ManageEngine
ADSelfService Plus

Required privileges and permissions

Table of contents

Document summary

This guide will walk you through the process of delegating an Active Directory user account with the required permissions for using the self-service features in ADSelfService Plus. ADSelfService Plus does not require "Domain Admin" membership in order to allow users to reset their passwords, unlock their accounts, update their profiles, or access any of its other features. Based on the principle of least privilege, you can delegate only the permissions required for the self-service operations to a user account manually.

Note: If you don't provide any authentication details while adding domains, ADSelfService Plus will get its privileges one of two ways:

- If ADSelfService Plus is installed to run as a console application and no credentials are provided, then by default it uses the permissions of the user who installed the product.
- If ADSelfService Plus is installed to run as a service and no credentials are provided, then by default it uses the permissions of the account used to run the service.

ADSelfService Plus overview

ManageEngine ADSelfService Plus, an integrated Active Directory self-service password management and single sign-on solution, helps reduce password reset tickets and spares end users the frustration caused by computer downtime. It offers,

- Self-service password reset and account unlock
- Password and account expiration notifier
- Password policy enforcer
- Enterprise single sign-on and password synchronizer
- Endpoint multi-factor authentication for machine logins
- Directory self-update and employee search

These features, designed to strike a balance between ensuring network security and ease-of-access, warrants improved ROI, and a productive IT workforce.

Required permissions

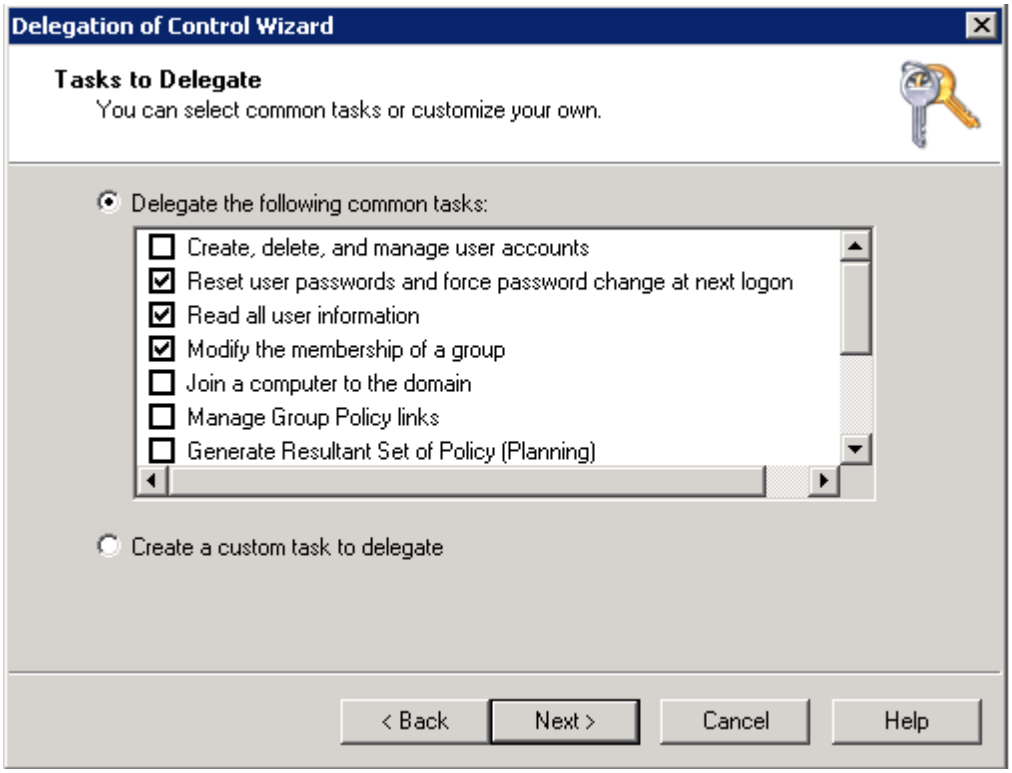
Feature	Permission(s) required
Self-service password reset	**Reset password** for user objects **Read pwdLastSet** for user objects **Write pwdLastSet** for user objects
Self-service account unlock	**Read lockoutTime** for user objects **Write lockoutTime** for user objects
Self-update user attributes	**Read** for user objects **Write** for user objects
Display fine-grained password policy	**Read** for msDS-PasswordSettings objects **Read** for msDS-PasswordSettingsContainer objects
Self-service mail group subscription	**Read Members** for group objects **Write Members** for group objects
NTLM single sign-on	**Create** for computer objects **Read** for computer objects
Force enrollment using logon script	**Read scriptPath** for user objects **Write scriptPath** for user objects
View deleted users report	Membership in Domain Admins group
GINA installation	Membership in Domain Admins group
Configuration of high availability	Membership in Domain Admins group

Configuring permissions

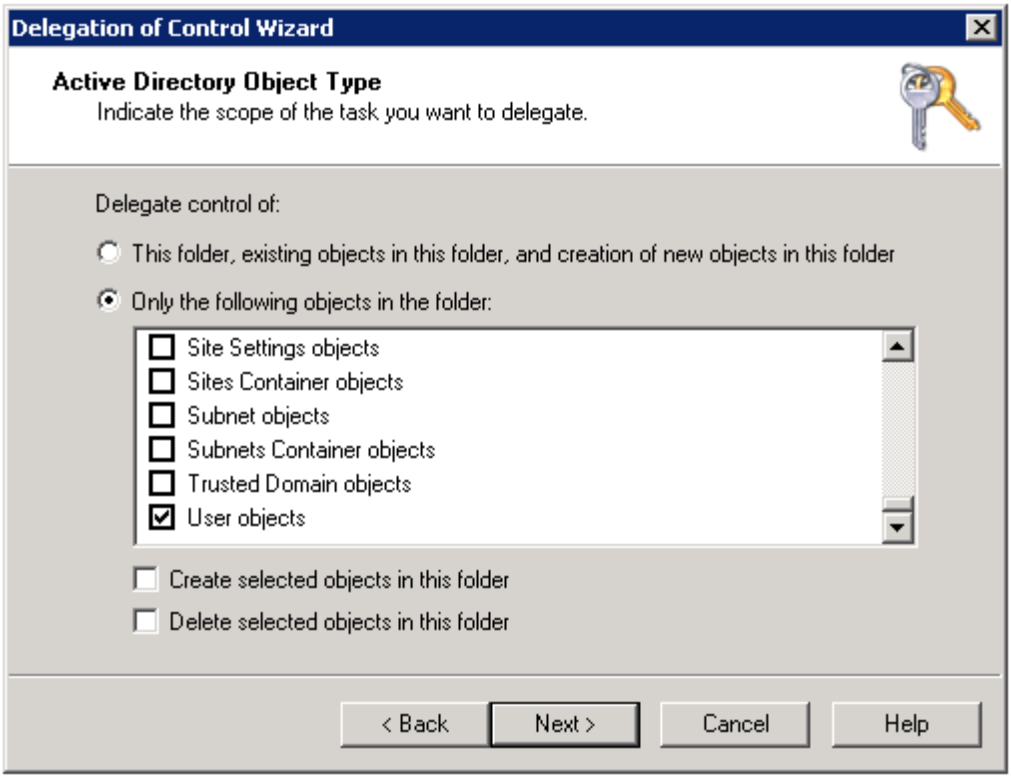
To access all ADSelfService Plus features

For users to access all features of ADSelfService Plus, you'll need to grant the ADSelfService Plus service account the following permissions:

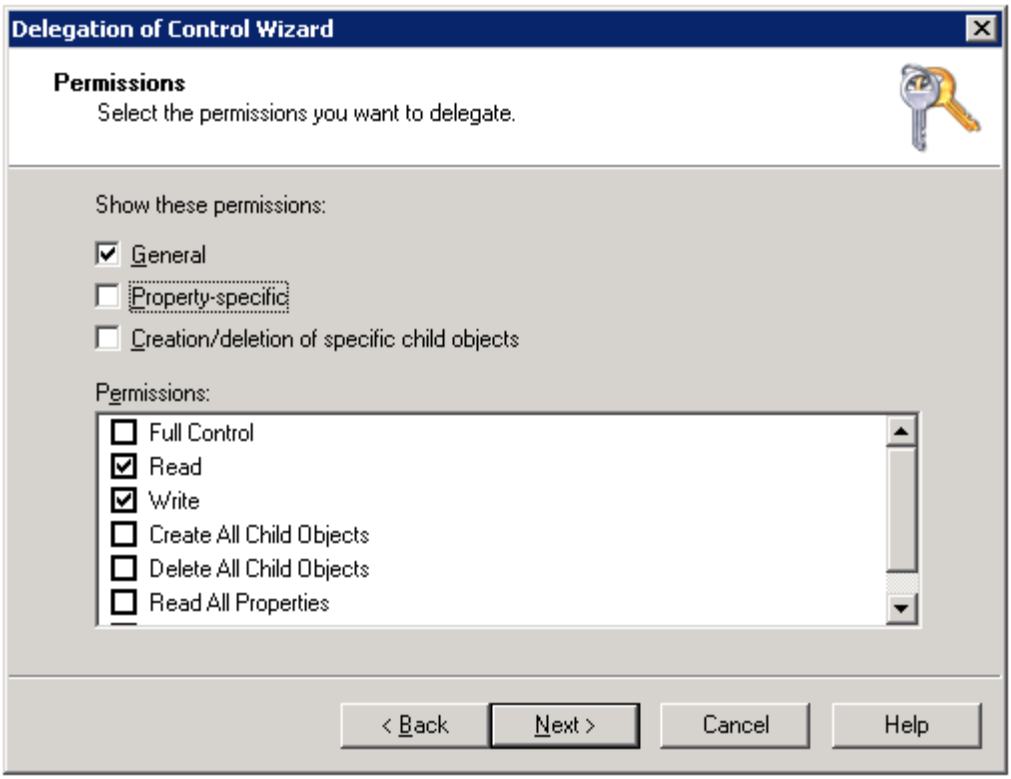
1. Right-click the **domain** in ADUC and select **Delegate Control** from the context menu.
2. Click **Next** in the welcome dialog box.
3. Click **Add** to select the user account or service account, then click **OK** followed by **Next**.
4. Select **Delegate the following common tasks** and check the **Reset user passwords and force password change at next logon**, **Read all user information**, and **Modify the membership of a group** boxes, then click **Next**.



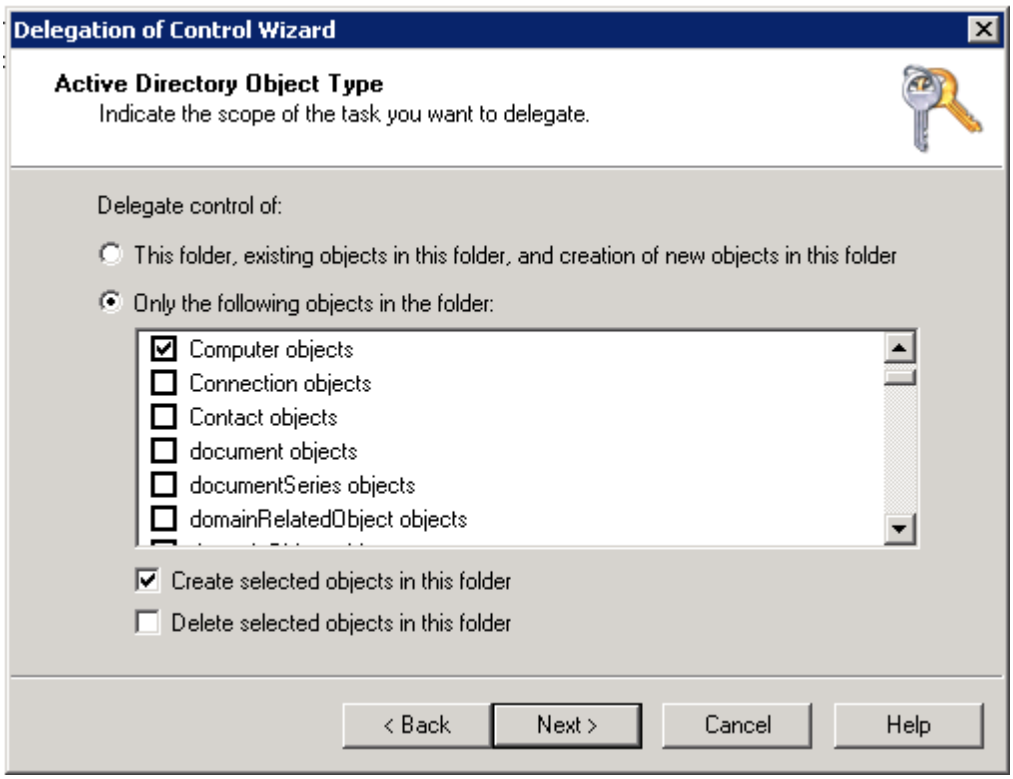
5. Click **Finish** and repeat steps **1-3.**
6. Select **Create a custom task to delegate** and click **Next.**
7. Select **Only the following objects in the folder.** In the given list, select **User Objects.**



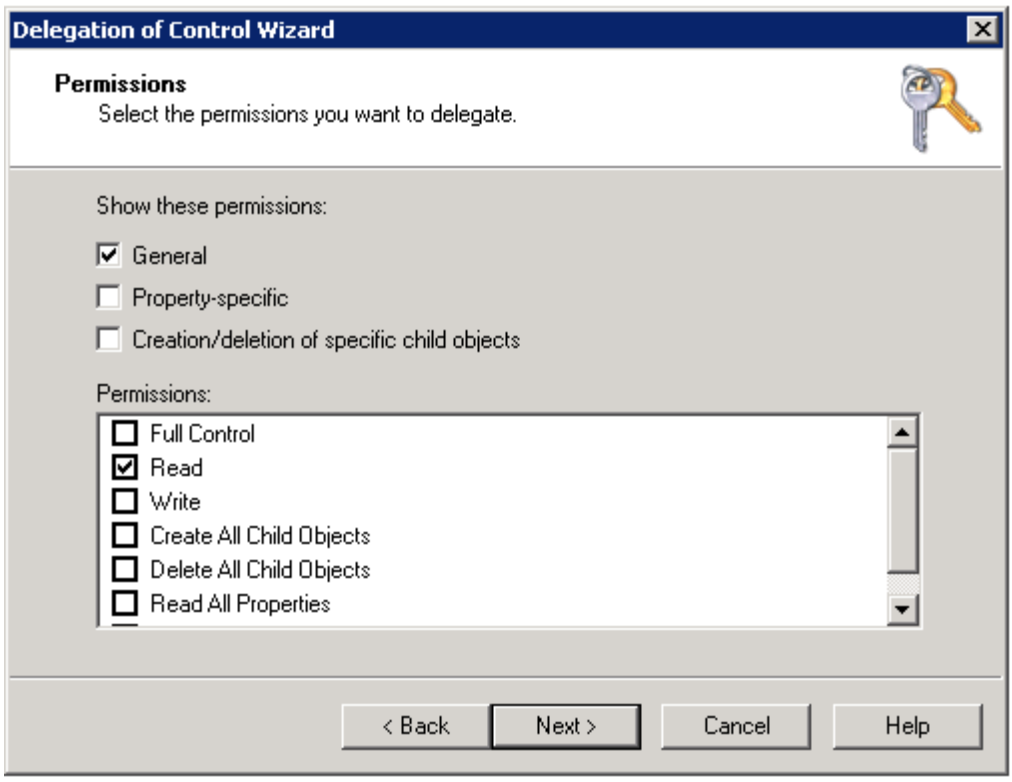
8. Select the **General** box. Under Permissions, check the boxes for **Read** and **Write** before clicking **Next.**



9. Click **Finish** and repeat steps 1-3.
10. Select **Create a custom task to delegate** and click **Next**.
11. Select **Only the following objects in the folder**. In the given list, select **Computer Objects** and **Create selected objects in this folder**.



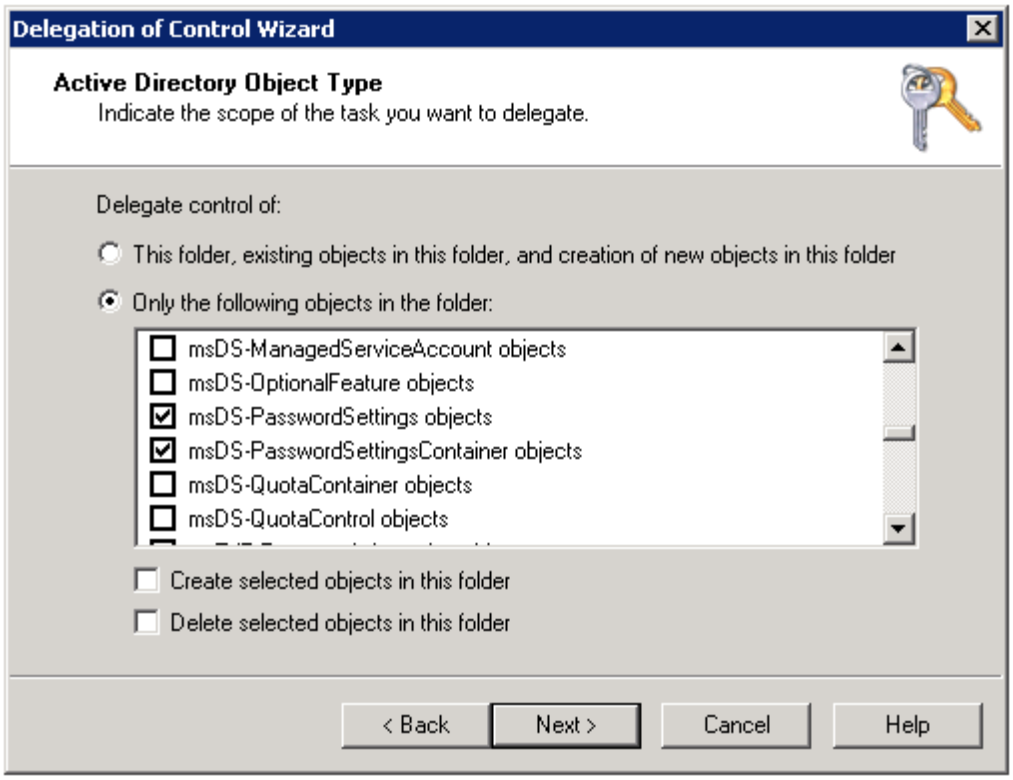
12. Select the **General** box. Under Permissions, check **Read** before clicking **Next**.



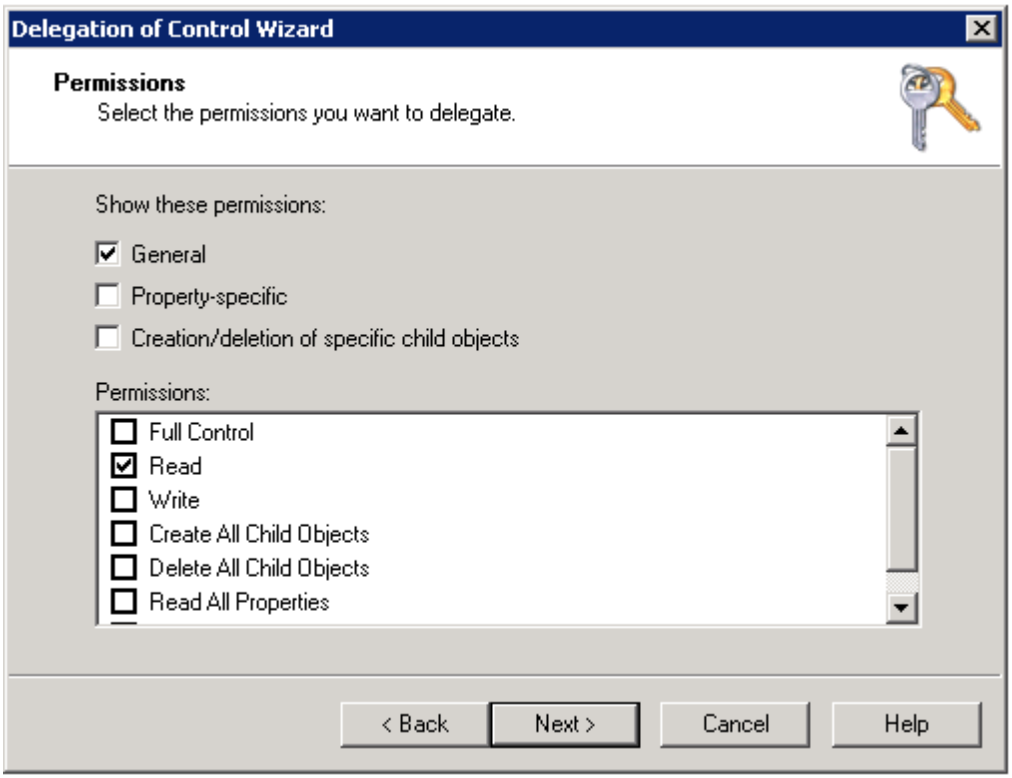
13. Click **Finish** and repeat steps 1-3.

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

15. Select **Only the following objects in the folder**. In the given list, select **msDS-PasswordSettings objects** and **msDS-PasswordSettingsContainer objects**. Click **Next**.



16. Select the **General** box. Under Permissions, check **Read** before clicking **Next**.



17. Click **Finish**.

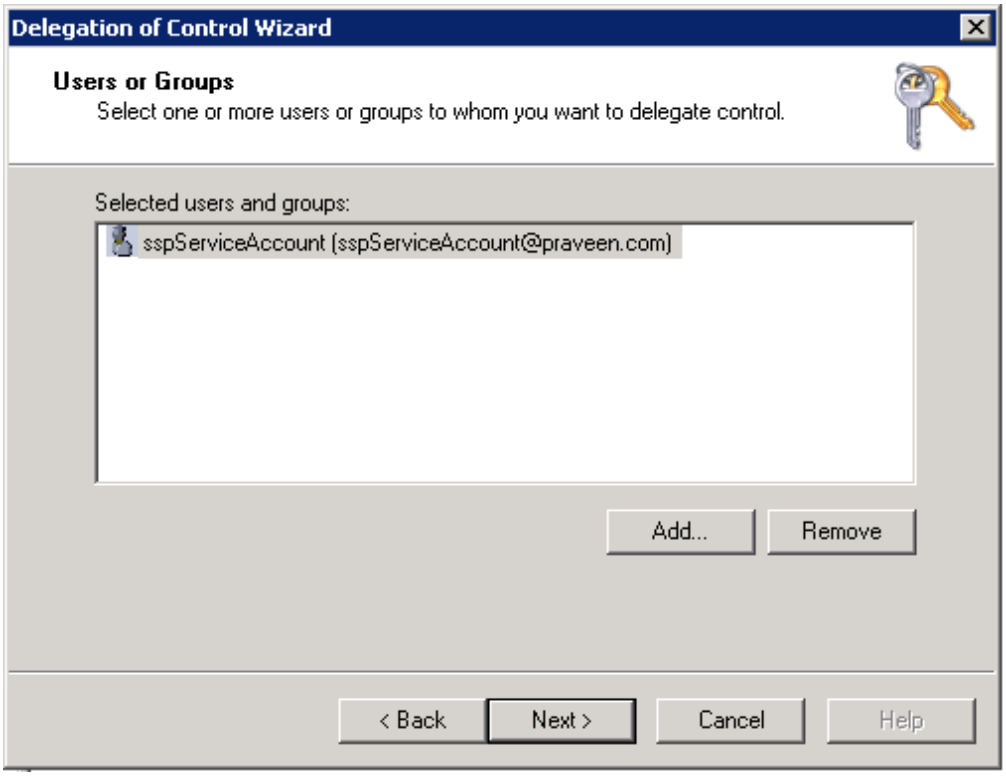
Self-service password reset

In order for this feature to work, you need to delegate the *permission to reset users' passwords* in the ADUC console. To do this, follow the steps below:

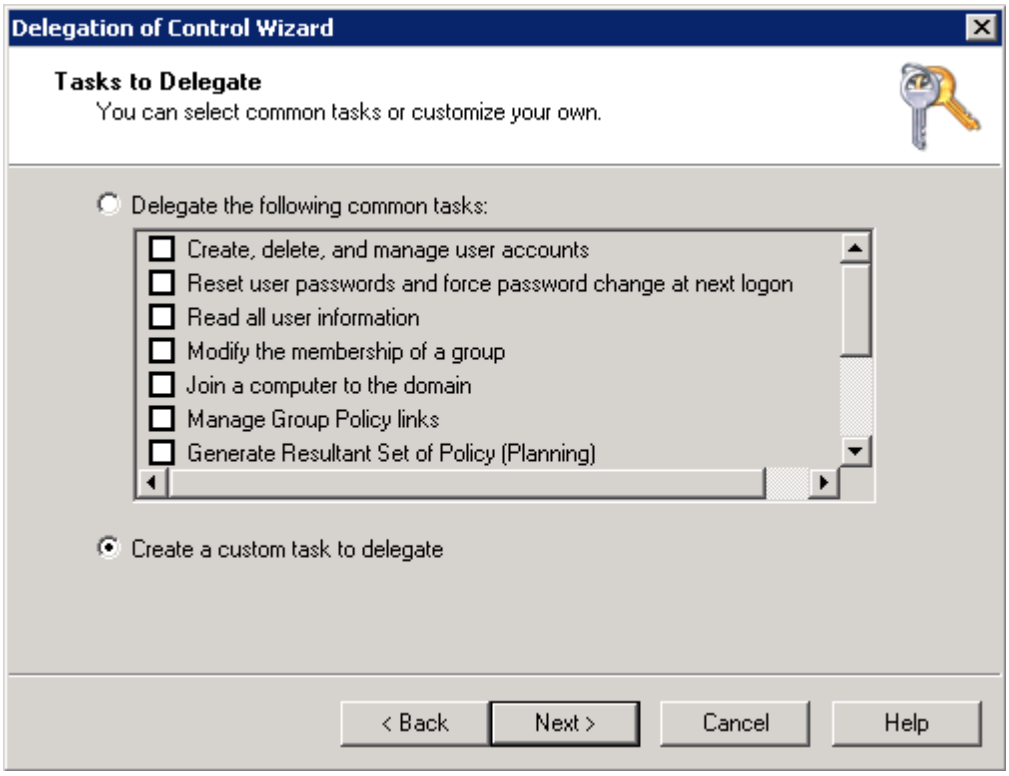
1. Right-click the **OU** or **domain** in ADUC and select **Delegate Control** from
2. Click **Next** in the welcome dialog box.

3. Click **Add** to select the ADSelfService Plus user account or service account, then click **OK**.

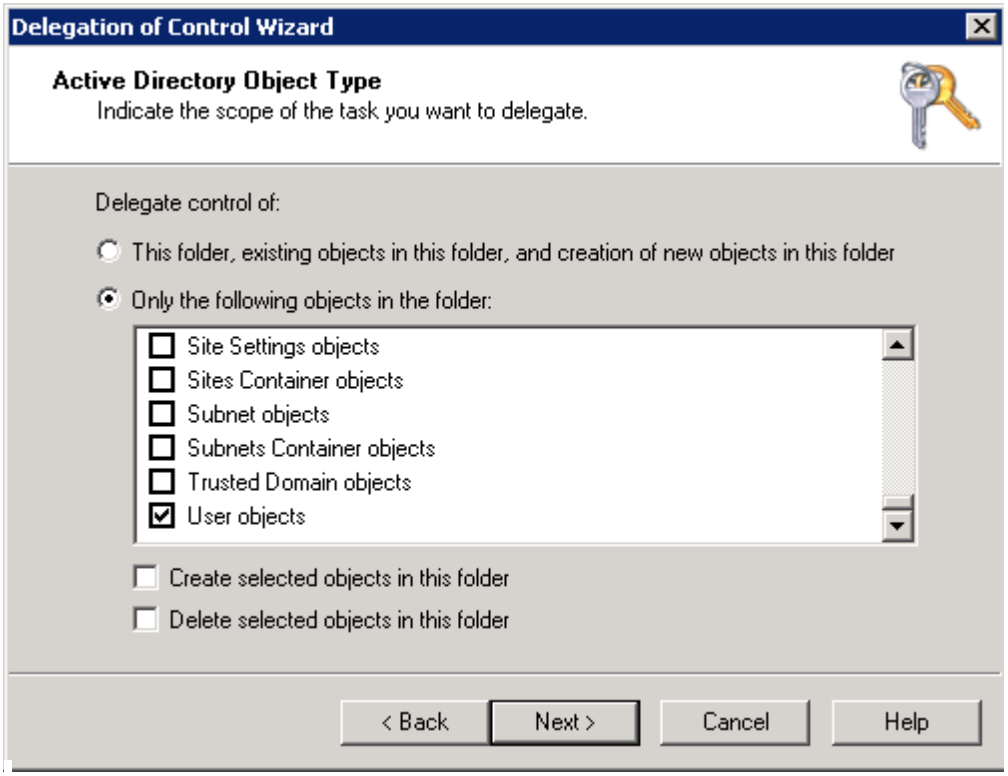
4. Click **Next**.



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

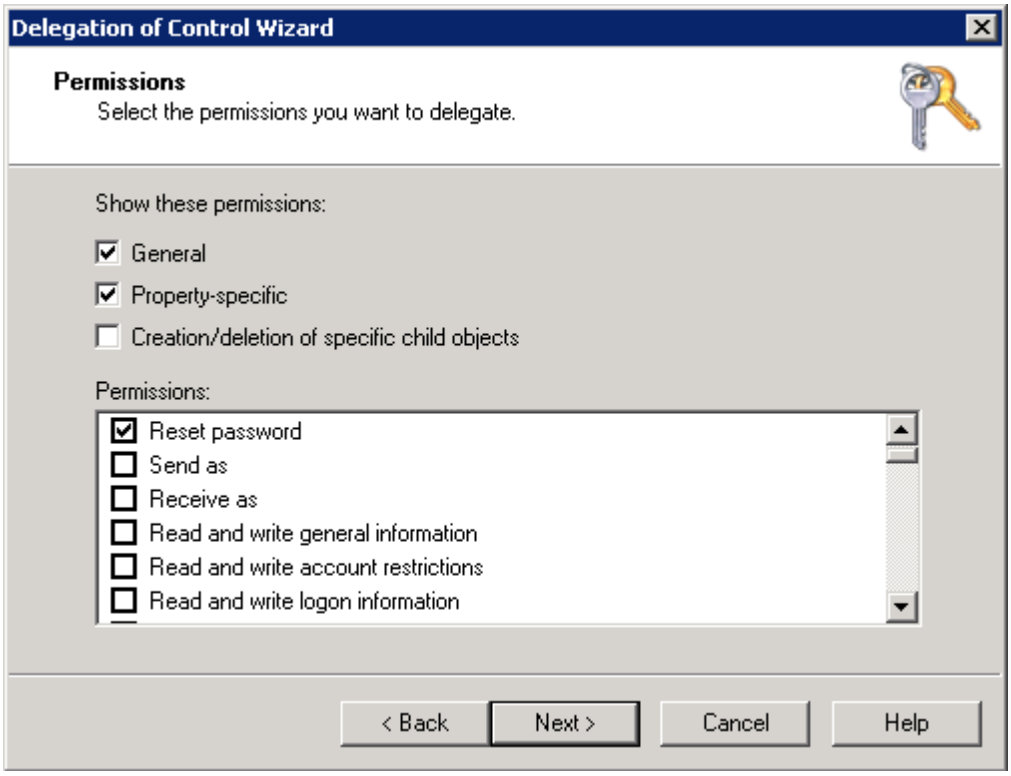


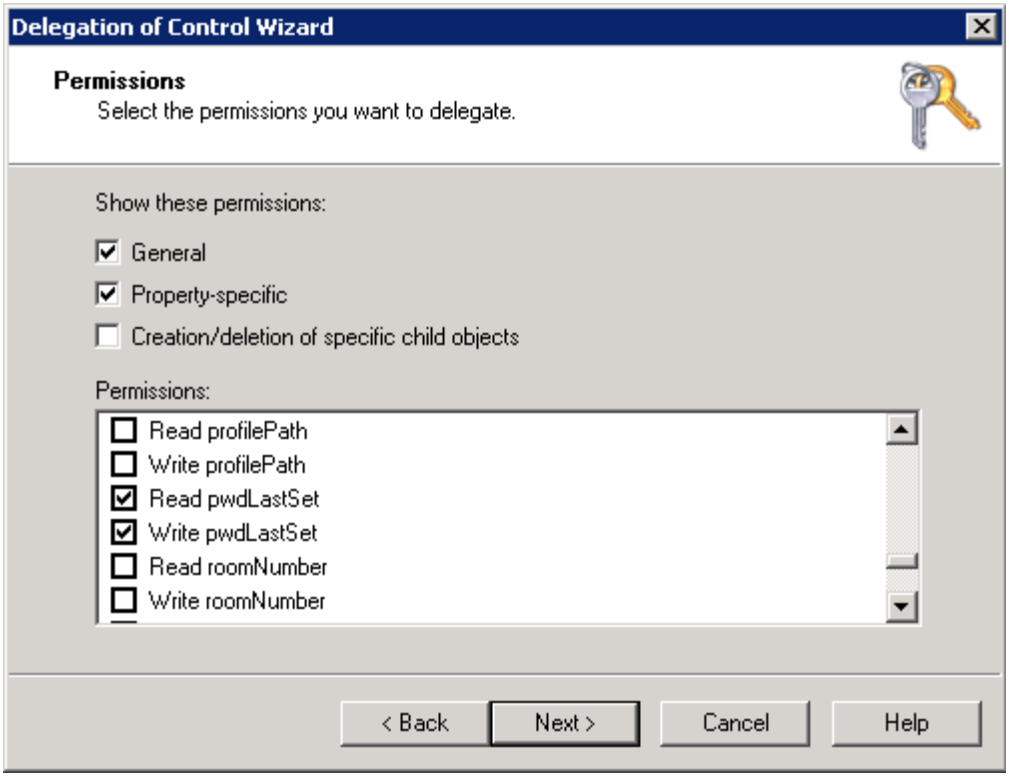
6. Select **Only the following objects in the folder**. In the given list, select **User objects and click Next**



7. Check the **General** and **Property-specific** boxes.

8. Under Permissions, check the boxes for **Reset password, Read pwdLastset,** and **Write pwdLastset** before clicking **Next**.





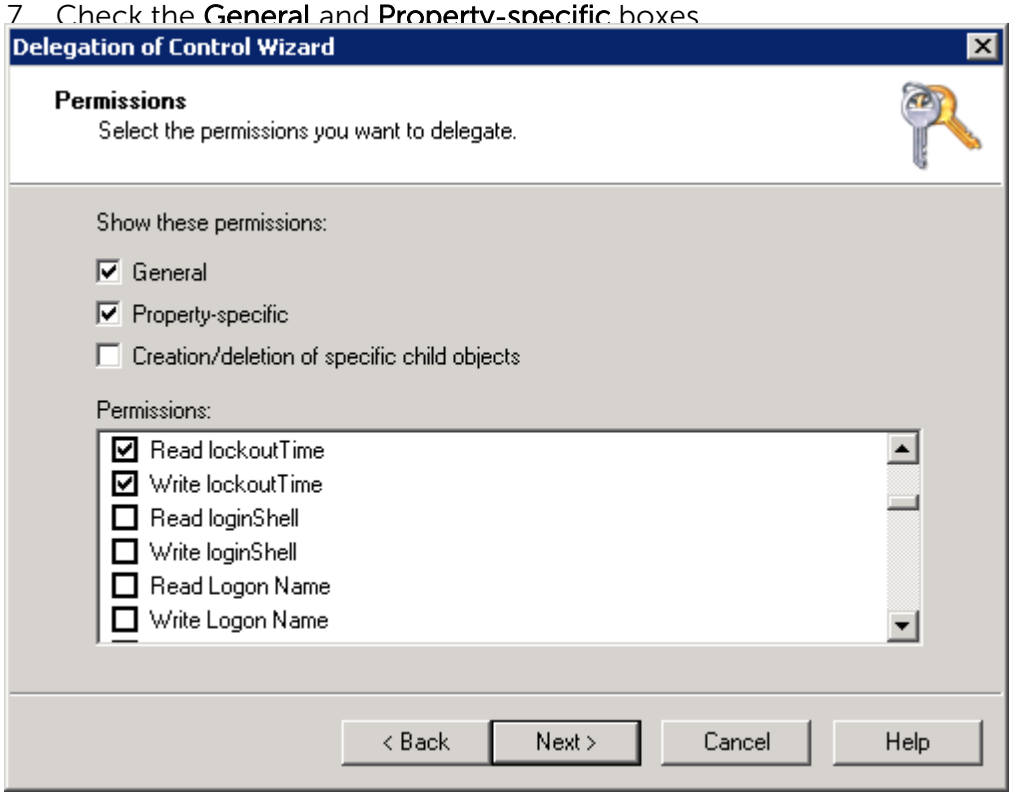
9. Click **Finish**.

Note: This permission only enables password reset.

Self-service account unlock

For this feature to work, you need to delegate the *permission to unlock users' accounts* in the ADUC console. To do this:

1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.
2. Click **Next** in the welcome dialog box.
3. Click **Add** to select the ADSelfService Plus user account or service account, then click **OK**.
4. Click **Next**.
5. Select **Create a custom task to delegate** and click **Next**.
6. Select **Only the following objects in the folder**. In the given list, check **User objects** and click **Next**.
7. Check the **General** and **Property-specific** boxes.



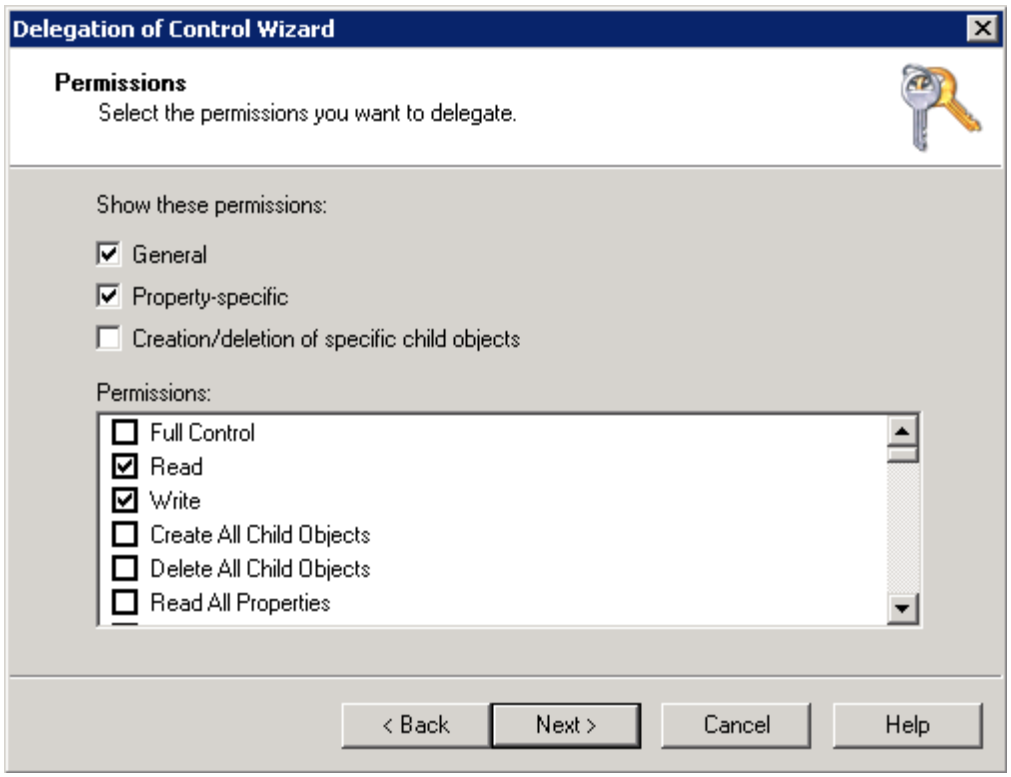
8. Under Permissions, check the **Read lockoutTime** and **Write lockoutTime** boxes and click **Next**.
9. Click **Finish**.

Note: This permission only enables account unlock.

Directory self-update

To utilize this feature, you need to delegate the *permission to modify user attributes* in the ADUC console. Follow the steps below to do so:

1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.
2. Click **Next** in the welcome dialog box.
3. Click **Add** to select the user account or service account, then click **OK**.
4. Click **Next**.
5. Select **Create a custom task to delegate** and click **Next**.
6. Select **Only the following objects in the folder**. In the given list, select **User objects** and click **Next**.
7. Check the **General** and **Property-specific** boxes.



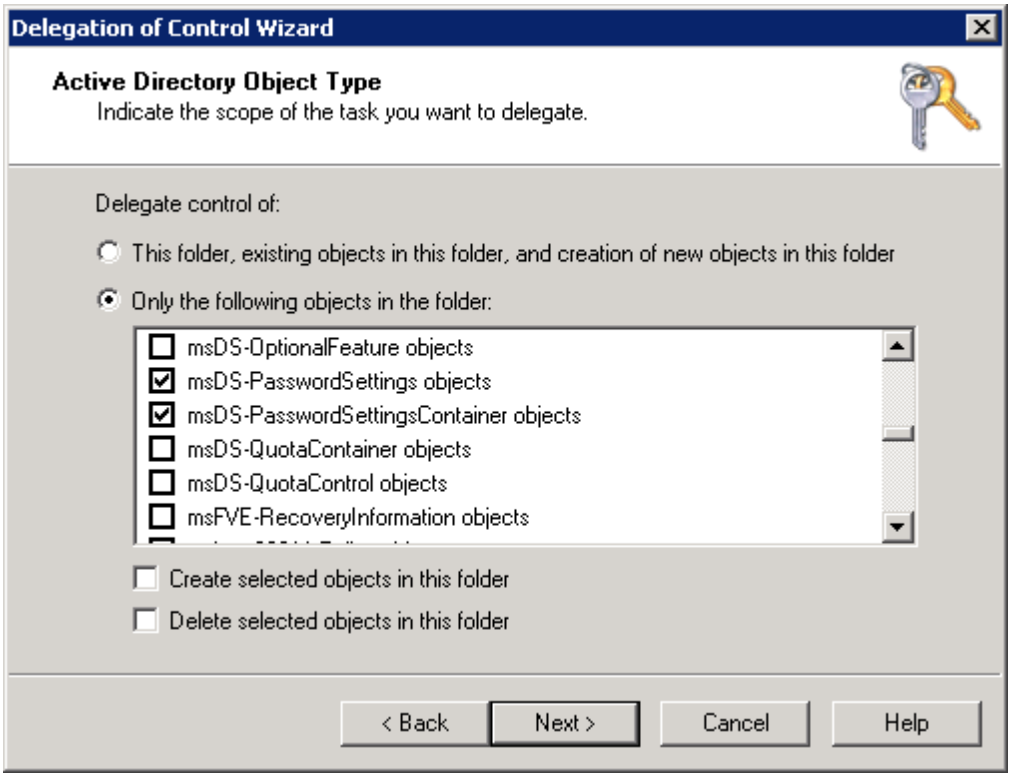
8. Under Permissions, check the **Read** and **Write** boxes (or select the **Read** and **Write boxes of specific attributes that need to be available for end user self-update), and click Next.**
9. Click **Finish**.

Note: This permission only enables self-update.

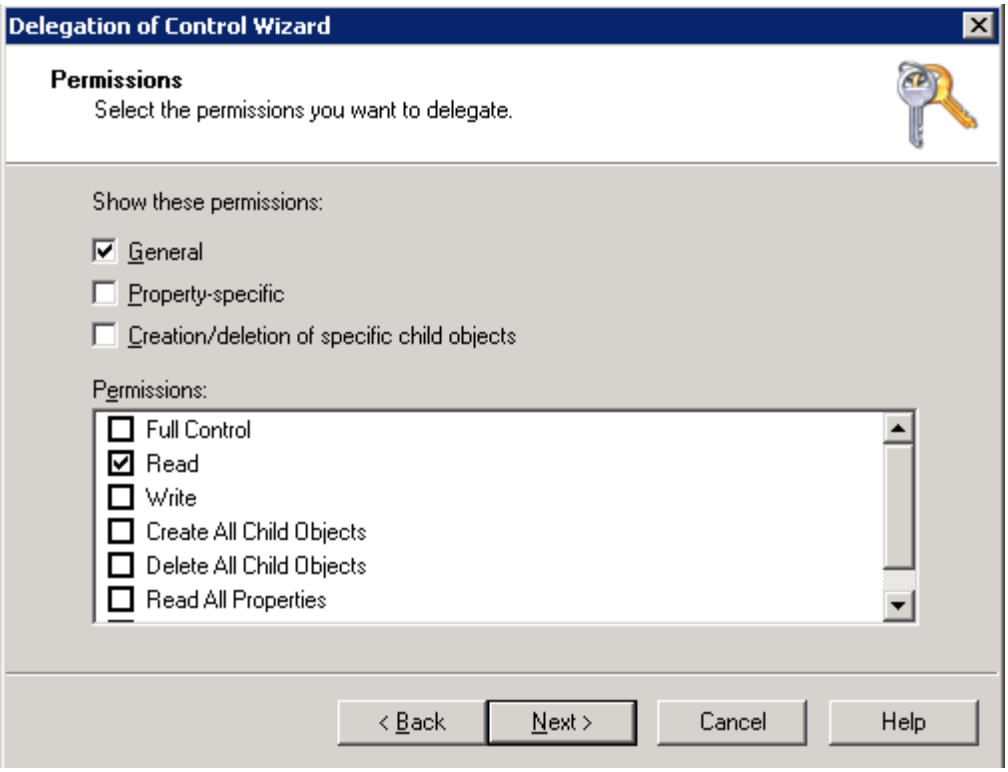
Display fine-grained password policy

If you want to display the exact password policy requirements in the reset/change password screen for users with fine-grained password policy enabled, then you need to delegate the *permission to read the users' Password Settings Objects (PSOs)* in ADUC. Follow the steps below to do this:

1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.Click **Next** in the welcome dialog box.
2. Click **Add** to select the user account or service account, then click **OK**.
3. Click **Next**.
4. Select **Create a custom task to delegate** and click **Next**.
5. Select **Only the following objects in the folder**. In the given list, select **msDS-PasswordSettings objects** and **msDS-PasswordSettingsContainer objects** before clicking **Next**.



7. Check the **General** box.



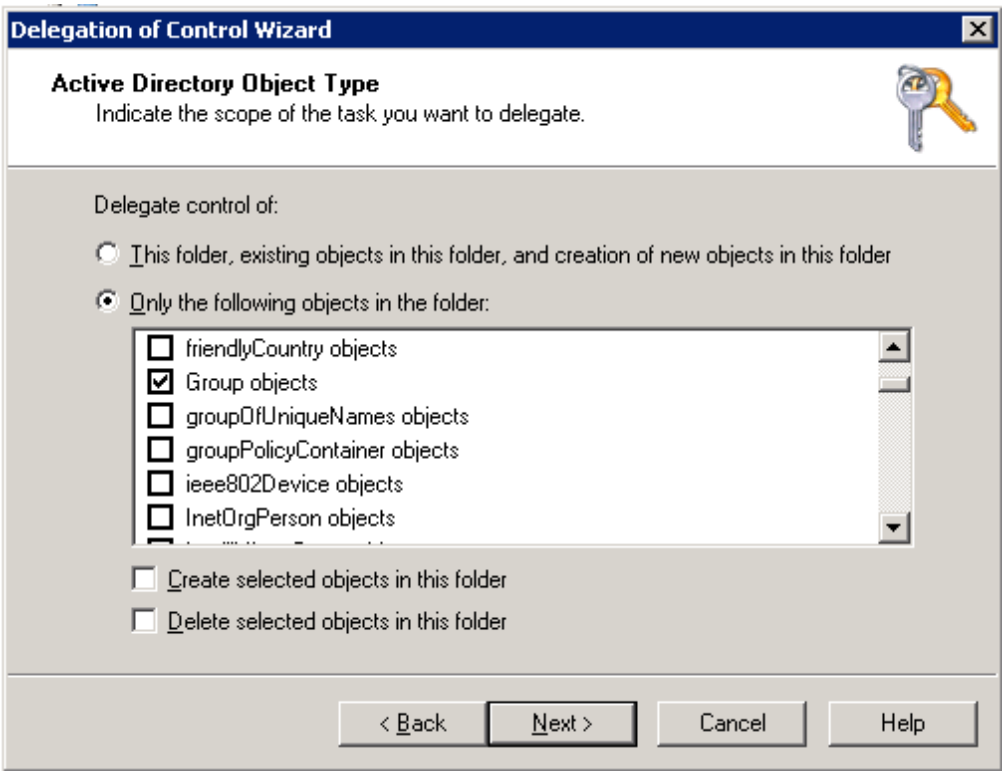
8. Under Permissions, select **Read** and click **Next**.
9. Click **Finish**.

Note: This permission only fetches the password policy.

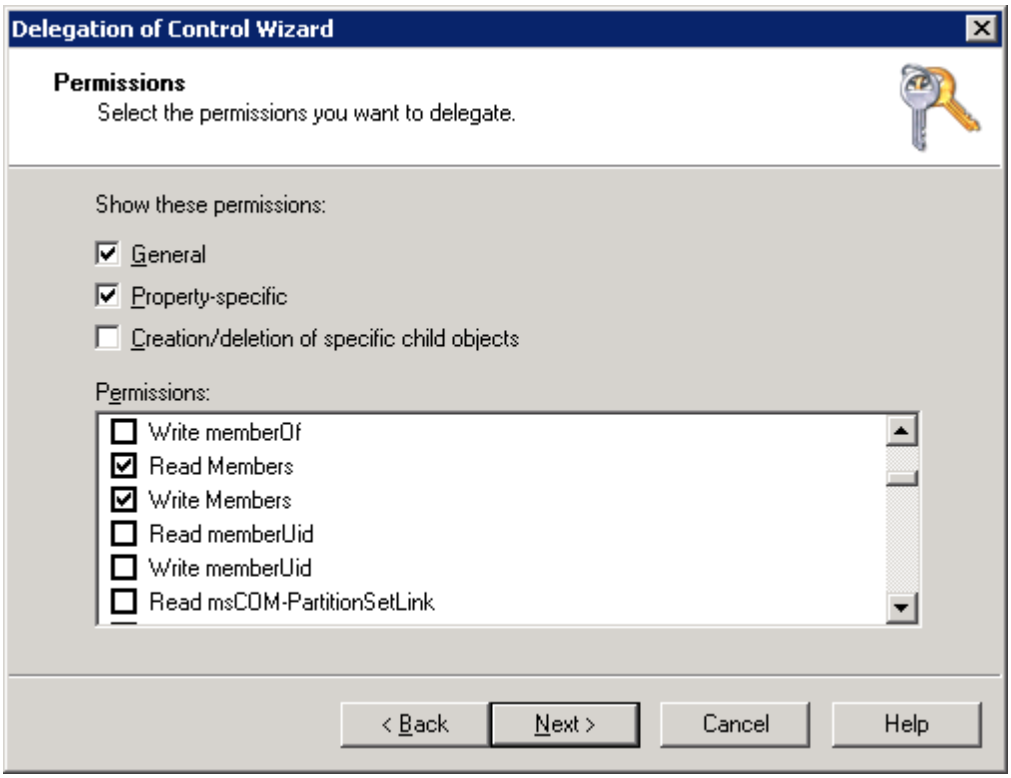
Self-service mail group subscription

To use this feature, you need to delegate the *permission to modify members of a group* in the ADUC console. Follow the steps below to do so:

1. Right-click the OU or domain where the group containing members that require modification belongs in ADUC, and select Delegate Control from the context menu.
2. Click **Next** in the welcome dialog box.
3. Click **Add** to select the user account or service account, then click **OK**. Click **Next**.
4. Select **Create a custom task to delegate** and click **Next**.
5. Select **Only the following objects in the folder**. In the given list, select **Group objects** and click **Next**.



6. Check the boxes for **General** and **Property-specific**.
7. Under Permissions, check the **Read Members** and **Write Members** boxes and click **Next**.



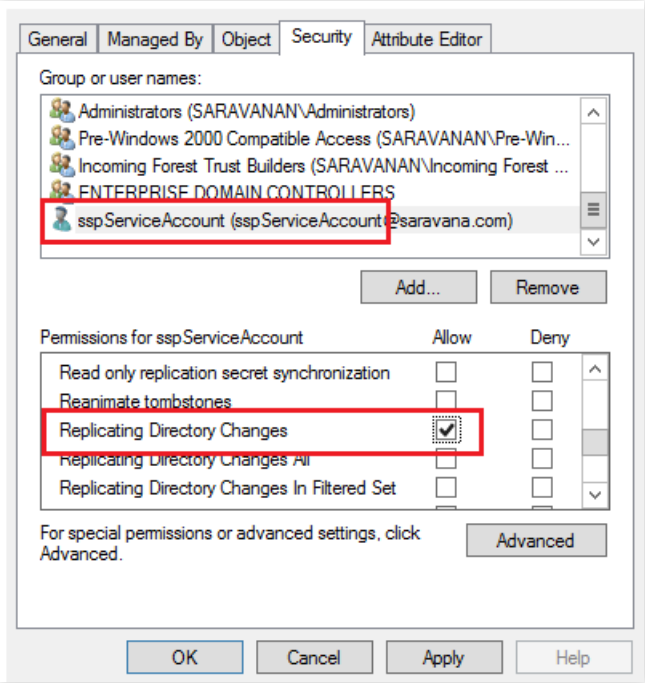
8. Click **Finish.**

Note: This permission only enables mail group subscription.

Synchronizing deleted AD user objects with ADSelfService Plus

To synchronize Active Directory objects with ADSelfService Plus without any issue, you need to provide the Replicate Directory Changes permission to the user or service account used in ADSelfService Plus. To do this, follow the steps below:

1. In the ADUC console, right-click the **domain or OU** and select **Properties.**
2. Under the **Security** tab, click **Add** to select the user or service account.
3. In the **Permissions** section, **Allow** the **Replicate Directory Changes** permission.

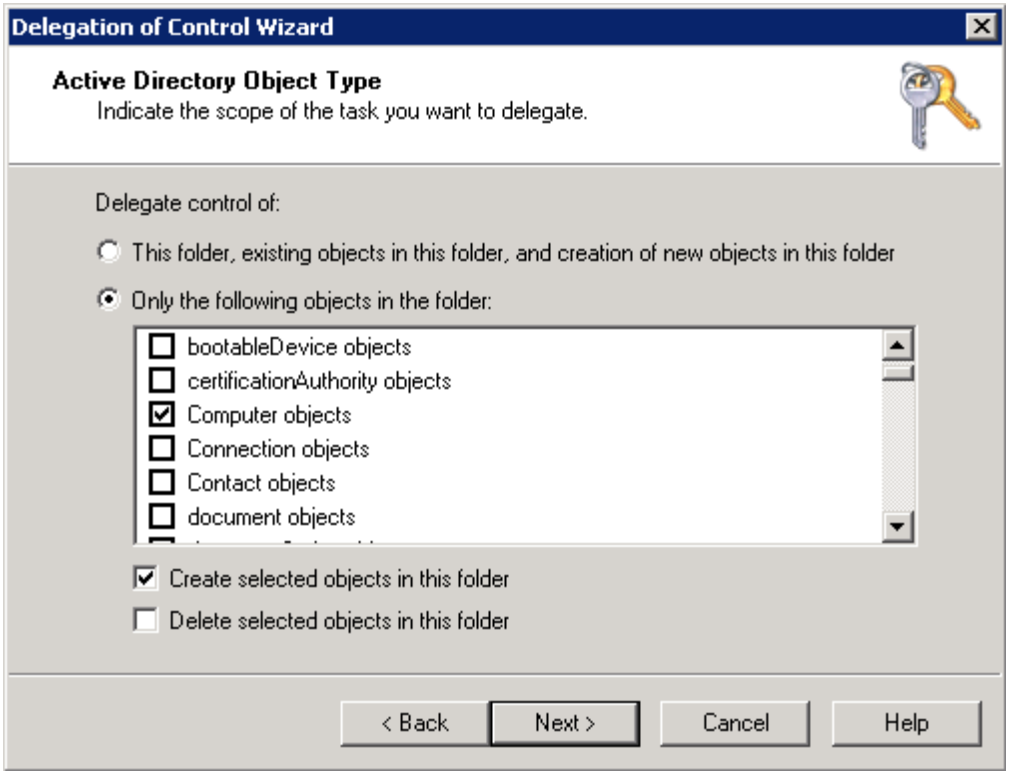


4. Click **OK.**

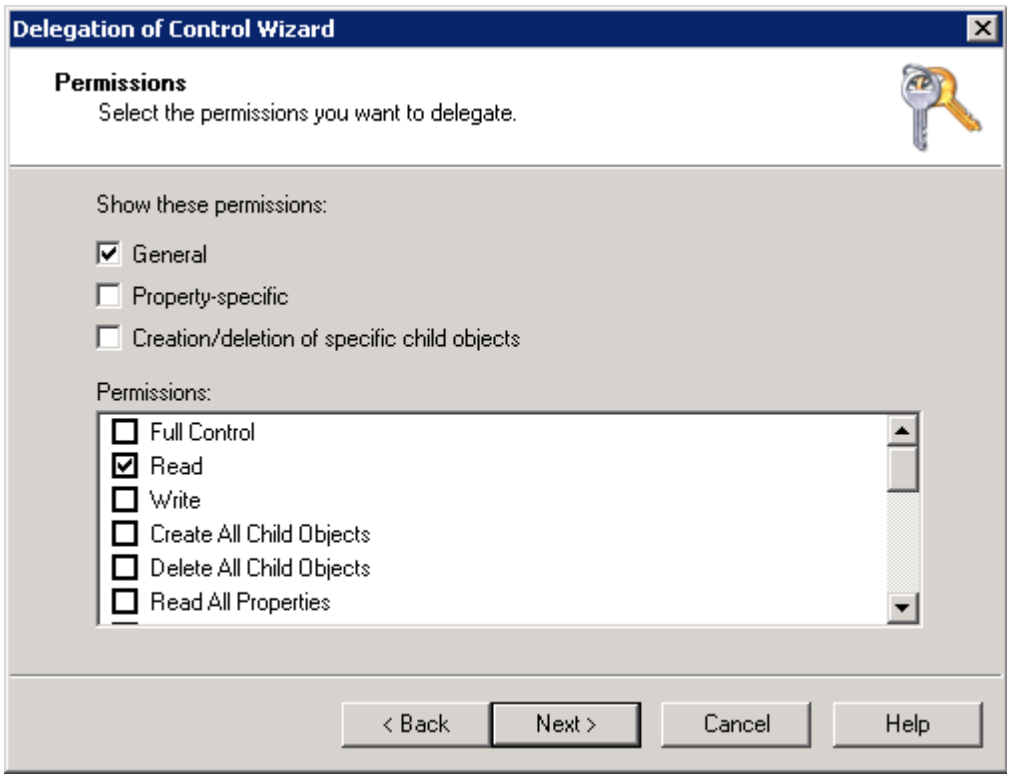
Single sign-on to ADSelfService Plus via NTLMv2

For this feature to work, you need to delegate the *permission to create and read computer accounts* in the ADUC console. To do this, follow the steps below:

1. Right-click the Computers OU or domain in ADUC and select Delegate Control from the context menu.
2. Click **Next** in the welcome dialog box.
3. Click **Add** to select the ADSelfService Plus user account or service account, then click **OK**.
4. Click **Next**.
5. Select **Create a custom task to delegate** and click **Next**.
6. Select **Only the following objects in the folder**. In the given list, select **Computer objects** and **Create selected objects in this folder** and click **Next**.



7. Check the **General** box.
8. Under Permissions, check the **Read** box and click **Next**.



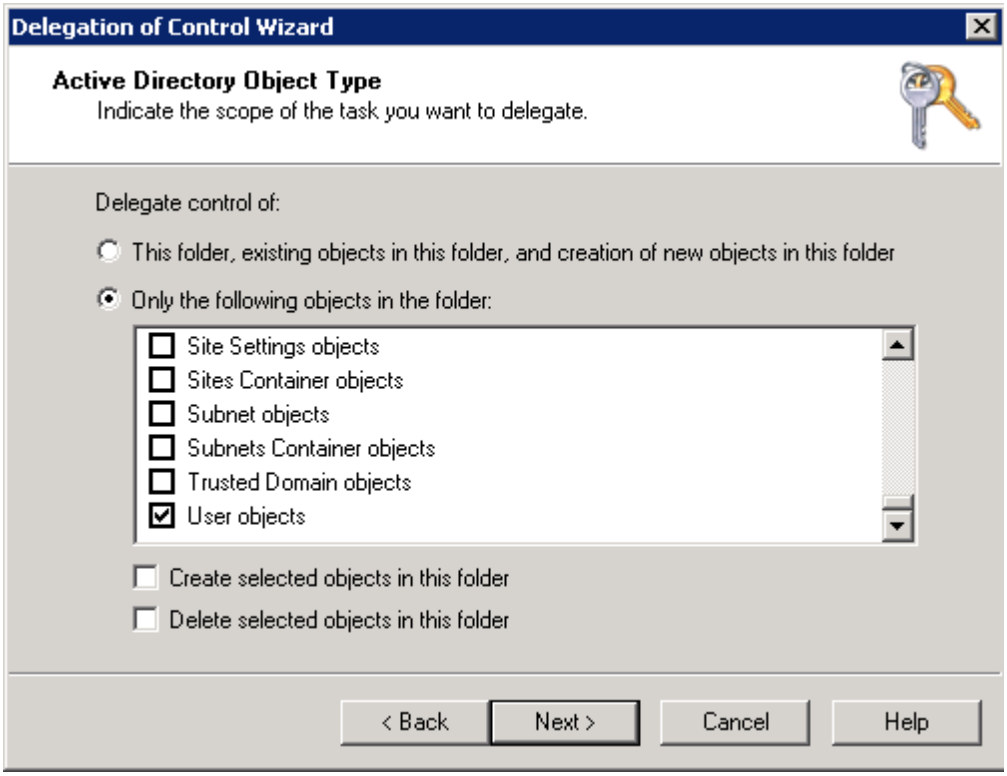
9. Click **Finish**.

Note: This permission only enables you to configure NT LAN Manager (NTLMv2) SSO to ADSelfService Plus.

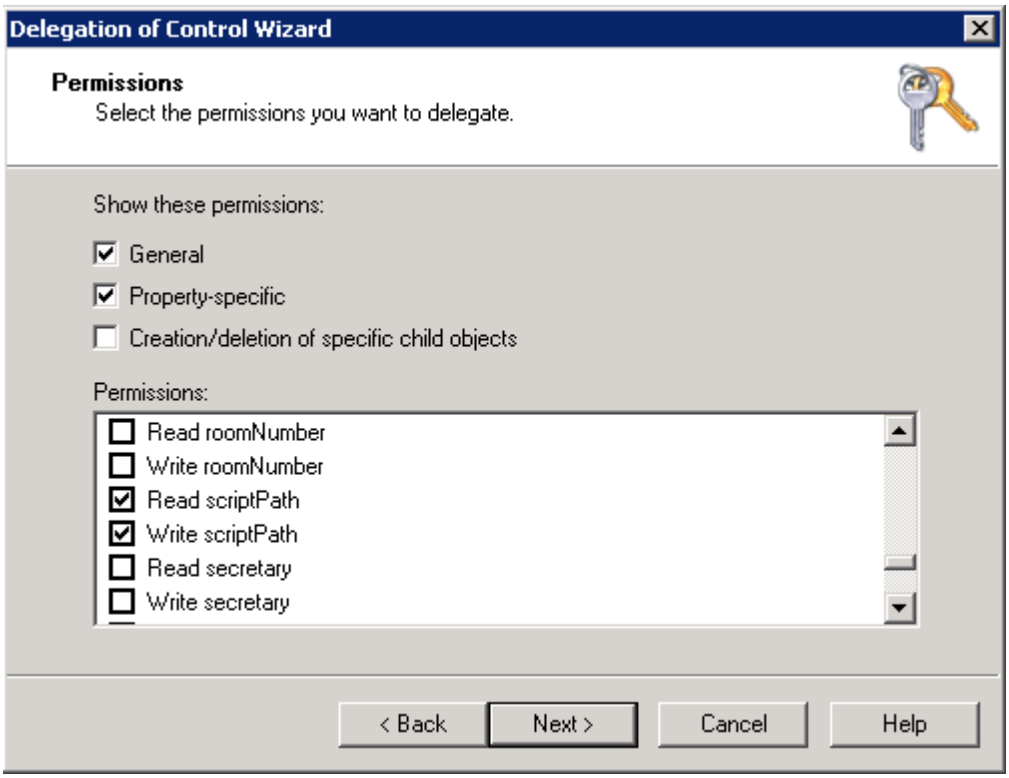
Force enrollment using a logon script

To use this feature, you need to delegate the *permission to modify the user scriptPath* in the ADUC console. Follow the steps below to do this:

1. Right-click the OU or domain in ADUC and select Delegate Control from the context menu.
2. Click **Next** in the welcome dialog box.
3. Click **Add** to select the user account or service account, then click **OK**.
4. Click **Next**.
5. Select **Create a custom task to delegate** and click **Next**.
6. Select **Only the following objects in the folder**. In the following list, check **User objects** and click **Next**.



7. Check both the **General** and **Property-specific** boxes.
8. Under Permissions, check the **Read scriptPath** and **Write scriptPath** boxes and click **Next**.



9. Click **Finish.**

Note: This permission only enables logon script path modification.

To view a deleted users report

The minimum requirement to view this report is membership in the **Domain Admins** group.

To perform GINA installation

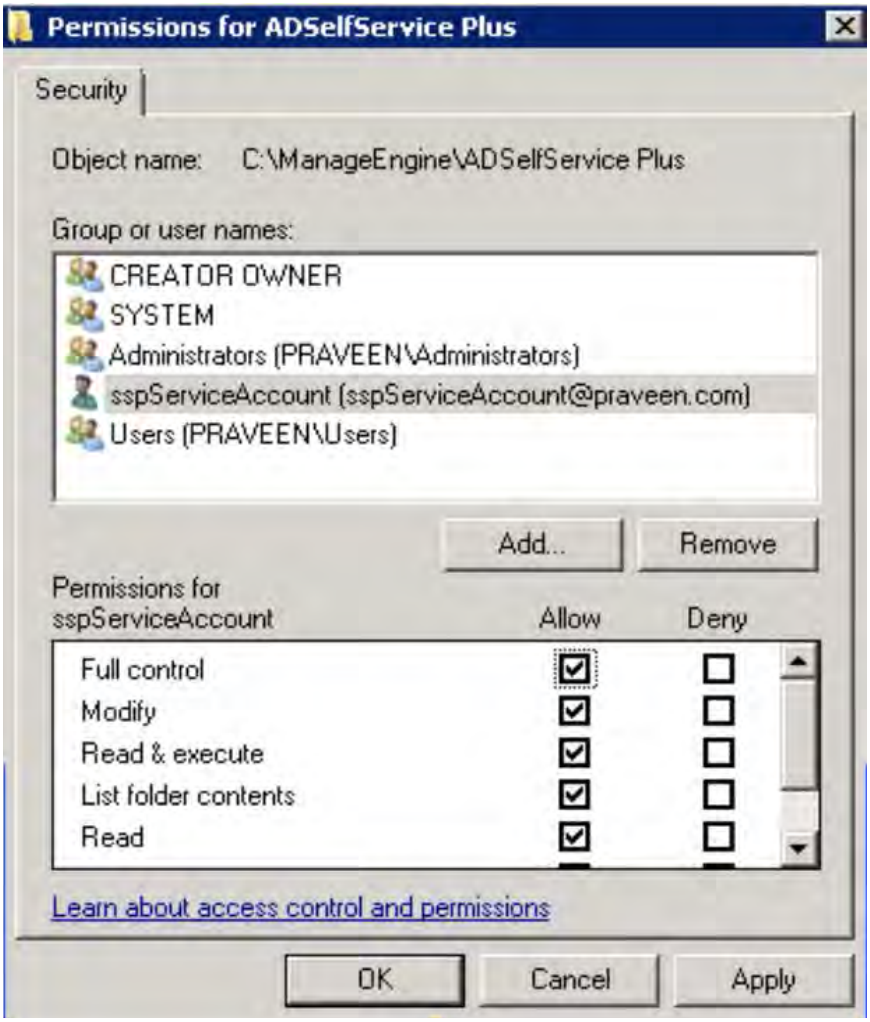
The minimum requirement to perform GINA installation from ADSelfService Plus' web console is membership in the **Domain Admins** group.

If Domain Admin credentials are not available for use, you can install GINA manually via Group Policy Objects (GPOs) or using System Center Configuration Manager (SCCM).

Folder permissions for other actions

The service account used to run ADSelfService Plus and the local user account used to start ADSelfService Plus must be granted **full control** permission to the product installation folder. Otherwise, you won't be able to:

- Install service packs
- Generate reports
- Start up the product
- Apply licenses
- Update dashboard graphs
- Back up and restore data
- Display employee photos and offer users self-update options



To configure high availability

The minimum requirement to configure high availability in ADSelfService Plus is membership in the Domain Admins group. Domain Admin privileges are only mandatory during the initial setup of high availability. Once high availability has been configured, the service account can be changed to one with lesser privileges based on other features configured. Ensure that folder sharing between both the instances is uninterrupted.