# 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.

Acti	ve Directory Users	and Computers		
File Action View Help				
🕨 🔿 🙍 🚮 🔏 🗋 💥 🖾 🙆	🛛 📰   🖏 🐂	i 🔻 🖸 🕏		
<ul> <li>Achie Directory Users and Computers [WII</li> <li>Sered Ouesand Computers [WII</li> <li>Sered Ouesand Computers [WII</li> <li>Sered Ouesand Computers</li> <li>Computers</li> <li>Computers</li> <li>Computers</li> <li>Domain Centroflers</li> <li>Domain Centroflers</li> <li>Domain Member Servers</li> <li>Domain Member Servers</li> <li>Domain Centroflers</li> <li>Faculty</li> <li>FreighSexuity Principals</li> <li>Manage Service Accounts</li> <li>Users</li> <li>Users</li> <li>Users</li> <li>View</li> <li>Cut</li> <li>Delete Rename</li> <li>Rename</li> <li>Expert Link.</li> </ul>	None 2016 2017 2019 2019 2019 2020 2020	Type Organizational Organizational Organizational Organizational Organizational	Description	

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

Delegation of Control Wizard
Users or Groups Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
< Back Next > Cancel Help

- 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

Select Users, Computers, or Groups	x
Select this object type:	
Users, Groups, or Built-in security principals From this location:	Object Types
school.local	Locations
Enter the object names to select (examples):	Check Names
	Gilcolt Hallos
Advanced OK	Cancel

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

	_
Tasks to Delegate You can select common tasks or customize your own.	<b>\$</b>
Delegate the following common tasks:	
Greate a custom task to delegate	

- 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.

نه 🖻 🖄 🔿		1 1 1 1	2 🖬 🔻 🧧 🎗	
Active Directory Users	and Computers [WI	Name	Type There are no items to sh	Description ow in this view.
Computers Custom Se Domain Co Domain Me New		•		
All Tasks     All Tasks	*			
<ul> <li>▶ 2019</li> <li>▶ 2020</li> <li>▶ 2020</li> <li>▶ 2020</li> </ul>	Help			

- 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

Select Users, Computers, or Grou	x zqu
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
school.local	Locations
Enter the object names to select ( <u>examples</u> ):	
Domain Membership Managers	Check Names
O	OK Cancel

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

Delegation of Control Wizard	x
Tasks to Delegate You can select common tasks or customize your own.	R
Delegate the following common tasks:     Create, delete, and manage user accounts     Reset user passwords and force password change at next logon     Reset al user information     Create, delete and manage infOrOPerson accounts     Orate, delete, and manage infOrOPerson accounts     Reset inetOrgPerson passwords and force password change at next K     III      Create a custom task to delegate	
< Back Next > Cancel	Help

- 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

Delegation of Control Wizard	x
Active Directory Object Type Indicate the scope of the task you want to delegate.	P
Delegate control of:	folder
application/Version objects     bostableDevice objects     cetificationAuthorty objects     Computer objects     Computer objects     Contract objects     Critact objects     @Create selected objects in this folder	× *
< Back Next > Cancel	Help

- 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

Delegation of Control Wizard	x
Permissions Select the permissions you want to delegate.	P
Show these pergresses Show these pergresses Depending second Specific child objects Permissions	
Change baseword     Gene baseword     Send as     Gene baseword     Send as     Gene baseword     Read work account restrictore     Fead and write personal information	
< Back Next > Cancel	Help

- 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

	Delegation of Control Wizard	×
R.	Completing the Delegation of Control Wizard         You have successfully completed the Delegation of Control wizard.         You chose to delegate control of objects in the following Active Directory folder:         school local/Computers         The groups, users, or computers to which you have given control are:         Domain Membership Managers (SCHOOL\Domain Mer	
	They have the following permissions:	

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.