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.

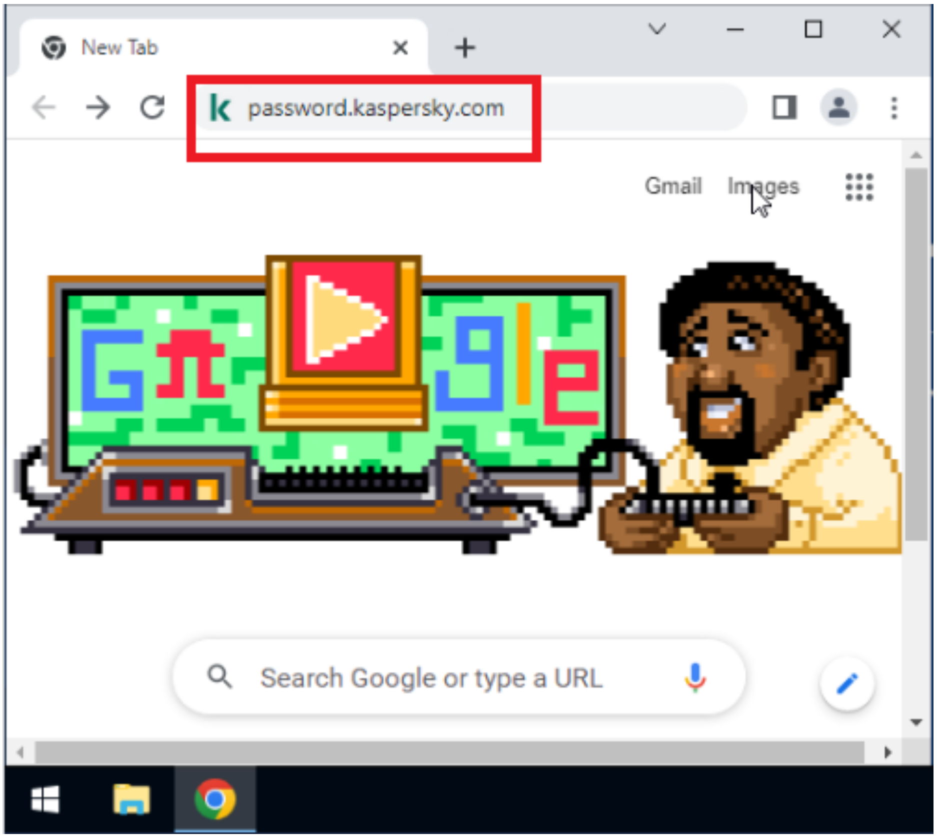
About the Lab Instructions and Solutions

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.

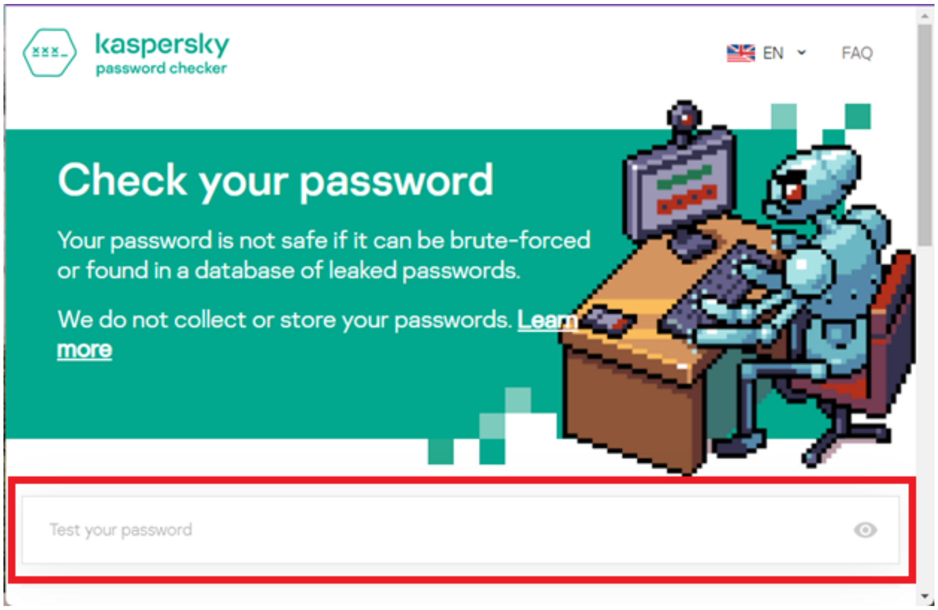
Exercise 1: Check Password Strength

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 **fido1973**. Press **Enter**. Kaspersky will provide feedback on the strength of the tested password.

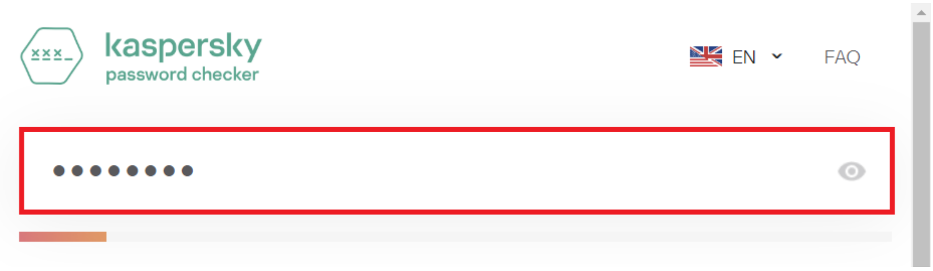


Check your password

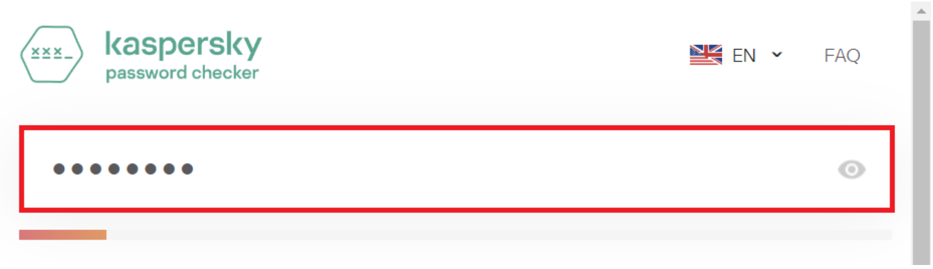
Your password is not safe if it can be brute-forced or found in a database of leaked passwords.

We do not collect or store your passwords. Learn more

Test your password



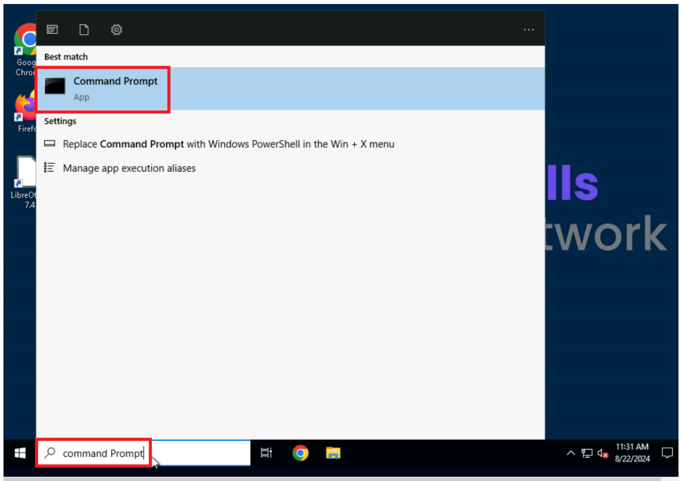
3. Next, we will check a password created by a user who was required to create an 8-digit password using a capital letter, at least one number, and at least one symbol. Click the **Test your password** box and type **Fido1973!**. Kaspersky will provide feedback on the strength of the tested password.
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. **M**ary **h**ad **1** **l**ittle **l**amb **i**t's **f**leece **w**as **w**hite **a**s **s**now **!** 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

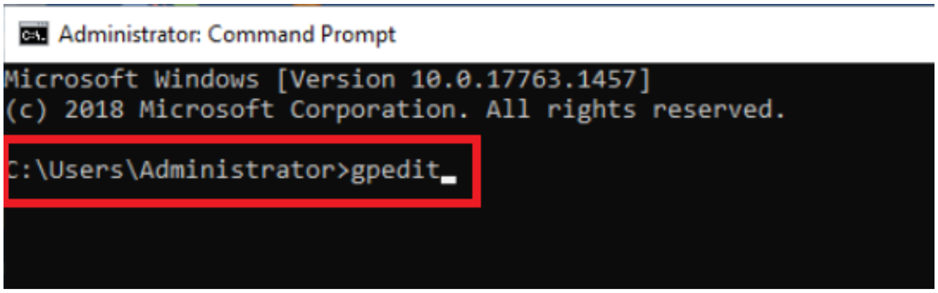
Now we will learn how to enforce strong password policies for Windows users using the **Local Group Policy Editor**. The Local Group Policy Editor is a Microsoft Management Console (MMC) snap-in. It is used to configure and monitor Group Policies and user settings.

1. Type **Command Prompt** on the search bar and click on it.



Best match
Command Prompt
App
Settings
Replace Command Prompt with Windows PowerShell in the Win + X menu
Manage app execution aliases
command Prompt
11:31 AM
8/22/2024

2. Type **gpedit** at the command prompt and press **Enter***.



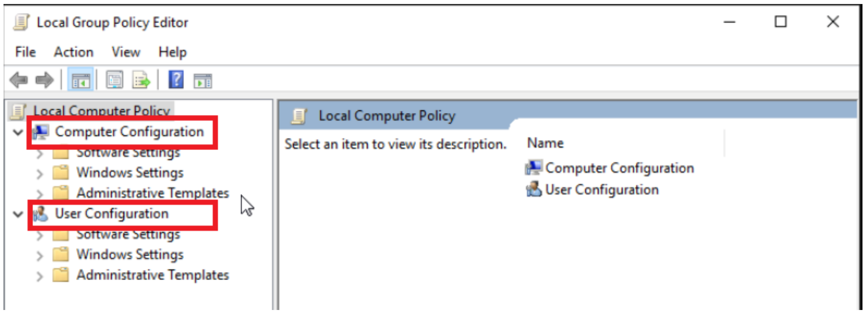
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpedit_
```

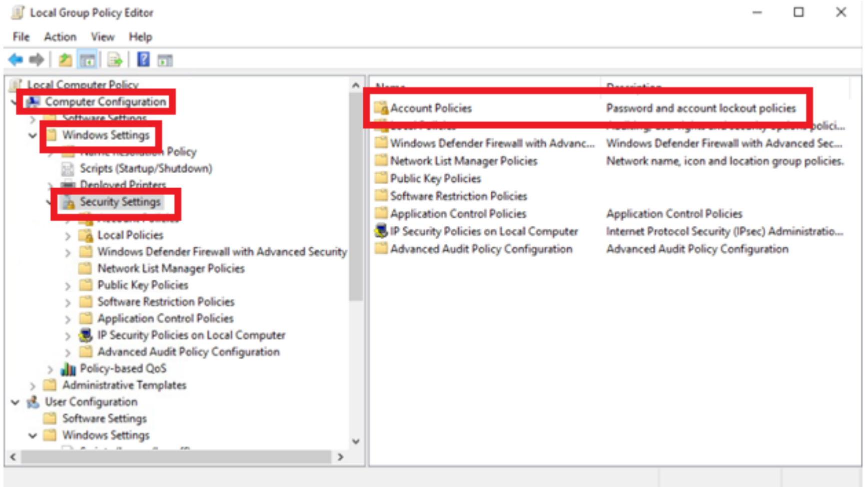
3. This will open the **Local Group Policy Editor**. Here you will see that the Local Computer Policy is broken into two configurations:

- **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.



Select an item to view its description.

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.



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

5. Next, under the Account Policies folder, click the **Password Policy** folder. On the right pane, you will see five policies:

```
1. 1
1. **Enforce password history**: This policy determines how many unique passwords need to be used before an old password can be reused. Microsoft recommends this be set to 24.
```

Copied!

```
1. 1
1. **Maximum password age**: This policy determines how many days a password can be used before the system requires a password change. Microsoft recommends that this be set somewhere between 30 and 90 days.
```

Copied!

```
1. 1
1. **Minimum password age**: This policy determines how many days a password must be used before the system requires a change. Microsoft recommends this be set to one day.
```

Copied!

```
1. 1
1. **Minimum password length**: This policy determines the fewest number of characters required in a password. Microsoft recommends that this be set somewhere between 8 and 14.
```

Copied!

```
1. 1
1. **Minimum password length audit**: This policy is designed for organizations who want to track user password lengths. Microsoft recommends using this only in specific scenarios.
```

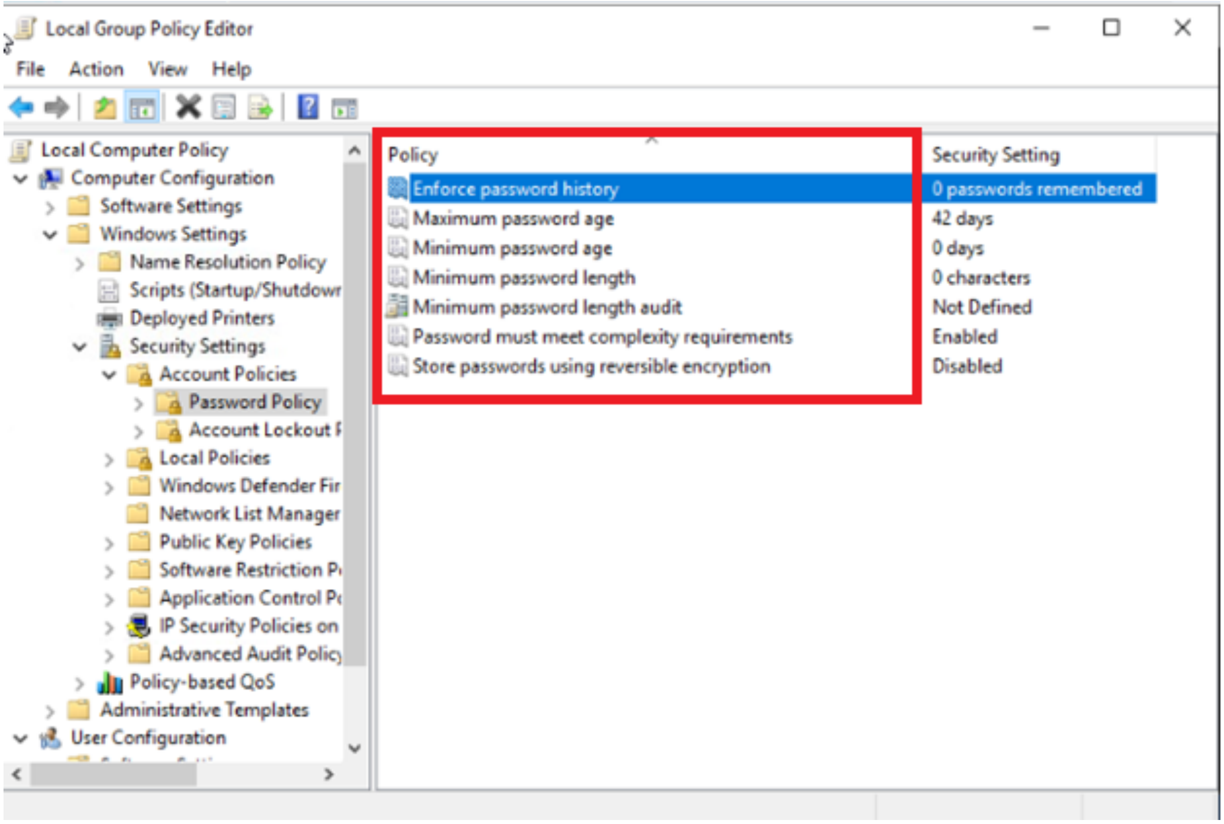
Copied!

```
1. 1
1. **Password must meet complexity requirements**: This policy indicates that passwords must meet Windows Security complexity requirements. Microsoft recommends that complexity requirements be enabled, especially if you are not enforcing other, more complex, password policies.
```

Copied!

```
1. 1
1. **Store passwords using reversible encryption**: This policy is specific to applications that use protocols requiring the user's password for authentication. Microsoft recommends that this option be disabled.
```

Copied!



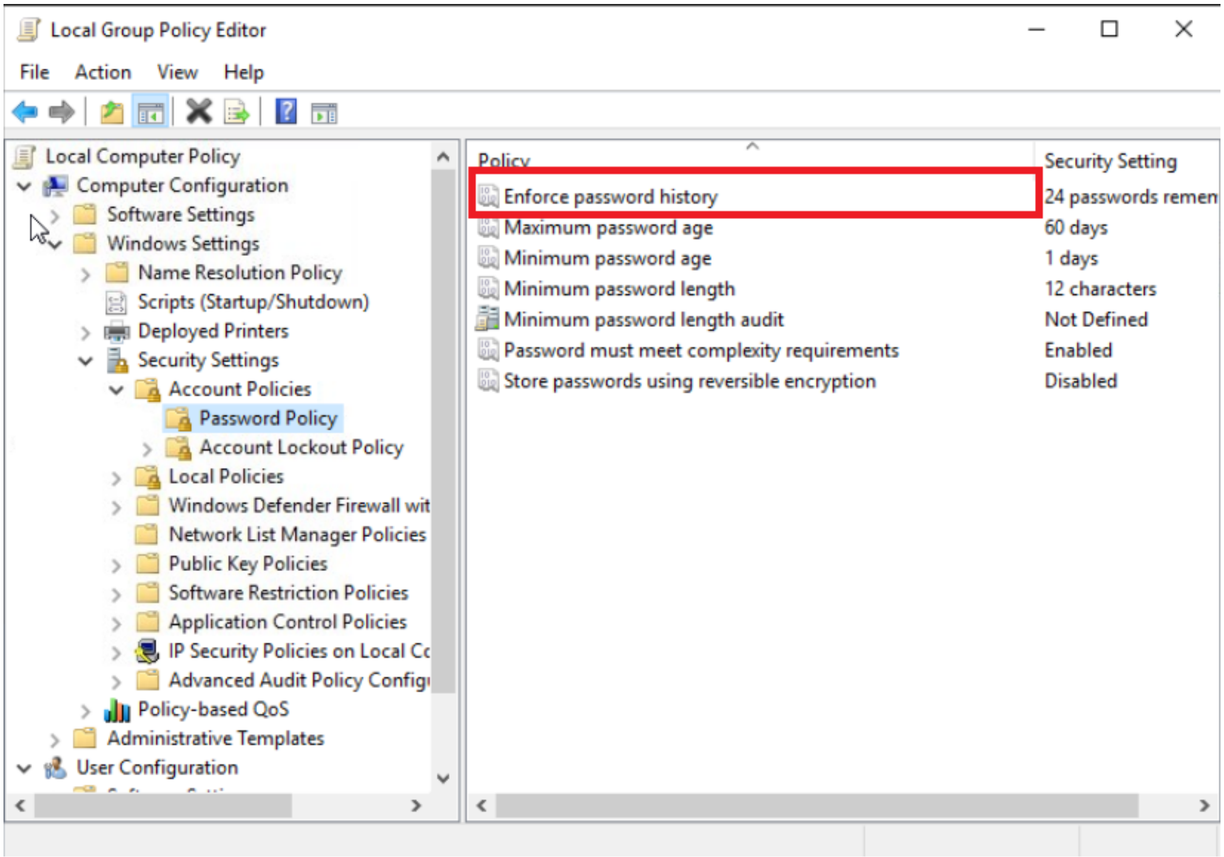
Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Exercise 3: Configure Password Policies

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

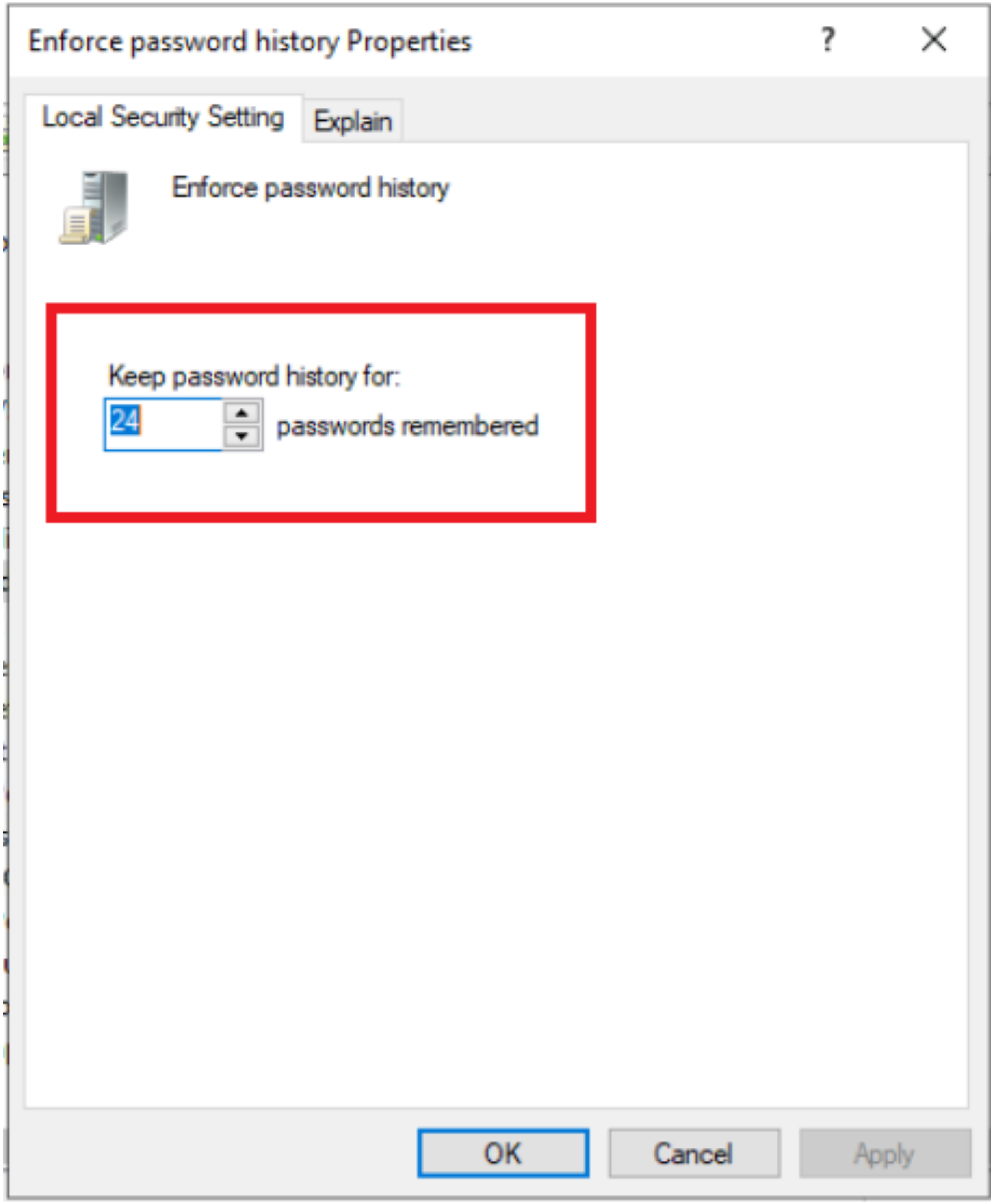
- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length

1. Double-click **Enforce password history**.



Policy	Security Setting
Enforce password history	24 passwords remen
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

2. Microsoft recommends that **Enforce password history** be set to 24. Type **24** into the box and click **OK**.



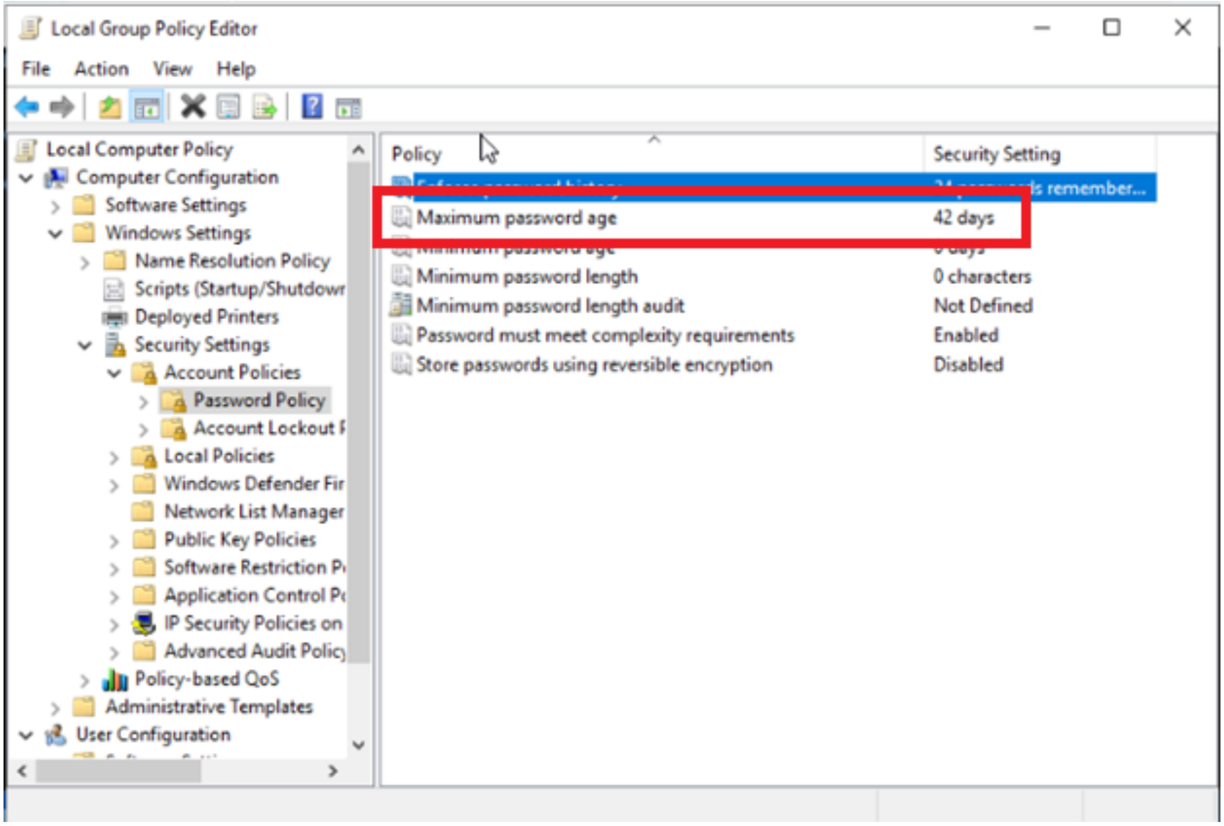
Enforce password history Properties

Enforce password history

Keep password history for:

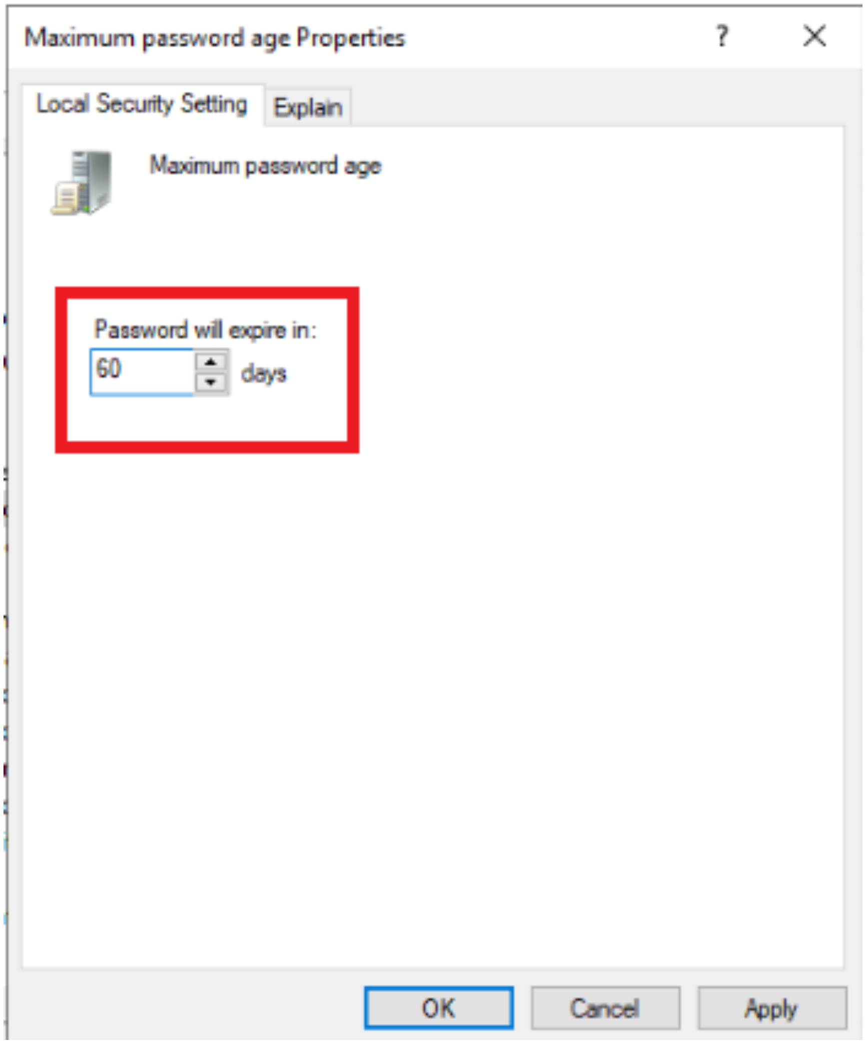
24 passwords remembered

3. Double-click **Maximum password age**.



Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

4. Microsoft recommends that passwords should be set to expire somewhere between 30 and 90 days. Type **60** into the box and click **OK**.

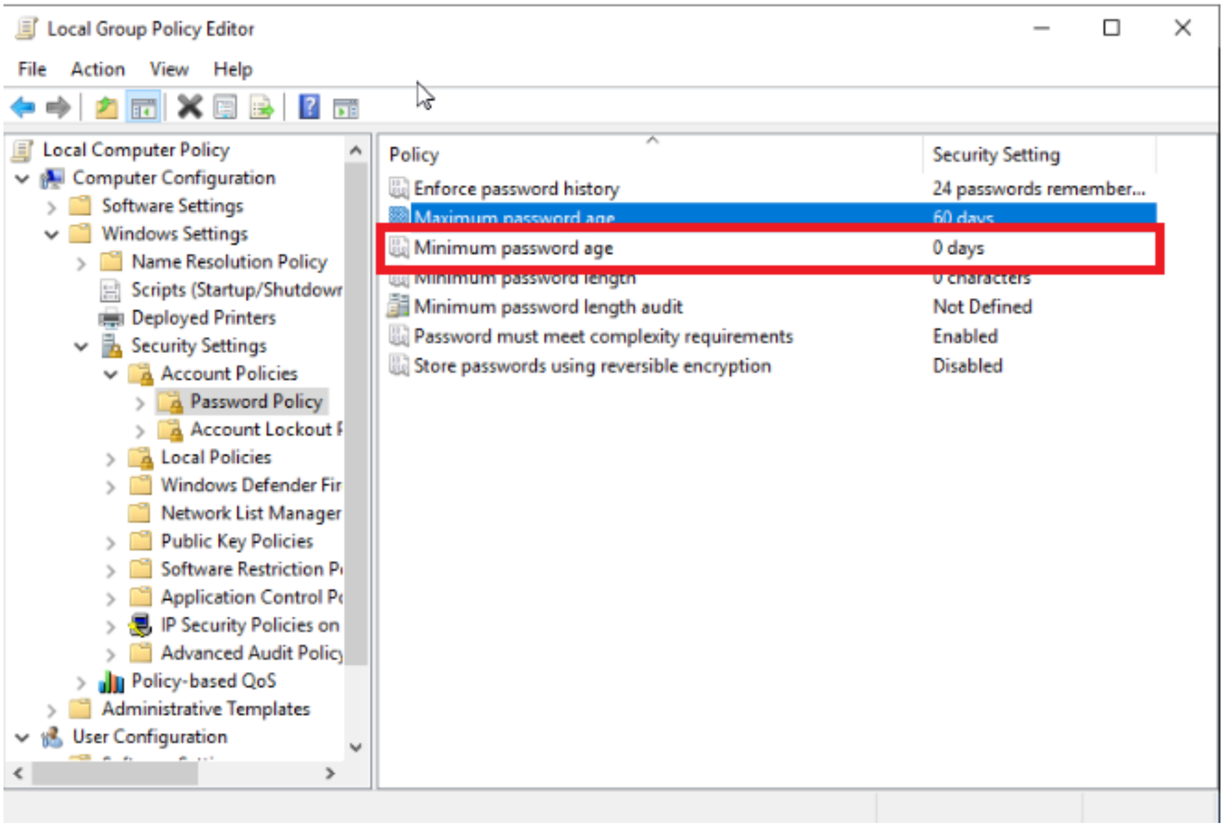


Maximum password age

Password will expire in:

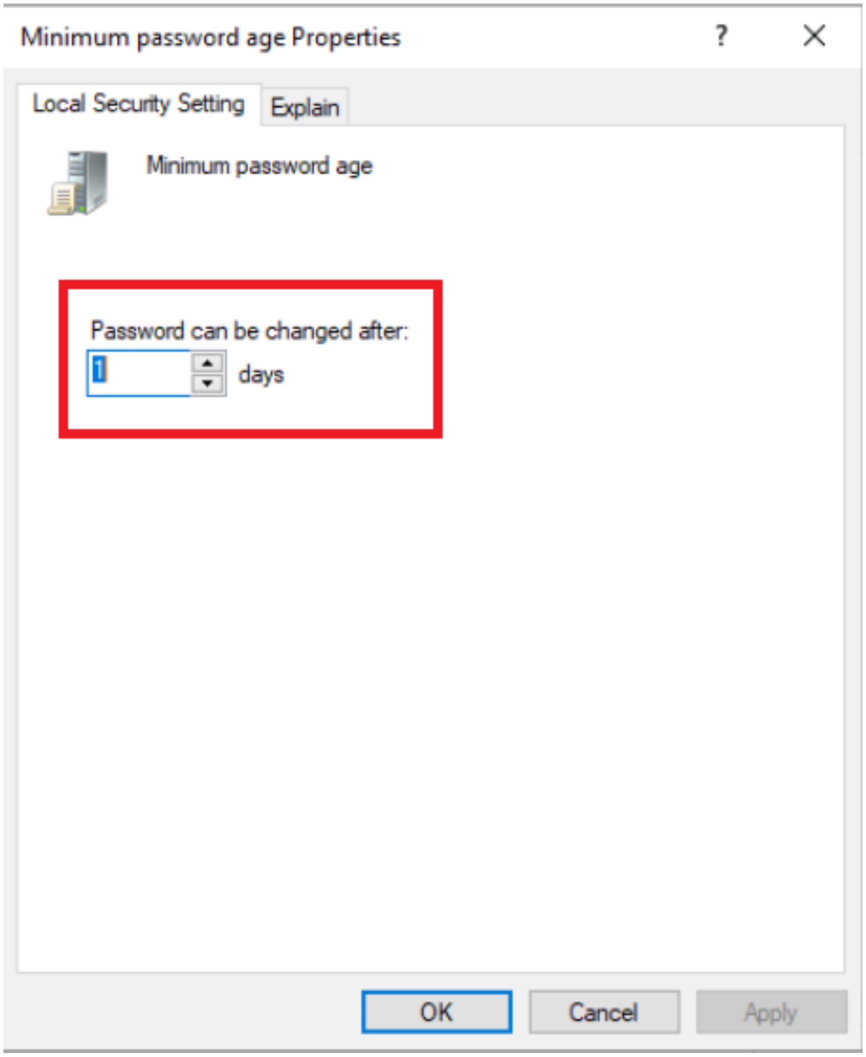
60 days

5. Double-click **Minimum password age**.



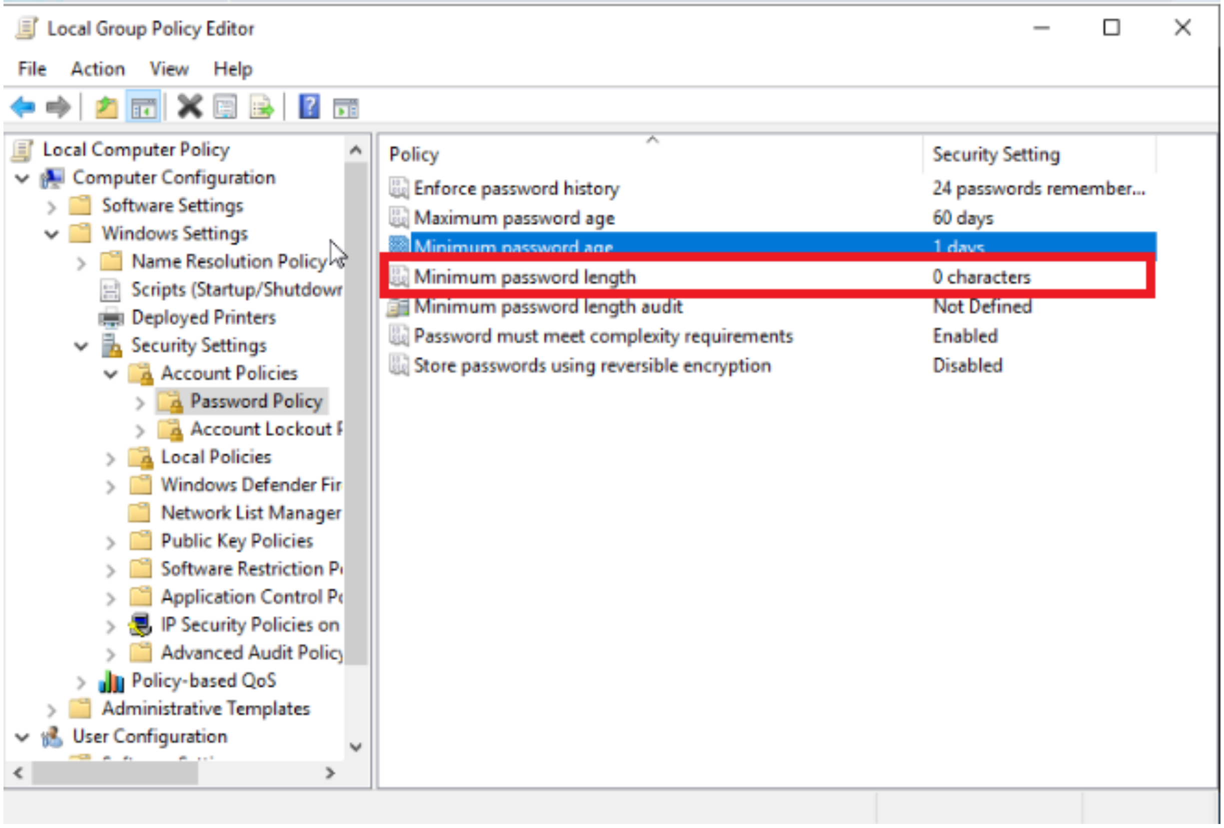
Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

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**.



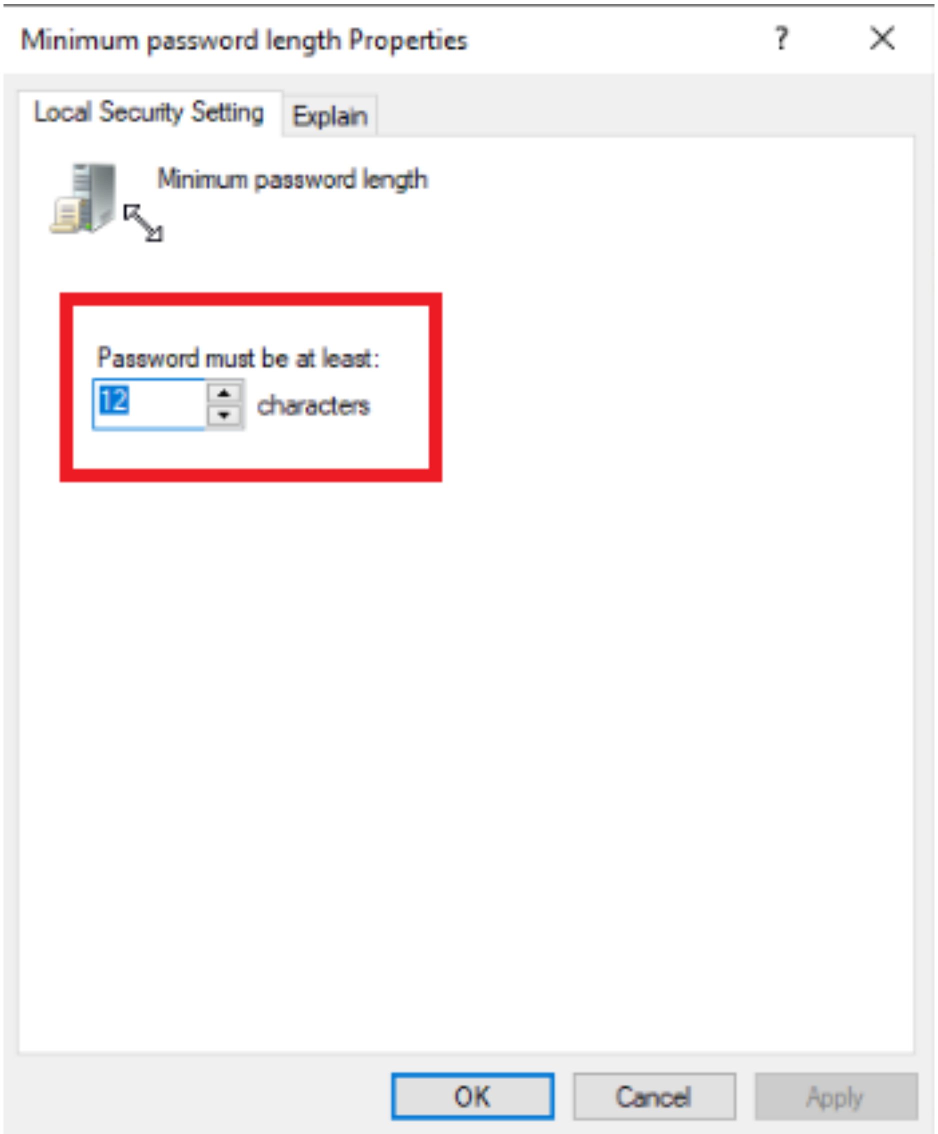
Password can be changed after: 1 days

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



Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

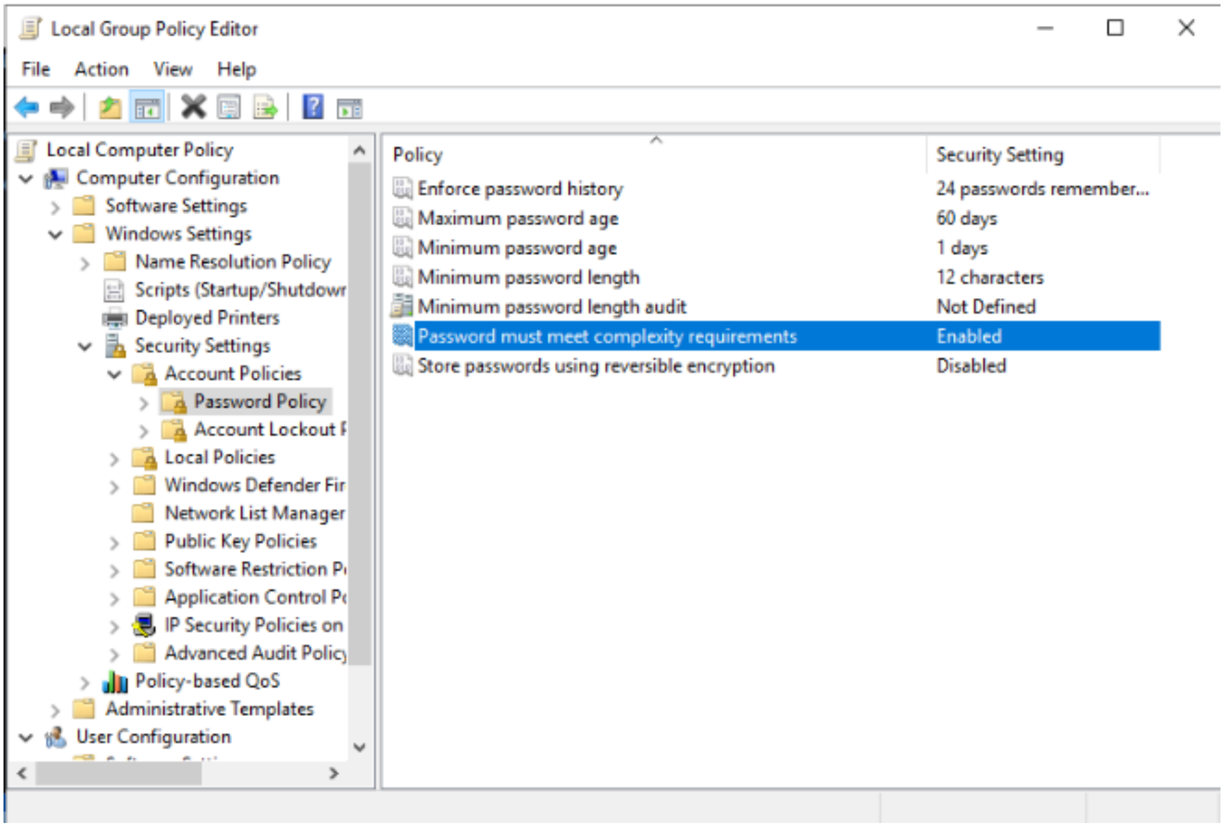
8. Microsoft recommends that passwords be at least 8 characters and no more than 14 characters. Type **12** into the box and click **OK**.


Minimum password length Properties

Minimum password length

Password must be at least:
12 characters

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



Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

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