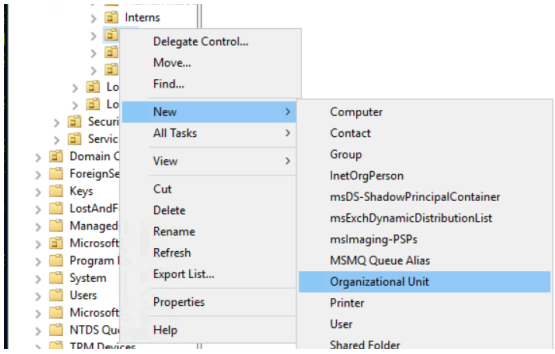
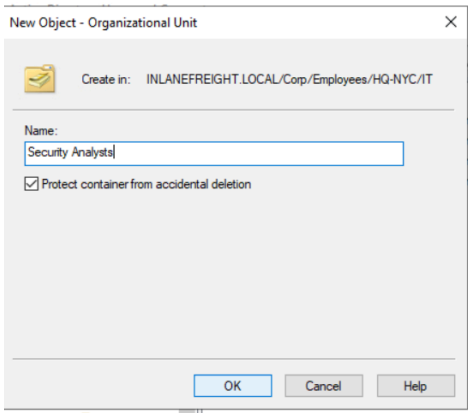
Configuring groups and performing basic administrative tasks with Microsoft Active Directory (part 2)

Creating a new group and adding new-hires to it

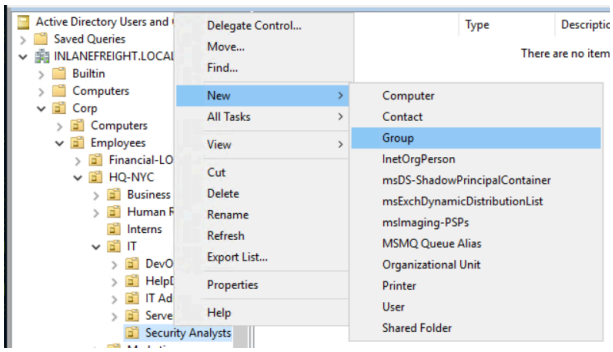
I now needed to create a new group within the IT hive and add the new-hires to this group.



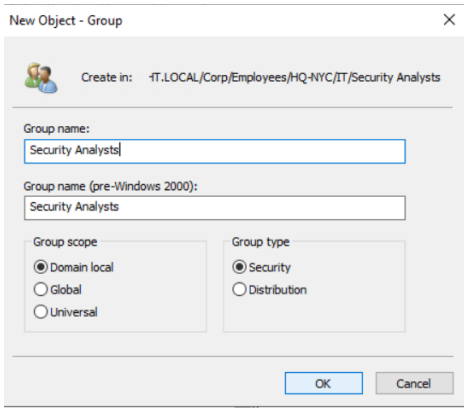
To do this, I right-clicked on IT before selecting ‘New’ followed by ‘Organizational Unit’



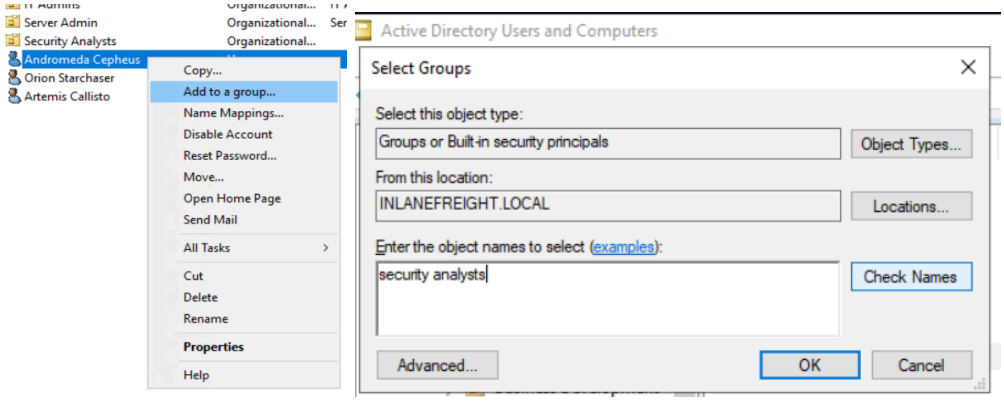
This opened up the page displayed above. I the inputted the name of the OU before clicking on ‘OK’



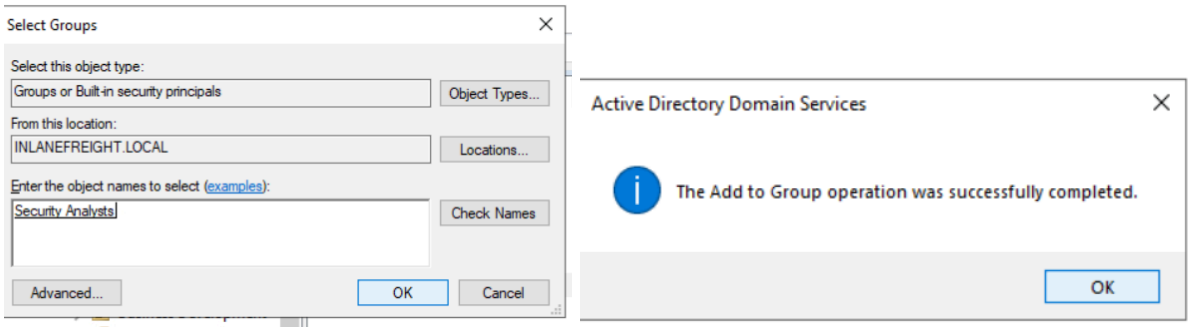
I now needed to right-click on the new organisational unit that I had created (Security Analysts), to create the new group within it. I clicked on ‘New’ before selecting ‘Group’.



This opened up the window displayed above. I then needed to name the group and select the scope and type of the group. I selected ‘Domain local’ and ‘Security’ before clicking ‘OK’.



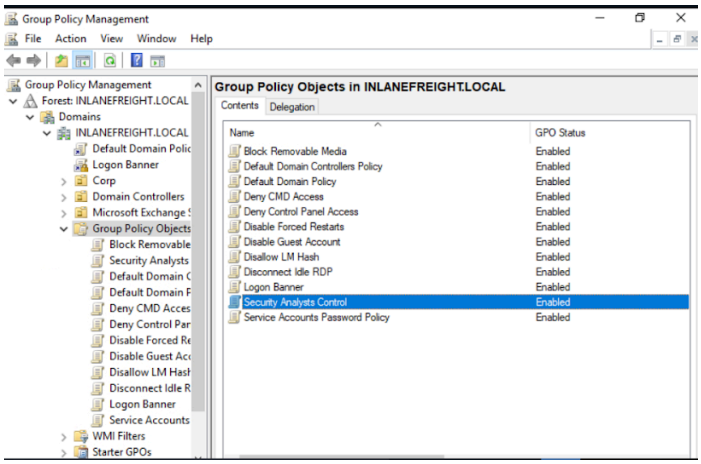
The group had now been created and I now needed to insert the new-hires into it. To do this, I found their accounts in the ‘IT’ OU and right-clicked them before selecting ‘Add to a group…’ as shown in the first screenshot above. This opened up the page displayed in the second screenshot above. I now needed to search for the group that I had just created, by inputting the name of the group, before clicking on ‘Check Names’.



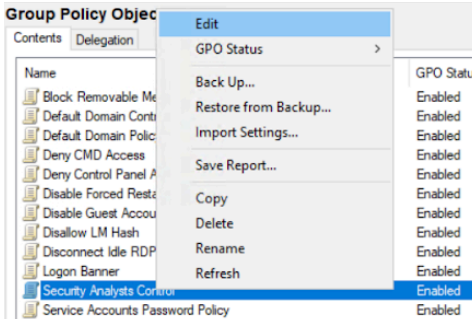
After seeing the name of the group had become underlined as shown in the first screenshot above, I knew that the group had been found and selected. I then clicked ‘OK’ after which the prompt shown in the second screenshot above was presented, to which I clicked ‘OK’. The new-hires had now been added to the new group ‘Security Analysts’.

Configuring a group policy

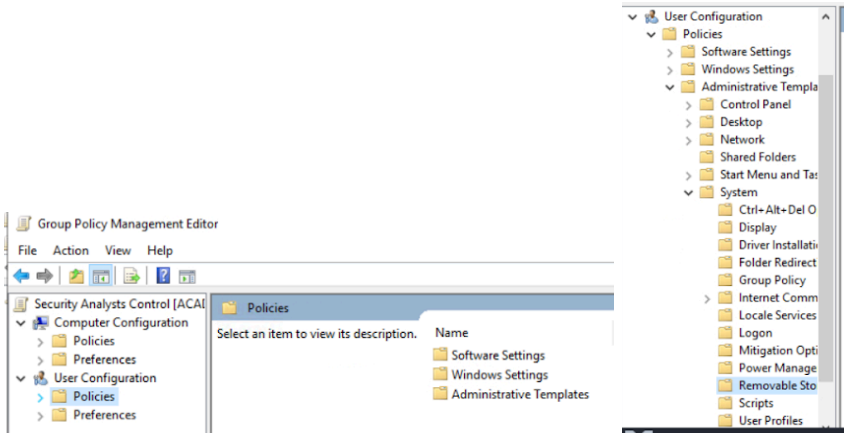
I now needed to modify the group policy for the new group that I had created, so that users within it could access CMD while removable media access was blocked. I also needed to update password policy settings.



Firstly, I opened GPMC and then expanded ‘Group Policy Objects’. I then made a copy of the group policy ‘Logon Banner’ as instructed because I only needed to modify this copied version to complete the new group policy, instead of creating a brand new one. I renamed this policy to ‘Security Analysts Control’ as displayed in the screenshot above.

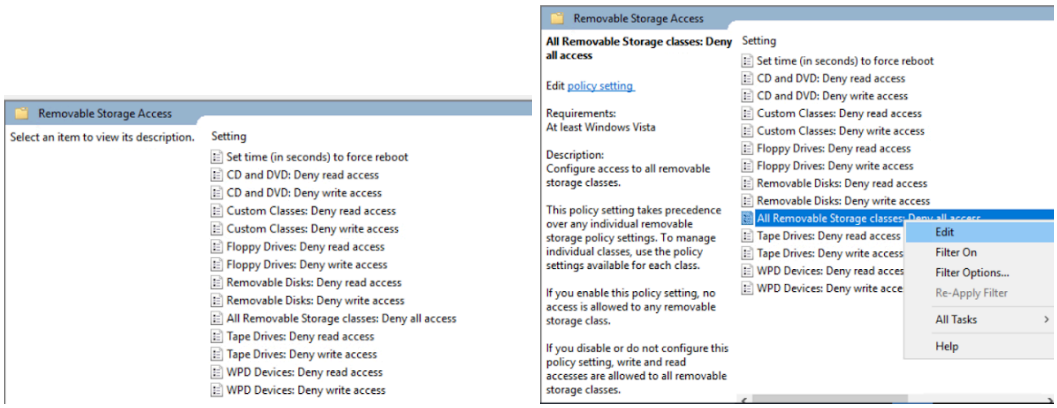


In order to begin modifying the policy, I right-clicked it before selecting ‘Edit’ as shown in the screenshot above.

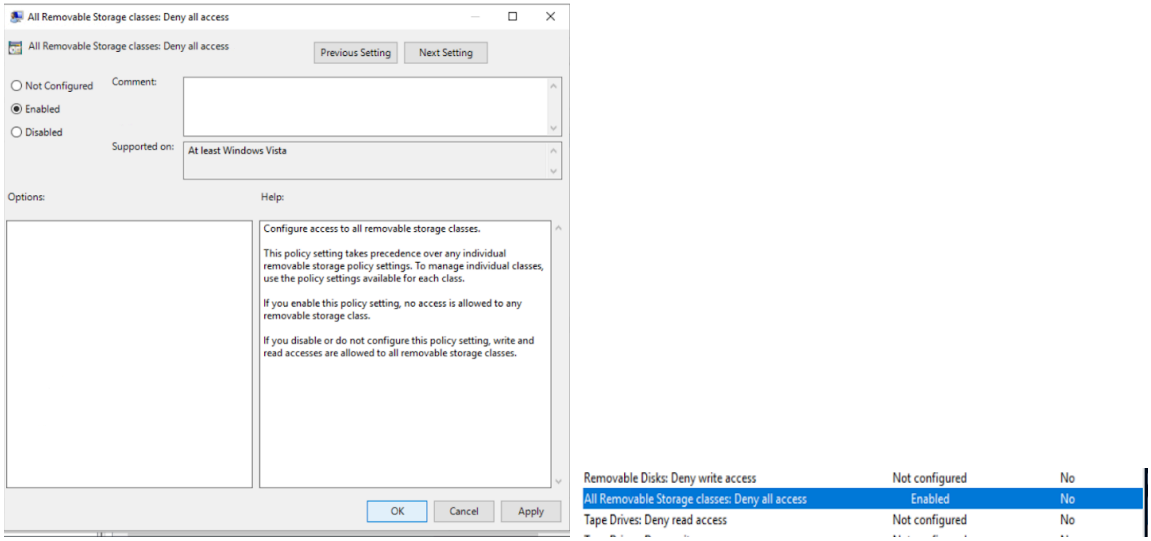


This opened the page displayed in the first screenshot above. I now need to navigate my way to ‘Removable Storage Access’ by expanding ‘Policies’ under ‘User Configuration’, then

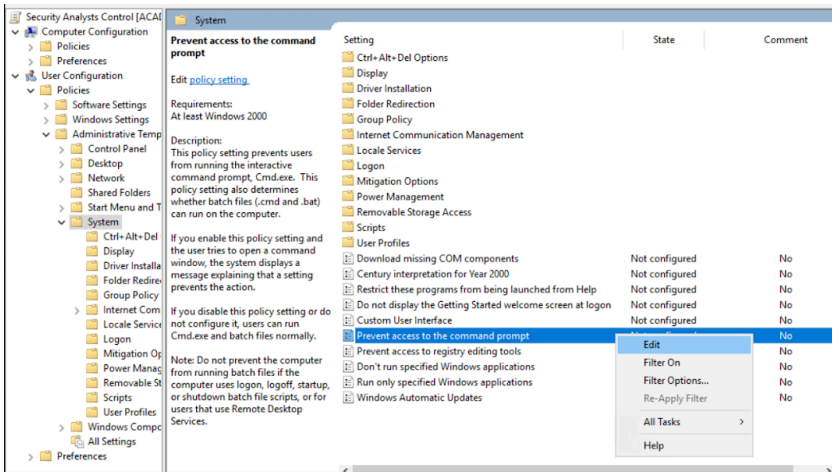
‘Administrative Templates…’ followed by ‘System’ and finally ‘Removable Storage Access’. This navigation process is portrayed in the second screenshot above.



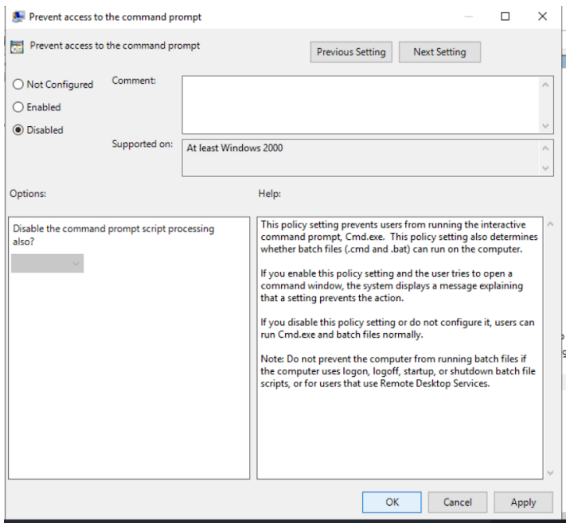
The settings displayed above appeared within ‘Removable Storage Access’. I then right-clicked on ‘All Removable Storage classes: Deny all access’ and selected ‘Edit’.



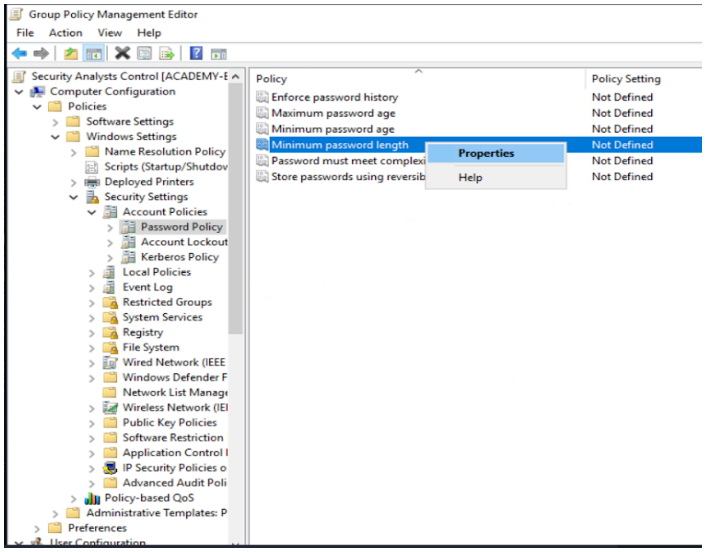
This opened up the window displayed in the first screenshot above. I then selected the ‘Enabled’ option before clicking ‘Apply’ followed by ‘OK’. As shown in the ‘Help’ section in the first screenshot above, we can see that by enabling this policy setting, all access to removable storage classes will be denied. The second screenshot shows that the policy setting has been changed to ‘Enabled’. I now needed to enable access to CMD for the users in this group as it is required for their jobs.



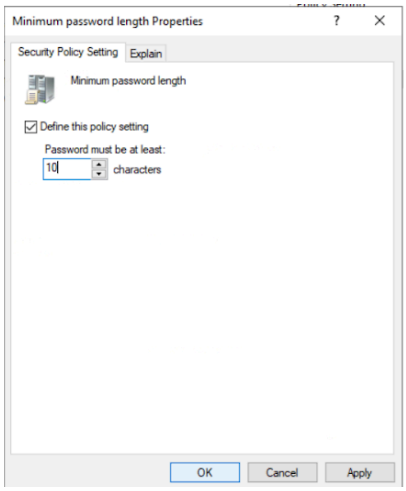
To do this, I navigated back to the ‘System’ hive under ‘User configuration’ as shown in the screenshot above. I then right-clicked ‘Prevent access to the command prompt’ before selecting the ‘Edit’ option.



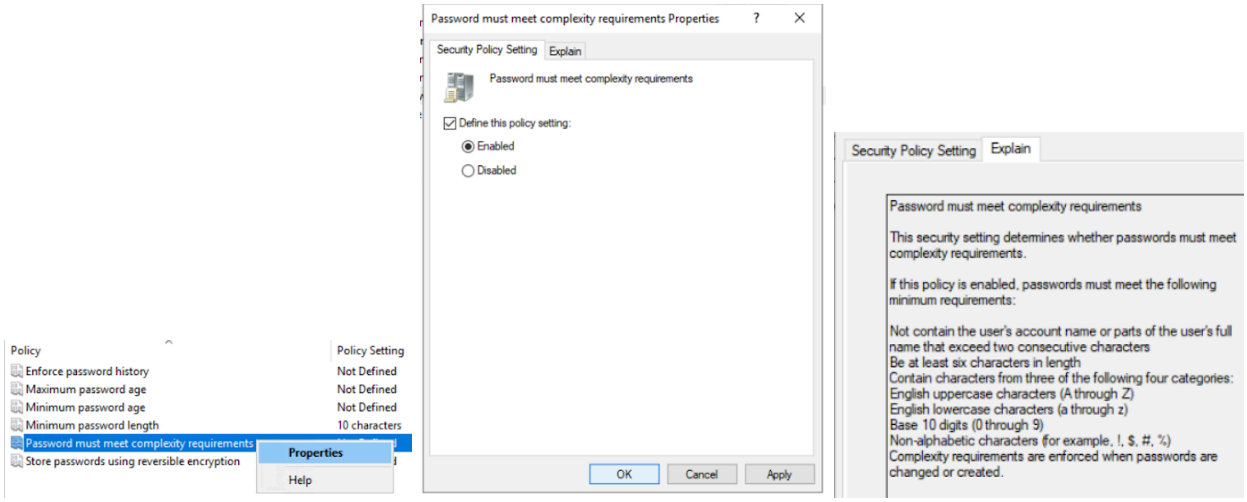
I then selected the ‘Disabled’ option before clicking ‘Apply’ followed by ‘OK’ as displayed in the first screenshot above. As shown in the ‘Help’ section in the first screenshot above, we can see that by disabling this policy setting, access to CMD will be granted. The second screenshot above shows that this policy setting has now been disabled meaning that users within this group would be able to utilise the command prompt- Cmd.exe as required by their jobs. I now needed to modify group policies that affect computers within this group, in particular the password policies.



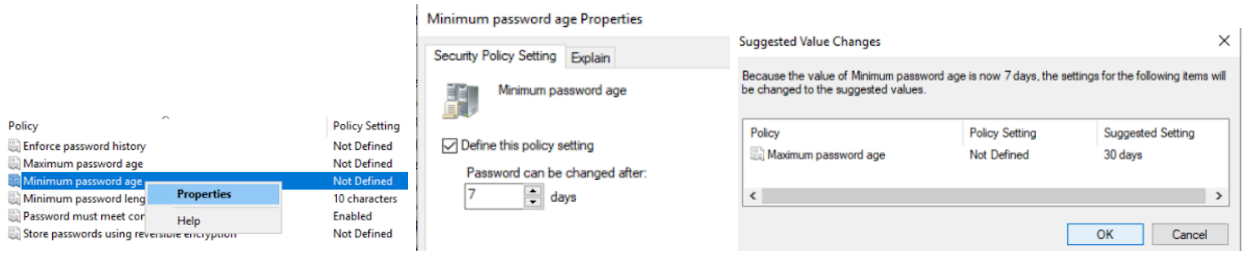
To do this I needed to navigate to the ‘Password Policy’ section. To do this, I expanded the ‘Computer Configuration’ hive (earlier, I was in ‘User Configuration’) before expanding ‘Policies’. I then expanded ‘WIndows Settings’ then ‘Security Settings’ followed by ‘Account Policies’. I then clicked on ‘Password Policy’ as shown in the screenshot above. I then right-click on ‘Minimum password length’ before selecting ‘Properties’.



This opened up the window displayed above. I then checked the box ‘Define this policy setting’ before inputting the number 10 in the box shown in the screenshot above. This means that users of computers within this group will have to create passwords that are a minimum of 10 characters long. I then clicked ‘Apply’ before ‘OK’.



I then opened up the ‘Properties’ window for ‘Password must meet complexity requirements’. This opened up the window shown in the second screenshot above. I then checked the ‘Define this policy setting’ before selecting ‘Enabled’. This means that passwords must now also meet the complexity requirements defined by the company as shown in the third screenshot above.



I then opened the ‘Properties’ window for ‘Minimum password age’ to determine how long a user must use a password before they can change it. This opened up the window displayed in the second screenshot above. I then checked the ‘Define this policy setting’ box before inputting the number 7 in the box shown in the second screenshot above. I then clicked on ‘Apply’ which opened up the window displayed in the third screenshot above. This window suggested a ‘Maximum password age’ (how long until the user must reset their password) of 30 days, to which I clicked ‘OK. I then clicked ‘OK’ again. I had now set the password policy settings for users using computers in the new group I created.

Summary

In this project I learned how to perform basic administrative tasks in Microsoft Active Directory such as adding/removing users in AD, resetting locked accounts, creating groups, and adding users to those groups. I then configured the group policies of that group by modifying access to removable storage and CMD as well as enabling and defining password policies. This has been a very interesting experience as I was exposed to software that IT professionals use in their jobs and the tasks that they complete.