

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Disable Local Administrator in Domain Computers</i>	

Request Information				
Requestor	Rovie Salvatierra			
Implementing Team	Systems and Server Operation			
Ticket Number/s	201914923			
Change Classification	X	Major		Minor
After the fact		Yes		No
Emergency		Yes		No
Proposed Change Date	April 26, 2019			
Proposed Change Start/End Time	18:00 – 19:00			
Proposed Change Verification Time	19:30			

Objective of the change
Create a GPO to disable the local administrator account of all PCs within the PCI-DSS scope.

Technical/Operational Impact of the change		
Negative: PCs are not required to reboot after the implementation of the GPO.	Beneficial: Only domain admins are allowed to administer any computer system components, disallowing any bypass on UAC policies.	Neutral: One vulnerability factor of domain computers is mitigated

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


Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
Desktop Operations	Jim Villanueva	0917-867-6413
Network Operations	Maurice Mendoza	0917-632-8103
Server Operations	Rovie Salvatierra	0917-627-4325

Test Environment implementation and Verification Summary
<ol style="list-style-type: none"> <li>1. There's already an existing GPO applied to member servers in the domain, and it's working and the local administrator is disabled.</li> <li>2. For testing purposes, created a test GPO in Hercules.</li> <li>3. The test GPO is set under Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options.</li> <li>4. Define the policy "Accounts: Administrator account status" by setting it to Disabled.</li> </ol>

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Disable Local Administrator in Domain Computers</i>	

### Accounts: Administrator account status Properties

Security Policy Setting
Explain



#### Accounts: Administrator account status

☒ Define this policy setting:

☐ Enabled

☒ Disabled

*Figure 1*

- The test PC FSSO-TEST was joined to the openaccessbpo.com domain, and the test user account used was mroxas. Tried accessing the command line as administrator.
- Tried entering the default OAMIT administrator, and it's not accepting the credentials entered.
- Tried using a domain admin account, rsalvatierra, and login was successful.

#### Test Environment Results Summary

All PCs within the PCI-DSS scope will have the local administrator account disabled. The OAMIT account won't succeed in logging in as a local account as well.  
Only domain admin and IT elevated users will be able to administer computer system components.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Disable Local Administrator in Domain Computers</i>	

#### Configuration Change Template

Baseline File	3.1.137 Domain Forest
Baseline Version	9

#### Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
The existing <b>COMP_GPO_LOCALSEC</b> group policy is defined to enable Administrator account.	Edit the GPO an.	The GPO information will be updated to state that the local administrator account won't be usable.	Group Policy tab

#### Physical Implementation Procedures / Advisory

No physical implementation required.

We will notify the IT team by the end of the day that they will have to use their elevated accounts when it's required.

#### Backup Procedures

1. Log-on to GL2-VWIN-DC01 using your administrator account.
2. Launch the Server Manager > Tools > Group Policy Management.
3. Expand the Forest > Domains > openaccess.bpo > Group Policy Objects.
4. Right click and select Back Up All, then save it temporarily on the desktop. Make sure to name it accordingly (e.g GPO\_mmddyyy).
5. Access Pelops at 172.17.0.1 and copy the GPO back-up to Backup/AD\_Server/GPO.

#### Technical Configuration Procedures

1. Log on to GL2-VWIN-DC01 using your administrator credentials.
2. Access the Server Manager > Tools > Group Policy Management.
3. Expand the Forest > Domains > openaccess.bpo > Group Policy Objects.
4. Locate the group policy COMP\_GPO\_LOCALSEC, then right-click on it and choose Edit.
5. Once the console is open, go to Policies > Windows Settings > Security Settings > Local Policies.
6. Select Security Options. You'll see all the security policies you can apply.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Disable Local Administrator in Domain Computers</i>	

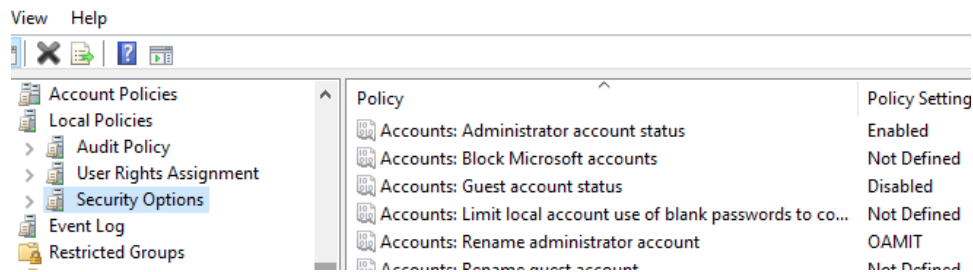


Figure 2

7. Double-click on **Accounts: Administrative account status**.
8. On the Security Policy Settings, select **Disable**, then click **OK**.

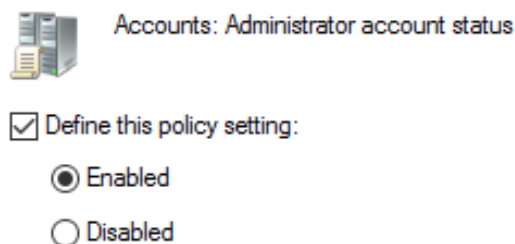


Figure 3

9. Once done, click on the refresh button.

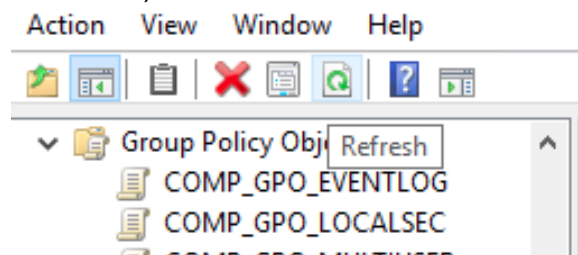


Figure 4

10. Still on the server, launch PowerShell as an administrator.
11. Send the command **gpupdate /force**.

#### Verification Procedures

1. Try logging in using the local administrator account. It should not accept any of the local administrator profiles, even after several tries.
2. Check any available agents that are currently logged in, but available for quick testing.
3. From the agent's profile, launch task manager and/or command prompt as an administrator. This will prompt for the administrator credentials.
4. When the local administrator account is entered, you should not be able to proceed.
5. You should only be able to successfully use the restricted application using the domain admin or IT privileged account.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Disable Local Administrator in Domain Computers</i>	

#### Back-out Procedures

1. From the Group Policy Management console, edit the COMP\_GPO\_LOCALSEC.
2. Revert back the Security Policy Settings of the **Accounts: Administrative account status**, and set it to Enabled.
3. Save the settings and launch PowerShell.
4. Send the command **gpupdate /force**.