Windows Enterprise
OU Administration
Using Password Setting Objects (PSOs)

Steven L. Kunz [ITSYS]
June 30, 2015

Background

Password Setting Objects (PSOs) allow fine-grained password policies which allow IT admins to apply a specific password policy to a given collection of users. The alternate password policies enforce greater security standards than the default domain policy. More details on how PSOs are designed by Microsoft and how they are implemented at Iowa State University are available in the "Planning for Password Setting Objects (PSOs)" document here:

http://tech.its.iastate.edu/windows/admin/PSO_Planning.pdf

Applying a PSO to Selected Users in Your OU

Enterprise Admins will add college/departmental OUs (for their faculty/staff) to each PSO list upon request. IT admins can only submit requests for OUs they manage (applying PSOs to only their faculty/staff).

1) Move the users needing a specific PSO to into an OU within your OU structure. If there are nested OUs ALL users in the nested OUs will be included.

   IMPORTANT! If you apply this to a powerful user in your OU and they HATE it and they have the power to recheck "Password never expires" on their user object then you have accomplished nothing. Ditto for being able to move their account out of the OU that applies the PSO to them. You need to isolate who can manage powerful accounts and trust them to do the right thing.

2) Supply the following in an email to its-ad-admins@iastate.edu containing the following:

   - Policy Name to be applied (see "Stock PSOs" below).
   - Fully qualified domain name of the OU (available off the "Object" tab for the OU in Active Directory Users and Computers).
   - A mailing list address of people who will be notified when the OU is renamed, moved or disappears.

3) The supplied mailing list will receive an email when your OU has been added to the proper PSO list. You can verify that the PSO has been applied by checking the groups the users are a member of. You should see membership in a "!ISU-PSO<n>" group matching your request (this is the shadow-group membership created from being contained in the OU you provided). You can also use the "dsquery" command supplied in the "Help Desk Issues" section below.

4) Once an OU is integrated into the automated processing, users will have the PSO applied automatically as they are moved into and out of the OU. **IMPORTANT!** Automated processing

occurs only once per hour (about 15 minutes after the hour). As a result it may take up to an hour for a PSO to apply to a user based on membership in your OU.

5) If their current password is older than the maximum age allowed by the PSO they will have to change their password at the next login (with the required constraints from the table below). If there are started tasks or services configured to run under an account whose password is expired due to the new PSO setting that task or service will immediately being to fail.

6) It is your responsibility to inform the user of the new password rules that now apply to them. Neither you nor the user will receive any type of automated email relating the application (or removal) of a PSO policy based on the OU they reside in.

7) See "Implementation Details" below for important implications of the "Password never expires" account tab setting. DO NOT check "Password never expires" if you want a PSO to apply to that user!

Stock PSOs

The following is a list of stock PSOs:

Priority	Policy Name	Minimum Len	Char Classes	Max Life	History	Lockout (cnt/dur)
1	PSO1 (HiSecurity)	20	3	30	5	5/1
2	PSO2A	8	2	90	10	5/1440
3	PSO2 (PCI)	8	3	90	5	5/30
4	PSO3 (ITAdmin)	16	3	30	5	5/1
5	PSO4 (Staff1)	16	3	180	5	5/1
6	PSO5 (Staff2)	8	3	180	5	5/1
7	PSO6 (Service)	30	3	Infinite	5	5/1
(none)	Default Domain	8	2	Infinite	5	5/1

Notes:
1) Listed in highest to lowest precedence.
2) "Minimum Len" is in characters.
3) "Max Life" is in days.
4) "History" is the number of remembered passwords used to reject previously used ones.
5) "Lockout" is failed attempts in minutes. A "cnt/dur" notation of "5/1" means "lockout after 5 attempts for 1 minute".

Implementation Details

There are a few details that any OU administrator must know before applying a PSO to a user.

1) By default, all NetID-based user objects are provisioned in Active Directory with the "Password never expires" attribute set (this setting is on the "Account" tab for the user object in Active Directory User and Computers"). If the "Password never expires" check-box IS checked then any PSO maximum age

setting that applies to the user is ineffective (since this setting takes precedence over the PSO setting). As a result, when applying a PSO to a user the automated script will automatically "uncheck" the "Password never expires" setting on the user object.

2) A user is required to change their password at the next login once their password age exceeds the PSO "maximum life" and the "Password never expires" box is unchecked on their user object. The automated shadow-group process will automatically uncheck "Password never expires" on each user object it adds to a PSO shadow group. When a user object is removed from the shadow-group the "Password never expires" box will be re-checked for the user.

3) Warning: The default maximum password life via default Domain Policy is 180 days. Manually unchecking "Password never expires" and NOT applying any PSO will cause that user to have a forced password change should their password age be over 180 days! As mentioned in the previous point, the automated shadow-group process will correctly check and uncheck the "Password never expires" box. Use caution when manually checking/unchecking this box. You can disable the granular password settings (if the user should have a password policy applied to them and you check it) or apply the domain default "180 day" expiration (if the user has no password policy applied and you uncheck it). It is recommended you NEVER manually check/uncheck the "Password never expires" box on users objects you manage.

Help Desk Issues

The biggest help desk issue relating to PSOs being applied to a user is that password lengths/styles that previously worked (eight character minimum, two character sets) now produce an error message that may not clearly indicate the reason (other than the password does not meet requirements). A help desk person will have to be able to figure out if a PSO applies to a user and what the rules for that PSO are. Using Active Directory Users and Computers the help desk staff could view the groups the user is a member of. Given the naming convention, IT admins can see if a PSO applies to a user by seeing they are a member of a "!ISU-PSO<n>" shadow group.

A command-line tool may also be used to figure out the effective policy. An example of a command to determine effective policy is:

dsquery user –samid <netid> | dsget user –effectivepso

Important: The above command will only work on systems with the RSAT toolset installed (Remote Server Administration Tools) with Active Directory components included. This would include Vista and Windows Server 2008 systems with the feature installed. The above command will not work on XP with the old "Adminpak" tools.

The resultant output will look like:

```
effectivepso
"CN=PSO1,CN=Password Settings Container,CN=System,DC=iastate,DC=edu"
```

This response indicates “PSO1” applies to that NetID-based user. Using documentation on the PSO the help desk staff can tell the person what the new restrictions are.