ManageEngine 卓豪
ADSelfService Plus

所需权限与授权

目录

文档摘要

本指南将逐步指导您如何为Active Directory用户账户分配使用ADSelfService Plus自助服务功能所需的权限。ADSelfService Plus无需用户具备“域管理员”身份即可重置密码、解锁账户、更新个人资料或使用其他功能。遵循最小权限原则，您只需手动向用户账户授予执行自助服务操作所需的具体权限即可。

Note：若在添加域名时未提供任何身份验证信息，ADSelfService Plus 将通过以下两种方式之一获取权限：

- 若将ADSelfService Plus安装为控制台应用程序运行且未提供凭证，则默认情况下该程序将使用安装该产品的用户的权限。
- 若将ADSelfService Plus安装为服务运行且未提供凭证，则默认情况下它将使用运行该服务所使用的账户权限。

ADSelfService Plus 概述

ManageEngine ADSelfService Plus是一款集成化的Active Directory自助密码管理与单点登录解决方案，可有效减少密码重置请求，并避免终端用户因计算机停机而产生的困扰。它 o仟ers

- 自助密码重置及账户解锁
- 密码和账户过期通知器
- 密码策略执行器
- 企业单点登录和密码同步器
- 机器登录的端点多因素认证
- 目录自动更新和员工搜索

这些功能旨在平衡网络安全保障与访问便捷性，从而提升投资回报率（ROI）并培养高效的IT人才团队。

所需权限

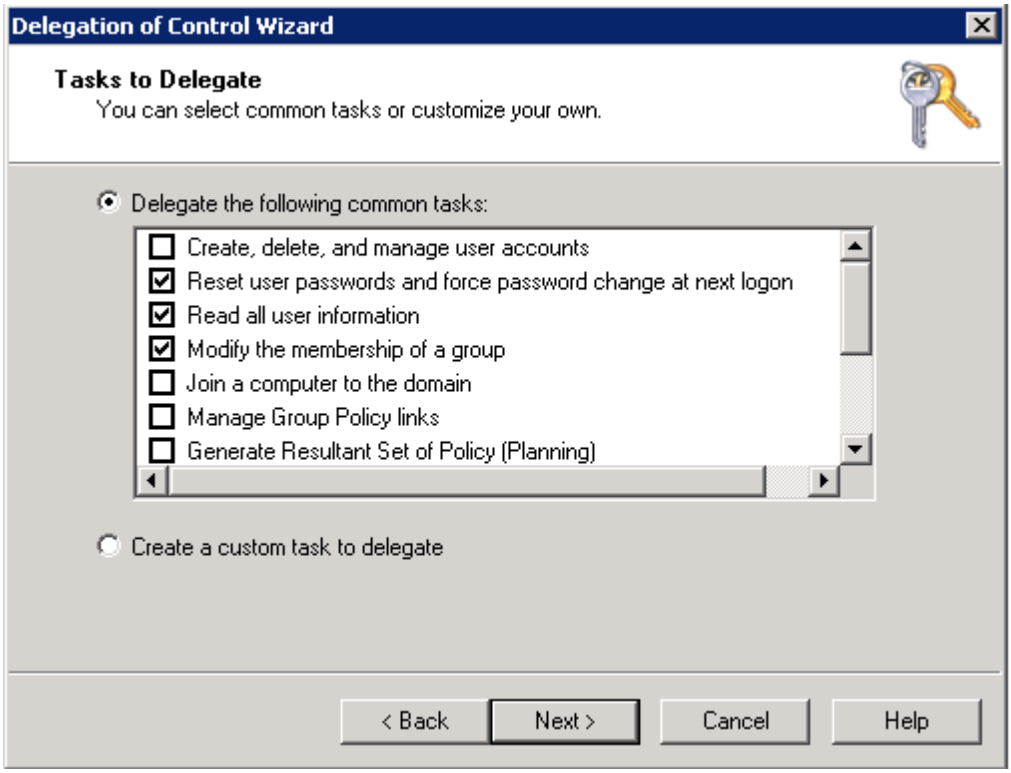
特征	所需权限：
自助密码重置	重置用户对象的密码；读取用户对象的上次设置密码；写入用户对象的上次设置密码
自助账户解锁	读取用户对象的锁定时间；写入用户对象的锁定时间
自更新用户属性	阅读用户对象 文书；书面文件　对于用户对象而言：
显示细粒度密码策略	用于 MS DS 密码设置对象的广告 MS DS密码设置容器的广告对象
自助邮件组订阅	读取组对象中的成员；写入组对象中的成员
NTLM 单点登录	计算机对象的属性 计算机对象广告
使用徽标和脚本强制完成注册	为用户对象读取脚本路径；为用户对象写入脚本路径。
查看已删除用户的报告	加入“主要管理员”组
GINA安装	加入“主要管理员”组
高可用性配置	加入“域名管理员”组

配置权限

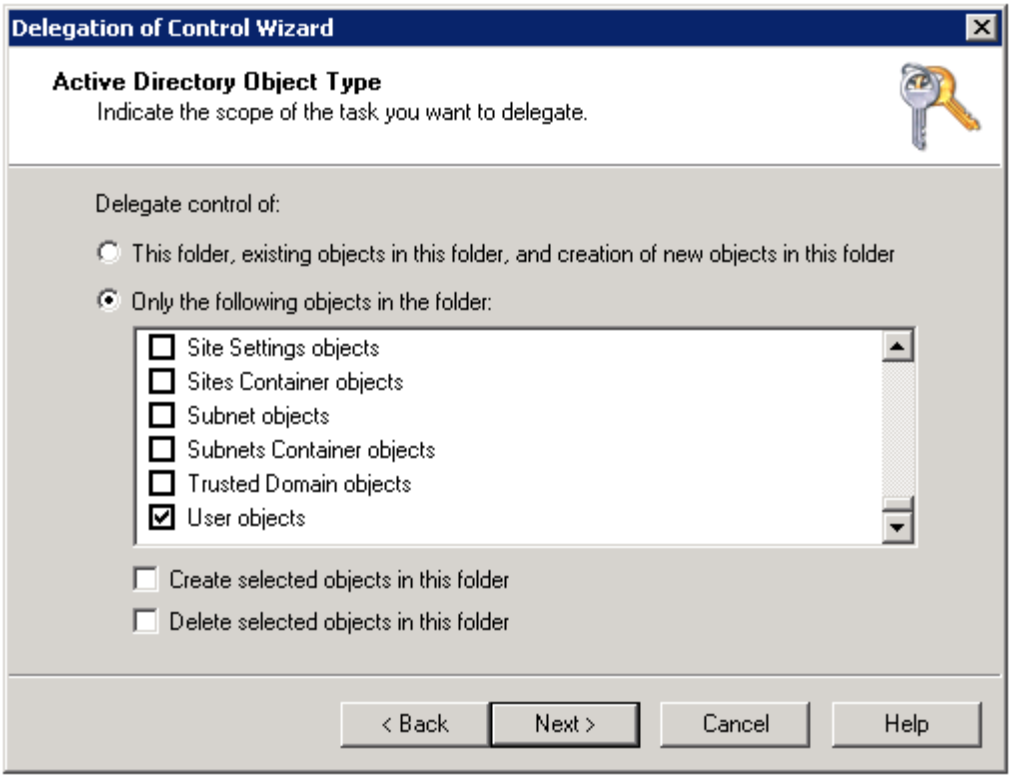
要使用所有 ADSelfService Plus 功能

若用户需使用ADSelfService Plus的所有功能，您需要为该服务账户授予以下权限：

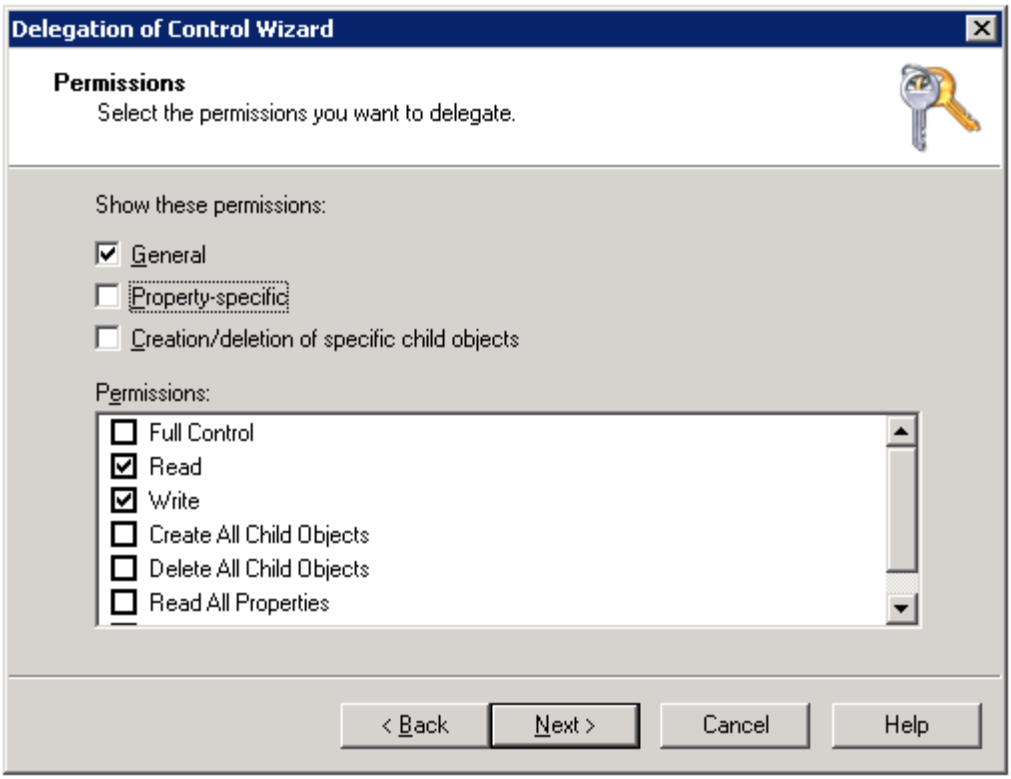
1. 在 ADUC 中右键单击**域**，从上下文菜单中选择**委派控制权**。
2. 在欢迎对话框中点击**下一步**。
3. 点击**添加**以选择用户账户或服务账户，然后点击**确定**，再点击**下一步**。
4. 选择**授权以下常见任务**并勾选**“重置用户密码及在下次登录时强制更改密码”**、**“读取所有用户信息”**以及**“修改组成员资格”**复选框，然后点击**“下一步”**。



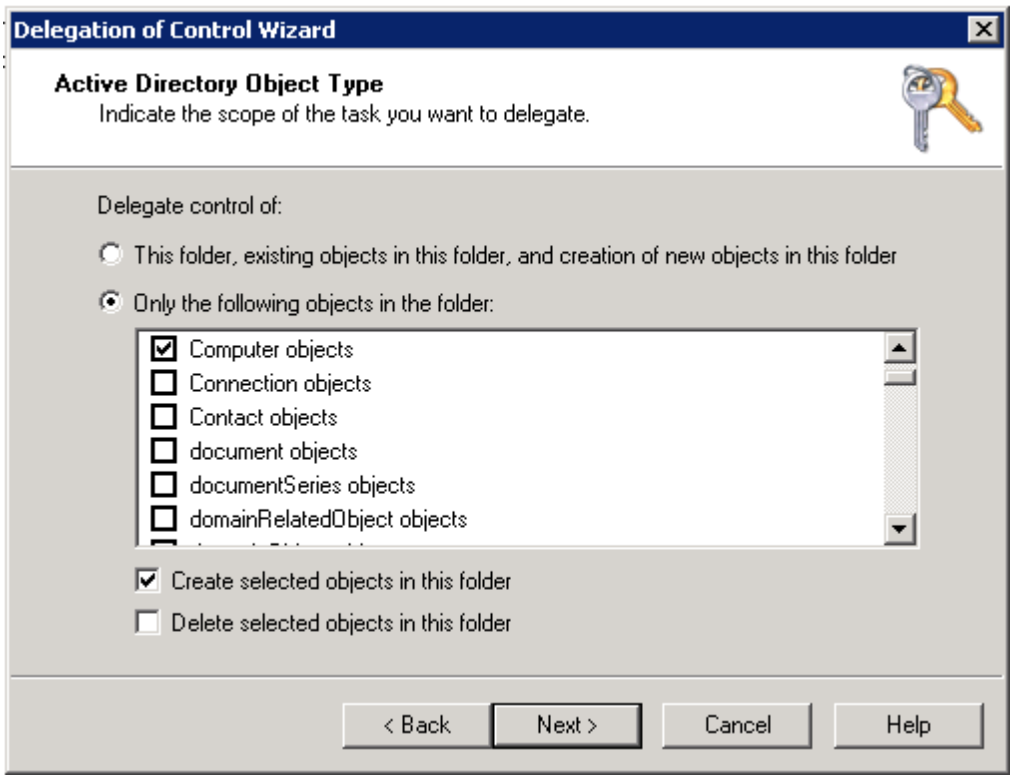
5. 单击**完成**，然后重复步骤**1-3**。
6. 选择**创建自定义任务以委派**，然后单击**“下一步”**。
7. 选择**文件夹中的以下对象。**在给定列表中，选择**用户对象。**



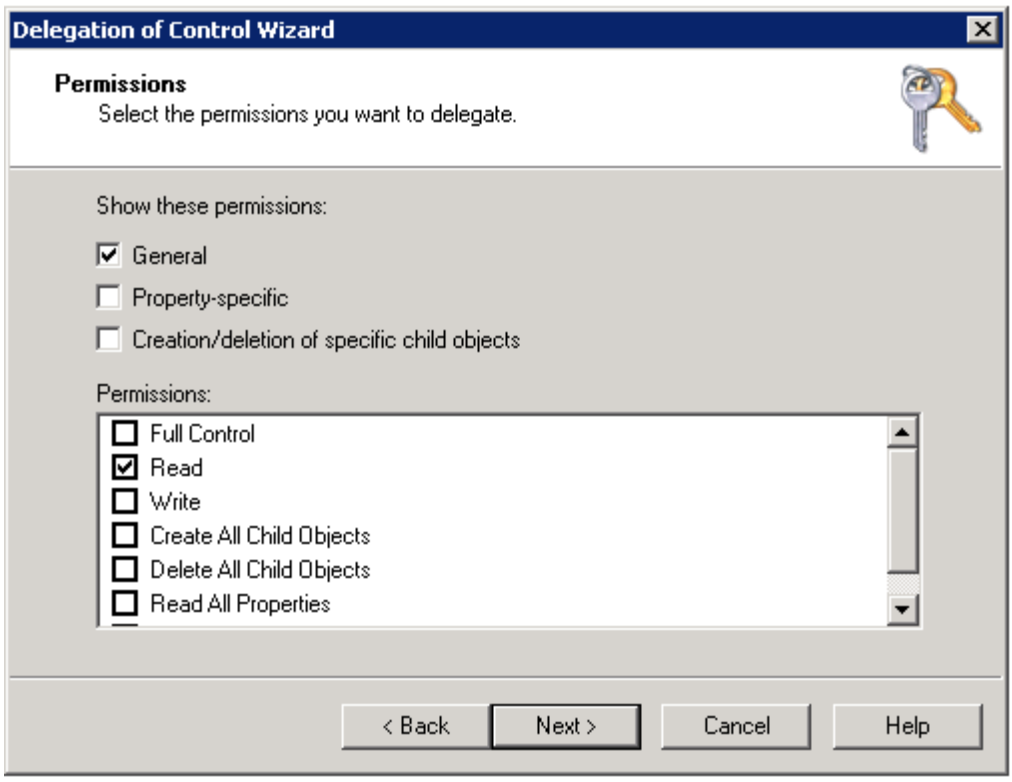
8. 选择**常规**框。在“权限”下，选中**读取**和**写入**复选框，然后点击**下一步**。



9. 点击**完成**，然后重复步骤1-3。
10. 选择**创建自定义任务以委派**，然后单击**“下一步”。**
11. 选择**文件夹中的以下对象：**从列表中选择**“计算机对象”**”，然后**在该文件夹中创建所选对象。**



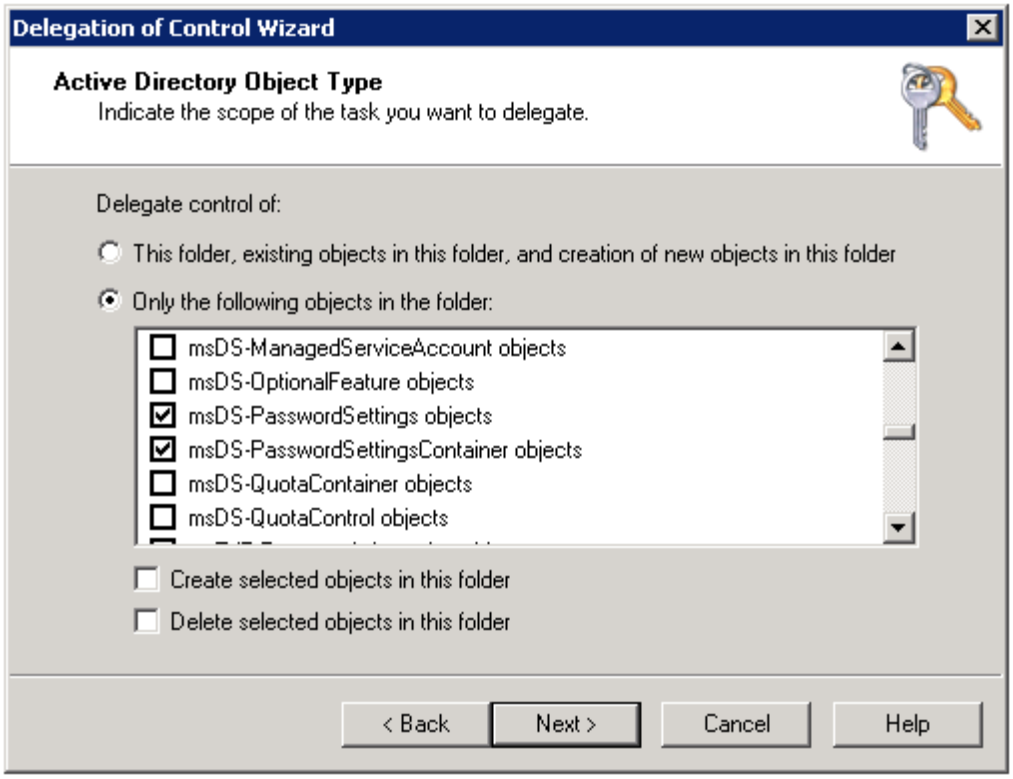
12. 选择**常规**框。在“权限”下，选中**读取**，然后单击**下一步**。



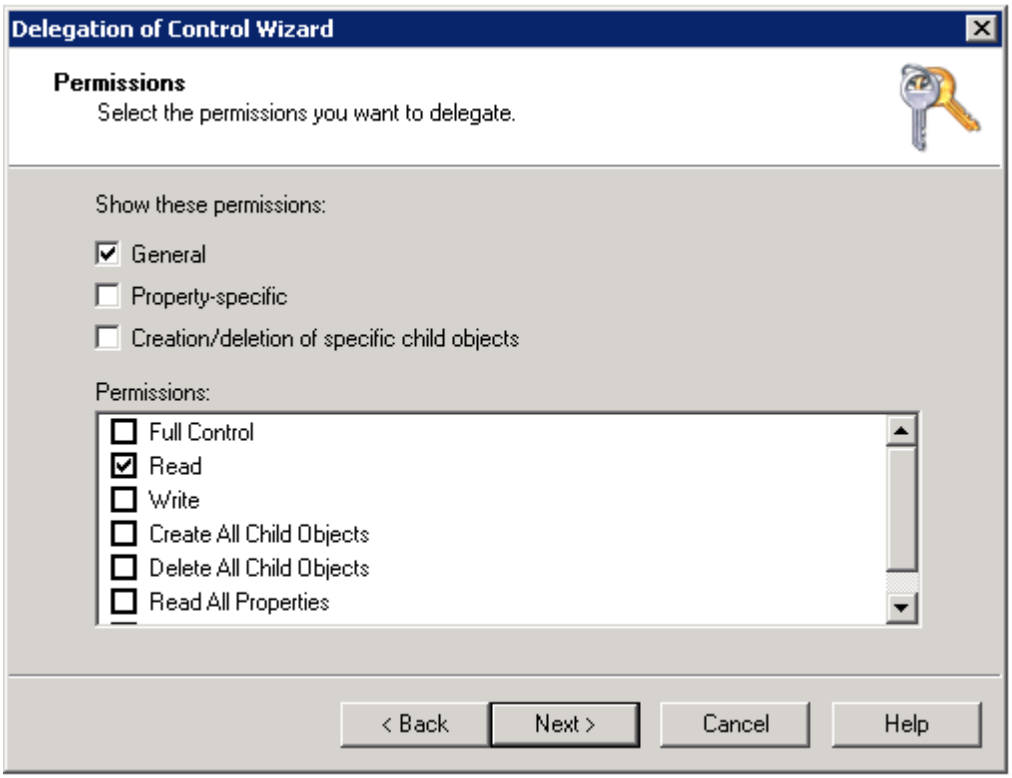
13. 点击**完成**，然后重复步骤1-3。

14. 选择**创建自定义任务以委派**，然后单击**“下一步”。**

15. 选择**文件夹中的以下对象：**在给定列表中，选择**msDS-PasswordSettings 对象**和**msDS-PasswordSettingsContainer 对象。**单击**下一步。**



16. 选择**常规**框。在“权限”下，选中**读取**，然后单击**下一步**。



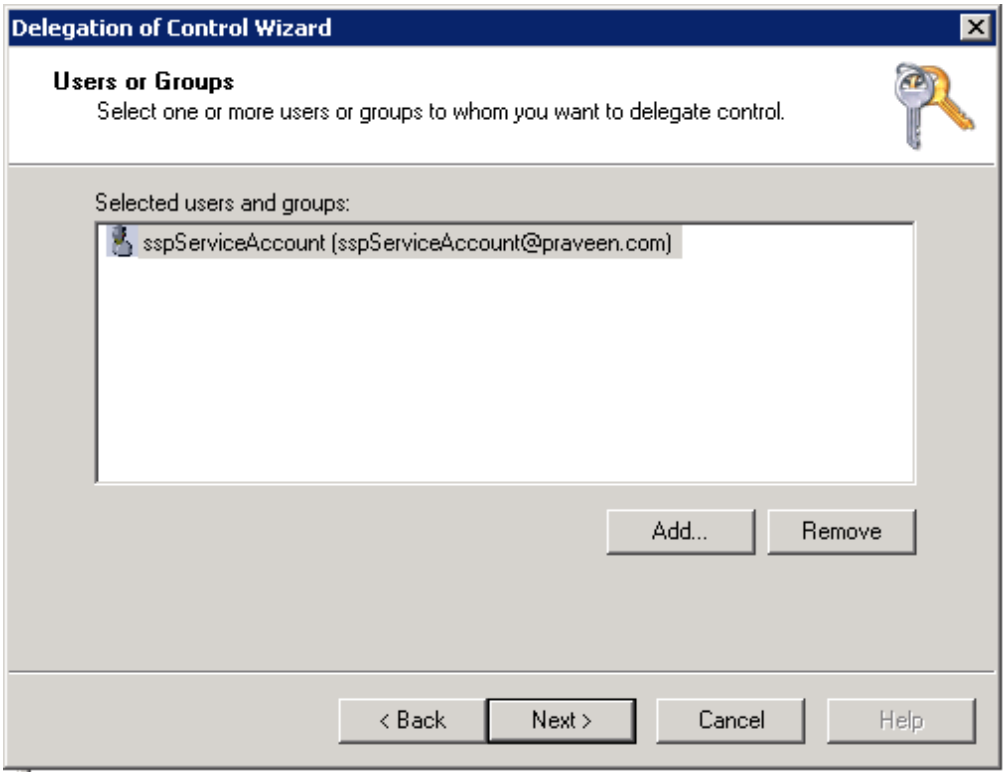
17. 单击**“完成”**。

自助密码重置

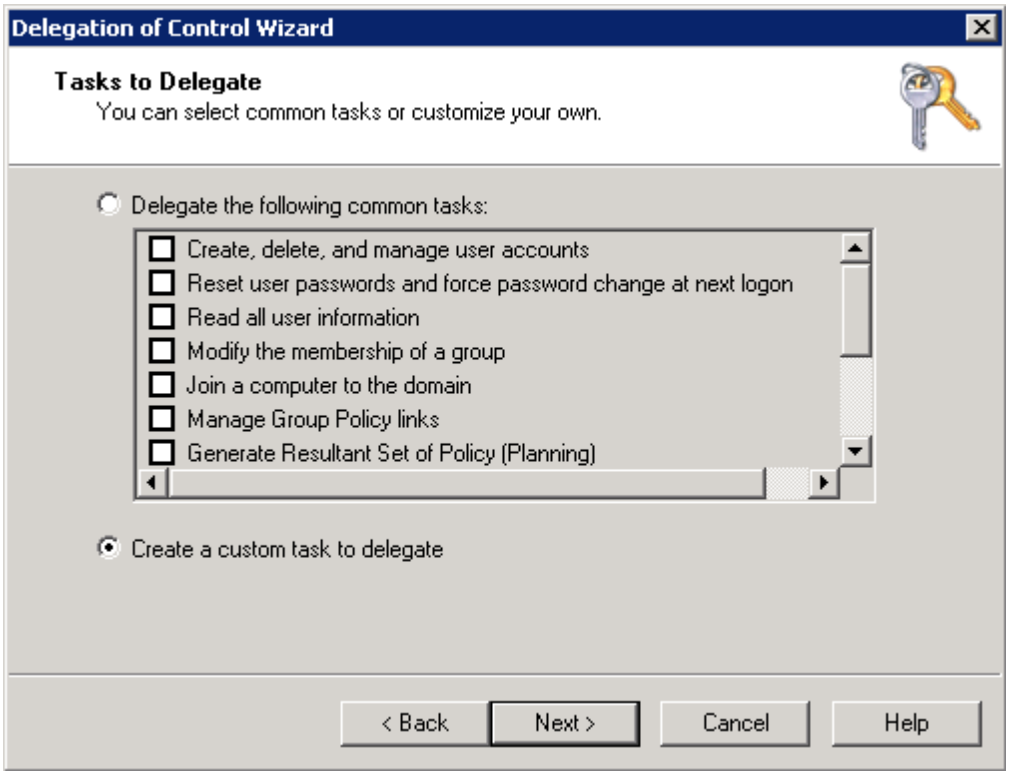
要使此功能正常运行，您需要在 ADUC 控制台中授予*重置用户密码的权限*。具体操作步骤如下：

1. 在 ADUC 中右键单击**组织单位**或**域**，然后选择**委派控制权**。
2. 在欢迎对话框中点击**下一步**。

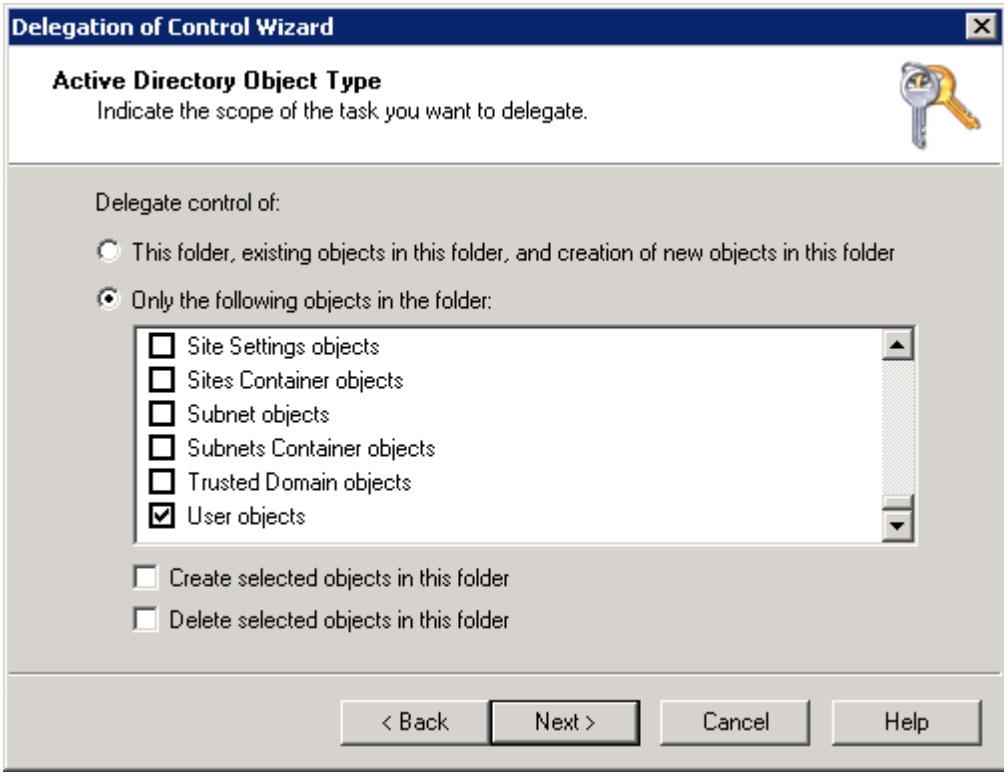
3. 单击**添加**以选择ADSelfService Plus用户帐户或服务帐户，然后单击**确定**。
4. 单击**下一步**。



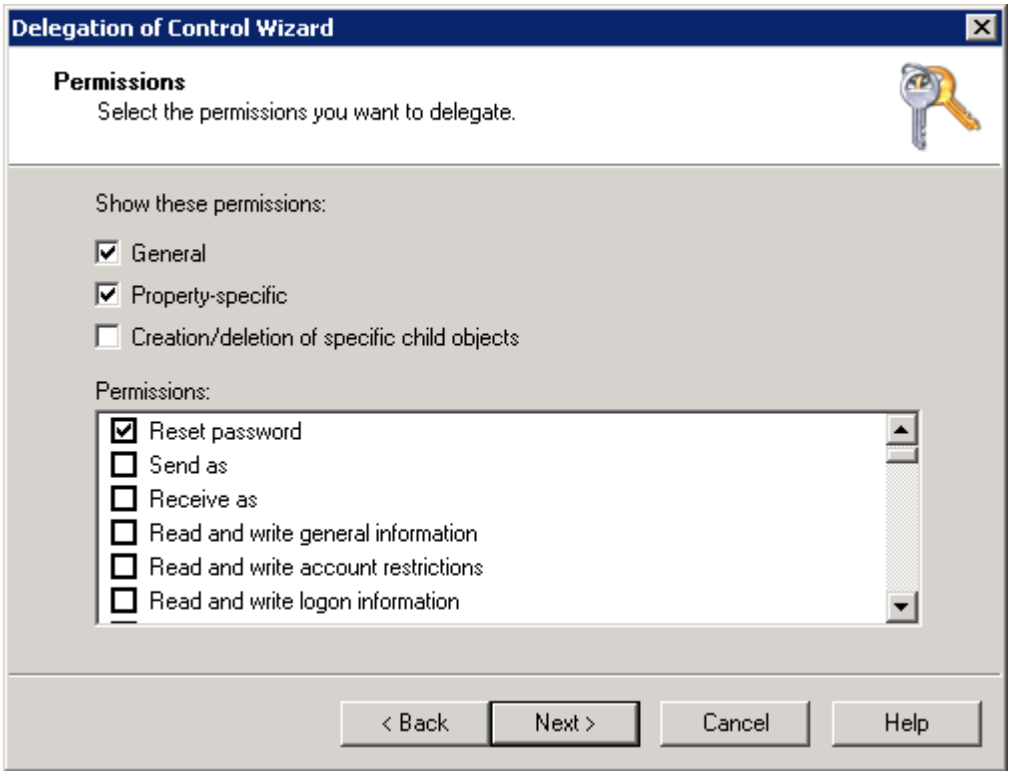
5. 选择**创建自定义任务以委派**，然后单击**“下一步”。**

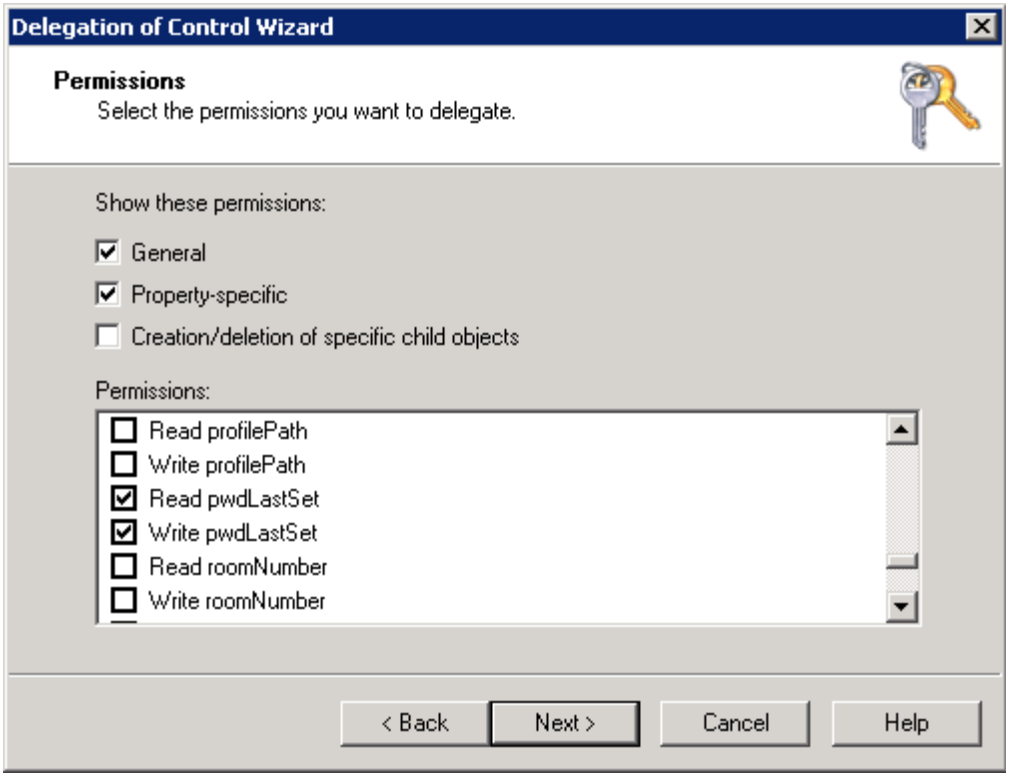


6. 选择**文件夹中的以下对象。**在给定列表中，选择**用户对象并点击“下一步”**



7. 选中“**通用**”和“**特定属性**”复选框。
8. 在“权限”选项下，在点击**下一步**之前，勾选**重置密码、读取上次设置的密码**以及**写入上次设置的密码**的复选框。


Delegation of Control Wizard
Permissions
Select the permissions you want to delegate.
Show these permissions:
General
Property-specific
Creation/deletion of specific child objects
Permissions:
Reset password
Send as
Receive as
Read and write general information
Read and write account restrictions
Read and write logon information
< Back
Next >
Cancel
Help


Delegation of Control Wizard
Permissions
Select the permissions you want to delegate.
Show these permissions:
General
Property-specific
Creation/deletion of specific child objects
Permissions:
Read profilePath
Write profilePath
Read pwdLastSet
Write pwdLastSet
Read roomNumber
Write roomNumber
< Back
Next >
Cancel
Help

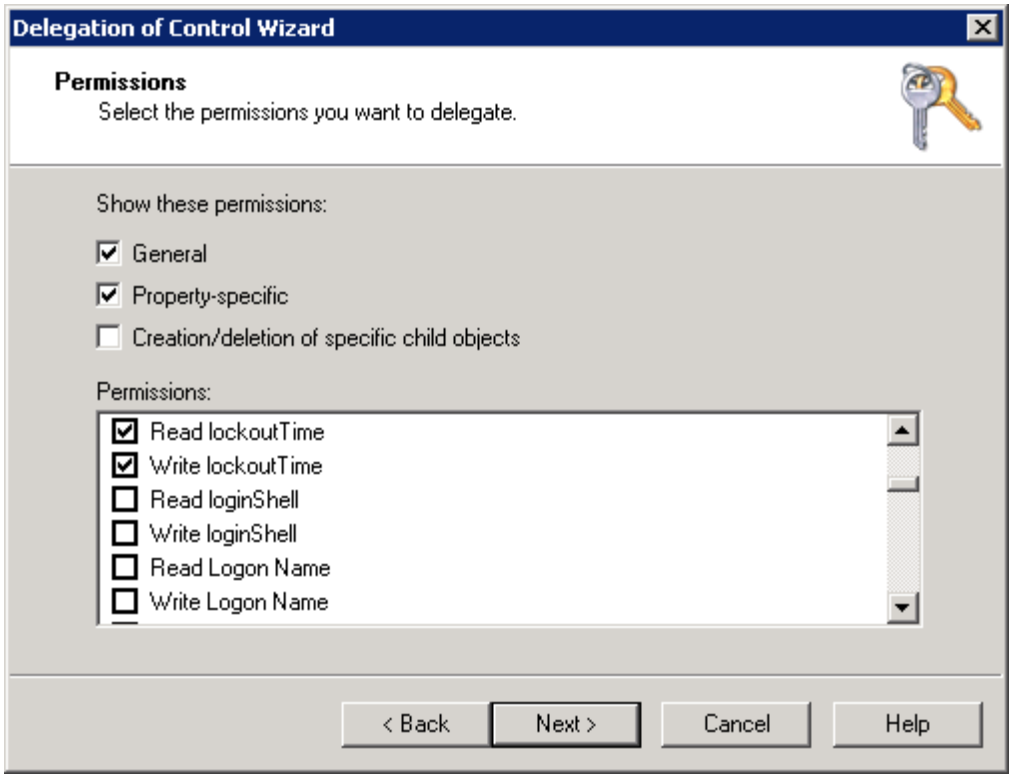
9. 单击**“完成”**。

注：该权限仅可启用密码重置功能。

自助解锁账户

要使此功能正常运行，您需要在 ADUC 控制台中授予*解锁用户账户的权限*。具体操作如下：

1. 在 ADUC 中右键单击组织单位（OU）或域，然后从上下文菜单中选择“委派控制”。
2. 在欢迎对话框中点击**下一步**。
3. 单击**添加**以选择ADSelfService Plus用户帐户或服务帐户，然后单击**确定**。
4. 单击**下一步**。
5. 选择**创建自定义任务以委派**，然后单击**“下一步”**。
6. 选择**文件夹中的以下对象。**在给定列表中，选中**用户对象**并单击**下一步。**
7. 选中**“常规”**和**“属性特定”**复选框



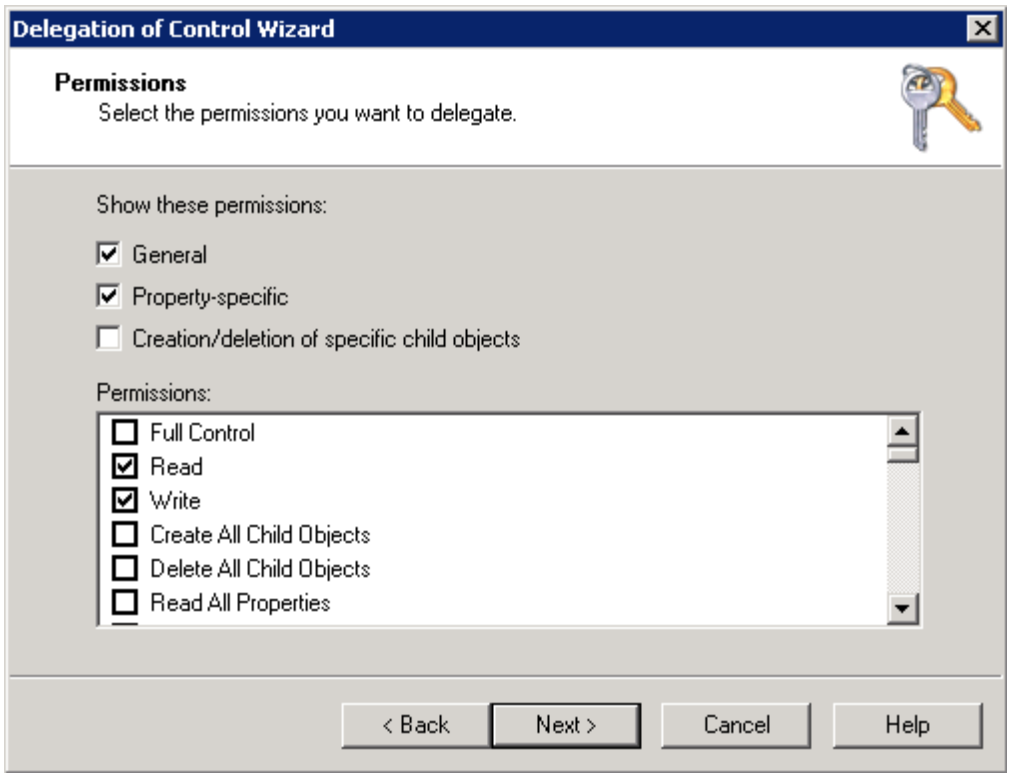
8. 在“权限”下，选中**读取锁定时间**和**写入锁定时间**复选框，然后单击**下一步**。
9. 单击**“完成”**。

注意：此权限仅可解锁账户。

目录自动更新

要使用此功能，您需要在 ADUC 控制台中授予*修改用户属性的权限*。请按照以下步骤操作:

1. 在 ADUC 中右键单击组织单位（OU）或域，然后从上下文菜单中选择“委派控制”。
2. 在欢迎对话框中点击**下一步**。
3. 单击**添加**以选择用户帐户或服务帐户，然后单击**确定**。
4. 单击**下一步**。
5. 选择**创建自定义任务以委派**，然后单击**“下一步”。**
6. 选择**文件夹中的以下对象。**在给定列表中，选择**用户对象**并点击**“下一步”。**
7. 选中**“通用”**和**“特定属性”**复选框。



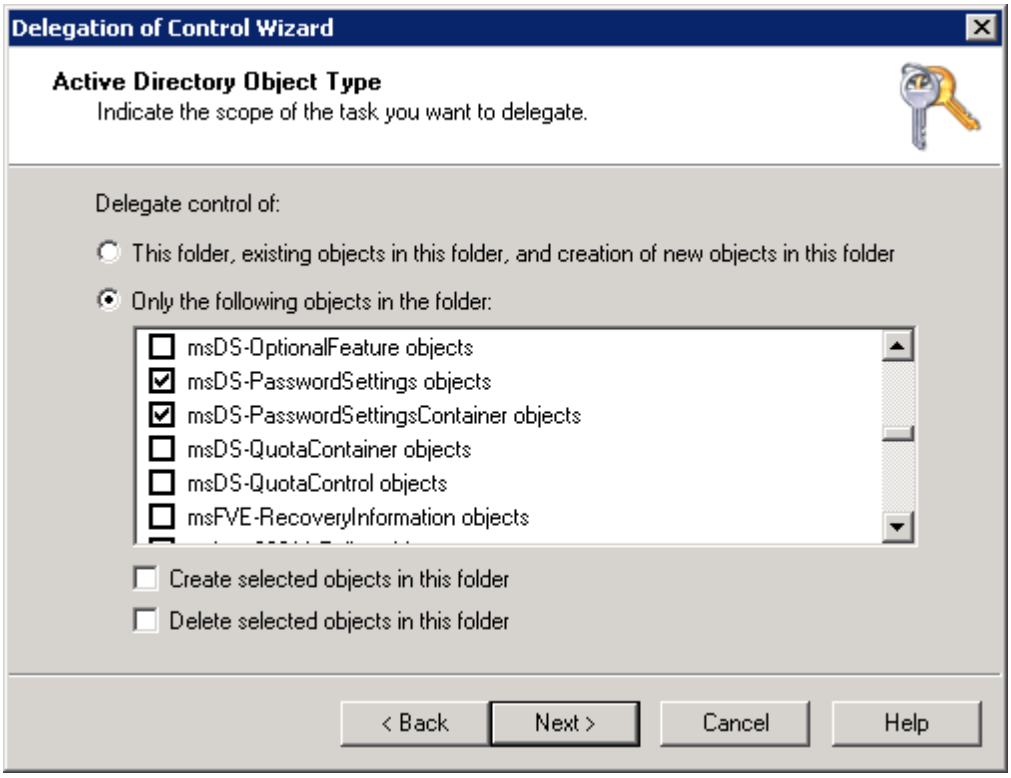
8. 在“权限”选项下，选中**“读取”**和**“写入”**复选框（或选择**需要为最终用户自助更新可用的特定属性的“读取”**和**“写入”复选框），然后单击“下一步”。**
9. 单击**“完成”。**

注：该权限仅启用自动更新功能。

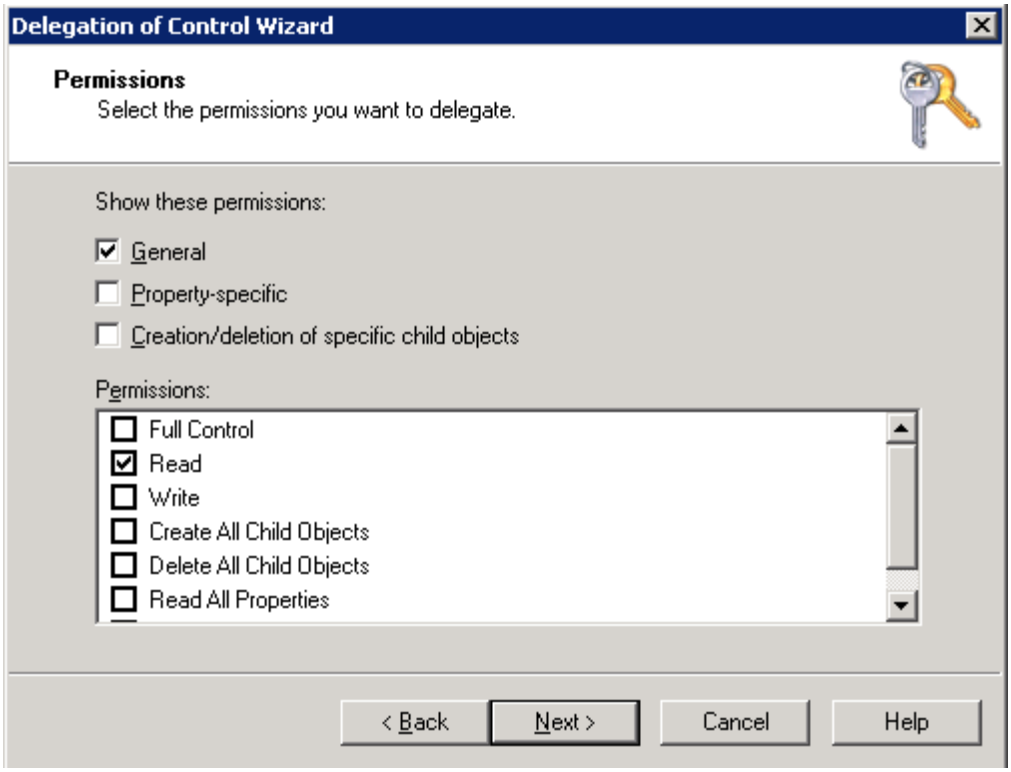
显示细粒度密码策略

若要在启用了细粒度密码策略的用户重置/更改密码界面中显示精确的密码策略要求，则需在 ADUC 中授予用户*读取其密码设置对象（PSO）的权限*。请按照以下步骤操作:

1. 在 ADUC 中右键单击组织单位（OU）或域，从上下文菜单中选择“委派控制”。在欢迎对话框中点击**下一步**。
2. 单击**添加**以选择用户帐户或服务帐户，然后单击**确定**。
3. 单击**下一步**。
4. 选择**创建自定义任务以委派**，然后单击**“下一步”。**
5. 选择**文件夹中的以下对象。**在给定列表中选择**在点击“下一步”之前，请先选择 msDS-PasswordSettings 对象**和 **msDS-PasswordSettingsContainer 对象。**



7. 勾选**常规**框。



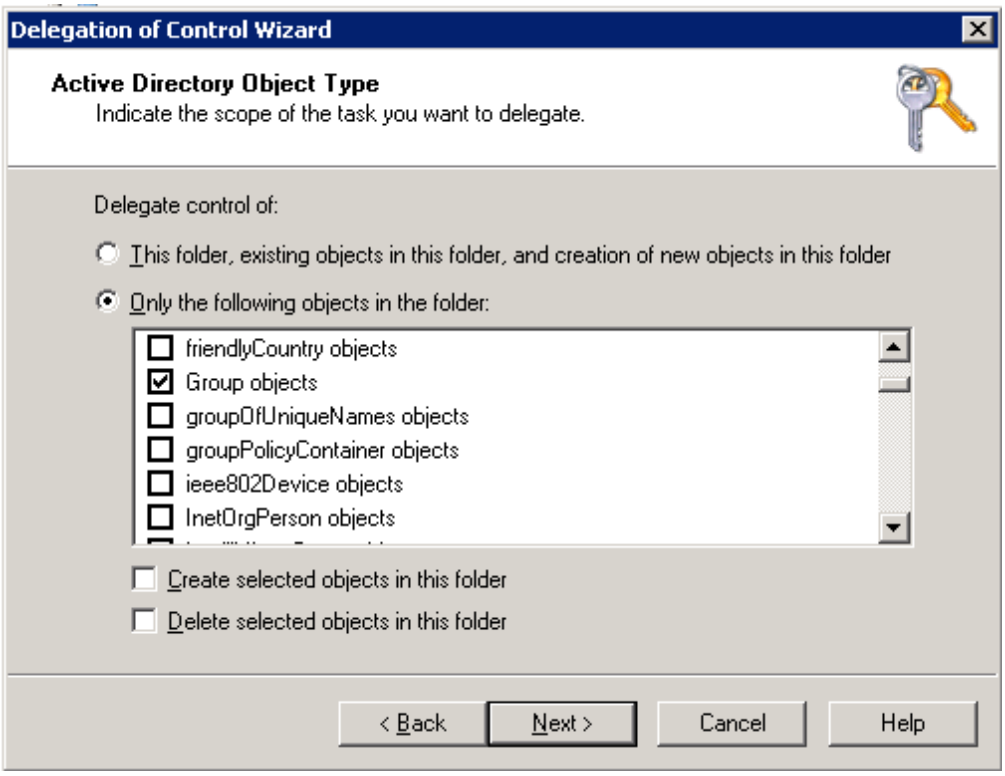
8. 在“权限”下，选择**读取**并点击**下一步**。
9. 单击**“完成”。**

注意：此权限仅用于获取密码策略。

自助式邮件组订阅

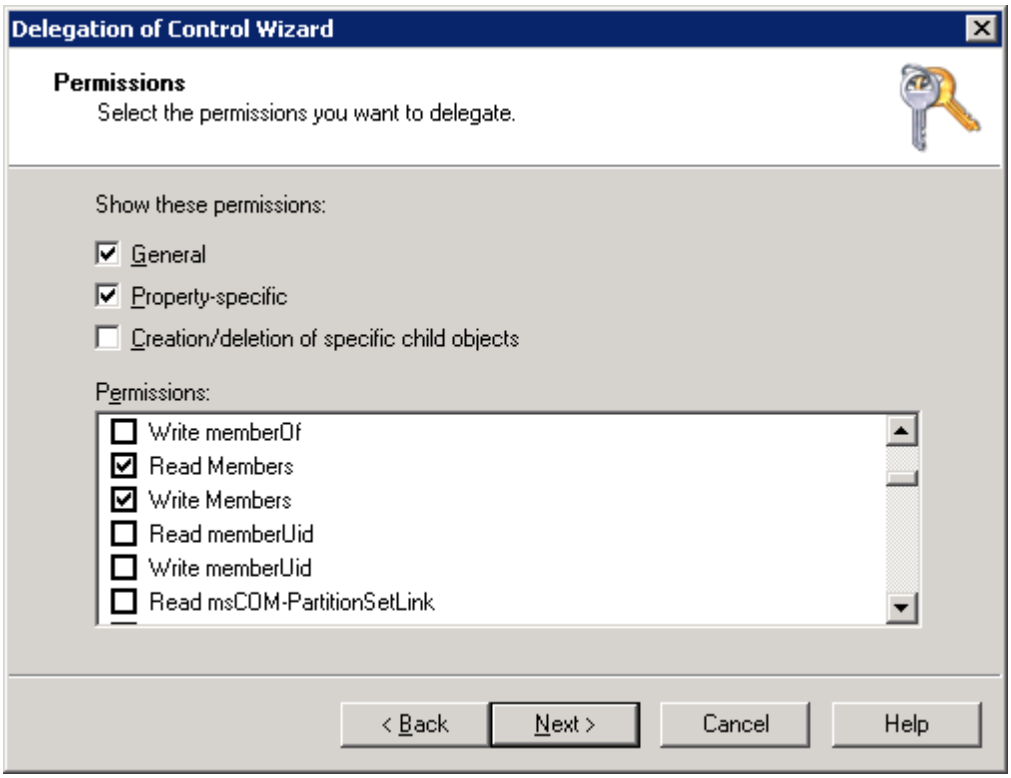
要使用此功能，您需要在 ADUC 控制台中授予*修改组成员的权限*。请按照以下步骤操作：

1. 右键单击包含需修改成员的组所属 ADUC 中的组织单位（OU）或域，然后从上下文菜单中选择“委派控制”。
2. 在欢迎对话框中点击**下一步**。
3. 点击**添加**以选择用户账户或服务账户，然后点击**确定**。点击**下一步**。
4. 选择**创建自定义任务以委派**，然后单击**“下一步”。**
5. 选择**文件夹中的以下对象。**在给定列表中，选择**组对象**并单击**下一步。**



6. 为“通用”及“特定房产”选项打勾。

7. 在“权限”下，勾选“读取成员”和“写入成员”复选框，然后单击“下一步”。



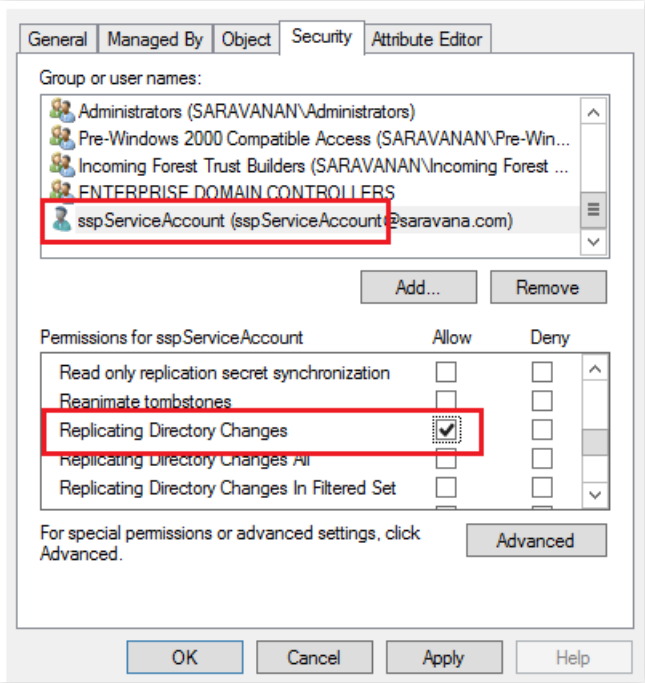
8. 单击**“完成”**。

注意：此权限仅可启用邮件组订阅功能。

将 AD 用户对象与 ADSelfService Plus 同步

要确保将 Active Directory 对象与 ADSelfService Plus 无缝同步，需为 ADSelfService Plus 中使用的用户或服务账户授予“复制目录更改”权限。具体操作步骤如下：

1. 在 ADUC 控制台中，右键单击**域或组织单位**，然后选择**属性。**
2. 在**安全**选项卡下，单击**添加**以选择用户或服务帐户。
3. 在“权限”部分，**允许**“复制目录更改”权限。

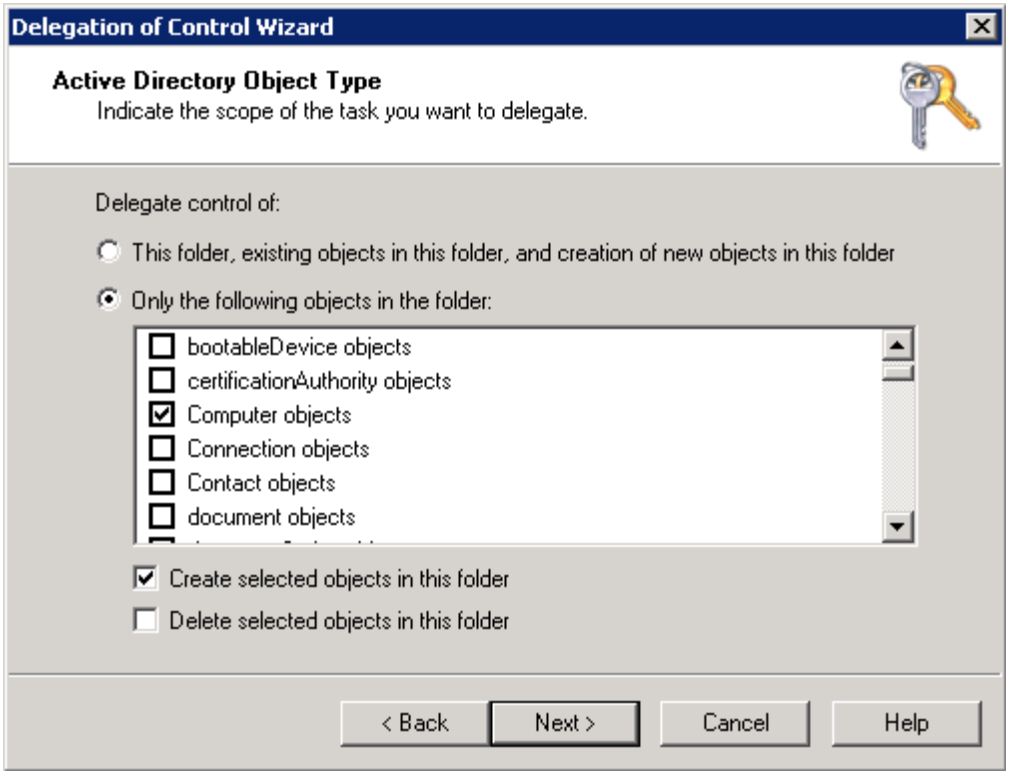


4. 单击**确定。**

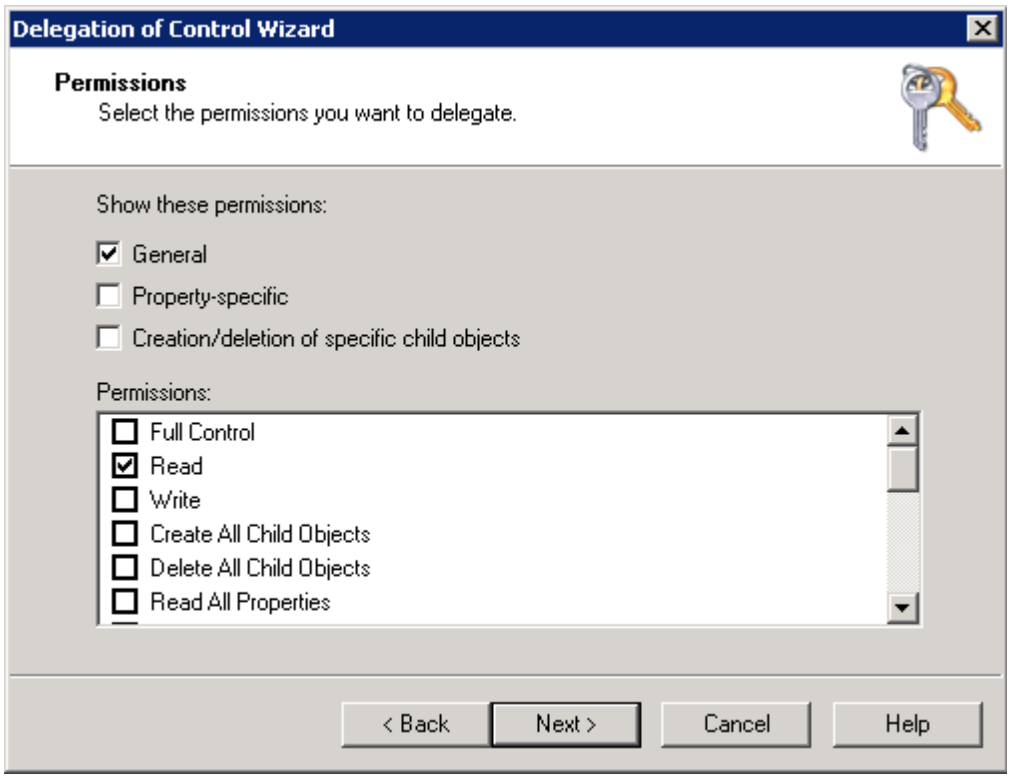
通过 NTLMv2 单点登录至 ADSelfService Plus

要使此功能正常运行，您需要在 ADUC 控制台中授予*创建和读取计算机账户的权限*。请按照以下步骤操作：

1. 右键单击 ADUC 中的计算机组织单位（OU）或域，然后从上下文菜单中选择“委派控制”。
2. 在欢迎对话框中点击**下一步**。
3. 单击**添加**以选择ADSelfService Plus用户帐户或服务帐户，然后单击**确定**。
4. 单击**下一步**。
5. 选择**创建自定义任务以委派**，然后单击**“下一步”。**
6. 选择**文件夹中的以下对象：**在给定列表中，选择**计算机对象**并**在此文件夹中创建所选对象**，然后单击**下一步。**



7. 勾选**常规**框。
8. 在“权限”下，选中**读取**复选框，然后单击**下一步**。



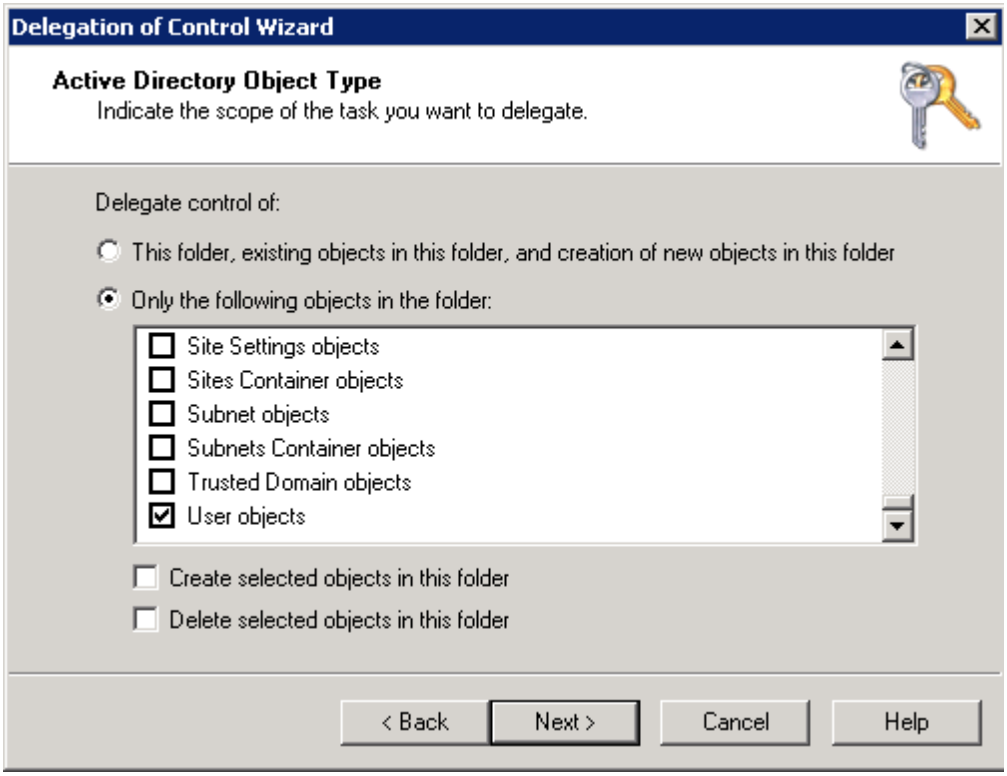
9. 单击**“完成”。**

注意：该权限仅允许您将NT局域网管理器（NTLMv2）SSO 配置为AD自助服务增强版。

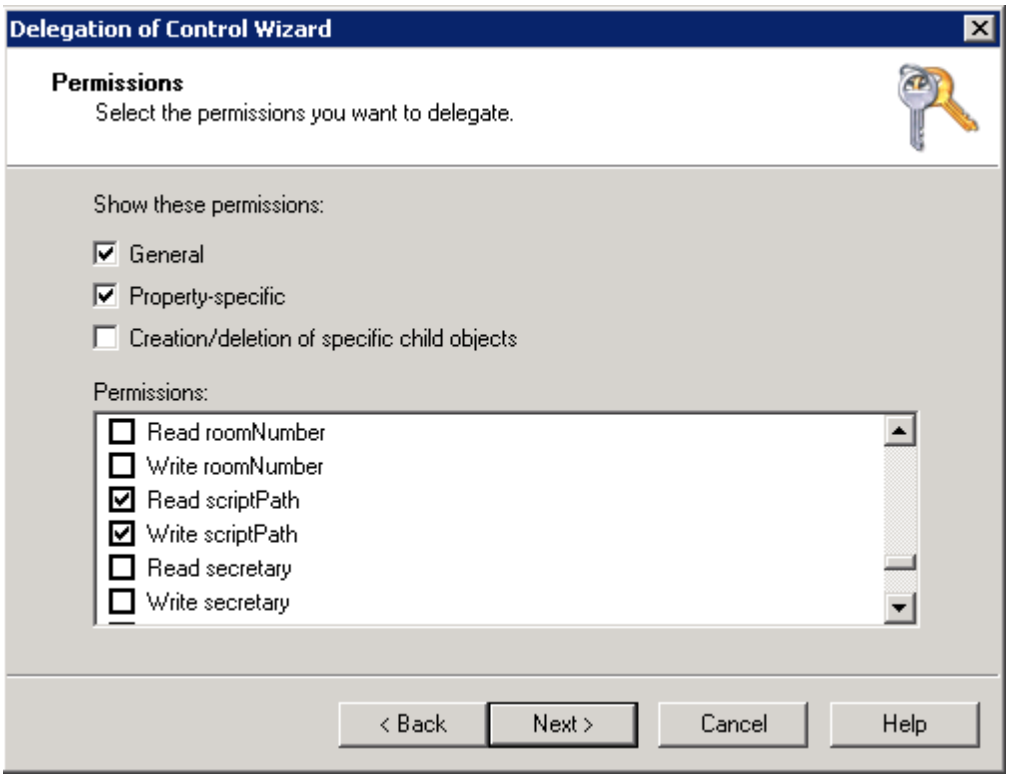
使用登录脚本强制完成注册

要使用此功能，您需要在 ADUC 控制台中授予*修改用户脚本路径的权限*。请按照以下步骤操作:

1. 在 ADUC 中右键单击组织单位（OU）或域，然后从上下文菜单中选择“委派控制”。
2. 在欢迎对话框中点击**下一步**。
3. 单击**添加**以选择用户帐户或服务帐户，然后单击**确定**。
4. 单击**下一步**。
5. 选择**创建自定义任务以委派**，然后单击**“下一步”。**
6. 选择**文件夹中的以下对象。**在下列列表中，选中**用户对象**并单击**下一步。**



7. 选中“**常规**”和“**特定属性**”两个复选框。
8. 在“权限”下，选中**读取**scriptPath和**写入**scriptPath复选框，然后单击**下一步**。



9. 单击**“完成”**。

注：该权限仅允许修改登录脚本路径。

查看已删除用户的报告

查看此报告的最低要求是属于**Domain Admins**组成员。

执行 GINA 安装

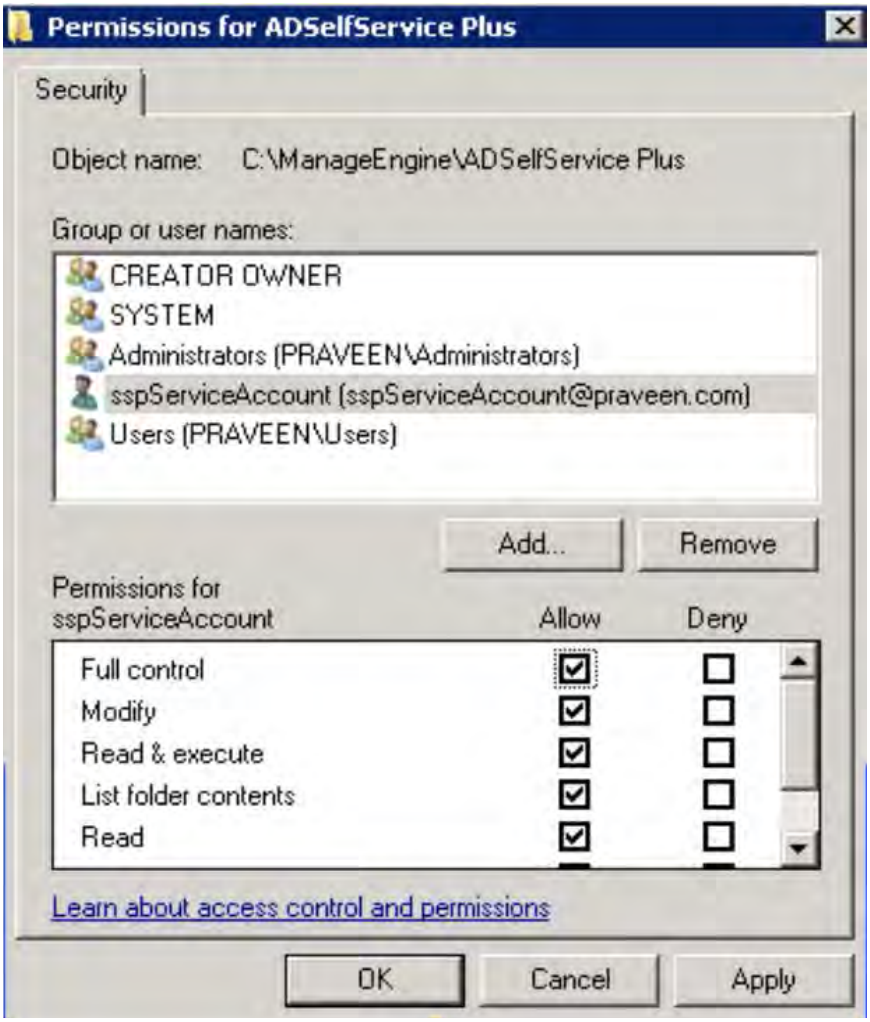
从ADSelfService Plus网页控制台执行GINA安装的最低要求是属于**域管理员**组成员。

若无法使用域管理员凭据，您可通过组策略对象（GPO）或System Center Configuration Manager（SCCM）手动安装GINA。

其他操作的文件夹权限

用于运行ADSelfService Plus的服务账户以及用于启动ADSelfService Plus的本地用户账户，必须被授予对产品安装目录的**完全控制权限**。否则，您将无法执行以下操作:

- 安装服务包
- 生成报告
- 启动产品
- 应用许可证
- 更新仪表板图表
- 备份和恢复数据
- 显示员工照片并为用户提供自我更新选项



配置高可用性

在ADSelfService Plus中配置高可用性所需的最低权限是成为“域管理员”组成员。域管理员权限仅在高可用性初始设置阶段为必需；一旦高可用性配置完成，可根据其他已配置功能将服务账户更改为具有较低权限的账户。请确保两个实例之间的文件夹共享始终 不间断。