8.14.5 Fine-Grained Password Policy Facts

In a Windows network, granular (fine-grained) password policies allow you to create password policies for users and global groups separate from the password policy applied to the entire domain. For example, you could use granular password policies to require that administrators use 14-character passwords and that normal users use only eight-character passwords.

You should know the following facts about granular password policies:

- Only users who are members of the Domain Admins group can set granular password policies, but you can delegate the ability to set these policies to others.
- Granular password policies are saved as a Password Settings object (PSO) in the Password Settings container (PSC).
  - There is one default PSC. It cannot be renamed, deleted, or moved.
  - You can create additional PSCs, but they will not take effect.
  - The PSC holds one or more PSOs. You can define multiple PSOs, each with unique password policy settings.
- PSOs have attributes for all of the settings that can be defined in the Default Domain policy (except Kerberos settings).
- The **msDS-PSOAppliesTo** property in the PSO identifies the objects to which the password policy applies.
  - Policies can be applied to user accounts or global security groups.
    - Each granular policy can be applied to multiple users and/or groups.
    - Granular password policies affect only users within the current domain.
  - Policies are not enforced when applied to OUs, the domain, or other group types.
    - To apply a granular policy to all users within an OU, create a global security group that contains all OU members. Apply the policy to the group.
    - When you move a user account to a different OU, remember to also change the group membership so that the granular password policy no longer applies.
- The **msDS-PasswordSettingsPrecedence** property is used to resolve conflicts if multiple PSOs are applied to a group.
  - If a PSO has been applied directly to a user, that PSO is in effect, regardless of the precedence value.
  - If multiple PSOs are applied to global security groups of which the user is a member, the PSO with the lowest precedence value will be in effect.
  - If two or more PSOs are applied to a user or if two or more PSOs are applied to groups with the same precedence value, the PSO with the lowest identifier will be in effect.

To use ADSI Edit to create a PSO, complete the following:

1. Open ADSI Edit and connect to the default naming context for the domain.
2. Browse to **System** > **Password Settings Container**.
3. Right-click the container and select **New** > **Object**.
4. Complete the wizard steps to create the password policy by defining the password and account lockout parameters.
5. After you create the PSO, edit its properties to identify the users or global security groups to which the PSO applies.
6. If you applied the PSO to groups, add user accounts to groups as necessary.

In Windows Server 2012 and Windows Server 2016, granular passwords can also be managed using the Active Directory Administrative Center. To accomplish this, complete the following:

1. In Server Manager, select **Tools** > **Active Directory Administrative Center**.
2. Expand your domain.
3. Browse to **System** > **Password Settings Container**.
4. In the Password Settings container, you can create, edit, and delete PSOs.