Managing Active Directory

Work Station:
One of the most common devices, within the active directory. Each user in the domain will likely be logging onto a workstation. This is done to do work, or browse. These devices should never have a privileged user signed into them.

Servers:
Second most common within an active directory domain, generally used to provide services to the user or other servers.

Domain Controllers:
Third most common device within the active directory. These allow you to manage the active directory in an OU created by windows.

Group policies:
Group Policy Objects (GPO) Are a collection of settings that can be applied to the OUs. They can be aimed at either users or computers.
Go to start menu - Group Policy Management Tool

1. GPOs are created in the Group Policy Objects section.
2. GPOs are then assigned to OUs.

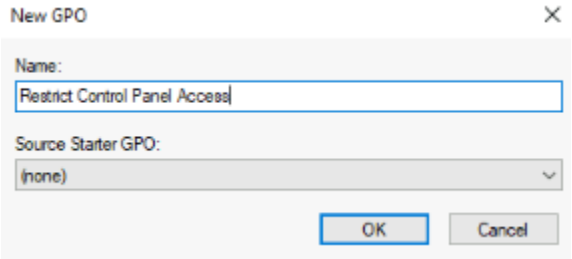
GPOs are distributed to the network via a network share called SYSVOL.
C:\Windows\SYSVOL\sysvol
Once a change has been made to sysvol however it can take up to 2 hours for a computer to catchup.
You can manually force this to speed up by doing:
gpupdate /force

PRACTICAL EXAMPLE:
As part of our job, we have been tasked with implementing some GPOs which will:

1. Block non-IT users from accessing the control panel
2. Make workstations and servers lock their screen automatically after 5 minutes of user inactivity to avoid people leaving their stations exposed.

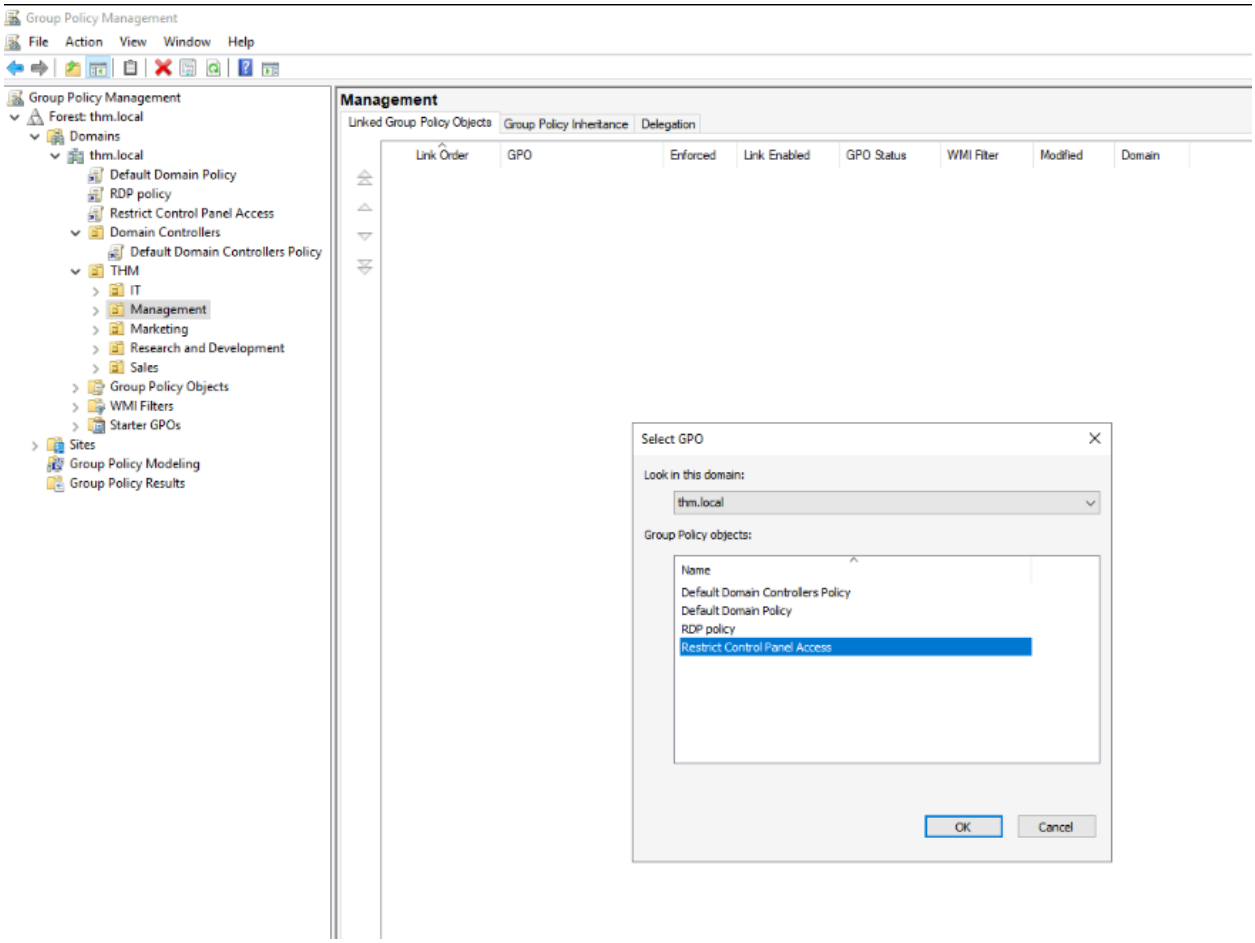
First thing I did was launch the Group Policy Objects application via the search bar which brought up the application.
I saw that there were already 3 prefabricated policies on there, Default domain controllers policy, default domain policy and finally RDP policy.

Now upon right-clicking the thm.local I could “Create GPO in this domain and link it here”

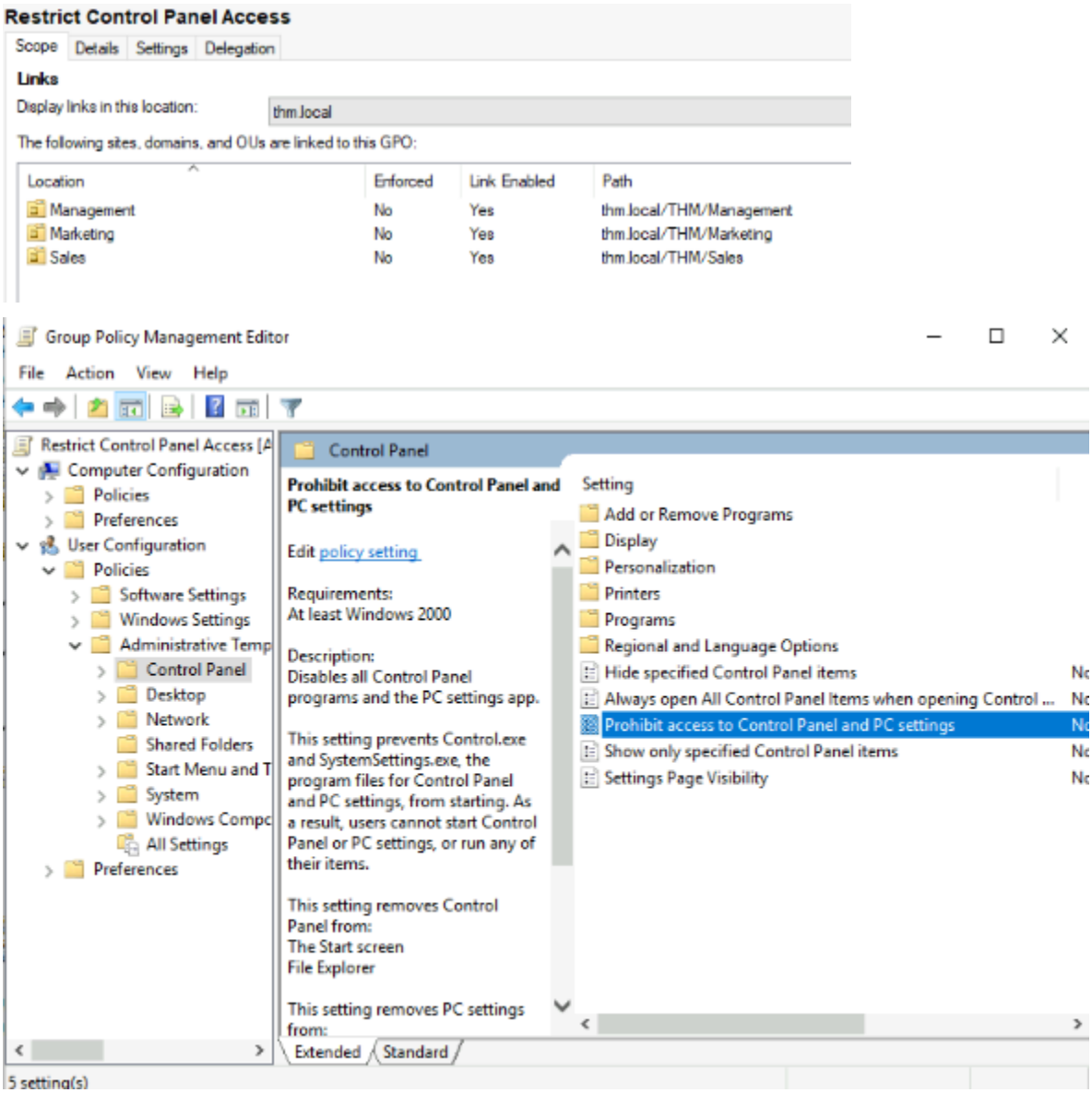


As the first task states, we want to block non-IT users from accessing the control panel, so by identifying what exactly the GPO is, in this case, restriction on the access control panel it allows those who configure the GPOs what it is and the purpose of it.

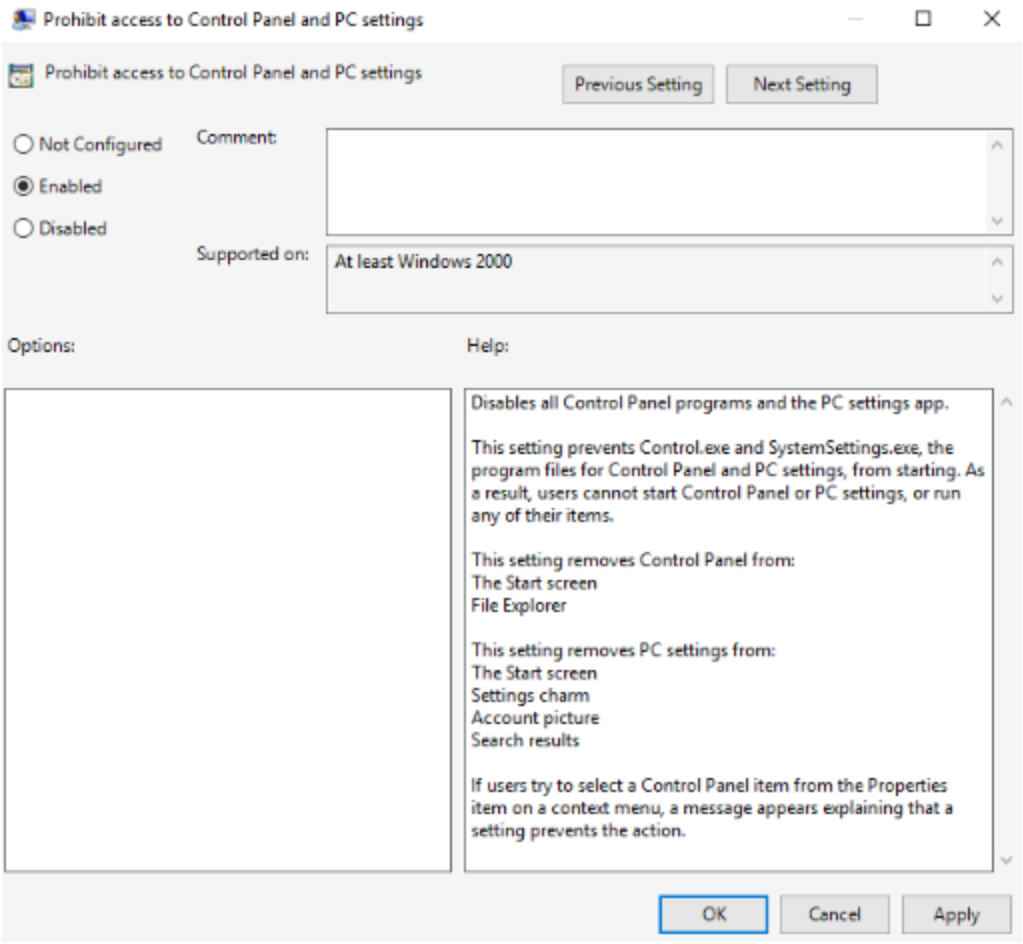
Once selecting okay I can see that it has now joined the other GPOs, but has not been assigned to anything yet, that is because we need to configure it first.



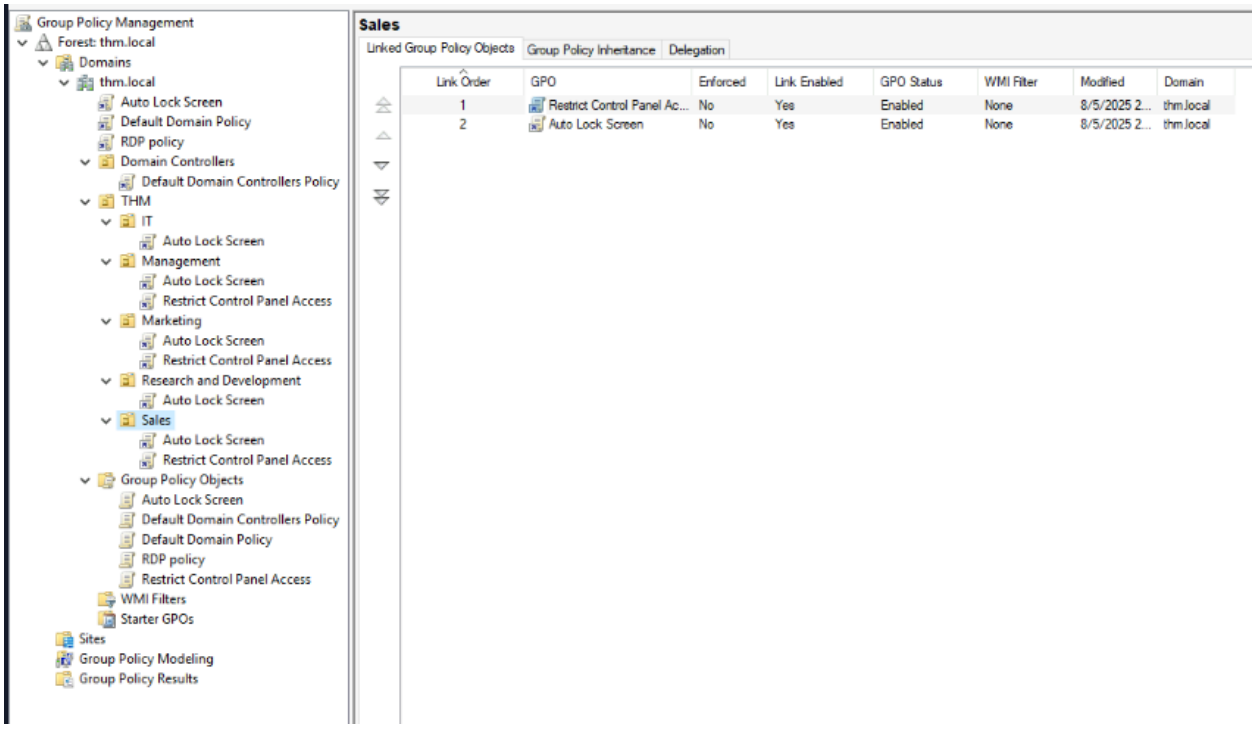
We can now right click the different application groups on the left and link them to GPOs, in this case we link it to our restrict control panel access group. We will do this for Marketing, Management and Sales groups as per instruction.



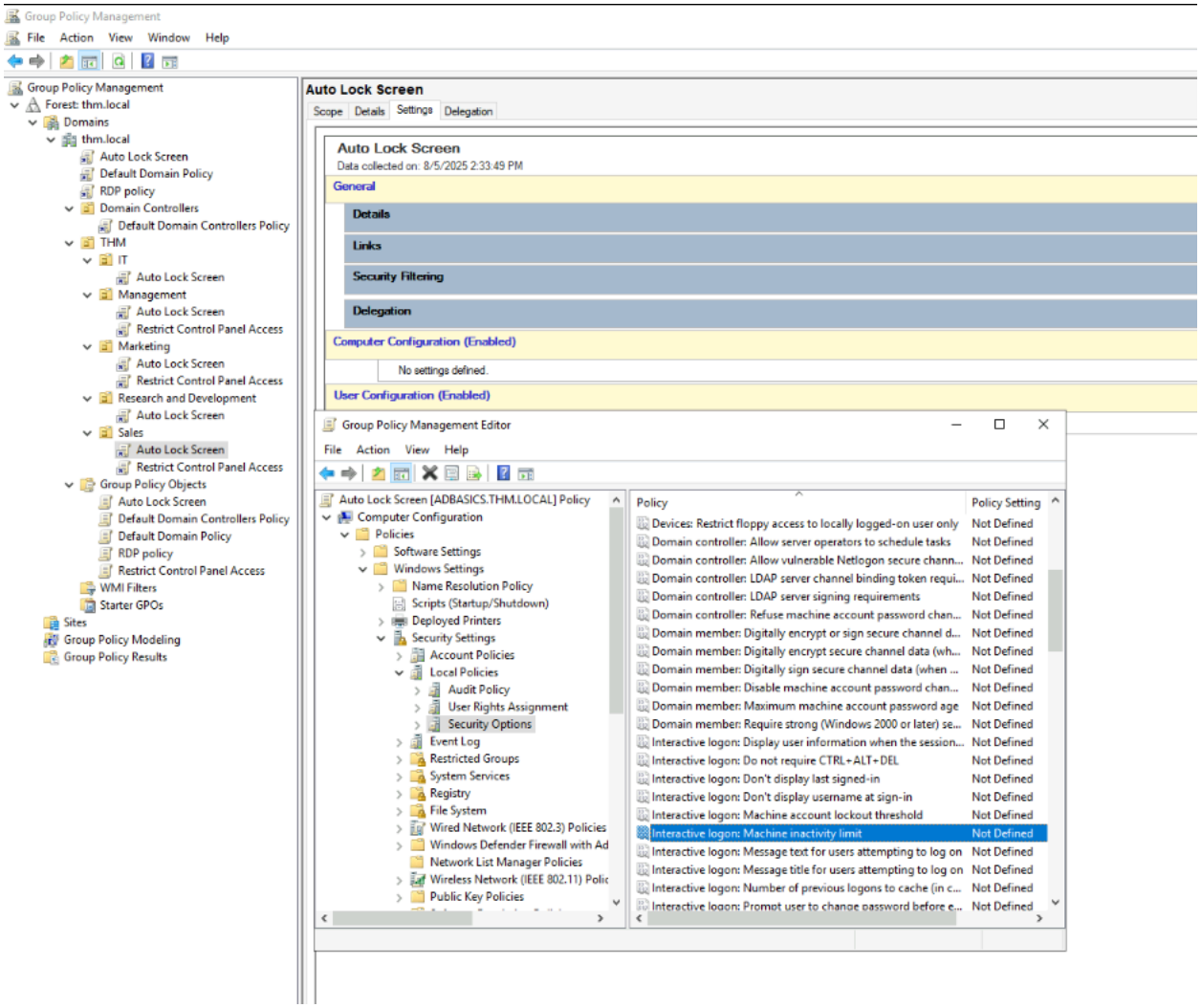
I then go into the settings and enable prohibit access to the Control Panel and PC settings, this disabling the users assigned to this group that they will not be able to access, hence completing our first task.



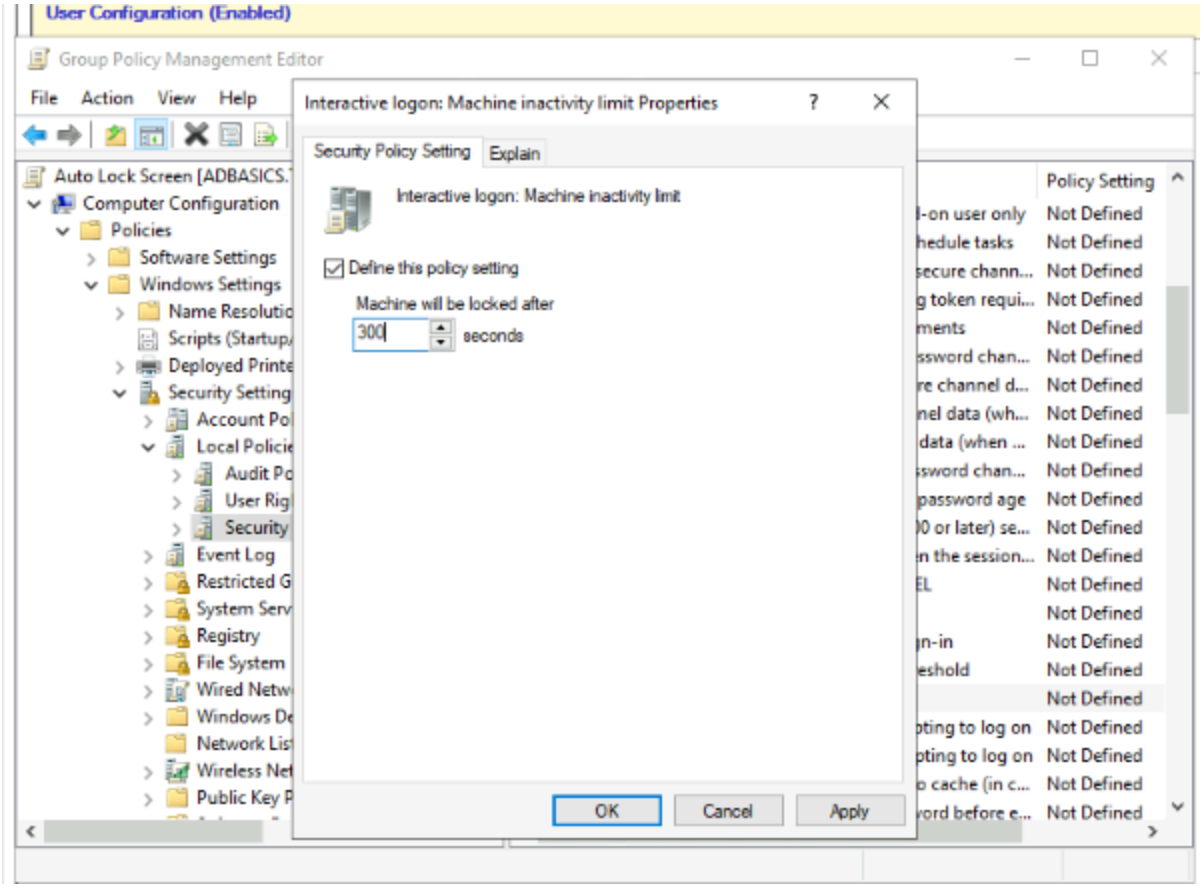
Once that is done, we create a new group called “Auto Lock Screen, but assign it for ALL users.



Once we have configured the groups, I then moved onto configuring the actual group itself, by going into settings again.



Here we can see it is not yet defined. So we will limit it now,



Like so then click “ok” and there we go!

So now, if we were logged in as a user in one of those groups specified, we will either have restricted access to the control panel, and our computer will auto lock after 5 minutes!