FINEGRAINED PASSWORD POLICY /PASSWORD SETTING OBJECT

This feature introduced in Windows Server 2008 allows you to override password policy set at the domain level.

It applies password settings to subsets of users that you may like to differentiate from the domain policy.

You can use GUI –Active Directory Administration Center (Graphical User Interface) ADSIedit, LDP or Powershell to create PSOs (Password Settings Objects).

Note that PSOs are not like GPOs:

1. They're not managed via GPMC.

2. They're not linked to OUs, Sites or Domains.

PSOs apply to User and Group objects (ie. ultimately apply to User Accounts)

As an example, with FGPP you can have a Domain password policy that defines a minimum password length of 8 characters which will be applied to all users in the domain.

Then have a PSO that sets 24 characters for all user accounts that are members of the "All Service Accounts".

Using ADAC (Windows 8 or Server 2012) (see Active Directory Administrative Center)

1.Open Active Directory Administrative Center

2. Select the List View

3. Expand the System Container

4. Open the Password Settings container

5. Right click on the Password Settings container and click on New – Password Settings

6. Configure the desired PSO properties (Max password Age, Min Password Length, etc).

4. Assign the PSO to a user or group

Creating a PSO using ADSI Edit

Active Directory Service Interfaces Editor (ADSI Edit) provides a view of every object and attribute in an Active Directory Domain Services (AD DS) forest. You can use ADSI Edit to **query**, **view,** and **edit** AD DS objects and attributes.

To create a PSO using ADSI Edit

1. Click Start, click Run, type adsiedit.msc, and then click OK.
2. In the ***ADSI Edit*** snap-in, right-click ADSI Edit, and then click Connect to.
3. In Name, type the fully qualified domain name (FQDN) of the domain in which you want to create the PSO, and then click OK.
4. Double-click the domain.
5. Double-click DC=<domain_name>.
6. Double-click CN=System.
7. Click CN=Password Settings Container. All the PSO objects that have been created in the selected domain appear.
8. Right-click CN=Password Settings Container, click New, and then click Object.
9. In the Create Object dialog box, under Select a class, click msDS-PasswordSettings, and then click Next.
10. In Value, type the name of the new PSO, and then click Next.
11. Continue with the wizard, and enter appropriate values for all mustHave attributes.

View a Resultant PSO for a User or a Global Security Group

You can view the resultant Password Settings object (PSO) for a user object:
Viewing the resultant PSO for users using the Active Directory module for Windows PowerShell
Viewing the resultant PSO for users using the Windows interface
Viewing the resultant PSO for users from the command line using dsget

To view the resultant PSO for a user using Windows interface

1. Open Active Directory Users and Computers.
2. On the View menu, ensure that Advanced Features is checked.
3. In the console tree, click Users.
4. In the details pane, right-click the user account for which you want to view the resultant PSO, and then click Properties.
5. Click the Attribute Editor tab, and then click Filter.
6. Ensure that the Show attributes/Optional check box is selected.
7. Ensure that the ***Show read-only attributes/Constructed check box*** is selected.
8. Locate the value of the msDS-ResultantPSO attribute in the Attributes list