Google Cyber Security

Users and Permissions on Windows Machines

Full Name: Klajdi Cami

- **Policy for Creating Strong Passwords**

First, we define the policy for creating strong passwords. We do this by following these steps:

Press on your Windows machine:
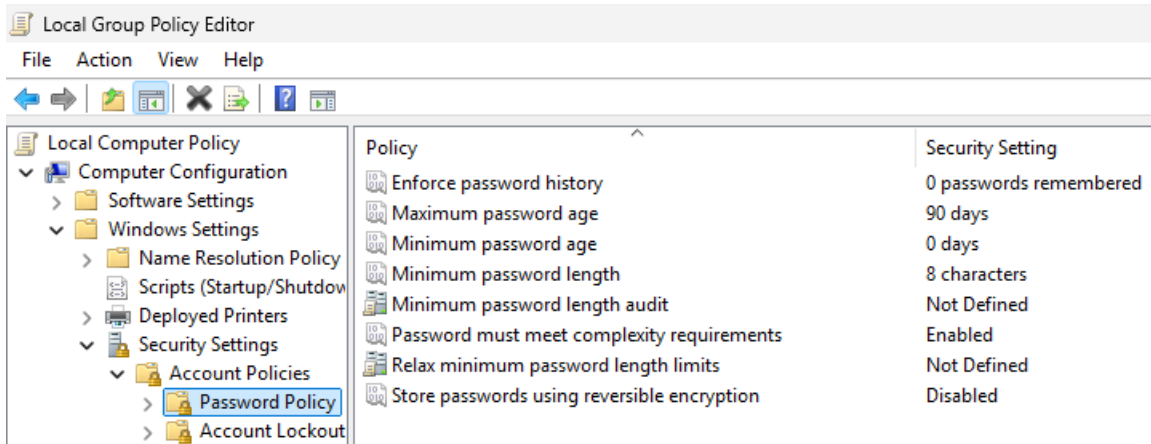
Win + R

In the window that opens, type:

gpedit.msc

Then follow the path:

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

In the Password Policy, make the following changes:

- Set the password to expire in 90 days
- Set the minimum password length to 8 characters
- Enable the option that enforces password complexity rules

- **Creating Users on Windows**

To create users on a Windows machine, follow these steps:

Start > Settings > Accounts > Other Users > Add Account

In the window that opens, click "**I don't have this person's sign in information**" and then "**Add a user without a Microsoft account**"

Activity: Create five users (**user1, user2, user3, user4 & admin1**) by assigning appropriate passwords. Set users **user1, user2, user3, and user4** as standard users, and **admin1** as an administrator.

Answer:
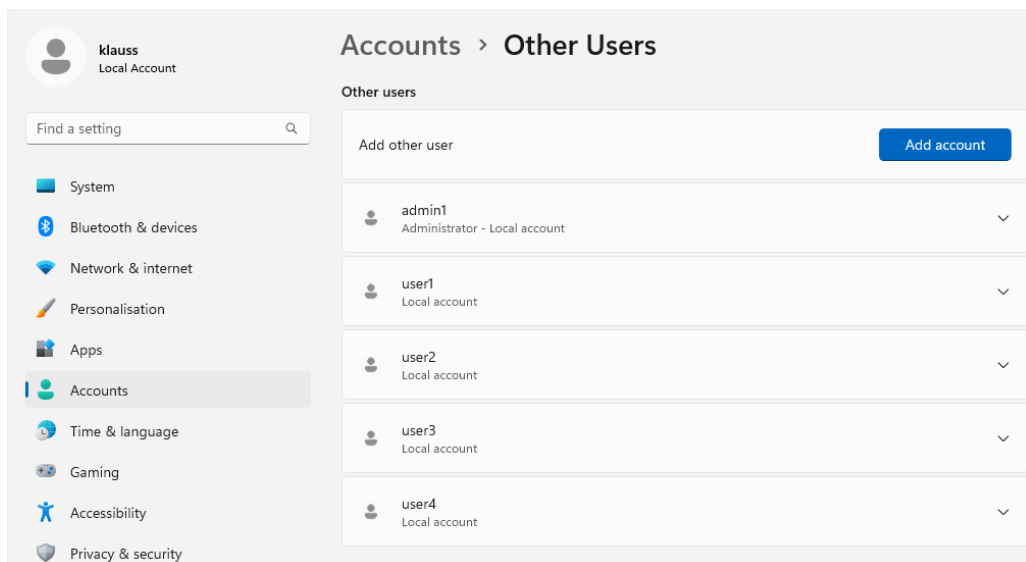
- **Creating a Group**

To create a new group, follow these steps:

Open a **File Explorer**, right-click on **This PC** and choose:

Show more options > Manage

Then select:

Computer Management > Local Users and Groups > Groups
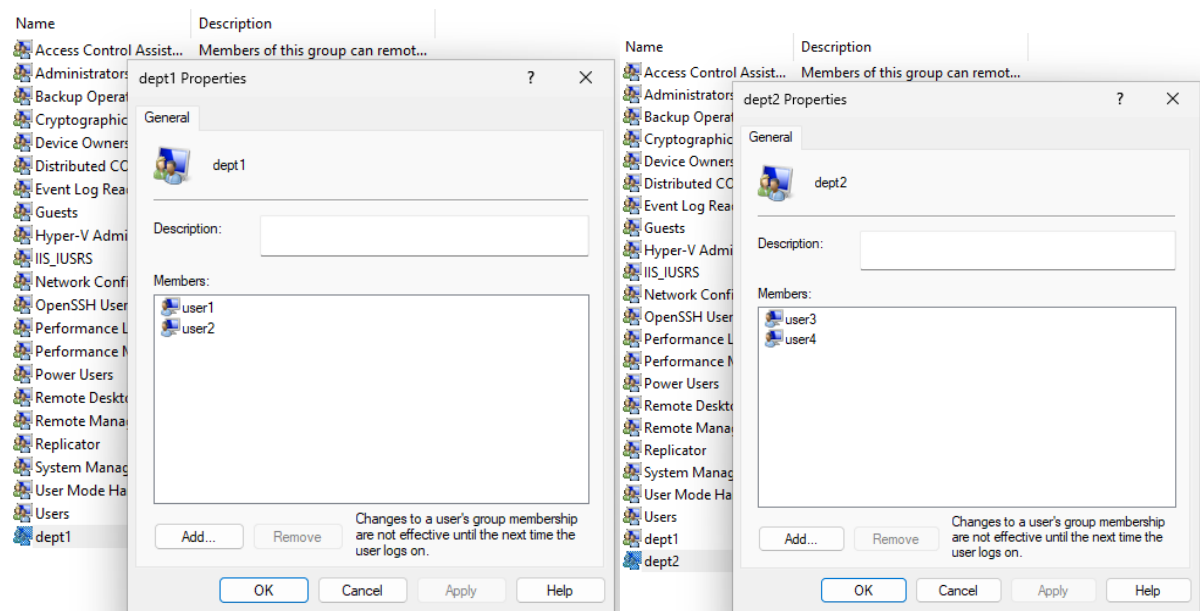
Right-click and select:

New Group > Add

Add the users and finally create the group.

Activity: Create two groups (**dept1** and **dept2**) and add **user1** and **user2** to group **dept1**, and **user3** and **user4** to group **dept2**.

Answer:

Using the above process, we create each group and add the corresponding users to it.

- **Creating and Assigning File Access Rights to System Users in Windows**

Log in with the user who installed Windows and create two folders in **Users (C:\Users)** named **Dept1** and **Dept2**. Then, place one .doc file inside each.

To set permissions on a system resource, right-click on the resource and select:

Properties > Security > Advanced > Change Permissions

Then choose:

Disable Inheritance

and

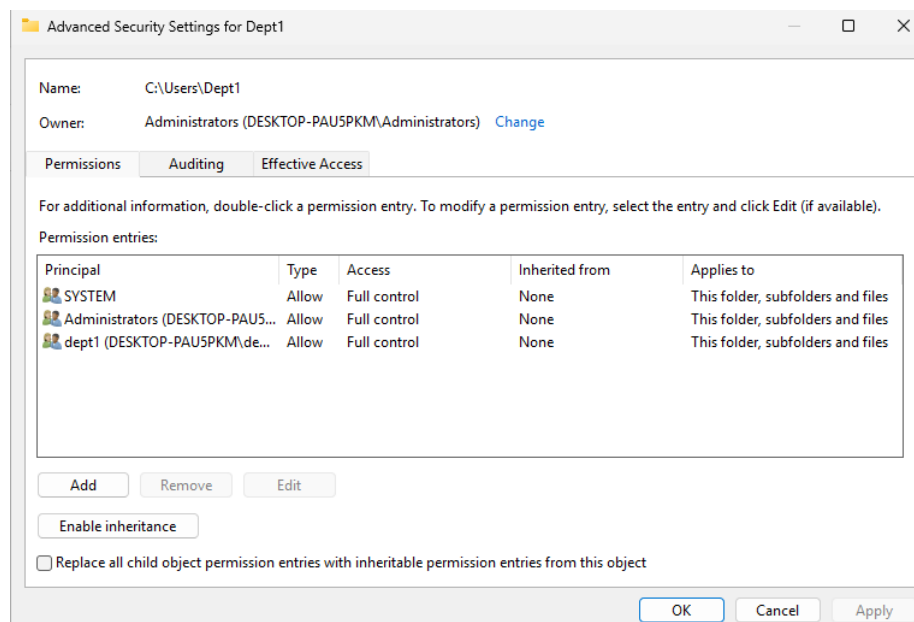**Convert inherited permissions into explicit permissions on this object**

Activity: For the **Dept1** folder, give full access rights to the users of **Dept1** and the system owner. For the **Dept2** folder, give full access rights to the users of **Dept2** and the system owner.

Answer:

We follow the above process and assign the requested permissions to folders **Dept1** and **Dept2**.

and
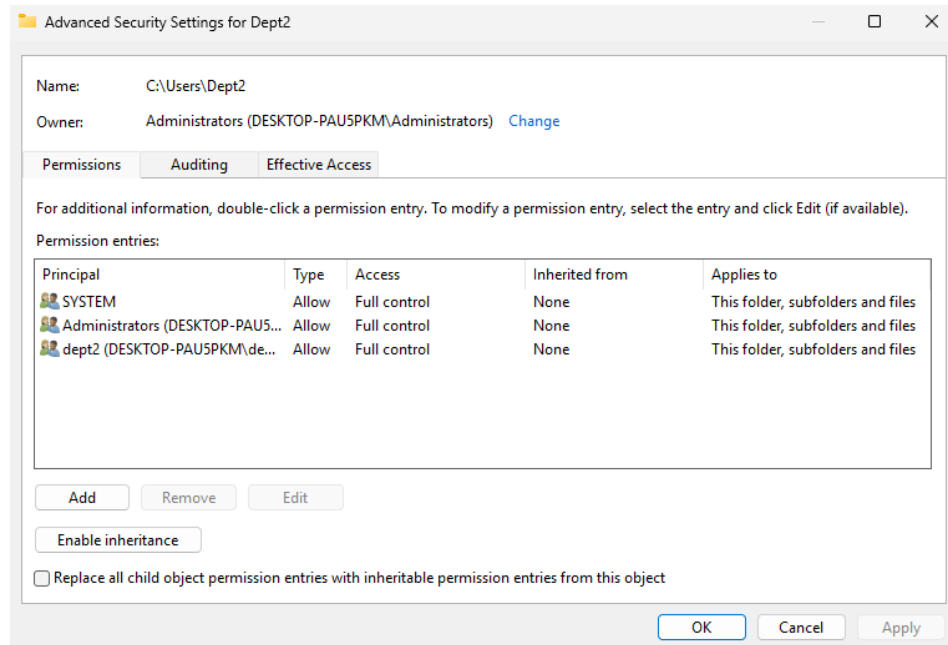
Activity:

Change the permissions of the **Dept1** and **Dept2** folders so that users in **Dept1** have full access to **Dept2**, while users in **Dept2** have read, execute, and list folder contents permissions on **Dept1**. Then, try editing the .doc file in **Dept1** as **user3** and try creating a new folder inside **Dept1**. What do you observe?

Answer:

We similarly update the permissions of the two folders.

Advanced Security Settings for Dept1 — □ ×

Name: C:\Users\Dept1

Owner: Administrators (DESKTOP-PAU5PKM\Administrators)   Change

Permissions   Auditing   Effective Access

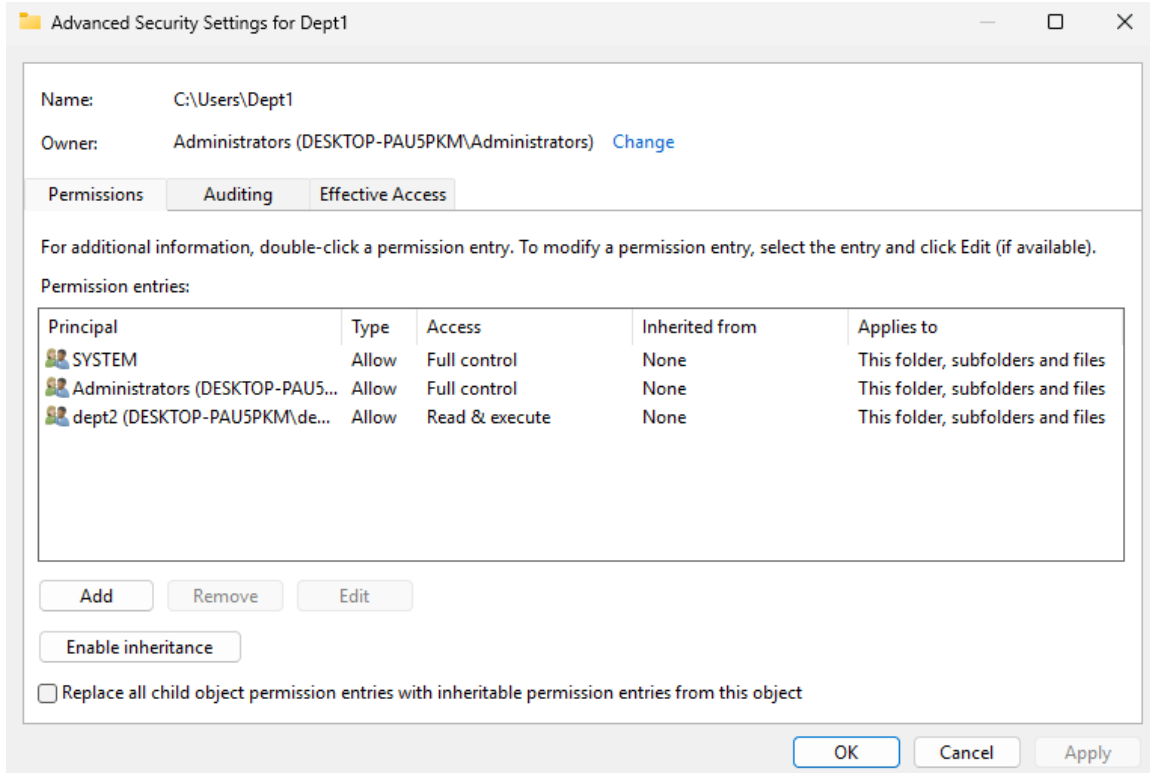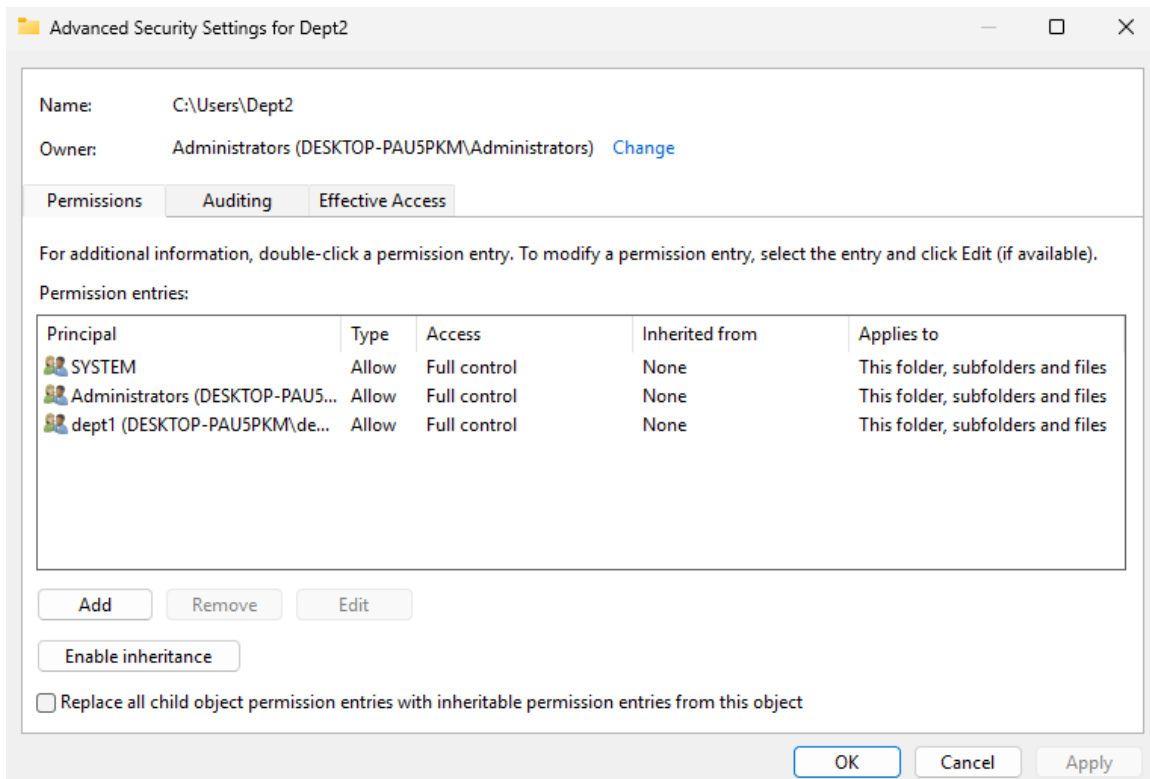For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Principal	Type	Access	Inherited from	Applies to
SYSTEM	Allow	Full control	None	This folder, subfolders and files
Administrators (DESKTOP-PAU5...	Allow	Full control	None	This folder, subfolders and files
dept2 (DESKTOP-PAU5PKM\de...	Allow	Read & execute	None	This folder, subfolders and files

Add   Remove   Edit

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK   Cancel   Apply

And

Advanced Security Settings for Dept2 — □ ×

Name: C:\Users\Dept2

Owner: Administrators (DESKTOP-PAU5PKM\Administrators)   Change

Permissions   Auditing   Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Principal	Type	Access	Inherited from	Applies to
SYSTEM	Allow	Full control	None	This folder, subfolders and files
Administrators (DESKTOP-PAU5...	Allow	Full control	None	This folder, subfolders and files
dept1 (DESKTOP-PAU5PKM\de...	Allow	Full control	None	This folder, subfolders and files

Add   Remove   Edit

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK   Cancel   Apply

Since **user3** belongs to group **Dept2**, they are not allowed to edit the file, as this group only has read, execute, and list permissions for the specific folder.

Additionally, if we try to create a new folder inside **Dept1**, a message appears informing us that administrator (admin) approval is required to complete the action. In other words, it is not permitted.

- **Removing Access Rights to Applications from System Users on Windows**

To remove access rights to applications from system users on Windows, follow the steps below:

1. Open **Edit Group Policy** from the Start menu
2. Navigate to **Administrative Templates > System > Don't run specified Windows applications**
3. Select **Enabled > Show**
4. Suppose we want to disable Notepad. Type the executable name (**notepad.exe**) of the application and click OK.
5. Click **Apply** and **OK**
6. Confirm that the setting is now enabled
7. If we try to open Notepad, we will see that access is blocked.