ACTIVE DIRECTORY – DELEGATING ADMINISTRATIVE RIGHTS

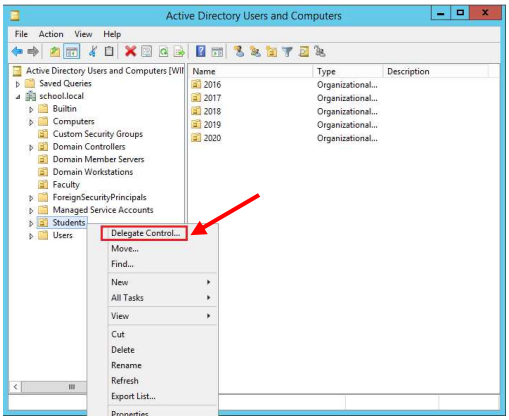
Delegating rights in Active Directory (AD) is critical for many IT organizations'. By delegating administration rights, domain users or groups can be granted permissions they need without adding these domain users to privileged groups (e.g., Domain Admins, Enterprise Admins). The simplest way to accomplish delegation is by using the **Delegation of Control** wizard in **Active Directory Users and Computers** MMC snap-in. This document will discuss a few common delegation permissions commonly used in IT organizations'.

GRANT RIGHTS TO RESET USER PASSWORDS

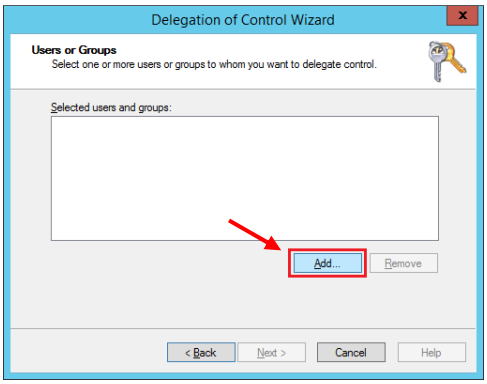
Suppose we want to delegate rights to members of a security group **Password Managers** to be able to reset passwords for users in Students OU in your AD domain. To accomplish this, perform these steps**

*****It is assumed that the security group "Password Managers" already exists***

- Open the **Active Directory Users and Computers** management console
- Right-click on the Organizational Unit (OU) rights to be delegated on e.g. Students and select **Delegate Control.** Click **Next** to advance from the **Welcome** screen.

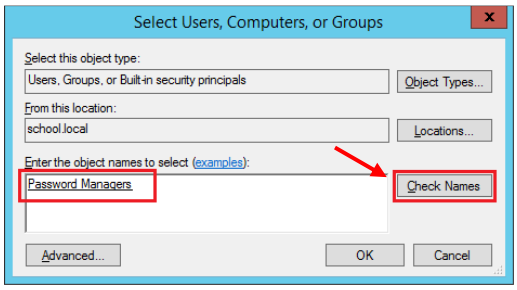


- On the **Users or Groups** screen, click the **Add** button

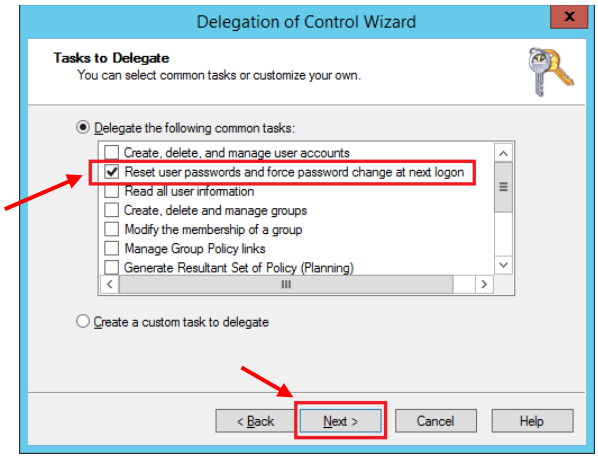


- In the **Select Users, Computer or Groups** dialog box enter the name of the User or Group** that rights need to be delegated to. Click on **Check Names** to make sure the group name was typed correctly and click on **OK.** Once back on the **Users or Groups** screen, click **Next**

  It is recommended to use Security Groups for delegation rather than Domain Users



- On the **Tasks to Delegate** screen, select **Reset users and passwords and force password change at next logon** and click **Next.**



- Verify that all the information is correct on the **Completing the Delegation of control Wizard** screen page and click **Finish** to complete the task

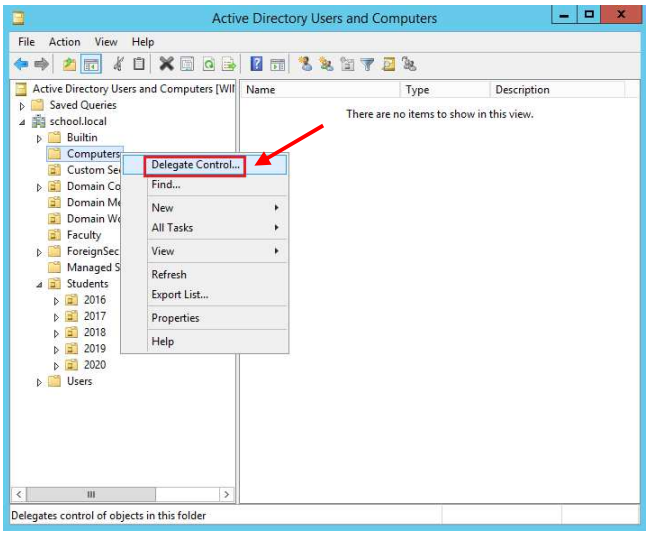
When the Delegation of Control Wizard is completed this will add the requested rights/permissions to the Student OU for security group **Password Managers**. Adding a specific domain user to this security group will give them the permissions to reset passwords for domain users under the Student OU.

GRANT RIGHTS TO JOIN MACHINES TO WINDOWS DOMAIN

Suppose we want to delegate rights to members of a security group **Domain Membership Managers** to be able to join machines to Active Directory domain. To accomplish this, perform these steps**

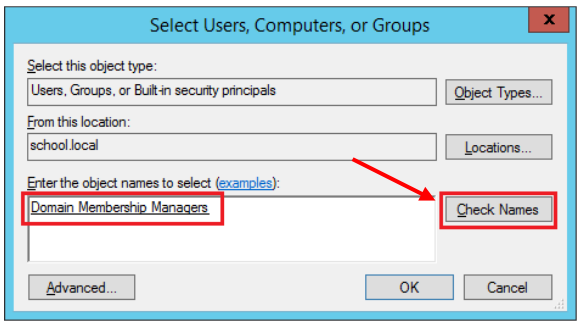
It is assumed that the security group "Domain Membership Managers" already exists

- Open the **Active Directory Users and Computers** management console
- Right-click on the Container or Organizational Unit (OU) rights need to be delegated on e.g. Computers and select **Delegate Control.** Click **Next** to advance from the **Welcome** screen.

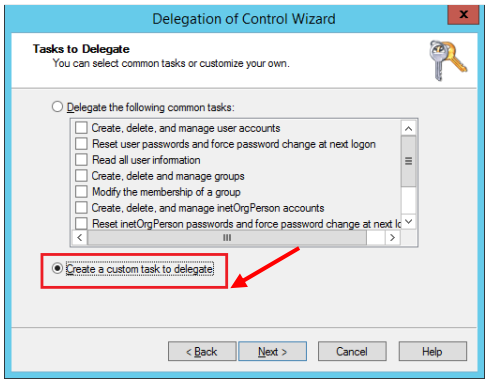


- On the **Users or Groups** screen, click the **Add** button
- In the **Select Users, Computer or Groups** dialog box enter the name of the User or Group** that rights need to be delegated to. Click on **Check Names** to make sure the group name was typed correctly and click on **OK.** Once back on the **Users or Groups** screen, click **Next**

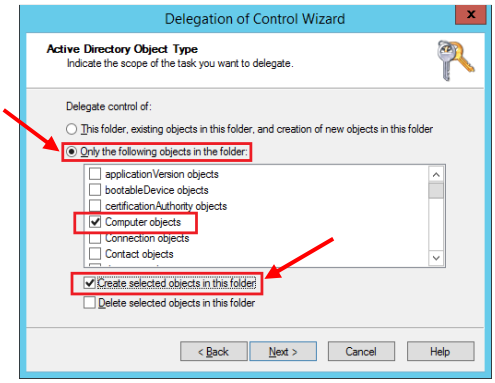
It is recommended to use Security Groups for delegation rather than Domain Users



- On the **Tasks to Delegate** screen, select **Create Custom task to delegate** and click **Next.**

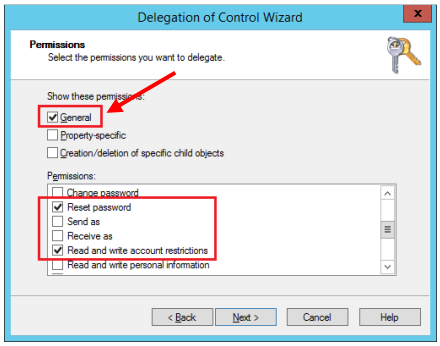


- On the **Active Directory Object type** screen, select **Only the following objects in folder** and check the box for **Computer Objects**. Also, check the box for **Create selected objects in this folder** and click **Next**



- On the **Permissions** screen, check the boxes for the following options:

  - Reset Password
  - Read and write account restrictions
  - Validate write to DNS hostname
  - Validate write to service principal name



- Once the options have been selected, click **Next**
- Verify that all the information is correct on the **Completing the Delegation of control Wizard** screen page and click **Finish** to complete the task

When the Delegation of Control Wizard is completed this will add the requested rights/permissions to the Computer container for security group **Domain Membership Managers**. Adding a specific domain user to this security group will give them the permissions to join unlimited machines to the domain.