GROUP POLICY OBJECTS

By Brennen Tse:

**Purpose:**

Create Untitled School District’s Active Directory, separate students and teachers, and apply security policies uniformly to computers and users.

**Background:**

A Group Policy Object is a collection of virtual policy settings that is applied to a certain group of things like users or computers or organizations. GPOs are another tool to regulate settings for the Active Directory. These GPOs are all controlled from the Group Policy Management Console, where you can create different policies affecting security, software, maintenance, folders, settings and more.

The three types of GPOs are local, non-local and starter.

-**Local Group Policy Objects**: Local GPOs are policy settings that only apply to a local computer and the users who log in. These are policies usually applied on a case-by-case basis for special situations and access.

-**Non-local Group Policy Objects**: These are GPOs who apply to more than one Windows computer or user. This category applies to the majority of policies implemented on Active Directory’s organizational units or domains, as these objects can contain hundreds of computers and users.

-**Starter Group Policy Objects**: These GPOs are templates that can be used for quick deployment of policies and serve as a baseline for further expansion.

The most helpful aspect of Group Policy Objects in regard to cybersecurity is their ability to secure a network or organization through certain policies that can be implemented or rolled-back quickly. GPOs can uniformly implement security measures like disabling access to sensitive systems like Control Panel or Command Prompt (I go more into depth on these in the [Security](#_Security_Policies:) Section).

The main benefits of GPOs are its efficiency, ease of administration, enforcement of password policy like length or expiry time and centralization of folders.

The main drawbacks of GPOs include their sequential process which can increase login times, limited flexibility, no version or auditing control and difficult maintenance if documentation is limited.

**Table of Contents:**

1. [Creating Active Directory Structure and Users](#_Creating_the_School)
2. [Creating Group Policy Objects (Computer)](#_Group_Policy_Objects)
3. [Group Policy Objects (User Security Policy)](#_Group_Policy_Objects_1)
4. [List of Security Policies with Description](#_Security_Policies:)
5. [Confirmation of Correct Policy Implementation](#_Confirmation_of_Proper)
6. [Problems](#_Problems:)
7. [Conclusion](#_Conclusion:)

# Creating the School Organization Structure in Active Directory:

|  |  |
| --- | --- |
| In Active Directories, I created an example School District Organizational Unit. |  |
|  |  |
| Inside that OU, I created two further OU’s |  |
| These two organizational units are computers for the computer policy and members for teachers and students. I created the members OU so that those two child OU’s can inherit the group policies of the overall members. |  |
| Here you can see the two nested child OU’s of students and teachers. |  |
| Drag the Client PC that we added in the previous step into the new computers OU For the untitled School district. |  |
| I created a new user to use for this example. |  |
| Name can be whatever, I’m just using the system of last name first initial for the username system. |  |
| Give the user a temporary password, and to maintain security policy always check that user MUST change password at next logon for data privacy. |  |
| Check the details here to make sure they’re correct. |  |
| Drag George Burdell to the students section so that it can be part of the Untitled School District OU. |  |
| Here you can see some of the example students. |  |

# Group Policy Objects (Computer):

|  |  |
| --- | --- |
| Head back to server manager and click Group Policy Management |  |
| When you open Group Policy Management, navigate down forest, domains to windows.local and find the Untitled School district OU. |  |
|  |  |
| Create a GPO for the computers first |  |
| To edit the Group Policy, right click and press edit. |  |
| For an example computer group policy, I’m editing the power options by adding a new one that increases the battery threshold for low battery warning. // Create a power plan that changes the default % low battery level alert to 20% instead of 10% to give students more time to charge. |  |
| Right click to select new and select Power Plan. |  |
| I changed the battery % threshold from 10% for low battery level to 20% instead. |  |
| I then signed in on the Windows 10 Client with the new user account I created earlier to see if the changes have taken effect. |  |
| As per our earlier policy, the user has to change their password before signing in and we can see that here. |  |
| Create a new password. |  |
| Open the Run pop-up and run the command “gpupdate”, this will update the client’s policy to the latest Group Policy. |  |
| You can see that it’s been confirmed. |  |
| By going into the control panel to hardware and sound, we can confirm that there has been a new plan added to the Power options. If this Untitled School Battery Warning is selected, when the computer reaches 20%, it’ll send an alert. |  |



# Group Policy Objects (User Security Policies)

|  |  |
| --- | --- |
| Now that we’ve confirmed that we can edit the GPO for the Computer policies, I want to create a GPO for the member’s security. |  |
| I named the GPO Security. |  |
| Like as to edit all GPO’s, right click and select edit to be brought to the Management Editor. |  |
| Here in the Management Editor we can now implement the security policies. |  |

# Security Policies:

List of Policies:

1. [Restrict Access to Control Panel](#_Moderate_Access_to)
2. [Prevent Windows Lan Manager Hash Storage](#_Prevent_Windows_from)
3. [Command Prompt Access Control](#_Restrict_Access_to)
4. [Disable Forced System Restarts](#_Disable_forced_system)
5. [Disallow Insertable Devices (CD’s, USBs)](#_Disallow_Removable_Media)
6. [Restrict Software Installation](#_Restrict_Software_Installations:)
7. [Disable the Guest Account](#_Disable_Guest_Account:)

# Moderate Access to the Control Panel

Description: Moderating access to the control panel is a vital security policy because the control panel is a large security vulnerability as it can control all aspects of your computer. Only authorized IT staff should be able to access and change settings.

|  |  |
| --- | --- |
| To access this setting, go to User Configuration > Policies > Administrative Temples > Control Panel and double click. |  |
| Click enabled and apply the setting to prohibit access. |  |

# Prevent Windows from storing Lan Manager Hash

Description: Hashes are where Windows stores user account passwords. There are two types of hashes, a LAN Manager (LM) has and a Windows NT hash for passwords, storing them in the Security Accounts Manager database. LM hashes are weak and exploitable so they shouldn’t be stored.

|  |  |
| --- | --- |
| To access this policy, go to Computer Configuration > Policies > Windows Settings > Local Policies > Security Options > Network Security Do not store LAN Manager hash |  |
| Enable this policy and click apply. |  |

# Restrict Access to the Command Prompt

The Command Prompt can run commands that give high-level access to users and may be used to evade and bypass other system restrictions. Therefore, it is critical that unauthorized users are prevented from accessing this vulnerability by disabling it. If an authorized user tries to input commands, they will be greeted with a message stating that there are restrictions on any actions.

|  |  |
| --- | --- |
| To access this command, go to User Configuration>Policies>Administrative Templates>System |  |
| Enable the “Prevent access to the command prompt” policy and click apply. |  |

# Disable Forced System Restarts:

Forced restarts occur for many reasons like security updates or software updates. However, users may not notice these warnings and be automatically restarted, losing important and valuable work that wasn’t saved. To prevent this, disable forced restart. This is more a QOL improvement then security.

|  |  |
| --- | --- |
| To access this policy, go to Computer Configuration>Policies>Administrative Templates>Windows Components>Windows Update>No auto-restart with logged on users |  |
|  |  |
| Enable this policy and click apply. |  |

# Disallow Removable Media (Drives, DVD, CD’s, and USB drives)

It is good practice for any organization with sensitive data to implement a security policy that disallows removable media from being inserted into any devices. These media drives can contain all sorts of malicious code and if plugged into the right terminal may infect the entire network.

|  |  |
| --- | --- |
| To enable this policy, go to User Configuration>Policies>Administrative Templates>System>Removable Storage Access> All Removeable Storage Classes Deny all access. Enable the policy then click apply. |  |

# Restrict Software Installations:

If software installations are not restricted, the user may install unwanted apps or compromised software that can infect your system. Although some can slip through the cracks, having a security policy that automatically prevents these installations is a best practice. If new software needs to be downloaded, that request can be forwarded through the IT department first.

|  |  |
| --- | --- |
| To access this policy, go to Computer Configuration>Policies>Administrative Templates>Windows Components>Windows Installer>Prohibit User Installs. |  |
|  |  |
| Enable the policy of Prohibit User Installs and click apply. |  |

# Disable Guest Account:

Having guest accounts enabled can easily compromise your data security as these accounts can access computers without passwords. Although these are disabled by default, it’s good to check anyways.

|  |  |
| --- | --- |
| To check this policy, go to Computer Configuration>Policies>Windows Settings>Local Policies>Security Options>Accounts:Guest account status Properties and confirm that it’s disabled. |  |

# Confirmation of Proper Implementation:

The two easiest ways to check that the group policy objects have been implemented correctly are trying to gain access to the disabled systems of the control panel and the command prompt. If we cannot access them, we know that it was successful.

|  |  |
| --- | --- |
| Login with a user account that has the GPO applied to it. Since George Burdell is a student, his account automatically inherits the GPO from the members OU that students is nested within. |  |
| When trying to access Command Prompt, we can confirm that it has been disabled. |  |
| Similarly when trying to open Control Panel, we receive an error message saying that the operation has been canceled due to restrictions. |  |
| And that’s it! We’re done for now. This is only 7 of thousands of policies that can be implemented depending on the need and use case. |  |

# Problems:

Unlike with the configuration of Active Directory, enabling and assigning group policy objects went pretty smoothly. The only problems I faced was some issues with signing on from some of the student’s accounts. The main reason for this problem was that the passwords were either mistyped or after the first login the password didn’t request a change, mainly because the prompt to do so was left blank on accident.

# Conclusion:

Group Policy Objects are a critical part of any organization’s domain control and Active Directory service, no matter how big or small it is. Because of the ease of use, efficiency and uniformity of the policies implemented by GPOs, they are a fast and secure way to configure the security policies on users, computers, organizations, and more. They help with organization, management, and quality of life, mainly for IT administrators. Its wide array of policy options means that basically every issue or vulnerability has a policy to rectify it.