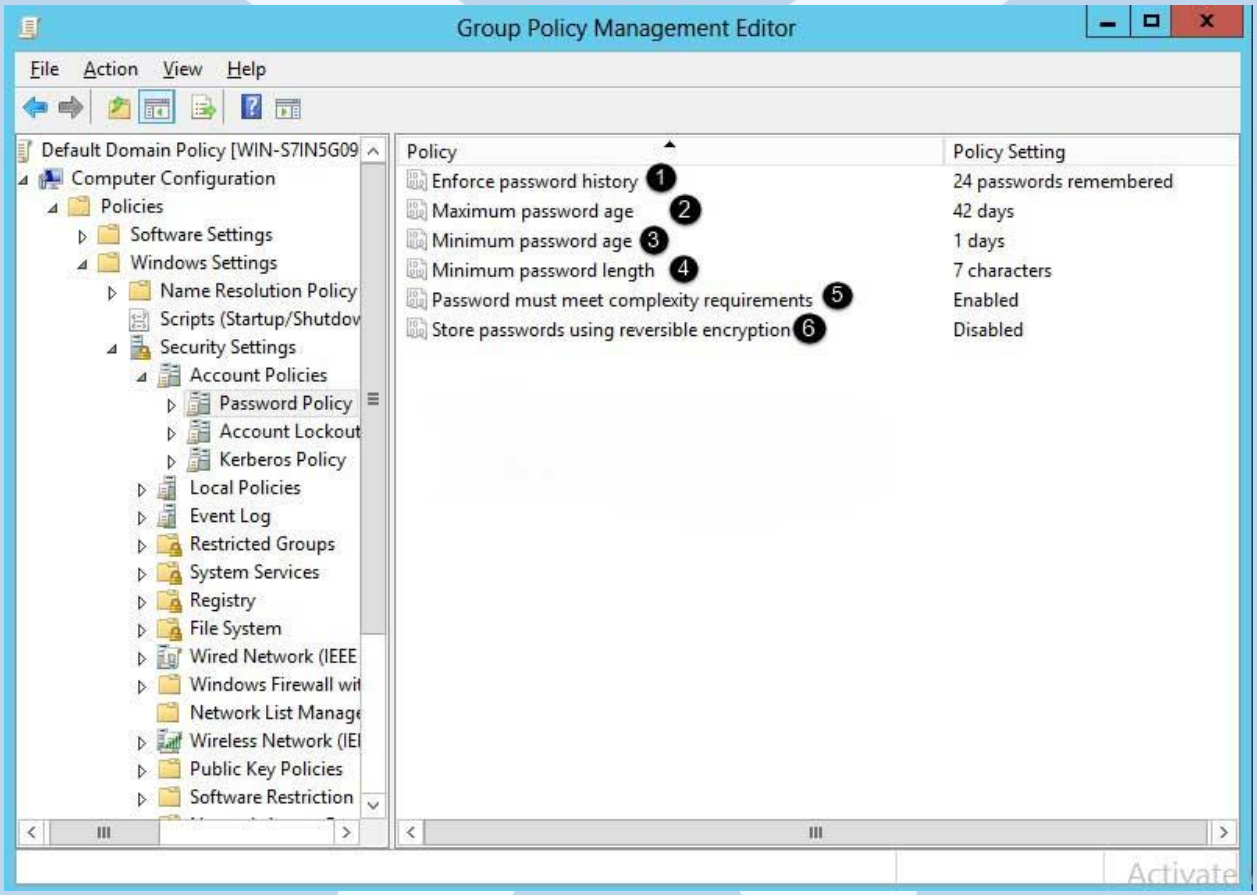
ایجاد Policy برای مدیریت رمز عبورAccount

۱- از منوی start پنجره run را انتخاب کرده و عبارت gpmcmsc یا gpedit.msc را تایپ کنید تا به پنجره group policy managementهدایت شوید.

۲- بر روی Default Domain Policy راست کلیک و گزینه Edit را انتخاب نمایید.

۳- در کنسول GPME وارد مسیر زیر شوید:

Computer Configuration \Policies\ Windows Setting \ Security Settings \Account Policy password policies



آیتم های زیرشاخه Password Policy عبارتند از:

1 Enforce Password History با استفاده از این گزینه می توان مشخص کرد که کاربر تا چه تعداد رمز عبور واردشده از گذشته را حق ندارد انتخاب کند.

2 Maximum Password Age: حداکثر بعد از گذشت چه مدت‌زمانی کاربر باید رمز عبورش را عوض کند. که در اینجا ۴۲ روز است.

3 Minimum Password Age حداقل مدت‌زمانی که کاربر اجازه تغییر رمز عبورش را دارد. که در اینجا یک روز است.

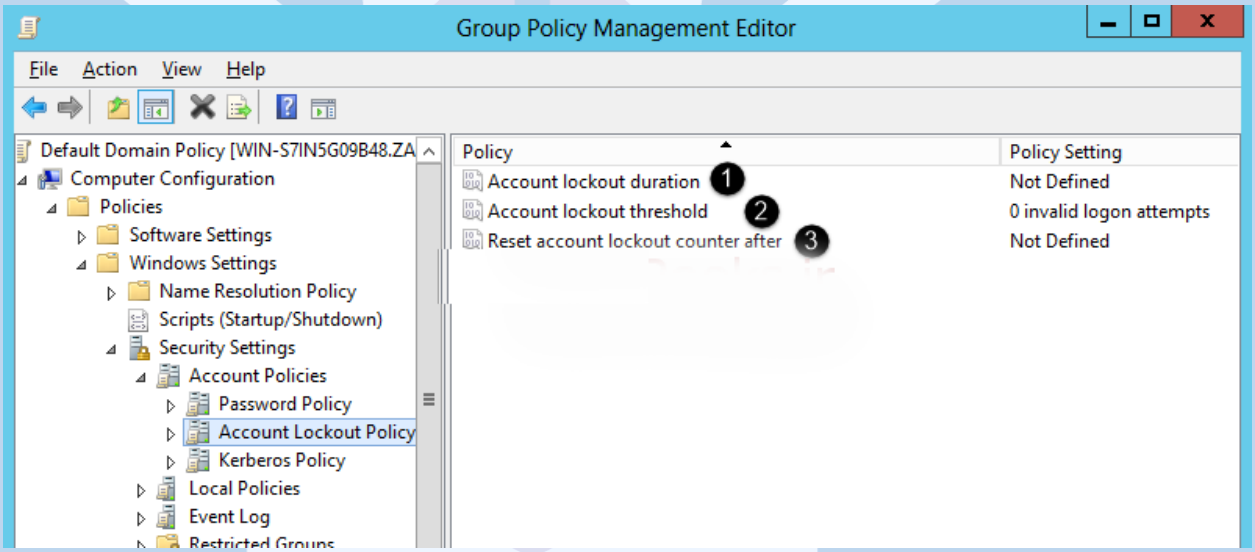
4 Minimum Password Length حداقل طول رمز عبور را مشخص می‌کند که در اینجا ۷ کاراکتر است.

5 Password must meet Complexity Requirements مشخص میکند که رمز عبور باید پیچیده باشد. رمز عبوری پیچیده است که سه شرط از چهار مورد زیر را داشته باشد.

- حروف کوچک
- حروف بزرگ
- کاراکترهای خاص
- عدد

6 Store Password Using Reversible Encryption با فعالسازی این گزینه رمز عبور به صورت متن معمولی ذخیره خواهد شد. توصیه می‌شود به‌هیچ‌وجه این گزینه را فعال نکنید.

۱. در زیرشاخه Account Lockout policis با موارد زیر روبرو خواهید شد:



آموزش ویندوز سرور ۲۰۱۲ تنظیمات مربوط به پسورد با استفاده از Group Policy

1 Account to lockout Duration با استفاده از این گزینه میتوان مشخص کرد که Account برای چه مدتی قفل شود.

2 Account to Lockout Threshold با استفاده از این گزینه میتوان مشخص کرد که بعد از چند بار عملیات Logon ناموفق Account قفل شود.

3 Reset Account Lockout Counter after با استفاده از این گزینه میتوان مشخص کرد که ویندوز بعد از گذشت چه مدت‌زمانی تعداد دفعات ورود اشتباه را نادیده میگیرد (قبل از اینکه حساب قفل شود).