Password Policy for local computers

This will affect all users including administrators.

To set up a **local password policy** on Windows XP pro, 7 pro \ ENT, 10 pro \ ENT, or 11 pro \ ENT computers — including:

* Lock after **3 failed login attempts**
* Minimum **password length of 12**
* **Password complexity** enabled
* **Remember last 24 passwords**

You can configure this through **Local Security Policy** and

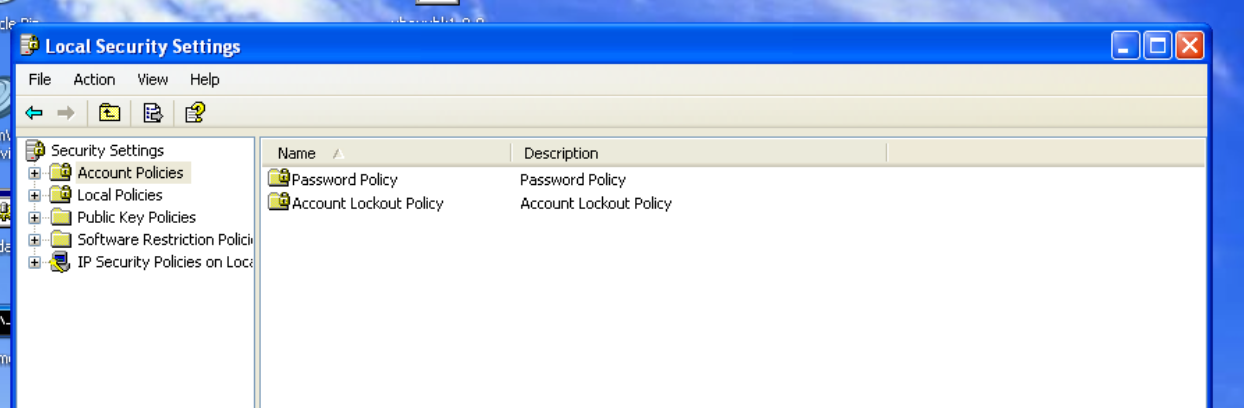
**are from Windows 10**

**1. Open Local Security Policy**

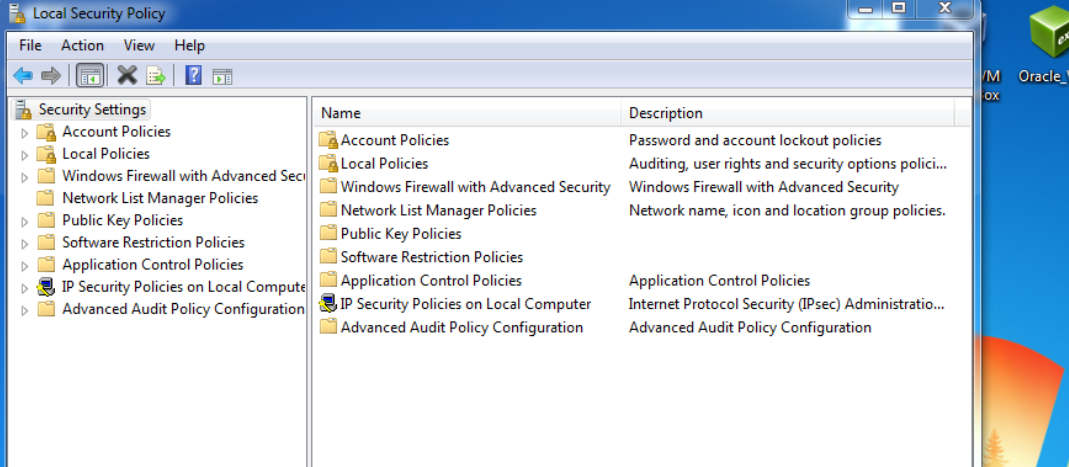
* Press Win + R, type secpol.msc, and press Enter.

If secpol.msc doesn't work (XP) , you may need to use gpedit.msc or access via Control Panel.

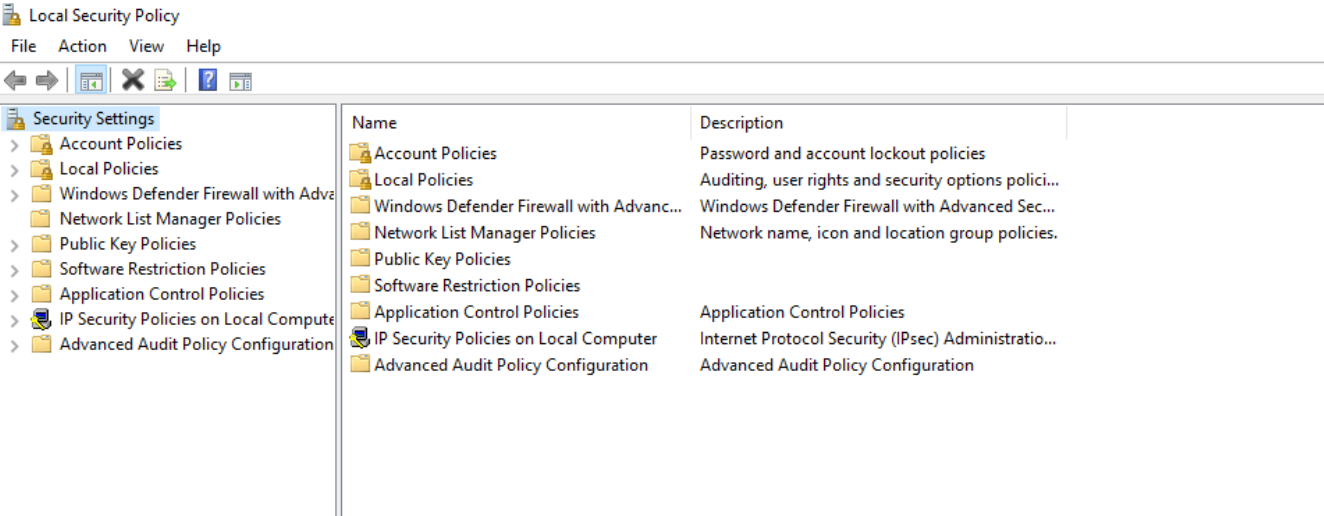
Windows XP



Windows 7



Windows 10

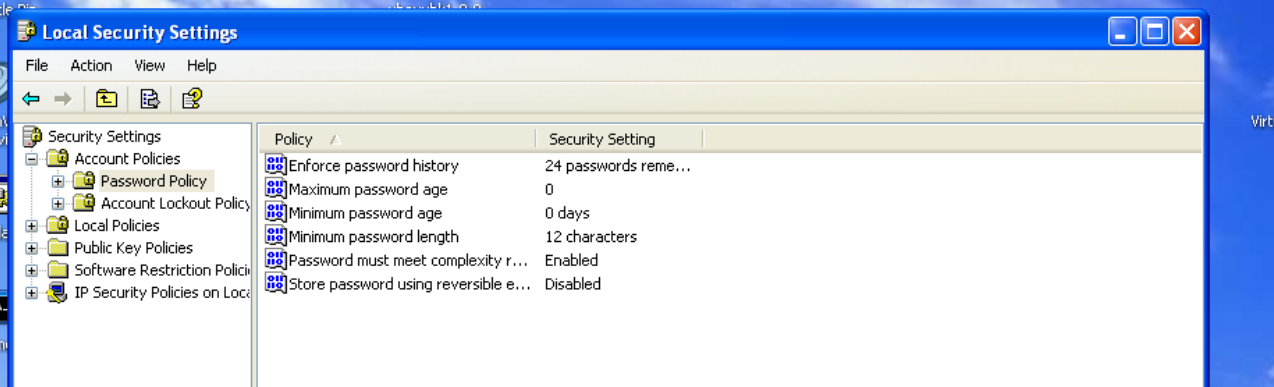


**🔧 2. Configure Password Policies**

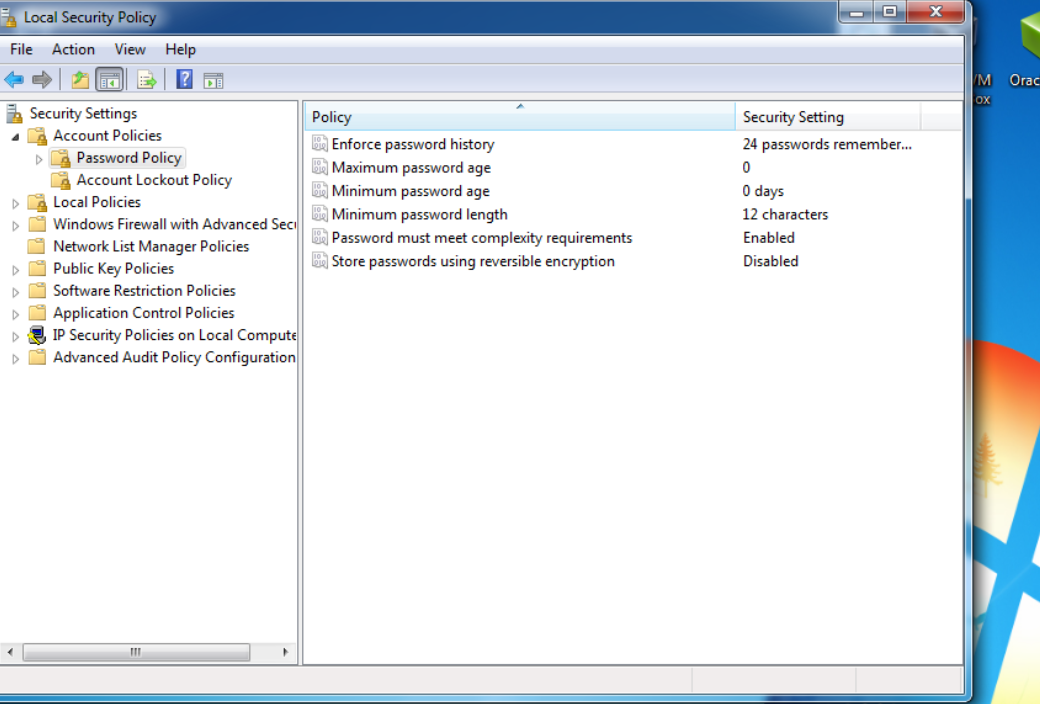
In the left pane:

Security Settings > Account Policies > Password Policy

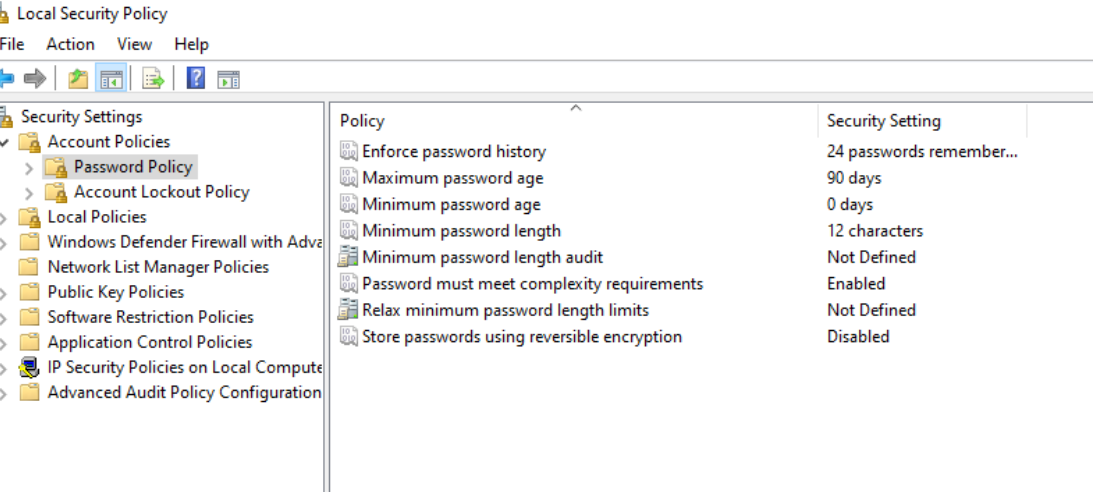
Windows XP



Windows 7



Windows 10



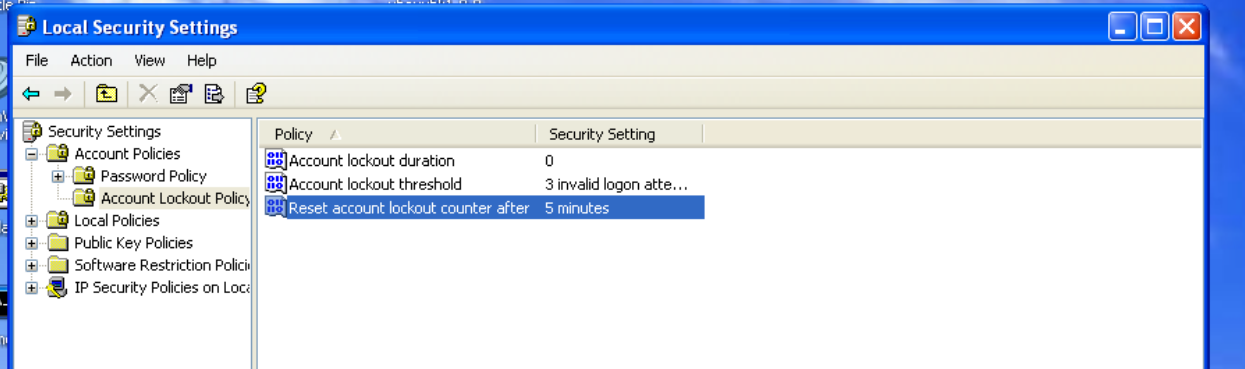
Set the following:

* **Enforce password history** → 24 passwords remembered
* **Maximum password age** → (Set as per your policy, e.g., 90 days)
* **Minimum password length** → 12
* **Password must meet complexity requirements** → Enabled

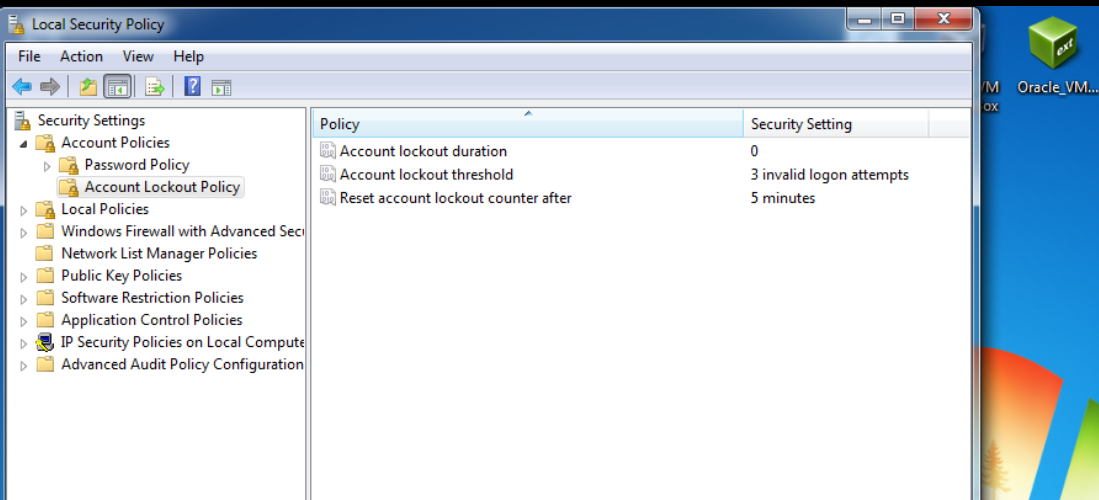
🔹 Complexity includes: uppercase, lowercase, digit, and special character.

**3. Configure Account Lockout Policy**

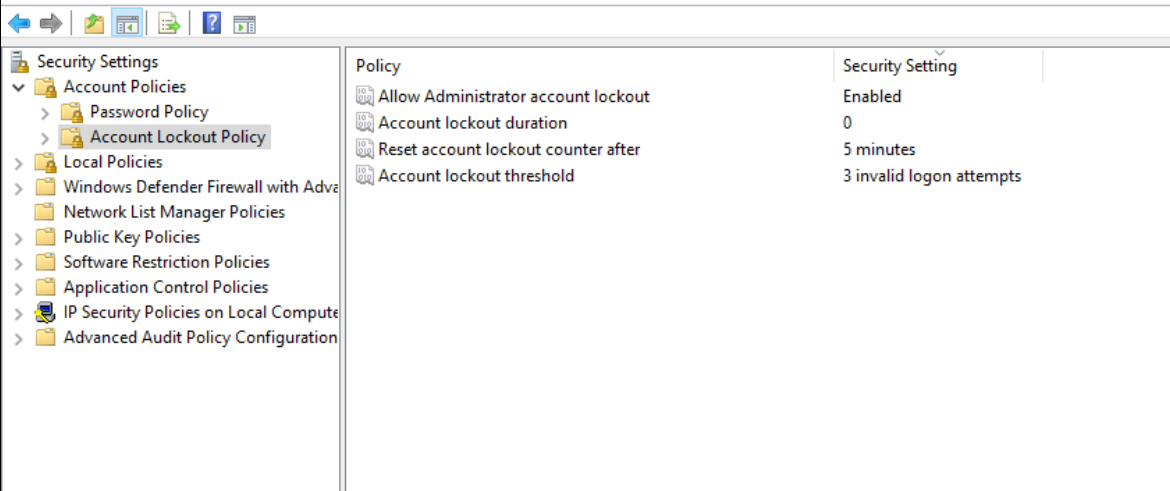
Windows XP

****

Windows 7



Windows 10

****

Still in Local Security Policy:

Security Settings > Account Policies > Account Lockout Policy

Set the following:

* **Account lockout threshold** → 3 invalid login attempts
* It will prompt you to set:
  + **Account lockout duration** → e.g., 0 minutes
  + This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it –The recommended setting is “0” because set to anything else will allow a threat acter to continue to test for passwords (brute force)
  + **Reset account lockout counter after** → e.g., 5 minutes
  + Default: None, because this policy setting only has meaning when an Account lockout threshold is specified. As that will be set to zero this setting will do nothing but you cannot set this to 0.

These values can be adjusted to match your security preferences.

**Tips**

* After applying these changes, they are enforced at the next login.

**Recap of Your Final Policy:**

* ✔ Lock account after **3 failed login attempts**
* ✔ Minimum password length: **12**
* ✔ Enforce **password complexity**
* ✔ Remember **last 24 passwords**
* ✔ **Passwords expire** every **90 days**
* ✔ **Users can reset password anytime** (Minimum age = 0)

**Summary of Settings – \this needs to be documented in the SyOPS**

| **Policy Setting** | **Value** |
| --- | --- |
| Enforce password history | 24 passwords |
| Maximum password age | 90 days |
| Minimum password age | 0 days |
| Minimum password length | 12 characters |
| Password complexity | Enabled |
| Account lockout threshold | 3 attempts |
| Account lockout duration | 5 minutes (example) |
| Reset lockout counter after | 5 minutes (example) |