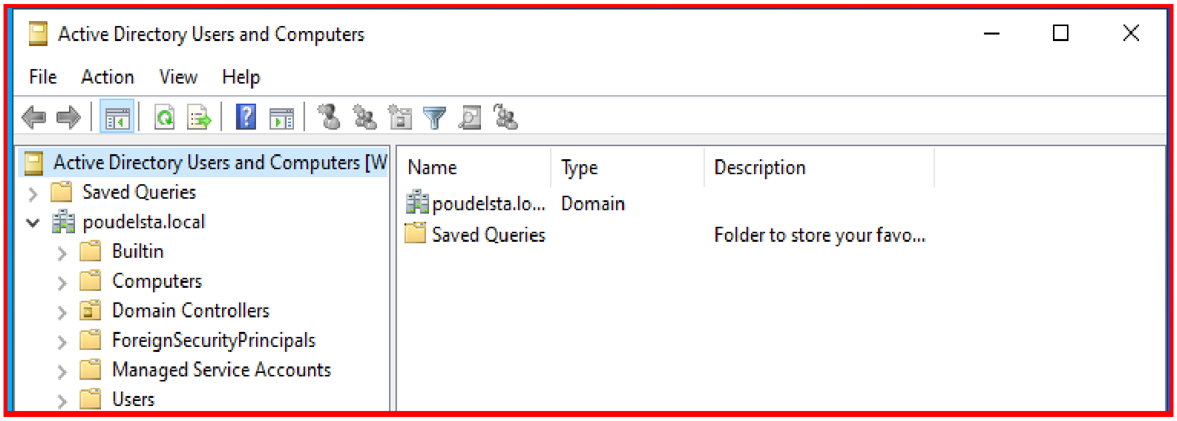
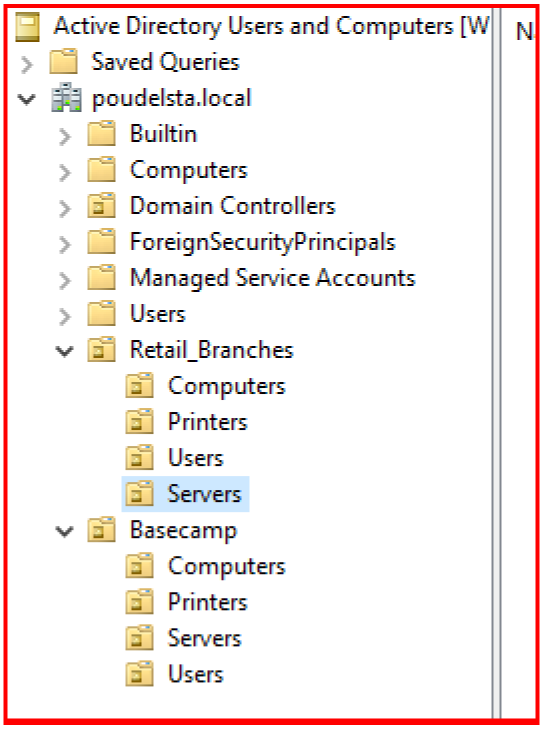
Basic Active Directory Setup and Group Policy Management

1. **Open Active Directory Users and Computers (ADUC):**
   - We will click on **Active Directory Users and Computers** inside the Windows Administrative Tools folder. This is a primary tool for IT professionals.
   - Here, we can see our domain, **poudelsta.local**, and all the built-in containers.

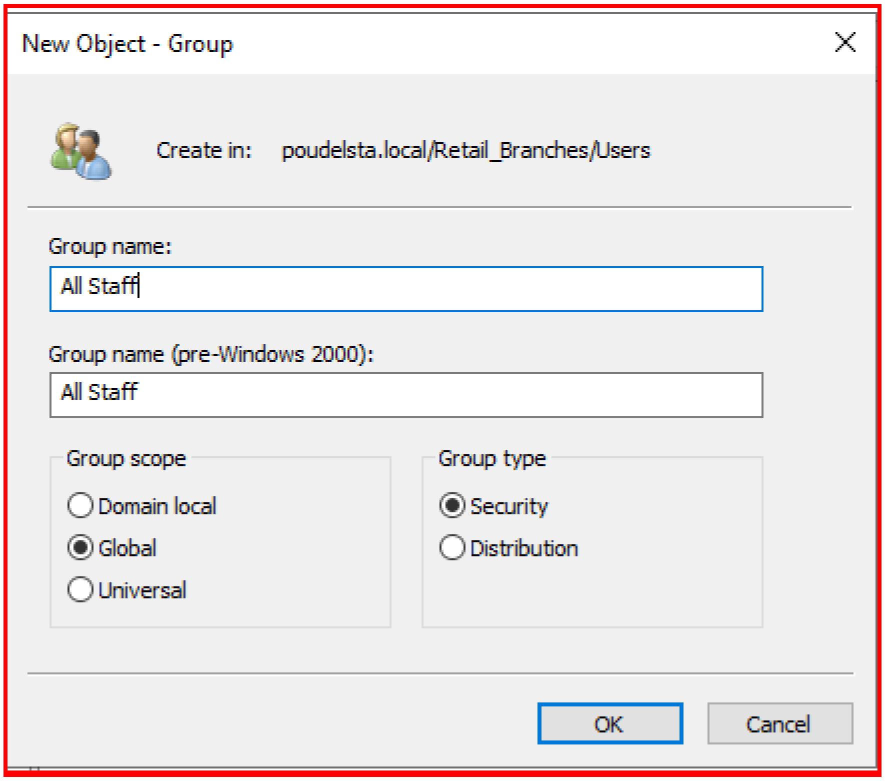


Name	Type	Description
poudelsta.lo...	Domain	
Saved Queries		Folder to store your favo...

2. **Create Organizational Units (OUs):**
   - We will create our first Organizational Unit (OU). **Right-click** on our domain (**poudelsta.local**), select **New > Organizational Unit**.
   - We will name the first one **Retail Branches** and click **OK**.
   - We will create a second top-level OU named **Basecamp**.
   - **Note:** For clear organization, within both the **Retail Branches** and **Basecamp** OUs, we will create sub-OUs named **Computers**, **Printers**, **Servers**, and **Users**.



3. **Create a New User Account:**
   - We will navigate to the **Users** OU under **Retail Branches**. **Right-click** on the **Users** OU, then select **New > User**.
   - We will input the user's information (First Name, Last Name, User logon name) and click **Next**.



New Object - Group

Create in: poudelsta.local/Retail_Branches/Users

Group name:
All Staff

Group name (pre-Windows 2000):
All Staff

Group scope
○ Domain local
● Global
○ Universal

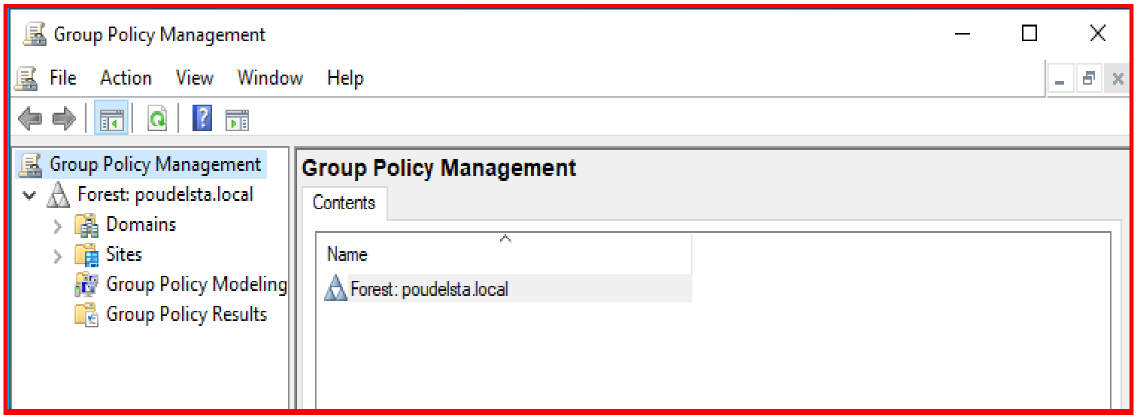
Group type
● Security
○ Distribution

- We will create a password for the user and check the box that says **"User must change password at next logon"**. We will leave other options unchecked. Click **Next**, and then click **Finish**. (While onboarding is often scripted in production, we add users manually for this homelab.)
- **Simulating Password Reset:** If a user forgets their password, we would right-click the user account, select **All Tasks > Reset Password**. We will create a new temporary password and check **"User must change password at next logon."**

4. **Create Security and Distribution Groups:**
   - We will now create a group under the **Users** OU of **Retail Branches**.
   - **Right-click** the **Users** OU, then select **New > Group**.
   - We will name the group **All Staff**.
   - **Reviewing Group Options:**
     - **Group Scope** (Determines where the group can be used):
       - **Domain local:** Used to assign permissions to local domain resources.

        - **Global:** Can be used across any domain in the same forest. (Typically used for user organization).
        - **Universal:** Can be used across multiple domains in the same forest or trusting forests.
    - **Group Type** (Determines the group's purpose):
        - **Security:** Used to assign permissions (what users can access) and user rights (what users can do).
        - **Distribution:** Used only to create email distribution lists.
- For the **All Staff** group, we will set the **Group Scope** to **Global** and the **Group Type** to **Distribution**.
- We will repeat this process to create a **Branch Manager, All Frontline Staff, IT Admin, Sr IT Admin, Finance Staff, HR Staff, and HR Intern** group.

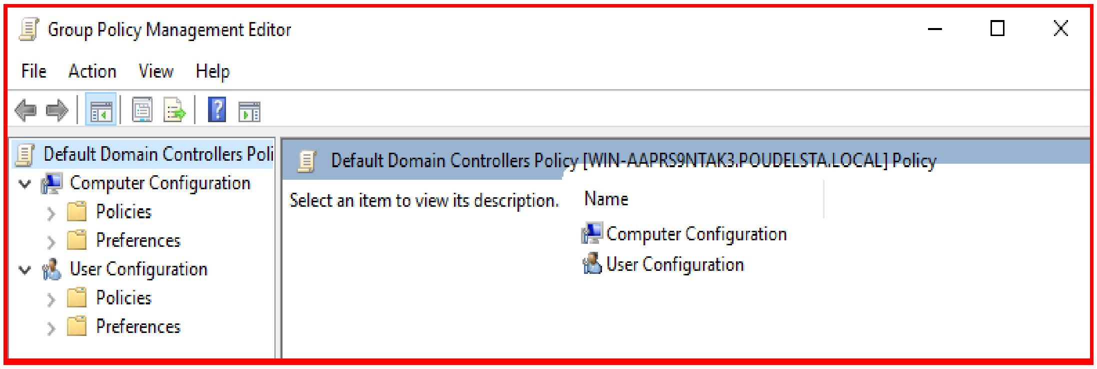
5. **Open Group Policy Management Console (GPMC):**
    - We will click on the Start menu, navigate to the **Windows Administrative Tools** folder, and open **Group Policy Management**.



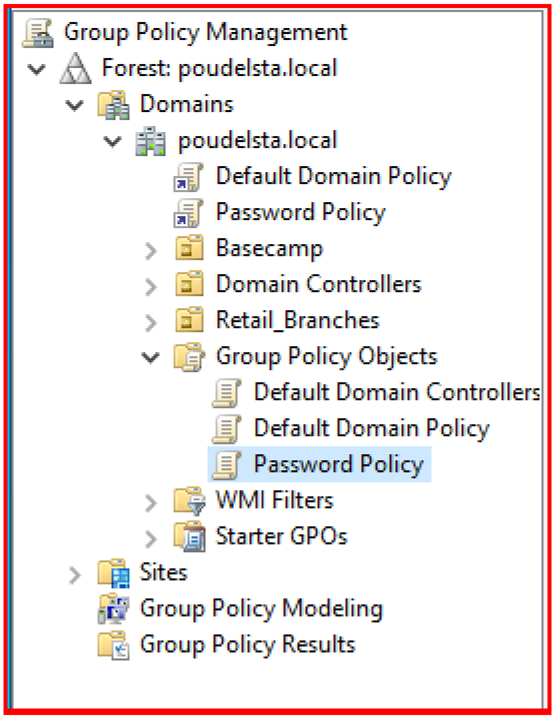
    - On the left, we will navigate through **Forest > Domains > poudelsta.local**. We can see the OUs we created (**Basecamp** and **Retail Branches**).

6. **Understand Group Policy Configuration:**
    - We need to understand the two main configuration sections in the Group Policy Editor:

        - **Computer Configuration:** Settings that apply to the **computer itself**, regardless of who logs on (e.g., security settings, startup scripts).
        - **User Configuration:** Settings that apply to the **user**, regardless of which computer they log into (e.g., desktop wallpaper, drive mappings).
    - **Policies vs. Preferences:**
        - **Policies:** Cannot be changed by the user (e.g., password policies, security restrictions).
        - **Preferences:** Can often be changed by the user and are used for configuring non-mandatory settings (e.g., mapped network drives, shortcuts).

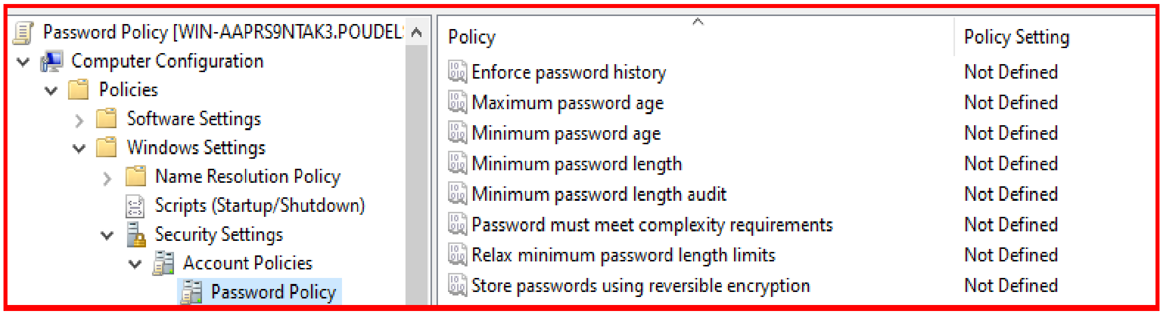

Group Policy Management Editor
File
Action
View
Help
Default Domain Controllers Poli
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Controllers Policy [WIN-AAPRS9NTAK3.POUDELSTA.LOCAL] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration

7. **Create the Password Policy GPO:**
    - **Right-click** on our domain (**poudelsta.local**) and click **"Create a GPO in this domain, and Link it here..."**.
    - We will name the new GPO **Password Policy** and click **OK**.



- Group Policy Management
  - Forest: poudelsta.local
    - Domains
      - poudelsta.local
        - Default Domain Policy
        - Password Policy
        - Basecamp
        - Domain Controllers
        - Retail_Branches
        - Group Policy Objects
          - Default Domain Controllers
          - Default Domain Policy
          - Password Policy
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

- **Right-click** on the new **Password Policy** GPO and click **Edit**.
- Password Policy is a Computer Configuration. Since this is a domain-level security setting, we navigate through **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**.

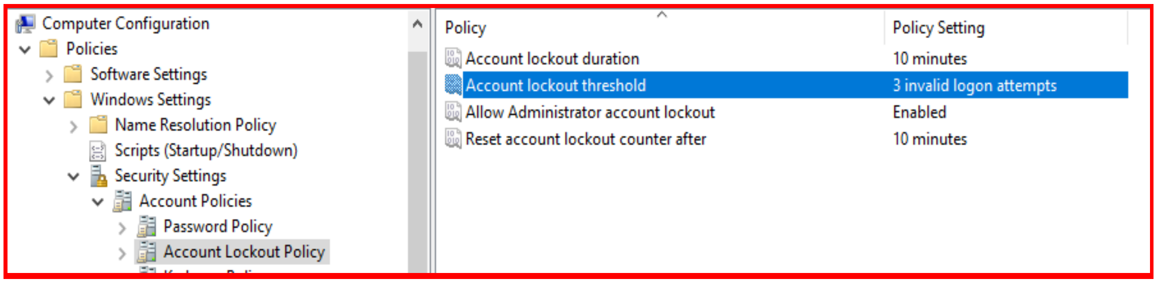


- Password Policy [WIN-AAPRS9NTAK3.POUDEL
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
            - Password Policy

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Minimum password length audit	Not Defined
Password must meet complexity requirements	Not Defined
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Not Defined

- We will double-click and change **Minimum password length**, **Complexity requirements**, and **Maximum password age**. (Changing the maximum age will automatically prompt us to set a minimum password age.)

8. **Create the Account Lockout Policy GPO:**
    - We will create a second GPO linked to the domain named **Account Lockout Policy**.
    - **Right-click** on Account Lockout Policy and click **Edit**.
    - We navigate through **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy**.

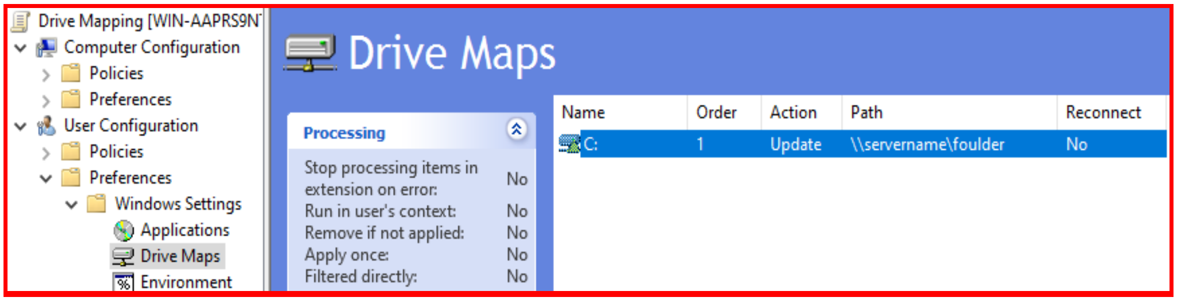


Computer Configuration
- Policies
  - Software Settings
  - Windows Settings
    - Name Resolution Policy
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
        - Password Policy
        - Account Lockout Policy

Policy	Policy Setting
Account lockout duration	10 minutes
Account lockout threshold	3 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

   - We will double-click **Account lockout threshold** and define the policy setting to **3 invalid logon attempts**. Click **Apply**. This action will automatically set the Account lockout duration (we will leave this default). Click **OK**.

9. **Create the Drive Mapping GPO (User Preference):**
    - We will right-click on our domain poudelsta.local and click the first option "Create a GPO in this domain, and Link it here". We will create a GPO linked to the domain named **Desktop Wallpaper**.
    - **Right-click on** Desktop Wallpaper and click **Edit**.
    - Drive mapping is a **User Configuration Preference**. We navigate through **User Configuration > Preferences > Windows Settings > Drive Maps**.
    - **Right-click** on **Drive Maps**, select **New > Mapped Drive**.
    - We will set the **Location** (the network path to the shared folder) and select a **Drive Letter** (e.g., **"C"**). Click **OK**.



Drive Mapping [WIN-AAPRS9N
- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
  - Preferences
    - Windows Settings
      - Applications
      - Drive Maps
      - Environment

Drive Maps

Processing

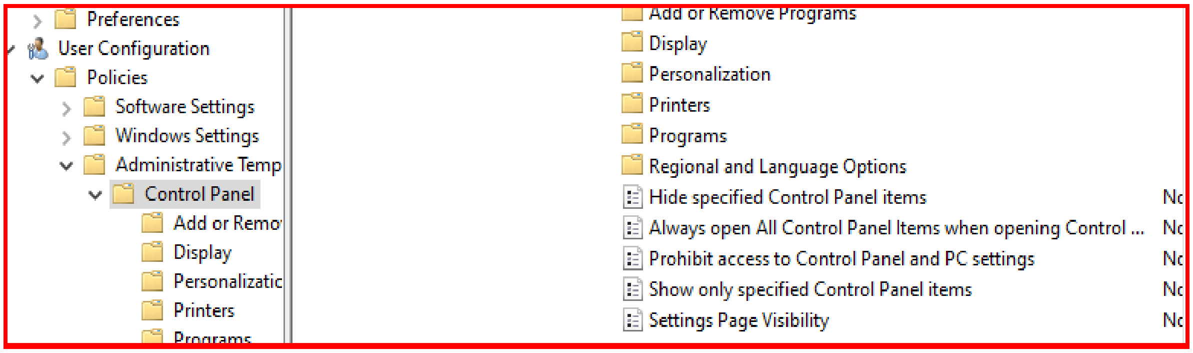
Stop processing items in extension on error:	No
Run in user's context:	No
Remove if not applied:	No
Apply once:	No
Filtered directly:	No

Name	Order	Action	Path	Reconnect
C:	1	Update	\\servername\foulder	No

- ***Note:*** *Drive mapping in Windows assigns a local letter (like C:) to a shared network resource.*

10. **Create the Desktop Wallpaper GPO (User Policy):**
    - We will right-click on our domain poudelsta.local and click the first option “Create a GPO in this domain, and Link it here”. We will create a GPO linked to the domain named **Desktop Wallpaper**.
    - **Right-click on** Desktop Wallpaper and click **Edit**.
    - This is a **User Configuration Policy** since we don't want the user to change it. We navigate through **User Configuration > Policies > Administrative Templates > Desktop > Desktop**.
    - We will double-click on the **"Desktop Wallpaper"** setting, select **Enabled**. Under **Wallpaper Name**, we will add the network path to the wallpaper file. For **Wallpaper Style**, we will select **Fill**. Click **Apply** and then **OK**.

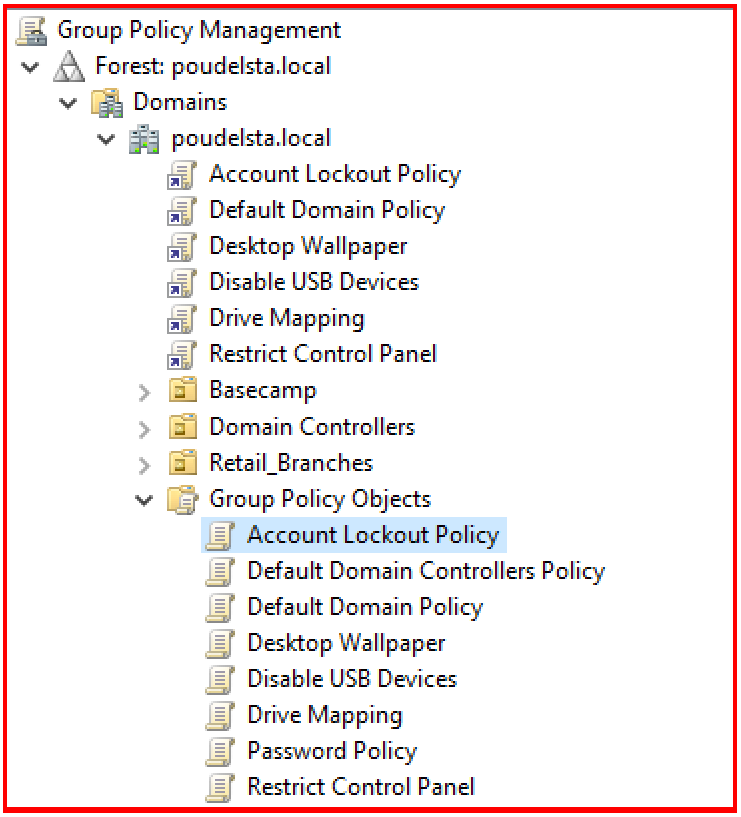
11. **Create the Restrict Control Panel GPO (User Policy):**
    - We will right-click on our domain poudelsta.local and click the first option “Create a GPO in this domain, and Link it here”. We will create a GPO linked to the domain named **Restrict Control Panel**.
    - **Right-click** on Restrict Control Panel and click **Edit**.
    - This is a **User Configuration Policy**. We navigate through **User Configuration > Policies > Administrative Templates > Control Panel**.



    - We will double-click **"Prohibit access to Control Panel and PC Settings"**, select **Enabled**, then **Apply** and **OK**.

12. **Create the Disable USB Devices GPO (Computer Policy):**
   - We will right-click on our domain poudelsta.local and click the first option “Create a GPO in this domain, and Link it here”. We will create a GPO linked to the domain named **Disable USB Devices**.
   - **Right-click** and click **Edit**.
   - This is a **Computer Configuration Policy**. We navigate through **Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access**.
   - We will double-click **"All Removable Storage Classes: Deny all access"**. We will select **Enabled**, then **Apply** and **OK**.

We did set up 6 GPOs, and we can see them like this:



- Group Policy Management
  - Forest: poudelsta.local
    - Domains
      - poudelsta.local
        - Account Lockout Policy
        - Default Domain Policy
        - Desktop Wallpaper
        - Disable USB Devices
        - Drive Mapping
        - Restrict Control Panel
        - Basecamp
        - Domain Controllers
        - Retail_Branches
        - Group Policy Objects
          - Account Lockout Policy
          - Default Domain Controllers Policy
          - Default Domain Policy
          - Desktop Wallpaper
          - Disable USB Devices
          - Drive Mapping
          - Password Policy
          - Restrict Control Panel