Lab Assignment

Cybersecurity Professional Program

Microsoft Security

Microsoft Security Policies & Authentication

MS-10-L3
Handling Local Security Policies

Lab Objective

Become familiar with Microsoft's security features for local domain environments.

Lab Mission

Implement policies to enhance organizational security.

Lab Duration

30–45 minutes

Requirements

- Basic working knowledge of Windows Server
- Basic working knowledge of Windows Client

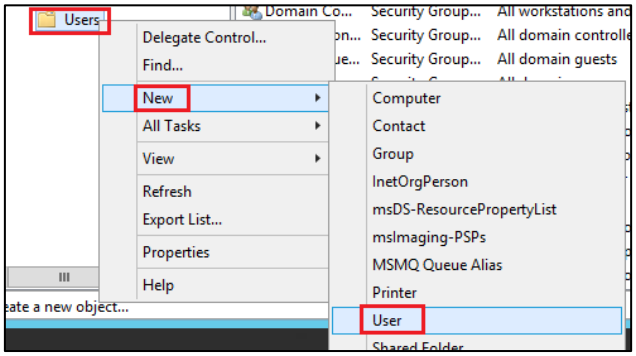
Resources

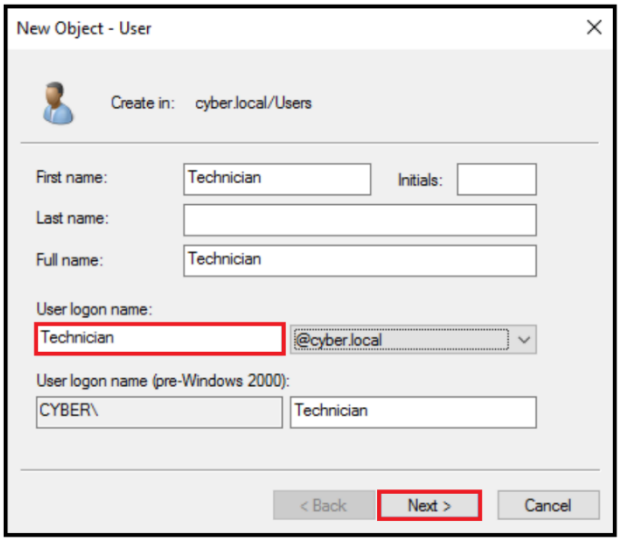
- Environment & Tools
  - VirtualBox
    - Windows Server 2016
    - Windows 10 Client

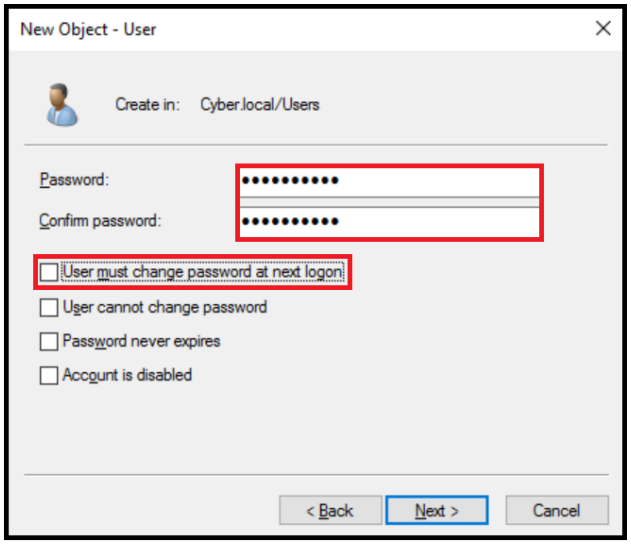
Lab Task 1: Prevent Local Login

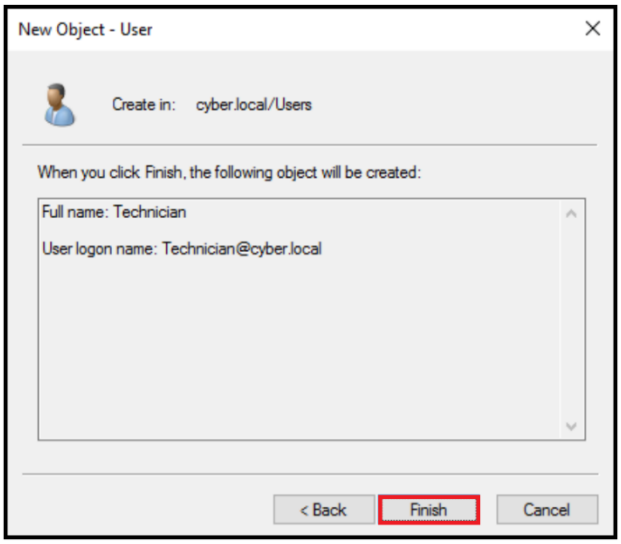
In this task, you will implement a policy to prevent users from logging in to a computer.

1 In **Active Directory Users and Computers**, create a new user **Technician** in the ***Users*** Organizational Unit (OU) for later use in the lab. Assign **Technician** the password **Aa123456!@**.

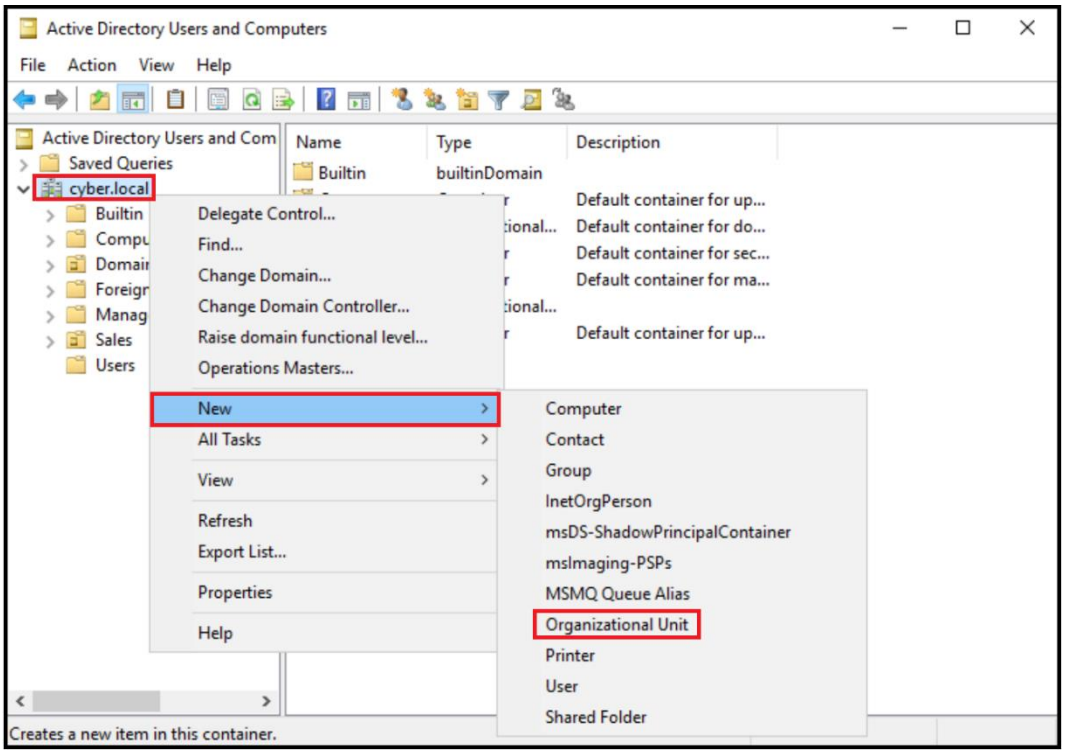




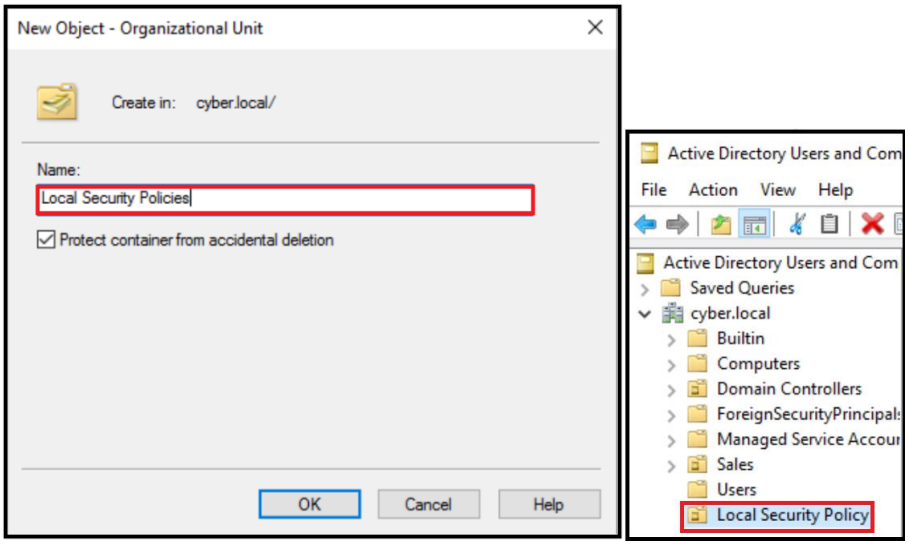




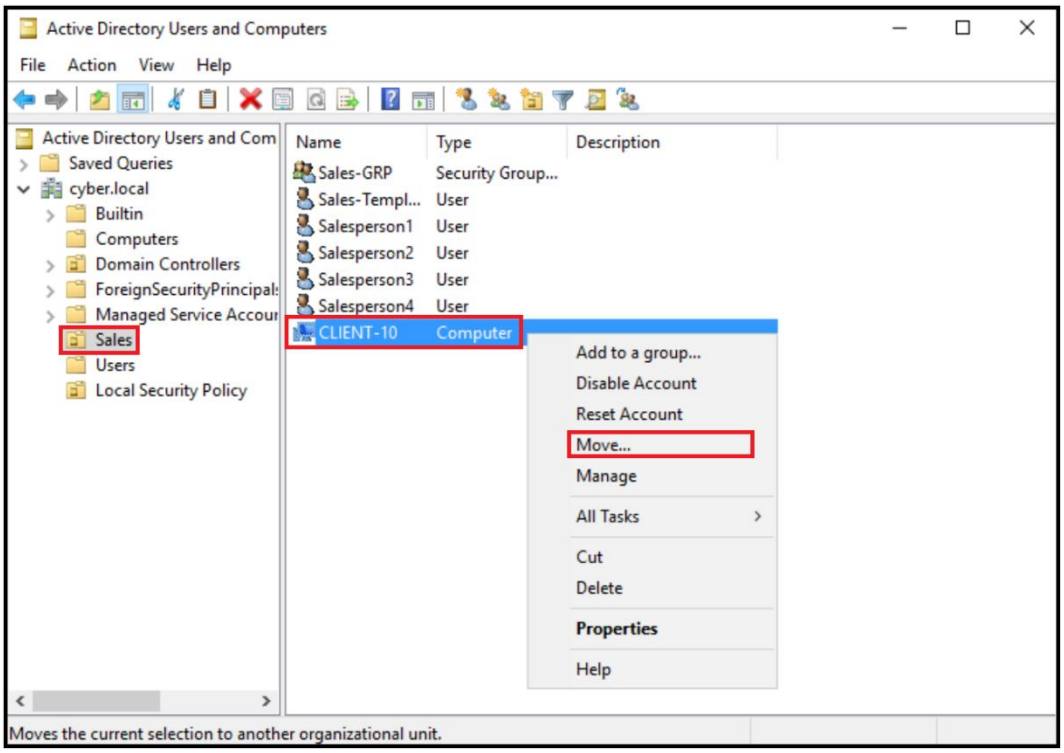
2 On Server1, create a new OU named **Local Security Policies**. Go to **Active Directory Users and Computers** and right-click the ***cyber.local*** domain to create a new OU.



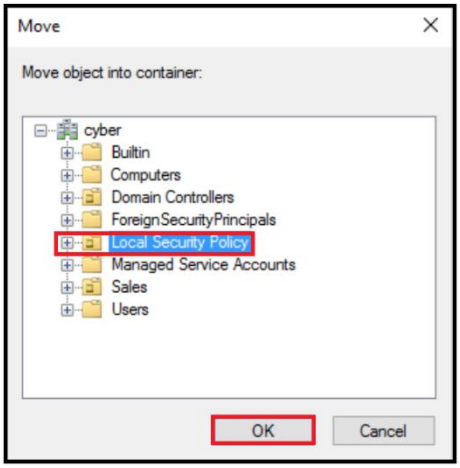
Name the OU **Local Security Policies** and click **OK**. Verify the OU was created.



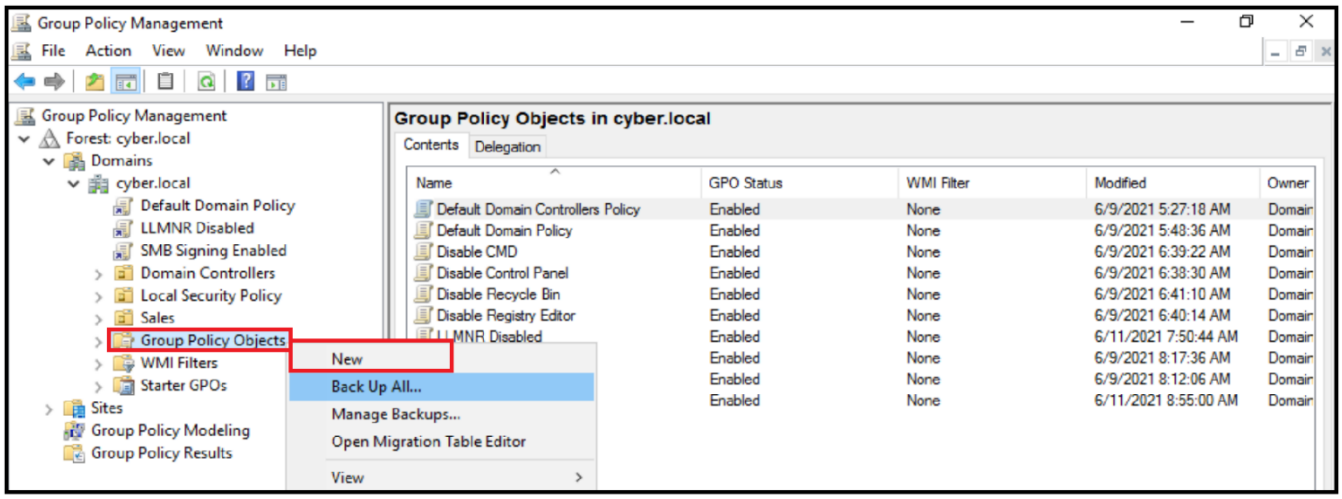
3 Locate and move Client 10 to the **Local Security Policies** OU by right-clicking it and clicking ***Move…***



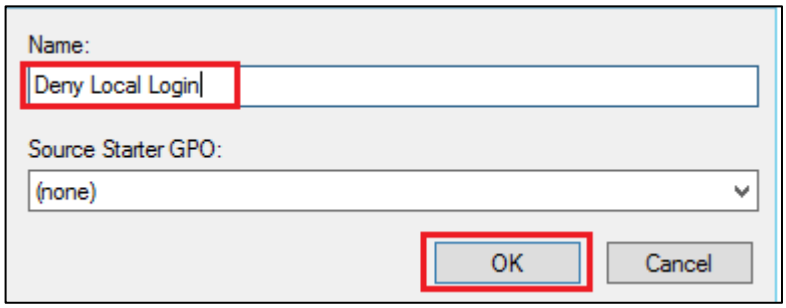
4 Select ***Local Security Policies*** and click **OK**.

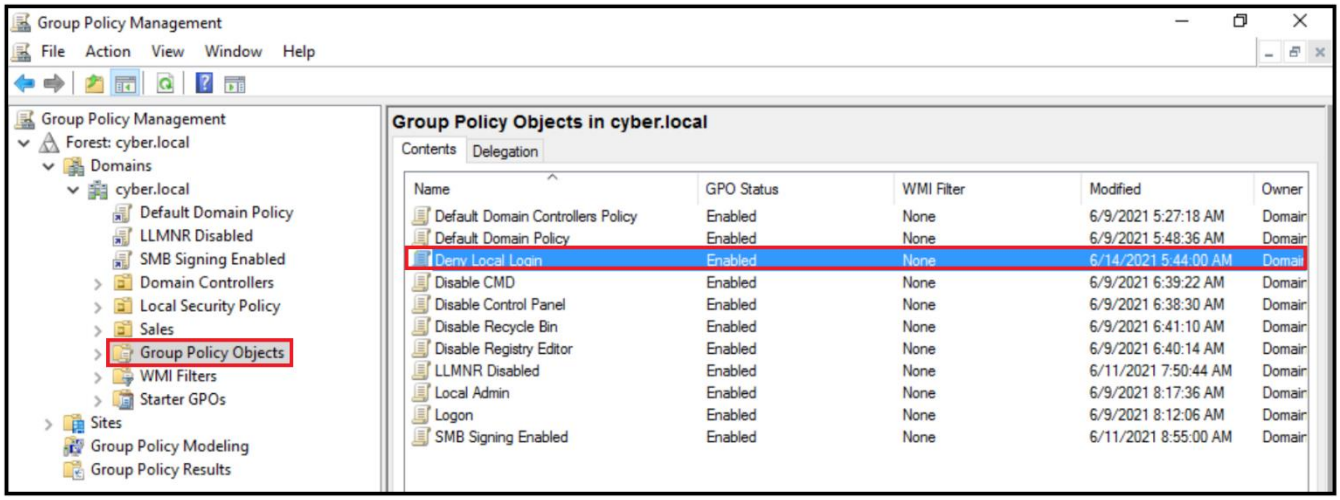


5 Create a new Group Policy Object (GPO) named **Deny Local Login** in the ***Group Policy Objects*** folder. To do so, open ***Group Policy Management*** and navigate to ***Forest: cyber.local*** > ***Domains*** > ***cyber.local***. Then, right-click ***Group Policy Objects*** and click ***New***.

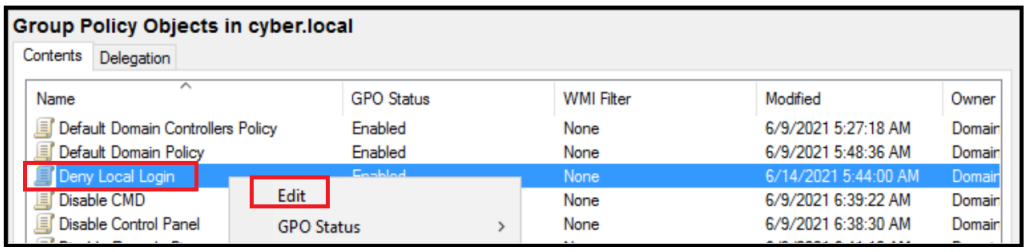


6 Name the GPO **Deny Local Login** and click **OK**. Verify the GPO was created.

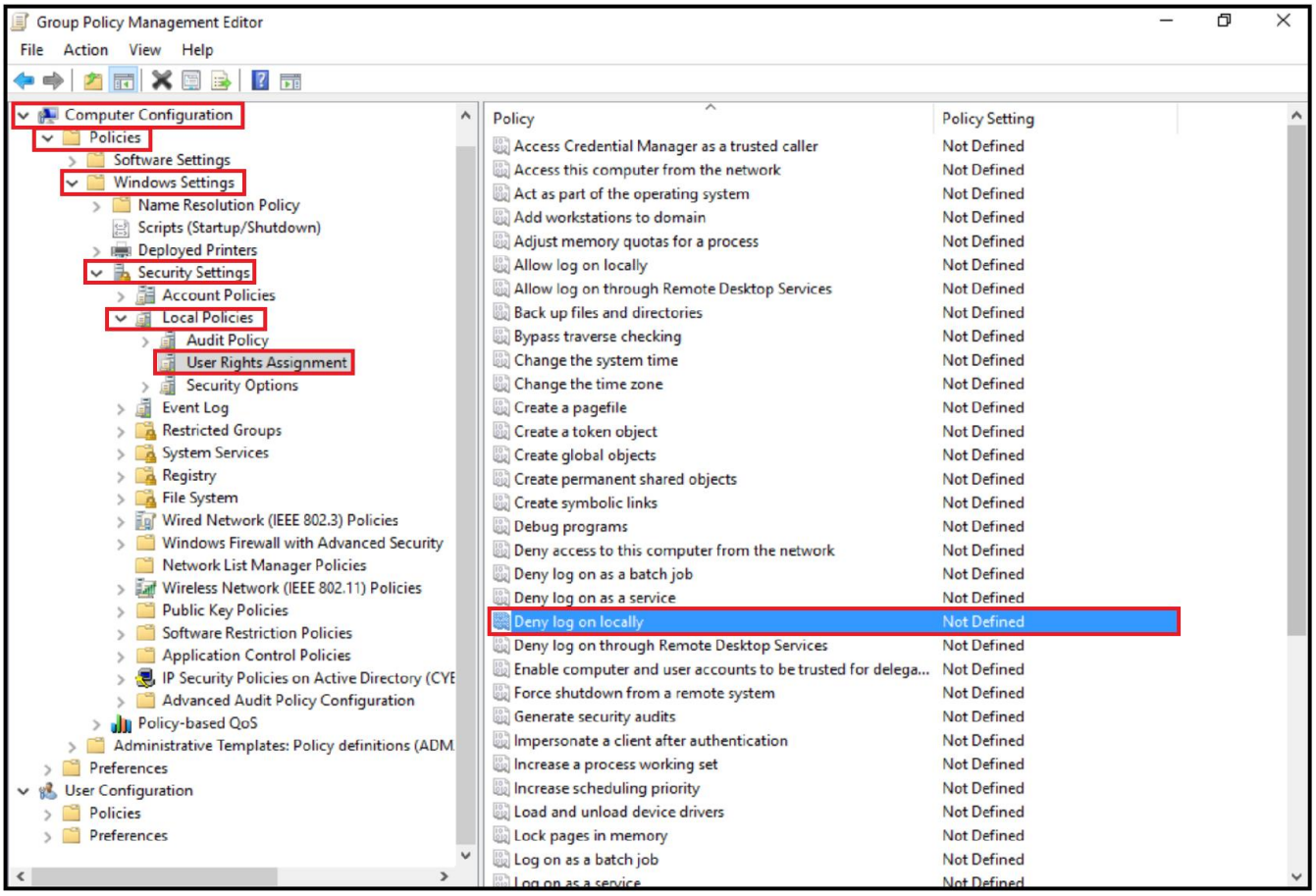




Right-click the ***Deny Local Login*** GPO and click ***Edit***.

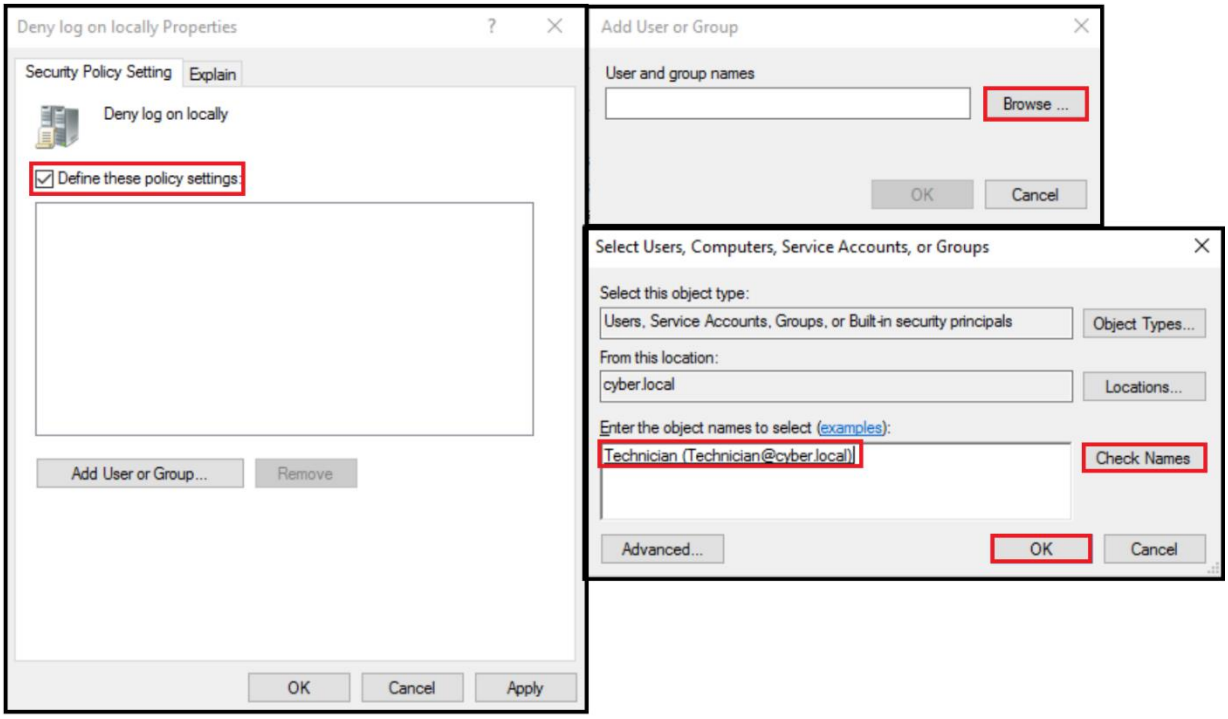


7 Navigate to ***Computer Configuration*** > ***Policies*** > ***Windows Settings*** > ***Security Settings*** > ***Local Policies*** > ***User Rights Assignment*** > ***Deny log on locally***

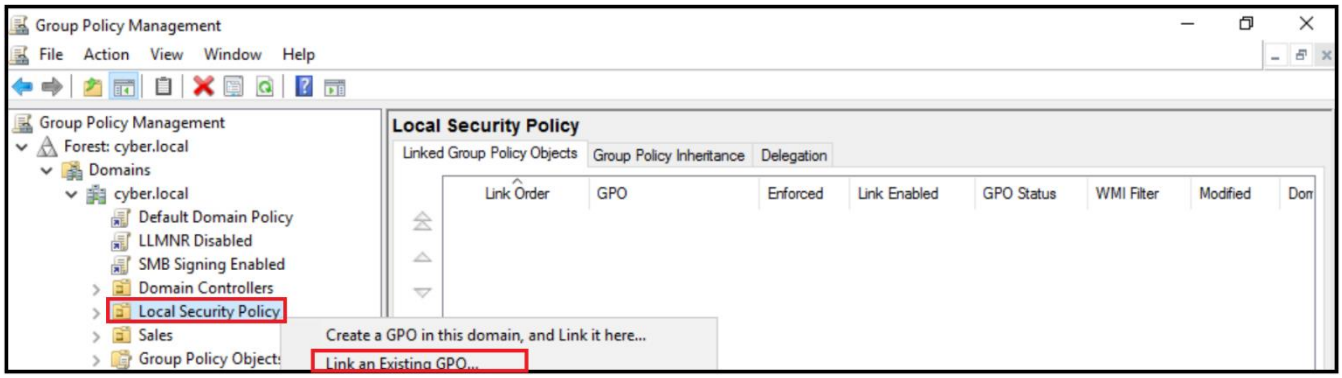


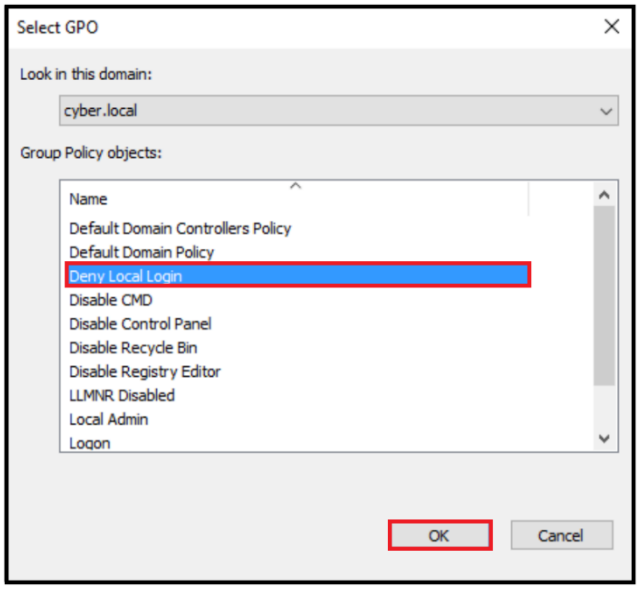
8 Double-click the policy ***Deny log on locally***, enable it, and add user **Technician**.

Note: This policy can be configured with any domain user. In this example, you are using the user account named **Technician**.

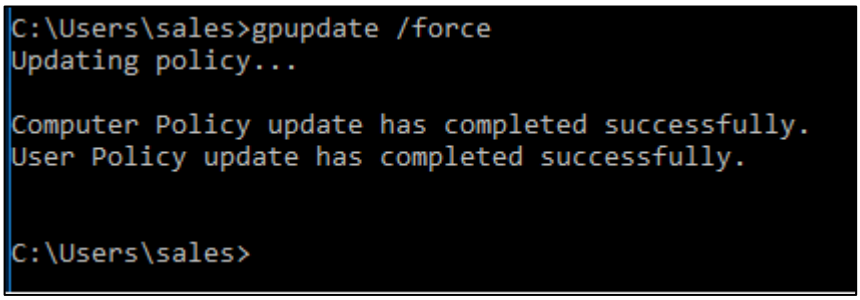


9 Right-click ***Local Security Policies***, click ***Link an Existing GPO…***, select the ***Deny Local Login GPO***, and click **OK**.





10 Update the policy in the Windows 10 VM. Log in as the Administrator user on the Windows 10 VM, open the Command Prompt, and run the ***gpupdate /force*** command.

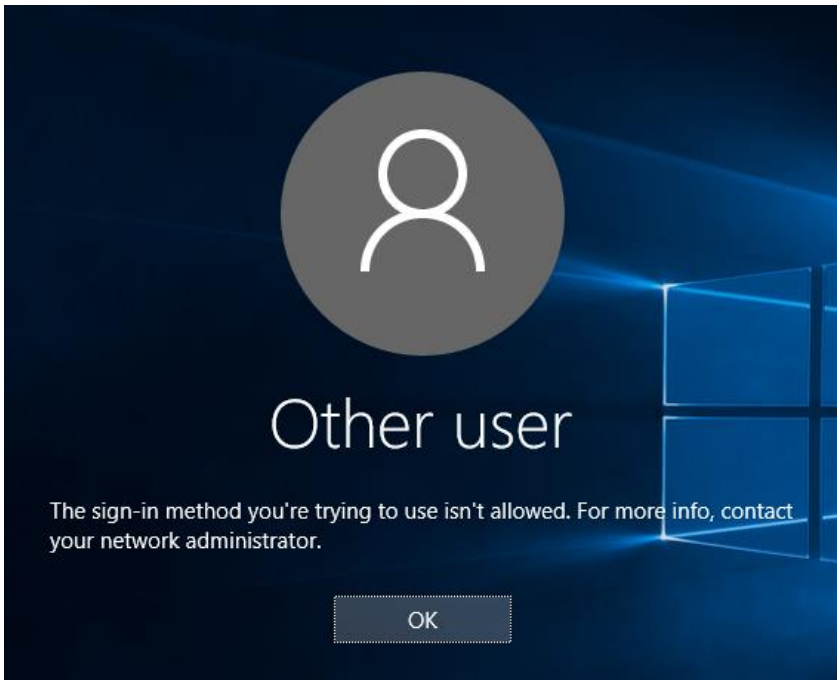


```
C:\Users\sales>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\sales>
```

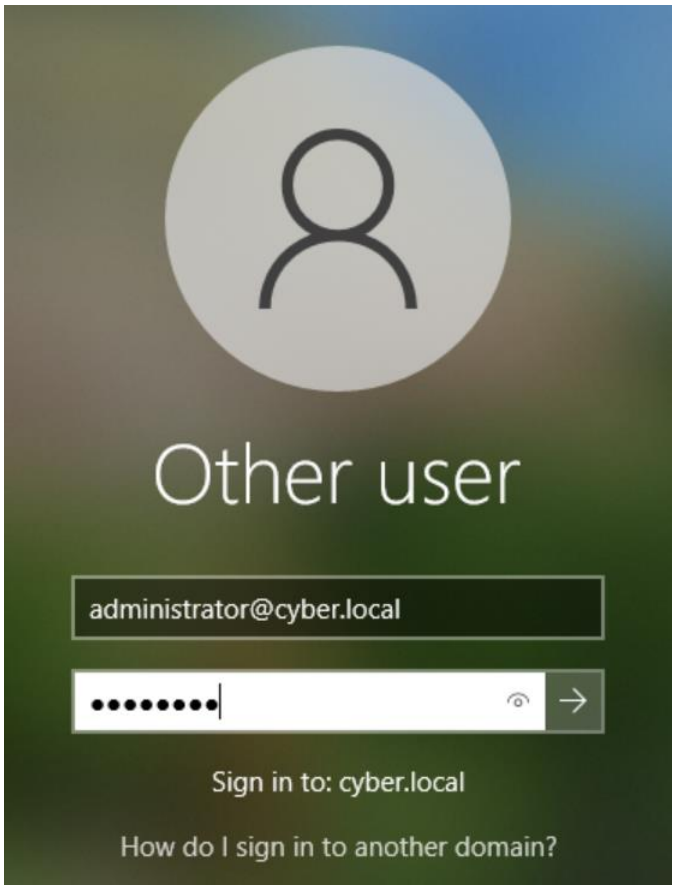
11 Log out, try to log in as the user Technician, and note that the login fails.



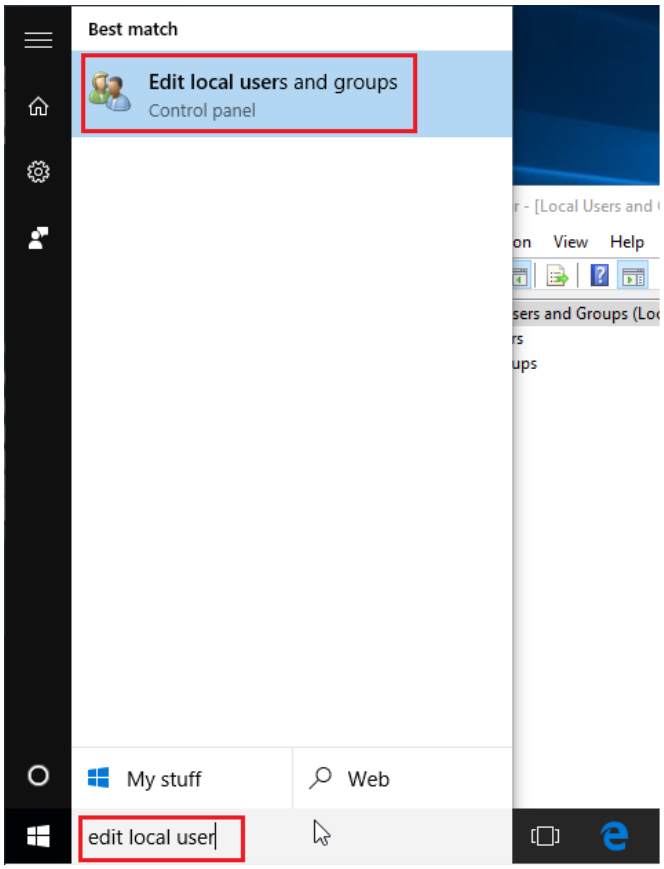
Lab Task 2: Rename the Administrator

In this task, you will implement a policy to rename an administrator's account.

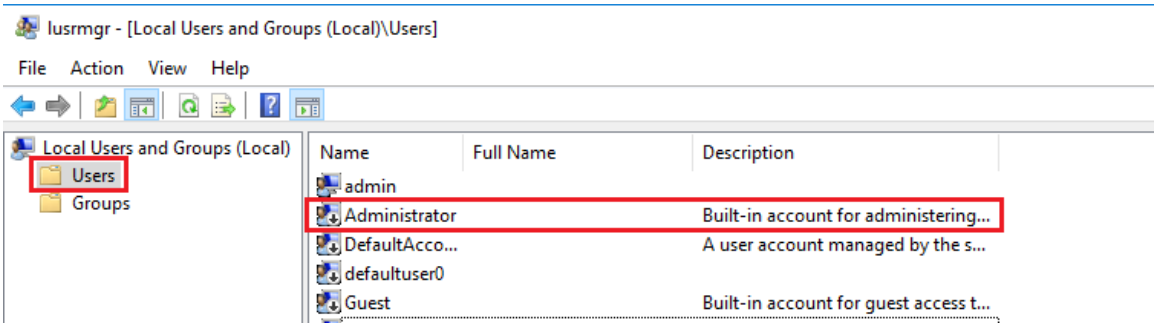
1 Log in to the Windows 10 VM with account **administrator@cyber.local**.



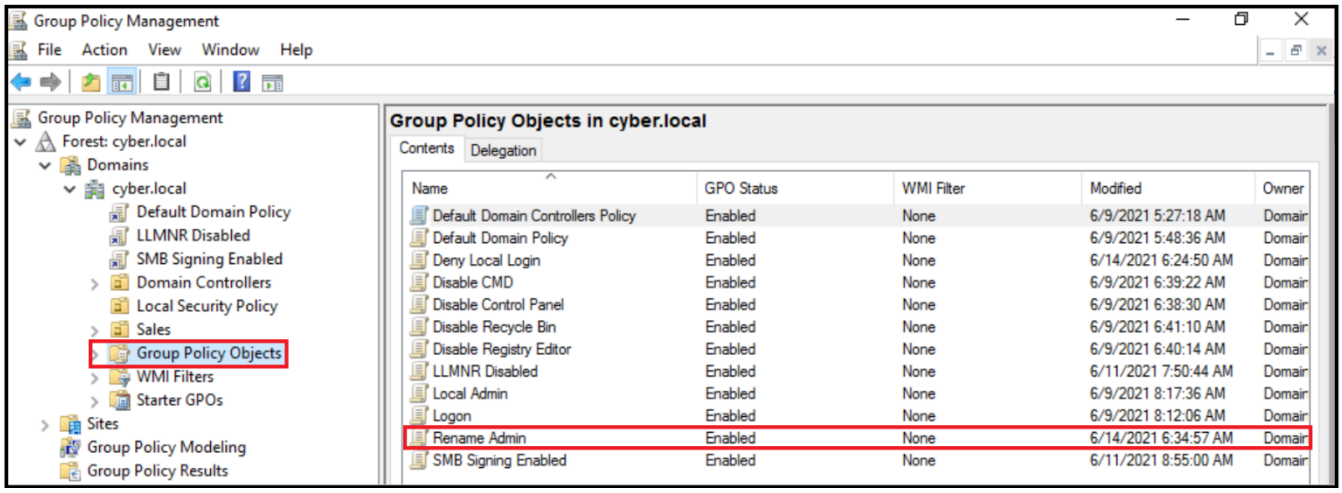
2 Search for the **Edit local users and groups** tool and open it.



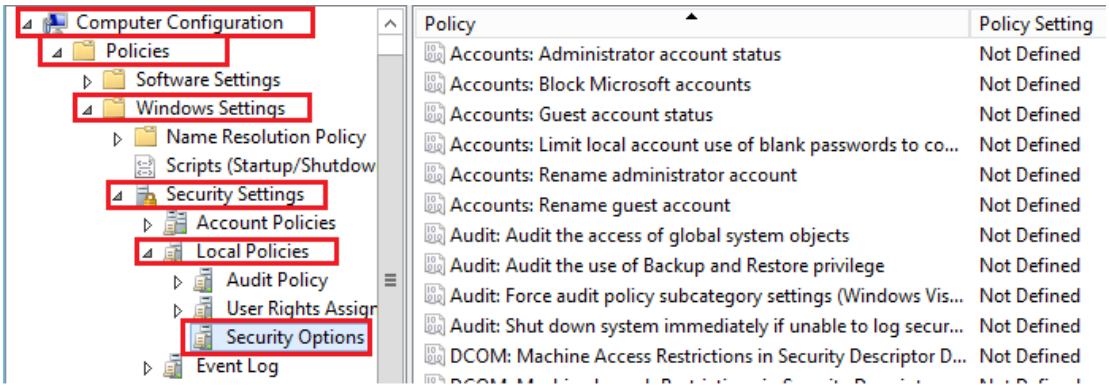
3 Open the ***Users*** folder and view the account named **Administrator**.



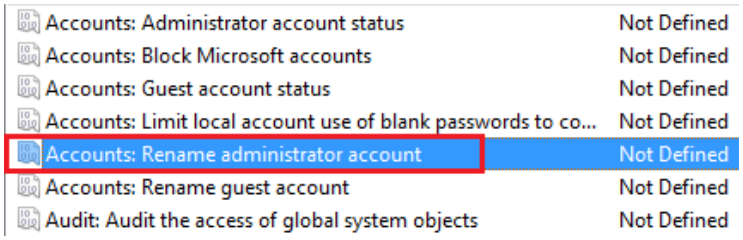
4 On Server1, create a new GPO named **Rename Admin** in the ***Group Policy Objects*** folder.



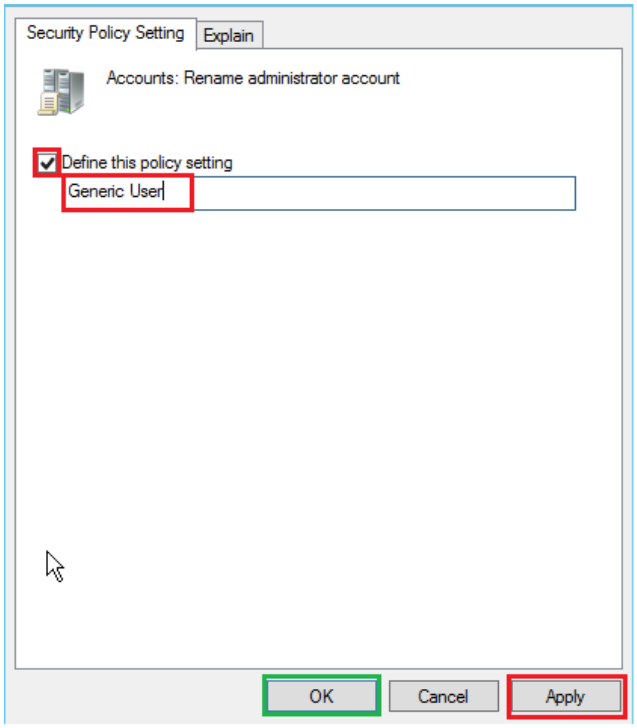
5 Edit the GPO and navigate to ***Computer Configuration*** > ***Policies*** > ***Windows Settings*** > ***Security Settings*** > ***Local Policies*** > ***Security Options***

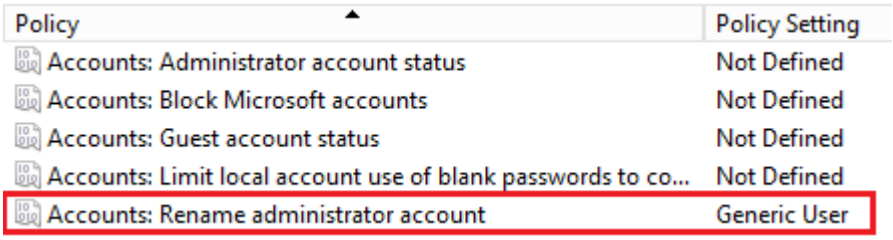


6 Open the configuration of the policy ***Accounts: Rename administrator account*** by double-clicking it.

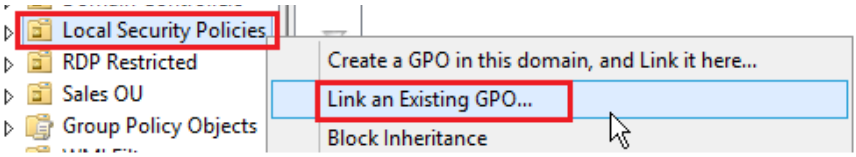


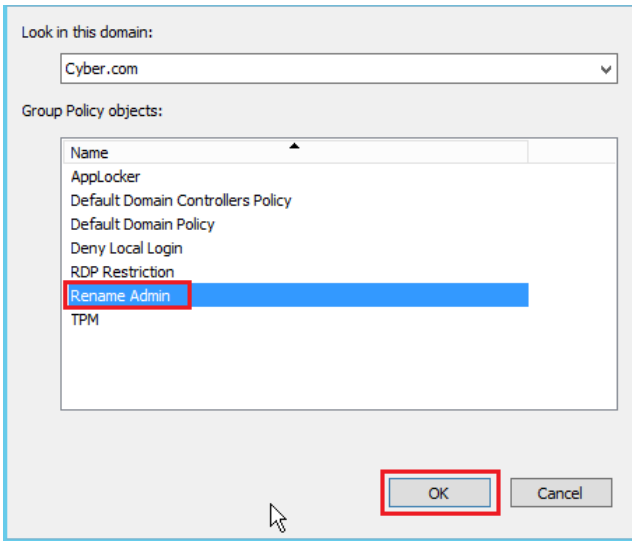
7 Configure the policy to rename administrator accounts to **Generic User**. Verify the policy was changed.





8 Link the GPO **Rename Admin** to the **Local Security Policies** OU. Open ***Group Policy Management***, right-click ***Local Security Policies***, click ***Link an Existing GPO…***, click ***Rename Admin***, and click **OK**.





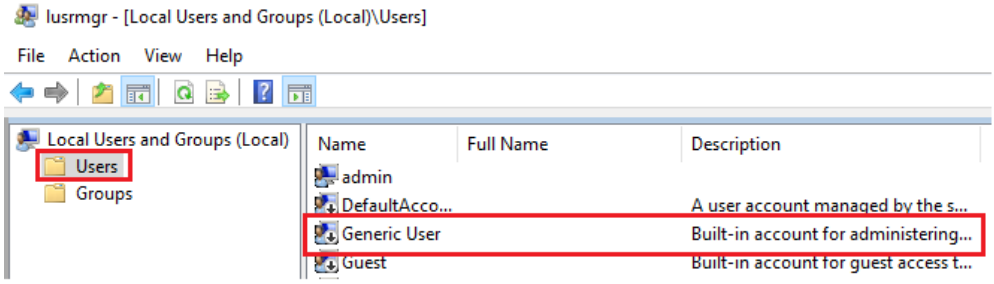
9 Update the policy in the Windows 10 VM. Open the Command Prompt in the Windows 10 VM and run ***gpupdate /force***

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator>_
```

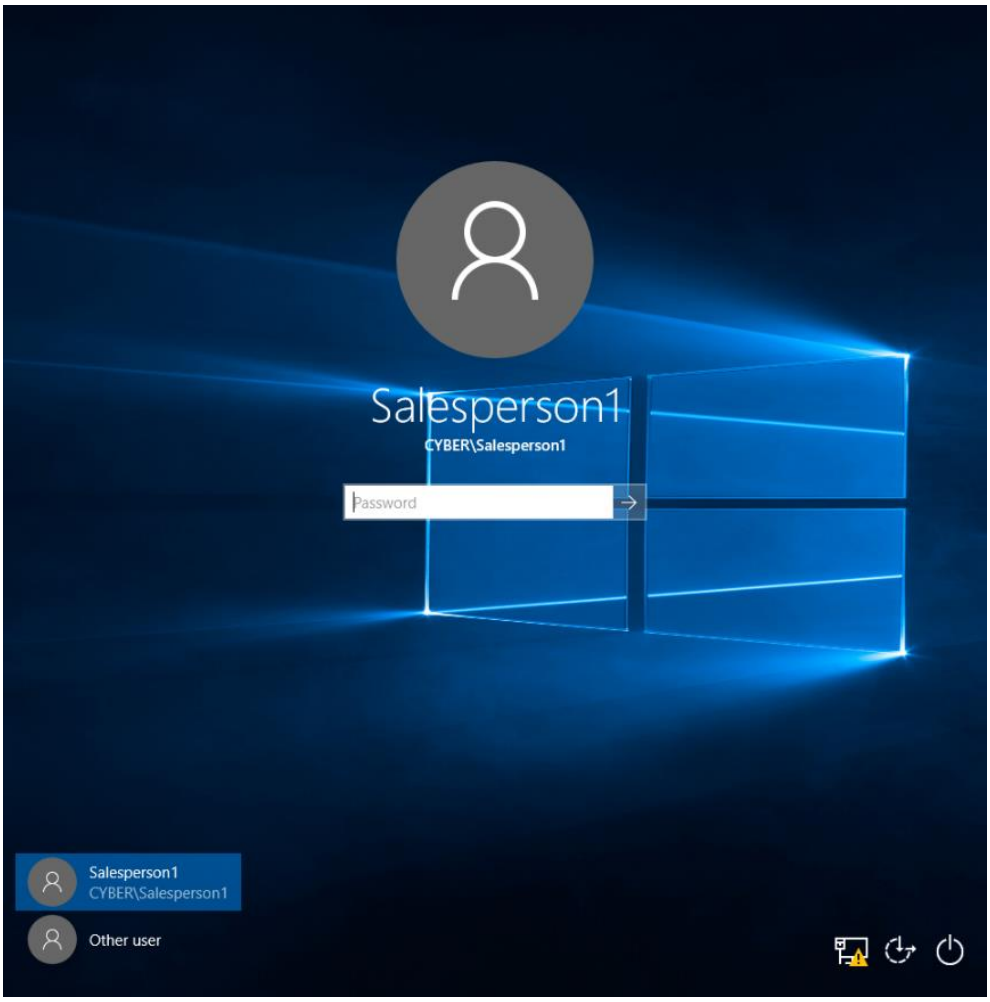
10 Reopen **Edit local users and groups** or refresh it and verify that the policy was applied. Note that the Administrator user was renamed.



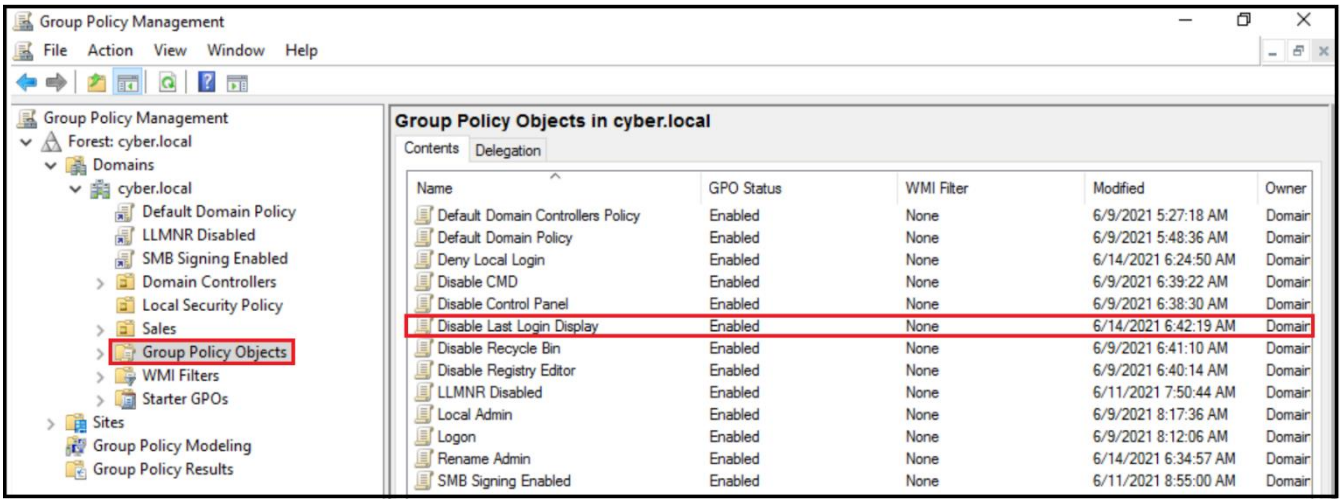
Lab Task 3: Disabling Account Display

In this task, you will implement a policy that prevents a display of the last logged-in account.

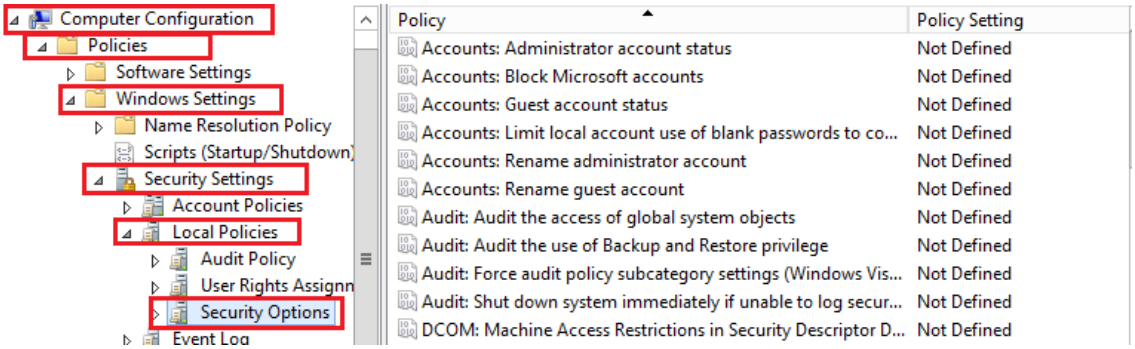
1 Log off the current user in Client10. Click **Start**, click the username at the top, and select ***Sign out***. Note that it displays the last-used account.


Salesperson1
CYBER\Salesperson1
Password
Salesperson1
CYBER\Salesperson1
Other user

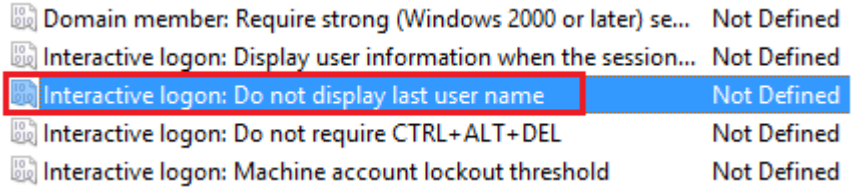
2 On Server1, create a new GPO named **Disable Last Login Display** in the ***Group Policy Objects*** folder.



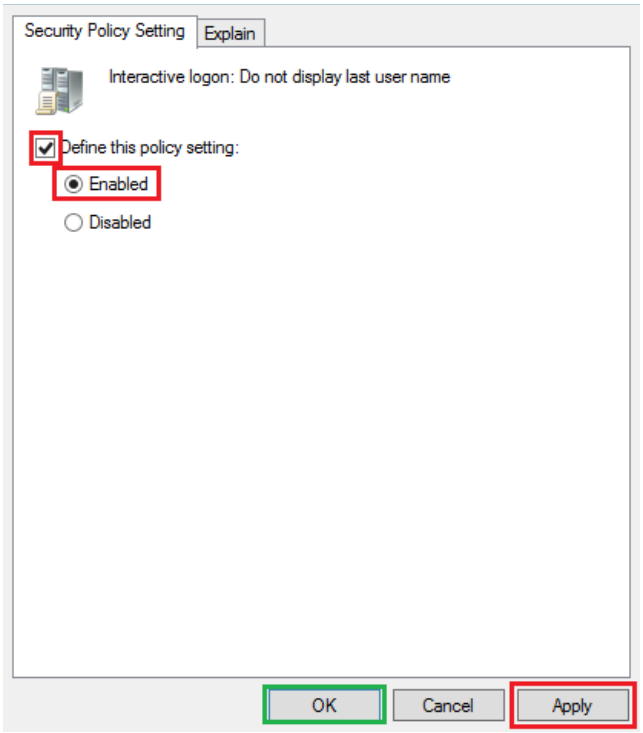
3 Edit the GPO and navigate to ***Computer Configuration*** > ***Policies*** > ***Windows Settings*** > ***Security Settings*** > ***Local Policies*** > ***Security Options***



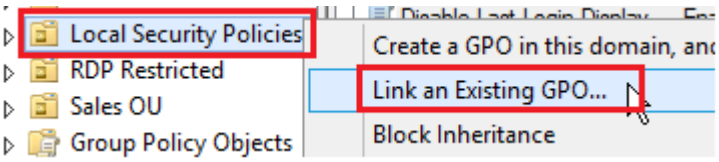
4 Open the configuration of the policy ***Interactive logon: Do not display last user name*** by double-clicking it.

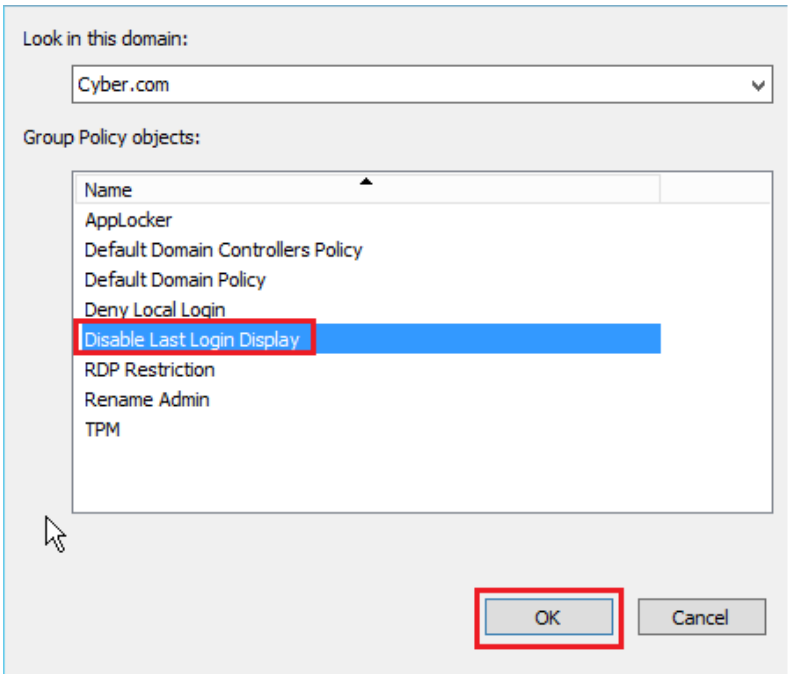


5 Enable it by selecting ***Enabled*** to activate the policy—Click **Apply** and **OK**.



6 Link the GPO to the **Local Security Policy** OU. Right-click ***Local Security Policies***, click ***Link an Existing GPO…***, select the ***Disable Last Login Display*** GPO, and click **OK**.





7 Log on to the Windows 10 VM, open the Command Prompt, and run ***gpupdate /force*** to update the policy.

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

8 Log out and check if the policy was applied. Note that the last logged-in account is not displayed.