


Delegate Moving User, Group and Computer Accounts Between Organizational Units in Active Directory

 learn.microsoft.com/en-us/archive/technet-wiki/20747.delegate-moving-user-group-and-computer-accounts-between-organizational-units-in-active-directory

- Article
- 01/17/2024

This Wiki article shows the permissions needed to delegate moving user, group and computer accounts between Organizational Units in Active Directory.

This is summarized in the following table:

Object	Organizational Unit	Permission Tab	Apply to	Permission
User	Source Organizational Unit	Object	This object and all descendant objects (*)	Delete User objects
		Properties	Descendant User objects	Write Distinguished Name
		Properties	Descendant User objects	Write name (**)
		Properties	Descendant User objects	Write Name (**)
	Destination Organizational Unit	Object	This object and all descendant objects (*)	Create User objects
Group	Source Organizational Unit	Object	This object and all descendant objects (*)	Delete Group objects
		Properties	Descendant Group objects	Write Distinguished Name
		Properties	Descendant Group objects	Write name (**)

		Properties	Descendant Group objects	Write Name (**)
	Destination Organizational Unit	Object	This object and all descendant objects (*)	Create Group objects
Computer	Source Organizational Unit	Object	This object and all descendant objects (*)	Delete Computer objects
		Properties	Descendant Computer objects	Write Distinguished Name
		Properties	Descendant Computer objects	Write name (**)
		Properties	Descendant Computer objects	Write Name (**)
		Object	This object and all descendant objects (*)	Create Computer objects

(*) If you would like to allow moving a user, group or computer object from an Organizational Unit and not its sub-Organizational Units, you can choose **This object only** as the value of **Apply to**.

(**) note that "Write name" (lower case) and "Write Name" (upper case) refer to different property permissions - setting both is required.

****Remark 1:** **In Active Directory Users and Computers administrative tool (dsa.msc), ****distinguishedName** **is a filtered property that is not displayed by default. You might want to use **adsiedit.msc** instead, where the property filters do not apply. Alternatively, you might change the "distinguishedName" property value from 7 (filtered) to 0 (not filtered) in the [computer] [user] and [group] sections of the **dssec.dat** file as described in the following article:

How to Allow the Delegation of Filtered Properties in Active Directory Users and Computers: <http://social.technet.microsoft.com/wiki/contents/articles/20746.how-to-allow-the-delegation-of-filtered-properties-in-active-directory-users-and-computers.aspx>

****Remark 2:** **To be able to delegate only moving user, group or computer objects between Organizational Units with no extra permissions (such as administrator permissions), you can refer to "Using scripts running with service accounts to achieve

administrative tasks" Section in the following article.

Delegation of Administration in Active

Directory: <http://social.technet.microsoft.com/wiki/contents/articles/20292.delegation-of-administration-in-active-directory.aspx>