Delegation & Least Privilege

1. Introduction

Delegation of control in Active Directory allows administrators to assign specific tasks—such as resetting user passwords or modifying group memberships—to non-administrative users or groups. This reduces reliance on highly privileged accounts and ensures day-to-day operations are manageable by frontline teams like Helpdesk. Delegating only what is necessary not only streamlines IT operations but also improves accountability and auditing.

The principle of least privilege is central to organizational security. Granting users only the minimum rights needed to perform their duties helps prevent accidental or intentional misuse of access. In this task, we focus on securely delegating password reset capabilities and performing a privilege cleanup within the Domain Admins group to ensure a minimal and justifiable use of elevated permissions.

2. Objective

This task aims to reinforce the organization's Active Directory security by operationalizing two fundamental principles: **delegation of control** and the **principle of least privilege**. The goal is to ensure that administrative capabilities are distributed only to those who require them, reducing both the risk of insider threats and the impact of potential account compromises.

By delegating the "Reset Password" permission specifically to the Helpdesk group, we aim to improve helpdesk efficiency while avoiding unnecessary exposure of full administrative rights. This approach allows day-to-day support tasks to be handled quickly, without compromising the integrity of the domain's privileged accounts.

Additionally, reviewing and cleaning up the "Domain Admins" group helps enforce tighter control over the environment. This includes removing users who were granted elevated privileges unnecessarily, thus eliminating potential vectors for privilege abuse, lateral movement, or privilege escalation attacks. Overall, the objective is to create a well-structured access model that aligns with security best practices and supports maintainable, role-based access management.

Key goals include:

- **Delegate Specific Permissions to Helpdesk**
  By delegating only the "Reset Password" permission to the Helpdesk group, we enable them to perform necessary support tasks without granting broader administrative access. This reduces the risk of misuse while improving operational efficiency. The goal is to ensure that Helpdesk members can perform their duties without impacting security.

- **Minimize Domain Admin Membership**
  Reducing the number of users in the "Domain Admins" group is essential for maintaining tight control over privileged access. Limiting membership ensures that only trusted personnel have domain-wide control, reducing security risks. This helps prevent accidental misuse and minimizes the attack surface.

- **Enforce Least Privilege Principle**
  Applying the least privilege principle restricts users and groups to only the permissions necessary for their specific tasks. This minimizes the risk of privilege escalation and access to sensitive data. Ensuring that only required permissions are granted enhances security by limiting unnecessary access.

- **Test Delegated Rights in Real Scenarios**
  After delegating the "Reset Password" rights, testing ensures that the Helpdesk group can perform password resets without additional permissions. This helps confirm that the delegation was correctly implemented and is functioning as intended. Verifying this step ensures no security loopholes exist.

- **Maintain Role-Based Access Clarity**
  Maintaining clear, documented roles for users ensures that only the appropriate individuals have access to certain resources. This simplifies administration and reduces errors. A well-defined role structure helps manage access efficiently while aligning with security policies

3. Methodology

The methodology for implementing **Delegation and Least Privilege** follows a structured approach to ensure proper delegation of administrative tasks while maintaining security and minimizing the risk of privilege abuse. The process begins with enabling advanced features within Active Directory to access the necessary controls for delegation. We then proceed with delegating specific permissions to the Helpdesk group, ensuring they have the ability to reset passwords without granting broader administrative access.

The next steps involve verifying that the delegated permissions work effectively by testing the ability of Helpdesk users to reset passwords. Finally, the methodology includes a review of the **Domain Admins** group to remove unnecessary privileged accounts, ensuring that only authorized users retain elevated permissions. By following this methodology, we maintain a secure and manageable environment while adhering to the principle of least privilege.

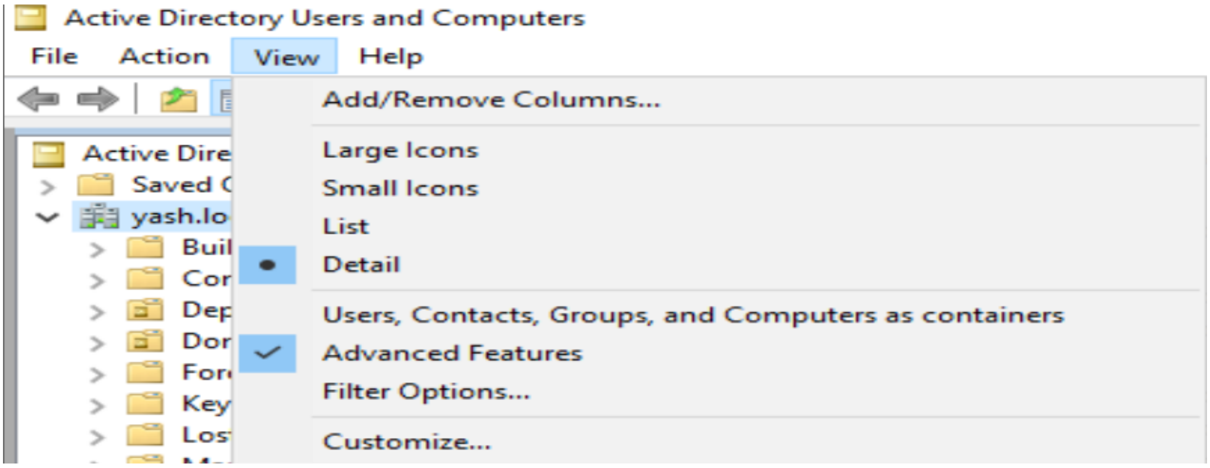
3.1 Enabling Advanced Features & Delegation Control

In this phase, we begin by enabling the **Advanced Features** in Active Directory Users and Computers (ADUC) to access additional options needed for delegation. This step is crucial as it ensures we have all necessary controls and features to manage permissions effectively. Following that, we proceed with **Delegation Control** by selecting the "Helpdesk" group and delegating the "Reset Password" permission. This allows the Helpdesk team to perform specific tasks without granting them full administrative privileges.

Navigation Path:
ADUC → View → Advanced Features → Right-click on Helpdesk group → Delegate Control

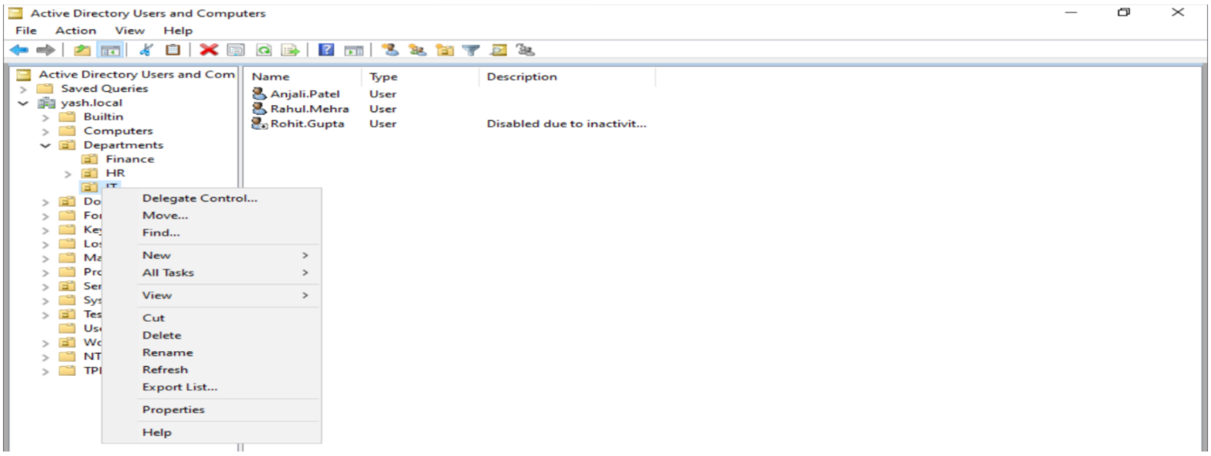
- **Enable Advanced Features**
  Open Active Directory Users and Computers (ADUC) and enable **Advanced Features** to access additional options necessary for delegation control.

(Enabling these features ensures you can manage permissions at a more granular level and delegate control effectively.)



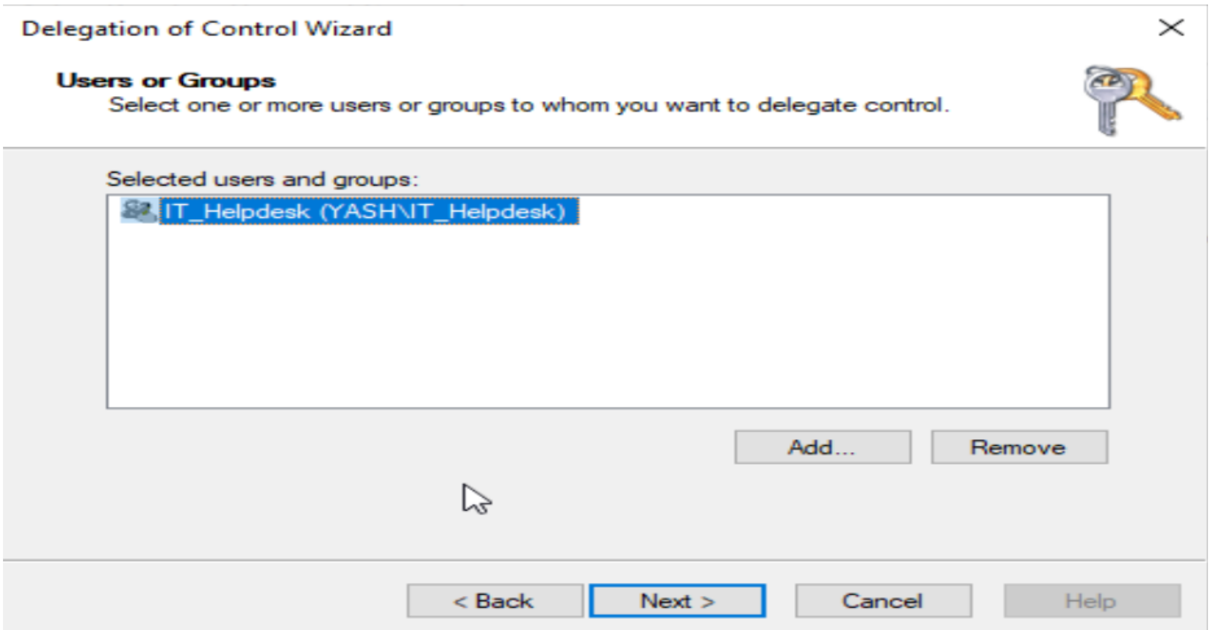
- **Delegate Control to Helpdesk Group**
  Right-click on the Helpdesk group in ADUC and select Delegate Control. This will allow you to assign specific permissions to the Helpdesk team for tasks such as resetting passwords.

  (Open "Delegate Control Wizard".)



Name	Type	Description
Anjali.Patel	User	
Rahul.Mehra	User	
Rohit.Gupta	User	Disabled due to inactivit...

("Delegate Control Wizard" window showing Helpdesk group selection.)



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:
IT_Helpdesk (YASH\IT_Helpdesk)

3.2 Delegating Password Reset Permissions and Verifying Login

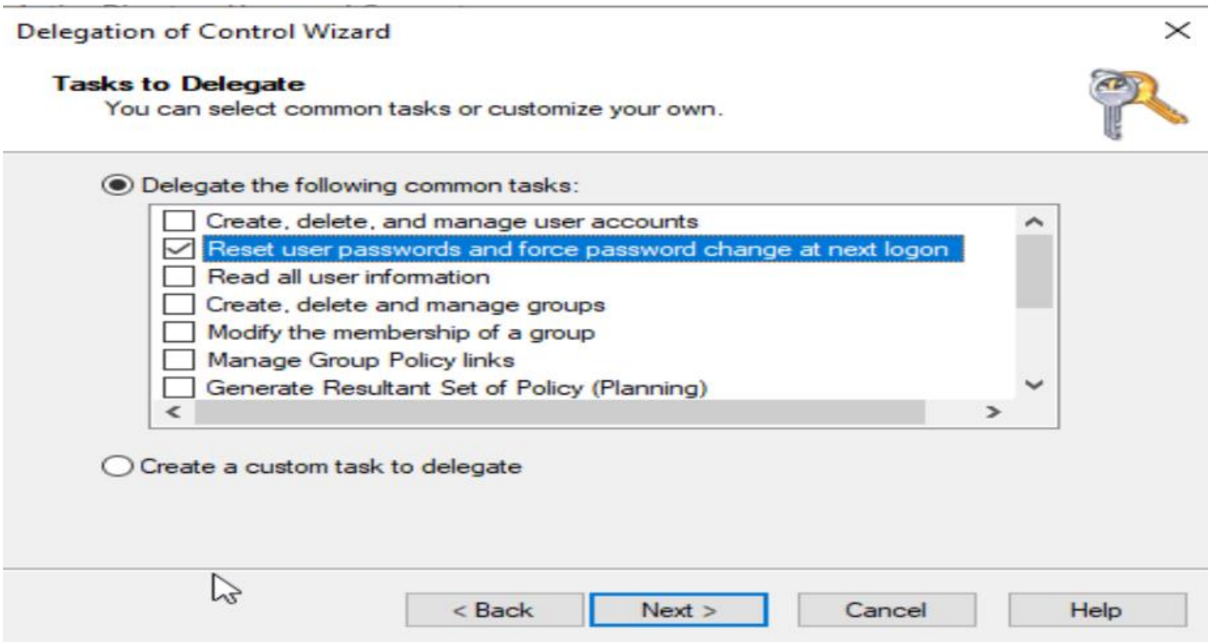
Once delegation is configured, we enable the **Reset User Password** and **Change Password at Next Logon** options to ensure that Helpdesk users can reset passwords securely and require the user to change their password after a reset. This phase is followed by verifying that the delegated permissions work correctly. We test this by logging into a user account within the Helpdesk group and confirming that they can reset passwords as intended without encountering any issues.

Navigation Path:

ADUC → Helpdesk Group → Properties → Delegate Control → Select Permissions → Reset Password

- **Enable Reset User Password & Change Password at Next Logon**
  Enable the **Reset User Password** and **Change Password at Next Logon** options to ensure that Helpdesk users can reset user passwords and force users to change their passwords upon the next login.

(Enabling this ensures that Helpdesk members can complete password resets without any additional permissions. The "Change Password at Next Logon" setting adds an extra layer of security.)



Delegation of Control Wizard

Tasks to Delegate

You can select common tasks or customize your own.

● Delegate the following common tasks:

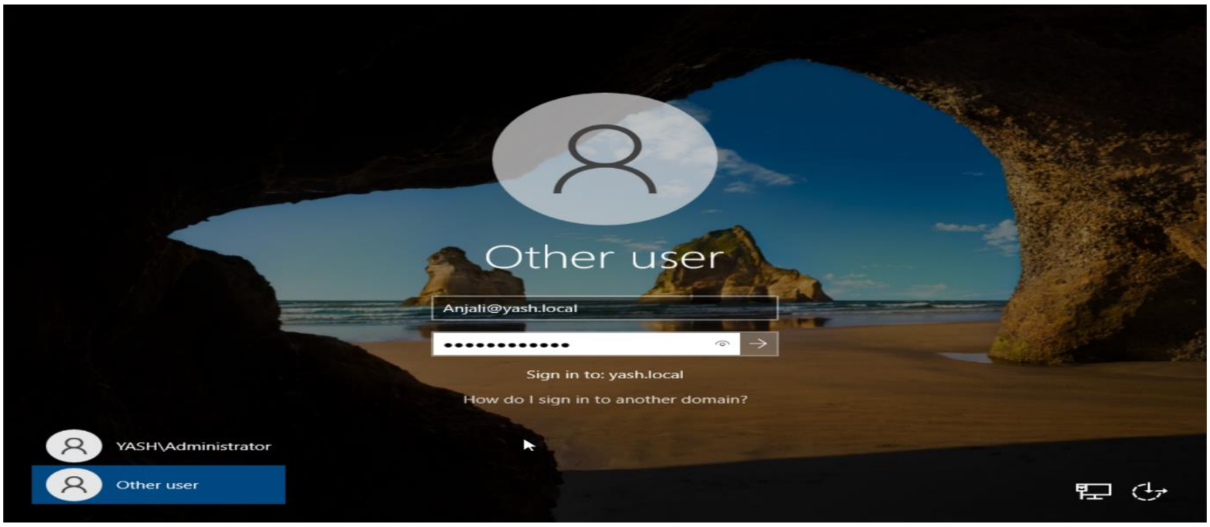
- □ Create, delete, and manage user accounts
- ☑ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

- **Verify Permissions by Testing Login**

  Log in with a user account that belongs to the Helpdesk group and verify that the delegated permissions are working as intended. Ensure the Helpdesk can reset passwords and enforce password changes without issues.

  (Try login.)

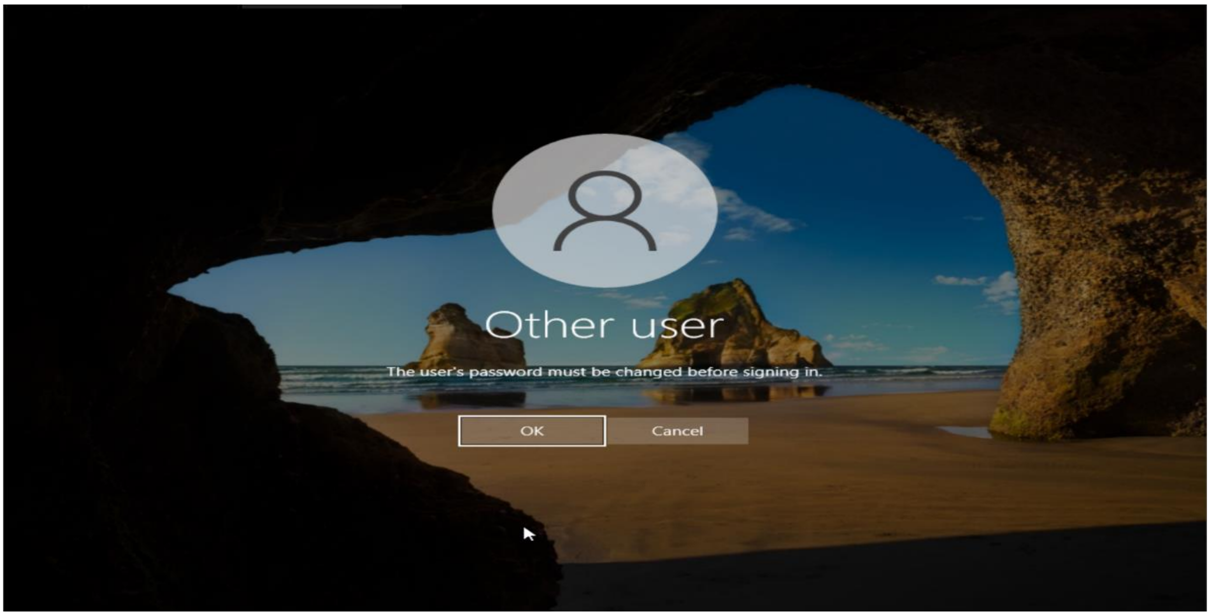


Other user

Anjali@yash.local

•••••••••••••

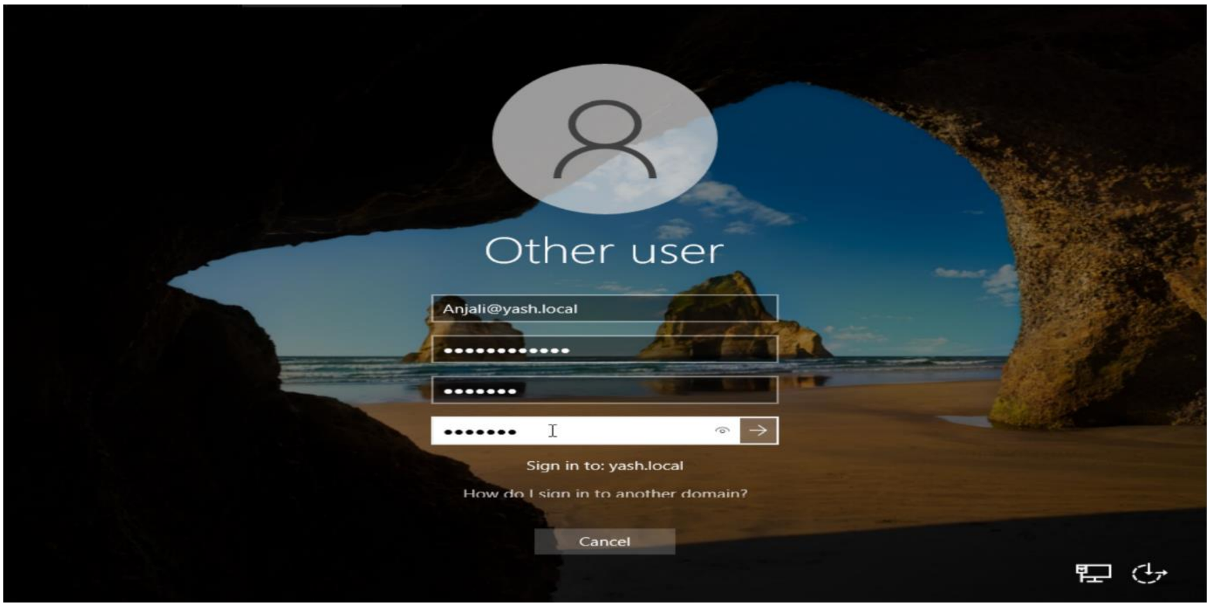
Sign in to: yash.local



Other user

The user's password must be changed before signing in.

(Changing password.)



Other user

Anjali@yash.local

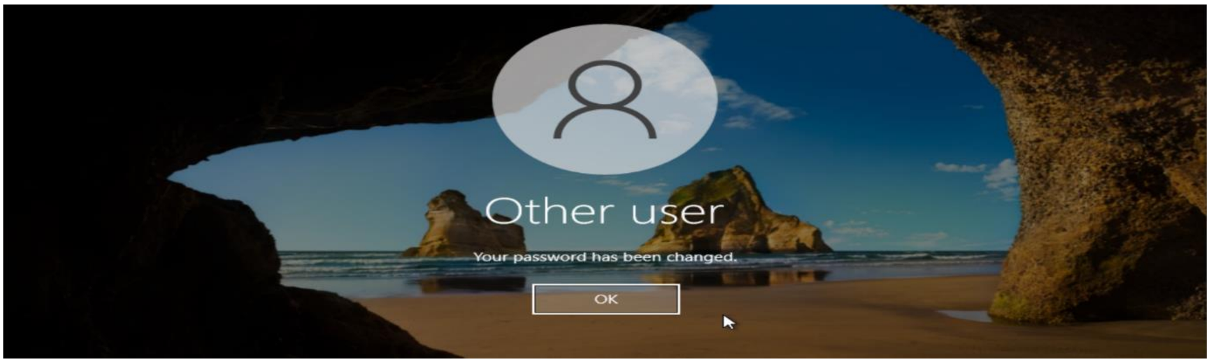
•••••••••••••

••••••••

•••••••

Sign in to: yash.local

How do I sign in to another domain?



Other user

Your password has been changed.

3.3 Reviewing Domain Admin Group & Removing Unnecessary Accounts

In this phase, we examine the **Domain Admins** group properties and review its membership to ensure only necessary users are included. This is a crucial step in enforcing the principle of least privilege. After auditing, we proceed to **remove unnecessary accounts** from the Domain Admins group, thereby reducing the number of privileged accounts and enhancing security.

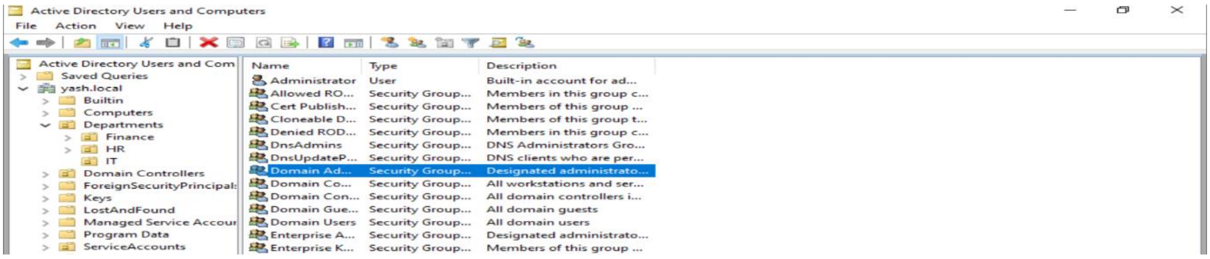
Navigation Path:

ADUC → Domain Admins Group → Properties → Members → Remove Unnecessary Accounts

- **Review Domain Admins Group Membership**

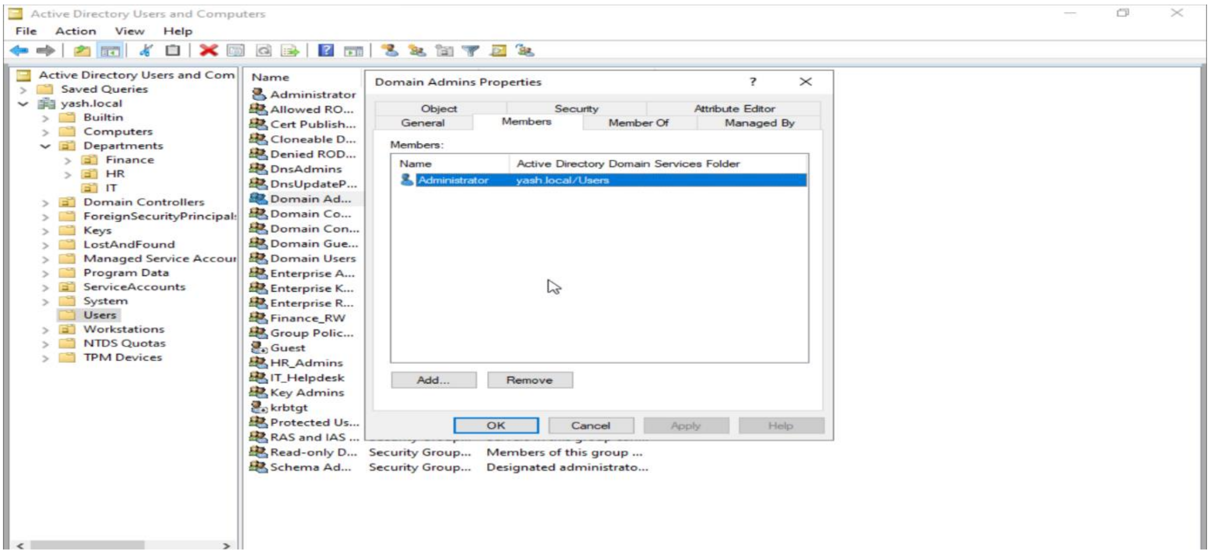
  Open the properties of the **Domain Admins** group and review its membership. Identify and audit any users who have been assigned elevated privileges unnecessarily.

  (Reviewing this group helps ensure that only trusted users with a legitimate need have access to critical system-wide administrative permissions.)



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...

  (After removing Unnecessary accounts)



Members:

Name	Active Directory Domain Services Folder
Administrator	yash.local/Users

4. Results And Findings

This section summarizes the outcome of implementing delegation and least privilege within the Active Directory environment. It highlights the successful delegation of password reset rights, validation of those permissions, and cleanup of privileged accounts.

- **Advanced Features Successfully Enabled**
  ADUC was configured to show advanced features, allowing detailed permission management and access to critical delegation options.

- **Helpdesk Group Delegated Password Reset Rights**
  The Helpdesk group was successfully assigned the ability to reset user passwords and enforce password changes at next login.

- **Delegated Rights Verified Through Testing**
  Helpdesk users were able to reset a test user's password without elevated admin access, confirming that the delegation worked as intended.

- **Domain Admin Group Audited**
  Membership of the Domain Admins group was reviewed and several unnecessary accounts were identified.
- **Unnecessary Privileged Accounts Removed**
  Redundant users were removed from the Domain Admins group, minimizing the attack surface and aligning with security best practices.

5. Recommendations

Based on the implementation and results, the following recommendations are made to enhance security and maintain a proper access control model across the domain.

- **Regularly Audit Privileged Groups**

  Periodic audits of privileged groups like "Domain Admins" are crucial to maintaining a secure AD environment. These audits help identify unauthorized accounts, inactive users, or legacy admin accounts that no longer require elevated access. This minimizes potential attack vectors and supports compliance with security best practices.

- **Use Role-Based Access Control (RBAC)**

  Implementing RBAC ensures users are only granted permissions necessary for their job roles. By assigning permissions based on roles (e.g., Helpdesk, Network Admin, Auditor), it becomes easier to manage access control and prevents privilege escalation. RBAC also simplifies onboarding and offboarding processes.

- **Automate Delegation Reviews**

  Delegated permissions should be continuously monitored using PowerShell scripts or third-party tools. Automated reviews can quickly detect when delegation deviates from the intended policy, such as newly assigned permissions or accounts gaining unintended rights. This reduces manual effort and improves security oversight.

- **Provide Helpdesk Training**

  Helpdesk users with delegated rights must be properly trained on secure practices, especially when handling password resets. Training should include recognizing social engineering attempts, verifying user identity before resetting passwords, and understanding the scope of their delegated authority to prevent accidental misuse.

- **Document Delegation Policies**

  Maintain clear and updated documentation that outlines who has delegated access, what actions they can perform, and the reasons for that delegation. This ensures transparency, aids in future audits, and helps in quickly responding to incidents or changes in organizational roles.

6. Conclusion

The completion of this task demonstrated the effective application of the principle of least privilege within a domain environment. By delegating specific administrative rights—such as password reset permissions—to non-privileged groups like Helpdesk, we were able to streamline user support operations while maintaining strong access control boundaries. This not only reduced the dependency on Domain Admins for routine tasks but also lowered the overall security risk by limiting elevated access.

Testing validated that the delegated permissions functioned as expected, confirming that Helpdesk users could reset passwords without being granted full administrative access. Moreover, auditing the Domain Admins group allowed us to identify and remove unnecessary or outdated accounts, thereby strengthening the security posture of the environment. The steps followed in this implementation align with industry best practices, emphasizing regular audits, role-based access control, and clear delegation policies.

In conclusion, this task highlights how carefully planned and tested delegation can balance security and efficiency. It reinforces that a secure Active Directory setup is not just about enforcing restrictions but about intelligently distributing access where it is truly needed. Moving forward, these changes should be routinely reviewed, documented, and refined to ensure the environment remains both secure and functional.