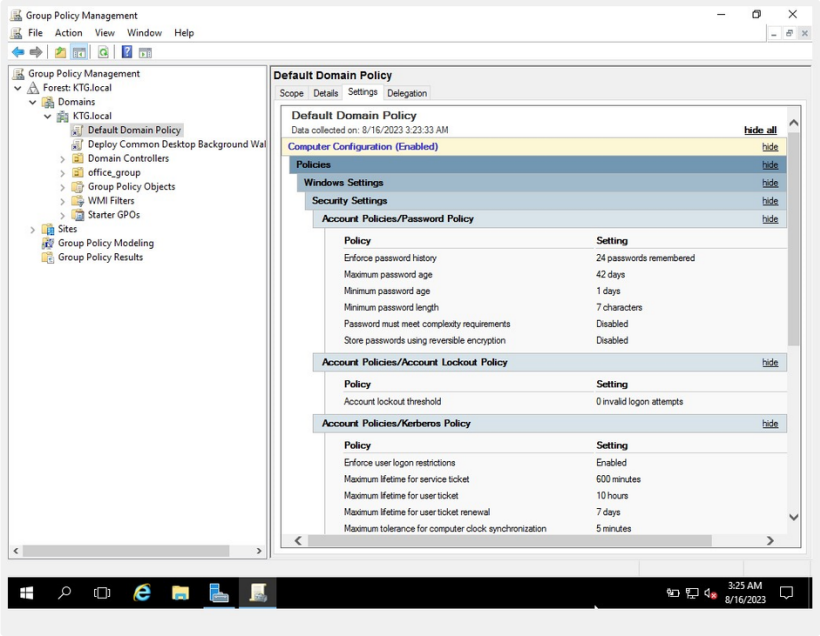
Configure an Active Directory Password Policy Using GPO.

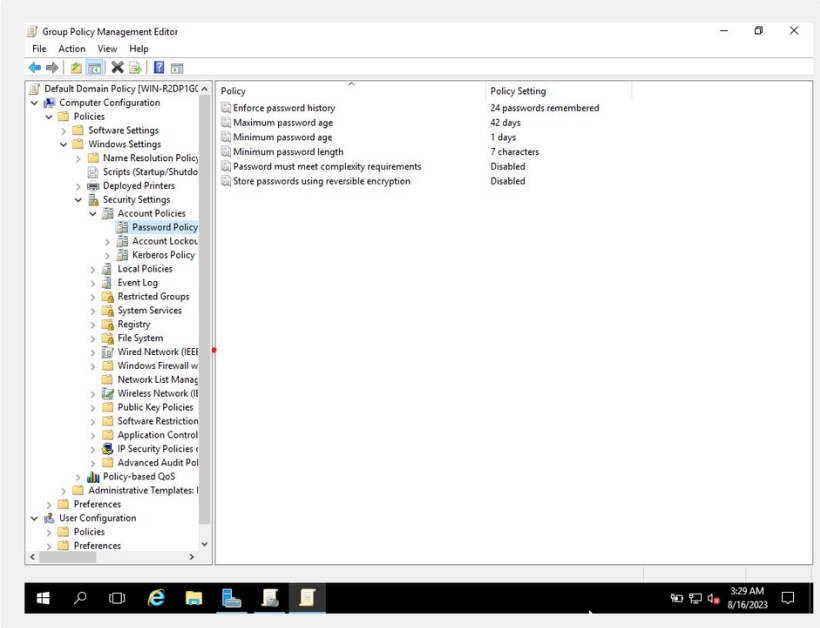
Date: 16-08-2023

Password Policy Enabling using GPO:

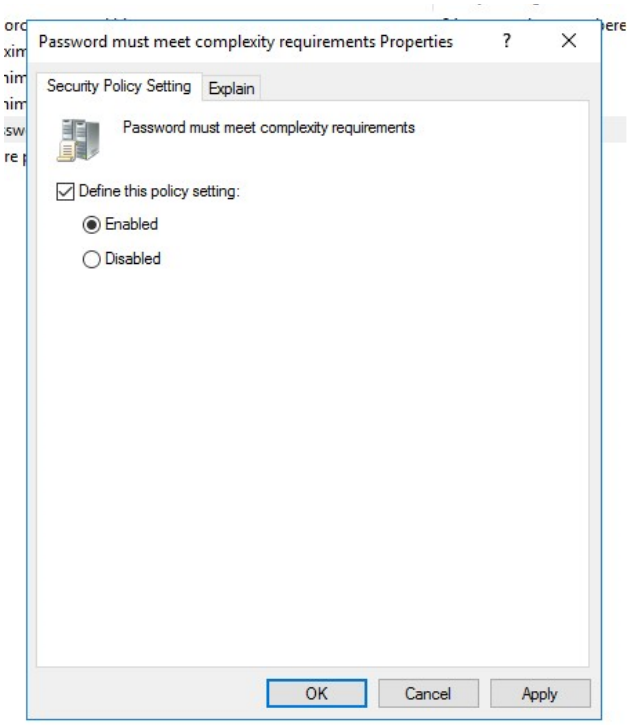
- To configure an Active Directory password policy using GPO, open windows server 2016 and go to group policy management.
- Expand the domain from left hand side, we can see Default Domain Policy. Double click on it we can see a window and go to settings >> click on show all. By this we can check the present password policies mentioned here.



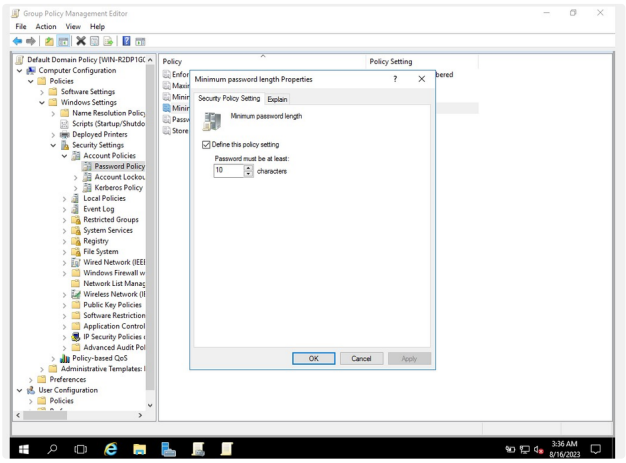
- The next step will be open Default Domain Policy and go to Computer Configuration >> Policies >> Windows Settings >> Security >> Account Policies >> Password Policies.



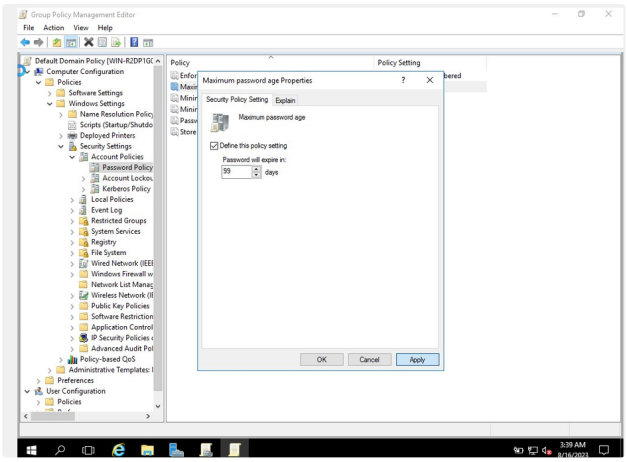
- We can see the window of password policies, which include Enforce password history, Maximum password age, Minimum password age, Minimum password length, Password must meet complexity requirements and store passwords using reversible encryption.
- Make sure that password complexity should be enabled, from the given terms 3 out of 4 should be satisfied. All four out of four rules cannot be satisfied unless we are using third party tools.



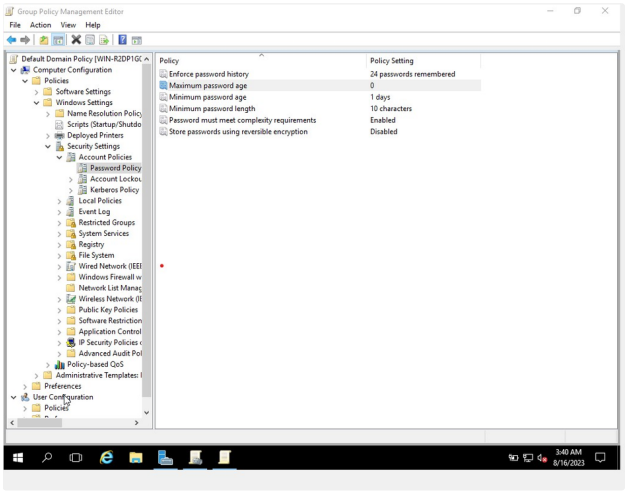
- Minimum Password length, here we can keep the maximum length up to 128 characters. By enabling the relax minimum password length limit. Password length of 10 characters is used here.



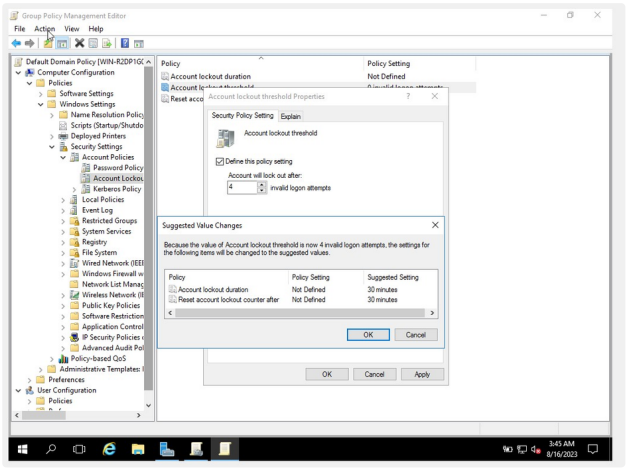
- Maximum Password Age is explained as the time period for password expiration. Here we can we give 99 days, then password will be expired after 99 days/ zero in this case password will not be expired.



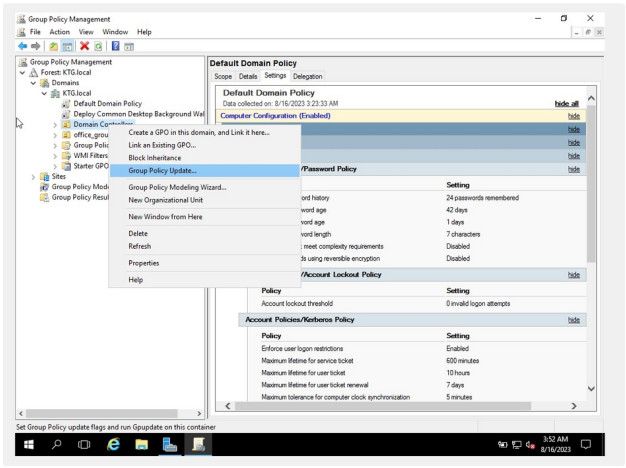
- Enforce Password History generally used in conjunction with the password history so when a password expires it stores someone else changing the password 24 times one after the other and then go back to their same old password.



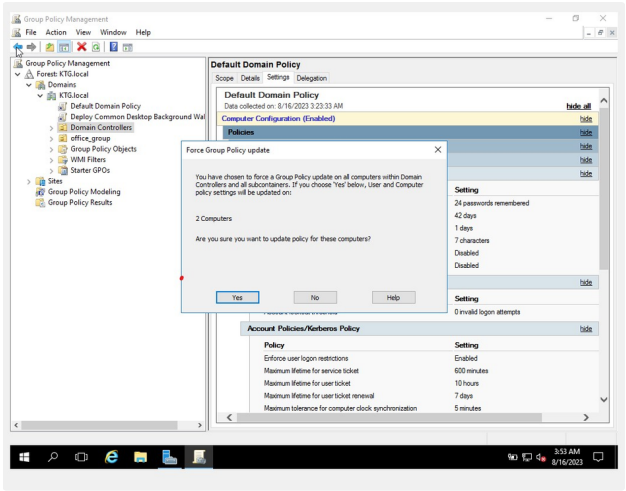
- Account Lockout Policy, by default it is disabled but we can enable it. By clicking on Account Lockout policy, we can see a window mentioned with Account Lockout Duration, Account Lockout Threshold, Reset Account Lockout Counter.
- Click on Account Lockout Threshold, it explains that if someone puts an incorrect password in for an account, however many times. I generally set it to four, so if someone puts a wrong password 4 times in a row, what will happen is lock that account. By default, it gets locked for 30 minutes and then automatically unlocks it.
- Account Lockout Duration, using this however we can do is to set it to zero, so then if I can't get locked out for bad passwords. An administrator has to then unlock it, but we generally leave it to 30 minutes.



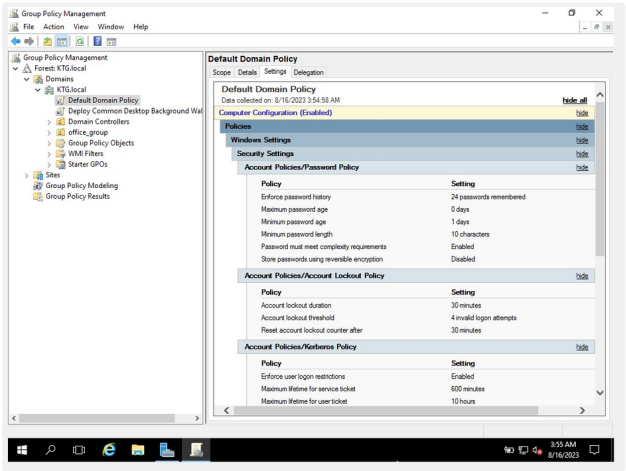
- Now we've configured the group policy password policy settings. now we need to close the global policy editor.
- Go to Default Domain Policy, right click and update the group policy and refresh it, now open the wizard and click on show all to see the changes we made during the configuration process.



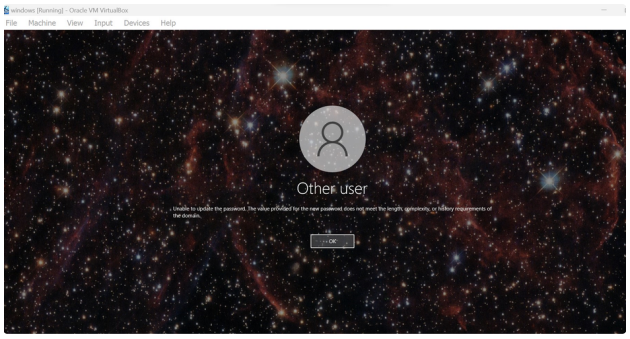
- Now we will get a pop-up of force group policy update as shown below.



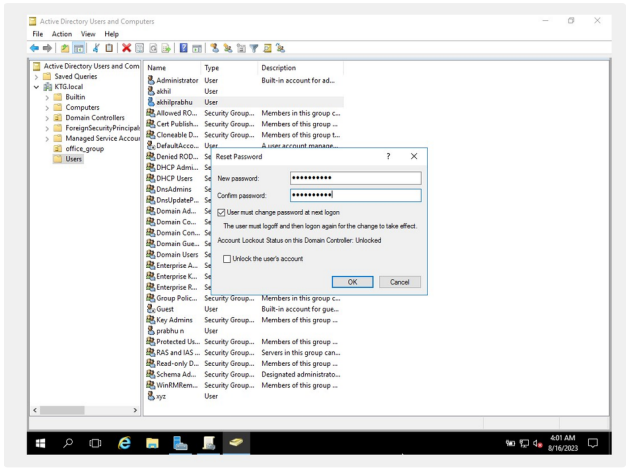
- After configuring the process and updating the group policy we can see the results of password policies that we have updated.



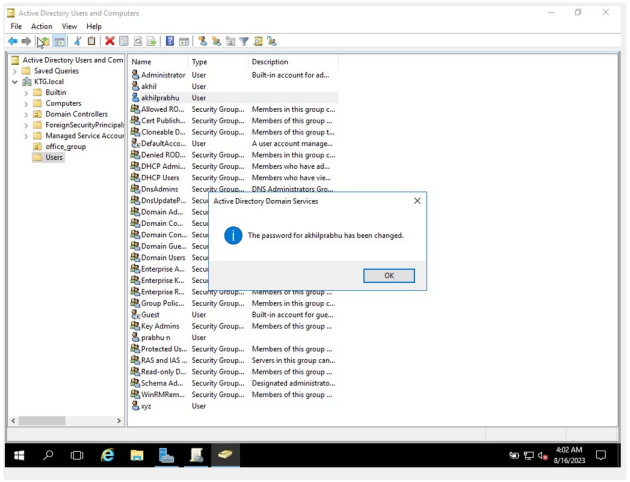
- To test this we need to update the group policies in the command prompt using the command gpupdate /force. Now open server manager and go to Active Directory Users and Computers, pick an user and try to give a password without following the rules.



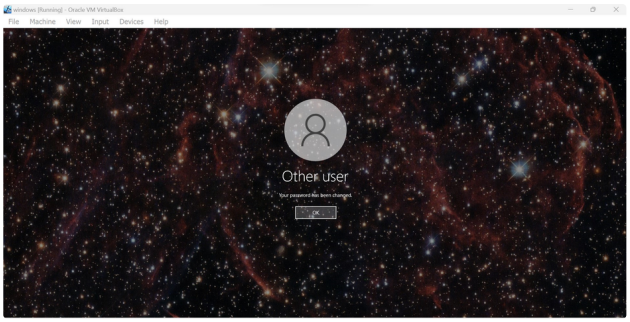
- We are unable to create a password without following the terms mentioned during the configuration.
- We need to reset the password by applying the rules then only we can proceed froward.



- After following the rules, we can get a pop-up of successfully created password.



- Now we can login into the account by creating the password with the policy configuration that we have made.



- By default, Windows allows only one password policy per domain. However, in Windows Server 2008 and later, you can implement Fine-Grained Password Policies (FGPP) to set different policies for specific groups or OUs.
- Regularly review and update the password policy to stay current with security best practices. Consider annual or semi-annual reviews and make adjustments as needed.