Nome: Ennio da Silva Vitor

Date: 02 - 05 - 2015

Assessment 2 group policy

2017

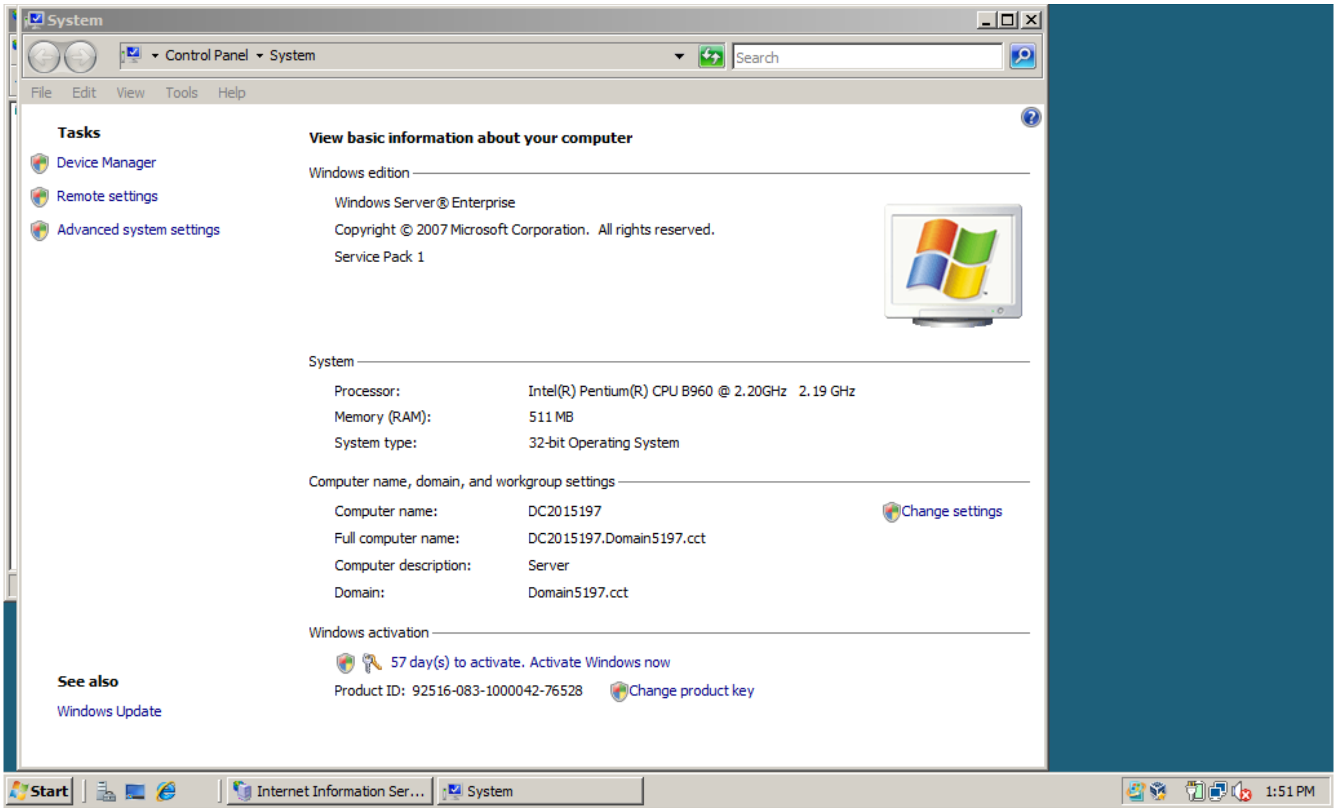
Summary of contents

Introduction

The objective of this assessment, is to create two organizational units, Academics and Students and also apply a user policy for each group.

Each policy will have five appropriated modifications, that will control permissions in order to protect the system, allowing the users to focus only on complete their tasks without modify or access parts of the system that can be sensible, where they could collect not authorized information or access to areas of the system that could bring future problems for the organization.

The screenshot below shows the system where all this assessment will be done. The active directory is already set as a domain controller "Domain5197.cct.



View basic information about your computer

Windows edition

Windows Server® Enterprise
Copyright © 2007 Microsoft Corporation. All rights reserved.
Service Pack 1

System

Processor: Intel(R) Pentium(R) CPU B960 @ 2.20GHz 2.19 GHz
Memory (RAM): 511 MB
System type: 32-bit Operating System

Computer name, domain, and workgroup settings

Computer name: DC2015197
Full computer name: DC2015197.Domain5197.cct
Computer description: Server
Domain: Domain5197.cct

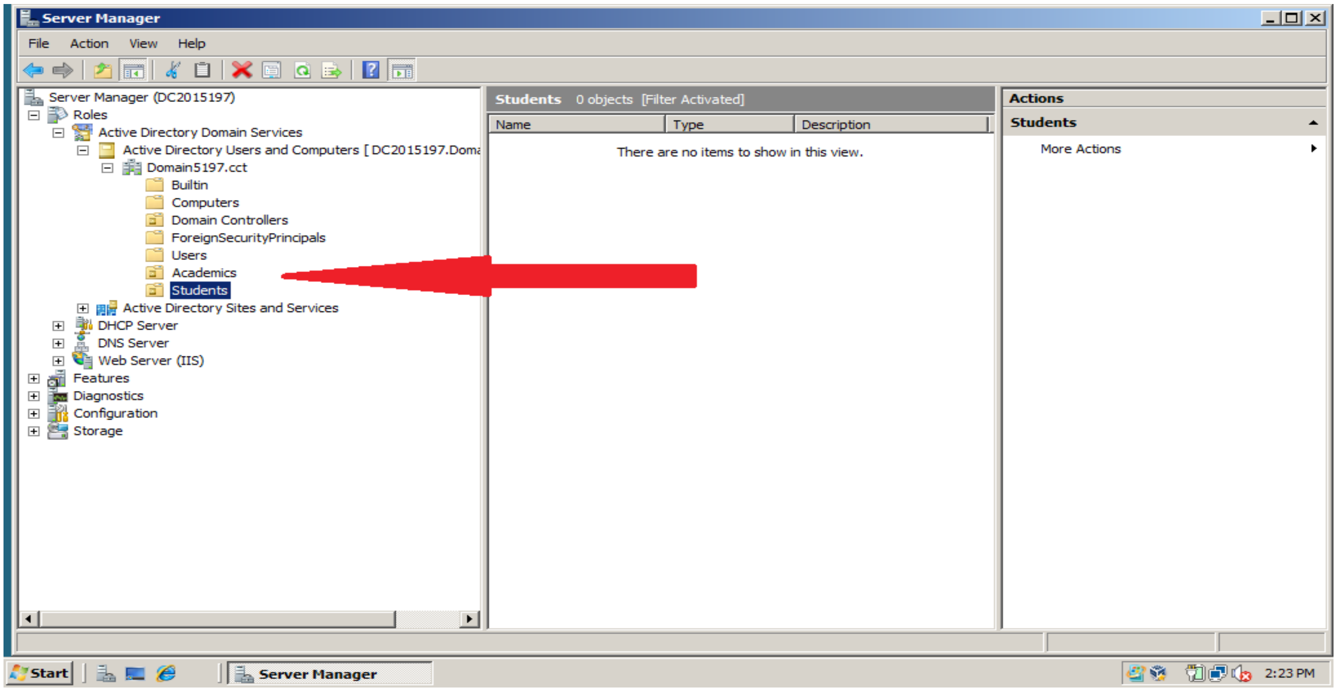
Windows activation

57 day(s) to activate. Activate Windows now
Product ID: 92516-083-1000042-76528

Screenshot: System information.

The screenshot below shows the two organization units Academics and Students.

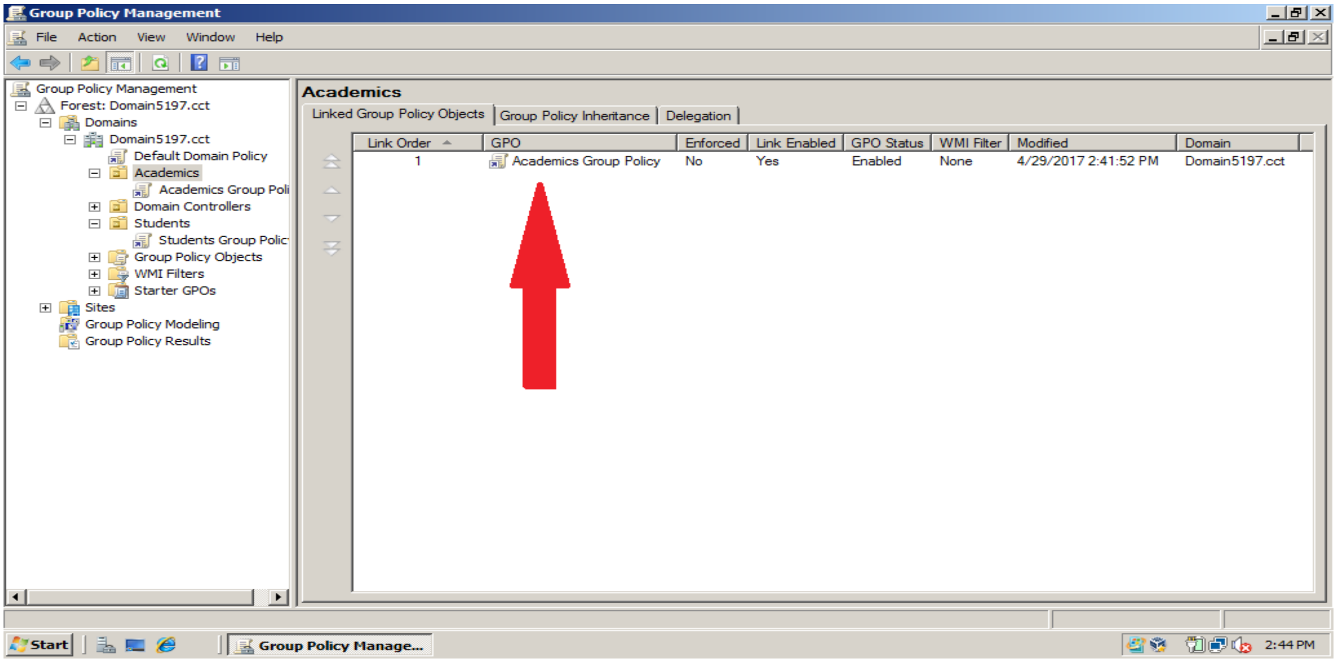
They were created in the Server Manager into the Domain5197.cct.



There are no items to show in this view.

Screenshot: Academics and Students Organizational units.

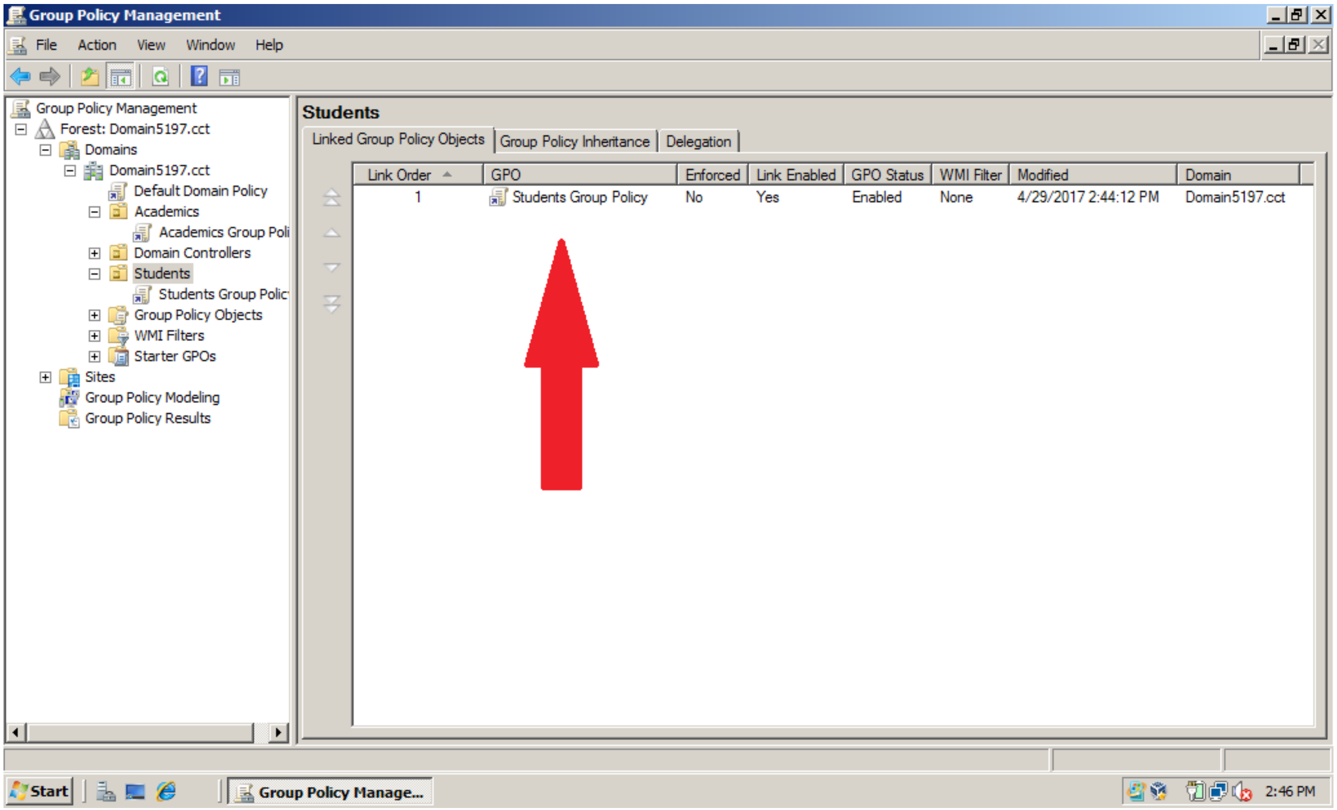
Also in the next screenshot shows that the Academics Group Policy have been created.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Academics Group Policy	No	Yes	Enabled	None	4/29/2017 2:41:52 PM	Domain5197.cct

Screenshot: Academics Group Policy.

In the screenshot below, the Students group policy is also set.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Students Group Policy	No	Yes	Enabled	None	4/29/2017 2:44:12 PM	Domain5197.cct

Screenshot: Students Group Policy.

Analysis of the Organizational units

To implement the group policies, we must identify the needs, computer experiences and corporate security requirements for the Students and Academics Organizational units.

This assessment requires that we chose five modifications on the policy of each group. There is no previous policies to those groups, and also the requirements does not specify which changes should be done. So based on best practices when designing group policies the Default Domain Policy will be kept as it is, because there are basic solutions to protect the domain controller.

The required changes that will be made are local, that means the system is more protected, because each group have to be analyzed, so for each group, the changes will be different. The list of changes are very big and a proper solution will not modify all of it , but will select the ones that will cover the group needs.

Goals

The goals of this assessment is to create a policy for each organizational unit that will let them work on their own tasks and generally protect the system against any inappropriate use, that could be conscious or unconscious.

The actions to define the permissions will remove potential harmful and nonessential functionalities for the users.

Settings for ***Academics*** Organizational unit

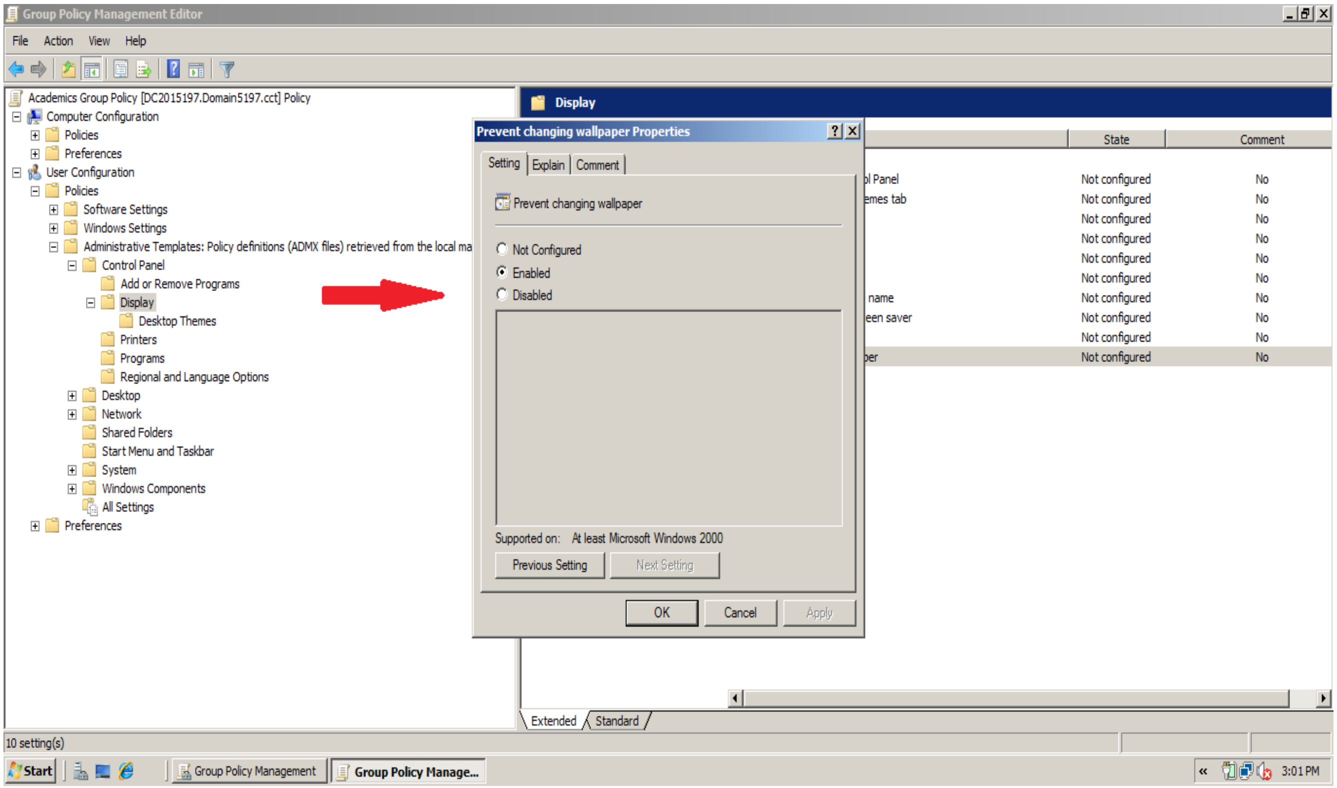
The overview scenario for the Academics Organizational Group is:

- They should have regular access to basic functionalities.
- They may install new components into the system.
- they can not modify the settings to the system, or appearance of the system.

Based on the overview above, a basic restriction to the Academics can be set as:

- **Prevent changing wallpaper.**

For this setting the user will have access to the desktop tab but, all the options of the tab will be disabled. so the user will not be able to change the wallpaper of the computer. This setting helps the company to keep a standard, where all the computer could have a specific wallpaper to be shown.



Prevent changing wallpaper Properties

Setting | Explain | Comment

Prevent changing wallpaper

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Microsoft Windows 2000

Previous Setting | Next Setting

OK | Cancel | Apply

	State	Comment
ol Panel	Not configured	No
emes tab	Not configured	No
	Not configured	No
	Not configured	No
	Not configured	No
	Not configured	No
name	Not configured	No
een saver	Not configured	No
	Not configured	No
per	Not configured	No

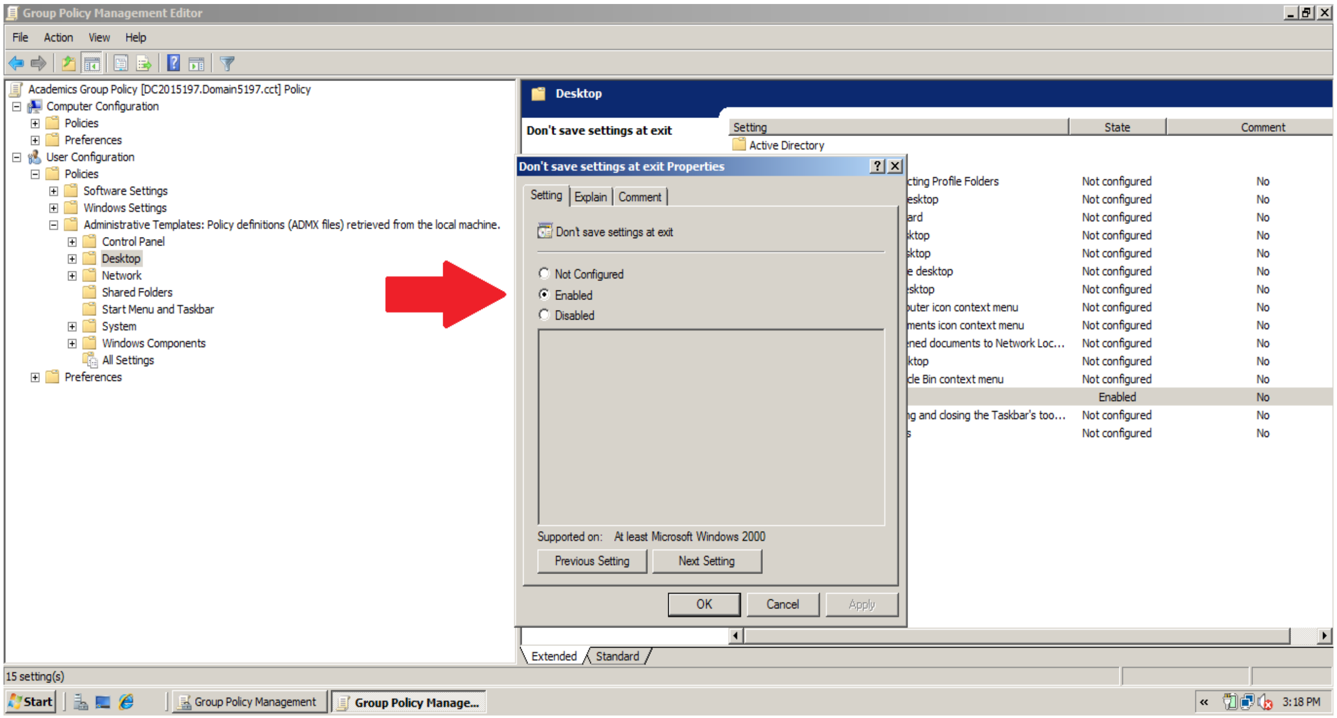
Screenshot: Academics Group Policy(Prevent changing wallpaper).

- Don't save settings at exit.

This setting allows the user to change the desktop, but some settings, such as the position of open windows or the size and position of the taskbar, are not saved when users log off. however shortcuts placed on the desktop are always saved.

Again this is a setting to control the appearance of the system and it will help to keep the system nice and simple.

Configuring the system to be always organized could help the user to be more productive, because the user will know already where to find what they want into the system.



Don't save settings at exit

Don't save settings at exit Properties

Don't save settings at exit

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Microsoft Windows 2000

Setting	State	Comment
cting Profile Folders	Not configured	No
esktop	Not configured	No
ard	Not configured	No
ktop	Not configured	No
sktop	Not configured	No
e desktop	Not configured	No
sktop	Not configured	No
uter icon context menu	Not configured	No
ments icon context menu	Not configured	No
ned documents to Network Loc...	Not configured	No
ktop	Not configured	No
cle Bin context menu	Not configured	No
	Enabled	No
g and closing the Taskbar's too...	Not configured	No
s	Not configured	No

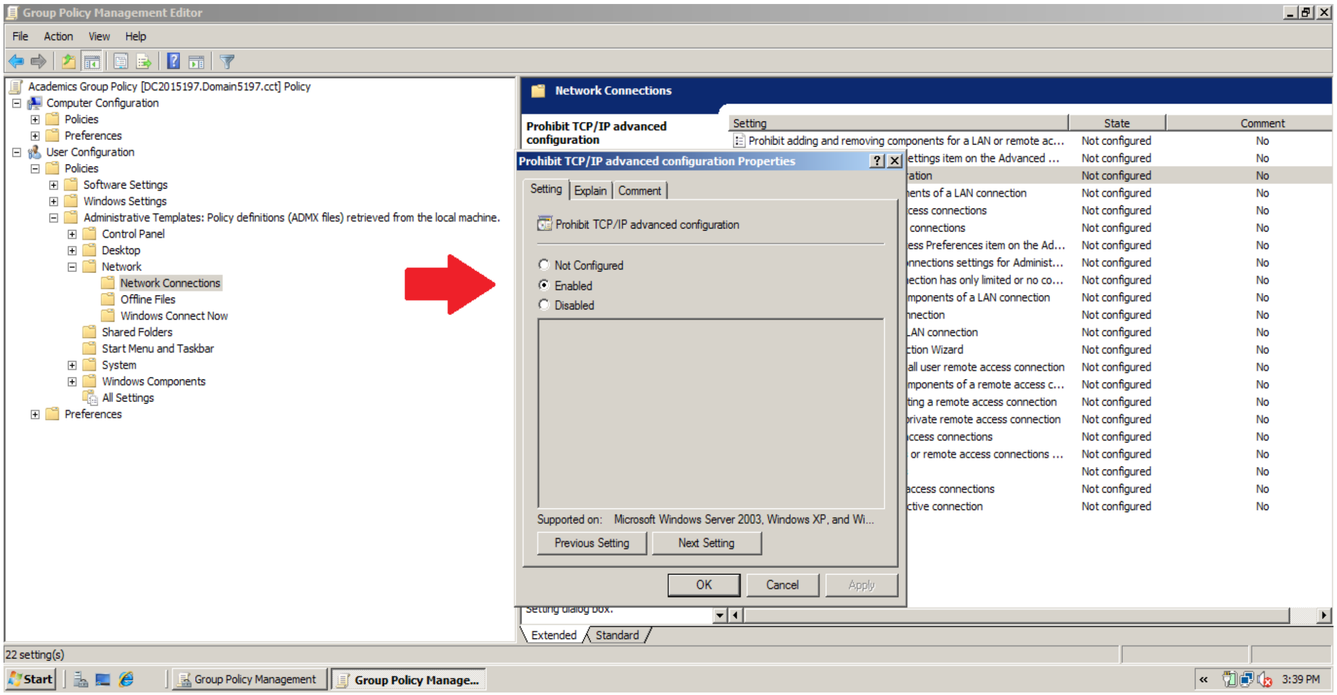
Screenshot: Academics Group Policy(Don't save settings at exit).

- Prohibit TCP/IP advanced configuration.

The setting below as enabled will protect the TCP/IP advanced configuration, that means the users will no longer be able to change the TCP/IP address, DNS address or windows setting at that tab.

By blocking those addresses, the system will be protected, so the user will not do any mistake and disconnect the computer from the network or modify the address without permission.

this setting is a also a security setting, because there is no chance to the user change the address of the machine or try to access other DNS if exists.



Prohibit TCP/IP advanced configuration

Setting	State	Comment
Prohibit adding and removing components for a LAN or remote ac...	Not configured	No
ettings item on the Advanced ...	Not configured	No
ation	Not configured	No
ents of a LAN connection	Not configured	No
cess connections	Not configured	No
connections	Not configured	No
ess Preferences item on the Ad...	Not configured	No
nnections settings for Administ...	Not configured	No
ection has only limited or no co...	Not configured	No
mponents of a LAN connection	Not configured	No
nnection	Not configured	No
LAN connection	Not configured	No
ction Wizard	Not configured	No
all user remote access connection	Not configured	No
mponents of a remote access c...	Not configured	No
ting a remote access connection	Not configured	No
rivate remote access connection	Not configured	No
ccess connections	Not configured	No
or remote access connections ...	Not configured	No
	Not configured	No
access connections	Not configured	No
ctive connection	Not configured	No

Prohibit TCP/IP advanced configuration Properties

Setting | Explain | Comment

Prohibit TCP/IP advanced configuration

○ Not Configured
● Enabled
○ Disabled

Supported on: Microsoft Windows Server 2003, Windows XP, and Wi...

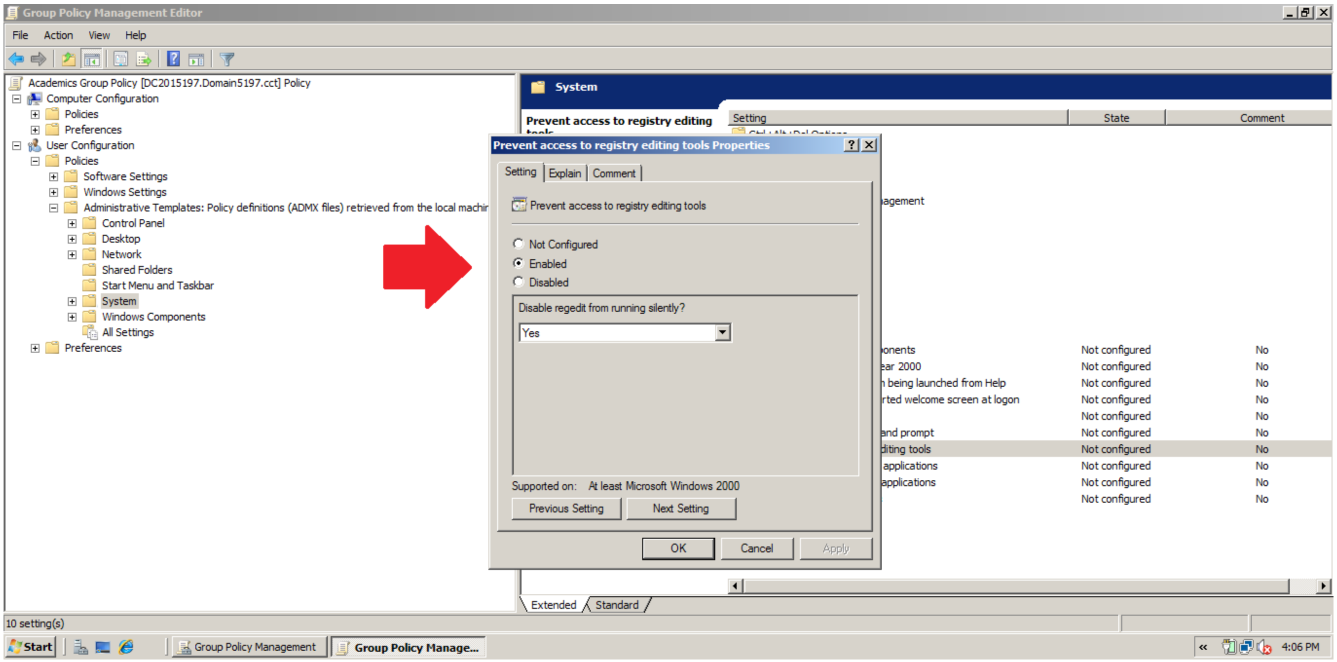
Previous Setting | Next Setting

OK | Cancel | Apply

Screenshot: Academics Group Policy(Prohibit TCP/IP advanced configuration).

- Prevent access to registry editing tools.

The setting below will prevent the user to have access to the Registry editing tools. This action will keep the system stable, because the Registry have all the values to calculate how the system will operate, so if any of those values will be changed, the system could stop working.



Prevent access to registry editing tools Properties

Setting | Explain | Comment

Prevent access to registry editing tools

○ Not Configured
● Enabled
○ Disabled

Disable regedit from running silently? Yes

Supported on: At least Microsoft Windows 2000

Previous Setting | Next Setting

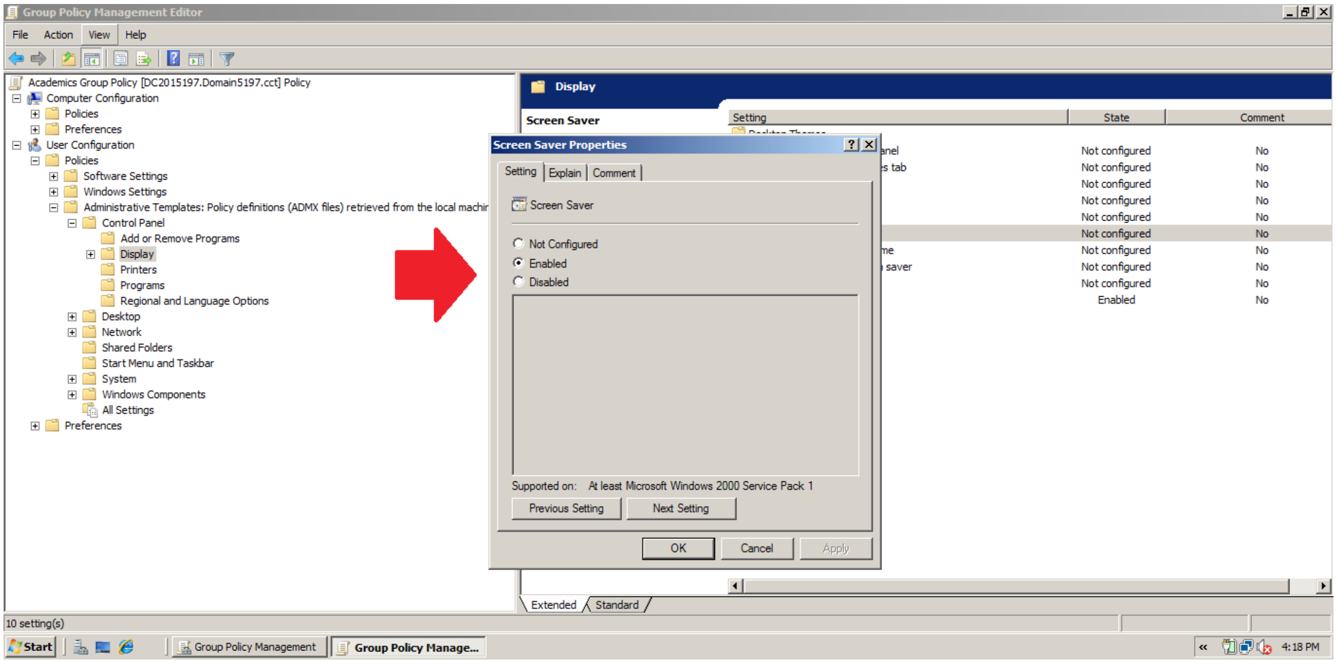
OK | Cancel | Apply

Setting	State	Comment
agement		
onents	Not configured	No
ear 2000	Not configured	No
n being launched from Help	Not configured	No
rted welcome screen at logon	Not configured	No
	Not configured	No
and prompt	Not configured	No
diting tools	Not configured	No
applications	Not configured	No
applications	Not configured	No
	Not configured	No

Screenshot: Academics Group Policy(Prevent access to registry editing tools).

- Screen Saver.

This setting will block any screen saver to run. It will also make the system looks simple and professional, the user will no long change or install Screen savers that should not be running. This actions also prevent the system against virus that are into those kind of software. Because if the users know that the screen savers do not run, they will not try to install any screen saver that could be from a unknown developer.



Screen Saver Properties

Setting | Explain | Comment

Screen Saver

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Microsoft Windows 2000 Service Pack 1

Previous Setting | Next Setting

OK | Cancel | Apply

Setting	State	Comment
Desktop Themes		
anel	Not configured	No
s tab	Not configured	No
	Not configured	No
	Not configured	No
	Not configured	No
	Not configured	No
me	Not configured	No
saver	Not configured	No
	Not configured	No
	Enabled	No

Screenshot: Academics Group Policy(Screen Saver).

Settings for ***<u>Students</u>*** Organizational unit

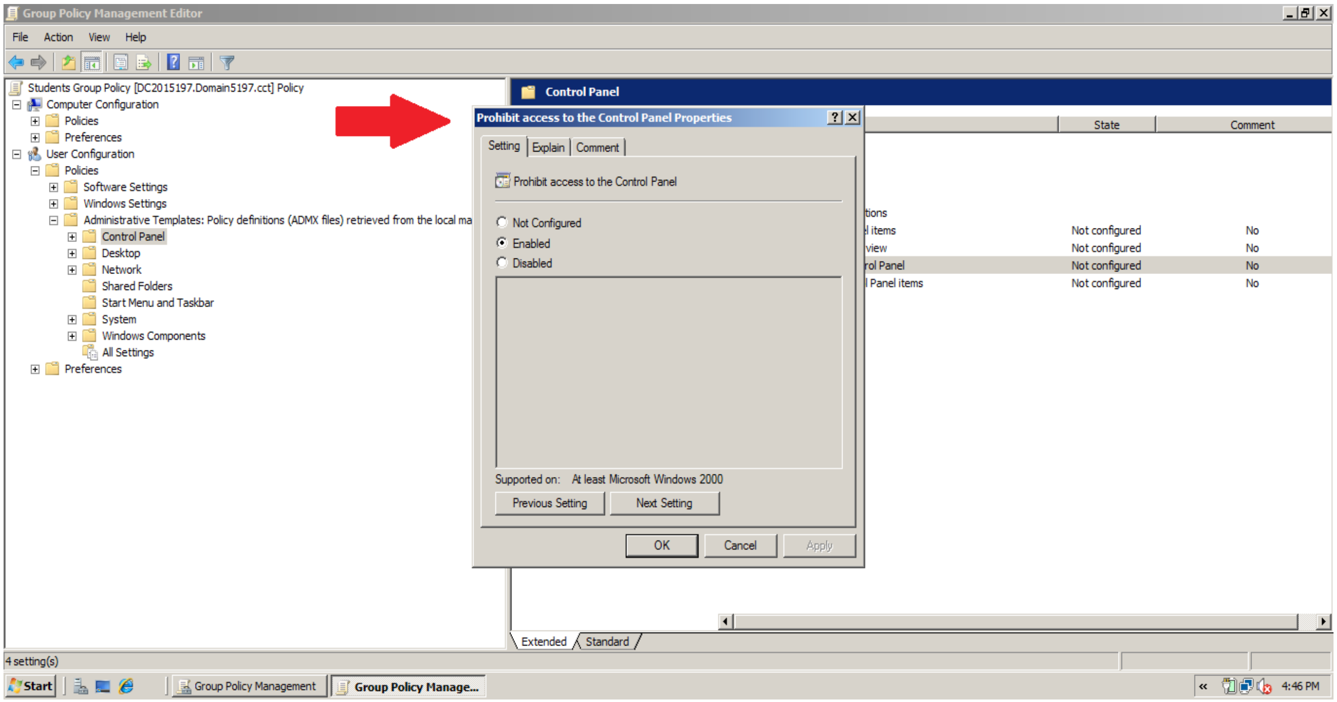
The overview scenario for the Students Organizational unit is:

- Student's information should be private, so personal information should be deleted.
- Students should not modify the system or its appearance.
- Students should not access the control panel.

Based on the overview above, a basic restriction to the Academics can be set as:

- Prohibit access to the Control Panel.

This setting will prohibit the users to access the control panel, this is a security action and also keeps the system simple and organized, allowing any user to keep the productivity while using the system. with this setting the user can not access tools to modify the system of personalize the system.



Students Group Policy [DC2015197.Domain5197.cct] Policy
- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX files) retrieved from the local ma
      - Control Panel
      - Desktop
      - Network
      - Shared Folders
      - Start Menu and Taskbar
      - System
      - Windows Components
      - All Settings
  - Preferences

Prohibit access to the Control Panel Properties

Setting | Explain | Comment

Prohibit access to the Control Panel

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Microsoft Windows 2000

Previous Setting | Next Setting

OK | Cancel | Apply

	State	Comment
tions		
l items	Not configured	No
view	Not configured	No
rol Panel	Not configured	No
l Panel items	Not configured	No

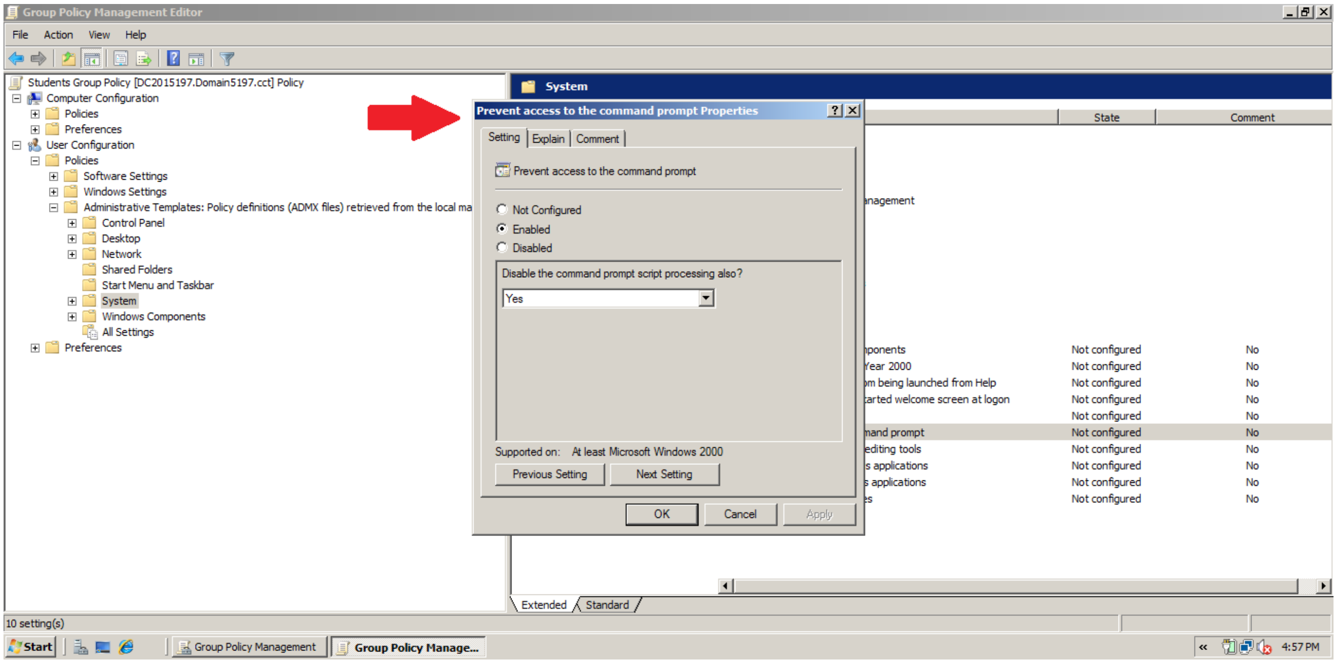
4 setting(s)

Screenshot: Students Group Policy(Prohibit access to the Control Panel).

- Prevent access to the command prompt.

This setting prevents the access to the command prompt. By this configuration the user can not access or modify the system by the command prompt.

If the administrator of the system is creating a policy to protect the system, the command prompt could be a door of access to make changes on the system, so the only way is to block the access, and just if the students really need the access it can be allowed by the supervision of the Academics.



Students Group Policy [DC2015197.Domain5197.cct] Policy
- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX files) retrieved from the local ma
      - Control Panel
      - Desktop
      - Network
      - Shared Folders
      - Start Menu and Taskbar
      - System
      - Windows Components
      - All Settings
  - Preferences

System

Prevent access to the command prompt Properties

Setting | Explain | Comment

Prevent access to the command prompt

○ Not Configured
● Enabled
○ Disabled

Disable the command prompt script processing also?
Yes

Supported on: At least Microsoft Windows 2000

Previous Setting | Next Setting

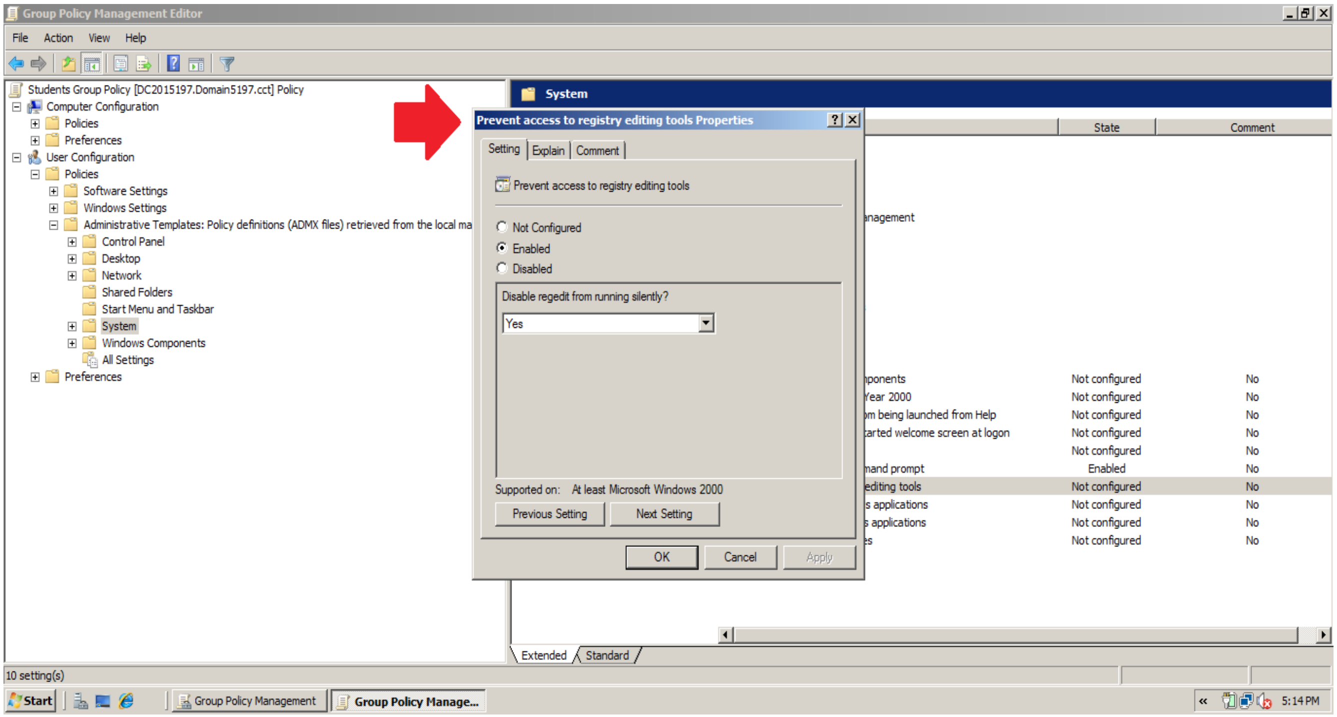
OK | Cancel | Apply

	State	Comment
nagement		
ponents	Not configured	No
Year 2000	Not configured	No
om being launched from Help	Not configured	No
tarted welcome screen at logon	Not configured	No
	Not configured	No
nand prompt	Not configured	No
editing tools	Not configured	No
s applications	Not configured	No
s applications	Not configured	No
es	Not configured	No

Screenshot: Students Group Policy(Prevent access to the command prompt).

- Prevent access to the registry editing tool.

The system should be protected against and changes on the values that calculate the processes to run the operational system, and the students does not have to have access to those values, so, when preventing any access to the registry editing tool, the user will not be able to change any value that could make the system to stop work.



Group Policy Management Editor

Students Group Policy [DC2015197.Domain5197.cct] Policy
- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions (ADMX files) retrieved from the local ma
      - Control Panel
      - Desktop
      - Network
      - Shared Folders
      - Start Menu and Taskbar
      - System
      - Windows Components
      - All Settings
  - Preferences

System

Prevent access to registry editing tools Properties

Setting | Explain | Comment

Prevent access to registry editing tools

○ Not Configured
● Enabled
○ Disabled

Disable regedit from running silently? Yes

Supported on: At least Microsoft Windows 2000

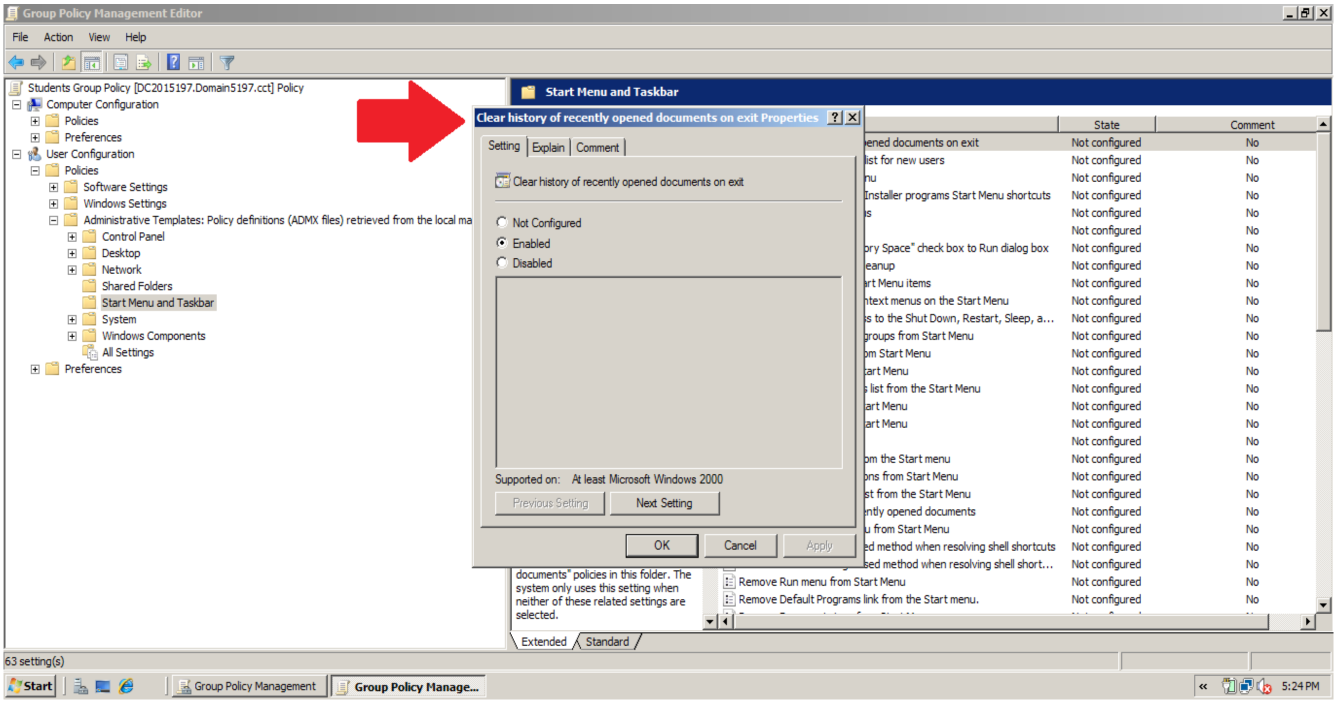
	State	Comment
nagement		
ponents	Not configured	No
Year 2000	Not configured	No
m being launched from Help	Not configured	No
arted welcome screen at logon	Not configured	No
	Not configured	No
mand prompt	Enabled	No
editing tools	Not configured	No
s applications	Not configured	No
s applications	Not configured	No
s	Not configured	No

10 setting(s)

Screenshot: Students Group Policy(Prevent access to the registry editing tool).

- Clear history of recently opened documents on exit.

To protect the privacy of the students, every time that the student logs off, the list of the recent documents in the menu bar will be deleted. So the next student will not see each file the previous student was working with. This is done by enabling the Clear history of recently opened documents on exit.



Clear history of recently opened documents on exit Properties

Clear history of recently opened documents on exit

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Microsoft Windows 2000

documents" policies in this folder. The system only uses this setting when neither of these related settings are selected.

	State	Comment
ened documents on exit	Not configured	No
list for new users	Not configured	No
nu	Not configured	No
Installer programs Start Menu shortcuts	Not configured	No
s	Not configured	No
	Not configured	No
ory Space" check box to Run dialog box	Not configured	No
leanup	Not configured	No
rt Menu items	Not configured	No
ntext menus on the Start Menu	Not configured	No
s to the Shut Down, Restart, Sleep, a...	Not configured	No
groups from Start Menu	Not configured	No
om Start Menu	Not configured	No
art Menu	Not configured	No
s list from the Start Menu	Not configured	No
art Menu	Not configured	No
art Menu	Not configured	No
	Not configured	No
om the Start menu	Not configured	No
ons from Start Menu	Not configured	No
st from the Start Menu	Not configured	No
ntly opened documents	Not configured	No
u from Start Menu	Not configured	No
ed method when resolving shell shortcuts	Not configured	No
sed method when resolving shell short...	Not configured	No
Remove Run menu from Start Menu	Not configured	No
Remove Default Programs link from the Start menu.	Not configured	No

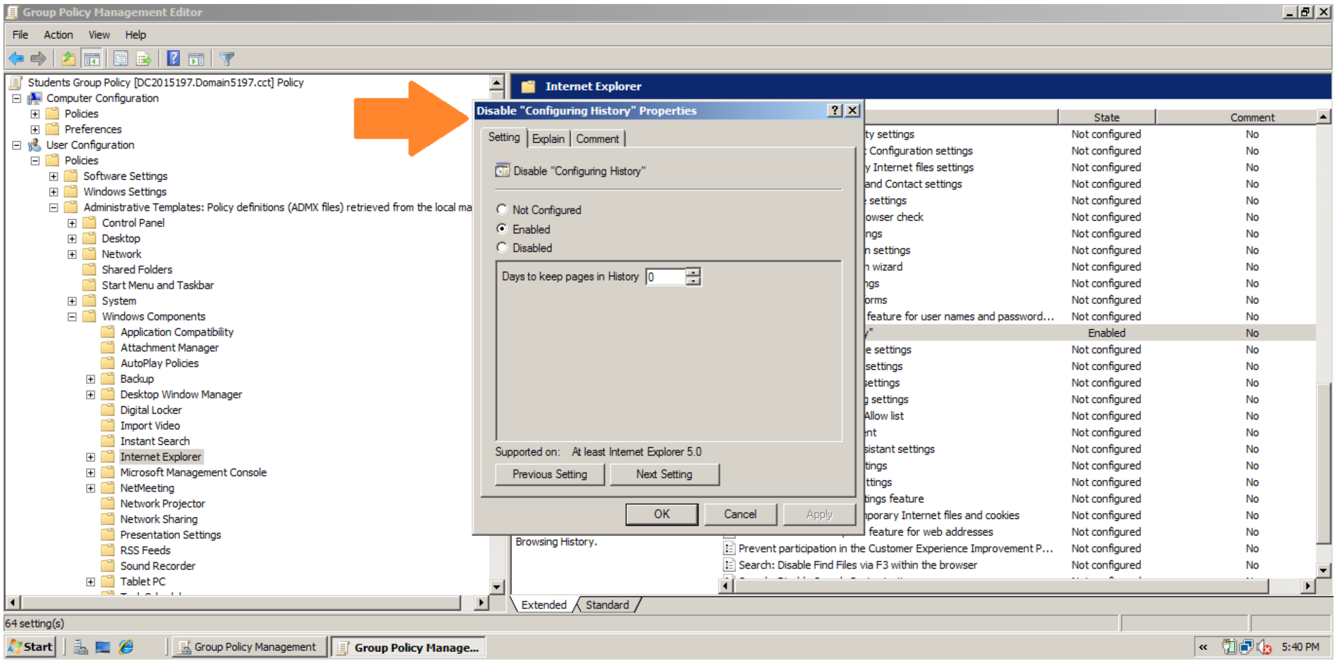
63 setting(s)

Screenshot: Students Group Policy(Clear history of recently opened documents on exit).

- Disable "Configuring History" functionality.

The last setting for the Students Organization Unit is to disable the user to change the configuration of the history of the web pages, this setting also do not allow the user to delete the history of the pages .

As the objective of this policy is to protect the student's privacy, this setting will also configure the days to keep the history to zero, it means that the system will no long keep the history of the web pages, that is a good solution when the computer is shared because the next user will not see what the previous one was doing.



Disable "Configuring History" Properties

Disable "Configuring History"

○ Not Configured
● Enabled
○ Disabled

Days to keep pages in History: 0

Supported on: At least Internet Explorer 5.0

	State	Comment
ty settings	Not configured	No
Configuration settings	Not configured	No
y Internet files settings	Not configured	No
and Contact settings	Not configured	No
settings	Not configured	No
owser check	Not configured	No
ngs	Not configured	No
n settings	Not configured	No
n wizard	Not configured	No
ngs	Not configured	No
orms	Not configured	No
feature for user names and password...	Not configured	No
y"	Enabled	No
e settings	Not configured	No
settings	Not configured	No
settings	Not configured	No
g settings	Not configured	No
Allow list	Not configured	No
nt	Not configured	No
sistant settings	Not configured	No
tings	Not configured	No
ttings	Not configured	No
tings feature	Not configured	No
porary Internet files and cookies	Not configured	No
feature for web addresses	Not configured	No
Prevent participation in the Customer Experience Improvement P...	Not configured	No
Search: Disable Find Files via F3 within the browser	Not configured	No

Screenshot: Students Group Policy(Disable "Configuring History" functionality).

References

Microsoft (2017). Step-by-Step Guide to Understanding the Group Policy Feature Set.Available at: https://msdn.microsoft.com/en-us/library/bb742376.aspx [Accessed on 30th April 2017]

Microsoft (2017). Group Policy Planning and Deployment Guide. Available at: https://technet.microsoft.com/en-us/library/cc754948(v=ws.10).aspx [Accessed on 30th April 2017]

Microsoft (2008). Best Practices for Optimizing Group Policy Performance. Available at:https://technet.microsoft.com/en-us/library/2008.01.gpperf.aspx [Accessed on 30th April 2017]

Microsoft (2017). Group Policy Preferences. Available at: https://technet.microsoft.com/en-us/library/dn581922(v=ws.11).aspx [Accessed on 30th April 2017]

Microsoft (2017). How to prevent and remove viruses and other malware. Available at:https://support.microsoft.com/en-us/help/129972/how-to-prevent-and-remove-viruses-and-other-malware [Accessed on 2nd May 2017]

I hereby declare that all of the work is done by my own.
Ennio da Silva Vitor
ID: 2015197