Irine May Ompaling 202105203
BSIT 4-2

Week 4 Lab Activity: Managing Users and Groups on Windows

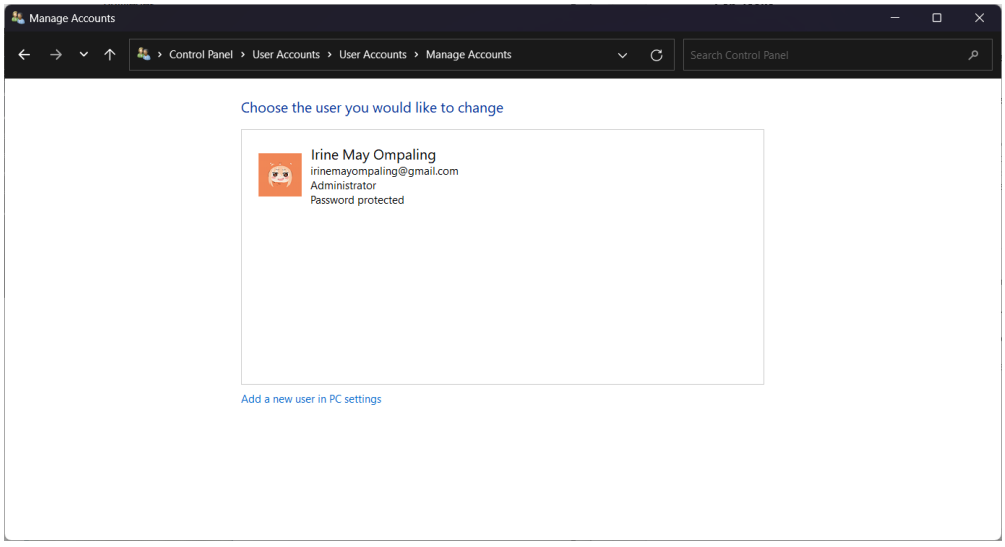
Objective:

In this lab, students will practice creating and managing user accounts and groups on a Windows system, setting permissions, and controlling access to directories. By completing these tasks, students will learn how to organize and secure user access within a Windows environment.

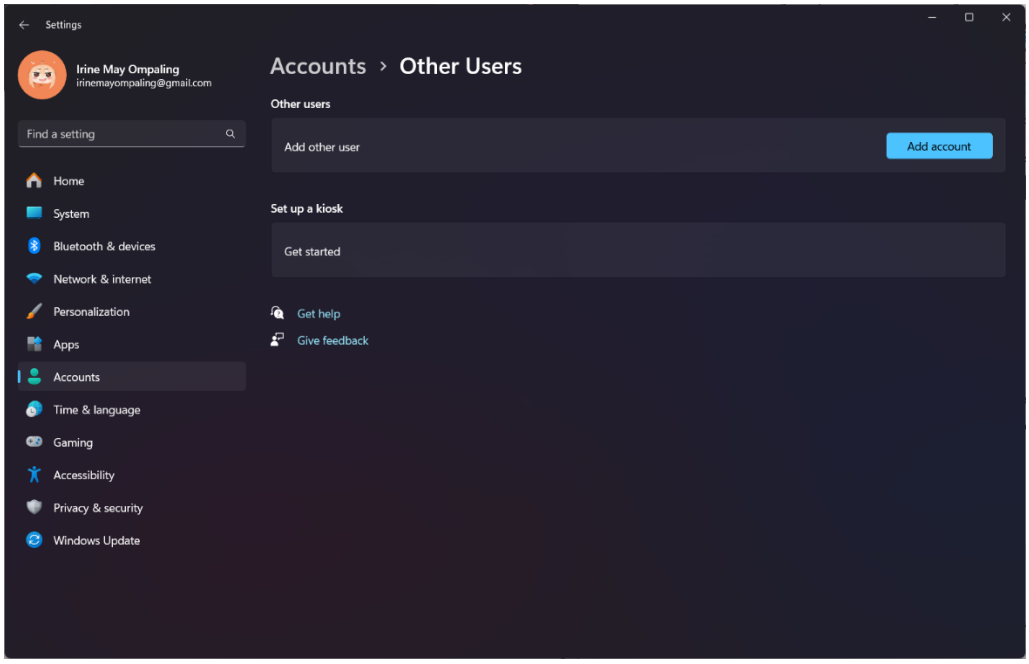
Lab Tasks

1. Creating and Managing User Accounts

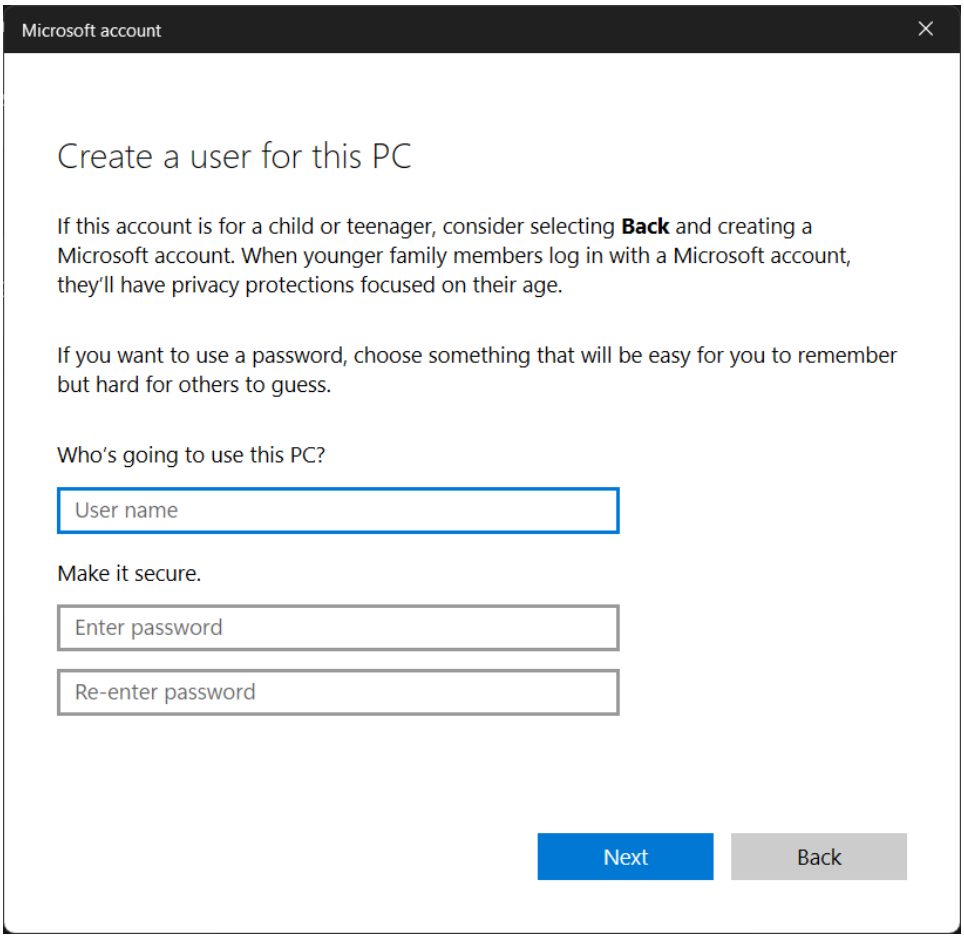
- **Task:** Create two user accounts: one with standard permissions and another with administrator permissions.
- **Instructions:**
    1. Open **Control Panel → User Accounts → Manage Another Account**.



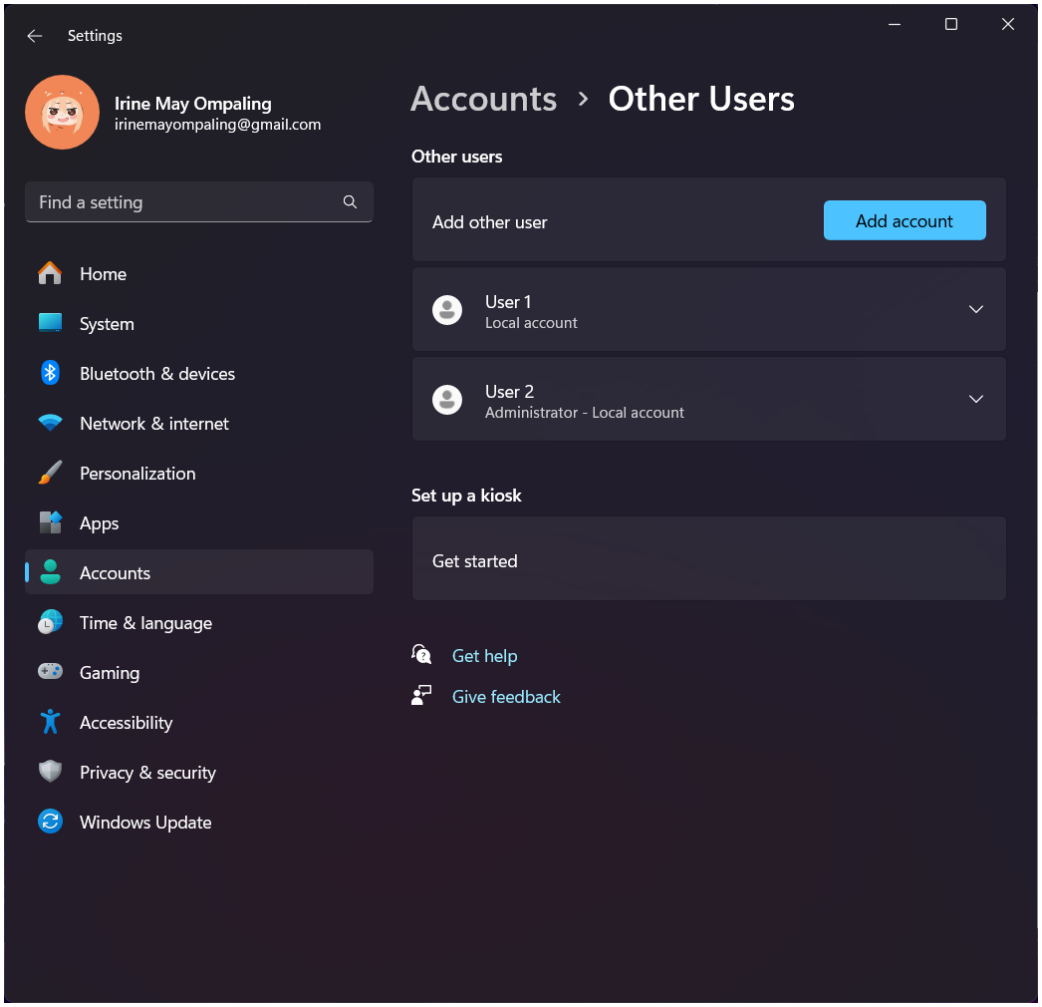
    2. Click **Add a new user in PC settings**.



3. In the **Settings** window, go to **Family & other users**.
4. Select **Add someone else to this PC** to create a new account.



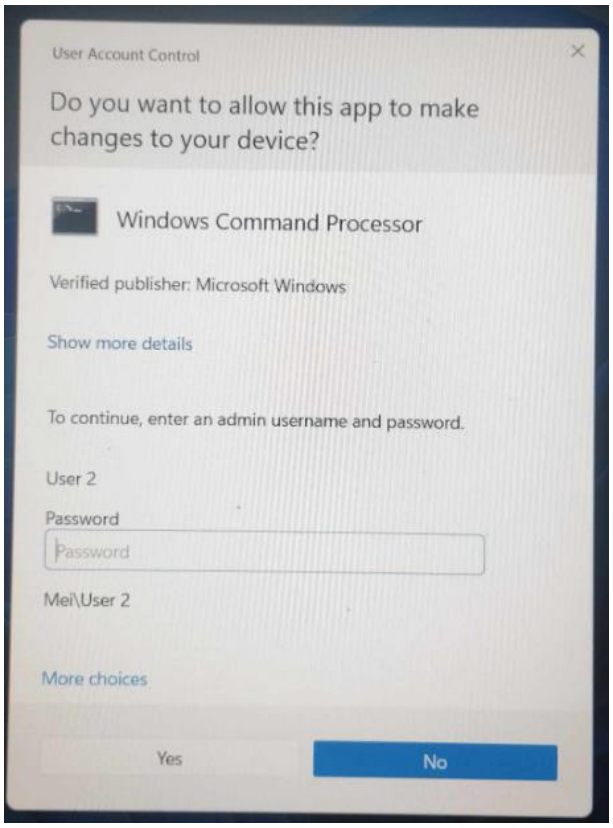
5. Set up one user as a **Standard User** and another with **Administrator** privileges.



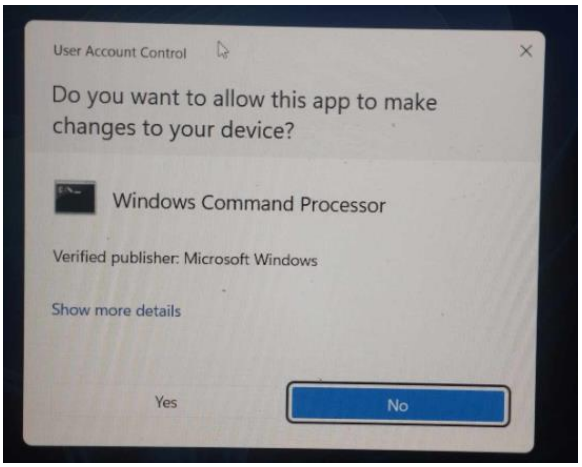
6. Log in as each user to verify their access levels.

- **Verification:** Confirm that the standard user has limited access, while the administrator user has full permissions.

User 1

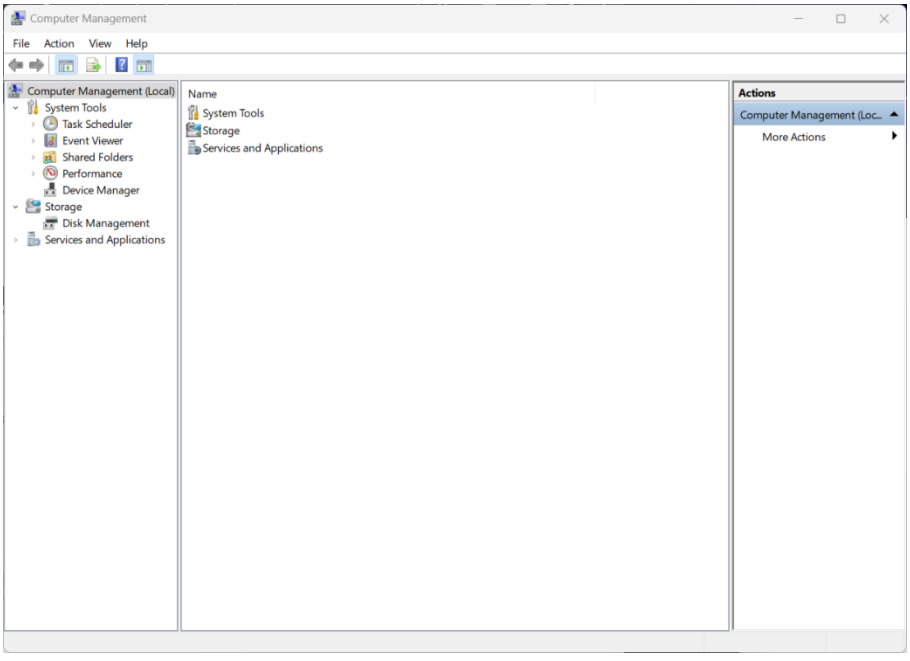


User 2

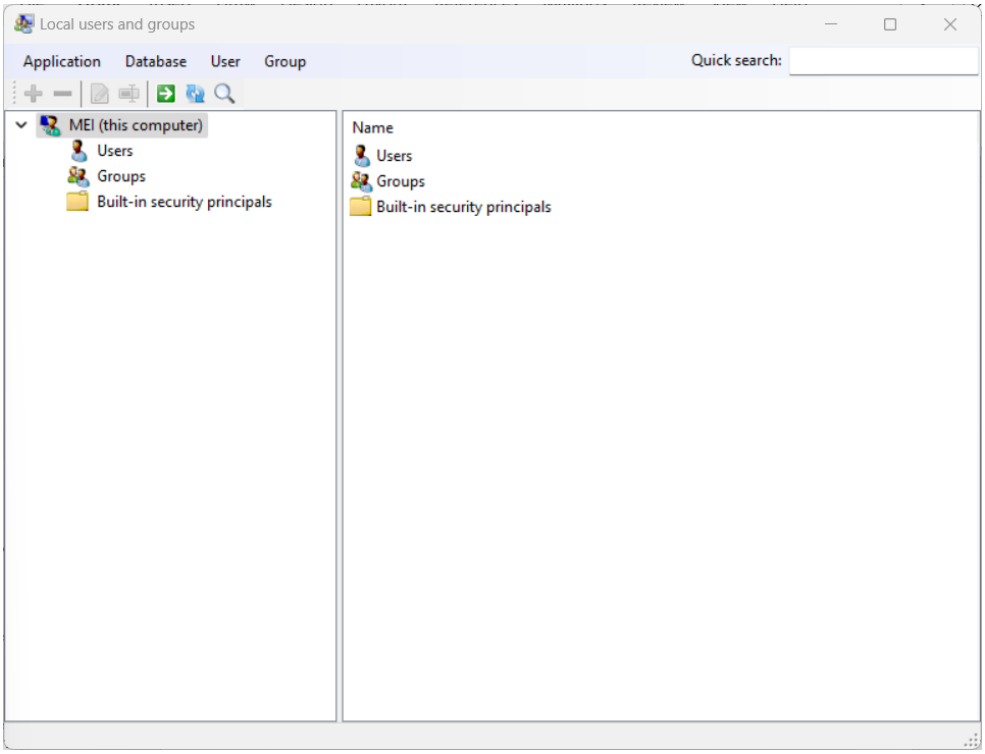


2. Creating and Assigning Groups

- **Task:** Create two groups: "Developers" and "Support," and assign users to these groups.
- **Instructions:**
    1. Open **Computer Management** by typing "Computer Management" in the Windows search bar.



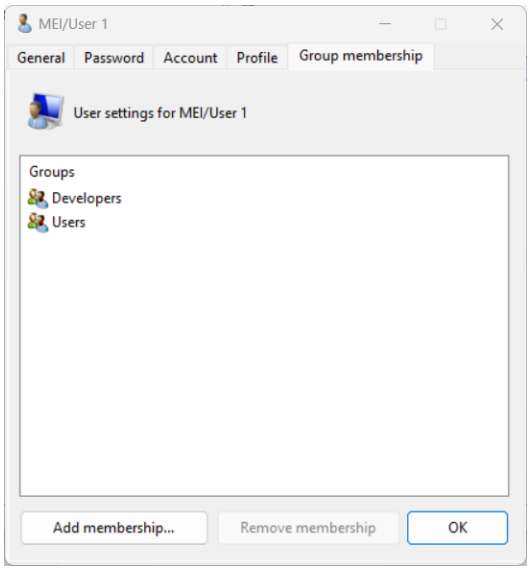
2. Navigate to **Local Users and Groups → Groups**.



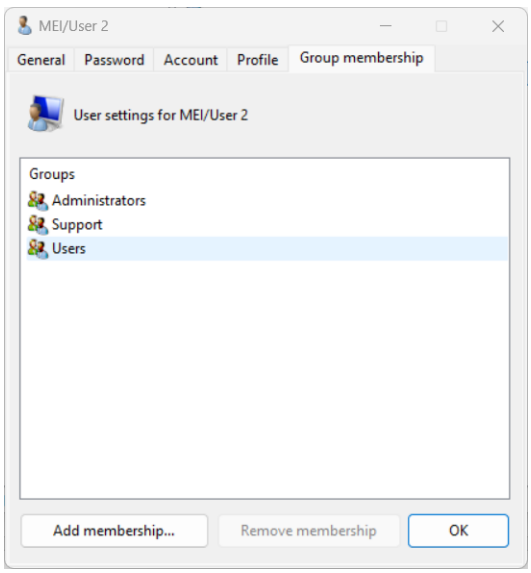
3. Right-click inside the Groups panel and select **New Group**.
4. Create a group named **Developers** and another group named **Support**.
5. To add users to each group, double-click the group (e.g., "Developers"), select **Add**, and choose the user accounts you created in Task 1.

- **Verification:** Confirm that each user has been added to the correct group by checking each group's membership list.

User 1

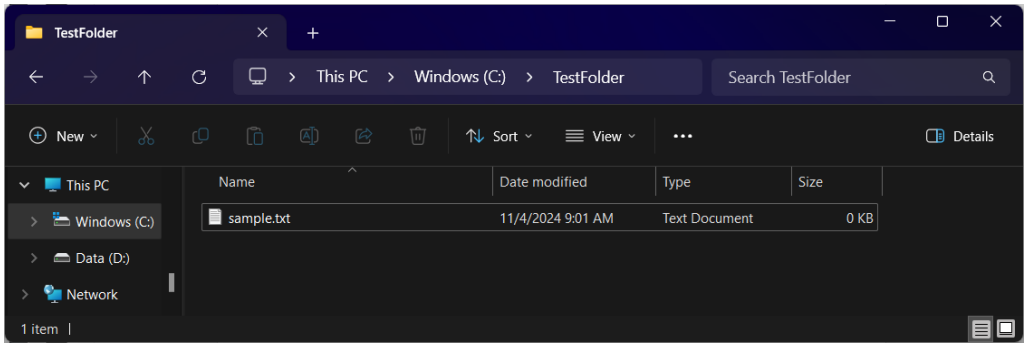


User 2

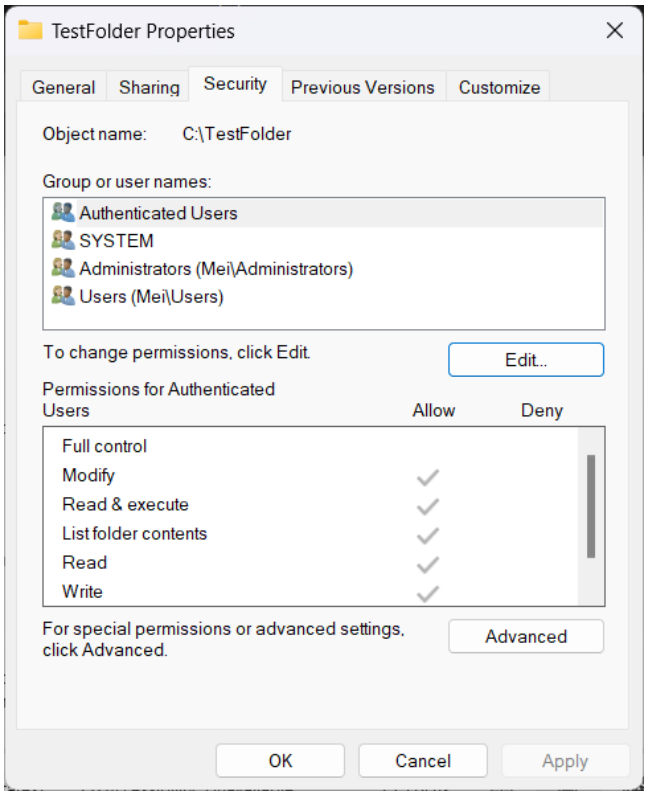


3. Setting and Testing Permissions

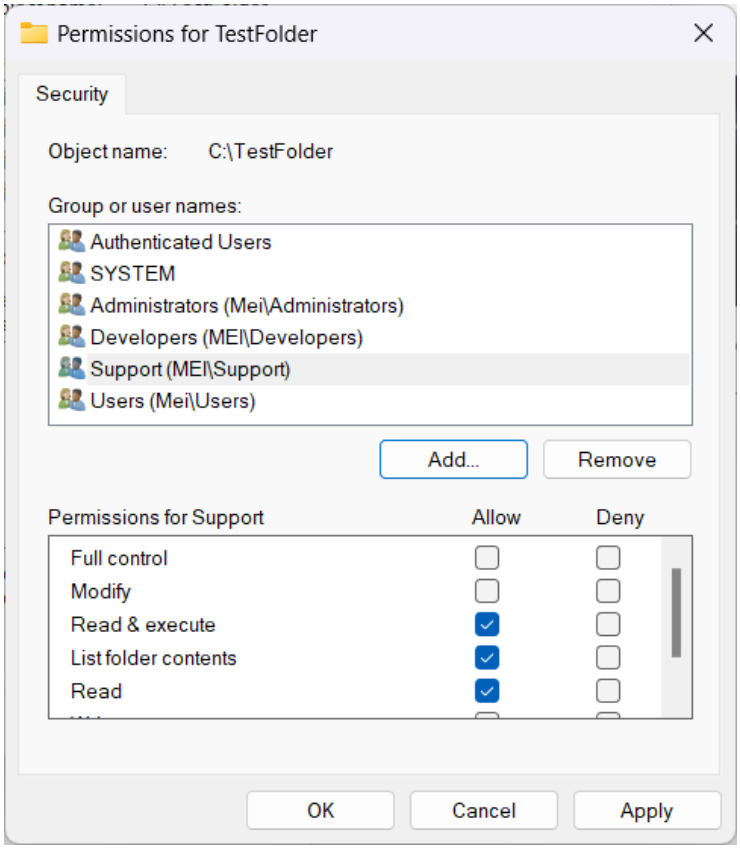
- **Task:** Set permissions for each group on a specific folder to control access.
- **Instructions:**
    1. Create a test folder, such as C:\TestFolder, and place a sample file inside (e.g., sample.txt).



    2. Right-click the folder, select **Properties** → **Security** → **Edit**.

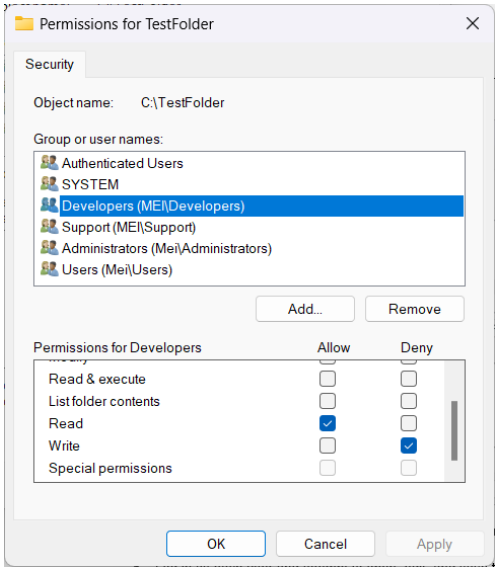


3. Add the "Developers" and "Support" groups to the list of users and groups in the **Security** tab.

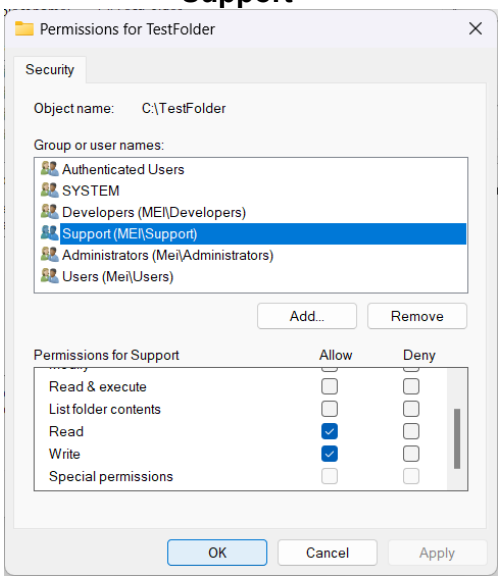


4. Set **Read-only** permissions for the "Developers" group and **Read and Write** permissions for the "Support" group.

Developers

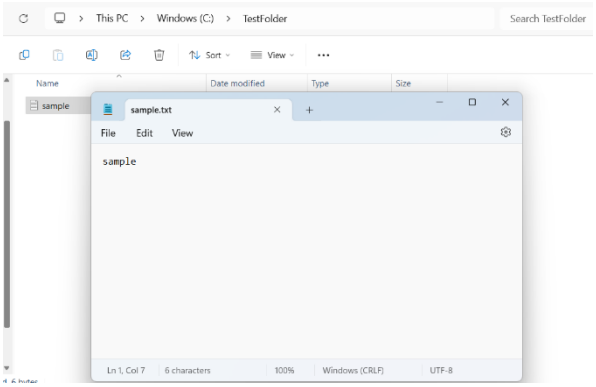


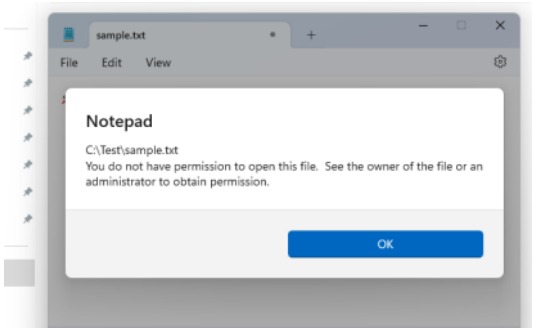
Support



5. Log in as each user and attempt to open, edit, and save the sample.txt file to test the permissions.

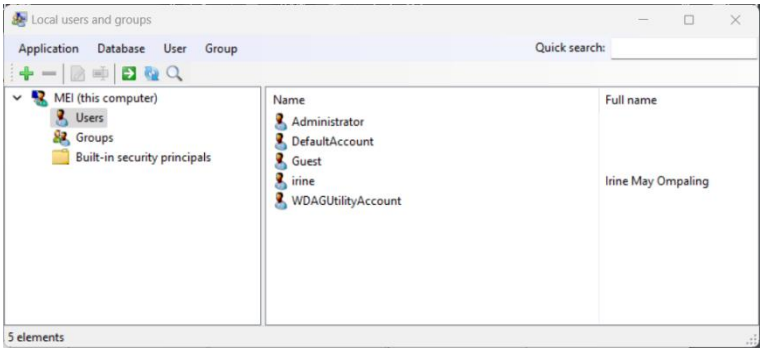
- **Verification:** Ensure that only users in the "Support" group can modify the file, while users in the "Developers" group can only read it.

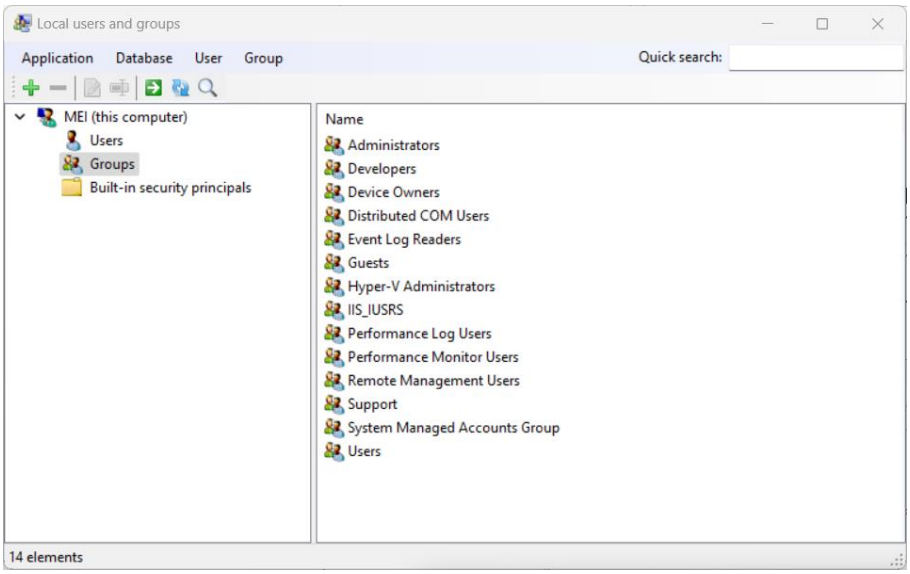




4. Removing Users and Groups

- **Task:** Remove one user account and one group from the system.
- **Instructions:**
  1. In **Computer Management**, go to **Local Users and Groups** → **Groups**.
  2. Right-click the "Developers" group and select **Delete** to remove the group.
  3. Next, go to **Local Users and Groups** → **Users**, right-click on the standard user account you created earlier, and select **Delete**.
- **Verification:** Check that the deleted user and group are no longer available in the system's user and group listings.





Completion Checklist

1. Two user accounts were created: one with standard permissions and one with administrator permissions.
2. Two groups were created: "Developers" and "Support," with users assigned to each.
3. Permissions were set for each group on a test folder, and access was verified.
4. One user and one group were successfully removed from the system.

Submission Requirements

- Screenshots of each completed task showing users, groups, and permission settings.
- Short written answers to the following questions:
    1. **Why is it beneficial to assign permissions through groups instead of directly to individual users?**

       - Assigning permissions through groups instead of individual users streamlines administration by allowing mass permission changes and reducing management overhead since one change to a group affects all members.
    2. **What could go wrong if a standard user account is given administrator privileges?**

       - A standard user with administrator privileges could accidentally or intentionally install malware, modify critical system settings, or delete important files that could compromise the entire system's security and stability.

3. **How do access permissions contribute to system security?**

   - Access permissions enhance system security by controlling who can read, write, or execute files and resources, ensuring sensitive data is only accessible to authorized users while maintaining the principle of least privilege.