

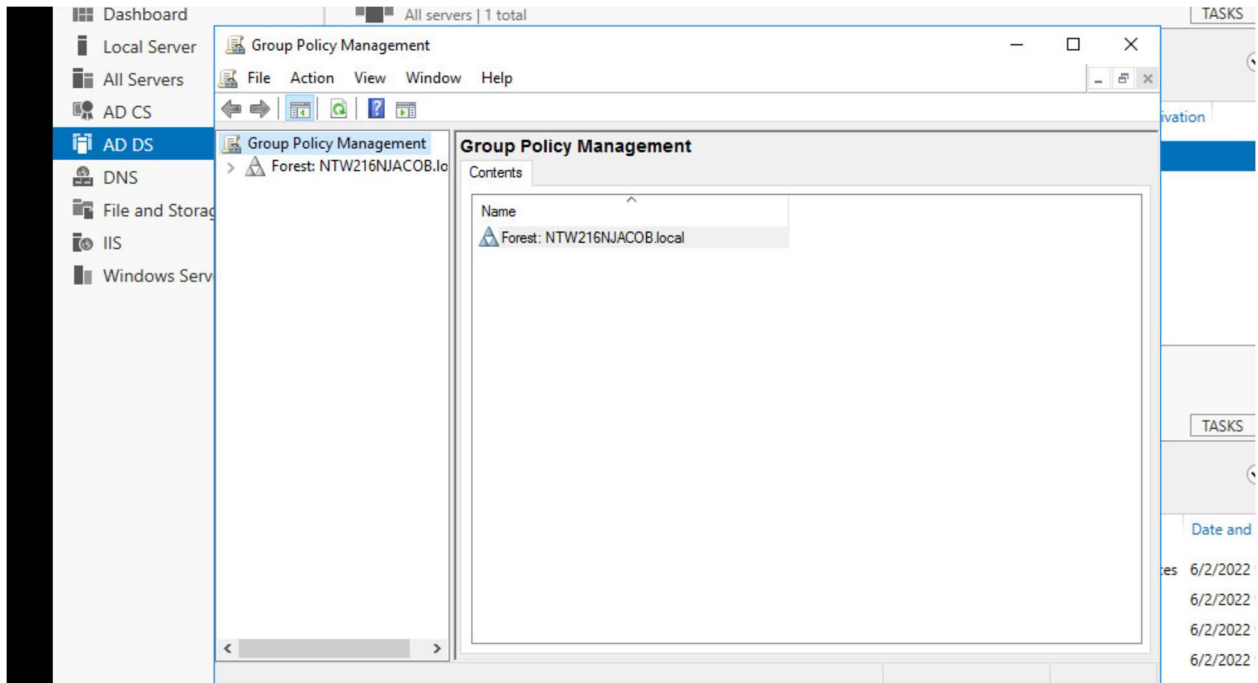
Set Group Policies

Nicholas Jacob

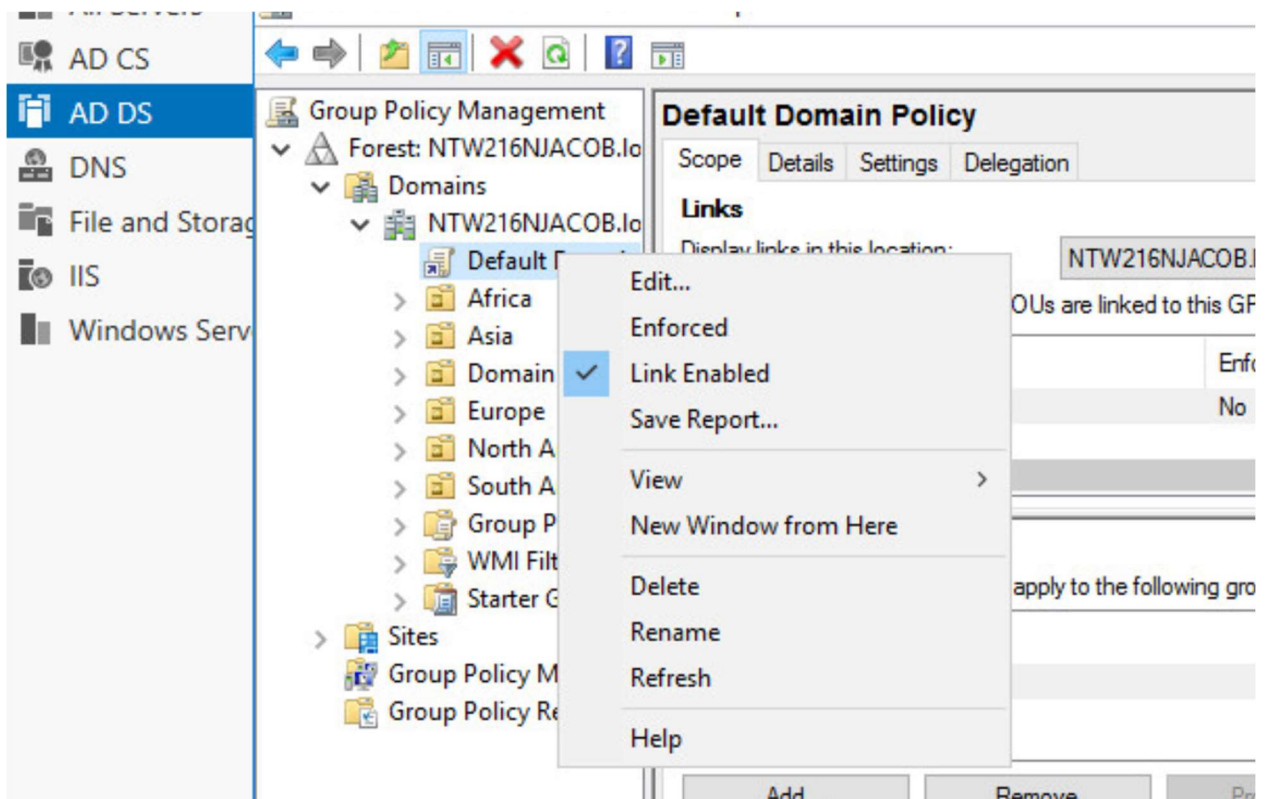
University of Advancing Technology

June 5, 2022

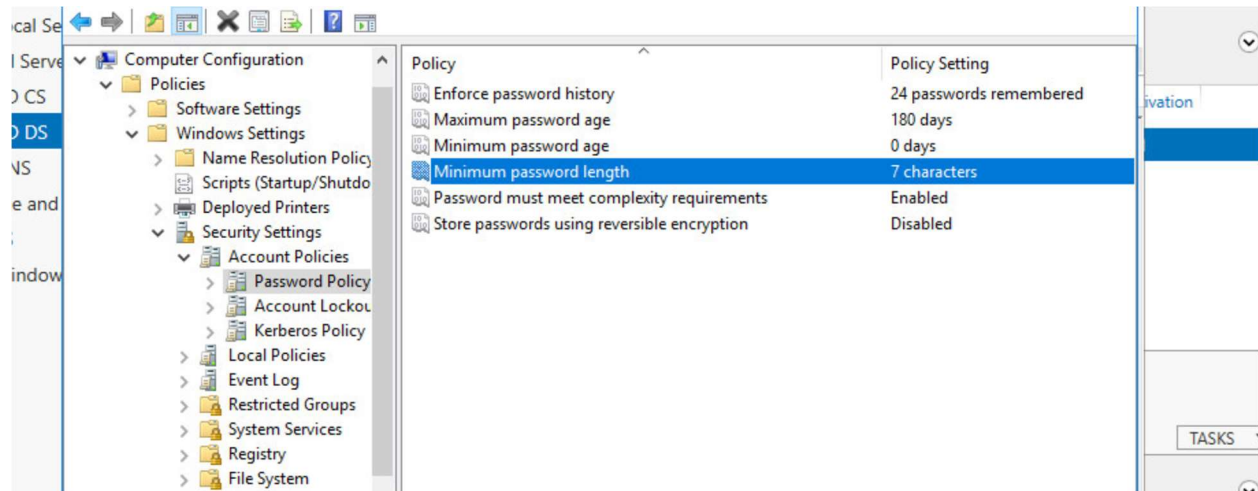
Open the Group Policy Management tool within the active directory



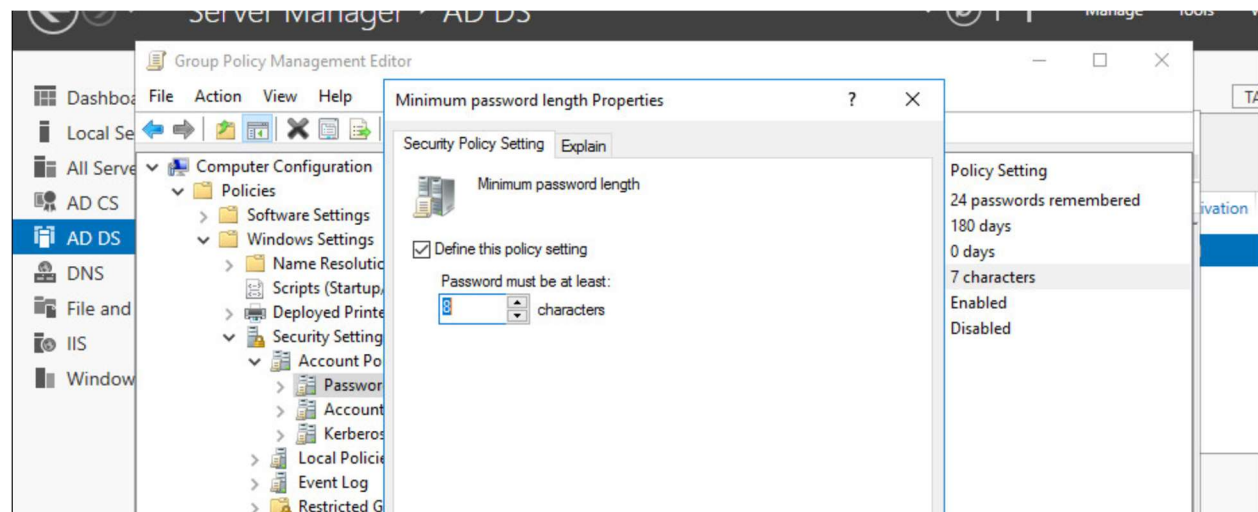
Under the domain, right-click the Default Domain Policy and hit Edit



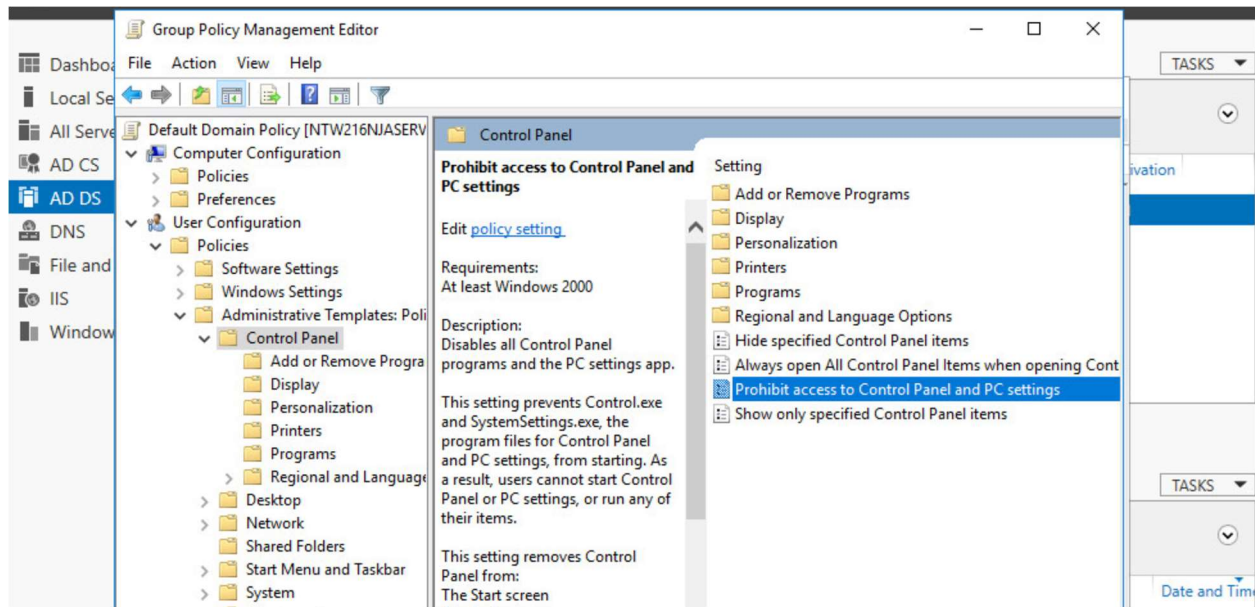
Under Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies, Password Policy double-click the Minimum Password Length setting



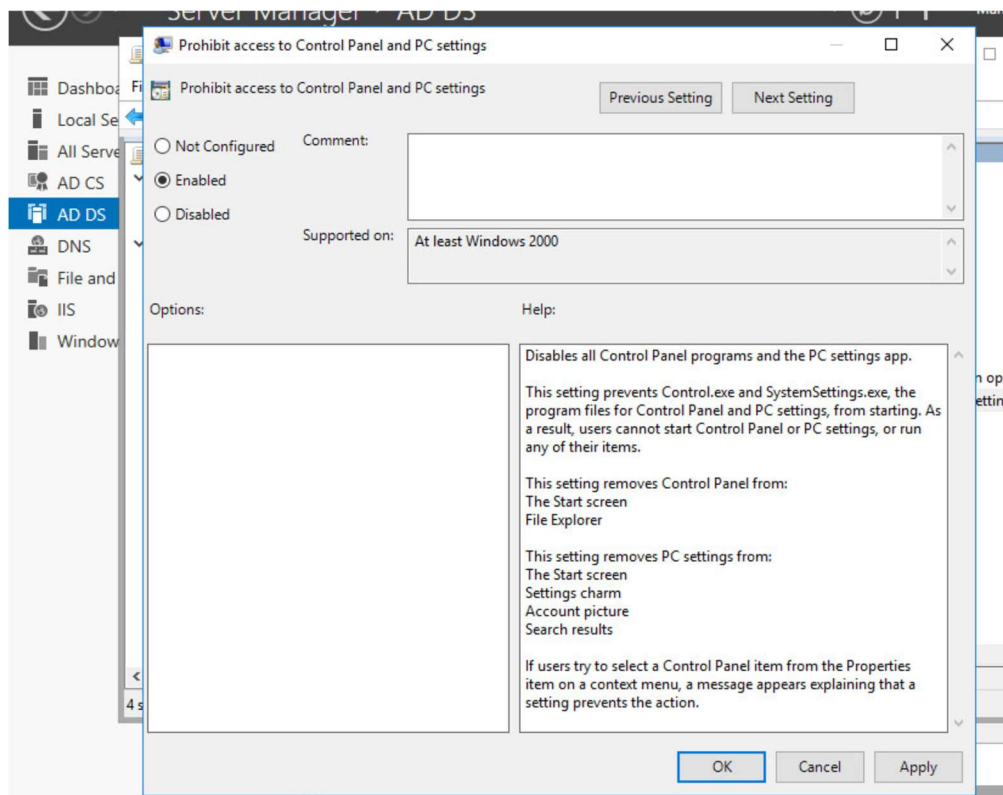
Ensuring the Define this policy setting box is checked, increase the password characters to 8 and hit OK



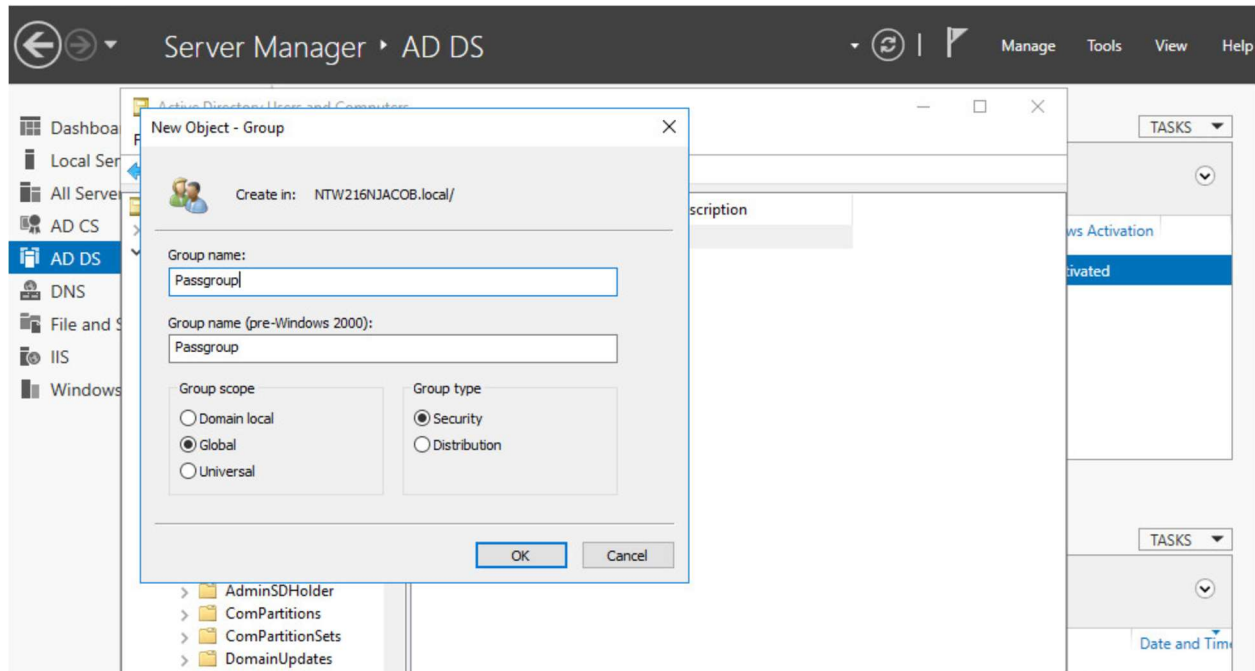
Double-click Prohibit Access To Control Panel And PC Settings under User Configuration, Policies, Administrative Templates, Control Panel



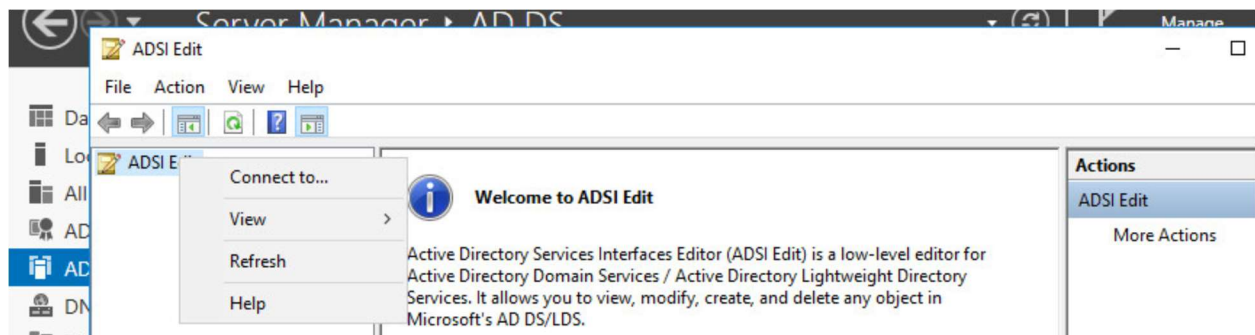
Select Enable and hit OK



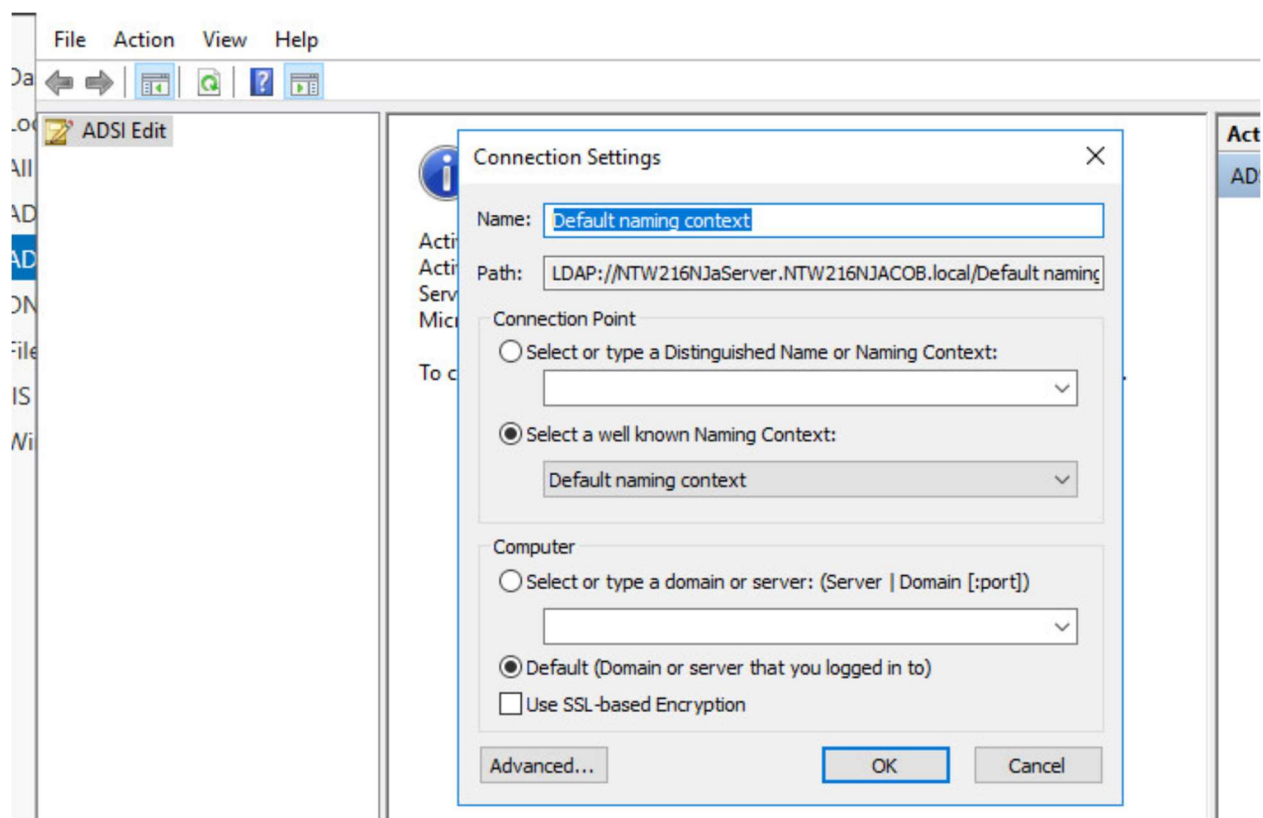
Create a Global group named Passgroup



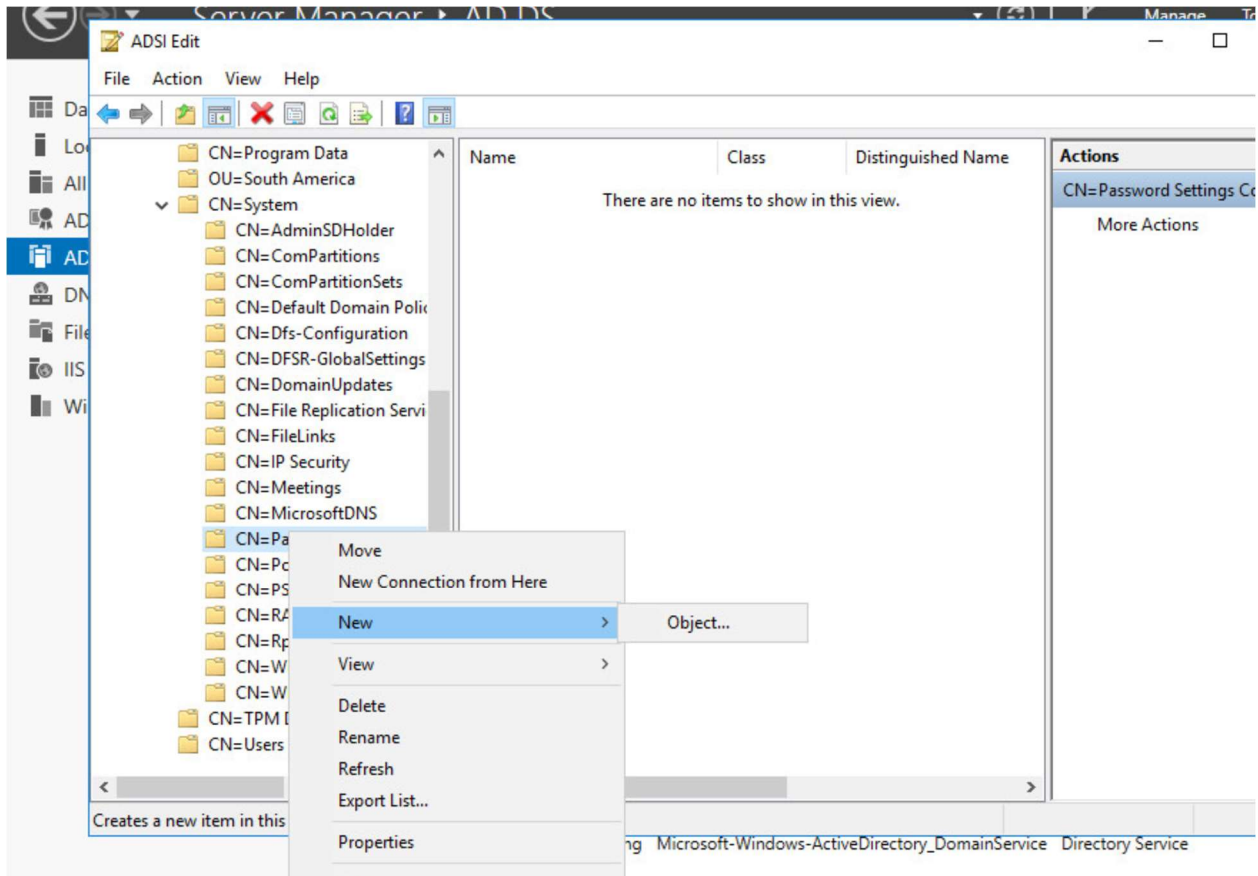
Open ADSI Edit found under Windows Administrative Tools in the start menu, right-click ADSI Edit, Connect To



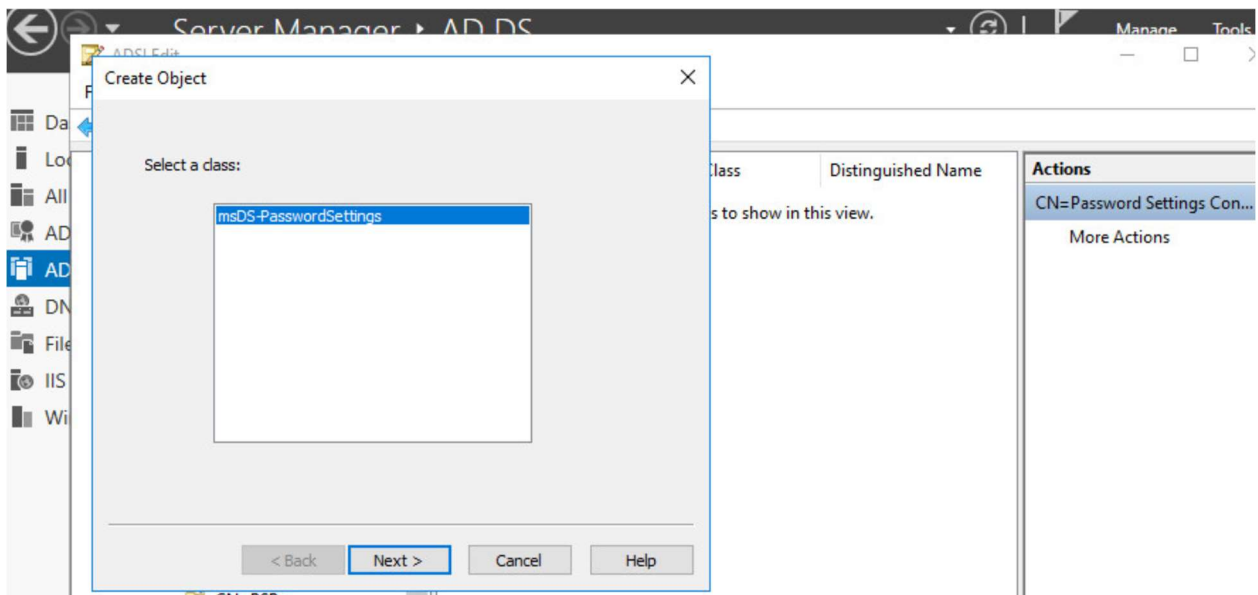
Hit OK



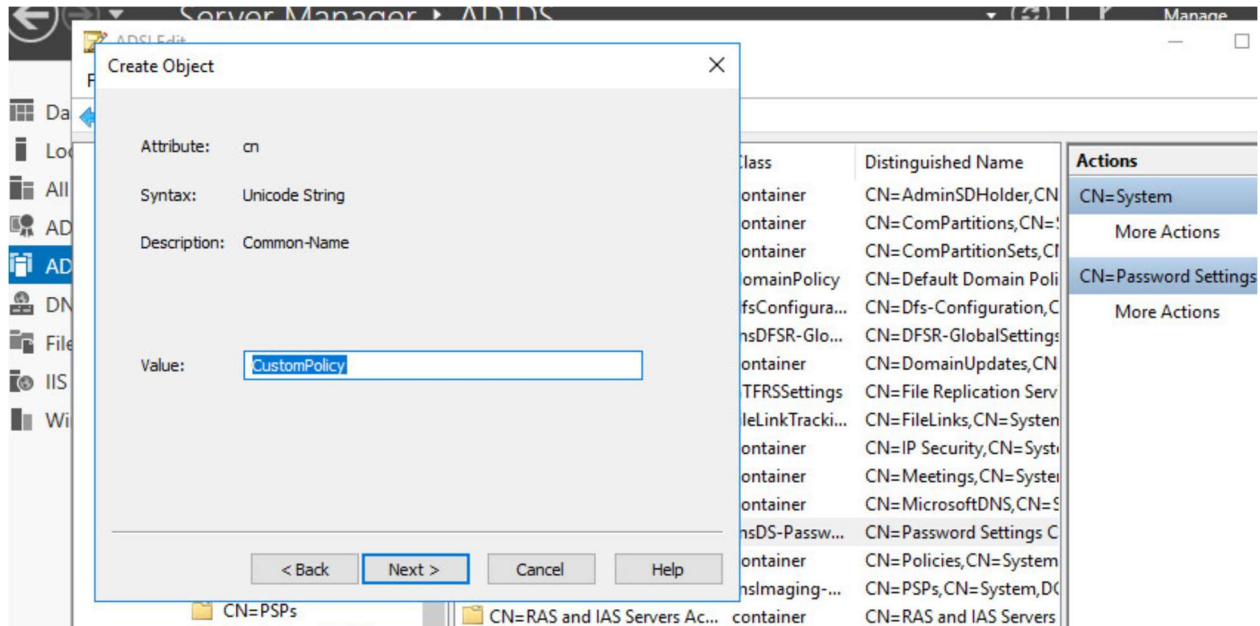
Right-click the CN=Password Settings Container under DC=NTW216NJACOB,DC=local, CN=System, select New, Object



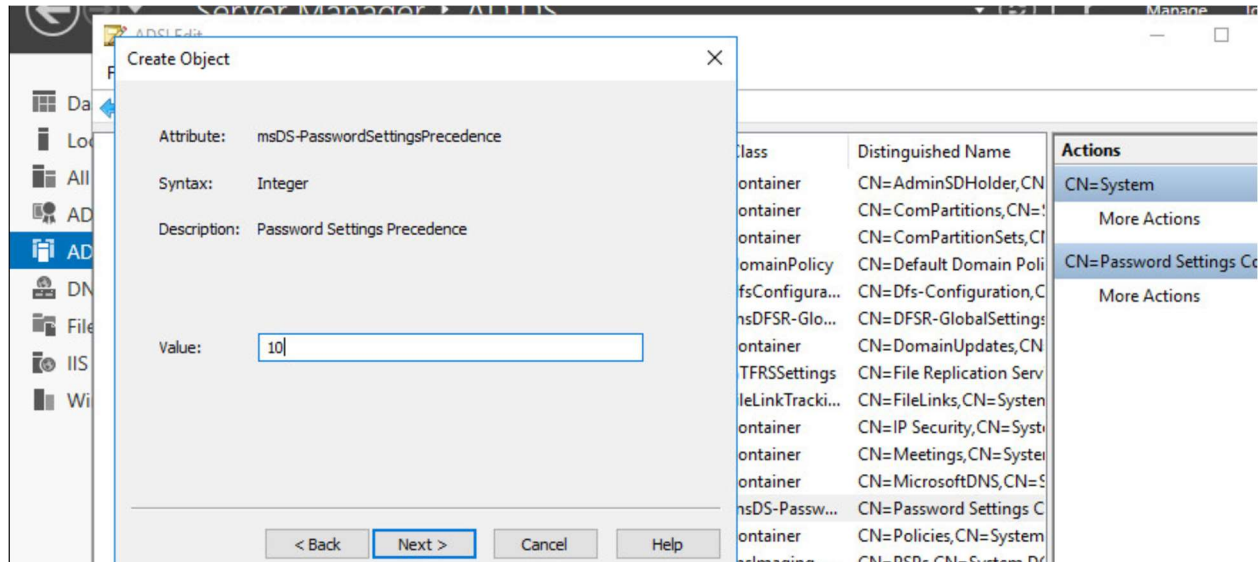
There is only one class to select, select it and hit next



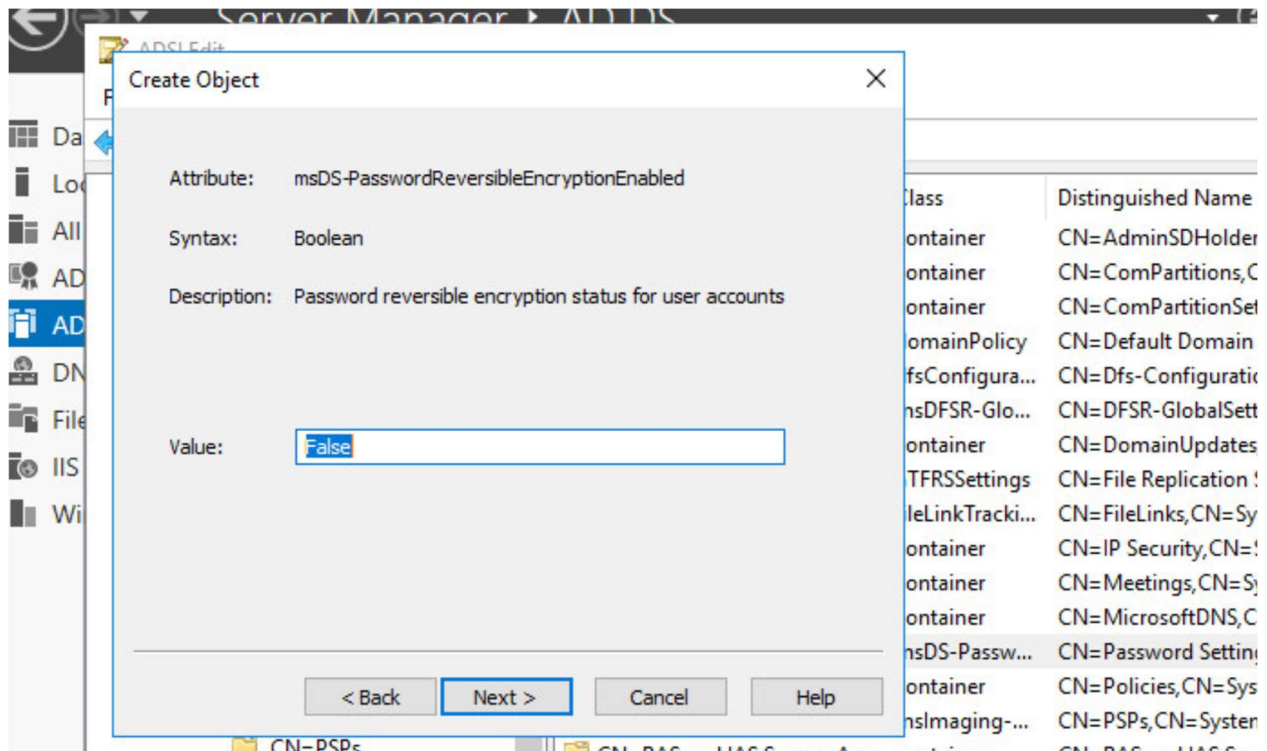
Enter CustomPolicy as the value and hit Next



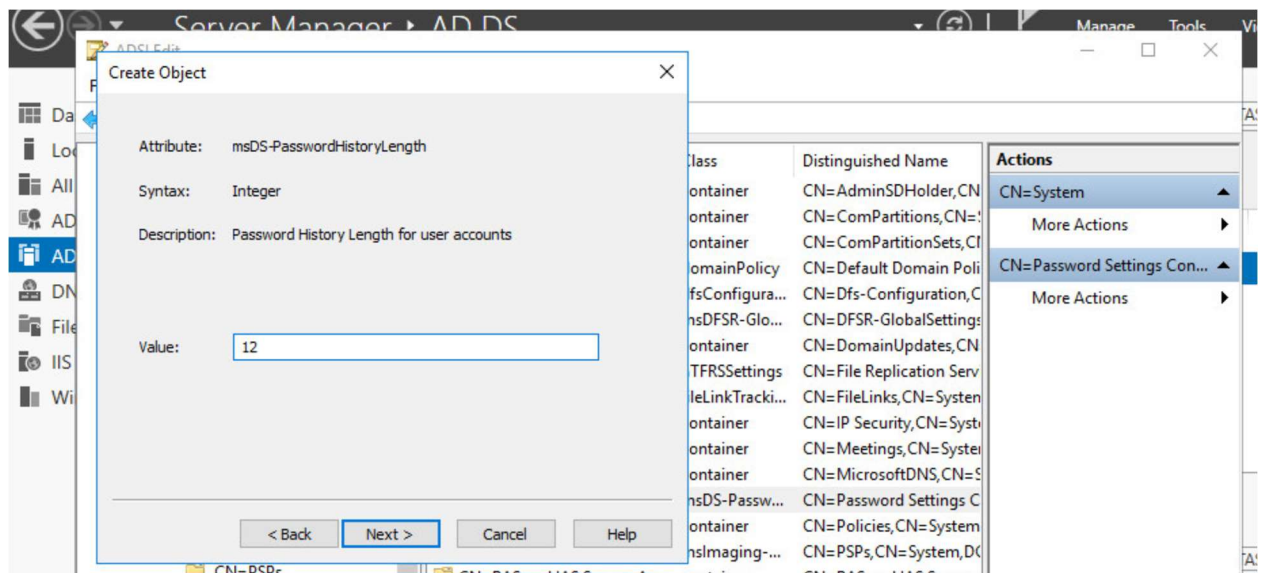
Enter 10 as your value and hit Next



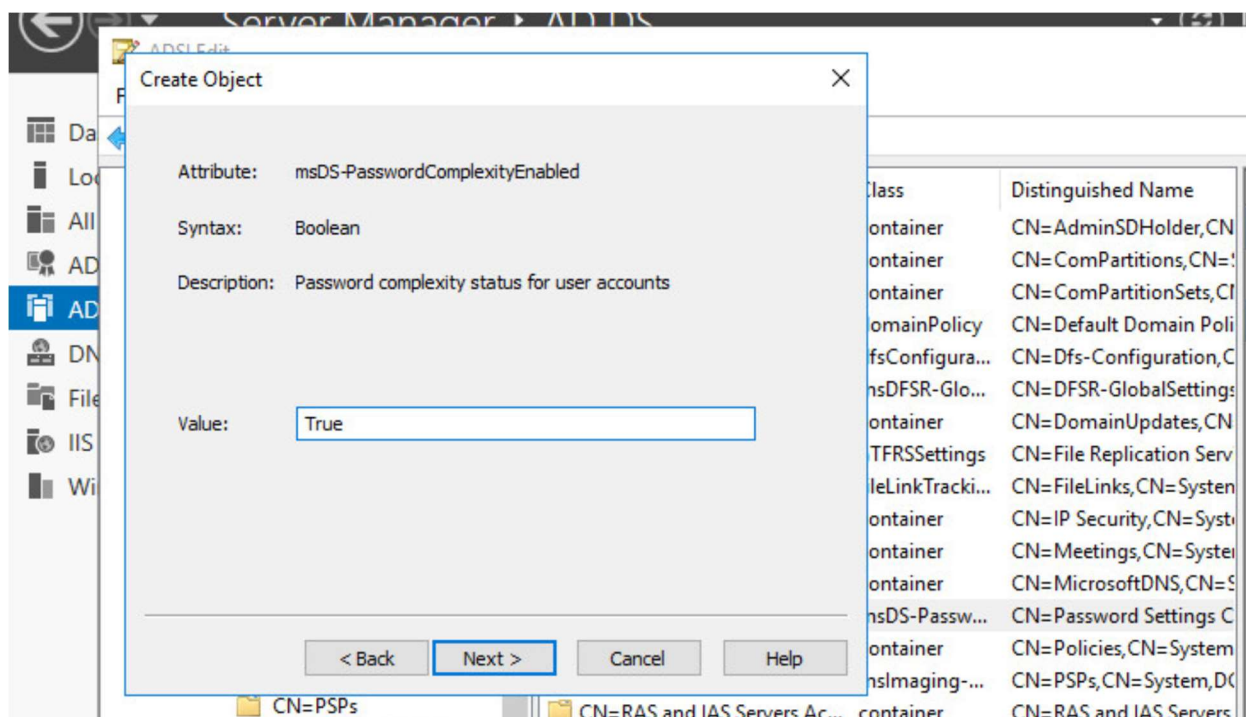
Enter False as your value and hit Next



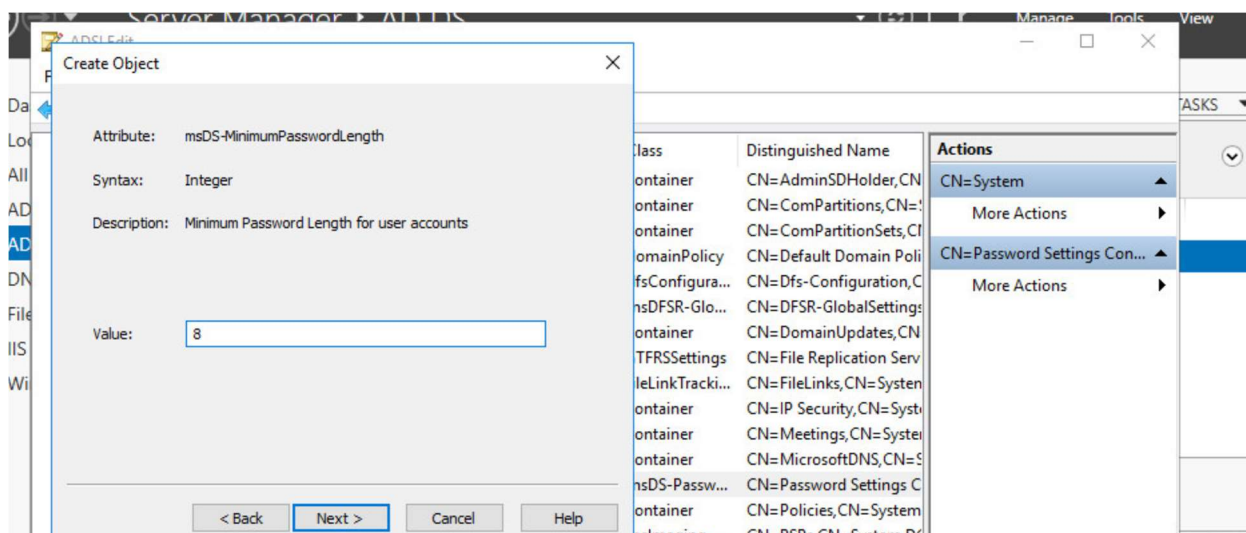
Enter 12 as your value and hit Next



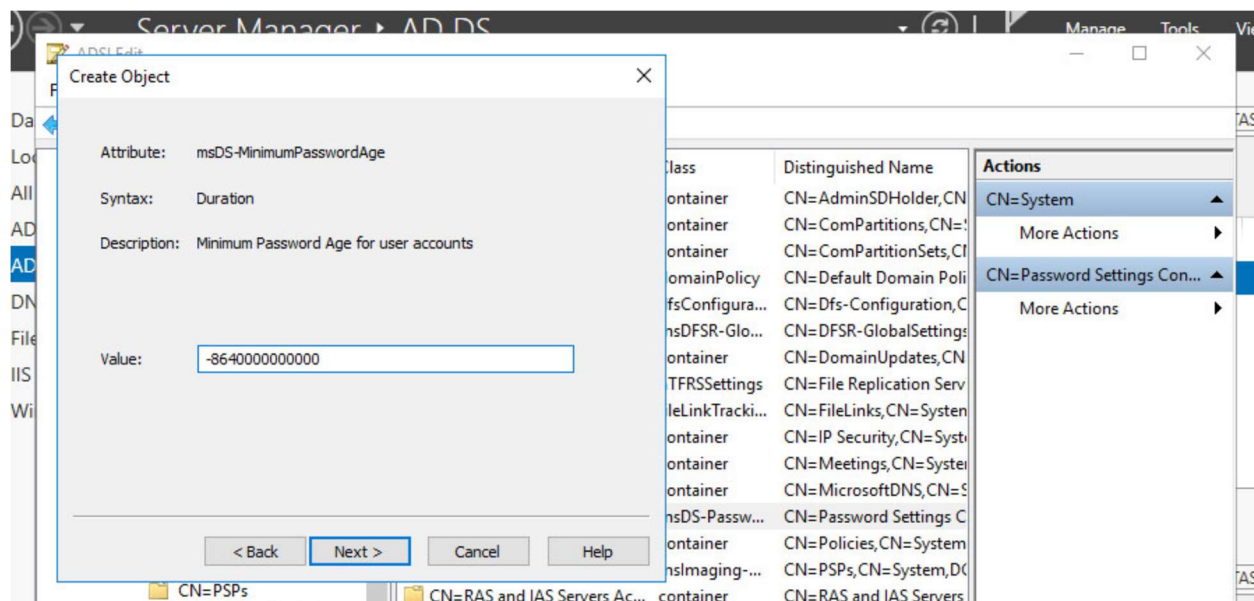
Type True as your value and hit Next



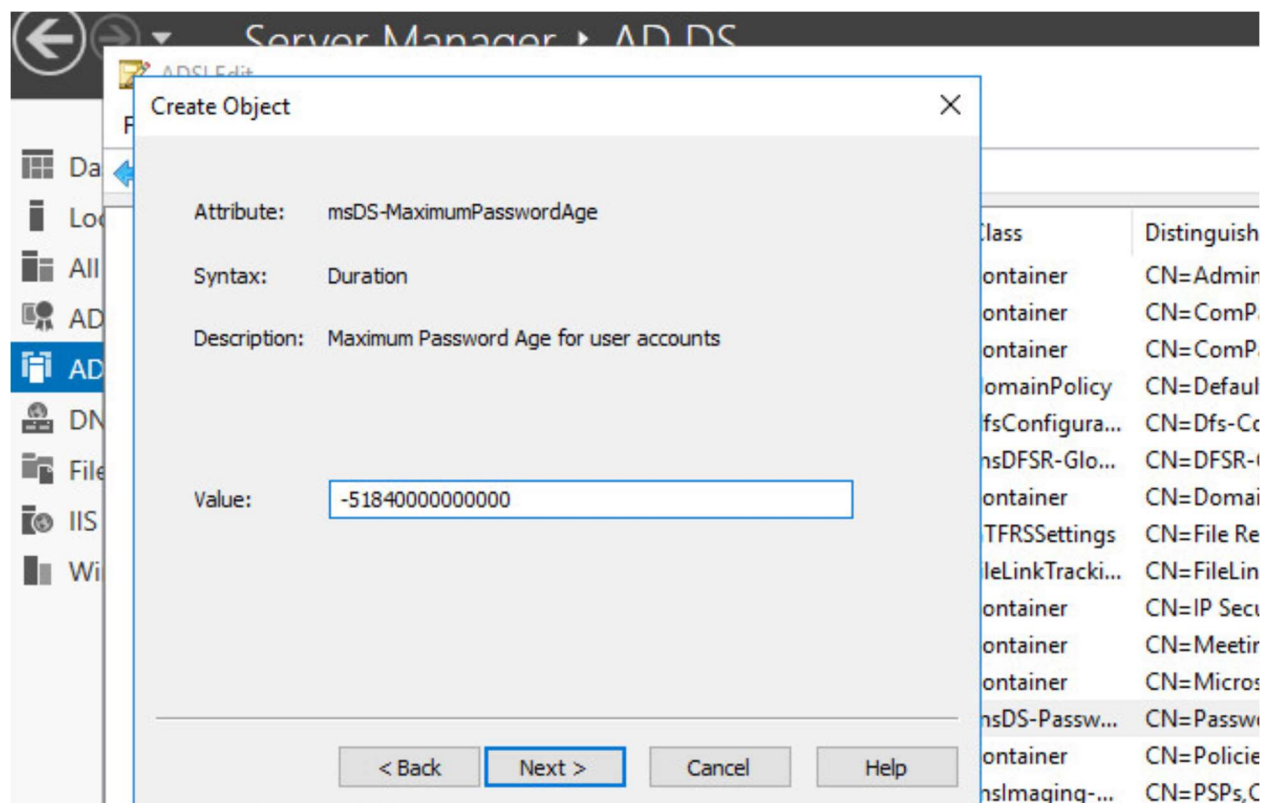
Set the value as 8 and hit next



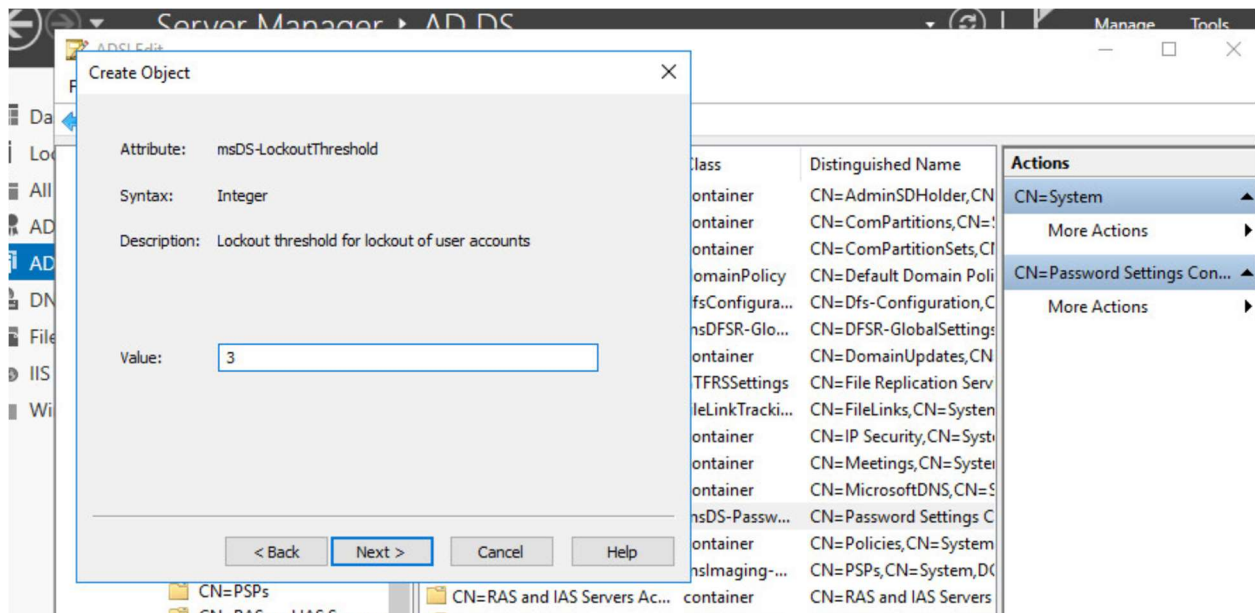
Enter -8640000000000 as your value and hit next



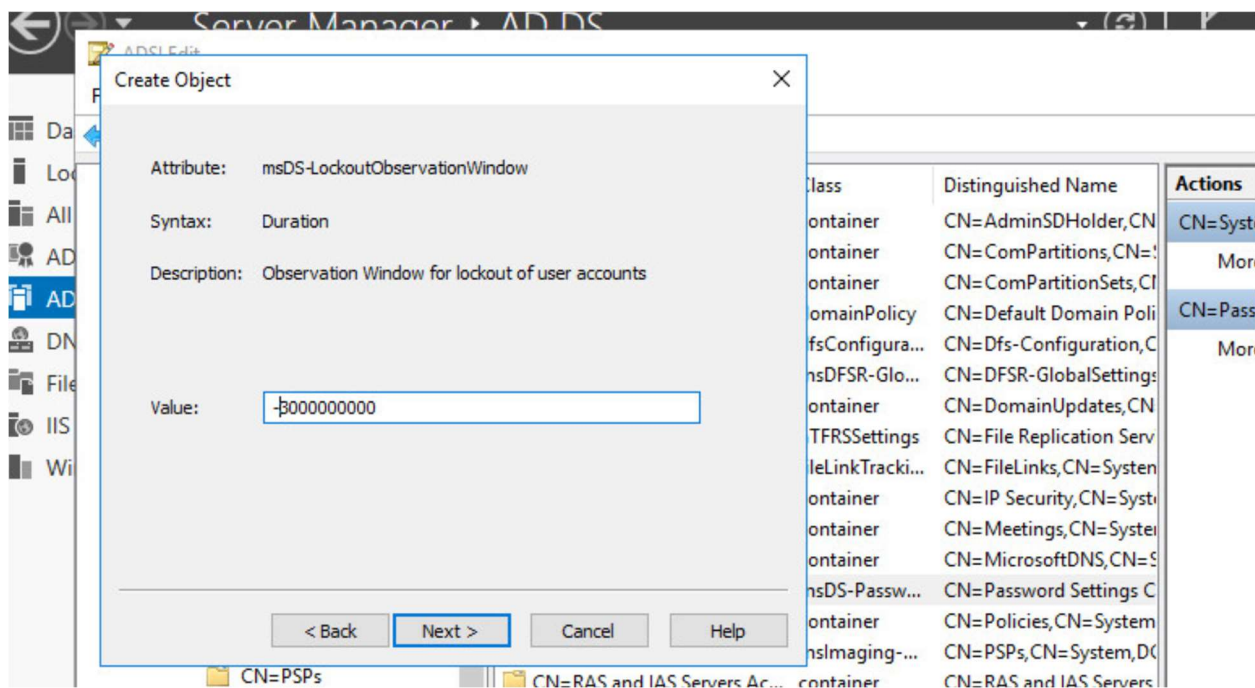
Enter -51840000000000 as your value and hit next



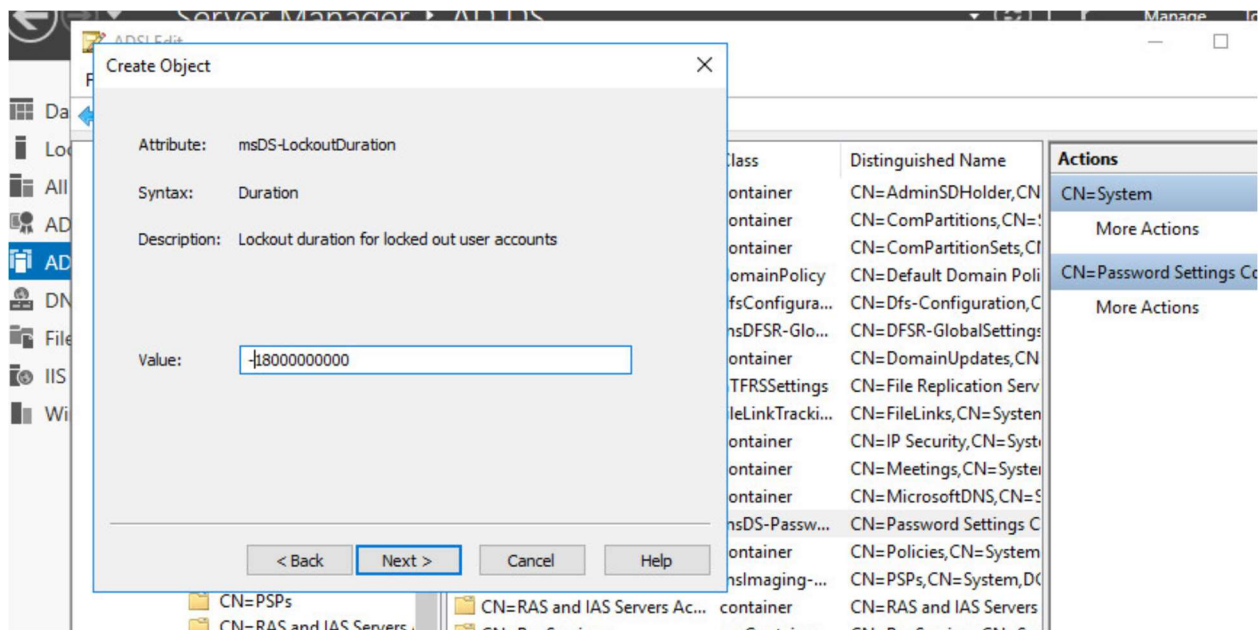
This next value will be 3, hit Next



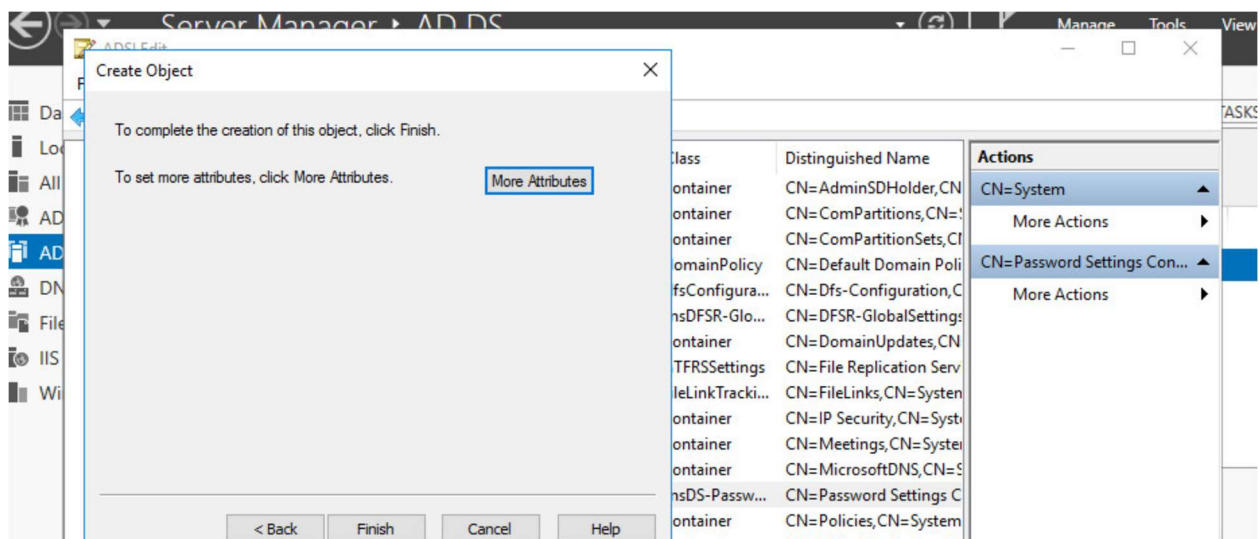
Enter -3000000000 as your value and hit Next



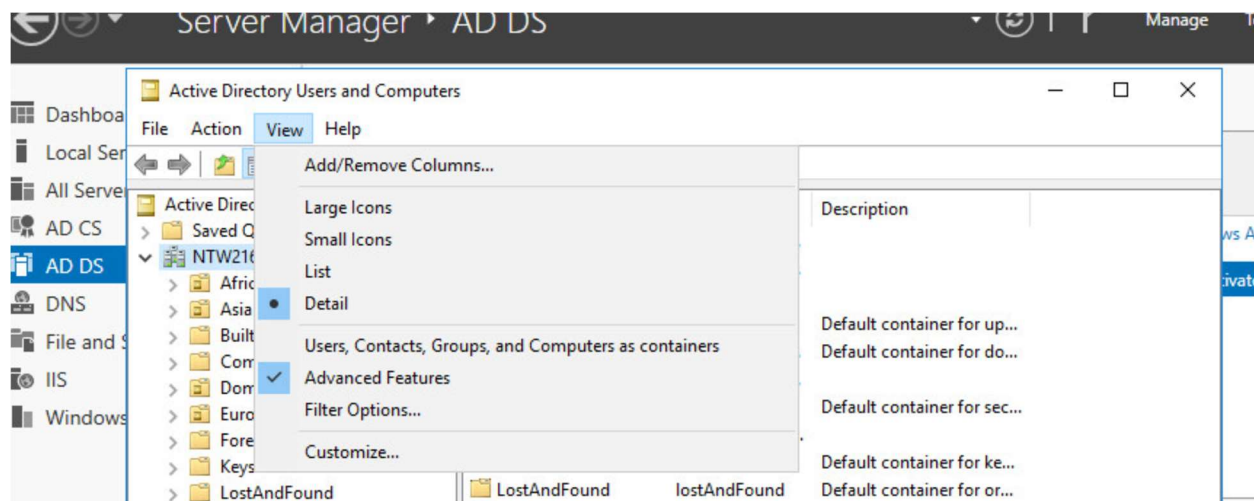
Enter -18000000000 in the Value box and hit next



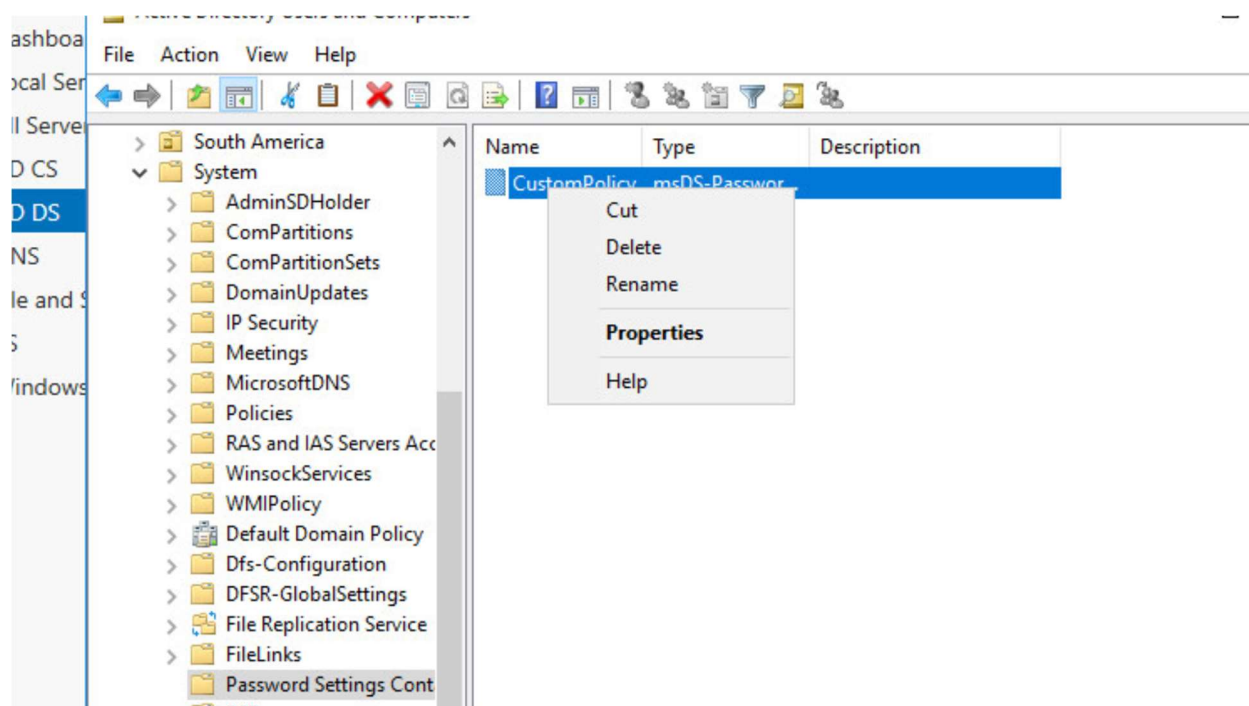
Click Finish



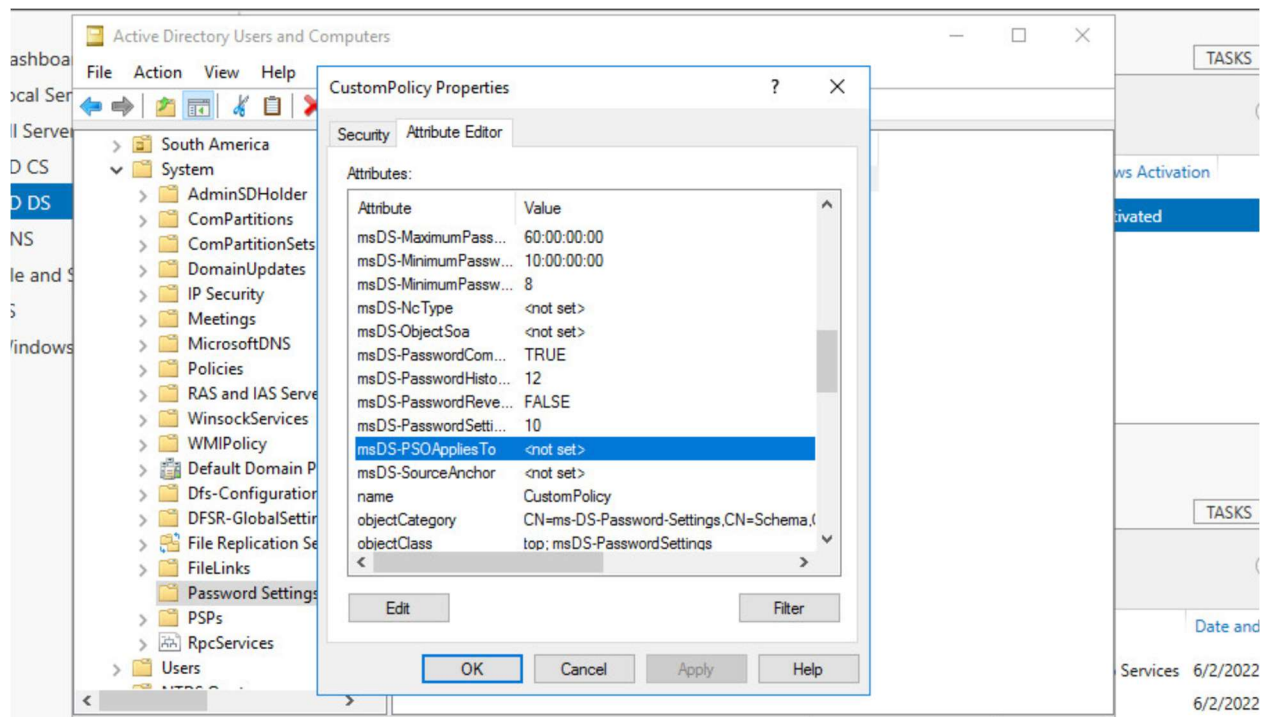
In the Active Directory Users and Computers screen Check the Advanced Features option under the View tab at the top of the window



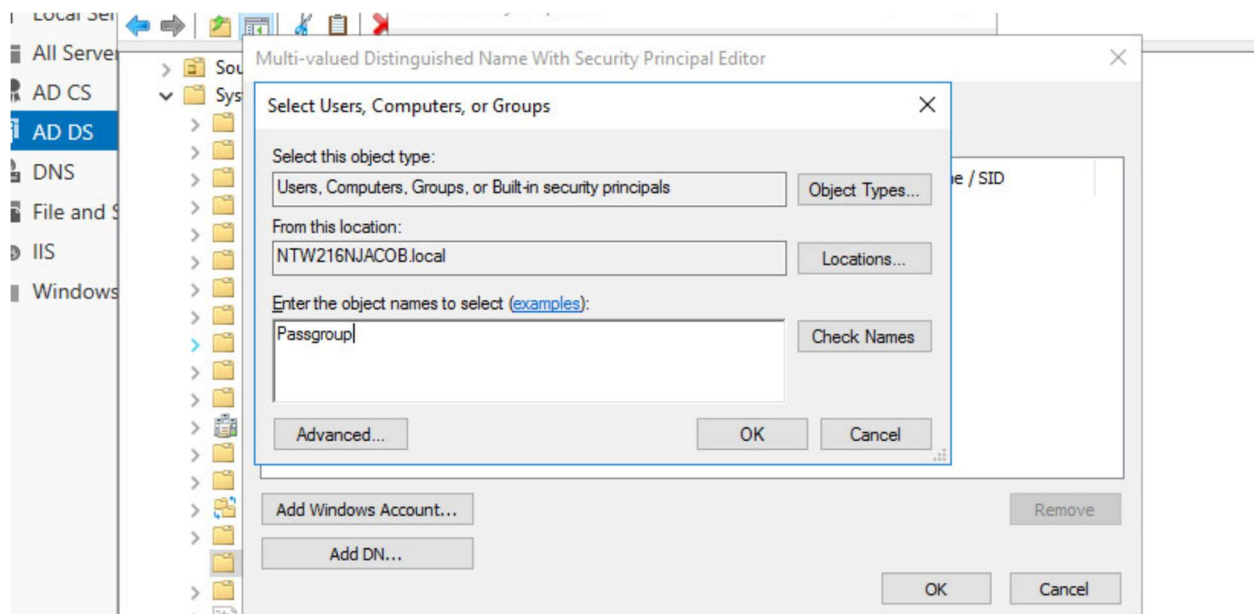
Right-click CustomPolicy under System, Password Settings container, and hit Properties



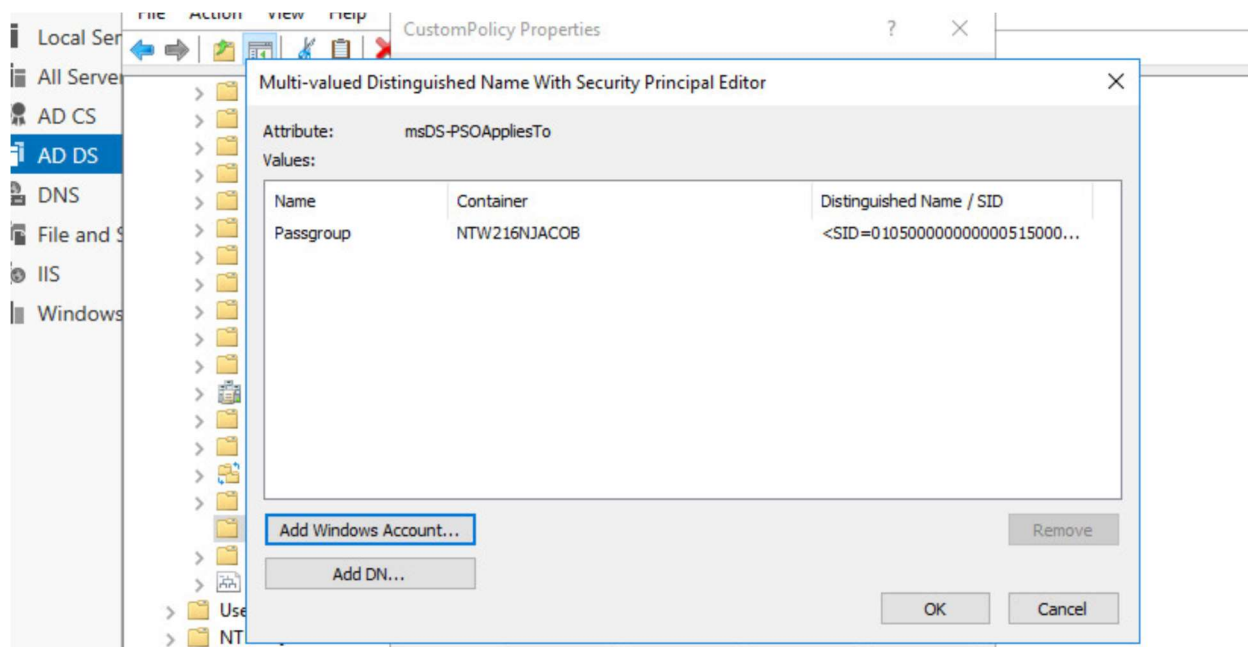
In the Attribute Editor tab, select msDS-PSOAppliesTo and hit Edit



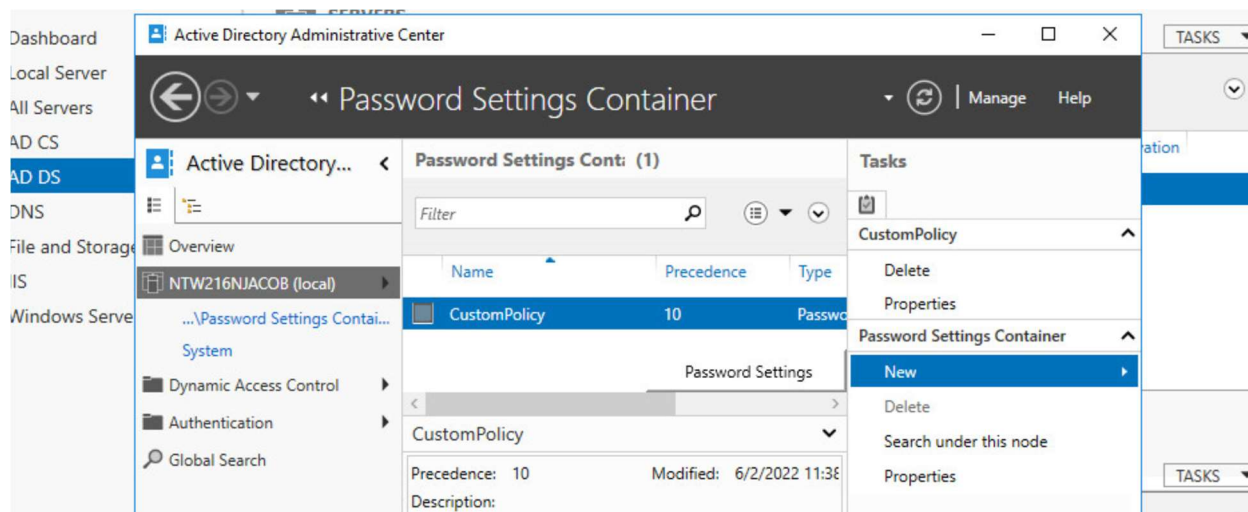
Hit Add Windows Account, Enter Passgroup and click Check Names, then OK



Hit Okay again



Open the Active Directory Administrative Center, Click Password Settings container under the domain, system. Hit New under Tasks on the right hand side and choose Password Settings



Enter the data as shown in the Screenshot

Create Password Settings: ITpso

Tasks: [Dropdown] Sections: [Dropdown]

Password Settings

Directly Applies To

Name: * ITpso
Precedence: * 10

☒ Enforce minimum password length
Minimum password length (characters): * 8

☒ Enforce password history
Number of passwords remembered: * 24

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:
IT Department Password Policy

Password age options:

☒ Enforce minimum password age
User cannot change the password withi... * 1

☒ Enforce maximum password age
User must change the password after (... * 60

☒ Enforce account lockout policy:
Number of failed logon attempts allowed: * 5
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
------	------

Add... Remove

More Information

OK Cancel

Hit Add, type IT and click Check Names then hit Ok, hit OK

Select Users or Groups

Select this object type:
Users or Groups

From this location:
NTW216NJACOB.local

Enter the object names to select (examples):
IT

Check Names

Advanced... OK Cancel

☐ 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 (... * 60

☒ Enforce account lockout policy:
Number of failed logon attempts allowed: * 5
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 a