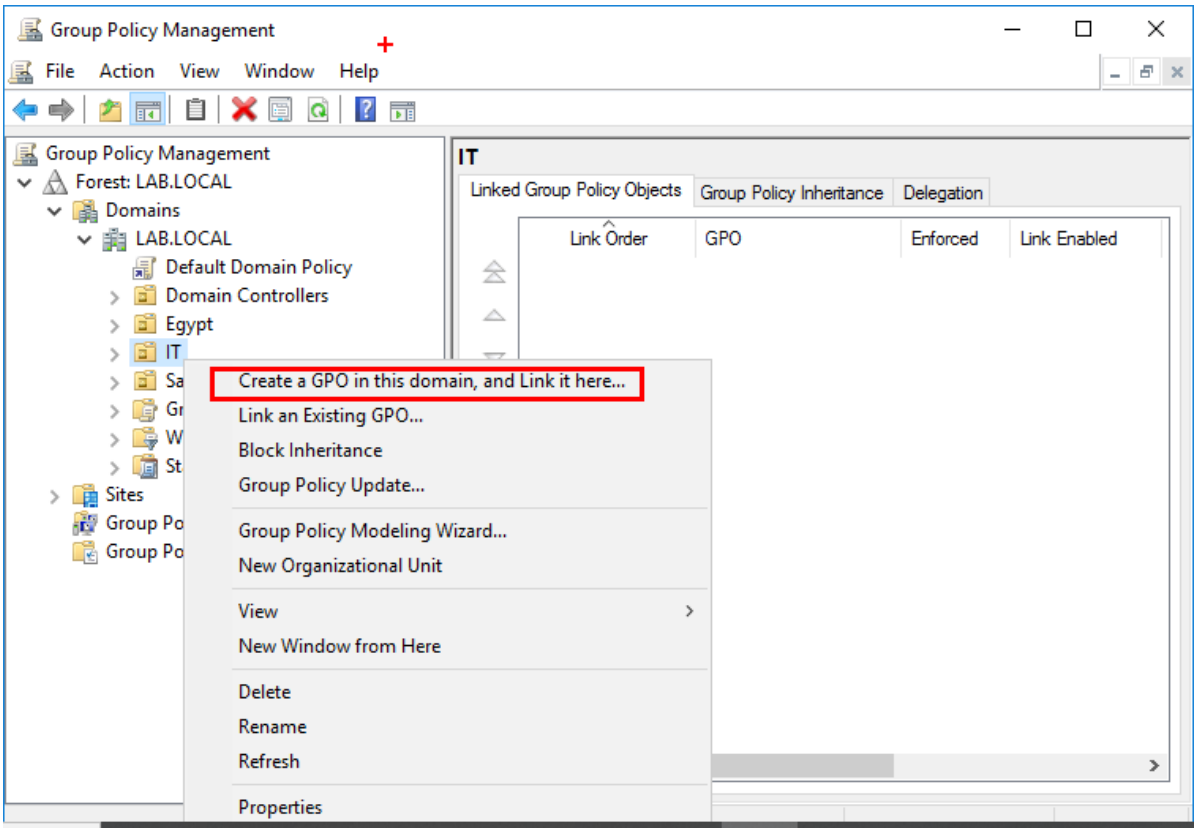
Lab Guide

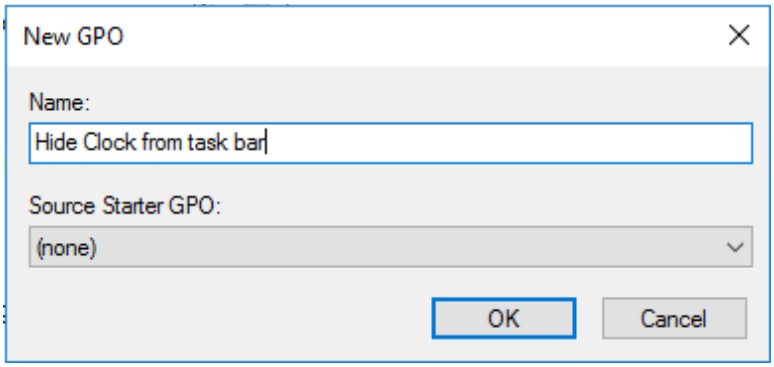
Group Policy Management

Implementing Group Policy Object

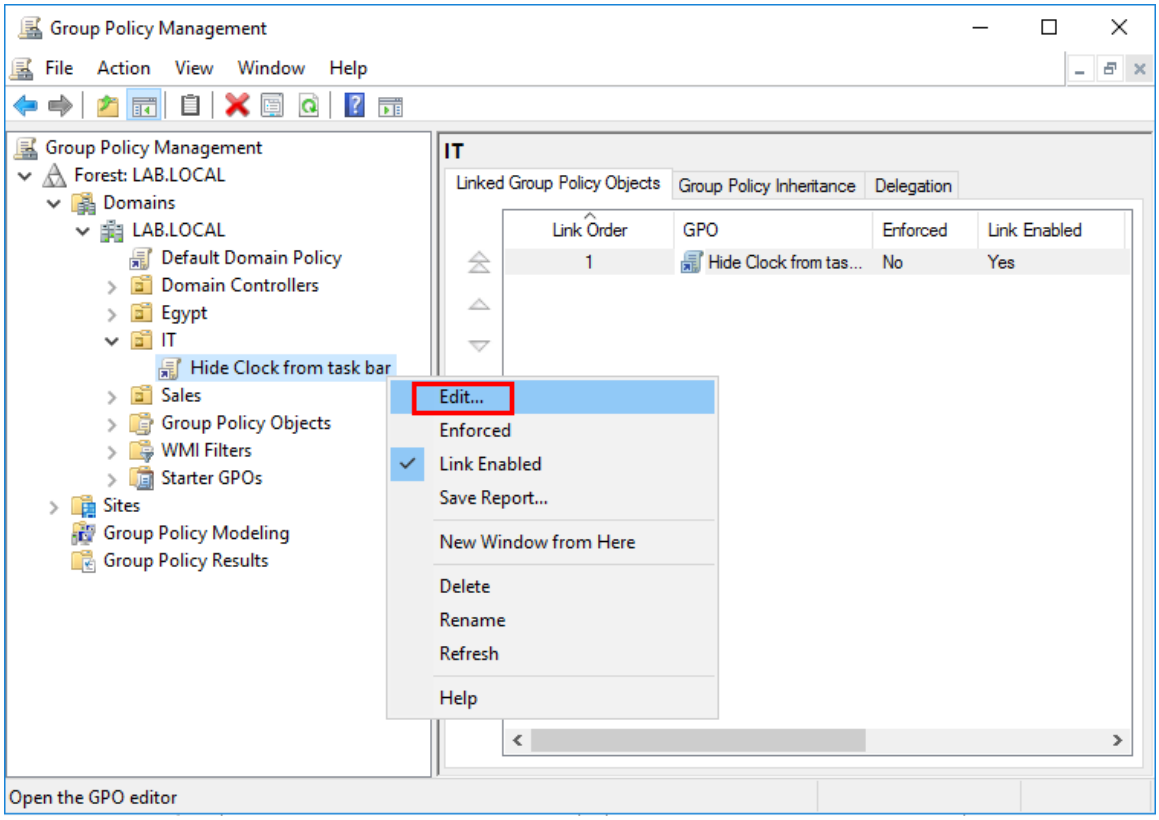
1. Group Policy can be used for various tasks, lets try first with a simple Setting to hide the clock from the taskbar
   From **Server Manager**, click on **Tools**, and select **"Group Policy Management"**
   R-click on the target OU, and click **Create a GPO in this domain and link it here…**



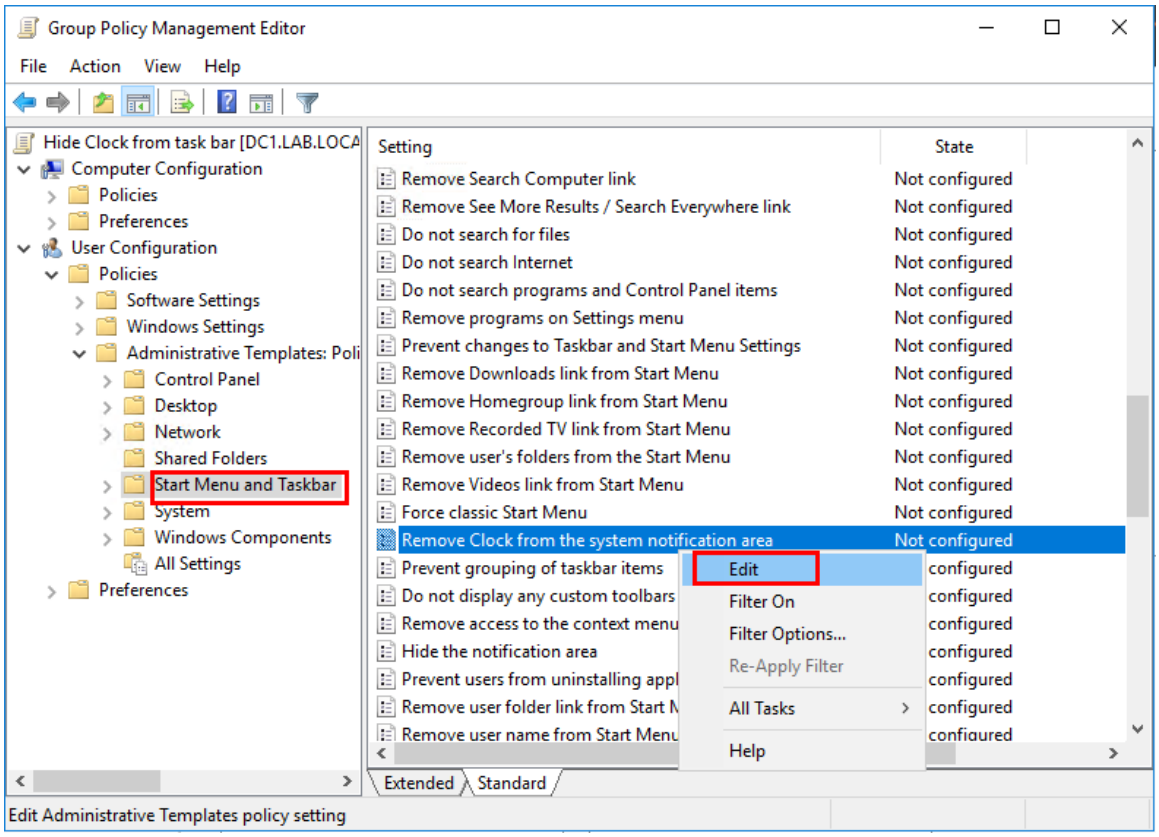
2. The wizard will ask for a **New GPO** name, give it a name and click **Ok**



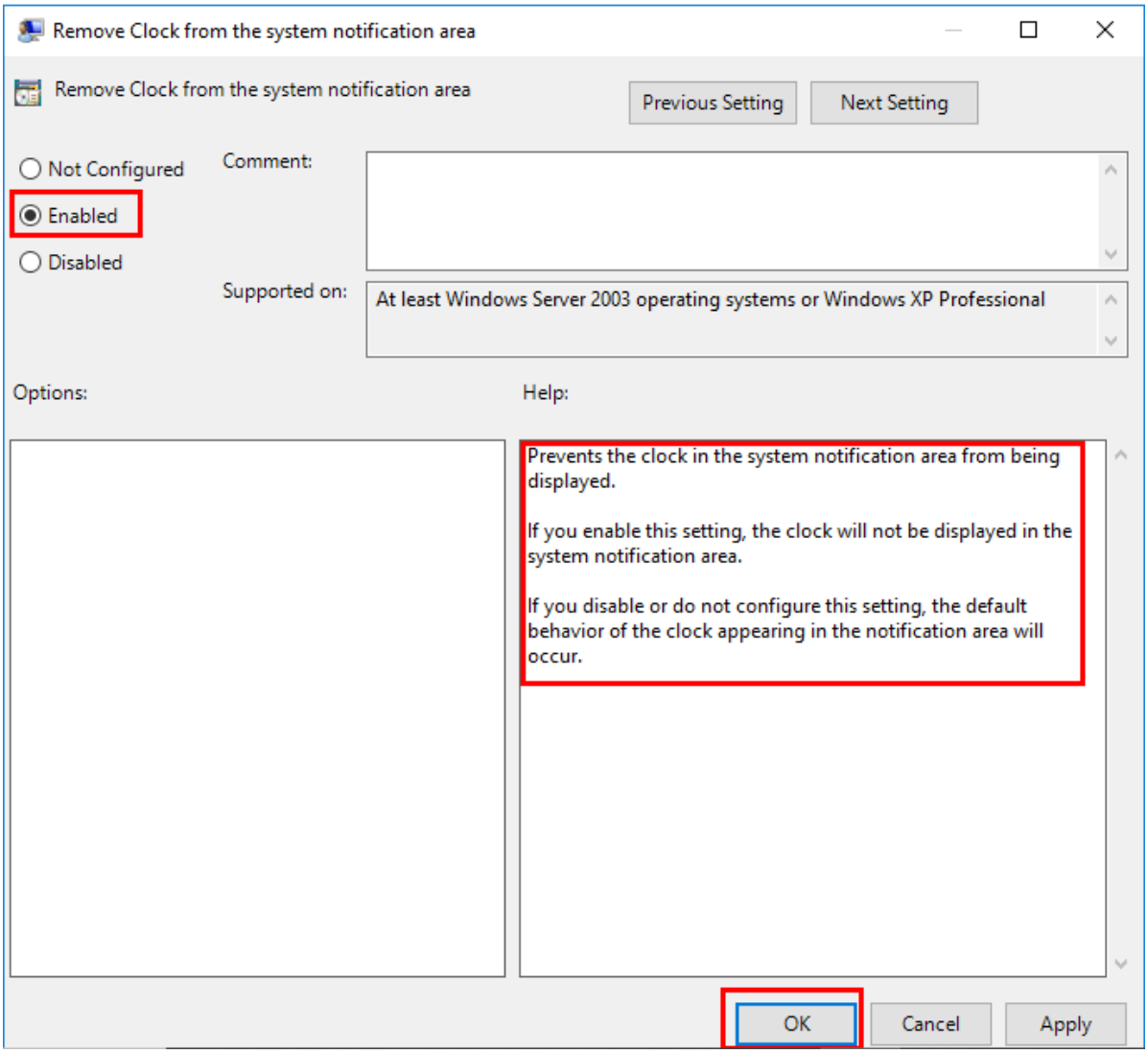
3. Now the GPO is created and we need to open it in the editor, and change the required setting, r-click on the GPO and select **Edit..**



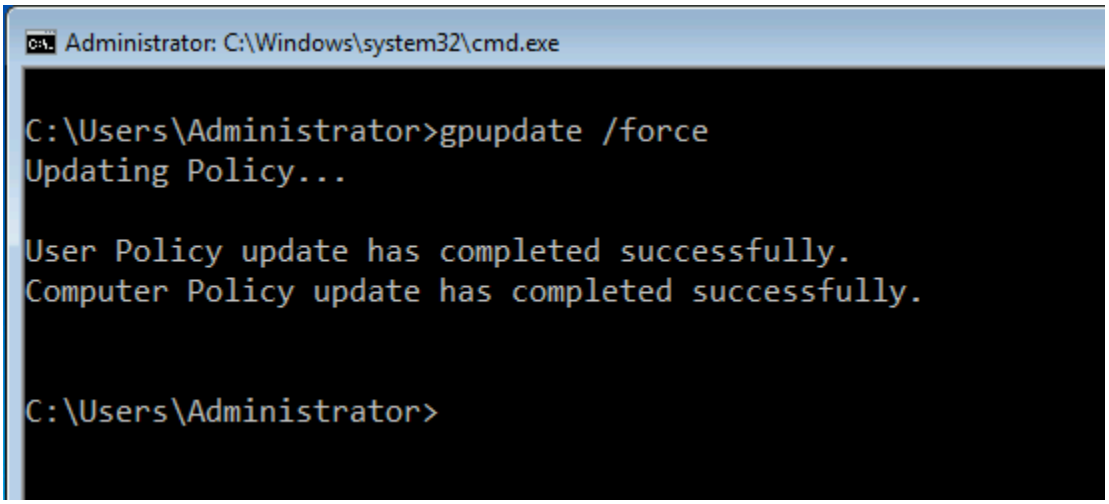
4. Now with the editor opened, we navigate to the target setting, as shown in the figure below, r-click on the setting and select **Edit**, or you can just double click on it.



5. In the setting windows, you will find an explanation on what exactly it does, click on **Enabled**, and click **Ok**

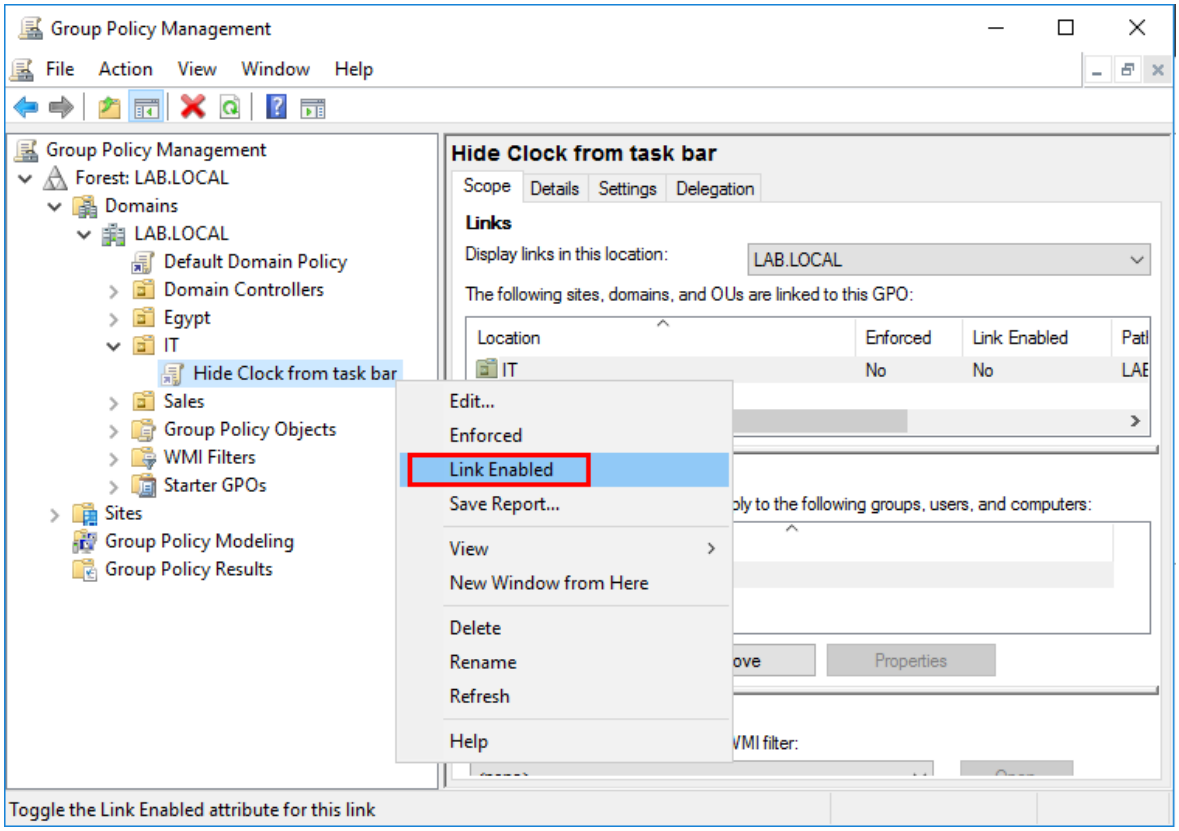


6. The setting is now changed, just close the editor and update the group policy on the client machine using the command **gpupdate /force** in CMD as show below:

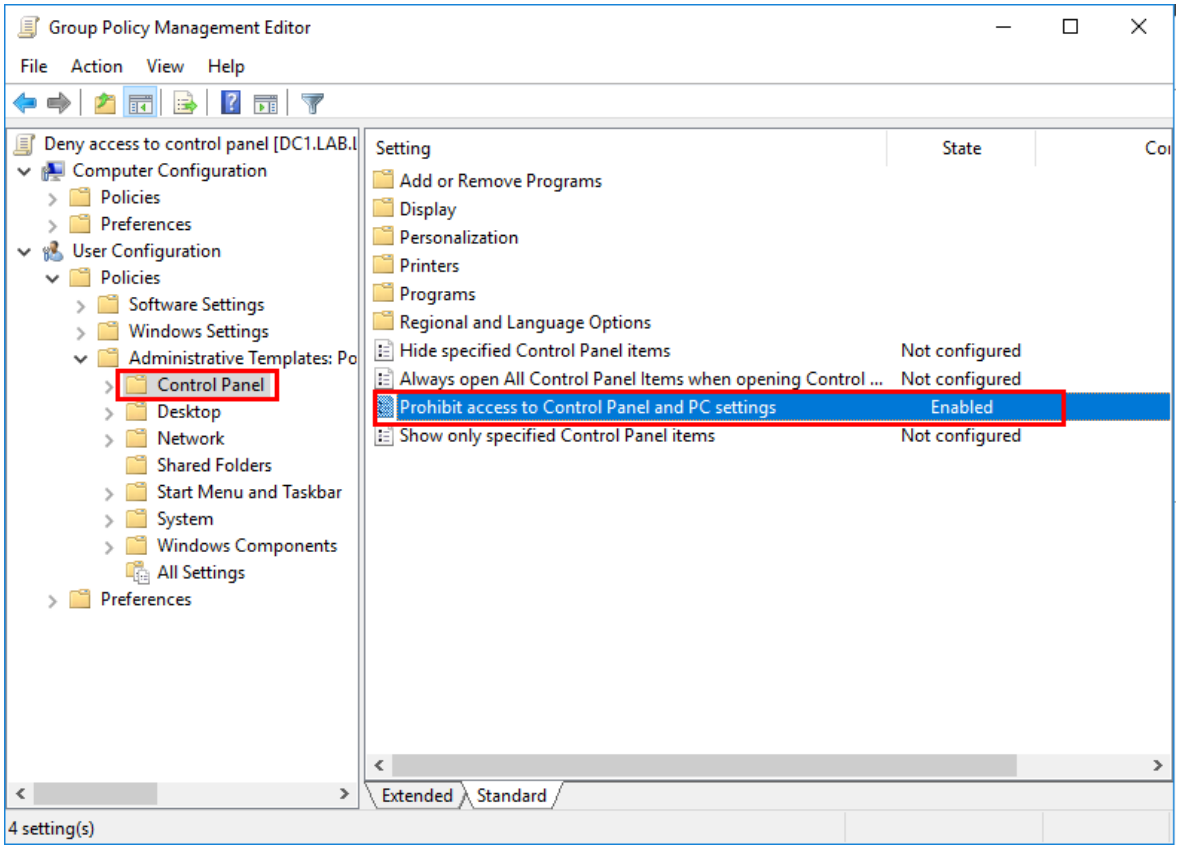


The client machine will update the policy eventually as it asks the domain controller for updates every 90 : 120 minutes, but in a lab environment we use the command as we don't have to wait.

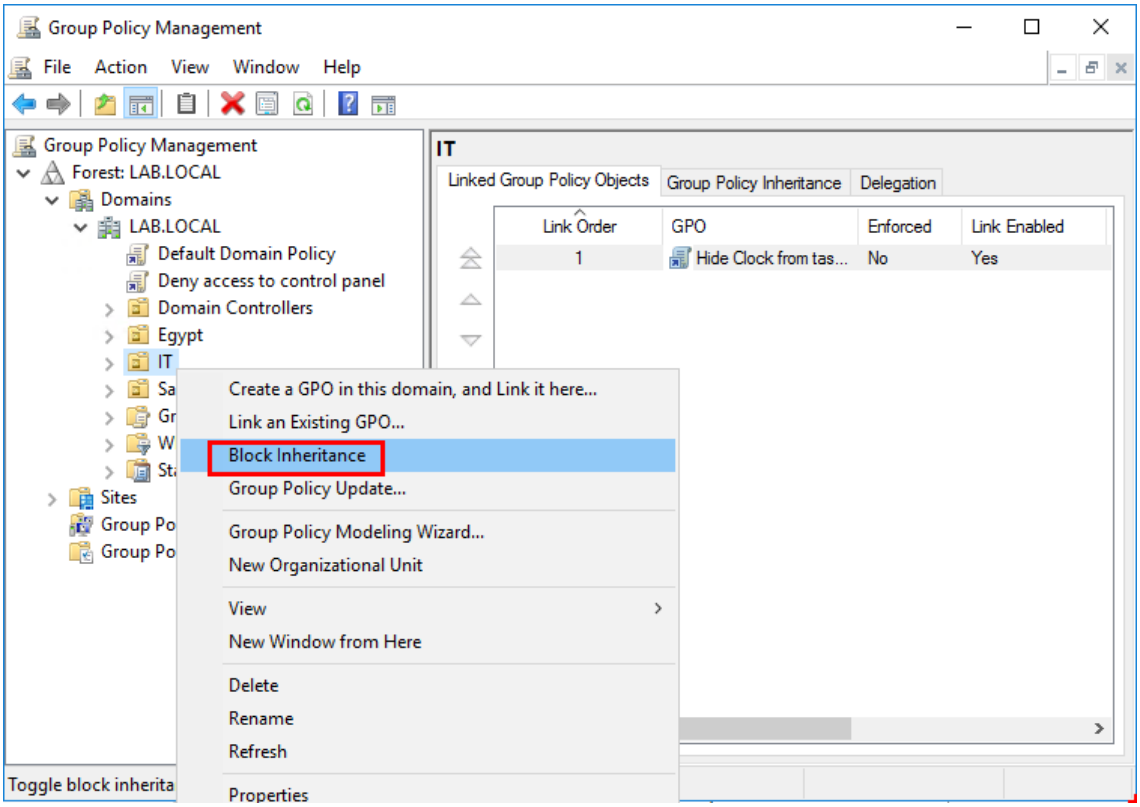
7. If you r-click on the GPO and clear the selection on **Link Enabled** option, it means the **GPO link** is still there but the GPO is not applied, you could use this option to temporary disable the GPO.



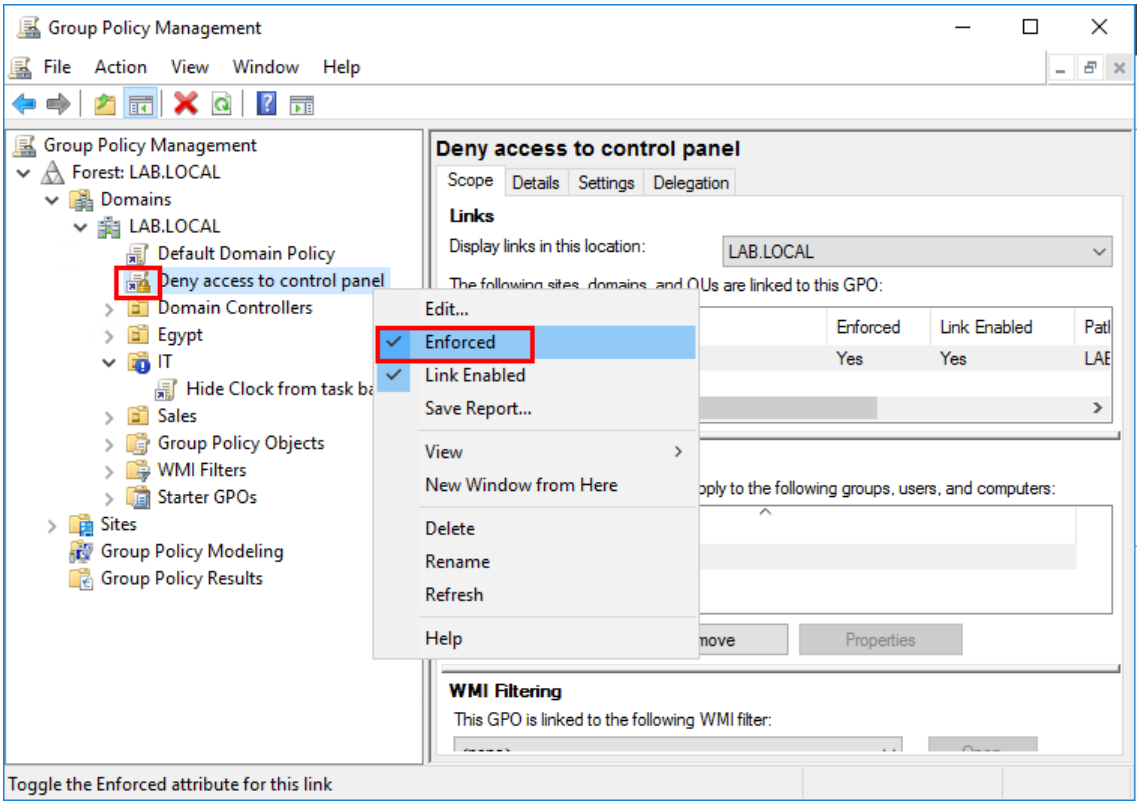
8. Now we create another GPO, with the name **"Deny Access to Control Panel"** and link it to the whole domain **"Lab.local".** This setting will restrict access to **Control Panel**



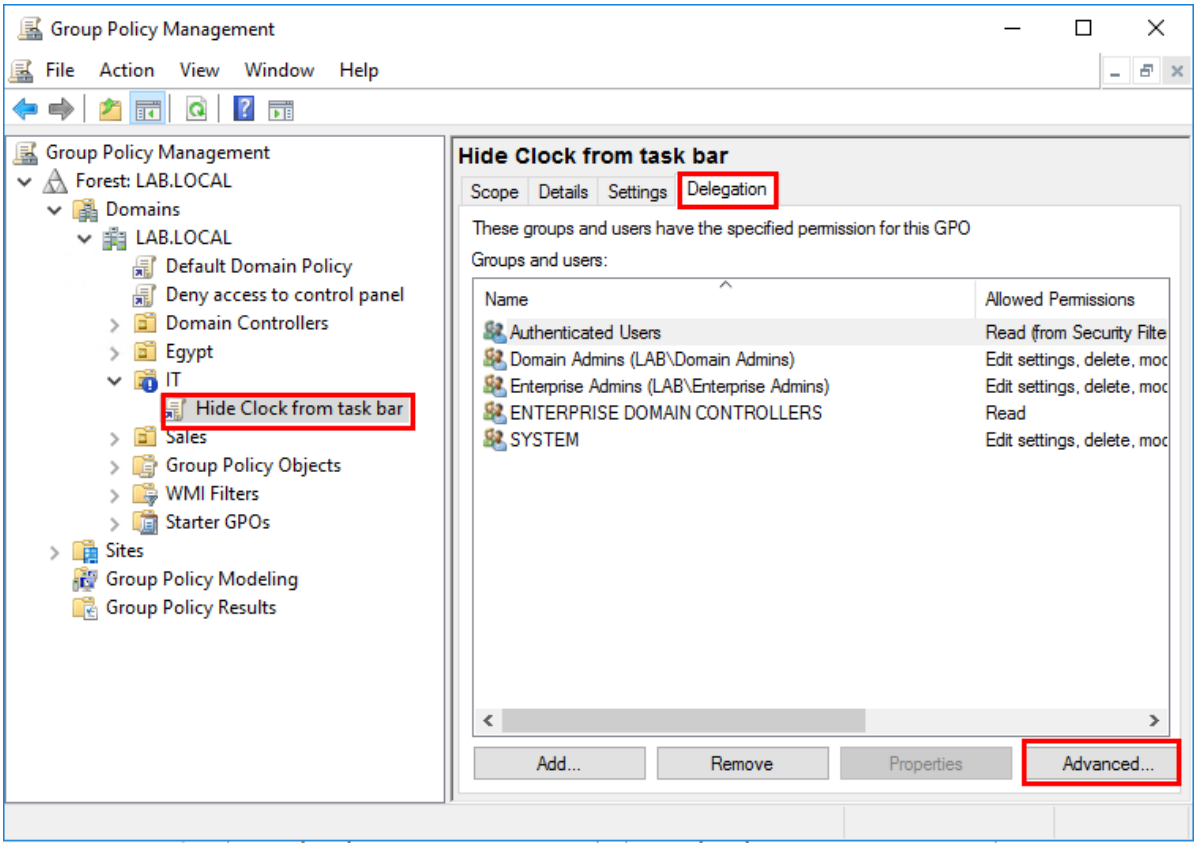
9. By inheritance the GPOs linked to the domain apply to all OUs.
   You can stop the inheritance on a specific OU, this means you will apply only special GPOs explicitly on that OU, to disable the inheritance, r-click on the OU and select **Block Inheritance**



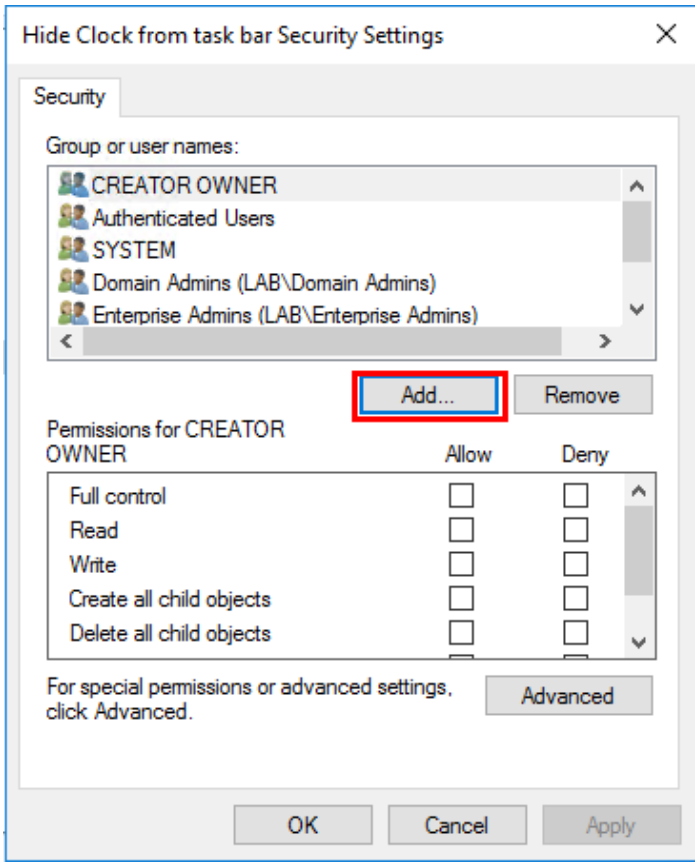
10. Now as requirements can change, it came up that there are no exceptions from “Deny access to control panel” policy to anyone, so we enable the **Enforced** option for the GPO, and it will go through any level with blocked inheritance on any OU below in the hierarchy. (it will put a small lock on the GPO icon)



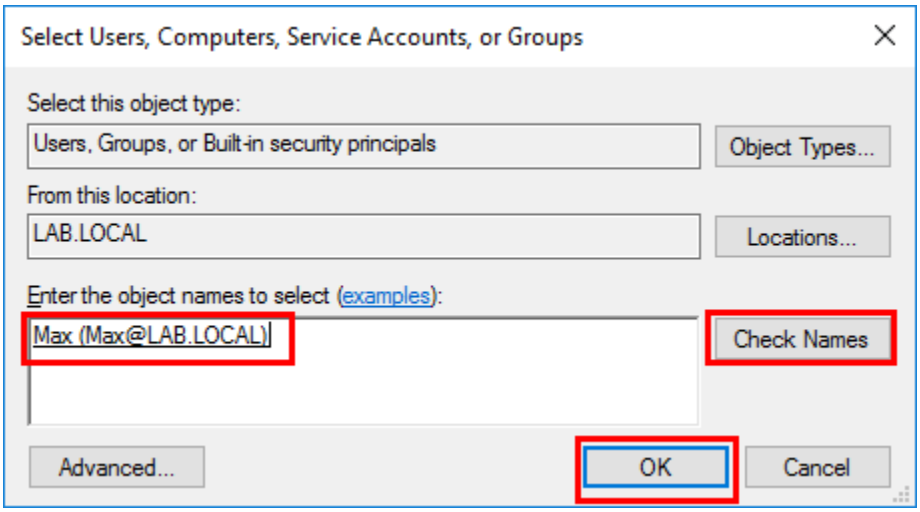
11. Security filtering enable you to disable the GPO for any object without having to remove it from the OU. Click on the GPO to select it, then open the **Delegation** tab, and click on **Advanced**



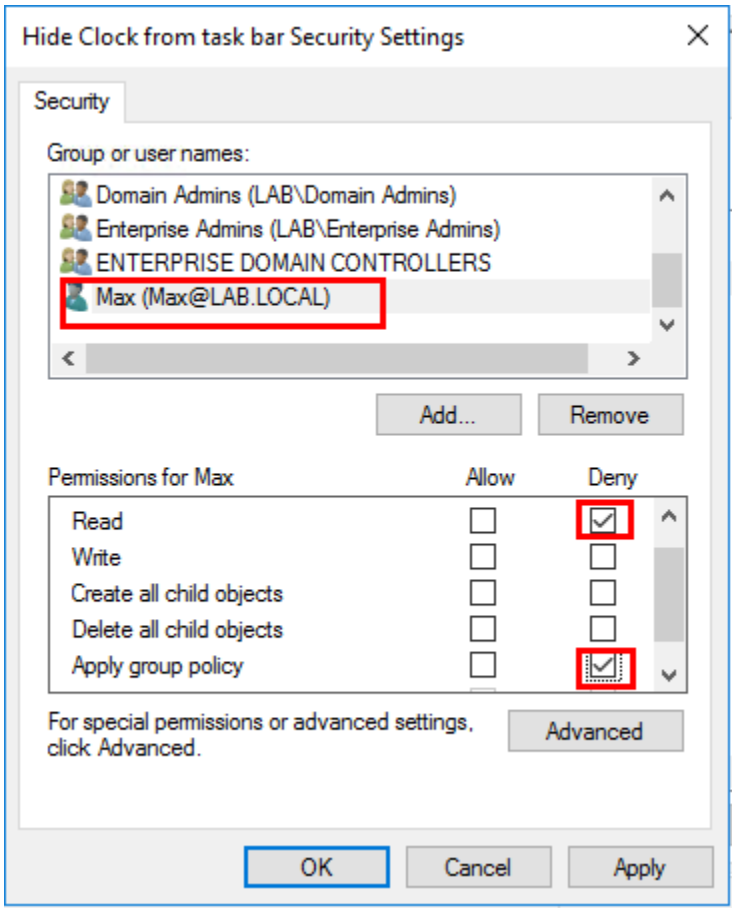
12. This will open the ACL to edit the permission for the GPO, click in Add



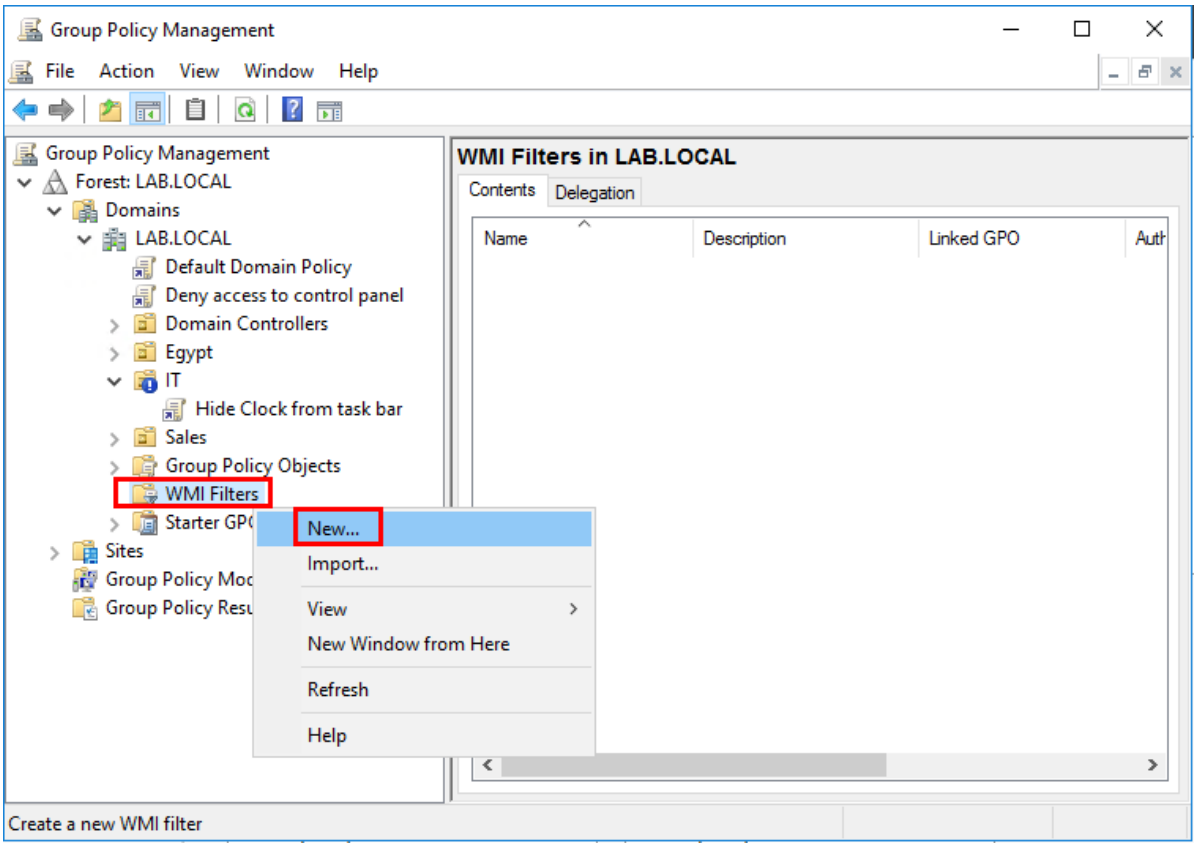
13. Type in the username and click **Check Names** to confirm it, then click **Ok**, this will add the user to the ACL



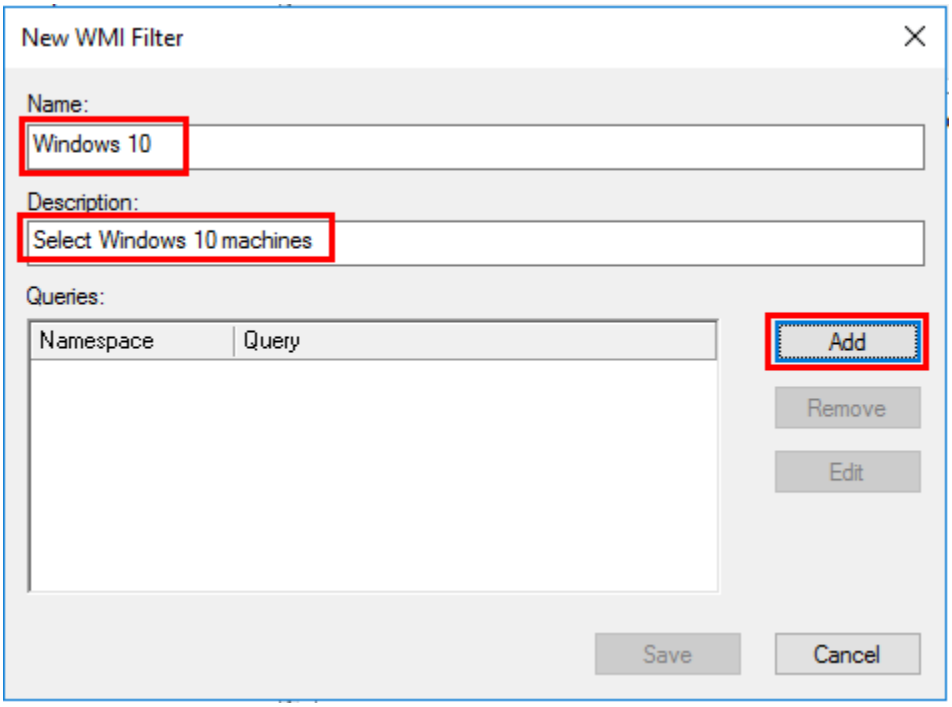
14. Now with the user account selected, put a check to **Deny "Read"** and **"Apply group policy"** permissions.
In the warning click **Yes**, it just confirms on you the **Deny** overrides any other permission.
Now after the client update the policy, **"Max"** will find out that this specific GPO doesn't apply on him.



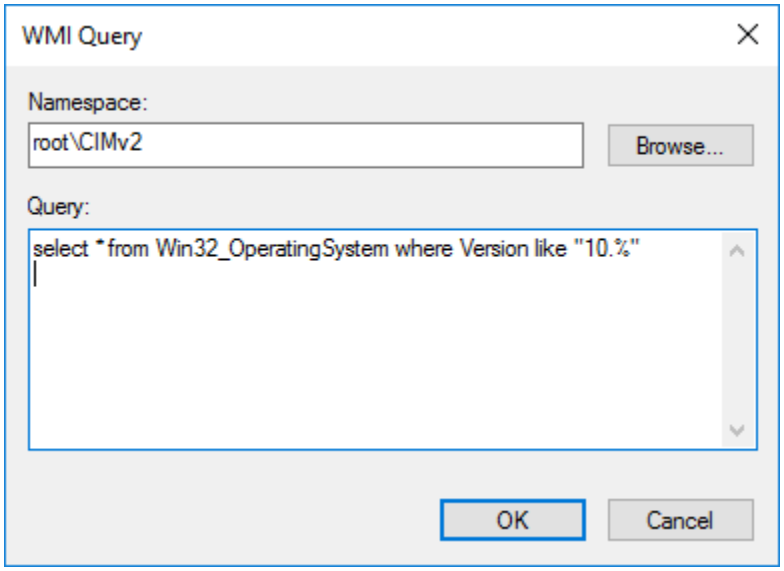
15. If you want to apply a WMI filter for GPO, go to **WMI Filters**, r-click and select **New...**



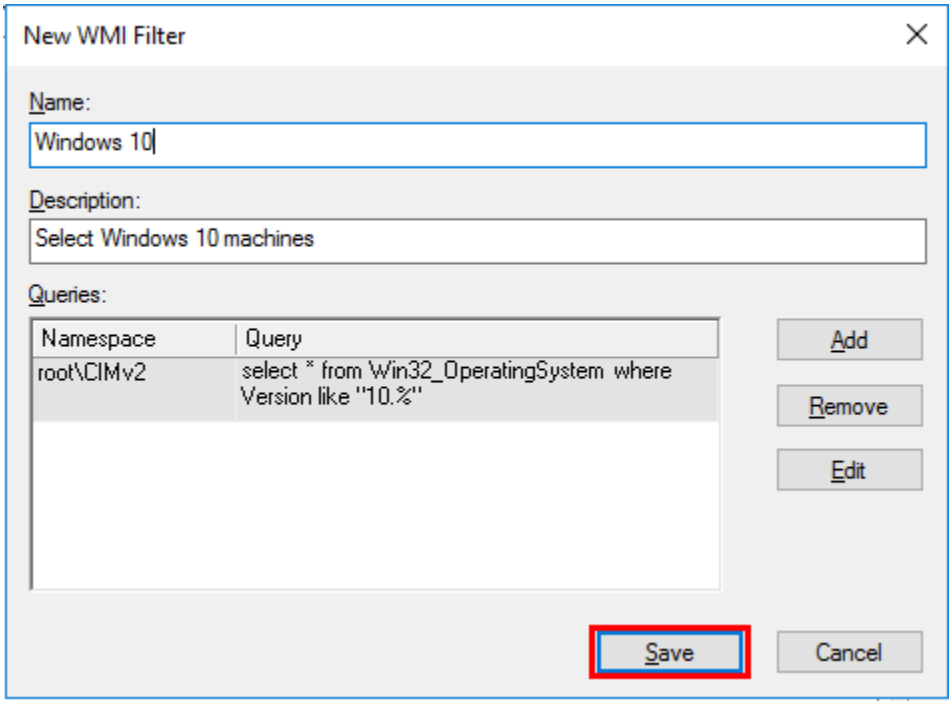
16. In the New **WMI Filter** window, type a name and description if you will, and click **Add**
We will add a filter to select only machines that run Windows 10



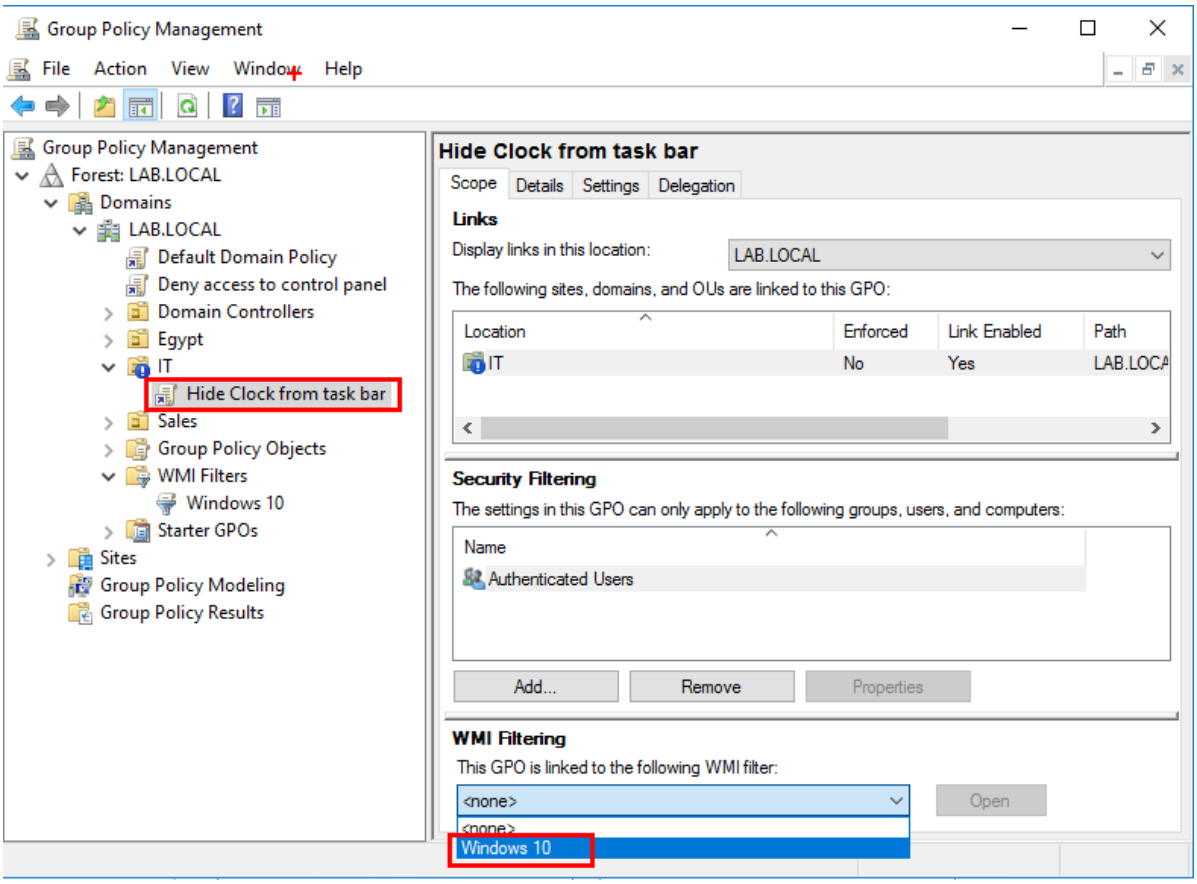
17. In the **WMI Query** window type in the query **“select * from Win32_OperatingSystem where Version like "10.%"** and click **Ok**



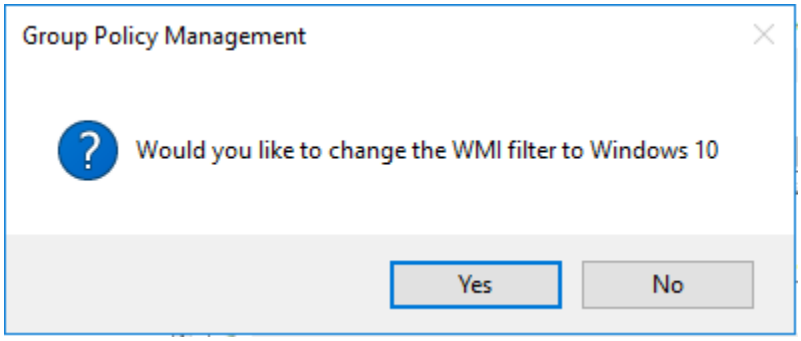
18. In the **New WMI Filter** window, click **Save**



19. Now we apply the filter to a GPO, select the required GPO, and select the filter as shown in the figure below:



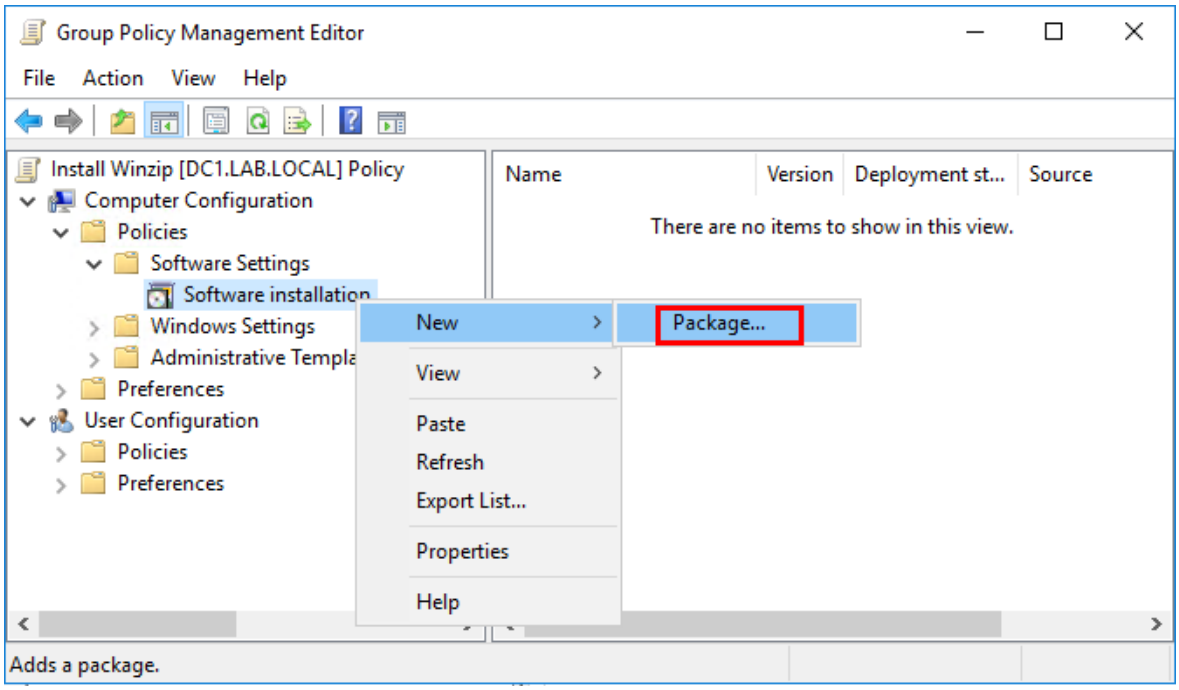
20. In the confirmation window click **Yes**



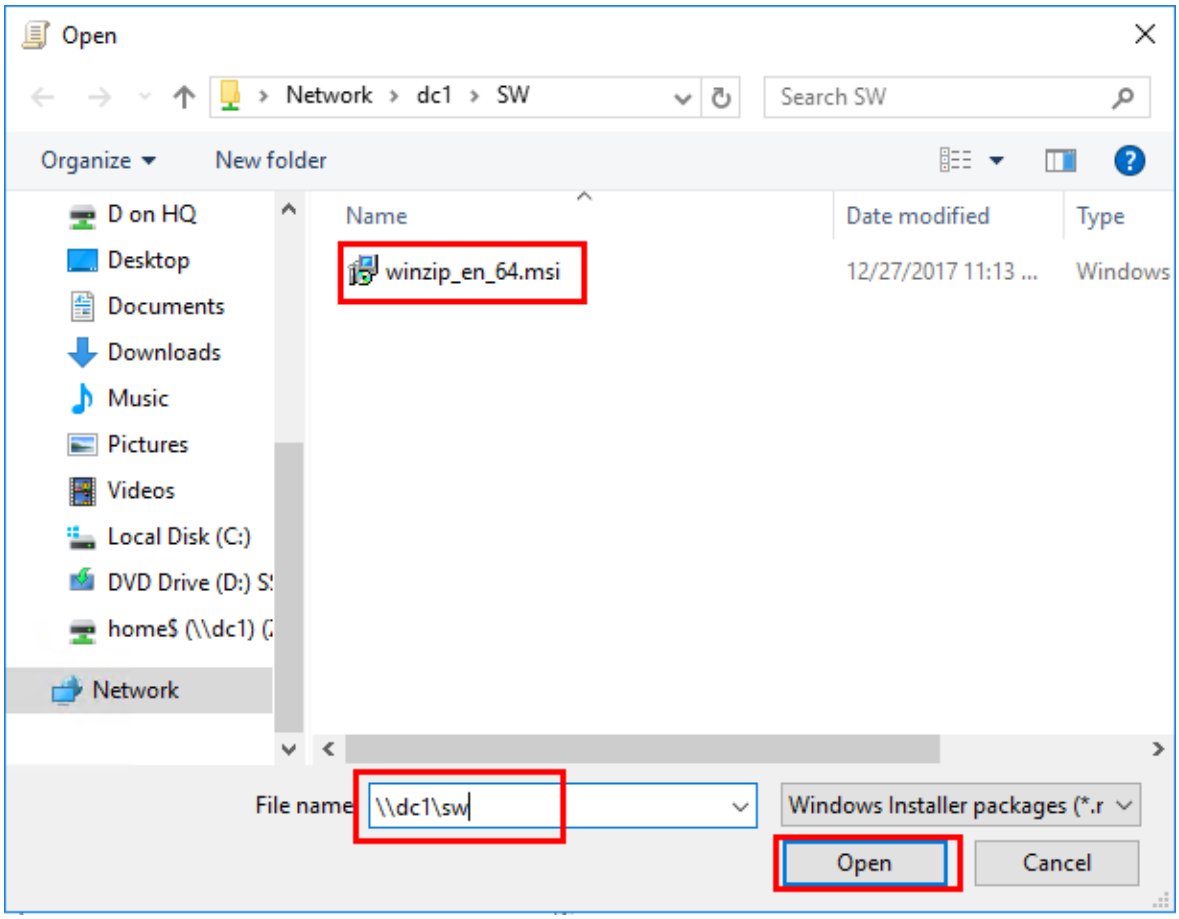
Now this policy will apply only the Windows 10 machines in the target OU as the filter is configured.

Use GPO to install software

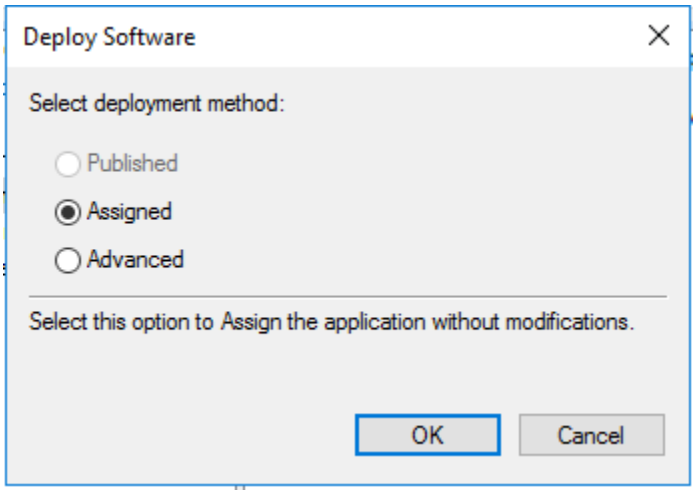
1. First, the software must be shared in a folder for everyone with a read permission.
2. Create a GPO and link it to the target OU, then r-click on it and select edit to open the editor, select the option to add a New **Package** in the path shown in the figure below:



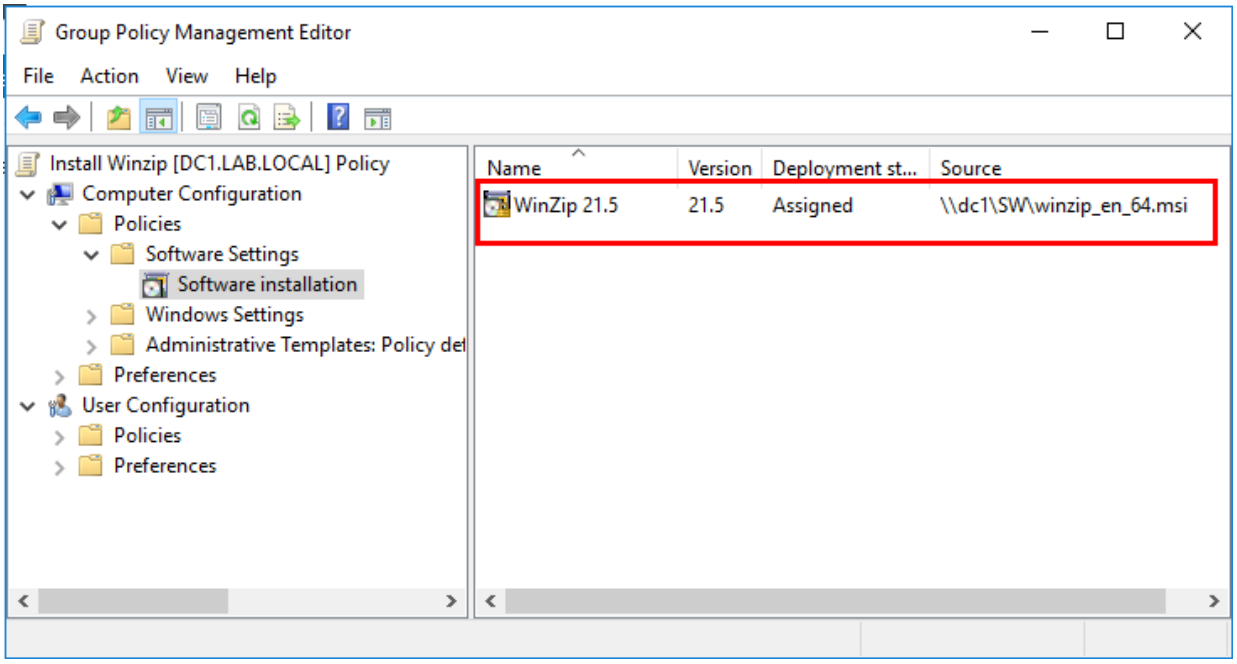
3. In the open window, you must type the UNC path for the network share for the software to be installed



4. In the **Deploy Software** windows click **Ok**

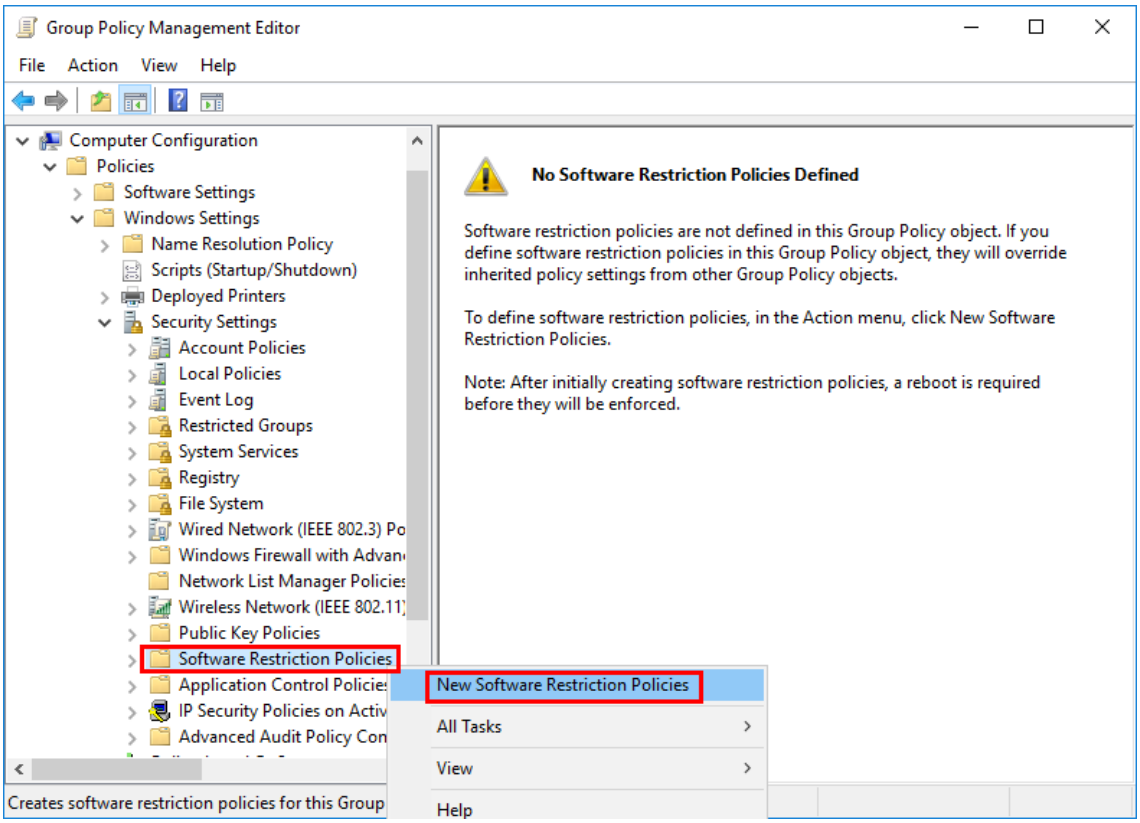


5. Wait moments for the file to be loaded and you will see the following window, close the window, and go to the client to update the policy, it will ask for a restart and the software will be installed after the restart.

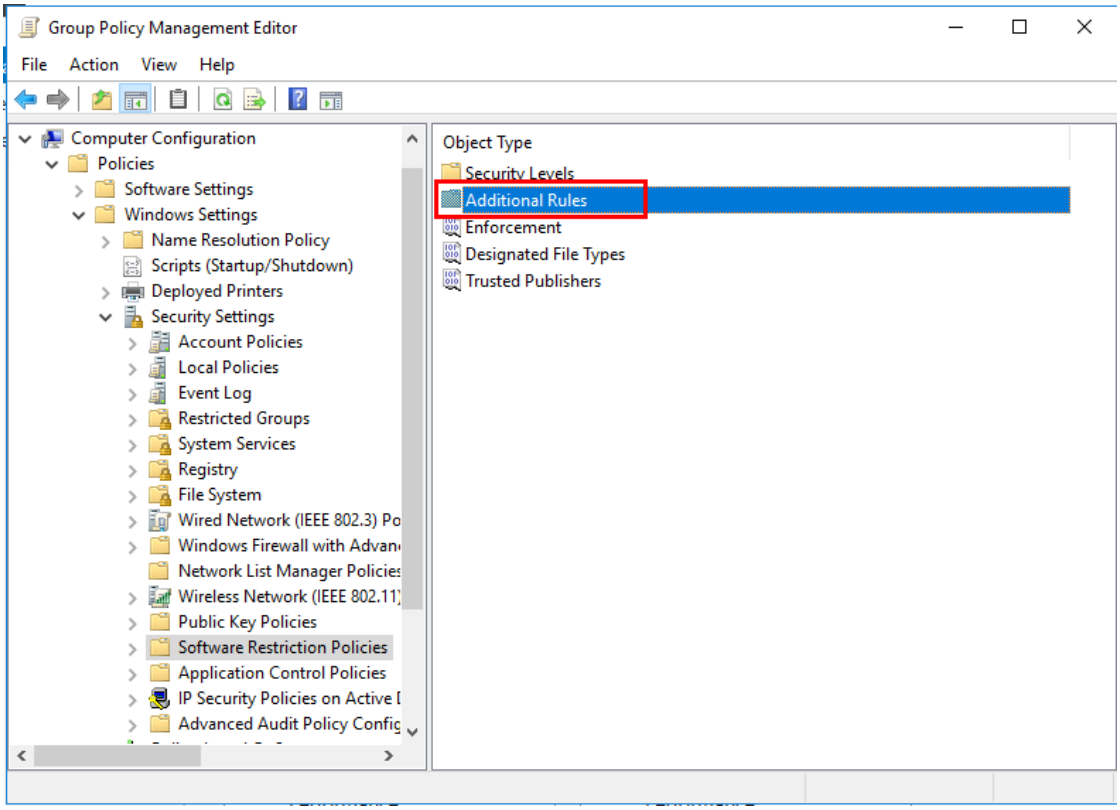


Software restriction using GPO

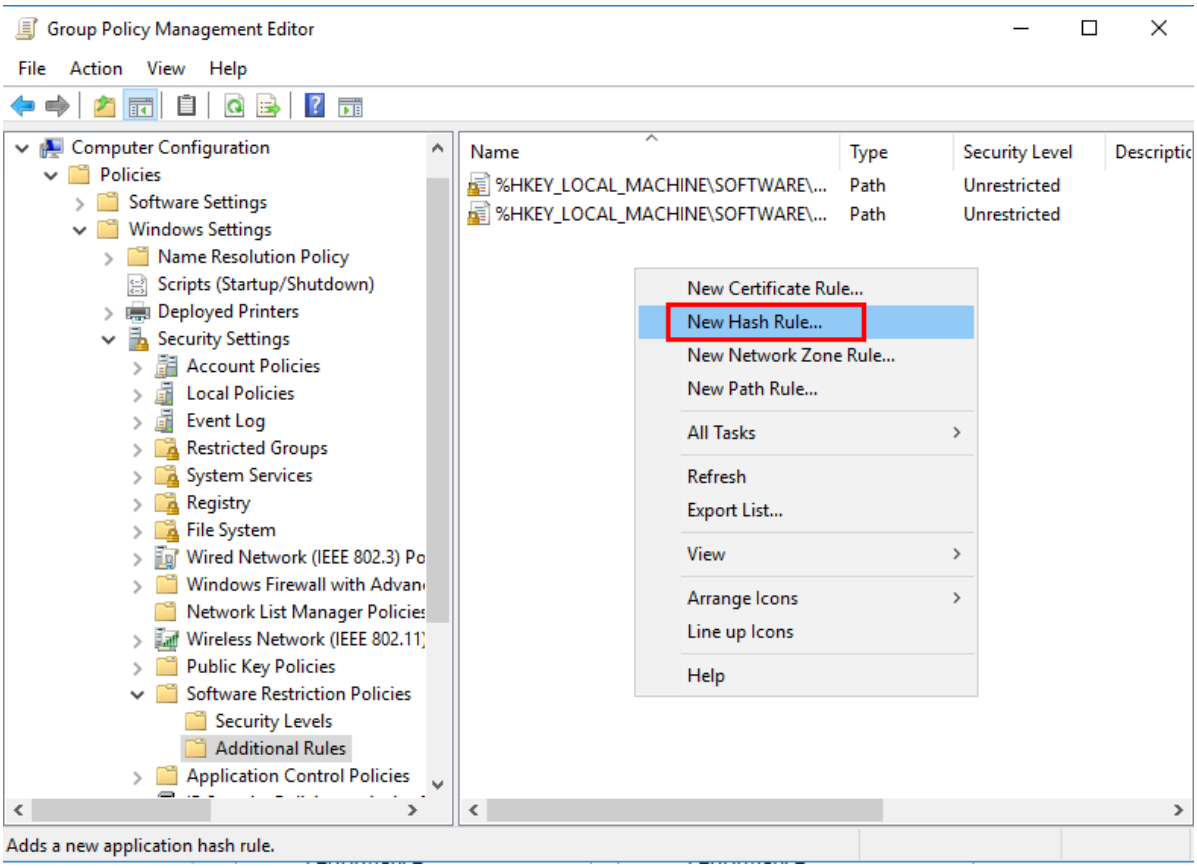
1. Get the executable file for that software you would like to restrict access to. I will use the .exe file to Solitaire, that is installed on Windows 7
2. Create a GPO for the target OU as usual, open the editor, go to the setting shown in the figure below:



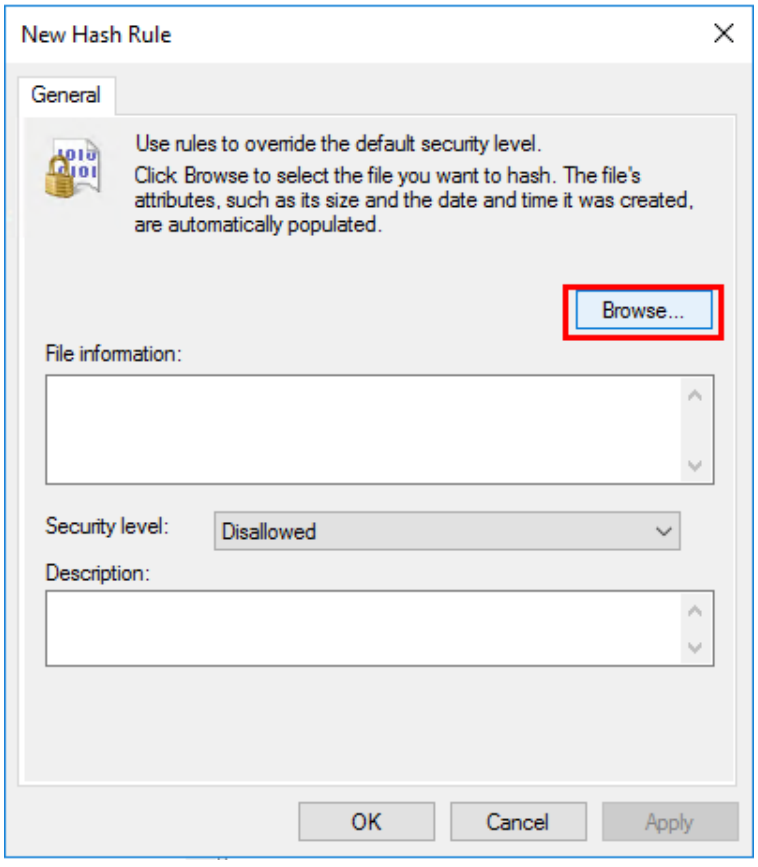
3. Double click on the Additional Rules folder



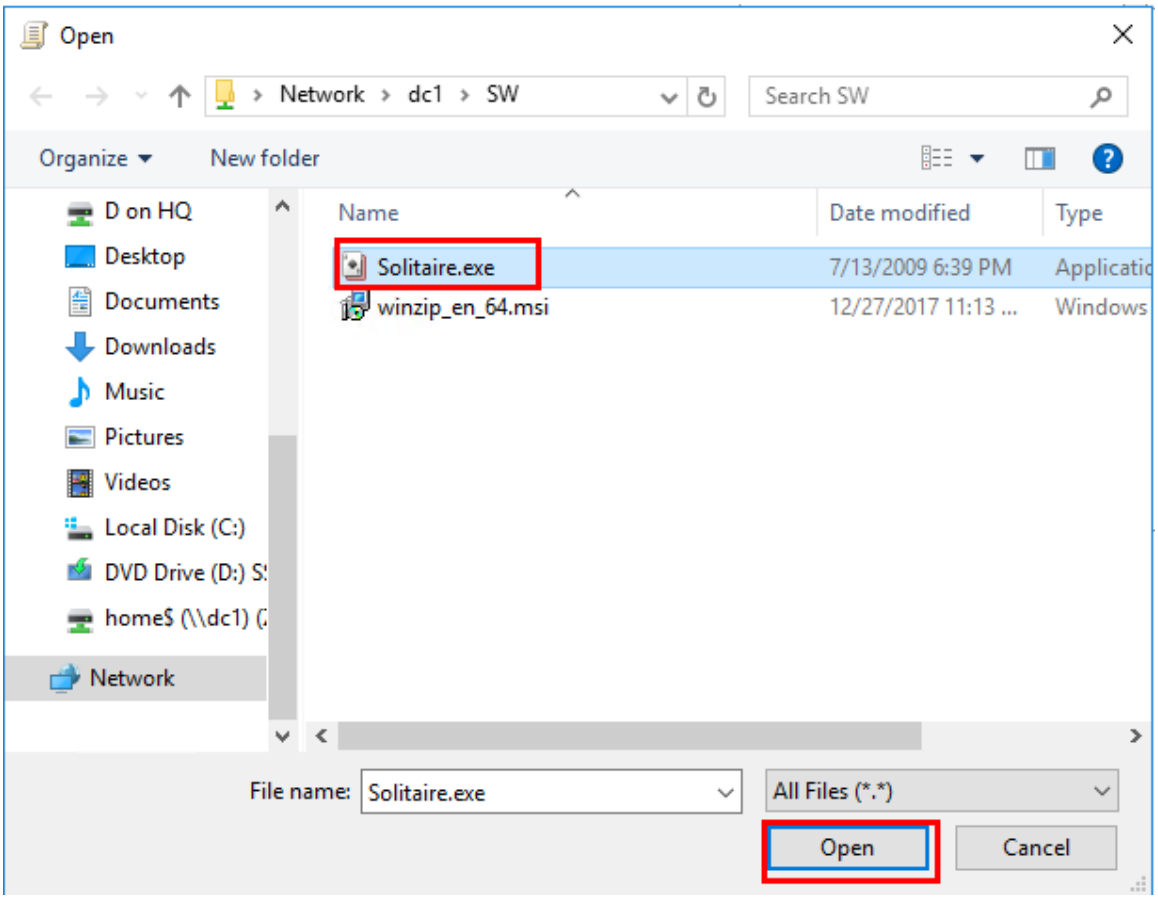
4. R-click in the free space inside and select **New Hash Rule…**



5. In the **New Hash Rule** window click **Browse**



6. Select the .exe file and click **open**



7. Notice that the default **Security level** is **Disallowed**, click **Ok** to close the window.