Hands-On Lab: Windows Password Management

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; Windows Password Management

Table of Contents

[Introduction 2](#_Toc75508760)

[Objective 2](#_Toc75508761)

[Estimated Completion Time 2](#_Toc75508762)

[Materials Required 2](#_Toc75508763)

[Minimum System Configuration 2](#_Toc75508764)

[Managing Windows 10 Sign-ins 3](#_Toc75508765)

[Account Policies Options 8](#_Toc75508766)

[Account Lockout Policy Options 10](#_Toc75508767)

[Self-Reflection and Response: 12](#_Toc75508768)

[Instructor’s Response: 12](#_Toc75508769)

# Introduction

We rely on computers to store our information. There are aspects of the computer drive, however, that if not properly configured can allow someone to access the system and view, steal, or corrupt the information contained therein. In this set of labs, we will look at the Windows configuration for system passwords that control access to the computer and the best practices for configuring these settings.

## Objective

Upon completion of this activity, the student will be able to:

* Review and configure password management policies in a Windows client computer.

These activities will help you complete future labs in this course.

## Estimated Completion Time

If you are prepared, you should be able to complete:

* The Windows password management lab in 30 minutes to 1 hour.

## Materials Required

Completion of this lab requires a standard Windows 10 installation.

## Minimum System Configuration

To complete the labs included, it is recommended that you operate them from a computer system (desktop or laptop) that is running Windows 10 and has:

* Intel i5 or better CPU
* 8 GB RAM (minimum) - 16 GB RAM (recommended)
* 1 TB Hard Drive with at least 250 GB free (minimum) - 350 GB free (recommended)
* Microsoft Windows 10 or latest version

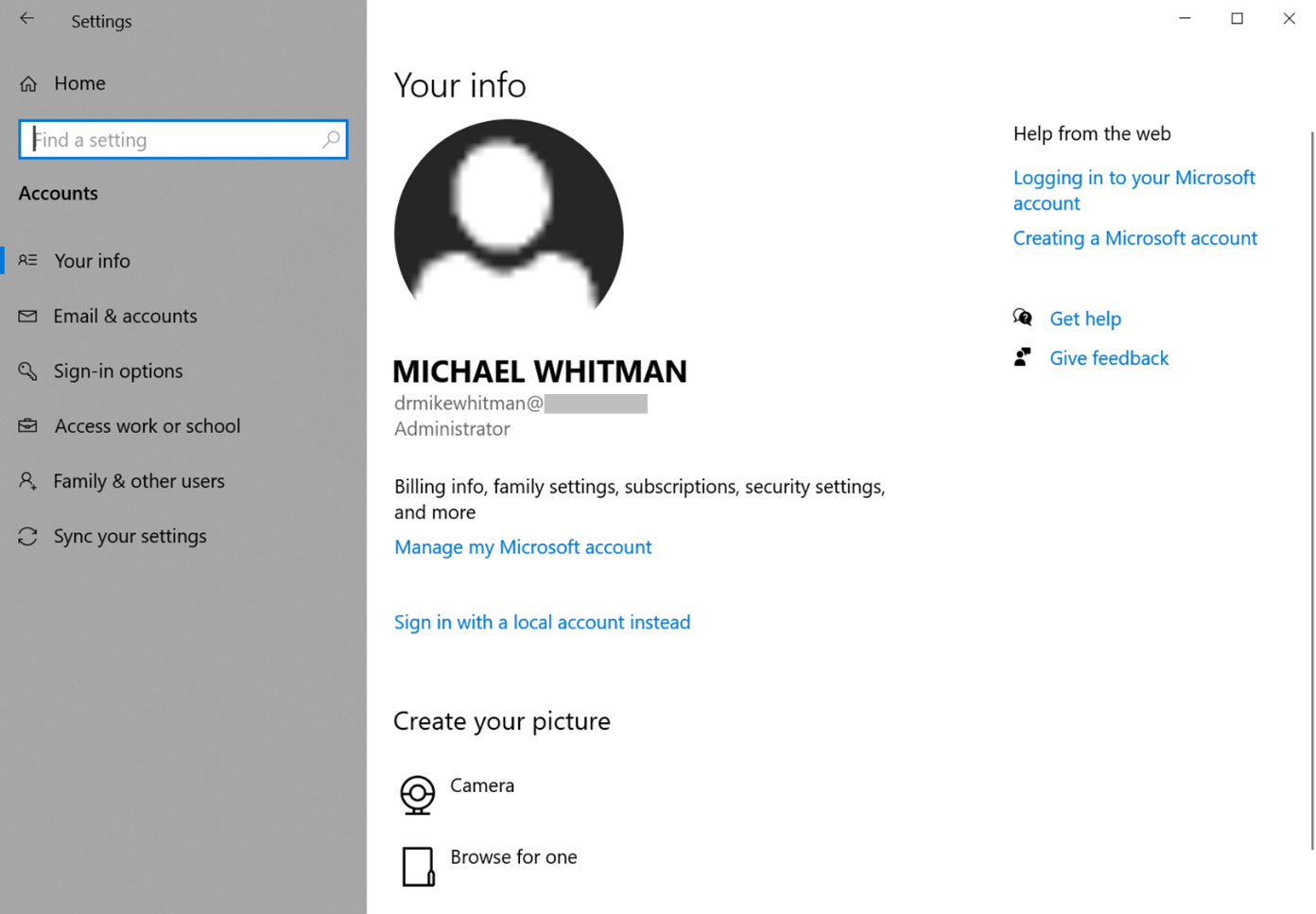
Password Management in Windows 10

If you own the computer you are performing this lab on, you are the administrator and can dramatically change how you access the system through sign-in and password policy management. If you are using a computer in a college or university lab, many of these settings may not be available to you. Ask your instructor for their recommendation as to whether you should perform this lab on your own computer or on one in the lab.

## Managing Windows 10 Sign-ins

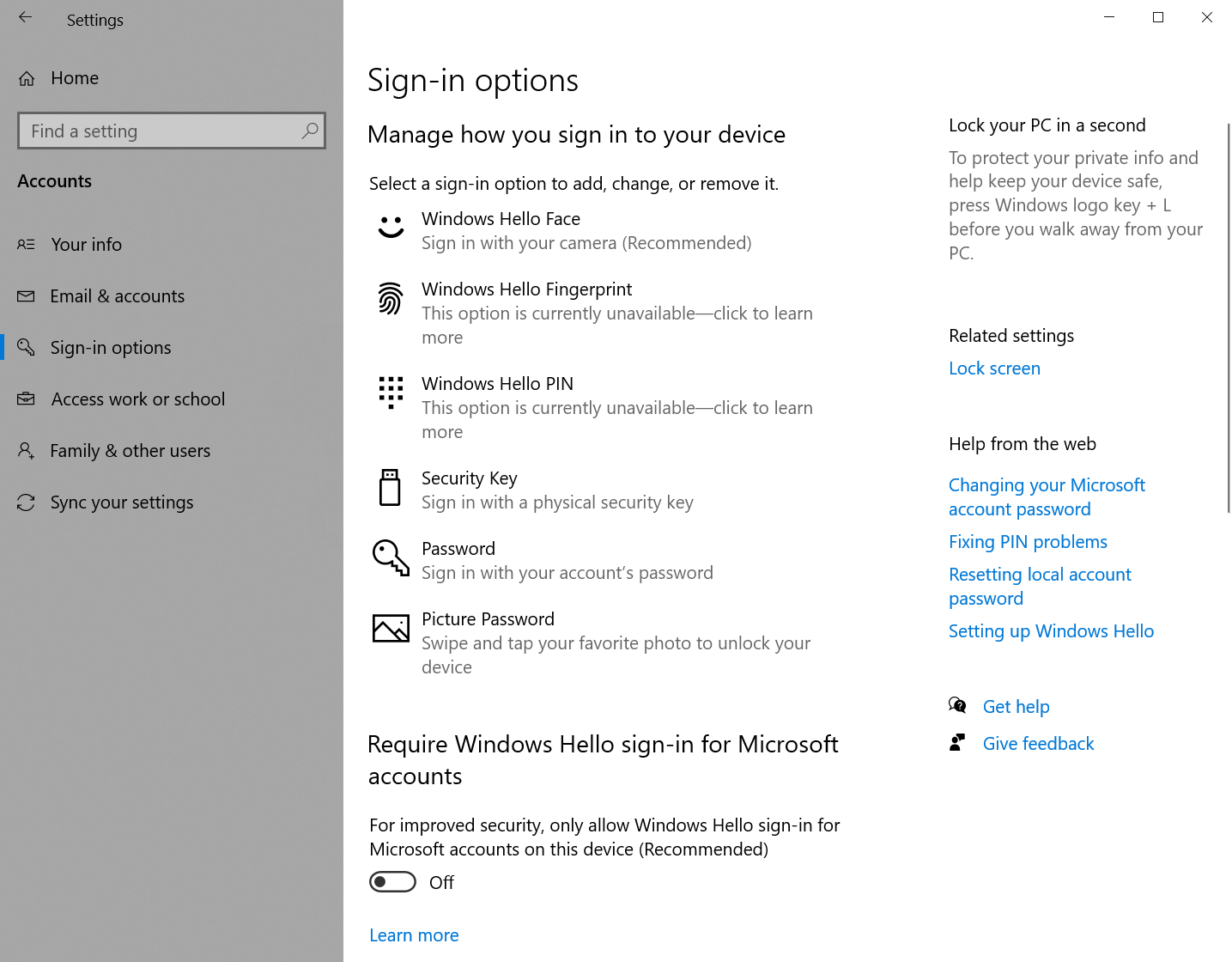
The first thing we’ll look at is the sign-in settings in Windows 10. These control the manner in which you sign-in, and whether you allow certain shortcuts to simplify login.

1. Click the **Start** button in the lower left of your Windows 10 menu bar, then, select the Windows button, shaped like a gear. This opens the *Windows Settings* menu.
2. Select the **Accounts** option. You should see the *Accounts* menu shown in Figure L04-1.



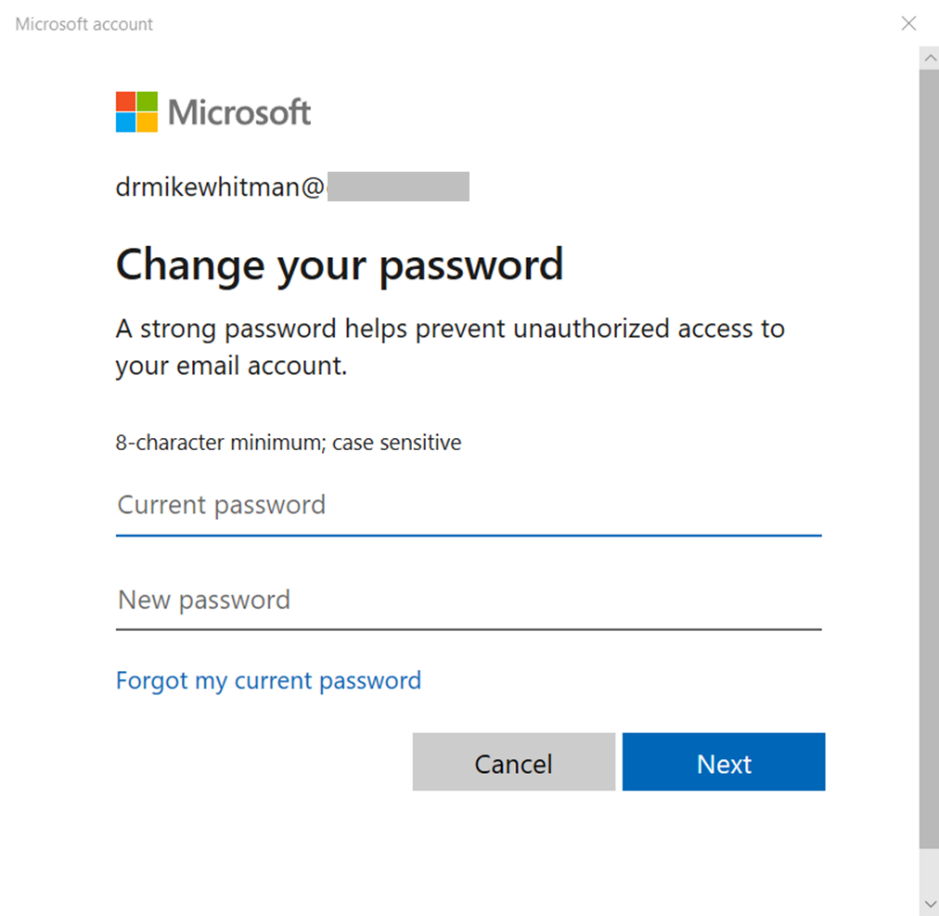
**Figure L04-1** Microsoft Windows 10 Accounts Menu

1. On the left menu, select **Sign-in options**. You should see the *Sign-in options* menu shown in Figure L04-2 below. Note: many of these options may not be available on a college/university or private organization system.



**Figure L04-2** Microsoft Windows 10 Sign-in options Menu (top)

1. The following options are available to users in Windows 10 to allow alternate sign-in options:
   1. Windows Hello Face uses a web camera to perform facial recognition.
   2. Windows Hello Fingerprint uses a fingerprint reader (not available on example system).
   3. Windows Hello PIN uses a Personal Identification Number (PIN).
   4. Security Key uses a physical security key like a USB dongle.
   5. Password uses the Windows 10 account username and password for standard login.
   6. Picture Password uses a graphical image.
2. You may be able to set up any of the above on your personal system, by selecting the option and following the prompts. These options are inherently secure as they are only used from your system’s keyboard, with the exception of “e. Password” which is used anytime you connect to the system remotely as well.
3. Select **e. Passwords**. This brings up the *Change your password* window you use to change your password as shown in Figure L04-3.



**Figure L04-3** Windows Change your password menu

1. If your current password does not comply with industry best practice, it is recommended you change it. It is also recommended that you change your password at least every six months to one year. Best practices recommend that your password complies with the “10.4” guideline:

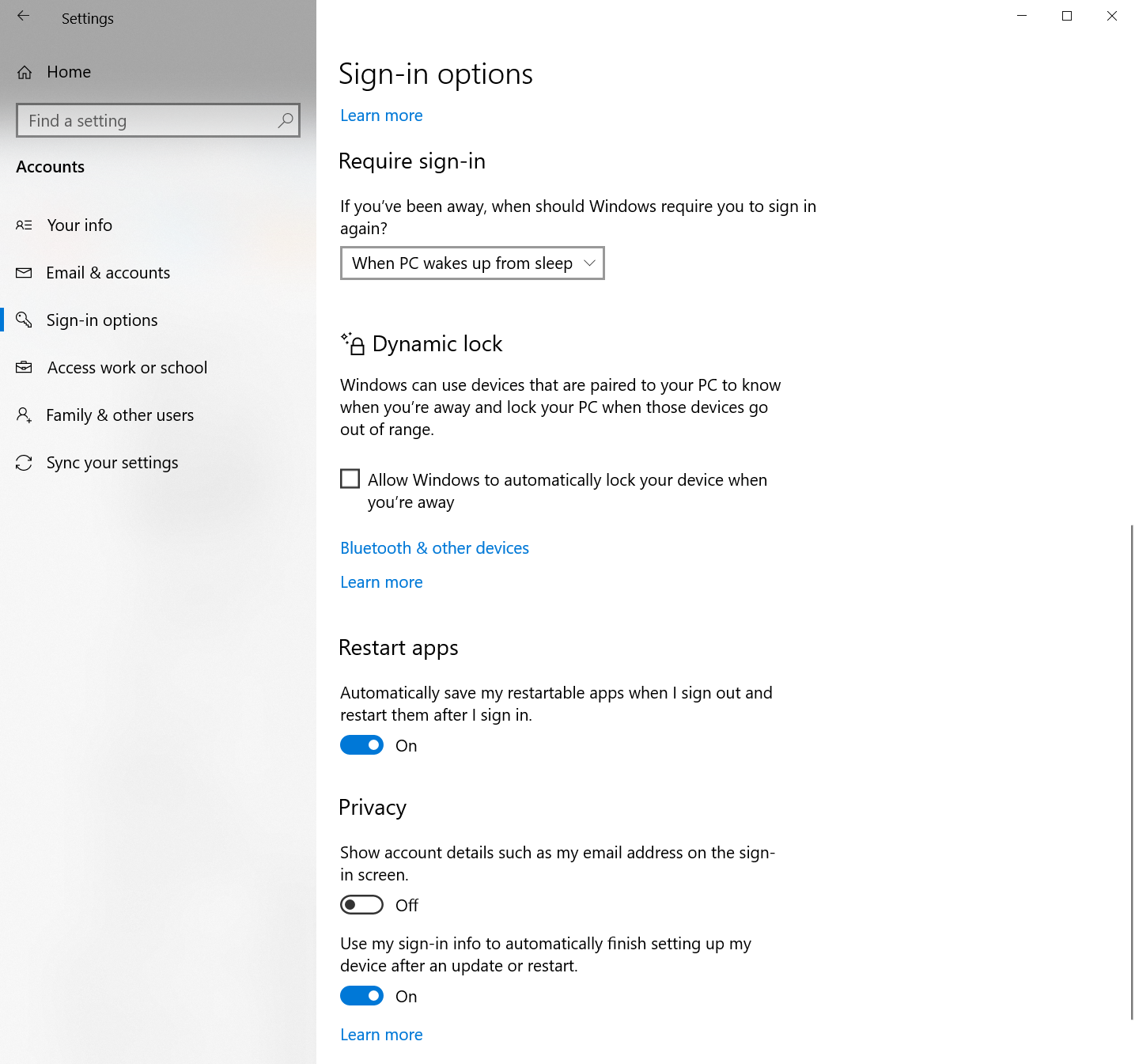
* Password is at least ten characters long
* Password contains at least one:
  + Upper case letter – note some versions allow non-English characters
  + Lower case letter
  + Number 0-9
  + System permitted special character -e.g. [~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/](mailto:~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/).

Microsoft requires passwords to meet minimum complexity requirements:[[1]](#endnote-2)

* Passwords may not contain your account username
* Passwords must contain at least three of the above character types, including non-English characters and some Unicode characters.

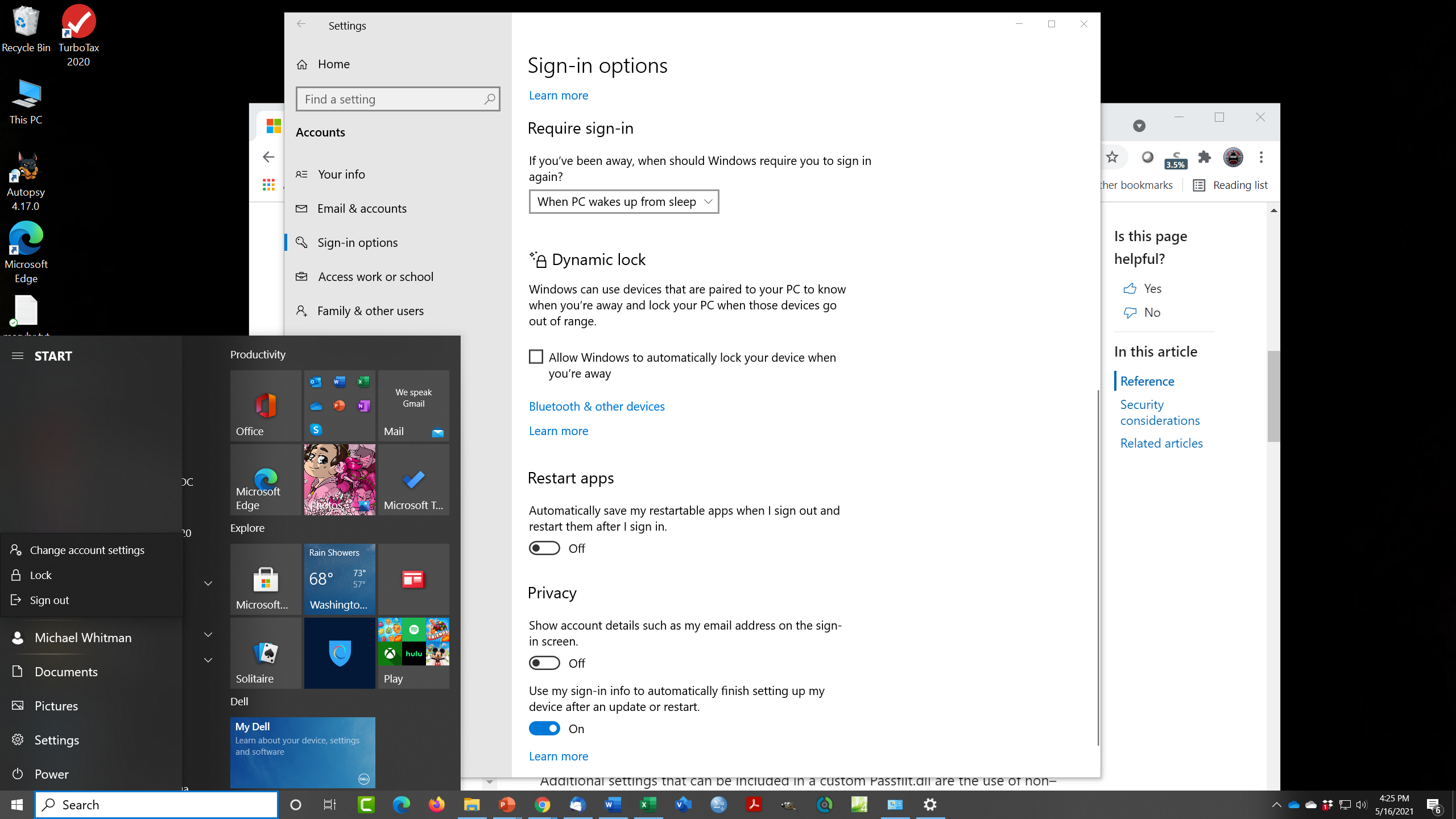
Having at least eight characters and complying with the Microsoft requirements provides over 218 trillion different password possibilities.

1. Return to the Sign-in Options menu by selecting the **Cancel** button. Further down this menu you’ll see the Require sign-in option as shown in Figure L04-4. Note: you may need to scroll down to see these additional options.



**Figure L04-4** Microsoft Windows 10 Sign-in options menu (bottom)

1. Selecting the options below Require sign-in provide the options to mandate signing-in after the system wakes up from sleep or never. It is not recommended to select Never on a system that may be accessed by another user. You can always log out of your system, transitioning back to the sign-in screen by selecting the **Window Start** button on the left side of the taskbar, then select your **Account** menu option indicated by your name at the top of the Start menu and then selecting **sign-out**, as shown in Figure L04-5 below. It is always recommended that you sign-out of any computer you’re using when you leave the keyboard. On some keyboards, you can just select the **Windows Key + the L key** to do the same thing.



**Figure L04-5** Microsoft Windows 10 Start menu Sign out option

1. A new feature in Windows 10 is Dynamic lock. This allows you to pair a personal communications device like your smart phone or tablet with your computer using Bluetooth. If you move that device out of range of the computer, it will automatically lock your computer. This is handy if you need to suddenly rush out of range of the computer (like you’re late for class!).
2. Other options on this menu include the *Restart apps* option, which will reload the programs you are using when you sign out of your system and then sign back in.
3. The *Privacy* option allows you to hide your email address on the sign-in screen, while the second option allows the system to finish setup of your computer after an update or restart.

Configuring Windows Password Policies

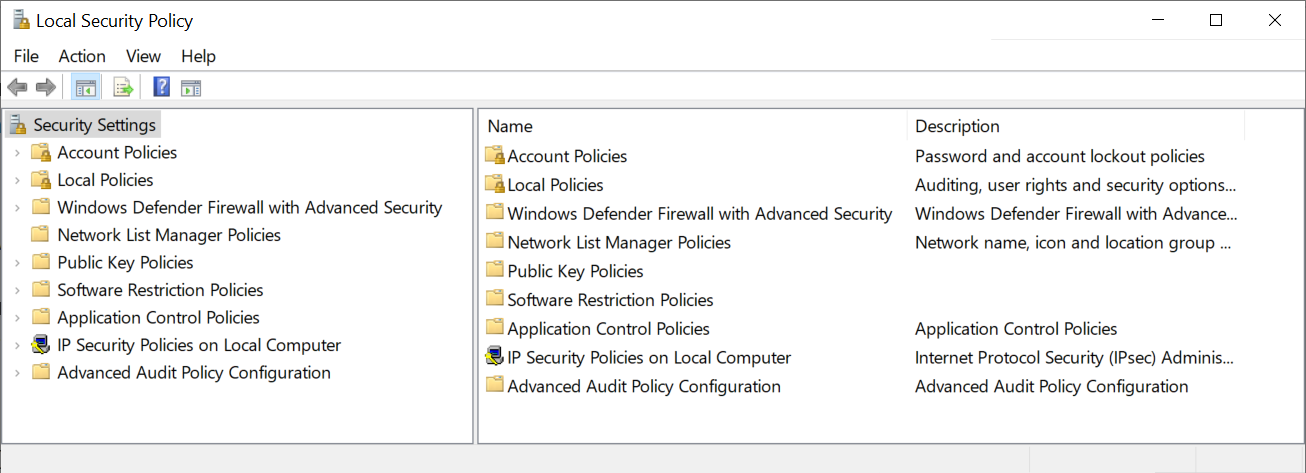
Microsoft Windows 10 has much more complex password policies which you can configure. The following Windows documents can provide more information:

* https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
* https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings

Note: you must have administrator rights on your system to make any changes, but you should be able to at least look at the current settings.

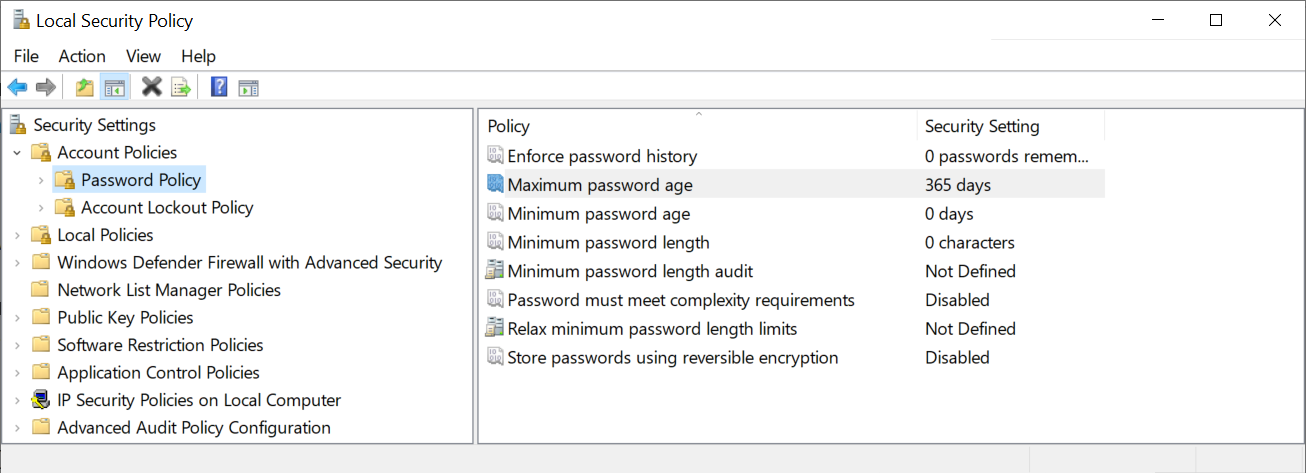
## Account Policies Options

1. First, open Local Security Policy. In the Windows Task Bar search field, type **secpol.msc**, and then press **ENTER**. You should see a window like Figure L04-6.



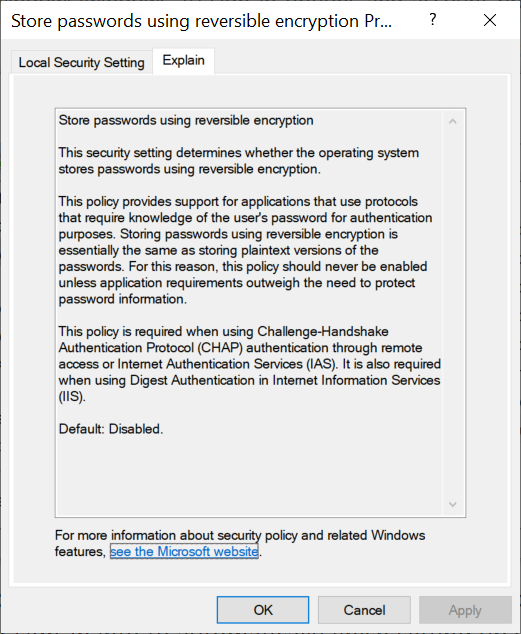
**Figure L04-6** Windows 10 Local Security Policy MMC

1. Under **Security Settings** of the console tree (left side), click **Account Policies** and then click **Password Policy**.
2. As shown in Figure L04-7 below, here you can specify the policies that will shape the use of passwords on this system. Again, you may not be able to change these values on an organizational computer.



**Figure L04-7** Security Settings Account Password Policy Options

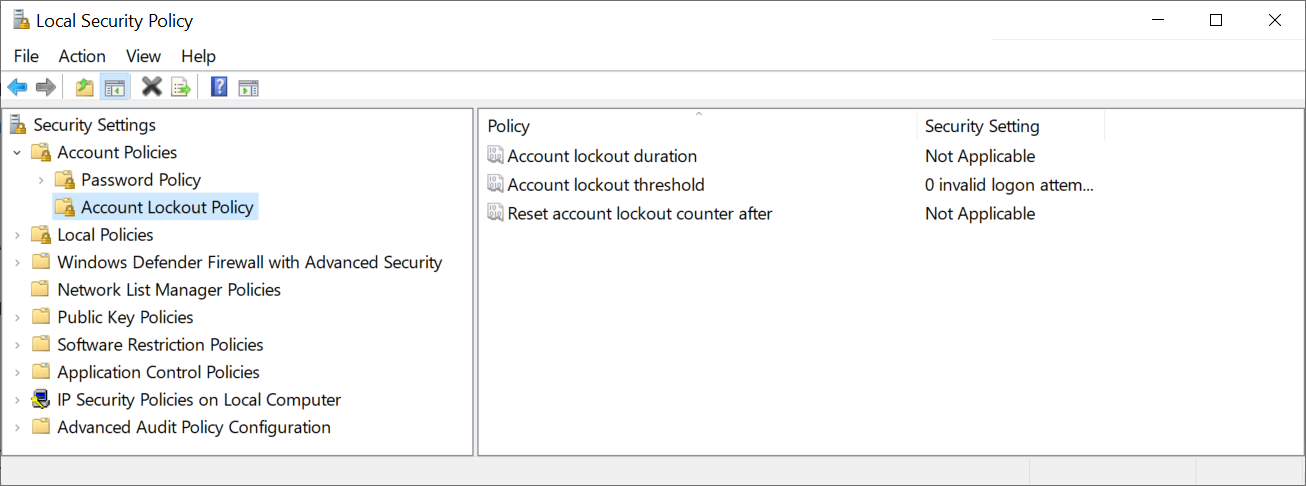
1. The options available are:
   1. Enforce password history – which regulates the number of passwords that the system remembers, to prevent (or allow) reuse of passwords.
   2. Maximum password age – the amount of time before passwords must be changed – in this example every 365 days.
   3. Minimum password age – the least amount of time before passwords can be changed – here it’s disabled.
   4. Minimum password length – how short a password can be on this system
   5. Minimum password length audit – whether or not a too-short password will be noted in the system logs as a warning
   6. Password must meet complexity requirements – whether you will enforce the complexity requirements explained in the previous lab.
   7. Relax minimum password length limits – allows you to change the value associated with minimum limits beyond the current system restriction of 14. In other words, currently you can’t specify a minimum password limit of 15 or more character, unless you change this setting.
   8. Store passwords using reversible encryption – unless specified the system records your password in a non-reversible encrypted format. Some applications may need this changed if you want to use your default systems login to access outside resources.
2. To change one of the above settings, right click on the entry and select **Properties**. To learn more about a particular option, you can select the Explain tab at the top of the properties window, as shown in Figure L04-8.



**Figure L04-8** Password Policy Properties Explain feature

## Account Lockout Policy Options

1. Go back to left side of the Local Security Policy MMC and select **Account Lockout Policy**. This opens the Account Lockout options as shown in Figure L04-9. Here you will be able to see and change the policy options associated with failed password attempts resulting in a system lockout.



**Figure L04-9** Security Settings Account Lockout Policy

1. Here you have three options associated with failed sign-in attempts:
   1. Account lockout duration – how long someone is locked out if they fail the specified number of invalid logon attempts – available range of 0 to 99,999 minutes (approximately 69½ days)
   2. Account lockout threshold – how many wrong guesses a user is allowed when signing in – available range of 0 to 999 failed attempts
   3. Reset account lockout counter after – how long after a failed attempt before the system “forgets” the failed attempt, in other words, if you try and fail, available range of 1 to 99,999 minutes
2. Close any open properties windows and close the Local Security Policies MMC.

# Self-Reflection and Response

Please share your experiences in using the Widows Password Management system.

|  |
| --- |
|  |

Please share your experiences in exploring the Windows Password Policies:

|  |
| --- |
|  |

## Instructor’s Response

|  |
| --- |
|  |

Resources

1. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements> [↑](#endnote-ref-2)