Configuring Password Policies with Windows Server 2012 Password Settings objects (PSOs)

Windows Server 2012 introduces fine grained password policies with GUI for management. This is huge improvement since Windows Server 2003 only allowed one password policy per domain. Windows Server 2012 Active Directory Administrative Center allows administrators to manage and create new password polices. Now administrators can configure different password polices for different users and groups.

How to configure Password Polices in Windows Server 2012

1. Open Active Directory Administrative Center.

2. Browse to Domain(local) > System > Password Settings Container.

3. Click "New" > "Password Settings" on the right pane.
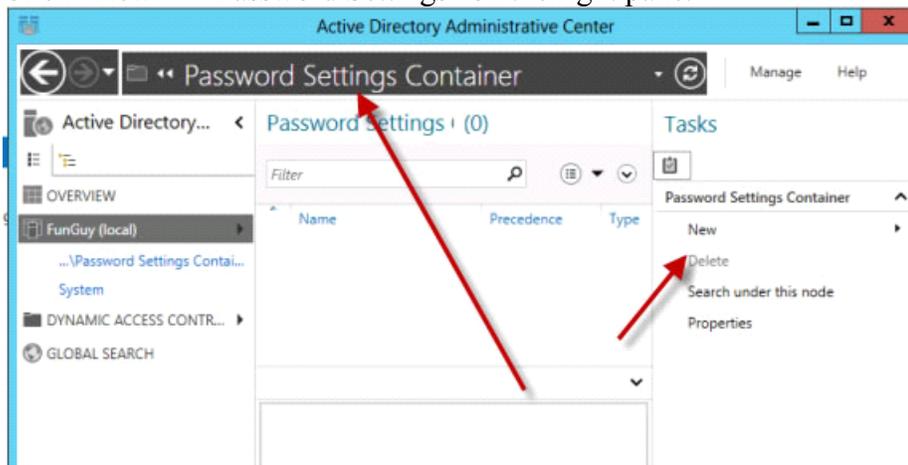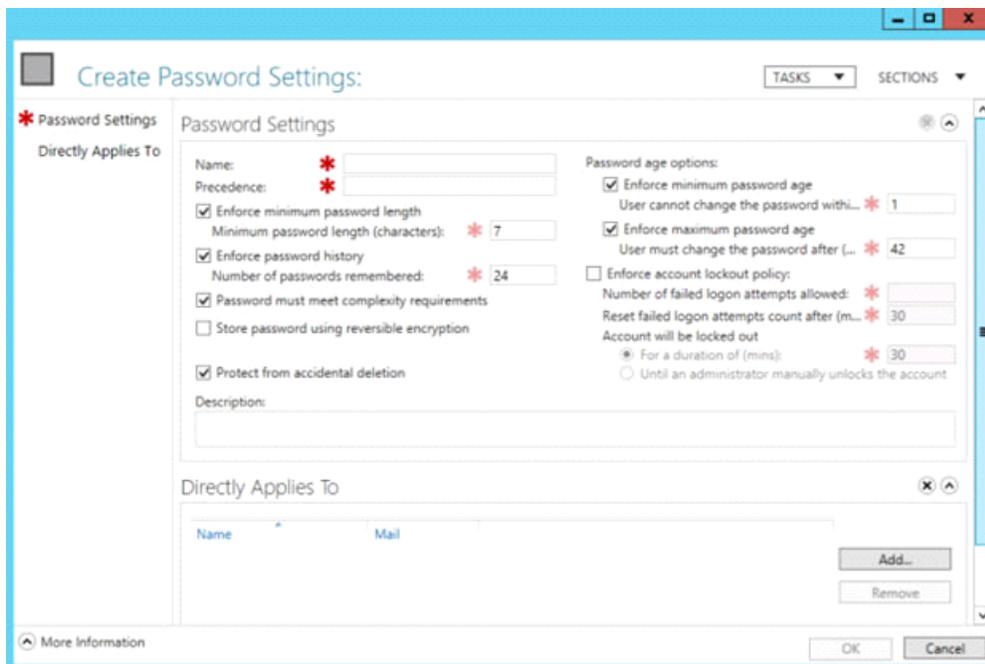
1. From here you can create a new policy and select which active directory group you want

    applied to.

2. Below settings are configurable:

    - Enforce minimum password length

- Minimum Password length

- Enforce Password history

- Number of passwords remembered

- Password must meet complexity requirements

- Store password using reversible encryption

- Protect from accidental deletion

- Enforce minimum password age

- User cannot change the password within x days

- Enforce maximum password age

- User must change the password after x days

- Enforce account lockout policy

- Number of failed logon attempts allowed

- Reset failed logon attempts count after x days

- Account will be locked out for a duration of