

Implementing Delegation of Administration

When you sit down to implement delegation of administration, you first need to decide on which actions you want to delegate out. Microsoft continues to add specific tasks for you to easily setup. These tasks are common tasks that most companies need to delegate out, regardless of the size of the organization. The benefit of having this prebuilt list of tasks is that you can mask the actual permissions that need to be set on the OUs.

To understand how the delegation of administration can be set, let's look at a step-by-step on how to establish the delegation of administration that we just looked at for the resetting of passwords. The structure of OUs is shown in Figure 1.

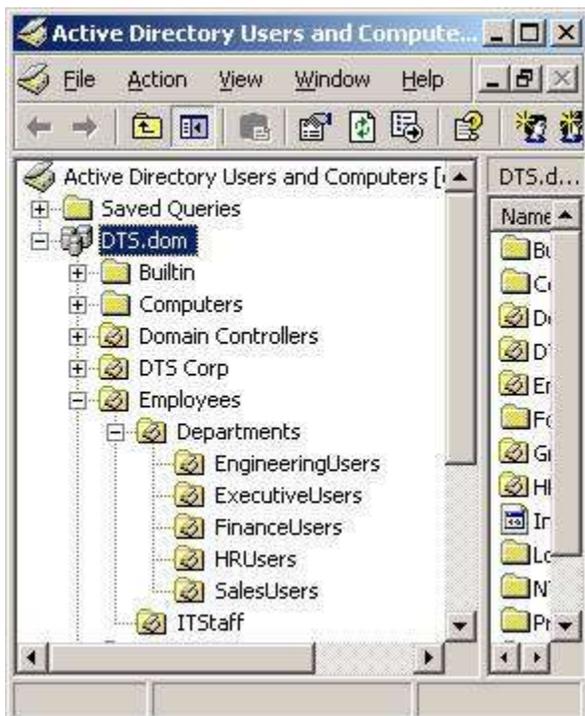


Figure 1: Active Directory structure of organizational units

To establish the delegation of administration for the IT users to reset passwords for all employees in all departments, you need to create a group for this as a best practice. I have created a group named `ITResetPasswords` and placed all of the IT users that need this capability in this group. From here, you need to right click on the `Departments` OU and select the `Delegate Control` menu option, as shown in Figure 2.

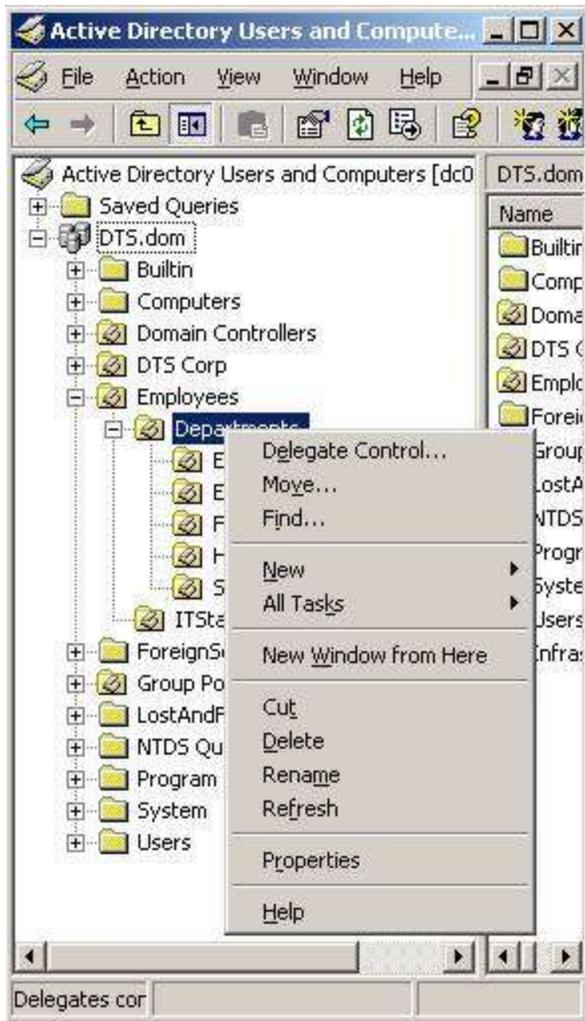


Figure 2: Delegate Control menu option establishes the delegation of administration for that OU

The delegation wizard will ask you the following questions:

1. The group that you want to give the abilities to (see Figure 3)
2. The task that you want to delegate (see Figure 4)

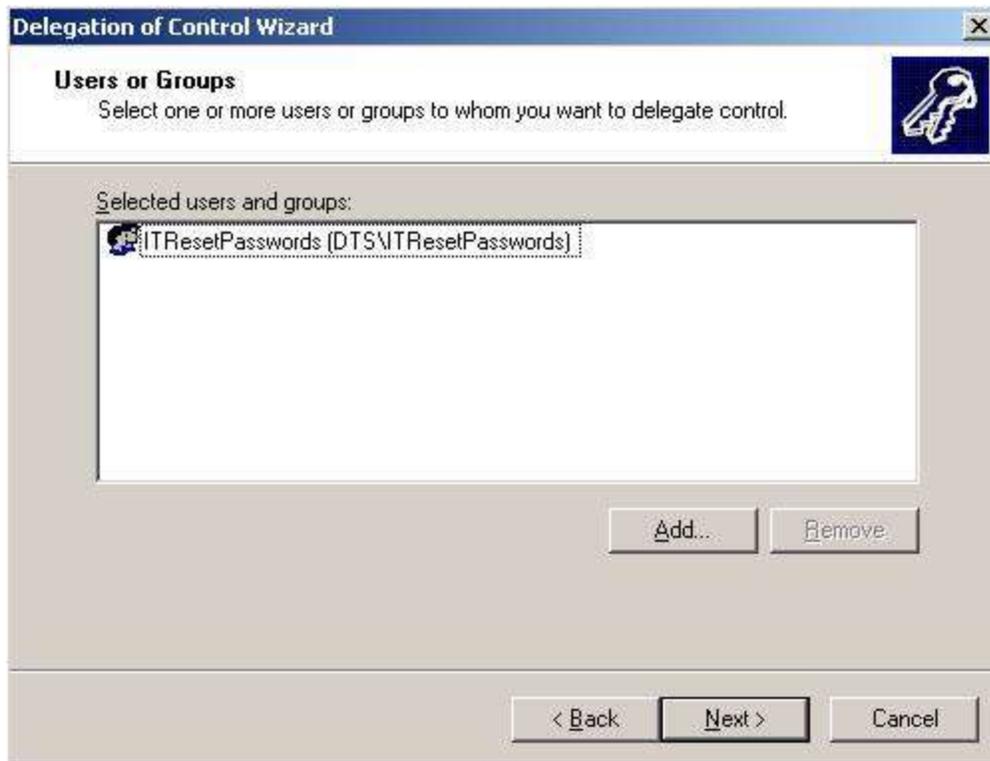


Figure 3: You need to select which groups will have the ability to perform the task

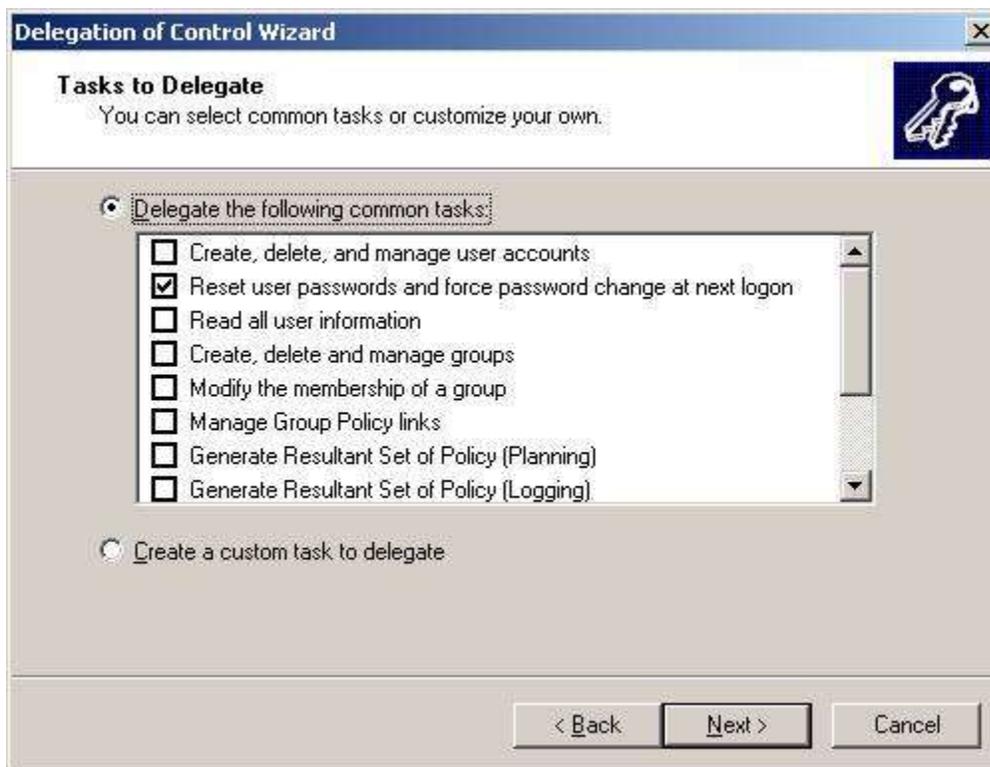


Figure 4: You need to select which tasks the groups will be able to perform

After you select these two options and finish up the wizard, it appears as if nothing really happens. However, what has happened is really quite significant, considering the abundance of permissions that exist for a single OU. There are over 10,000 individual permissions that can be set for a single OU. This one delegation sets only 3 individual permissions, as shown in Figures 5 and 6.

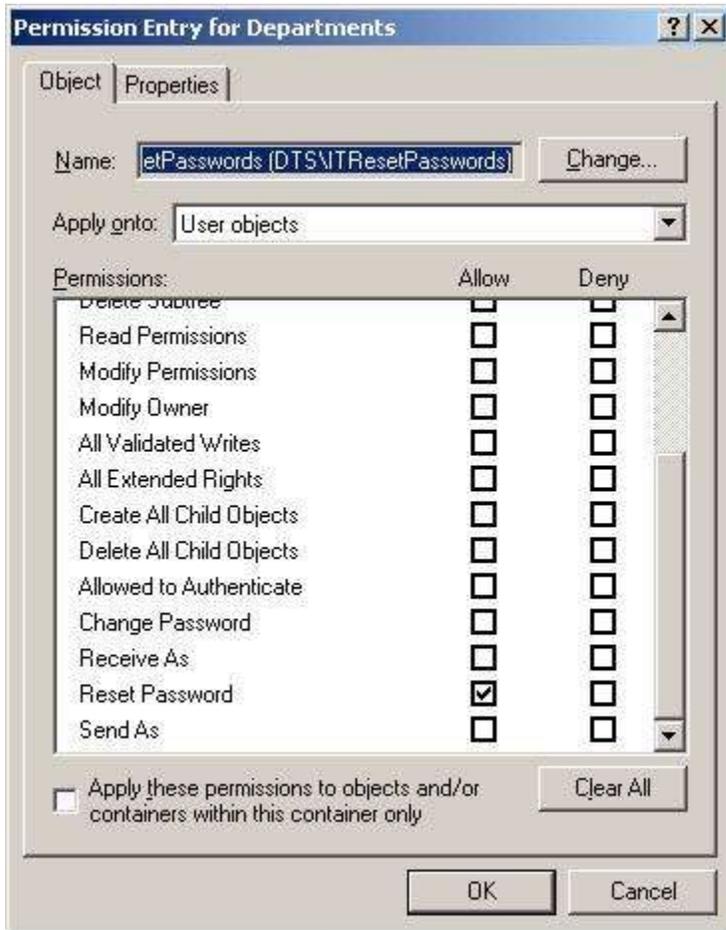


Figure 5: Permissions set to reset password for user accounts under the OU

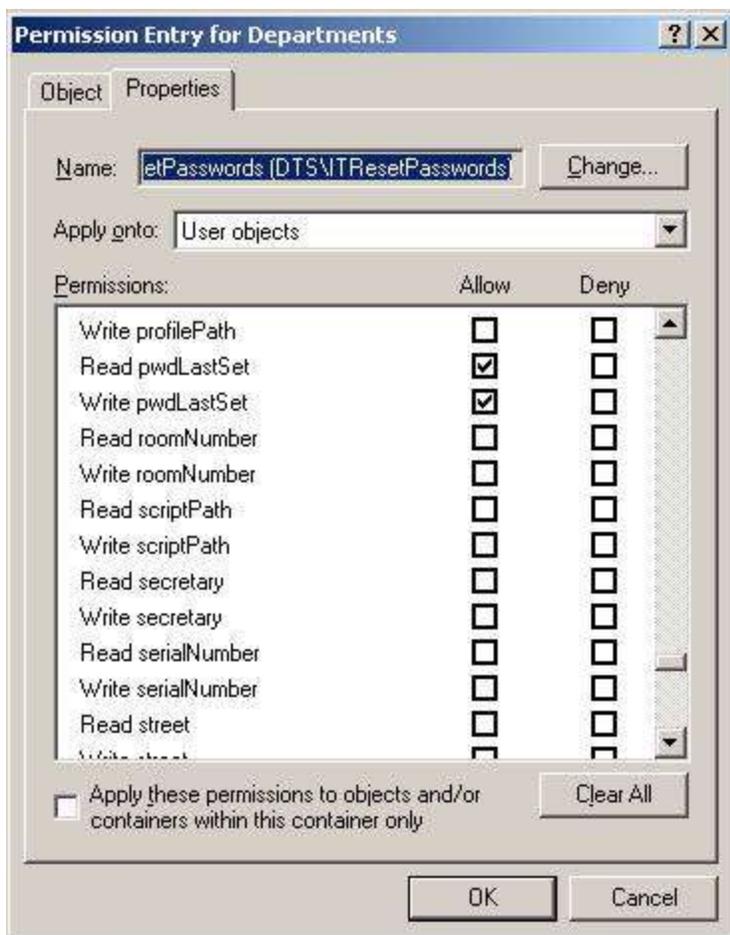


Figure 6: Permissions allowing user to force users to change password next time password is used

You can see by the size of the scroll bars in both Figures above that there are numerous permissions to choose from. The wizard masks this complexity by setting the correct permissions for you.

For you to configure permission for the HRResetPasswords group, which targets only the user accounts in the HRUsers OU, you need to follow the same steps. First, add the appropriate users to the HRResetPasswords group. Second, use the Delegate Control menu option at the HRUsers OU, configuring the group and task that delegates the resetting of passwords. Finally, inform the users in the group that they can now reset passwords for all users in this OU.