Report: Fine-Grained Password Policies

1. Introduction

Fine-Grained Password Policies (FGPPs) provide a flexible and secure approach to managing password requirements in a Windows Server environment. Unlike the Default Domain Policy, which applies universally to all users in the domain, FGPPs allow administrators to create Password Settings Objects (PSOs) and apply them to specific users or groups. This capability is essential in organizations where different roles demand varying levels of security.

In this task, the focus is on applying a stricter password policy exclusively to the Domain Admins group without impacting regular users. This aligns with the principle of least privilege and helps ensure that privileged accounts are protected with enhanced controls such as longer minimum password lengths, complexity requirements, and shorter maximum password ages. The goal is to minimize the risk of account compromise for sensitive roles by enforcing stronger authentication measures.

2. Objective

The key objective of this task is to strengthen the security of privileged accounts—specifically members of the **Domain Admins** group—by implementing a **Fine-Grained Password Policy** using a **Password Settings Object (PSO)**. Unlike the default domain password policy, which applies uniformly across all users, this task aims to apply more stringent password requirements such as increased minimum length, greater complexity, and shorter password lifespan only to accounts that require higher protection. This targeted approach helps mitigate the risk of credential theft and privilege escalation.

Another important objective is to validate the **correct scope and functionality** of the PSO. By assigning it to the Domain Admins group and testing password creation or modification on both administrative and standard accounts, we can confirm that the stricter rules are enforced as expected. The results of this task will serve to highlight how FGPPs allow organizations to

segregate password policies based on roles and responsibilities, leading to better compliance with organizational security policies and industry best practices. Ultimately, this exercise demonstrates the importance of **customizable, risk-based security controls** in Active Directory environments.

Key goals include:

- Enhance Password Security for Privileged Accounts
  The primary goal is to enforce stricter password policies for Domain Admins through a PSO. Stronger settings like increased minimum length, complexity, and shorter expiry reduce the risk of password-based attacks on high-privilege accounts.

- Implement Role-Based Policy Segregation
  By using FGPPs, password requirements can be customized for different roles or groups within the domain. This allows administrators to apply stronger controls to sensitive accounts without burdening regular users.

- Verify Correct PSO Application
  A key goal is to ensure the PSO applies only to the Domain Admins group and not to unintended users. Testing and validation confirm that the policy targets are scoped correctly and that it overrides the default domain policy as intended.

- Demonstrate Policy Enforcement in Practice
  The task involves testing password change scenarios to prove that the stricter settings are enforced for Domain Admins. Comparing behavior with standard users helps validate that the PSO is operational and functional.

- Improve AD Security Posture Through Granular Control
  Using PSOs provides better control and flexibility in managing account security, helping organizations meet compliance standards. This goal supports a layered security approach by tailoring defenses to the level of risk associated with each user role.

3. Methodology

The implementation of Fine-Grained Password Policies (FGPPs) was carried out using the **Active Directory Administrative Center (ADAC)** and targeted specifically at securing administrative accounts. The methodology is divided into three distinct phases to ensure clarity in configuration, application, and testing.

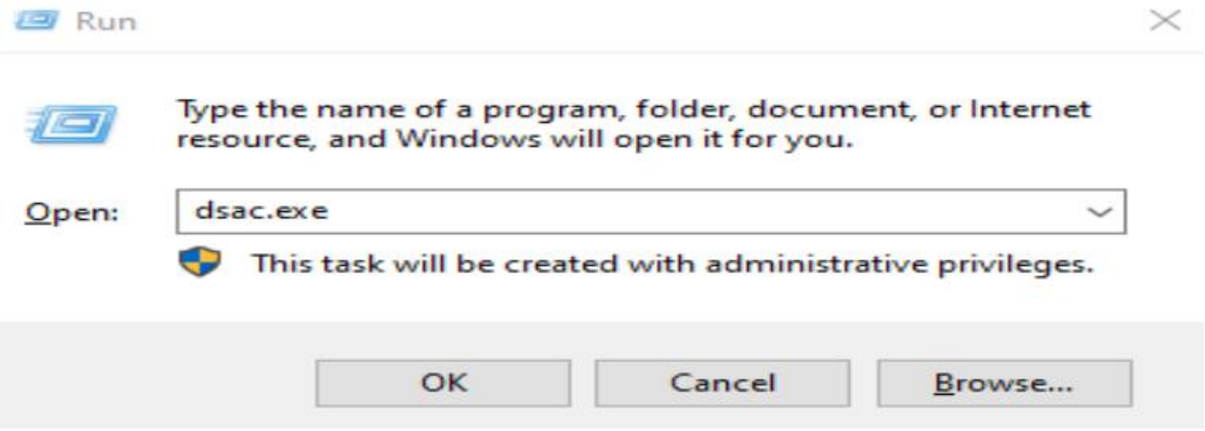
3.1 Accessing the Password Policy Management Interface

This initial phase involves launching the management console required for creating and applying FGPPs. The Active Directory Administrative Center provides a graphical interface to manage Password Settings Objects (PSOs).

- **Open Active Directory Administrative Center (ADAC)**

  We begin by launching ADAC from running dsac.exe. This tool allows the creation and assignment of FGPPs.

  (This screenshot should show the ADAC window open on the desktop)



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dsac.exe

This task will be created with administrative privileges.

Active Directory
ADMINISTRATIVE CENTER

© Microsoft Corporation. All rights reserved.

3.2 Creating and Applying the PSO

In this phase, we define the stricter password settings under a new PSO and apply it to the Domain Admins group, ensuring only privileged accounts are affected.

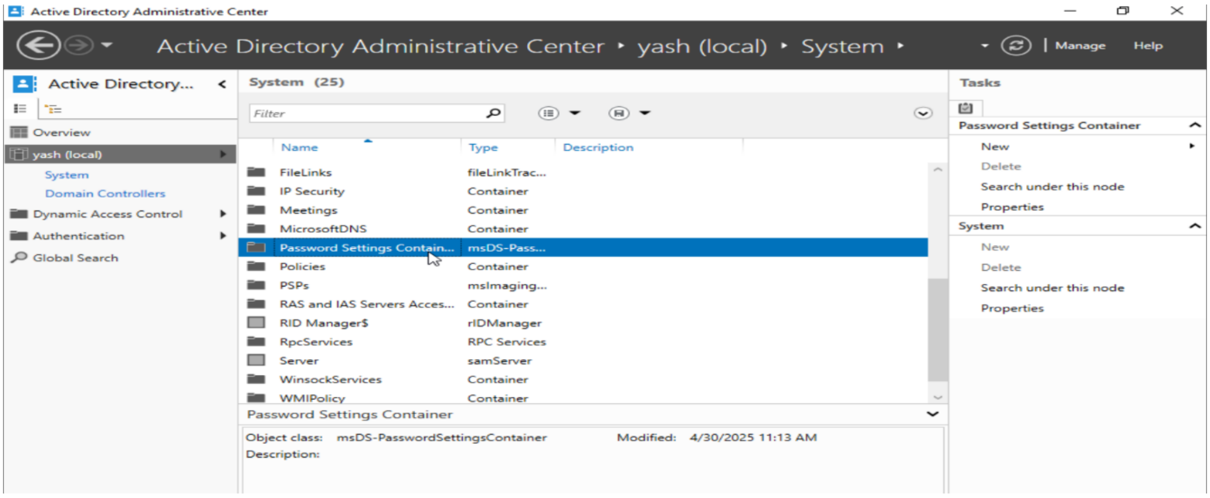
- **Create Password Setting: AdminStrictPolicy**

  In ADAC, navigate to:

  → System → Password Settings Container → New → Password Settings

  We define a new PSO named AdminStrictPolicy with tighter password rules.

  (This screenshot shows Password Settings Conatainer.)



System (25)

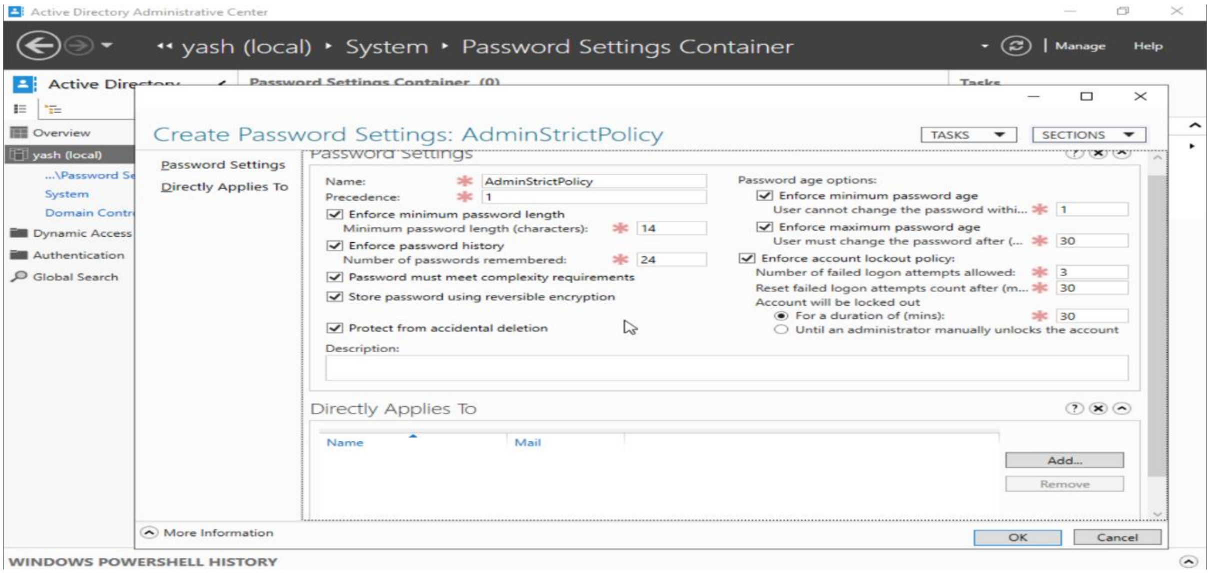
Name	Type	Description
FileLinks	fileLinkTrac...	
IP Security	Container	
Meetings	Container	
MicrosoftDNS	Container	
Password Settings Contain...	msDS-Pass...	
Policies	Container	
PSPs	msImaging...	
RAS and IAS Servers Acces...	Container	
RID Manager$	rIDManager	
RpcServices	RPC Services	
Server	samServer	
WinsockServices	Container	
WMIPolicy	Container	

Password Settings Container

Object class: msDS-PasswordSettingsContainer Modified: 4/30/2025 11:13 AM

Description:

(Creation of new password policy.)



Create Password Settings: AdminStrictPolicy

Password Settings

Name: AdminStrictPolicy

Precedence: 1

☑ Enforce minimum password length

Minimum password length (characters): 14

☑ Enforce password history

Number of passwords remembered: 24

☑ Password must meet complexity requirements

☑ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

Password age options:

☑ Enforce minimum password age

User cannot change the password withi... 1

☑ Enforce maximum password age

User must change the password after (... 30

☑ Enforce account lockout policy:

Number of failed logon attempts allowed: 3

Reset failed logon attempts count after (m... 30

Account will be locked out

● For a duration of (mins): 30

○ Until an administrator manually unlocks the account

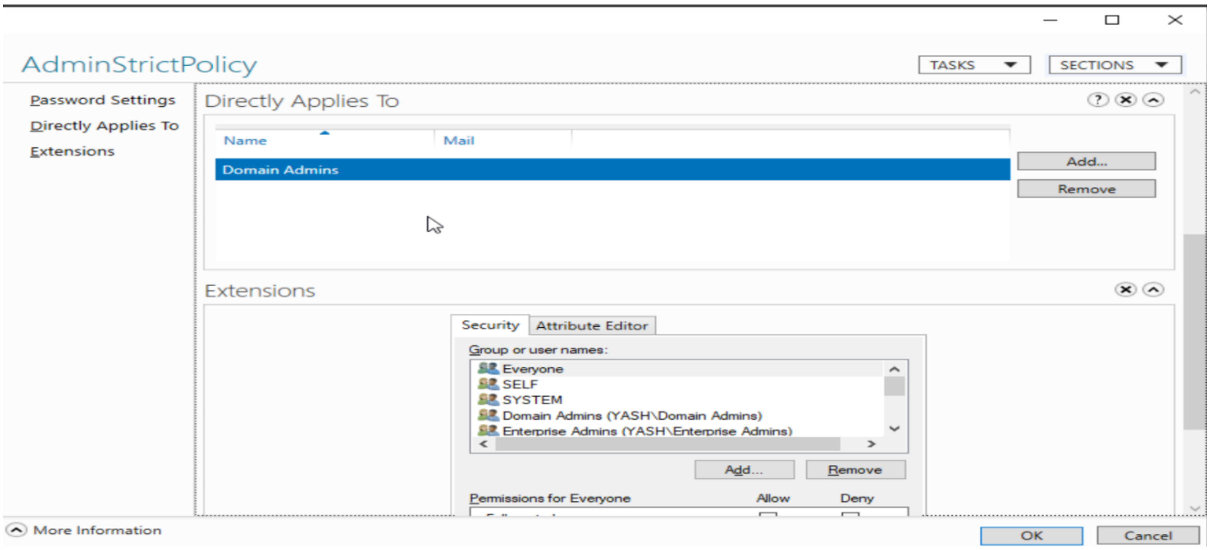
Directly Applies To

Name	Mail

- **Apply PSO to Domain Admin Group**

  Under the “Directly Applies To” field in the AdminStrictPolicy settings, we assign the **Domain Admins** group. This ensures the stricter policy is only enforced for high-privilege accounts.

  (This screenshot should show the completed PSO with the “Directly Applies To” field open, displaying that the Domain Admins group has been added.)



Domain Admins

Everyone
SELF
SYSTEM
Domain Admins (YASH\Domain Admins)
Enterprise Admins (YASH\Enterprise Admins)

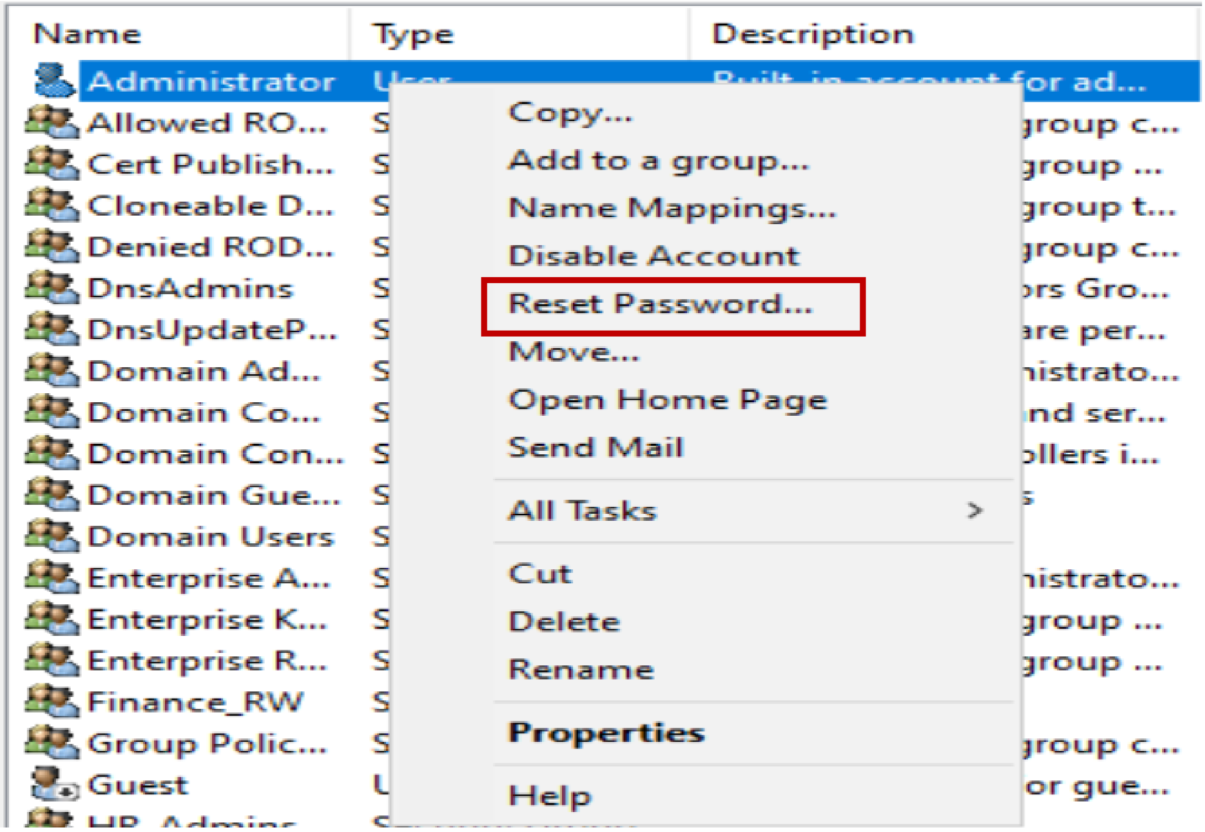
3.3 Testing and Validation

The final phase involves verifying that the PSO behaves as intended by testing password changes for both an admin and a regular user.

- **Test Local User vs Admin User Password Change**

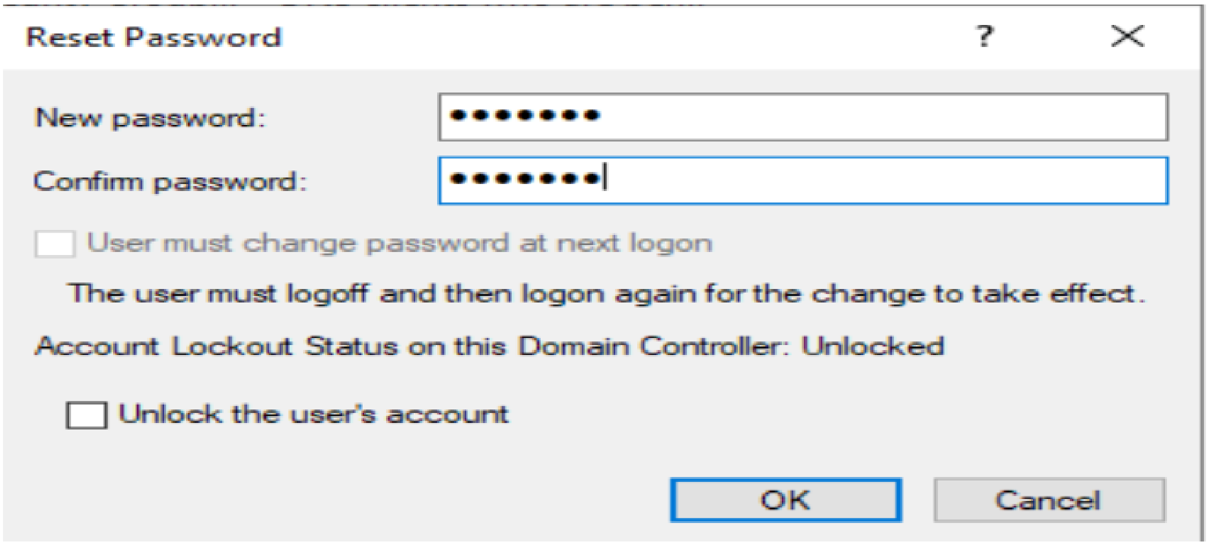
  We attempt to change the password for a Domain Admin user and compare the behavior to a standard local domain user. The admin should face stricter rules, such as longer minimum length or enforced complexity.

(Reset Password For Admin account.)



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	S	group c...
Cert Publish...	S	group ...
Cloneable D...	S	group t...
Denied ROD...	S	group c...
DnsAdmins	S	ors Gro...
DnsUpdateP...	S	are per...
Domain Ad...	S	nistrato...
Domain Co...	S	nd ser...
Domain Con...	S	ollers i...
Domain Gue...	S	s
Domain Users	S	
Enterprise A...	S	nistrato...
Enterprise K...	S	group ...
Enterprise R...	S	group ...
Finance_RW	S	
Group Polic...	S	group c...
Guest	U	or gue...
HR Admins	S	

(Set weak password for admin account)



Reset Password

New password: ••••••••

Confirm password: ••••••••

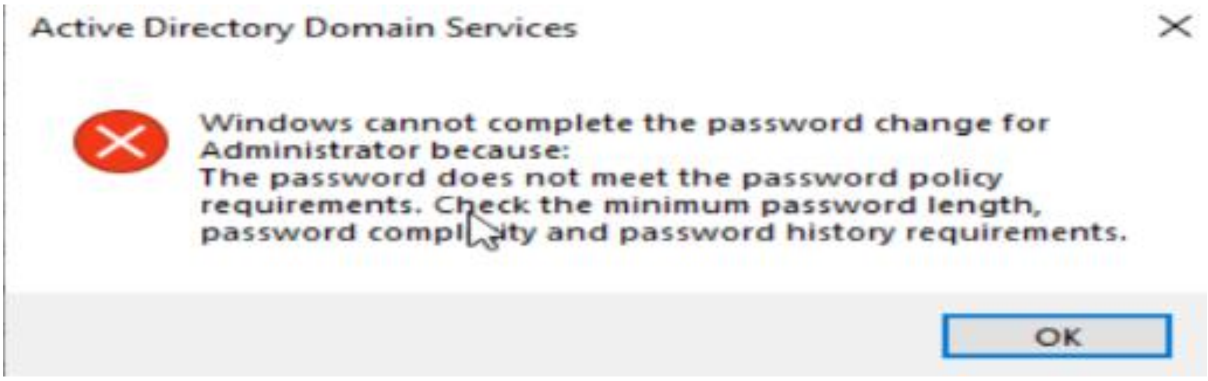
□ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

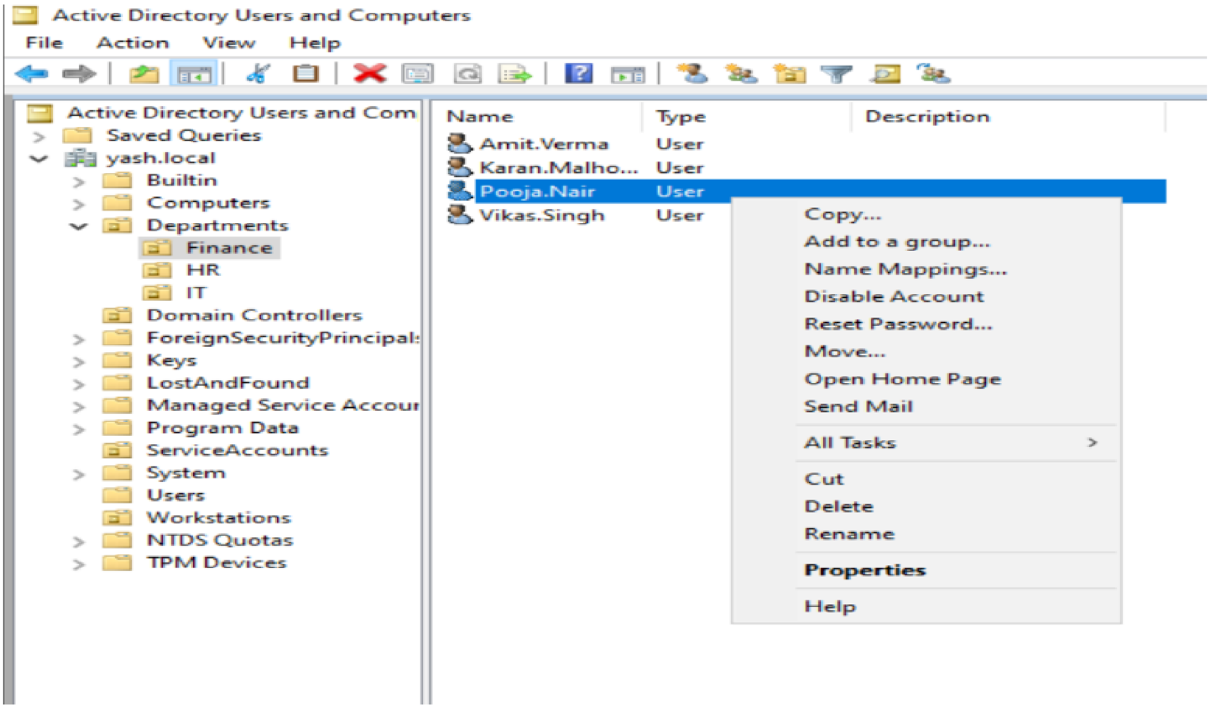
□ Unlock the user's account

(We can’t able to set a weak password to admin account)



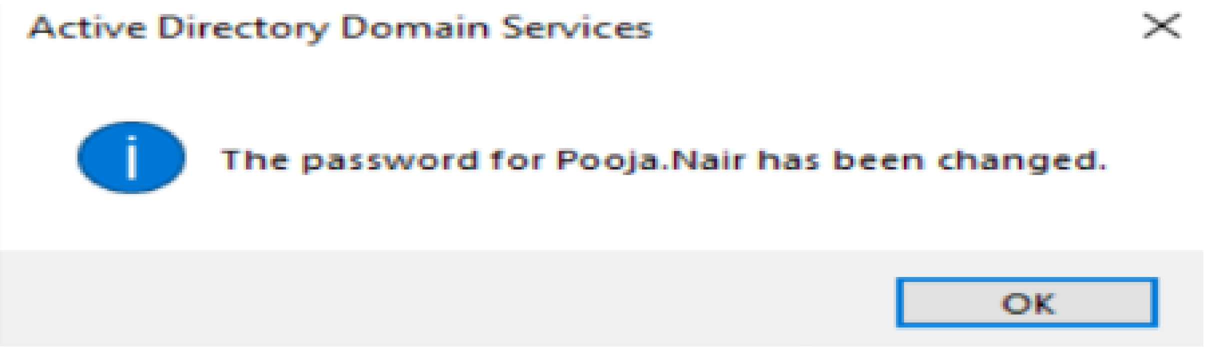
Windows cannot complete the password change for Administrator because:
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

(Reset password for local user)



Name	Type	Description
Amit.Verma	User	
Karan.Malho...	User	
Pooja.Nair	User	
Vikas.Singh	User	

(Tried same password on local user.)



The password for Pooja.Nair has been changed.

4. Results And Findings

The implementation of the AdminStrictPolicy PSO for Domain Admins yielded positive and measurable outcomes. The results confirmed that Fine-Grained Password Policies are functioning as intended and differentiating between privileged and non-privileged accounts.

- **Successful Creation of AdminStrictPolicy PSO**
  The PSO was successfully created with custom settings including a 14-character minimum, password complexity enforcement, and a 30-day expiration. This validated the capability of the domain to support FGPP.

- **PSO Properly Linked to Domain Admins Group**
  The PSO was applied specifically to the Domain Admins group using the "Directly Applies To" field in ADAC. This ensured the policy affected only the intended users without altering the global domain policy.

- **Admin Accounts Enforced with Stricter Rules**
  When attempting to change the password of a Domain Admin, the system enforced the stricter rules—such as rejecting passwords under 14 characters or without complexity. This proved that the PSO was active and effective.

- **Regular Users Not Affected by PSO**
  Password changes for non-admin users proceeded with the default domain policy. This demonstrated successful targeting of the PSO and avoided unnecessary disruption for standard users.

- **No Conflicts or Errors During Application**
  No errors or conflicts were encountered during PSO creation or enforcement, indicating stable integration with existing domain configurations.

5. Recommendations

Based on the findings from implementing the `AdminStrictPolicy` for Domain Admins, the following best practices are recommended to enhance password security and domain hygiene across the organization:

- **Expand FGPP Usage to Other High-Privilege Groups**
  While the AdminStrictPolicy was applied to Domain Admins, it's essential to extend similar fine-grained policies to other high-risk groups like Enterprise Admins, Schema Admins, and service management groups. This ensures a broader defense-in-depth approach by reducing the attack surface from all privileged accounts.

- **Regularly Review PSO Assignments and Settings**
  Over time, organizational needs and group memberships may change. Periodic reviews of Password Settings Objects help maintain their relevance, ensure they're not misapplied, and verify that security standards are being met consistently across all sensitive accounts.

- **Avoid Assigning FGPPs to Individual Users**
  Applying PSOs to individual users creates complexity and administrative burden. It's better to manage PSO assignments through security groups, which ensures scalability, easier auditing, and centralized policy control, especially in large or dynamic environments.

- **Monitor PSO Effectiveness Using Logs**
  Administrators should enable auditing on password-related events and review Event Logs regularly. This helps detect policy violations, unsuccessful password changes, and user confusion—allowing for faster issue resolution and verification that the policies are functioning as expected.

- **Educate Admins on Policy Differences**
  It's important that privileged users understand the stricter rules that apply to them. Clear communication and awareness training can reduce helpdesk tickets related to password errors and encourage compliance, minimizing resistance to security enforcement.

6. Conclusion

The successful deployment of a Fine-Grained Password Policy (FGPP) for Domain Admins represents a critical improvement in the organization’s password security strategy. By creating the AdminStrictPolicy and applying it specifically to high-privilege accounts, we achieved enhanced control over password strength requirements without affecting regular users. This targeted enforcement helps mitigate risks posed by weak or reused passwords among accounts that hold elevated privileges.

The testing phase clearly demonstrated the PSO's effectiveness: admin accounts were subjected to stricter password complexity and length requirements, while regular domain users were unaffected, ensuring minimal disruption to everyday operations. Additionally, the configuration process through Active Directory Administrative Center (ADAC) was straightforward and did not introduce any policy conflicts or errors within the domain.

Implementing FGPPs also aligns with industry best practices and compliance frameworks that demand tailored security measures for administrative accounts. This project underscores the importance of role-specific security, and paves the way for broader adoption of granular policies across other critical account types. Future efforts should focus on continuous monitoring, expanding PSOs to other sensitive groups, and maintaining policy clarity across the directory environment to ensure a robust and adaptive password policy architecture.