

# Hands-on Lab: Enforce Strong Password Policies

Estimated time needed: **30** minutes

## About This Lab

In this lab, we will use Kaspersky's password checker to learn how vulnerable our passwords are. Using the Local Group Policy Editor, we will also learn how to enforce strong password policies within the Microsoft Windows operating system.

In this hands-on lab, you will:

- Check password strength.
- Review Windows Local Group Policy Editor.
- Configure password policies.

## Important Notices about This Lab

### About Lab Sessions

Lab sessions are not persisted. This means that every time you connect to this lab, a new environment is created for you. Any data or files you saved in a previous session are no longer available. To avoid losing your data, plan to complete these tasks in a single session.

### About the Lab Instructions and Solutions

Microsoft Windows operating system features can vary based on the Windows edition. If completing these exercises on your machine, your navigation and solutions may differ from what's presented in this lab.

## Exercise 1: Check Password Strength

In this exercise, we will use Kaspersky's password checker to test password strength. This tool will show you how safe a password is. It considers how long it would take an attacker to brute-force your password. It also compares your password to a database of leaked passwords that any attacker could have access to.

1. Click the Chrome icon to open the Chrome browser. Type **password.kaspersky.com** into the address bar.
2. First, we will check a password created by a user who was required to make a password using letters and numbers. The user used his pet's name and his year of birth so he could remember the password. Click the **Test your password** box and type **fidol973**. Press **Enter**. Kaspersky will provide feedback on the strength of the tested password.
3. Next, we will check a password created by a user who was required to create an 8-digit password using a capital letter, at least one number, and at least one symbol. Click the **Test your password** box and type **Fido1973!**. Kaspersky will provide feedback on the strength of the tested password.
4. Lastly, we will test a password created by a user who was required to create a 12-digit password using a capital letter, at least one number, and at least one symbol. Instead of using common words, they used the first letter of each word in a phrase they would remember. **Mary had 1 little lamb it's fleece was white as snow !** Click the **Test your password** box and type **Mh1llifwwas!**. Kaspersky will provide feedback on the strength of the tested password.

## Exercise 2: Review Windows Local Group Policy Editor

Now we will learn how to enforce strong password policies for Windows users using the **Local Group Policy Editor**. The Local Group Policy Editor is a Microsoft Management Console (MMC) snap-in. It is used to configure and monitor Group Policies and user settings.

1. Type **Command Prompt** on the search bar and click on it.
2. Type **gpedit** at the command prompt and press **Enter**.
3. This will open the **Local Group Policy Editor**. Here you will see that the Local Computer Policy is broken into two configurations:
  - **Computer Configuration**: This holds settings that are applied to the computer when it is started.
  - **User Configuration**: This holds settings that are applied to users when they sign into the computer.
4. Click **Computer Configuration**. Click **Windows Settings**. Select **Security Settings**. On the right panel you will see several policy types along with a description of the types of policies included in that section. Click the **Account Policies** folder.
5. Next, under the Account Policies folder, click the **Password Policy** folder. On the right pane, you will see five policies:
  - **\*\*Enforce password history\*\***: This policy determines how many unique passwords need to be used before an old password can be reused.

- **\*\*Maximum password age\*\***: This policy determines how many days a password can be used before the system requires a password change.
- **\*\*Minimum password age\*\***: This policy determines how many days a password must be used before the system requires a change.
- **\*\*Minimum password length\*\***: This policy determines the fewest number of characters required in a password. Microsoft recommends that passwords be at least 8 characters long.
- **\*\*Minimum password length audit\*\***: This policy is designed for organizations who want to track user password length.
- **\*\*Password must meet complexity requirements\*\***: This policy indicates that passwords must meet Windows Security requirements.
- **\*\*Store passwords using reversible encryption\*\***: This policy is specific to applications that use passwords.

## Exercise 3: Configure Password Policies

In this lab, we will configure the following settings based on Microsoft recommendations:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length

1. Double-click **Enforce password history**.
2. Microsoft recommends that **Enforce password history** be set to 24. Type **24** into the box and click **OK**.
3. Double-click **Maximum password age**.
4. Microsoft recommends that passwords should be set to expire somewhere between 30 and 90 days. Type **60** into the box and click **OK**.
5. Double-click **Minimum password age**.
6. Microsoft recommends that users should be required to wait at least one day before they can change their password. Type **1** into the box and click **OK**.

7. Double-click **Minimum password length**.

8. Microsoft recommends that passwords be at least 8 characters and no more than 14 characters. Type **12** into the box and click **OK**.

9. Note that all of your recent changes will appear under the **Security Setting** preview on the right pane.

## Practice Exercises

### 1. Problem: Create a Complex Password

You have been asked to create a password for a new account. The website requires that your password have at least:

- Eight digits.
- One capital letter.
- One number.

Create a password that you can remember that will take at least one week to crack. Use the Kaspersky Password Checker at **password.kaspersky.com** to ensure password strength.

- ▶ Click here for a hint.
- ▶ Click here for the solution.

### 2. Problem: Enable Password Policies

If other, more complex policies are not set, Microsoft recommends that **Password must meet complexity requirements** is set to **Enabled**. Open the **Password must meet complexity requirements** policy. Enable the policy. View the **Explain** tab to see which requirements are set when this is enabled.

- ▶ Click here for a hint.
- ▶ Click here for the solution.

**Congratulations! You have completed this lab and are ready for the next topic.**

## Authors

Dee Dee Collette

Copyright (c) 2022 IBM Corporation. All rights reserved.