MS-Windows: Active Directory

Password Settings Objects (PSOs)

First published: 08-Jul-2010; last amended 20-Oct-2014

Purpose of this Document:

The introduction of fine-grained password policies is new to Windows Server 2008 and represents a leap forward, allowing for the implementation of multiple Account Policies on a single domain.

This document introduces Password Settings Objects (PSOs), their requirements and benefits, and explains how to setup and apply PSOs on an Active Directory domain.

Account Policies:

Microsoft Windows Server 2000 and 2003 Active Directory domains allowed for the definition of only one set of effective Account Policies (Password Policies, such as *Maximum Password Age*, and Account Lockout Policies, such as *Lockout Threshold*). Even though additional Account Policies could be defined on Organisational Units (OUs) via Group Policy Objects (GPOs), these Account Policies were always ignored, i.e. only the Default Domain Policy would take effect.

This meant that if you wanted to apply different Account Policy settings to different users you were likely to create additional domains, each with a different Default Domain Policy.

Windows Server 2008 introduced a more flexible solution, which allows for Account Policy settings to be defined at a more granular level. Using PSOs you can now define multiple Account Policy settings for different sets of users belonging to a single domain.

An obvious benefit of PSOs is the ability to define multiple Account Policies to suit the differing security requirements of various groups of users, e.g. stricter policies over sensitive, privileged accounts such as those belonging to IT administrators.

How to implement PSOs:

PSOs are only available from Microsoft Windows Server 2008, and only apply to domains where the domain functional level is set to Windows Server 2008.

By default, only members of the Domain Admins security group can create PSOs as they have *Create Child* and *Delete Child* permissions over the Password Settings Container object.

It is important to note that PSOs can only be applied to user and inetOrgPerson objects and global security groups. I.e. a PSO will be ignored if it is linked to an OU or to a Universal security group.

Access to a tool such as ADSIEdit is required to create the PSOs.

Using an account that is a member of the Domain Admins security group, run ADSIEdit on a Microsoft Windows Server 2008 domain controller.

- After connecting to the target domain, navigate to *CN=System -> CN=Password Settings Container*.
- Right-click and select *New -> Object*.
- Choose the *msDS-PasswordSettings* class.
- Now name the new PSO, set a precedence value, which establishes the PSO's priority in situations where a user is a member of multiple groups with different password policies, and define the appropriate Account Policy settings. Then enter the names of the objects that this PSO will apply to.

The values defined must conform to a pre-defined standard and range. Refer to the *Additional Resources* section for more information on this.

After a PSO has been created, you can use the *Attribute Editor* tab available via ADSIEdit or the standard Active Directory Users and Computers interface to modify the PSO.

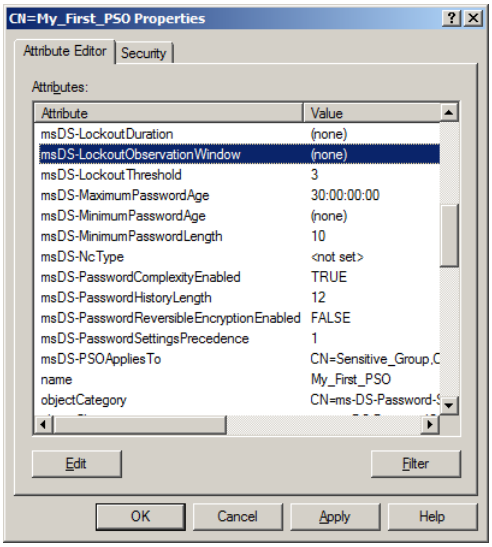

Figure 1 – View of the PSO's attributes via ADSIEdit

MS-Windows: Active Directory

Password Settings Objects (PSOs)

First published: 08-Jul-2010; last amended 20-Oct-2014

How to determine the PSO in effect over an object:

There is no interface available to list the PSO that applies to a particular user or group object. To make the association, you need to inspect the *ms-DS-PSOAppliesTo* attribute in each defined PSO.

If an object is defined in multiple PSOs, the PSO that has the lowest *msDS-PasswordSettingsPrecedence* value will take precedence.

However, if a PSO is applied directly to a user object it will over-ride PSOs applied to groups which this user object is a member of, regardless of the set *msDS-PasswordSettingsPrecedence* value of the over-ridden PSOs.

To clarify:

- *John Doe* is a member of the group *Sensitive_Users*
- *SamplePSO_1* (which has a precedence of 1) is applied to group *Sensitive_Users*
- *SamplePSO_3* (which has a precedence of 3) is applied directly to user *John Doe*

In this scenario, the Account Policy settings defined in *SamplePSO_3* will be in effect over user *John Doe*.

SekChek's reporting on PSOs:

Both the SekChek Classic and SekChek Local tools report on the use of PSOs. These analyses are available from extracts run with V5.0.4 (or later) of the SekChek Classic for Windows Extract Software; and for scans run with V1.4.4 (or later) of the SekChek Local for AD tool.

Additional Resources:

You can refer to Microsoft's TechNet article *AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide* (http://technet.microsoft.com/en-us/library/cc770842(WS.10).aspx), which describes PSOs and their creation in further detail. The article also provides the relevant acceptable value range for each of the attributes.

This paper was written by Sanjay Pather, an Operations Manager at SekChek Information Protection Services. Sanjay is responsible for the quality of SekChek reports and research and testing of security controls on the various platforms supported by SekChek.