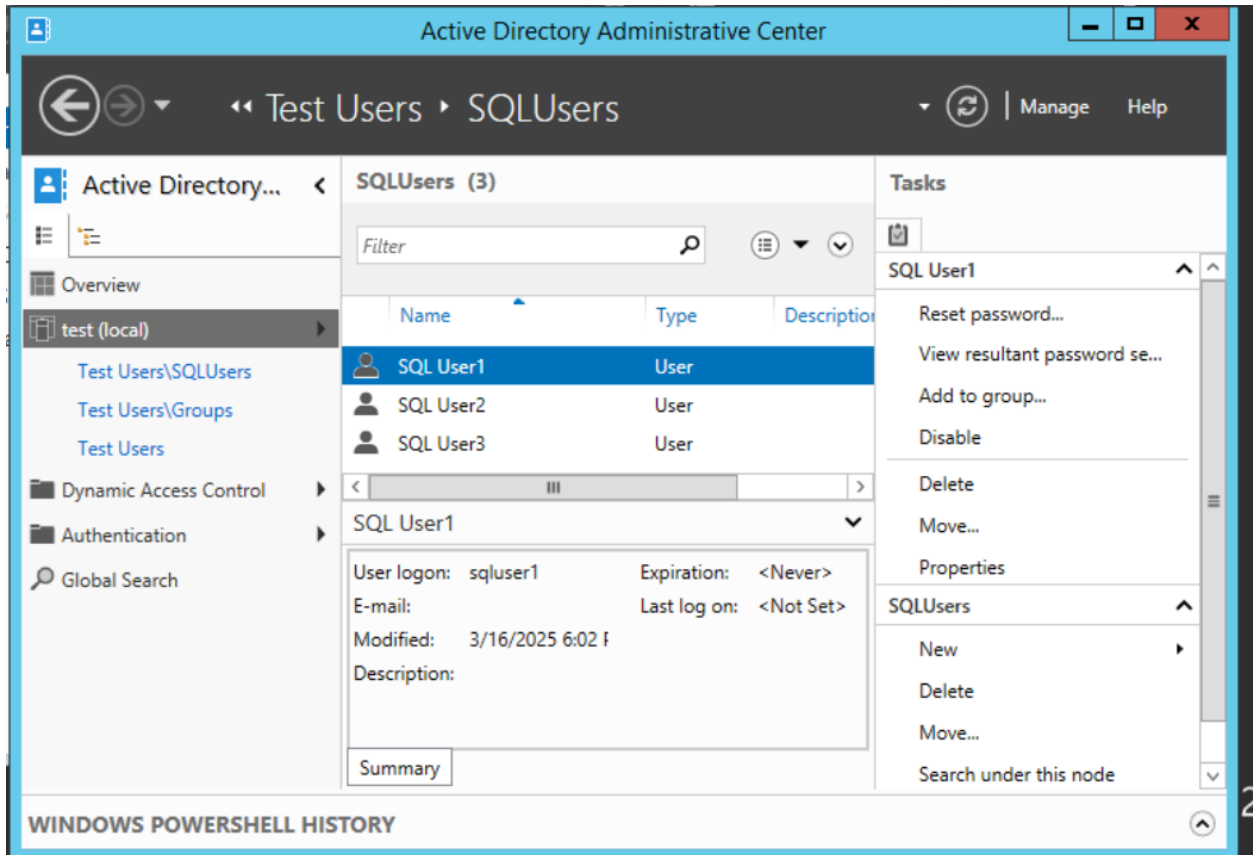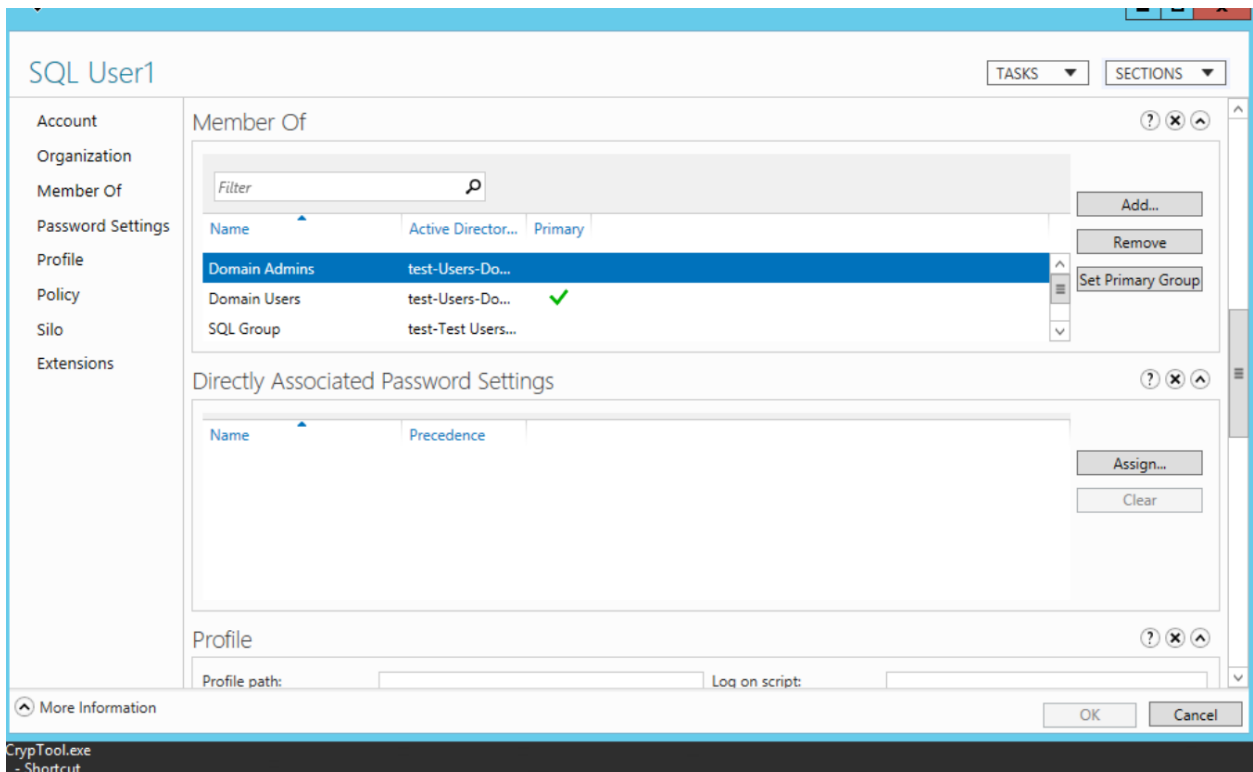# Homework 4 – Active Directory and Group Policy Objects

- (**Task 1**) Show in a screenshot that the three domain users (sqluser1, sqluser2, sqluser3) are created in **SQLUsers** OU. Also show in a screenshot that **sqlgroup** is created in the **Groups** OU.


- (**Task 2**) Go to sqluser1 properties and show in a screenshot that sqluser1 is a member of **Domain Admins** and **sqlgroup**.

- (**Task 3**) Run the following query on SQL Server and show in a screenshot that you indeed logged-on with sqluser1.
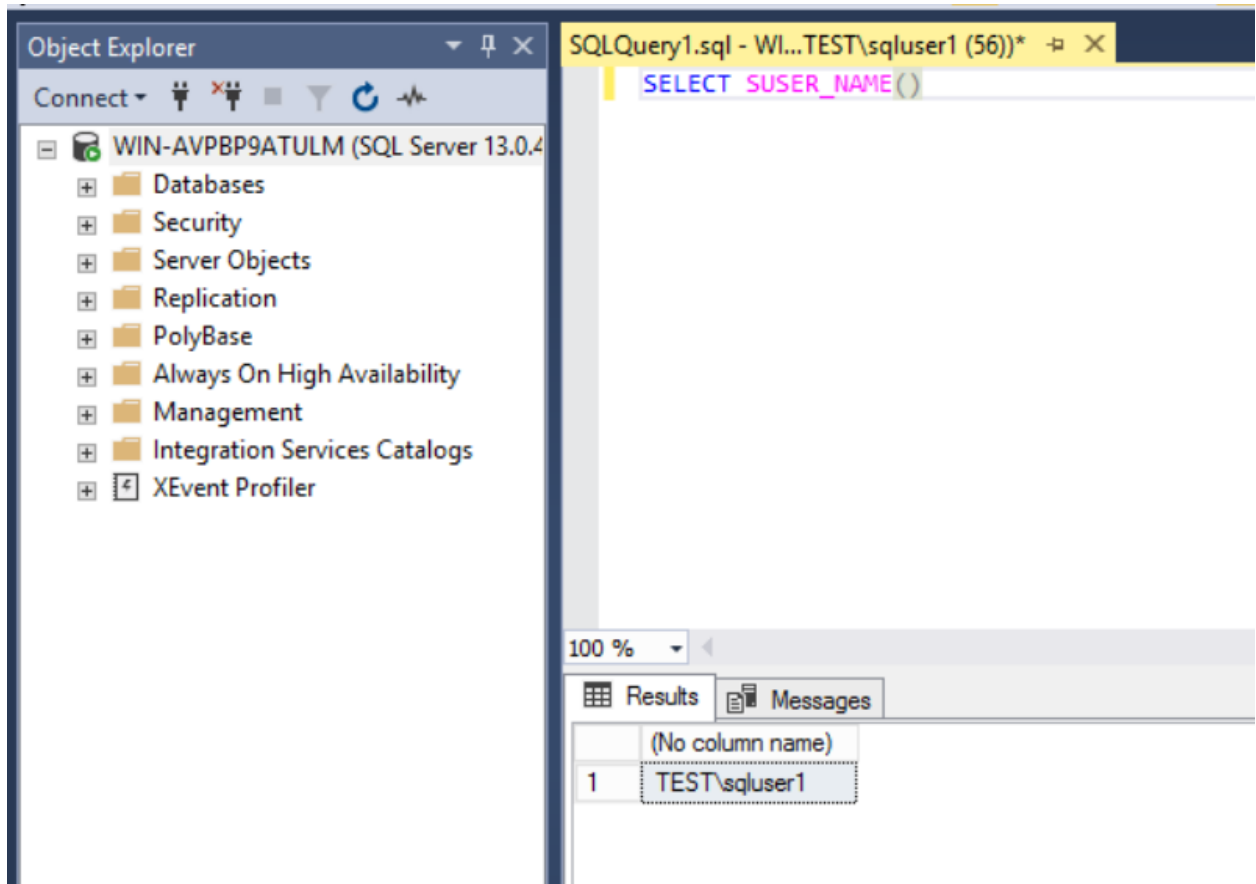
- (**Task 4**) Logon to SQL Server. Create a login "**Cardinal1**". Select **SQL Server authentication**. Enter the password "1234567", and show in a screenshot that the login <u>cannot</u> be created. Explain why?
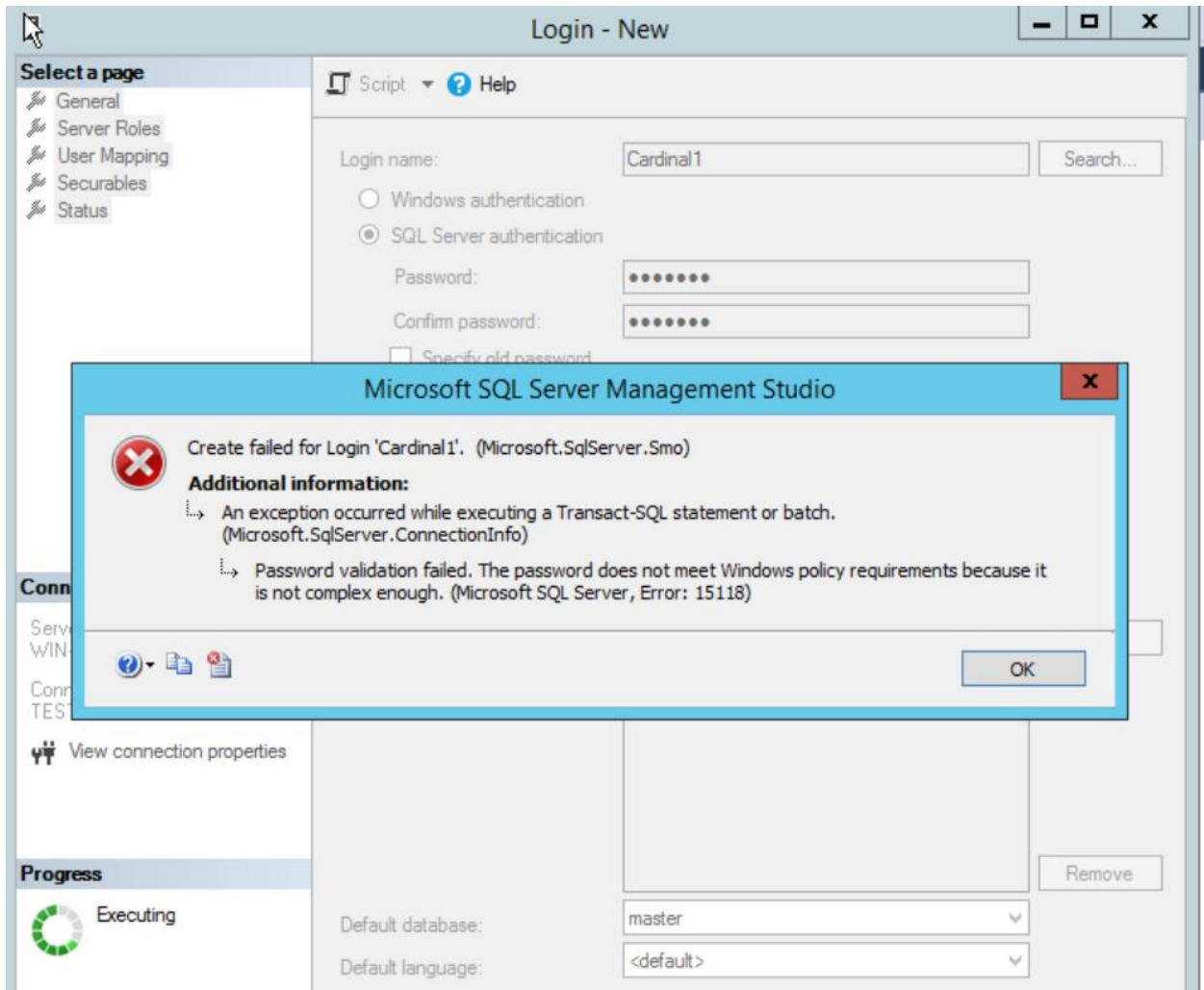
The log in failed due to the password not meeting the complexity requirements set in Active Directory

- (**Task 5**) Create a login "**Cardinal1**". Select **SQL Server authentication**. Enter the password "1234567", and show in a screenshot that the login is created. Explain why this was possible. Explain also the relationship between the GPO and the SQL Server password policy.
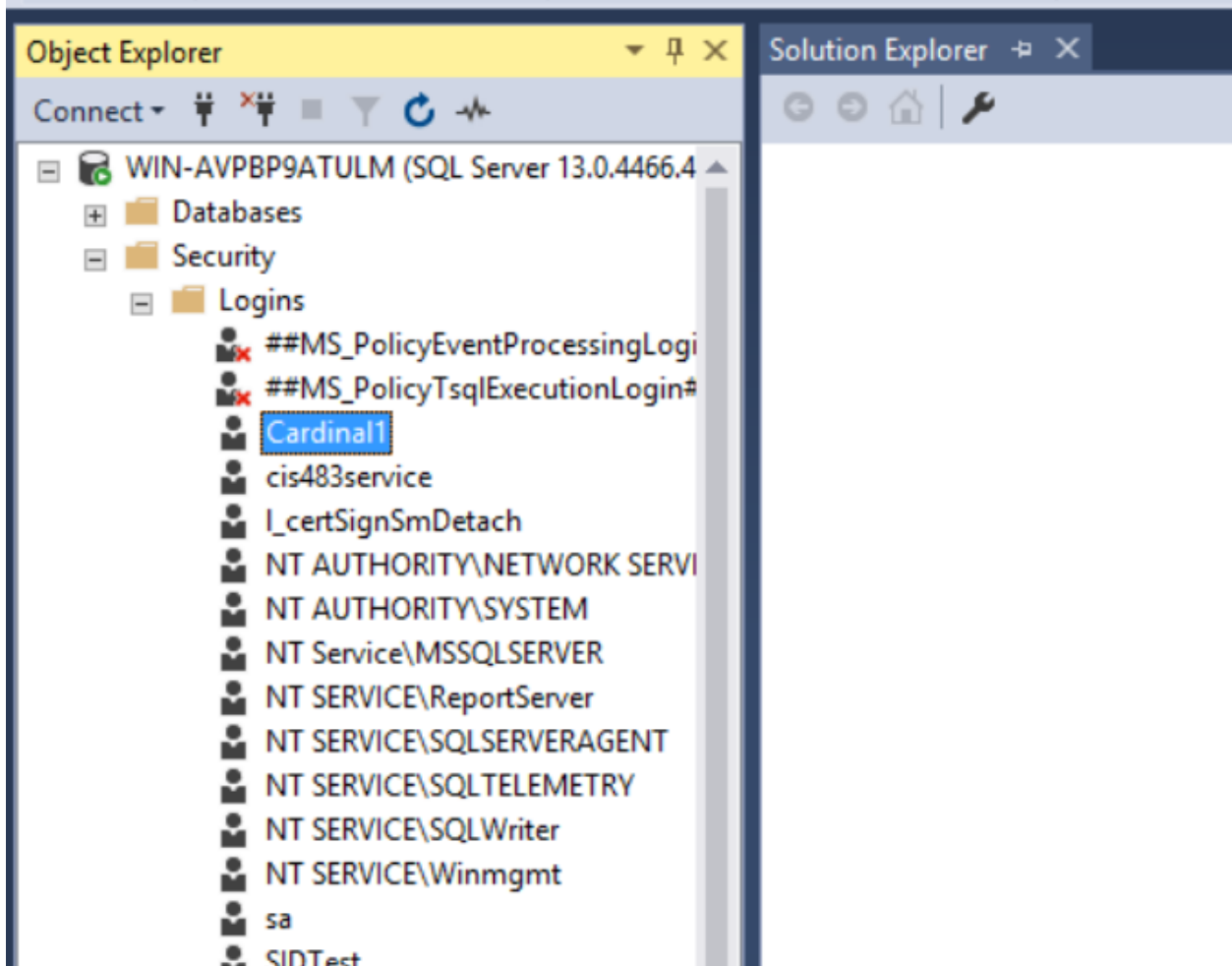
This was possible due to disabling the password complexity requirements in the group policy settings. The GPO manages the password requirements for all Windows logins including SQL Server.

- (**Task 6**) Create a new AD account using the command **New-ADUser** explained on pp 12-13. Show in a screenshot that the account is indeed created (example below). Also, attach a screenshot that displays the PowerShell execution.

Name	Type	Description
Jrew Simpson	User	
SQL User1	User	
SQL User2	User	
SQL User3	User	

Jrew Simpson (Disabled)

User logon: J.Si
E-mail:
Modified: 3/16/2025 7:51 PM
Description:

Expiration: <Never>
Last log on: <Not Set>

```
PS C:\Users\Administrator> New-ADUser `
>> -Name "Jrew Simpson" `
>> -GivenName "Jrew" `
>> -Surname "Simpson" `
>> -SamAccountName "J.si" `
>> -UserPrincipalName "J.Si@test.ad" `
>> -Path "OU=SQLUsers,OU=Test Users,DC=test,DC=a" `
```