* Update the Default-First-Site-Name to SiteName: example (HQ-Office)  
  Active Directory Sites and Services, rename
* Configure Domain Password and Lockout Policy (GPO)  
  The best practice is edit the Default Domain Policy GPO to define the password, account lockout, and kerberos policies for the domain, and nothing else.  
  Additionally, do not define password, account lockout, or kerberos policies for the domain in any other GPO.
* For Additional password policy set fine-grained password policy (password setting object) PSO  
  PSO are applied to users or groups.  
  Create a new Password Settings from AD Administrator Center (ADAC) System/Password Settings Container  
  PSO with the highest precedence (closest to 1) take effect  
  If one of more PSOs are linked directly to the user, PSOs linked to group are ignored.  
  *msDS-ResultantPSO* : displays PSO that will affect a user  
  To view *msDS-ResultantPSO* : On the Attribute Editor tab Filter and ensure that Constructed attribute is selected
* Add Active Directory Schema Snap-In: Open an elevated command prompt: regsvr32 schmmgmt.dll
* STIG Password Policy

|  |  |
| --- | --- |
| Account Policies/Password Policy |  |
| Enforce password history | 24 passwords remembered |
| Maximum password age | 60 days |
| Minimum password age | 1 days |
| Minimum password length | 14 characters |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |
|  |  |
| Account Policies/Account Lockout Policy |  |
| Account lockout duration | 15 minutes |
| Account lockout threshold | 3 invalid logon attempts |