# Week 6 Windows Server Activities – Active Directory

Activities

[Week 6 Windows Server Activities – Active Directory 1](#_Toc177548214)

[Activity 6-1: Creating, Linking, and Unlinking GPOs 1](#_Toc177548215)

[Activity 6-2: Configuring and Testing a Local and Domain GPO 3](#_Toc177548216)

[Activity 6-3: Creating and Using Starter GPOs 5](#_Toc177548217)

[Activity 6-4: Demonstrating GPO Inheritance Blocking 7](#_Toc177548218)

[Activity 6-5: Demonstrating GPO Enforcement 8](#_Toc177548219)

[Activity 6-6: Setting a Domain Level Policy 10](#_Toc177548220)

[Activity 6-7: Setting the Default Domain Policy 11](#_Toc177548221)

[Assignment Submission 12](#_Toc177548222)

**How to Create Screenshots:** Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

# Activity 6-1: Creating, Linking, and Unlinking GPOs

Time Required: 10 minutes

Objective: Create, link, and unlink GPOs.

Required Tools and Equipment: Server1

Description: You want to be sure you know how to create and test GPOs, so you create a test OU and a GPO linked to it.

1. Log on to **Server1** with your administrator account, if necessary.
2. Open the **Group Policy Management** console. Right-click the **Sales OU 🡪** **Create a GPO in this domain and Link it here**.
3. In the New GPO dialog box 🡪, type **GPO3** in the Name text box, and then click OK.
4. If necessary, click the **Sales OU**. In the right pane, notice that **GPO3** is listed as Enabled. Changes you make to the GPO take effect on any users or computers in the Sales OU that update their policies.
5. Right-click **GPO3** 🡪 click **Delete**. Click OK. This action deletes only the link to the GPO, not the GPO itself.
6. Click the Group Policy Objects folder to see all your GPOs, including the default GPOs. Insert a screenshot.

Click or tap here to enter text.

1. Right-click **GPO3** and point to GPO Status. You can enable or disable a GPO or just disable the Computer Configuration or User Configuration settings. You can also backup and restore a GPO from here.
2. Right-click the **Sales OU** 🡪 click **Link an Existing GPO**. In the Select GPO dialog box, click **GPO3**, and then click OK.
3. Right-click the **Administrators OU** and click **Link an Existing GPO**. In the Select GPO dialog box, click **GPO3** and then click OK.
4. Right-click the Administrators OU and click **Create a GPO in this domain, and Link it here**.
5. In the New GPO dialog box, type **GPO1** in the Name text box 🡪 click OK.
6. Go to **User Configuration 🡪 Policies 🡪 Administrative Templates 🡪 Control Panel**. In the right pane, double-click the **Prohibit access to Control Panel and PC settings** policy to open the dialog box. Set it to **Enabled**. Click **Ok**.
7. Click the **Administrators OU**. Notice that both **GPO1** and **GPO3** are linked to the Administrators OU. If both GPOs had the same policy setting configured but with different values, the value of the policy setting in GPO1 would take precedence because it would be applied last.
8. Click **GPO3** in the right pane and click the up arrow to the left of the Link Order column. GPO3 now has link order 1 and GPO1 has link order 2, so GPO3 takes precedence if any settings conflict.
9. Right-click **GPO3** and click **Delete**. Click OK in the message box asking you to confirm the deletion.
10. Right-click **GPO1** and click **Delete**, and then click OK. No policies should be linked to the Administrators OU now.
11. If you’re continuing to the next activity, leave the Group Policy Management console and Active Directory Users and Computers open; otherwise, log off or shut down Server1.

# Activity 6-2: Configuring and Testing a Local and Domain GPO

Time Required: 15 minutes

Objective: Configure and test a GPO.

Required Tools and Equipment: Server1 and Win11

Description: Now that you have a new GPO and an OU to test it on, you move the Win11 computer account to the new OU and test some computer settings in the GPO. You will also look at how local and domain group policies interact.

1. Start **Win11**. Log on to **Server1** as your administrator level account and open Active Directory Users and Computers, if necessary.
2. Click the **Computers** folder, drag the **Win11** computer account to the **Workstations OU**, if necessary. Click Yes in the warning message about moving Active Directory objects.
3. Open the **Group Policy Management** console, if necessary. Click to expand the Workstations OU.
4. Link **GPO3** to the Workstations OU.
5. **Right Click** and click **Edit** to open it in the **Group Policy Management Editor**.
6. Click to expand **Computer Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Local Policies.** Click **User Rights Assignment**.
7. In the right pane, double-click **Allow log on locally** to open its Properties dialog box. Notice that the policy setting is currently not defined. Click the **Define these policy settings** check box, and then click **Add User or Group**. In the **Add User or Group dialog** box, click **Browse**. Type **Administrators** in the “Enter the object names to select” text box and click Check Names. Click OK three times.
8. Close the Group Policy Editor.
9. On **Win11**, log on to the domain as your administrator level account. Click Start, type in and **Local Security Policy**. The Local Security Policy contains only the security settings for the local computer and is the section of the policy that was modified earlier.
10. Click to expand Local Policies and then click **User Rights Assignment**. Notice that the icon next to the “Allow log on locally” policy looks like two towers and a scroll instead of the torn-paper icon next to the other policies. This icon indicates that the policy is defined by a domain GPO.  
    **NOTE:** If the “**Allow log on locally**” policy doesn’t have the domain GPO icon; the policy hasn’t been updated yet on your Win11 computer. If so, do the following: Close the Local Security Policy MMC, open a command prompt window, type **gpupdate /force**, and press Enter. Gpupdate.exe immediately updates group policies on the local computer. When it’s finished, open the Local Security Policy MMC and navigate back to User Rights Assignment.
11. Insert **a screenshot showing two towers and a scroll:**

Click or tap here to enter text.

1. In the right pane, double-click **Allow log on locally**. In the list box of users and groups, click **Administrators**. Neither the Add User or Group nor the Remove button is active because no users, not even administrators, can override domain polices on the local computer. Click Cancel.
2. Log off **Win11**, and then try to log back on as **Sales1**. Because you have restricted local logon to Administrators only, you’ll see the following message: “The sign-on method you’re trying to use isn’t allowed. For more info, contact your network administrator.” The logon method referred to in the message is interactive logon or local logon. Click OK.
3. On **Server1**, change the **Allow log on locally** policy on **GPO3** to **undefined** by clearing the Define these policy settings check box, and then click OK to close the Properties dialog box. Close Group Policy Management Editor.
4. On **Win11**, try again to log on as **Sales1**. You’ll probably get the same message about not being able to log on because the policy hasn’t been updated yet. Click OK.
5. At a command prompt, type **gpupdate /force** After this completes successfully, restart Win11.
6. Log on to **Win11** as **Sales1**. Only an administrator can run the Local Security Policy MMC, but there’s a workaround with the runas command. Click Start, type command to bring up the command prompt. Right-click the command prompt, use Run as Administrator. Type the username and password for your administrator level account and click Yes.
7. At the command prompt, type **secpol.msc** and press Enter.
8. In the **Local Security Policy** console, click to expand **Local Policies and User Rights Assignment**. In the right pane, double-click **Allow log on locally** to view the list of users and groups assigned this permission. Notice that this right is now assigned from a local GPO rather than a domain GPO, so you can make changes if needed.
9. Insert **a screenshot:**

Click or tap here to enter text.

1. Click OK.
2. Unlink **GPO3** from the **Sales OU**.
3. Log off Win11. Stay logged on to Server1 if you’re continuing to the next activity.

# Activity 6-3: Creating and Using Starter GPOs

Time Required: 10 minutes

Objective: Create Starter GPOs to be used to create new GPOs.

Required Tools and Equipment: Server1

Description: Now that you’re more comfortable working with GPOs, you want to start building a library of Starter GPOs for creating new GPOs. You create two: one in the Computer Configuration node for configuring printers and one in the User Configuration node for configuring Start menu options.

1. Log on to **Server1** as your administrator level account, if necessary.
2. Open the **Group Policy Management** console. Right-click the **Starter GPOs** folder and click New.
3. In the New Starter GPO dialog box, type **StartPrintersC** in the Name text box. (“Start” stands for Starter GPO, “Printers” refers to the Printers node, and “C” refers to the Computer Configuration node of the GPO.) In the Comment text box, type Starter GPO for the Printers node of Computer Configuration, and then click OK.
4. Right-click the **StartPrintersC** GPO you created and click Edit. In the Group Policy Starter GPO Editor, click to expand **Computer Configuration** 🡪 **Administrative Templates**, and then Click the Printers node. In the right pane, double-click **Automatically publish new printers in Active Directory**. In the Properties dialog box, click **Enabled**, and then click **Apply**. Read the explanation of this policy setting, and then click OK.
5. Double-click **Always render print jobs on the server**. In the Properties dialog box, click **Enabled**, and then click Apply. Read the explanation of this policy setting, and then click OK.
6. Close the Group Policy Starter GPO Editor. In the Group Policy Management console, right-click the Group Policy Objects folder and click New. In the New GPO dialog box, type **PrintConfigGPO** in the Name text box, click **StartPrintersC** in the Source Starter GPO list box, and then click OK.
7. Right-click **PrintConfigGPO** in the Group Policy Objects folder and click **Edit**. In the Group Policy Management Editor, expand **Computer Configuration**, and navigate to the **Printers** node under Administrative Templates to verify that your Starter GPO settings are there. Now you can link this new GPO to a container with computer accounts that have print servers installed, and the printer policies will be in effect on these servers.
8. Insert **a screenshot of these settings**.

Click or tap here to enter text.

1. Close the Group Policy Management Editor.
2. To see the other method of using Starter GPOs to create new GPOs, click the Starter GPOs folder in the Group Policy Management console. Right-click StartPrintersC and click New GPO From Starter GPO. The New GPO Wizard starts. Click Cancel.
3. Create another Starter GPO named **StartU**, which is used as a baseline for Start screen options.
4. Right-click the **StartU** GPO and click **Edit**. In the Group Policy Management Editor, click to expand **User Configuration** 🡪 **Administrative Templates**, and then click **Start Menu and Taskbar**.
5. Configure the following policies as shown:  
   **Lock the taskbar:** Enabled  
   **Remove Run menu from Start Menu:** Enabled
6. Insert **a screenshot of these settings.**

Click or tap here to enter text.

1. Stay logged on if you’re continuing to the next activity.

# Activity 6-4: Demonstrating GPO Inheritance Blocking

Time Required: 10 minutes

Objective: Enable the Block Inheritance option on an OU.

Required Tools and Equipment: Server1 and Win11

Description: You want to set some policies for personnel in the Marketing Department. However, salespeople don’t need to be subject to these policies, so you must block inheritance on the Sales OU.

1. Log on to Server1 as your administrator level account, if necessary.
2. Open the **Group Policy Management** console, Click the **Group Policy Objects** folder. Create a GPO in this folder named **StTaskMktGPO**, using the **StartU** Starter GPO you created earlier.
3. In the left pane, right-click **StTaskMktGPO** and click **Edit**. In the Group Policy Management Editor, click to expand **User Configuration**, and then navigate to the **Start Menu and Taskbar** node. Verify that the settings you configured in the starter GPO are configured. Notice that many of the settings you see are relevant only to Windows 7/Windows Server 2008 and earlier OSs.
4. Close the Group Policy Management Editor. In the Group Policy Management console, link the **StTaskMktGPO** GPO to the **Employees OU**.
5. Click to expand the **Sales OU**, if necessary, Click the **Sales OU**. In the right pane, click the **Group Policy Inheritance** tab. Notice that Sales is inheriting policies from both **StTaskMktGPO** and **Default Domain Policy.** **StTaskMktGPO** has a higher precedence than **Default Domain Policy**. Leave the Group Policy Management console open.
6. Log on to the domain from **Win11** as **sales1**.
7. Right-click the **taskbar**. The taskbar should be locked, and the **Lock the taskbar** option should be disabled. Right-click **Start** and click **Run**. You see an error message informing you the operation was canceled because of restrictions in effect on the computer.
8. Insert **a screenshot.**

Click or tap here to enter text.

1. Click OK in the message box, stay logged on to Win11.
2. On **Server1**, in the left pane of the Group Policy Management console, right-click the **Sales OU** under the **Employees OU** and click **Block Inheritance**. Notice that the list of GPOs in the Group Policy Inheritance tab does not include any GPO’s from above, just the ones that are directly in the Sales OU.
3. Insert **a screenshot:**

Click or tap here to enter text.

1. On **Win11**, open a command prompt window. Type **gpupdate /force** and press Enter. After gpupdate.exe updates group policies, close the command prompt window.
2. Right-click the **taskbar**. The **Lock the taskbar** option is no longer disabled. Click to clear **Lock the taskbar**. Right-click **Start** and click **Run**. The Run option is now available. Click Cancel.
3. Leave the Group Policy Management console open, stay logged on to Win11 for the next activity.

# Activity 6-5: Demonstrating GPO Enforcement

Time Required: 10 minutes

Objective: Enable the Enforced option on a GPO.

Required Tools and Equipment: Server1 and Win11

Description: You have decided that the Start menu policies you configured in your Starter GPO should be applied to all users in the domain. You create a GPO based on the Starter GPO, link the new GPO to the domain object, and enforce that GPO.

1. Log on to **Server1** as your administrator level account, if necessary.
2. Open the Group Policy Management console, if necessary, and click the Group Policy Objects folder. Create a GPO in this folder named **StTaskDomainGPO**, using the **StartU** Starter GPO you created earlier.
3. Link **StTaskDomainGPO** to the domain object (MyDomain.local). In the left pane, click the domain object. In the right pane, click the **Linked Group Policy Objects** tab, if necessary. The GPO with link order 1 has the stronger precedence—in this case, the Default Domain Policy.
4. In the right pane, click **StTaskDomainGPO**. To change the link order, click the up arrow to the left of the **Link Order** column. Click the down arrow so that **StTaskDomainGPO** again has link order 2.
5. Insert **a screenshot.**

Click or tap here to enter text.

1. Right-click **StTaskDomainGPO** and click **Enforced**. Click OK. Notice the padlock icon next to **StTaskDomainGPO** indicating that GPO inheritance is enforced.
2. On **Win11**, log on as **sales1**, if necessary, and open a command prompt window. Type **gpupdate /force** and press Enter. Close the command prompt window.
3. Verify that the settings from **StTaskDomainGPO** are now in effect: The taskbar should be locked, and the Run option from the Start menu no longer works.
4. Insert **a screenshot.**

Click or tap here to enter text.

1. Log off Win11.
2. On **Server1**, right-click **StTaskMktGPO** and click Delete. Click OK. This action unlinks the GPO from the domain object but doesn’t delete the GPO.
3. Right-click the **Sales OU** and click **Block Inheritance** to remove the Block Inheritance setting.
4. Close all open windows, stay logged on to Server1 for the next activity.

# Activity 6-6: Setting a Domain Level Policy

Time Required: 10 minutes

Objective: Enable logon directly to the desktop by setting a policy at the domain level.

Required Tools and Equipment: Server1

Description: You decide to lock the taskbar on the computers. You decide to create a GPO, set a logon policy, and link it to the domain so that it affects all users. You may have to research where these policies are located.

1. Log on to **Server1** as your administrator account, if necessary.
2. Open the **Group Policy Management** console, if necessary. Right-click the **domain object** and click **Create a GPO in this domain and Link it here**. Name the GPO **DesktopSettings**. Don’t use a Starter GPO.
3. Edit the GPO you just created.
4. Configure **“Lock the Taskbar”** policy as **Enabled** as a user policy. **User Configuration > Administrative Templates > Start Menu & Taskbar**
5. Configure “**Interactive Logon: Do not display last user name**” as a computer policy. This is in **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
6. Insert **a screenshot of the settings page of this GPO (Go to the bottom where it says Computer Configuration)**

Click or tap here to enter text.

1. Log on to Win11 or Server1, the taskbar should be locked and the last user name should not show.
2. Look through the Group Policy settings and choose 2 more settings for this GPO.
3. **List or screenshot each setting and why you chose it**.

Click or tap here to enter text.

1. **Insert a screenshot of the change it made in logging onto Win11 with a regular user**.

Click or tap here to enter text.

1. Close the Group Policy Management Editor, leave the Group Policy Management console open for the next activity.

# Activity 6-7: Setting the Default Domain Policy

Time Required: 5 minutes

Objective: Set password and other account policies in the Default Domain Policy.

Required Tools and Equipment: Server1

Description: The management has decided to enforce password and other account policies according to the policies recommended by a security audit.

**NOTE:** The only settings ever changed in the Default Domain Policy are the account policies. Never add other policies to this GPO.

1. Log on to Server1 as your administrator level account, if necessary.
2. Open the **Group Policy Management** console, if necessary. Right Click and **Edit** the **Default Domain Policy**.
3. Find and change the following Computer Configuration policies, leave the other settings alone. You may have to do some research to find these settings.
   1. Maximum password age: 90
   2. Minimum password length: 8
   3. Password must meet complexity requirements: Enabled
   4. Enforce password history: 24
   5. Account lockout threshold: 10
   6. Account lockout duration: 30 minutes
   7. Reset lockout counter after: 30 minutes
4. **Insert a screenshot of the settings page of this GPO showing the new settings** (Scroll to the bottom where it says Computer Configuration):

Click or tap here to enter text.

1. Close the Group Policy Management Editor. Leave the Group Policy Management console open for the next activity.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.