

Process Owner: IT Operations	FORM	F-CMG-3.1
	Add OU for DataScan and Link Default GPOs	

Request Information				
Requestor	Rovie G. Salvatierra			
Implementing Team	Systems and Server Operations			
Ticket Number/s	201915330			
Change Classification		Major	<input checked="" type="checkbox"/>	Minor
After the fact		Yes	<input checked="" type="checkbox"/>	No
Emergency		Yes	<input checked="" type="checkbox"/>	No
Proposed Change Date	May 08, 2019			
Proposed Change Start/End Time	16:00 – 17:00			
Proposed Change Verification Time	17:15			

Objective of the change
<ul style="list-style-type: none"> <li>To add OUs in the COMPUTERS and USERS for DataScan campaign in GL2 named P_DSCAN</li> <li>To transfer the DataScan user profiles to the DataScan USERS OU</li> <li>To link the default GPOs to the COMPUTERS and USERS OU for P_DSCAN</li> </ul>

Technical/Operational Impact of the change		
Negative: Increase in CPU and Memory utilization.	Beneficial: Organizational Unit is set for easier implementation of policies when requested.	Neutral: P_DSCAN will have their own OU.

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
GL2	JKA-VWIN-DC01	172.22.1.1	Domain Controller in GL2 site

Affected Departments and Corresponding Contact Persons		
Department	Contact Name	Contact Info
Server Operations	Rovie Salvatierra	0917-627-4325

Test Environment implementation and Verification Summary
This process has been tested and implemented previously with reference to ticket number 201808679.

Test Environment Results Summary
Please refer to the testing result in ticket number 201808679.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Add OU for DataScan and Link Default GPOs</i>	

### Configuration Change Template

Baseline File	3.1.137 DOMAIN FOREST
Baseline Version	9

#### Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing OU yet for the Datascan campaign.	Add OU for DataScan and link the default GPO.	Additional OU will be added on the list. The GPO list of campaigns will be updated to reflect P_DSCAN.	OU tab, GPO tab

### Physical Implementation Procedures / Advisory

No physical implementation will be facilitated.

### Backup Procedures

No back-up procedure for Active Directory Users and Computers.

### Technical Configuration Procedures

1. Log on to GL2-VWIN-DC01 via RDP using your own domain admin credentials.
2. Press Windows + R simultaneously the enter **dsa.msc** to launch Active Directory Users and Computers.
3. Expand the openaccess.bpo domain, then expand the MKT\_GL2 OU.
  - Right click on the **COMPUTERS** OU > New > Organizational Unit > name is P\_DSCAN > Save
  - Right click on the **USERS** OU > New > Organizational Unit > name is P\_DSCAN > Save
4. Move the following users to the **P\_DSCAN USERS** OU:  
 Jouhn lyvan Go  
 Melvin Ong  
 Madaline Tan  
 James Tan  
 Wanda Tan  
 Jose Castaneda
5. Close the Active Directory Users and Computers Console.
6. Next, press Windows + R simultaneously the enter **gpmc.msc** to launch the Group Policy Management console.

 <b>OPEN ACCESS</b> <small>WE SPEAK YOUR LANGUAGE</small>	Proprietary and Confidential	Effectivity: April 1, 2019	Page 2
			Template Version : <b>02</b>

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Add OU for DataScan and Link Default GPOs</i>	

7. Expand the openaccess.bpo domain, then Group Policy Object. Copy the GPO for WSUS Patch for AVA first before linking the rest of the default GPOs.
8. Right click on COMP\_PATCH\_AVA > Copy. Then, right click on Group Policy Object > Paste.
9. Rename the copied GPO to COMP\_PATCH\_DSCAN. Right click on it then Edit.
  - Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update
  - Scroll down and select the **Enable client-side targeting**
  - Edit the **Target group name for this computer** to P\_DSCAN
10. Next, link the following GPOs:
  - > go to MKT\_GL2\USERS, right click on P\_DSCAN and select Link and Existing GPO
    - USER\_GPO\_GLOBAL\_WALLPAPER
    - USER\_GPO\_XCMD
    - USER\_GPO\_XCTRLPANEL
    - USER\_GPO\_XMDDR
    - USER\_GPO\_XTASKMGR
  - > go to MKT\_GL2\COMPUTERS, right click on P\_DSCAN and select Link and Existing GPO
    - COMP\_PATCH\_DSCAN
11. Close the console and launch the PowerShell as administrator. Send the command gpupdate /force. Exit the server.
12. Finally, in order for the computers assigned for DataScan to get updates as scheduled from the WSUS server, log on to GL2-VWIN-WSUS01 using your domain admin account.
13. Launch the Server Manager > Tools > Windows Server Update Services.
14. Expand the GL2-VWIN-WSUS01 > Computers, right click on All Computers then select Add Computer Group. See screenshot example below:

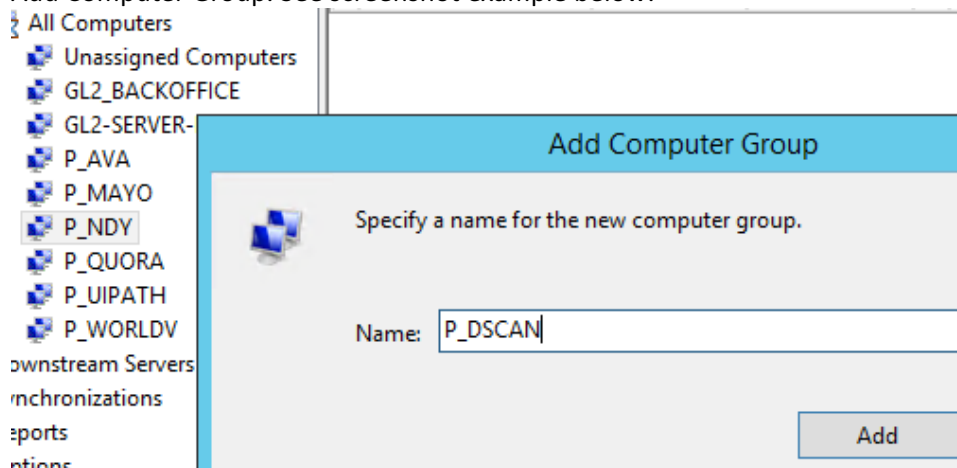


Figure 1

15. Exit the server.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Add OU for DataScan and Link Default GPOs</i>	

#### Verification Procedures

1. Advise any agent from DataScan to try logging in using their domain account. The wallpaper should show the updated OAM Wallpaper.
2. Users should not be able to access the following without administrative privilege:
  - task manager
  - control panel
  - command prompt
3. Check all USB Ports by inserting a flash drive. Users should not be able to use any removable storage.
4. Access the command prompt as an administrator and enter the command **wuauctl /detectnow /reportnow** to check if the computer can detect updates and report to WSUS server.

#### Back-out Procedures

1. Log on to GL2-VWIN-DC01 using your domain admin credentials.
2. Press Windows + R simultaneously the enter **dsa.msc** to launch Active Directory Users and Computers.
3. Expand the openaccess.bpo domain, then expand the MKT\_GL2 OU\COMPUTERS.
  - Right click on P\_DSCAN > Delete
4. Expand the openaccess.bpo domain, then expand the MKT\_GL2 OU\USERS.
  - Right click on P\_DSCAN > Delete