# Overview

Group policies can be created and linked at multiple locations and are processed in a specified order. The normal processing order works to process GPOs from least to most specific. This means that a GPO linked to an OU will override one linked at the domain. This order is the most logical way of configuring settings, but sometimes this order needs to be modified to allow or exclude certain GPO settings from being applied. In this lab, you will explore how the default processing order can be modified.

# Objectives

* Be able to create and link group policy objects.
* Be able to modify GPO policy processing.
* Be able to verify the operation of a group policy.

## Skills Reviewed

* Creating and Linking Group Policy objects.

## New Skills

* Configuring Group Policy Inheritance.
* Enforcing Group Policy.
* Filtering Group Policy.
* Verifying and troubleshooting group policy with **gpresult**.

# Initial Conditions

* Guided Practice – **Creating and Linking a GPO** is complete.

# Final Conditions

* A group policy named **Application Deny List** is created, linked to the domain, and set to be enforced.
* The **Greenville Administration** OU is blocking group policy inheritance.
* An OU named **GPO Exceptions** created in the root of the domain.
* A group named **No Application Deny list** created that is denied permission to apply the **Application Deny List** policy.
* **Joe Taylor** is a member of the **No Application Deny List** group.

# Instructions

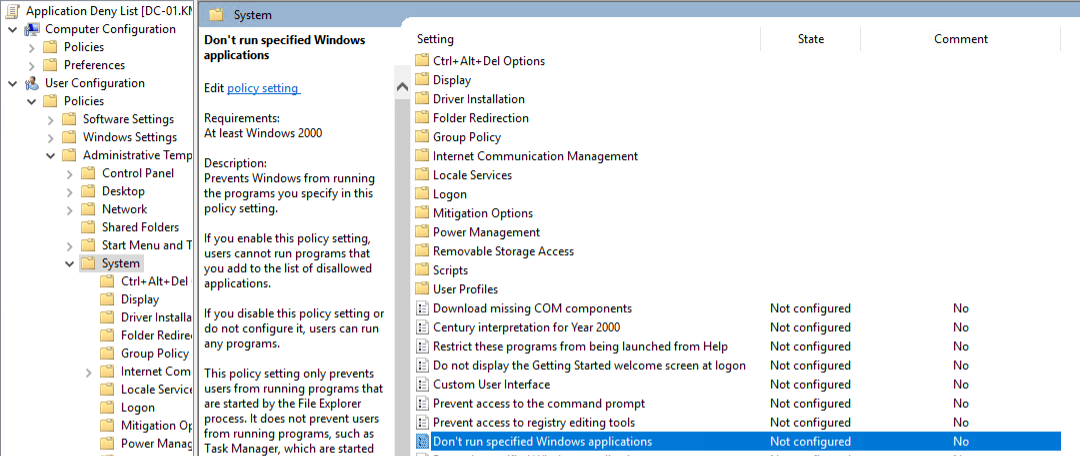
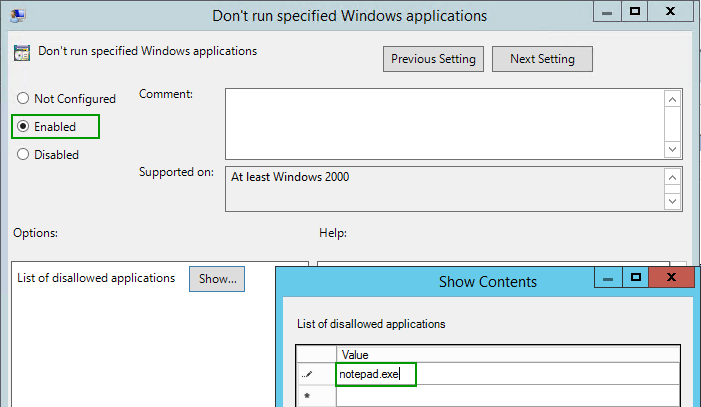
## Creating aN application Deny list

An application deny list is a group of programs that are not allowed to run on a computer. The method shown in this step is a simple method that is shown for demonstration purposes and should not be used in production.

Create a GPO to implement an **Application Deny List** by performing the following:

1. Logon to the **Server-01** virtual machine using an **KMWAdmin** account.
2. Open the **Group Policy Management** console.
3. Browse to the **Group Policy Objects** node under the **KMW.local** domain, right**-**click the node and select **New** from the context menu.

**Note:** Creating a GPO in this location will not link it to anywhere and thus not cause any changes in settings. This is considered a best practice as GPOs should be tested thoroughly before being placed into production.

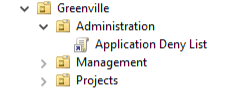
1. In the **New GPO** dialog box, type **Application Deny List** in the **Name**: text box and then click **OK**.
2. Right**-**click the **Application Deny List** policy and select **Edit**… from the context menu.
3. Browse to the **User Configuration🡪Policies🡪Administrative Templates🡪System** node. 
4. Double**-c**lick the **Don’t run specified Windows applications** policy to open the policy configuration dialog box.
   1. Select the **Enabled** option.
   2. Click the **Show…** button.
   3. Type **notepad.exe** in the **Show Contents** dialog box, as shown in the figure, and then click the **OK** button.
   4. Click the **OK** button again to close the policy configuration dialog box.
5. Close the **Group Policy Management Editor** window.

## Linking and Testing the group policy

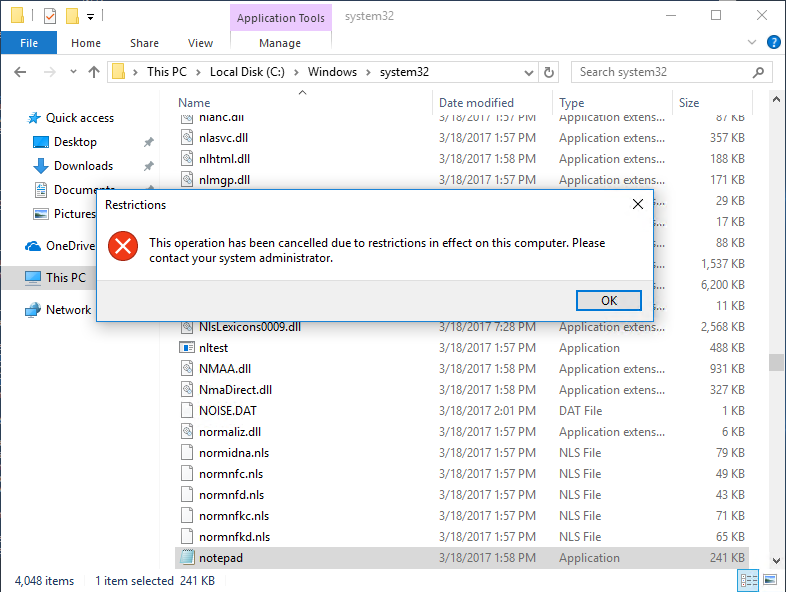
The group policy you created using the procedure above will prevent users from running the **notepad.exe** application.

In this step, you will test the policy by linking it to an OU. Logging on as a user in the OU and attempt to run the **notepad.exe** file and check the results.

Link the GPO to the **Greenville -> Administration** OU by performing the following:

1. Open **GPMC** and browse to **Domains 🡪 KMW.local 🡪 Greenville 🡪 Administration.**
2. Right**-**click the **Administration** OU and select **Link an Existing GPO…** from the context menu.
3. Choose the **Application Deny List** policy.
4. You should now see the group policy listed under the **Administration** OU as shown in the figure.

To test the policy, perform the following:

1. Logon to the **Client-01** virtual machine as **Joe Taylor** (jotaylor).
2. Type **Notepad** in the **search** and attempt to open the program. The system should prevent you from opening the link. If you browse to the location of the executable (**C:\Windows\System32\notepad.exe**) you will get the error message shown below.

## Testing GPO Inheritance

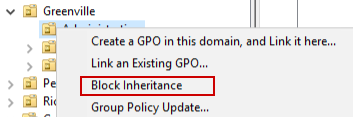
The settings in Group Policy objects are, by default, inherited by all the users/computers in the child containers. In this step, you will test inheritance.

1. **Unlink (**delete**)** the **group policy** from the **Greenville 🡪 Administration** OU and **link** it to the **domain**.
2. Logoff the **Client-01** machine and log back on as **Holly Brown** (hobrown) from **Richmond** 🡪 **Management OU**. This will refresh the policy for the user.
3. Attempt to open **Notepad** again. You should get the same result. In this case the policy is now being applied at the domain and is inherited by the users in the **Richmond 🡪 Management** OU.

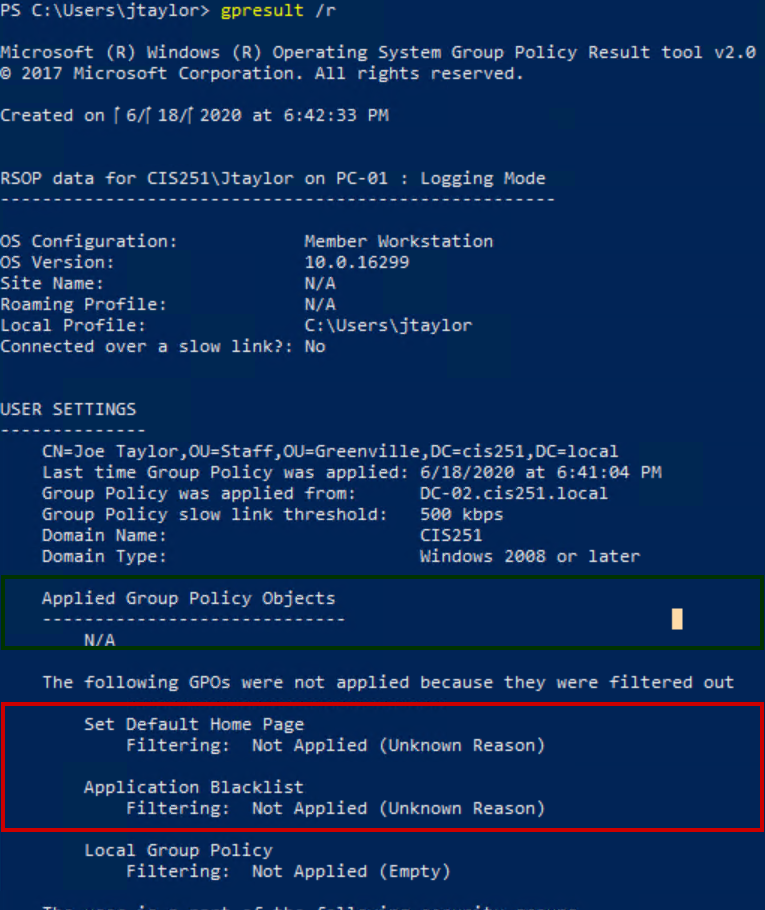
## Blocking GPO Inheritance

In this step, you will configure the **Greenville 🡪 Administration** OU to block inheritance. This will prevent settings from GPOs linked in parent containers from applying to the users in the **Greenville 🡪 Administration** OU.

Block the inheritance of GPOs in the **Greenville 🡪 Administration** OU, perform the following:

1. Open the **GPMC** and browse to the **Greenville 🡪 Administration** OU.
2. Right**-**Click on the **Administration** OU and **select** **Block Inheritance** from the context menu as shown in the figure on the right.
3. You should now see a little icon next to the **Administration** OU indicating that inheritance is blocked.
4. Logout of the **Client-01** virtual machine and log back in as **Joe Taylor** and verify that the **group policy** no longer applies (i.e. you can open **notepad**.) (You may have to force the update to apply by typing **gpupdate /force**.
5. You can also use the gpresult command to verify if a GPO is being applied. To do this, type the following in a PowerShell session:

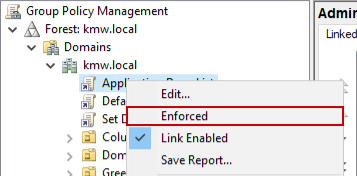
gpresult /r

1. You should see the output below. Notice the sections highlighted, there is a section showing Applied Group Policy Objects and GPOs that were filtered out.
2. Notice that it blocked both the **Set Default Home Page** and the **Application Deny List** policies. If you still wanted the **Default Home page** policy, you could link it to the **Administration** OU or set the **Enforced** option on the policy.

## Enforcing Group Policy

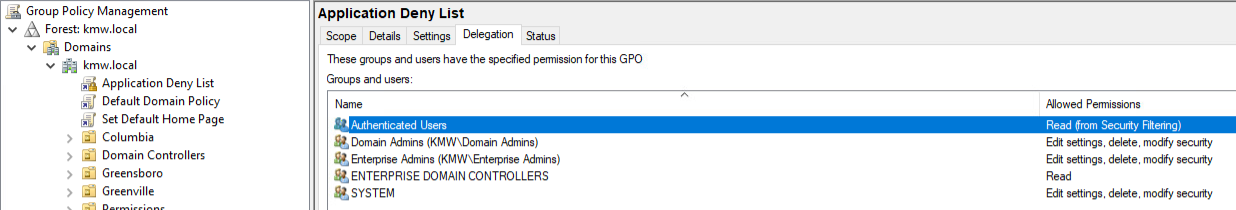
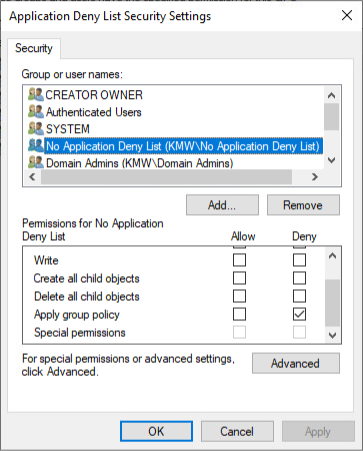
There are times, such as when you are configuring a GPO to apply security settings, that you want to prevent a policy from being blocked. In this case, you can set the GPO to Enforced to prevent it from being blocked.

To configure the Application Deny List policy to be enforced, perform the following:

1. Open the **GPMC.**
2. Locate the **Application Deny List** policy **linked** to the domain.
3. Right**-**click the policy and b **Enforced** from the context menu.
4. Notice when you select **Enforced**, the policy gets a lock next to it to show it has been enforced.
5. Test the policy by logging out and logging back in as **Joe Taylor** on **Client-01** and verifying that you can no longer open the **Notepad** application.

## Filtering Group Policy

On occasion you will want to prevent a GPO from applying to an individual or group of individuals in an OU. You could create an additional OU and place that user or group of users in the OU and configure the GPOs as necessary, but this is a bit complicated and makes for arbitrary OU creation. A simpler way is to create a group, place the users in that group and deny them permission to apply the GPO. In this step, you will configure a group of users and deny them permission to apply the **Application Deny List** GPO.

1. On **Server-01**, open **Active Directory Users and Computers.**
2. Create an **OU** called **GPO Exceptions** in the **root** of the domain**.**
   1. This is done because GPO troubleshooting can be complicated and being able to easily find the groups that have been denied permissions to a GPO is helpful.
3. In the **GPO Exceptions** OU create a globalsecurity group named **No Application Deny List.**
4. Add **Joe Taylor** to the **No Application Deny List** group.
5. Open the **GPMC** console.
6. Select the **Application Deny List** policy and select the **Delegation** **tab**. The default permissions are shown in the figure below.
7. In the **Delegation** window, click the **Advanced**… button to open the **Application Deny List Security Settings** dialog box.
8. Click the **Add**… button and add the **No Application Deny List** group.
9. Configure the permission so that the group is **denied** permission to **Apply group policy** as shown in the figure.
10. Close the dialog box and verify that the **No Application Deny List** entry is shown in the **Delegation** window and it has **Custom** in the **Allowed Permissions** column.
11. Verify that the policy nolonger is being applied to **Joe Taylor** by logging in and out of the **Client-01** machine and verifying that he can now open **Notepad**.

**Note**: You may have to log out and back an additional time to update your access token to reflect that you are a member of the **No Application Deny List** group.

## Submission requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

Invoke-Pester -Path C:\Scripts\GP18-Modifying\_Group\_Policy \_Processing.test.ps1

**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP18-Modifying\_Group\_Policy \_Processing.test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below

Text

Description automatically generated

1. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document**
2. **Upload** the **document** in the submission area of the assignment