TNE10005/TNE60002

Network Administration

Lab 8

Configuring

Group Policies

in a

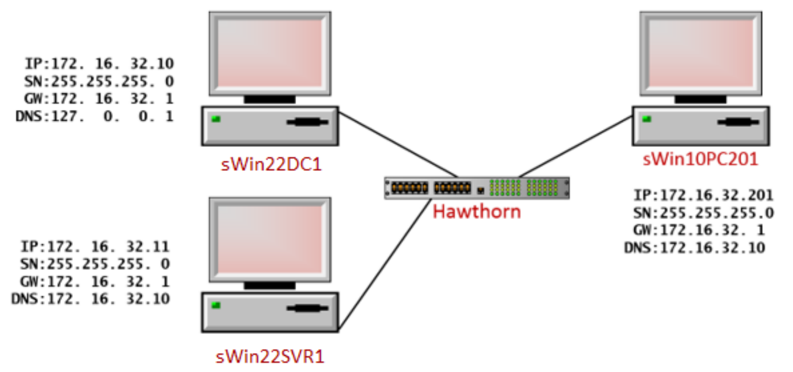
Windows Server 2022 Domain

SWINBURNE UNIVERSITY OF TECHNOLOGY

Aim

The aim of this lab is to understand how to configure and deploy Group Policies

Topology



Lab 8 Figure 1

Preliminary settings

1. Revert the virtual machines (VMs) **sWin22DC1**, **sWin22SVR1** and **sWin10PC201.** Check the Hyper-V settings and ensure the three VMs have their **Network Adapter** configured for the **Hawthorn** virtual switch.
2. Launch **sWin22DC1**, when it displays the logon screen, launch **sWin22SVR1** and **sWin10PC201**.
3. Log on to **sWin22DC1** as **Administrator.** Ensure that **sWin22DC1** configured with the IPv4 address **172.16.32.10/24**.
4. Ensure that the **DNS address for sWin10PC201** contain the sWin22DC1's IPv4 address.
5. Join **sWin10PC201** to the **sWin.Local** domain.

6. At **sWin22DC1**, create at least three user accounts and at least two global groups: **G_ICTProcurement** and **G_ICTSupport** (create more if you want).

   Of the three users, assign one user account to be a member of both global groups. Assign the remaining user accounts so that they are members of only one group and that both groups has more than one member.

Local Policies

Hardening a desktop

7. Log on to **sWin10PC201** as **Administrator**.
8. Click the **Win** ⊞ key to bring up the **Start screen.** At the **Start screen**, start typing **gpedit.msc,** then select the **gpedit.msc (Microsoft Common Console Document)** to load the **Local Group Policy**.
9. First we will **turn off autoplay** so that when a user inserts a CD or USB device, it will not automatically load the autorun script.

   In the **Computer Configuration** section, expand the **Administrative Templates** container, then expand the **Windows Components** container.

10. Double-click the **Autoplay Policies** container, and double-click the **Turn off Autoplay** policy. Click on the **Enabled** option button and enter a comment along the line of “Policy set by <name> to prevent malware being copied by autorun scripts”.

    Set the **Turn of Autoplay on:** setting to **All drives**. Click **OK.**

11. Double-click on **Set the default behavior for Autorun**, click the **Enabled** option button, enter a relevant comment and set the **Default Autorun Behavior** option to **Do not execute any autorun commands.** Click **OK**.

Prohibiting access to the Control Panel

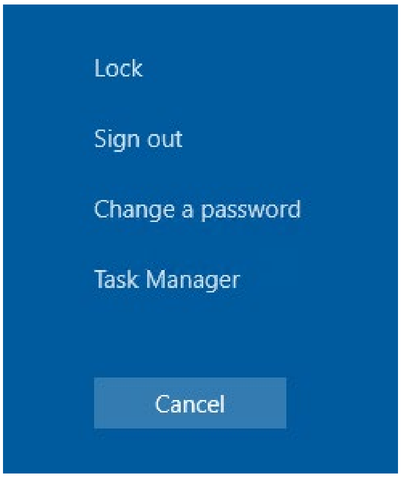
If the workstation we are configuring is planned to be used for a single purpose (e.g. library catalogue), then it is desirable to restrict users from having access to the control panel.

12. Verify that you can access the control panel. To do so, at the **Start screen**, type **Control panel,** then select it to run. Once verified, close the Control panel.
13. Back in gpedit, in the **User Configuration,** expand the **Administrative templates**, then click on the **Control Panel** container.
14. Double-click on **Prohibit access to the Control Panel and PC settings**, and entering in a descriptive comment, click the **Enabled** option button, then **OK**.
15. At the **Start screen,** start typing **Control Panel** and observe whether it still appears in the **Best match** list.

    If it does, launch it. Were you successful? ______________

Ctrl+Alt+Del Options

When we press the Ctrl+Alt+Del (or **Ctrl+Alt+End** in the guest machine) options we are given the following options:



Lab 8 Figure 2

If the workstation we are configuring is to be used for a single purpose by many people you may want to remove some of these options. For example, the **Lock this computer** option is frustrating for other users as they are unable to use the PC while locked.

We will now remove this option:

16. Verify that you have this option by pressing Ctrl+Alt+Del (Ctrl+Alt+End in a guest machine). Once you have verified the option, press **Cancel**.

17. In the **Local Group Policy Editor** console, find in the **User Configuration, Administrative Templates, System, Ctrl+Alt+Del options** container, the **Remove Lock Computer** option.

    Double-click on the option, and **Enable** this setting, entering a descriptive comment. Click **OK.**

    Test to see if your settings have been applied by pressing Ctrl+Alt+Del (Ctrl+Alt+End in a guest machine).

18. Repeat the steps for the **Remove Task Manager** option. Verify that it is working.

Creating an Organisational Unit Structure

19. Switch back to **sWin22DC1**, in **Active Directory Users and Computers**, create an OU called **ICT**.
    (see Lab6, p.9, step 34 if you cannot remember how to create an OU).

20. Within the **ICT** OU create two child OUs **ICTSupport** and **ICTProcurement**.

21. Move one of the user accounts created in step 6 into the **ICTSupport** OU, move another into the **ICTProcurement** OU. Move any remaining user accounts along with the groups created in step 6 into the **ICT** OU. This can be achieved by clicking on the account and dragging it to the OU.

Delegating Control of an OU

We want a user from the ICT Support team to take over the management of the user account passwords and groups in the ICTSupport OU.

22. Right click on the **ICTSupport** OU.
23. Select **Delegate Control…** to start the wizard. Add the user account that you copied into the **ICTSupport** child OU.
24. Delegate the following tasks:
    a. Reset user passwords and force password change and next logon
    b. Create, delete and manage groups
    c. Modify the membership of a group
    d. Finish the wizard.

We have now given this user the rights required to do much of the day-to-day management of the user accounts in this OU. Consequently, we have delegated some of the urgent, but relatively unimportant tasks that can distract us from some of the longer term, but important tasks.

Creating a Custom Console

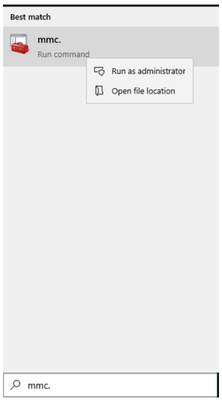
Now that we have delegated some of the day-to-day responsibilities, we also need to provide the users we have delegated access to the **Active Directory Users and Computers** console. The problem with this is it provides information to these users on the structure of our network. Information that may be useful to potential hackers.

It is safer to create a new console for these users with delegated permissions so that they only see the objects (OUs, accounts, etc).

We can do this by creating a **Custom Console.**

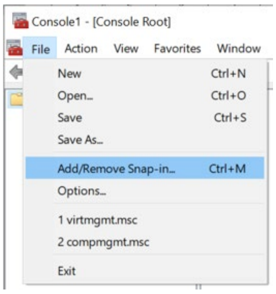
25. On the tool bar at the bottom left of the window, next to the the **Win** key ⊞, in the ***Type here to search*** box, type **mmc.**

    Click **Run as administrator** to launch the **MMC** (Microsoft Management Console) with the administrative privilege.



Lab 8 Figure 3

In the **Console1 – [Console Root]** window, click **File** then select **Add/Remove Snap-in….**



Lab 8 Figure 4

Select **Active Directory Users and Computers** snap-in, then click **Add>** and click **OK.**

26. Expand the sWin.local domain and get to the **ICTSupport** OU.

27. Right click on the **ICTSupport** OU and select **New Window from Here**.

    We have now created a custom console for this OU. We have one more thing to do though. We still have the initial console window that has the domain root, and all of the details we wanted to hide from our delegated user.

28. Click on the **Window** menu and select the **Console Root\ …** window. Now, without closing the whole console, close this window (i.e. click on the inner/lower □window. Now, without closing window).

29. We should now only have the ICTSupport OU window in the console.
    Save the console as **ICTSupportConsole**.

Creating a Group Policy Objects

Order of application

Before we start creating different GPOs, let’s undertake an exercise that will demonstrate the order in which GPOs are applied.

Many GPO settings are like light switches, if configured they can only be on or off. Like a light switch, if a person walks into a room and turns the light on, then the next person comes in and turns the light off, and the next person turns it on when they come in, it is always the last person that flicked the switch that determines whether the light is off or on.

The same is true with GPOs. While an administrator has some tricks up their sleeve to override this, the general rule is that when GPOs conflict over a setting, the last GPO applied will determine the setting.

Let’s see this in action.

Remember we configured the Local Group Policy on sWin10PC201 so that the Remove Lock Computer option was enabled. We will now create a GPO that will conflict with this Local Group Policy setting.On **sWin10PC201**, sign out. Then log on as a domain user whose user account is located in the **ICTProcurement** OU.Notes: Ensure to put **sWin** in front of the logon name to tell the computer that the account is from the swin domain. This is useful to know when you have a local account and a domain account with the same logon name)**.**

> If you could not log on and receive a message "*To sign in remotely, you need the right to sign in through Remote Desktop Services……*", on the VM (i.e. sWin10PC201), click on the **View** menu, then deselect **Enhanced session**.

Verify that the **Task Manager** option does not appear when we press **Ctrl+Alt+Del** key combination.

30. On **sWin22DC1** run **gpmc.msc** (or select **Group Policy Management** from the **Tools** menu in **Server Manager**).

    Expand the **Domains** container and expand **sWin.local** until you see **Group Policy Objects.**

31. Right click on **Group Policy Objects** and select **New**.

    Enter the name **Enable Task Manager** as the name of the new GPO.

32. Right click on this new GPO and select **Edit…** This will launch the GPO in gpedit.

33. Expand User Configuration > Policies > Administrative Templates > System, down to the **Ctrl+Alt+Del options** and in the **Remove Task Manager** properties, click on the **Disabled** option button.

    Notice that we now have a double negative. We have disabled the removing of the task manager. This means that the task manager should be available.
    Predict what the result of this GPO will now be:

    ____

    On sWin10PC201 verify if your prediction was correct. Was it? __________

    We have three points that need to be considered here:

    - GPO's must be linked to a container before they will be applied
    - Objects must reside in that container if the GPO is going to apply to them.
    - GPOs must propagate to other PCs before they can come into effect.

By default GPOs are reapplied every 5 minutes in a domain controller, and 90 ± 30 minutes to other computers in the domain. So a change in a GPO may take up to 120 minutes (i.e. 2 hours) before we will see it in effect on some workstations.

GPUpdate

Every time a computer reboots the computer configuration settings of all of the GPOs that are linked to container that the computer's account resides in are applied. Similarly when a user logs on to the domain the user configuration settings of all the GPOs that are linked…etc, are applied.

Another tool that allows an administrator to reapply GPOs is **GPUpdate.**

Typed in at the start menu or command line **gpupdate** will refresh all of the settings that have changed since the last application of GPOs.

We can modify **gpupdate** by using the following switches:

`gpupdate /force` - Will apply all GPO settings both user and computer configurations whether they have changed or not.

`gpupdate /target:user` - Will apply all of the user configuration settings, the word user can be substituted with computer to apply all ofthe computer configuration settings.

`gpupdate /boot -` Will cause the PC to reboot after the GPO has been applied

Every time you change a GPO setting, you should type **gpupdate** on both the domain controller and the workstation you are testing on.

Linking GPOs to Containers

Link the new GPO to the domain, type gpupdate on both **sWin22DC1** and **sWin10PC201**.

34. In the **Group Policy Management** windows right click on the **sWin.local** domain and select **Link an Existing GPO…** Select the **Enable Task Manager** GPO and click **OK**.

35. Run **gpupdate /force** on both **sWin22DC1** and **sWin10PC201**.

36. View your Ctrl+Alt+Del options on **sWin10PC201**

    What is the setting? ______________________________

    Which GPO is applied? ____________________________

37. Back on **sWin22DC1**, create a GPO called **Remove Task Manager** and link it to the **ICTSupport** OU. This time, remembering the double negative, set the **Remove Task Manager** setting to **Enabled**.

    Run **gpupdate /force** on both guest machines.

    Record the result of this change to sWin10PC201:

    ____

38. Now log on to **sWin10PC201** as the user account from **ICTSupport**. Explain any differences:

    ____

    ____

    ____

This exercise illustrates the following points.

- GPOs only apply to objects in the containers to which the GPOs are linked
- GPOs are applied in an order. When settings conflict, if the administrator has not overridden then, the setting in the last GPO applied will be configured.

Remember that the order in which GPOs are applied are:

a. Local Computer Policy
b. Site
c. Domain
d. OU
e. Child OUs (recursively

More GPO Settings

We will now learn about some other GPO settings. In each instance we will be creating a new GPO and linking it to the **ICT** OU.

Preventing Software Running Policies

There are a number of ways we can restrict users from running specific software. In this lab we will use the **Don't run specified Windows Applications** policy, but there are also Software Restriction Policies and AppLocker.

39. On **sWin22SVR1**, log in as one of the user account created in step 6, and run **calc.exe** (**Desktop app)** to ensure that you can run it.
40. On **sWin22DC1** in **GPMC** create and link a GPO called **RestrictRunningOfCalc** to **sWin.Local** domain.
41. Edit the GPO and browse to

    User Configuration\Policies\Administrative Templates\System.

42. Prevent users from running **calc.exe** by configuring the **Don't run specified Windows** applications policy setting.

> ***Note:***
>
> This policy setting only prevents users from running programs that are started by the **File Explorer process**. It does not prevent users from running programs, such as Task Manager, which are started by the system process or by other processes. Also, if users have access to the command prompt (Cmd.exe), this policy setting does not prevent them from starting programs in the command window even though they would be prevented from doing so using File Explorer.

43. Attempt to run **calc.exe** again (i.e. browse to C:\Windows\System32\calc.exe in File Explorer), it should not run.

> **Note:**
> The following settings can also be used to restrict the running of software:
>
> - **Software Restriction Policies** (*User configuration, Policies, Windows Settings, Security Settings.* Right-click *Software Restriction Policies* and choose *New Software Restriction Policies*).
> - **AppLocker** (*Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker*). Applocker has three major steps to be configured. Advantages of Applocker is that you can easily restrict all versions of a piece of software, or all software from a specific company. You can also run Applocker in Audit mode, which will let you track who is using the software.

Linking Multiple GPOs

We have seen throughout this lab that we can link multiple GPOs to the one container. The question that now arises is 'what if two GPOs linked to the same container conflict in a setting?'

Let's see if we can observe what happens.

Changing Priority of GPOs

44. Using GPMC, link to the **ICTProcurement** OU, first the **Remove Task Manager** GPO created in step 37 and then the **Enable Task Manager** GPO created in step 31.
45. On **sWin10PC201**, log in as the user account located in the **ICTProcurement** OU

    Which GPO is being applied? ________________________

46. Back in **GPMC** at the **ICTProcurement** OU, observe the link order of the **Remove Task Manager** and **Enable Task Manger** GPOs.

    Change the order of the GPOs so that **Enable Task Manager** is at position **1**.

    Do this by selecting the **Enable Task Manager** GPO and clicking on the ▯parrow.

47. Test **sWin10PC201**, which GPO setting has been applied? _______

Filtering GPOs

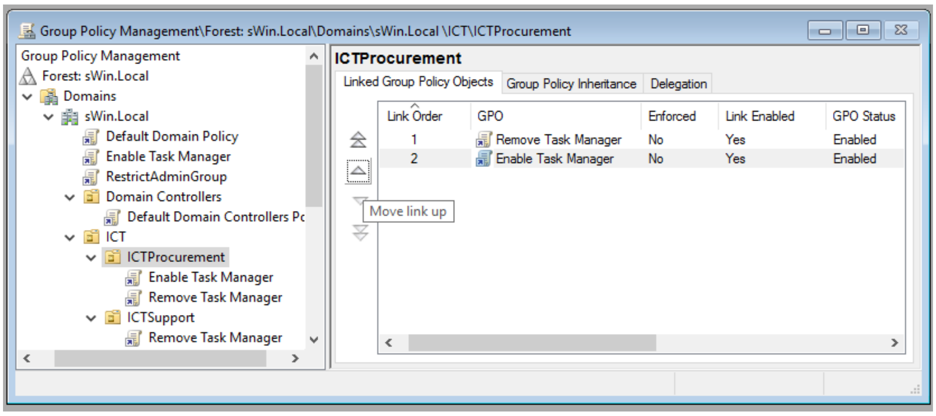
The term Group Policy Object refers to the fact that each is a collection or group of policies that can be linked to a container. The computer and user objects in those containers are configured with the settings in the respective computer configuration and user configuration policy settings.

You cannot link a GPO to a group, only to a Local Computer Policy, Site, Domain and OU.

Consequently students beginning in network administration can be confused.

While we cannot link a GPO to a group, we can change the permission of a GPO so that it is only applied to targeted groups. This is called Filtering.

There are three approaches to filtering: GPMC, GPO Security and WMI filtering.



Group Policy Management\Forest: sWin.Local\Domains\sWin.Local \ICT\ICTProcurement

- Group Policy Management
  - Forest: sWin.Local
    - Domains
      - sWin.Local
        - Default Domain Policy
        - Enable Task Manager
        - RestrictAdminGroup
        - Domain Controllers
          - Default Domain Controllers Pc
        - ICT
          - ICTProcurement
            - Enable Task Manager
            - Remove Task Manager
          - ICTSupport
            - Remove Task Manager

ICTProcurement

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Remove Task Manager	No	Yes	Enabled
2	Enable Task Manager	No	Yes	Enabled

Lab 8 Figure 5

WMI filtering is the most powerful and most complex. For example we can write a script that will check to see how much disk space is free before proceeding with software deployment, or it can check to see if a patch was previously installed prior to applying a policy. How to configure WMI filtering is beyond the scope of this unit. Students only need to know what WMI filtering is.

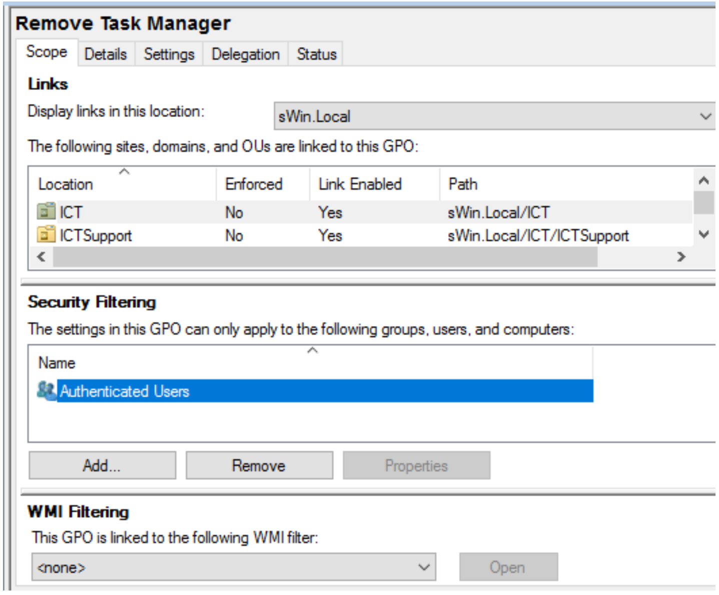
GPMC Filtering

48. In *GPMC delete* the link between the **ICTProcurement** OU and the **Enable Task Manager** GPO.

    Link the **Remove Task Manager** GPO to the **ICT** OU

49. In the **Group Policy Objects** container, click on the **Remove Task Manager** GPO.

    In the **Security Filtering** settings, notice that it currently has the **Authenticated Users** group configured.



Remove Task Manager

Links

Display links in this location: sWin.Local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
ICT	No	Yes	sWin.Local/ICT
ICTSupport	No	Yes	sWin.Local/ICT/ICTSupport

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Lab 8 Figure 6

Click **Remove**, then **Add...** the **G_ICTProcurement** group.

When filtering a GPO, you must ensure that the targeted accounts have read permissions.

Ensure that your GPO has **Allow Read** permissions assigned.

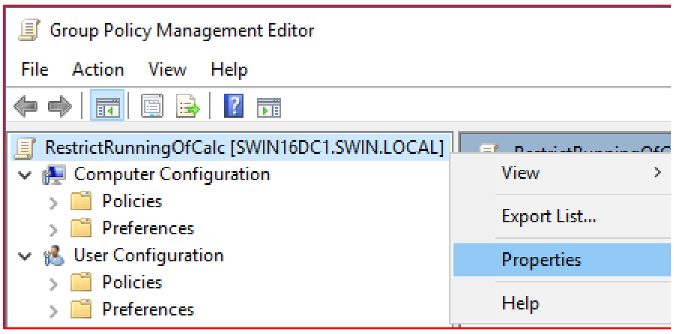
Now the **Remove Task Manager** GPO will only be applied to members of the **G_ICTProcurement** group.

You will also need to modify the read permissions of the GPO, which we will do in the next step.

Filtering with GPO Security

50. In GPMC right click on the **Restrict Running of Calc** GPO and select **Edit…**

At the top left of the GPO right click on the GPO name and select **Properties.**

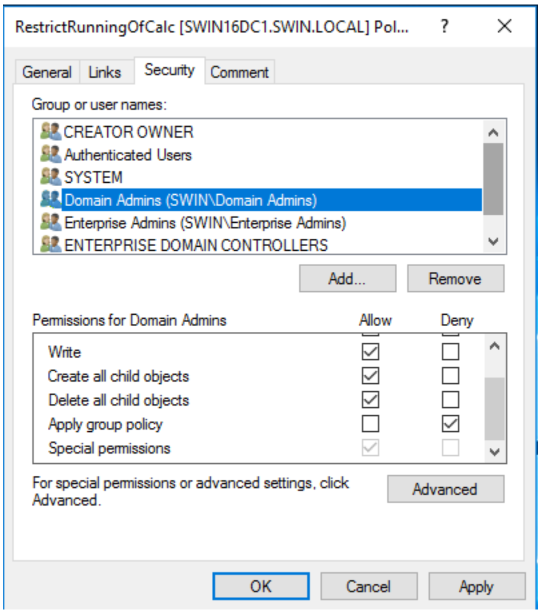


Lab 8 Figure 7

51. A familiar properties dialog will appear. Click on the **Security** tab and then click on the **Domain Admins** group.

In the Permissions for **Domain Admins**, scroll down until you can see the permission **Apply group policy**.

Place a tick in the **Deny** column for the **Apply group policy** permission.



RestrictRunningOfCalc [SWIN16DC1.SWIN.LOCAL] Pol...

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (SWIN\Domain Admins)
- Enterprise Admins (SWIN\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for Domain Admins	Allow	Deny
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□
Apply group policy	□	☑
Special permissions	☑	□

For special permissions or advanced settings, click Advanced.

Lab 8 Figure 8

This will mean that this GPO will apply to everyone except those in the Administrators group.

Please keep in mind that we sparingly use deny permissions.

52. On **sWin22SVR1**, log off and log on again as the **Administrator** and see if you can now run the calculator.

Modelling GPOs

Modelling is a fantastic tool for troubleshooting GPOs. In the lecture I spoke about how with Windows 2000 we used to have to unlink, update, and then test to see which GPO was causing problems for a PC or user. It took such a long time.

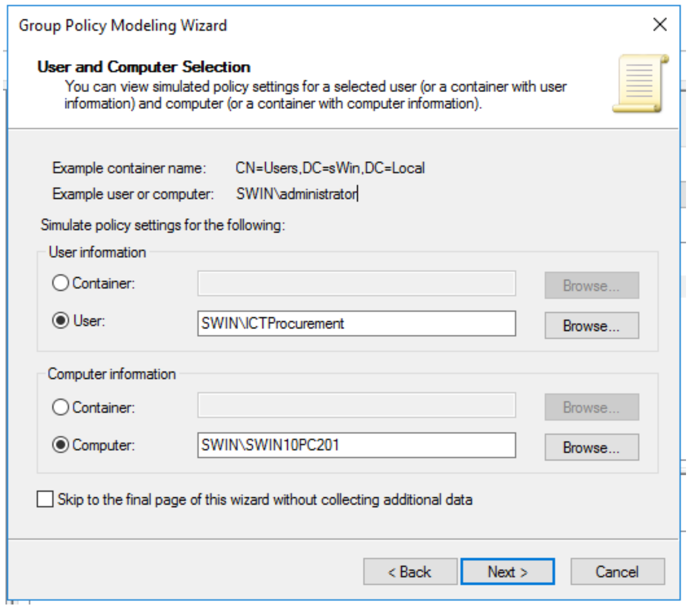
Group Policy Modelling is a wizard that will allow you to select a container, a user or a computer. It will then apply all of the group policies that apply and generate a report that tells you which GPO is causing what setting.

For example, you are an administrator and you need access to the task manager, but the computer you are on won't run the task manager. You can run the modelling with your account and the computer you were working on and drill through the report to find what GPO is causing it to be hidden.

This makes it much easier to correct errors in our GPOs.

You can also use **rsop.msc** and **gpresults** to troubleshoot GPOs. Like WMI filters, we don't need to know how to use rsop.msc in this unit, we only need to know that it can be used for troubleshooting GPOs.

53. In GPMC near the bottom of the left hand pane, right click on Group Policy Modeling and start the Wizard.
54. As we are modelling GPOs applied to this domain, select the defaults for the Domain Controller Selection.
55. In the User and Computer Selection step, enter the **ICTProcurement** user and the **sWin10PC201** computer.



Group Policy Modeling Wizard

User and Computer Selection

You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=sWin,DC=Local

Example user or computer: SWIN\administrator

Simulate policy settings for the following:

User information

○ Container:

● User: SWIN\ICTProcurement

Computer information

○ Container:

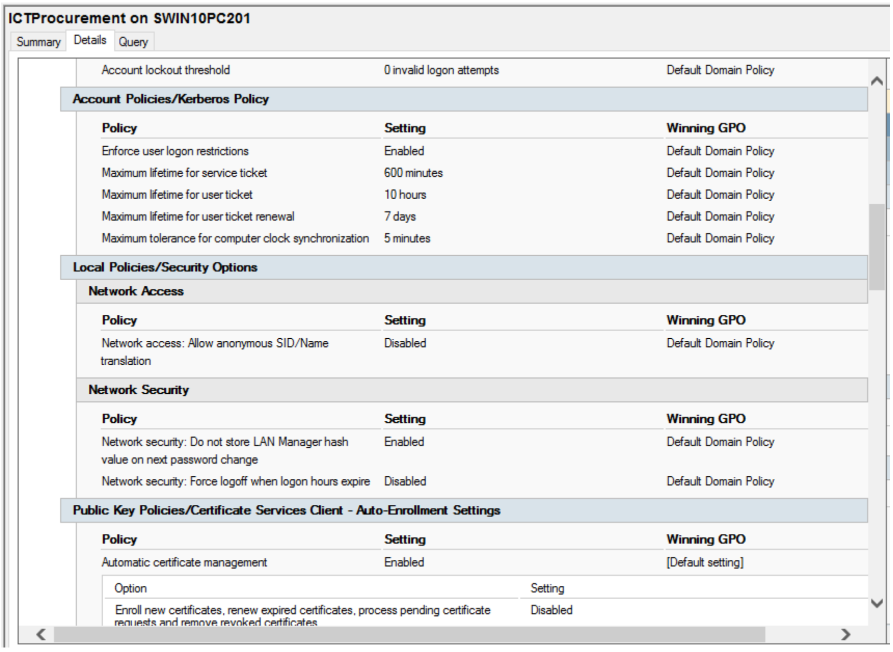
● Computer: SWIN\SWIN10PC201

□ Skip to the final page of this wizard without collecting additional data

Lab 8 Figure 9

Tick the **Skip to the final page...** check box and click **Next**.

56. Ignore any warnings about not trusting this page (after all Microsoft generated it). On the report, click on the **Details** tab to see what GPOs are being applied.



ICTProcurement on SWIN10PC201

Account lockout threshold	0 invalid logon attempts	Default Domain Policy

Account Policies/Kerberos Policy

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy

Local Policies/Security Options

Network Access

Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy

Network Security

Policy	Setting	Winning GPO
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

Policy	Setting	Winning GPO
Automatic certificate management	Enabled	[Default setting]

Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Disabled

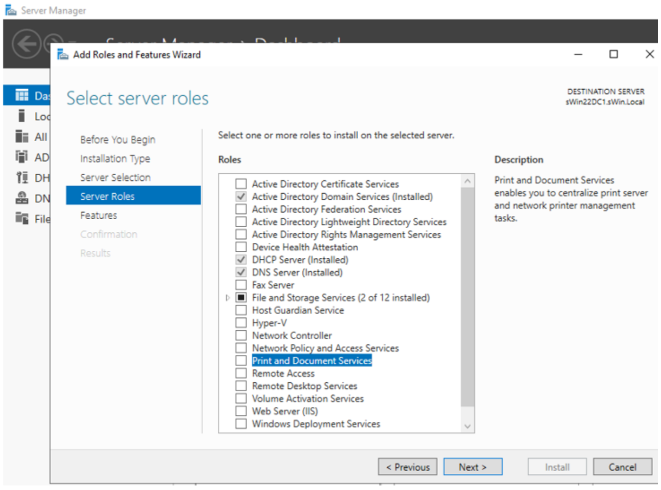
Lab 8 Figure 10

Deploying Printers with GPOs

57. In GPMC Create a new GPO called **IctPrinterDeploy** and link it to the **ICT** OU.

Create a new Printer

58. First, let add the Print Services by adding the **Print and Document Services** Server Roles.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
sWin22DC1.sWin.Local

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Print and Document Services enables you to centralize print server and network printer management tasks.

Lab 8 Figure 11

After Server Roles is added. In **Server Manager**, under the **Tools** menu, click to launch the **Printer Management** console.

59. Expand **Print Servers**, then expand **sWin22DC1 (local)**. Right click **Printers** and select **Add Printer…** The Network Printer Installation Wizard will then start:

a. On the **Printer Installation** page, select **Add a new printer using an existing port:** For this lab we will use the port **LPT1**, but normally the printer will have a network card installed and have its own IP address. Click **Next**.

b. On the **Printer Driver** page, select **Install a new driver**, and click **Next**.

c. On the **Printer Installation** page, select the **MS Publisher Color Printer**, and click **Next**.

d. On the **Printer Name and Sharing Settings** page, name the printer **ICT_Printer**, and share it as **ICT_Printer**. Click next, and on the **Printer Found** page, click **Next** again.

e. When the driver and printer have successfully installed, click **Finish.**

Set Permissions on the Printer

This step is not essential for deploying a printer, but if you don't want to have to be the person looking after all printer problems, you will need to ensure that someone has sufficient permissions to manage the printer.

60. Right click the printer **ICT_Printer** and select **Properties**, then the **Security** tab. In the same way as you would allocate NTFS permissions, give the group **G_ICTSupport** both the **Manage this printer** and **Manage documents** permissions. Click **OK** until you are back at **Print Management**.

Deploying the Printer Using GPOs

61. Back in **Print Management** right click **ICT_Printer** and select **Deploy with Group Policy…**

62. Next to the field **GPO name:** click the **Browse** button. Find the **IctPrinterDeploy** GPO, and click **OK**.

63. We will deploy this printers to the Users in the ICT OU, but if this GPO was linked to an OU that had computer accounts in it we would want to deploy the printer to computers

    a. Select the Checkbox **The users that this GPO applies to (per user)**, and click **Add**.

    b. Verify that the UNC for the printer appears in the **Printer Name** column, and click **OK**.

    c. You will get a message telling the operation succeeded. Click **OK**.

Test Deployment

64. Log on to **sWin22SVR1** as one of the users created above (if you are already logged in, execute a **gpupdate /force**) and verify that the printer has been deployed (Settings, Devices, Printers & Scanners)

Extension

Managing GPOs

Explore how you can use GPMC to backup and restore your GPOs

Find out how to use rsop.msc or the command line tool gpresult to troubleshoot GPOs.

Reminder

Record the concepts, design strategies, techniques, configurations and commands that you learn in this week laboratory class.

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

End of Lab