**CSI3670**

**Winter 2019**

**Lab 5b: Group Policy**

**Due March 21st at 11:59pm**

**Synopsis:**

In this lab, we’ll create a local user and destroy their self-confidence by locking down their machine. We’ll also do some file sharing so that you can share files between teams.

**New User Creation**

First, let’s create a user that you’ll manage. Congratulations, you are now supervising somebody else. You should get a bump in pay, but unfortunately we don’t have the available budget for raises at the moment.

1) Login to your GCP VM (you should have ADDS installed on there from a prior lab).

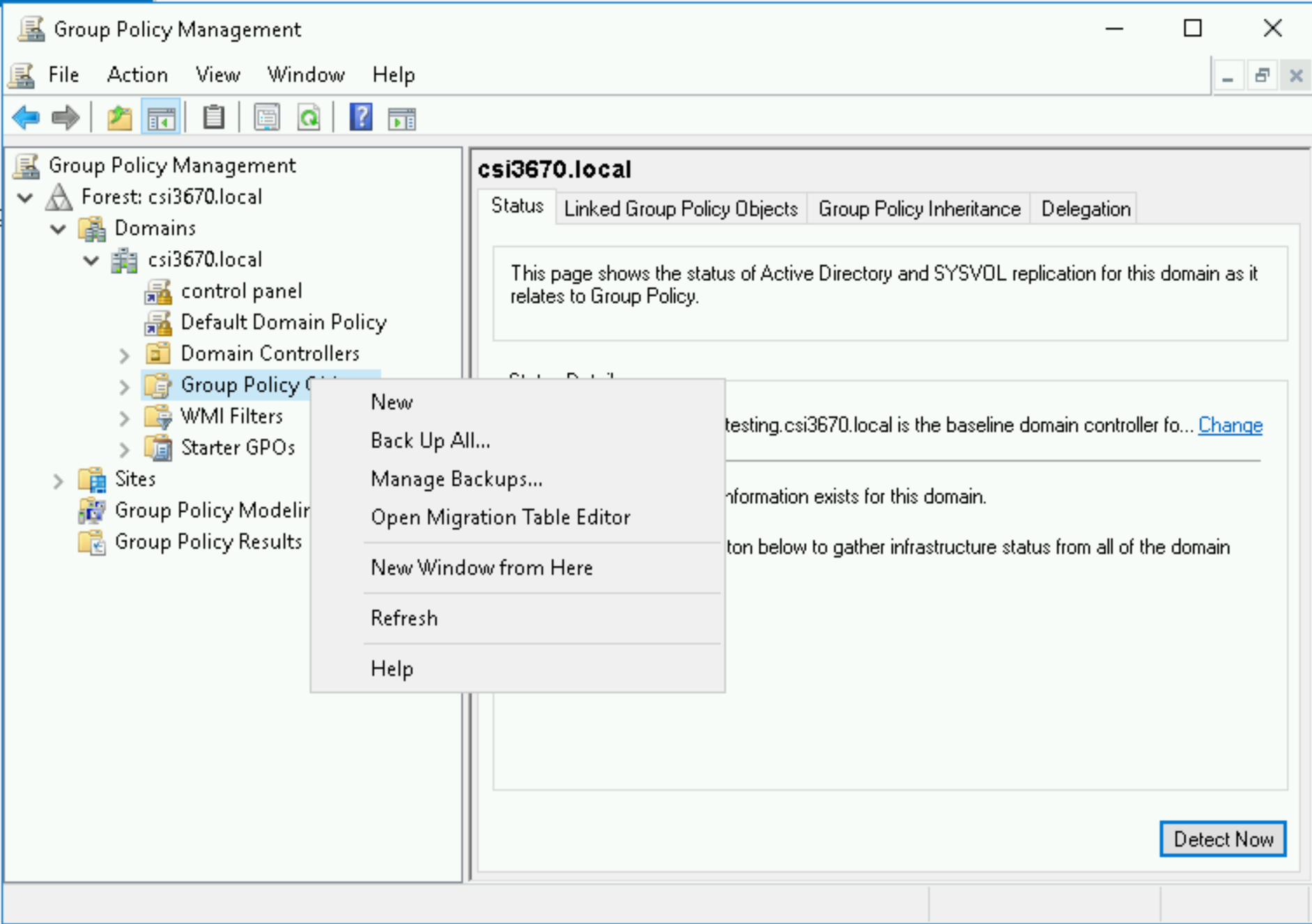
2) Open up the AD Users and Computers window. Under the Users folder, create a new User. Give this user a unique name, something like <yourlastname>-TempUser. Hopefully by now it is obvious that you have to replace <yourlastname>, including the angle brackets.

3) Give this user a password that’s easy for you to remember. Temp12345 will suffice. Uncheck ‘User must change password at next logon.

**4) Take a screenshot of the user after successfully adding and paste into Q8.**

5) Now, let’s create a Group Policy. Open up the Group Policy Management window. Expand Forest (csi3670.local), Domains, and your domain. Right click on Group Policy Objects and click New. Name it <yourlastname>-GPO. **Take a screenshot of your newly-created GPO.**

**Please do not do this on your CTO VM. We do not want rogue group policies infecting our term project forest!**



6) Right-click on your new GPO and click Edit. For this one, assign the following policies to the **User:**

(Remember, to set or restrict a restriction, find it in the tree of possible objects, right-click → Edit, and set to enabled).

**If you get lost in the tree, searching for the right attribute can be … difficult. There are several tools out there, such as** [**https://gpsearch.azurewebsites.net/**](https://gpsearch.azurewebsites.net/) **or simple Googling. Here is a list of methods for finding them:** [**https://4sysops.com/archives/four-ways-to-search-for-group-policy-settings/**](https://4sysops.com/archives/four-ways-to-search-for-group-policy-settings/)

*(This is not an easy task … Googling may give you the fastest result). The HowToGeek website seems to be a decent repository for answers if you search for, say, "disable access to registry, group policy"*

a) Disable access to the Registry

b) Enforce password complexity requirements

c) Disable access to the Control Panel and PC settings

d) Prevent access to the Command Prompt

e) Require password prompt on resume from hibernate/suspend

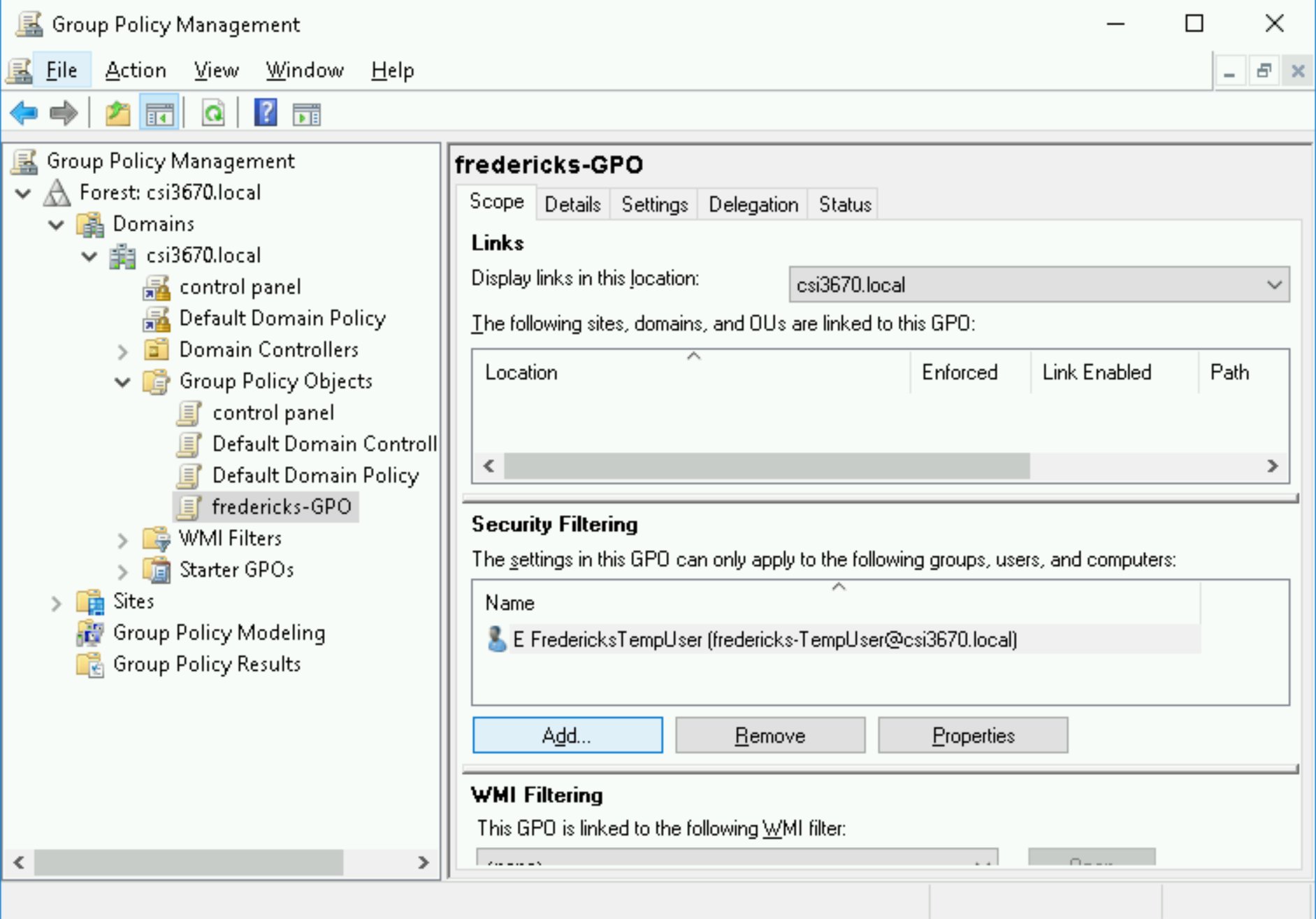
f) Password-protect the screensaver

**Take a screenshot of each line item showing it is being enforced and paste into Q8.**

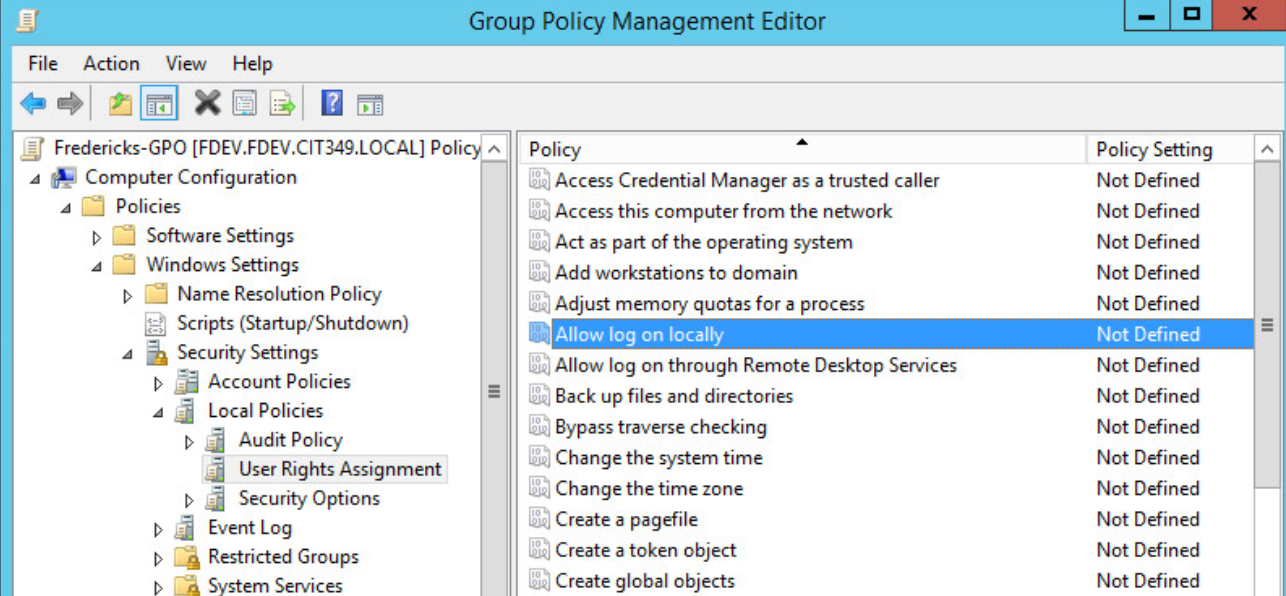
That’s probably good for now. As you can see you can enable/disable nearly everything in Windows via a GPO.

7) Now, we need to apply this GPO to your new user. In the Group Policy Management window, drill down in the left pane until you’ve expanded your domain. Right-click and ‘Link an Existing GPO...’ Add the newly created GPO.

Left-click on your GPO in the left pane. Under Security Filtering, remove ‘Authenticated Users’ and add in your newly-created user. Mine looks like this when I’m done:

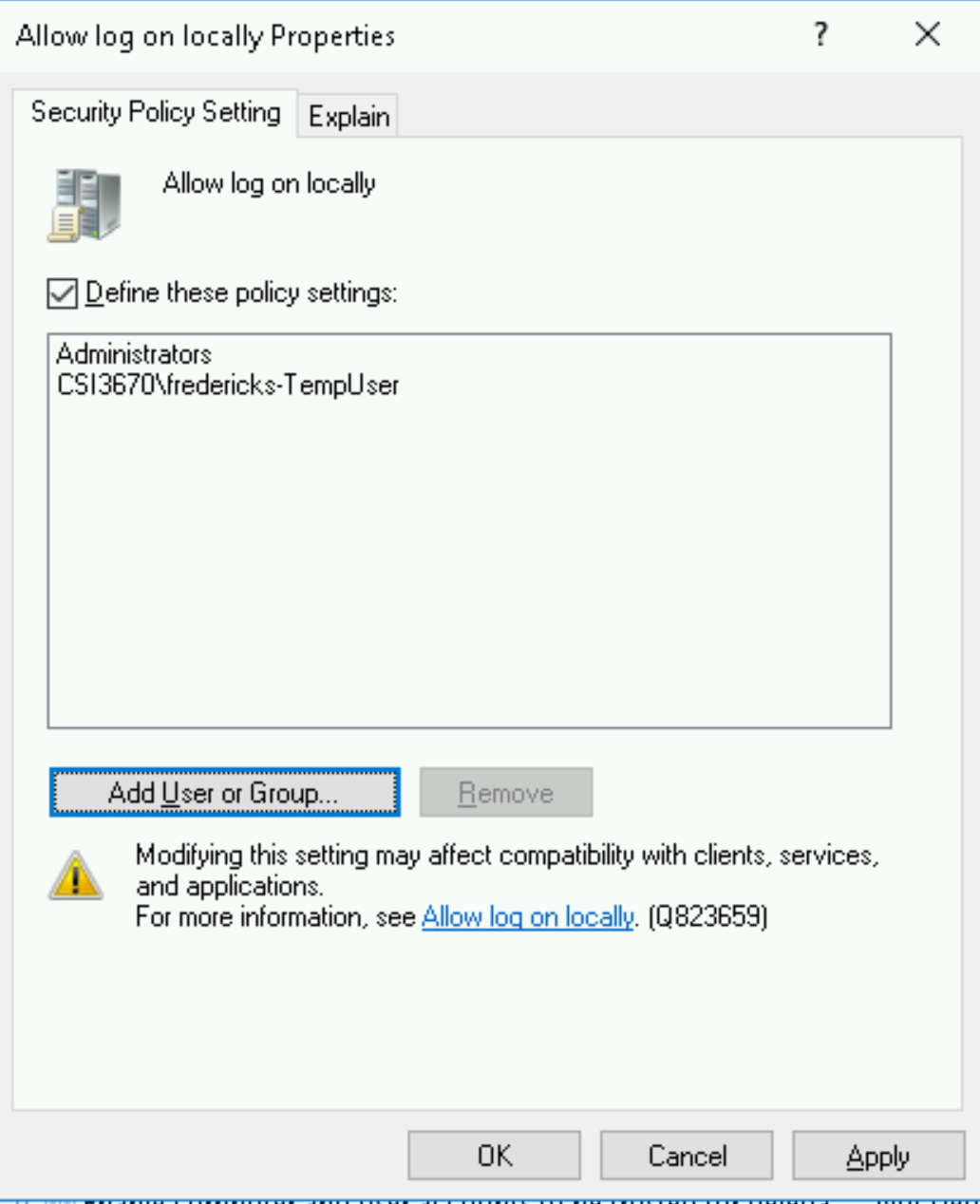


8) We need to allow the new user to login locally. In the Group Policy Management Editor, follow the screenshot:



Right click → Properties → Check: Define the policy settings

Add your username by clicking ‘Add User or Group’ then Browse. Add your username, check names, and OK. You’ll also need to add the Administrators group:



To allow this user access to login locally, we’ll need to add them to the Administrators group. Seems to be a bit of a workaround/hack, but fairly common when trying to login to a DC locally. Open up AD Users and Computers, right click on your user and click Add to Group. Add ‘Domain Admins’ to the field and click OK.

Lastly, open up a command prompt as an Administrator and run: gpupdate /force. If you receive an error logging in (that the method is not allowed), reboot the machine.

*If that did not work, do the exact same set of steps (in 8) for the Default Domain Policy.*

**9) Now, logout and log back in as your new user (you’ll probably need to login as CSI3670\<new username>). Take a screenshot of you:**

**a) Trying to access the Control Panel.**

**b) Trying to access the Registry.**

Finish early? Term project work time then!

**Homework**

1) What is the difference between applying a GPO to a User vs. a Computer?

2) What does it mean for a GPO to be stateless?

3) What is the order that GPOs are applied? What happens if an **enforced** policy is higher in the application level than one that **blocks inheritance**?

4) How would you create a file share, using Windows Server, that could share with a Linux machine?

5) What is the difference between a Group Policy **setting** vs a Group Policy **preference**?

6) What type of GPO would you need to create if you wanted it to apply to any workstation with a particular set of hardware specifications, rather than by user or computer?

7) In terms of group policy, what is required if we are dealing with Windows machines that are different versions? How would you ensure that you can support both the newest and oldest versions of Windows on your network?

8) Make sure you read through carefully and supply all necessary screenshots.