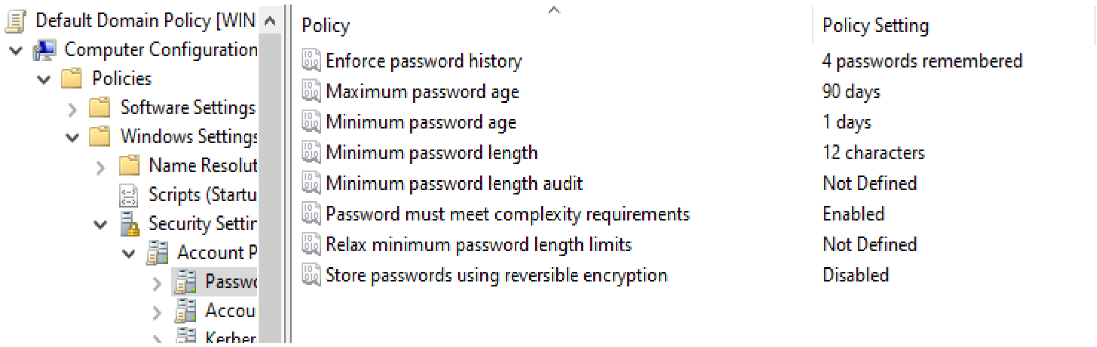
Domain Security: Password, Lockout, and User Rights

Part 1: Default Domain Policy Configuration

We will configure the core security settings that apply to the entire domain by editing the **Default Domain Policy**.

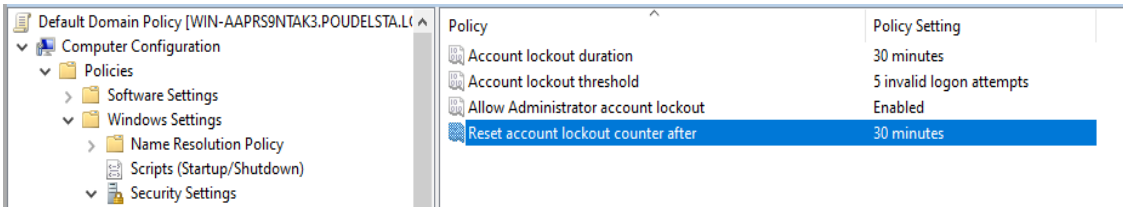
1. **Configure Password Policy:**
    - We will open **Group Policy Management**.
    - Under our domain (**Poudelsta.local**), we will **right-click Default Domain Policy** and click **Edit**.
    - We will navigate to: **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**.
    - We will double-click and configure the following standard settings:
        - **Enforce Password History:** Change this to **4** passwords remembered (a standard setting for remembering previous passwords). Click **Apply** and **OK**.
        - **Maximum password age:** Change this to **90 days** (a common organizational standard).
        - **Minimum password length:** Change this to **12 characters**.
        - We will continue configuring all other relevant policies here as needed (e.g., Complexity requirements, Minimum password age).



Policy	Policy Setting
Enforce password history	4 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

2. **Configure Account Lockout Policy:**

- In the same Group Policy Editor window, navigate to: **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy**.
- We will configure the following:
    - **Account lockout duration:** Double-click, check the box to **Define this policy setting**, and change the duration to **30 minutes**. Click **Apply** and **OK**.
    - **Account lockout threshold:** Change this to **3 invalid logon attempts**. Click **Apply** and **OK**.
    - **Reset account lockout counter after:** Change this to **30 minutes** as well. Click **Apply** and **OK**.



Default Domain Policy [WIN-AAPRS9NTAK3.POUDELSTA.L(
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings

Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	30 minutes

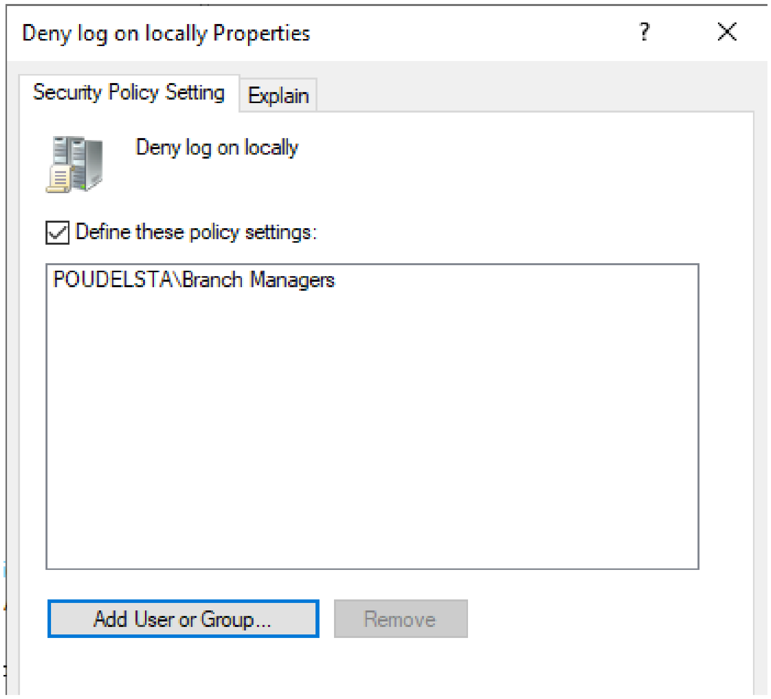
Part 2: User Rights Assignment (Role-Based Access)

This section is for assigning and restricting *what* a user can do (user rights), which is separate from *what* resources they can access (permissions).

1. **Create User Rights GPO:**
    - We will open **Group Policy Management**.
    - **Right-click** on **Group Policy Objects** and click **New**. We will name it **User Rights**.
    - **Right-click** on the new GPO and click **Edit**.
    - We will navigate to: **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.

2. **Deny Log On Locally:**
    - We will look for **Deny log on locally**.

- Double-click on it, check the box for **Define these policy settings**, and click **Add User or Group**.
- We will input the **Branch Manager** group (or any group that should not log on directly to the server console). Click **OK**, then **Apply**.



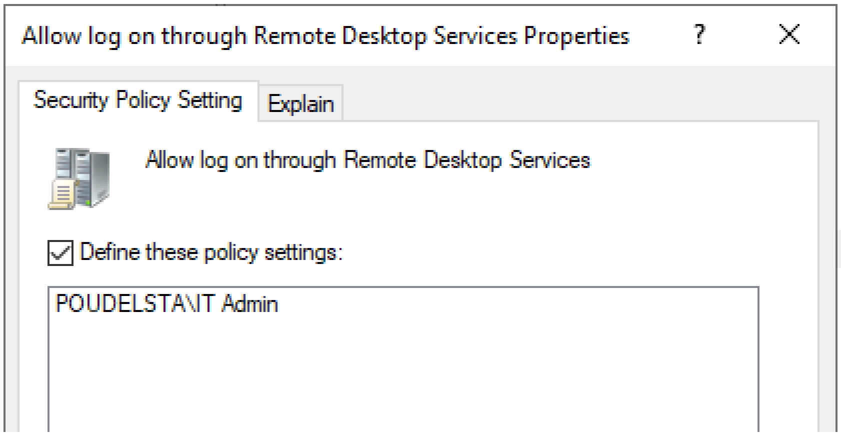
Deny log on locally Properties

Deny log on locally

☑ Define these policy settings:

POUDELSTA\Branch Managers

3. **Allow Remote Desktop Access:**
   - We will find **Allow log on through Remote Desktop Services** and double-click it.
   - Check the box for **Define these policy settings** and click **Add User or Group**.
   - We will input the **IT Admin** group (or any group that should be able to remotely access servers). Click **OK**, then **Apply**.
   - **Note:** We must then link this **User Rights** GPO to the appropriate OU (e.g., the Servers OU or the root domain) where the targeted computer objects reside.



Allow log on through Remote Desktop Services Properties

Allow log on through Remote Desktop Services

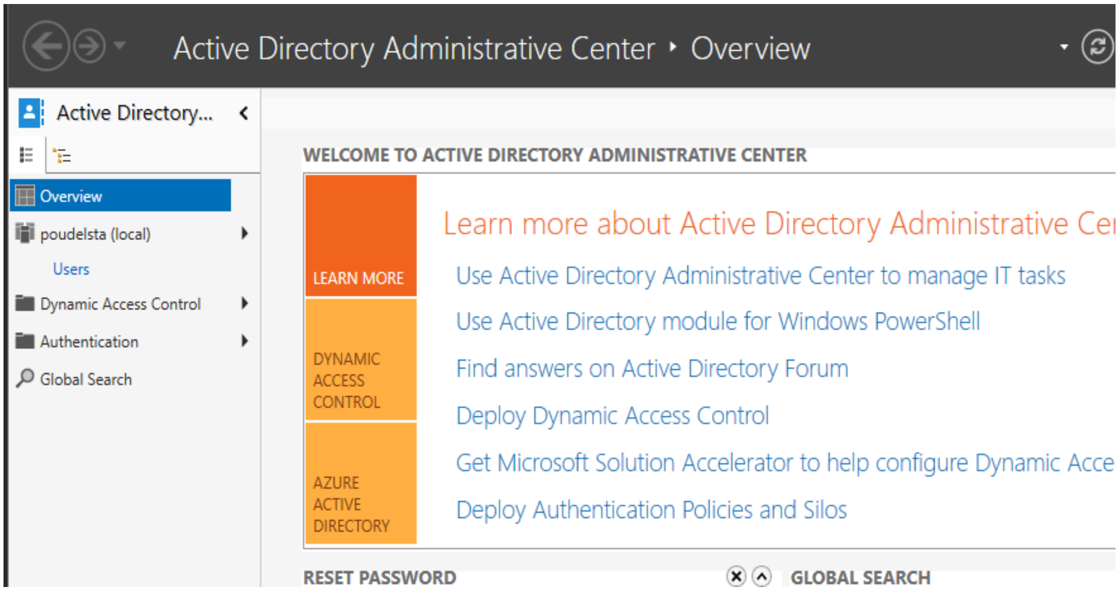
☑ Define these policy settings:

POUDELSTA\IT Admin

Part 3: Implementing Fine-Grained Password Policies (FGPP)

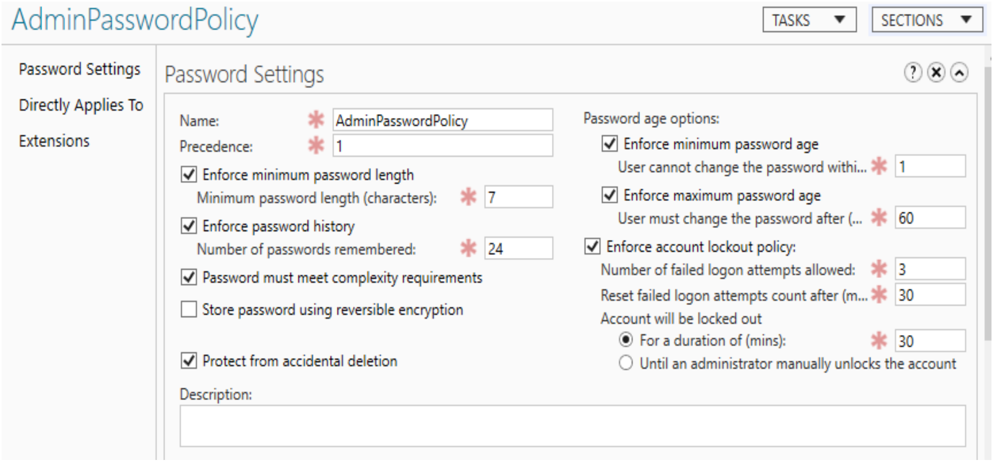
FGPPs allow us to apply *different* password policies to different groups of users (e.g., strict passwords for admins, relaxed for regular users). This is done through the **Active Directory Administrative Center (ADAC)**, not GPOs.

1. **Open Active Directory Administrative Center (ADAC):**
   - We will find and open **Active Directory Administrative Center** within the Windows Administrative Tools folder.



Active Directory Administrative Center ▸ Overview
Active Directory...
Overview
poudelsta (local)
Users
Dynamic Access Control
Authentication
Global Search
WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER
LEARN MORE
DYNAMIC ACCESS CONTROL
AZURE ACTIVE DIRECTORY
Learn more about Active Directory Administrative Ce
Use Active Directory Administrative Center to manage IT tasks
Use Active Directory module for Windows PowerShell
Find answers on Active Directory Forum
Deploy Dynamic Access Control
Get Microsoft Solution Accelerator to help configure Dynamic Acce
Deploy Authentication Policies and Silos
RESET PASSWORD
GLOBAL SEARCH

2. **Create the Administrator Password Settings Object (PSO):**
   - On the right-hand pane, click the arrow next to our domain name, then **System**, and double-click the **Password Settings Container**.
   - In the upper-right pane, click **New > Password Settings**.



AdminPasswordPolicy

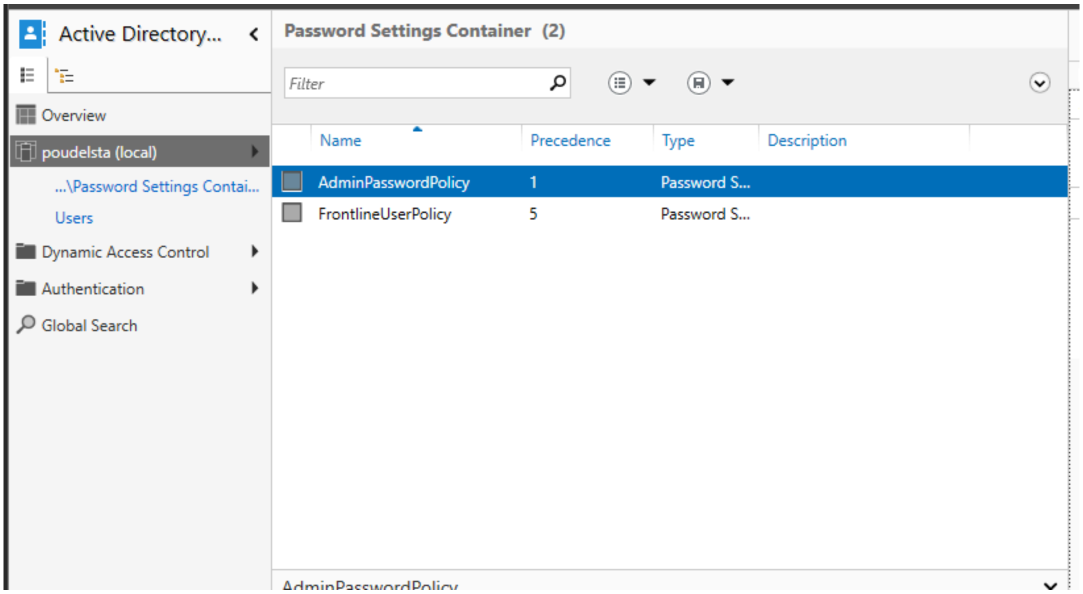
Password Settings

Name: * AdminPasswordPolicy
Precedence: * 1
☑ Enforce minimum password length
Minimum password length (characters): * 7
☑ Enforce password history
Number of passwords remembered: * 24
☑ Password must meet complexity requirements
☐ Store password using reversible encryption
☑ Protect from accidental deletion
Description:

Password age options:
☑ Enforce minimum password age
User cannot change the password withi... * 1
☑ Enforce maximum password age
User must change the password after (... * 60
☑ Enforce account lockout policy:
Number of failed logon attempts allowed: * 3
Reset failed logon attempts count after (m... * 30
Account will be locked out
● For a duration of (mins): * 30
○ Until an administrator manually unlocks the account

   - We will name it **AdminPasswordPolicy**.
   - **Precedence:** We will give it a number **1** (the lowest number means the highest priority).
   - **Configuration:** We will change the settings to be stricter for admins (e.g., Minimum password length: **22** characters; Password history: **5** remembered; Maximum password age: **60 days**). We will ensure **Enforce account lockout policy** is checked.
   - **Apply to Group:** Under **Directly Applies To**, click **Add** and input the **IT Admin** group. Click **OK**.

3. **Create the Standard User PSO:**
   - We will follow the same steps to create a second PSO, for example, **StandardUserPolicy**.
   - We will give this a **higher Precedence number** (e.g., **5**).
   - We will set less strict policy settings (e.g., Minimum password length: **12** characters; Maximum password age: **90 days**).
   - We will apply this policy to the **Domain Users** group.



Password Settings Container (2)

Name	Precedence	Type	Description
AdminPasswordPolicy	1	Password S...	
FrontlineUserPolicy	5	Password S...	

AdminPasswordPolicy