

Active Directory Project Report

Introduction

In this project, I walked through a series of essential Active Directory tasks, including:

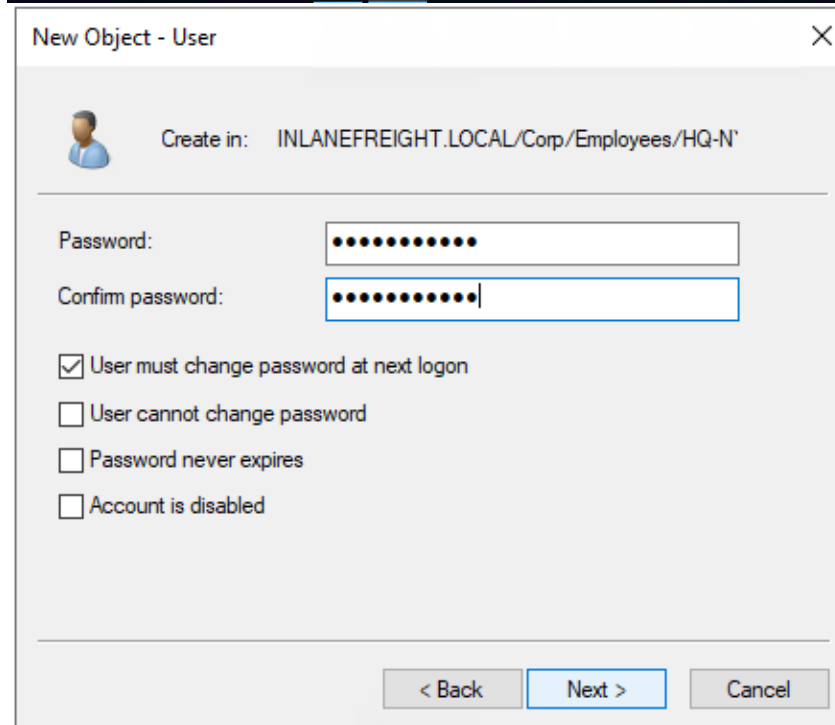
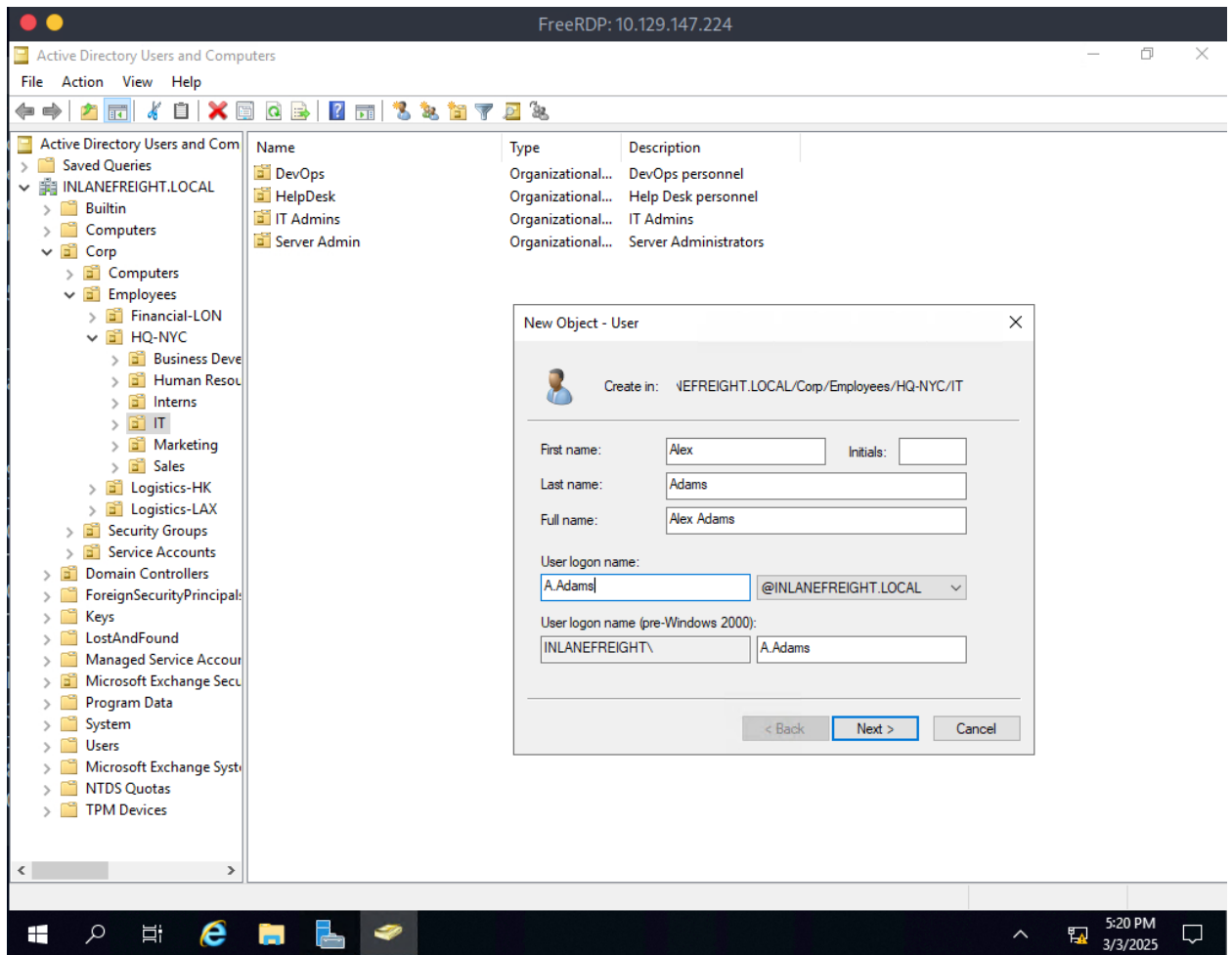
- Adding and removing users from a domain
- Unlocking user accounts
- Creating Organizational Units (OUs) and Security Groups
- Managing Group Policy Objects (GPOs)
- Joining a domain
- Moving objects within a domain

This report details each step I took to complete these tasks.

1. Adding Users to a Domain

To add a new user, **Alex Adams**, to the `inlanefreight.local` domain, I followed these steps:

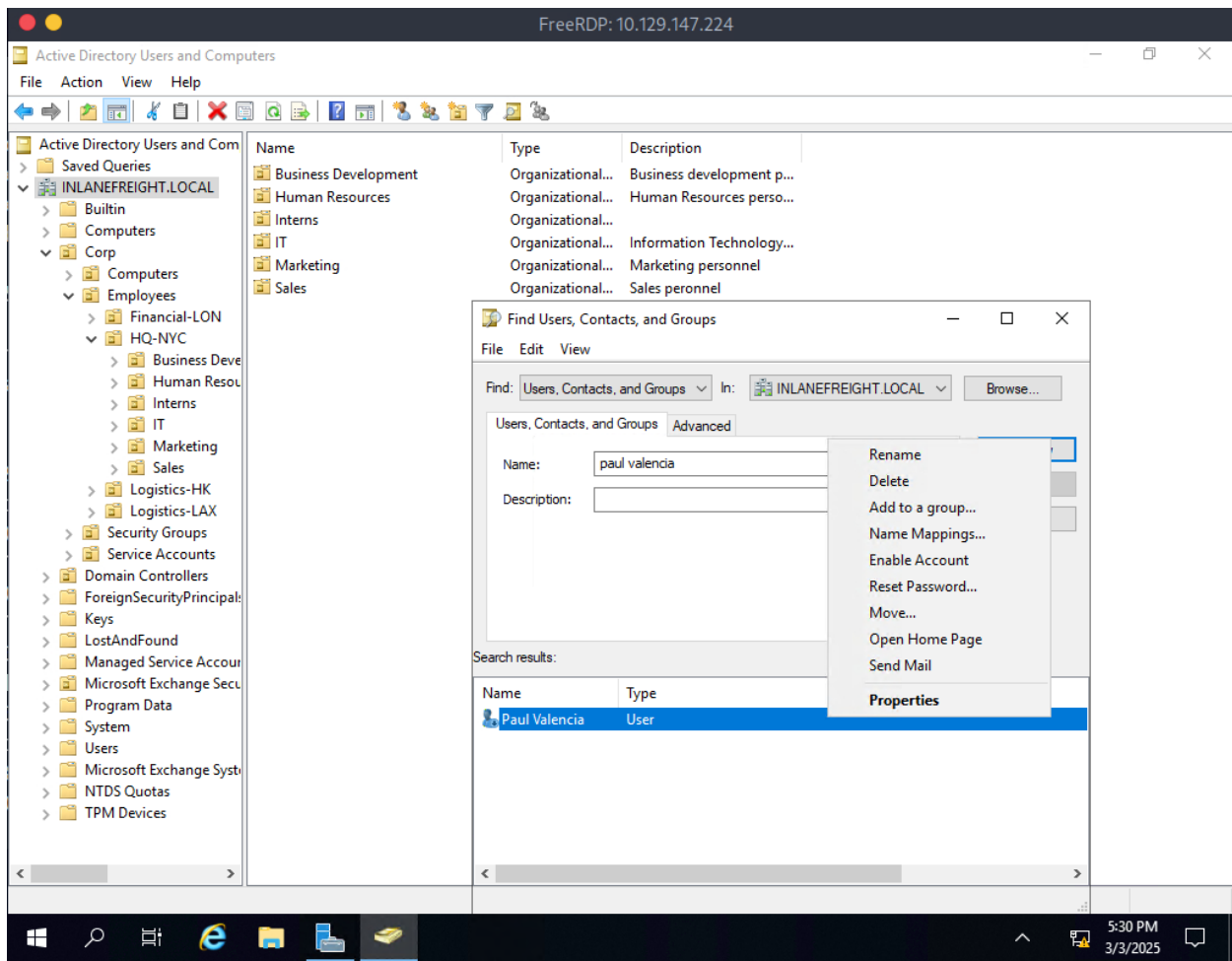
1. Opened the **Active Directory Users and Computers** snap-in.
2. Added **Alex Adams** to the **"IT" Organizational Unit (OU)**.
3. Set it so that Alex would be required to set a password upon first login.



2. Removing Users from a Domain

To remove **Paul Valencia** from the `inlanefreight.local` domain:

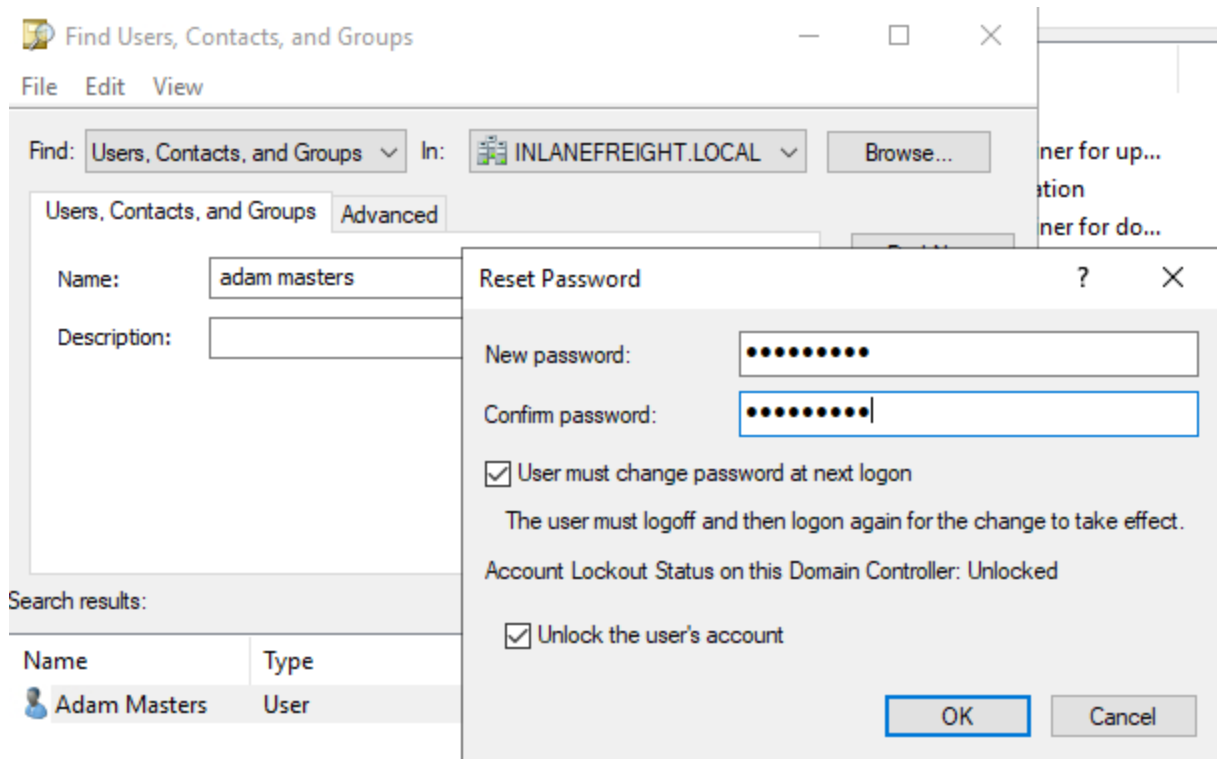
1. I right-clicked on the domain icon and selected **Find**.
2. Searched for **Paul Valencia**.
3. Right-clicked the user entry and selected **Delete**.



3. Unlocking a User's Account

To unlock **Adam Masters'** account:

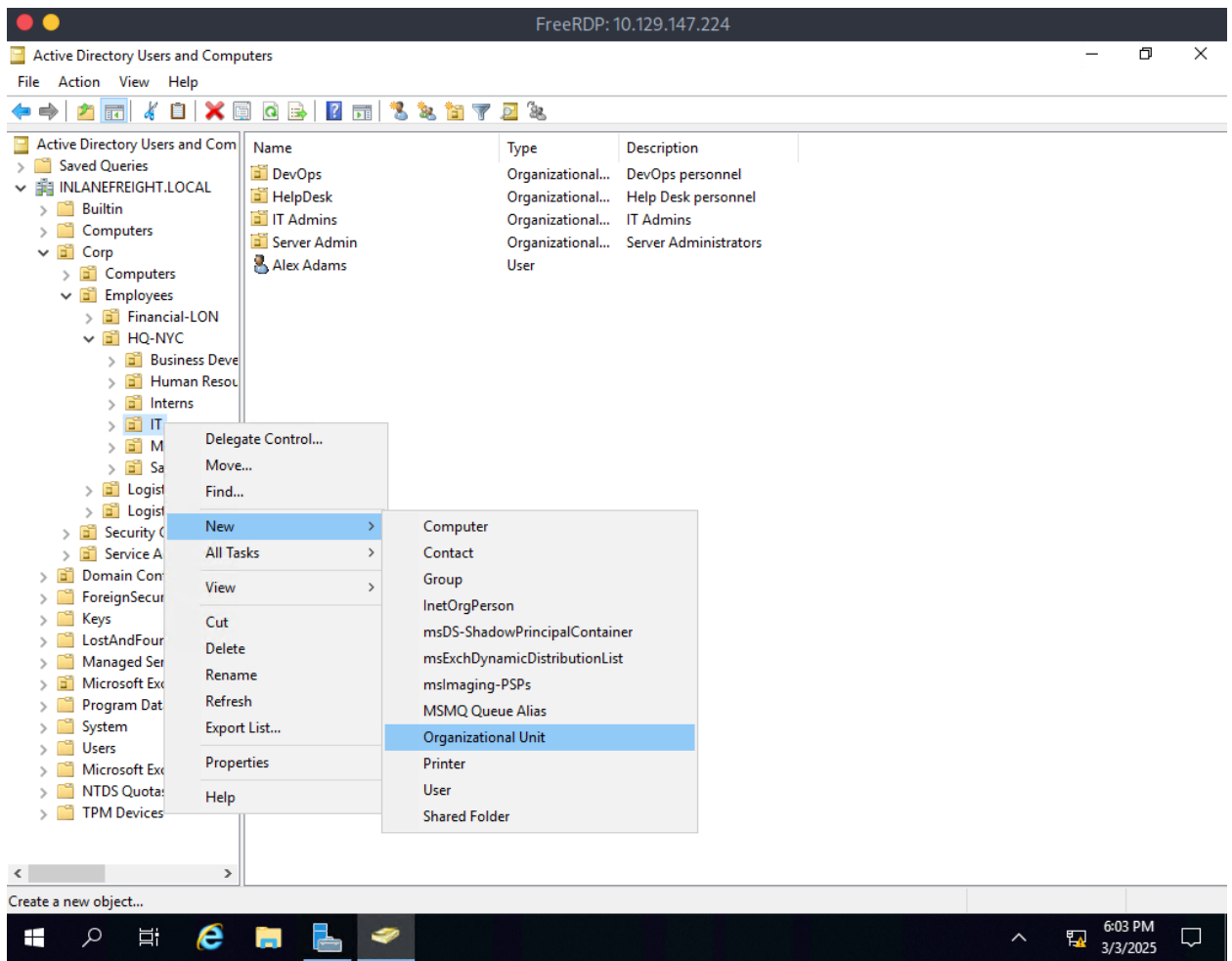
1. I right-clicked on the user and selected **Reset Password**.
2. Entered a new password.
3. Checked the following options:
 - **Require user to reset password at next logon**
 - **Unlock user account**

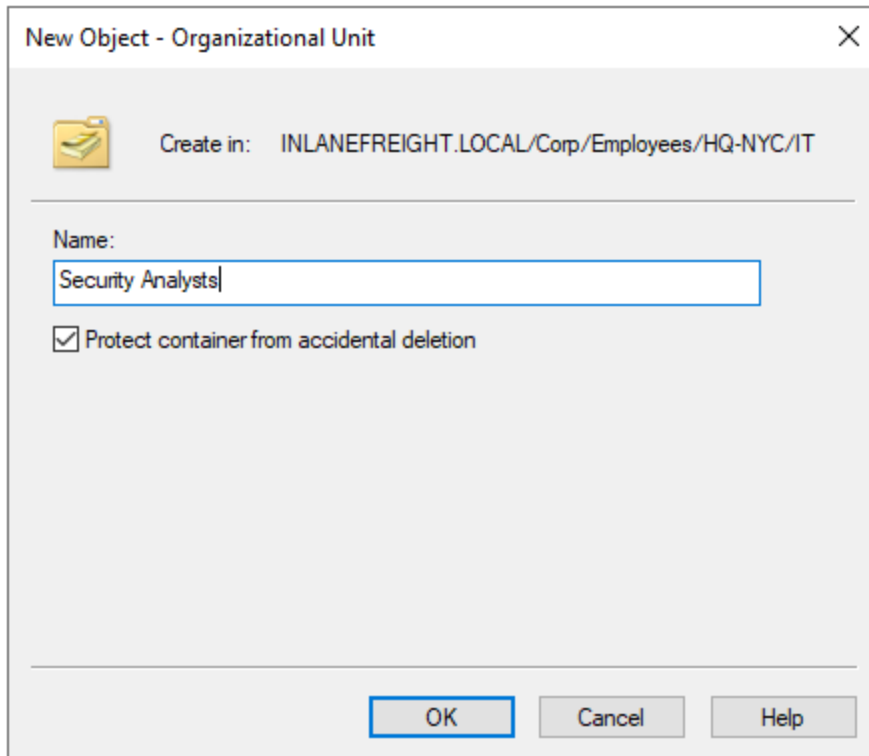


4. Creating a New Security Group and Organizational Unit (OU)

Creating an OU

1. I navigated to the **IT OU**, right-clicked, and selected **New > Organizational Unit**.
2. Named the new OU "**Security Analysts**" and clicked **OK**.





New Object - Organizational Unit

Create in: INLANEFREIGHT.LOCAL/Corp/Employees/HQ-NYC/IT

Name:

Security Analysts

☒ Protect container from accidental deletion

OK Cancel Help

Creating a Security Group

1. Right-clicked on the **Security Analysts OU**.
2. Selected **New > Group**.
3. Named the group "**Security Analysts**".
4. Set **Group Scope** as **Domain Local** and **Group Type** to **Security**.
5. Clicked **OK**.


Name	Type	Description
DevOps	Organizational...	DevOps personnel
HelpDesk	Organizational...	Help Desk personnel
IT Admins	Organizational...	IT Admins
Server Admin	Organizational...	Server Administrators
Security Analysts	Organizational...	
Alex Adams		

Delegate Control...
 Move...
 Find...
New >
 All Tasks >
 Cut
 Delete
 Rename
 Refresh
 Properties
 Help

Computer
 Contact
Group
 InetOrgPerson
 msDS-ShadowPrincipalContainer
 msExchDynamicDistributionList
 mslmaging-PSPs
 MSMQ Queue Alias
 Organizational Unit
 Printer
 User
 Shared Folder

New Object - Group

×


 Create in: -IT.LOCAL/Corp/Employees/HQ-NYC/IT/Security Analysts

Group name:

Group name (pre-Windows 2000):

Group scope
☒ Domain local
☐ Global
☐ Universal

Group type
☒ Security
☐ Distribution

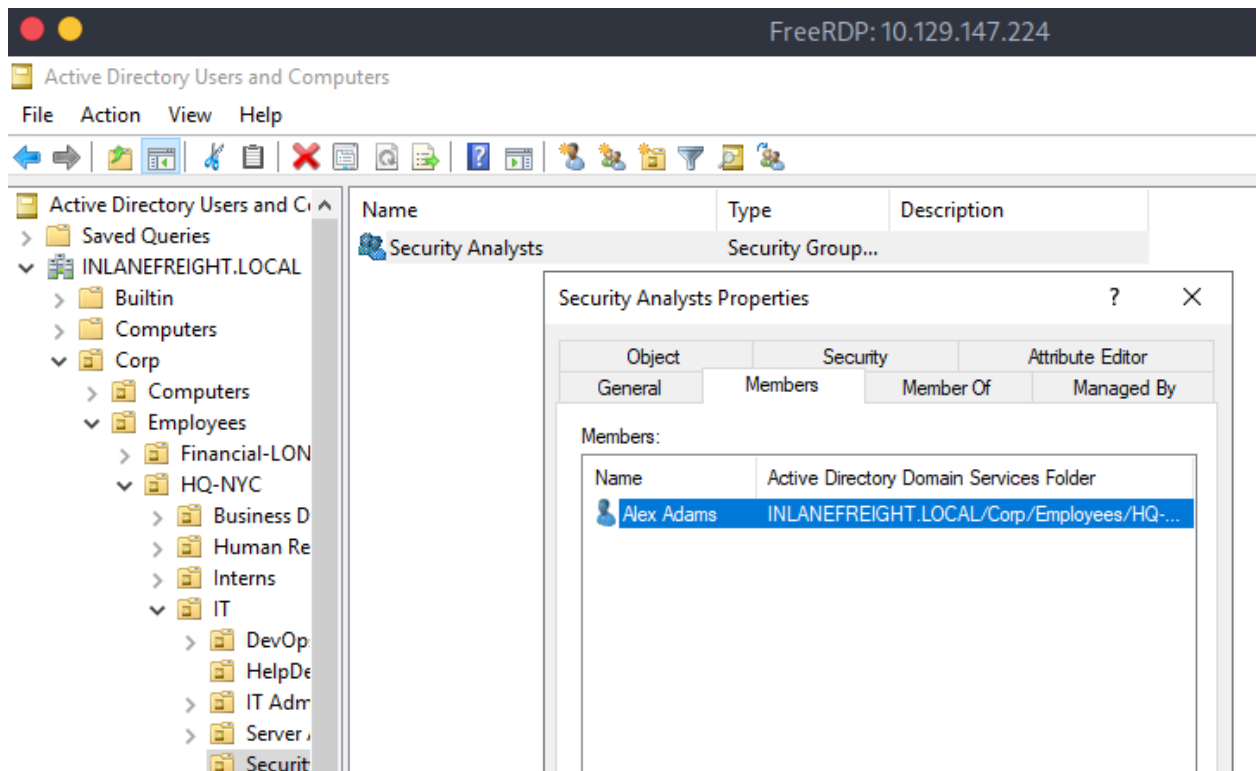
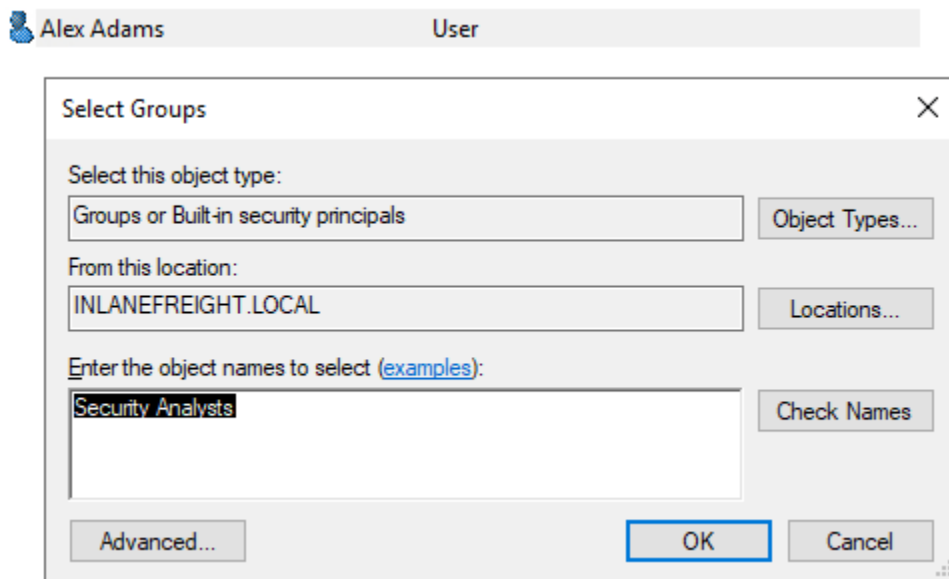
OK

Cancel

5. Adding a User to a Security Group

To add **Alex Adams** to the **Security Analysts** group:

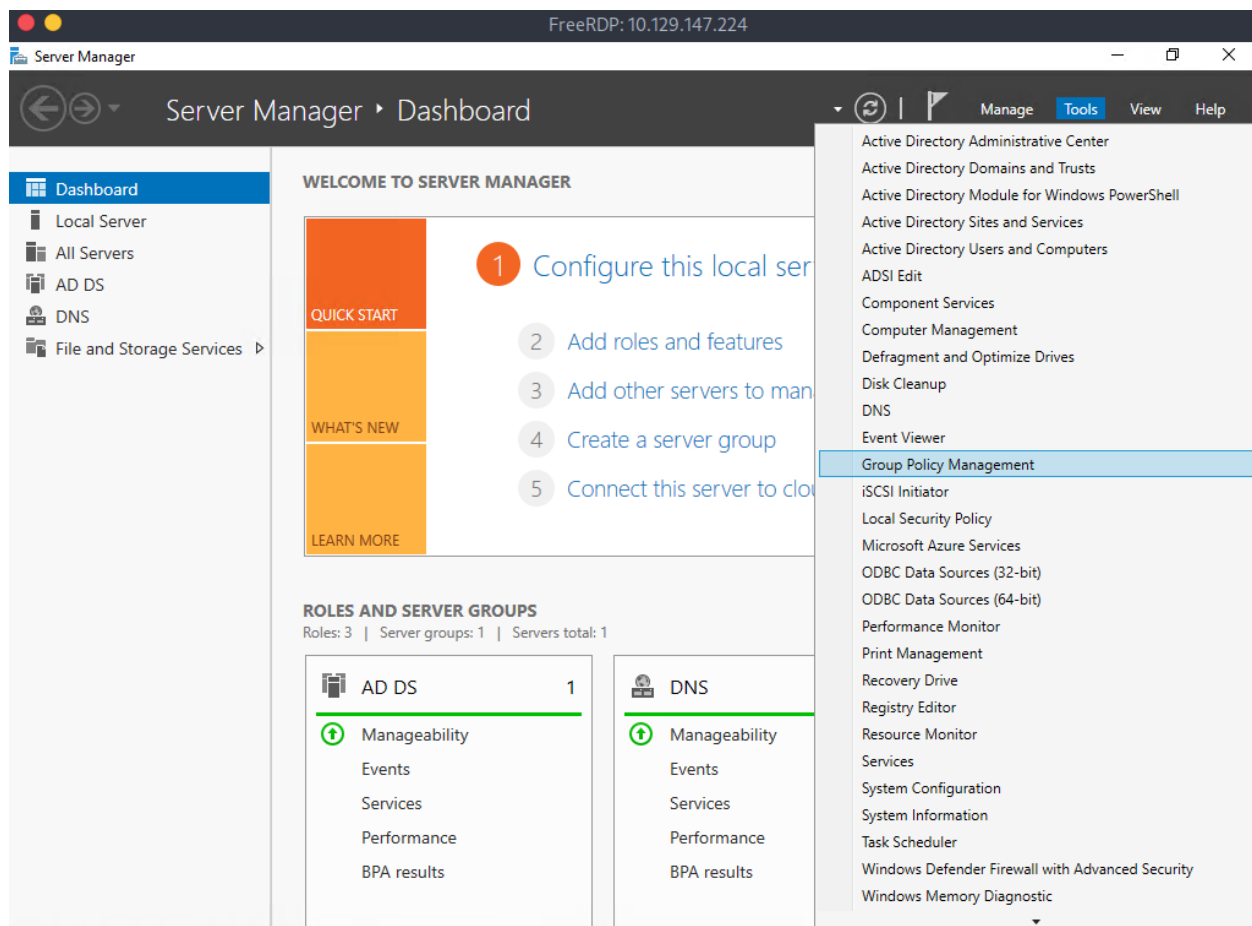
1. I right-clicked on **Alex Adams** and selected **Add to a group**.
2. Entered "**Security Analysts**" and clicked **OK**.
3. Verified that Alex was successfully added to the group.



6. Managing Group Policy Objects (GPOs)

Copying and Renaming an Existing GPO

1. I opened **Group Policy Management** from the Server Manager tools.
2. Opened **PowerShell** and ran:
3. `Copy-GPO -SourceName "Logon Banner" -TargetName "Security Analysts Control"`
4. Linked the new GPO to the **Security Analysts OU** with:
5. `New-GPLink -Name "Security Analysts Control" -Target "ou=Security Analysts,ou=IT,OU=HQ-NYC,OU=Employees,OU=Corp,dc=INLANEFREIGHT,dc=LOCAL" -LinkEnabled Yes`



```

FreeRDP: 10.129.216.2
Administrator: Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\hnb-student_admin> Copy-GPO -SourceName "Logon Banner" -TargetName "Security Analysts Control"

DisplayName       : Security Analysts Control
DomainName        : INLANEFREIGHT.LOCAL
Owner             : INLANEFREIGHT\Domain Admins
Id                : 80b3bb54-b46f-4de4-8a55-72541e42b22f
IpoStatus         : AllSettingsEnabled
Description       :
CreationTime      : 3/4/2025 12:23:52 PM
ModificationTime  : 3/4/2025 12:23:52 PM
UserVersion       : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter         :

PS C:\Users\hnb-student_admin> New-GPLink -Name "Security Analysts Control" -Target "ou=Security Analysts,ou=IT,OU=HQ-NYC,OU=Employees,OU=Corp,dc=INLANEFREIGHT,dc=LOCAL" -LinkEnabled Yes

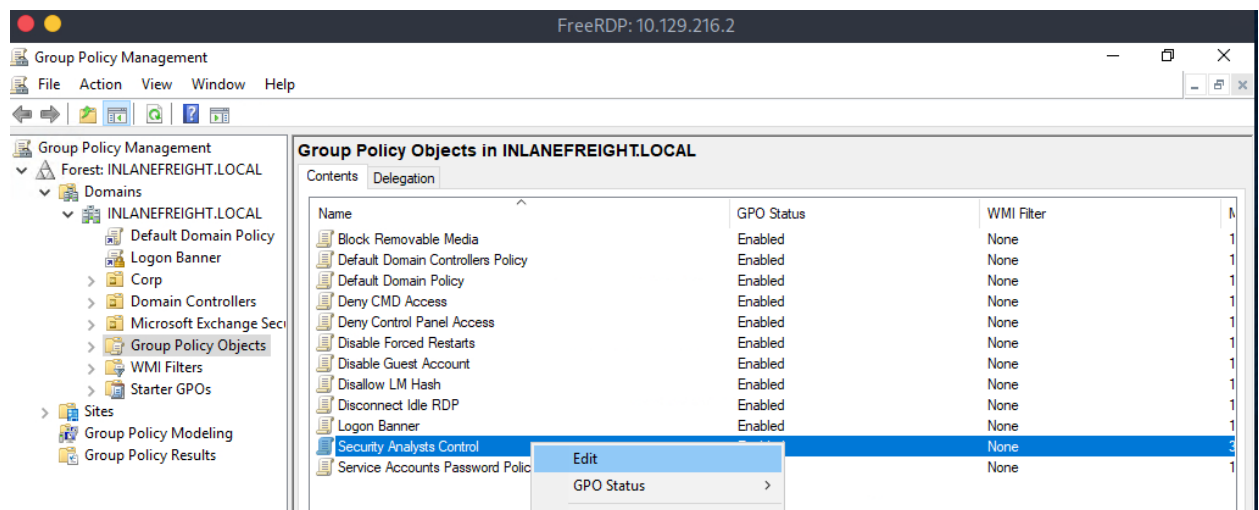
IpoId            : 80b3bb54-b46f-4de4-8a55-72541e42b22f
DisplayName       : Security Analysts Control
Enabled          : True
Enforced         : False
Target           : OU=Security Analysts,OU=IT,OU=HQ-NYC,OU=Employees,OU=Corp,DC=INLANEFREIGHT,DC=LOCAL
Order           : 1

PS C:\Users\hnb-student_admin>

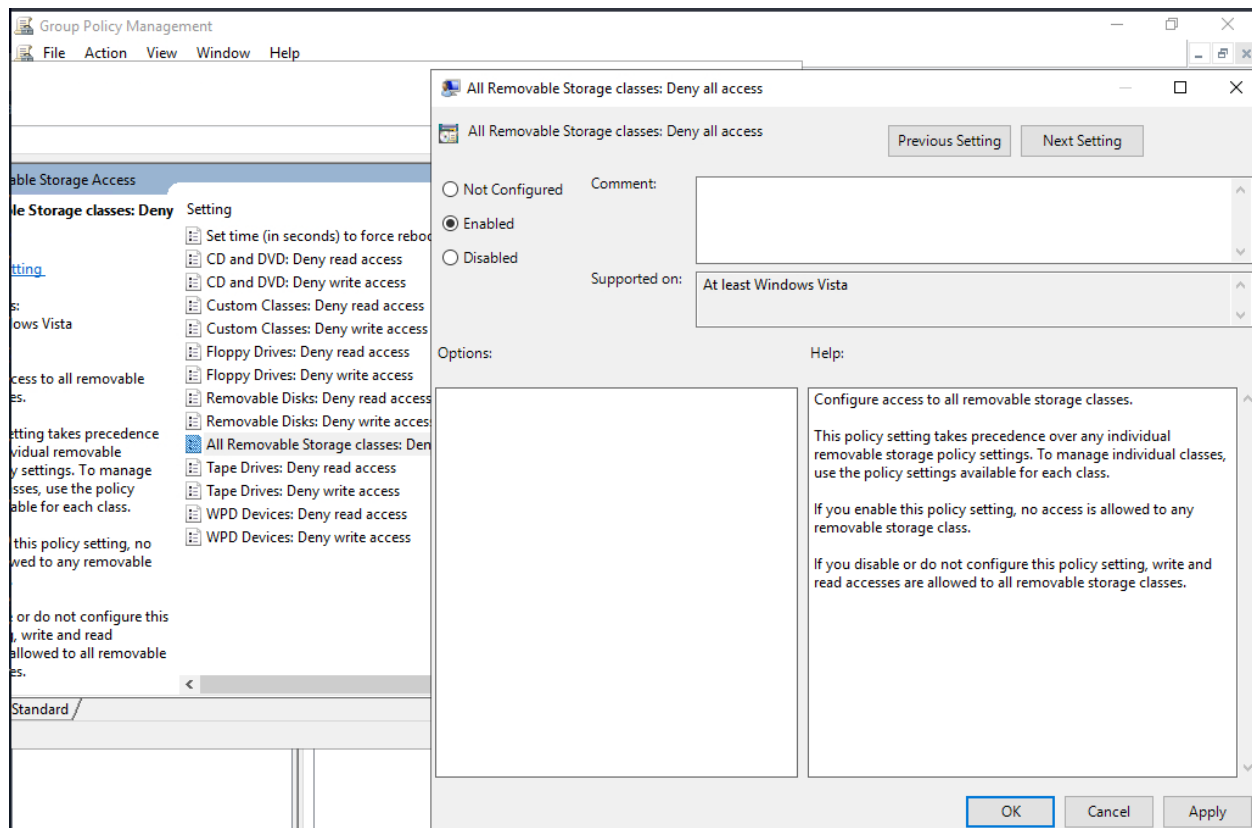
```

Modifying Group Policy Settings

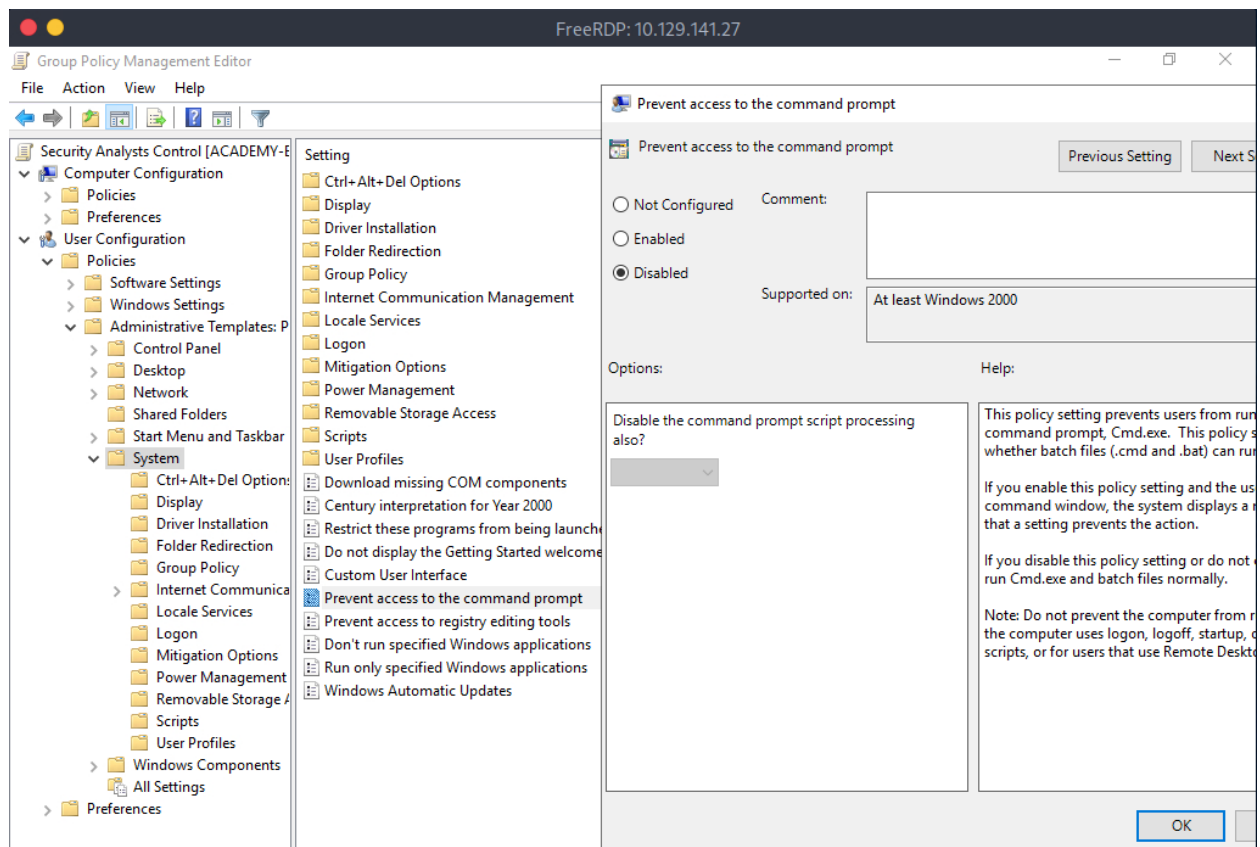
1. I opened **Group Policy Management Console (GPMC)** and right-clicked **Security Analysts Control**, selecting **Edit**.



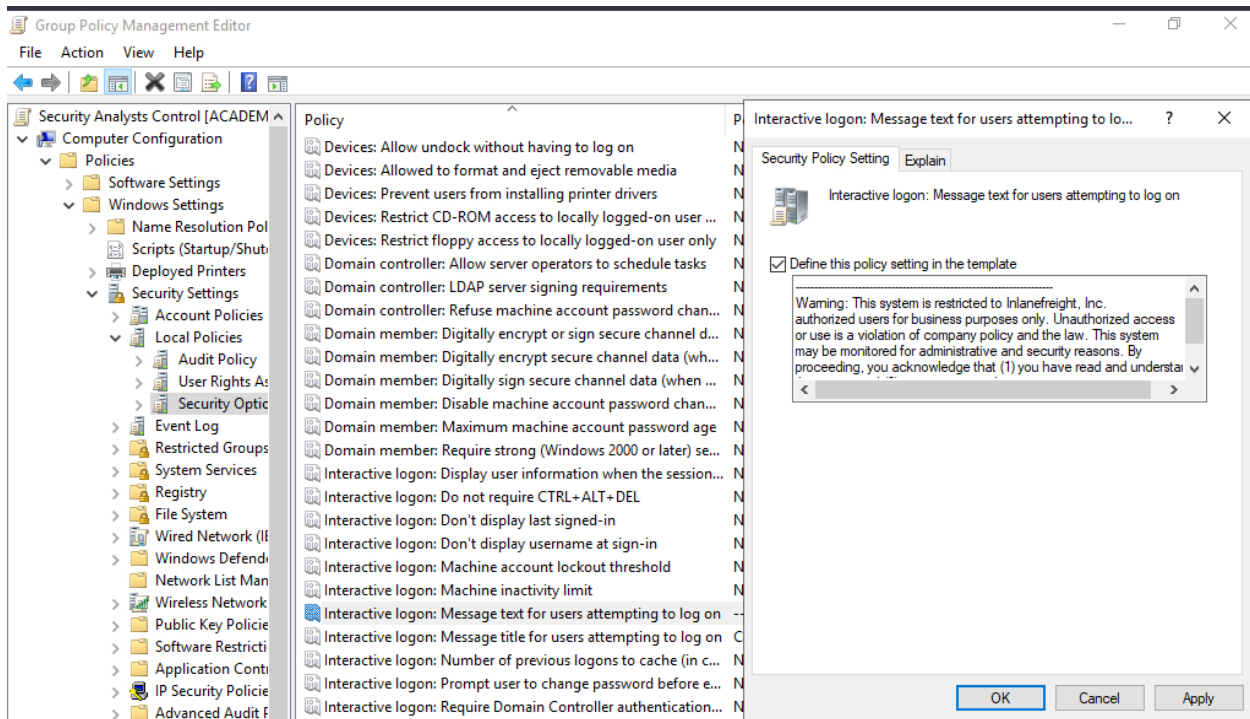
2. Adjusted the following policies:
 - o **Blocked Removable Storage:**
 - **Path:** *User Configuration > Policies > Administrative Templates > System > Removable Storage Access*
 - Set to **Enabled**.



- **Allowed Security Analysts Access to Command Prompts:**
 - **Path:** *User Configuration > Policies > Administrative Templates > System*
 - **Disabled Prevent Access to the Command Prompt.**

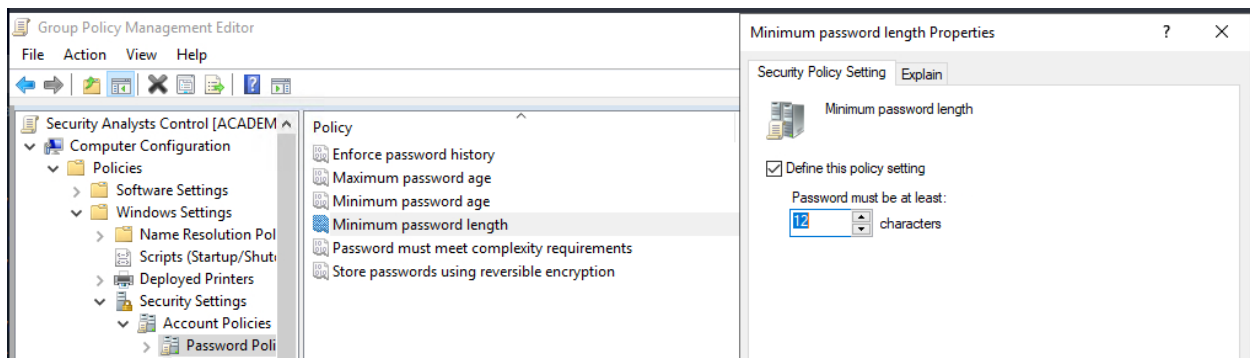


- **Verified Logon Banner Functionality:**
 - **Path:** *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options*
 - Checked that the **Interactive Logon Message Text** remained unchanged.

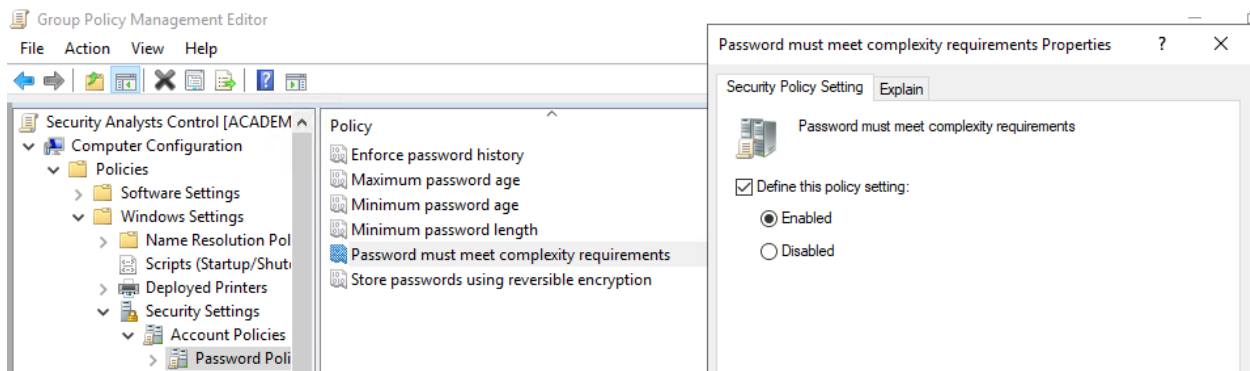


- **Strengthened Password Policies:**

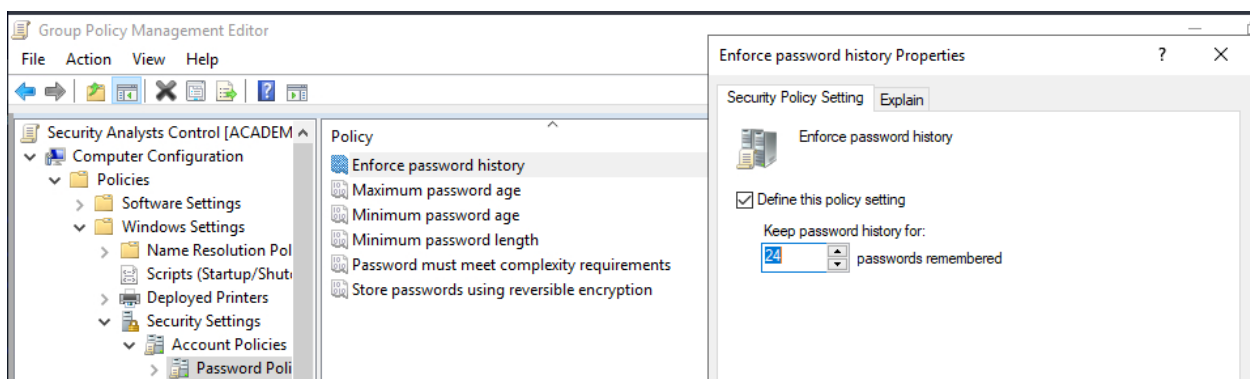
- **Path:** *Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy*
- **Set Minimum Password Length to 12 characters.**



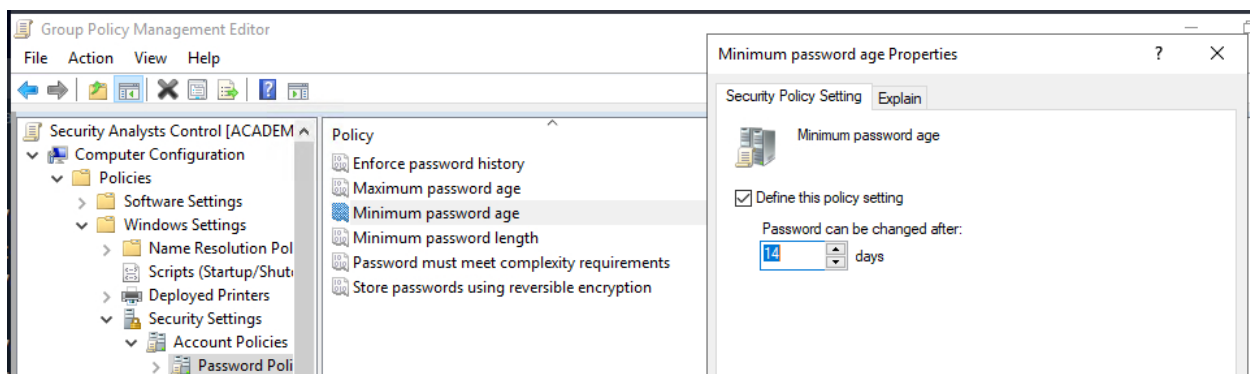
- **Enabled Require Complex Passwords.**

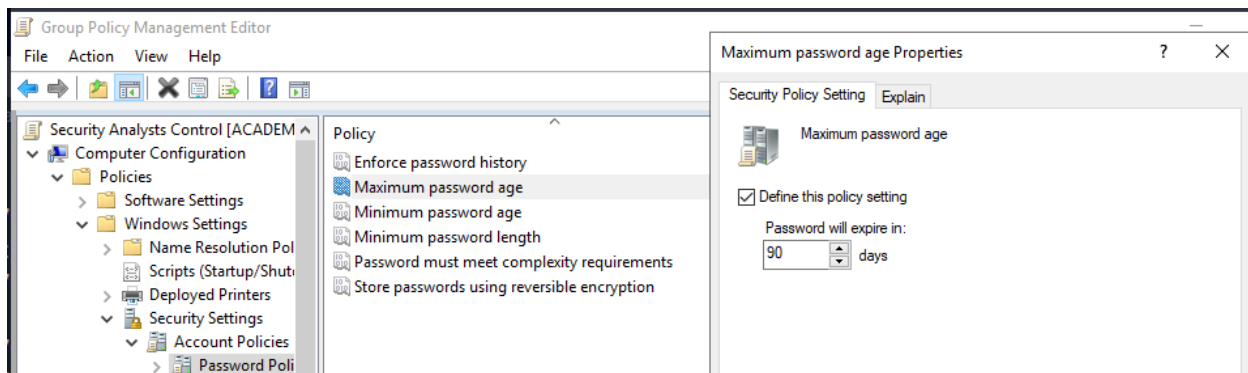


- **Enabled Enforce Password History (set to 24).**



- **Set Minimum Password Age to 5 days and Maximum Password Age to 90 days.**

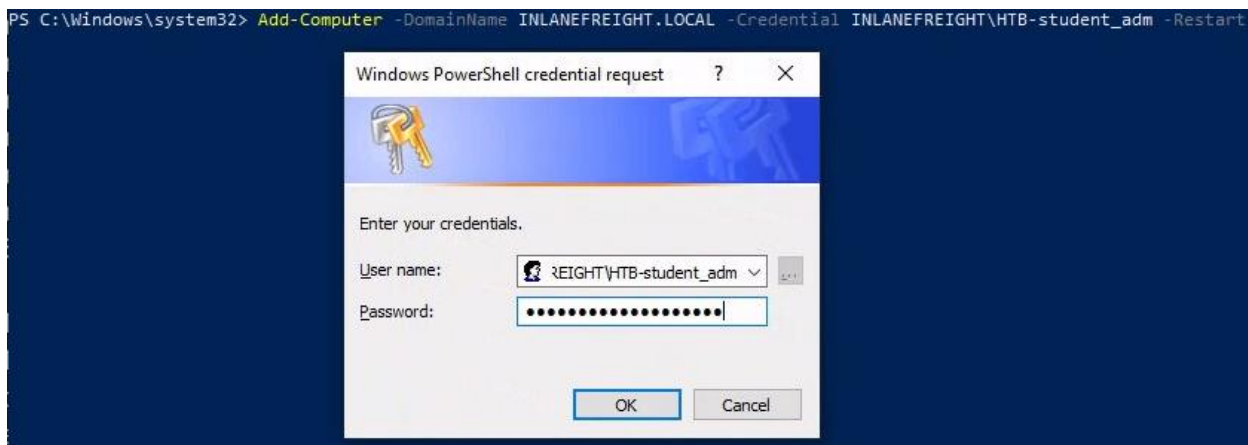




7. Adding a Computer to the Domain

To add a newly provisioned security analyst's computer to the domain:

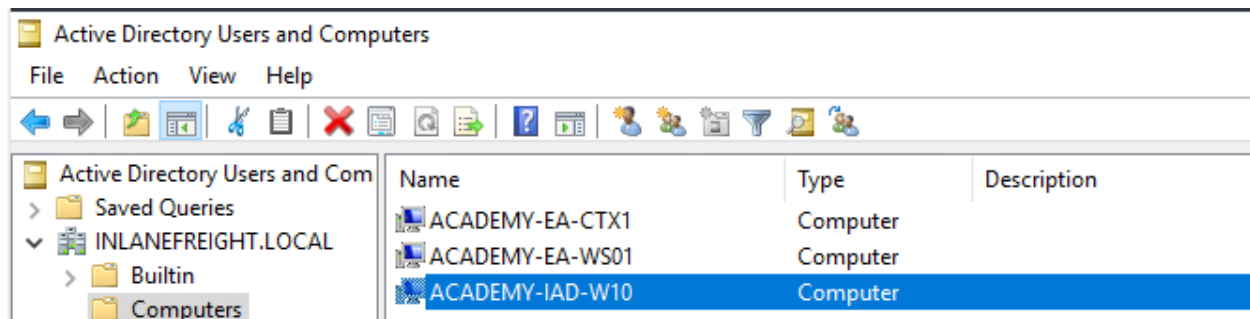
1. I connected to the system via xfreerdp.
2. Opened **PowerShell (Administrator)** and ran:
3. `Add-Computer -DomainName INLANEFREIGHT.LOCAL -Credential INLANEFREIGHT\HTB-student_adm -Restart`
4. Entered the required credentials and executed the command.



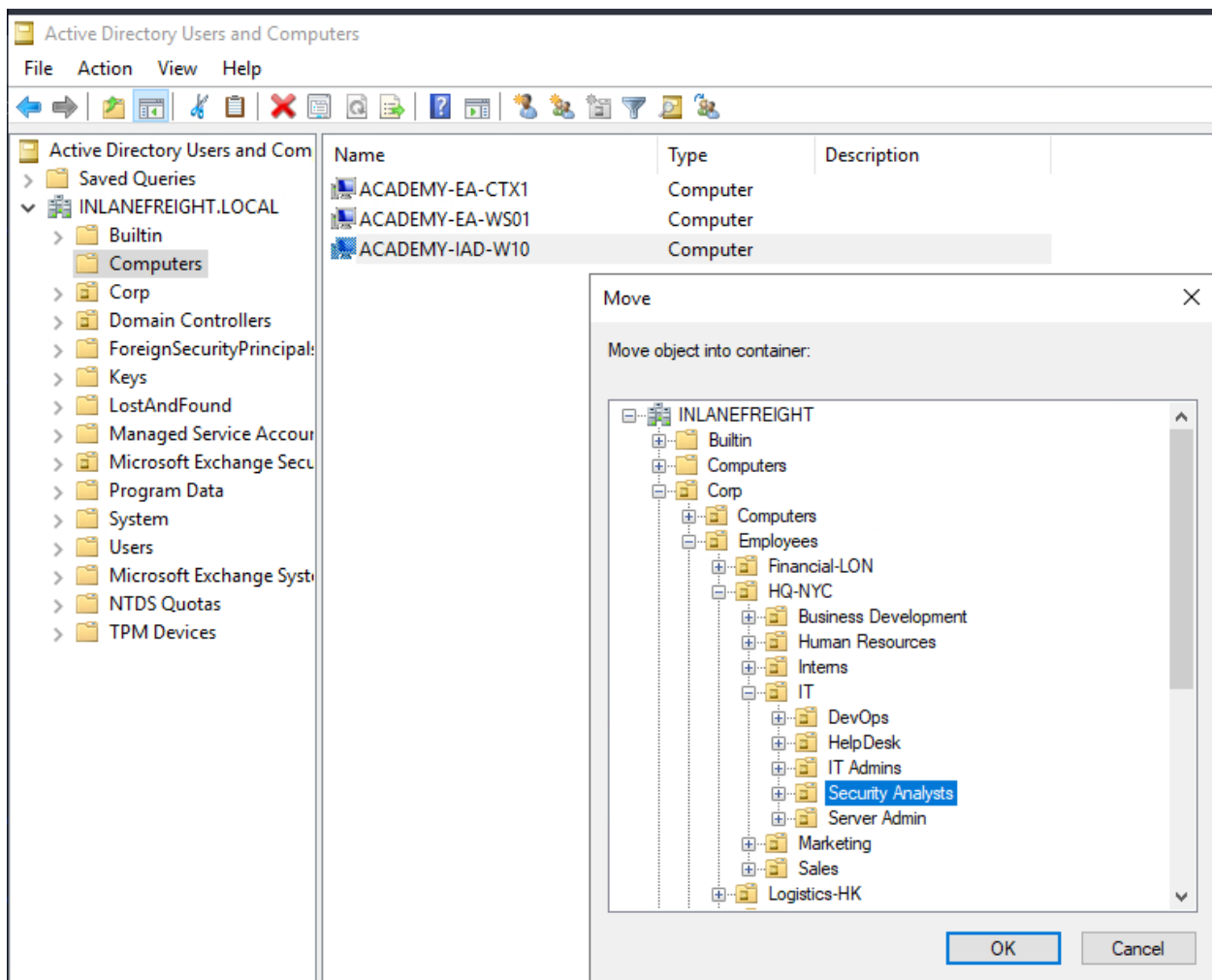
8. Moving a Computer Object to a New OU

To move the newly provisioned computer to the **Security Analysts OU**:

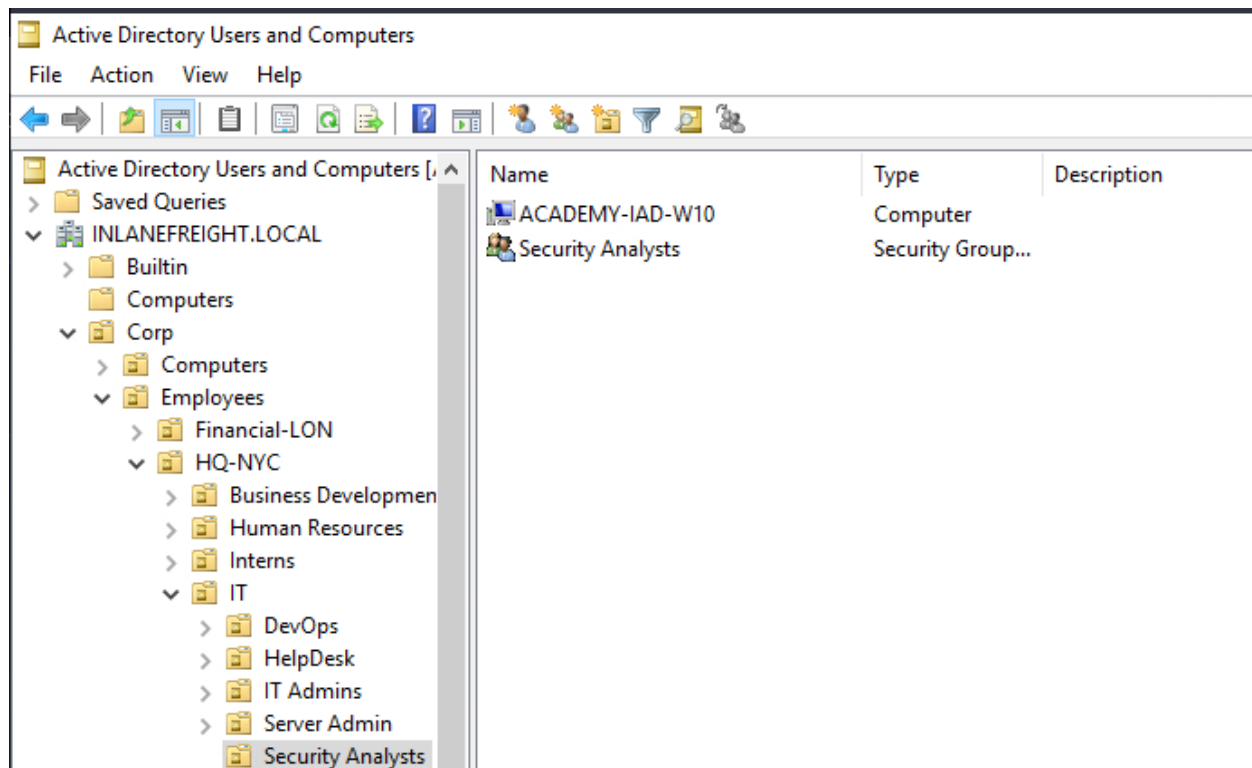
1. I opened **Active Directory Users and Computers**.
2. Located the computer object.



3. Right-clicked, selected **Move**, and chose **Security Analysts OU**.



4. Confirmed that the computer object was successfully moved.



Summary

This project allowed me to gain hands-on experience with essential Active Directory administration tasks. From managing users and security groups to implementing Group Policy and integrating new devices, I followed structured steps to ensure a secure and efficient domain environment.

By carefully setting up OUs, enforcing strong password policies, and managing Group Policy Objects, I reinforced best practices for security and administrative efficiency. Working through these tasks provided me with a deeper understanding of how Active Directory streamlines user and device management.