

LAB 4-9 CONFIGURING PASSWORD POLICY SETTINGS IN THE DEFAULT DOMAIN POLICY

Checkoff

	Located default user policy
	Edited policy
	Set up password policy
	Set up account lockout policy
	Filled out table

Note: No matter WHERE you configure Password Policies, they ALWAYS apply to the entire domain. This is the only set of policies that does that and many a network administrator has pulled his or her hair out trying to set specific policies on individual OUs.

1. Go into your group policies management.
2. Expand your domain.
3. Select Default Domain Policy.
4. Click Edit.
5. In the Computer Configuration section, click the plus signs next to Windows Settings, and Account Policies to expand them.
6. Enable the following policies:
 - a. Password Policy
 - i. Enforce Password History: 7 passwords
 - ii. Minimum Password Length: 4 characters
 - iii. Minimum Password Age: 1 day (users can only change their password every 24 hours)
 - iv. Maximum Password Age: 30 days (users MUST change their password every 30 days, but can do so sooner if they want to)
 - b. Account Lockout Policy
 - i. Lock out account for one hour
 - ii. Lock out after 10 bad attempts
7. Save and close.
8. Log into your workstation as GPO Harry.
9. Change your password. Try a blank password.
10. Try to change it again. Does it work?
11. Show me!

Fill out the table below

Policy	What it does	Why use it?
Enforce password history		
Minimum password age		
Maximum password age		
Minimum password length		

Password complexity		
---------------------	--	--

