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	Vizard	Group Policy Inheritance GPO	Delegation	Link Ena	ibled	
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 bad	
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
 Image: Second state of the second st	🔜 File Action View Window Help		_ 8 >
Image: Group Policy Management ✓ Forest: LAB.LOCAL ✓ Domains ✓ Default Domain Policy > Default Domain Controllers > Egypt ✓ Hide Clock from task bar > Sales > Group Policy Objects > Group Policy Objects > Group Policy Objects > Sales > Stater GPOs > Stater GPOs > Stater GPOs Sites Group Policy Ndeling ✓ C Delete Rename Refresh Help	🗢 🤿 🖄 📷 📋 🗶 🗐 🙆 🛛 🖬		· · · · · · · · · · · · · · · · · · ·
	Group Policy Management Group Policy Management Group Policy Abalance Common Controllers Common Controllers Controllers Common Controllers	IT Linked Group Policy Objects Group Policy Inheri Link Order GPO	tance Delegation Enforced Link Enabled n 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 Hide Clock from task bar [DC1.LAB.LOCA Policies Preferences Preferences Software Settings Software Settings Software Settings Mindows Settings Control Panel Desktop Network Shared Folders System System Windows Components All Settings Preferences 	Setting Image: Remove Search Computer link Image: Remove See More Results / Search Every Image: Do not search for files Image: Do not search Internet Image: Do not search Internet Image: Do not search Internet Image: Do not search programs and Control Pa Image: Remove programs on Settings menu Image: Prevent changes to Taskbar and Start Ment Image: Remove Downloads link from Start Ment Image: Remove Homegroup link from Start Ment Image: Remove Recorded TV link from Start Ment Image: Remove Videos link from Start Menu Image: Remove Videos link from Start Menu Image: Remove Clock from the system notification Image: Prevent grouping of taskbar items Image: Do not display any custom toolbars Image: Remove access to the context menu Image: Hide the notification area	/where link inel items enu Settings iu enu enu enu Edit Filter On Filter Options Re Apply Filter	State Not configured Conf	^
	Prevent users from uninstalling appl Remove user folder link from Start N	All Tasks	configured	<u> </u>
	Kemove user name from Start Menu	Help	confidured	>
< >>	\Extended \Standard /			
Edit 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	ification area			_		×
om the system noti	fication area		Previous Setting	Next Setting		
Comment:						^
Supported on:	At least Window	vs Server 2003	operating systems o	or Windows XP Profe	essional	~
		Help:				
		Prevents th displayed. If you enab system not If you disab behavior of occur.	e clock in the system le this setting, the clo fication area. le or do not configur the clock appearing	notification area fro ock will not be displa re this setting, the de in the notification a	om being nyed in the efault rea will	
	om the system notion the system notion the system notion of the system not system notion of the system not system not system notion of	om the system notification area om the system notification area Comment: Supported on: At least Windov	om the system notification area Comment: Supported on: At least Windows Server 2003 Help: Help: If you enabisystem notification of occur.	om the system notification area m the system notification area Comment: Supported on: At least Windows Server 2003 operating systems of Help: Prevents the clock in the system displayed. If you enable this setting, the clo system notification area. If you disable or do not configur behavior of the clock appearing occur. OK	om the system notification area methe system notification area Previous Setting Next Setting Comment: Supported on: At least Windows Server 2003 operating systems or Windows XP Profe Help: Prevents the clock in the system notification area fre displayed. If you enable this setting, the clock will not be displa system notification area. If you disable or do not configure this setting, the de behavior of the clock appearing in the notification a cccur. OK Cancel	om the system notification area Previous Setting Next Setting Comment: Supported on: At least Windows Server 2003 operating systems or Windows XP Professional Help: Prevents the clock in the system notification area from being displayed. If you enable this setting, the clock will not be displayed in the system notification area. If you disable or do not configure this setting, the default behavior of the clock appearing in the notification area will occur. OK Cancel App

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 Color Group Policy Domains Group Policy Objects Group Policy Modeling Group Policy Results Toggle the Link Enabled attribute for this link Group Policy Results	Hide Clock from task bar Scope Details Settings Delega Links Display links in this location: The following sites, domains, and O Location IT Edit Enforced Link Enabled Save Report View >> New Window from Here Delete Rename Refresh Help	ation LAB.LOCAL Us are linked to th oly to the followin ove VMI filter:	his GPO: Enforced No ng groups, use Properties	Link Enable No	d Pati 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
	<		>
< >	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					-	e ×
🗢 🔿 🙍 🗊 📋 🗙 🗐 🍳 📝 🗊						
Group Policy Management	IT					
✓ ▲ Domains	Linke	d Group Policy Objects	Group Policy Inheritance	Delegation		
V 🚔 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						
> 📓 Sa Create a GPO in this do	main, and	Link it here				
> 📴 Gr Link an Existing GPO						
> 📴 W Block Inheritance						
Sti Group Policy Update						
Group Po						
Group Policy Modeling	wizard					
New Organizational Un	t					
View			>			
New Window from Her	e					
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	(desire a)	
Domain Admins (LAB\Domain Section 2.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	Aamins) orise Admins)	~
<	nee / taniney	>
	Add	Remove
OWNER	Allow	Deny
Full control		□ <u>^</u>
Read		
Write		
Create all child objects		
Delete all child objects		
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 har Security	Settings	×
Hide Clock from task bar security	Settings	^
Security		
Group or user names:		
Domain Admins (LAB\Domain Reference Admins (LAB\Enter	Admins) prise Admins)	^
SE ENTERPRISE DOMAIN CON	TROLLERS	
👗 Max (Max@LAB.LOCAL)		
		~
<		>
	Add	Remove
Permissions for Max	Allow	Deny
Read		
Write		
Create all child objects		
Delete all child objects		
Apply group policy		\checkmark
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...

Crown Balies Management				
📓 File Action View Window Help				- 8 ×
🗢 🔿 🚈 🔲 🗎 🞑 👔 🖚				
 Group Policy Management Group Policy Management Forest: LAB.LOCAL Domains LAB.LOCAL Default Domain Policy Deny access to control panel Domain Controllers Egypt Egypt Filde Clock from task bar Sales Group Policy Objects WMI Filters Starter GP(New 	WMI Filters Contents Del Name	in LAB.LOCAL egation Description	Linked GPO	Autł
Group Policy Moc				
Group Policy Rest View	>			
New Window fro	om Here			
Refresh				
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							
🗢 🄿 🙇 📰 🖾 🚱 👔							
 Install Winzip [DC1.LAB.LOCAL] Policies Policies Software Settings Software installation 	olicy	Name	There are no	Version o items to	Deployment st show in this view.	Source	
> 📔 Windows Settings	New	>	Package.				
 Administrative Templa Preferences User Configuration Policies Preferences 	View Paste Refresh Export L Properti Help	> ist es					
<		*					>
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		×
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare \Rightarrow$ Network \Rightarrow dc1 \Rightarrow SW $\checkmark \textcircled{O}$	Search SW	Q
Organize 🔻 New folder	:== ▼ □	1
 D on HQ Desktop Documents Downloads Music Pictures Videos Local Disk (C:) DVD Drive (D:) S: home\$ (\\dc1) () 	Date modified 12/27/2017 11:13	Type Windows
		>
File name \\dc1\sw	Windows Installer packages Open Canc	(*.r ∨ :el

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		
Use ru Click E attribu are au	les to override the default security level. Browse to select the file you want to hash. The file's tes, such as its size and the date and time it was crea tomatically populated.	ited,
File information:	Brows	e
		^
		~
Security level:	Disallowed	\sim
Description:		
		\sim
	OK Cancel A	nolv

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

🗐 Open		×
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare$ Network > dc1 > SW \checkmark \eth	Search SW	Q
Organize 🔻 New folder		
D on HQ Name	Date modified	Туре
Desktop Solitaire.exe	7/13/2009 6:39 PM	1 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.

New Hasł	n Rule				×
General					
	Use rules to override the default security level. Click Browse to select the file you want to hash. The file's attributes, such as its size and the date and time it was created, are automatically populated.				
File infor	mation:				Browse
solitaire solitaire Executa Microso	.exe (6.1 .exe able for S ft® Wind	.7600.16385) Solitaire Game Jows® Operat	ing System		< ×
Security Descript	level: ion:	Disallowed	i		~
					<
			ОК	Cancel	Apply