Practical 4 - Implementing Windows Security Configurations - Part 2

Pre-Requisites

Objectives

- Users and Groups - Creating Groups
- Users and Groups - Creating Users
- Configuring Local Group Policy Objects
- Allow/Deny File Permissions
- **Access Control List** in MS Windows
- Security Configuration in MS Windows
- Account Management in MS Windows & **Active Directory Services**

Exercise 1
Remove "student" account from [Administrators] group
Create a Group [IT2524] and add "student" to this group

Exercise 2
Create another User <PublicUser> and add into [IT2524] group

Exercise 3
"student" is unable to change System Time
Using Local Group Policy Editor (gpedit.msc), set policy to allow group [IT2524] to change System Time → student should be able to change System Time

Exercise 4
Set policy so as to deny login for [IT2524] group → "student" is unable to login

Exercise 5
To deny "student" to use notepad.exe, add "student" to group [IT2524], then set notepad.exe Permissions to Deny [IT2524] from Read & Execute

Exercise 6
Use of **cacls** command to grant or deny access to files and folders.

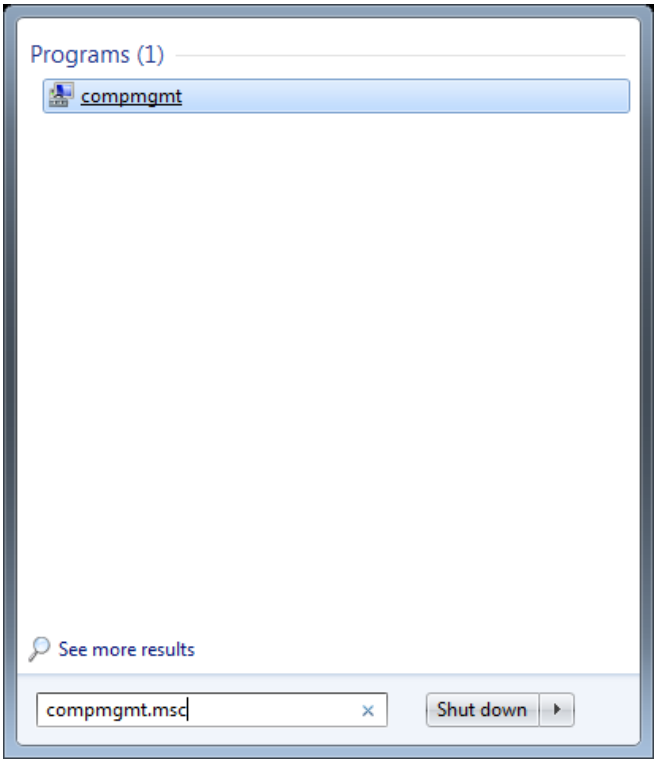
Exercise 7
Use of **secedit** command to check for compliance with security policy against a template.

Exercise 8
Write a Powershell script file to create accounts for a group of users
Write a Powershell script file to add these accounts to the Guest group
Write a Powershell script file to delete the group of accounts

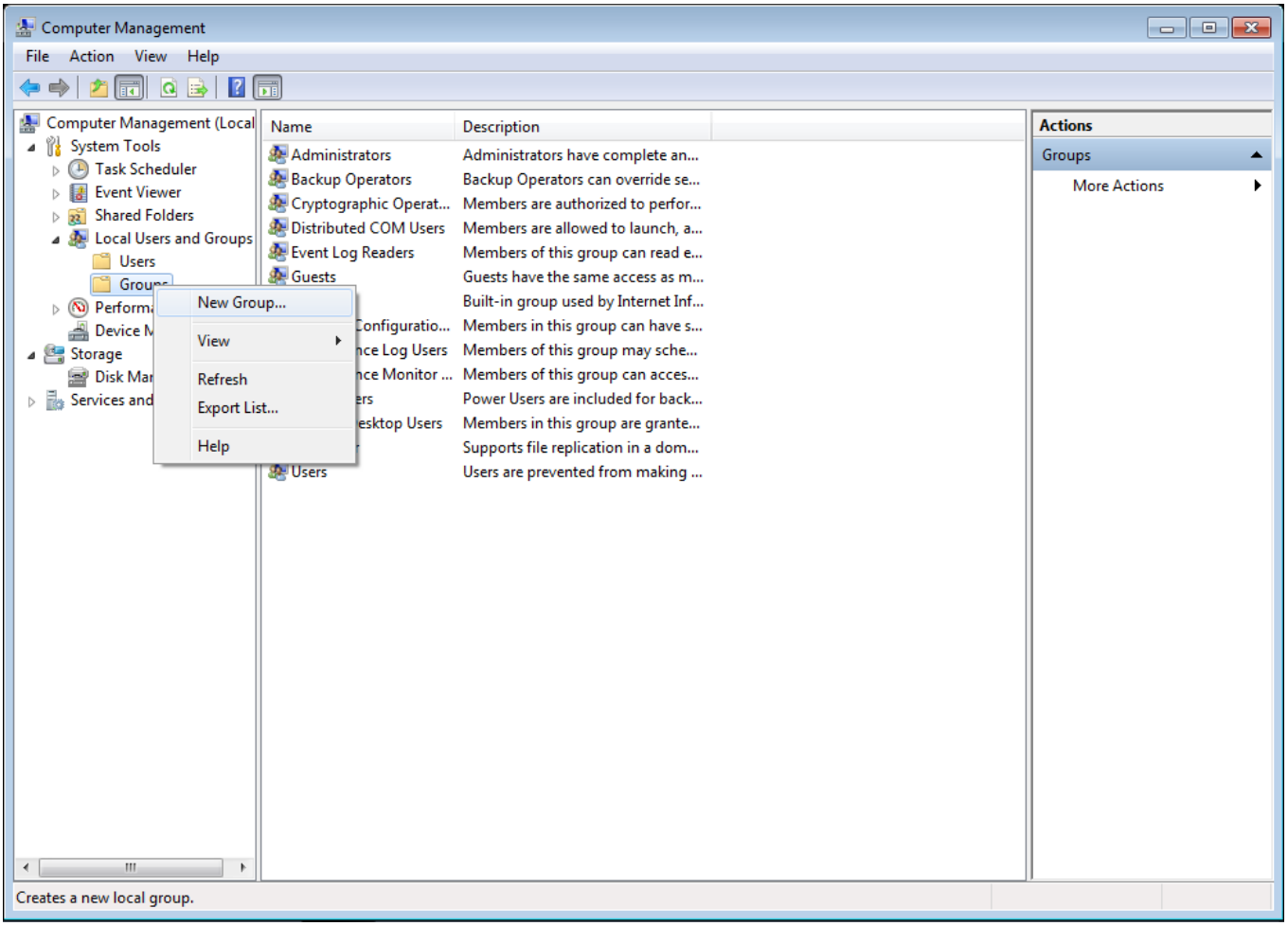
You will need Administrator rights to do this practical. Therefore, you will need to use VMWare Workstation or Player to run a virtual image of Windows, giving you administrator rights.

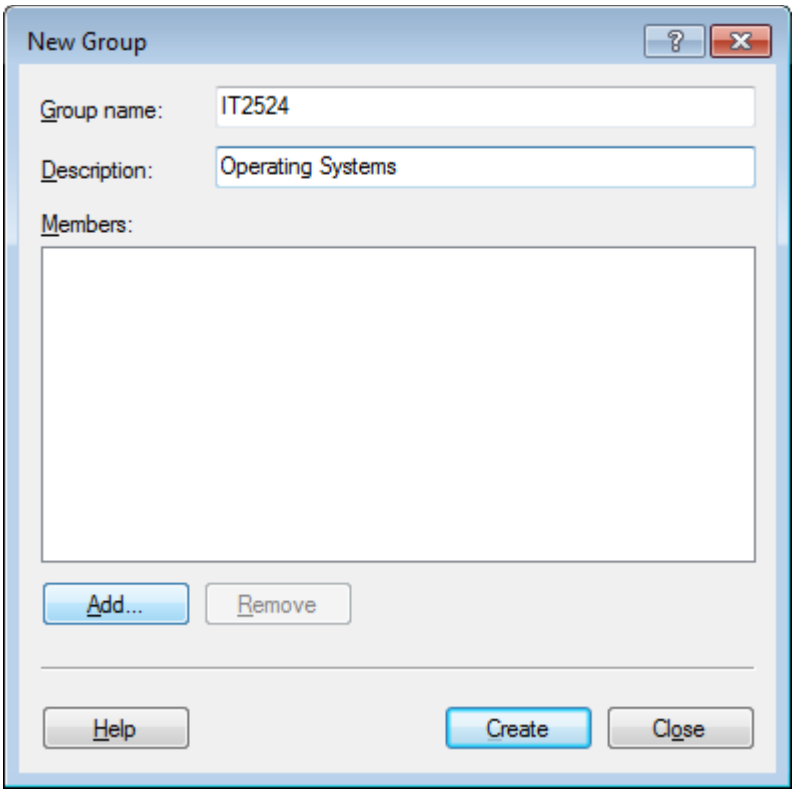
Exercise 1 - Users and Groups - Creating Groups

1. Login as SIT and run the compmgmt.msc command as shown.

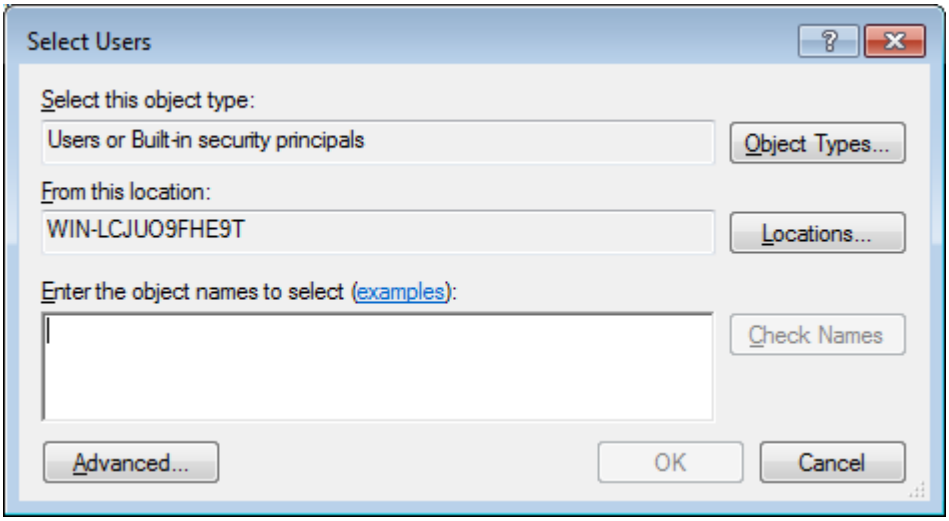


Right click on the "Local Users and Groups" -> "Groups" and select the "New Group …" option.

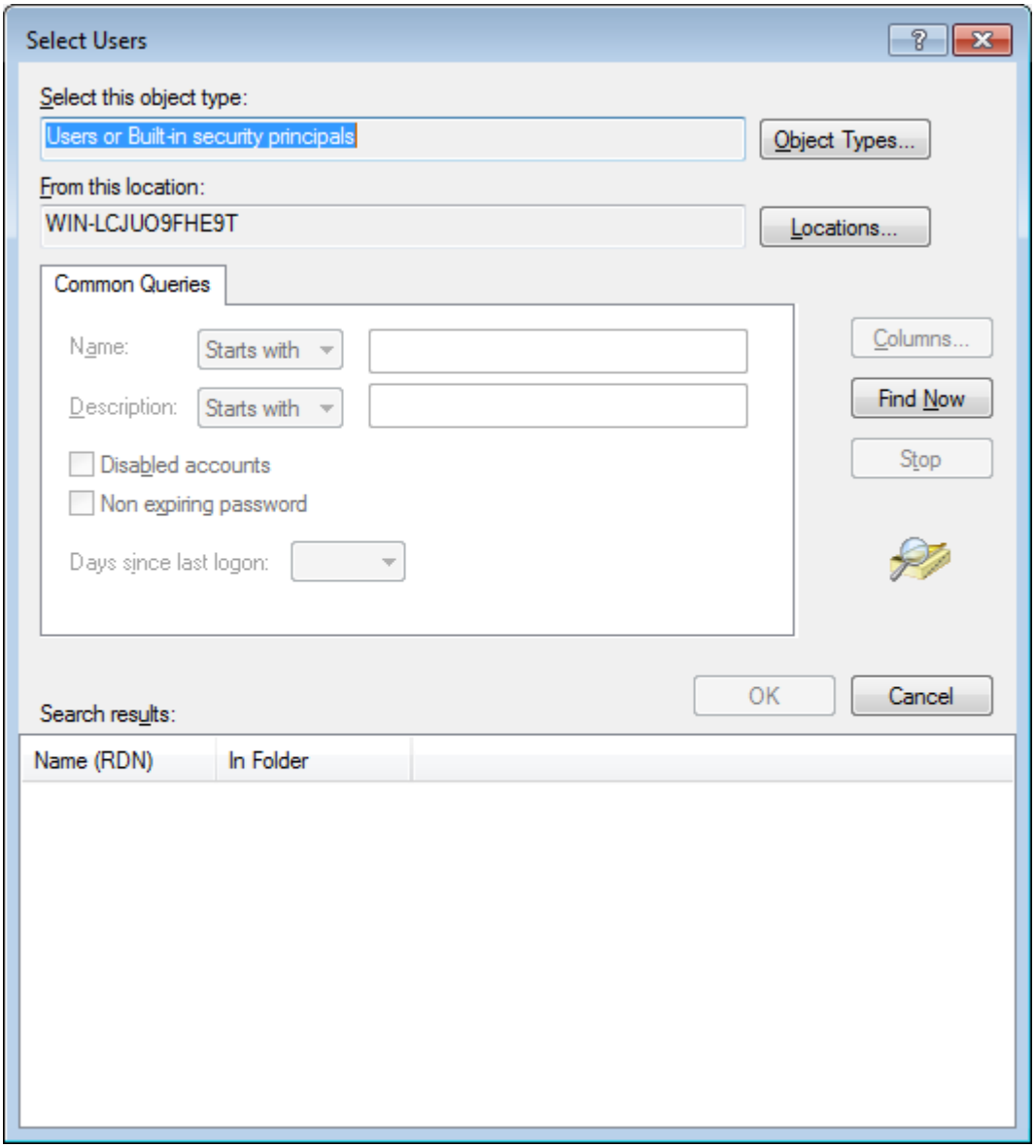

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Storage
Services and
Name
Description
Administrators
Administrators have complete an...
Backup Operators
Backup Operators can override se...
Cryptographic Operat...
Members are authorized to perfor...
Distributed COM Users
Members are allowed to launch, a...
Event Log Readers
Members of this group can read e...
Guests
Guests have the same access as m...
Built-in group used by Internet Inf...
Members in this group can have s...
Members of this group may sche...
Members of this group can acces...
Power Users are included for back...
Members in this group are grante...
Supports file replication in a dom...
Users
Users are prevented from making ...
New Group...
View
Refresh
Export List...
Help
Actions
Groups
More Actions
Creates a new local group.


New Group
Group name:
IT2524
Description:
Operating Systems
Members:
Add...
Remove
Help
Create
Close

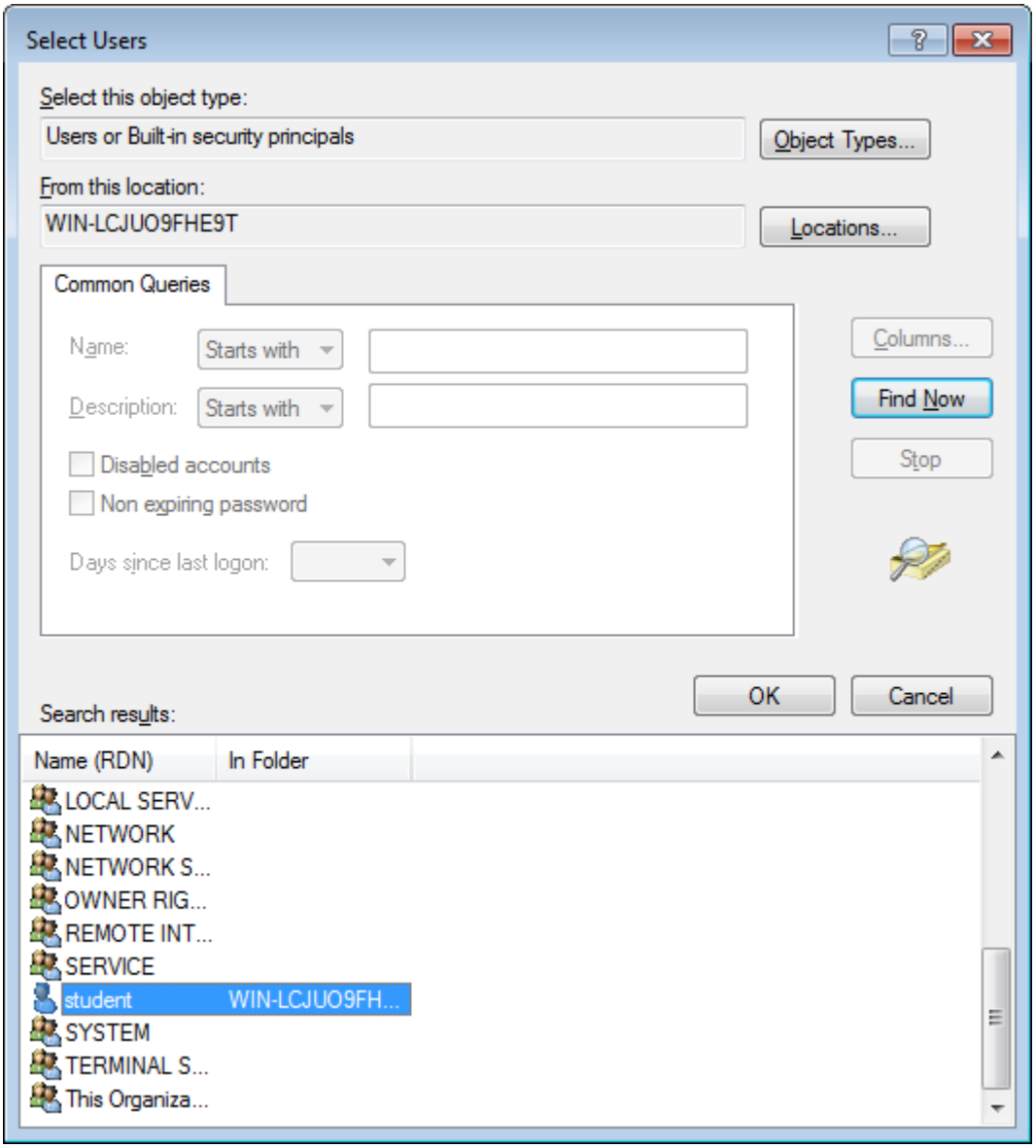
Click on the Add button to add users to the IT2524 group.



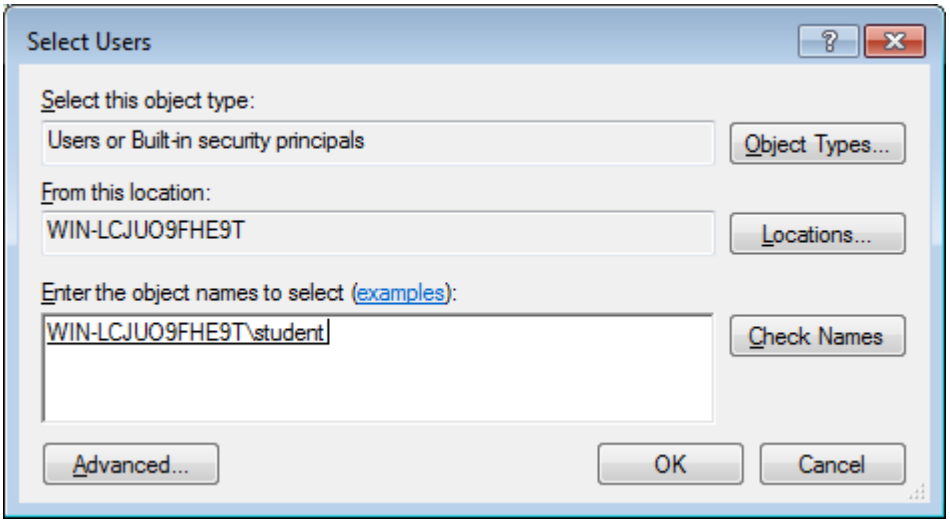
Click on the Advanced button.



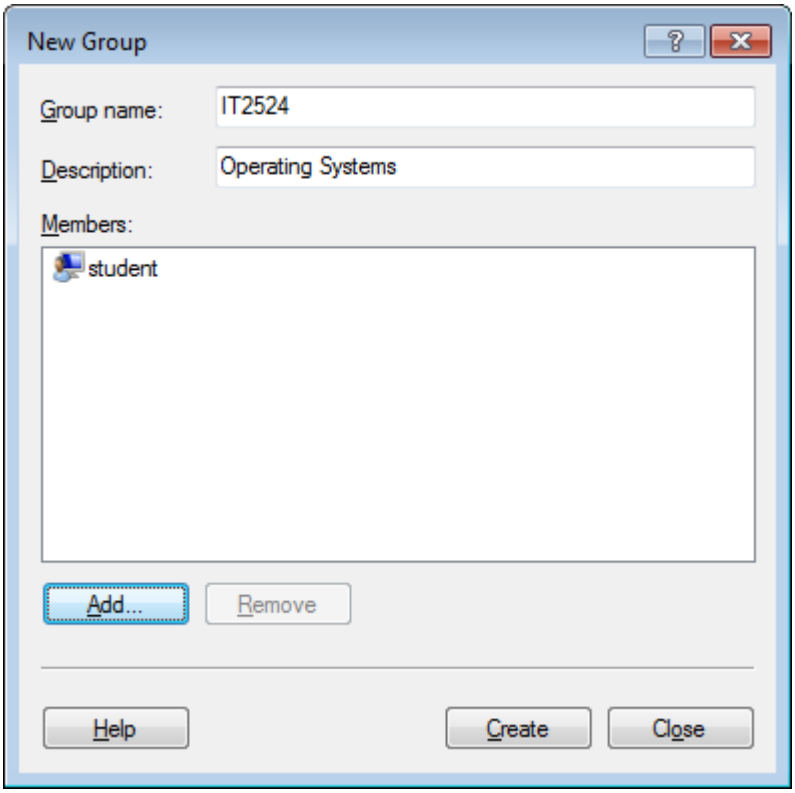
Click on the "Find Now" button.



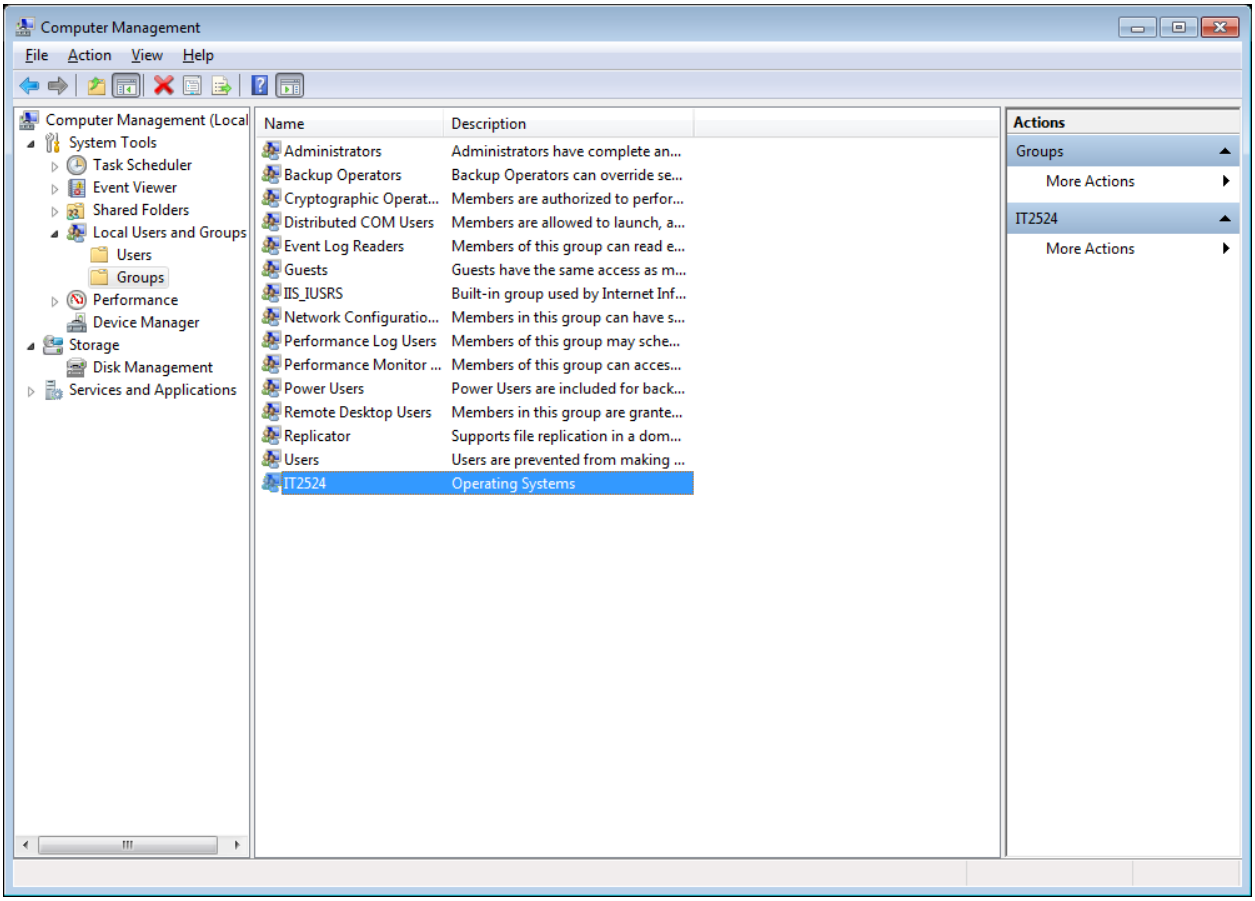
Locate the user id "student" and click the OK button to add the user to the IT2524 group.



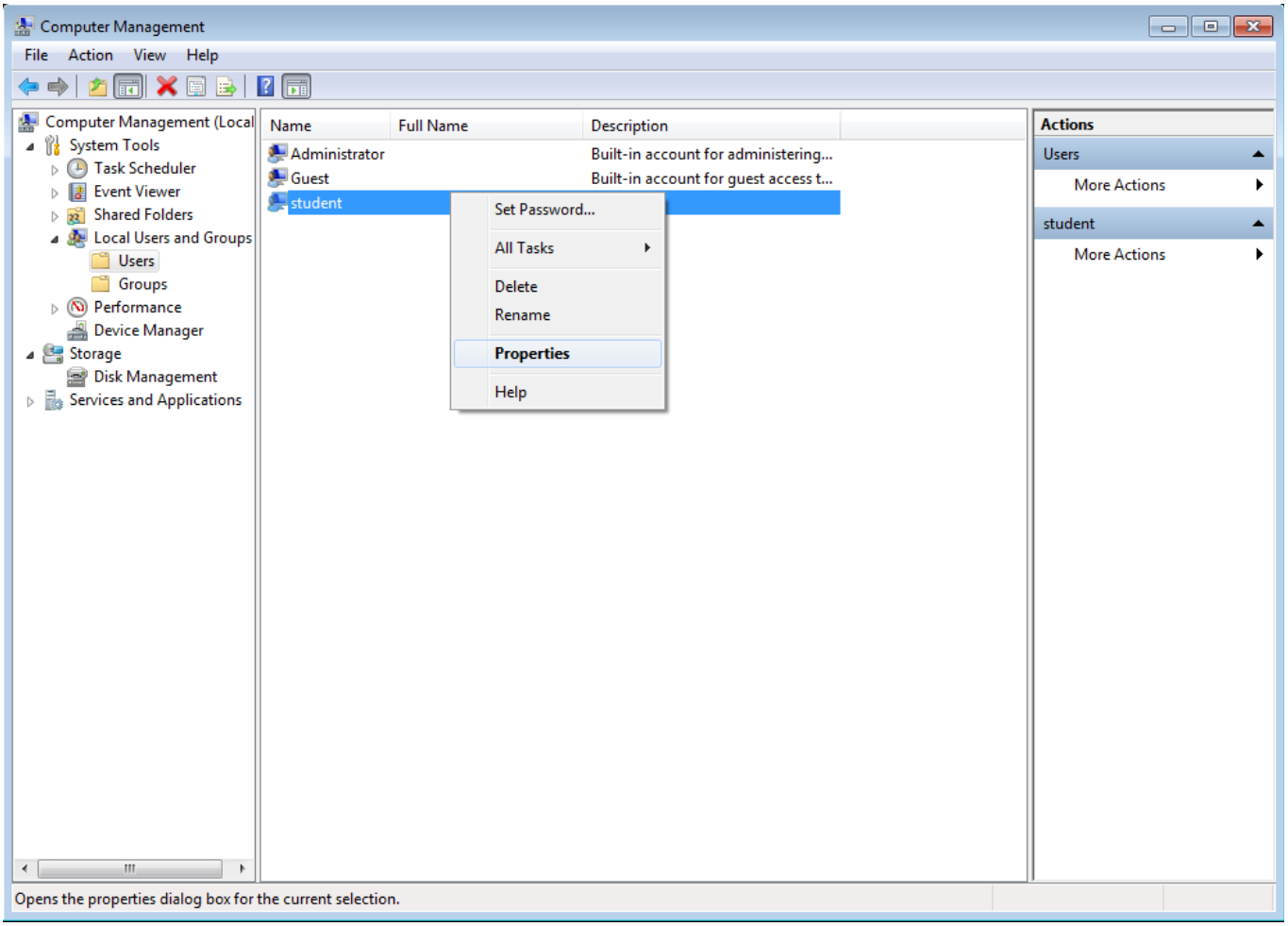
Click the OK button when you are done.

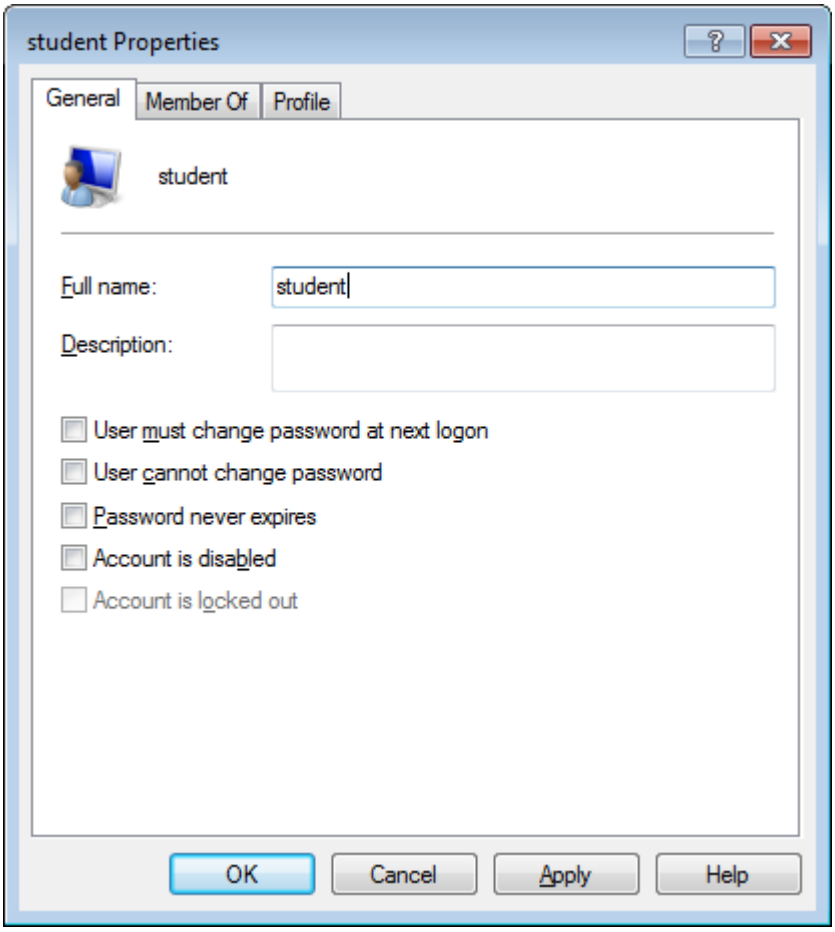


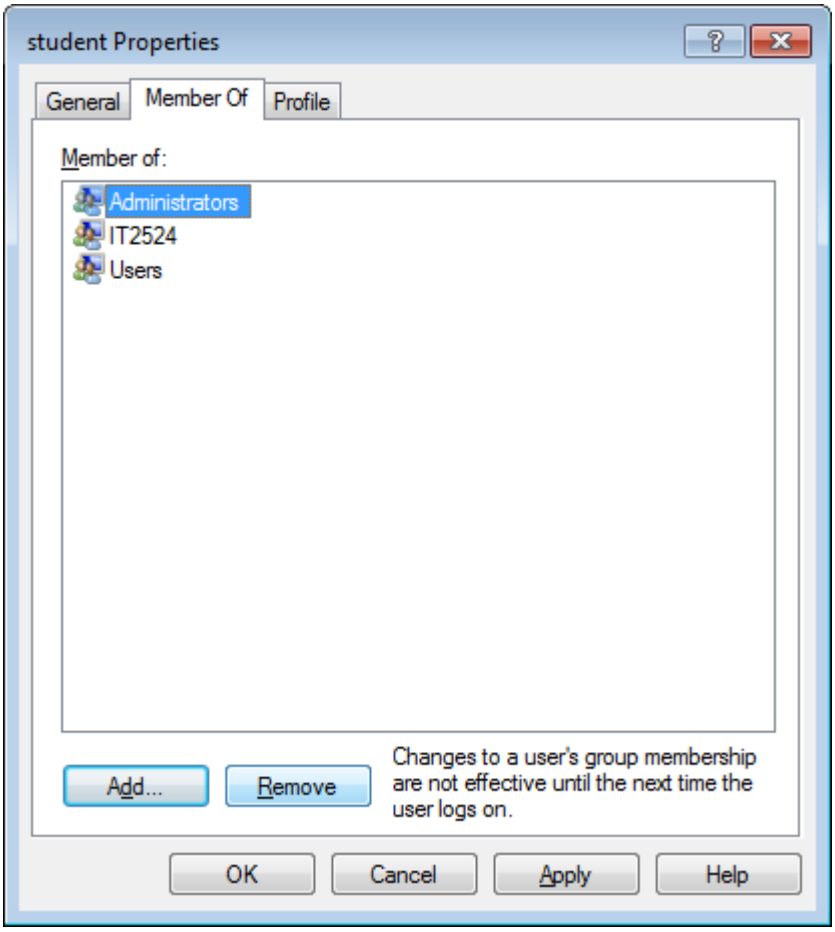
Click the Create button to create the IT2524 group. Click the Close button to close the dialog window when you are done.



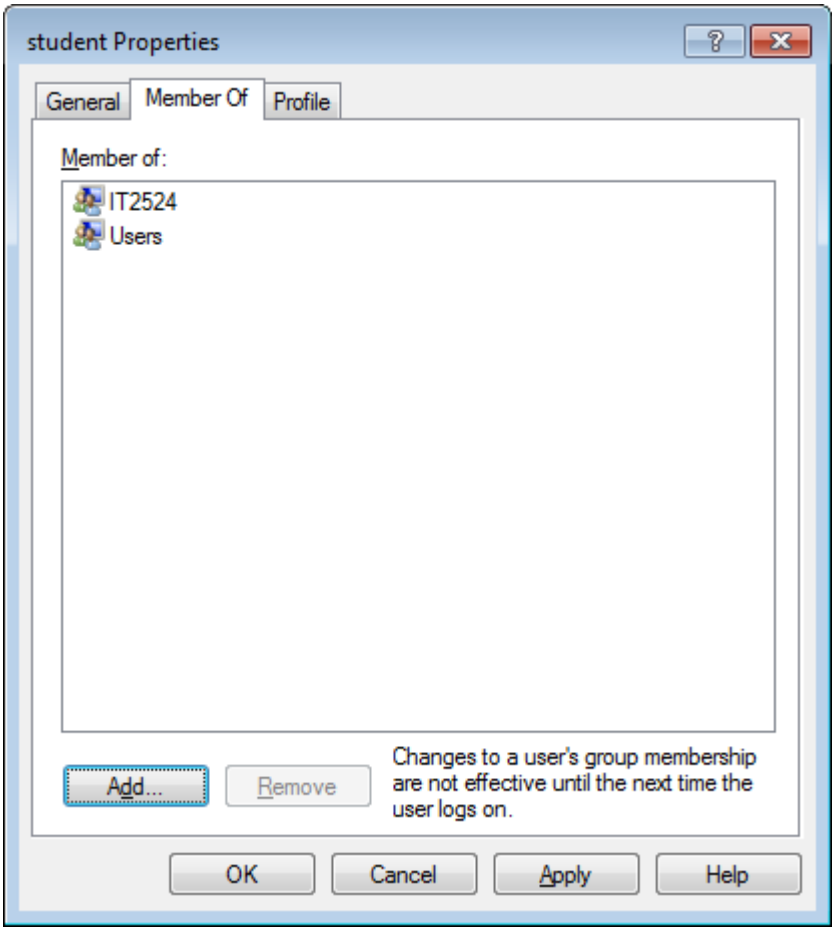
Select "Local Users and Groups" -> "User". Follow the steps as shown to remove the Administrator role from the user student.


Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
Guest
Built-in account for guest access t...
student
Set Password...
All Tasks
Delete
Rename
Properties
Help
Actions
Users
More Actions
student
More Actions
Opens the properties dialog box for the current selection.


student Properties
General
Member Of
Profile
student
Full name:
student
Description:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Account is locked out
OK
Cancel
Apply
Help



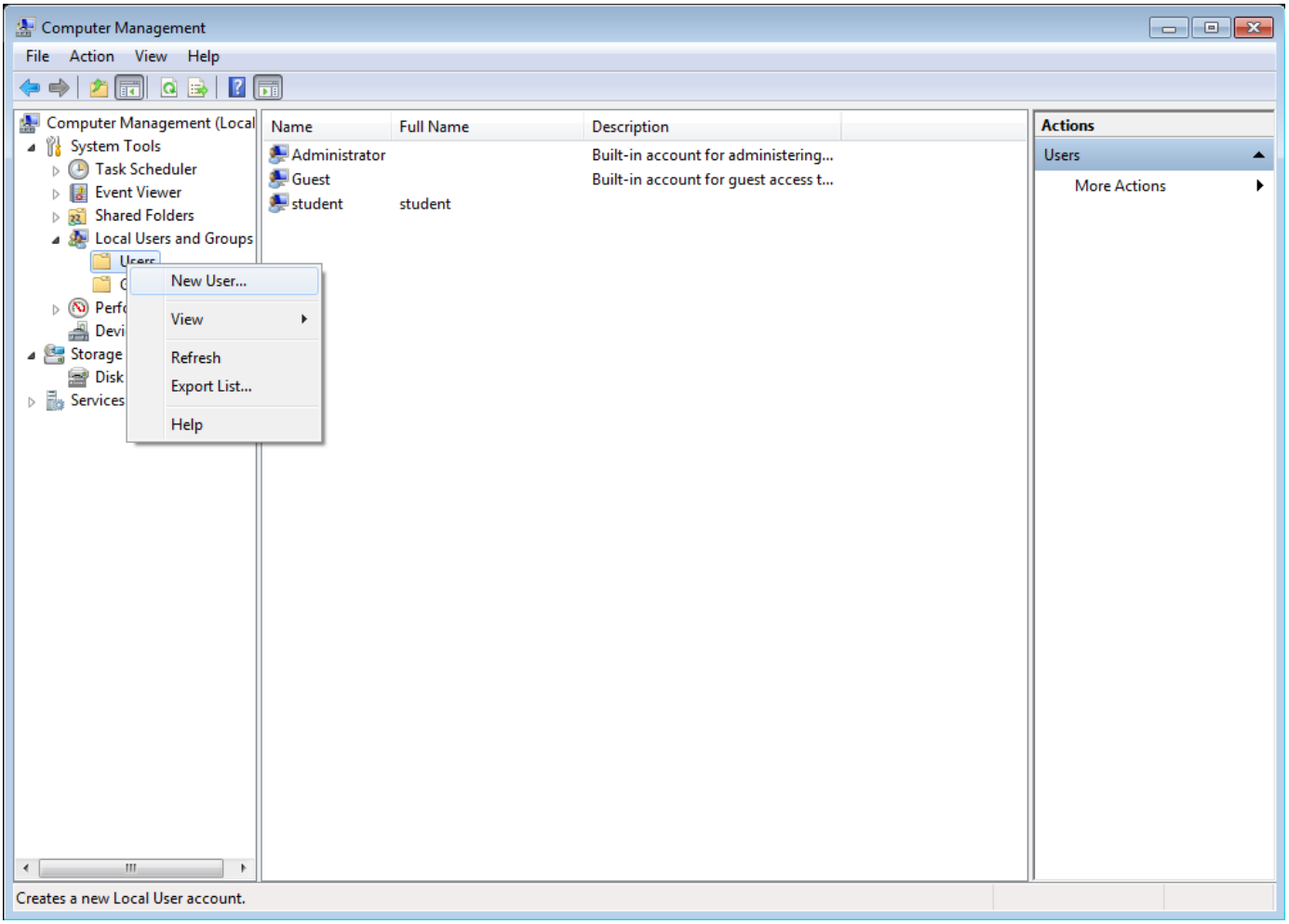
Select “Administrators” and click on the remove button.

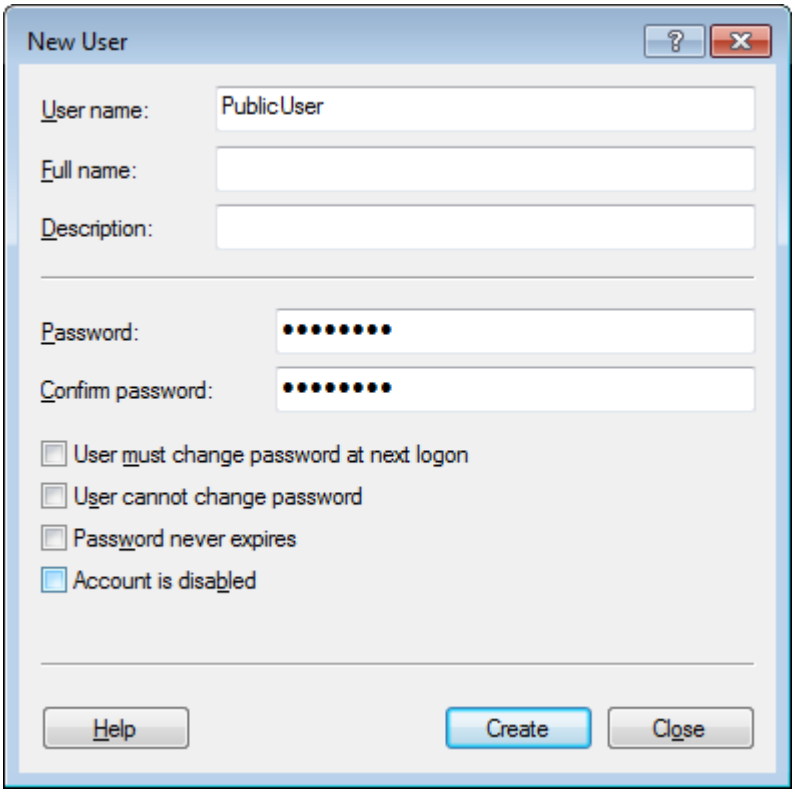


Click on the Apply button and then the OK button to close the dialog window.

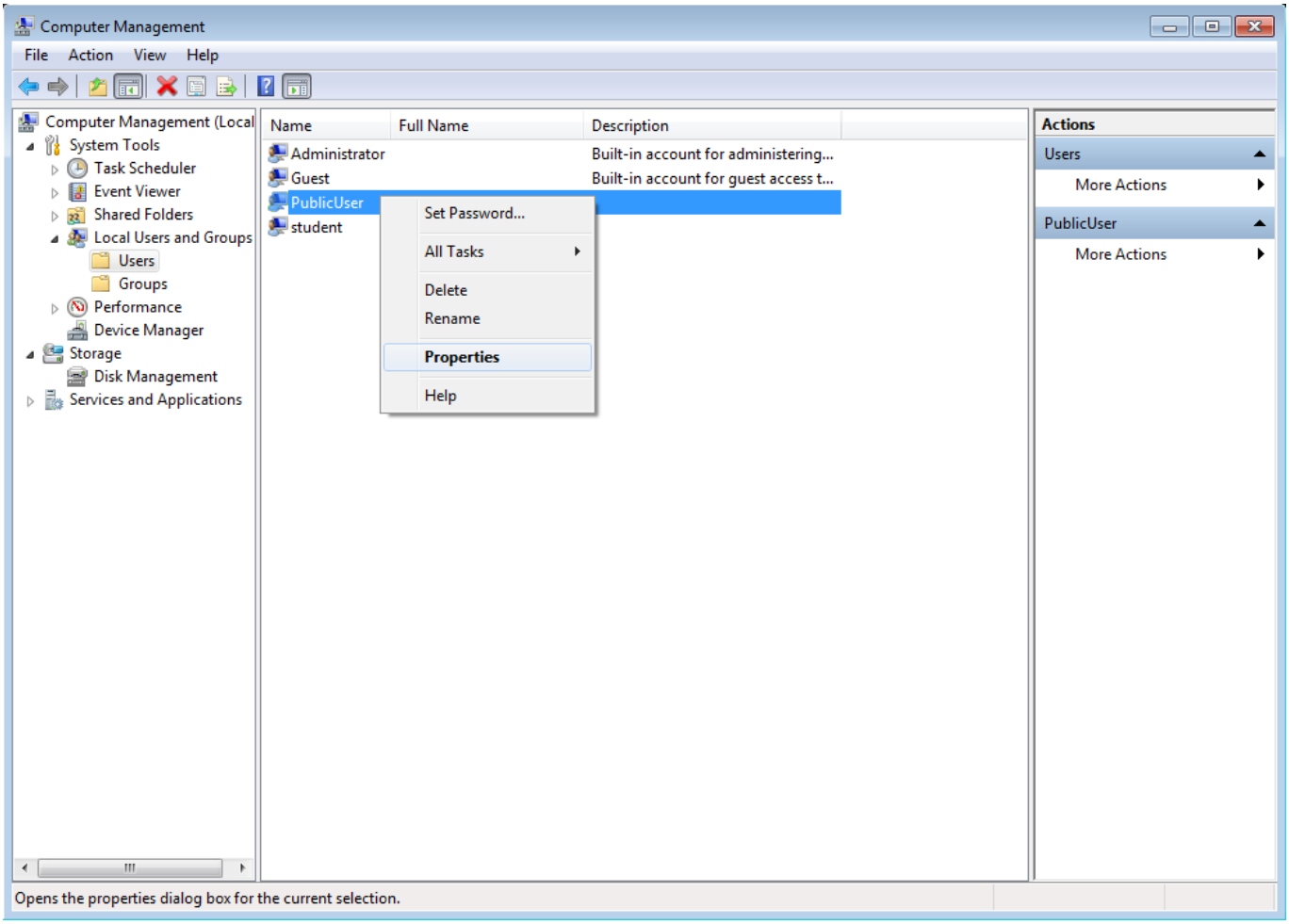
Exercise 2 - Users and Groups - Creating Users

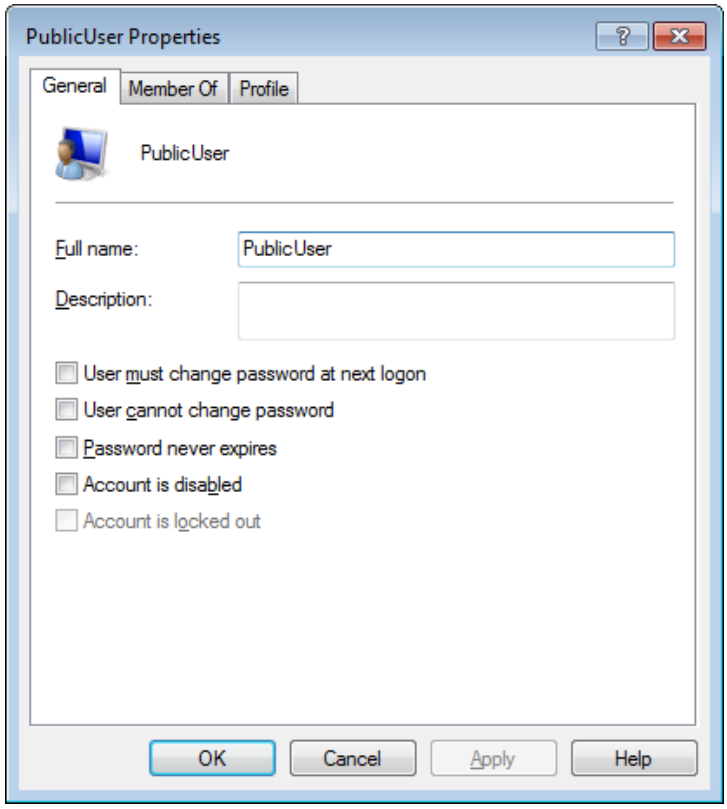
1. Follows the steps as shown to create a new user account. Name the user account as "PublicUser" and assign it only to the IT2524 group.

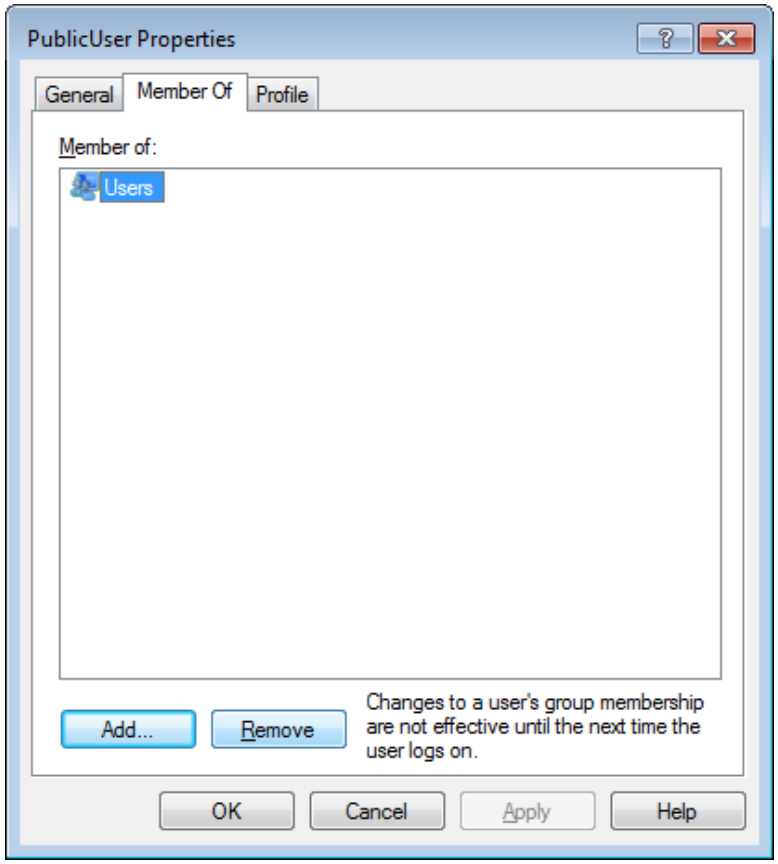




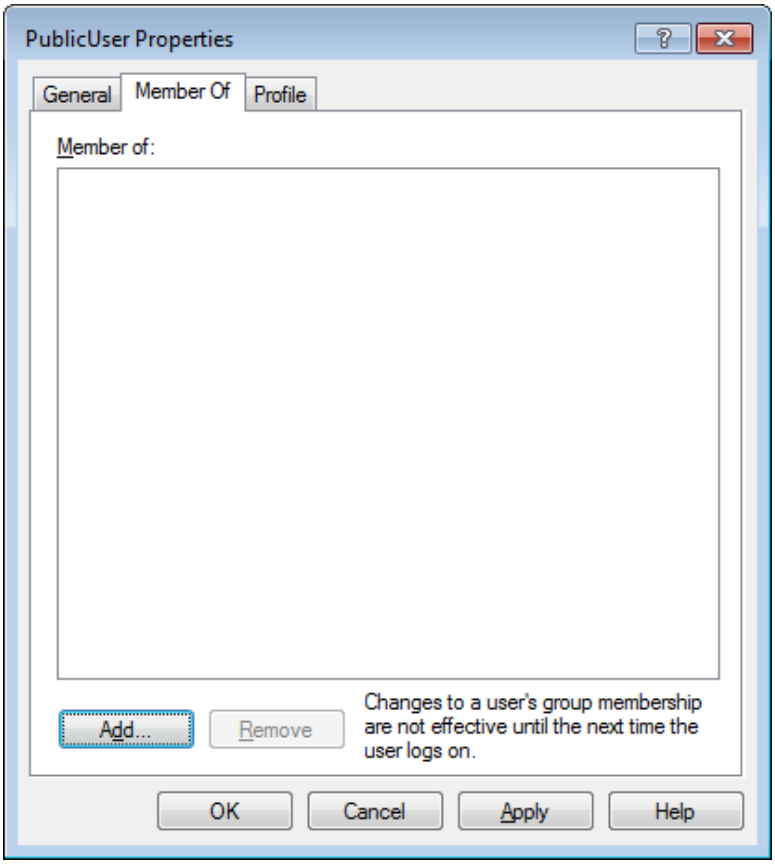
For ease of recall, use the password **P@ssw0rd**. Click on the Create button to create the user and click on the Close button when you are done.


Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
Guest
Built-in account for guest access t...
PublicUser
student
Set Password...
All Tasks
Delete
Rename
Properties
Help
Actions
Users
More Actions
PublicUser
More Actions
Opens the properties dialog box for the current selection.

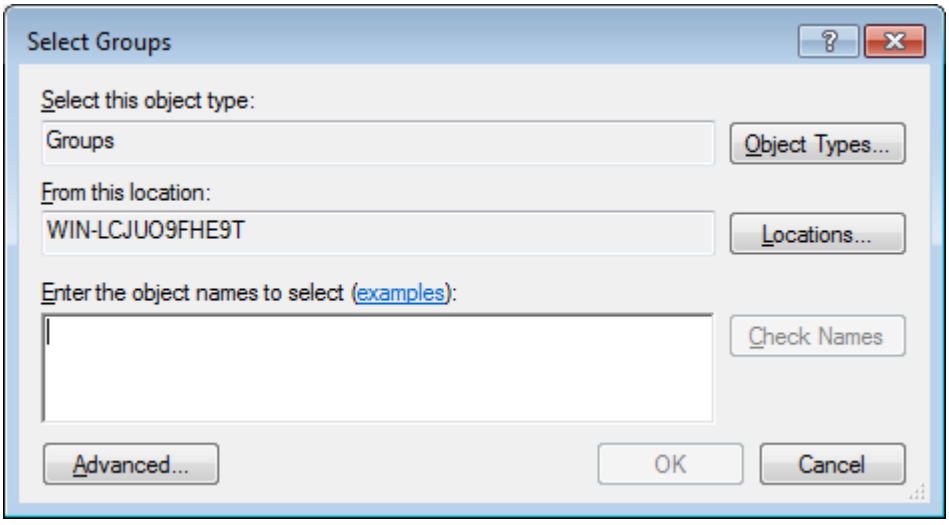




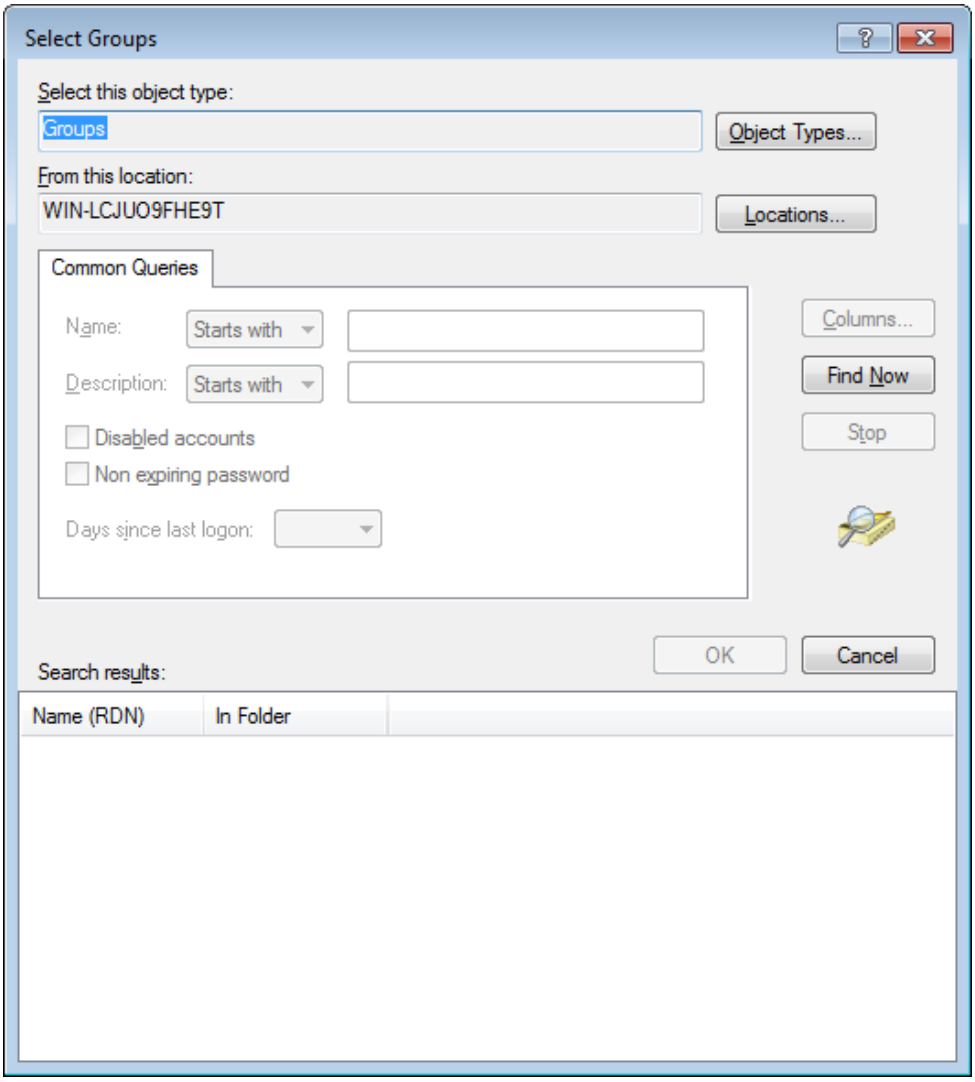
Click on the Remove button to remove PublicUser from the Users group.

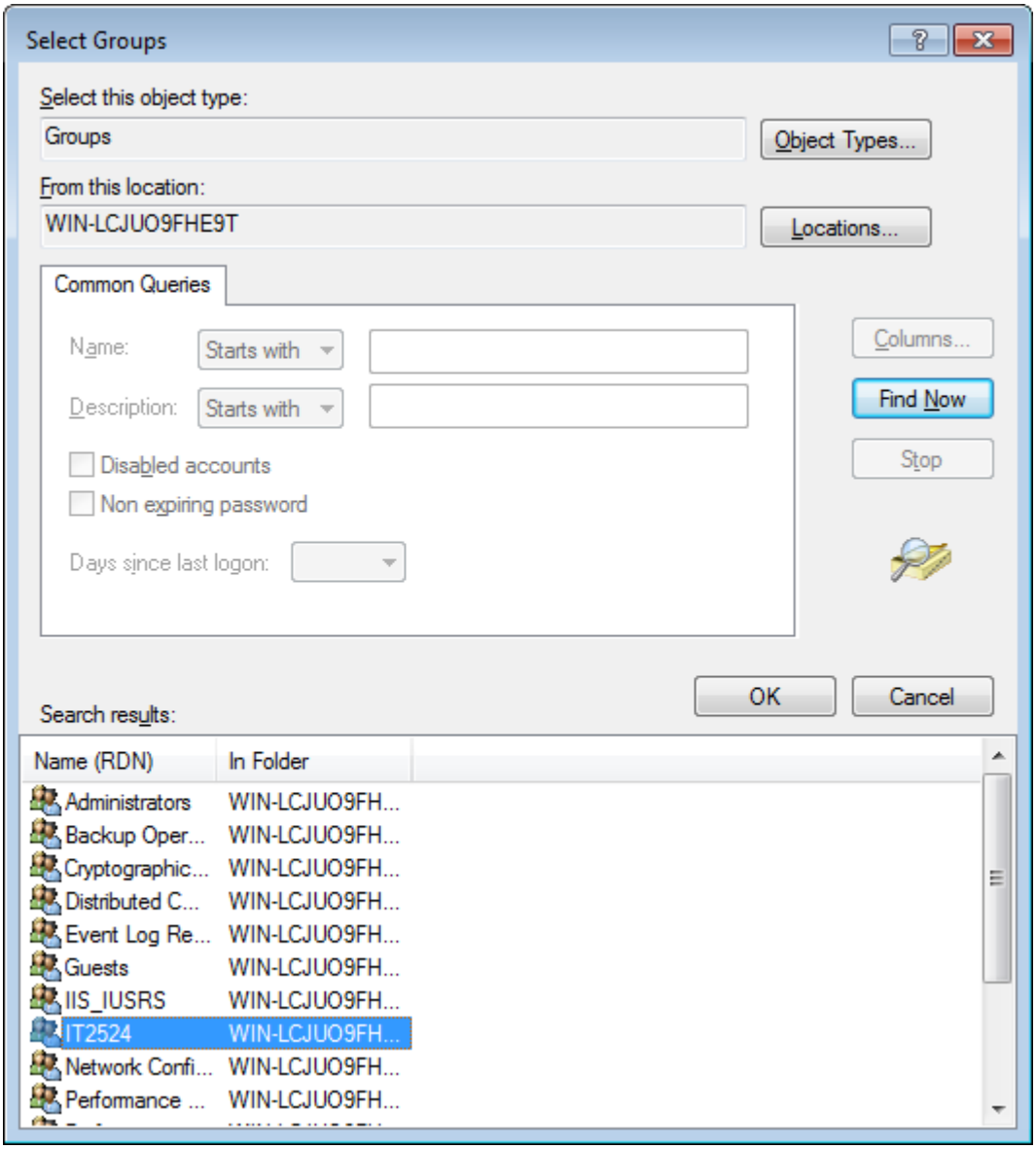


Click 'Add'
Follow the steps as shown to add PublicUser to the IT2524 group.

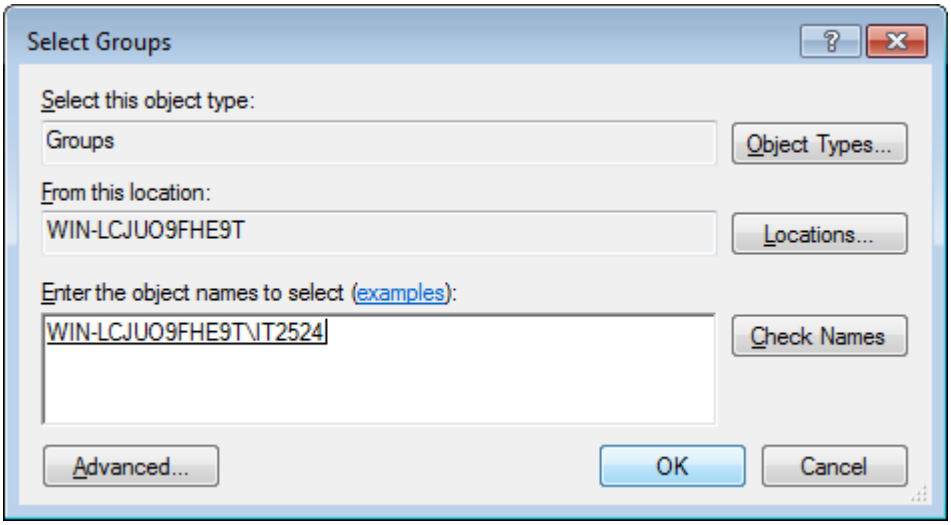


Click on the Advanced button and "Find Now" to list all groups.

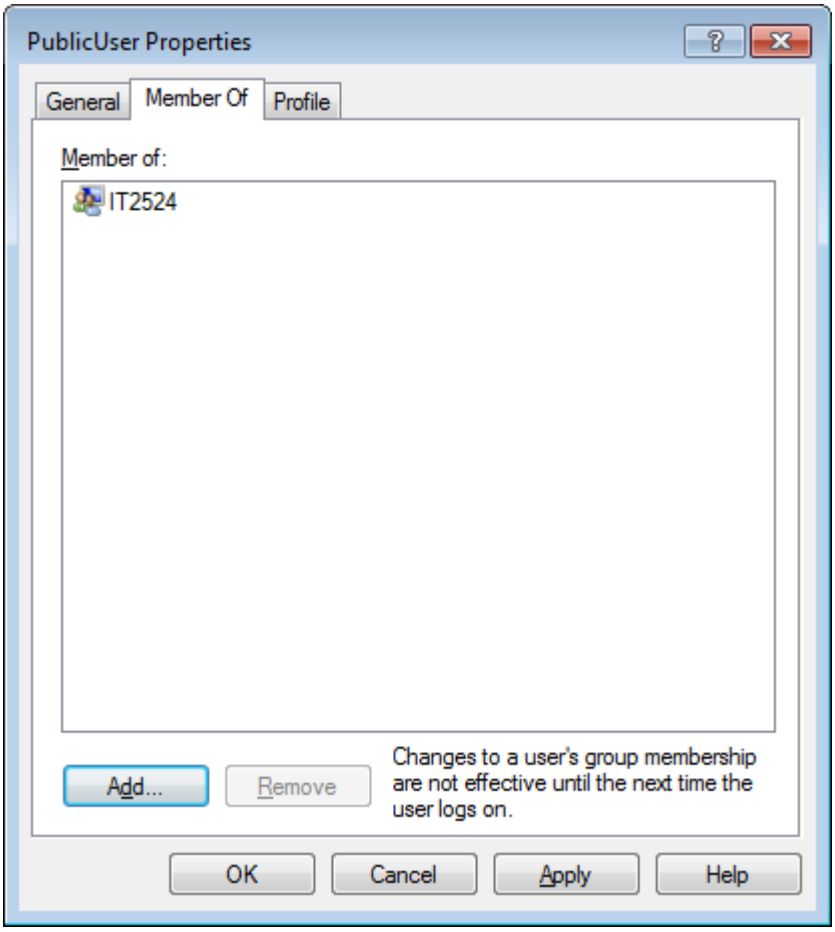

Select Groups
Select this object type:
Groups
Object Types...
From this location:
WIN-LCJUO9FHE9T
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name (RDN)
In Folder



Select the IT2524 group and click on the OK button.



Click on the OK to add PublicUser to the IT2524 group.



Click on the Apply button and the OK button when you are done.

Question 1

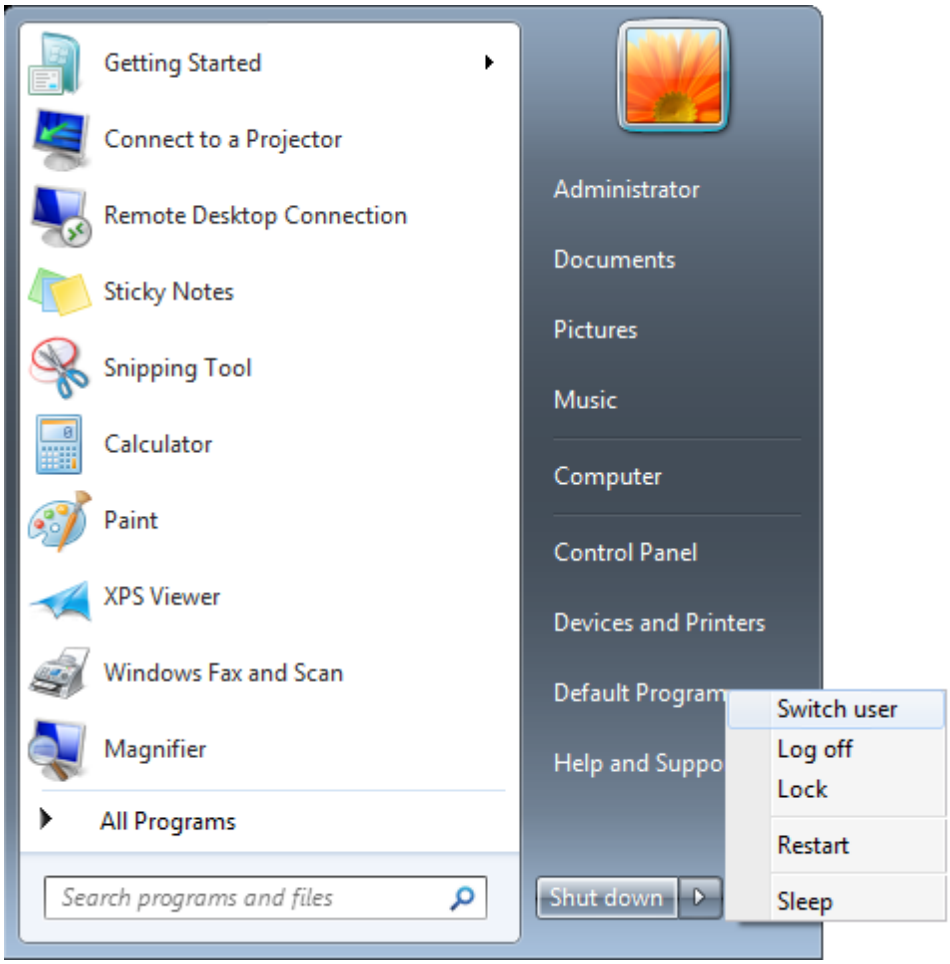
Try to logon user PublicUser. Are you able to logon with this account?

(No. Because you do not belong to the "**Users**" group.)

Configuring Local Group Policy Objects

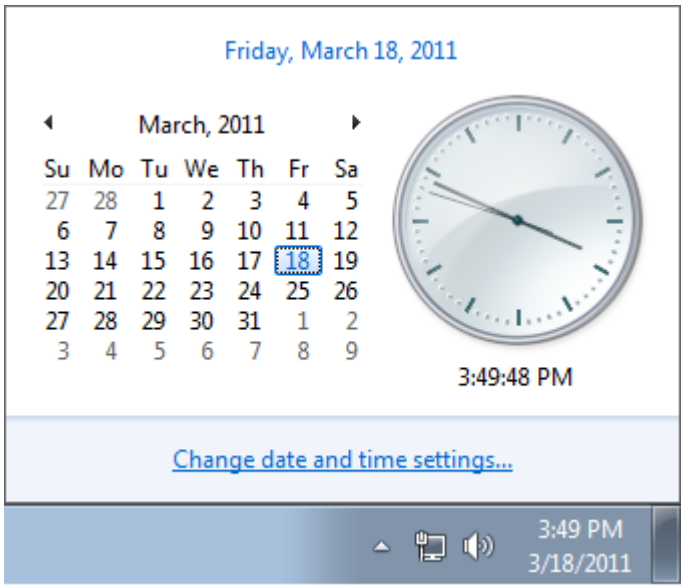
Exercise 3 - Setting local policy

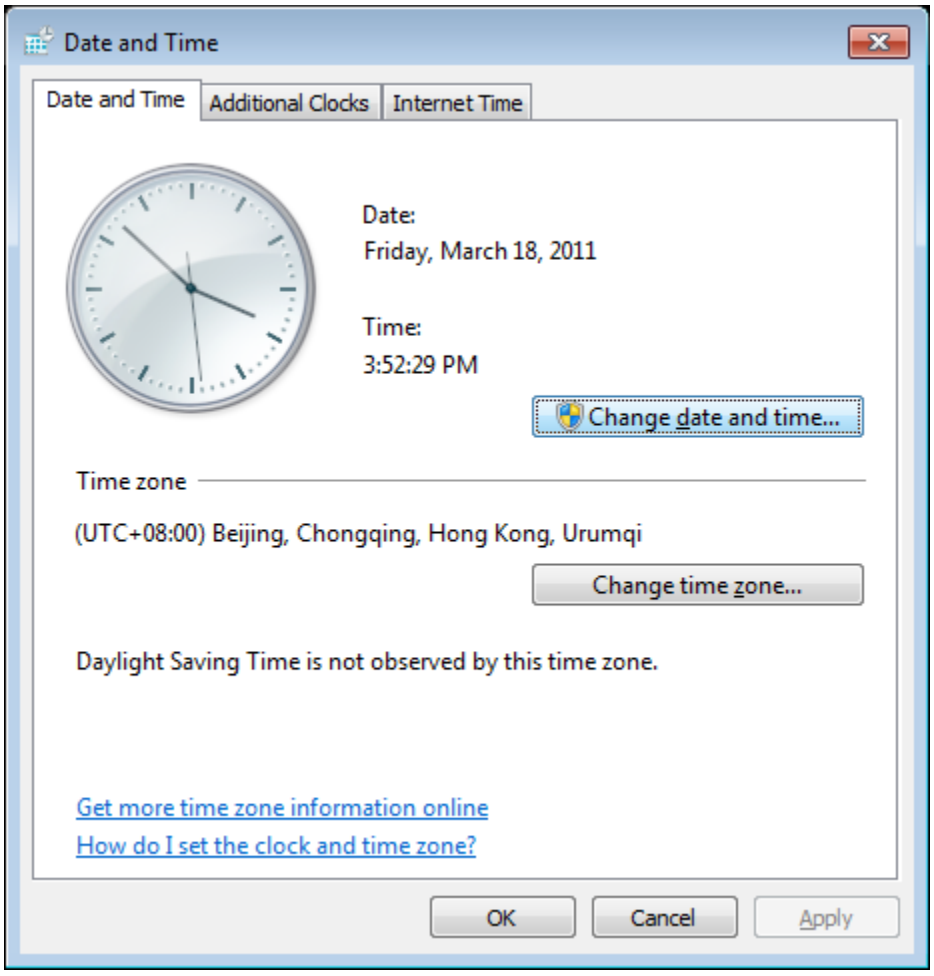
1. Switch the login user to Student.

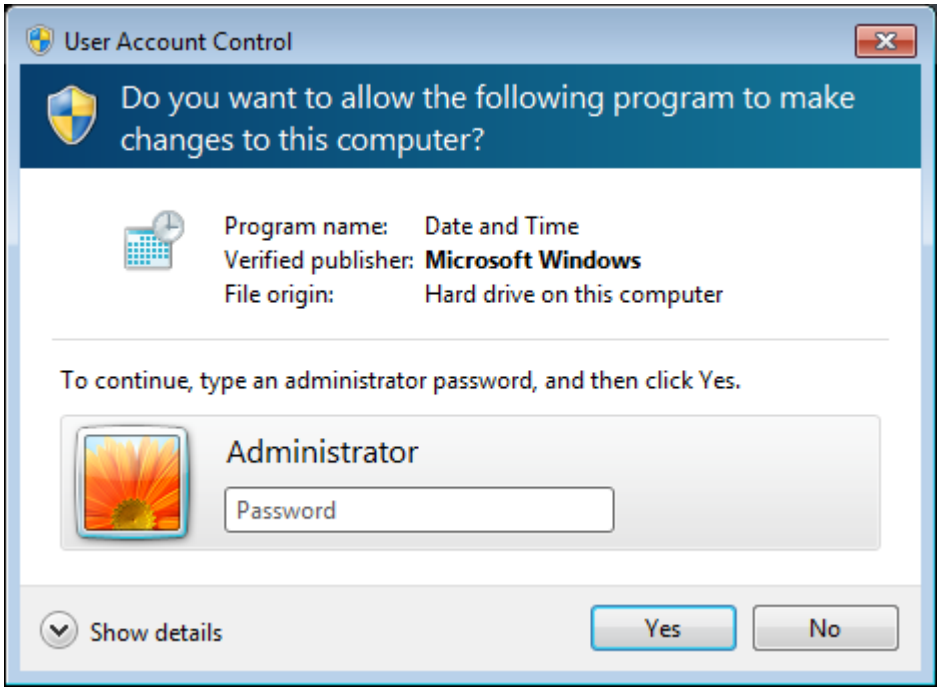


Question 2

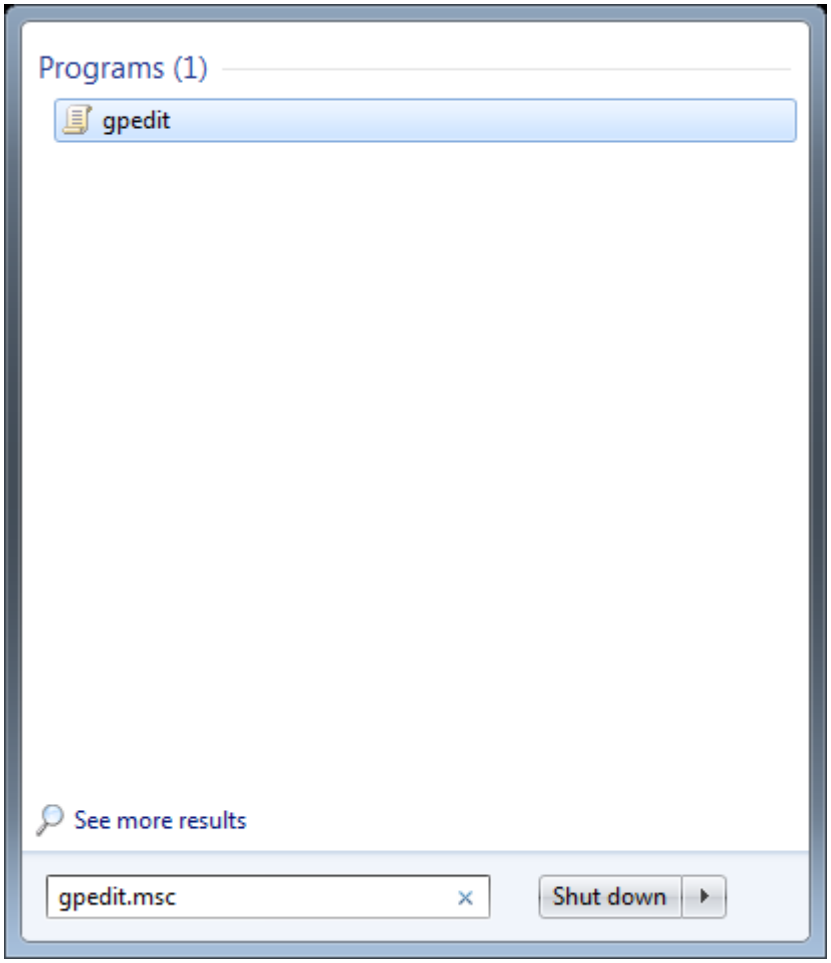
Try to change the system time. Is the Student account allowed to change the system time?
Answer : **By default, Users group is not allowed to change the system time.**

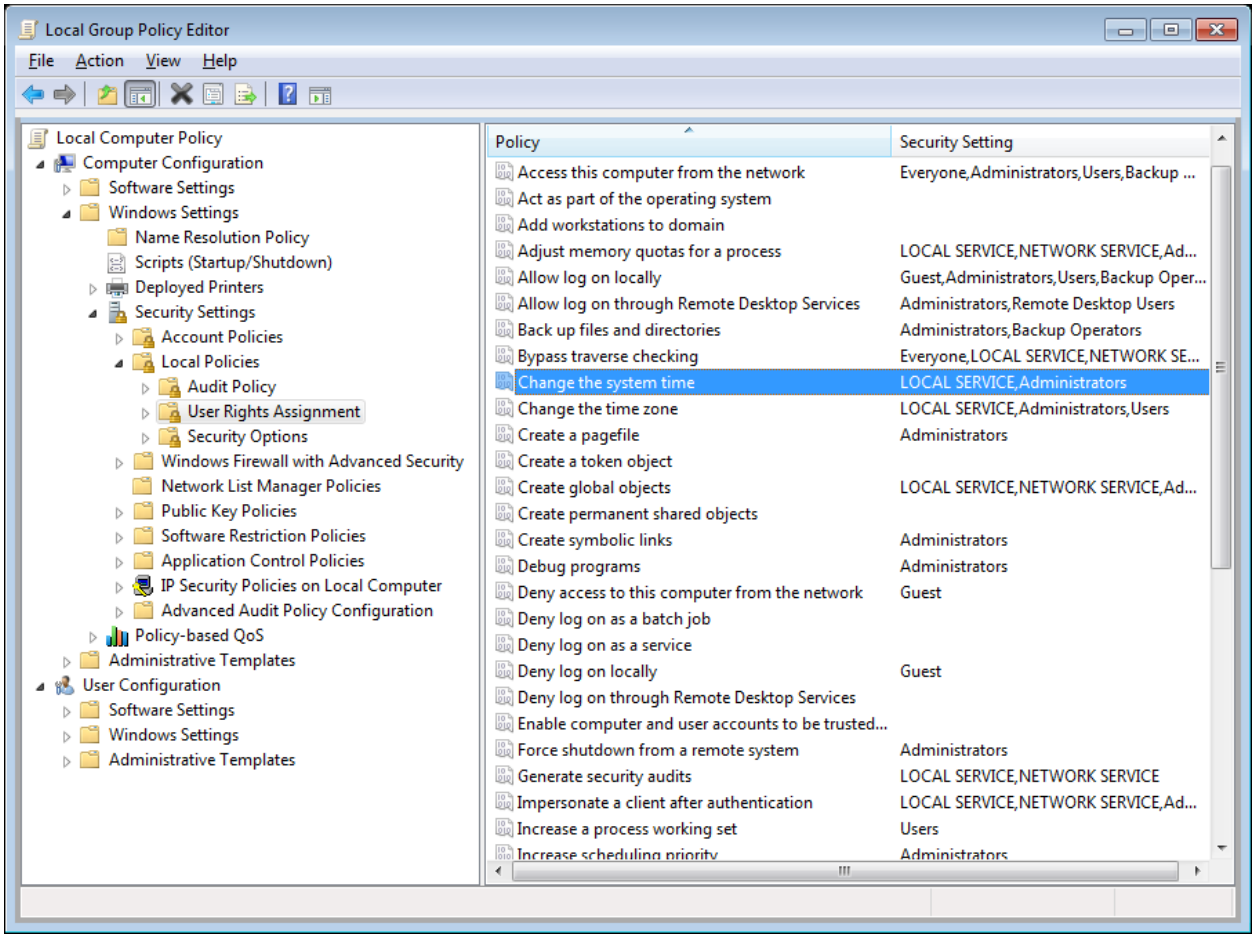




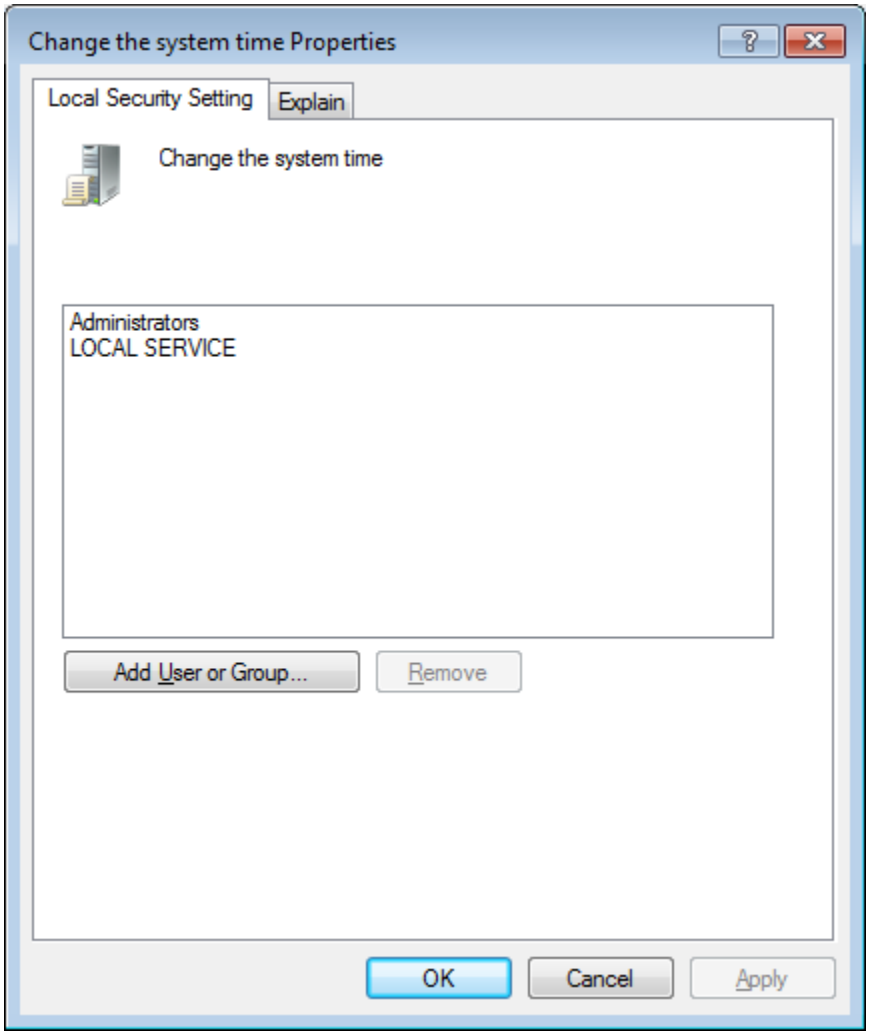


2. Switch user to **SIT**. Run the gpedit.msc as shown.

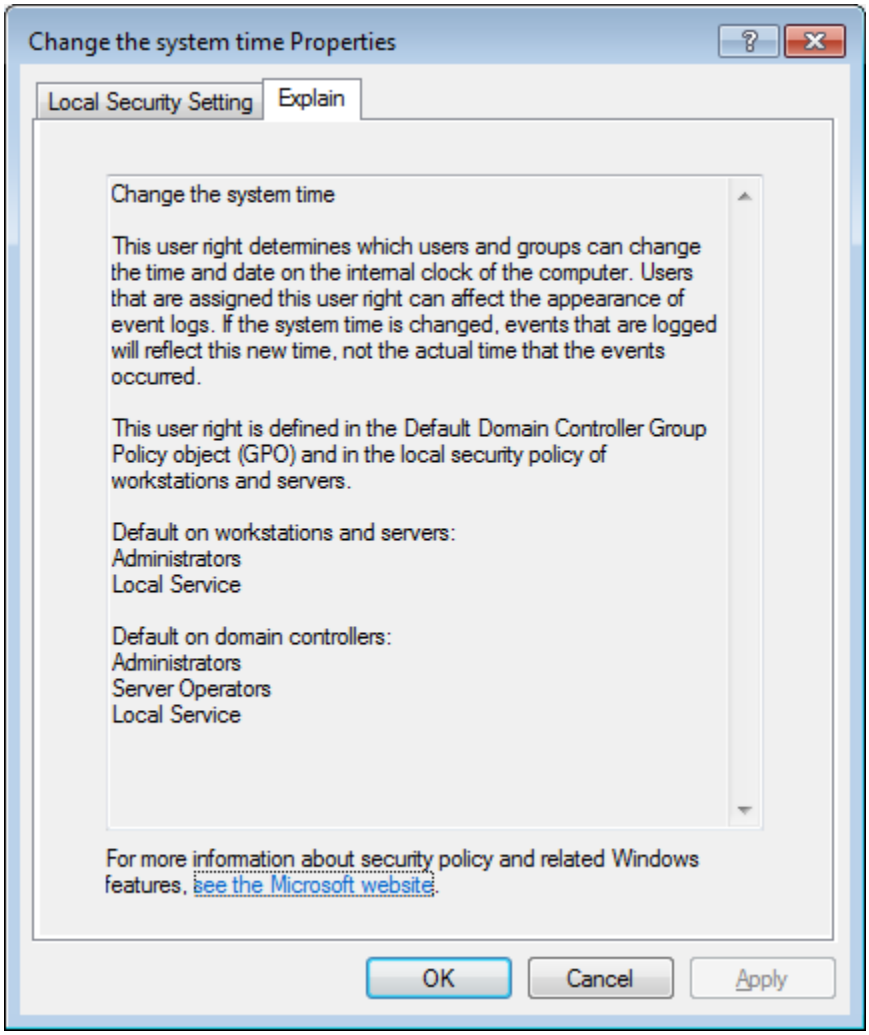




Double click on the "Change the system time" policy.



Click on the "Explain This Setting" tab to display the description of the setting.

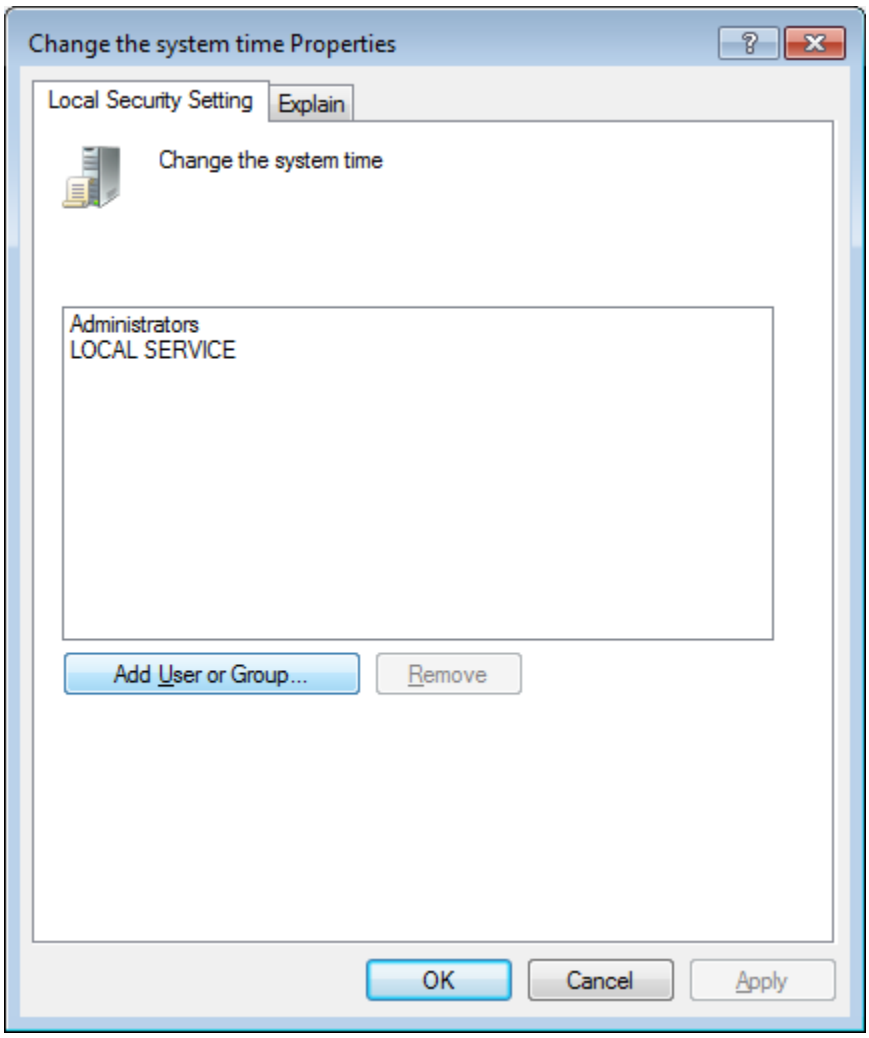


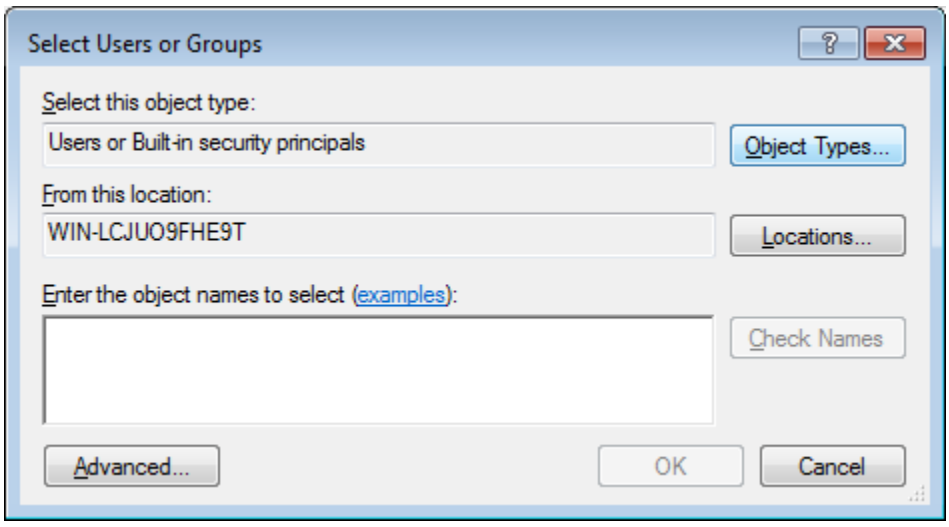
Question 3

By default, which are the groups allowed to change the system time?

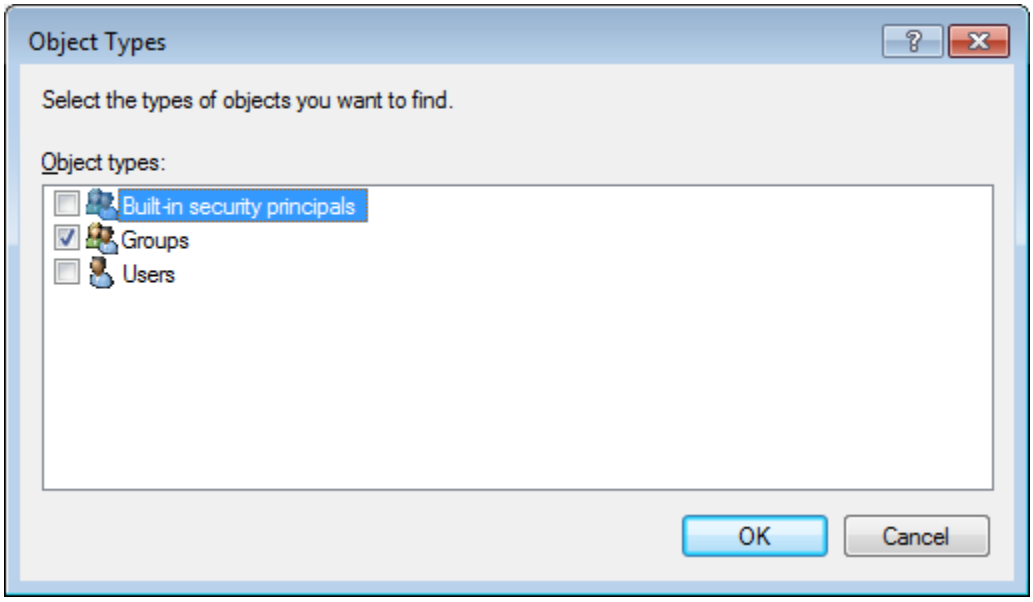
3. Change the local policy to allow the IT2524 group to change the system time.

   Click on "Add User or Group" button.

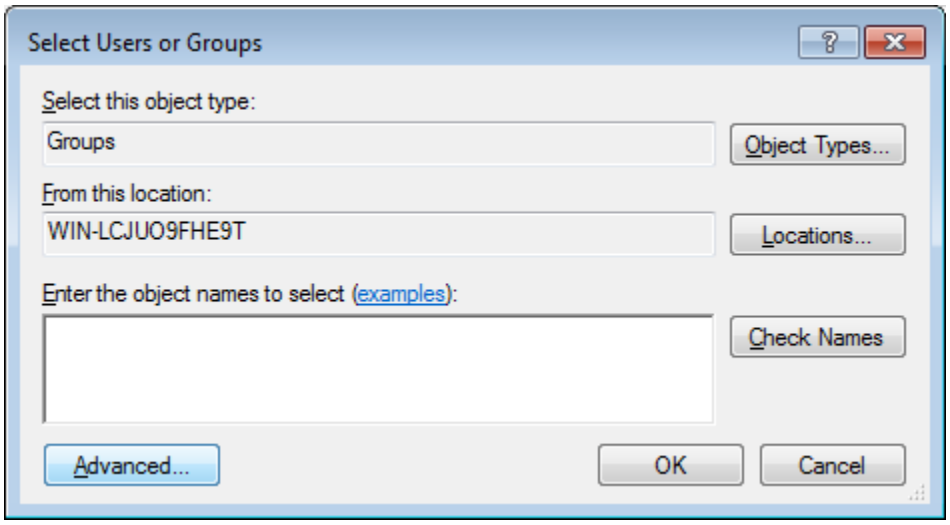




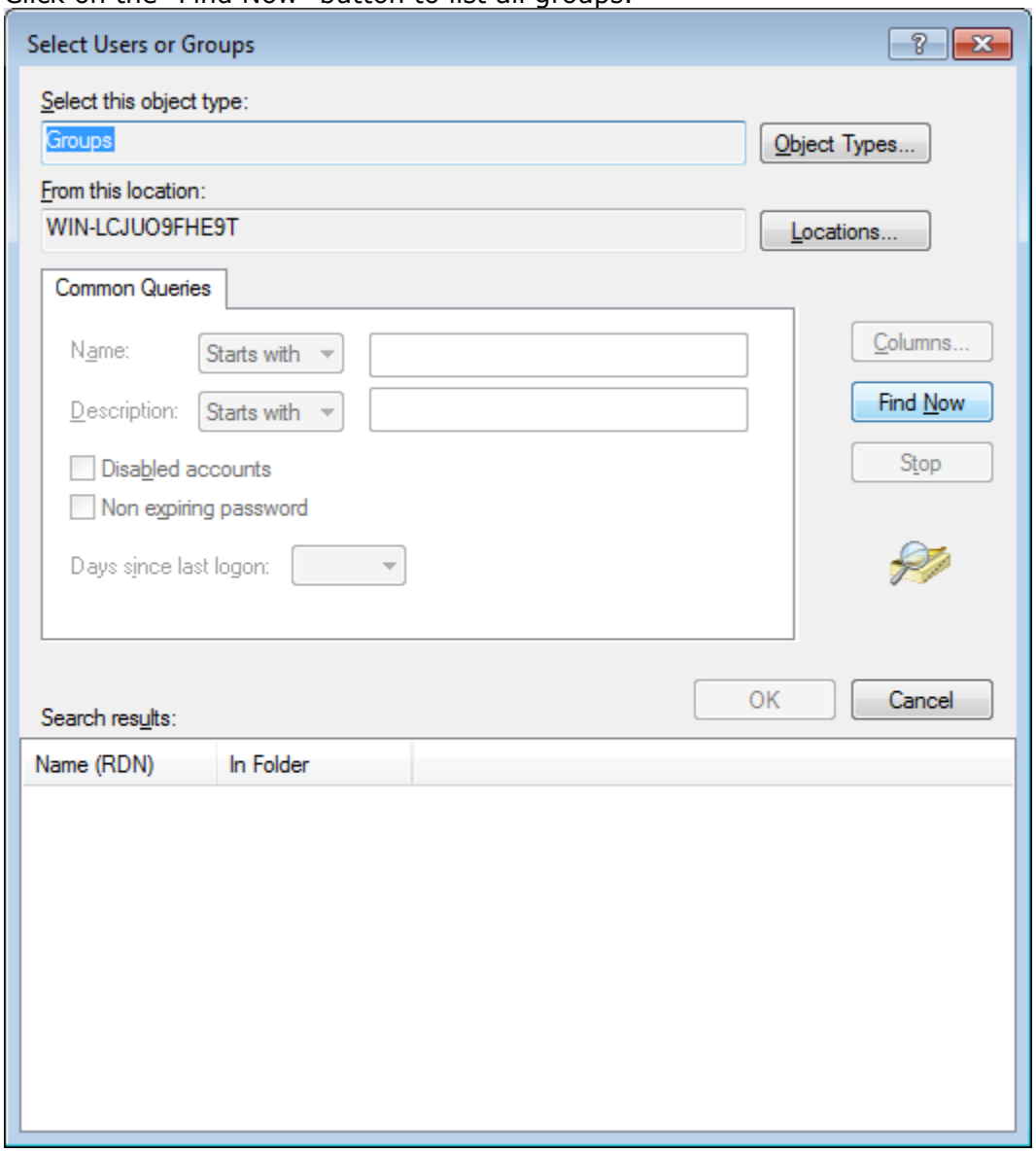
Click on the "Object Type" button and select the Groups checkbox. Click on the OK button when you are done.



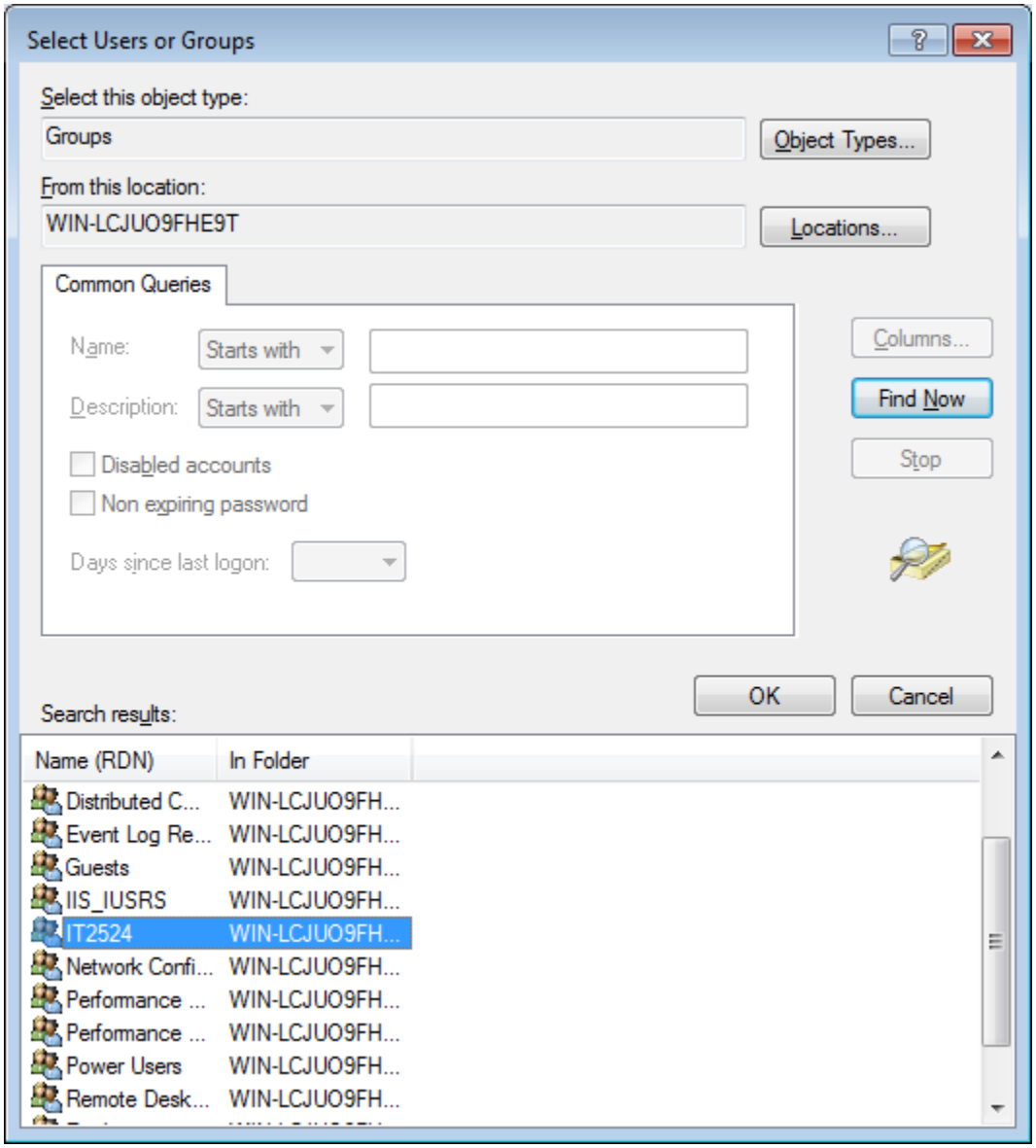
Click on the Advanced button.



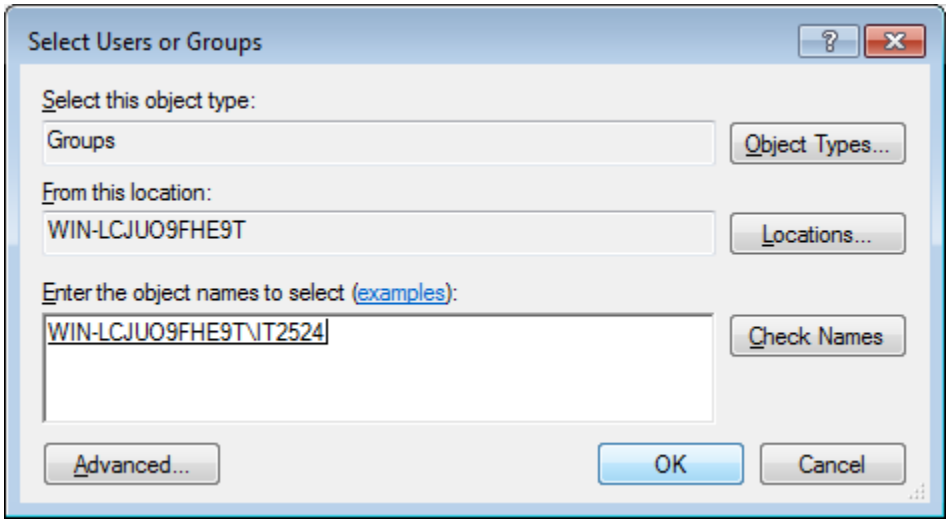
Click on the "Find Now" button to list all groups.



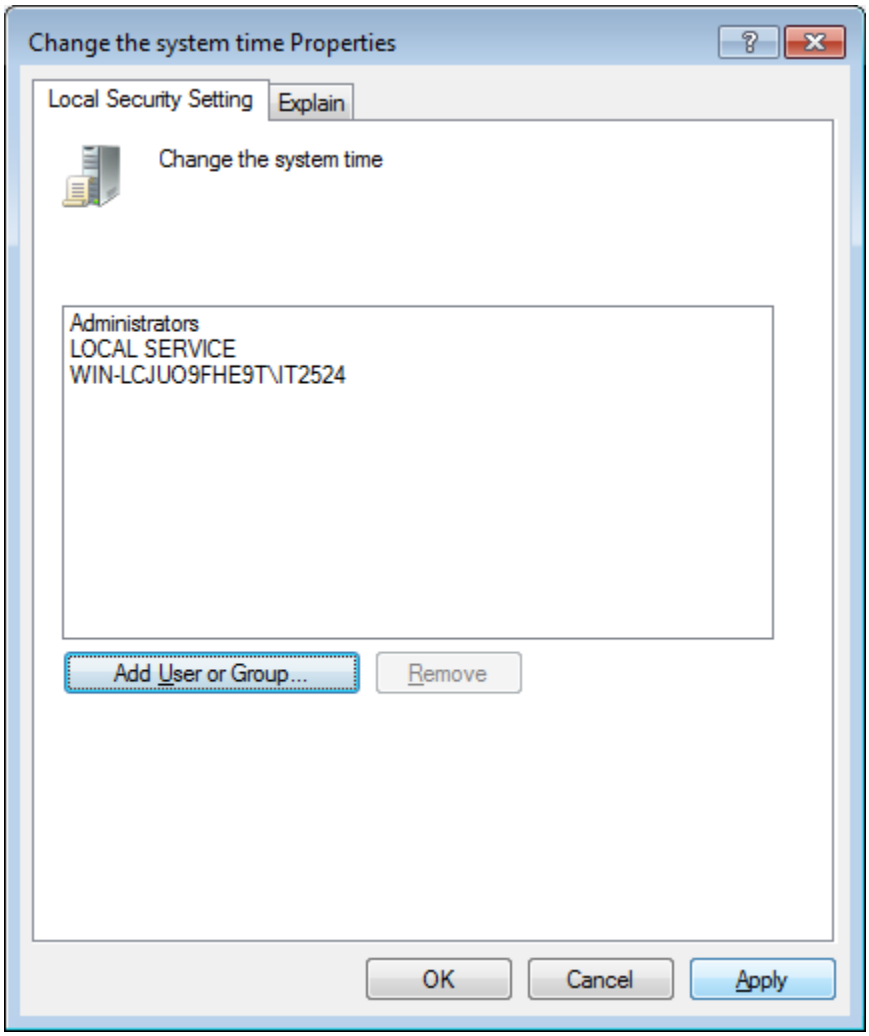
Click on the OK button to add IT2524 to the policy.



Click the OK button to close.



Click on the Apply button and the OK button.



Question 4

The Student user account is in the IT2524 group. The IT2524 group is allowed to change the system time. Can Student user account change the system time?

Answer

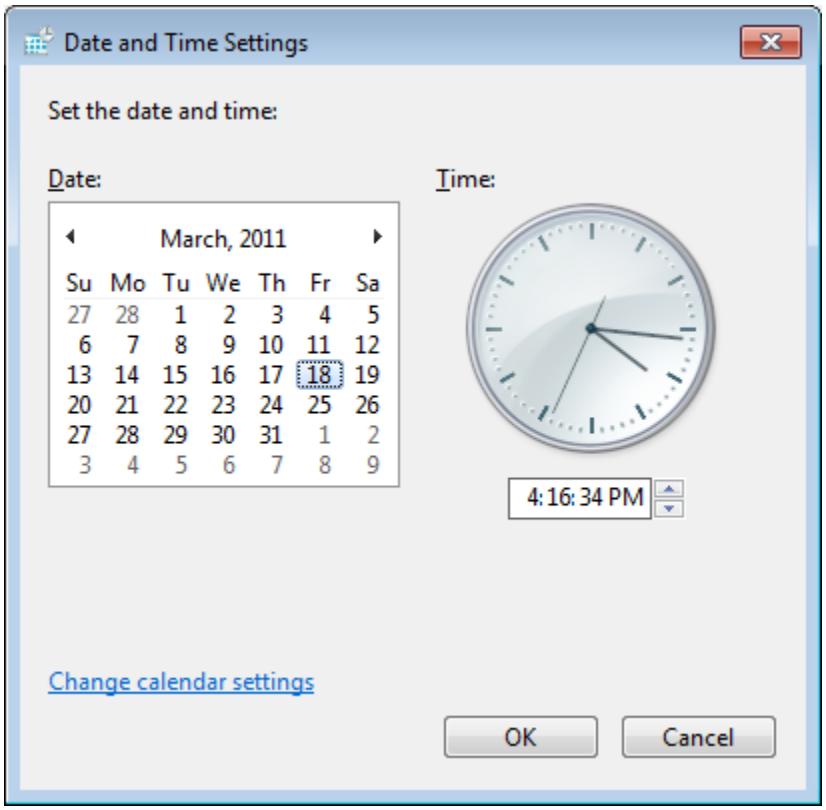
Yes

4. Switch the login user to Student.

Question 5

Try to change the system time again. Can the system time be changed? If not, can you think of a solution on your own to get it working?

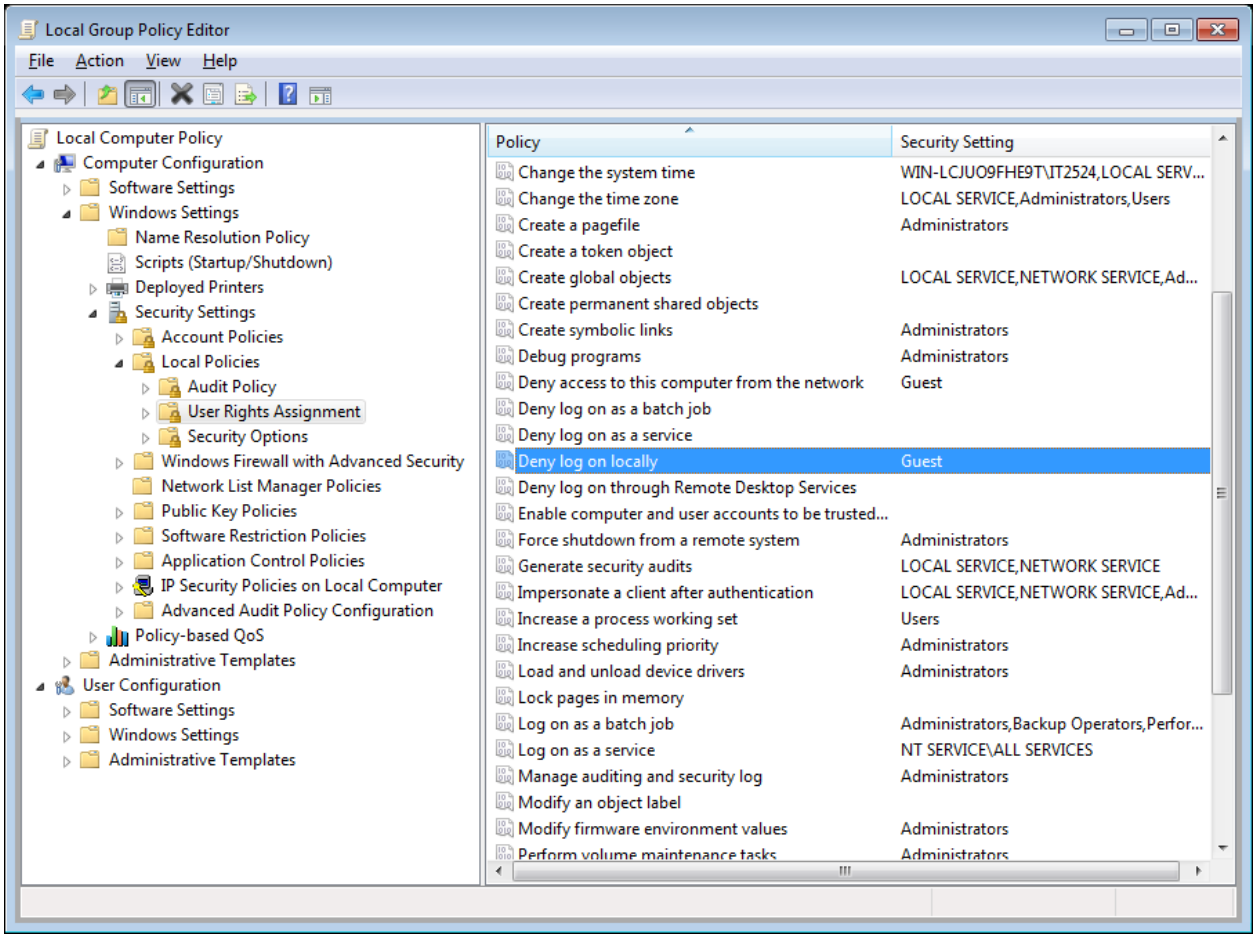
Hint:
Logout and login the Student account. (Student need to re-login again to reload the policies.)

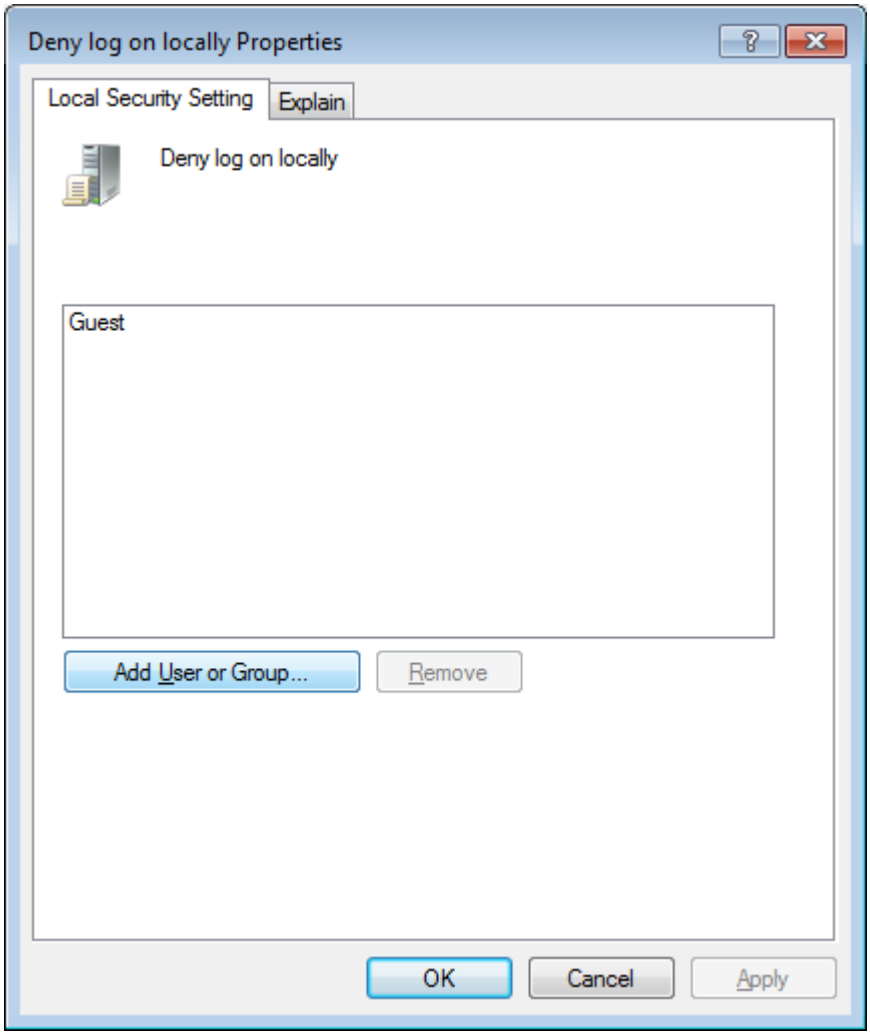


Exercise 4 - Setting local policy

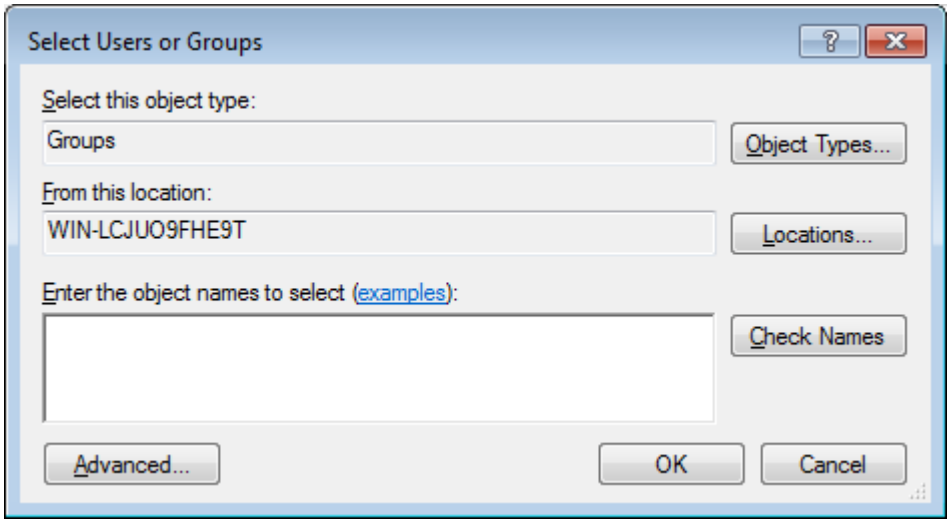
1. In this exercise, we will set the local policy to deny login for the IT2524 group.

   Switch user to "SIT". Run **gpedit.msc**.
   Follow the steps as shown to set the "Deny logon locally" policy.

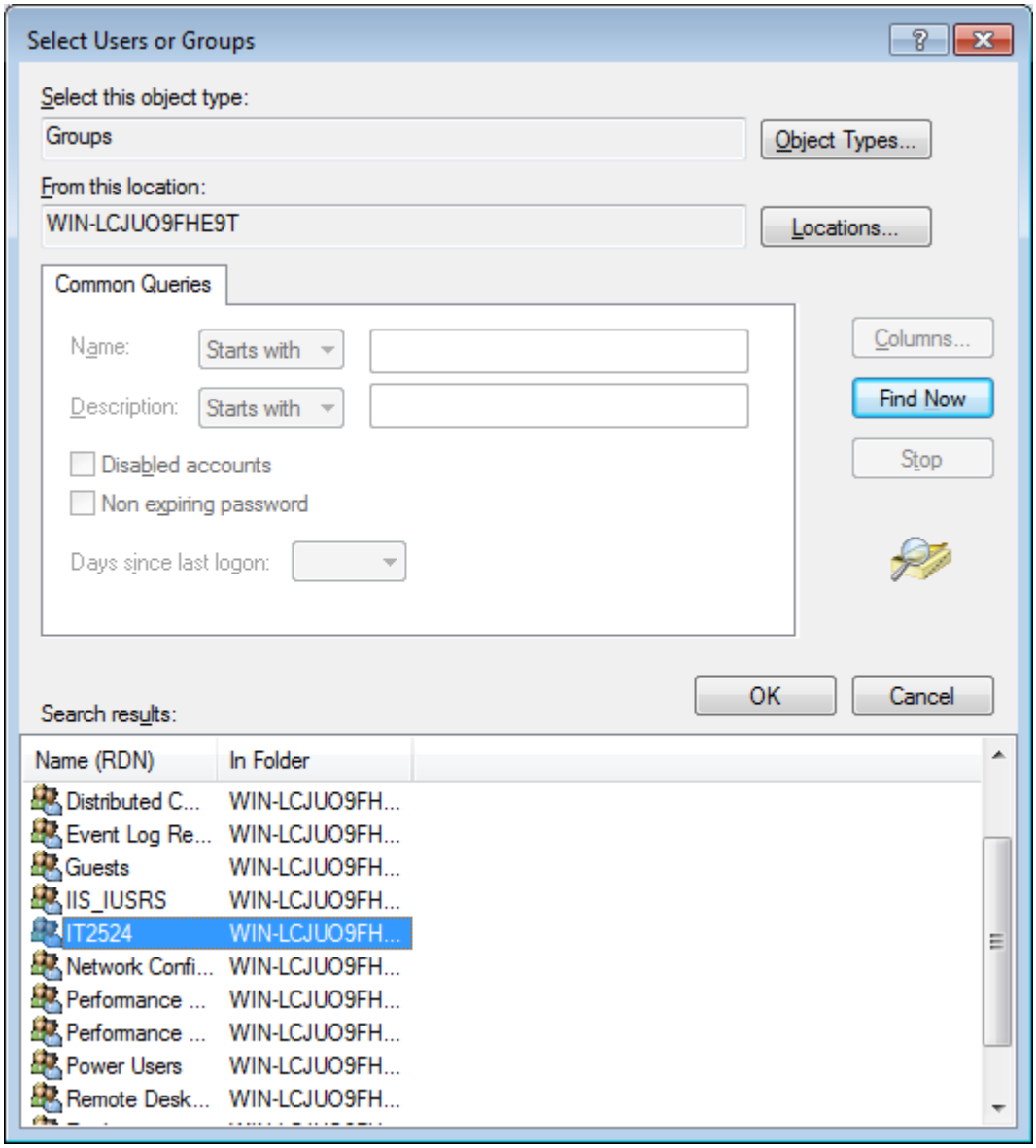




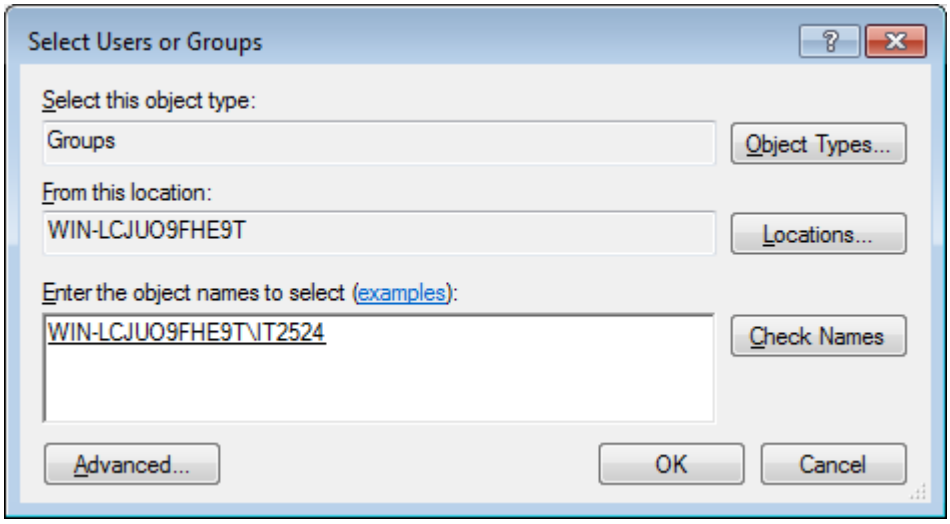
Click "Add User or Group…"

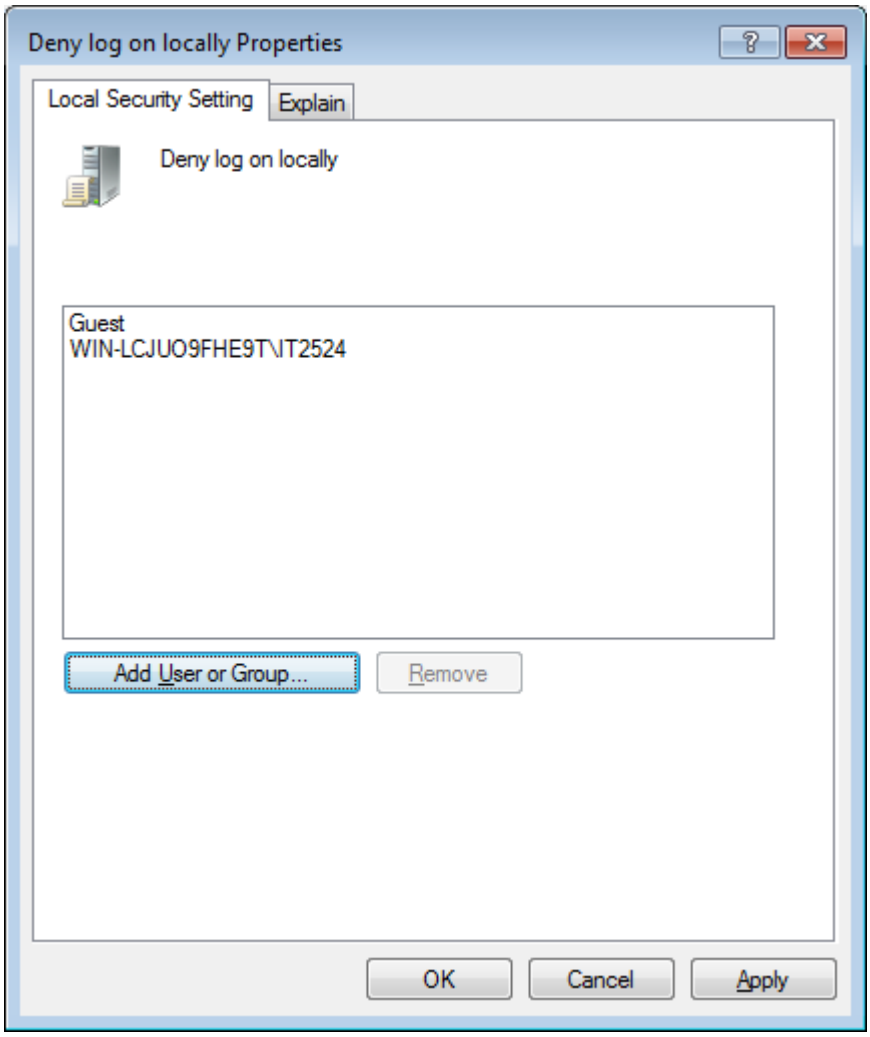


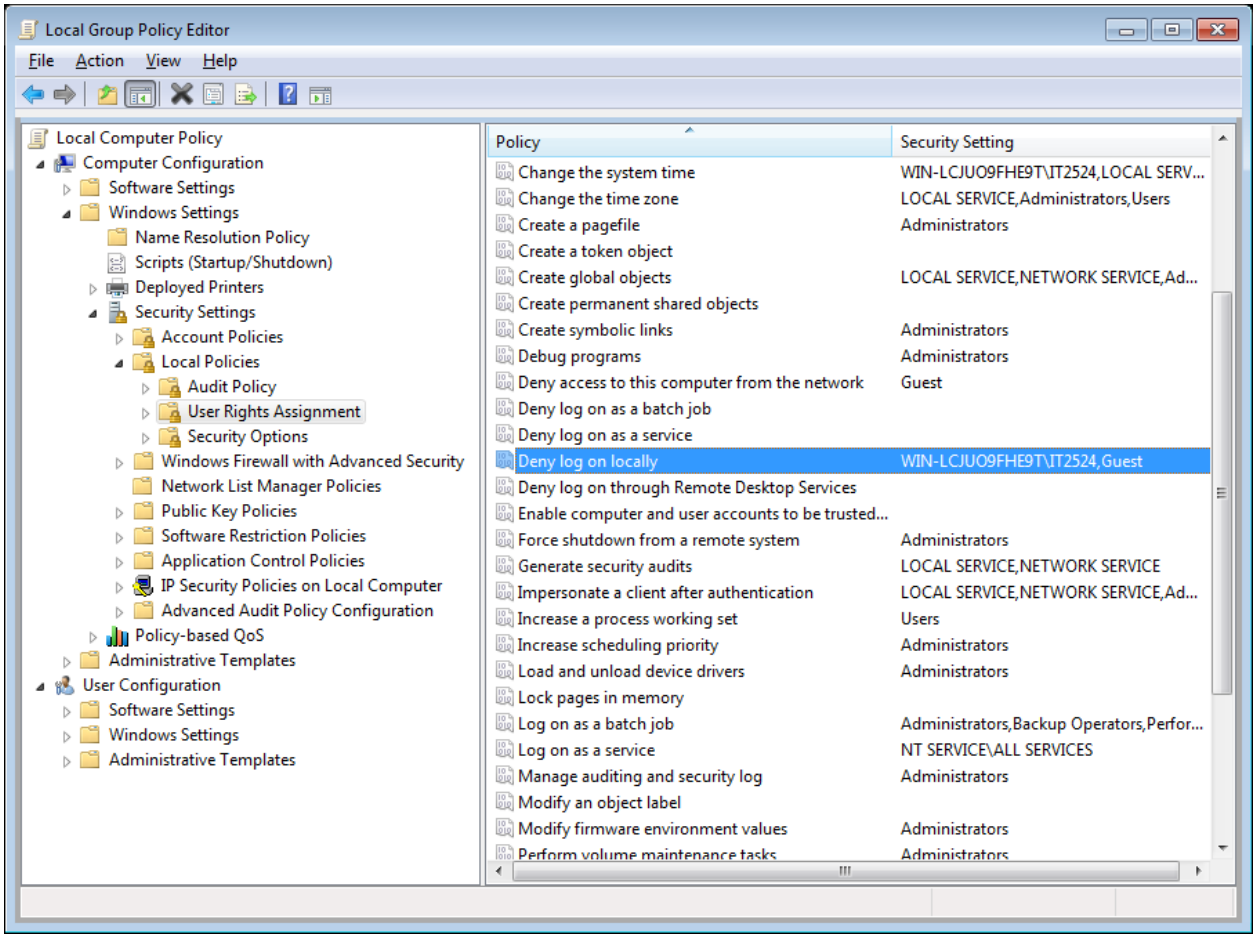
Click "Advanced…"



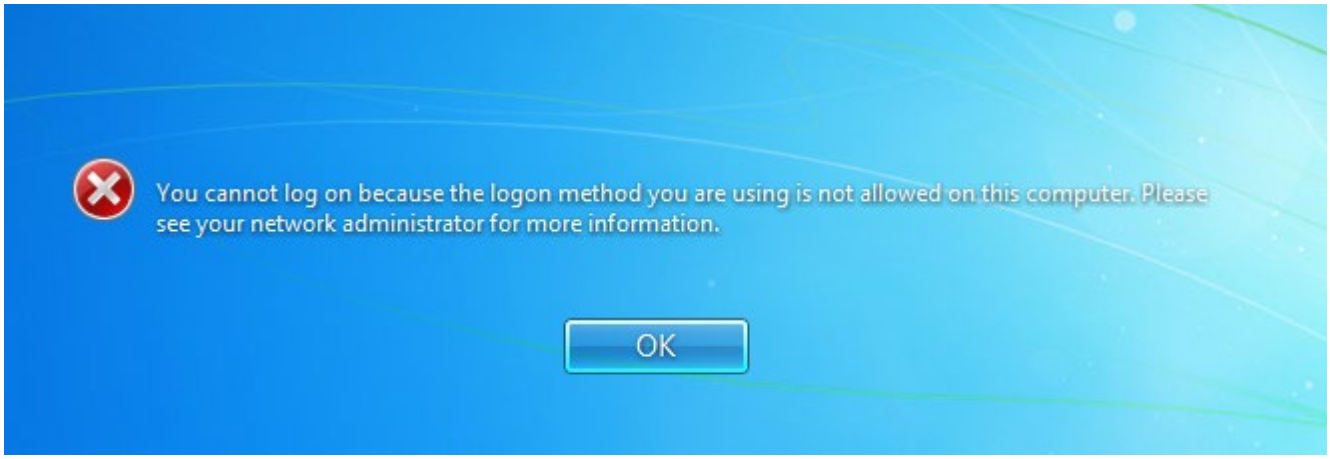
Change "Object Types…" to 'Groups'.
Click "Find Now"
Select IT2524, click "OK"


Select Users or Groups
Select this object type:
Groups
Object Types...
From this location:
WIN-LCJUO9FHE9T
Locations...
Enter the object names to select (examples):
WIN-LCJUO9FHE9T\IT2524
Check Names
Advanced...
OK
Cancel


Deny log on locally Properties
Local Security Setting
Explain
Deny log on locally
Guest
WIN-LCJUO9FHE9T\IT2524
Add User or Group...
Remove
OK
Cancel
Apply

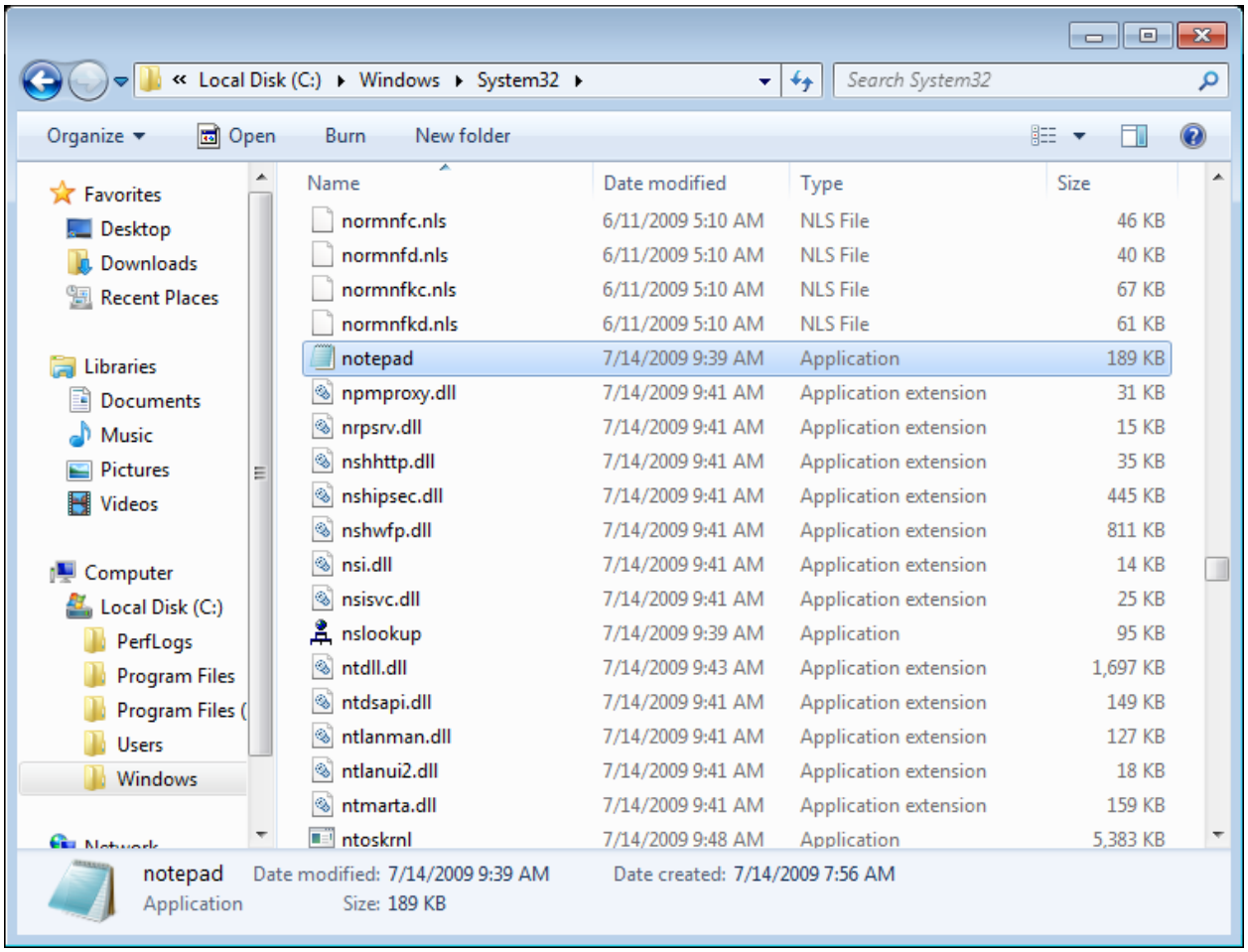


Now, try to switch to user Student. Are you able to login?



Switch to the SIT account.
Remove the "Deny log on locally" for the IT2524 group.
Login as **Student** to verify your configuration is correct.

Before beginning on the next exercise, first verify that the Student account can execute the "C:\WINDOWS\system32\notepad.exe".

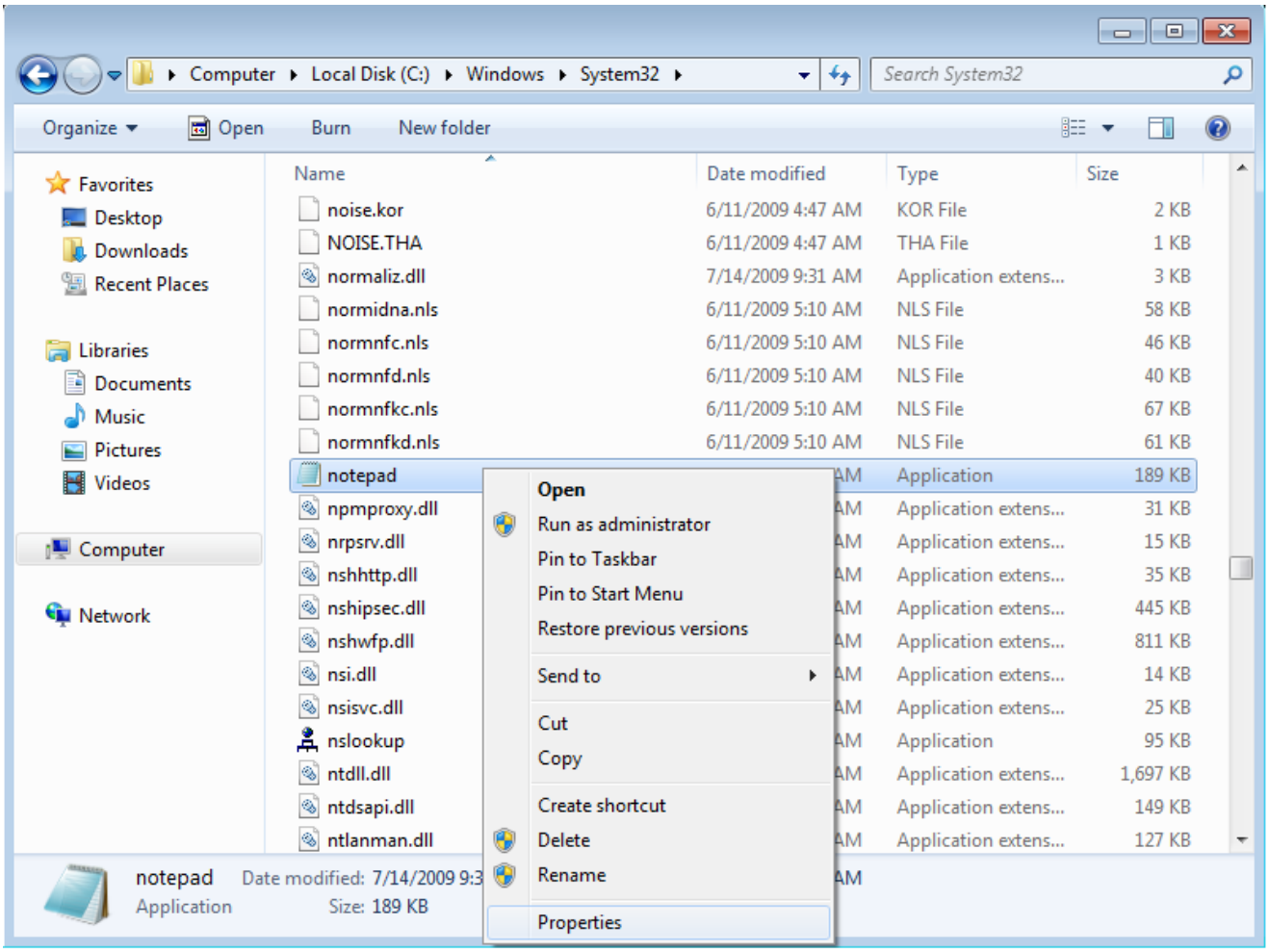


Exercise 5 - File Permissions

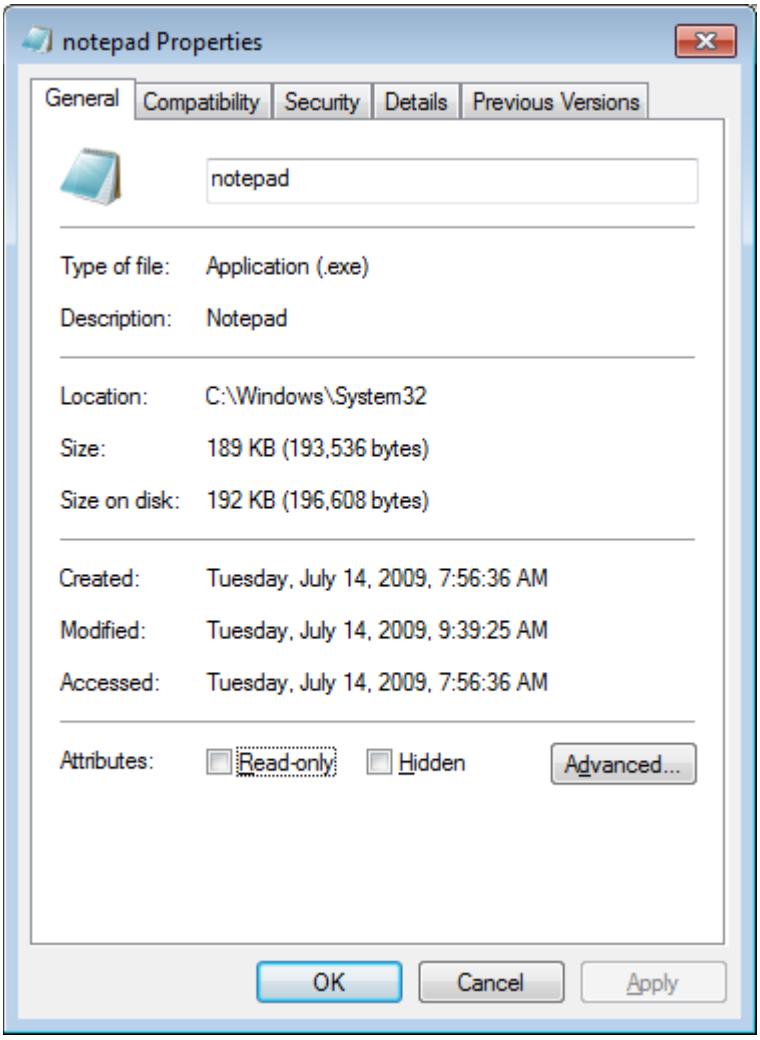
1. Switch to the **SIT** account.

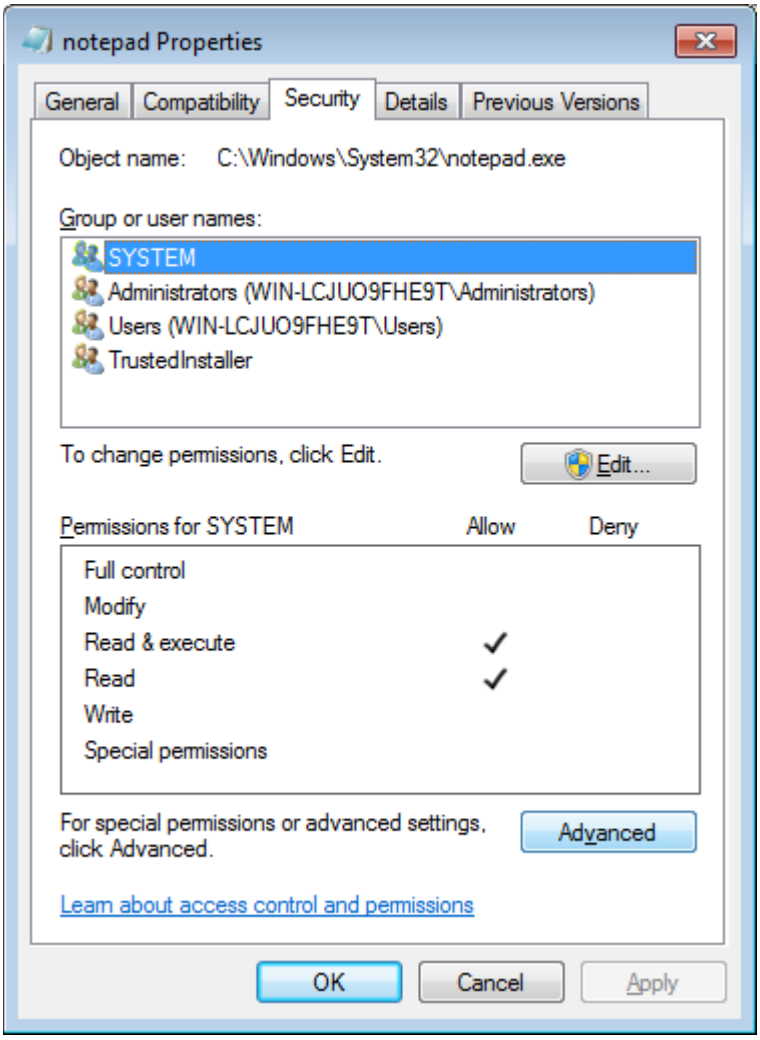
   We are going to change the settings such that 'student' cannot run 'notepad.exe'.

   Explore to C:\WINDOWS\system32\notepad.exe

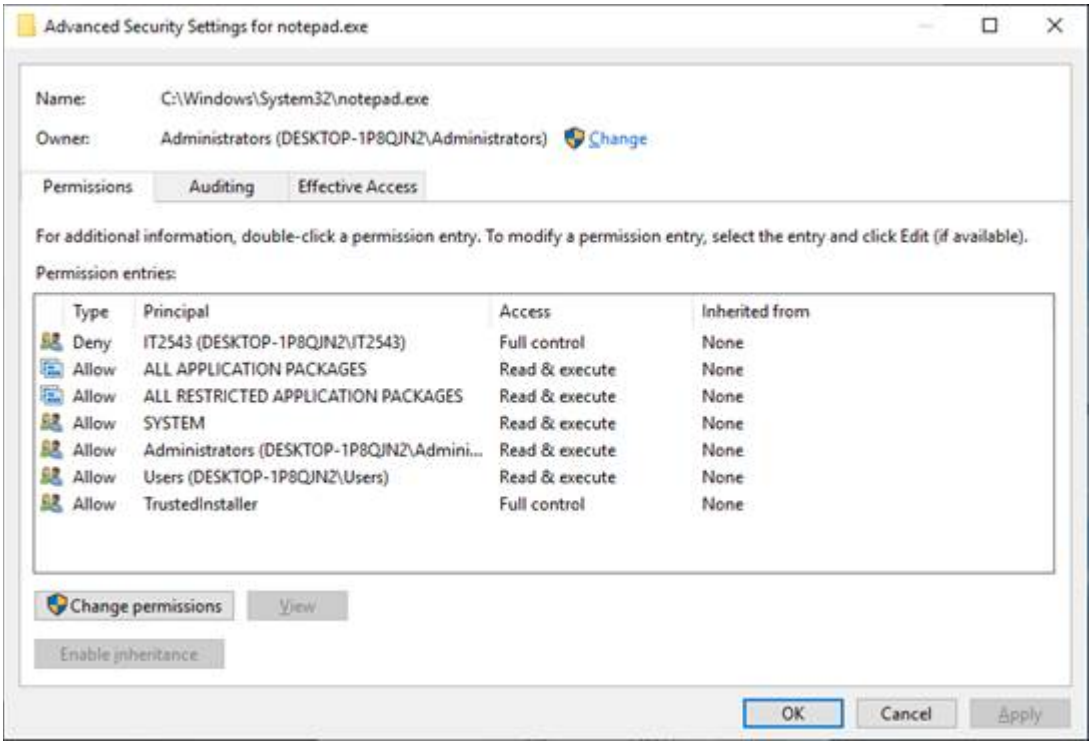


   Right-click on notepad.exe and select Properties.


notepad Properties
General
Compatibility
Security
Details
Previous Versions
notepad
Type of file: Application (.exe)
Description: Notepad
Location: C:\Windows\System32
Size: 189 KB (193,536 bytes)
Size on disk: 192 KB (196,608 bytes)
Created: Tuesday, July 14, 2009, 7:56:36 AM
Modified: Tuesday, July 14, 2009, 9:39:25 AM
Accessed: Tuesday, July 14, 2009, 7:56:36 AM
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply

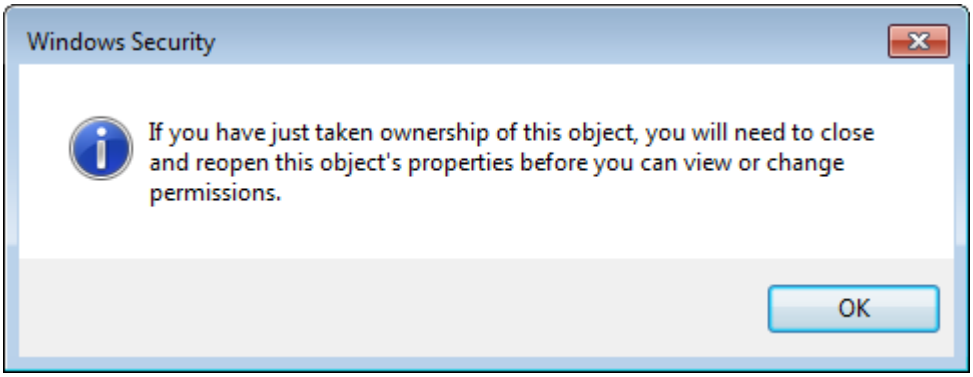


Click "Advanced"



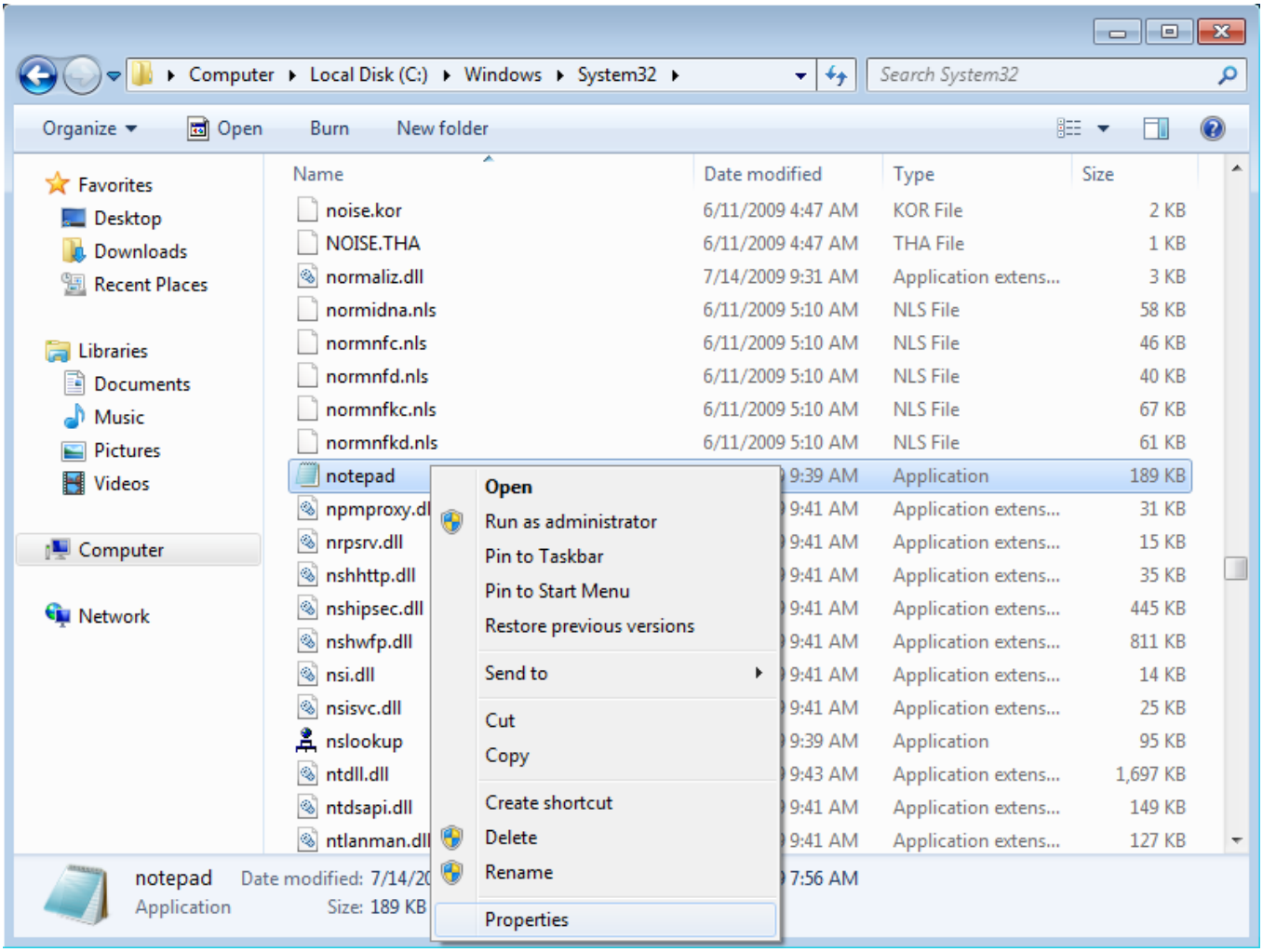
Select "Change" to edit owner and select SIT account as the owner.

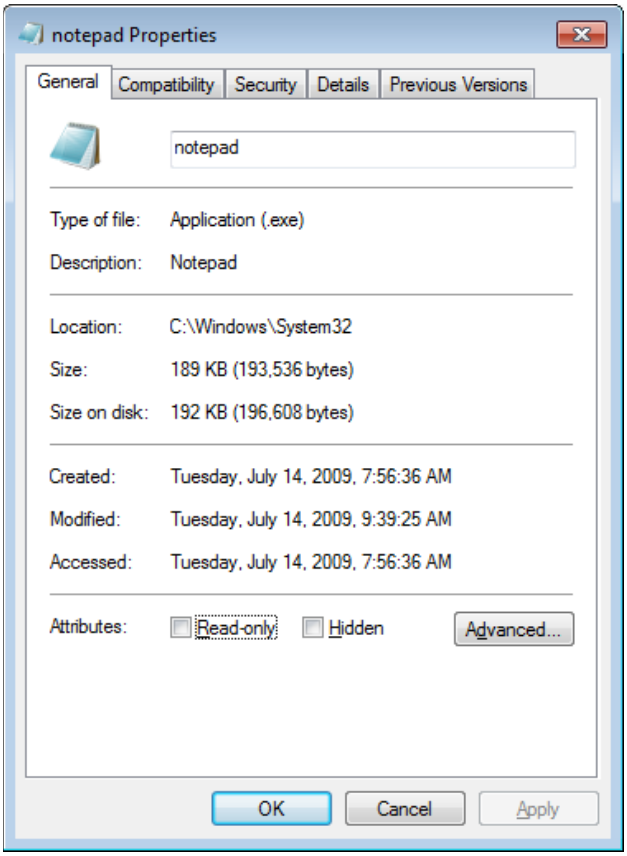
Click the Apply button and then the OK button.

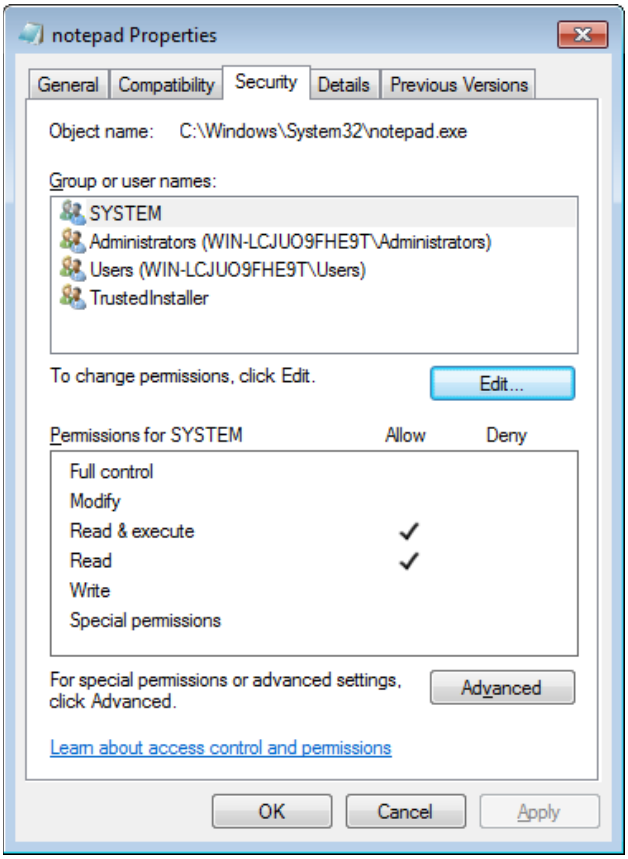


Click on the OK button to close dialog window.

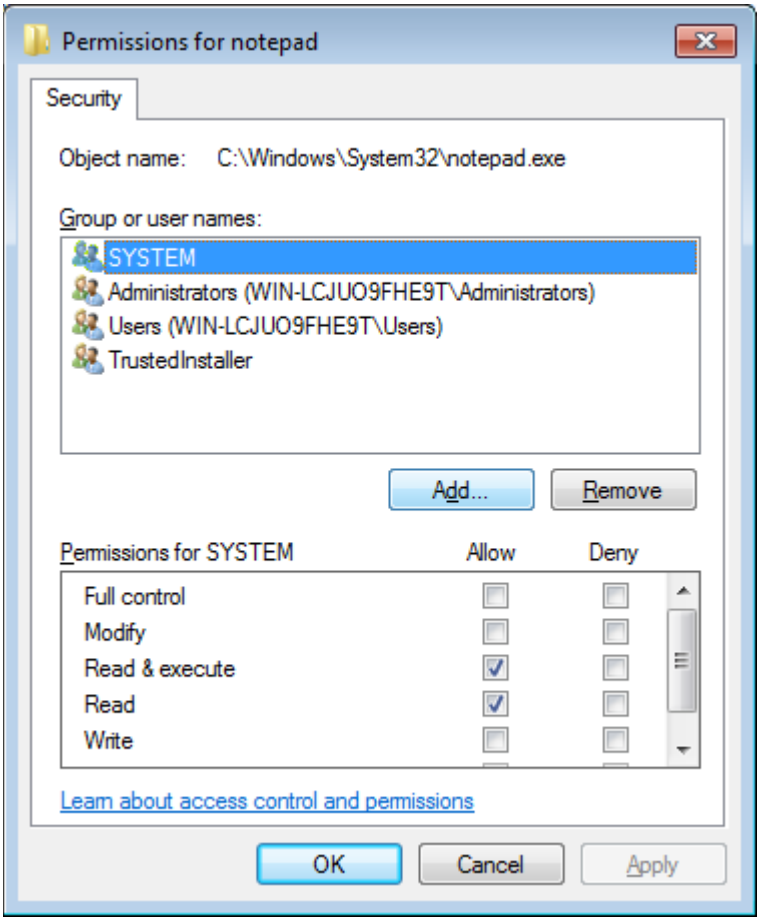
Next, we will disallow the IT2524 group from executing the "notepad.exe".


Computer ▸ Local Disk (C:) ▸ Windows ▸ System32 ▸
Search System32
Organize
Open
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
noise.kor 6/11/2009 4:47 AM KOR File 2 KB
NOISE.THA 6/11/2009 4:47 AM THA File 1 KB
normaliz.dll 7/14/2009 9:31 AM Application extens... 3 KB
normidna.nls 6/11/2009 5:10 AM NLS File 58 KB
normnfc.nls 6/11/2009 5:10 AM NLS File 46 KB
normnfd.nls 6/11/2009 5:10 AM NLS File 40 KB
normnfkc.nls 6/11/2009 5:10 AM NLS File 67 KB
normnfkd.nls 6/11/2009 5:10 AM NLS File 61 KB
notepad 9:39 AM Application 189 KB
npmproxy.dl 9:41 AM Application extens... 31 KB
nrpsrv.dll 9:41 AM Application extens... 15 KB
nshhttp.dll 9:41 AM Application extens... 35 KB
nshipsec.dll 9:41 AM Application extens... 445 KB
nshwfp.dll 9:41 AM Application extens... 811 KB
nsi.dll 9:41 AM Application extens... 14 KB
nsisvc.dll 9:41 AM Application extens... 25 KB
nslookup 9:39 AM Application 95 KB
ntdll.dll 9:43 AM Application extens... 1,697 KB
ntdsapi.dll 9:41 AM Application extens... 149 KB
ntlanman.dll 9:41 AM Application extens... 127 KB
Open
Run as administrator
Pin to Taskbar
Pin to Start Menu
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
notepad Date modified: 7/14/20 7:56 AM
Application Size: 189 KB

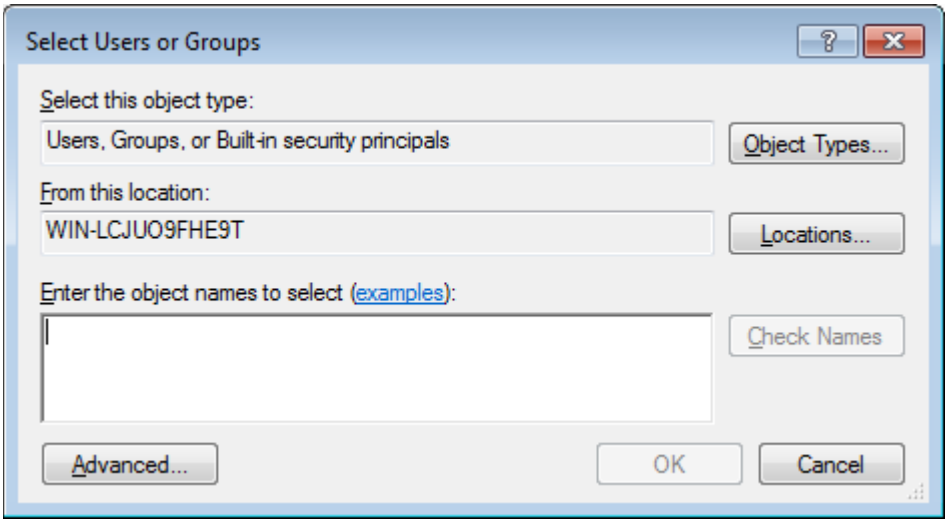

notepad Properties
General
Compatibility
Security
Details
Previous Versions
notepad
Type of file: Application (.exe)
Description: Notepad
Location: C:\Windows\System32
Size: 189 KB (193,536 bytes)
Size on disk: 192 KB (196,608 bytes)
Created: Tuesday, July 14, 2009, 7:56:36 AM
Modified: Tuesday, July 14, 2009, 9:39:25 AM
Accessed: Tuesday, July 14, 2009, 7:56:36 AM
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply


notepad Properties
General
Compatibility
Security
Details
Previous Versions
Object name: C:\Windows\System32\notepad.exe
Group or user names:
SYSTEM
Administrators (WIN-LCJUO9FHE9T\Administrators)
Users (WIN-LCJUO9FHE9T\Users)
TrustedInstaller
To change permissions, click Edit.
Edit...
Permissions for SYSTEM
Allow
Deny
Full control
Modify
Read & execute
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply

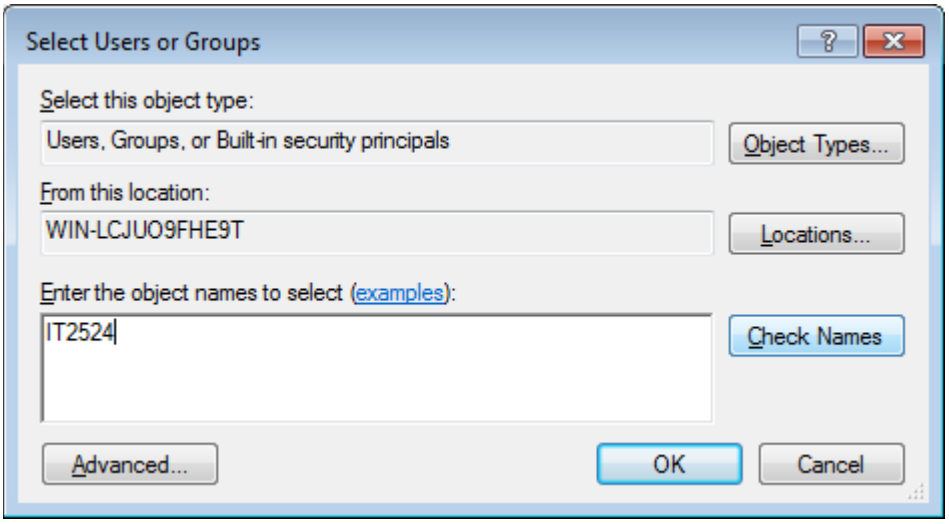
Click "Edit"



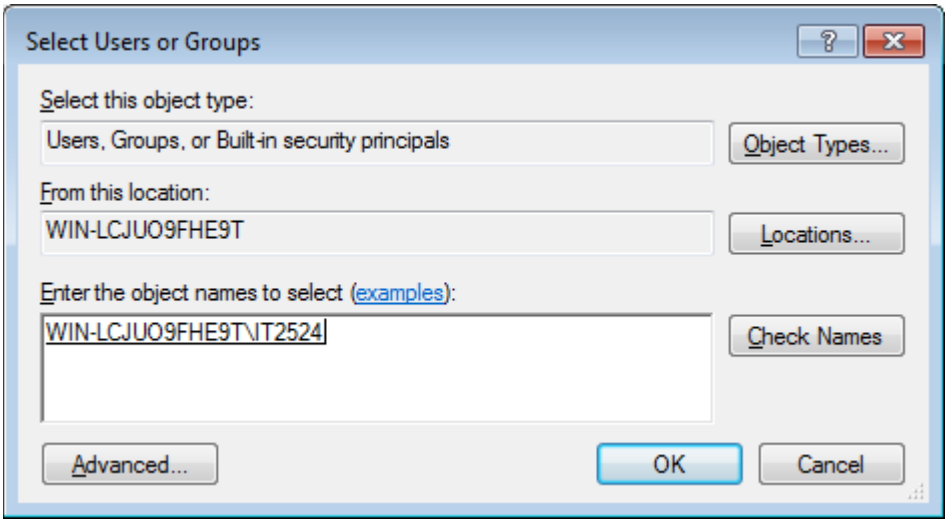
Click the Add button.

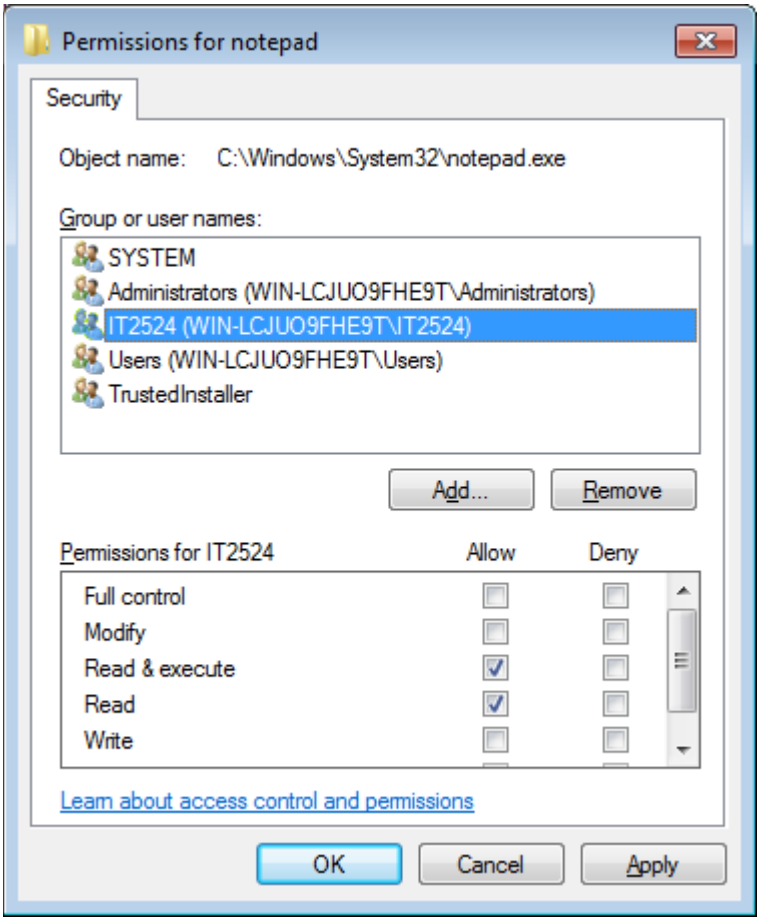


Enter the object name “IT2524” as shown.

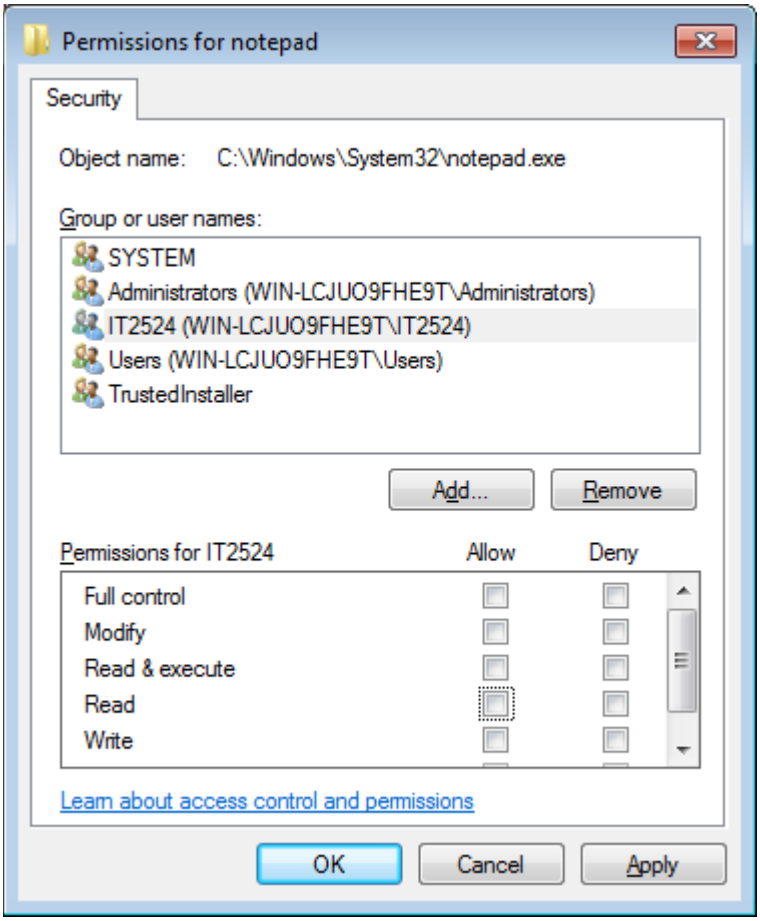


Click on the "Check Names" button.

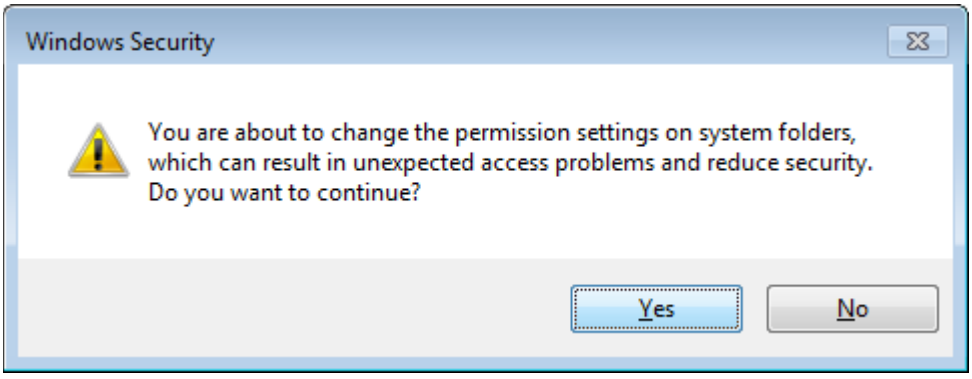




Remove the Allow permission for IT2524 group as shown.



Click on the Apply button to make the change.



Click on the OK button to close the dialog window.

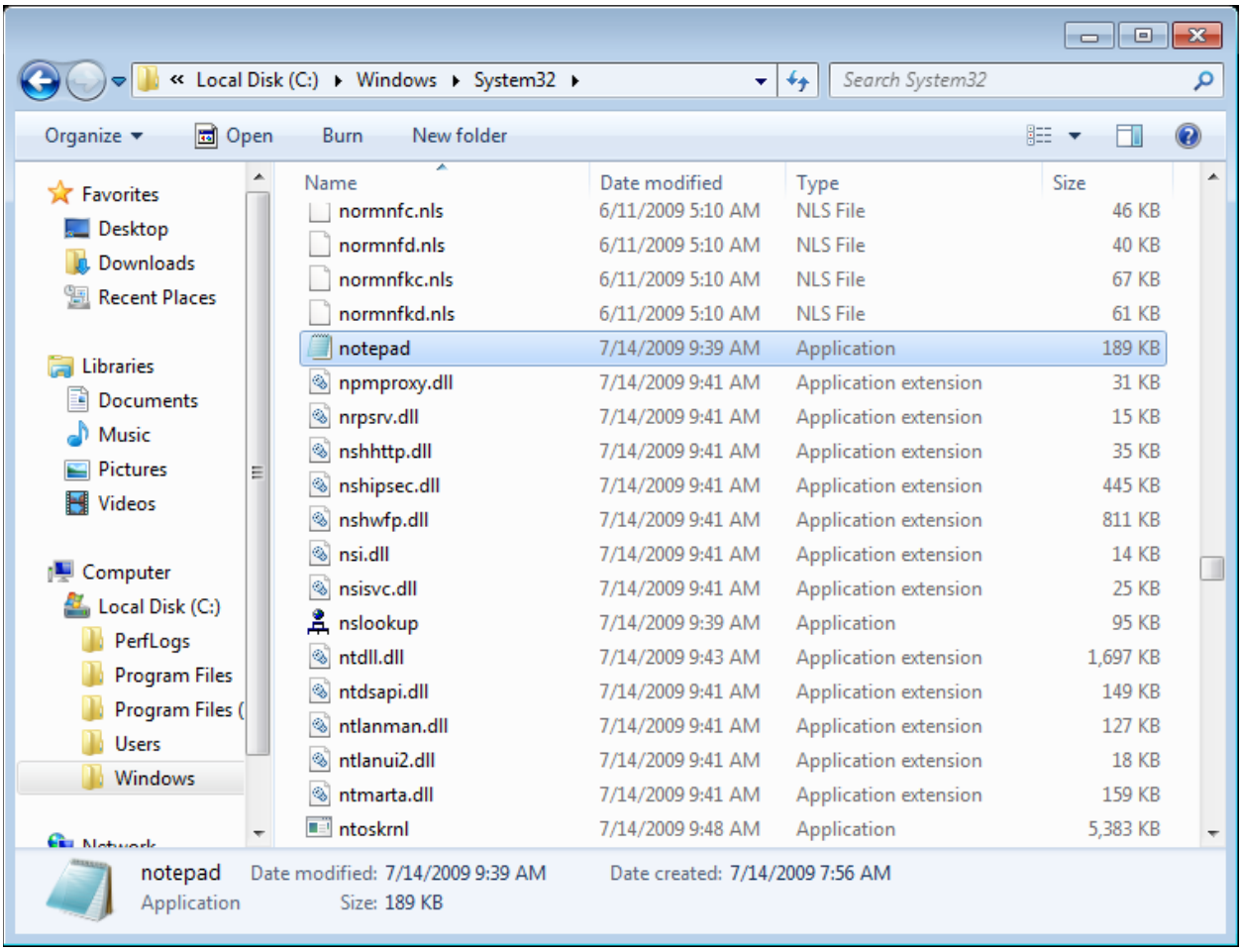
2. Switch to the **Student** account.

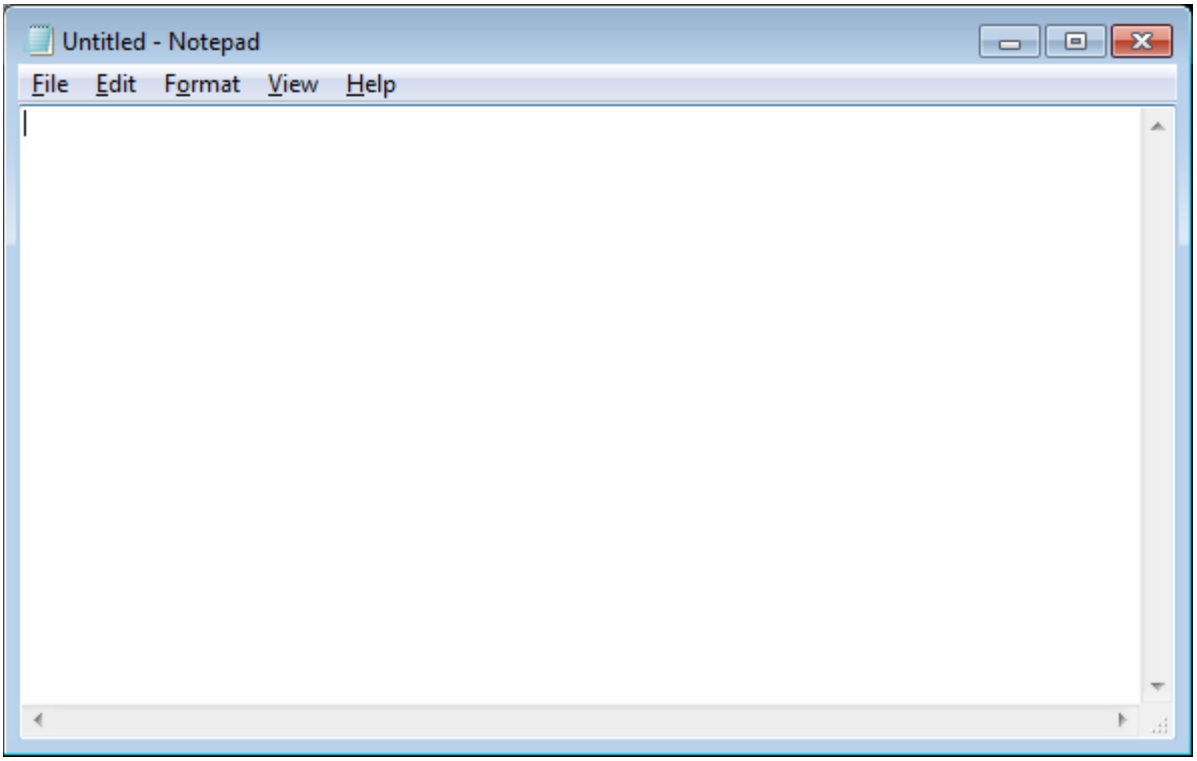
Question 6

Try to run the "notepad.exe". Can you execute it? If yes, what settings can prevent the Student account from running the program?

Answer

Yes. The Student account belongs to 2 groups - IT2524 and Users. Although IT2524 group dis-allowed executing "notepad.exe", the Users group allows executing it. Use the "Deny" settings instead.

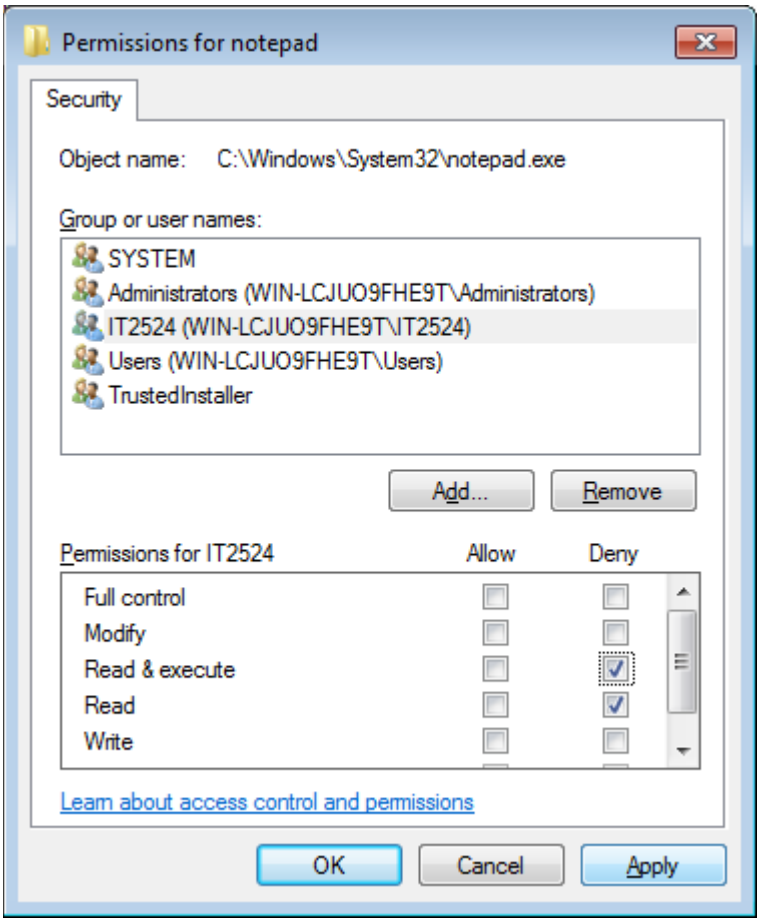


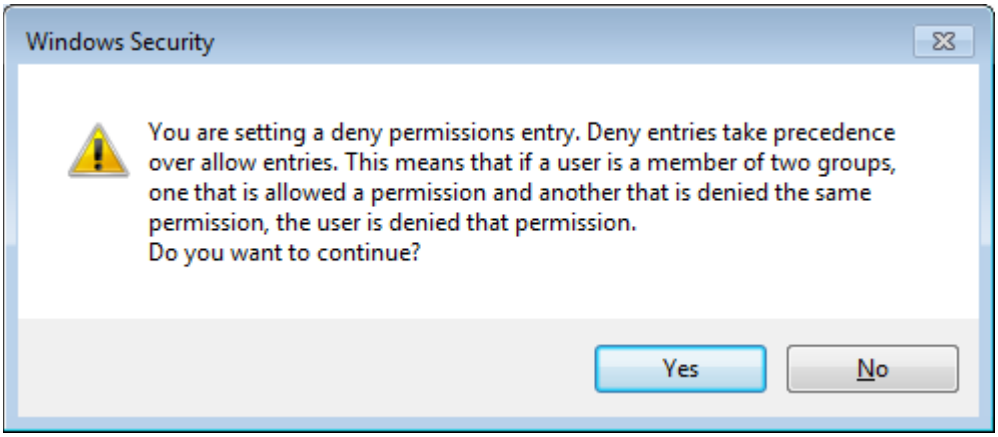


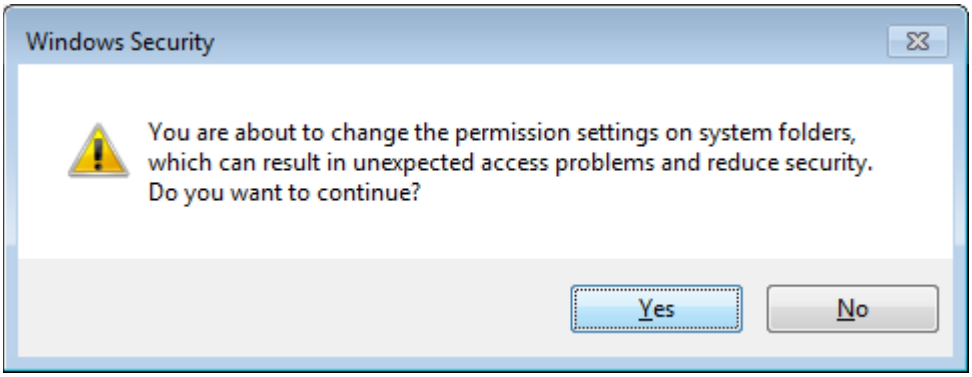
Logoff the Student account.

3. Switch to the SIT account.

   Set the permission to read and execution "Deny" for the IT2524 group.



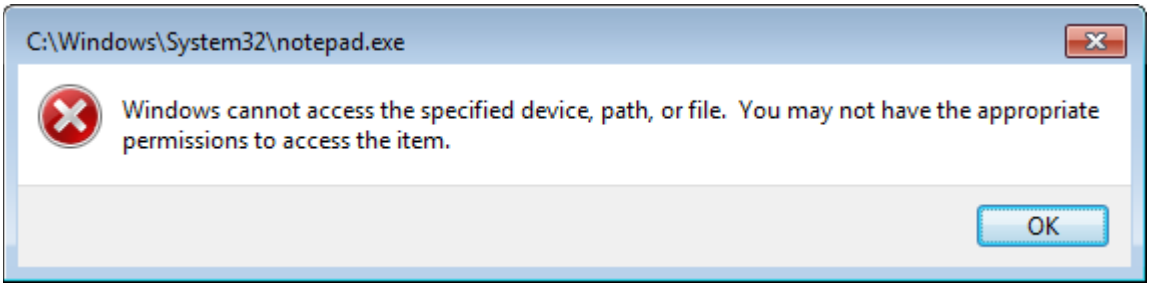




4. Switch to the Student account.

Question 7
Try to run the "notepad.exe". Can you execute it?

Answer
No.



Note
Deny entries take precedence over allow entries. If a user is a member of 2 groups, one allowed permission and the other denied the same permission, the user is denied of that permission.

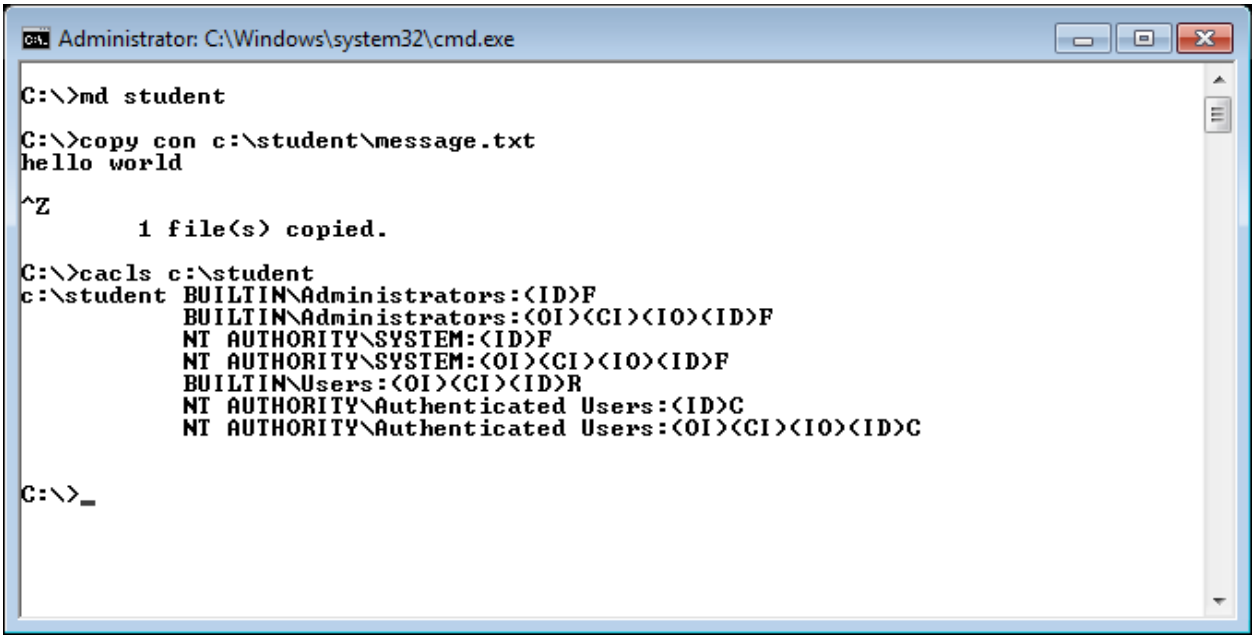
Exercise 6 – Access Control List in MS Windows

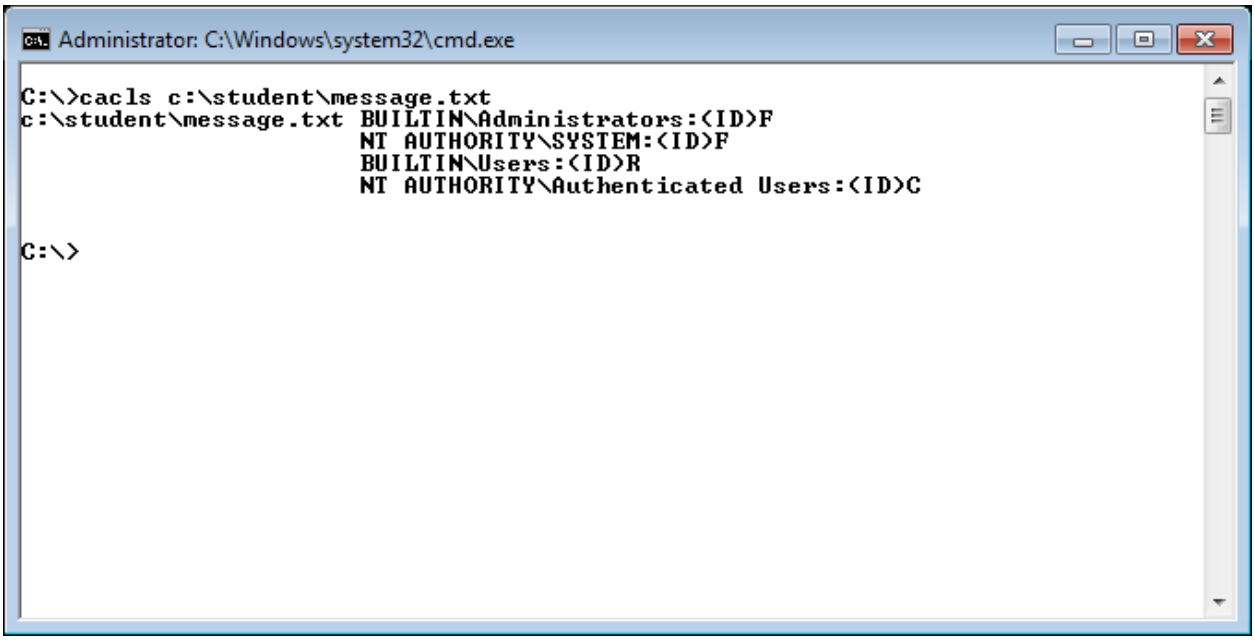
1. Login as **SIT**.
   Goto 'Programs' → 'Accessories', right-click on 'Command Prompt' and choose 'Run As Administrator'.

   The **cacls** command displays or modifies access control lists (ACLs) of folders and files.

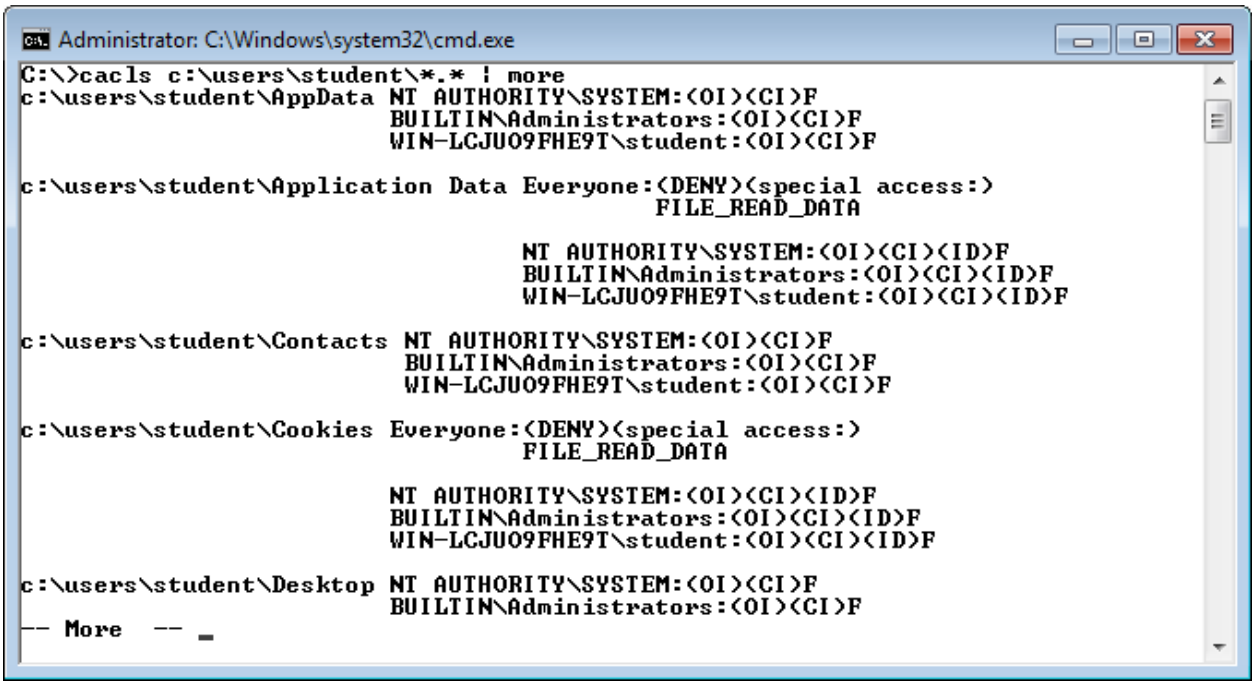
   > **Note**
   > An **Access Control List** is a list of permissions for securable object, such as a file or folder that controls the access to the object.

   List the permissions of a folder and the permissions of a file.

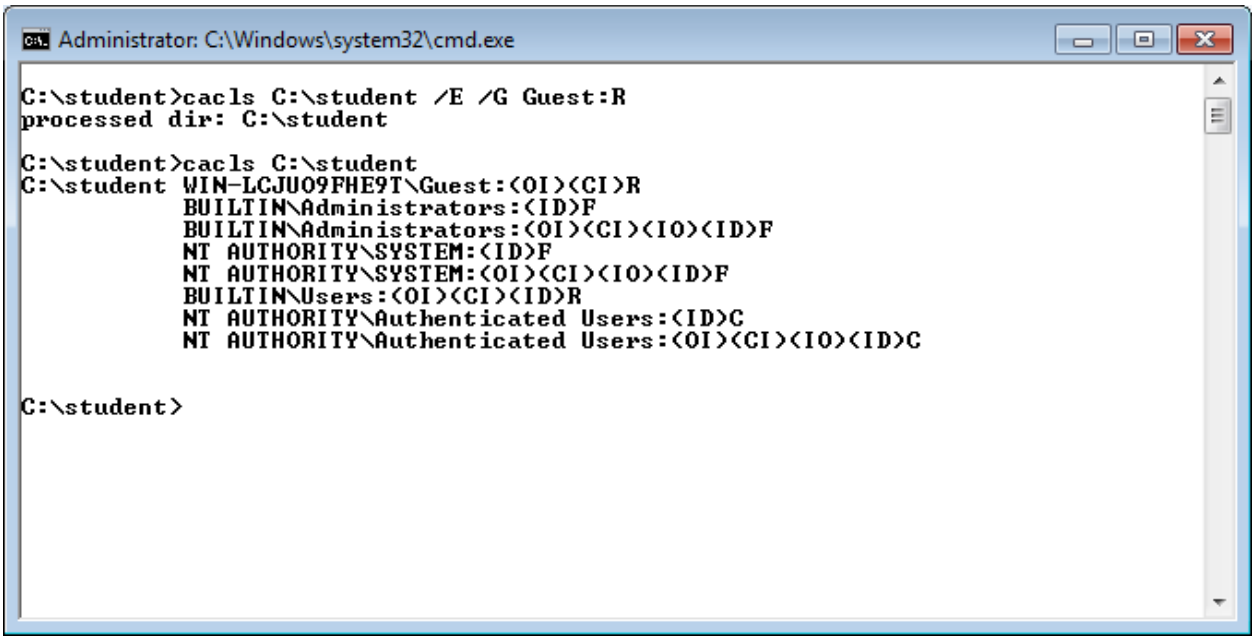




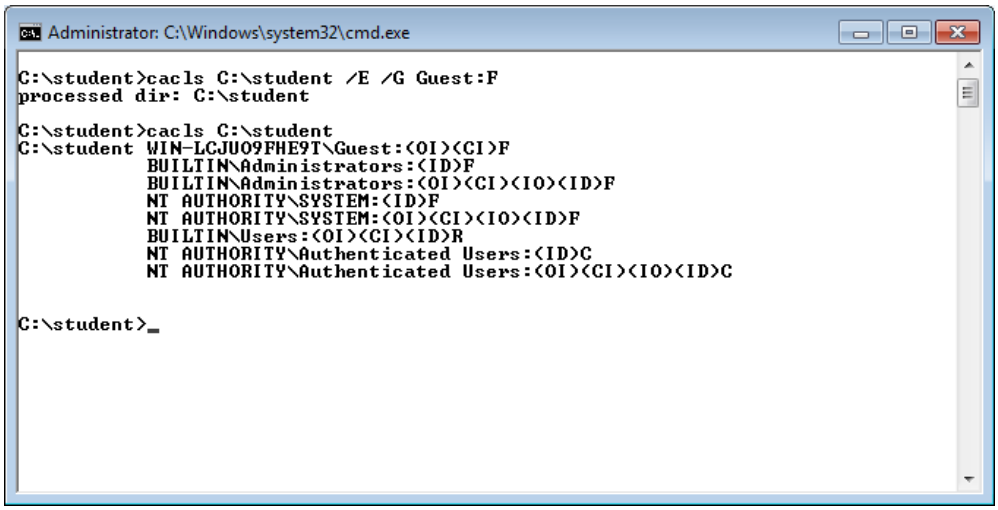
List the permissions of all files in a folder.



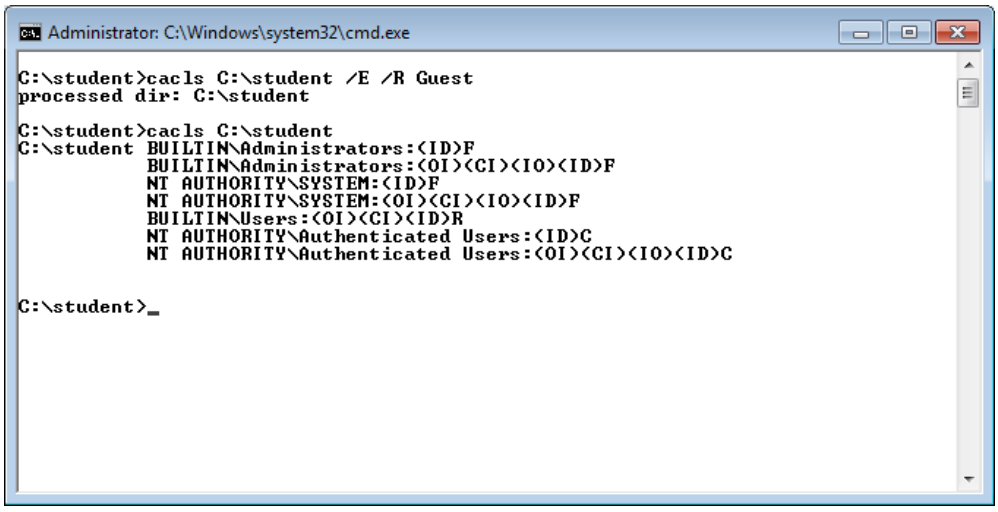
Run the "**cacls** /E /G Guest:R" command to grant Guest account read access to the folder.



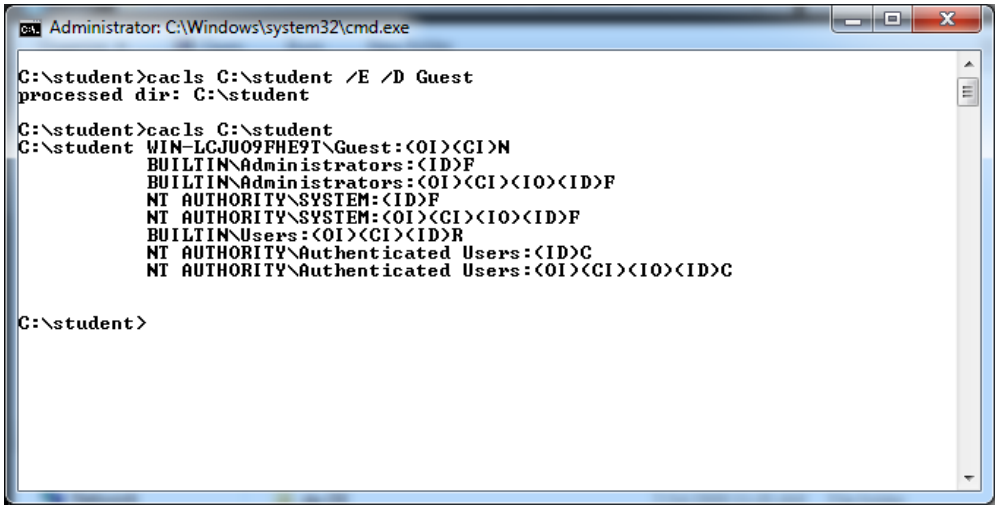
Run the "**cacls** /E /G Guest:F" command to grant Guest account full access to the folder.



Run the "**cacls** /E /R Guest" command to revoke Guest access to the folder.



Run the "**cacls** /E /D Guest" command to deny Guest access to the folder.

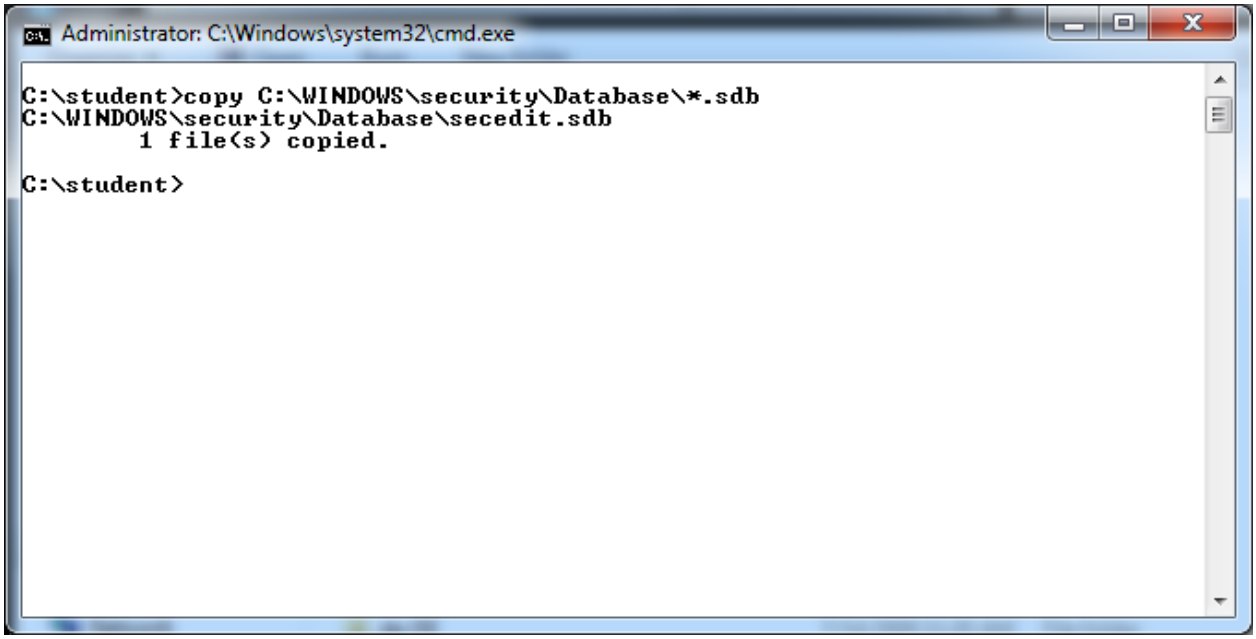


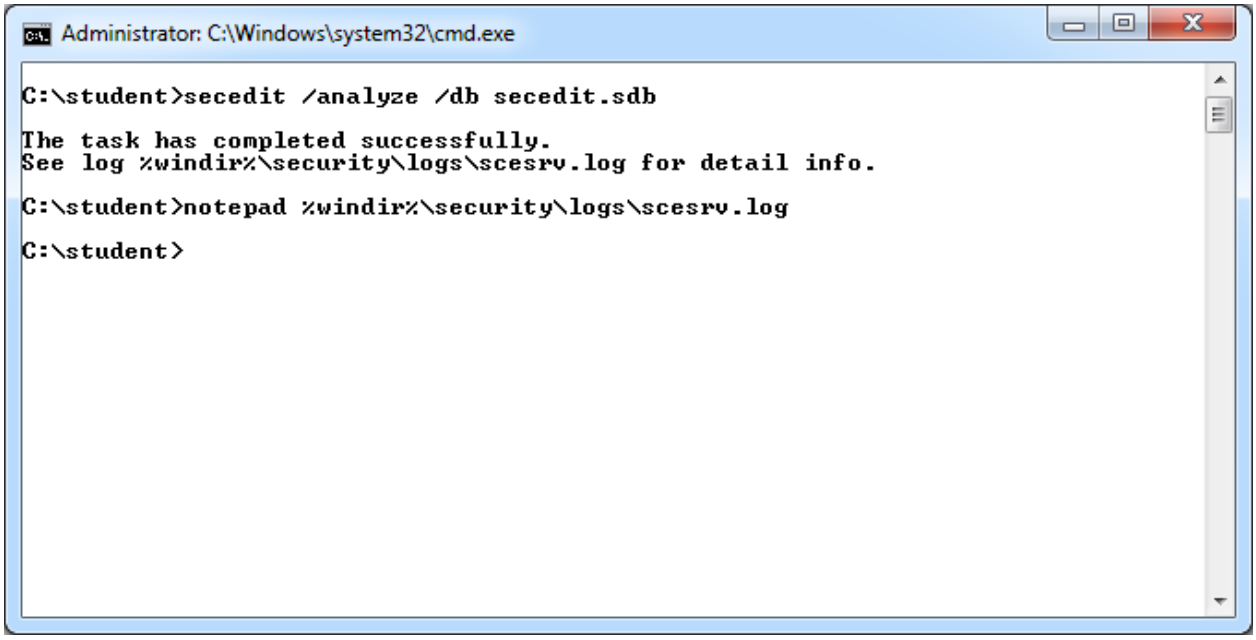
Exercise 7 – Security Configuration in MS Windows

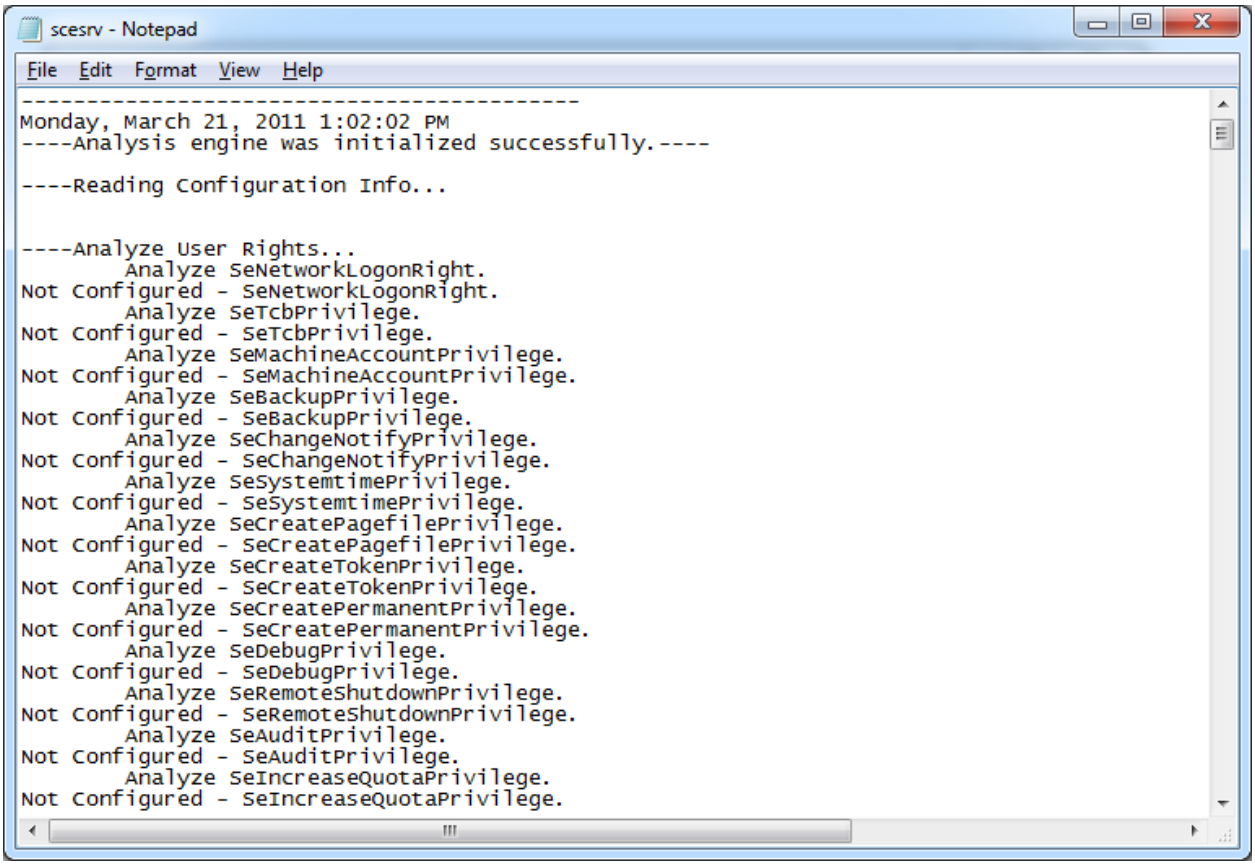
1. One of the biggest challenges for administrators is security compliance. In this exercise, you will learn the **secedit** command to help you to check for compliance.

> **Note**
> Security template is used to define the organization security policy. To check if a system adheres to the security policy, a template that defines the security policy is compared with the existing settings of the system. Any discrepancies mean that the system is not in compliance.

> **Note**
> The **secedit** command has six primary functions:
> - configure
> - analyze
> - import
> - export
> - validate
> - generate rollback

2. 


Administrator: C:\Windows\system32\cmd.exe
C:\student>secedit /analyze /db secedit.sdb
The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
C:\student>notepad %windir%\security\logs\scesrv.log
C:\student>

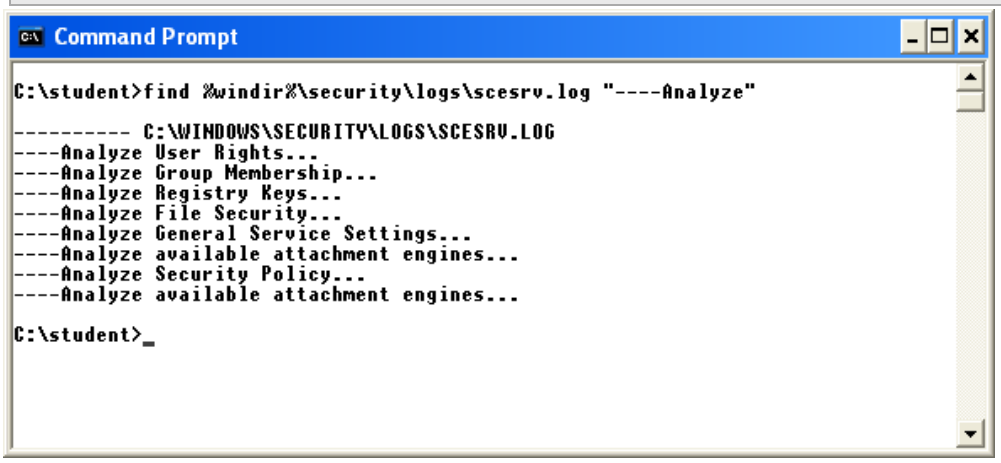

scesrv - Notepad
File Edit Format View Help
Monday, March 21, 2011 1:02:02 PM
----Analysis engine was initialized successfully.----
----Reading Configuration Info...
----Analyze User Rights...
Analyze SeNetworkLogonRight.
Not Configured - SeNetworkLogonRight.
Analyze SeTcbPrivilege.
Not Configured - SeTcbPrivilege.
Analyze SeMachineAccountPrivilege.
Not Configured - SeMachineAccountPrivilege.
Analyze SeBackupPrivilege.
Not Configured - SeBackupPrivilege.
Analyze SeChangeNotifyPrivilege.
Not Configured - SeChangeNotifyPrivilege.
Analyze SeSystemtimePrivilege.
Not Configured - SeSystemtimePrivilege.
Analyze SeCreatePagefilePrivilege.
Not Configured - SeCreatePagefilePrivilege.
Analyze SeCreateTokenPrivilege.
Not Configured - SeCreateTokenPrivilege.
Analyze SeCreatePermanentPrivilege.
Not Configured - SeCreatePermanentPrivilege.
Analyze SeDebugPrivilege.
Not Configured - SeDebugPrivilege.
Analyze SeRemoteShutdownPrivilege.
Not Configured - SeRemoteShutdownPrivilege.
Analyze SeAuditPrivilege.
Not Configured - SeAuditPrivilege.
Analyze SeIncreaseQuotaPrivilege.
Not Configured - SeIncreaseQuotaPrivilege.

Question 8

The **secedit** command performs a number of analyses. Write a command in CMD.EXE to list all the analysis performed recorded in the "scesrv.log" file.

Sample output file

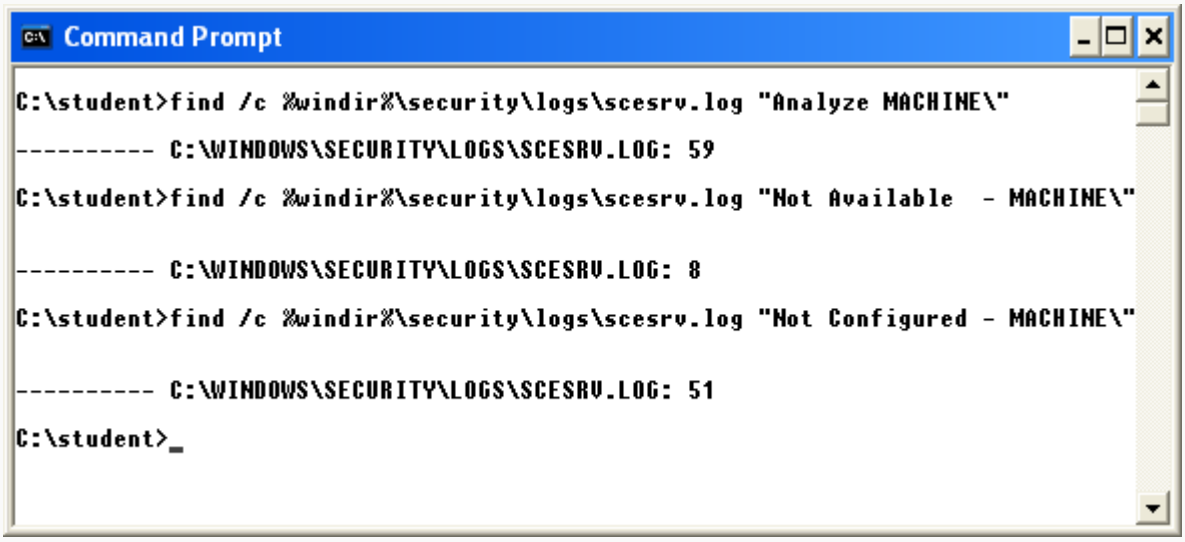
```
----Analyze User Rights...
----Analyze Group Membership...
----Analyze Registry Keys...
----Analyze File Security...
----Analyze General Service Settings...
----Analyze available attachment engines...
----Analyze Security Policy...
----Analyze available attachment engines...
```



Question 9

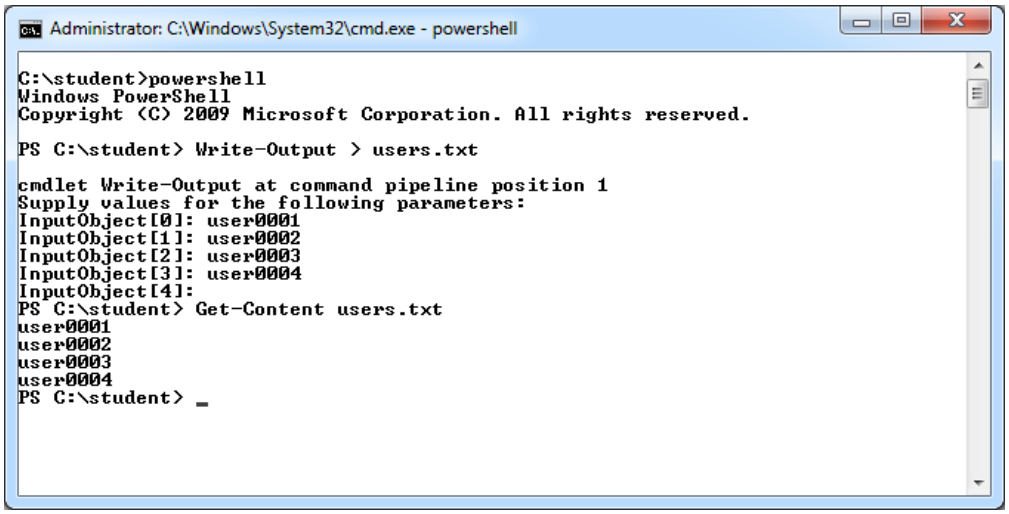
Write commands to count the total number of registry keys, the number of "Not Available" and the number of "Not Configured" registry keys recorded in the "scesrv.log" file. Verify your answers.

Answer

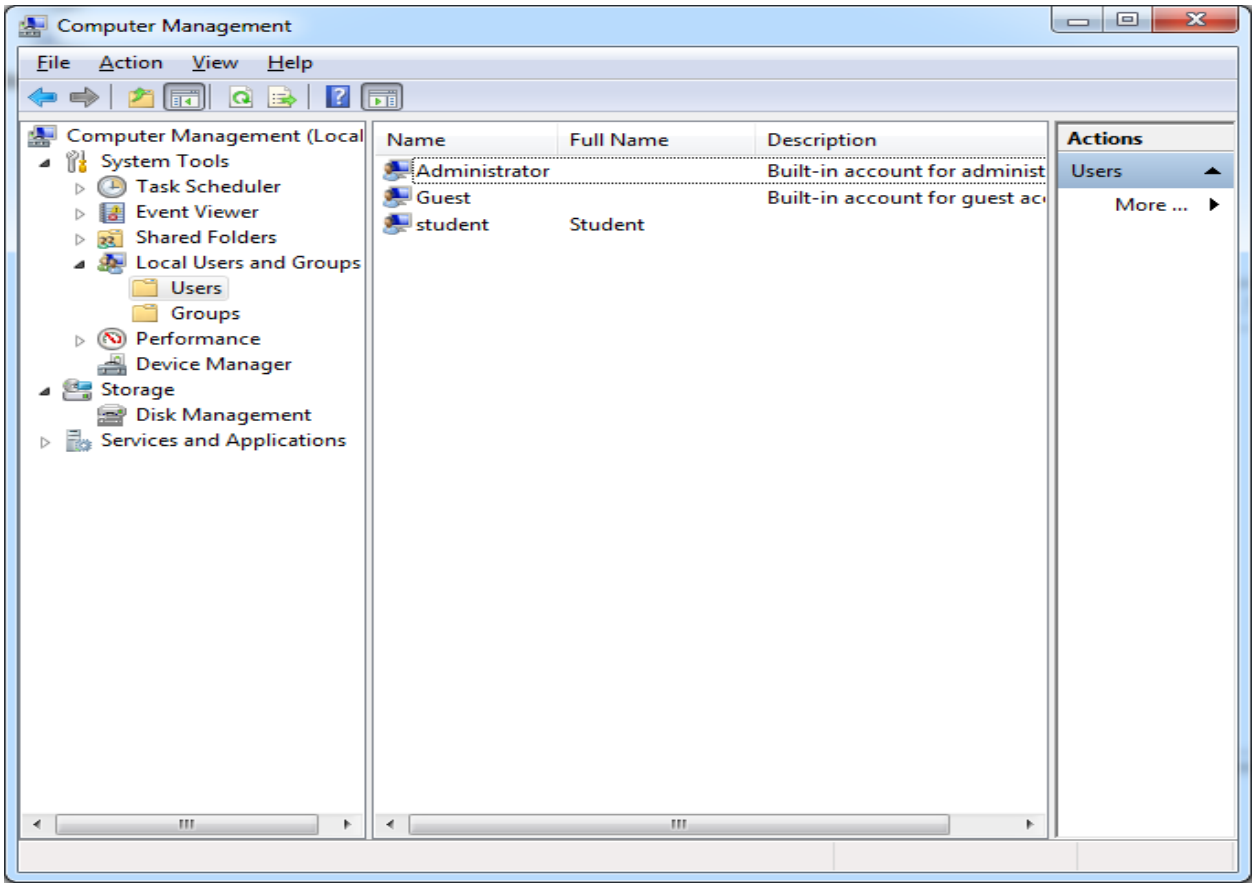


Exercise 8 – Account Management in MS Windows & Active Directory Services

1. The scenario for this exercise is creating new user accounts in bulk. The usernames to be recreated are listed in the "users.txt" file.
   Login as **SIT**.
   Follow the steps as shown to create "users.txt" file.



2. Use the Computer Management Console to verify that the user accounts to be created are not found in the system.



Write a Window PowerShell script to read "users.txt" and create account for the users listed in the file.

LISTING 4-1: create.ps1

```
$userlist=Get-Content users.txt
$host_name=hostname
foreach ($user in $userlist)
{
      $target=[ADSI]"WinNT://$host_name"
      $newuser=$target.Create("user", $user)
      $newuser.SetPassword("student")
      $newuser.SetInfo()
      $newuser.description = "Created by Windows PowerShell"
      $newuser.SetInfo()
      $newuser.psbase.InvokeSet('AccountDisabled', $false)
      $newuser.SetInfo()
      Write-Host "$user created"
}
```

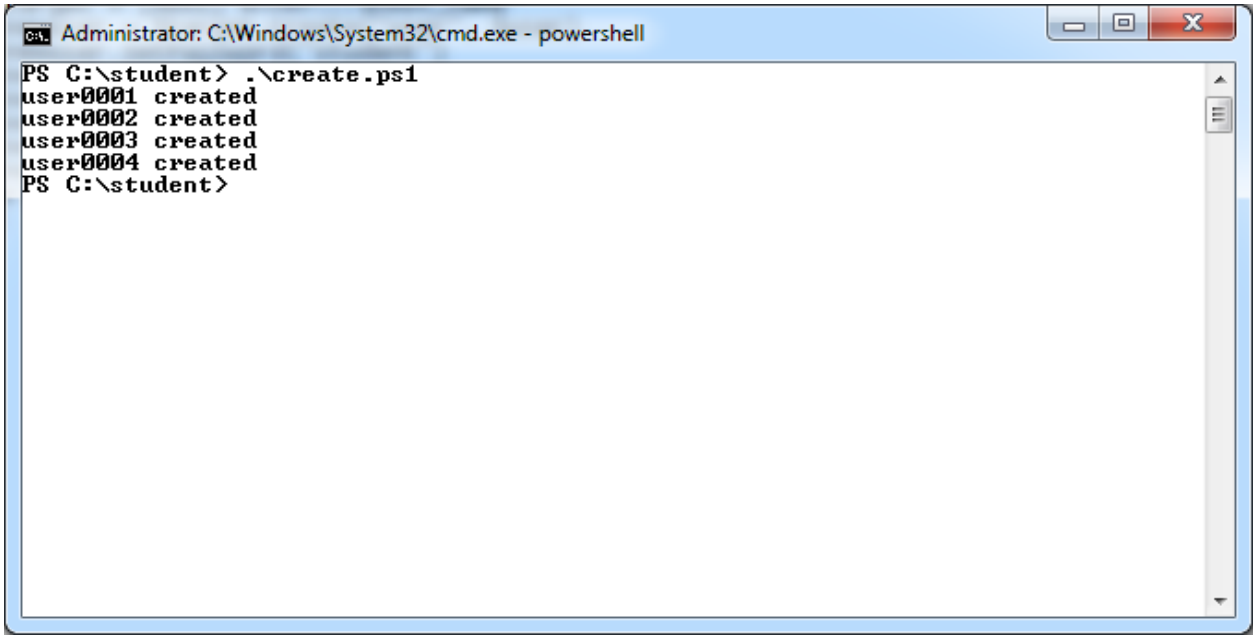
Note

Active Directory Service Interfaces (ADSI) is used to access features of the directory services. ADSI provides a single set of directory service interfaces for managing network resources in a distributed computing environment.

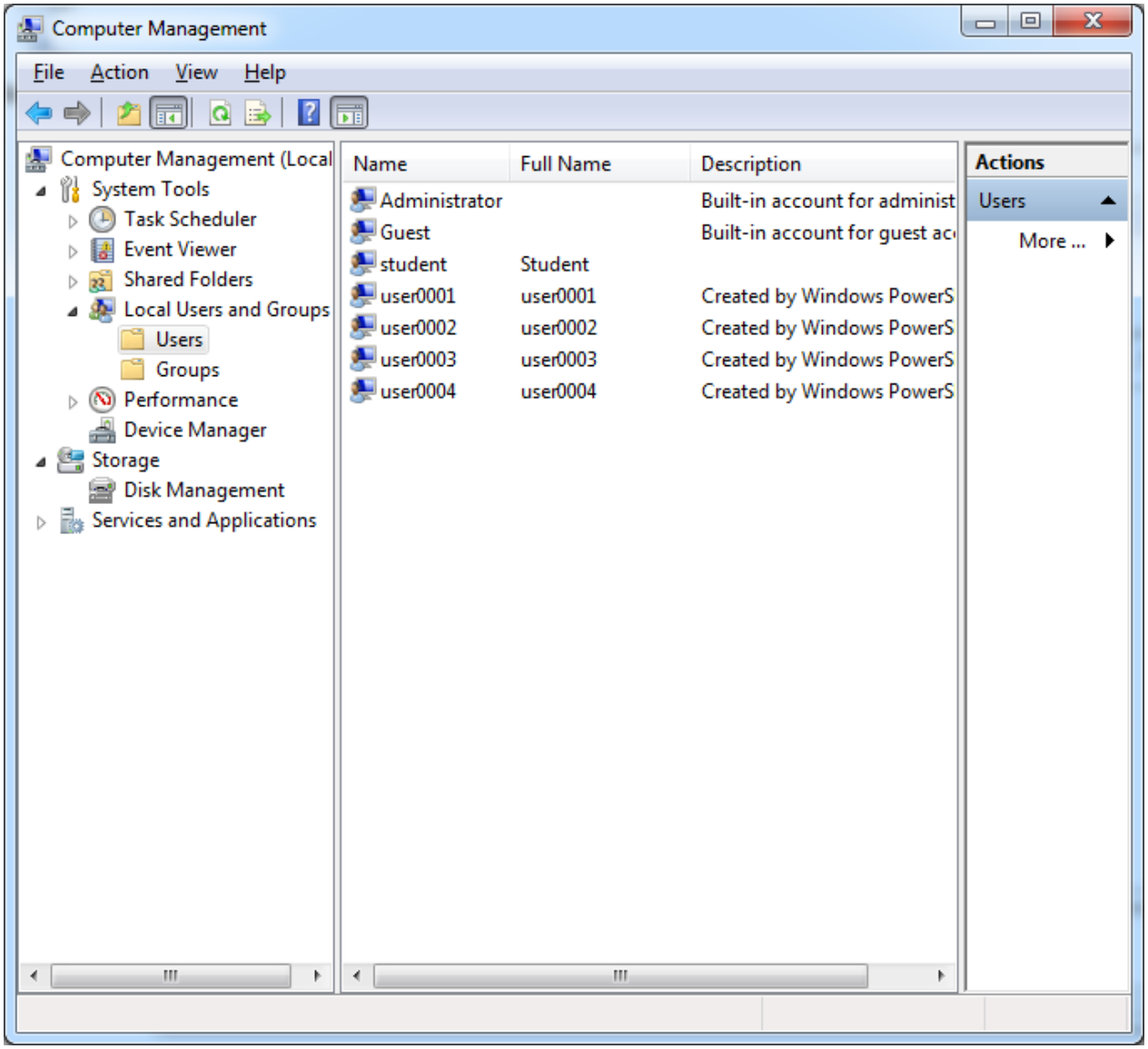
3. Run "create.ps1" to create the accounts.

You may need to first set the execution policy by running this command:

set-executionpolicy RemoteSigned



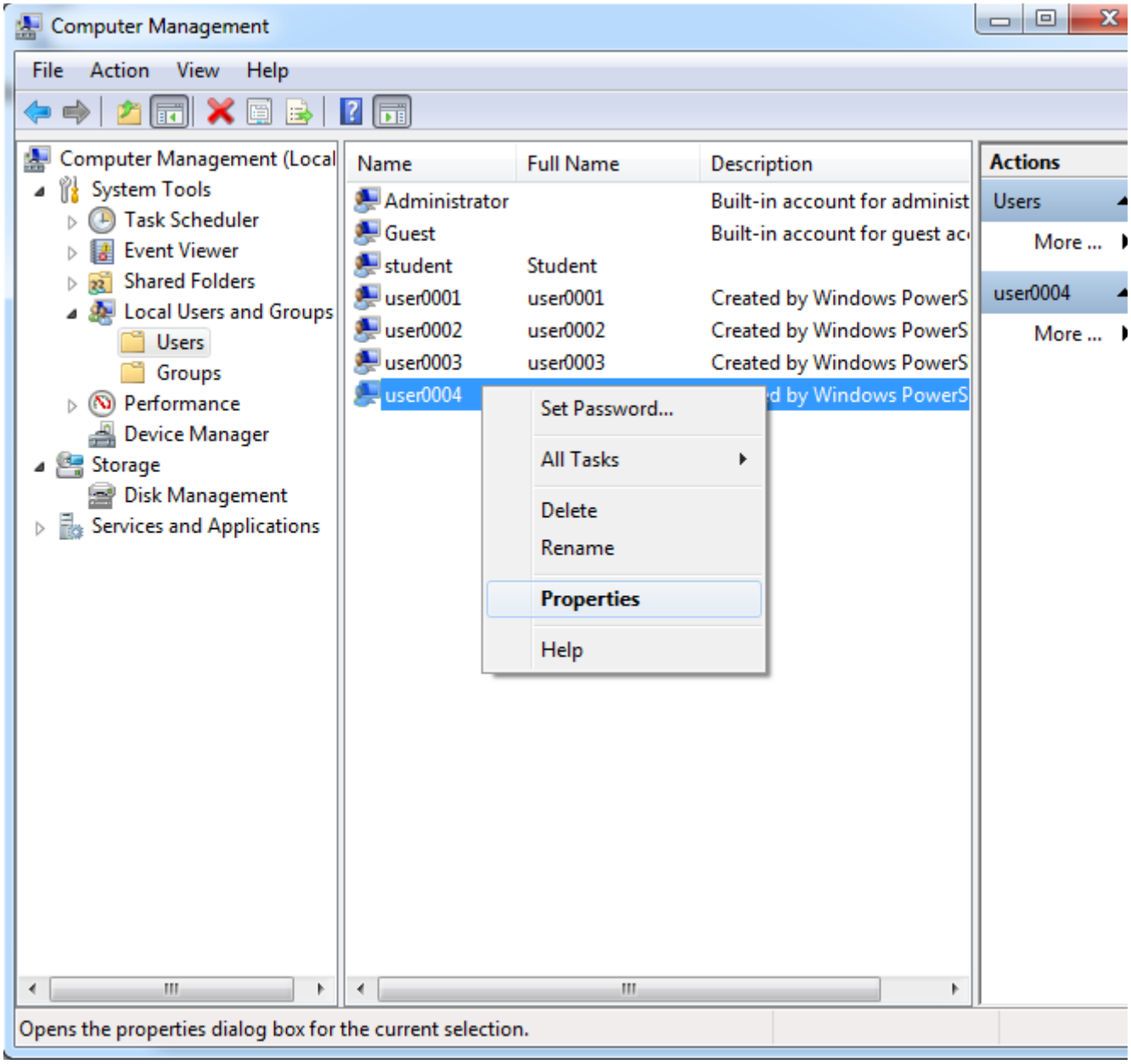
Use the Computer Management Console to verify that the user accounts are created successfully.

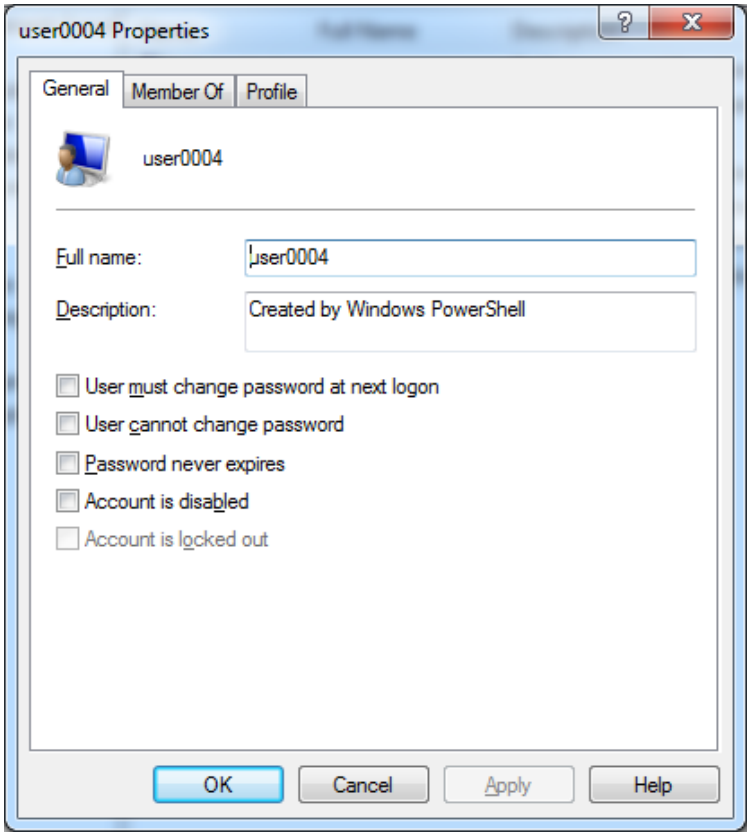


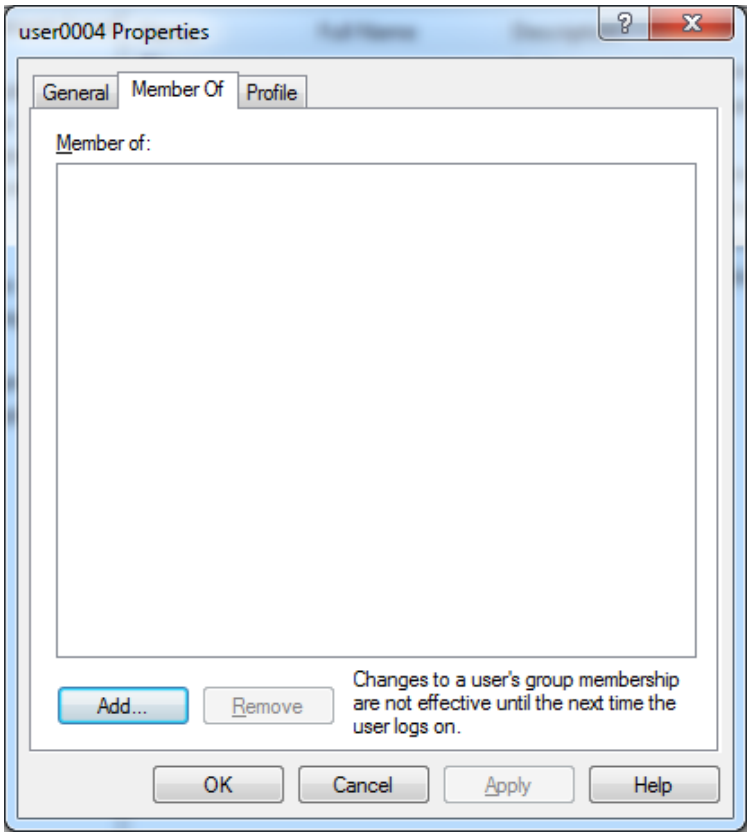
Question 10

Is the newly created user accounts member of any group?

No, the group is not specified in the script.




user0004 Properties
General
Member Of
Profile
user0004
Full name:
user0004
Description:
Created by Windows PowerShell
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Account is locked out
OK
Cancel
Apply
Help


user0004 Properties
General
Member Of
Profile
Member of:
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

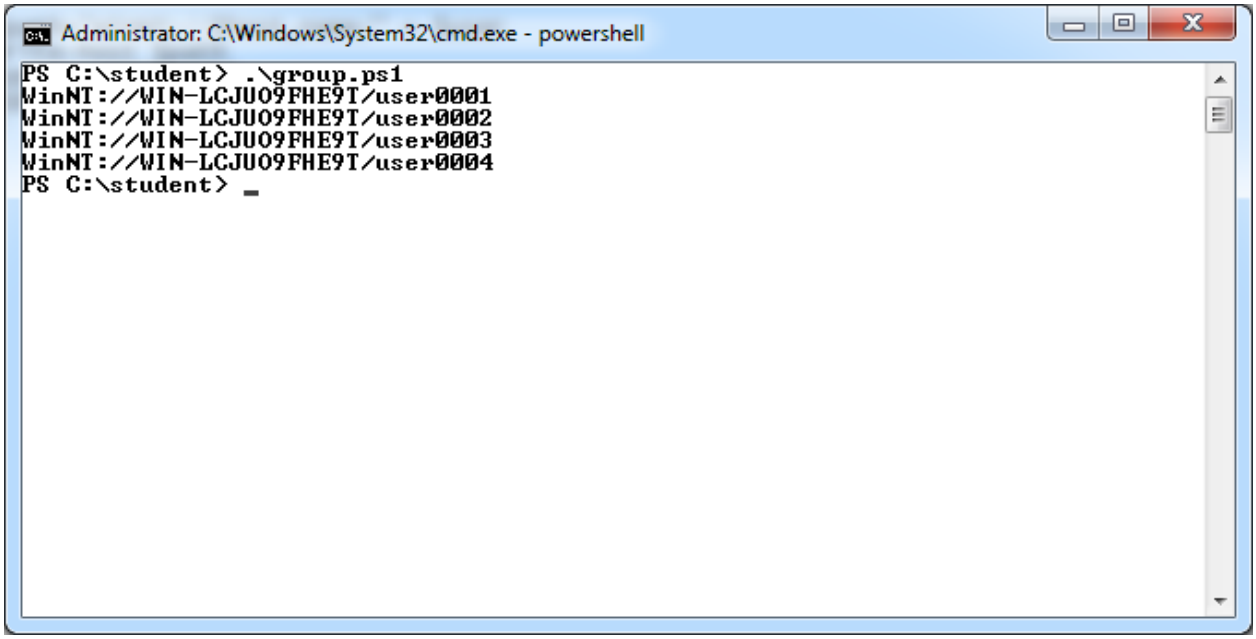
Write a Window PowerShell script to read "users.txt" and assign all the user accounts to the Guests group.

4 **LISTING 4-2**: group.ps1

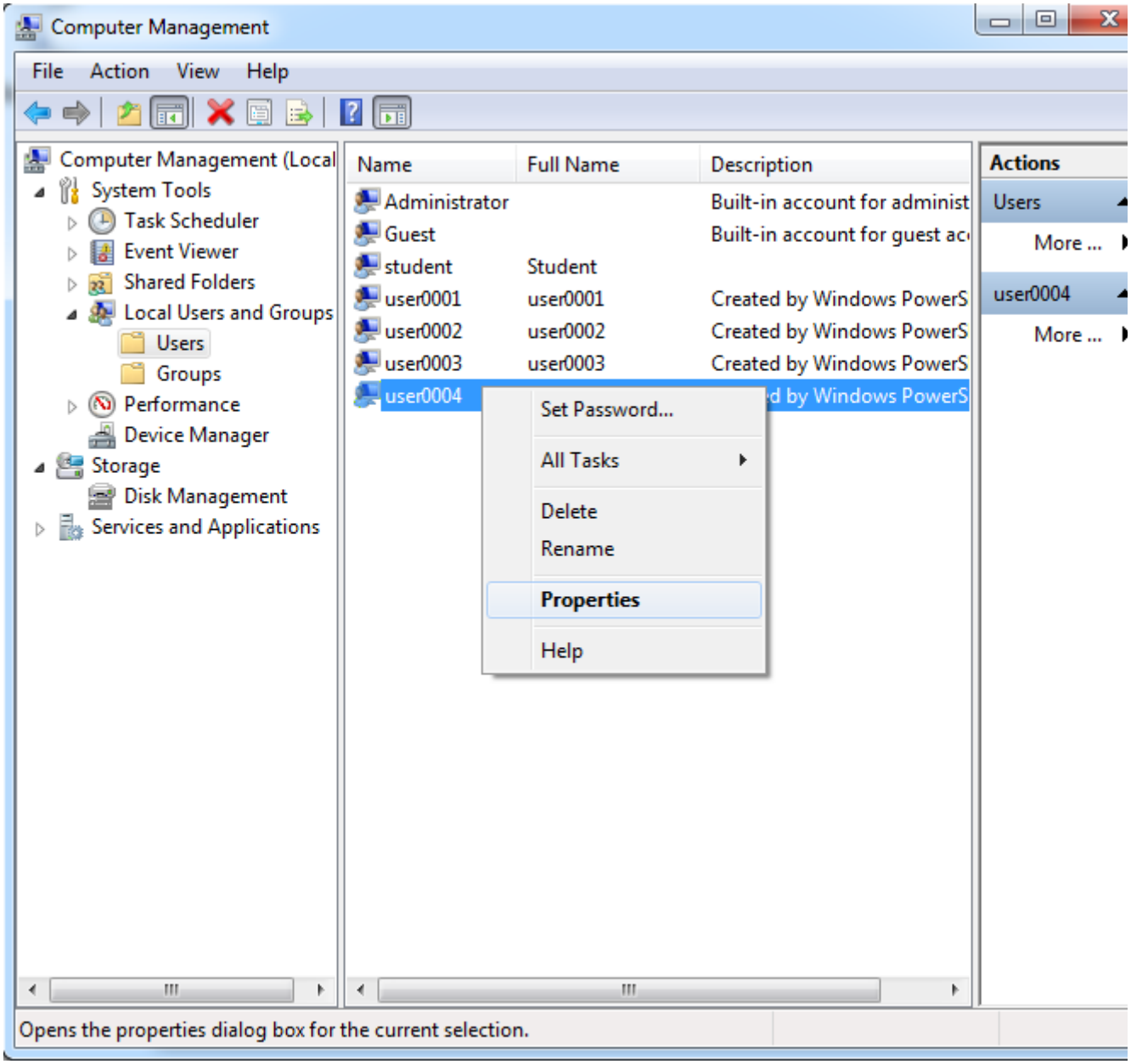
```
$userlist=Get-Content users.txt
$host_name=hostname
$group=[ADSI]("WinNT://$host_name/Guests")
foreach ($user in $userlist)
{
      $path="WinNT://$host_name/" + $user
      Write-host $path
      $group.add($path)
      $group.SetInfo()
}
```

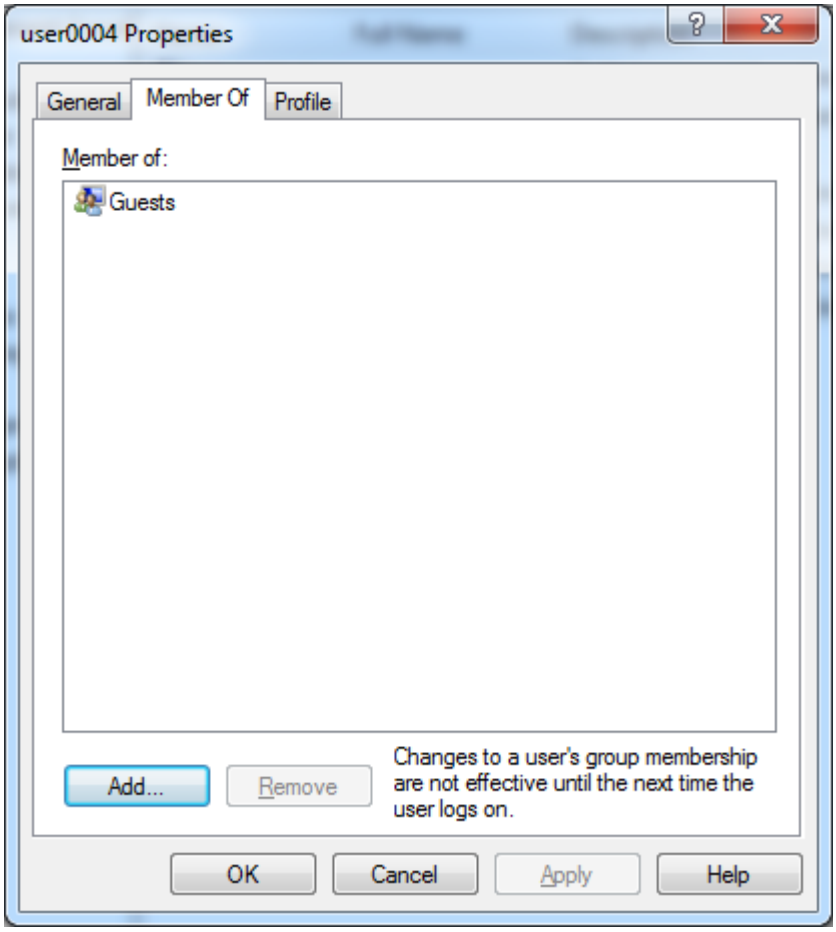
Run the script to assign the user accounts to the Guests group.

5



Use the Computer Management Console to verify that the user accounts are assigned to the correct group.





Question 11

Can you login to the accounts you have just created?

Note: By default the Guest account is deny log on locally.

Answer : Yes

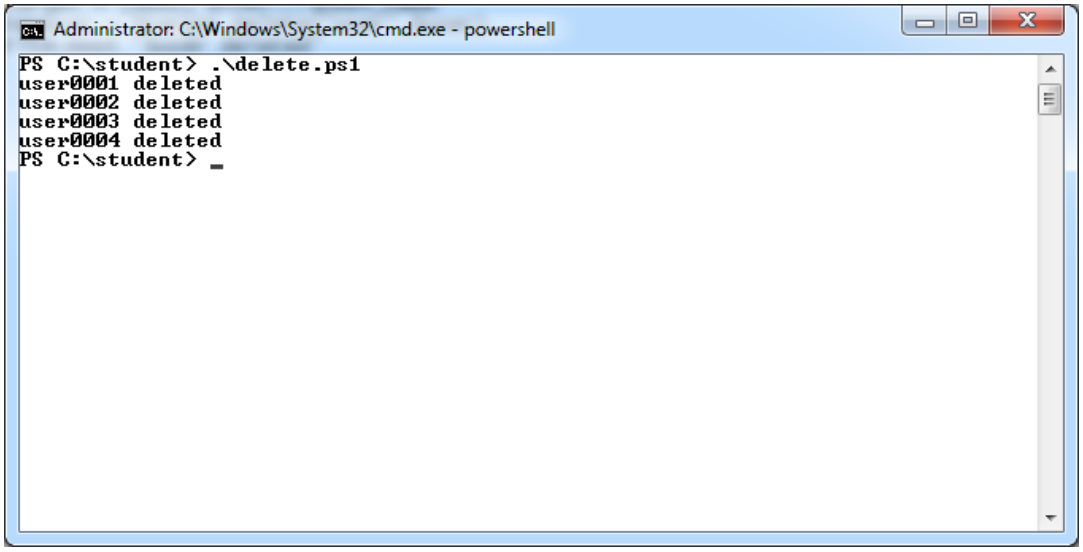
Question 12

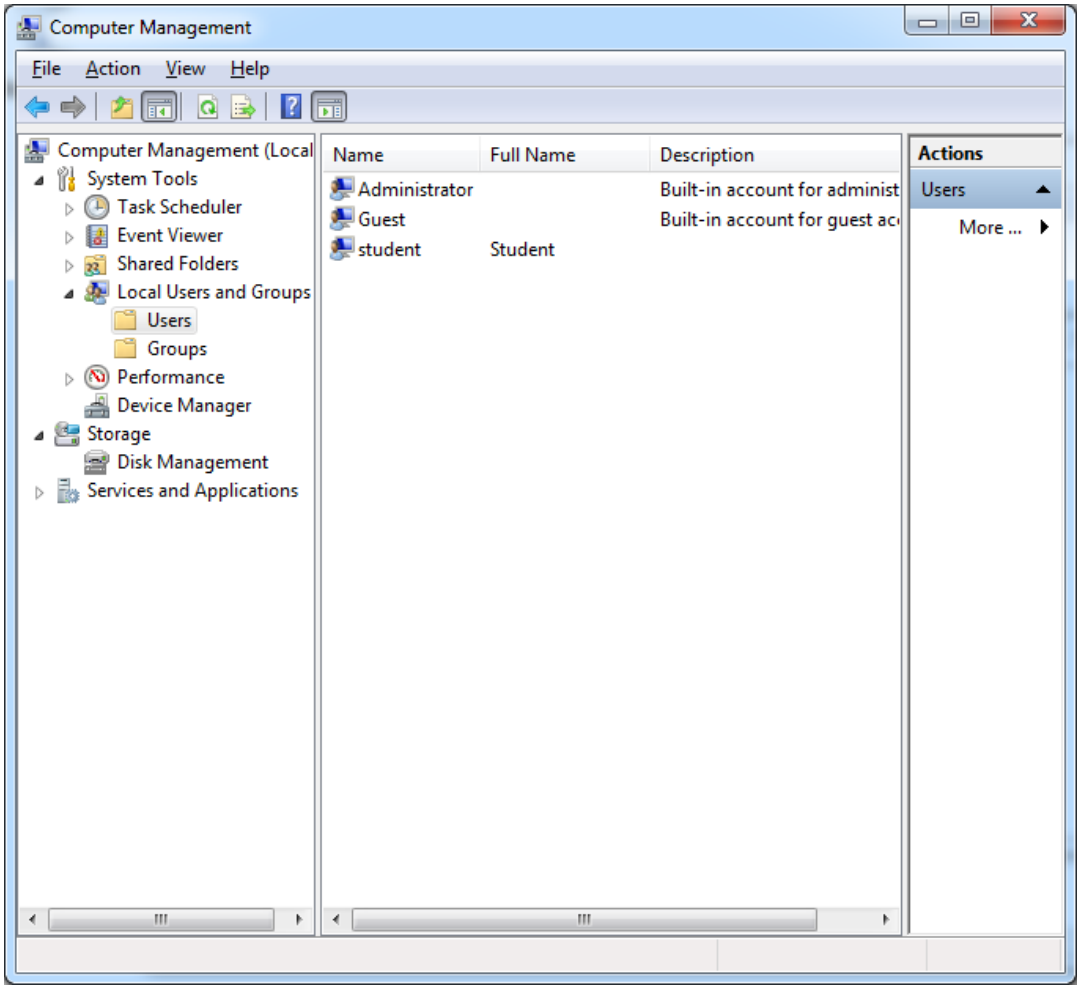
The user accounts created are no longer required. Write a Window PowerShell script to delete them. Name the script as "delete.ps1".

delete.ps1:

```
$userlist=Get-Content users.txt
$host_name=hostname
foreach ($user in $userlist)
{
     $target = [ADSI]"WinNT://$host_name"
     $newuser = $target.Delete("user", $user)
     Write-Host "$user deleted"
}
```

6
.





- End of Practical -