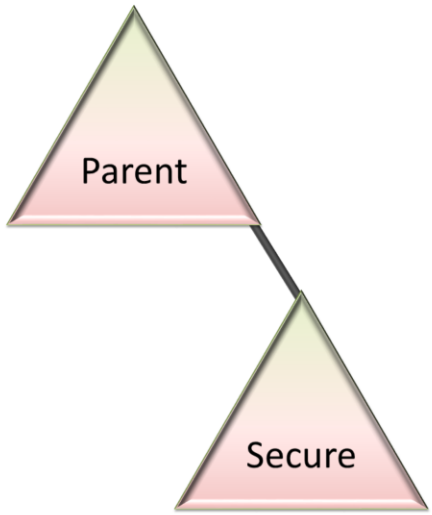
Fine-Grained Password Policies

For the free video please see
http://itfreetraining.com/70-640/fine-grained-password-policy

Active Directory allows multiple password policies to be created in the same domain. This is referred to as fine grained password policy. This video looks at how to use multiple passwords policies applying them to users and groups and how to use shadow groups to apply a password policy to an organizational unit.

Before Fine Grained Passwords

- Previously separate domains need to be created

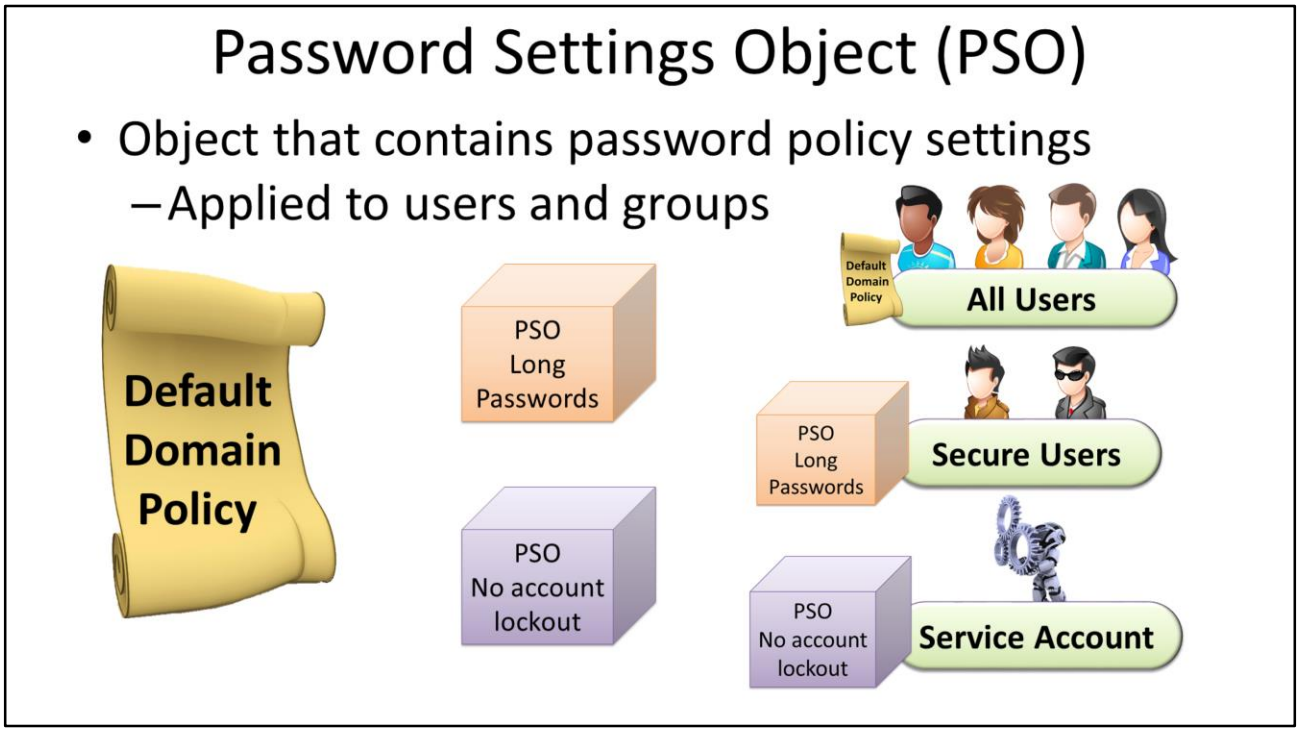


Before Fine Grained Passwords
Previously, if an administrator wanted to have separate password policies they would need to create separate domains. For example, if they had a secure domain and they wanted the users in the secure domain to have a longer password, a separate domain would need to be created. This is no longer required as multiple password policies can be created and used in the same domain.

Fine-Grained Passwords

- Requires Windows Server 2008 Domain Functional level
- Applied to Users and Groups
  - Not OU's

Fine-Grained Passwords
In order to use fine grained passwords, your domain needs to be Windows Server 2008 Domain Functional Level or higher. This essentially means that all Domain Controllers in your domain need to be Windows Server 2008 or higher and the domain functional level raised to at least Windows Server 2008. Additional password policies are applied to users or groups not OU's.



Password Settings Object (PSO)

A Password Settings Object or PSO contains all the same password settings that exist in the Default Domain Policy. In order to change settings and apply them to users and groups, you need to create a new PSO with the same settings as the Default Domain Policy except for the settings you want to change. You cannot choose to change a single setting, all settings must be configured.

When multiple PSO's are used

- Settings determined by Password Settings Precedence
- Value needs be 1 or greater
- Lower values have priority
- If multiple PSO's have the lowest priority
  - PSO with lowest GUID will be used
  - GUID unique number assigned to all AD objects

When multiple PSO's are used

Each PSO object has a setting called Password Settings Precedence. This value determines which PSO will be used when multiple PSO objects are being applied. The PSO with the lowest value will be used with the lowest value being 1. If there are multiple PSO's with the same Password Settings Precedence value than the PSO with the lowest GUID will be used. Every object in Active Directory has a unique GUID which acts like a serial number for the object, thus one PSO will always have a lower GUID.

Demonstration

Demonstration
To change the domain functional level or see what level your domain is currently at, open Active Directory users and Computers, right click the domain and select the option raise domain functional level.
In order to create a new PSO object, you need to run ADSI edit from administrative tools under the start menu. Once open, right click ADSI edit and select the "connect to" option to connect your domain.
Once connected, you need to expand through your domain to "CN=Password Settings Container" located under "CN=System". To create a new PSO, right click "CN=Password Settings Container" and select new object.
It is a simple matter to complete the questions in the wizard.

Questions that are in the new PSO wizard
Common-Name: This is a friendly name to identify the PSO.
Password Settings Precedence: Must be 1 or greater. When multiple PSO's are applied to the same user or group, the PSO with the lowest Password Settings Precedence value will be used.
Password reversible encryption status for user account: This indicates whether the password will be stored using a method so the password can be retrieved later on. Values for this are false or true.
Password History Length for user accounts: This indicates how many previous passwords Active Directory should remember and thus prevent the user from using. If the value is 0, no password history will be saved**.**
Password complexity status for user account: Indicates if a password needs to meet complex

password requirements. This means it must have 3 out of 4 of the following. A-Z, a-z, 0-9 or non-alpha numeric. Values are true or false.
Minimum Password Length for user accounts: This value indicates how long the value of the password should be. Valid settings are 0 to 255.
Minimum Password Age for users accounts: This indicates how long the password will need to be used before it can be changed. To disable the settings use the value (none). Otherwise use the setting DD:HH:MM:SS. For example 1 day, 3hours, 5 minutes and 20 seconds would be 1:03:05:20
Maximum Password age for user accounts: This indicates how long a password can be used before it has to be changed. The value needs to be entered in the format DD:HH:MM:SS. If you do not want the password to ever expire use the value (Never).
Lockout threshold for lockout of user accounts: This indicates the number of wrong password attempts that can be performed before the user account is locked out. Values are 0 through to 65535.
Observation Windows for lockout of user account: This indicates the time period that needs to expire for a reset of the invalid user password count to occur. The value needs to be entered in the format DD:HH:MM:SS. If you do not want the password to ever expire use the value (None).
Lockout duration for lockout user accounts: This value indicates how long a user account will remain locked until it unlocks itself. The value needs to be entered in the format DD:HH:MM:SS. If you do not want the password to ever expire use the value (Never).

Once you create the PSO object you need to associate the object with a user or group. To do this, open the properties for the object and open the attribute msDS-PSOAppliesTo and select the option edit and press the button add Windows Account.

If you want to check which Password Settings a user is obtaining this can be done in Active User in Computer. In order to see the setting, make sure that in Active Directory Users and Computers under the view menu advanced features is ticked. Once advanced options is ticked, open the properties for the user and select the tab attribute editor. To see the attribute, select the filter option and select the option constructed. The attribute msDS-ResultantPSO will tell you which PSO is being applied to that user.

Shadow Group Demonstration
A shadow group is a standard group. The difference is more of a concept than a group type. A shadow group contains all the users under an organizational unit. The members of the group can be kept up to date manually or using a script. There are many different scripts available to perform this. An example of such a script is given below.
“Creating And Managing Shadow Groups” http://dx21.com/ezine/p2p/article.aspx?ID=95
This script needs to be edited to indicate where the group is and where the OU is located.
At the top of the script, look for the following two lines and change them as required.
Const OULDAP = "LDAP://OU=[OUName],DC=[Domain],DC={Ext]"
Const SGLDAP = "LDAP://CN=[GroupName],OU=[OptionalOU],DC=[Domain],DC=[Ext]"

Once the script has been changed, you can run it as required or create a scheduled task to

run the script automatically.

References

"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 395-402
"Create a PSO" http://technet.microsoft.com/en-us/library/cc754461(v=ws.10).aspx
"Creating And Managing Shadow Groups" http://dx21.com/ezine/p2p/article.aspx?ID=95