Lab Guide

Group Policy Management

Implementing Group Policy Object

 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...

📓 Group Policy Management				- [×
📓 File Action View Window Help					-	8 ×
🗢 🔿 🚈 📰 📋 🗮 🖼 🖬						
Group Policy Management Group Policy Management Group Policy Management Group Policy Management Group Policy Domain Policy Group Policy Domain Controllers Group Policy Update Group Policy Update Group Policy Modeling M New Organizational Unit View New Window from Here Delete Rename	Wizard t	Group Policy Inheritance GPO	Delegation	Link Ena	abled	
Refresh		-				>
Properties						

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

New GPO	×
Name: Hide Clock from task bar	
Source Starter GPO:	
(none)	~
	OK Cancel

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..**

File Action View Window Help	🗟 Group Policy Management		- 🗆 X
Group Policy Management ✓ ▲ Forest: LAB.LOCAL ✓ ∰ LAB.LOCAL ↓ Inked Group Policy Objects Group Policy Inheritance Delegation ↓ Link Order GPO Enforced Link Enabled ↓ Link Order GPO Enforced Link Enabled ↓ Imk Enforced ↓ Imk Enforced ↓ Imk Enabled Save Report New Window from Here Delete Rename Refresh Help	🔜 File Action View Window Help		_ 8 >
 ✓ ▲ Forest: LAB.LOCAL ✓ ▲ Domains ✓ ▲ LAB.LOCAL ④ Default Domain Policy ▷ ▲ Domain Controllers > ▲ Egypt ✓ ■ Hide Clock from task bar > ▲ Sales > ④ Starter GPOs ✓ WMI Filters > ④ Starter GPOs ✓ Link Enabled Save Report New Window from Here Delete Rename Refresh Help 	💠 🤿 🙍 🛅 📋 🗙 🗐 🍳 🛛 🖬		· · · · · · · · · · · · · · · · · · ·
Open the GPO editor	 ✓ A Forest: LAB.LOCAL ✓ Domains ✓ LAB.LOCAL ✓ Default Domain Policy > Domain Controllers > Egypt ✓ IT ✓ Hide Clock from task bar > Sales > Group Policy Objects > WMI Filters > Sites Ø Group Policy Modeling Ø Group Policy Results 	Linked Group Policy Objects Group Policy Inher Link Order GPO 1 Hide Clock from Edit Enforced Link Enabled Save Report New Window from Here Delete Rename Refresh Help	Enforced Link Enabled m tas No Yes

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.

Group Policy Management Editor			_	×
File Action View Help				
🗢 🄿 🙋 📰 🗟 🛛 🕅 🦷				
Hide Clock from task bar [DC1.LAB.LOCA	Setting		State	1
E Computer Configuration	Remove Search Computer link		Not configured	
> 🦰 Policies	🖹 Remove See More Results / Search Even	ywhere link	Not configured	
> Configuration	Do not search for files		Not configured	
 Wer Configuration Policies 	🗈 Do not search Internet		Not configured	
 Policies Software Settings 	🗈 Do not search programs and Control Pa	anel items	Not configured	
Windows Settings	🖹 Remove programs on Settings menu		Not configured	
 Administrative Templates: Poli 	🖹 Prevent changes to Taskbar and Start M	lenu Settings	Not configured	
> Control Panel	🖹 Remove Downloads link from Start Mer	nu	Not configured	
> C Desktop	🖹 Remove Homegroup link from Start Me	enu	Not configured	- 1
> 📫 Network	E Remove Recorded TV link from Start Me	enu	Not configured	
Shared Folders	🖹 Remove user's folders from the Start Me	enu	Not configured	
> 🚞 Start Menu and Taskbar	🖹 Remove Videos link from Start Menu		Not configured	
> 📔 System	🖹 Force classic Start Menu		Not configured	
> indows Components	Remove Clock from the system notifica	tion area	Not configured	
🖺 All Settings	🖹 Prevent grouping of taskbar items	Edit	configured	
> 🧎 Preferences	🖹 Do not display any custom toolbars	Filter On	configured	
	🖹 Remove access to the context menu	Filter Options	configured	
	Hide the notification area		configured	
	🖹 Prevent users from uninstalling appl	Re-Apply Filter	configured	
	🖹 Remove user folder link from Start N	All Tasks	> configured	
	Remove user name from Start Menu	Help	configured	>
< >	Extended Standard	Theip		
dit Administrative Templates policy setting	(/			

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

om the system not	fication area				×
om the system noti	ication area Prev	ious Setting	Next Setting		
Comment:					^
					~
Supported on:	At least Windows Server 2003 opera	ating systems or W	Vindows XP Profes	sional	$\hat{}$
	Help:				
	displayed. If you enable this system notificatio If you disable or d	setting, the clock on area. lo not configure tl	will not be display his setting, the def	/ed in the fault	
	om the system notif Comment:	Comment: Supported on: At least Windows Server 2003 opera Help: Help: Prevents the clock displayed. If you enable this system notification If you disable or displayed of the clock	m the system notification area Previous Setting Comment: Supported on: At least Windows Server 2003 operating systems or V Help: Prevents the clock in the system not displayed. If you enable this setting, the clock system notification area. If you disable or do not configure t behavior of the clock appearing in occur.	om the system notification area Previous Setting Next Setting Comment:	om the system notification area Previous Setting Next Setting Comment:

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.

📓 Group Policy Management				_	
📓 File Action View Window Help					_ & ×
<table-cell-rows> 🔿 🗾 🗙 🖸 🖬</table-cell-rows>					
Group Policy Management Group Policy Management Group Policy Ablace Group Policy Domains Group Policy Domain Policy Group Policy Objects Group Policy Modeling Group Policy Results Toggle the Link Enabled attribute for this link Group Policy Inters	Hide Clock from task bar Scope Details Settings Delega Links Display links in this location: The following sites, domains, and O Image: Comparison of the comparison	LAB.LOCAL	Enforced No	Link Enable No	LAE
loggie the Link Enabled attribute for this link					

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

Group Policy Management Editor		_	×
File Action View Help			
🗢 🔿 🙍 🗊 🗟 🕅 🍸			
 Deny access to control panel [DC1.LAB.I Computer Configuration Policies Preferences User Configuration Policies Software Settings Windows Settings Administrative Templates: Po Control Panel Desktop Network Shared Folders System System Windows Components All Settings Preferences 	Setting Add or Remove Programs Display Personalization Printers Programs Regional and Language Options Hide specified Control Panel items Always open All Control Panel Items when opening Control Prohibit access to Control Panel and PC settings Show only specified Control Panel items	State Not configured Not configured Enabled Not configured	Coi
	٢		>
< >	Extended Standard		
4 setting(s)			

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**

📓 Group Policy Management					- 🗆	×
📓 File Action View Window Help					-	8 ×
🗢 🔿 🙍 🗊 📋 🗙 🗐 🍳 👔						
Group Policy Management	IT		_			
 Forest: LAB.LOCAL Image: Image: Image:	Linke	d Group Policy Objects	Group Policy Inheritance	Delegation		
✓ iiii LAB.LOCAL		Link Order	GPO	Enforced	Link Enabled	
📕 Default Domain Policy		1	Hide Clock from tas	No	Yes	
Deny access to control panel						
Domain Controllers						
> 🖬 Egypt > 🗃 IT						
Sa Create a GPO in this do	main, and	Link it here				
> 🔓 Gr Link an Existing GPO						
> 🕞 W Block Inheritance						
> iii Sta Group Policy Update						
Group Po Group Policy Modeling	Winord					
Group Po New Organizational Uni						
New Organizational On	L					
View			>			
New Window from Her	2					
Delete						
Rename			-			>
Refresh						_
Toggle block inherita Properties						

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

Hide Clock from task bar Security Settings					
Security					
Group or user names:					
SCREATOR OWNER		^			
Authenticated Users					
SYSTEM Strain Admins (LAB\Domain	(Admina)				
Enterprise Admins (LAB\Enter;		~			
<		>			
[[Add	Remove			
Permissions for CREATOR OWNER	Allow	Deny			
Full control		□ <u>^</u>			
Read					
Write					
Create all child objects					
Delete all child objects		<u> </u>			
For special permissions or advanced click Advanced.	d settings,	Advanced			
ОК	Cancel	Apply			

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

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
LAB.LOCAL	Locations
Enter the object names to select (examples):	
Max (Max@LAB.LOCAL)	Check Names
Advanced OK	Cancel

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.

Hide Clock from task bar Security	Settings	×
The clock norm task bar security	Settings	~
Security		
Group or user names:		
Domain Admins (LAB\Domain LAB\Enterprise Admins (LAB\Enterprise)		^
& ENTERPRISE DOMAIN CON		
Max (Max@LAB.LOCAL)		
		~
<		>
	Add	Remove
Permissions for Max	Allow	Deny
Read		
Write		
Create all child objects		
Delete all child objects		
Apply group policy		
For special permissions or advance click Advanced.	d settings,	Advanced
ОК	Cancel	Apply

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

indup Policy Management indup Policy Policy Policy Policy Policy Rese indup Policy Policy Management indup Policy	📓 Group Policy Management		
Forest: LAB.LOCAL		_	
Group Policy Management Contents Demains Default Domain Policy Default Domain Policy Deny access to control panel Description Dime Description Linked GPO Auth MMI Filters in LAB.LOCAL Contents Delegation Name Description Linked GPO Auth Name Description Linked GPO Auth Name Description Linked GPO Auth Description Linked GPO Auth Name Description Name Description Name Description Name Des	📓 File Action View Window Help		_ 8 ×
Forest: LAB.LOCAL Bomains Belegation Contents Delegation Default Domain Policy Deny access to control panel Contents Description Linked GPO Auther and the second second	🗢 🔿 🔁 📰 🗎 🖉 🕼 👘		
Image: Comp Policy Mode Image: Comp Policy Rest Image: Comp Policy Rest View	Group Policy Management	Contents Delegation	Auth
	😨 Group Policy Resu View		
Refresh	Refresh		
Help	Help		
	Create a new WMI filter	<	>

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

New WMI Filter			×
Name: Windows 10			
Description:			
Select Windows 10 m	achines		
Queries:			
Namespace	Query		Add
			Remove
			Edit
,		Save	Cancel

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

WMI Query	×
Namespace:	
root\CIMv2	Browse
Query:	
select *from Win32_OperatingSystem where Version like "1 	10.%"
	~
ОК	Cancel

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

New WMI Filter		×
<u>N</u> ame: Windows 10		
Description:		
Select Windows 1	0 machines	
<u>Q</u> ueries:		
Namespace	Query	<u>A</u> dd
root\CIMv2	select * from Win32_OperatingSystem where	
	Version like "10.%"	<u>R</u> emove
		<u>E</u> dit
	Save	Cancel

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

Group Policy Management	\times
Would you like to change the WMI filter to Windows 10	
Yes No	

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:

Group Policy Management Editor					_		×
File Action View Help	File Action View Help						
🗢 🄿 🙇 📰 🖾 🚱 👔							
 Install Winzip [DC1.LAB.LOCAL] Policy Computer Configuration Policies Software Settings Software installation 							
> 📔 Windows Settings	New	>	Package.				
 Administrative Templa Preferences User Configuration Policies Preferences 	View Paste Refresh Export L Properti Help						
<		*				1	>
Adds a package.							

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

🗐 Open		×
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare > Network > dc1 > SW \lor \bar{c}$	Search SW	Q
Organize 🔻 New folder		
👳 D on HQ 🔷 Name	Date modified	Туре
Desktop 👘 winzip_en_64.msi	12/27/2017 11:13	Windows
Documents		
👆 Downloads		
b Music		
E Pictures		
🔐 Videos		
🏪 Local Disk (C:)		
🖆 DVD Drive (D:) S!		
🛫 home\$ (\\dc1) (;		
i Network		
v <		>
File name \\dc1\sw	Windows Installer package	s (*.r ∨
	Open Car	icel

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

New Hash Rule		×
General		
Click E attribut	les to override the default security level. Irowse to select the file you want to hash. The file's es, such as its size and the date and time it was creater comatically populated.	d.
File information:	Browse	
		^
		~
Security level:	Disallowed \checkmark	
Description:		
		$\hat{}$
	OK Cancel App	ły

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

J Open		×
$\leftarrow \rightarrow \checkmark \uparrow$ \checkmark Network > dc1 > SW \checkmark \checkmark	Search SW	م
Organize 🔻 New folder		•
E D on HQ Name	Date modified	Туре
Desktop Solitaire.exe	7/13/2009 6:39 PM	Applicatio
🖆 Documents 🛛 🔂 winzip_en_64.msi	12/27/2017 11:13	. Windows
🖶 Downloads		
b Music		
E Pictures		
📑 Videos		
🏪 Local Disk (C:)		
🖆 DVD Drive (D:) S!		
🛖 home\$ (\\dc1) (.		
💣 Network		
~ <		>
File name: Solitaire.exe 🗸	All Files (*.*)	~
	Open	Cancel

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

Vew Hasł	n Rule				×
General					
	Click E attribut	rowse to sele	s size and the	ecurity level. want to hash. date and time i	
File info	mation:				Browse
solitaire Executa	.exe able for S	.7600.16385) Solitaire Game Jows® Operat	ing System		~
Security Descript		Disallowed	I		~
					~
			ОК	Cancel	Apply