Mini Project: NIST 800-171 Access Control Lab (Completed Controls)
Environment: Windows Lab

Project Overview

This lab demonstrates practical implementation of selected **NIST 800-171 Access Control (AC) family controls**.
Controls implemented:

- AC-2: Account Management
- AC-3: Access Enforcement
- AC-5: Separation of Duties
- AC-6: Least Privilege
- AC-11: Session Lock
- AC-17: Remote Access

Evidence is captured through screenshots showing configuration, permissions, and test results.

AC-2: Account Management

Objective: Manage user accounts to control access and ensure proper privileges.

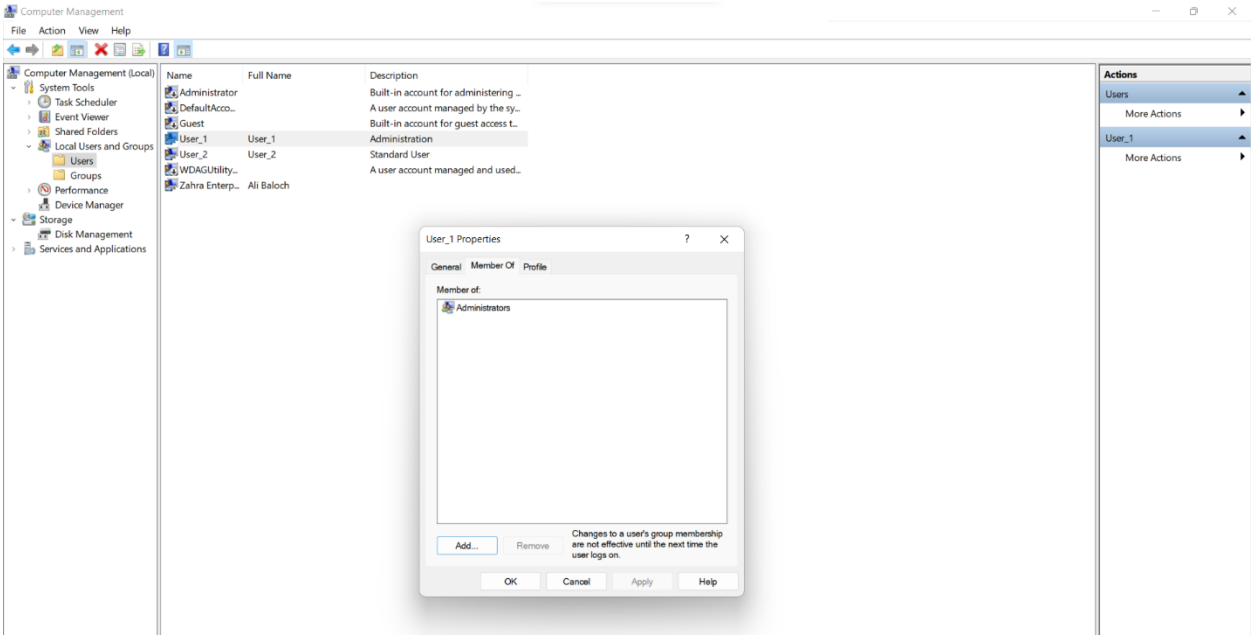
Steps:

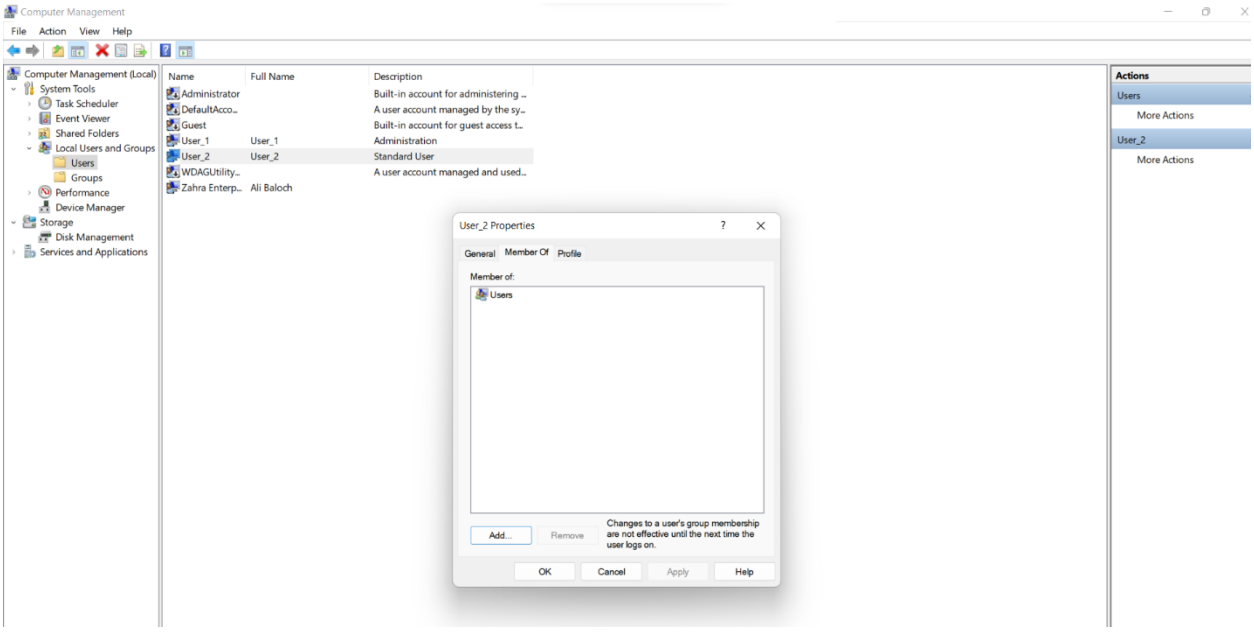
1. Create and configure user accounts: User_1 (Admin), User_2 (Standard).
2. Assign groups and permissions appropriately.
3. Test login and account restrictions.

Evidence / Screenshots:

- User accounts and group memberships
- Account creation and permissions
- Login tests

Screenshots:

1. 

2. 

AC-3: Access Enforcement

Objective: Enforce access control policies so users can only perform allowed actions.

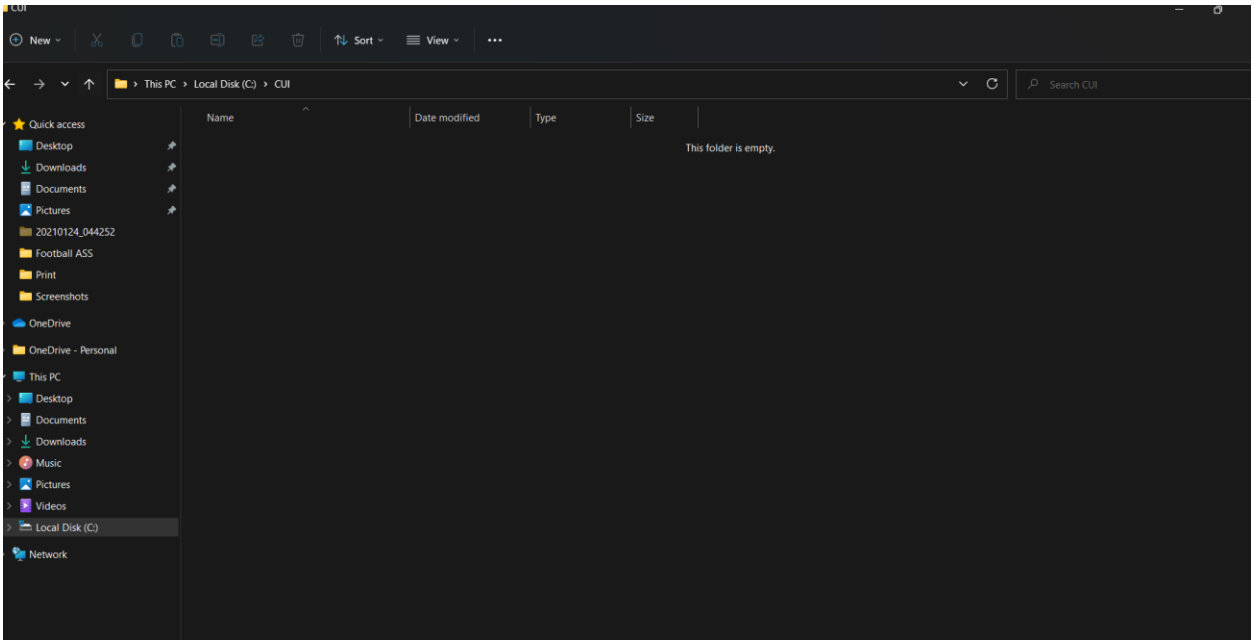
Steps:

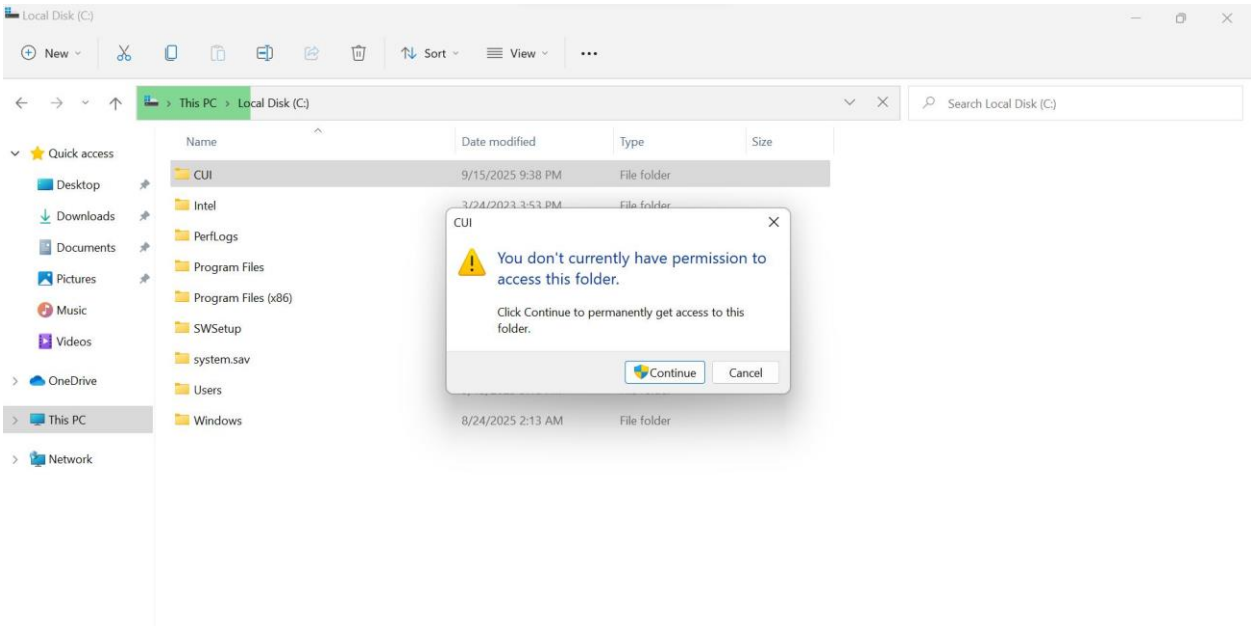
1. Configure User_1 as Admin, User_2 as Standard.
2. Test access to restricted areas or operations.
3. Verify access enforcement works correctly.

Evidence / Screenshots:

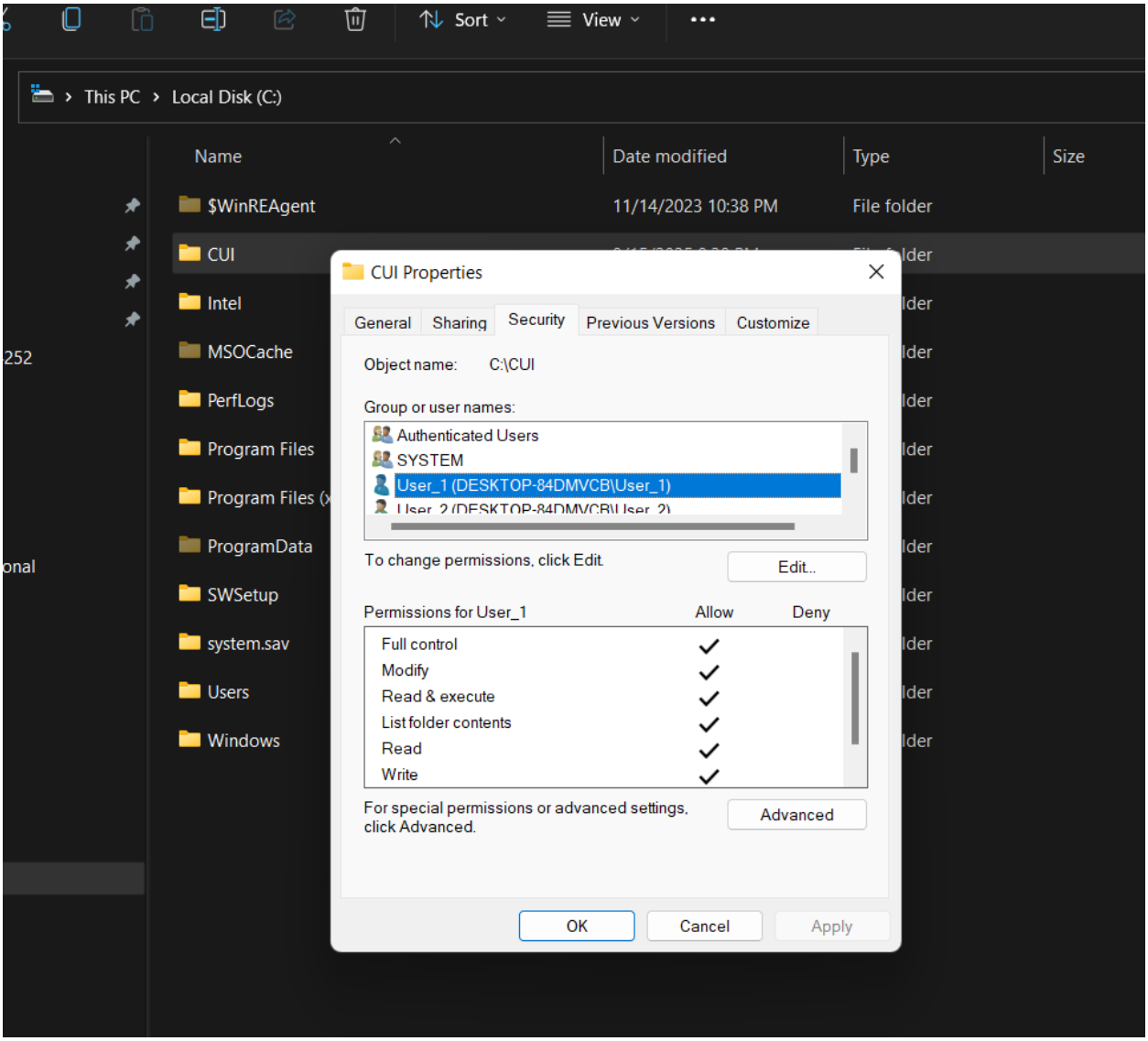
- Attempted restricted actions (denied)
- Allowed actions by Admin

Screenshots:

1. 


Local Disk (C:)
New
Sort
View
This PC
Local Disk (C:)
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
CUI
9/15/2025 9:38 PM
File folder
Intel
PerfLogs
Program Files
Program Files (x86)
SWSetup
system.sav
Users
Windows
8/24/2025 2:13 AM
File folder
CUI
You don't currently have permission to access this folder.
Click Continue to permanently get access to this folder.
Continue
Cancel

2.

3. 

AC-5: Separation of Duties

Objective: Prevent any single user from having too much control.

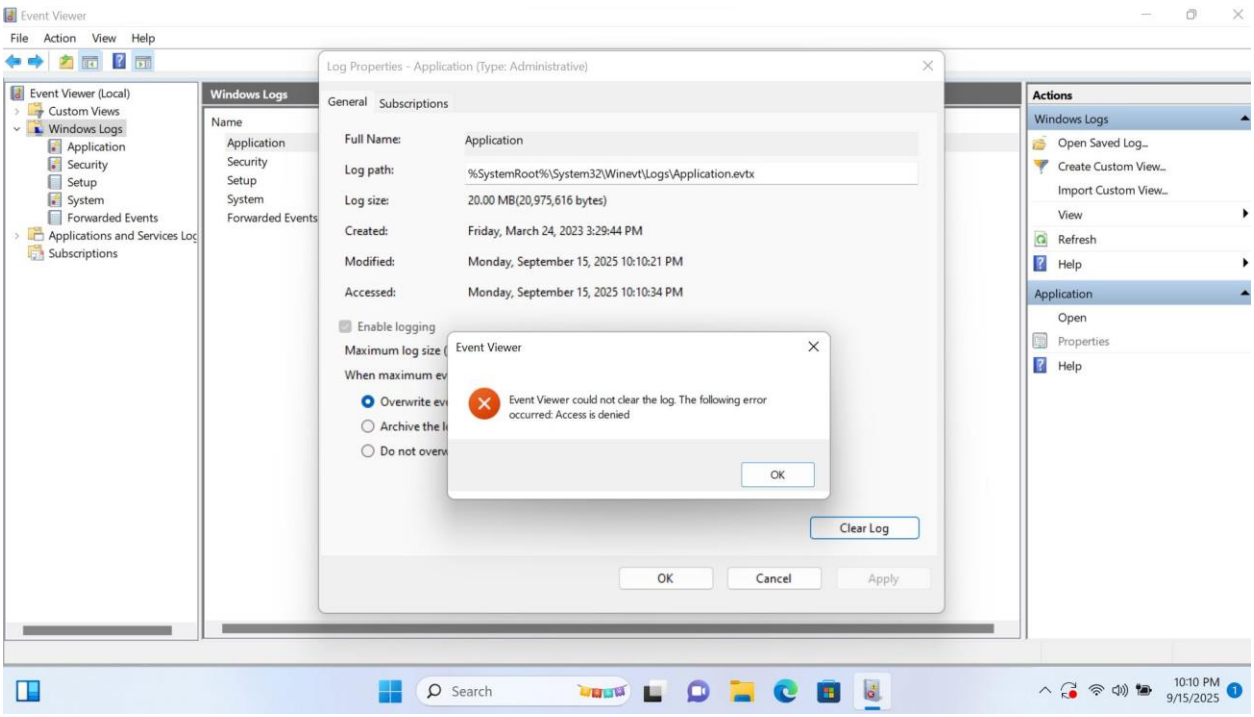
Steps:

1. User_1 as Admin
2. User_3 as Standard (Auditor) with read-only access to Event Logs
3. Verify User_1 can modify settings, User_3 can only view logs

Evidence / Screenshots:

- User_1 group membership
- User_3 group membership
- Event Log permissions
- Denied modification attempt by User_3

Screenshots:

1. 

AC-6: Least Privilege

Objective: Ensure users have only the access needed for daily tasks.

Steps:

1. User_1_Admin → admin rights

2. User_1_Standard → normal user rights
3. Daily tasks performed on User_1_Standard
4. Use User_1_Admin only for system changes

Evidence / Screenshots:

- Attempted admin action by User_1_Standard → denied
- Successful admin action by User_1_Admin
- Account group memberships

AC-11: Session Lock

Objective: Automatically lock system after inactivity.

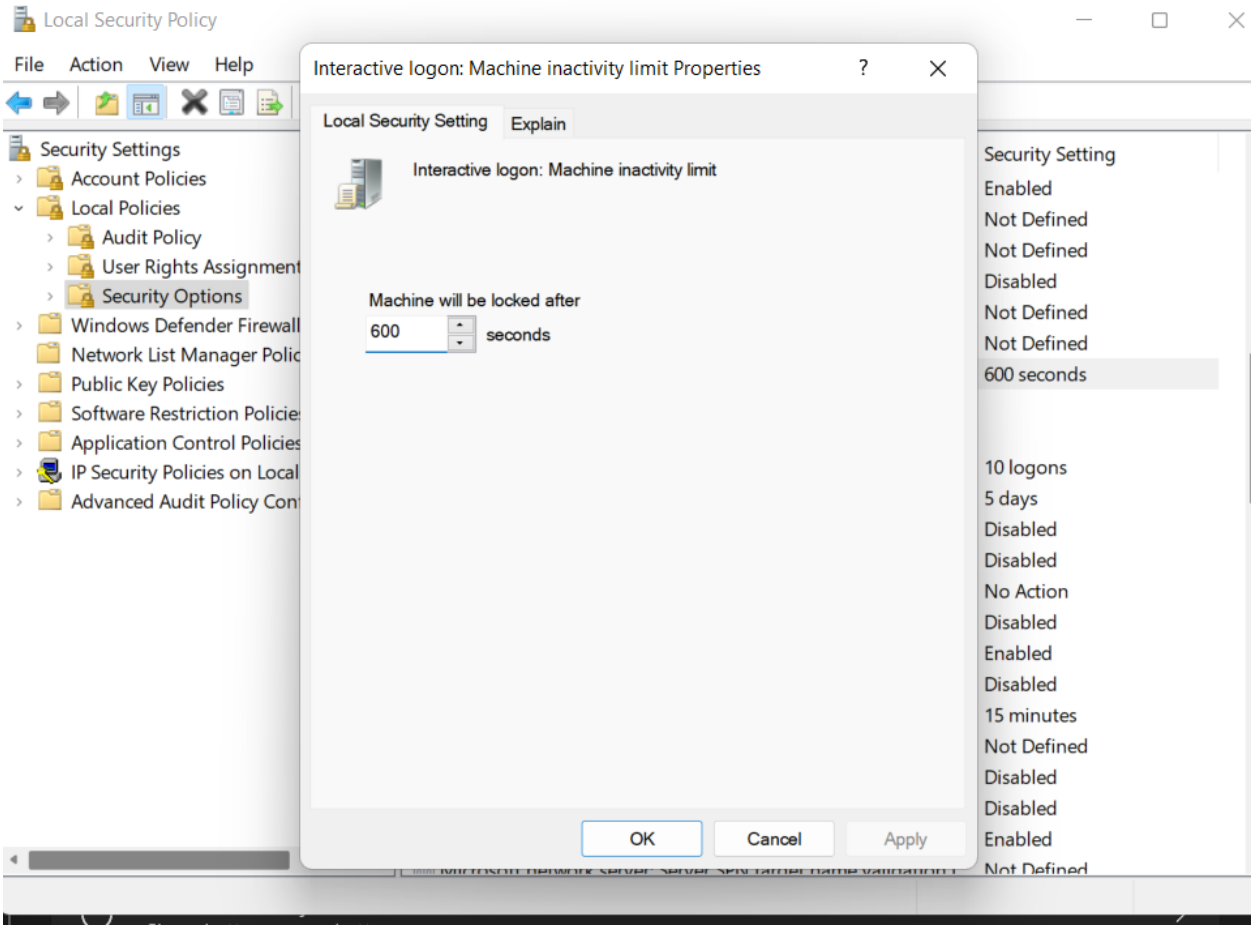
Steps:

1. Open secpol.msc → Security Options
2. Set **Interactive logon: Machine inactivity limit** → 10 min
3. Test inactivity lock

Evidence / Screenshots:

- Policy settings / screen saver settings
- Locked screen after 10 minutes

Screenshots:

1. 

AC-17: Remote Access

Objective: Restrict remote access to authorized users only.

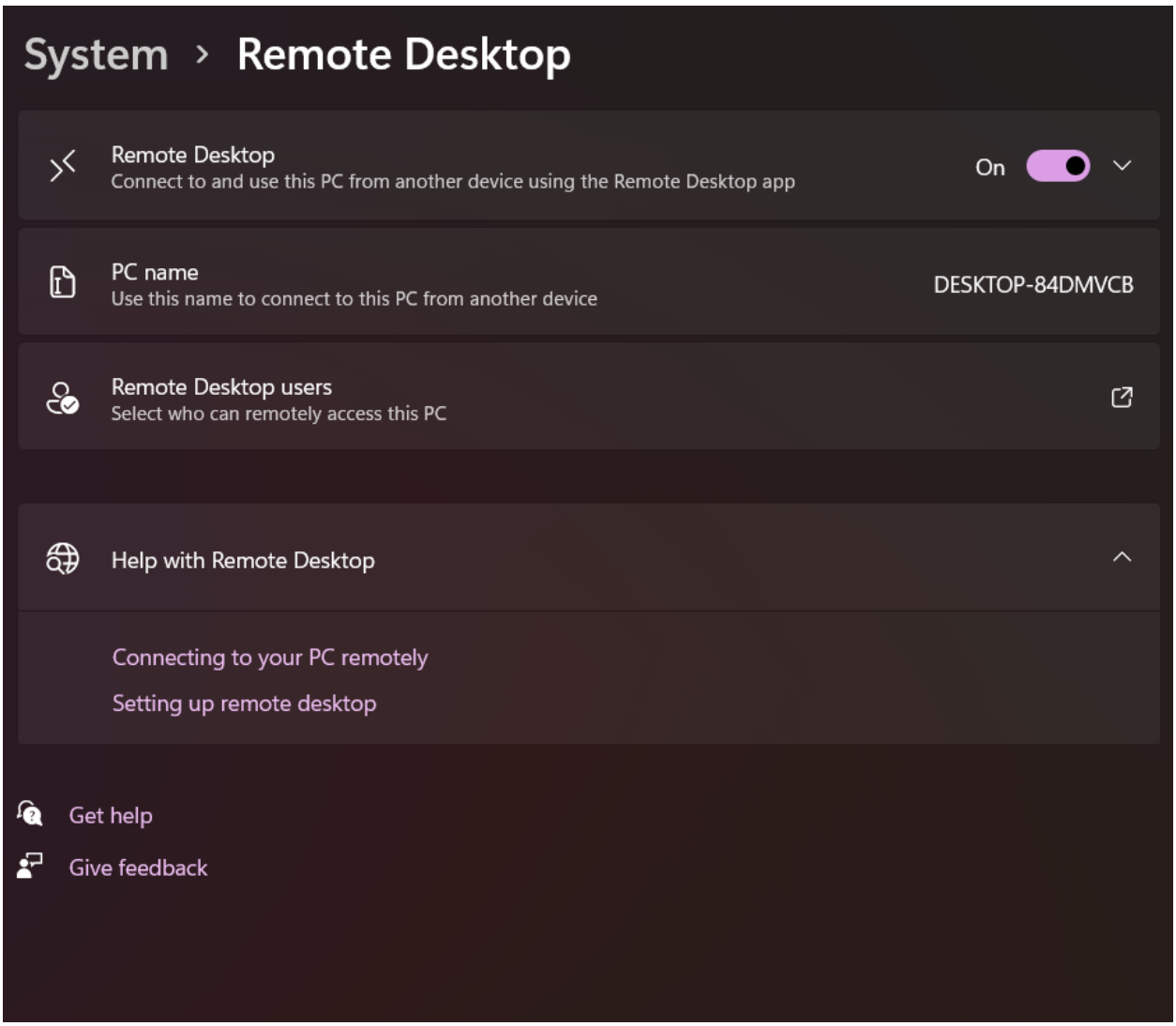
Steps:

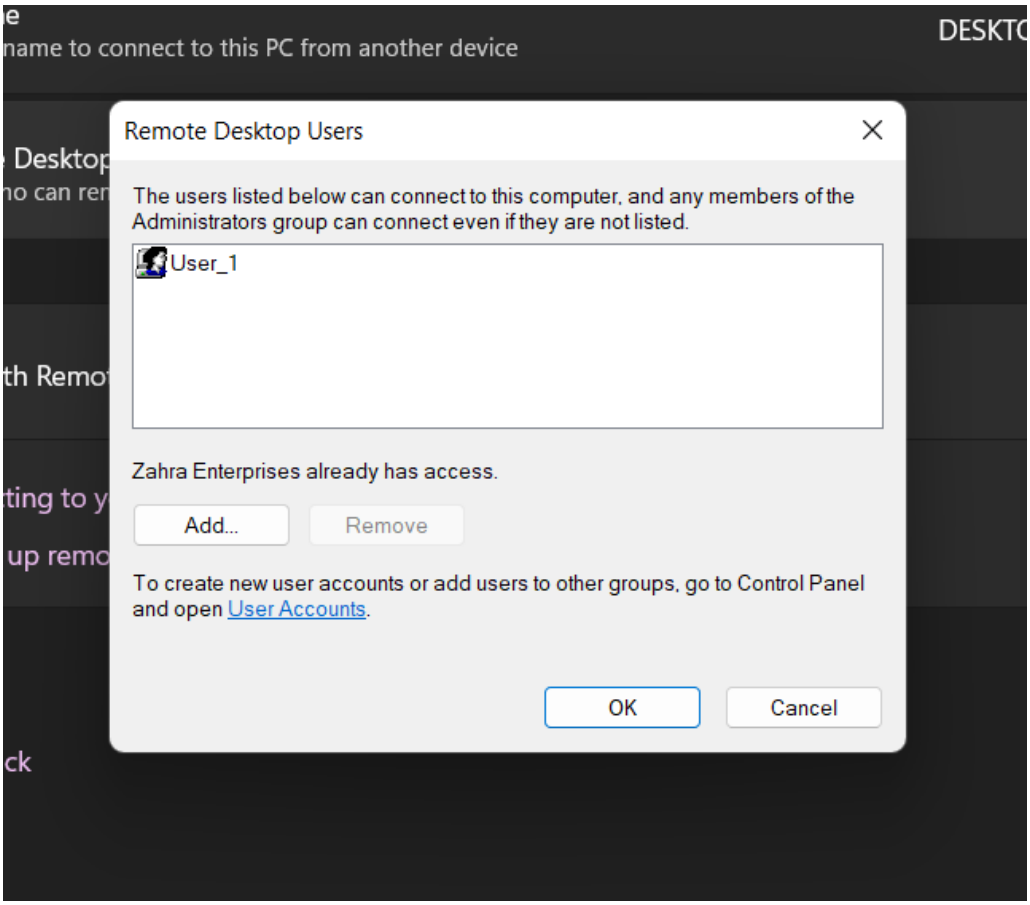
1. Enable Remote Desktop
2. Allow only User_1 to connect remotely
3. Note computer name
4. Test login as User_1 → success
5. Test login as User_2/User_3 → denied

Evidence / Screenshots:

- Remote Desktop settings (enabled)
- User_1 allowed access
- Failed login attempt for User_2/User_3
- Successful login for User_1

Screenshots:

1. 

2. 

Conclusion

This lab demonstrates practical implementation of **AC-2, AC-3, AC-5, AC-6, AC-11, and AC-17** in a Windows environment.

- Policies enforced include account management, access enforcement, separation of duties, least privilege, session lock, and secure remote access.
- Evidence captured via screenshots confirms correct configuration and enforcement of access control policies.