Active Directory GPO (Group Policies)

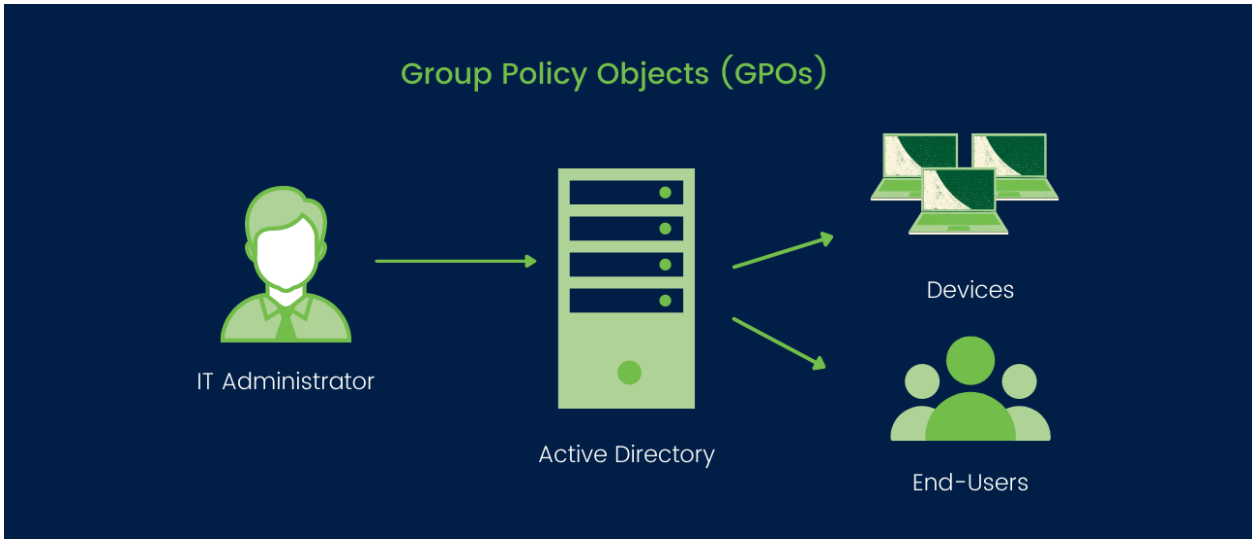
Part 4: Understanding and Creating Group Policies

1 Introduction

This project focuses on the implementation and management of Group Policy Objects (GPOs) within an Active Directory environment. GPOs are essential for managing and enforcing policies across a network, providing centralized control over user and computer configurations. This document outlines the process of setting up various GPOs to enhance security, manage user environments, and streamline administrative tasks.

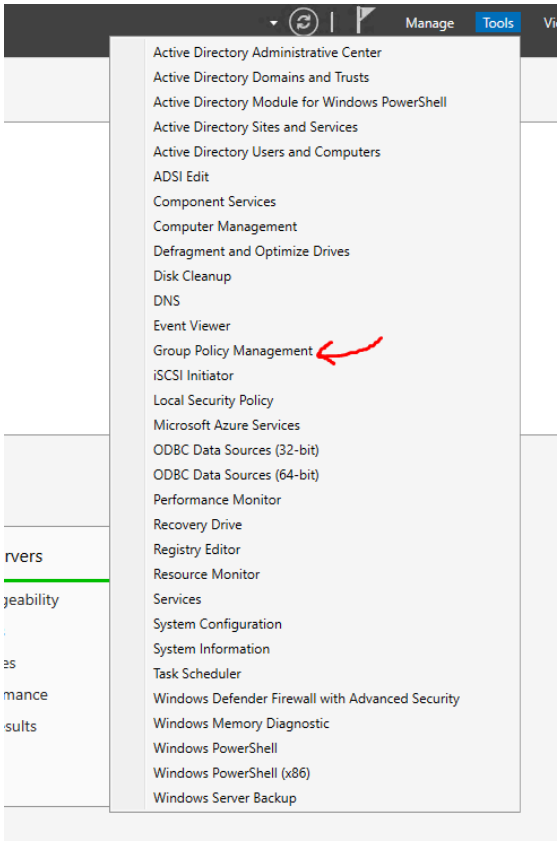
2 What are Group Policy Objects?

Group Policy Objects (GPOs) are a feature of Microsoft Windows that allow administrators to define and enforce settings across multiple computers and users within an Active Directory environment. GPOs provide a centralized method for managing operating system, application, and user settings, ensuring consistency and security across the network.

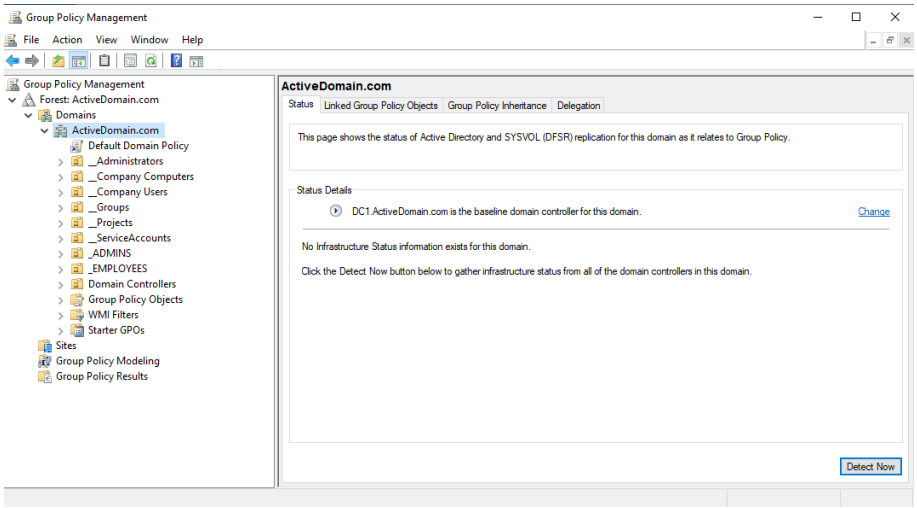


- Above showcases what a typical Group Policy Object is in an Active Directory.
- They often fall under two categories
    - Devices
    - End-Users
- And for each of these categories, there's two types of GPOs
    - Policies
    - Preferences
- Policies are enforced rules that devices or users have to follow
- Preferences are default rules given that can be altered by both devices and users

3 Setting up GPO



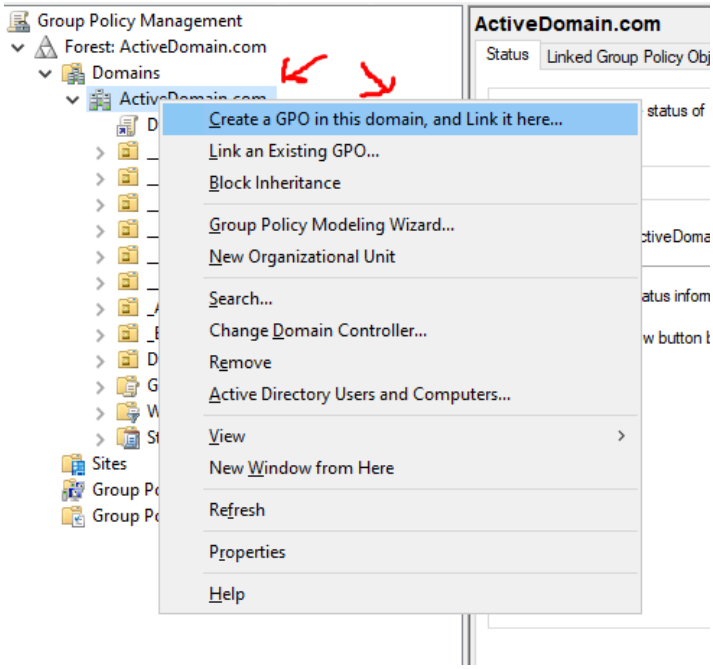
- To access GPO, we'll need to go to Group Policy Management



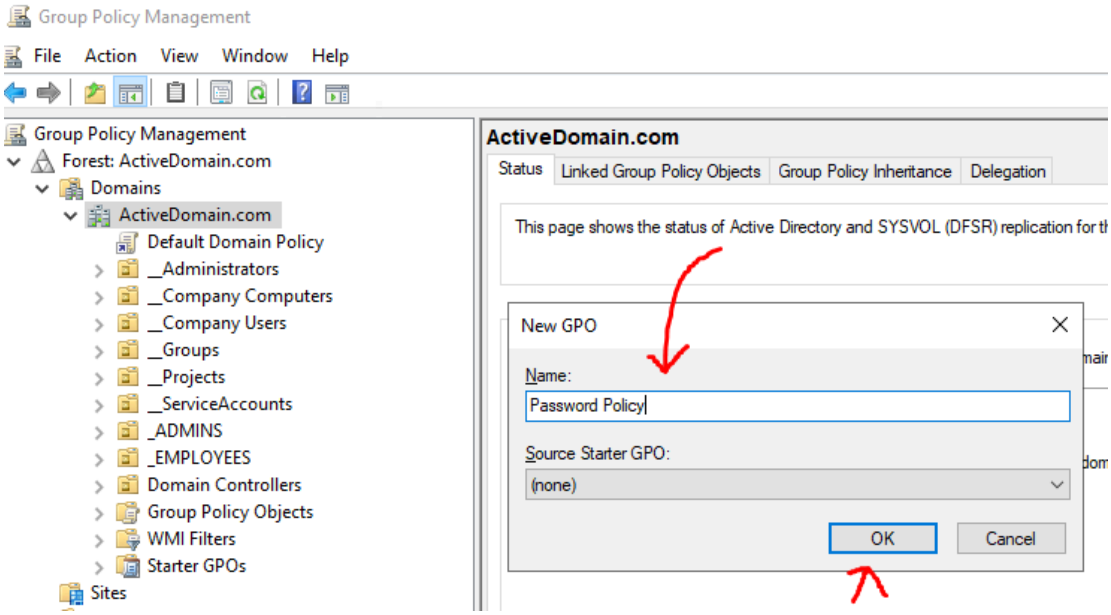
- This will open up the Group Policy Management Window

3.1 Password Policy

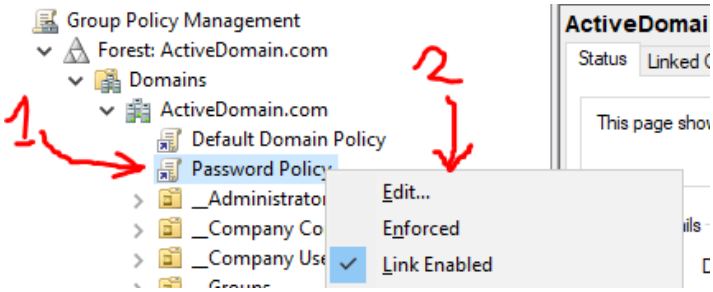
Configuring the Password Policy GPO establishes rules for password complexity, length, and expiration, enhancing security by enforcing strong password practices across the organization.



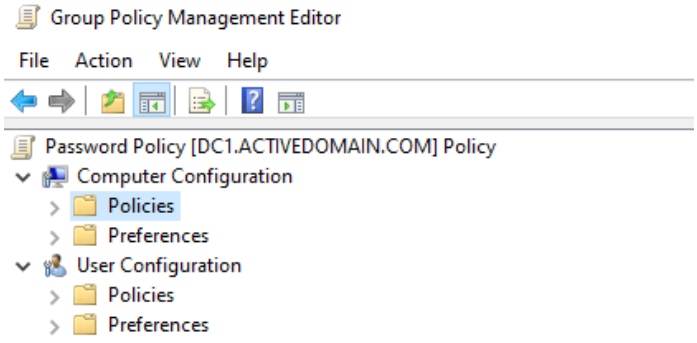
- Open up the folders until we get our Domain
- Right click our Domain > Create a GPO in this domain



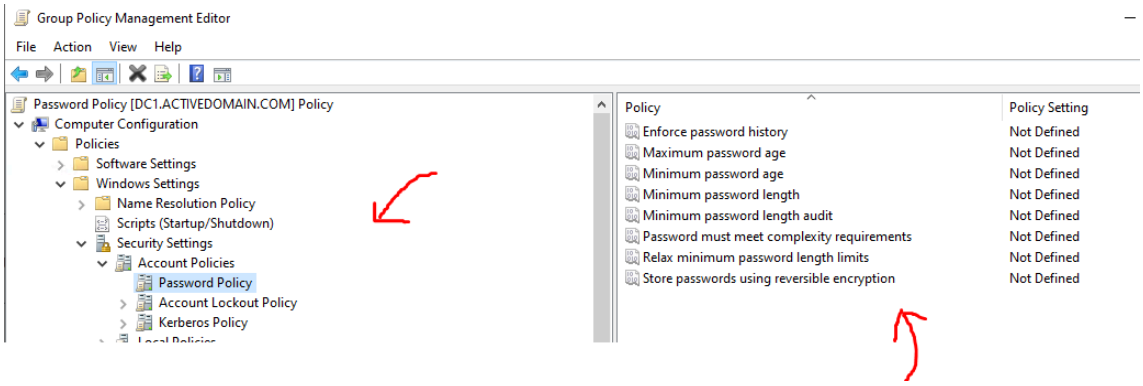
- We'll name it Password Policy, click OK



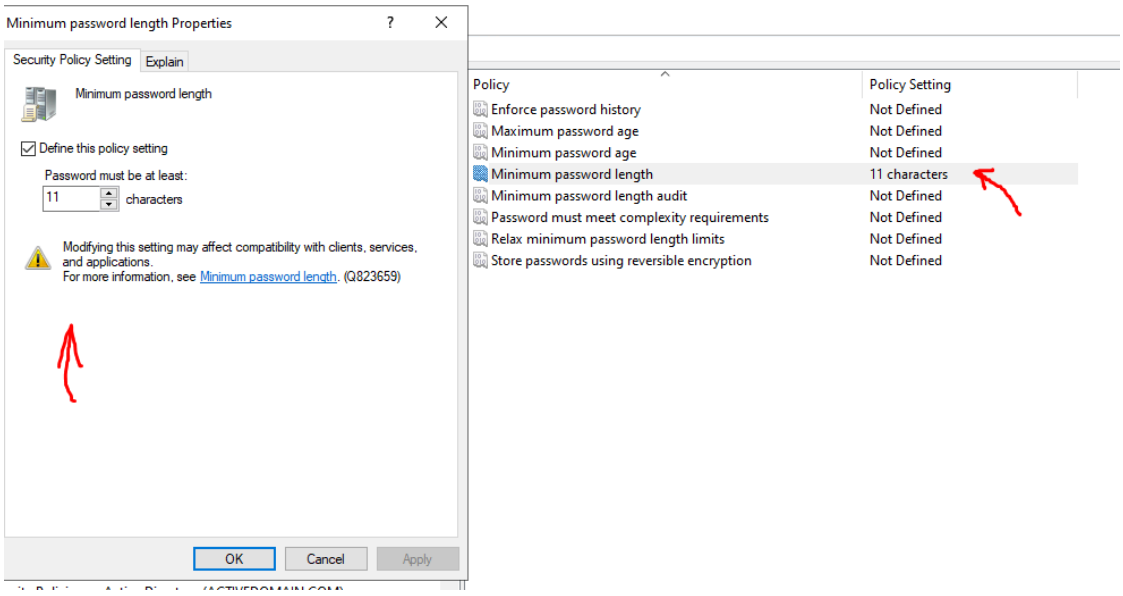
- We've now created the Password Policy
- We'll then right click it then select Edit



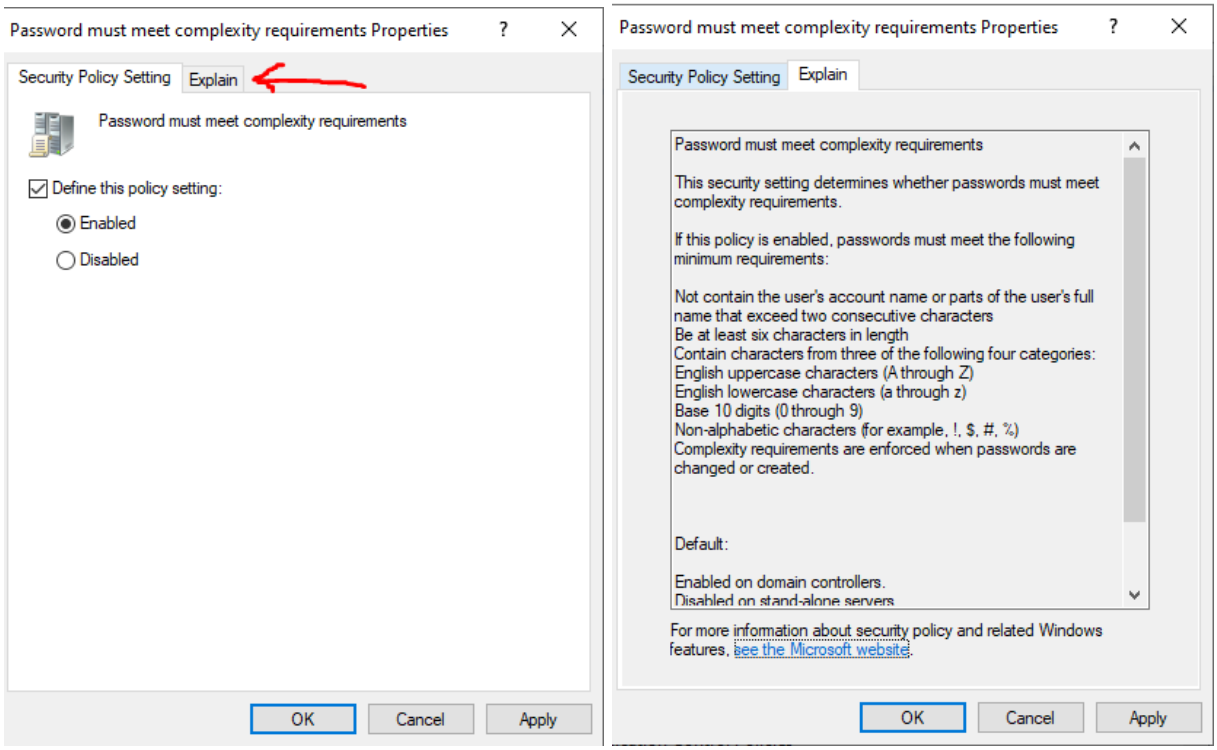
- We'll then be taken to here. As mentioned before, policies are restricted to two types of configurations.
    - Computer Configurations
    - User Configurations
- And with each of these configurations, there are two types of policies
    - Policies - These are strict rules that must be adhere to
    - Preferences - These are default given rules that can be altered



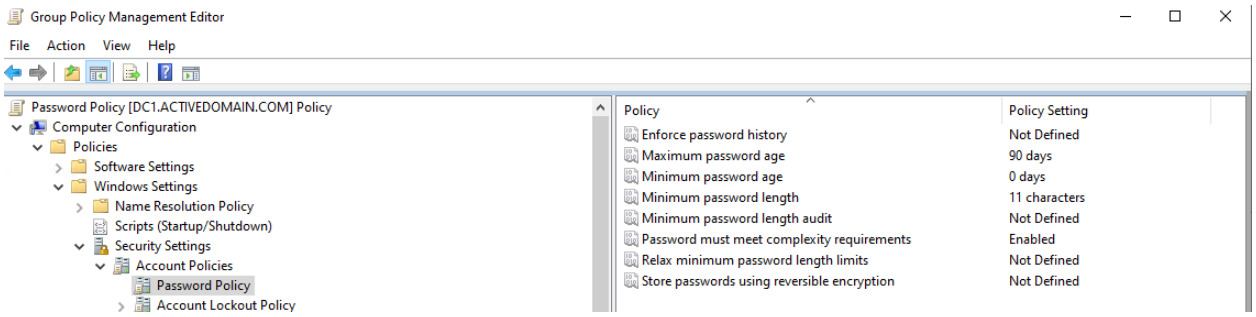
- From where, we're going to configure our Password Policy
- Go to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
- From there we will have a list of different policies we can define



- We can then add a password policy. This will be the minimum of 11 characters



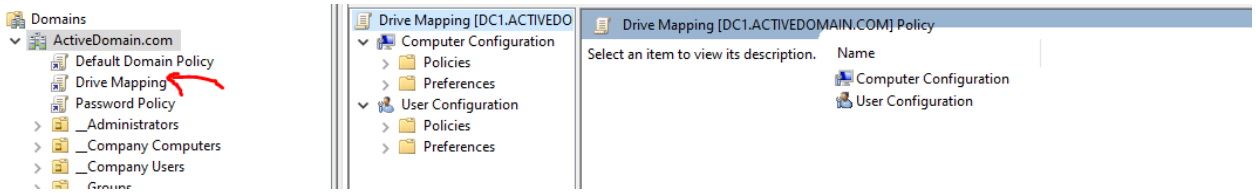
- Some policies have a little more to them. In this example, we have the passwords meeting a complexity requirement.
- This requirement can then be further explained through the explain properties
- As we can see, there are a set of rules given. These are the default rules given by windows server.



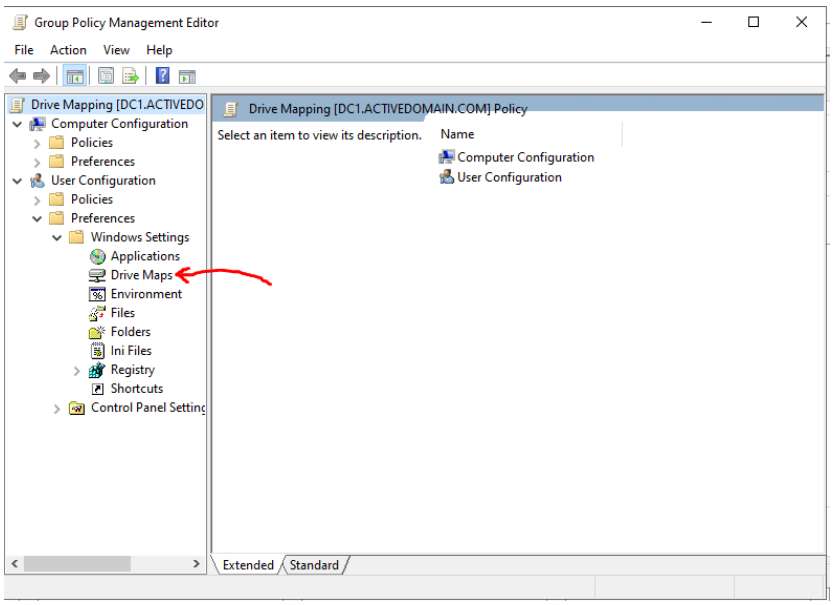
- After you're done, all the policy definitions should be created for our Password Policy!

3.2 Drive Mapping Preferences

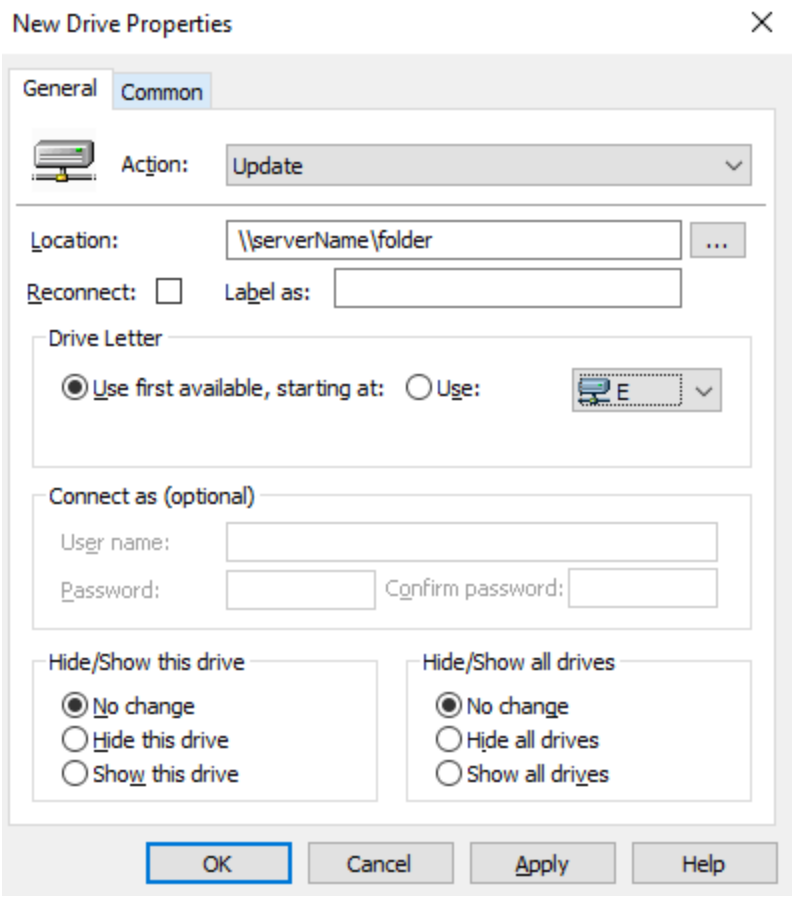
The Drive Mapping Preferences GPO automates the process of mapping network drives for users, ensuring consistent access to shared resources and improving user efficiency.



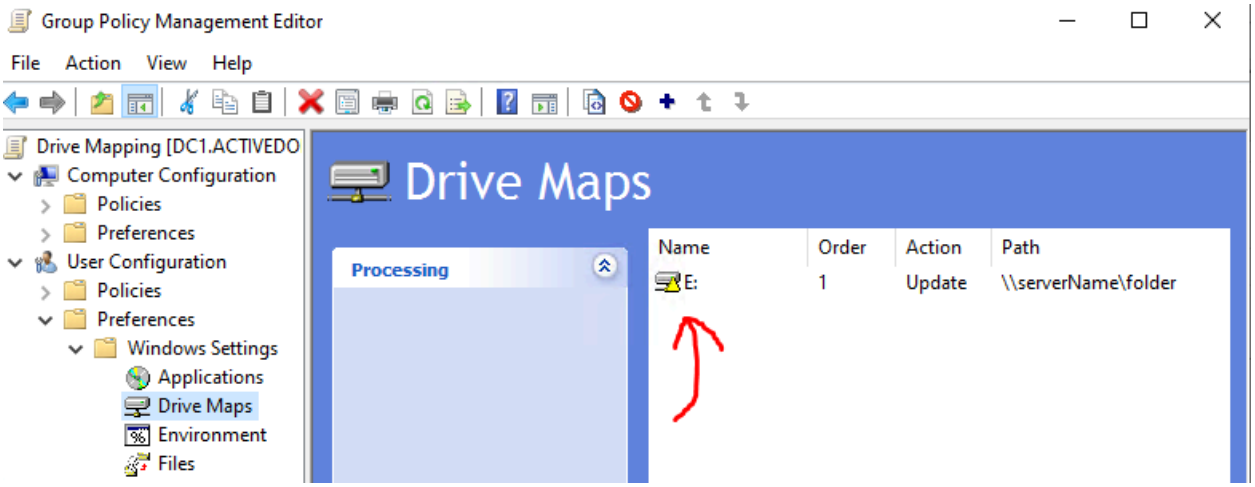
- First we'll make the Drive Mapping GPO in the same way we made the Password Policy
- Right click our domain > New GPO > Name it Drive Mapping > OK > Right Click Drive Mapping > Edit



- This will be a User Configuration and it'll be under Preferences
- Here we'll go to Windows Settings > Drive Maps > Right Click > New Map Drive



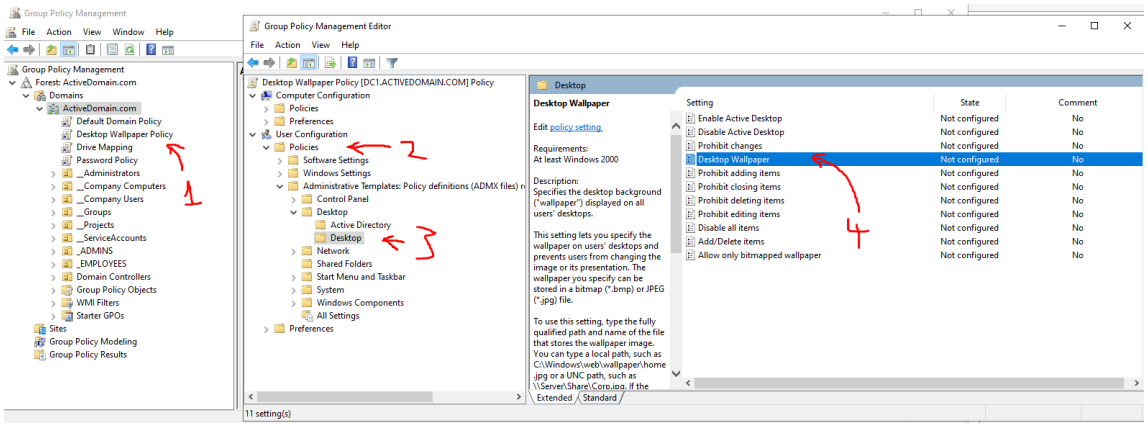
- Here we can set a location, and select a Drive Letter
- After we click Apply > OK



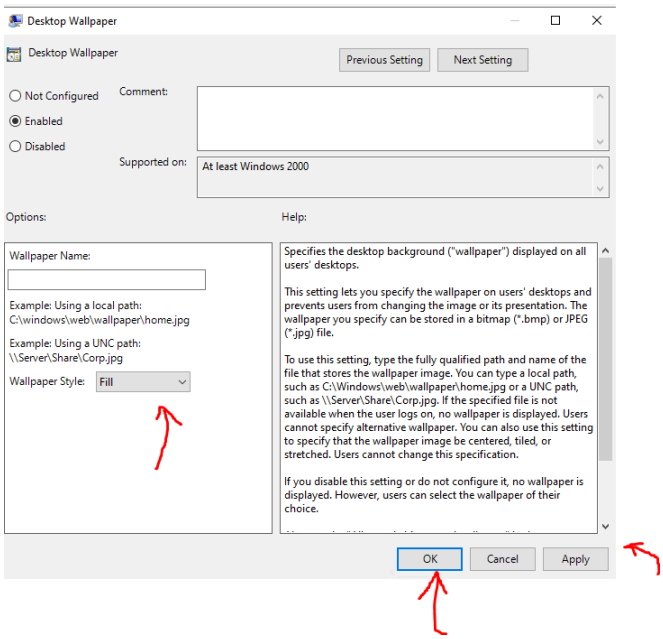
- Here we can confirm that the drive map has been created

3.3 Desktop Wallpaper Policy

The Desktop Wallpaper Policy GPO sets a standard desktop background for all users, which can be used to reinforce corporate branding or ensure a uniform look across the organization.



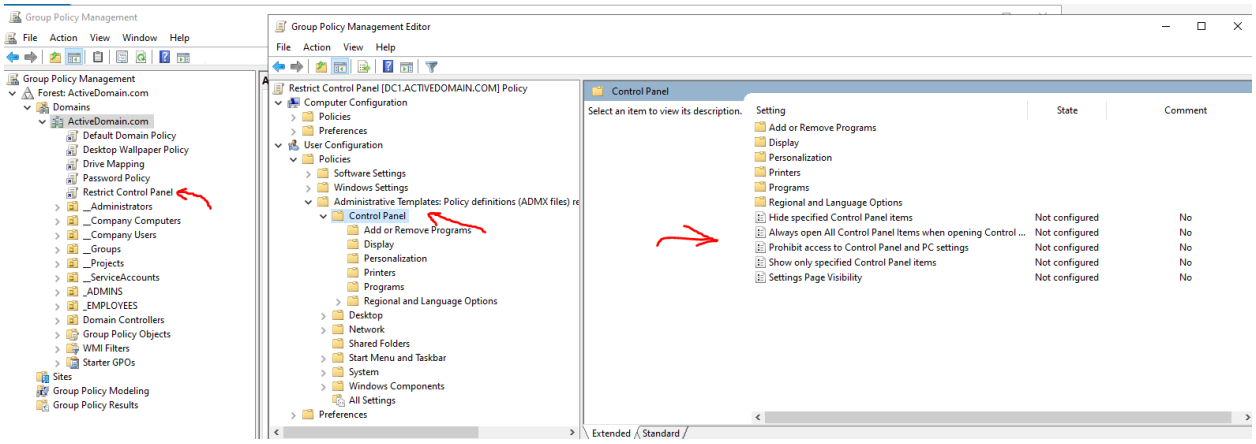
- Here we will create a GPO for Desktop Wallpaper Policy
- We create a new GPO and call it Desktop Wallpaper
- This GPO will be a User Configuration Policy
- Go to Policies > Administrative > Desktop > Desktop
- Select Desktop Wallpaper > Right click > Edit



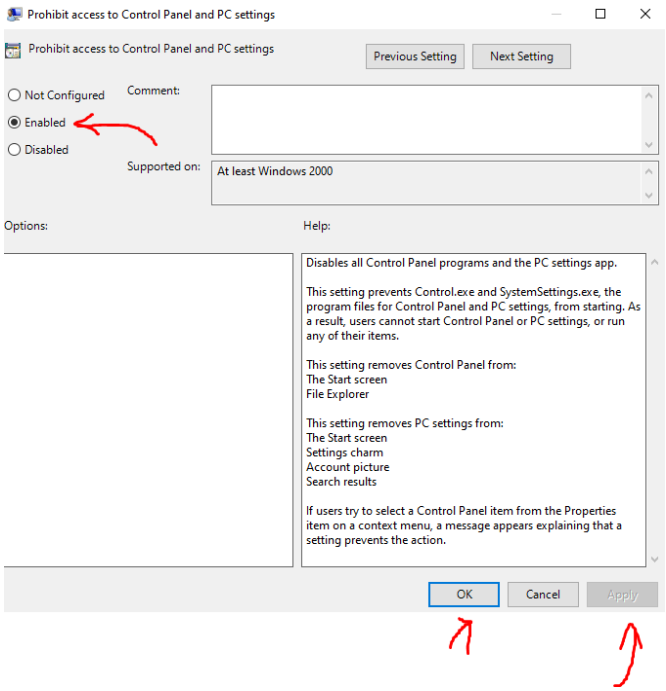
- Here we can fill our Wallpaper then we just click Apply > OK and it'll be ready to go
- The reason why we have this is because we want to restrict the wallpaper that would be used. Some may use inappropriate wallpapers so it's best it's kept consistent and controlled.

3.4 Control Panel Policy

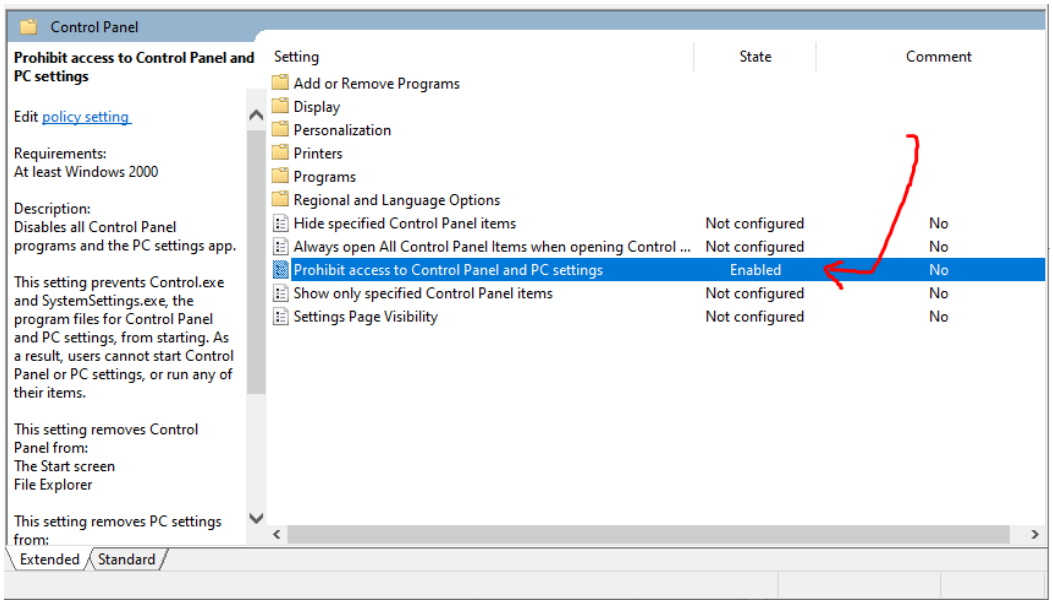
The Control Panel Policy GPO restricts or customizes access to Control Panel settings, helping to prevent unauthorised changes and maintain a consistent user environment.



- As before, create new GPO
- Name it Restrict Control Panel
- It'll be a User Configuration Policy
- Go to User Config > Policy > Administrative > Control Panel



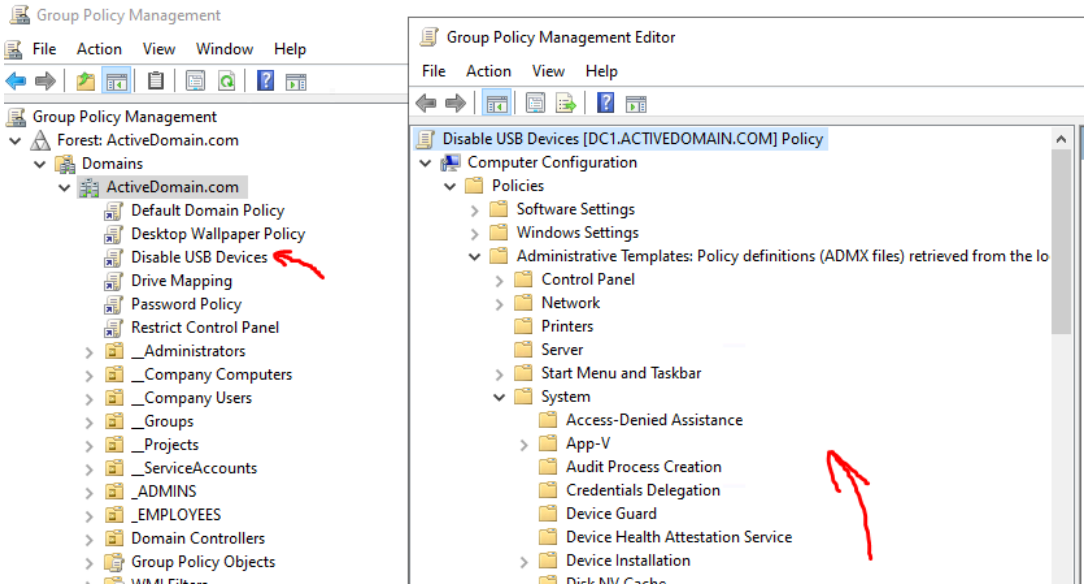
- For this example, we're going to prohibit the control panel entirely
- Right click Prohibit access to Control Panel and PC Settings > Edit
- Click on Enable and then Apply and OK



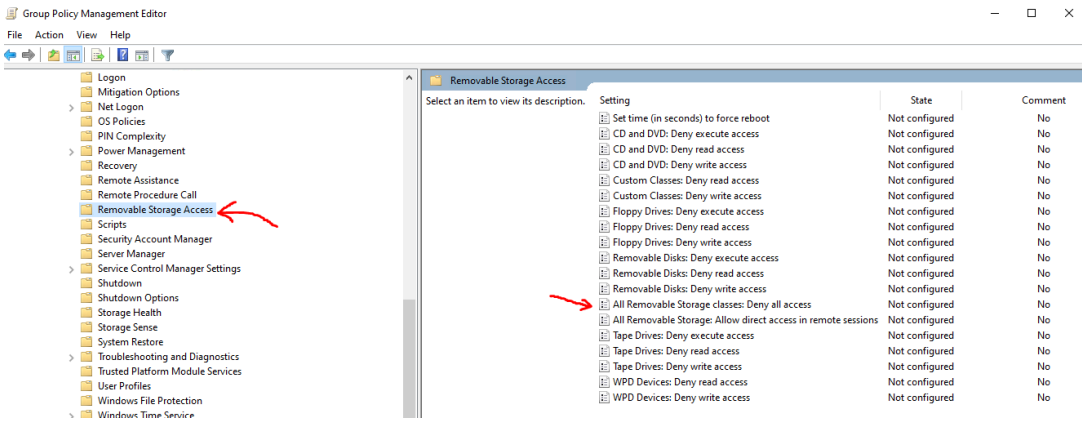
- It has now been enabled.

3.5 Disable USB Devices Policy

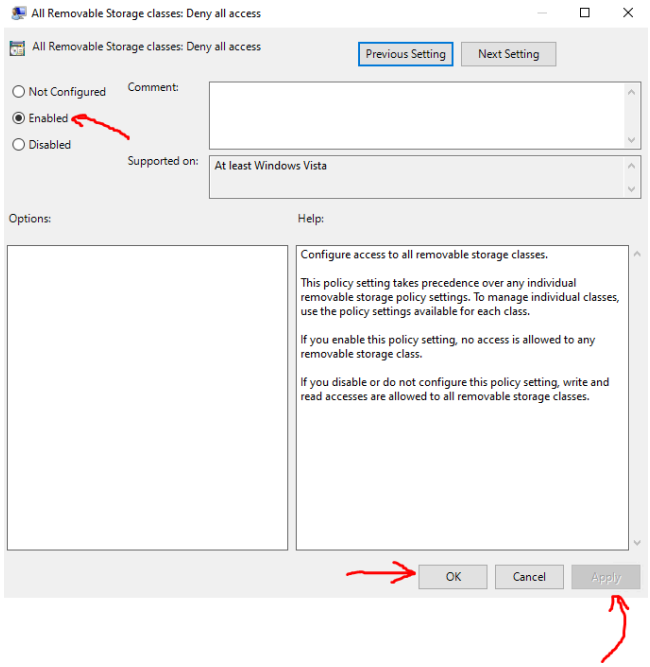
The Disable USB Devices Policy GPO restricts the use of USB ports, mitigating potential security risks by preventing unauthorized data transfers and the introduction of malware via removable media.



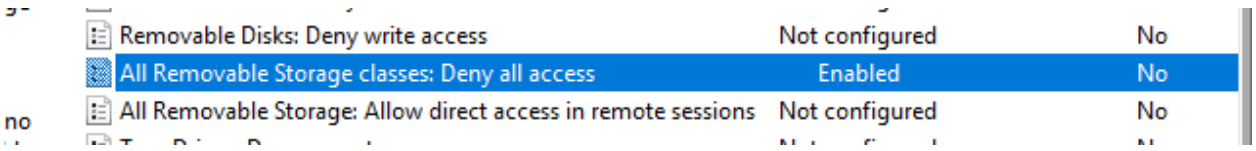
- As before, we create a new GPO, name it Disable USB Devices
- It'll be a Computer COnfiguration under Policies then go to Administrative > System



- Go further down, select “Removable Storage ”
- Select “All Removable Storage Classes: Deny all access”
    - We’re selecting this for this lab as we’re going to be as safe as possible and disable all removable storages



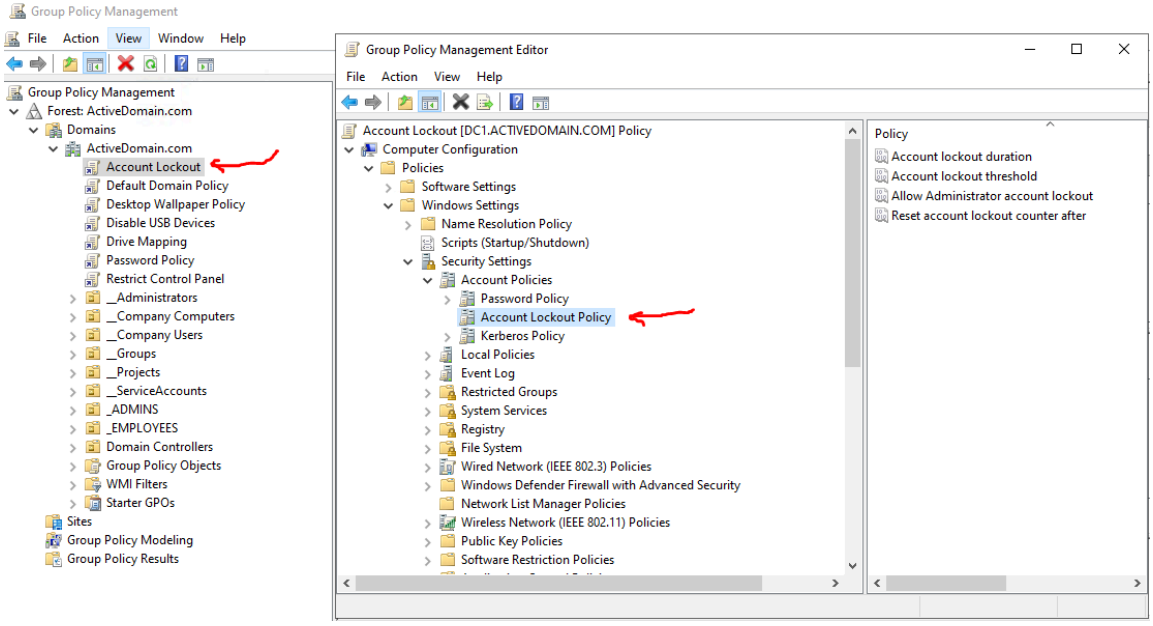
- Select Enable > Apply > OK



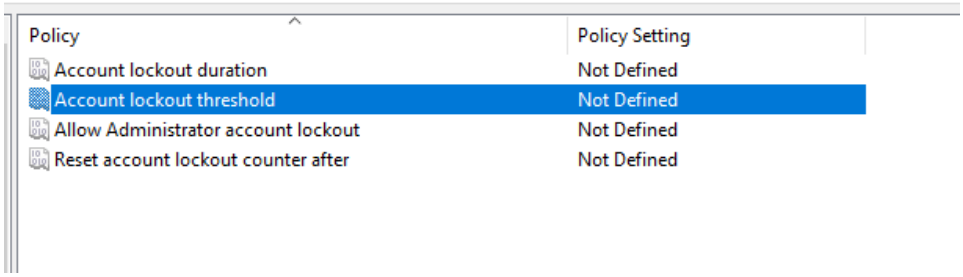
- From here we can see that it has been enabled.

3.6 Account Lockout Policy

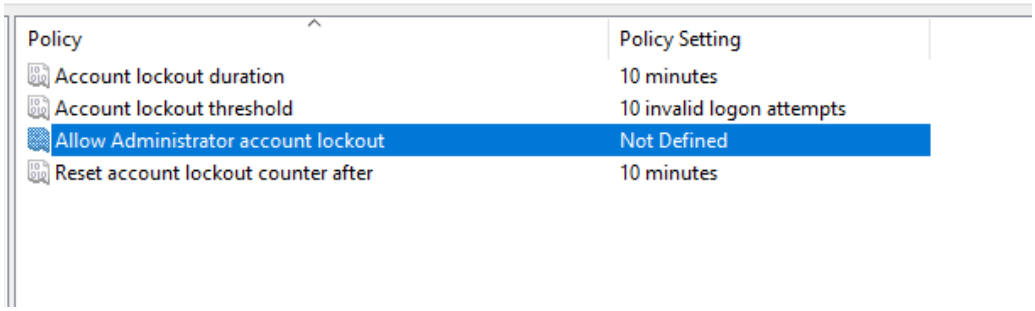
An Account Lockout Policy is a security measure that temporarily disables a user account after a specified number of failed login attempts, helping to prevent unauthorised access and brute force attacks.



- As before, create GPO call it Account Lockout
- It'll be a Computer Configuration under Policies > Window settings > Security > Account > Account lockout policy



- Here we can change the policies.



- Same as before, we just right click, edit and define the policies

4 Conclusion

In this project, we have explored the implementation of Group Policy Objects (GPOs) within an Active Directory environment, demonstrating how they can be utilised to enhance security, manage user environments, and streamline administrative tasks. By setting up GPOs for password policies, drive mappings, desktop wallpapers, control panel restrictions, and USB device management, we have illustrated the power and flexibility of GPOs in enforcing consistent configurations across a network. These policies not only help in maintaining a secure and efficient IT environment but also provide centralized control, making it easier for administrators to manage and enforce rules across the organization. As organizations continue to rely on Active Directory for network management, understanding and effectively deploying GPOs will remain a critical skill for IT professionals.