Control Panel Home

Manage your credentials

Create a password reset disk

Manage your file encryption
certificates

Configure advanced user
profile properties

Change my environment
variables

Make changes to your user account

Make changes to my account in PC settings

🛡 Change your account name

🛡 Change your account type

🛡 Manage another account

🛡 Change User Account Control settings

👤 user
Local Account
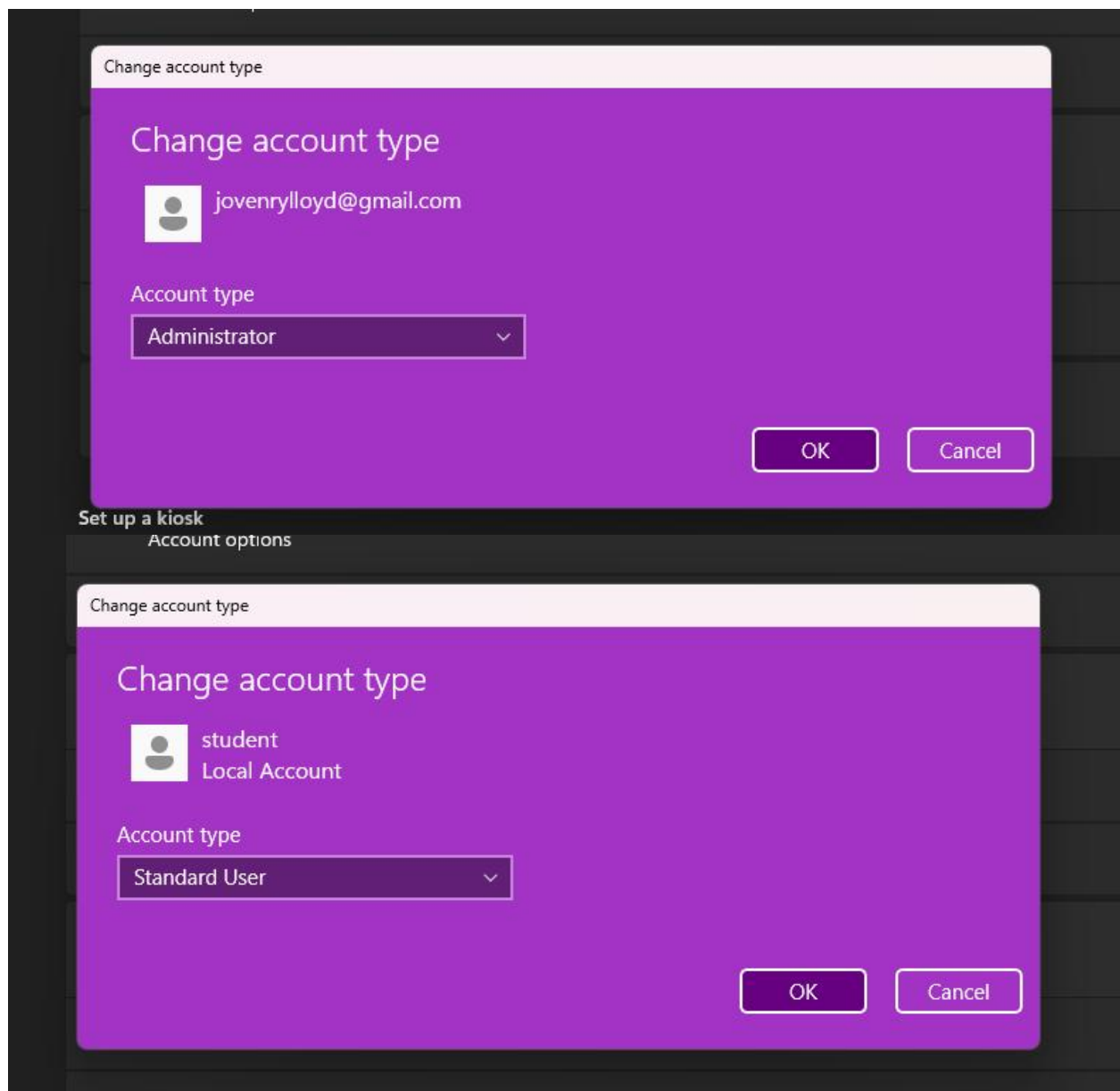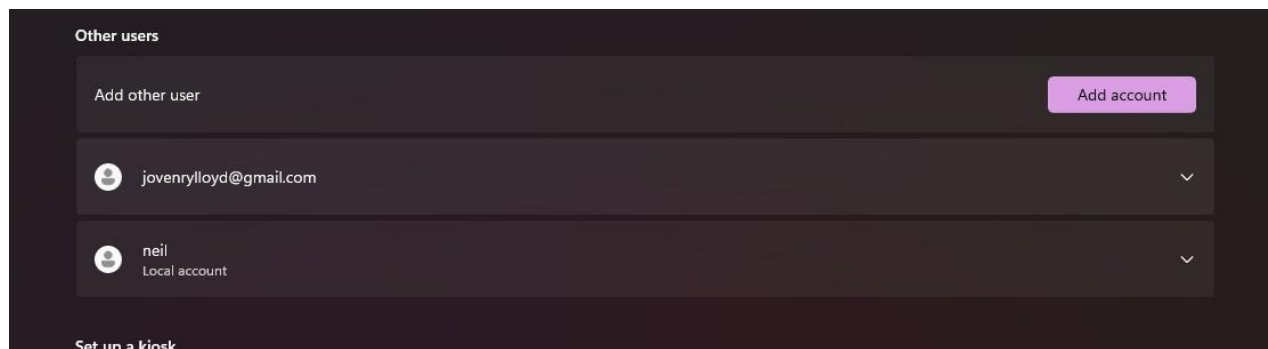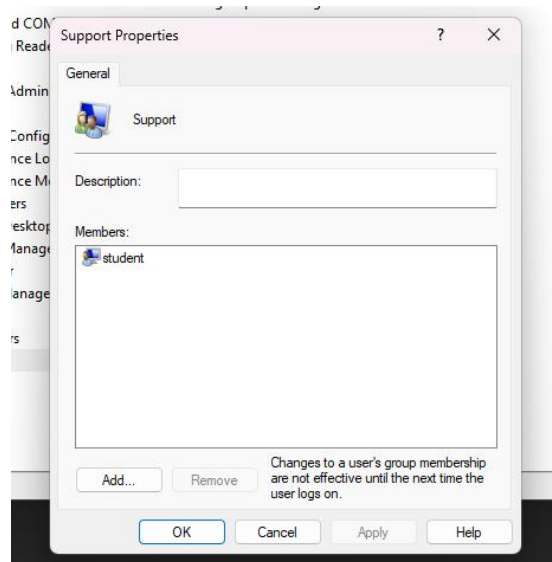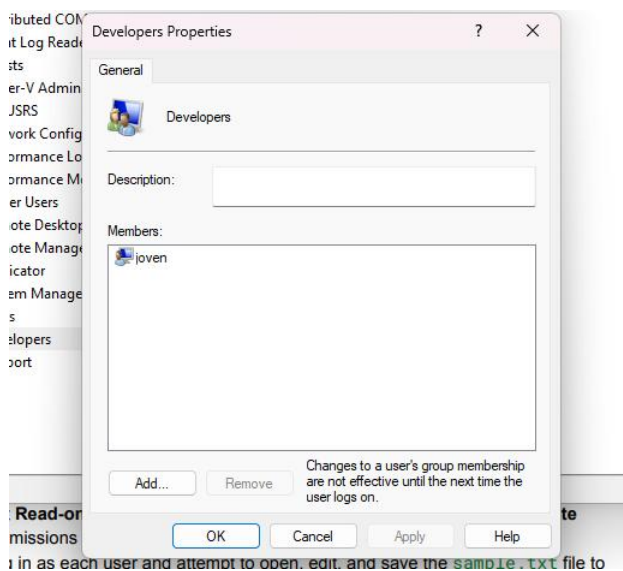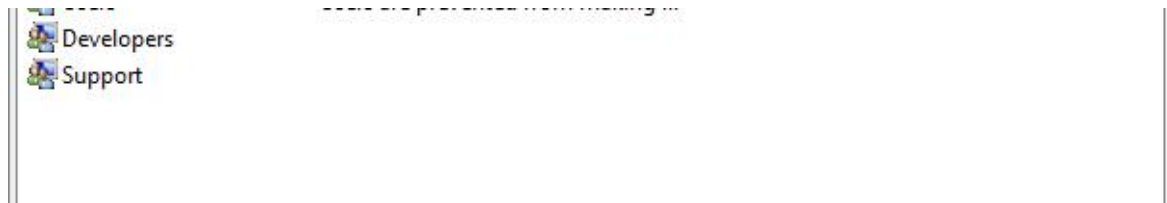Administrator

Choose the user you would like to change

👤 user
Local Account
Administrator

👤 neil
Local Account
Password protected

Add a new user in PC settings

Other users

Add other user   [Add account]

👤 jovenrylloyd@gmail.com   ⌄

👤 neil
     Local account   ⌄

Set up a kiosk

Change account type

Change account type

👤 jovenrylloyd@gmail.com

Account type

[Administrator   ⌄]

[OK]   [Cancel]

Set up a kiosk
Account options

Change account type

Change account type

👤 student
     Local Account

Account type

[Standard User   ⌄]

[OK]   [Cancel]

groups.
- **Instructions:**

Computer Management

File   Action   View   Help

Computer Management (Local
System Tools
  Task Scheduler
  Event Viewer
  Shared Folders
  Local Users and Groups
  Performance
  Device Manager
Storage
  Disk Management
Services and Applications

Name
System Tools
Storage
Services and Applications

Actions
Computer Management (L...
  More Actions

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

Developers
Support

Developers Properties ? X

General

Developers

Description:

Members:
joven

Changes to a user's group membership are not effective until the next time the user logs on.

Add...   Remove   OK   Cancel   Apply   Help

Support Properties ? X

General

Support

Description:

Members:
student

Changes to a user's group membership are not effective until the next time the user logs on.

Add...   Remove   OK   Cancel   Apply   Help

📁 Program Files (x86)	9/23/2024 1:10 PM	File folder	
📁 Test Folder	11/4/2024 8:47 AM	File folder	
📁 TURBOC3	10/16/2024 8:30 AM	File folder	

| 📄 sample.txt | 11/4/2024 8:47 AM | Text Document | 0 KB |

group of user names:

👤 Jovenry Villa-or (jovenrylloyd@gmail.com)
👤 student (DESKTOP-9HG3D29\student)

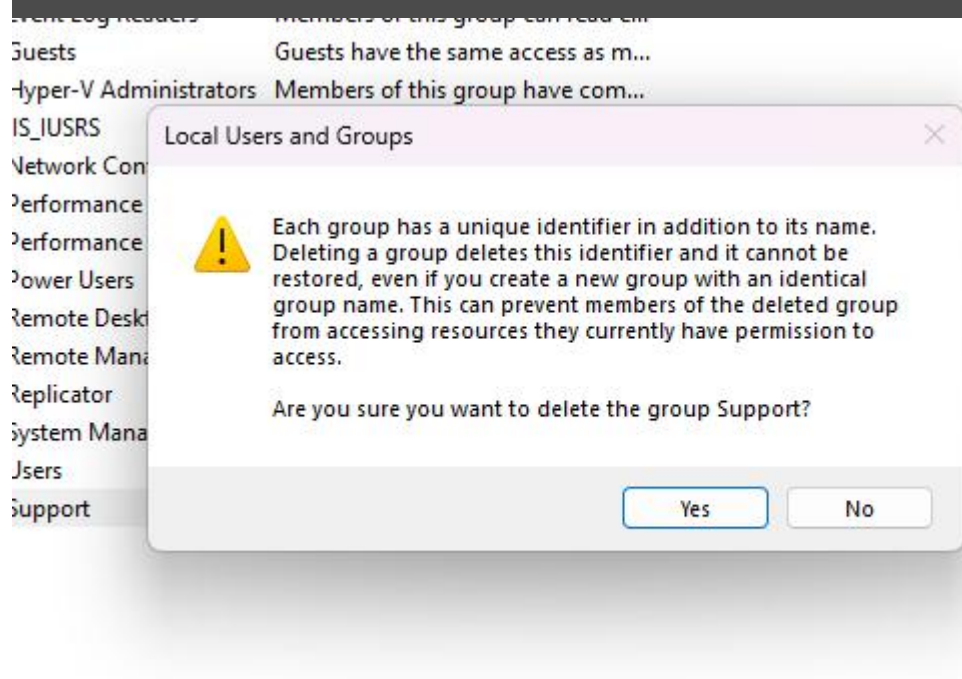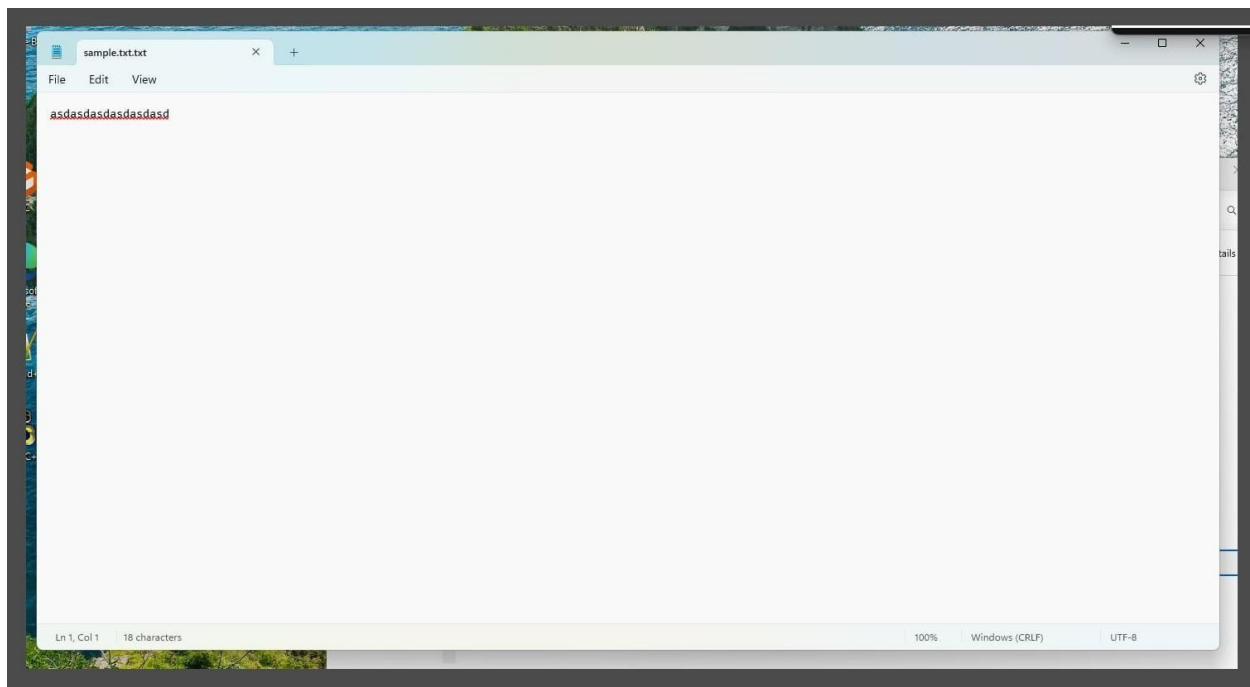| List folder contents | ✓ |
| Read | ✓ |

Read & execute	✓
List folder contents	✓
Read	✓
Write	✓

Notepad

C:\Test Folder\sample.txt.txt
You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.

OK

sample.txt.txt

File Edit View

asdasdasdasdasdasd

Ln 1, Col 1   18 characters   100%   Windows (CRLF)   UTF-8

Guests   Guests have the same access as m...
Hyper-V Administrators   Members of this group have com...
IS_IUSRS
Network Con
Performance
Performance
Power Users
Remote Deskt
Remote Mana
Replicator
System Mana
Users
Support

Local Users and Groups

⚠ Each group has a unique identifier in addition to its name.
Deleting a group deletes this identifier and it cannot be
restored, even if you create a new group with an identical
group name. This can prevent members of the deleted group
from accessing resources they currently have permission to
access.

Are you sure you want to delete the group Support?

[Yes]   [No]

Submission Requirements:

Why is it beneficial to assign permissions through groups instead of directly to individual users?

Assigning permissions through groups makes managing user access easier. By putting users into groups based on their roles or tasks, administrators can quickly set up the right permissions. When new users join or someone's role changes, admins don't need to adjust permissions for each person individually. Instead, they can just add or move the user to the correct group. This approach saves time, reduces mistakes, and keeps access more organized and secure.

What could go wrong if a standard user account is given administrator privileges?

Giving administrator privileges to a regular user can create serious security risks. With higher access, a user might accidentally or intentionally change important settings, install harmful software, or see sensitive information that should be private. This could lead to big problems, like data leaks, system issues, or weakened security. Such actions could disrupt work and expose the organization to risks, so it's important to be very careful about who gets administrator access.

How do access permissions contribute to system security?

Access permissions are important for keeping systems secure. By following the "least privilege" rule, users only get the access they need to do their specific jobs—nothing more. This helps prevent mistakes, like accidental deletions, and reduces the chance of harmful actions that could damage sensitive data or system stability. Managing access permissions well protects valuable information and lowers the risk of unauthorized access or data leaks, making the organization's operations safer overall.