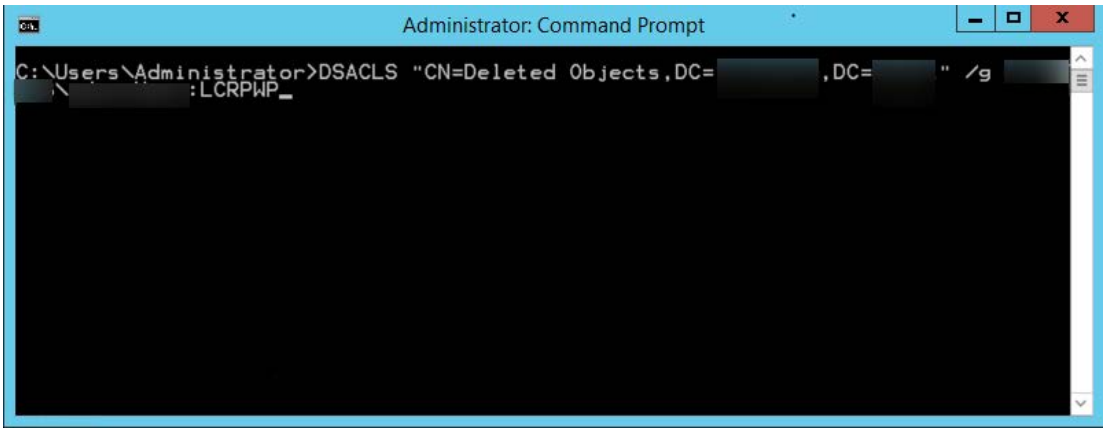
1. Log in to your domain controller and launch the command prompt as an administrator.
2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=**admanagerplus**, DC=**com**" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.

3. To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP

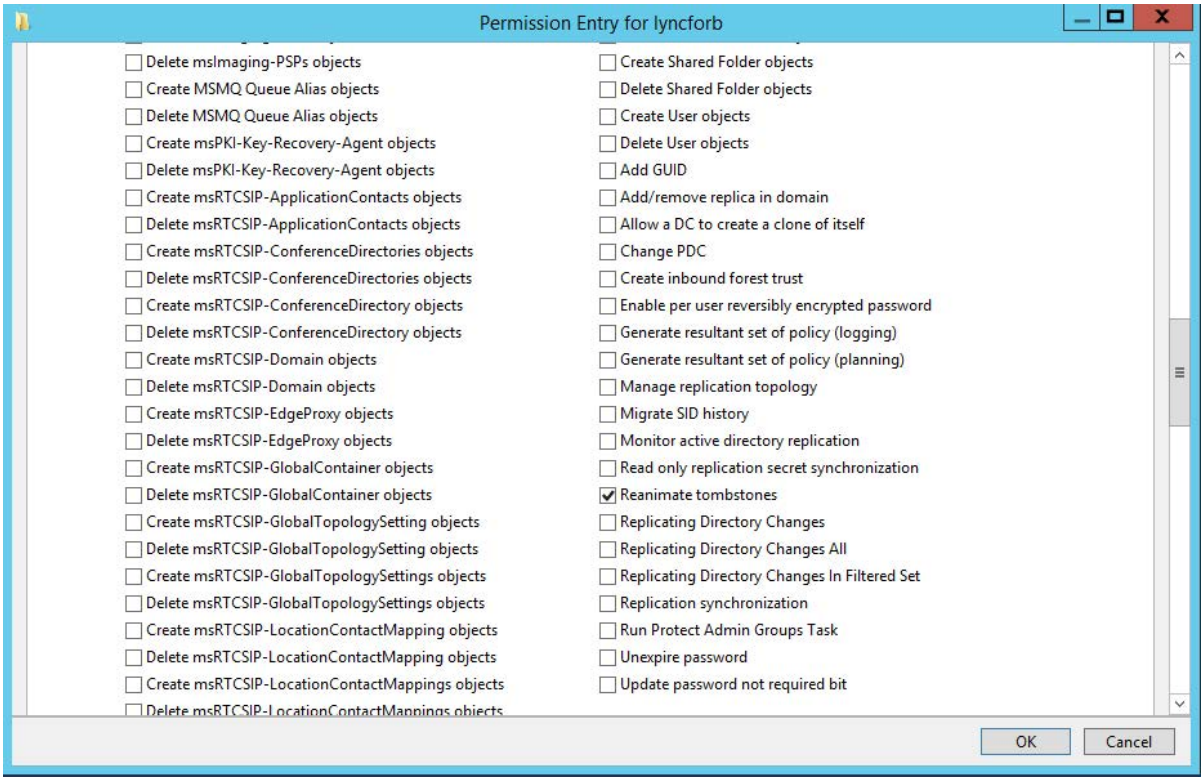


Note: Replace "LukeJohnson" with the security principal of your choice.

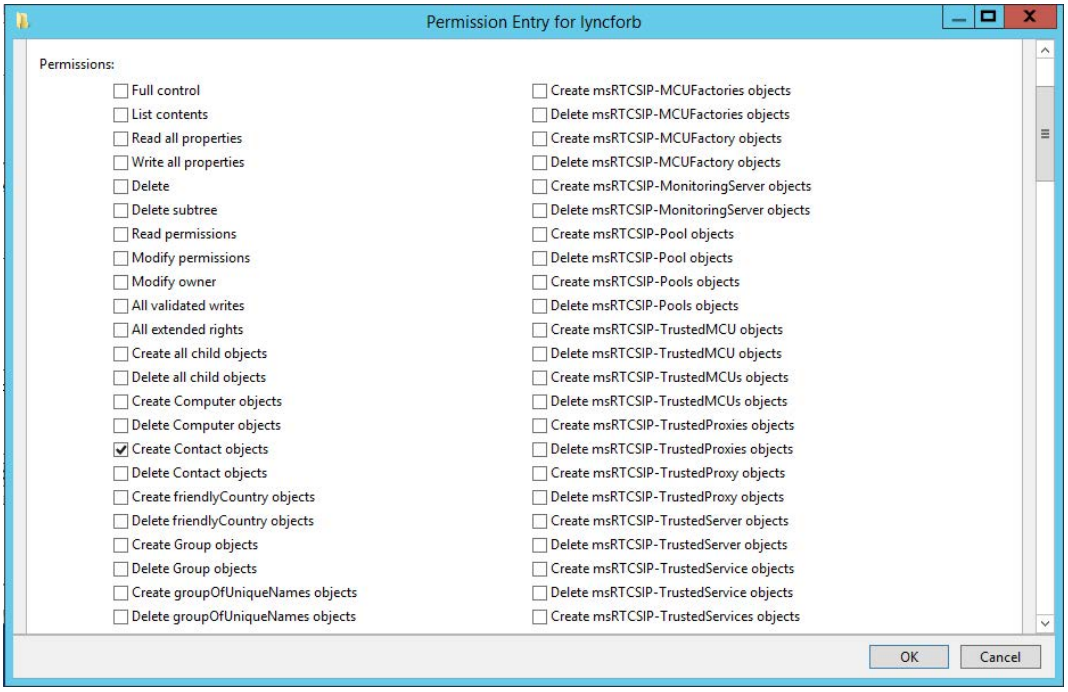
4. Next, connect to the default naming context, right-click on the domain root, and select **Properties.**

5. In the **Security** tab, click **Advanced.**

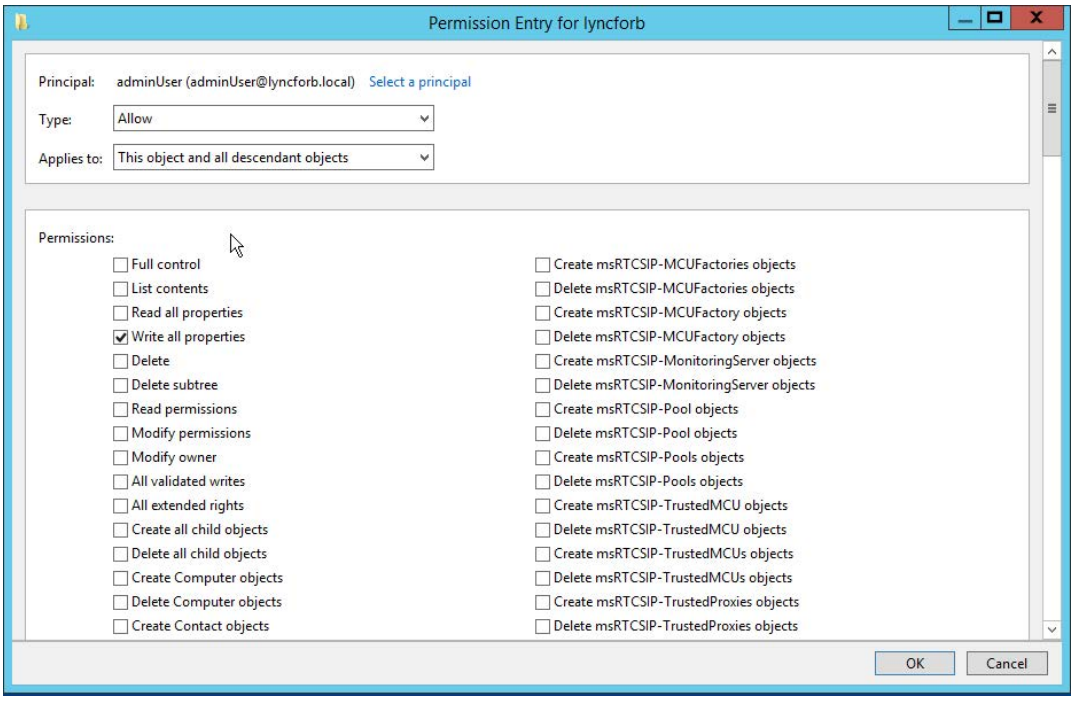
6. Add the user or group, and select the following rights:
   a. Reanimate tombstones



b. Create Contact objects



c. Write all properties



Note: Apply the **Reanimate tombstones rights** to the object being secured and its descendant objects.

7. Click **OK.**

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

Computer Management

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

Operation: Create computers

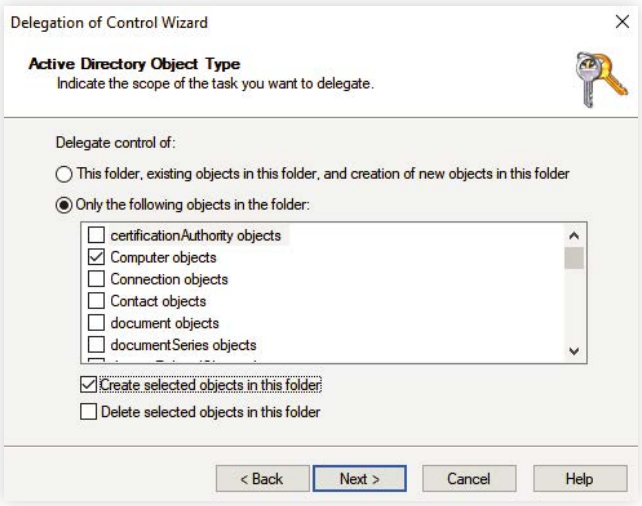
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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

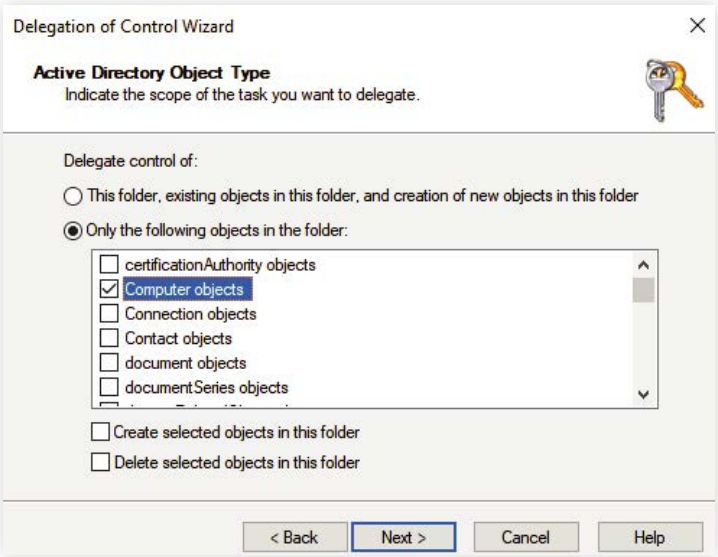
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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, or

- 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 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.**

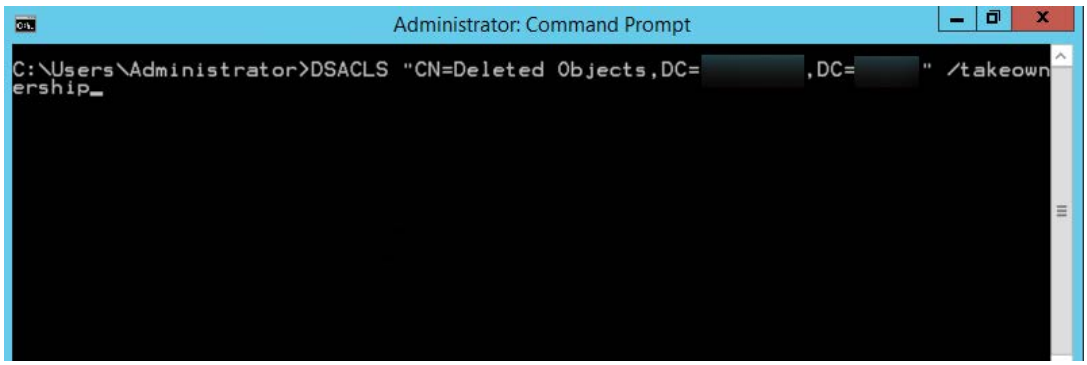
Operation: Restore computers

Permissions needed:
- The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group, or
- Permissions to restore AD computers must be manually given to the required security principles as shown in the below steps.

Steps to grant the permissions required to restore a deleted AD computer

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container.
To grant the required permissions:

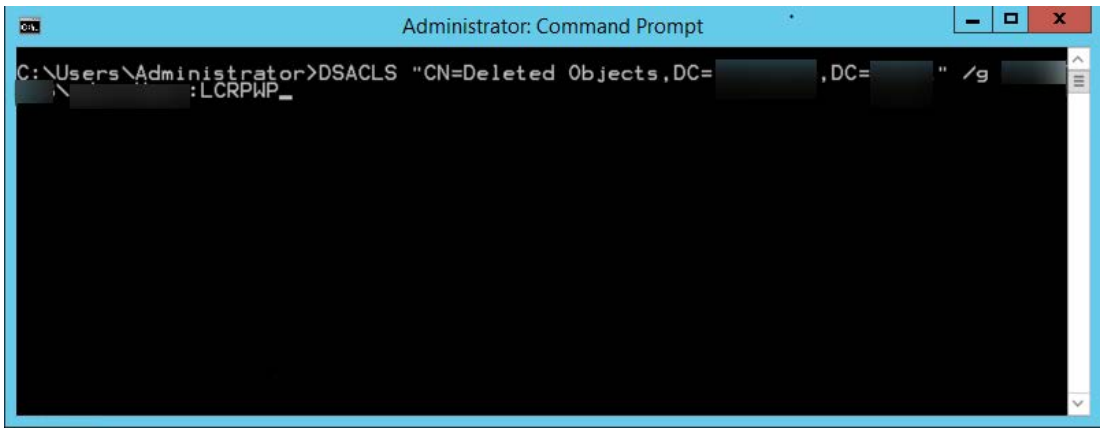
1. Log in to your domain controller and launch the command prompt as an administrator.
2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=**admanagerplus**, DC=**com**" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.

3. To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP

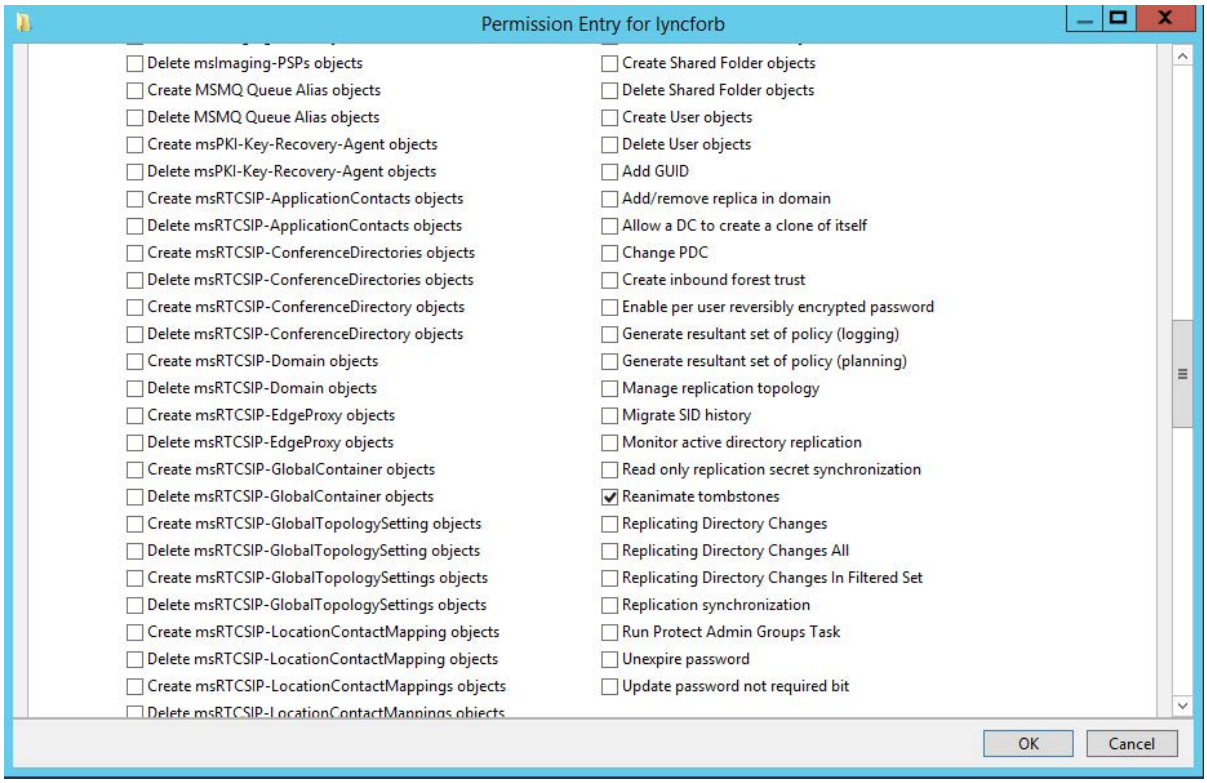


Note: Replace "LukeJohnson" with the security principal of your choice.

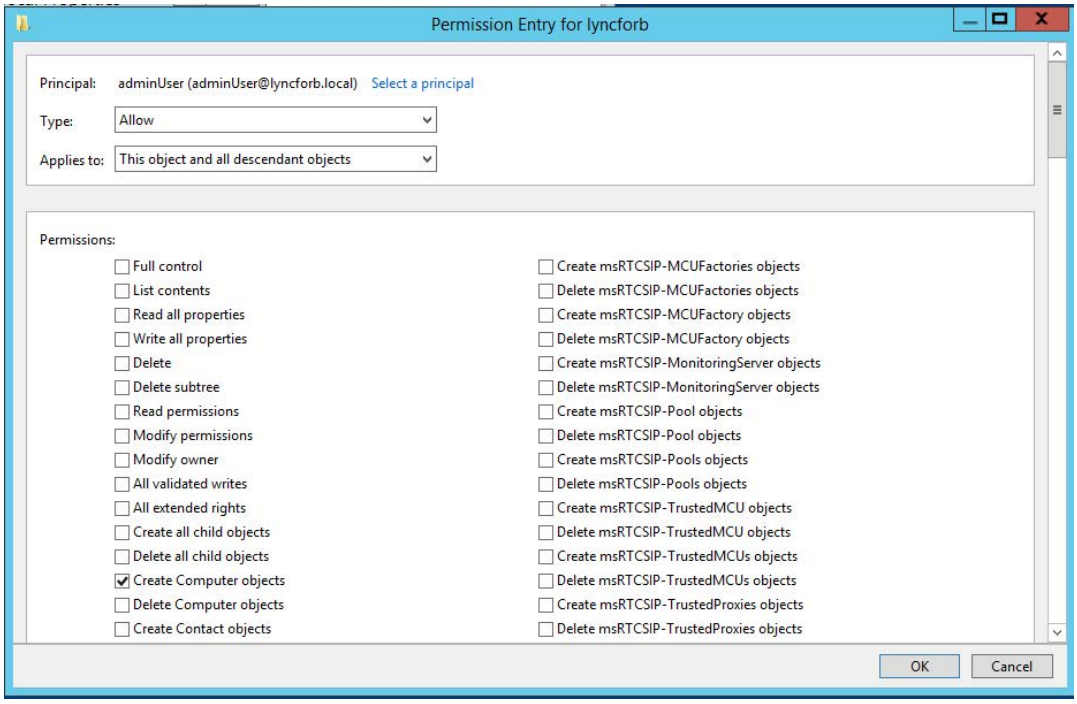
4. Next, connect to the default naming context, right-click on the domain root, and select **Properties.**

5. In the **Security** tab, click **Advanced.**

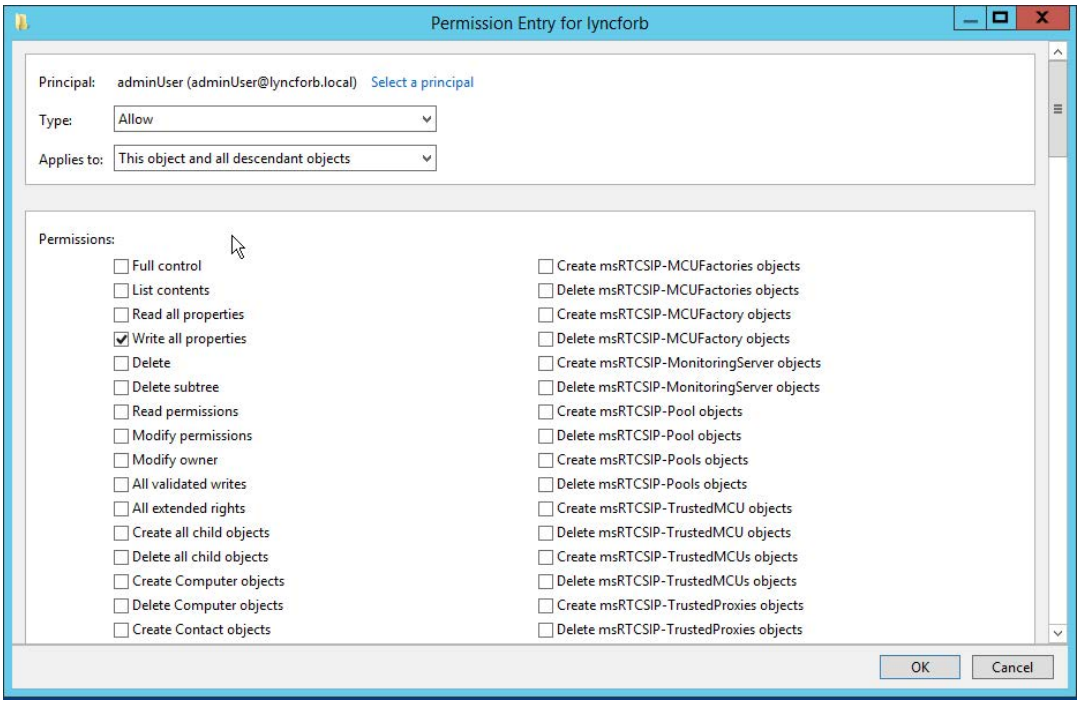
6. Add the user or group, and select the following rights:
   a. Reanimate tombstones



b. Create Computer objects



c. Write all properties



Note: Apply the **Reanimate tombstones rights** to the object being secured and its descendant objects.

7. Click **OK.**

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

Group Management

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

Operation: Create Groups

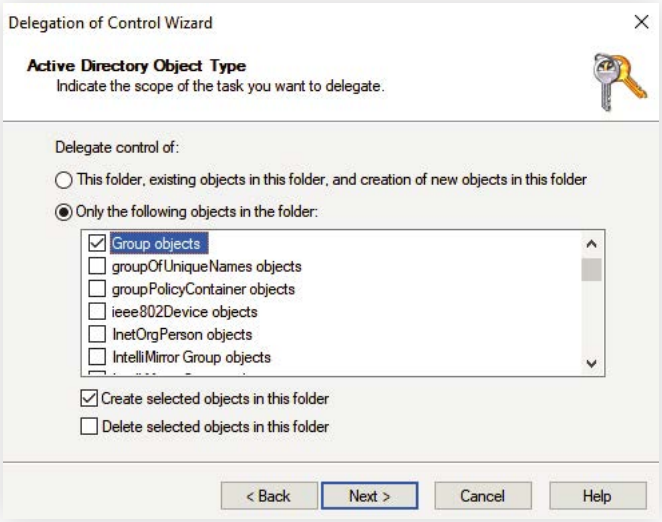
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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

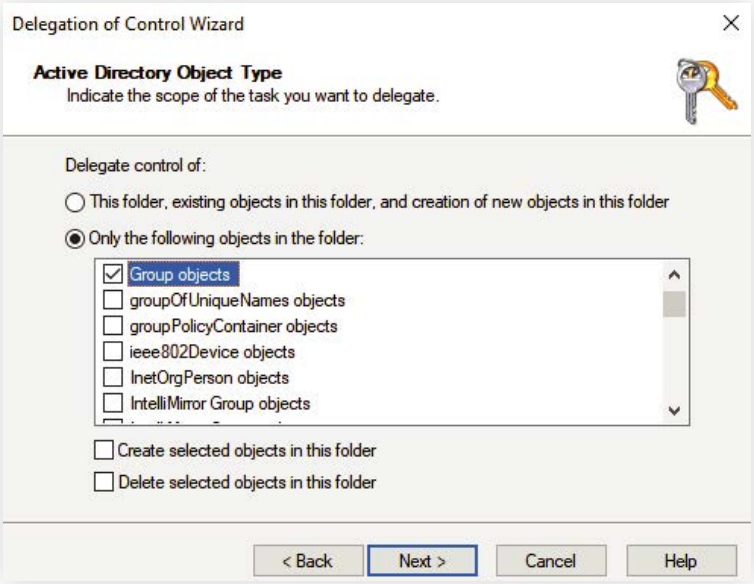
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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

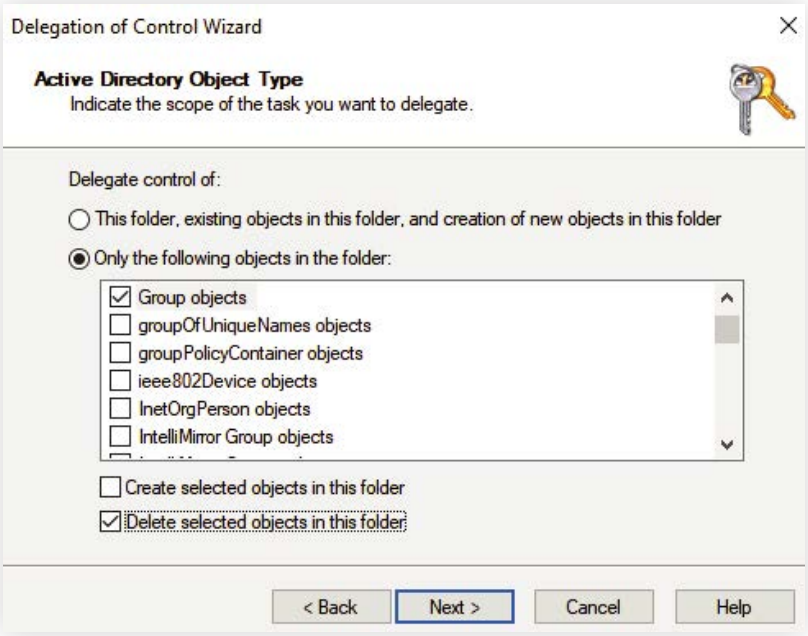
Permissions needed:

- Must be a member of the Account Operators Group, or

- 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.**

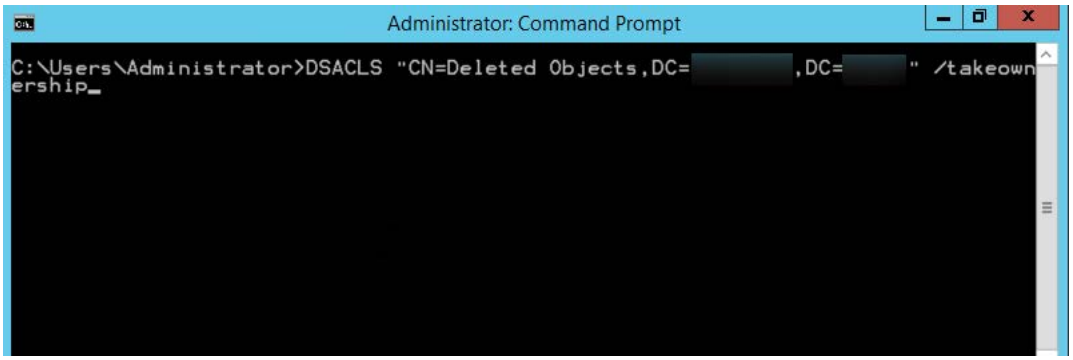
Operation: Restore groups

Permissions needed:
- The users modifying the permissions on the deleted objects container must be a member of the Domain Admins group, or
- Permissions to restore AD groups must be manually given to the required security principles as shown in the below steps.

Steps to grant the permissions required to restore a deleted AD group

Any object deleted from AD is stored in the deleted objects container and can be restored before the end of its tombstone lifetime period. To restore a deleted AD object, non-administrators must have sufficient permission to access this container.
To grant the required permissions:

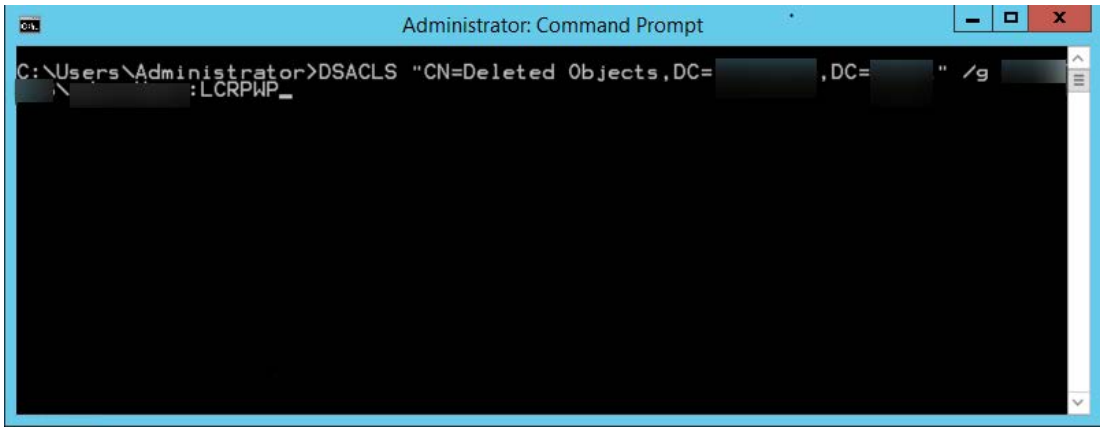
1. Log in to your domain controller and launch the command prompt as an administrator.
2. Specify a command in the following format: dsacls "CN=Deleted Objects,DC=**admanagerplus**, DC=**com**" /takeownership



Note:

- Every domain in a forest will have its own deleted objects container, so it's essential to specify the domain name of the deleted objects container for which you would like to modify permissions.
- Replace **admanagerplus** and **com** with your domain components.

3. To grant permission to a security principal to access the deleted objects container, specify a command in the following format: dsacls "CN=Deleted Objects,DC=admanagerplus,DC=com" /g ADMANAGERPLUS\LukeJohnson:LCRPWP

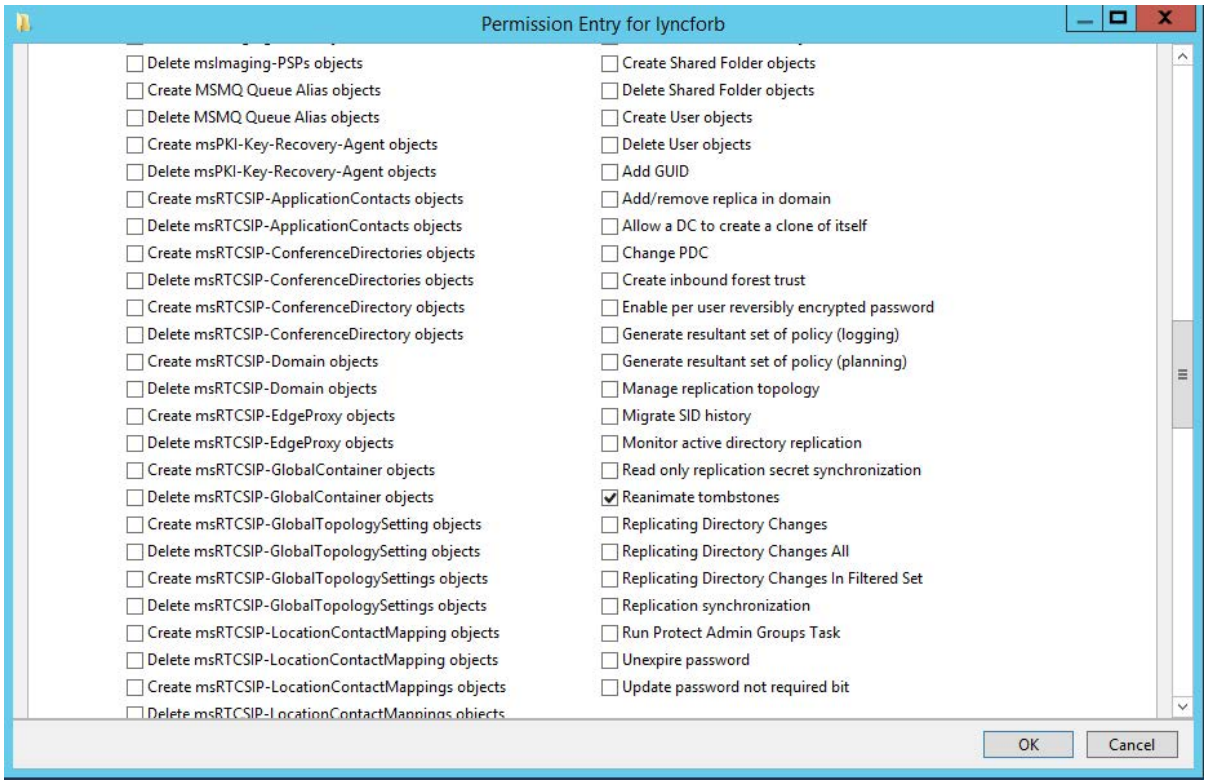


Note: Replace "LukeJohnson" with the security principal of your choice.

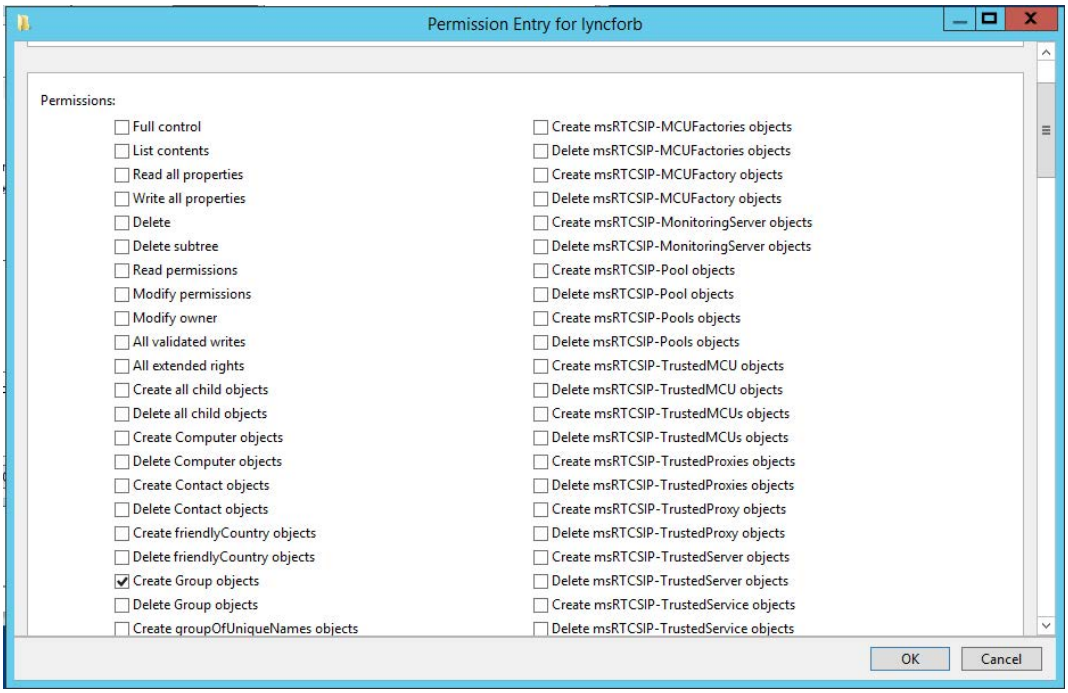
4. Next, connect to the default naming context, right-click on the domain root, and select **Properties.**

5. In the **Security** tab, click **Advanced.**

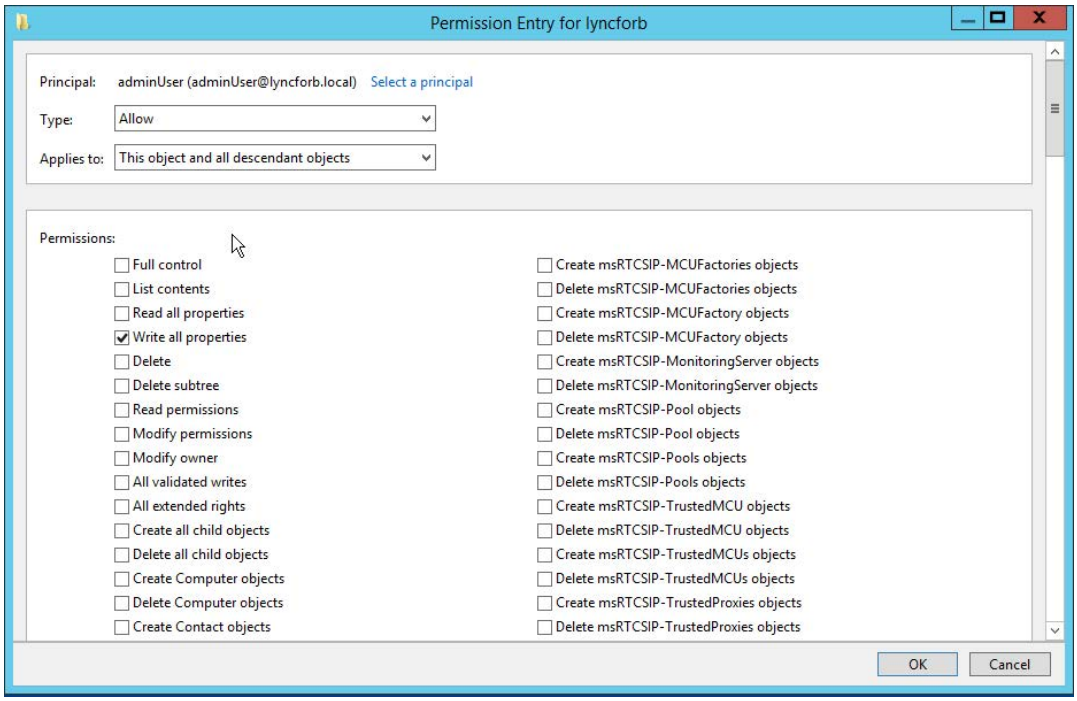
6. Add the user or group, and select the following rights:
   a. Reanimate tombstones



b. Create Group objects



c. Write all properties



Note: Apply the **Reanimate tombstones rights** to the object being secured and its descendant objects.

7. Click **OK.**

Note: Only objects deleted after the delegation of the above-mentioned permissions can be restored.

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 **Edit setting** permission selected on the GPOs. **Note:** To learn how to delegate Edit setting permissions to a group or user on a GPO, refer to this document.
Enable/disable user configuration settings	- Must have **Edit setting** permission selected on the GPOs. **Note:** To learn how to delegate permissions to a group or user on a GPO, refer to this document.
Enable/disable computer configuration settings	- Must have **Edit setting** permission selected on the GPOs. **Note:** To learn how to delegate permissions to a group or user on a GPO, refer to this document.
Enable/disable/remove GPO links	- Must select **Link GPOs** in the **Permissions** drop-down list. **Note:** To learn how to delegate permissions to link group policy objects, refer to this document.
Edit GPO settings	- Must have Edit setting permission selected on the GPOs. **Note:** To learn how to delegate permissions to a group or user on a GPO, refer to this document.
Enforce GPO links	- Must select **Link GPOs** in the **Permissions** drop-down list. **Note:** To learn how to delegate permissions to link group policy objects, refer to this document.
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.

Reporting	- Ensure the account running the product (services.msc or Command Prompt context) has the necessary privileges for establishing remote PowerShell connections to the domain's DCs. **Note:** Refer to this page for prerequisites and configurations to enable remote PowerShell connections. If you encounter any issues while establishing a connection, check this page for troubleshooting.

Note: Members of the Domain Admins and Enterprise Admins groups can perform all the above-mentioned GPO management and reporting operations using ADManager Plus. For operations requiring PowerShell remoting, the specified prerequisites must be met.

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

Note: Besides the permissions listed above, the *Replication Directory Changes* permission has to be granted for effective data synchronization between AD and ADManager Plus if the service account does not have domain administrative privileges.

Operation: Generate BitLocker reports

Permissions needed:

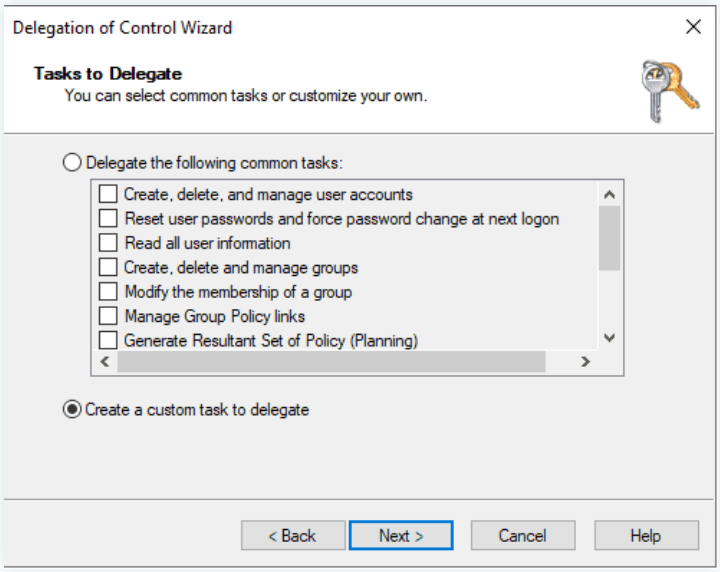
- Must have the View permission in the desired OUs and domains

Steps to grant permissions to view BitLocker recovery keys

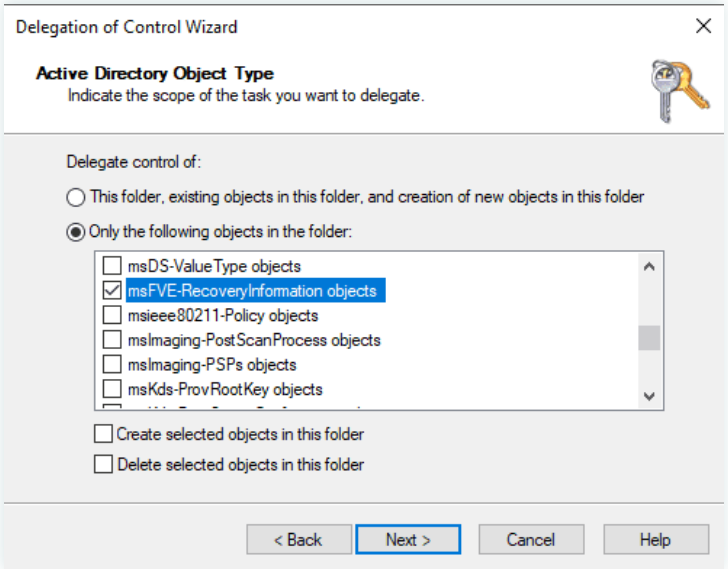
1. Log in to your domain controller and launch **Active Directory Users and Computers.**
2. Locate and right-click the **domain** or **OU** for which you wish to grant the required permissions and select **Delegate Control**. The Delegation of Control wizard will pop-up.
3. Click **Next.**

4. Select the desired **user account** or **group**, and click **Next.**

5. Select **Create a custom task to delegate** and click **Next.**

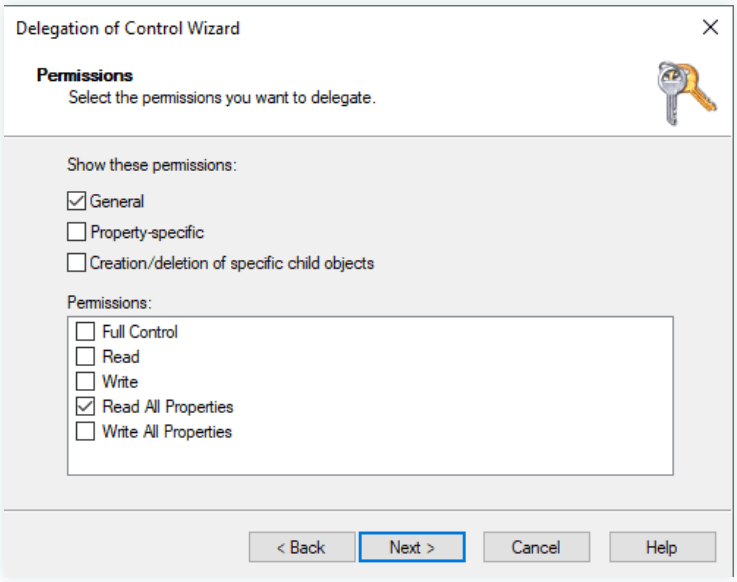


6. Select the **Only the following objects in the folder** option, check ms**TPM-InformationObject objects** and **msFVE-RecoveryInformation objects**, and then click **Next.**

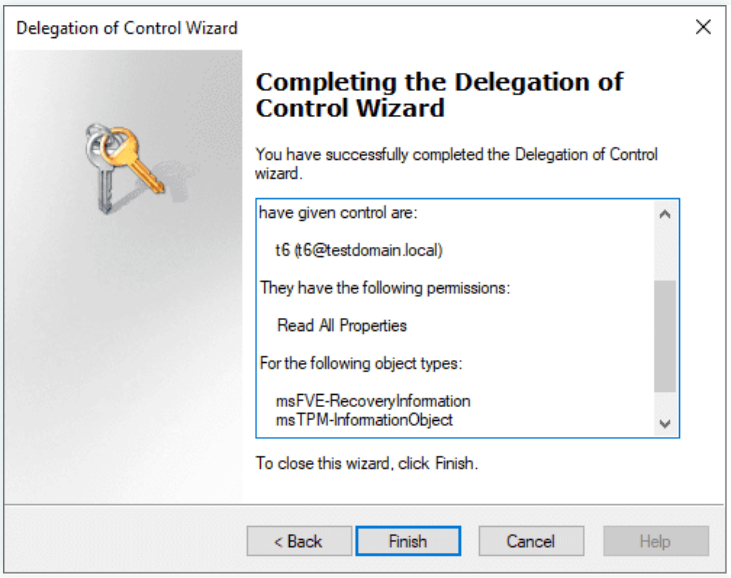


7. Under the *Show these permissions* section, select **General** and **Property-specific.**

8. Under the *Permissions* section, select the **Read, Write**, and **Read All Properties** permissions, and then click **Next.**



9. Click **Finish.**



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 and above	- Must be a part of the Organization Management group
Creating Exchange mailboxes for existing Active Directory users	Exchange 2007	- Must have Exchange Recipient Administrator role and Account Operator role.
	Exchange 2010 and above	- 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 permissions and write permissions on the mailbox store where the mailbox is located.
	Exchange 2010 and above	- Must be a part of the Organization Management group
Exchange reporting	All versions (2019, 2016, 2013, 2010, 2007, and 2003)	- Must have the Exchange View Only Administrator role.

Note: Only enterprise admins can perform cross-forest Exchange management.

Microsoft 365 Management and Reporting

The roles and permissions (minimum scope) required for a service account configured in ADManager Plus are listed below.

Module	Role name	Scope
Management	User administrator	Manage users, contacts, and groups.
	Privileged authentication administrator	Reset passwords and block or unblock administrators.
	Privileged role admin	Manage role assignments in Azure Active Directory.
	Exchange administrator	Update mailbox properties.
	Teams service admin	Manage Microsoft Teams.
Reporting	Global reader	Get reports on all Microsoft 365 services.
	Security reader	Get read-only access to security features, sign-in reports, and audit logs.

The roles and permissions (minimum scope) required for an Azure Active Directory application configured in ADManager Plus are listed below.

Module	API name	Permission	Scope
Management	Microsoft Graph	User.ReadWrite.All	User creation, modification, deletion, and restoration
		Group.ReadWrite.All	Group creation, modification, deletion, and restoration; adding or removing members and owners

Reporting	Microsoft Graph	User.Read.All	Reports on users and group members
		Group.Read.All	Group reports
		Contacts.Read	Contact reports
		Reports.Read.All	Usage reports
		Organization.Read.All	License detail reports
		AuditLog.Read.All	Audit log reports
	Azure Active Directory Graph	Domain.Read.All	Domain-based reports

To know about the prerequisites for configuring a Microsoft 365 account in ADManager Plus, click here.

Active Directory migration

Operations	Permissions needed
User migration	Enterprise admin

Google Workspace 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 https://www.googleapis.com/auth/admin.directory.domain.readonly
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 Prerequisites

High availability (HA) 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.
- Ensure that this user account has the NTFS and share permissions on both the primary and the secondary servers along with C$(admin share).

Note: The user account must be a member of the Domain Admins group when configuring High Availability. Once HA has been successfully enabled, you may replace this user account with a least-privileged user account that has the necessary permissions to run the ADManager Plus services using these steps.

Steps to configure High Availability in ADManager Plus:

To enable High Availability in ADManager Plus:

1. Logon to ADManager Plus on the primary server.
2. Navigate to the Admin tab and click on **High Availability.**
3. Select **Enable High Availability.**
4. Under the **Primary Server URL** field, enter the URL of ADManager Plus running on the primary server.
5. Under the **Standby Server** section, enter the:

a. URL or IP address of ADManager Plus running on the standby server.

b. ADManager Plus built-in administrator credentials in the standby server.

6. Under the **Virtual IP** section, enter:

   a. An IP using which you can access both the primary and the standby server. When this IP is used to access the product, the data is routed through the server that is available at that point of time.

   Note: Only an unused IP can be used as a virtual IP. To ensure that an IP is unused, try pinging the IP using the command prompt. If the 'Request timed out' error is thrown, then that IP can be used as a virtual IP.

   b. The **Virtual Host Name** which is the alias given to a virtual IP. A virtual host name can be set by using the DNS server,

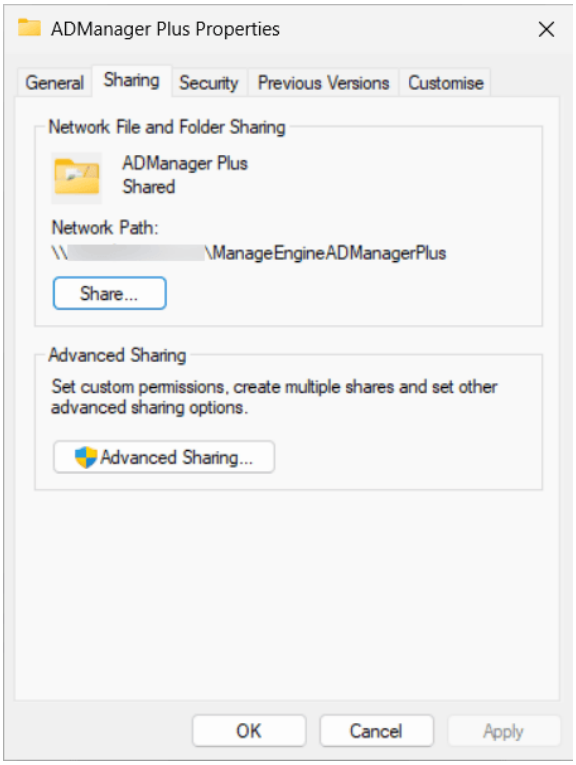
7. Click **Save.**

Note:
Later, you can remove this user account from the Domain Admins group.

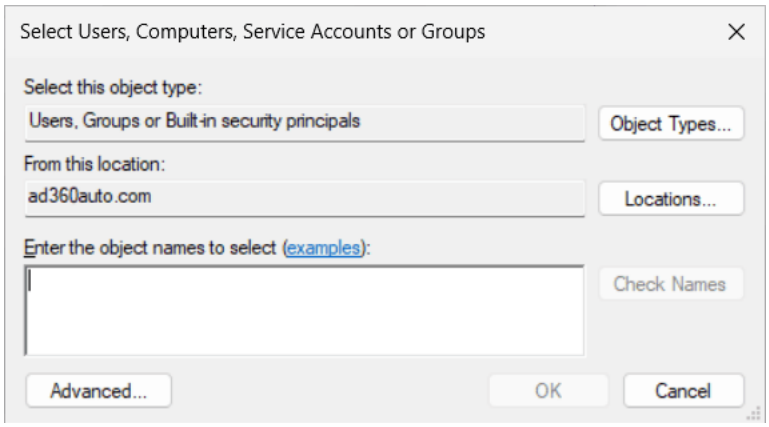
Steps to configure a least-privileged user for High Availability

After completing the HA configuration using a Domain Admins account, follow the steps below to replace that account with a user account that is not a domain administrator in services.msc.

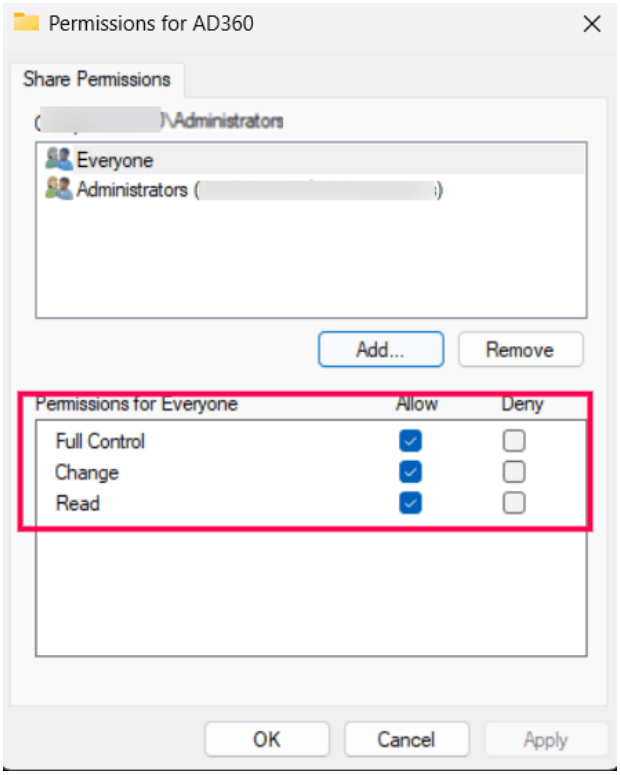
1. Create a domain user that will be used to run the ADManager Plus service on both machines.
2. Grant this user full permissions to the product installation folder on both machines:
   - Navigate to the ADManager Plus installation directory.
   - Right-click the **ADManager Plus** folder and open the **Sharing** tab.



   - Select Advanced Sharing > Permissions > Add.



- Enter the newly created domain user and click **OK.**
- Once added, grant the user **Full Control.**



- Click **Apply** and **OK** to save the changes.
- Repeat these steps on both servers.

3. Assign local administrator privileges to the newly created user on both machines to ensure Virtual IP functionality.
   - Log in to the computer with an existing administrator account.
   - Open the **Run** dialog, enter **lusrmgr.msc** to open the Local Users and Groups manager.
   - In the left pane, select **Groups.**
   - In the right pane, double-click the Administrators group.
   - In the *Administrators Properties* window, click **Add.**
   - In the *Select Users* window, click **Locations** and choose your domain.
   - Enter the domain username in the format **DOMAIN\username** or click **Advanced > Find Now to search** for and select the user.
   - Click **OK**, then **Apply,** and **OK** again to confirm.
   - The domain user is now added as a local administrator on the computer.
   - Repeat these steps in both the primary and secondary servers.
4. Open **services.msc** on both servers and update the **ManageEngine ADManager Plus** service to run using the newly created user instead of the Domain Admin account.
5. Restart the ADManager Plus services in order:
   - First restart the **primary server's** service.
   - Then restart the **secondary server's** service.
6. No changes to domain settings are required. Updating the service logon user in **services.msc** is sufficient.

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

ManageEngine
ADManager Plus

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus

M365 Manager Plus | RecoveryManager Plus

About ADManager Plus

ADManager Plus is an identity governance and administration (IGA) solution that simplifies identity management, ensures security, and improves compliance. With ADManager Plus, manage the user life cycle from provisioning to deprovisioning, run access certification campaigns, orchestrate identity management across enterprise applications, and protect data on your enterprise platforms with regular backups. Use over 200 reports to gain valuable insights into identities and their access rights. Improve the efficiency of your IGA operations with workflows, automations, and role-based access control policies. ADManager Plus' Android and iOS applications help with on-the-go AD and Entra ID management.

For more information about ADManager Plus, visit manageengine.com/products/ad-manager/.

$ Get Quote Download