In this lab you will create and apply Password Setting Objects (PSOs) formally know as Fine Grained Password Policies (FGPP).

Required Materials:

SRV1, CLIENT1 images from previous labs.

**Background: Password Setting Objects**

Prior to Server 2008 there could be only one password and account lockout policy applied to all users in a domain. Creating separated domains just to have different password or account lockout polices would cause increased cost and complexity to the network with little benefit. Microsoft introduced Fine Grained Password Polices (FGPP) with Server 2008 which allows multiple sets of policies to be used simultaneously within a single domain. However, FGPP in Server 2008 and 2008 R2 did not have a GUI interface. Using FGPP required using ADSIEDIT or PowerShell. For a GUI interface, administrators had to find third party tools. Starting with Server 2012, Microsoft finally provided GUI tools for this function.

PSOs are not group policies, they are Active Directory objects. Like Group Policies, they can be applied to user accounts. Unlike Group Policies, they cannot be applied to Sites, Domains or OUs but they can be applied to global security groups.

*[If you really want to have a PSO apply to all users in a particular OU, Microsoft suggests creating a "shadow group" that is just a global security group in which you place all the users in the OU. When a PSO is applied to the shadow group it therefore applies to all the users in the OU. However, if you move a user into our out of that OU, you must manually update the global security group membership.]*

Using PSOs allows you to have more restrictive policies for sensitive accounts such as administrators and domain admins than are applied to less sensitive accounts such as standard domain users. For example, you might want administrators to use long pass phrases while allowing domain users to have shorter passwords. As another example you might require administrators to change their passwords more frequently than other users.

There is one significant limits to using PSOs: The domain must be in at least Server 2008 Domain Functional Level (the Forest Functional Level can be lower.)..

Part 1: Password Setting

In the following section you will establish and document the default password policies.

1. Make sure there are no GPOs linked to the domain that override the password policies set in the Default Domain policy. Note your current settings.

Enforce Password History\_\_\_\_\_\_\_\_ passwords remembered

Maximum password age\_\_\_\_\_\_\_\_ days

Minimum password age\_\_\_\_\_\_\_\_ days

Minimum password length\_\_\_\_\_\_\_\_ characters

Password must meet complexity requirements \_\_\_\_\_\_\_\_\_\_

Store passwords using reversible encryption \_\_\_\_\_\_\_\_\_\_

**In the following section your will create the accounts and groups you need to implement and test PSOs.**

1. Create the following global security groups

Secure Passwords

Simple Passwords

1. Create the following user accounts (do not require password change at next logon)

Logon Name Initial Password Group Membership

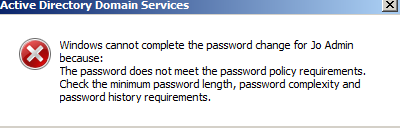
JoAdmin Password#1 Domain Admins, Secure Passwords

SamUser Password#1 Domain Users, Simple Passwords

**In the following section you will verify that the default policy is working**

1. Right click on the user account in Active Directory Users and Computers and select Reset Password...
2. Try to reset the JoAdmin password to the passphrase **mypasswordstinks**

*Note: if you get the message that the passwords didn't match, try again. A failure message that refers to a conflict with the password policy should like the following.*



The failure message means that the password you tried to create does not meet the requirements. In this case it does not meet the complexity requirement because it is all lower case letters.

1. Did you get the message above? **[Y / N ]** *(If you don't, fix the problem.)*

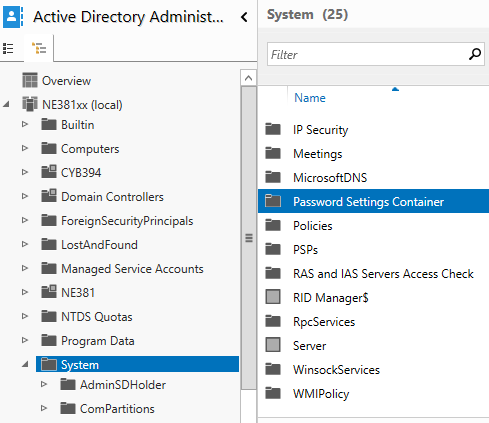
*Why does this password fail? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

1. Now try to reset the SamUser password to **fido** .
2. Were you able to change the password? **[Y / N ]**

What criteria was not met? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Part 2: Install and Run the GUI Tool

1. You should be logged on to SRV1 with your administrative credentials.
2. From the Tools menu in Server manager, open the Active Directory Administrative Center. Click on System under the domain and select the password Settings



1. Right click on Password Settings Container and choose New then Password Settings.
2. Create the following settings

Name: **Secure Password Policy**

Precedence: **1**

Minimum Password Length: **15**

Remember **12** passwords

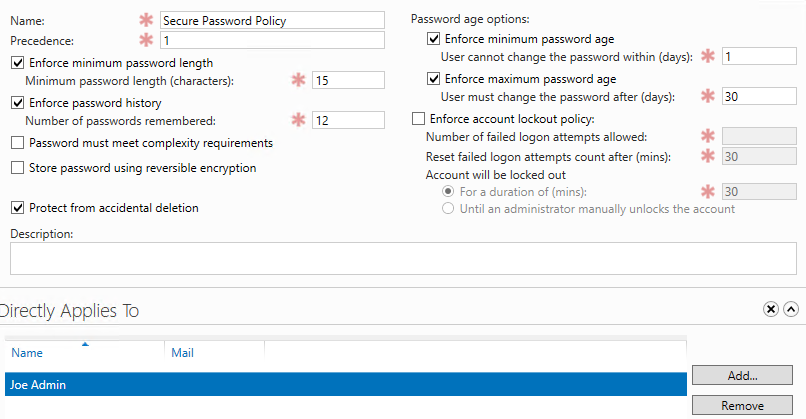
Uncheck complexity requirement

Minimum Password Age: **1**

Maximum Password Age: **30**

Set the policy to apply to: **Secure Passwords group**

*This will allow selected administrators to have long, simple passphrases that don’t need to meet complexity requirements.*



1. Create another FGPP. Call this one Insecure Password Policy with the following settings and apply it to the Simple Passwords group.

Precedence: **2**

Minimum Password Length: **4**

Remember **1** password

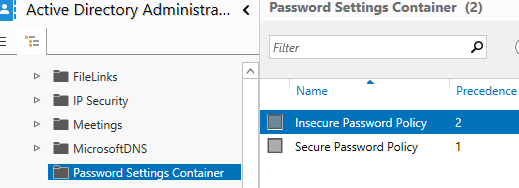
Uncheck complexity requirement

Minimum Password Age: **1**

Maximum Password Age: **180**

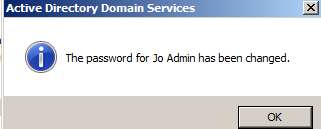
*This will allow selected users or groups to have very short passwords that don’t need to be complex. (This would not be a good setting for a real network!)*

1. To verify right click or double click on each policy in turn in the Password Settings Container and select Properties.



**In the following section you will test to see if the policies you created and applied actually override the default GPO.**

1. In Active Directory Users and Computers, reset the JoAdmin password to mypasswordstinks. Be sure to **uncheck** the box that requires changing the password at next logon! Don't continue until you get the confirming message



Although this failed before, it should succeed now because of the new PSO.

1. On the CLIENT1 image, Logon as **JoAdmin** with the new passphrase.

Was this successful? **[ Y / N ]** *(This should work)*

1. Try to reset the JoAdmin password to **fido** in Active Directory Users and Computers

Was this successful? **[ Y / N ]** *(This should fail)*

Why does this fail? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Reset **SamUser** to have the password of **fido**
2. Logon to CLIENT1 with the SamUser account with the password of **fido** to prove it worked.

Was this successful? **[ Y / N ]** *(This should succeed)*

1. Try to reset the SamUser password to mypasswordstinks

Was this successful? **[ Y / N ]**  *(This should succeed)*

1. If you disabled or unlinked any account polices at the beginning of this lab, you can enable or link them again.