

AD Administration: Guided Lab

We Could Use A Bit Of Help..

Bucky Barnes
Thu 1/6/2022 9:25 AM
To: Helpdesk

So, our normal admin staff is swamped right now after our last audit of the enterprise, can you help us out by tackling some of the tickets we have in queue and taking care of a few tasks for us? We need someone to help with the following:

- Add a few new hires into AD, They start on Monday, and we need to have their accounts ready by then.
- Remove a few old inactive user and computer objects we found during the audit.
- Unlock Adam Masters' account since he locked himself out again... (see trouble-ticket)
- Create a new Security Group for the New-hire analysts, and a new OU for the group and their corresponding PCs
- Our team has provisioned the New-hires computers, they just need to be added to the domain. Once added, validate that their objects are in the correct OU.
- Create and apply a new Group Policy duplicated from another already in GPMC and modify it for the Analyst users.
- Validate the DNS records for the Host (Sharepoint02.inlanefreight.local)

If you could tackle those tasks for us, it would take a lot of weight off our backs while we finish cleaning up the environment. Let us know if you can help.

R/S
B. Barnes CISSP.
I.T Teamlead
Inlanefreight LLC.
" Zhelaniye. Rzhavyi. Semnadsat'. Rassvet. Pech'. Devyat'. Dobroserechnyy. Vozvrashcheniye na rodinu. Odin. Gruzovoy vagon....Soldat?"
"Ya gotov otvechat."

[Reply](#) | [Forward](#)

Today we will serve as domain administrators to InlaneFreight. We have been tasked to help IT department with managing Active Directory environment.

Preparation:

For this lab HackTheBox gave us access to a domain-joined Windows server from which we will perform any actions on AD.

First we must connect to Windows server via RDP from our machine (Pwnbox provided by website or our own VM).

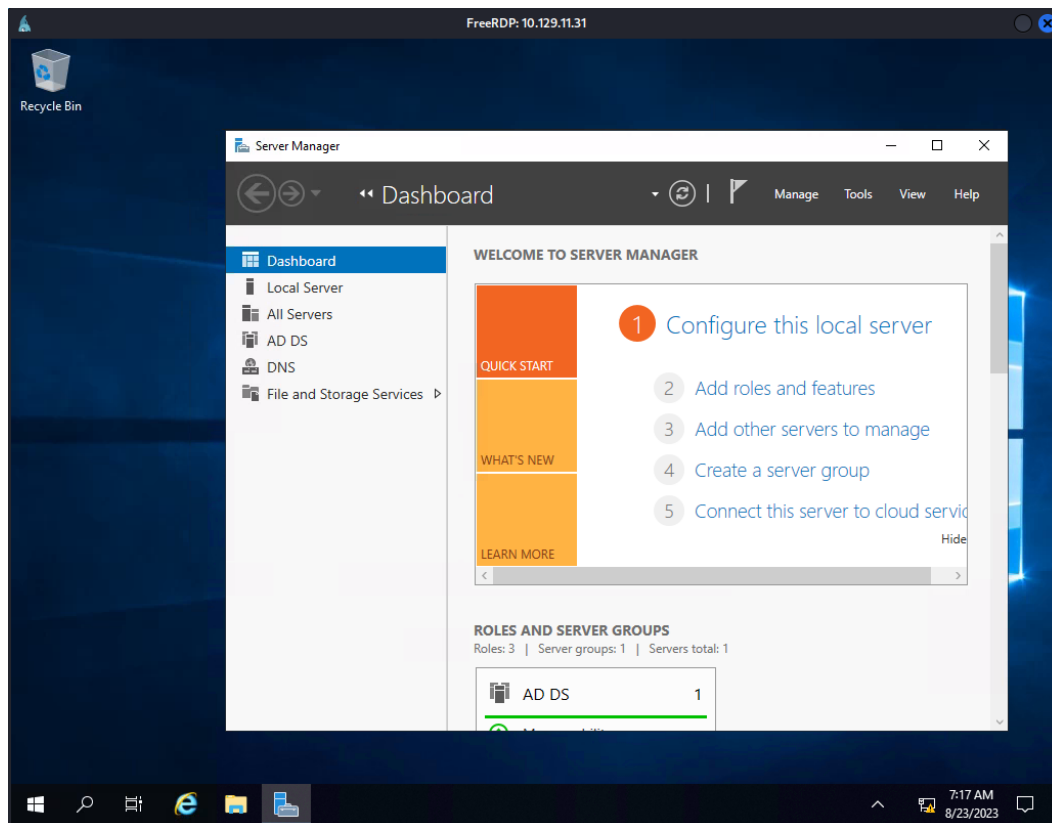
- **IP** == 10.129.11.31
- **Username** == http-student_adm
- **Password** == Academy_student_DA!

We will use **xfreerdp** to connect

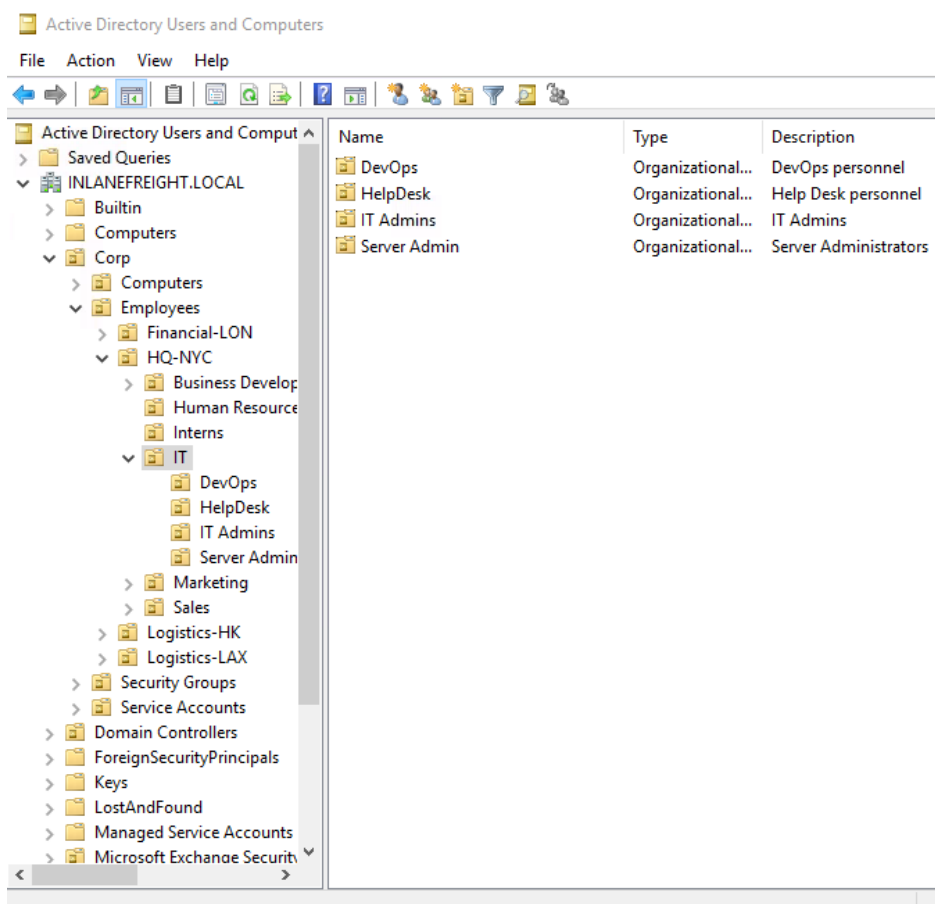
```
(kali@kali)-[~]  
$ xfreerdp /v:10.129.11.31 /u:htb-student_adm /p:Academy_student_DA!
```

```
The above X.509 certificate could not be verified, possibly because you do not have  
the CA certificate in your certificate store, or the certificate has expired.  
Please look at the OpenSSL documentation on how to add a private CA to the store.  
Do you trust the above certificate? (Y/T/N) Y
```

After successful connection we are greeted by this view



Now we will access Active Directory via Active Directory Users and Computers (ADUC) MMC tool.

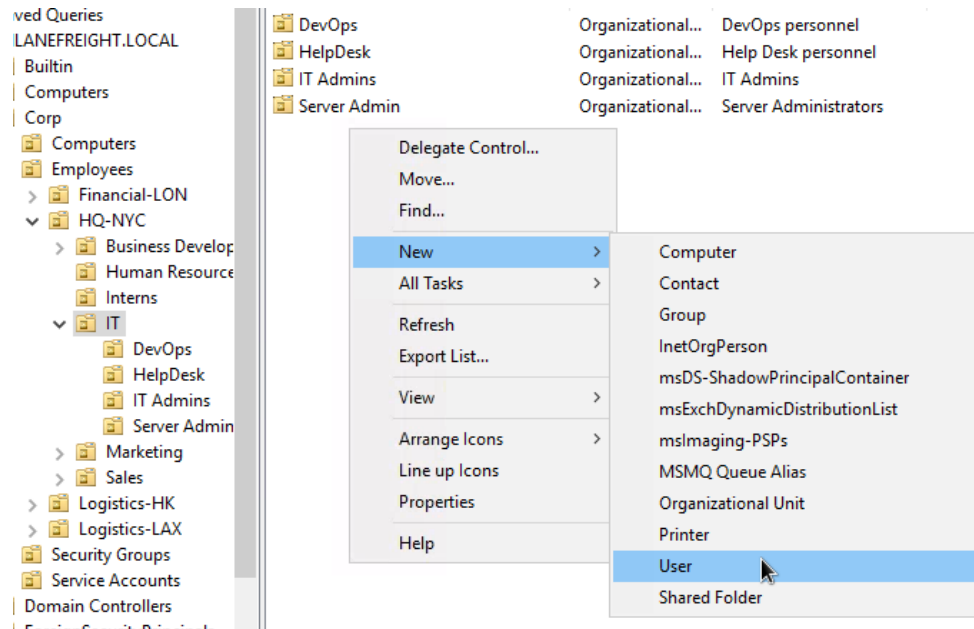


Task 1: Manage Users

Our first job is to add new hires into AD. They are called: “Andromeda Cepheus”, “Orion Starchaser”, “Artemis Callisto”. Each user should have following attributes set:

- Full name
- Email (first-initial.lastname@inlanefreight.local)
- Display name
- User must change password at next login

We navigate to **Corp > Employees > HQ-NYC > IT** and create new users there

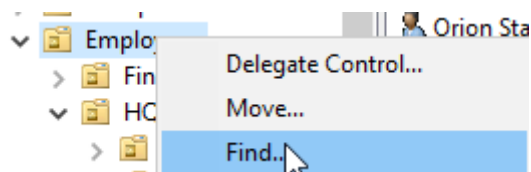


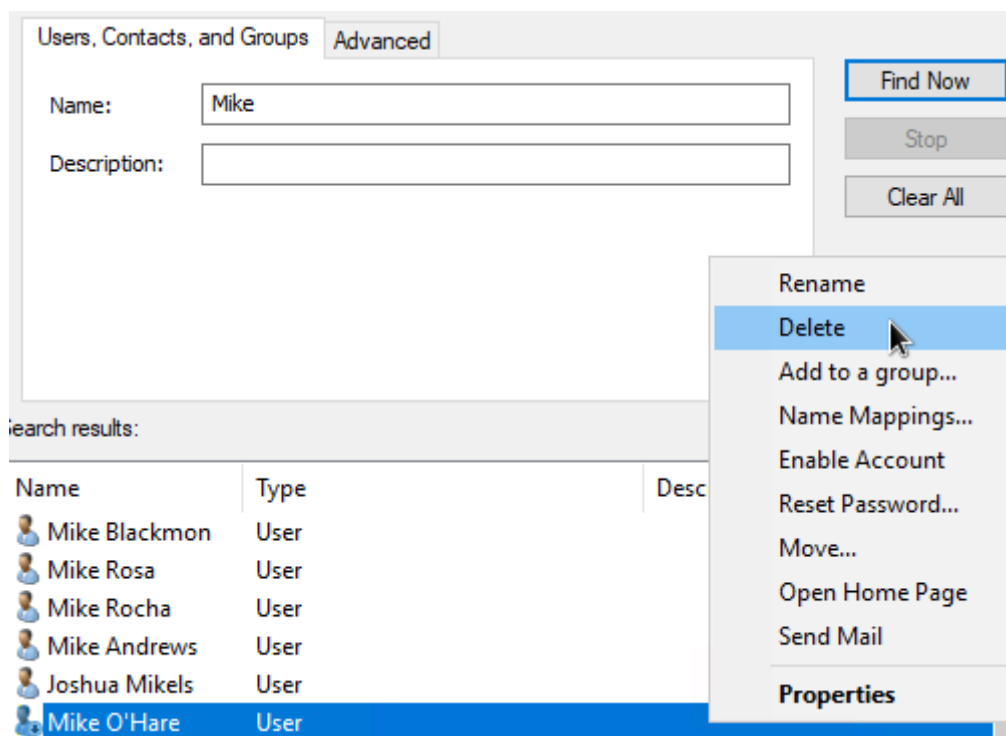
We end up with something like this. It is worth noting that our task for now was not to assign them to individual OUs

Name	Type	Description
DevOps	Organizational...	DevOps personnel
HelpDesk	Organizational...	Help Desk personnel
IT Admins	Organizational...	IT Admins
Server Admin	Organizational...	Server Administrators
Andromeda Cepheus	User	
Orion Starchaser	User	
Artemis Callisto	User	

Next we must remove unactive users: “Mike O’Hare”, “Paul Valencia”. Which is quite easy.

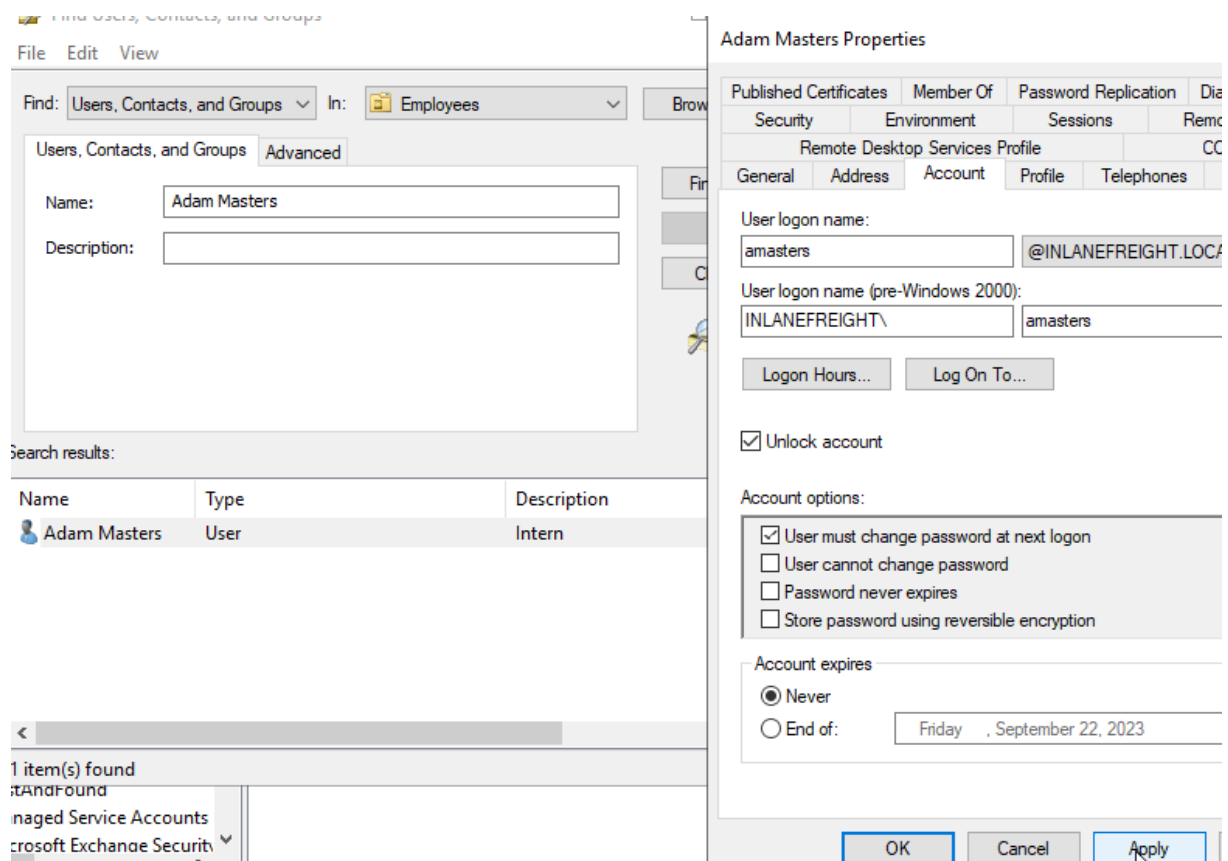
But how will we find them? Let’s use find functionality on “Employee”





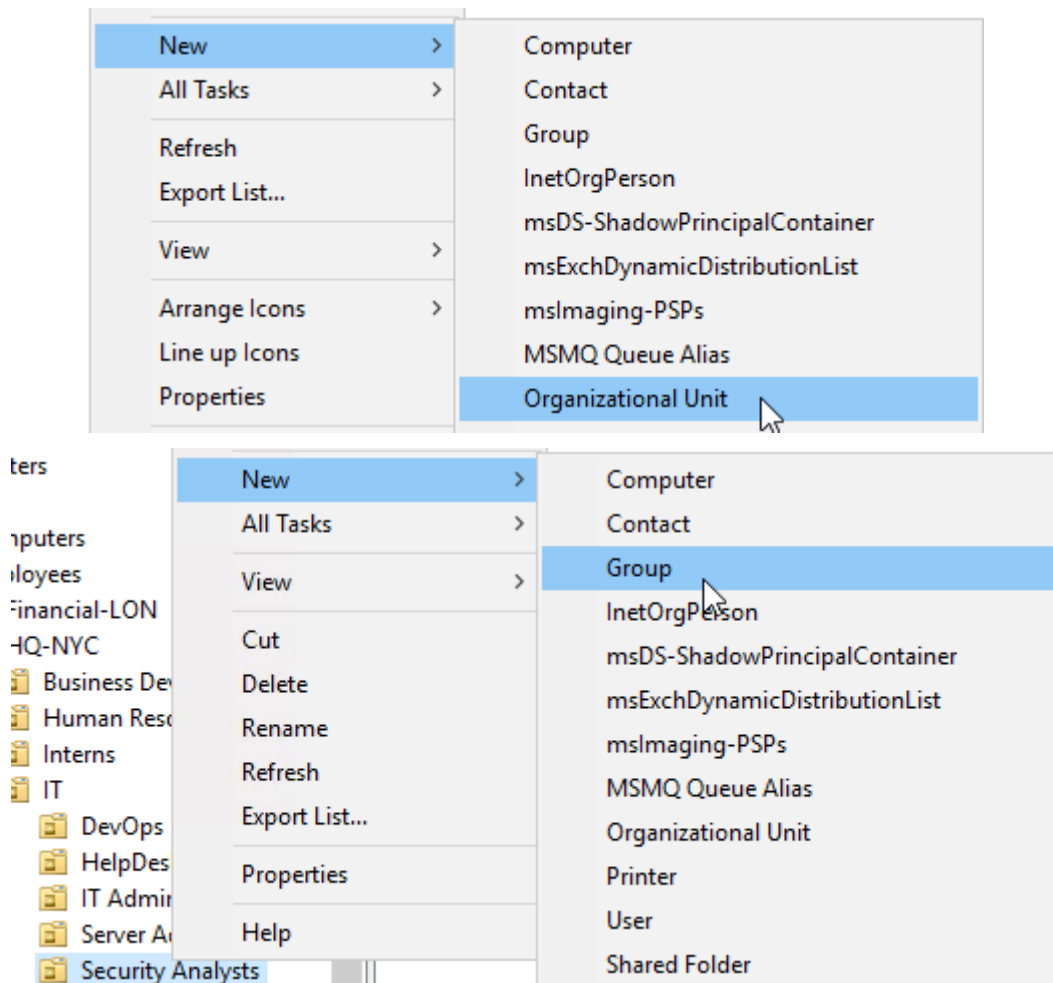
Same procedure with Paul Valencia.

Lastly "Adam Masters" account is locked because he typed his password wrong too many times. Our job is to unlock his user account and force him to change password at the next login.



Task 2: Manage Groups and Other Organizational Units

Time to clean up and assign new employee to the new group called "Security Analysts" nested in OU named the same under IT.

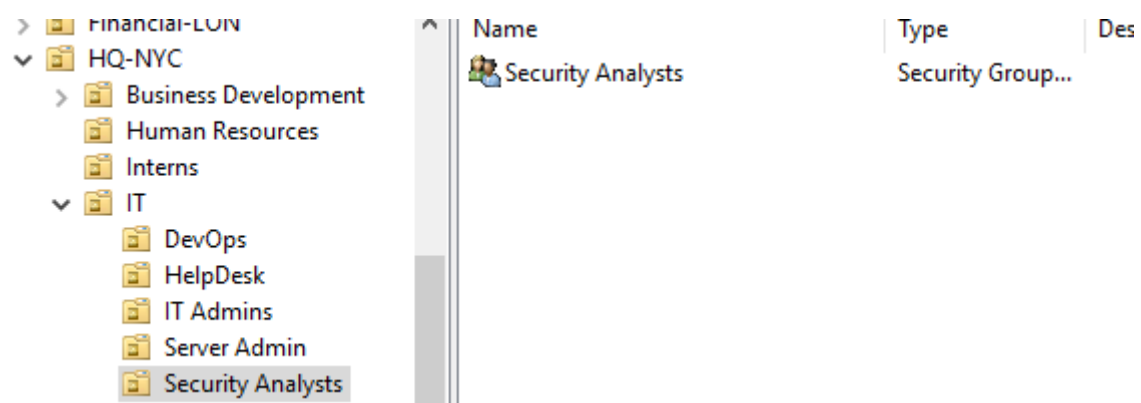


Group name:

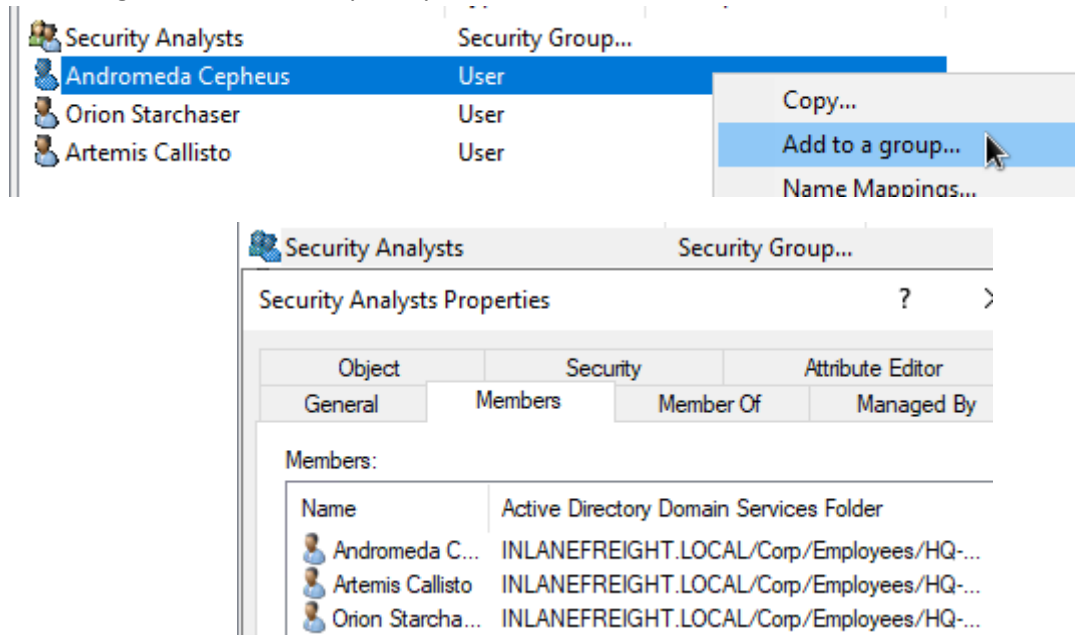
Group name (pre-Windows 2000):

Group scope:
☒ Domain local
☐ Global
☐ Universal

Group type:
☒ Security
☐ Distribution



Now let's add our new users to this group. First we move these users to their appropriate OU and then assign them to "Security Analysts".

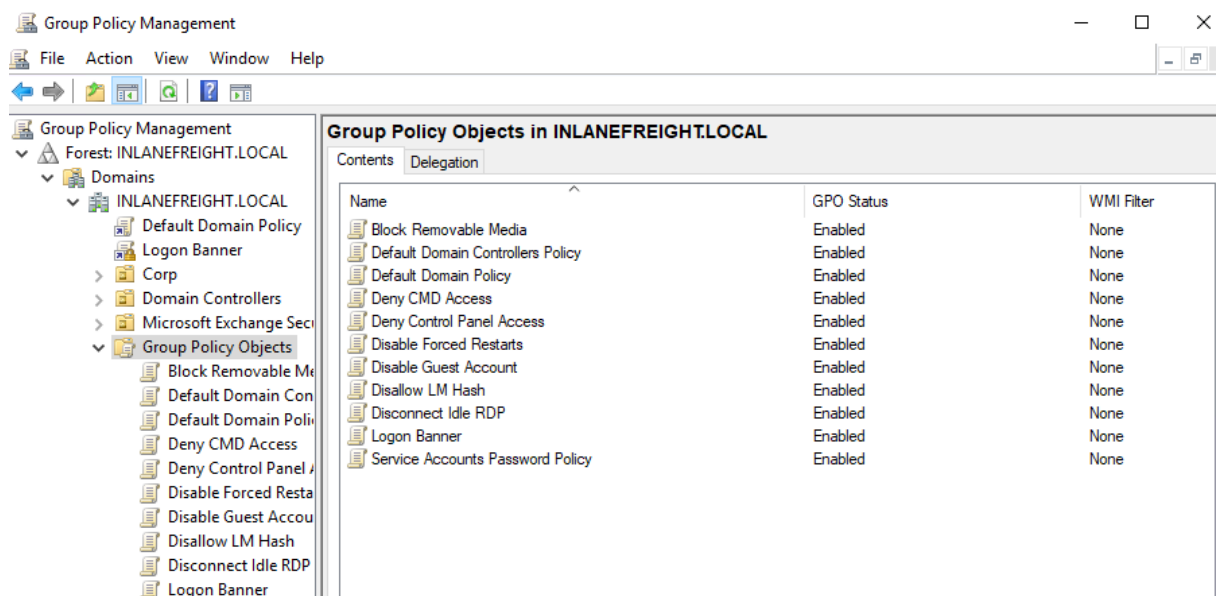


Task 3: Manage Group Policy Objects

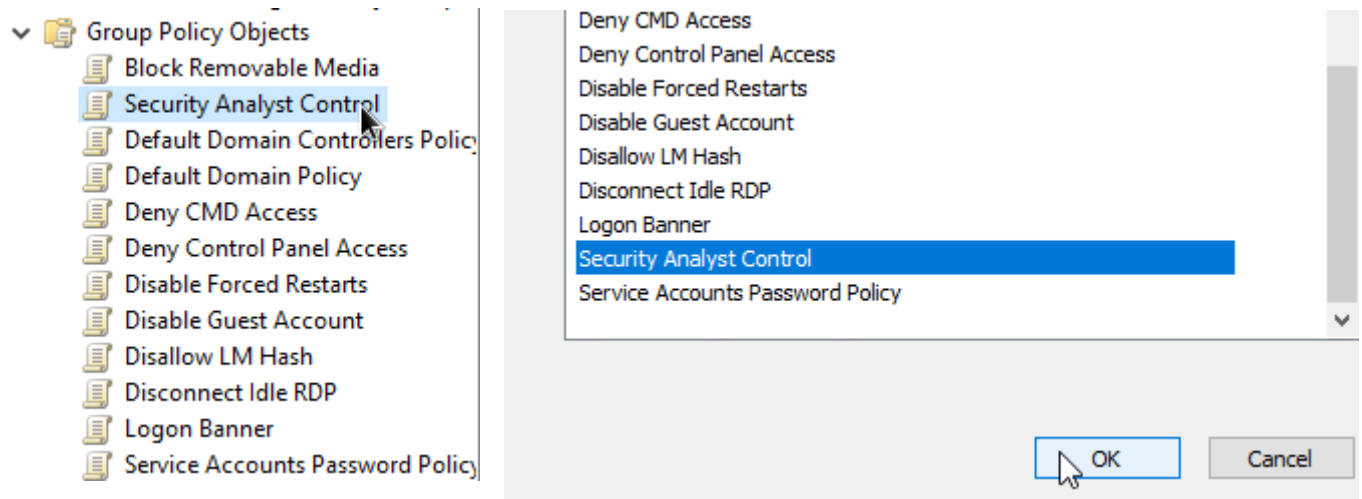
Next we have been tasked to duplicate group policy "Logon Banner", rename it **Security Analysts Control** and modify it to work for the new Analysts OU.

- We will be modifying the Password Policy settings for users and allow them to access PowerShell and CMD since their daily job require it.
- For computer setting we need to ensure that the Logon Banner is applied and that removable media is blocked from access.

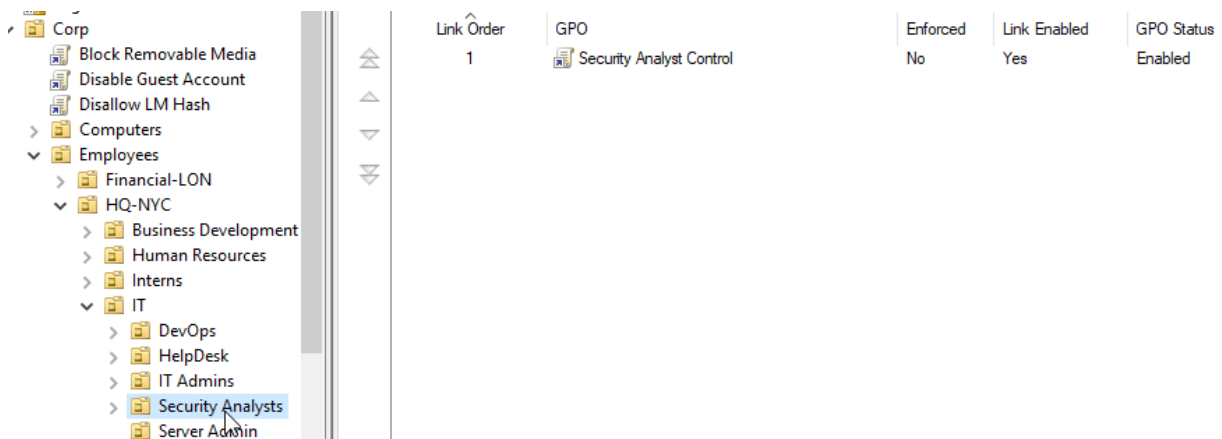
First must access **Group Policy Management** tab



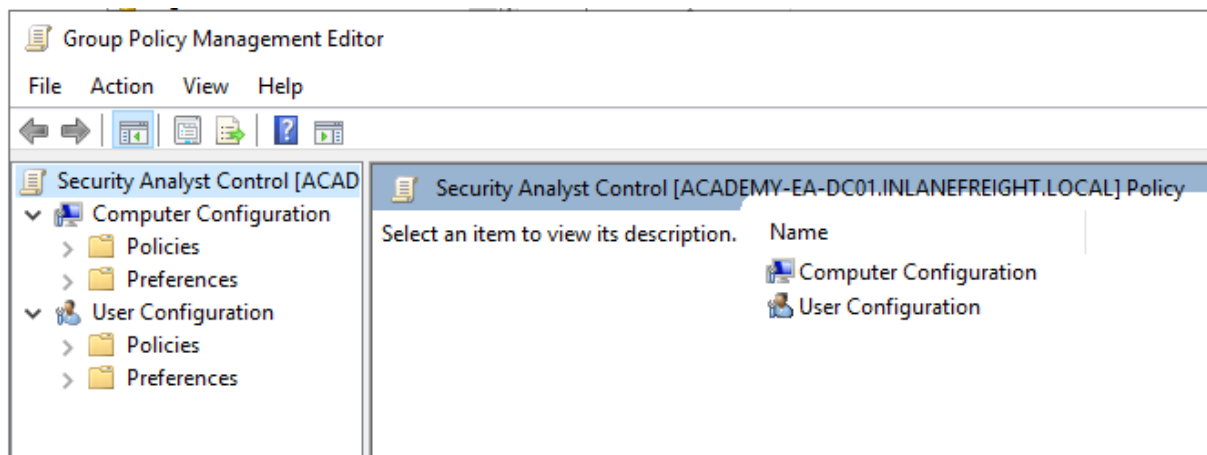
Let's duplicate Logon Banner and rename it. Then will link this GPO with OU "Security Analysts"



And here it is.



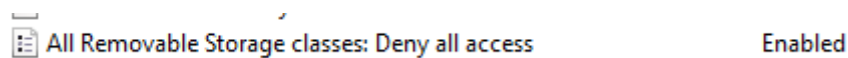
Now by right-click on "Security Analyst Control" and edit we access GPMC



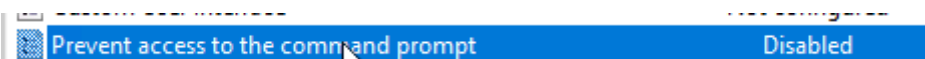
We are tasked to ensure that removable media are blocked from access and to expressly allow security analysts to access PowerShell and CMD.

These options can be found in:

User Configuration > Policies > Administrative Templates > System > Removable Storage Access

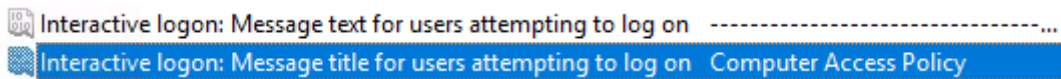


User Configuration > Policies > Windows Settings > Administrative Templates > System.



For Computer Settings we must ensure that Logon Banner is applied and that the password policy settings for this group are strengthened.

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.



Settings should be already enabled since we copied Logon Banner GPO. We are validating the settings and ensuring everything is fine.

Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy

Policy	Policy Setting
Enforce password history	5 passwords remembered
Maximum password age	30 days
Minimum password age	7 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

We set up password policy according to our organization's password policy.

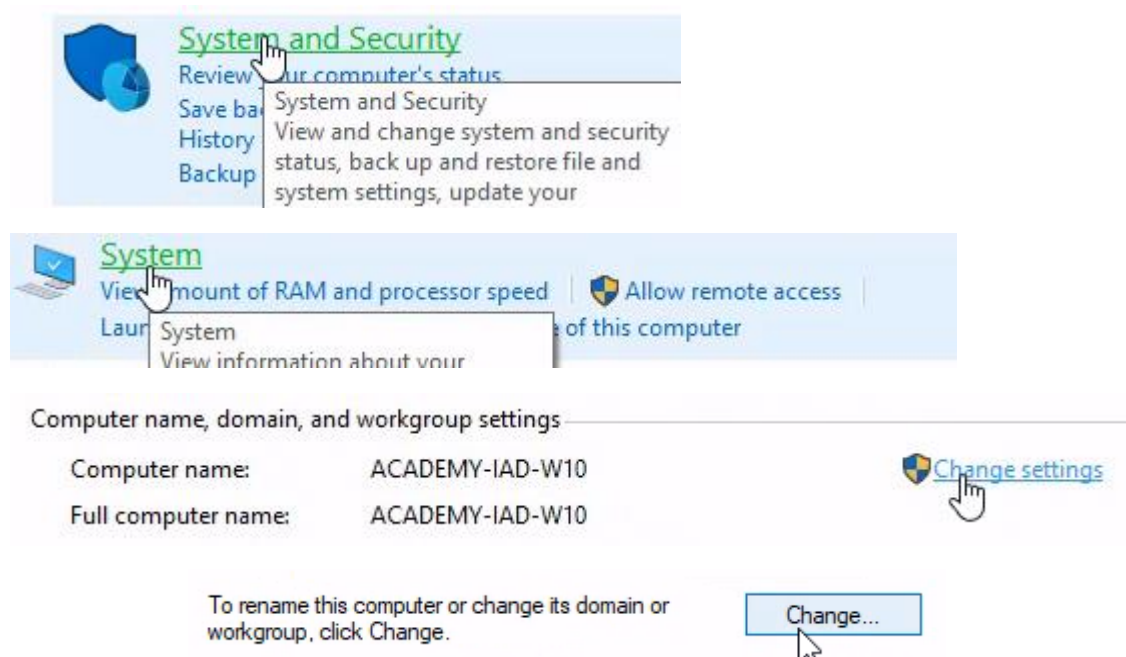
Task 4: Add and Remove Computers To The Domain

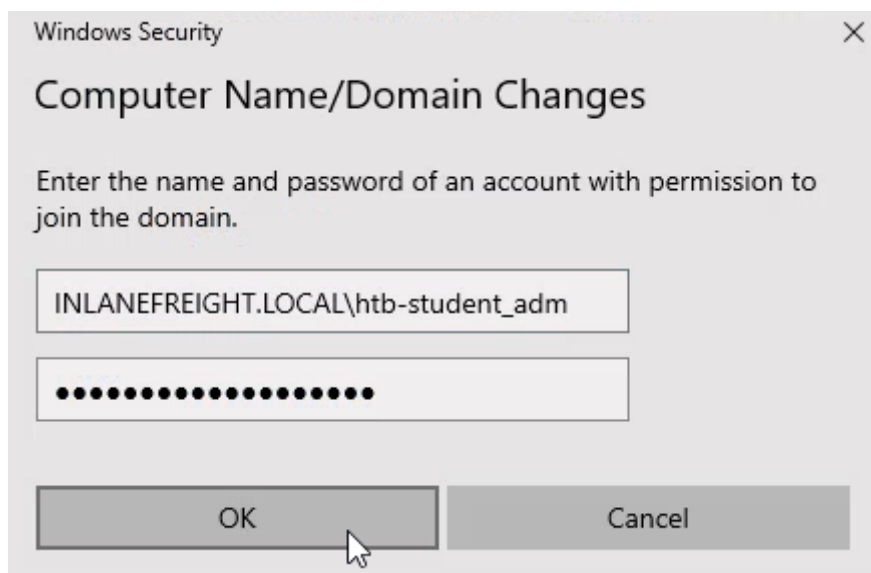
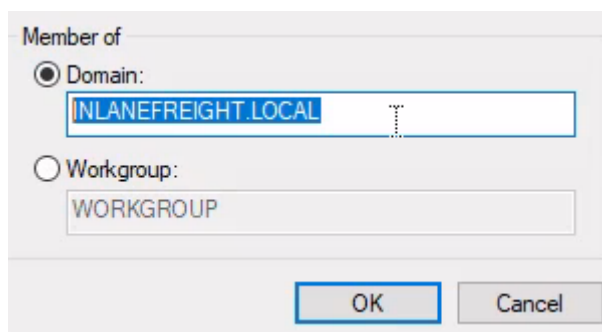
Our new users will need computers to perform their daily routines. The host we need to join to the INLANEFREIGHT domain is called "ACADEMY-IAD-W10" and has following credentials:

- User == Image
- Password == Academy_student_AD!

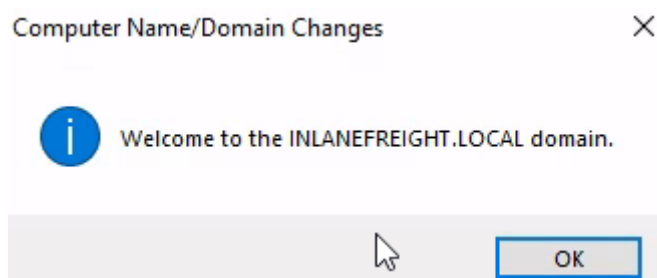
First we log in to the computer via RDP or manually and navigate to control panel.

To add the computer to the domain we are going to use Windows GUI.





To add user to the domain we will utilise our domain administrator account from previous tasks that has all necessary permissions.



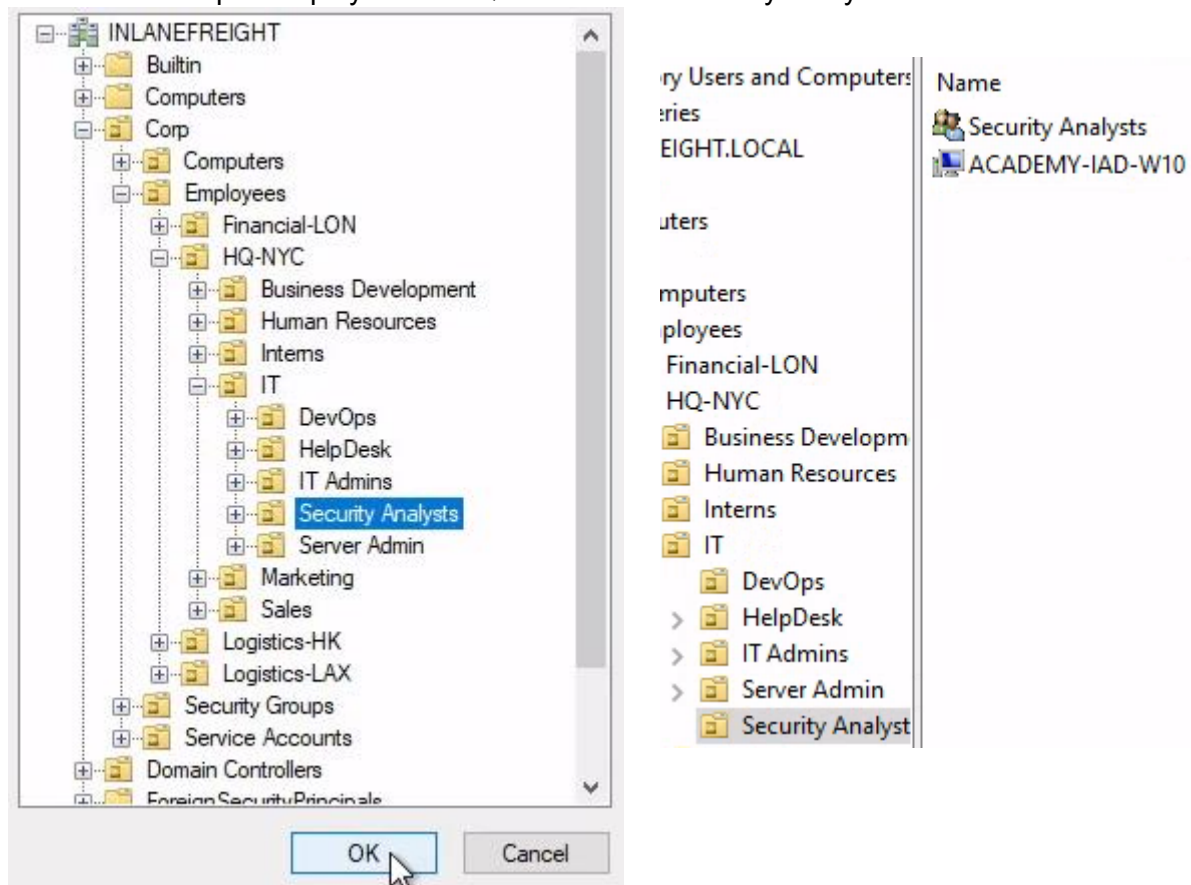
Success! Device is now connected to INLANEFREIGHT.LOCAL domain. Now we need to move this computer to correct OU. Let's return to our domain administrator account and perform this action.



We can see that this device appeared in Computers tab.

Let's right click on it and select **move**.

Then select Corp > Employees > HQ-NYC -> IT ->Security Analysts



As we can see ACADEMY-IAD-W10 computer is now in Security Analysts OU.

This concludes this lab exercises. Thanks for reading and I hope you found the information here useful.

Source: <https://academy.hackthebox.com/module/74/section/708>