# Week 7 Windows Server Activities - Active Directory

Activities

[Week 7 Windows Server Activities - Active Directory 1](#_Toc210333245)

[Activity 7-1: Using GPO Security Filtering 1](#_Toc210333246)

[Activity 7-2: Creating a Software Restriction Policy 3](#_Toc210333247)

[Activity 7-3: Creating an Application Control Policy 5](#_Toc210333248)

[Activity 7-4: Creating the ADMX Central Store 8](#_Toc210333249)

[Activity 7-5: Managing Google Chrome with Group Policies 8](#_Toc210333250)

[Assignment Submission 10](#_Toc210333251)

**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 7-1: Using GPO Security Filtering

Time Required: 15 minutes

Objective: Change the default security filtering on a GPO and examine the results.

Required Tools and Equipment: Server1 and Win11

Description: You’re unsure how GPO security filtering works, so you decide to test some settings with a test OU and test GPO.

1. Log on to **Server1** as your administrator level account, if necessary.
2. Open the Group Policy Management console, if necessary. Click to expand the Group Policy Objects folder, and then click **GPO1**. In the right pane, click the **Scope** tab, if necessary.
3. In the **Security Filtering** dialog box in the right pane, click the **Add** button. Type **G\_Sales**, click **Check Names**, and then click **OK**. Add **Domain Computers** in the same way. (The Domain Computers security group is needed for the computer to read the Group Policy.)
4. In the **Name** list box, click **Authenticated Users** and click the **Remove** button. Click OK to confirm that you want to remove the delegation privilege. The **G\_Sales** Global Group and Domain Computers are now the only security principals with **Read and Apply Group Policy** permissions for **GPO1**.
5. Click the **Settings** tab. Scroll down to User Configuration. The **“Prohibit access to Control Panel and PC settings”** policy should be set to **Enabled**. If they aren’t there, please add them to the User Configuration of this group policy.
6. **Insert a screenshot.**

Click or tap here to enter text.

1. Link **GPO1** to the **Sales OU**.
2. On **Win11**, log on to the domain as **Sales1**.
3. Click **Start**, type **Control Panel**, Click **Control Panel**. You see a message that the operation was canceled because of restrictions on the computer.
4. **Insert a screenshot**.

Click or tap here to enter text.

1. Click OK. Because GPO1 is linked to the Sales OU, the Control Panel is restricted for Sales1.
2. Log off and log on as **Accounting1**. Open the **Control Panel**. You have access because Accounting1 isn’t in the WMI filter for GPO1. Close the Control Panel.
3. On **Server1**, change the security filtering for **GPO1** to add **Authenticated Users** back and remove **G\_Sales** and **Domain Computers**.
4. With **GPO1** selected in the left pane of the Group Policy Management console, click the **Delegation** tab in the right pane, and then click the **Advanced** button.
5. In the **GPO1 Security Settings** dialog box, click **Add**. Type **G\_Sales**, click **Check Names**, and then click OK.
6. If necessary, click **G\_Sales** in the list box at the top, click the **Read** check box in the **Deny** column, and then click **OK**. Click **Yes** to confirm that you want to set a **Deny** permission. The current permissions on the GPO allow all Authenticated Users members, except **G\_Sales**, to access the GPO.
7. **Insert a screenshot of these settings**.

Click or tap here to enter text.

1. On **Win11**, you should still be logged on as **Accounting1**. Open a command prompt 🡪 type **gpupdate** 🡪 press Enter to update group policies.
2. After the policy update is finished, try to open the **Control Panel** to verify that it’s no longer available to **Accounting1**.
3. **Insert a screenshot**.

Click or tap here to enter text.

1. Log off **Win11** and log on as **Sales1**. Verify that the Control Panel is available to Sales1. Log off Win11.
2. On **Server1**, remove **G\_Sales** from GPO1’s DACL. Add Authenticated Users back in.
3. Unlink **GPO1** from the **Sales OU**.
4. Close the Group Policy Management console. Stay logged on if you’re continuing to the next activity.

# Activity 7-2: Creating a Software Restriction Policy

Time Required: 10 minutes

Objective: Create a software restriction policy and test it.

Required Tools and Equipment: Server1 and Win11

Description: You want to begin locking down some computers in your company by restricting which programs users can run. You want to use settings in the Software Restriction Policies folder, so you decide to create a simple policy to test this feature. This policy is created in the User Configuration section of the GPO, but the process is the same in the Computer Configuration section.

1. Log on to Server1 as your administrator level account, if necessary.
2. Open the Group Policy Management console, and then open GPO1 in the Group Policy Management Editor. Expand **User Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Software Restriction Policies**. Right-click **Software Restriction Policies** and click **New Software Restriction Policies**.
3. Click the Security Levels folder in the left pane to see the three default rules in the right pane. The Unrestricted rule has a small check mark, indicating that it’s currently selected as the default. Double-click Disallowed to open this rule’s Properties dialog box. Click Set as Default. Click Yes, and then click OK.
4. Click the **Additional Rules** folder. Two path rules were created automatically that refer to a Registry key specifying the Windows directory and the Program Files directory. Leave them as is (recommended). Double-click the path rule listed first to open the dialog box. This path rule refers to the SystemRoot folder, which is C:\Windows on most systems, and it’s set to Unrestricted. Click Cancel. Look at the second path rule, which refers to the Program Files folder and is also unrestricted. Click Cancel.
5. Click **Software Restriction Policies** in the left pane. Double-click **Enforcement** in the right pane. In the Properties dialog box, click the All users except the local administrator’s option button. Read the other options and their descriptions, and then click OK.
6. Double-click Designated File Types in the right pane. In the Properties dialog box, scroll through the list of file types that are considered executable files, and then click Cancel. Close the Group Policy Management Editor.
7. In the Group Policy Management console, link **GPO1** to the **Employees OU**. This is where the users accounts are located, so this policy applies only to those users.
8. Log on to the domain from Win11 as your administrator level account. Open a command prompt window, type **gpupdate /force**, and press Enter. Close the command prompt window.
9. Create a folder on the local disk, c:\temp. Open Notepad and type the following commands  
   **dir /s  
   pause**
10. Save the file as "c:\temp\test.bat" and exit Notepad. Remember to use quotes around the filename so that Notepad doesn’t add the .txt extension. This simple batch file runs the dir command and lists files in subdirectories to test the software restriction policy you just created.
11. To be sure your batch file works, right-click Start, click Run, type c:\temp\test.bat in the Open text box, and press Enter. You exempted local administrators from the policy, so an Administrator account can still run this program. You see a long listing of all files and folders on the C drive.
12. Log off Win11 and then log on again as Sales1.
13. Start Notepad to verify that you can run programs in the C:\Windows directory. Exit Notepad.
14. Right-click Start, click Run, type c:\temp\test.bat in the Open text box, and press Enter. You see a message stating that your system administrator has blocked the program.
15. **Insert a screenshot:**

Click or tap here to enter text.

1. Click OK.
2. Log off Win11. On Server1, unlink **GPO1** from the Workstations OU.
3. In the Group Policy Objects folder, open GPO1 in the Group Policy Management Editor. Navigate to the Software Restriction Policies node under Computer Configuration, and then right-click it and click **Delete Software Restriction Policies**. Click Yes.
4. Stay logged on if you’re continuing to the next activity.

# Activity 7-3: Creating an Application Control Policy

Time Required: 10 minutes

Objective: Create an application control policy.

Required Tools and Equipment: Server1 and Win11

Description: You want to see how the Application Control Policies settings work differently from software restriction policies, so you create a rule in the AppLocker node.

1. Log on to Server1 as your administrator level account, if necessary.
2. Logon to Win11 as your administrator account, open a command prompt and do a  
   **gpupdate /force** to make sure the policies you applied in the last exercise are removed.
3. Open the Group Policy Management console, and then open **GPO1** in the Group Policy Management Editor. Expand **Computer Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Application Control Policies**. Click **AppLocker** and in the right pane, read the Getting Started, Configure Rule Enforcement, and Overview sections to see what’s available.
4. Click **Configure rule enforcement**. Notice that none of the Configured check boxes are selected; rules are enforced by default unless you click the Configured check box and then click “Audit only.” You need to click the Configured check box to enforce rules only if you need to override settings on a conflicting GPO. For now, leave the default settings, and click Cancel.
5. Click to expand **AppLocker** so that you see the four rule categories under it. Click **Executable Rules**. In the right pane, right-click empty space and click **Create Default Rules**. Click each of the default rules and examine the properties so that you know how you can change the default rules if needed. Be careful not to make any changes to the rules; click Cancel to close the properties of each rule when you’re finished examining it.
6. In the left pane, right-click **Executable Rules** and click **Create New Rule** to start the **Create Executable Rules Wizard.** Read the information in the Before You Begin window, and then click Next.
7. In the **Permissions** window, click the action **Deny**, and click the Select button next to the User or group text box.
8. In the Select User or Group dialog box, type **G\_Sales**, click Check Names, and click OK. **G\_Sales** contains the users **Sales1** and **Sales2**. By specifying that only this group is allowed, all other users are prohibited from accessing the applications defined in the rule. Click Next.
9. In the **Conditions** window, accept the default option Publisher and click Next. In the Publisher window, click Browse next to the Reference file text box. In the Open dialog box, double-click Windows NT, double-click Accessories, and click notepad.exe. Click Open.
10. In the **Publisher** window, move the slider up and down to see how it changes which properties are included in the rule. Leave the slider all the way down at File version, and then click Next.
11. In the **Exceptions** window, click Next. In the Name window, type NotePad in the Name text box. In the description text box, type **Deny G\_Sales notepad.exe** and click Create.
12. The Application Identity service must be set to Automatic on computers affected by AppLocker. Under the **Security Settings** node in this GPO, click **System Services** and double-click **Application Identity** in the right pane. Click Define this policy setting and then click **Automatic**. Click OK.
13. Close the Group Policy Management Editor, and in the Group Policy Management console, link GPO1 to Sales.
14. Log on to **Win11** as **Sales1**. Open a command prompt window. Type **gpupdate /force** and press Enter to make sure the new policy is applied. Close the command prompt window.
15. Start Notepad to verify that you can run programs in the C:\Windows directory. Exit Notepad.
16. Right-click Start, click Run, type **notepad** in the Open text box, and press **Enter**. You see a message stating that your system administrator has blocked the program. Because **Sales1** is included in the rule, this user account isn’t permitted to run the application.
17. **Insert a screenshot of the error message:**

Click or tap here to enter text.

1. Click OK.
2. Log off Win11.
3. On Server1, unlink GPO1 from the Workstations OU.
4. In the Group Policy Objects folder, open GPO1 in the Group Policy Management Editor. Navigate to the Application Control Policies node, and then right-click AppLocker and click Clear Policy. Click Yes, and then click OK.
5. Stay logged on if you’re continuing to the next activity.

# Activity 7-4: Creating the ADMX Central Store

Time Required: 10 minutes

Objective: Create the ADMX central store.

Required Tools and Equipment: Server1

Description: You want administrators to be able to work on group policies and customize administrative templates from any Windows Server 2019 or Windows 10 computer. To keep ADMX files from becoming unsynchronized, you need to create a central store.

1. Log on to Server1 as your administrator level account, if necessary.
2. Open **File Explorer** and navigate to **C:\Windows**. Click the **Windows** folder in the left pane. Copy the **PolicyDefinitions** folder in the right pane.
3. Navigate to **C:\Windows\SYSVOL\sysvol\domain\Policies**. Paste the **PoliciesDefinitions** folder under **Policies**. By pasting the entire **PolicyDefinitions** folder, there’s no need to create the folder structure.
4. Double-click the new **PolicyDefinitions** folder to inspect the contents. There should be more than 170 ADMX files and a language-specific folder.
5. **Insert a screenshot showing this new folder and the contents:**

Click or tap here to enter text.

1. To see the contents of an ADMX file, you can open it with Notepad. To associate ADMX files with Notepad, double-click Desktop.admx. You see a message stating that Windows can’t open this type of file. Click Try an app on this PC. When asked how you want to open the file, click the Use this app for all .admx files check box, and then click Notepad.
2. Browse through the Desktop.admx file to get an idea of how these files are structured, and then close all open windows.

# Activity 7-5: Managing Google Chrome with Group Policies

Time Required: 15 minutes

Objective: Manage Google Chrome with Group Policies

Required Tools and Equipment: Server1 and Win11

Description: You will download and deploy group policies to manage Google Chrome.

1. Download the zip file of Google Chrome policies from <https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip>
2. Unzip the file. Go to the folder **windows > admx**. Copy and paste **chrome.admx** and **google.admx** to **C:\Windows\SYSVOL\sysvol\mydomain\Policies\PolicyDefinitions**
3. Go back to the extracted Google policy files. Go to **windows > admx**. Copy and paste the two files in en-US to the en-US folder underneath **C:\Windows\SYSVOL\sysvol\mydomain\Policies\PolicyDefinitions**
4. Open Group Policy Management. Right Click on the **Workstations OU**, and Click Create a GPO in this domain, and link it here. Name the GPO, **Manage Google Chrome**.
5. Right Click the **Manage Google Chrome** GPO, and Click **Edit**.
6. Go to **Computer Configuration 🡪 Administrative Templates 🡪 Google 🡪 Google Chrome**.
7. Go to 🡪 **Startup,** **Home page and New Tab Page**
8. Open 🡪 **Use New Tab Page as homepage 🡪 Enabled** Click OK.
9. Open 🡪 **Configure the New Tab page URL** 🡪 **Enabled** 🡪 Enter <https://www.wncc.edu> Click OK.
10. Open 🡪 **URLs to open on startup** 🡪 **Enabled**, Show: <https://www.wncc.edu> Click OK.
11. Go to 🡪 **Content Settings** 🡪 **Default popups setting:** **Enabled, Allow all sites to show pop-ups** 🡪 Click OK.
12. Close the Group Policy Management Editor.
13. Click on the new GPO and click Details. Change the GPO Status to User configuration settings disabled.
14. Logon to Win11 as your administrator level account.
15. Download and install Google Chrome.
16. Logon as **Sales1**.
17. Run **gpupdate /force** at the command line.
18. Try out Google Chrome, close the start page, does the home page now go to wncc.edu? (You may need to close and start Google Chrome a couple of times.)
19. **Insert a screenshot:**

Click or tap here to enter text.

1. **Insert a screenshot of Google Chrome settings showing this setting:**

Click or tap here to enter text.

1. **Check out Google Chrome content settings, are popups allowed?**

Click or tap here to enter text.

1. **Insert a screenshot of this setting:**

Click or tap here to enter text.

**NOTE:** Unlink any Group Policies that you created.

**Do not** unlink **Default Domain Policy or Default Domain Controllers Policy**

## Assignment Submission

Attach this completed document to the assignment in Blackboard.