# MIKETOIS

You read it here



Filed under PSO …

APR 24 2012
LEAVE A COMMENT

2008, ACTIVE DIRECTORY, FINE-GRAINED PASSWORD POLICY, PSO

## PSO – FINE-GRAINED PASSWORD AND LOCKOUT POLICY

You can override the domain password and lockout policy by using a fine-grained password policy.
Fine-grained password policy enables you to configure a policy that applies to one or more groups or users in your domain.
To use fine-grained password policy, your domain must be at the Windows Server 2008 domain functional level.

A fine-grained password policy is implemented by creating a Password Settings Object.

To create the PSO, use ADSI Edit.

The following example assumes your domain is miketois.com. Substitute your domain accordingly.
Let's suppose that the minimum length of passwords within your domain is 8 characters, and accounts will lockout if there are 10 incorrect logon attempts within an hour.
But, for those working in HR, it needs to be 14 characters, and the user account will lockout after 5 incorrect attempts within 30 minutes.
Let's suppose there is a global group called HR. The following example creates a PSO called HRPSO and applies it to a global group called HR, located in the Users OU.

1. Open ADSI Edit from the Administrative Tools folder.
2. Right-click ADSI Edit and choose Connect To.
3. In the Name box, type miketois.com. Click OK.
4. Expand miketois.com and select DC=miketois,DC=com.
5. Expand DC=miketois,DC=com and select CN=System.
6. Expand CN=System and select CN=Password Settings Container.
PSOs are created and stored in the Password Settings Container (PSC).
7. Right-click the PSC->New->Object.
The Create Object dialog box prompts you to select the type of object to create.
There is only one choice, which is msDS-PasswordSettings.
8. Click Next.
Each time you click next, you will be prompted for the value for each attribute of a PSO.
Some of these attributes are Boolean, some are integer, and some are a duration, specified as dd:mm:hh:ss.

9. Configure each attribute as indicated in the following list. Click Next after each attribute.
**Common Name: HRPSO**. This is the friendly name of the PSO.
**msDS-PasswordSettingsPrecedence: 5**. This sets the precedence to 5. (1 is the highest).
**msDS-PasswordReversibleEncryptionEnabled: False**. The password is not stored using reversible encryption.
**msDS-PasswordHistoryLength: 25**. The user cannot reuse any of the last 25 passwords.
**msDS-PasswordComplexityEnabled: True**. Password complexity rules are enforced.
**msDS-MinimumPasswordLength: 14**. Passwords must be at least 14 characters long.
**msDS-MinimumPasswordAge: 1:00:00:00**. A user cannot change his or her password within one day of a previous change.
**MaximumPasswordAge: 30:00:00:00**. The password will expire after 30 days..
**msDS-LockoutThreshold: 5**. The account will lockout after 5 invalid attempts.
**msDS-LockoutObservationWindow: 0:00:30:00**. Five invalid logons (specified by the previous attribute) within 30 minutes will result in the account being locked out.
**msDS-LockoutDuration: 01:00:00:00**. An account, if locked out, will remain locked for one day or until it is unlocked by an administrator. A value of zero will result in the account remaining locked out until an administrator unlocks it.
The attributes listed above are required.
10. Click the More Attributes button.
11. In the Edit Attributes box, add the following:
In the Select a Property to view, the default should be adminDescription. Type **CN=HR,CN=Users,DC=miketois,DC=com** and click Set.
Change the Select a Property to view to msDS-PSOAppliesTo and type **CN=HR,CN=Users,DC=miketois,DC=com** and click Add.
Click OK and then click Finish.
PSOs are applied in real time. There is no need to run some kind of gpupdate-type tool. If the PSO has been configured correctly, it should now be applying itself to the HR group and its members.

**Confirming the PSO Has Been Applied**

Checking the Attribute Editor on a user account which is a member of the HR security group will confirm that the PSO is being applied.
If you have created an empty group with the intention of populating it later, you can confirm that the PSO is been applied to the group.

To check a group, in Active Directory Users and Computers, on the View menu, enable the Advanced Features.
Expand your domain and the Users OU.
Locate the HR group, right click it and choose Properties.
Click the Attribute Editor.
This lists the attributes associated with the HR group.
Click the Filter button and under Show read-only attributes, ensure Constructed and Backlinks are selected.
In the list of attributes, locate **msDS-PSOAppliesTo**. It should contain the value CN=HRPSO,CN=Password settings Container,CN=System,DC=miketois,DC=com. (Obviously, in your domain the path to the object will be different). If this is not set, review the entries you made when you configured the PSO.

To check if the PSO is applied to a member of the HR group, expand your domain and locate a user's account which is a member of the HR group.
Right click it and choose Properties.
Click the Attribute Editor.
This lists the attributes associated with the user's account.

Click the Filter button and under Show read-only attributes, ensure Constructed and Backlinks are selected.
In the list of attributes, locate **msDS-PSOAppliesTo**. It should contain the value **CN=HRPSO,CN=Password settings Container,CN=System,DC=miketois,DC=com**. (Obviously, in your domain the path to the object will be different). If this is not set, review the entries you made when you configured the PSO.

Tagged Active Directory, AD, AD Admin, Fine-Grained Password Policy, msDS-ResultantPSO, PSO, server 2008, windows server

Search

## RECENT POSTS

- PSO – Fine-Grained Password and Lockout Policy
- ActiveSync on Exchange 2003 error 'Your account does not have permission to sync with current settings. Contact your Administrator'
- Identifying and Fixing the Cause of svchost.exe running at 99% CPU
- Spoof Email And Why The Martians Aren't Coming
- Manganum – how to remove this malware without downloading any tools

## ARCHIVES

- April 2012

## CATEGORIES

- 2008
- Active Directory
- ActiveSync
- Email
- Fine-Grained Password policy
- Group Policy
- Hoax
- Malware
- NC_NET
- Powershell
- PSO
- Troubleshooting

## META

- Register
- Log in
- Entries RSS
- Comments RSS
- WordPress.com