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.

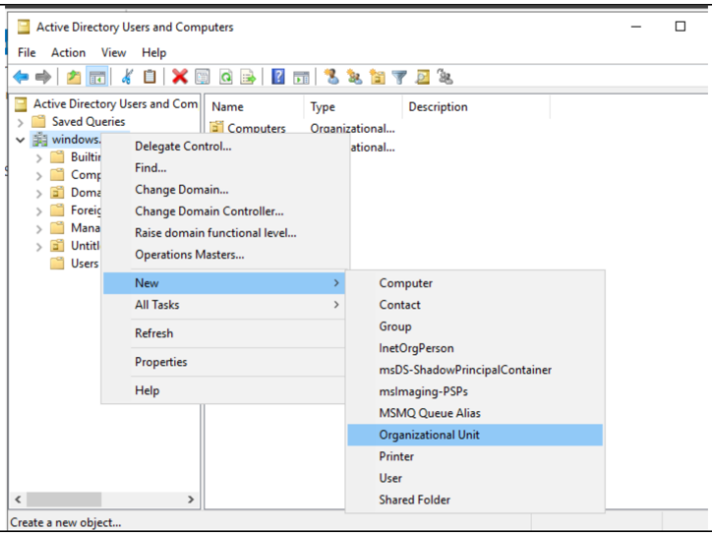
The most helpful aspect of Group Policy Objects in regard to cybersecurity is their ability to secure a network or organization through certain policies that can be implemented or rolled-back quickly. GPOs can uniformly implement security measures like disabling access to sensitive systems like Control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

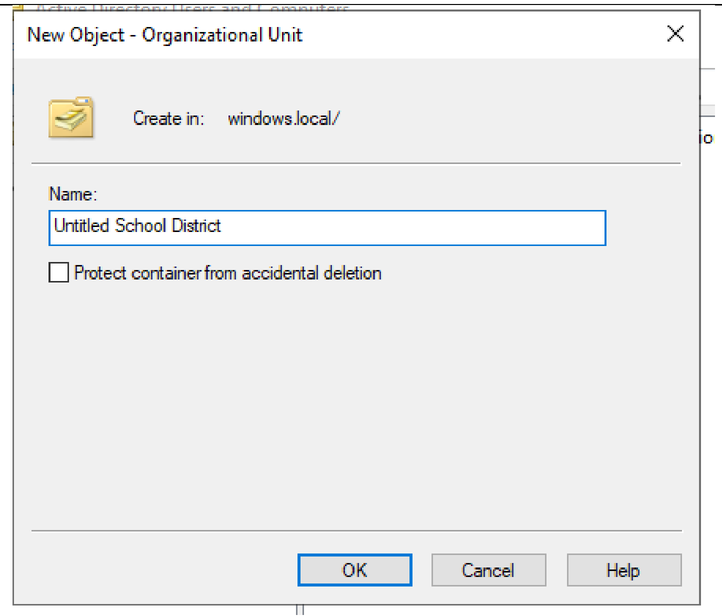
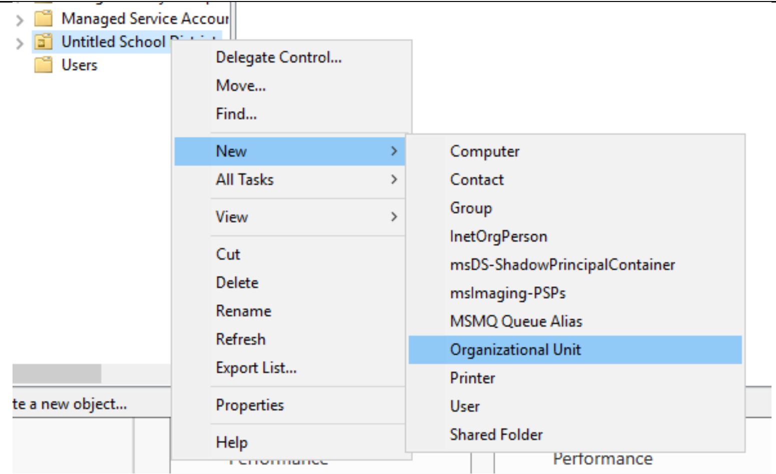
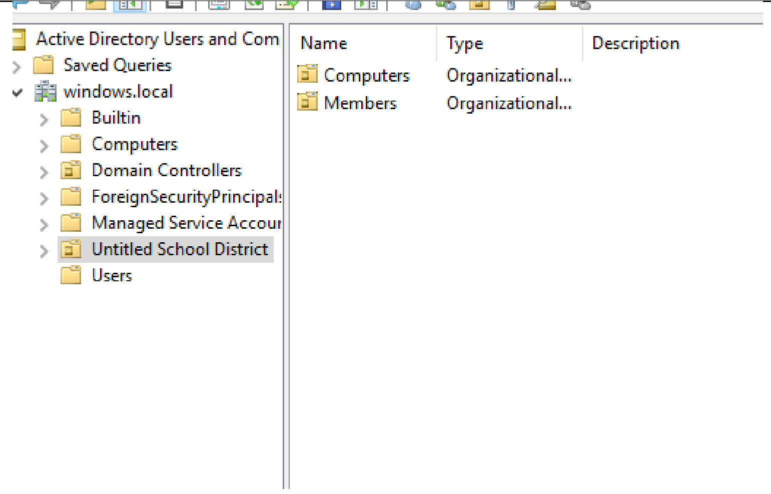
The main benefits of GPOs are its efficiency, ease of administration, enforcement of password policy like length or expiry time and centralization of folders.

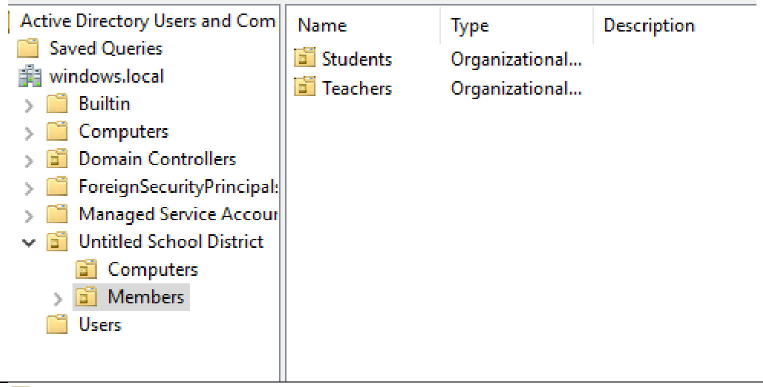
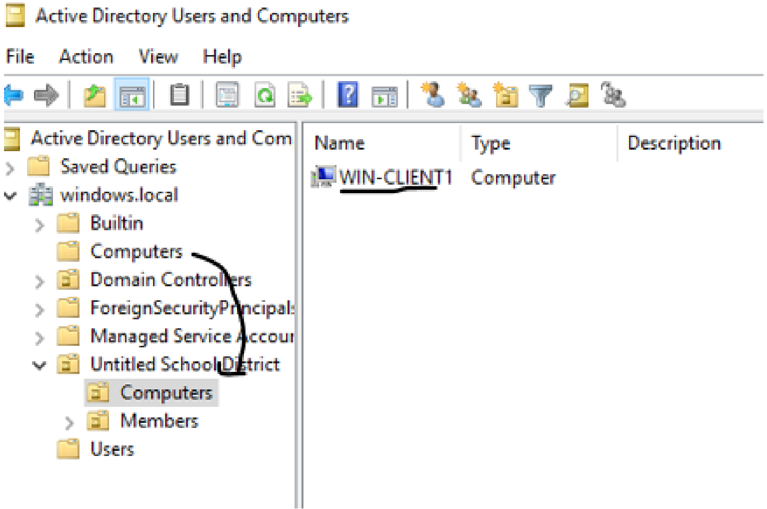
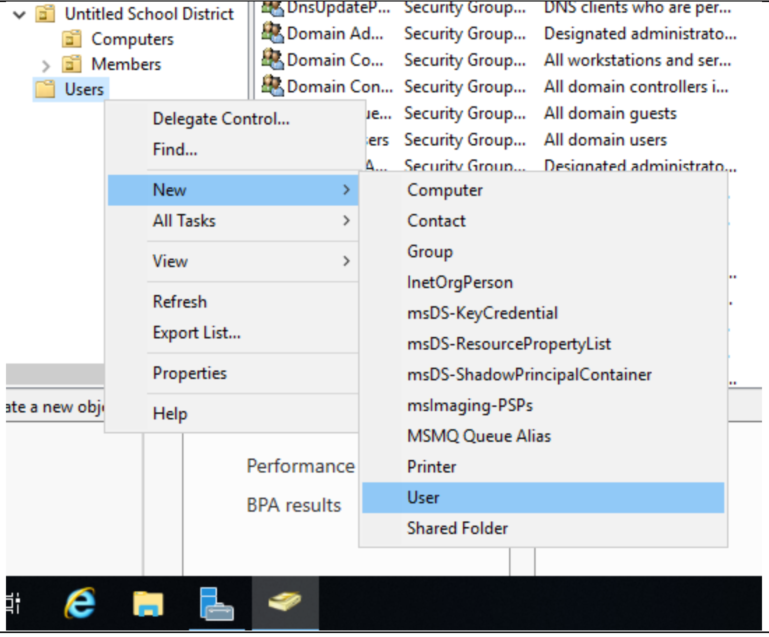
The main drawbacks of GPOs include their sequential process which can increase login times, limited flexibility, no version or auditing control and difficult maintenance if documentation is limited.

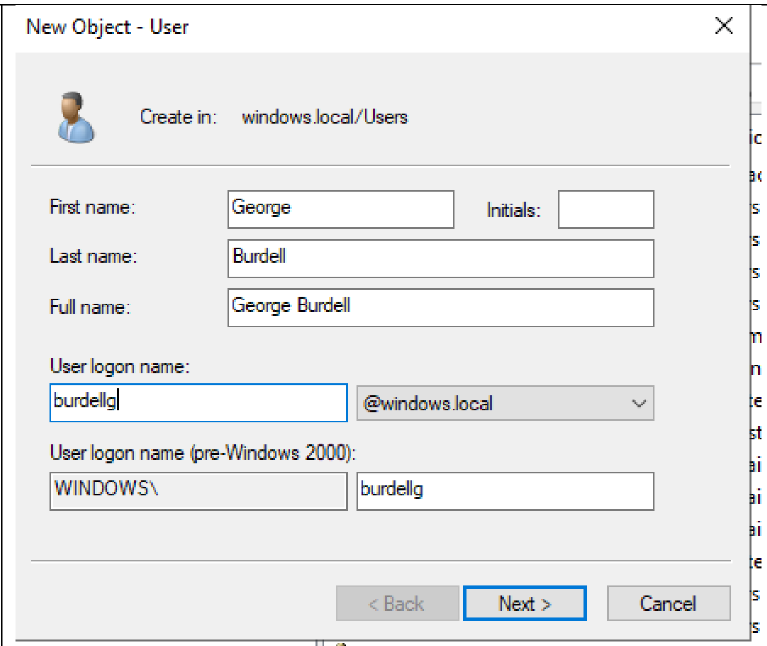
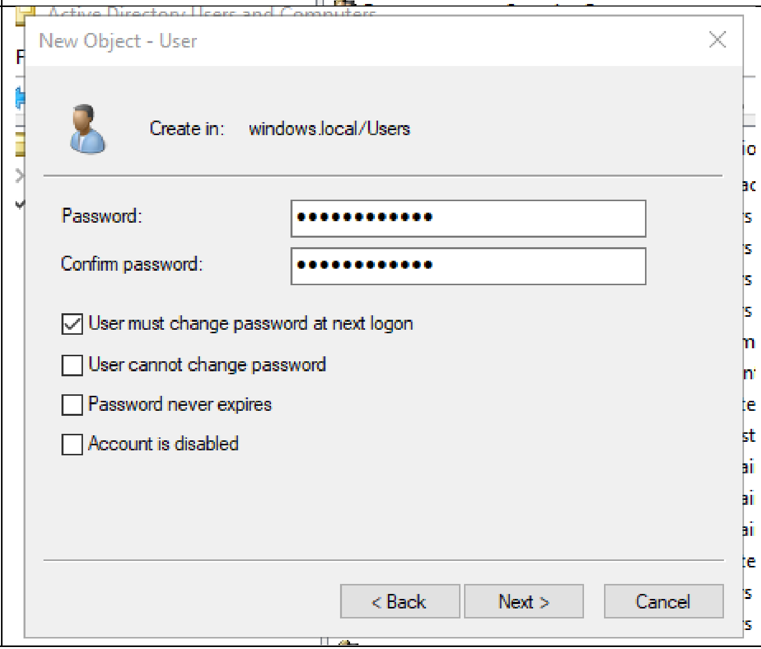
Table of Contents:

Creating the School Organization Structure in Active Directory:

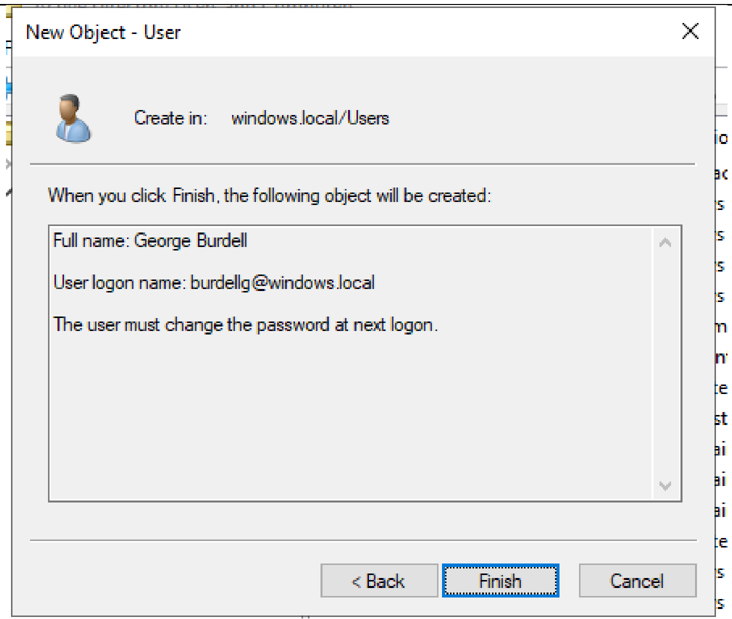
In Active Directories, I created an example School District Organizational Unit.	

	 New Object - Organizational Unit Create in: windows.local/ Name: Untitled School District ☐ Protect container from accidental deletion
Inside that OU, I created two further OU’s	 Managed Service Accour Untitled School Users Delegate Control... Move... Find... New All Tasks View Cut Delete Rename Refresh Export List... Properties Help Computer Contact Group InetOrgPerson msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias Organizational Unit Printer User Shared Folder te a new object... Performance
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.	 Active Directory Users and Com Saved Queries windows.local Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Untitled School District Users Name | Type | Description Computers | Organizational... Members | Organizational...

Here you can see the two nested child OU’s of students and teachers.	 Active Directory Users and Com Saved Queries windows.local Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Untitled School District Computers Members Users Name Type Description Students Organizational... Teachers Organizational...
Drag the Client PC that we added in the previous step into the new computers OU For the untitled School district.	 Active Directory Users and Computers File Action View Help Active Directory Users and Com Saved Queries windows.local Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Untitled School District Computers Members Users Name Type Description WIN-CLIENT1 Computer
I created a new user to use for this example.	 Untitled School District Computers Members Users DnsUpdateP... Security Group... DNS clients who are per... Domain Ad... Security Group... Designated administrato... Domain Co... Security Group... All workstations and ser... Domain Con... Security Group... All domain controllers i... Security Group... All domain guests Security Group... All domain users Security Group... Designated administrato... Delegate Control... Find... New All Tasks View Refresh Export List... Properties Help Computer Contact Group InetOrgPerson msDS-KeyCredential msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias Printer User Shared Folder ate a new obj Performance BPA results

Name can be whatever, I'm just using the system of last name first initial for the username system.	 New Object - User Create in: windows.local/Users First name: George Initials: Last name: Burdell Full name: George Burdell User logon name: burdellg @windows.local User logon name (pre-Windows 2000): WINDOWS\ burdellg < Back Next > Cancel
Give the user a temporary password, and to maintain security policy always check that user MUST change password at next logon for data privacy.	 New Object - User Create in: windows.local/Users Password: ••••••••••••• Confirm password: ••••••••••••• ☑ User must change password at next logon ☐ User cannot change password ☐ Password never expires ☐ Account is disabled < Back Next > Cancel

Check the details here to make sure they’re correct.



Create in: windows.local/Users

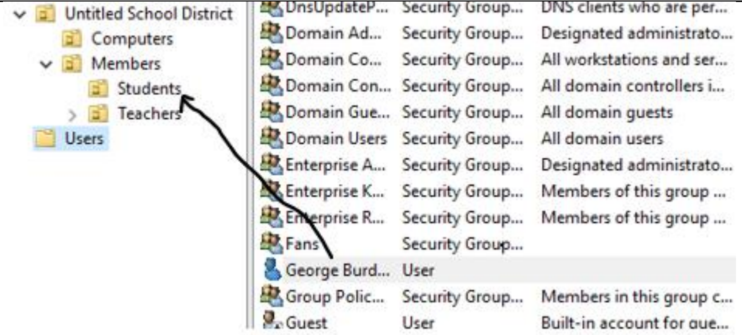
When you click Finish, the following object will be created:

Full name: George Burdell

User logon name: burdellg@windows.local

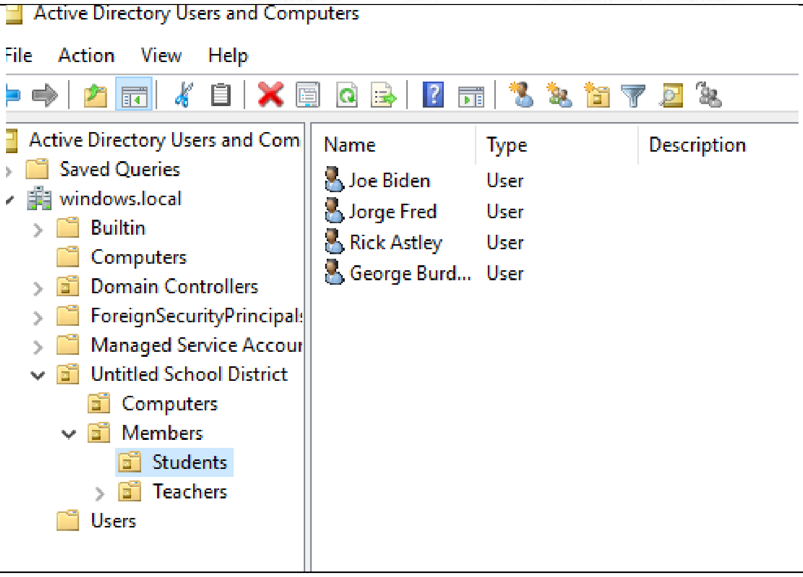
The user must change the password at next logon.

Drag George Burdell to the students section so that it can be part of the Untitled School District OU.



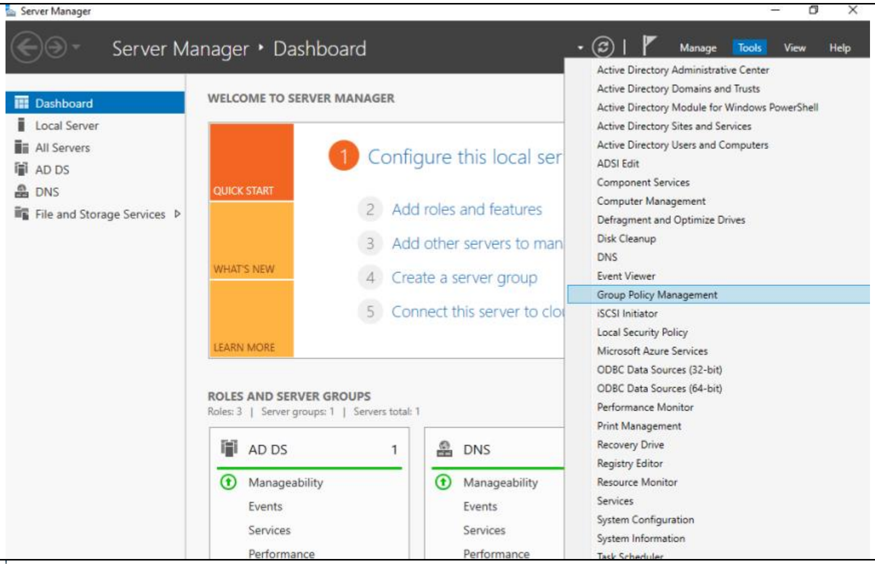
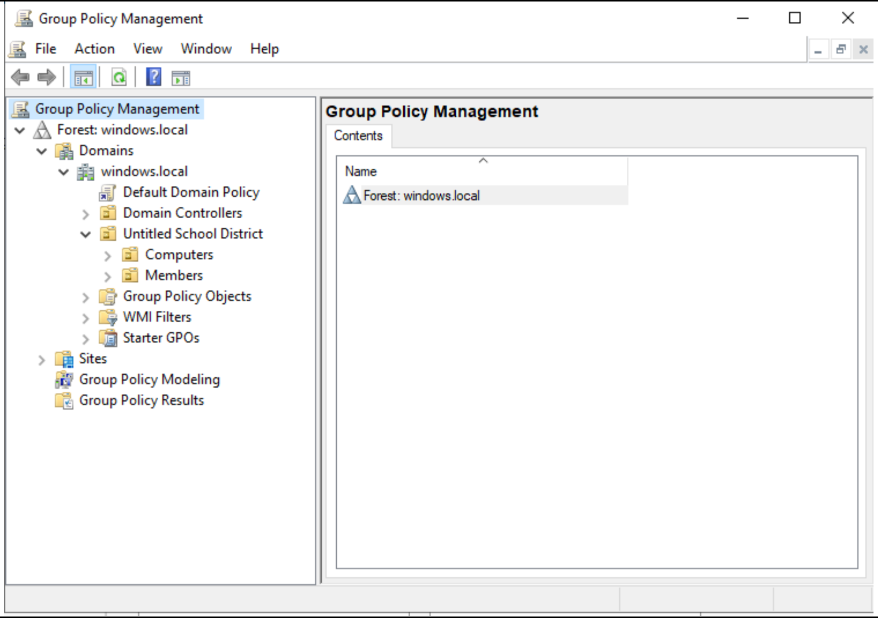
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Fans	Security Group...	
George Burd...	User	
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...

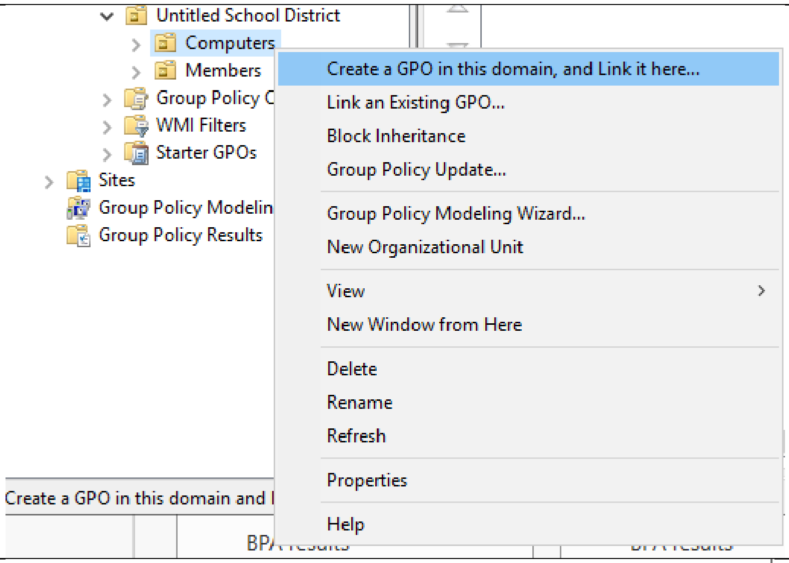
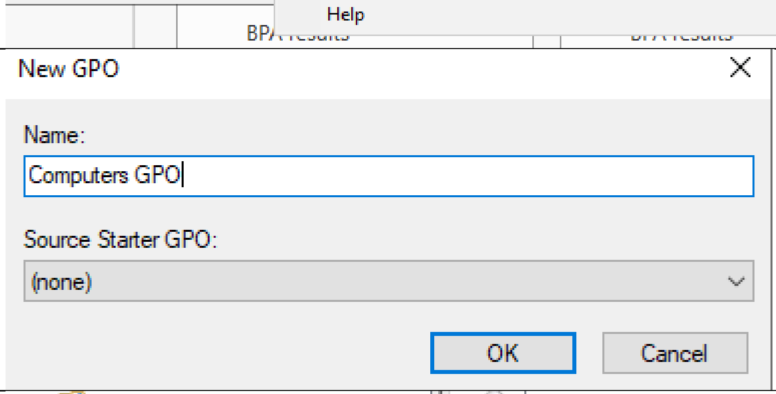
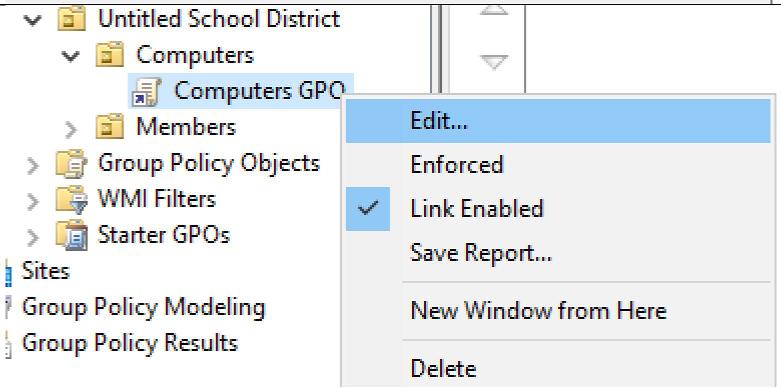
Here you can see some of the example students.

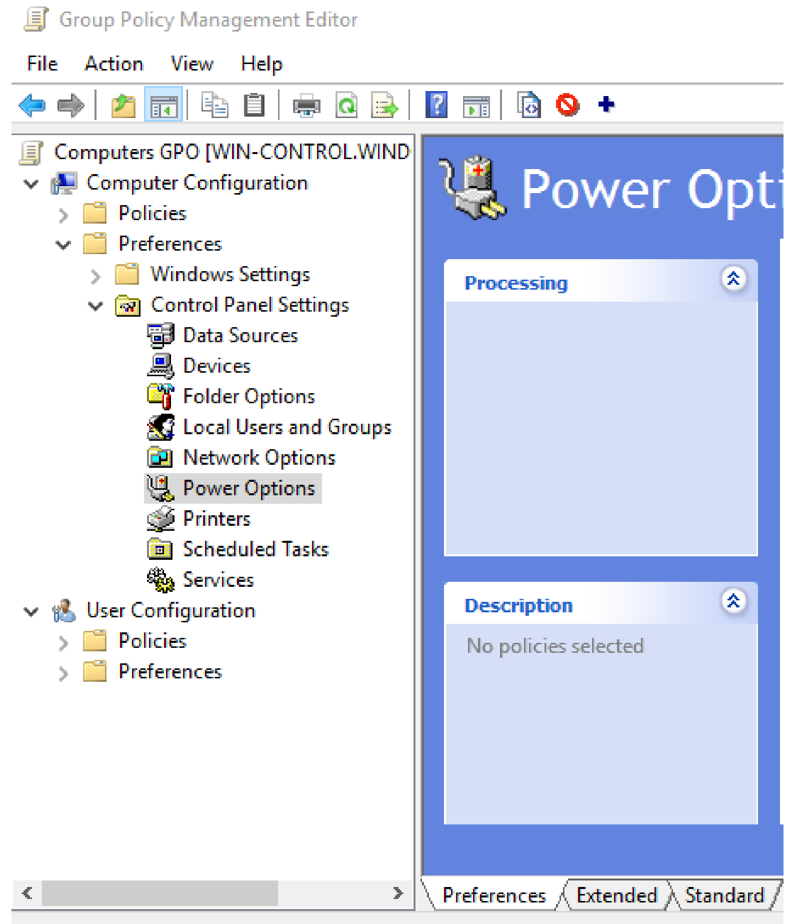
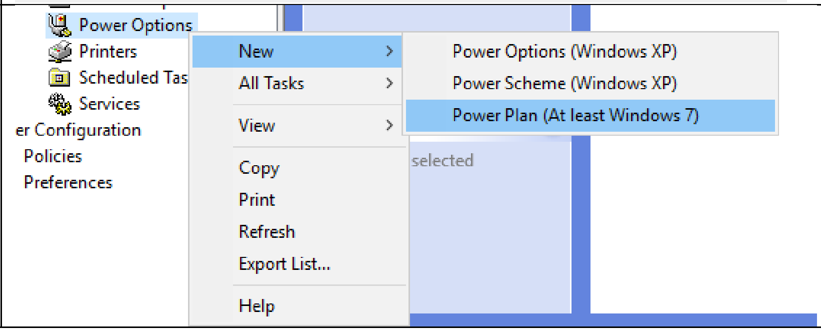


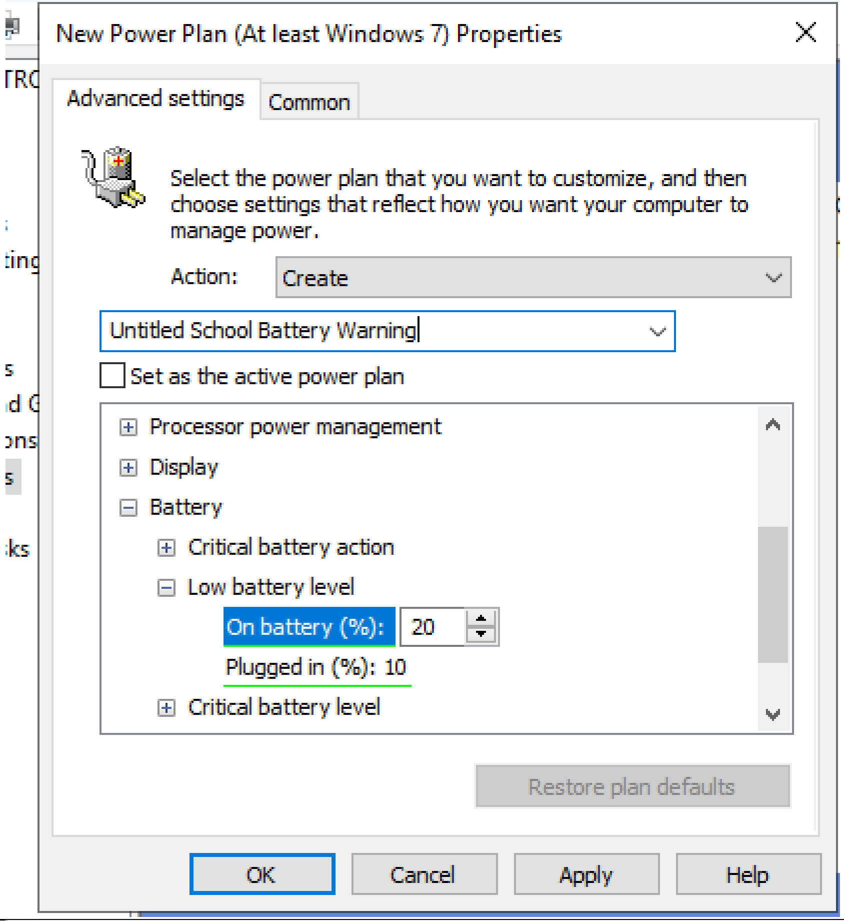
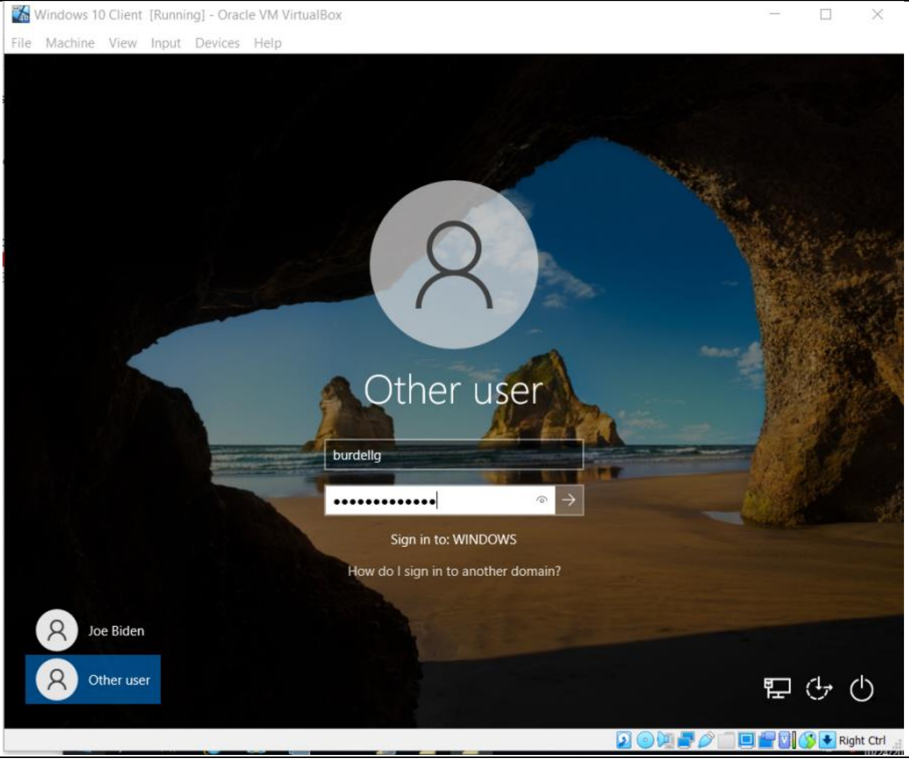
Name	Type	Description
Joe Biden	User	
Jorge Fred	User	
Rick Astley	User	
George Burd...	User	

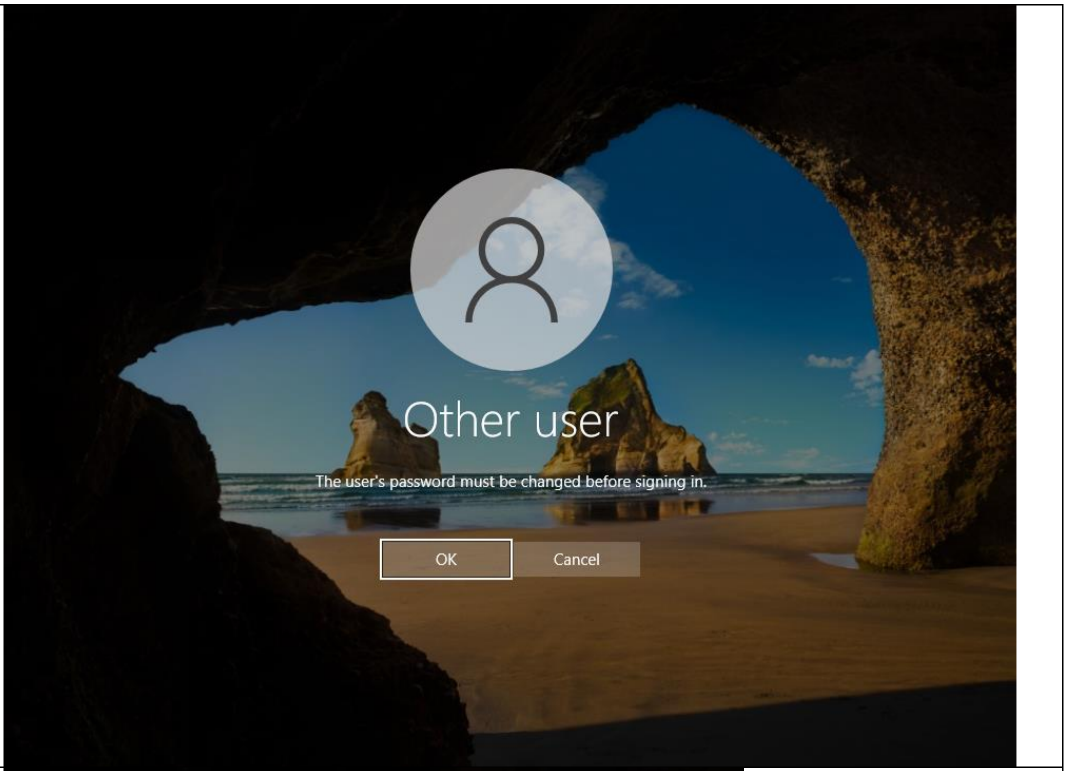
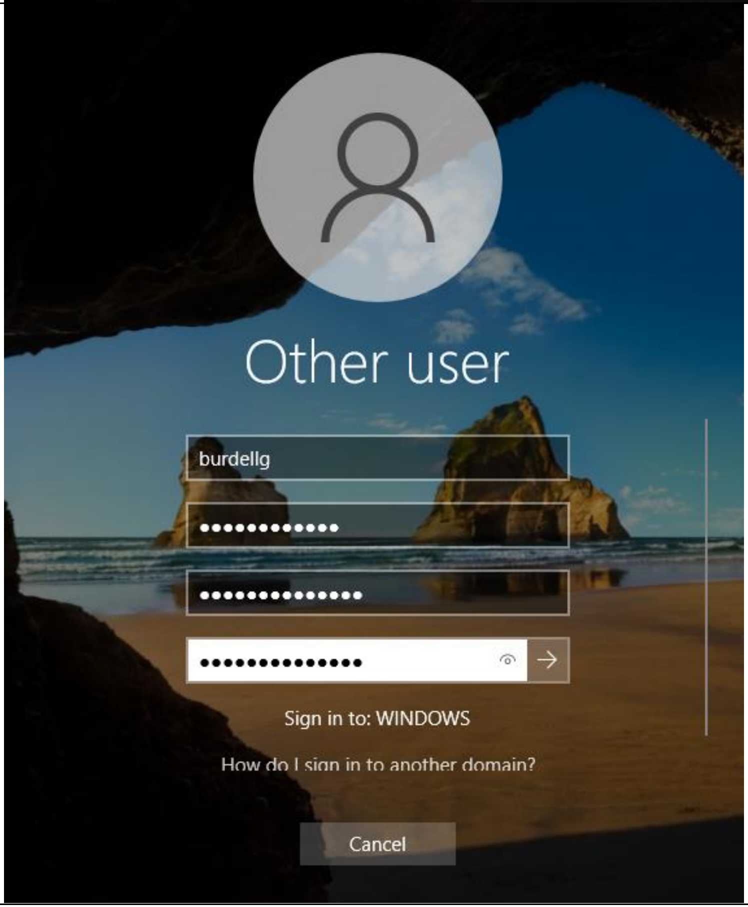
Group Policy Objects (Computer):

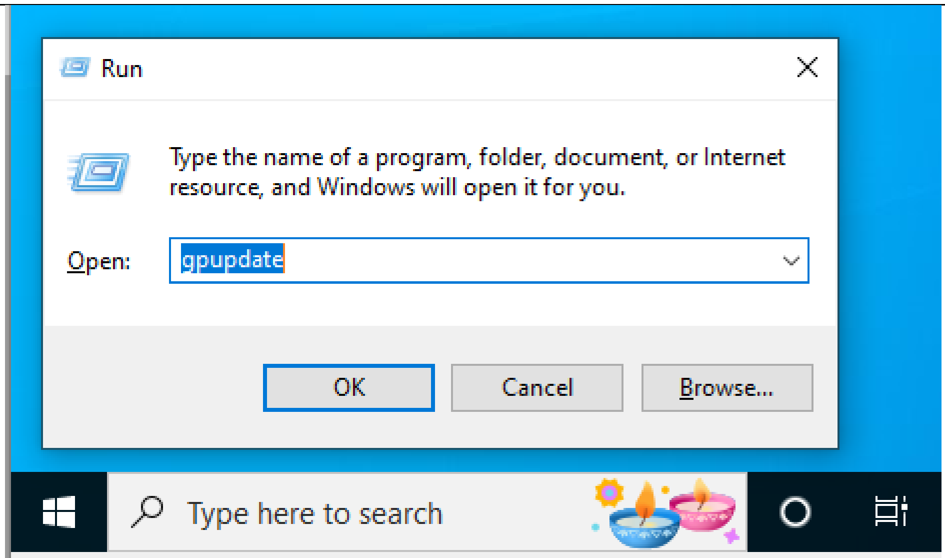
Head back to server manager and click Group Policy Management	 Server Manager Server Manager ▸ Dashboard Manage Tools View Help Dashboard Local Server All Servers AD DS DNS File and Storage Services ▸ WELCOME TO SERVER MANAGER QUICK START WHAT'S NEW LEARN MORE 1 Configure this local ser 2 Add roles and features 3 Add other servers to man 4 Create a server group 5 Connect this server to clo ROLES AND SERVER GROUPS Roles: 3 | Server groups: 1 | Servers total: 1 AD DS 1 Manageability Events Services Performance DNS Manageability Events Services Performance Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers ADSI Edit Component Services Computer Management Defragment and Optimize Drives Disk Cleanup DNS Event Viewer Group Policy Management iSCSI Initiator Local Security Policy Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Print Management Recovery Drive Registry Editor Resource Monitor Services System Configuration System Information Task Scheduler
When you open Group Policy Management, navigate down forest, domains to windows.local and find the Untitled School district OU.	 Group Policy Management File Action View Window Help Group Policy Management Forest: windows.local Domains windows.local Default Domain Policy Domain Controllers Untitled School District Computers Members Group Policy Objects WMI Filters Starter GPOs Sites Group Policy Modeling Group Policy Results Group Policy Management Contents Name Forest: windows.local

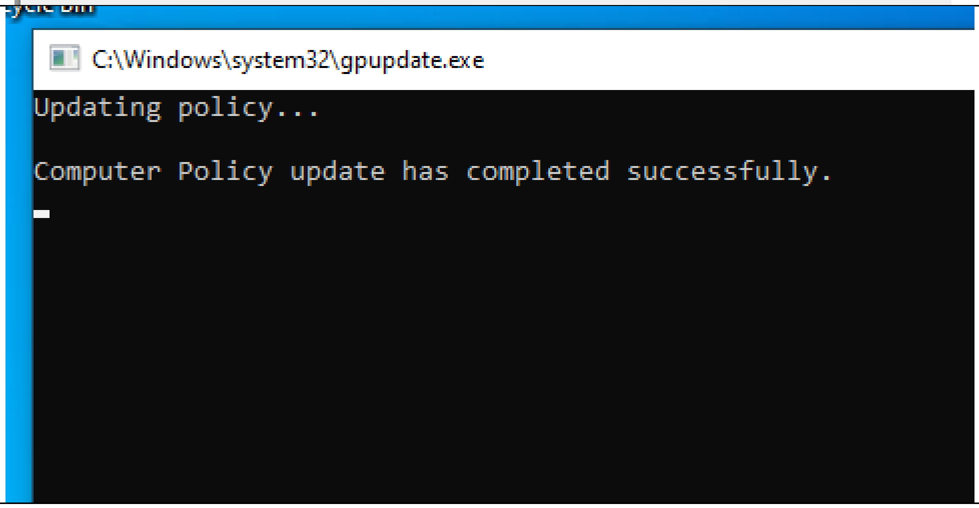
	 Untitled School District Computers Members Group Policy C WMI Filters Starter GPOs Sites Group Policy Modelin Group Policy Results Create a GPO in this domain, and Link it here... Link an Existing GPO... Block Inheritance Group Policy Update... Group Policy Modeling Wizard... New Organizational Unit View New Window from Here Delete Rename Refresh Properties Help Create a GPO in this domain and l BPA results
Create a GPO for the computers first	 Name: Computers GPO Source Starter GPO: (none)
To edit the Group Policy, right click and press edit.	 Untitled School District Computers Computers GPO Members Group Policy Objects WMI Filters Starter GPOs Sites Group Policy Modeling Group Policy Results Edit... Enforced ✓ Link Enabled Save Report... New Window from Here Delete

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.	 Group Policy Management Editor File Action View Help Computers GPO [WIN-CONTROL.WIND Computer Configuration Policies Preferences Windows Settings Control Panel Settings Data Sources Devices Folder Options Local Users and Groups Network Options Power Options Printers Scheduled Tasks Services User Configuration Policies Preferences Power Opti Processing Description No policies selected Preferences Extended Standard
Right click to select new and select Power Plan.	 Power Options Printers Scheduled Tas Services er Configuration Policies Preferences New All Tasks View Copy Print Refresh Export List... Help Power Options (Windows XP) Power Scheme (Windows XP) Power Plan (At least Windows 7) selected

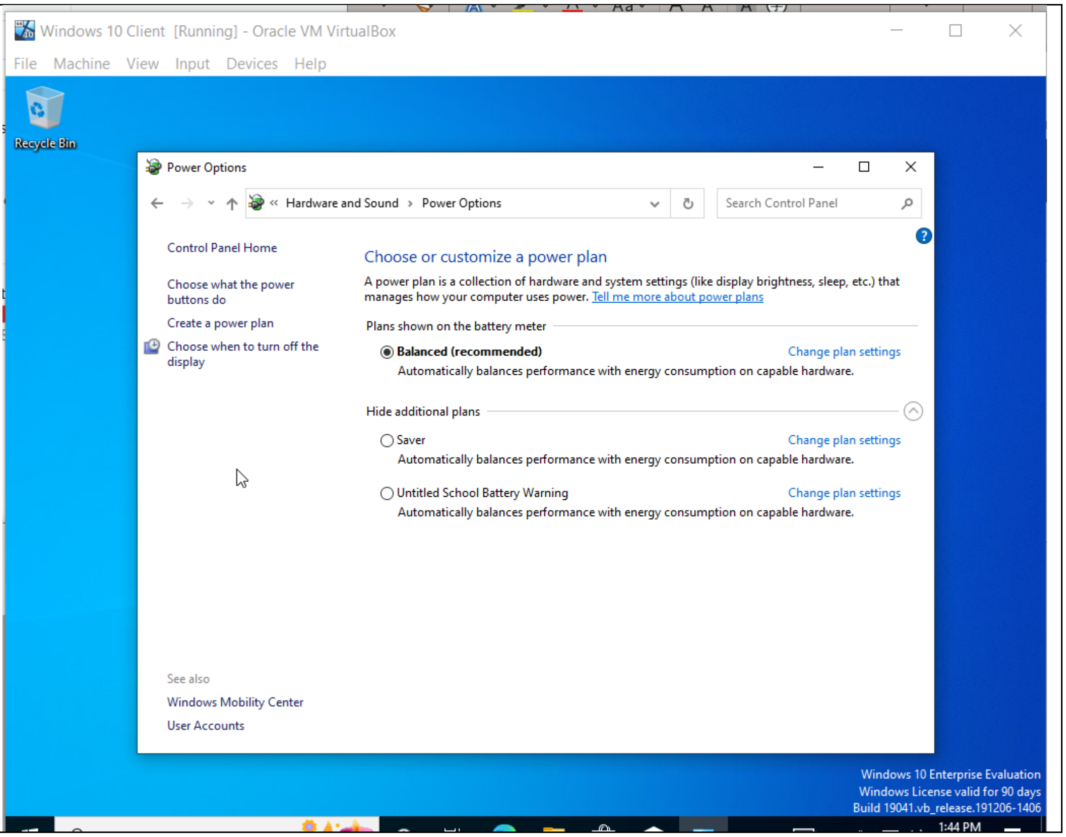
I changed the battery % threshold from 10% for low battery level to 20% instead.	 New Power Plan (At least Windows 7) Properties Advanced settings | Common Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power. Action: Create Untitled School Battery Warning ☐ Set as the active power plan ⊞ Processor power management ⊞ Display ⊟ Battery ⊞ Critical battery action ⊟ Low battery level On battery (%): 20 Plugged in (%): 10 ⊞ Critical battery level Restore plan defaults OK | Cancel | Apply | Help
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.	 Windows 10 Client [Running] - Oracle VM VirtualBox File Machine View Input Devices Help Other user burdellg •••••••••••••• Sign in to: WINDOWS How do I sign in to another domain? Joe Biden Other user Right Ctrl

As per our earlier policy, the user has to change their password before signing in and we can see that here.	 Other user The user's password must be changed before signing in.
Create a new password.	 Other user burdellg •••••••••••• •••••••••••••• ••••••••••••••• Sign in to: WINDOWS How do I sign in to another domain?

Open the Run pop-up and run the command "gpupdate", this will update the client's policy to the latest Group Policy.	 Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: gpupdate

You can see that it's been confirmed.	
	C:\Windows\system32\gpupdate.exe
	`Updating policy...`
	`Computer Policy update has completed successfully.`

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.



Windows 10 Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Recycle Bin

Power Options

« Hardware and Sound › Power Options

Search Control Panel

Control Panel Home

Choose what the power buttons do

Create a power plan

Choose when to turn off the display

Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

Plans shown on the battery meter

● **Balanced (recommended)** — Change plan settings

Automatically balances performance with energy consumption on capable hardware.

Hide additional plans

○ Saver — Change plan settings

Automatically balances performance with energy consumption on capable hardware.

○ Untitled School Battery Warning — Change plan settings

Automatically balances performance with energy consumption on capable hardware.

See also

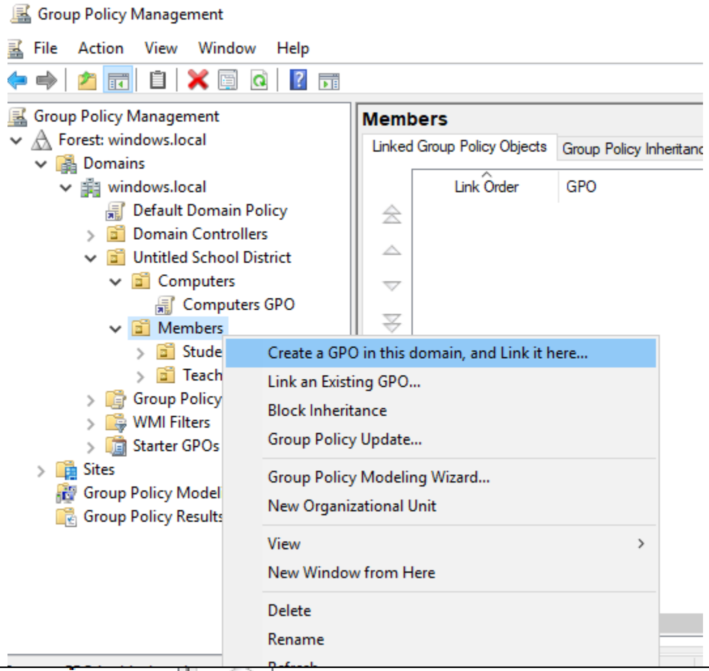
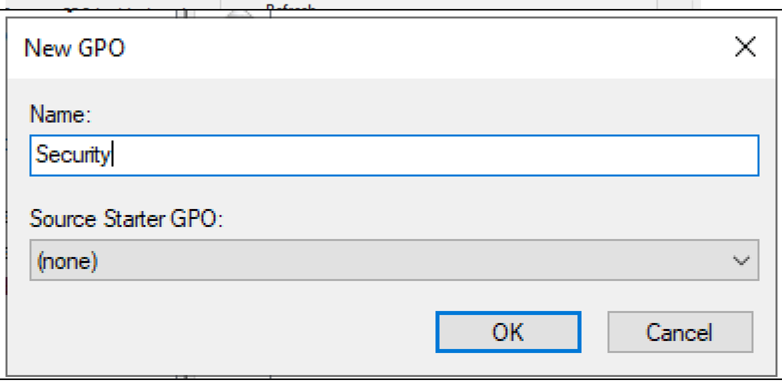
Windows Mobility Center

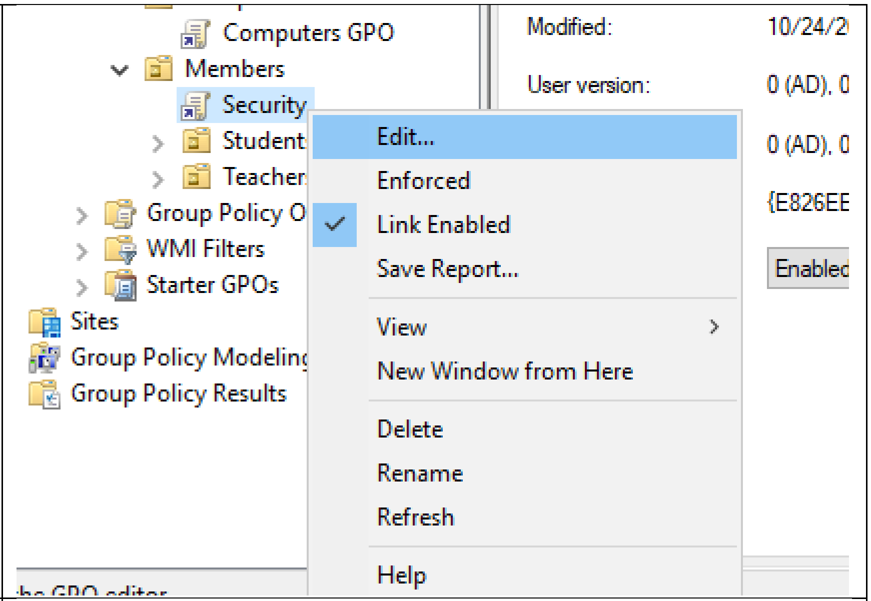
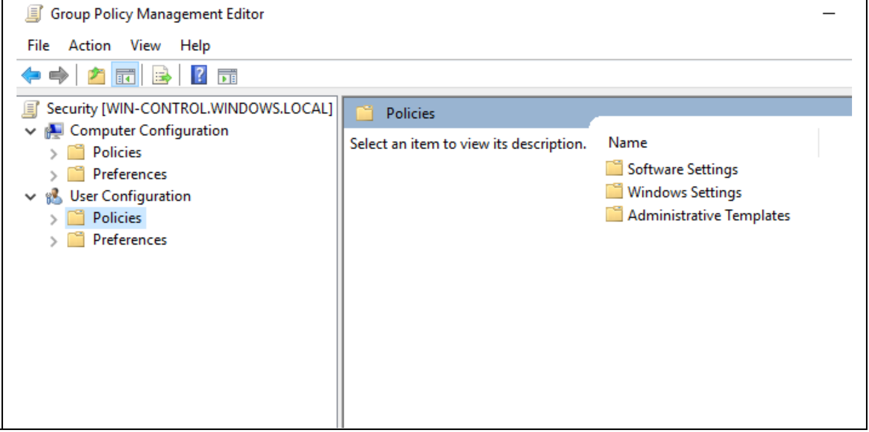
User Accounts

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406

1:44 PM

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.	 Group Policy Management File Action View Window Help Group Policy Management Forest: windows.local Domains windows.local Default Domain Policy Domain Controllers Untitled School District Computers Computers GPO Members Stude Teach Group Policy WMI Filters Starter GPOs Sites Group Policy Model Group Policy Results Members Linked Group Policy Objects Group Policy Inheritanc Link Order GPO Create a GPO in this domain, and Link it here... Link an Existing GPO... Block Inheritance Group Policy Update... Group Policy Modeling Wizard... New Organizational Unit View New Window from Here Delete Rename
I named the GPO Security.	 New GPO Name: Security Source Starter GPO: (none)

Like as to edit all GPO’s, right click and select edit to be brought to the Management Editor.	 Computers GPO Members Security Student Teacher Group Policy O WMI Filters Starter GPOs Sites Group Policy Modeling Group Policy Results Modified: 10/24/2 User version: 0 (AD), 0 0 (AD), 0 {E826EE Enabled Edit... Enforced ✓ Link Enabled Save Report... View New Window from Here Delete Rename Refresh Help he GPO editor
Here in the Management Editor we can now implement the security policies.	 Group Policy Management Editor File Action View Help Security [WIN-CONTROL.WINDOWS.LOCAL] Computer Configuration Policies Preferences User Configuration Policies Preferences Policies Select an item to view its description. Name Software Settings Windows Settings Administrative Templates

Security Policies:

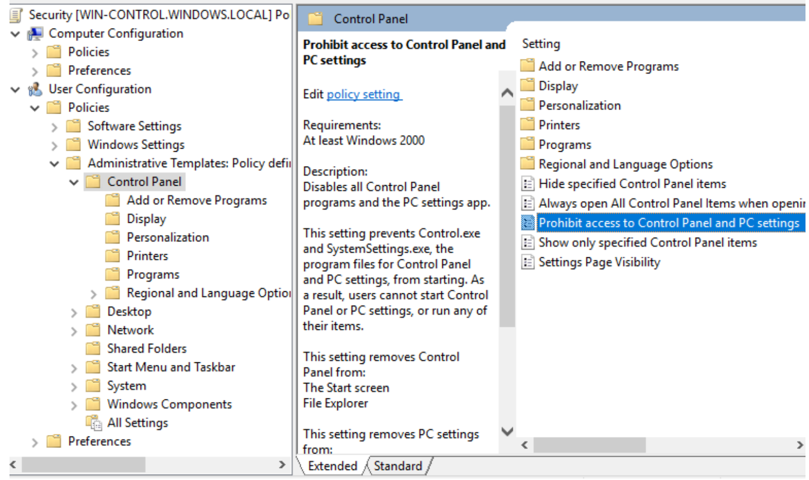
List of Policies:

1. Restrict Access to Control Panel
2. Prevent Windows Lan Manager Hash Storage
3. Command Prompt Access Control
4. Disable Forced System Restarts
5. Disallow Insertable Devices (CD’s, USBs)
6. Restrict Software Installation
7. Disable the Guest Account

1. 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.



Prohibit access to Control Panel and PC settings

Edit policy setting

Requirements:
At least Windows 2000

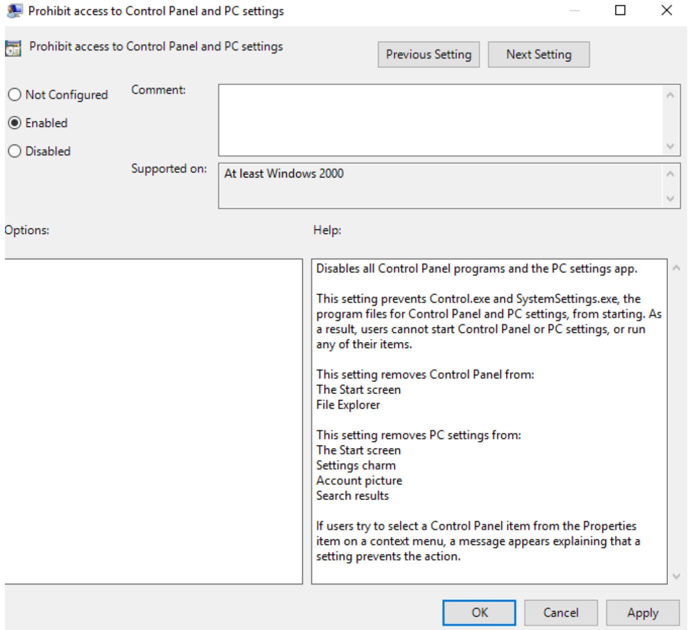
Description:
Disables all Control Panel programs and the PC settings app.

This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:

Click enabled and apply the setting to prohibit access.



Prohibit access to Control Panel and PC settings

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Disables all Control Panel programs and the PC settings app.

This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

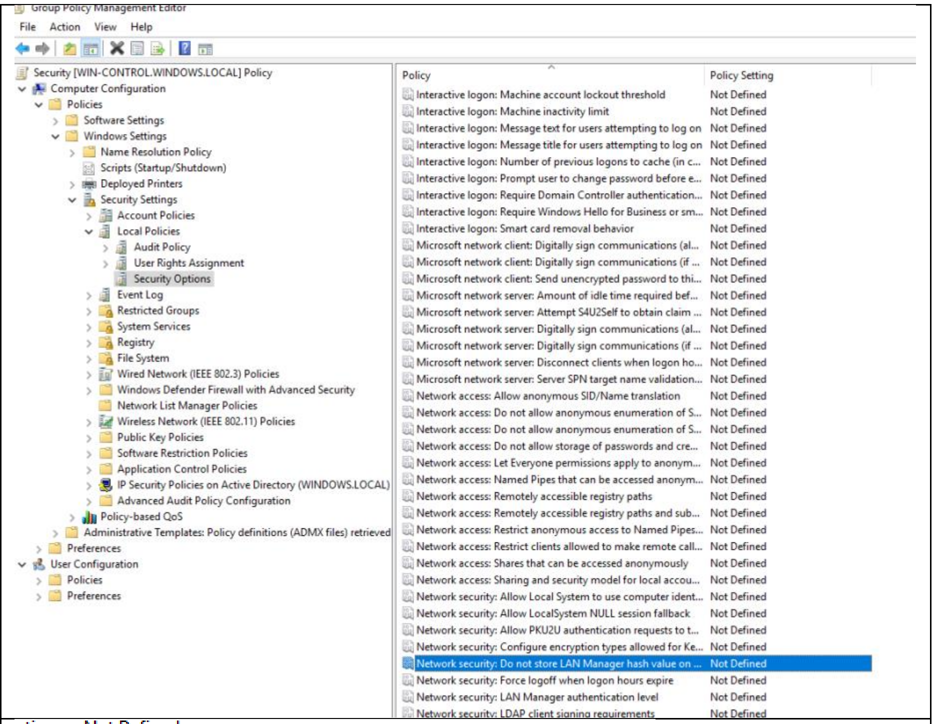
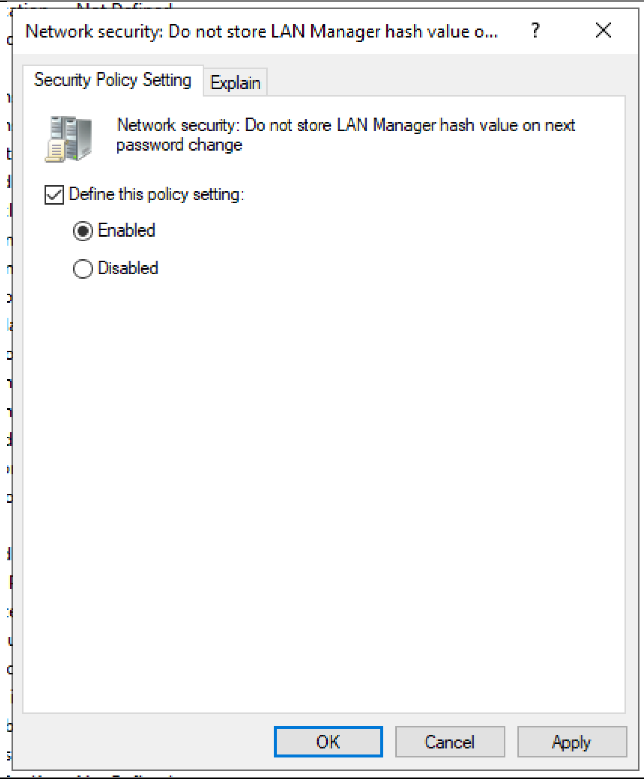
This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

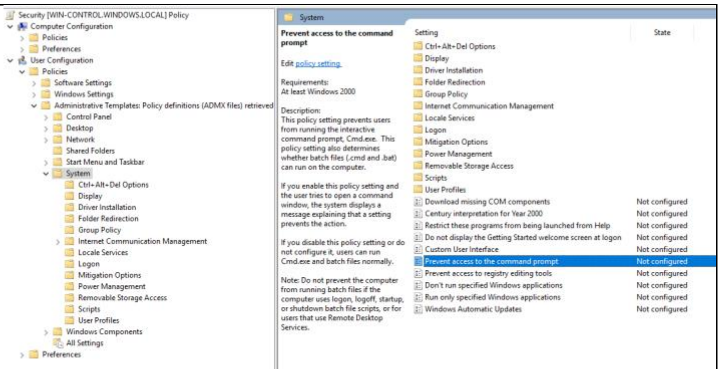
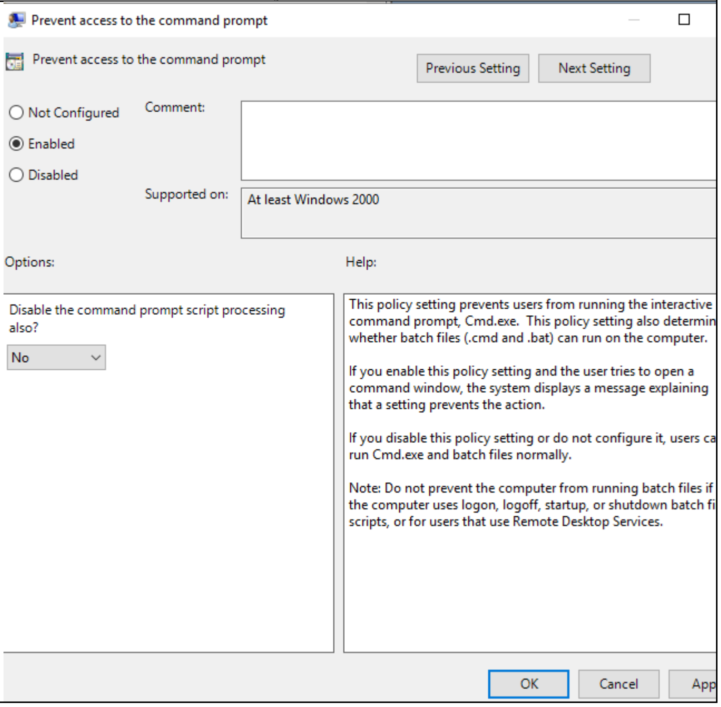
2. Prevent Windows from storing Lan Manager Hash

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	 Group Policy Management Editor File Action View Help Security [WIN-CONTROL.WINDOWS.LOCAL] Policy Computer Configuration Policies Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Audit Policy User Rights Assignment Security Options Event Log Restricted Groups System Services Registry File System Wired Network (IEEE 802.3) Policies Windows Defender Firewall with Advanced Security Network List Manager Policies Wireless Network (IEEE 802.11) Policies Public Key Policies Software Restriction Policies Application Control Policies IP Security Policies on Active Directory (WINDOWS.LOCAL) Advanced Audit Policy Configuration Policy-based QoS Administrative Templates: Policy definitions (ADMX files) retrieved Preferences User Configuration Policies Preferences Policy — Policy Setting Interactive logon: Machine account lockout threshold — Not Defined Interactive logon: Machine inactivity limit — Not Defined Interactive logon: Message text for users attempting to log on — Not Defined Interactive logon: Message title for users attempting to log on — Not Defined Interactive logon: Number of previous logons to cache (in c... — Not Defined Interactive logon: Prompt user to change password before e... — Not Defined Interactive logon: Require Domain Controller authentication... — Not Defined Interactive logon: Require Windows Hello for Business or sm... — Not Defined Interactive logon: Smart card removal behavior — Not Defined Microsoft network client: Digitally sign communications (al... — Not Defined Microsoft network client: Digitally sign communications (if ... — Not Defined Microsoft network client: Send unencrypted password to thi... — Not Defined Microsoft network server: Amount of idle time required bef... — Not Defined Microsoft network server: Attempt S4U2Self to obtain claim ... — Not Defined Microsoft network server: Digitally sign communications (al... — Not Defined Microsoft network server: Digitally sign communications (if ... — Not Defined Microsoft network server: Disconnect clients when logon ho... — Not Defined Microsoft network server: Server SPN target name validation... — Not Defined Network access: Allow anonymous SID/Name translation — Not Defined Network access: Do not allow anonymous enumeration of S... — Not Defined Network access: Do not allow anonymous enumeration of S... — Not Defined Network access: Do not allow storage of passwords and cre... — Not Defined Network access: Let Everyone permissions apply to anonym... — Not Defined Network access: Named Pipes that can be accessed anonym... — Not Defined Network access: Remotely accessible registry paths — Not Defined Network access: Remotely accessible registry paths and sub... — Not Defined Network access: Restrict anonymous access to Named Pipes... — Not Defined Network access: Restrict clients allowed to make remote call... — Not Defined Network access: Shares that can be accessed anonymously — Not Defined Network access: Sharing and security model for local accou... — Not Defined Network security: Allow Local System to use computer ident... — Not Defined Network security: Allow LocalSystem NULL session fallback — Not Defined Network security: Allow PKU2U authentication requests to t... — Not Defined Network security: Configure encryption types allowed for Ke... — Not Defined Network security: Do not store LAN Manager hash value on ... — Not Defined Network security: Force logoff when logon hours expire — Not Defined Network security: LAN Manager authentication level — Not Defined Network security: LDAP client signing requirements — Not Defined
Enable this policy and click apply.	 Network security: Do not store LAN Manager hash value o... ? × Security Policy Setting Explain Network security: Do not store LAN Manager hash value on next password change ☑ Define this policy setting: ● Enabled ○ Disabled OK Cancel Apply

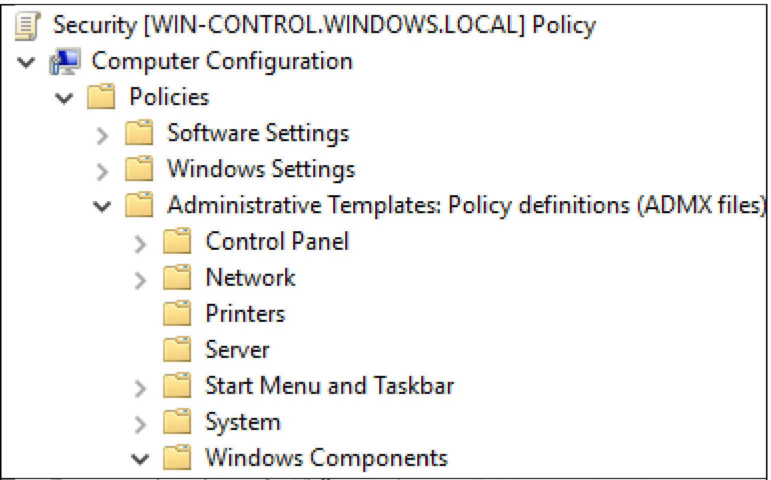
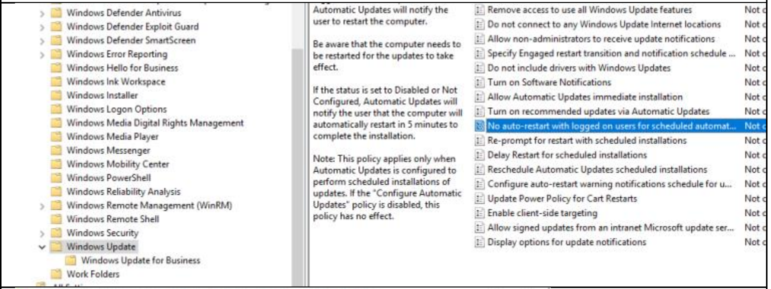
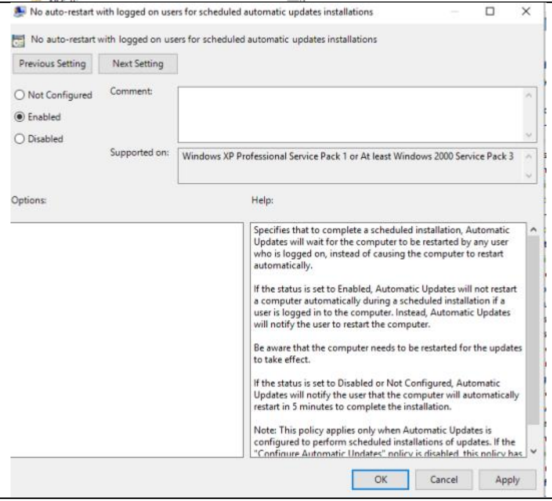
3. Restrict Access to the Command Prompt

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	 Security [WIN-CONTROL.WINDOWS.LOCAL] Policy Computer Configuration Policies Preferences User Configuration Policies Software Settings Windows Settings Administrative Templates: Policy definitions (ADMX files) retrieved Control Panel Desktop Network Shared Folders Start Menu and Taskbar System Ctrl+Alt+Del Options Display Driver Installation Folder Redirection Group Policy Internet Communication Management Locale Services Logon Mitigation Options Power Management Removable Storage Access Scripts User Profiles Windows Components All Settings Preferences System **Prevent access to the command prompt** Edit policy setting Requirements: At least Windows 2000 Description: This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action. If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally. Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services. Setting — State Ctrl+Alt+Del Options Display Driver Installation Folder Redirection Group Policy Internet Communication Management Locale Services Logon Mitigation Options Power Management Removable Storage Access Scripts User Profiles Download missing COM components — Not configured Century interpretation for Year 2000 — Not configured Restrict these programs from being launched from Help — Not configured Do not display the Getting Started welcome screen at logon — Not configured Custom User Interface — Not configured Prevent access to the command prompt — Not configured Prevent access to registry editing tools — Not configured Don't run specified Windows applications — Not configured Run only specified Windows applications — Not configured Windows Automatic Updates — Not configured
Enable the “Prevent access to the command prompt” policy and click apply.	 Prevent access to the command prompt Prevent access to the command prompt Previous Setting Next Setting ○ Not Configured ● Enabled ○ Disabled Comment: Supported on: At least Windows 2000 Options: Disable the command prompt script processing also? No Help: This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determin whether batch files (.cmd and .bat) can run on the computer. If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action. If you disable this policy setting or do not configure it, users ca run Cmd.exe and batch files normally. Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch fi scripts, or for users that use Remote Desktop Services. OK Cancel App

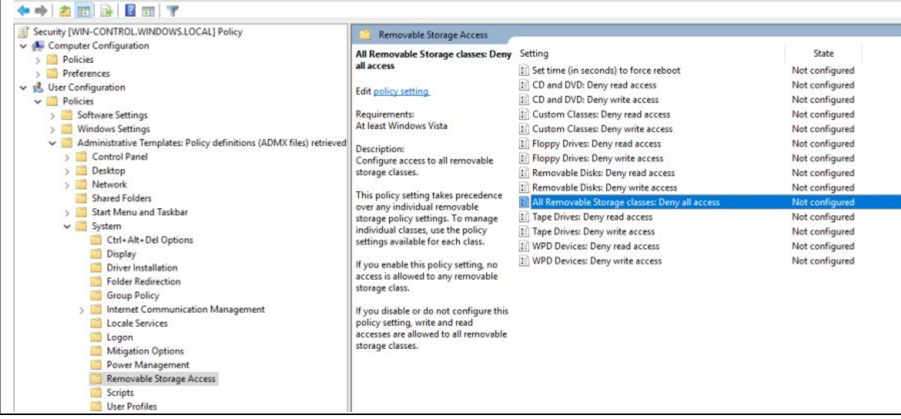
4. Disable Forced System Restarts:

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	 Security [WIN-CONTROL.WINDOWS.LOCAL] Policy Computer Configuration Policies Software Settings Windows Settings Administrative Templates: Policy definitions (ADMX files) Control Panel Network Printers Server Start Menu and Taskbar System Windows Components
	 Windows Defender Antivirus Windows Defender Exploit Guard Windows Defender SmartScreen Windows Error Reporting Windows Hello for Business Windows Ink Workspace Windows Installer Windows Logon Options Windows Media Digital Rights Management Windows Media Player Windows Messenger Windows Mobility Center Windows PowerShell Windows Reliability Analysis Windows Remote Management (WinRM) Windows Remote Shell Windows Security Windows Update Windows Update for Business Work Folders Automatic Updates will notify the user to restart the computer. Be aware that the computer needs to be restarted for the updates to take effect. If the status is set to Disabled or Not Configured, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation. Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the "Configure Automatic Updates" policy is disabled, this policy has no effect. Remove access to use all Windows Update features Not c Do not connect to any Windows Update Internet locations Not c Allow non-administrators to receive update notifications Not c Specify Engaged restart transition and notification schedule ... Not c Do not include drivers with Windows Updates Not c Turn on Software Notifications Not c Allow Automatic Updates immediate installation Not c Turn on recommended updates via Automatic Updates Not c No auto-restart with logged on users for scheduled automat... Not c Re-prompt for restart with scheduled installations Not c Delay Restart for scheduled installations Not c Reschedule Automatic Updates scheduled installations Not c Configure auto-restart warning notifications schedule for u... Not c Update Power Policy for Cart Restarts Not c Enable client-side targeting Not c Allow signed updates from an intranet Microsoft update ser... Not c Display options for update notifications Not c
Enable this policy and click apply.	 No auto-restart with logged on users for scheduled automatic updates installations No auto-restart with logged on users for scheduled automatic updates installations Previous Setting Next Setting ○ Not Configured ● Enabled ○ Disabled Comment: Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Options: Help: Specifies that to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted by any user who is logged on, instead of causing the computer to restart automatically. If the status is set to Enabled, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged in to the computer. Instead, Automatic Updates will notify the user to restart the computer. Be aware that the computer needs to be restarted for the updates to take effect. If the status is set to Disabled or Not Configured, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation. Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the "Configure Automatic Updates" policy is disabled, this policy has OK Cancel Apply

5. 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.	

- Security [WIN-CONTROL.WINDOWS.LOCAL] Policy
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) retrieved
        - Control Panel
        - Desktop
        - Network
        - Shared Folders
        - Start Menu and Taskbar
        - System
          - Ctrl+Alt+Del Options
          - Display
          - Driver Installation
          - Folder Redirection
          - Group Policy
          - Internet Communication Management
          - Locale Services
          - Logon
          - Mitigation Options
          - Power Management
          - Removable Storage Access
          - Scripts
          - User Profiles

Removable Storage Access

All Removable Storage classes: Deny all access

Edit policy setting

Requirements:
At least Windows Vista

Description:
Configure access to all removable storage classes.

This policy setting takes precedence over any individual removable storage policy settings. To manage individual classes, use the policy settings available for each class.

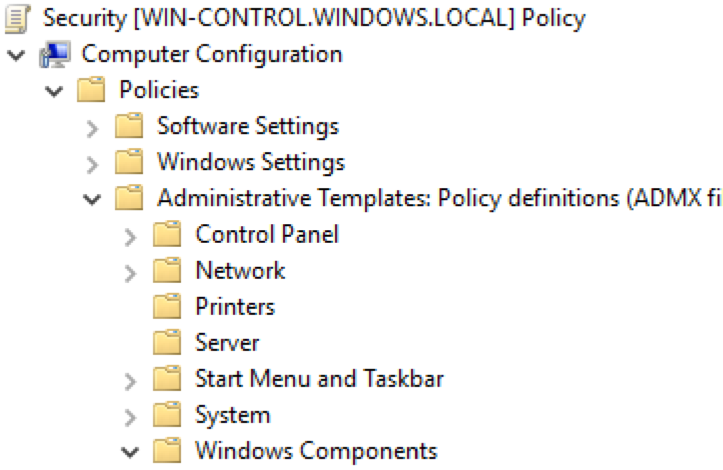
If you enable this policy setting, no access is allowed to any removable storage class.

If you disable or do not configure this policy setting, write and read accesses are allowed to all removable storage classes.

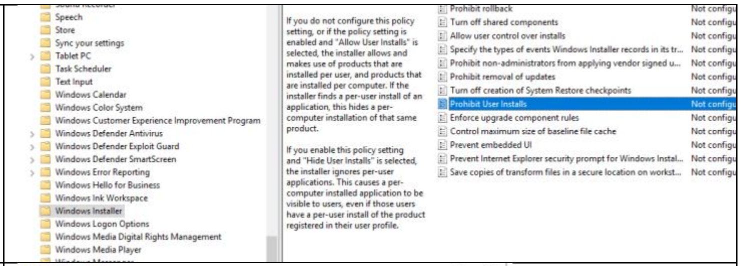
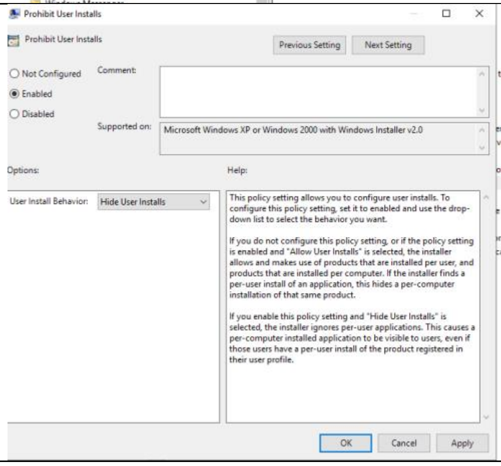
Setting	State
Set time (in seconds) to force reboot	Not configured
CD and DVD: Deny read access	Not configured
CD and DVD: Deny write access	Not configured
Custom Classes: Deny read access	Not configured
Custom Classes: Deny write access	Not configured
Floppy Drives: Deny read access	Not configured
Floppy Drives: Deny write access	Not configured
Removable Disks: Deny read access	Not configured
Removable Disks: Deny write access	Not configured
All Removable Storage classes: Deny all access	Not configured
Tape Drives: Deny read access	Not configured
Tape Drives: Deny write access	Not configured
WPD Devices: Deny read access	Not configured
WPD Devices: Deny write access	Not configured

6. 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.	

- Security [WIN-CONTROL.WINDOWS.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX fi
        - Control Panel
        - Network
        - Printers
        - Server
        - Start Menu and Taskbar
        - System
        - Windows Components

	
Enable the policy of Prohibit User Installs and click apply.	

Speech
Store
Sync your settings
Tablet PC
Task Scheduler
Text Input
Windows Calendar
Windows Color System
Windows Customer Experience Improvement Program
Windows Defender Antivirus
Windows Defender Exploit Guard
Windows Defender SmartScreen
Windows Error Reporting
Windows Hello for Business
Windows Ink Workspace
Windows Installer
Windows Logon Options
Windows Media Digital Rights Management
Windows Media Player

If you do not configure this policy setting, or if the policy setting is enabled and "Allow User Installs" is selected, the installer allows and makes use of products that are installed per user, and products that are installed per computer. If the installer finds a per-user install of an application, this hides a per-computer installation of that same product.

If you enable this policy setting and "Hide User Installs" is selected, the installer ignores per-user applications. This causes a per-computer installed application to be visible to users, even if those users have a per-user install of the product registered in their user profile.

Prohibit rollback	Not configu
Turn off shared components	Not configu
Allow user control over installs	Not configu
Specify the types of events Windows Installer records in its tr...	Not configu
Prohibit non-administrators from applying vendor signed u...	Not configu
Prohibit removal of updates	Not configu
Turn off creation of System Restore checkpoints	Not configu
Prohibit User Installs	Not configu
Enforce upgrade component rules	Not configu
Control maximum size of baseline file cache	Not configu
Prevent embedded UI	Not configu
Prevent Internet Explorer security prompt for Windows Instal...	Not configu
Save copies of transform files in a secure location on workst...	Not configu

Prohibit User Installs

Prohibit User Installs

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Microsoft Windows XP or Windows 2000 with Windows Installer v2.0

Options:

User Install Behavior: Hide User Installs

Help:

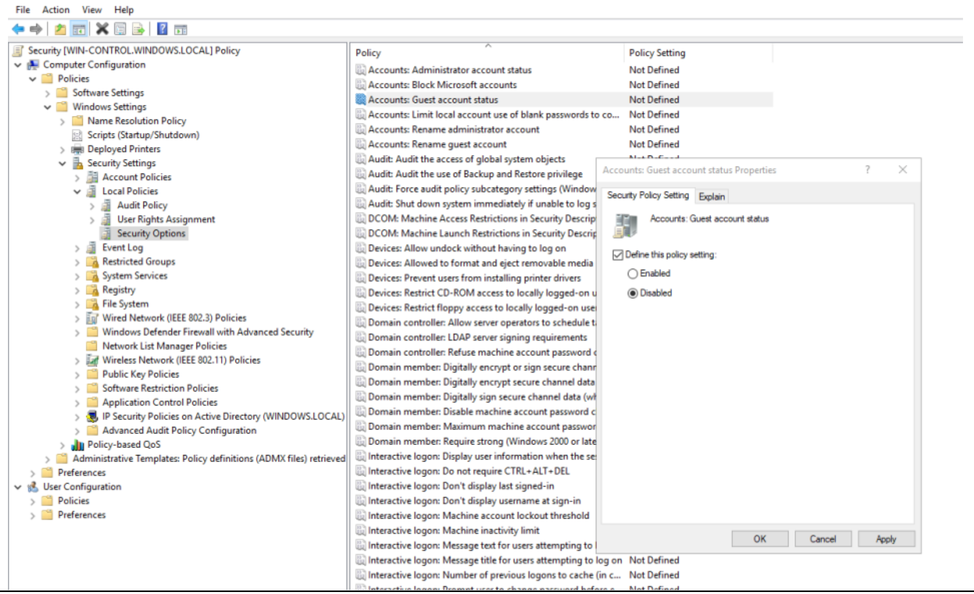
This policy setting allows you to configure user installs. To configure this policy setting, set it to enabled and use the drop-down list to select the behavior you want.

If you do not configure this policy setting, or if the policy setting is enabled and "Allow User Installs" is selected, the installer allows and makes use of products that are installed per user, and products that are installed per computer. If the installer finds a per-user install of an application, this hides a per-computer installation of that same product.

If you enable this policy setting and "Hide User Installs" is selected, the installer ignores per-user applications. This causes a per-computer installed application to be visible to users, even if those users have a per-user install of the product registered in their user profile.

7. 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.	

Security [WIN-CONTROL.WINDOWS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (WINDOWS.LOCAL)
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	
Audit: Audit the use of Backup and Restore privilege	
Audit: Force audit policy subcategory settings (Window	
Audit: Shut down system immediately if unable to log s	
DCOM: Machine Access Restrictions in Security Descrip	
DCOM: Machine Launch Restrictions in Security Descrip	
Devices: Allow undock without having to log on	
Devices: Allowed to format and eject removable media	
Devices: Prevent users from installing printer drivers	
Devices: Restrict CD-ROM access to locally logged-on u	
Devices: Restrict floppy access to locally logged-on use	
Domain controller: Allow server operators to schedule t	
Domain controller: LDAP server signing requirements	
Domain controller: Refuse machine account password c	
Domain member: Digitally encrypt or sign secure chann	
Domain member: Digitally encrypt secure channel data	
Domain member: Digitally sign secure channel data (wh	
Domain member: Disable machine account password c	
Domain member: Maximum machine account passwor	
Domain member: Require strong (Windows 2000 or late	
Interactive logon: Display user information when the se	
Interactive logon: Do not require CTRL+ALT+DEL	
Interactive logon: Don't display last signed-in	
Interactive logon: Don't display username at sign-in	
Interactive logon: Machine account lockout threshold	
Interactive logon: Machine inactivity limit	
Interactive logon: Message text for users attempting to	
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in c...	Not Defined

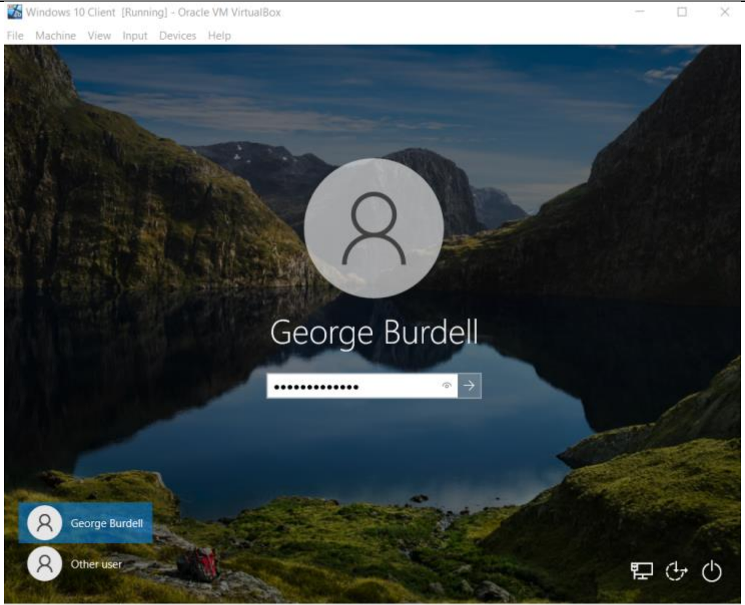
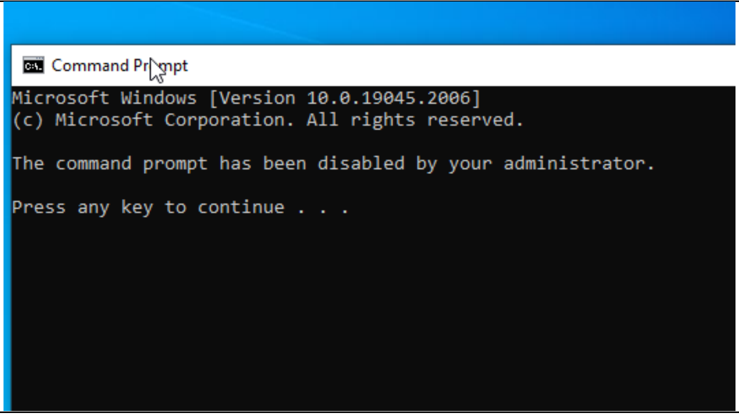
Accounts: Guest account status Properties

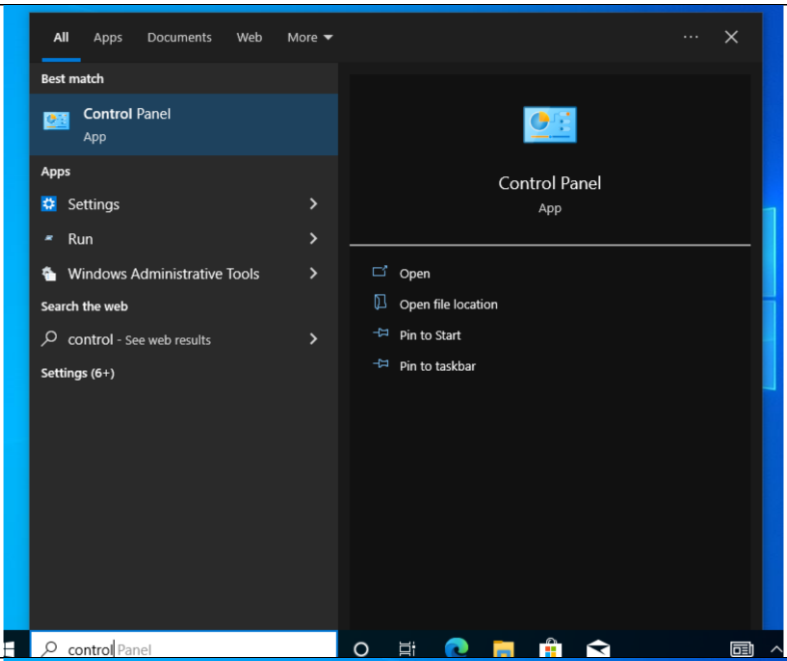
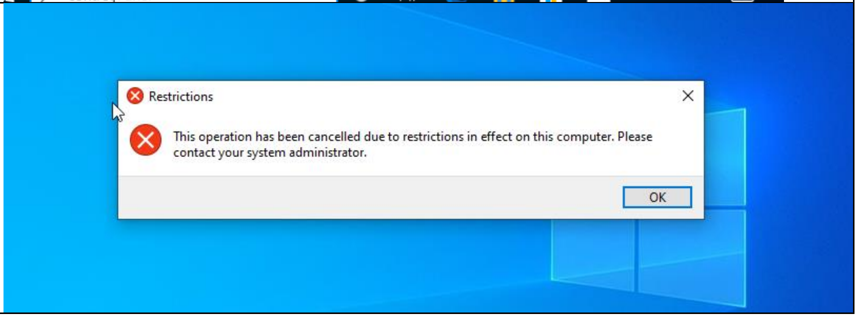
Accounts: Guest account status

☑ Define this policy setting:
○ Enabled
● 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.	 Windows 10 Client [Running] - Oracle VM VirtualBox File Machine View Input Devices Help George Burdell George Burdell Other user
When trying to access Command Prompt, we can confirm that it has been disabled.	 Microsoft Windows [Version 10.0.19045.2006] (c) Microsoft Corporation. All rights reserved. The command prompt has been disabled by your administrator. Press any key to continue . . .

Similarly when trying to open Control Panel, we receive an error message saying that the operation has been canceled due to restrictions.	 All Apps Documents Web More Best match Control Panel App Apps Settings Run Windows Administrative Tools Search the web control - See web results Settings (6+) Control Panel App Open Open file location Pin to Start Pin to taskbar control Panel
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.	Restrictions This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

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.