

Lab Report

Your Performance

Your Score: 1 of 3 (33%)







Elapsed Time: 35 minutes 20 seconds

Pass Status: Not Passed





Required Score: 100%

Task Summary

✖ Edit the Default Domain Policy security options [Hide Details](#)

-  Disable the local guest account
-  Rename the local administrator account skycaptain
-  Do not display the last logon username
-  Do not allow anonymous SID/name translation
-  Do not allow anonymous SAM account enumeration
-  Do not allow anonymous SAM account and share enumeration

✔ Edit the SupportGPO security options [Hide Details](#)

-  Do not cache previous logons
-  Require domain controller authentication to unlock the computer
-  Force logoff when logon hours expire
-  Do not allow system shutdown without a logon

✖ Disable the user settings in SupportGPO

Explanation

In this lab, you configure the following policies in the corresponding GPO:

Group Policy Object	Policy	Setting
Default Domain Policy	Accounts: Guest account status	Disabled
	Accounts: Rename administrator account	skycaptain
	Interactive logon: Do not display last user name	Enabled
	Network access: Allow anonymous SID/Name translation	Disabled
	Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
	Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
SupportGPO	Interactive logon: Number of previous logons to cache	0
	Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled
		Enabled

	Network security: Force logoff when logon hours expire	
	Shutdown: Allow system to be shut down without having to log on	Disabled
	Modify User configuration settings in the GPO settings	Disabled

You also need to **disable** the user configuration settings in the GPO status of the SupportGPO because all GPO settings for SupportGPO are in Computer Configuration.

Complete this lab as follows:

1. Edit security options as follows:

- a. From Hyper-V Manager, select **CORPSERVER**.
- b. Right-click **CorpDC** and select **Connect**.
- c. From Server Manager, select **Tools > Group Policy Management**.
- d. Expand **Forest:CorpNet.com > Domains > CorpNet.com**.
- e. Right-click **Default Domain Policy** and select **Edit**.
- f. Under Computer Configuration, expand **Policies > Windows Settings > Security Settings > Local Policies**.
- g. Select **Security Options**.
- h. Right-click the *policy* you want to edit and select **Properties**.
- i. Select **Define this policy setting**.
- j. Select **Enabled** or **Disabled**, or configure additional values for the policy.
- k. Click **OK**.
- l. Repeat steps 1d-1k for additional policies.
- m. Close Group Policy Editor.

2. Configure SupportGPO as follows:

- a. Expand the **Support OU**.
- b. Right-click **SupportGPO** and select **Edit**.
- c. Under Computer Configuration, expand **Policies > Windows Settings > Security Settings > Local Policies**.
- d. Select **Security Options**.
- e. Right-click the *policy* you want to edit and select **Properties**.
- f. Select **Define this policy setting**.
- g. Select **Enabled** or **Disabled**, or configure additional values for the policy.
- h. Click **OK**.
- i. Repeat steps 2e-2h for additional policies.
- j. Close Group Policy Editor.

3. Edit the GPO status:

- a. In the Group Policy Management console, expand **Group Policy Objects**.
- b. Right-click **SupportGPO** and select **GPO Status > User Configuration Settings Disabled**.