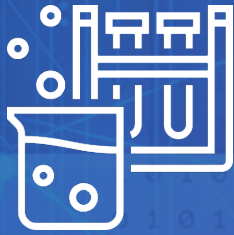


# Lab Assignment



Cybersecurity Professional Program

Microsoft Security

## Microsoft Security Policies & Authentication

**MS-10-L2**

**User Password Policies**

---

## Lab Objective

Learn how Active Directory Group Policy Management can configure password policies for users in the domain.

## Lab Mission

Set a strong password policy for the entire domain and configure the policy to handle user lockouts.

## Lab Duration

20–40 minutes

## Requirements

- Knowledge of the ADUC structure

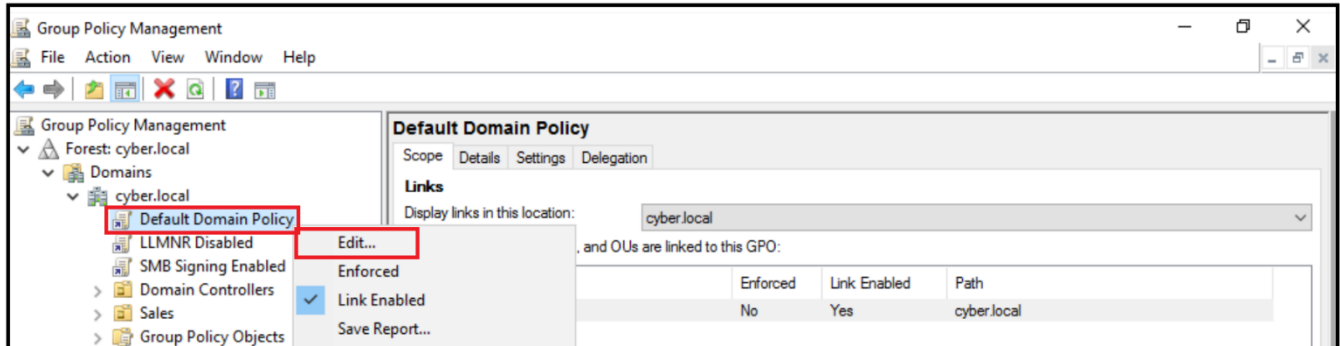
## Resources

- Environment & Tools
  - VirtualBox
    - Windows Server 2016 (DC)
    - Windows 10 (client)

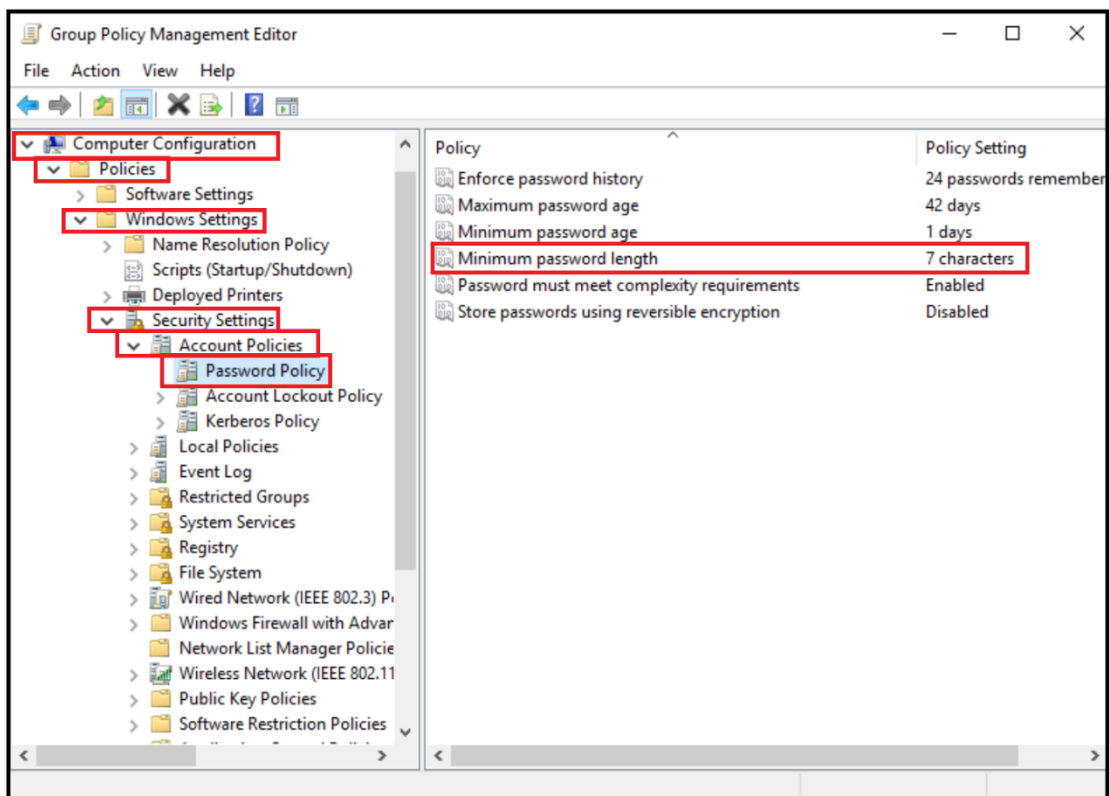
## Lab Task 1: Create and Apply Password Group Policy

Use Group Policy Management to create a password policy for all domain users.

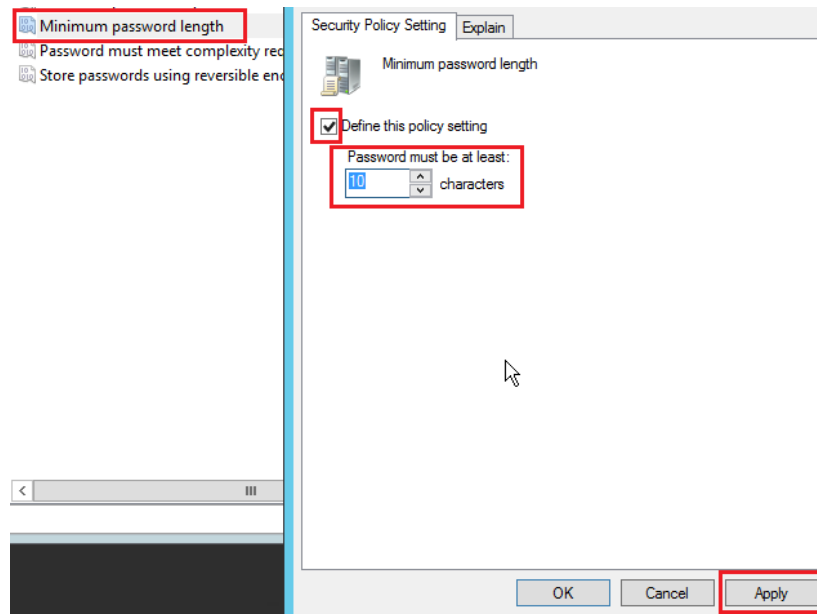
- 1 On Server1, open Group Policy Management in **Forest: Cyber.local > Domains > Cyber.local**, then right-click **Default Domain Policy**, and select **"Edit..."**



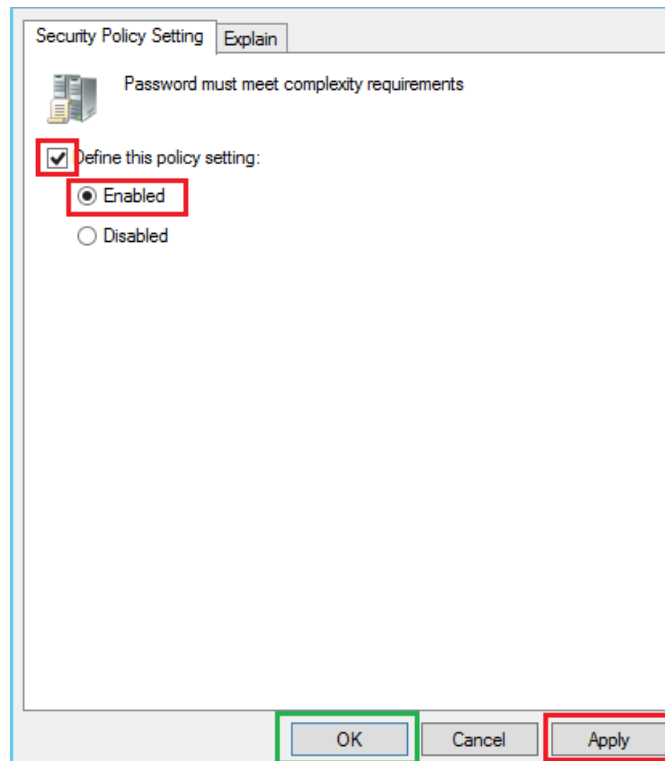
- 2 Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy > Minimum password length**



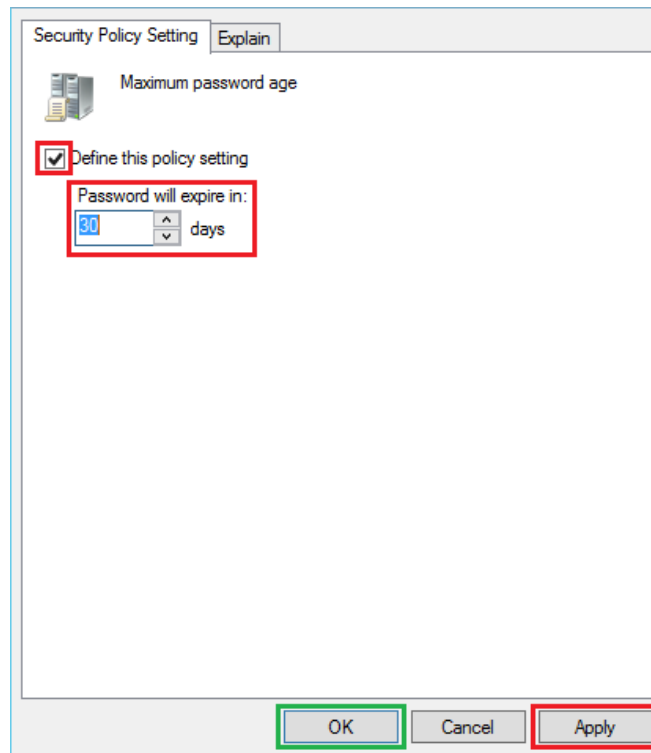
- 3 Double-click **Minimum password length**, select **Define this policy setting** and set the number of characters to 10.



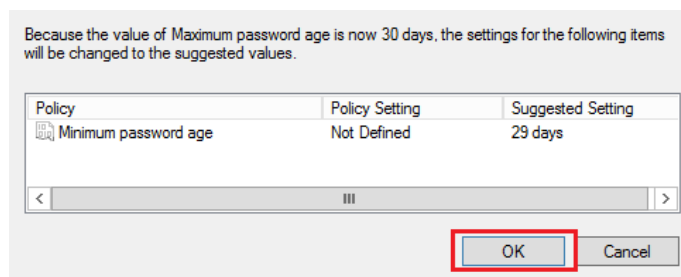
- 4 Go to **Password must meet complexity requirements** and verify that the policy is enabled. If not, select **Define this policy setting**, select **Enabled**, click **Apply**, and click **OK**.



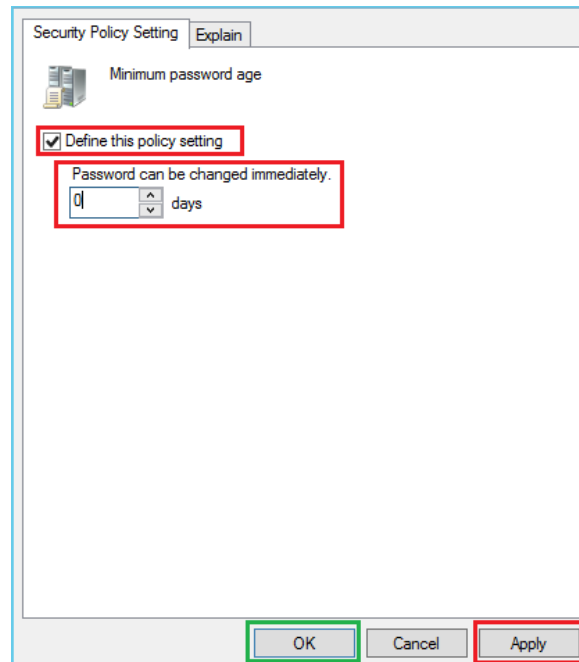
- 5 To force a password change each month, double-click **Maximum password age**, select **Define this policy setting** and set the Password to 30 days. Then, click **Apply** and **OK**.



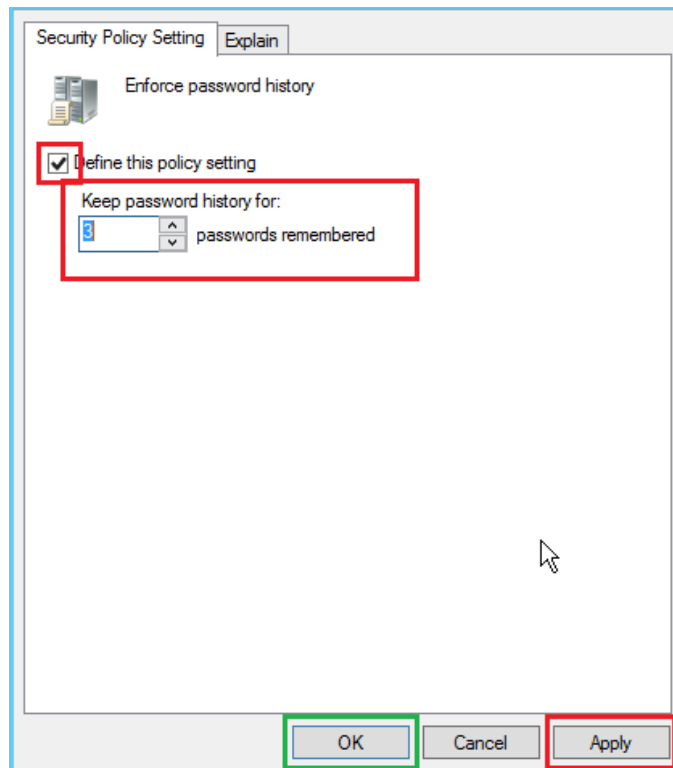
- 6 In the window with the **Minimum password age** option, click **OK**. This setting will determine how long users must keep a password before changing it.



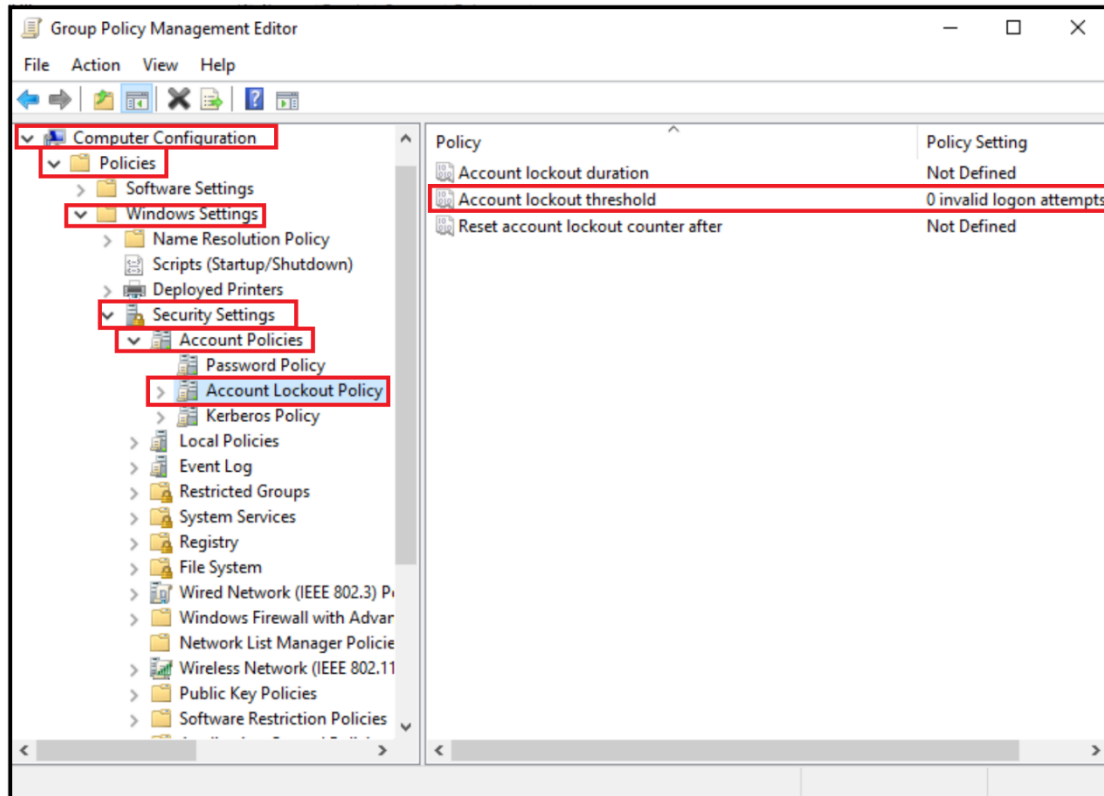
- 7 Because we want to test our password policy configuration later in the lab, we need to set the **Minimum password age** to zero. Double-click **Minimum password age** properties, select **Define this policy setting** and set the value to 0 days. Then, click **Apply** and **OK**.



- 8 Double-click **Enforce password history**, select **Define this policy setting** and change the number to 3. Then, click **Apply** and **OK**.

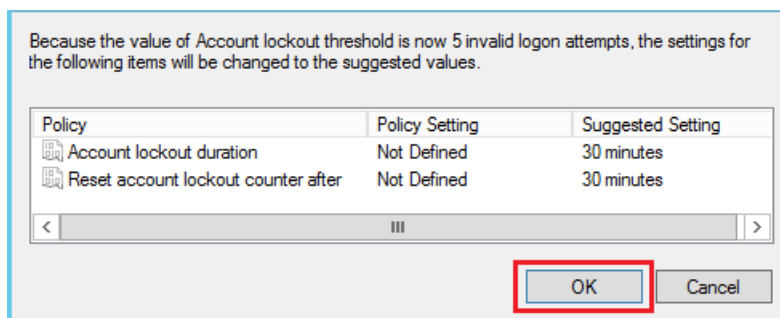
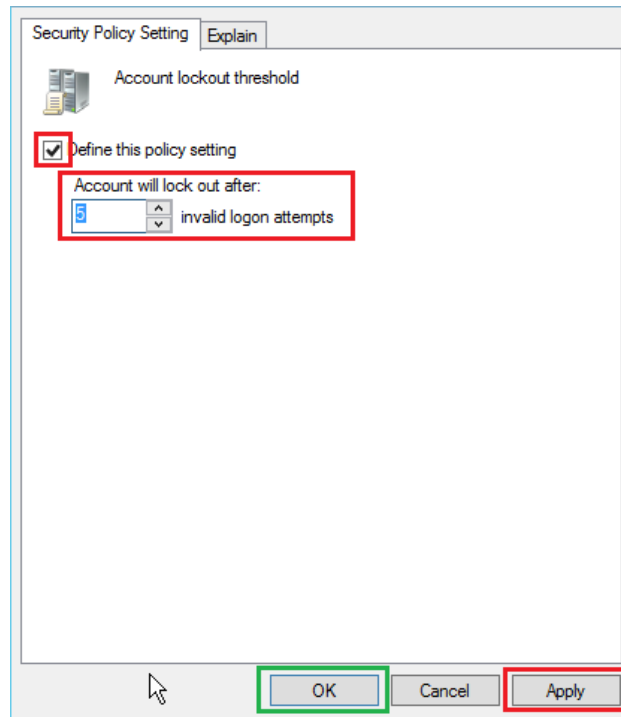


- 9 Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy > Account lockout threshold**

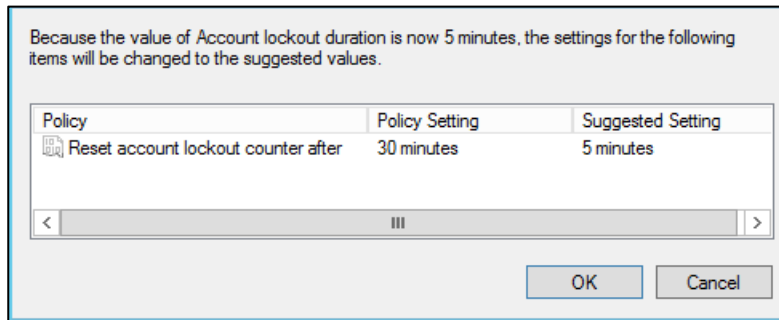
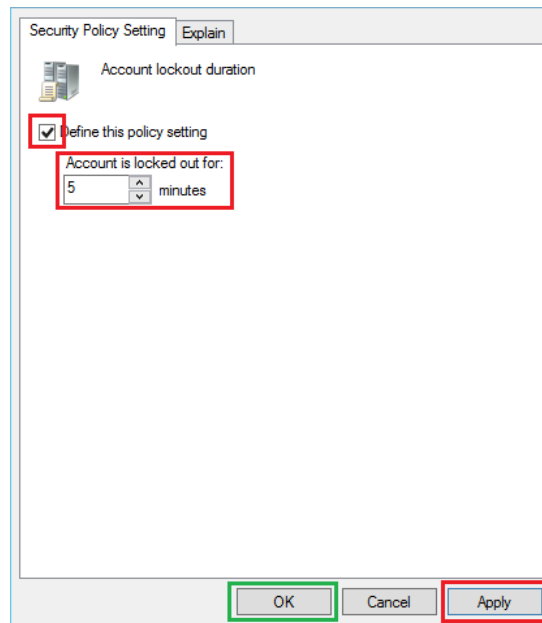




- 10** Configure the account lockout policy with an account lockout threshold of five invalid logon attempts. A window will appear with a request to change the settings for two other account lockout policies. Accept the changes for now by clicking **Apply** and **OK**.



- 11** Double-click **Account lockout duration** and change the value to 5 minutes. Then, click **Apply** and **OK**. In the message that appears, click **OK**.



## Lab Task 2: Verify Password Policies

Check if the group policies were configured correctly and applied.

- 1 Log into the Client10 VM with a regular user and run **gpupdate /force** from CMD.

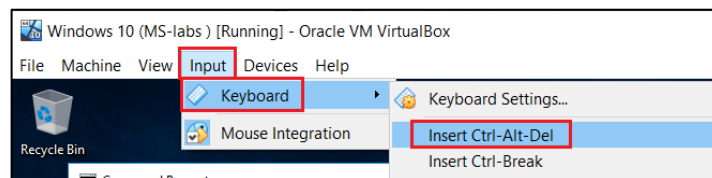
```
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Management>gpupdate /force
Updating policy...

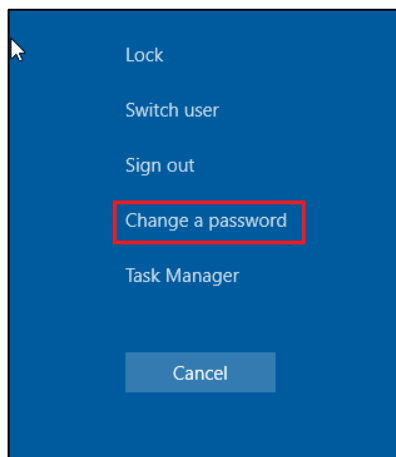
Computer Policy update has completed successfully.
User Policy update has completed successfully.

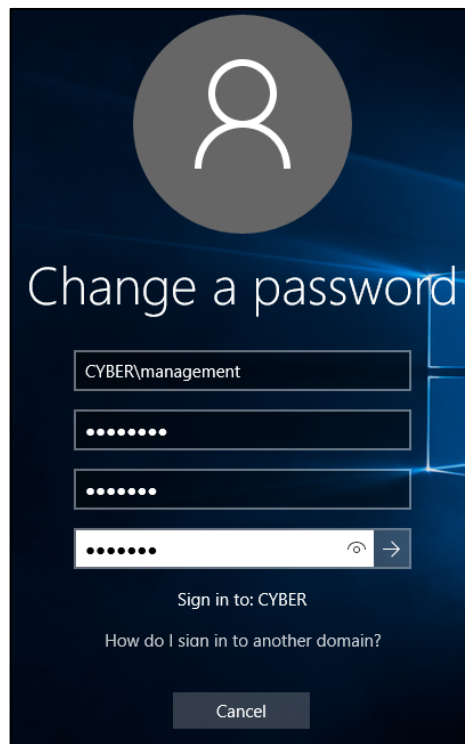
C:\Users\Management>
```

- 2 Press **Alt+Ctrl+Del** to get the option to change the Password. Note that an easy way to input **Alt+Ctrl+Del** on a VM is through the **Input** tab of the VM toolbar.

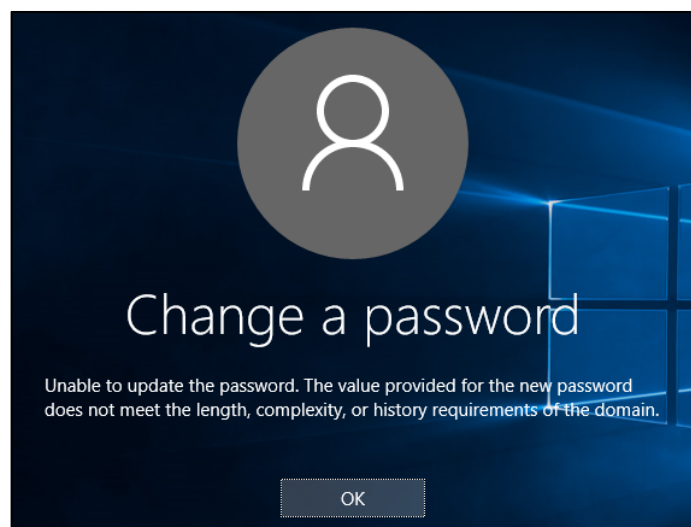


- 3 In the next window, select **Change a password** and change the Password to **Abc123!**, which does not conform with the password policy.

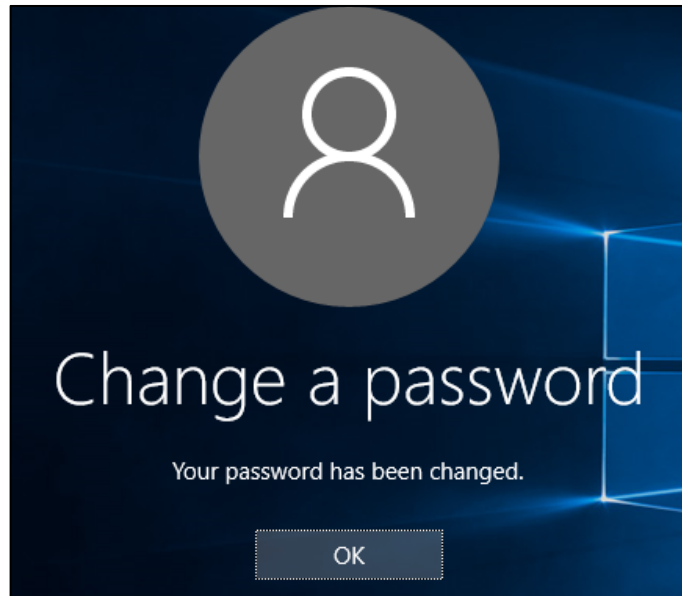




- 4 Verify the Password does not change because the one proposed does not meet the requirements. The following error message should appear:



- 5 Enter a password that matches the password policy configuration. Repeat steps 1 and 2, but instead, use **Presto123!** as the new Password. The Password should be changed.



- 6 Log out of the Windows 10 user and force an account lockout by inputting five incorrect passwords. You should receive the following error:

