Modifying GPOs

Written by Tyler Weiss

Assignment

This assignment involves modifying a Group Policy Object (GPO) related to Windows Password Policy. Your task is to navigate through the Group Policy Management console to locate and modify the GPO that governs password policies. This exercise will help you understand where GPOs are managed and how to configure them step by step.

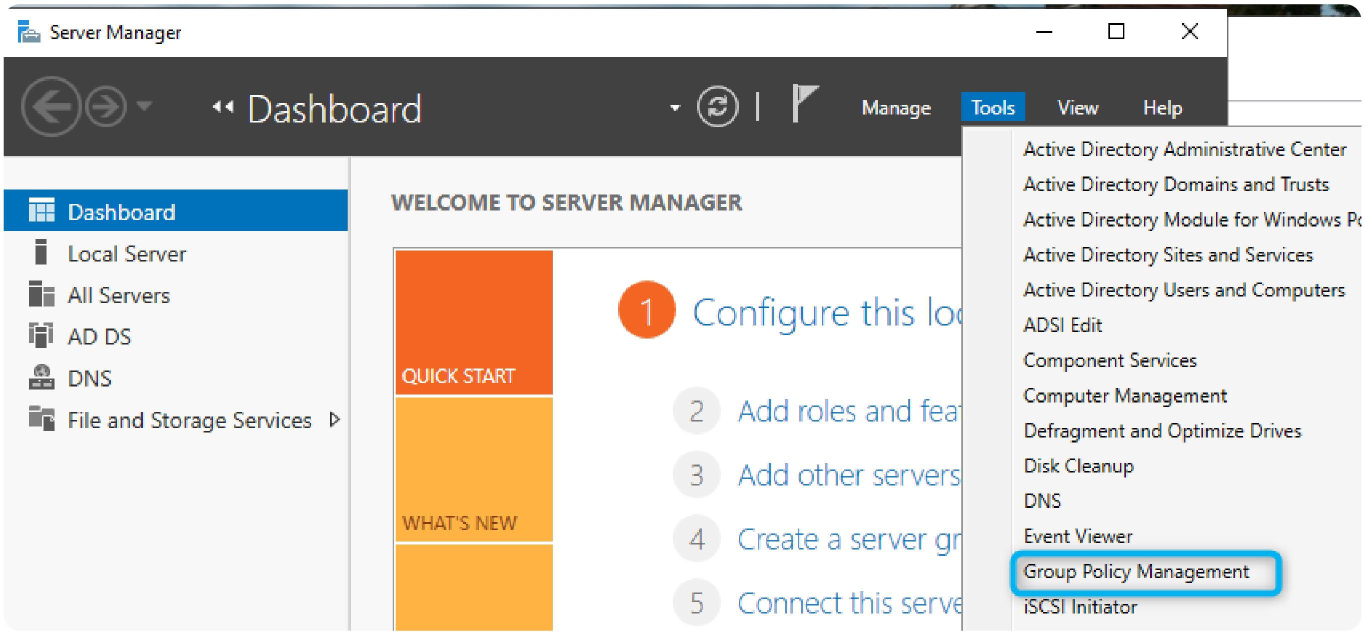
Capture screenshots at key points: opening Group Policy Management, locating the policy, accessing password settings, and applying your changes.

In your write-up, explain in simple terms what a GPO is and its significance in managing Windows environments. Discuss the role of the password policy within a GPO and how it helps in enforcing security standards across the domain. This explanation will demonstrate your understanding of GPOs’ function in network administration and security.

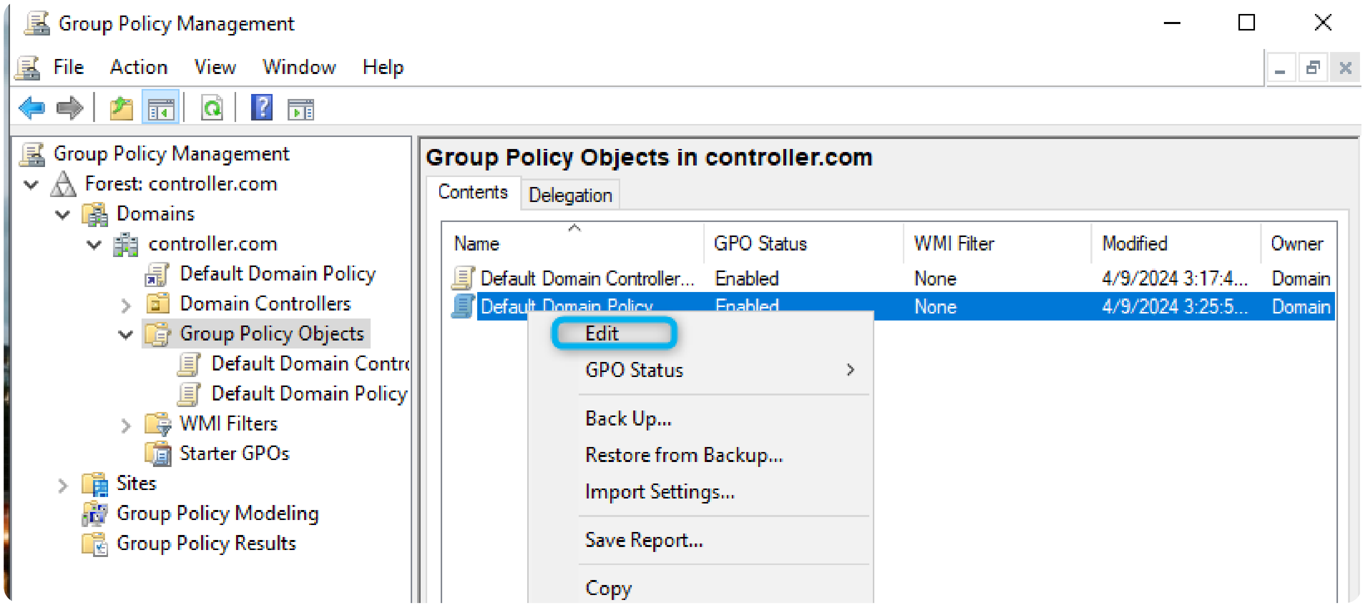
Exercise 1

A Group Policy Object (GPO) is a collection of policy settings with a unique name or Globally Unique Identifier (GUID). An Organizational Unit (OU) is the smallest unit that an administrator can assign Group Policy or permissions to. Users, groups, computers and other organizational units can be placed in OU's within Active Directory (AD) domains. GPOs are deployed to dictate the behavior of these OUs. The use of GPO's allows for regulation of computer and user configurations within AD domains. GPO's can be leveraged to achieve very granular control within AD environments. In this exercise we want to locate and modify the windows default password policy.

Step one is to locate the Group Policy Object (GPO) that we want to change. We can find these GPOs by opening the 'Server Manager'. In the 'Tools' drop-down menu select 'Group Policy Management'. The Group Policy Manager will displays all GPO's within the domains of a forest.

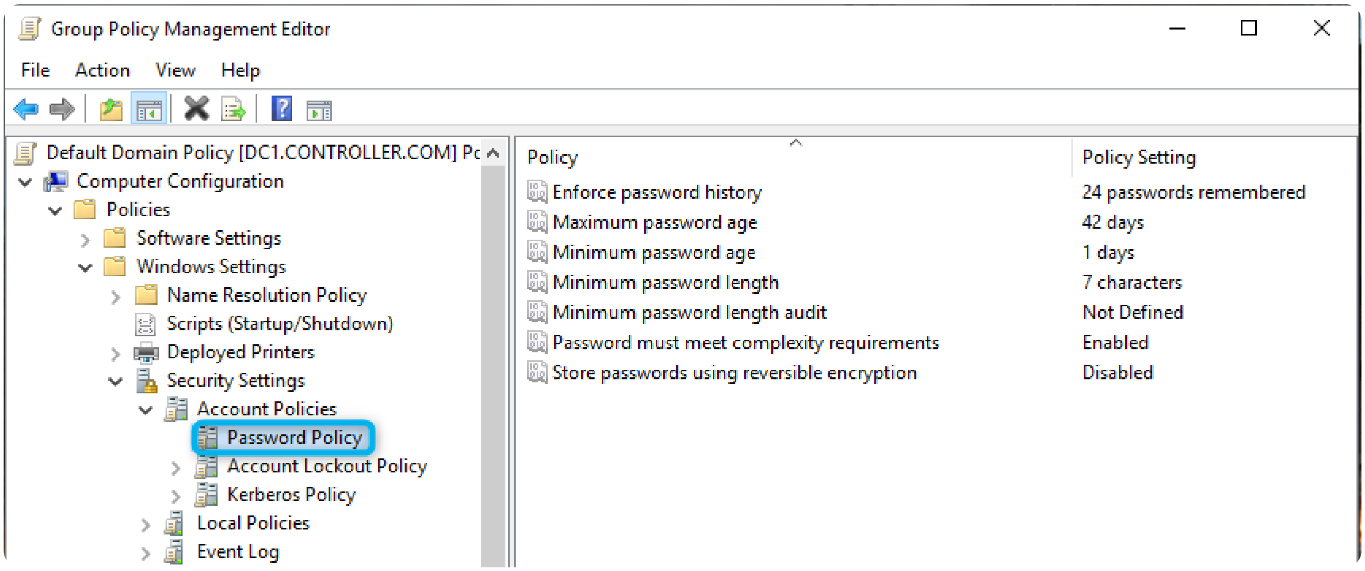


In the Group Policy Manager select the Forest and Domain where you want to edit a policy. Select 'Group Policy Objects' and Right-click the 'Default Domain Policy' and select edit. The 'Default Domain Policy', as the name states, are the collection of default policies for a domain and these policies will effect the entire domain unless explicitly overridden.



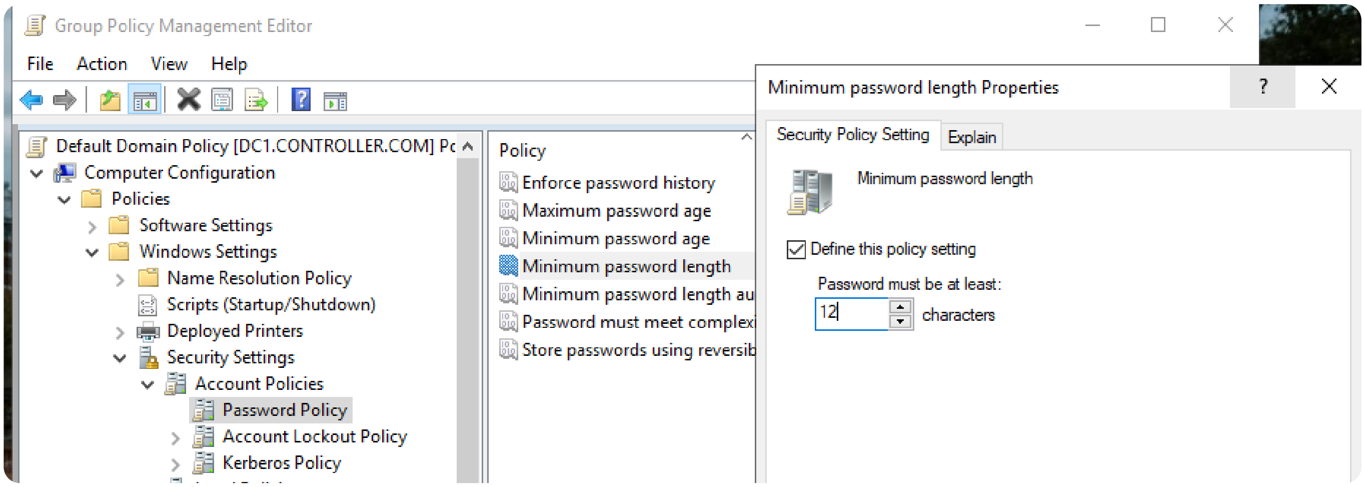
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	4/9/2024 3:17:4...	Domain
Default Domain Policy	Enabled	None	4/9/2024 3:25:5...	Domain

Our goal is to manage the GPO regarding passwords policy for Windows machines. This policy would fall under 'Computer Configuration' -> 'Policies' -> 'Security Settings' -> 'Account Policies'. It logical to that one can find this policy within the current hierarchy because it effects the security of user accounts within a domain on all computer systems. By selecting the 'Password Policy' GPO the policies within it are displays and available for editing.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

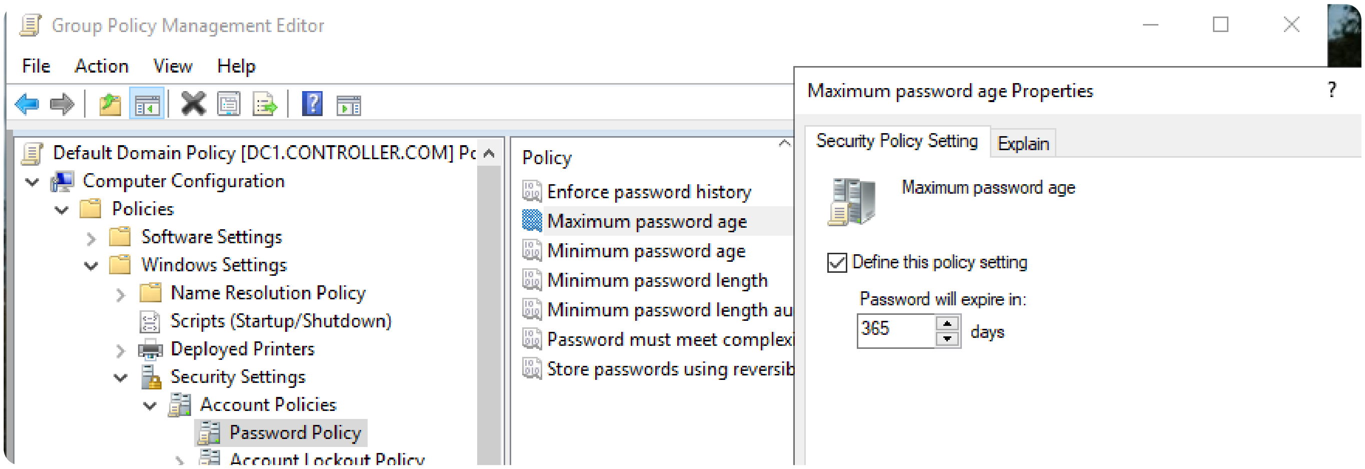
NIST guidelines recommend that a password should not be changed frequently because it leads to users making minor changes to previous passwords so it would be better to set the 'Maximum password age' to a 365 days. NIST guidelines also states that the minimum password length be at least 8 characters but to introduce more entropy we will use a 'Minimum password length' of 12 characters and make sure that 'Password must meet complexity requirements' is enabled. The remainder of the policies seem to be within standard. A policy can be edited by double clicking its name, editing it's setting and clicking the 'Apply' button. Once edited the policy changes should take within 90 minutes, with a random offset of 0 to 30 minutes, between Group Policy refresh times.



Minimum password length

☑ Define this policy setting

Password must be at least:
12 characters



Policy

Enforce password history
Maximum password age
Minimum password age
Minimum password length
Minimum password length au
Password must meet complexi
Store passwords using reversib

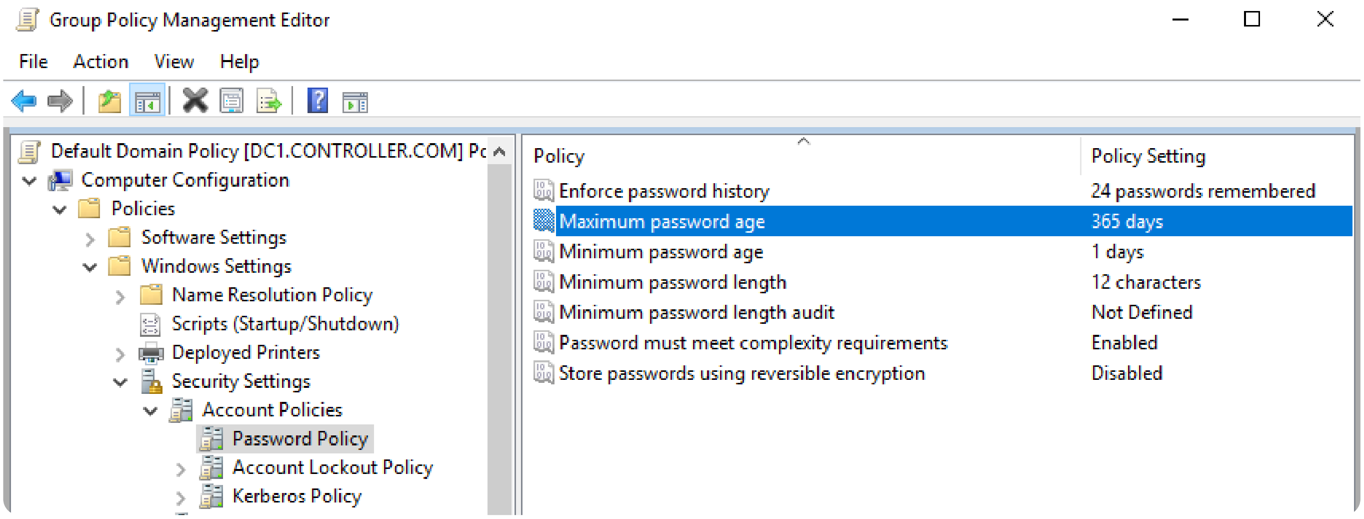
Maximum password age Properties ?

Maximum password age

☑ Define this policy setting

Password will expire in:

365 days



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	365 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled