

# Udacity Cybersecurity Course #1 Project

## Contents

### Learning Objectives:

- Explain security fundamentals including core security principles, critical security controls, and cybersecurity best practices.
- Evaluate specific security techniques used to administer a system that meets industry standards and core controls
- Assess high-level risks, vulnerabilities and attack vectors of a sample system
- Explain methods for establishing and maintaining the security of a network, computing environment, and application.

## Student Information

Student Name: Simon Chen

Date of completion: 1/22/2021

## Scenario

Congratulations!

You have been hired to secure the PC used at your friend's business: Joe's Auto Body. Joe provides car repair services throughout the tri-state area. He's had previous employees use it for activities un-related to work (e.g., web browsing, personal email, social media, games, etc.) and he now uses it to store his critical business information. He suspects that others may have broken into it and may be using it to transfer files across the internet. He has asked that you secure it for him according to industry best practices, so it can be once again used as a standard PC.

You will be given access to a virtual image of Joe's Auto Body's PC. It's a copy of the actual computer operating system in use that will be transferred to Joe's computer once you are done.

This template provides you with the high-level steps you'll need to take as part of securing a typical computer system. For each step, use the virtual Windows 10 PC to answer the questions and challenges listed in this project. You'll also need to explain how you got the answers and provide screenshots showing your work.

It's important that you read through the entire document before securing the system and completing this report.

To start, you need to login to the virtual PC. You can use Joe's account using the user-id and password below. You may also use any other account on the PC.

Account Name: JoesAuto

Password: @UdacityLearning#1

## 1. Reconnaissance

The first step in securing any system is to know what it is, what's on it, what it's used for and who uses it. That's the concept of systems reconnaissance and asset inventory. In this step, you'll document the hardware, software, user access, system and security services on the PC.

Complete each section below.

### **Hardware**

- *Fill in the following table with system information for Joe's PC.*

Device Name	Microsoft Windows 10 PRO
Processor	Intel(R) Xeon(R) Platinum 8171M CPU @2.60 GHZ
Install RAM	1.00 GB
System Type	X-64 Based PC
Windows Edition	Windows 10 PRO
Version	10.0.17763 Build 17763
Installed on	12/7/2018
OS build	Microsoft Corporation

- *Explain how you found this information:*

I found this information by first typing System Information on the Search Bar.

I went to the Systems Information Summary tab, and on there it lists the information.

- *Provide a screenshot showing this information about Joe's PC:*

System Information		
File Edit View Help		
System Summary	Item	Value
	OS Name	Microsoft Windows 10 Pro
	Version	10.0.17763 Build 17763
	Other OS Description	Not Available
Hardware Resources	OS Manufacturer	Microsoft Corporation
	System Name	JOESGARAGEPC
	System Manufacturer	Microsoft Corporation
	System Model	Virtual Machine
Components	System Type	x64-based PC
	System SKU	Unsupported
	Processor	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 2095 Mhz, 1 Core(s), 1 Logi...
	BIOS Version/Date	American Megatrends Inc. 090008, 12/7/2018
Software Environment	SMBIOS Version	2.3
	BIOS Mode	Legacy
	BaseBoard Manufacturer	Microsoft Corporation
	BaseBoard Product	Virtual Machine
	BaseBoard Version	7.0
	Platform Role	Desktop
	Secure Boot State	Unsupported
	PCR7 Configuration	Binding Not Possible
	Windows Directory	C:\windows
	System Directory	C:\windows\system32
	Boot Device	\Device\HarddiskVolume1
	Locale	United States
	Hardware Abstraction Layer	Version = "10.0.17763.1131"
	User Name	Not Available
	Time Zone	Coordinated Universal Time
	Installed Physical Memory (RAM)	1.00 GB
	Total Physical Memory	1.00 GB
	Available Physical Memory	43.4 MB
	Total Virtual Memory	2.69 GB
	Available Virtual Memory	968 MB
	Page File Space	1.69 GB
	Page File	D:\pagefile.sys
	Kernel DMA Protection	Off
	Virtualization-based security	Not enabled
	Device Encryption Support	Reasons for failed automatic device encryption: TPM is not usable, PCR7 bindi...
		A hypervisor has been detecte...

## Software

Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

- *List at least 5 installed applications on Joe's computer:*
  - 1) Candy Crush Friends
  - 2) Farm Heroes Saga
  - 3) Microsoft One Drive
  - 4) Spotify
  - 5) MusicBee 3.3.7367
- *Explain how you found this information. Provide screenshots showing this information.*

I found out this information by first going to settings then going to **apps and features**. I scrolled down and its list the apps that were installed on Joe's Computer. Most of the apps that I have listed above were installed on 1/22/2021. If I look at the date on Joe's computer its

1/22/2021, so it is the same date.

Settings

Home

Find a setting

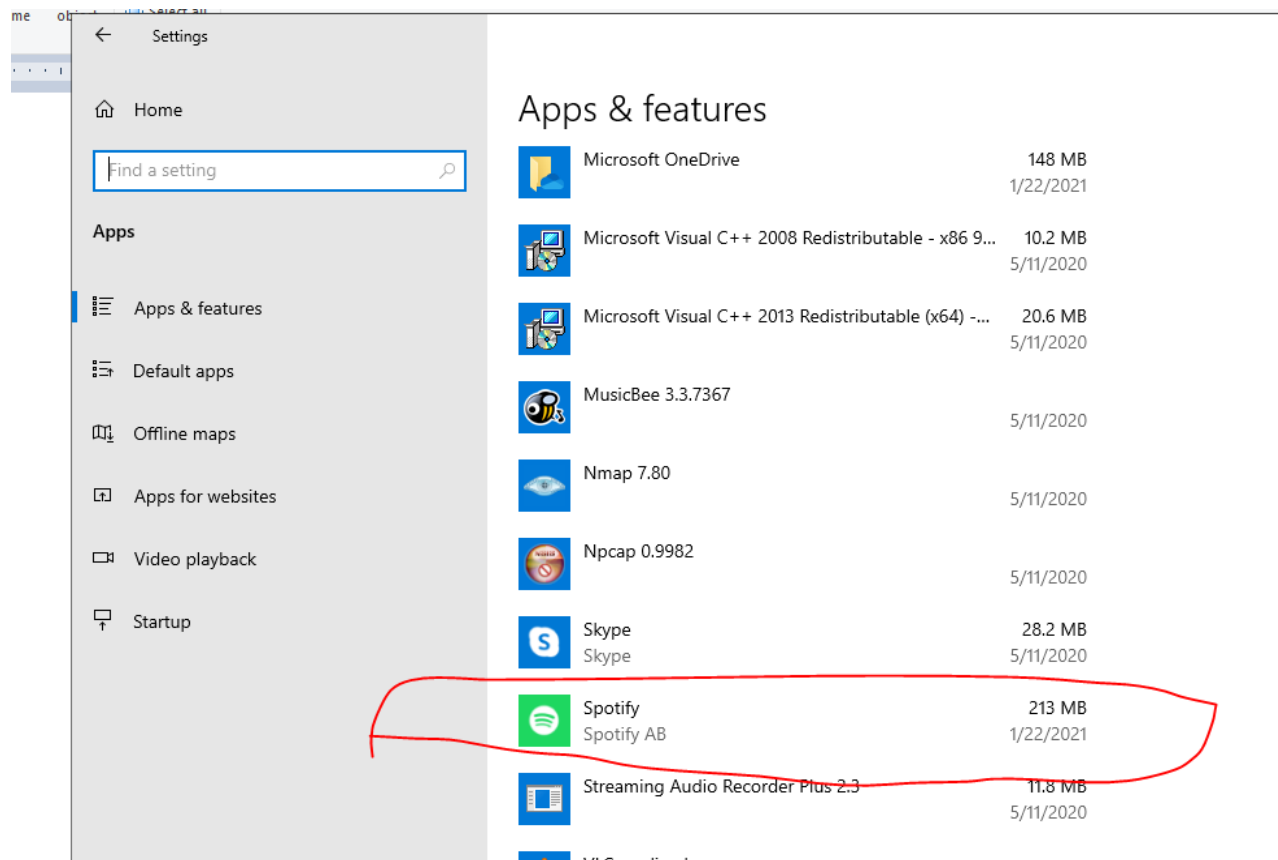
Apps & features

Sort by: Name Filter by: All drives

7-Zip 19.00 (x64)	4.96 MB	5/11/2020
Adobe Reader XI (11.0.01)	128 MB	5/11/2020
Candy Crush Friends king.com	215 MB	1/22/2021
Farm Heroes Saga king.com	240 MB	1/22/2021
Google Chrome		5/11/2020
Microsoft Edge Microsoft Corporation	17.7 MB	5/11/2020
Microsoft OneDrive	148 MB	1/22/2021
Microsoft Visual C++ 2008 Redistributable - x86 9...	10.2 MB	5/11/2020
Microsoft Visual C++ 2013 Redistributable (x64) -...	20.6 MB	5/11/2020
MusicBee 3.3.7367		5/11/2020
Nmap 7.80		5/11/2020
Npcap 0.9982		5/11/2020
Skype Skype	28.2 MB	5/11/2020

project-template 1 ... Settings

5:03 PM 1/22/2021



- *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

*The CIS step that it fulfills is Inventory and Control of Software Assets.*

*I believe the step is Inventory and Control of Software Assets because if they have this rule, then they will continually monitor which software is going to be downloaded on to the computer.*

## **Accounts**

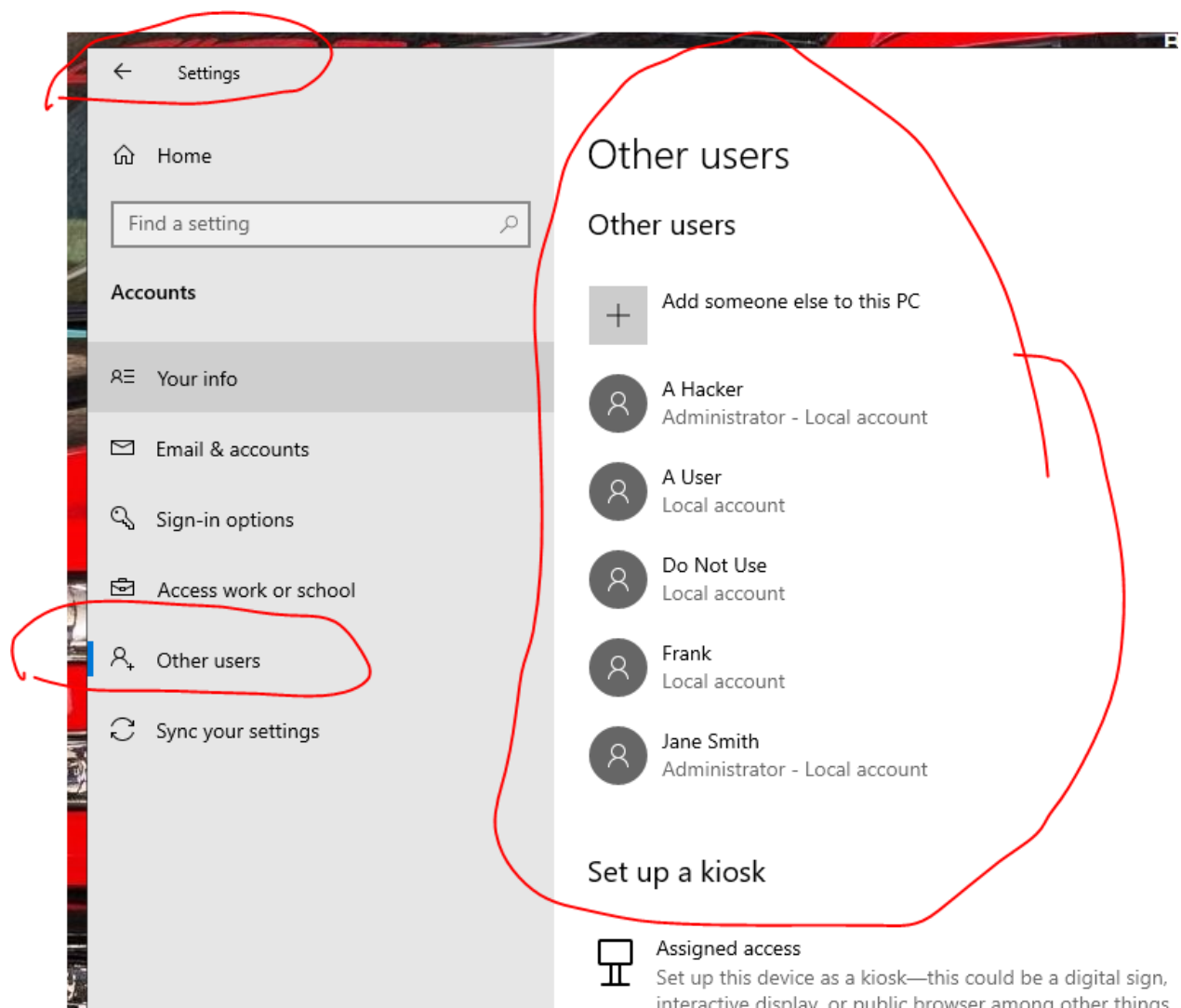
As part of your security assessment, you should know the user accounts that may access the PC.

- *List the names of the accounts found on Joe's PC and their access level.*

Account Name	Full Name	Access Level
Administrator	A Hacker	Local Account
	A User	local account
	Do Not USE	local account
	Frank	local account
Administrator	Jane Smith	local account

- Provide a screenshot of the Local Users.

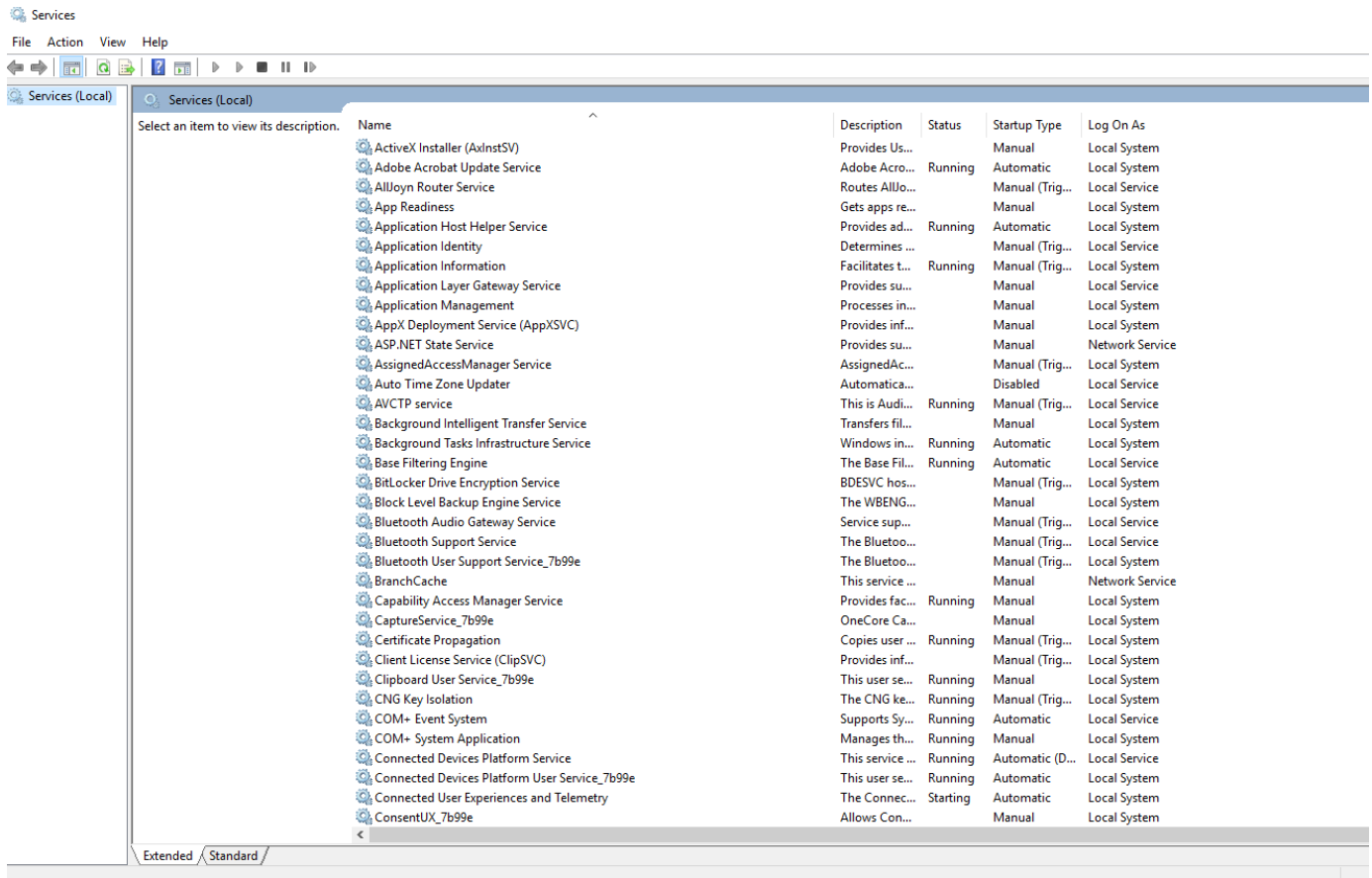
*I found the local users by first going to Settings, I clicked on accounts tab, on the left side of the panel, I clicked on Other Users. Once I open it, it lists the users.*



## Services

Services are applications often running in the background. Most of them provide needed functionality for the PC. Some may also be used to violate security policies.

- *Provide a screenshot of the services running on this PC.*

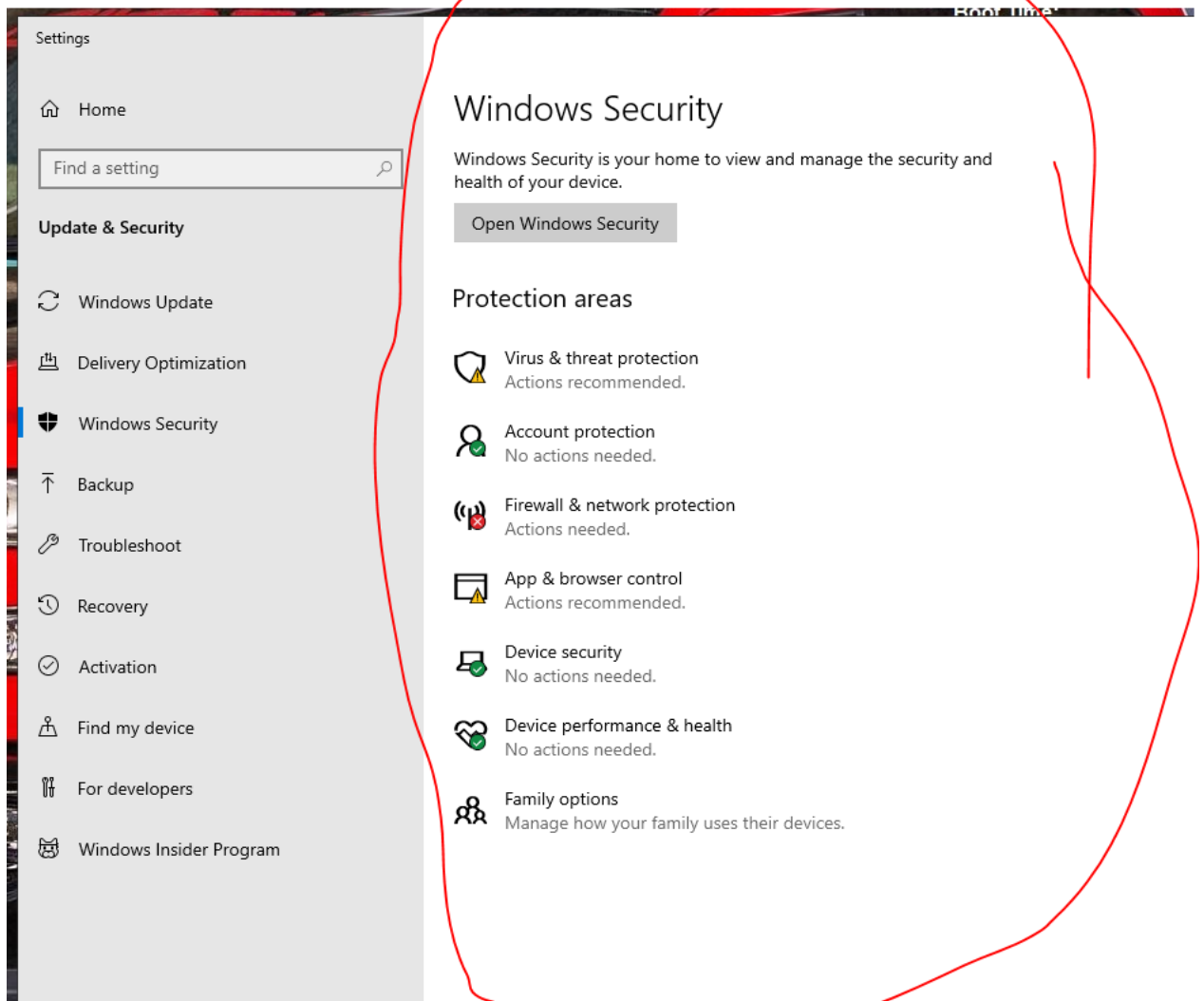


## Security Services

Joe wants to ensure that standard security services are running on his PC. He's content with using default Windows security settings and applications except for the rules outlined later. **Reminder that at this point you are just reporting what you observe. Do not make any changes to security settings yet.**

- *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using*

the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:



- 
- 
- The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing “Review your computer’s status and resolve issues.” Provide a screenshot of this below:



Security and Maintenance

← → ↕ ⬆ > Control Panel > System and Security > Security and Maintenance

Control Panel Home

Change Security and  
Maintenance settings

Change User Account Control  
settings

View archived messages

Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

Security



Maintenance



If you don't see your problem listed, try one of these:



Recovery

Refresh your PC without affecting  
your files, or reset it and start over.

- 
- 
- 
- Click on *View in Windows Security* to see the status there. Provide a screenshot of the **Firewall** settings.

Control Panel Home

Change Security and Maintenance settings

Change User Account Control settings

[View archived messages](#)

## Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

### Security

Network firewall

Currently not monitored

[Turn on messages about network firewall](#)

Virus protection

Currently not monitored

[Turn on messages about virus protection](#)

Internet security settings

Currently not monitored

[Turn on messages about Internet security settings](#)

User Account Control

Currently not monitored

[Turn on messages about User Account Control](#)

[How do I know what security settings are right for my computer?](#)

### Maintenance

If you don't see your problem listed, try one of these:



#### Recovery

Refresh your PC without affecting your files, or reset it and start over.

- 
- 
- From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:

Windows Defender Firewall

Control Panel > System and Security > Windows Defender Firewall

Control Panel Home

- Allow an app or feature through Windows Defender Firewall
- Change notification settings
- Turn Windows Defender Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

### Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

[What are the recommended settings?](#)

[Use recommended settings](#)

**Private networks** Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

**Guest or public networks** Not connected

- 
- 
- *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*

Change Security and Maintenance settings

Control Panel > System and Security > Security and Maintenance > Change Security and Maintenance settings

Turn messages on or off

For each selected item, Windows will check for problems and send you a message if problems are found. [How does Security and Maintenance check for problems?](#)

Security messages

<input checked="" type="checkbox"/> Windows Update	<input checked="" type="checkbox"/> Spyware and unwanted software protection
<input type="checkbox"/> Internet security settings	<input type="checkbox"/> User Account Control
<input type="checkbox"/> Network firewall	<input type="checkbox"/> Virus protection
<input checked="" type="checkbox"/> Microsoft account	<input checked="" type="checkbox"/> Windows activation

Maintenance messages

<input checked="" type="checkbox"/> Windows Backup	<input type="checkbox"/> Windows Troubleshooting
<input type="checkbox"/> Automatic Maintenance	<input checked="" type="checkbox"/> HomeGroup
<input type="checkbox"/> Drive status	<input type="checkbox"/> File History
<input checked="" type="checkbox"/> Device software	<input checked="" type="checkbox"/> Storage Spaces
<input checked="" type="checkbox"/> Startup apps	<input checked="" type="checkbox"/> Work Folders

[OK](#) [Cancel](#)

- 
-

- Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).

Security Feature	Status
Firewall product and status – Private network	Windows firewall is off and may be unprotected
Firewall product and status – Public network	Windows firewall is off and may be unprotected
Virus protection product and status	The Virus Protection is active and working, The Virus Protection is turned on and have been used by user.
Internet Security messages	Ok. All Internet Security are set to their recommended levels.
Network firewall messages	Windows firewall is off and ma be unprotected.
Virus protection messages	The Virus Protection is active and working. The Virus Protection is turned on and have been used by user.
User Account Control Setting	User Account Control Setting is turned off, but it will not notify you if it makes changes to the computer.

Windows Security

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options

## Security providers

Manage the apps and services that protect your device.

Antivirus


Windows Defender Antivirus  
Windows Defender Antivirus is turned on.


Firewall


Windows Firewall  
Windows Firewall is off and your device may be unprotected.


Web protection





 Home


 Virus & threat protection


 Account protection

 Firewall & network protection

 App & browser control

 Device security

 Device performance & health

 Family options

## Virus & threat protection

Protection for your device against threats.

### Current threats

No current threats.

Last scan: 1/22/2021 5:58 AM (quick scan)

0 threats found.

Scan lasted 2 minutes 30 seconds

37009 files scanned.

Quick scan

[Scan options](#)

[Threat history](#)

### Virus & threat protection settings

No action needed.

[Manage settings](#)

## Security and Maintenance

← → ↕ ⬆ ⬇ > Control Panel > System and Security > Security and Maintenance

Control Panel Home

Change Security and Maintenance settings

Change User Account Control settings

View archived messages

### Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

#### Security

Network firewall

[View in Windows Security](#)

Virus protection

[View in Windows Security](#)

Internet security settings

All Internet security settings are set to their recommended levels.

OK

User Account Control

Currently not monitored

[Turn on messages about User Account Control](#)

[How do I know what security settings are right for my computer?](#)

...

## Windows Security



Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

## Security providers

Manage the apps and services that protect your device.

### Antivirus

Windows Defender Antivirus

Windows Defender Antivirus is turned on.



### Firewall

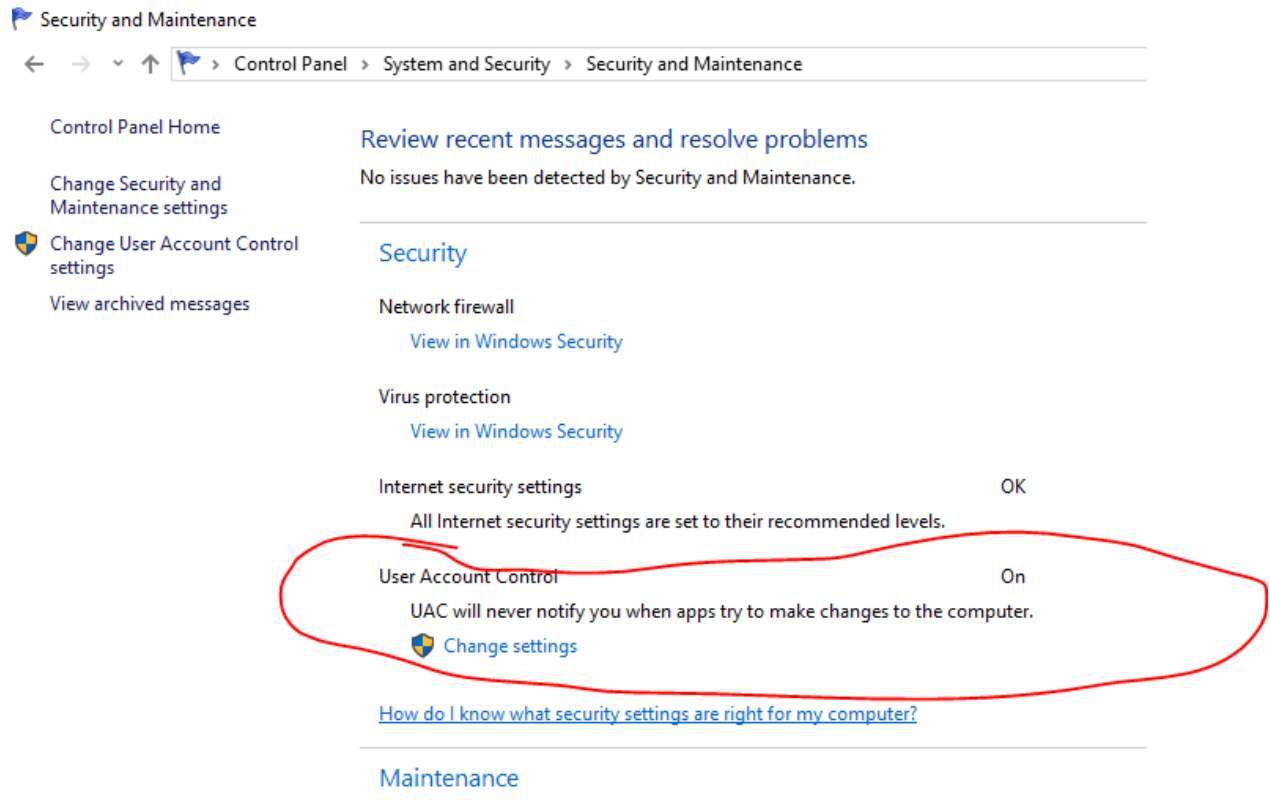
Windows Firewall

Windows Firewall is off and your device may be unprotected.



### Web protection

[Find security apps in Microsoft Store](#)



- Now that you are familiar with the security settings on Joe's PC, explain at least three vulnerabilities and risks with these settings. In other words, what can happen to Joe's PC if these are not changed?

[Hint: Refer to the CIS Controls document for ideas.]

- The first vulnerability is that if the network firewall is not turned on, then it is susceptible to viruses and intrusions. It needs to be activated for the computer to be safe.
- For the Virus protection, it needs to run every day to help protect the computer.

If the virus protection is turned off, then it is easier to get viruses and for hackers to steal information from the computer.

- For the Internet Security Settings, it is good condition and it is used to protect you while you are online. The user should always have it active, so that it protects the user from malicious websites.

## 2. Securing the PC

## **Baselines**

Joe has asked that you follow industry standards and baselines for security settings on this system.

- *What industry standard should Joe use for setting security policies at his organization and justify your choice?*

*I would use least privilege because I would limit everyone from using the computer at work. I would only give people access to Joe's computer that has authority.*

*The people that are on the computer should only use the computer for work only.*

*I checked that the apps that were downloaded on Joe's Computer were games.*

*I would make it a rule that only employees should use the computer for work, and not to use it to play games on the computer.*

*I would also recommend that Joe's computer be updated often by using patches, so that his computer is up to date.*

- *What industry baseline do you recommend to Joe?*  
*[Hint: Look in the documents folder]*

*I would promote safety on the computer. I would say that there should be antivirus software on the computer. Because if there is antivirus software, it blocks viruses on the computer. I noticed while I was doing research that the firewall has been turned off, so I would recommend Joe to turn on the firewall. If the firewall is turned on, then it protects the computer by blocked unwanted intruders.*

The System and Security functions in the Windows Control Panel are where you can establish the security settings for the PC. This is found from the Control Panel > System and Security > Security and Maintenance. On the Security and Maintenance window, you see a synopsis of the Windows 10 security settings.

- Assume Joe uses the CIS as his baseline, what controls or steps does this meet?

The step that it meet is Continuous Vulnerability Management. If Joe applies this rule,

then they will continually monitor the computer for vulnerabilities. They will scan the computer, and will look at firewall and virus protection to see if it is on.

## **System and Security**

At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

- Firewall
- Virus & Threat Protection
- App & Browser Control
- User Account Control settings
- Securing Removable Media



## Firewall

You need to ensure the Windows Firewall is enabled for all network access.

- Explain the process you take to do this.

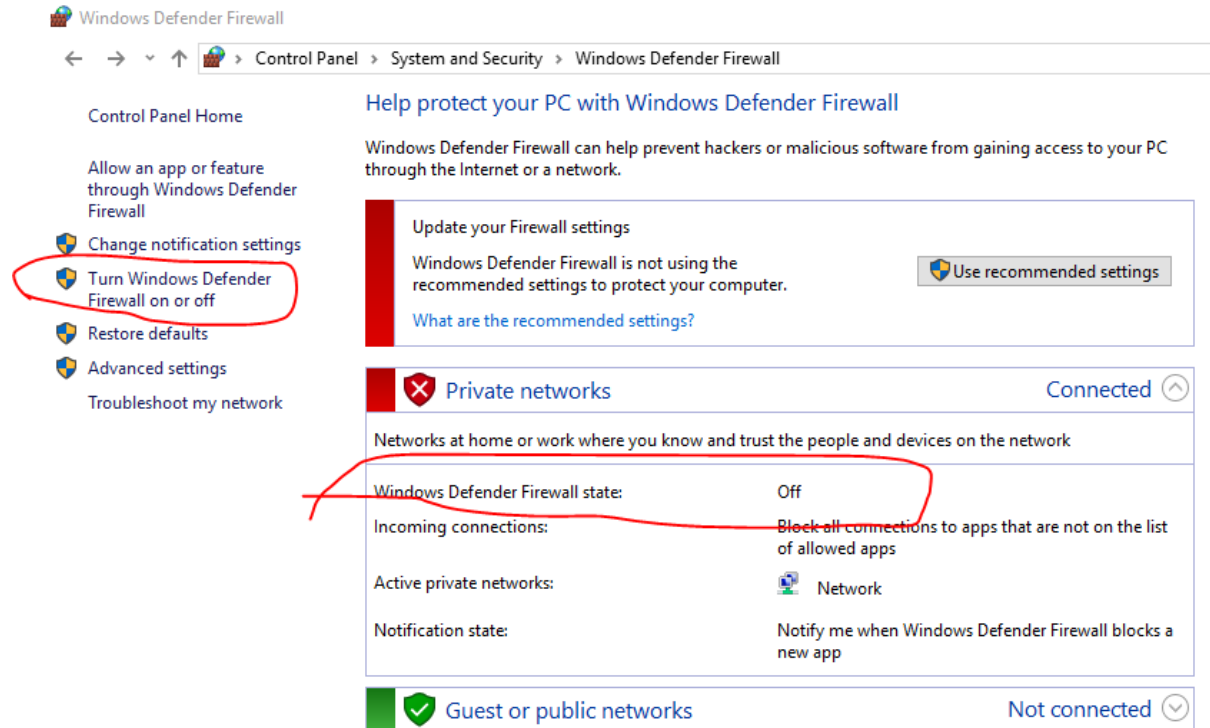
First, I will go to Control panel, then I will click on Systems and Security.

Next step that I will take is Click on the Windows Defender Firewall.

I checked that the firewall is currently turned off, so now I am going to turn the firewall on.

If I want to turn on the firewall, I will look on the left panel there a a tab that says

"Turn Windows Defender Firewall on or Off". I click on that button to turn on the firewall.





- Include screenshots showing the firewall is turned on.



## Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

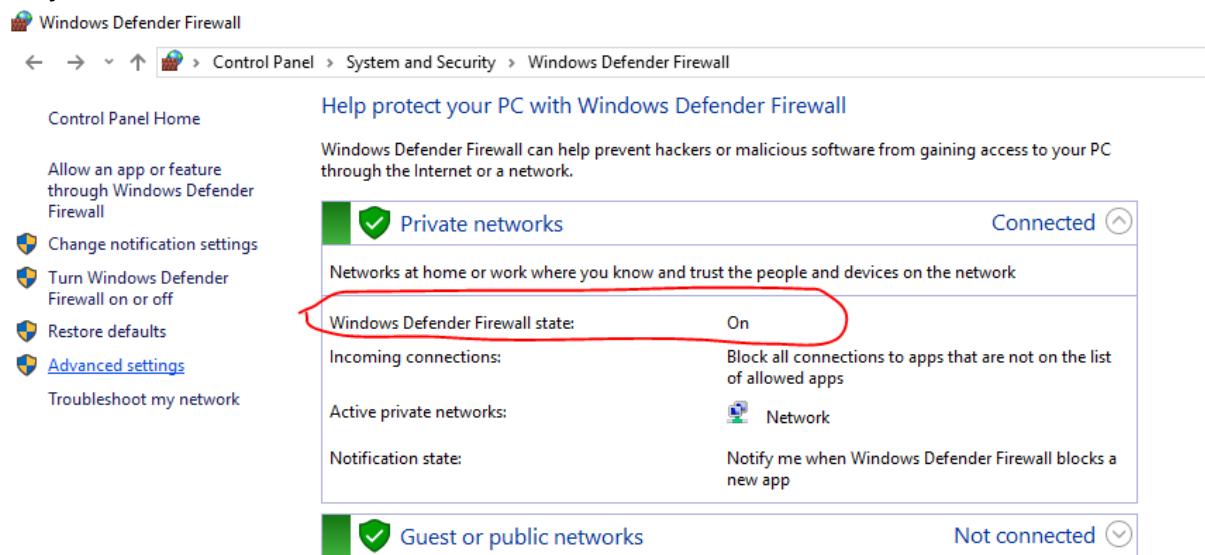
### Private network settings

-  ☒ Turn on Windows Defender Firewall
  - ☐ Block all incoming connections, including those in the list of allowed apps
  - ☒ Notify me when Windows Defender Firewall blocks a new app
-  ☐ Turn off Windows Defender Firewall (not recommended)

### Public network settings

-  ☒ Turn on Windows Defender Firewall
  - ☐ Block all incoming connections, including those in the list of allowed apps
  - ☒ Notify me when Windows Defender Firewall blocks a new app
-  ☐ Turn off Windows Defender Firewall (not recommended)

*I clicked on the turn on Windows Defender Firewall, and then I press ok . the image below shows that the firewall has been turned on .*



- What protection does this provide?

The firewall protects the computer by blocked intruders or unwanted users on the computer. It does this by blocking malicious websites, and shielding your computer from cyber attacks.

### **Virus & Threat Protection**

You need to ensure the Windows Defender anti-virus is enabled to always protect against current threats. It should be set to automatically update and continually scan the PC for malicious software. Note: Ignore any alerts about setting up OneDrive.

- *Explain the process you take to do this.*

*I will type Control Panel in the search bar, and once I am in the control panel then I will click on the Systems and Security tab. I will click on Security and Maintenance, then click on the Virus protection. I will then view in windows security. It seems that the virus and threat protection is enabled on the computer, and that the last time that it was scanned was 1/22/2021, so it means that the virus protection is activated.*

- *Include screenshots to confirm that anti-virus is enabled.*

Windows Security



Home



Virus & threat protection



Account protection



Firewall & network protection



App & browser control



Device security



Device performance & health



Family options



## Virus & threat protection

Protection for your device against threats.



### Current threats

No current threats.

Last scan: 1/22/2021 5:58 AM (quick scan)

0 threats found.

Scan lasted 2 minutes 30 seconds

37009 files scanned.

Quick scan

[Scan options](#)

[Threat history](#)



### Virus & threat protection settings

No action needed.

[Manage settings](#)



### Virus & threat protection updates

Protection definitions are up to date.

Last update: 1/22/2021 7:53 PM

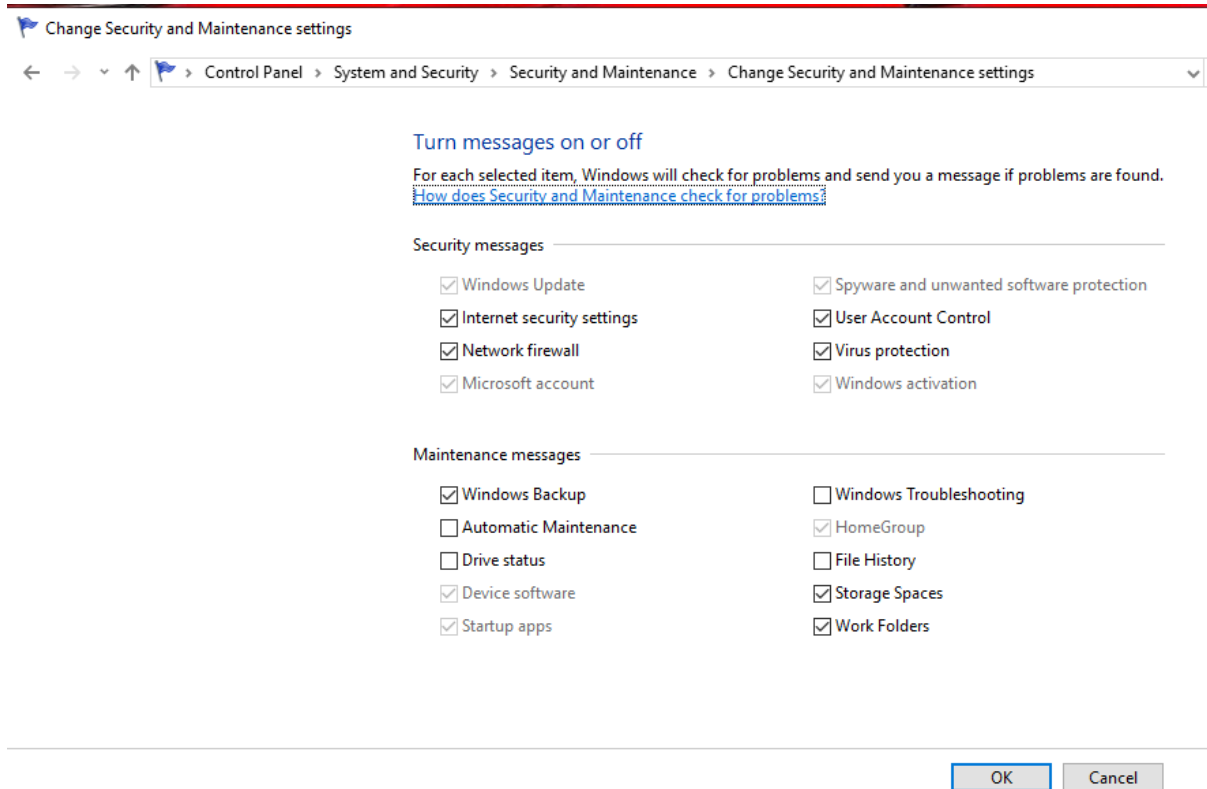
[Check for updates](#)



### Ransomware protection

Once you determine that virus & threat protection is on and updated, you need to turn on messages about the Network firewall and Virus protection. Refer to the instructions above for viewing the settings within Security and Maintenance, Review recent messages and resolve problems.

- Turn on the Network firewall and Virus protection messages using Change Security and Maintenance Settings.
- Show a screenshot here of them enabled.



- Provide at least two risks mitigated by enabling these security settings:
- 1) Virus Protection . The Virus protection is enabled so the computer continuously scan the computer for viruses. It makes the computer more safe.
- 2) Network Firewall is enabled. If the firewall is enabled, then it makes browsing the web safe. It can help block dangerous websites.
- From the CIS baseline controls, provide the controls satisfied by completing this.

The control that is satisfied is Controlled use of admin privilege. I believe that it is this rule because only one person should be allowed to monitor virus and firewall protection.

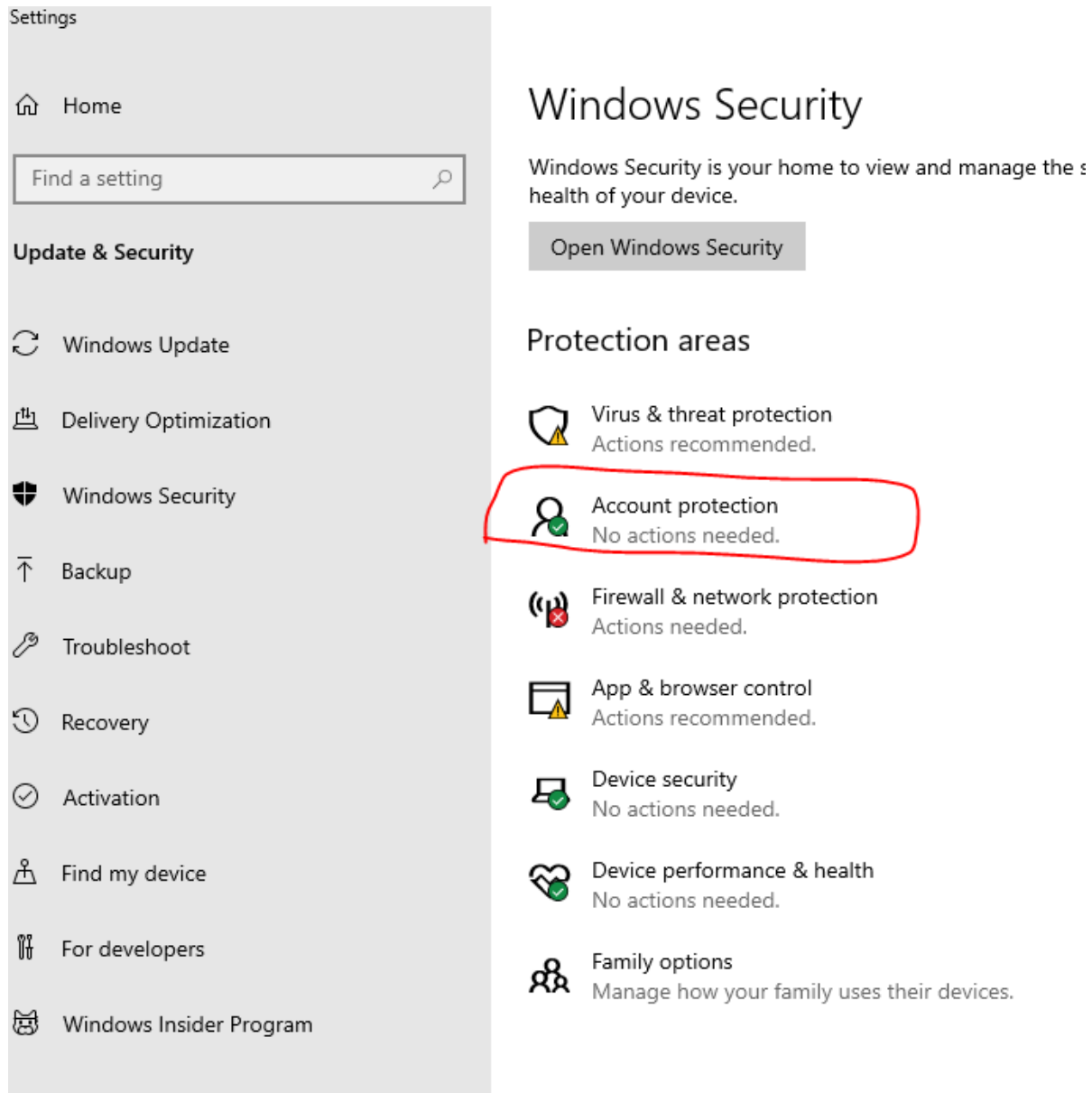
## App & Browser Control

The App protection within Windows Defender helps to protect your device by checking for unrecognized apps and files and from malicious sites and downloads. Review the settings found within the *Account protection window*, and *App & browser control windows* found on the *Windows Defender Security page*.

Advanced students: You should also review the settings on the Exploit protection page.

- Change the settings to provide **maximum** protection for Joe's PC and provide a screenshot of your results.

For the Action Protection window, it says no action needed.



-

≡

🏠 Home

🔒 Virus & threat protection

🔒 Account protection

🔒 Firewall & network protection

🔒 App & browser control

🔒 Device security

🔒 Device performance & health

## 👤 Account protection

Security for your account and sign-in.

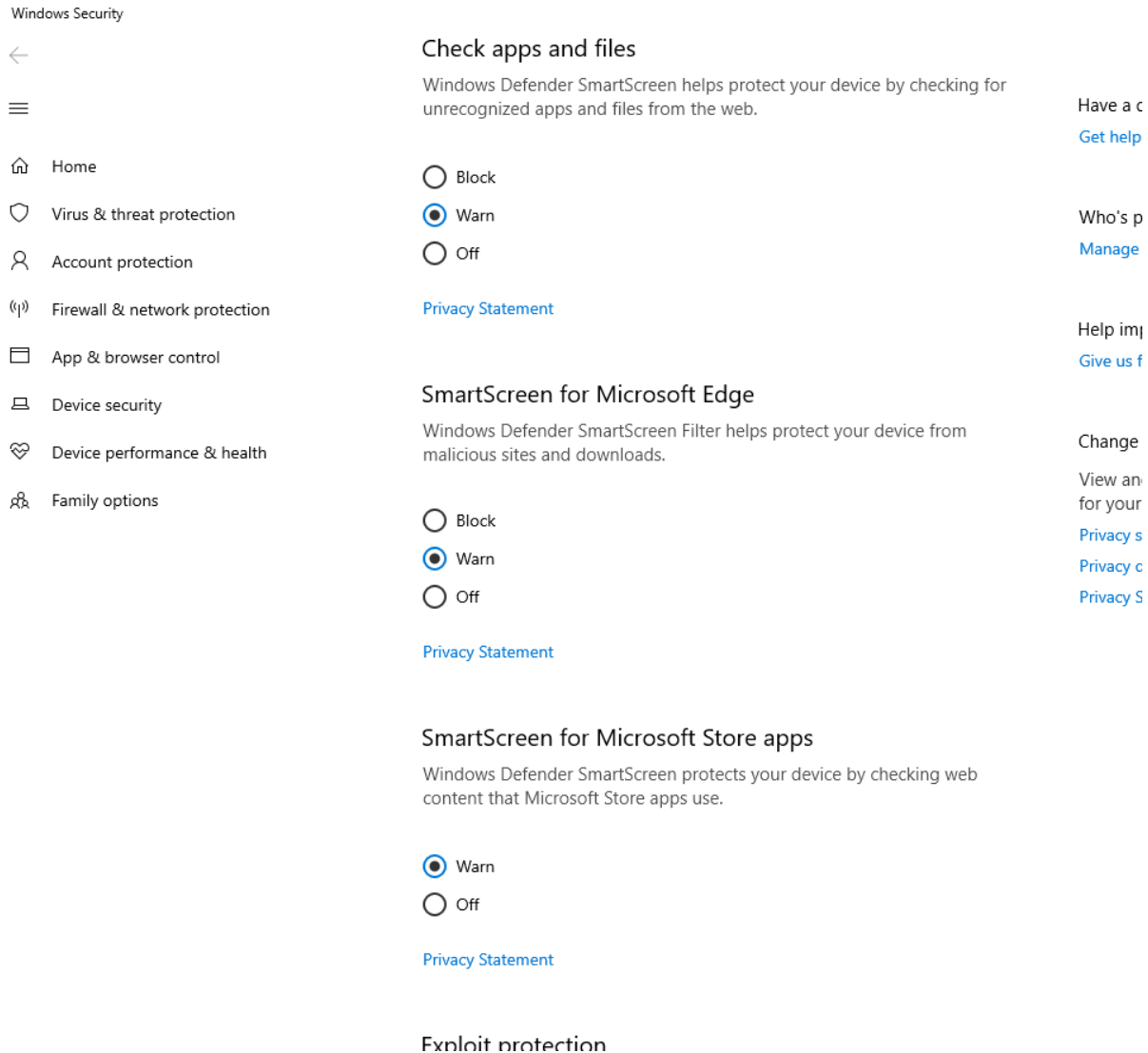
### 🔒 Dynamic lock

Dynamic lock is unavailable over remote sessions.

[Dynamic lock settings](#)

*When I tried to click on the Account Protection, it says Dynamic Lock.*

*I don't think that for Account Protection it needs to be activated because its already protected.*



For App & Browser Control Window, I click on the tab and then it gives me three options: Block, Warn, or Off. I believe that Block and Off will both close or block it. For this assignment, it says maximum protection for Joe's PC so I believe that the best option is to warn.

## User Account Control Settings

Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer. This is done through the User Account Control Setting.

- What is the current UAC setting on Joe's computer?

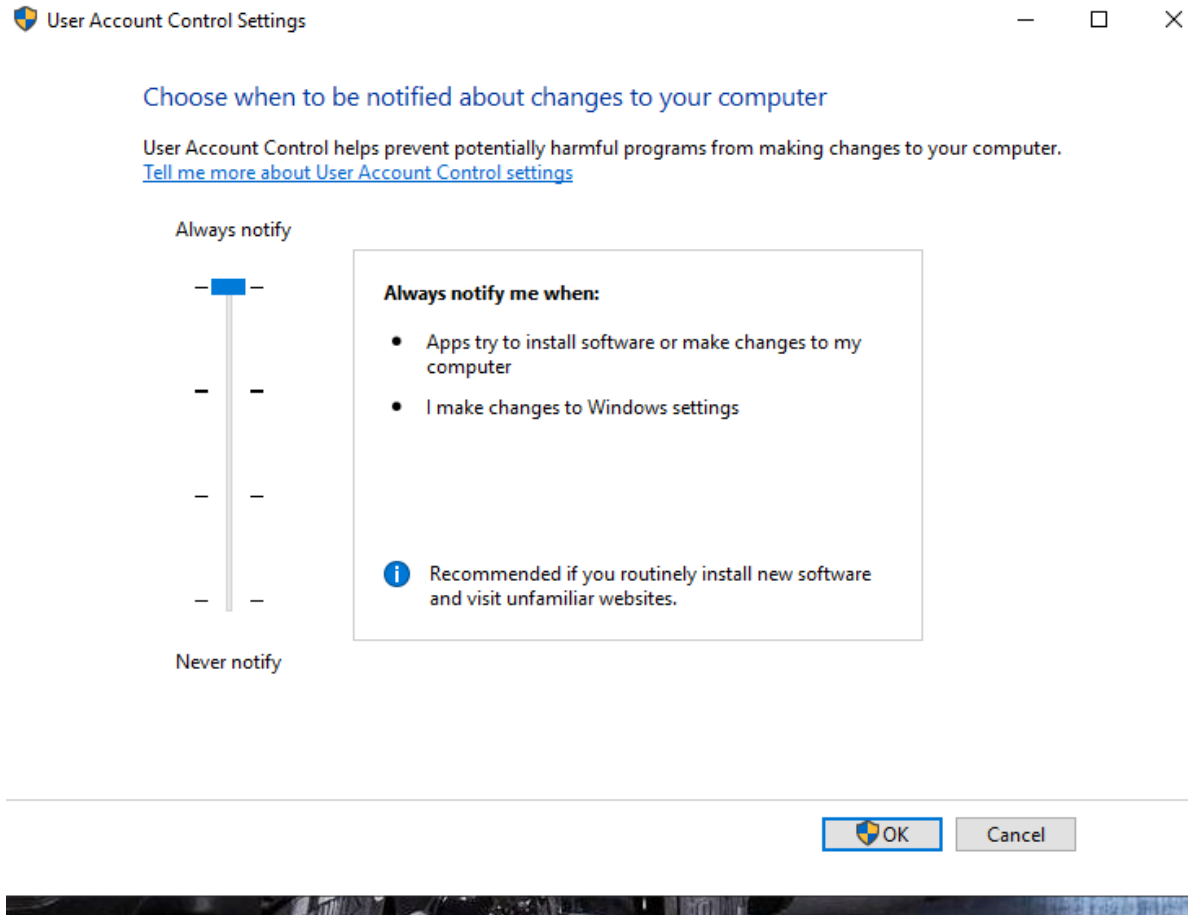
The current UAC setting on Joe's computer is that it is on never notify.



This is available from the above security settings.

- *What should it be set to? Include a screenshot of the new setting.*

*It should be set to Always Notify. It should be set to Always Notify to provide maximum security.*

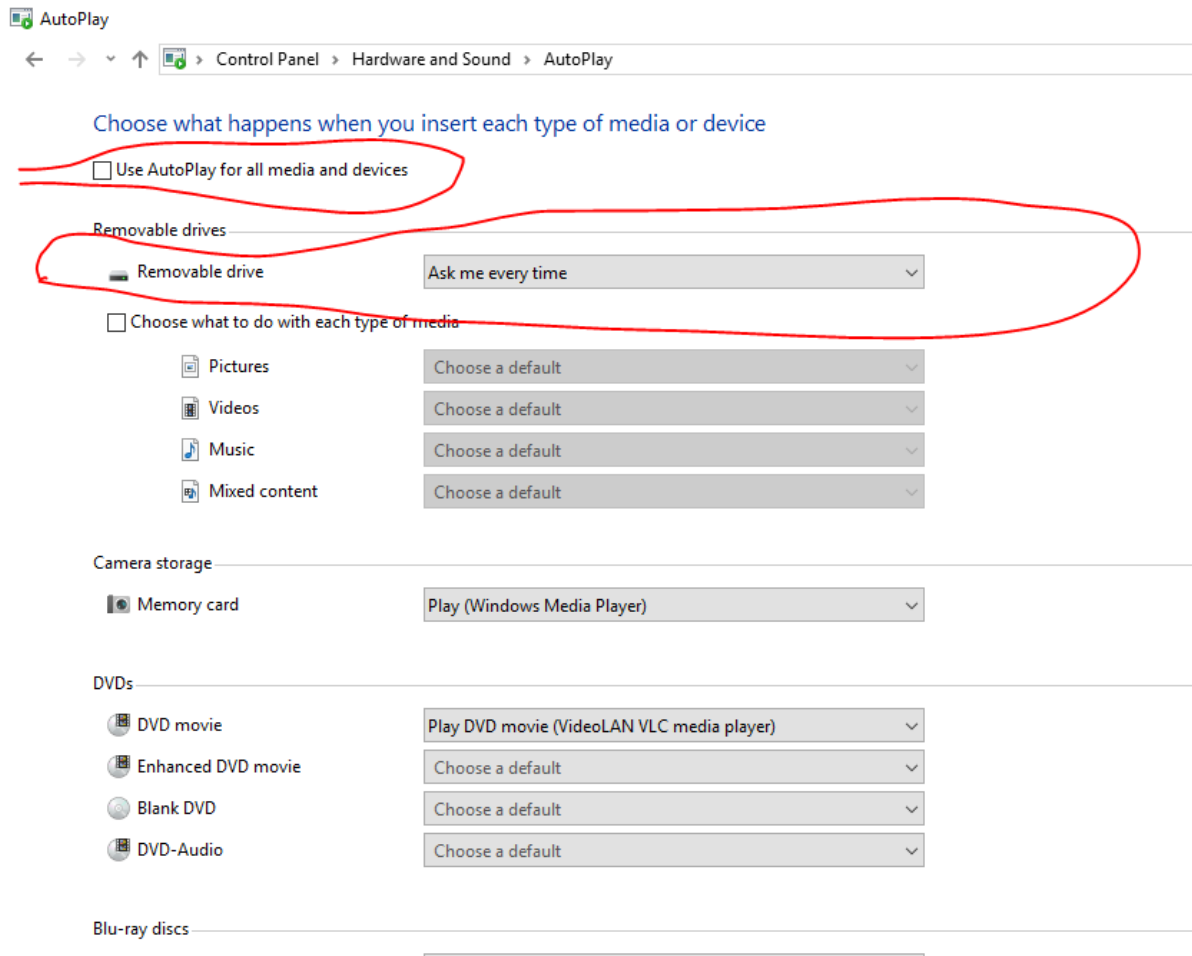


## Securing Removable Media

A security best practice is to not allow the use of removable hard drives (USB sticks, Memory Cards, and DVDs). They are needed as part of Joe's backup policy. The next best thing is to make sure that any applications don't automatically start when the media is inserted and the user is asked what should happen. This is set from the Control Panel > Hardware and Sound > Autoplay menu.

- *On Joe's computer, go to that function and deselect "Use AutoPlay for all media and devices."*

- For the Removable Drive, make the default, “Ask me every time.” Include a screenshot of your results.



### 3. Securing Access

Ensuring only specific people have access on a computer system is a common step in information security. It starts by understanding who should have access and the rules or policies that need to be followed.

On Joe’s computer, only the following accounts should be in use:

- JoesAuto
- Jane Smith (Joe’s assistant)
- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)

Joe’s Auto Access Rules:

- Only JoesAuto and A User should have administrative privileges on this PC.
- Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.
- All valid users should have a password following Joe's password policy below
  - At least 8 characters
  - Complexity enabled
  - Changed every 120 days
  - Cannot be the same as the previous 5 passwords
- Account should be automatically disabled after 5 unsuccessful login attempts. The account should be locked for 15 minutes and then should automatically unlock.
- Upon first logging into the PC, Joe wants a warning banner letting anyone using to know that this is to only be used for work at Joe's Auto Body shop by authorized people.
- There is to be no remote access to this computer.

## User Accounts

- *What user accounts should not be there?*

*1) A Hacker and 2) Do Not Use 3) Frank*

- *Bonus questions: What is Hacker's password?*

*Notahackers123*

- *Explain the steps you take to disable or remove unwanted accounts.*

*The steps that I took to disable or remove unwanted accounts is go to settings then Click on other users.*

*If I wanted to remove an account, I will click on the user and then click remove button.*

- *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*

*It is important to remove unneeded accounts from a pc because you shouldn't let everyone to have access to your computer. An example of a vulnerability is :You don't want a disgruntled employee on your computer because if he is angry and he uses your computer he might share the company's information with other people. You should limit computer use to a few people.*

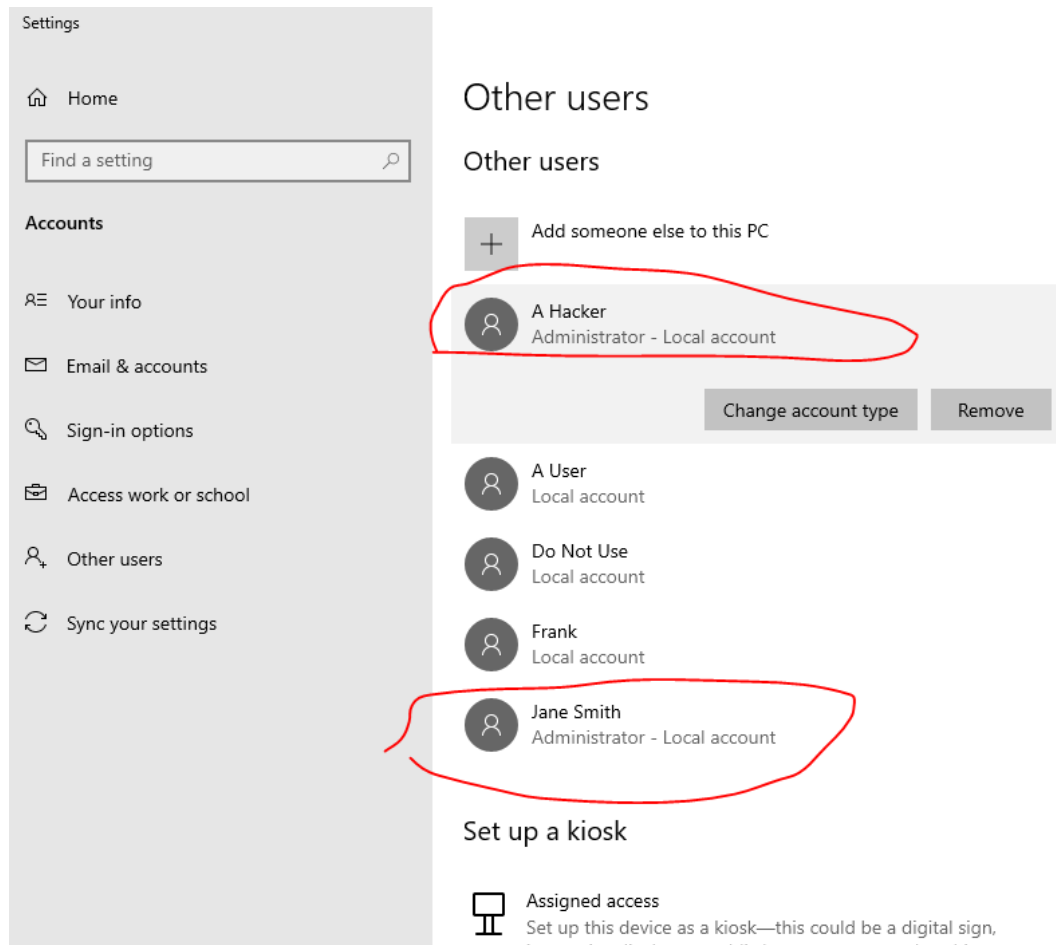
*You should only allow people with authorized access to your computer, so that it will make your company safe.*

Only specific accounts should have administrator privileges. This reduces the ability for unwanted applications to be installed including malware.

- Which account(s) have administrator rights that shouldn't?
- The Accounts that have administrator rights that shouldn't are :

*1) Jane Smith and 2) A Hacker*

- Explain how you determined this. Provide screenshots as needed.



The only administrator accounts is a hacker and Jane Smith.

The hacker shouldn't have admin privilege. I also believe that Jane smith shouldn't have admin privilege because I read the instructions and it says only JoesAuto and A User should have administrative privileges on this pc.

Administrator privileges for too many users are another security challenge.

- Provide at least three risks associated with users having administrator rights on a PC.
- 1)Creating or deleting user accounts.
- 2)Changing Passwords for an user account
- 3)Change Network Settings

Now you need to remove administrator privileges for any user(s) that should have it.

- *Explain the process for doing this. Include screenshots to show your work.*

*First, I would type Control Panel on the search bar then I would click on User Accounts.*

*When I click on User Accounts, then I click on account type.*

## Adjust your computer's settings

View by: [Category](#) ▼



### System and Security

Review your computer's status  
Save backup copies of your files with File History  
Backup and Restore (Windows 7)



### Network and Internet

View network status and tasks



### Hardware and Sound

View devices and printers  
Add a device



### Programs

Uninstall a program



### User Accounts

[Change account type](#)



### Appearance and Personalization



### Clock and Region

Change date, time, or number formats



### Ease of Access

Let Windows suggest settings  
Optimize visual display

## Choose the user you would like to change



### Joes Account

Local Account  
Administrator  
Password protected



### A Hacker

Local Account  
Administrator  
Password protected



### A User

Local Account  
Password protected



### Do Not Use

Local Account  
Password protected



### Frank

Local Account  
Password protected



### Jane Smith

Local Account  
Administrator  
Password protected

[Add a user account](#)

*For this example, I am going to choose A Hacker as an example. I am going to click on A Hacker Icon, the I click on change the account type .*

## Make changes to A Hacker's account

[Change the account name](#)

[Change the password](#)

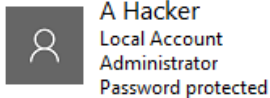
[Change the account type](#)

[Delete the account](#)

[Manage another account](#)



## Choose a new account type for A Hacker



☒ Standard

Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

☐ Administrator

Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

[Why is a standard account recommended?](#)

Change Account Type

Cancel

*If I wanted to change administrative privilege and not let A Hacker be and Administrator, then I would Click on Standard Button and last step is to change account type.*

- *What is the security principle behind this?*

*The Security principle behind this is that if you believe than an employee is not authorized to become an administrator, then you can have an option to change the employee from administrator to a standard user.*

*You should only let people that you trust to become an administrator for your company.*

- The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

I would say that the step is : Controlled use of Administrative Privilege.

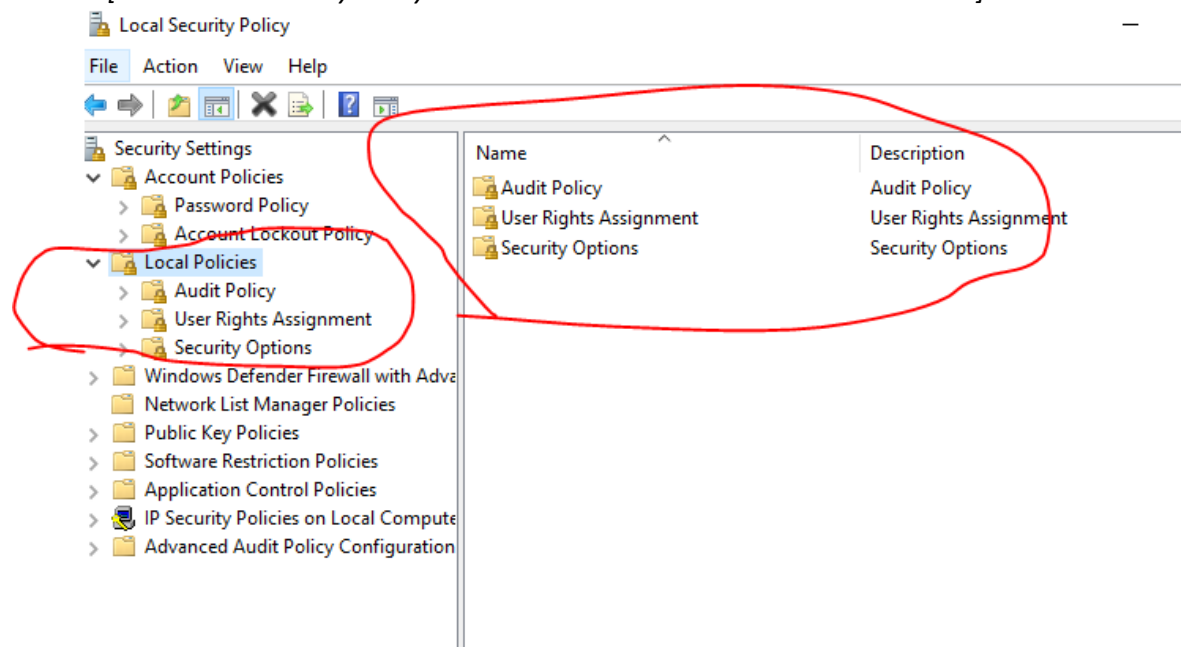
I believe that it is this step because they don't want everyone to have control to the computer.

They should only let people that are authorized on the computer to have administrative privilege.

## Setting Access and Authentication Policies

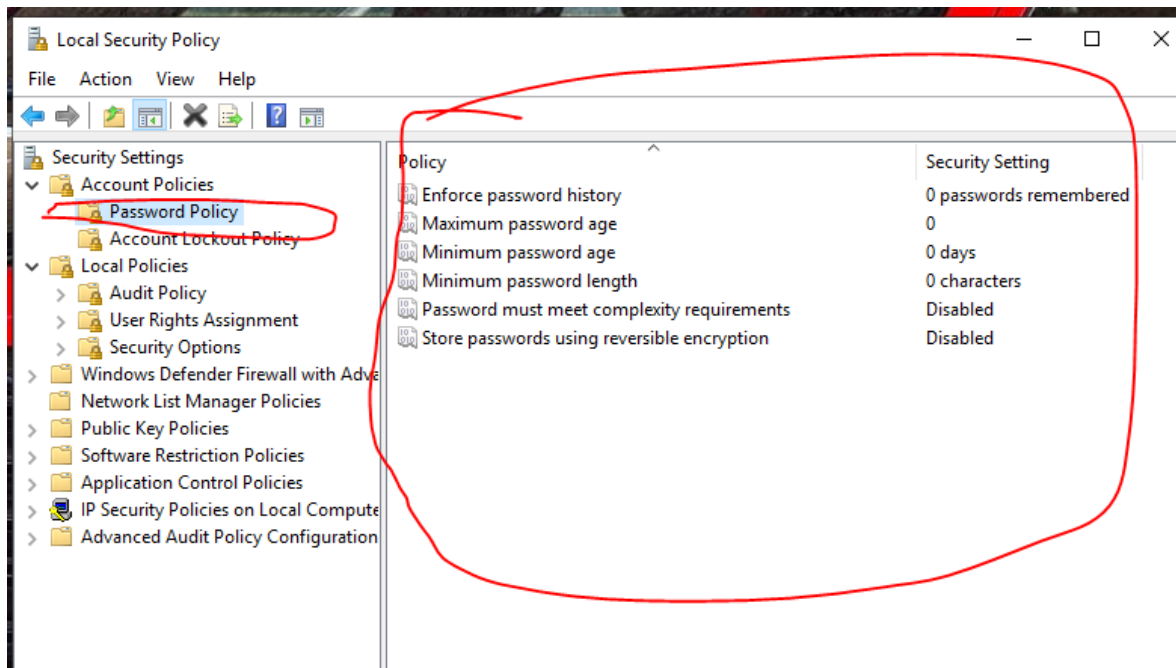
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type “Local Security Policy” to access it. Click the > arrow next to both “Account Policies” and “Local Policies” and review their contents.

- Provide a screenshot of the Local Security Policy window here.  
[Note: Local Security Policy is not available on Windows 10 Home edition.]

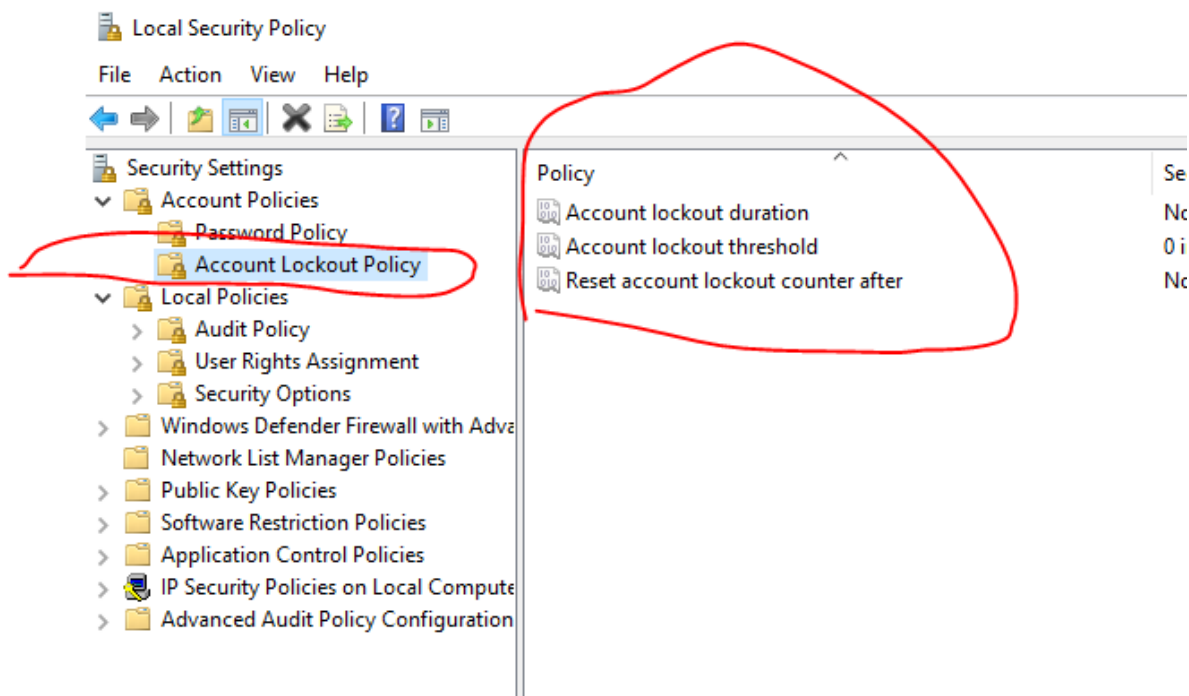


- Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.
  - Setting the Password Policy:
  - Setting the Account Lockout Policy:

\_\_\_ If I wanted to set the password policy, I first go to the Local Security Policy then I click on the password policy on the left panel. Once I click on it on the right, it shows the password policy under the policy tab.



If I wanted to set the account policy, then I would go to Local Security Policy-> click on Account Lockout Policy. It would show on the right the account policy.



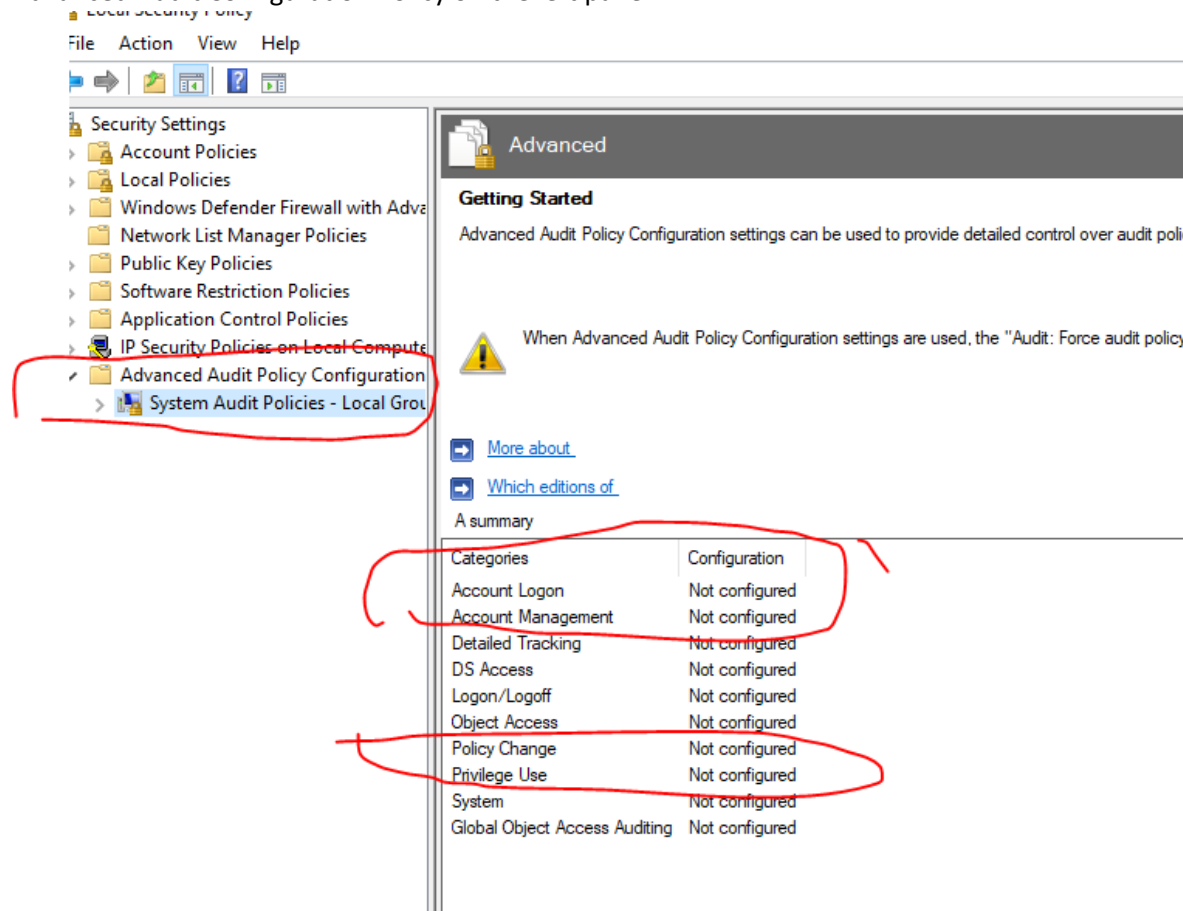
## ***Auditing and Logging***



Security best practices like those found in the CIS Controls or NIST Cybersecurity Framework require systems to log events. You need to enable the Audit Policy for Joe's PC to meet these standards.

- From the Local Security Policy window, select Audit Policy and make applicable changes to Joe's PC to enable minimal logging of logon, account, privilege use and policy changes.

I would start by typing Local Security Policy in the search bar. When I am on there I would click on the Advanced Audit Configuration Policy on the left panel.



- Provide a screenshot of your changes here.

Local Security Policy

FileActionViewHelp

Security Settings

> Account Policies

> Local Policies

> Windows Defender Firewall with Advanced Security

> Public Key Policies

> Software Restriction Policies

> Application Control Policies

> IP Security Policies on Local Computer

> Advanced Audit Policy Configuration

> System Audit Policies - Local Group Policy

> Account Logon

> Account Management

> Detailed Tracking

> DS Access

> Logon/Logoff

> Object Access

> Policy Change

> Privilege Use


> System

> Global Object Access Auditing

Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

Audit Credential Validation Properties

PolicyExplain

 Audit Credential Validation

☒ Configure the following audit events:

☒ Success

☐ Failure

OK

Cancel

Apply

Local Security Policy

File Action View Help

Security Settings

- > Account Policies
- > Local Policies
- > Windows Defender Firewall with Advanced Security
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Computer
- > Advanced Audit Policy Configuration
  - > System Audit Policies - Local Group Policy Objects
    - > Account Logon
    - > Account Management
    - > Detailed Tracking
    - > DS Access
    - > Logon/Logoff
    - > Object Access
    - > Policy Change
    - > Privilege Use
    - > System

Advanced

### Getting Started

Advanced Audit Policy Configuration settings can be used to...

When Advanced Audit Policy Configuration settings are configured...

[More about](#)

[Which editions of](#)

A summary

Categories	Configuration
Account Logon	Configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured

For Account:




- Security Settings
  - > Account Policies
  - > Local Policies
  - > Windows Defender Firewall with Advanced Security
  - > Network List Manager Policies
  - > Public Key Policies
  - > Software Restriction Policies
  - > Application Control Policies
  - > IP Security Policies on Local Computer
  - > Advanced Audit Policy Configuration
    - System Audit Policies - Local Group Policy
      - > Account Logon
      - > **Account Management**
      - > Detailed Tracking
      - > DS Access
      - > Logon/Logoff
      - > Object Access
      - > Policy Change
      - > Privilege Use
      - > System
      - > Global Object Access Auditing

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Not Configured
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Not Configured
Audit User Account Management	Not Configured

Audit Application Group Management Properties

Policy Explain

 Audit Application Group Management

☒ Configure the following audit events:

☒ Success

☐ Failure

OK Cancel Apply

Local Security Policy

File Action View Help

Security Settings

- > Account Policies
- > Local Policies
- > Windows Defender Firewall with Advanced Security
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Computer
- ▼ Advanced Audit Policy Configuration
  - ▼ System Audit Policies - Local Group Policy Objects
    - > Account Logon
    - > Account Management
    - > Detailed Tracking
    - > DS Access
    - > Logon/Logoff
    - > Object Access
    - > Policy Change
    - > Privilege Use
    - > System

Advanced

### Getting Started

Advanced Audit Policy Configuration settings can be

When Advanced Audit Policy Configuration is

[More about](#)

[Which editions of](#)

A summary

Categories	Configuration
Account Logon	Configured
Account Management	Configured
Detailed Tracking	Not configured

For Privilege Use:

Action View Help


Security Settings

- Account Policies
- Local Policies
- Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration
- System Audit Policies - Local Group Policy Objects
  - Account Logon
  - Account Management
  - Detailed Tracking
  - DS Access
  - Logon/Logoff
  - Object Access
  - Policy Change
  - Privilege Use
  - System
  - Global Object Access Auditing

Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Not Configured
Audit Other Privilege Use Events	Not Configured
Audit Sensitive Privilege Use	Not Configured

Audit Non Sensitive Privilege Use Properties

Policy Explain


Audit Non Sensitive Privilege Use

☒ Configure the following audit events:

☒ Success
☐ Failure

OK

Cancel

Apply

Local Security Policy

File Action View Help

Security Settings

- Account Policies
- Local Policies
- Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration
  - System Audit Policies - Local Group Policy Objects
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing

Advanced

### Getting Started

Advanced Audit Policy Configuration settings can be used to...

When Advanced Audit Policy Configuration settings are...

[More about](#)

[Which editions of](#)

A summary

Categories	Configuration
Account Logon	Configured
Account Management	Configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Configured
System	Not configured
Global Object Access Auditing	Not configured

Next is Policy Changes:

Local Security Policy

FileActionViewHelp

Security Settings

> Account Policies

> Local Policies

> Windows Defender Firewall with Adv

> Network List Manager Policies

> Public Key Policies

> Software Restriction Policies

> Application Control Policies

> IP Security Policies on Local Comput

> Advanced Audit Policy Configuration

> System Audit Policies - Local Grou

> Account Logon

> Account Management

> Detailed Tracking

> DS Access

> Logon/Logoff

> Object Access

> Policy Change

> Privilege Use

> System

> Global Object Access Auditing

Subcategory

Audit Audit Policy Change

Audit Authentication Policy Change

Audit Authorization Policy Change

Audit Filtering

Audit MPSSVC

Audit Other Po

Audit Events

Not Configured

Not Configured

Not Configured

Audit Audit Policy Change Properties

PolicyExplain

Audit Audit Policy Change

Configure the following audit events:

Success

Failure

OK

Cancel

Apply



Local Security Policy

File Action View Help

Security Settings

- > Account Policies
- > Local Policies
- > Windows Defender Firewall with Adv
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Compute
- > Advanced Audit Policy Configuration
  - > System Audit Policies - Local Gro
    - > Account Logon
    - > Account Management
    - > Detailed Tracking
    - > DS Access
    - > Logon/Logoff
    - > Object Access
    - > Policy Change
    - > Privilege Use
    - > System
    - > Global Object Access Auditing

Advanced

### Getting Started

Advanced Audit Policy Configuration settings can be u

When Advanced Audit Policy Configuration se

[More about](#)

[Which editions of](#)

A summary

Categories	Configuration
Account Logon	Configured
Account Management	Configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Configured
Privilege Use	Configured
System	Not configured

## 4. Securing Applications

As part of the inventory process, you determined computer programs or applications on the PC. The next step is to decide which ones are needed for business and which ones should be removed.

Unneeded programs could be vulnerable to attacks and allow unauthorized access into the computer. They also consume system resources and could also violate licensing agreements.

Joe has established the following rules regarding PC applications:

- Joe wants everyone to use the latest version of the Chrome browser by default.
- There should be no games or non-work-related applications installed or downloaded.
- Joe is also concerned that there are “hacking” programs downloaded or installed on the PC that should be removed.
- This PC is used for standard office functions. The auto-body has a separate service they use for their website and to transfer files from their suppliers.

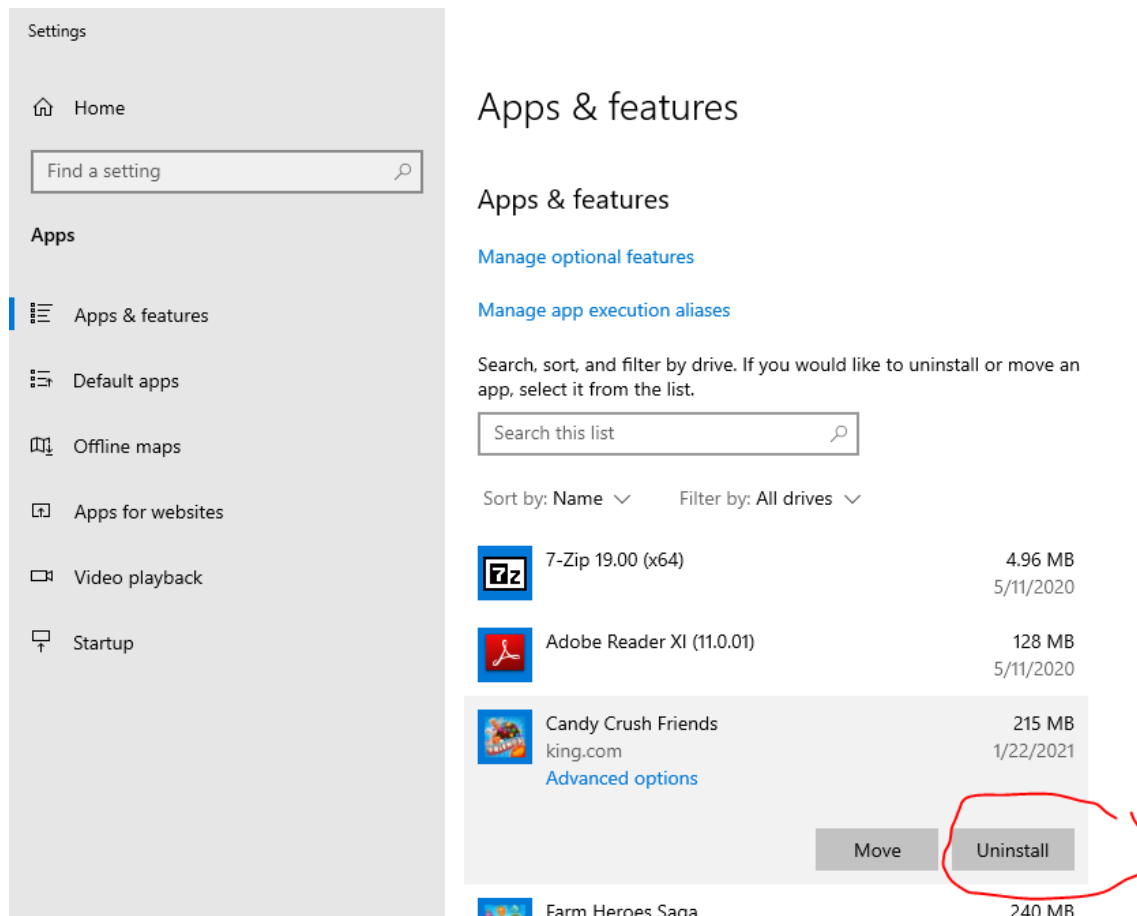
### ***Remove unneeded or unwanted applications***

- *List at least three application(s) that violate this policy.*
- *1) Google Chrome*
- *2) Candy Crush Friends*
- *3) Streaming Audio Recorder*
- *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*
- *1) If the google chrome is outdated, it needs to be updated to be more safe.*
- *2) Games is not needed on the business computer, and should be removed.*

*Playing games violate the companies policy. Having games on the computer waste the computer 's storage and it should be deleted.*

- 3) *You should get rid of hacking programs because it might have malware.*
- *Joe wants you to make sure unneeded applications or programs are no longer on the PC. Explain the steps you take to disable or remove them. Include screenshots to show your work.*

*I would type apps and features into the search bar, then I would click on the program that I wanted to remove. Let's take for example) Candy Crush Saga so I want to remove this game from my computer. I would click on it and click uninstall.*



## Default Browser

As mentioned in the policy, Joe wants all users to use Chrome as their browser by default.

- Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.

First, I would type apps and features in the search bar. When I get to apps and features, on the right side there is change default apps. I click on the Open Default app settings.

## Apps & features

### Installing apps

Choose where you can get apps from. Installing only apps from the Store helps protect your PC and keep it running smoothly.

☐ Turn off app recommendations

### Apps & features

[Manage optional features](#)

[Manage app execution aliases](#)

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

Sort by: **Name** Filter by: **All drives**

	7-Zip 19.00 (x64)	4.96 MB 5/11/2020
	Adobe Reader XI (11.0.01)	128 MB 5/11/2020
	Candy Crush Friends king.com	215 MB 1/22/2021
	Farm Heroes Saga king.com	240 MB 1/22/2021
	Google Chrome	

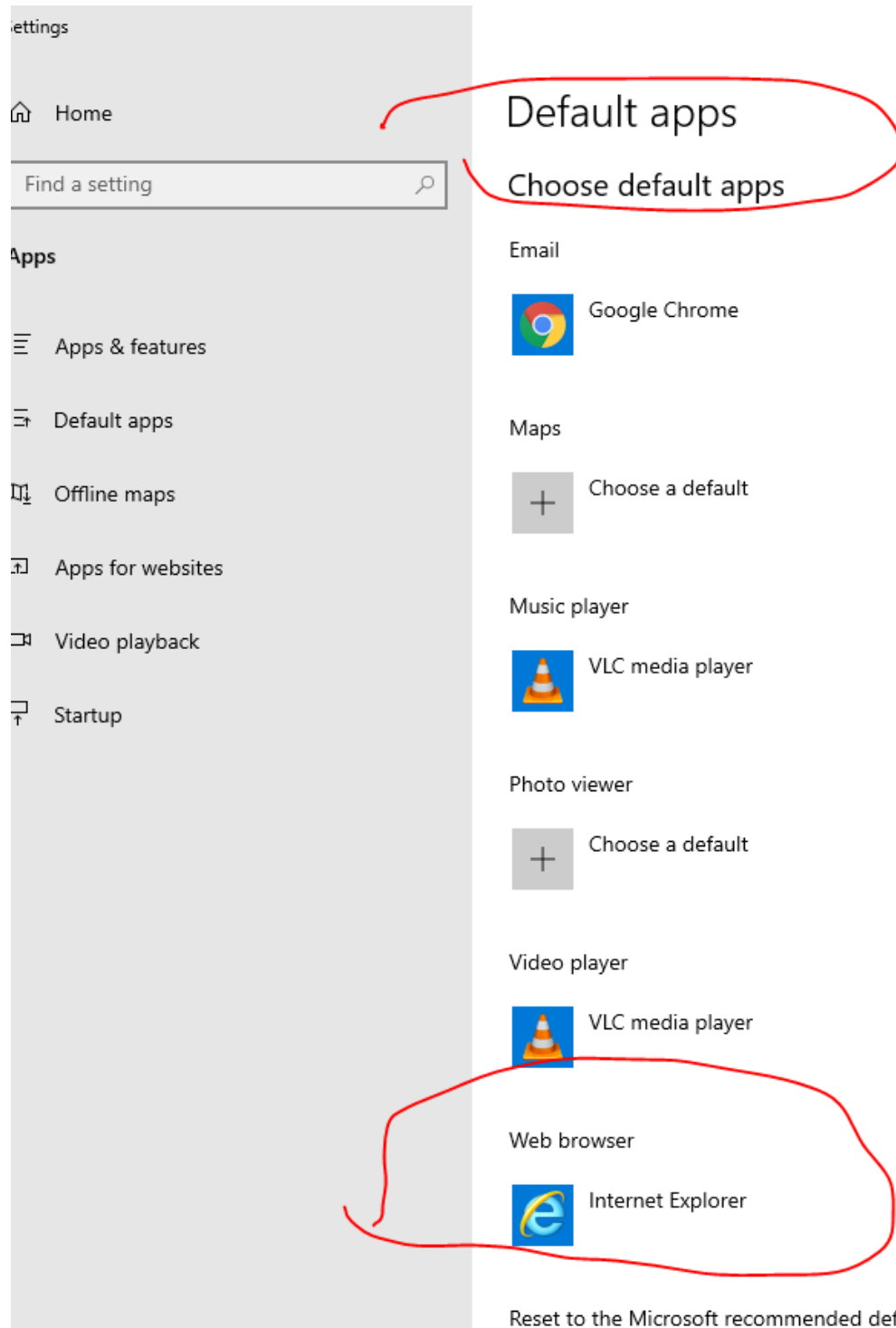
### Change app defaults

To choose the default apps that open your files, links, and more, go to Default app settings.

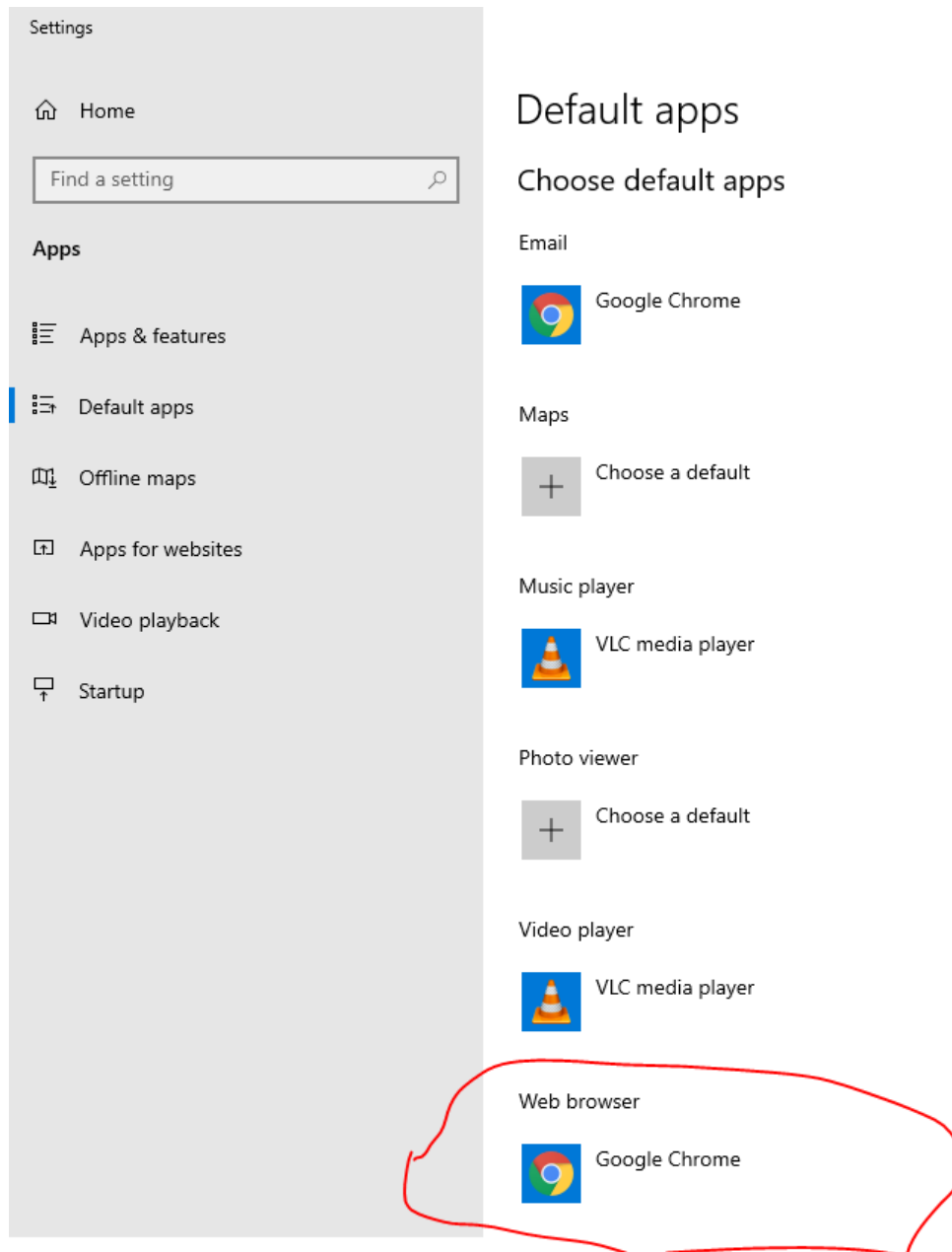
[Open Default app settings](#)

### Related settings

[Programs and Features](#)



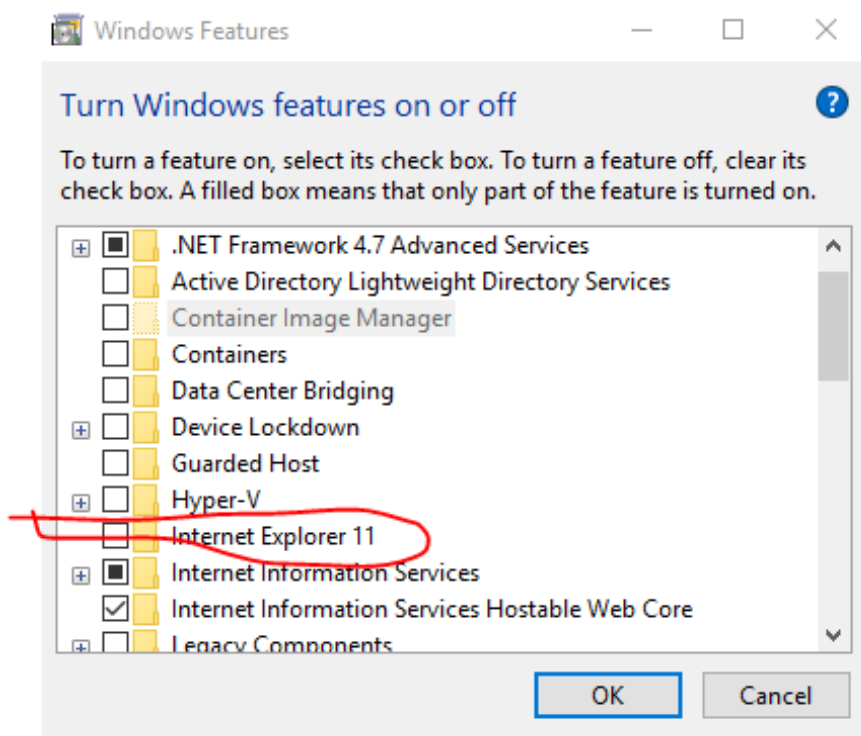
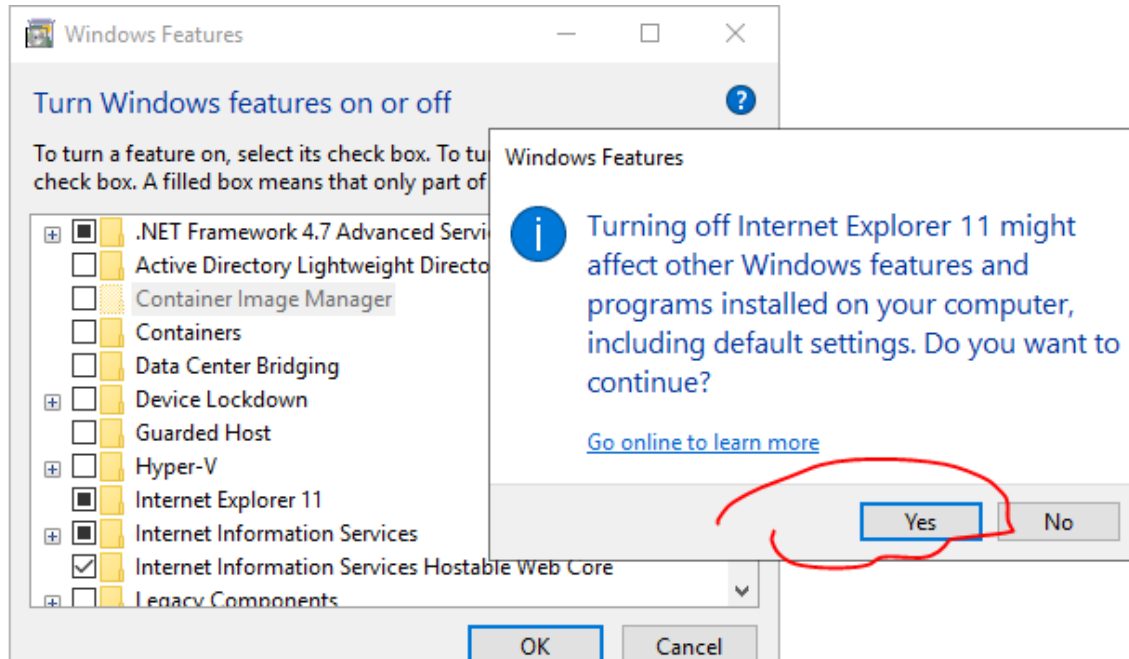
*Then I click on the Internet Explorer and click on Google Chrome to make Google Chrome as the default Browser.*



- *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
  - 1) Internet Explorer is outdated. It seems like no one uses Internet Explorer anymore. Google Chrome and Mozilla Firefox are more popular Internet Browsers.
  - 2) Internet Explorer has less safety features while Google Chrome is more safe and makes a better Internet Browser.

Because of the reasons you give above, Internet Explorer should be removed. To do that, go to the **Control Panel**, select **Programs**. On the **Programs and Features** window, select “**Turn Windows features on or off.**”

- Provide a screenshot showing Internet Explorer 11 is off.



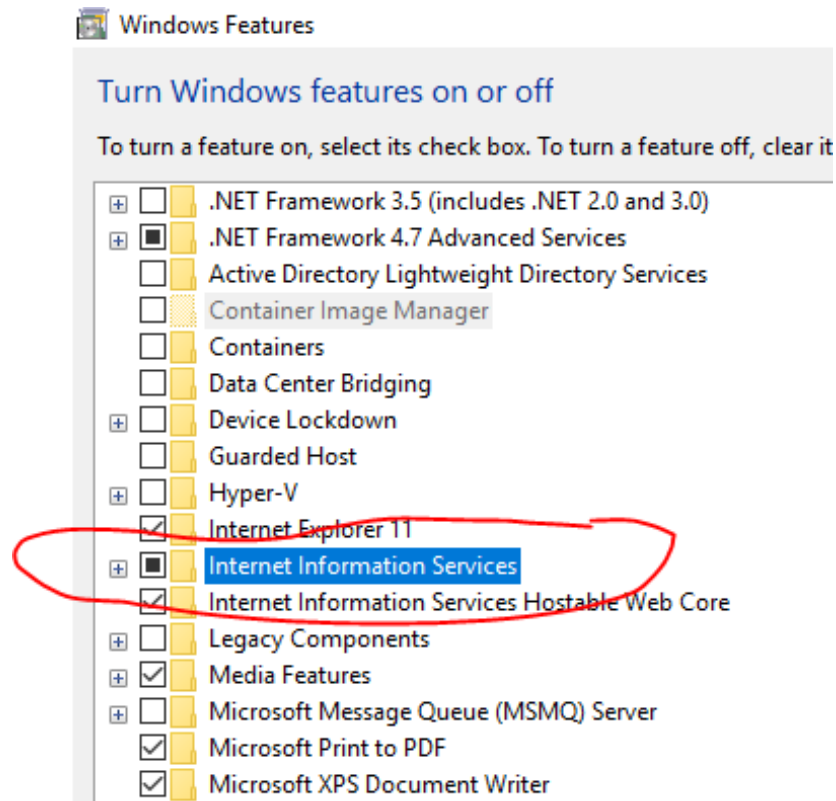
## Windows Services

There are Windows features running on Joe's computer that could allow unwanted activity or files. He suspects that someone may have used the PC as a web server in the past. Joe wants you to confirm if web services are turned on, stop it if it is and make sure it is not running whenever the computer restarts.

- How did you determine these services were running? Include screenshots to show how you found them.

I typed Windows Features into the search bar. When I am on the Windows features, I went to turn windows features on or off.

I determined that the services were running by Internet Information Services. To turn it off, I would click on the Internet Information Service.



- Advanced users should provide at least two methods for determining a web server is running on a host
- How do you disable them and make sure they are not restarted?

I believe I just click on the Internet Information Services, and that is how to disable them and make sure they are not restarted.



- Advanced Users: The File Transfer Protocol FTP service is also running on this PC and shouldn't. Explain the process for disabling it and ensuring it is not automatically restarted.

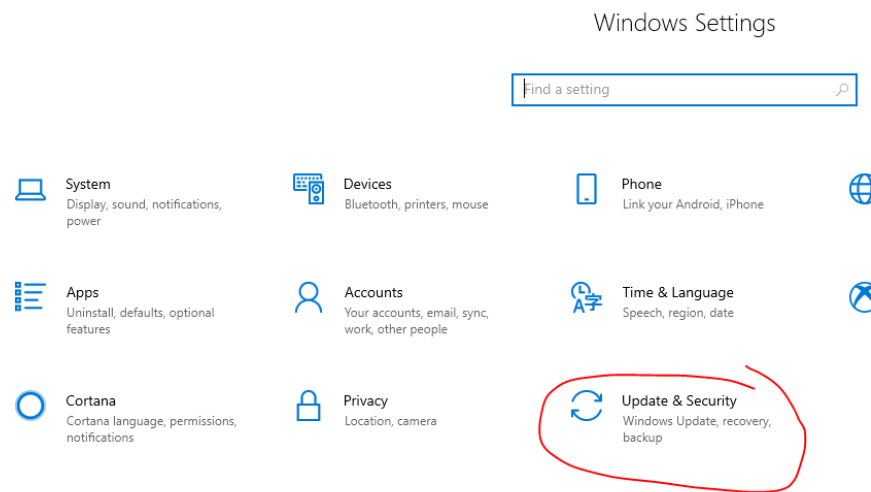
## ***Patching and Updates***

Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

- *Explain the process for doing this. Include screenshots as needed.*


*First, I would start by typing settings into the search bar. I would click on the updates & security icon. I would then scroll down and click on the download button to update the PC to its latest version.*

Settings



Windows Update

\*Some settings are managed by your organization  
[View configured update policies](#)

 **Updates available**  
Last checked: Yesterday, 5:47 AM

Feature update to Windows 10, version 1909  
**Status:** Pending download

Windows Malicious Software Removal Tool x64 - v5.85 (KB890830)  
**Status:** Pending download

2020-11 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Version 1809  
**Status:** Pending download

2020-10 Update for Windows 10 Version 1809 for x64-based Systems (KB4023057)  
**Status:** Pending download

2020-10 Security Update for Adobe Flash Player for Windows 10 Version 1809 for x64-based Systems (KB4486153)  
**Status:** Pending download

Microsoft .NET Framework 4.8 for Windows 10 Version 1809 for x64 (KB4486153)  
**Status:** Pending download

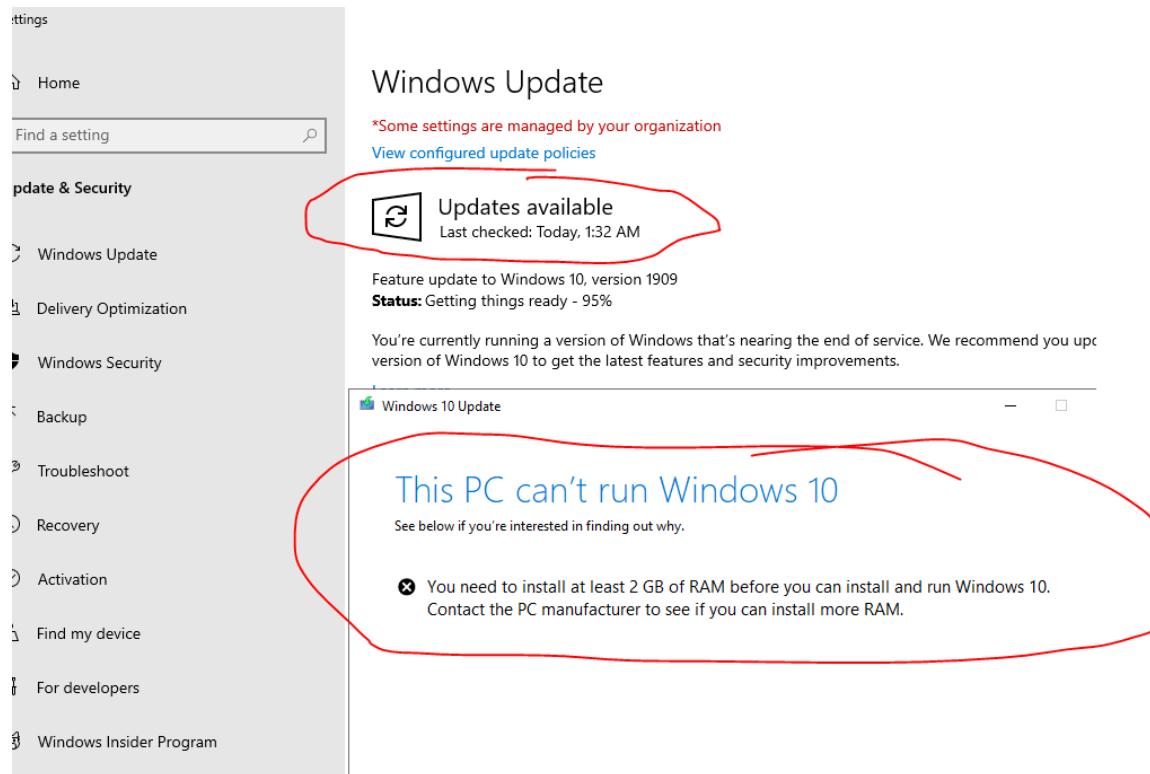
2019-02 Update for Windows 10 Version 1809 for x64-based Systems (KB4465065)  
**Status:** Pending download

Updates are ready to download

[Download](#)

You're currently running a version of Windows that's nearing the end of service. We recommend you update to the latest version.

- Go ahead and update this PC to the latest version. Warning this may take a while and require numerous restarts. When it is complete, provide a screenshot showing the PC is on the latest version.



*I updated the windows update to the most recent that I can. It is updated to today at 1:32 AM.*

*I tried to update it more, but it gave me an error message saying that I can finish updating it because the windows 10 computer ran out memory and its needs 2 GB of RAM.*

All applications should also be up to date on patches or fixes provided by the manufacturer. Any old versions of software should be uninstalled.

- *List at least two applications on Joe's PC that are out of date. List them below:*

- 1) Microsoft Visual C++ 2013
- 2) VNC Viewer 6.20.113

- *Explain the steps you took to determine this information.*

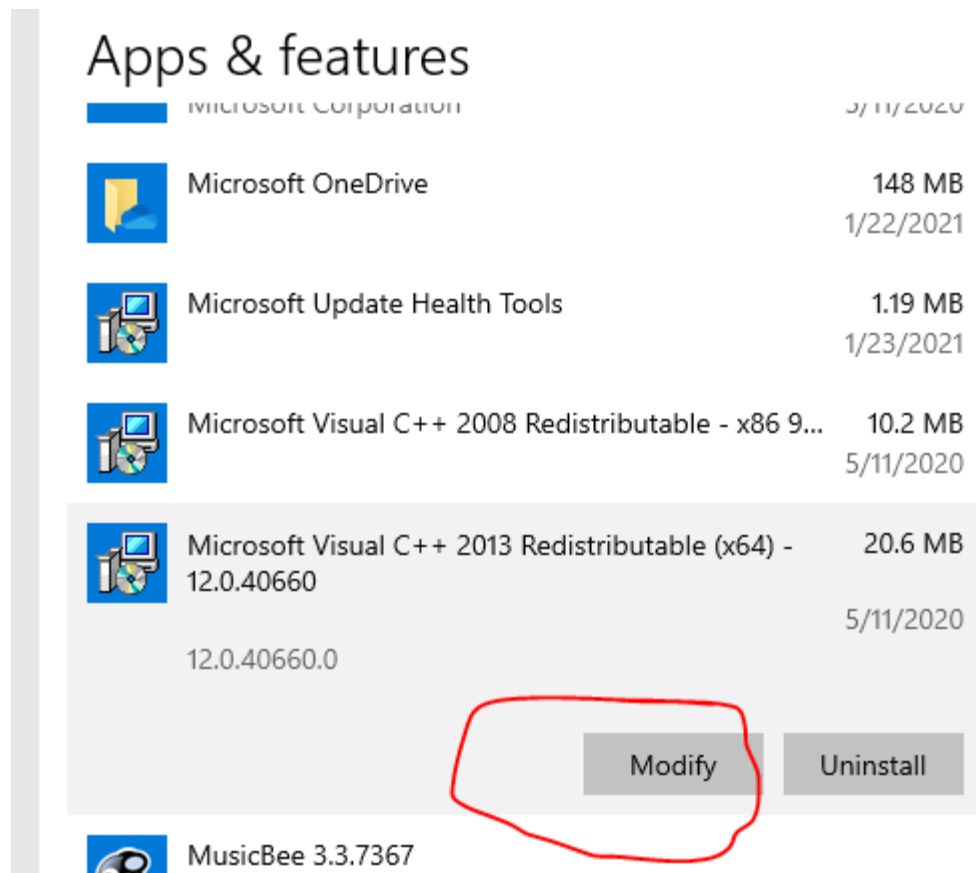
*I typed apps and features in the search bar, then I looked at the list of apps.*

*Next to the apps, there is a date and I believe that the date is when the apps were last updated.*

- *Explain the steps for updating each of these applications. Include screenshots as needed.*

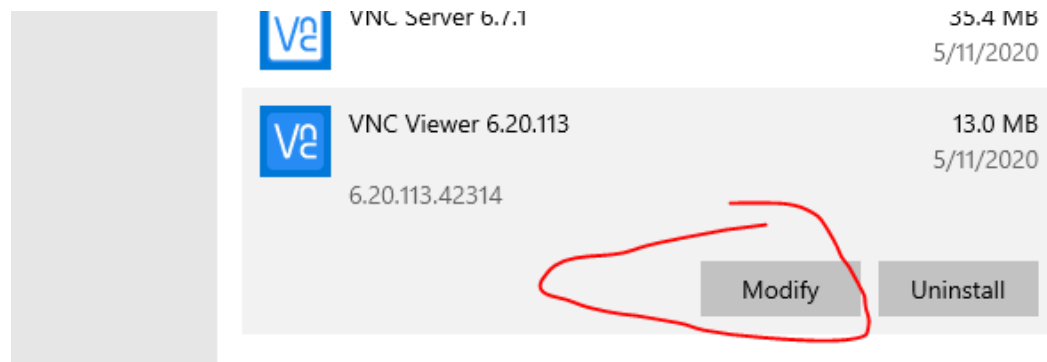
For Microsoft Visual C++ 2013, the last date it was updated at was 5/11/2020.

I tried to update it by , click in it and press modify.



For VNC Viewer, the last time it was updated was 5/11/2020.

I update it by click on the icon and press modify.



## 5. Securing Files and Folders

Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

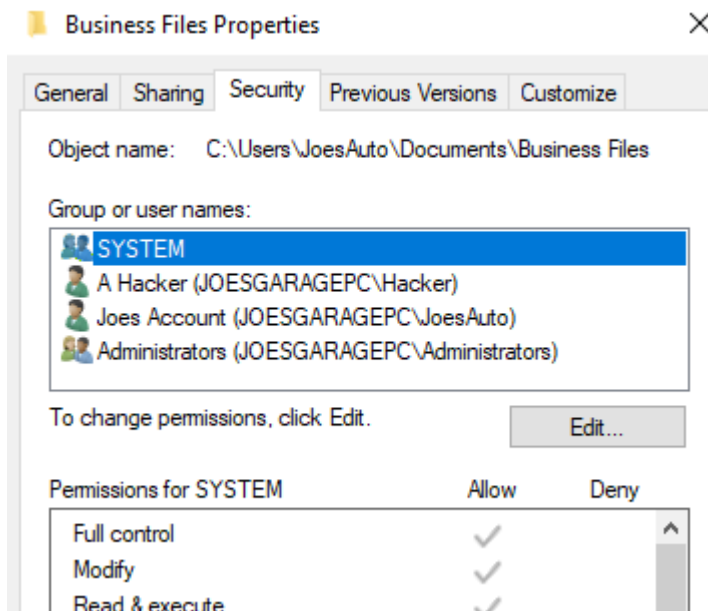
Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

## Encrypting files and folders

- Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that **ONLY** Joe and Jane have permissions to change Joes work files.  
[Hint: Right-click the folder and select Properties.]

I would type file explorer on the search bar, then click on business files.

I would right click then click on properties. Go to the security tab.



- Joe wants his work files encrypted with the password, "SU37\*\$xv3p1" Explain how you would do this. What encryption method do you recommend? You may use the pre-installed program 7-Zip for this.

I would do this by first clicking on Joe's folder, then I would right click and press on 7-ZIP.

I would then extract files.

The encryption method that I would recommend is that I would make it 12 characters, and I would make a password that is hard to guess.

- What security fundamental does this provide?

It shows that passwords should be encrypted to make it hard for hackers to guess your password.

- The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

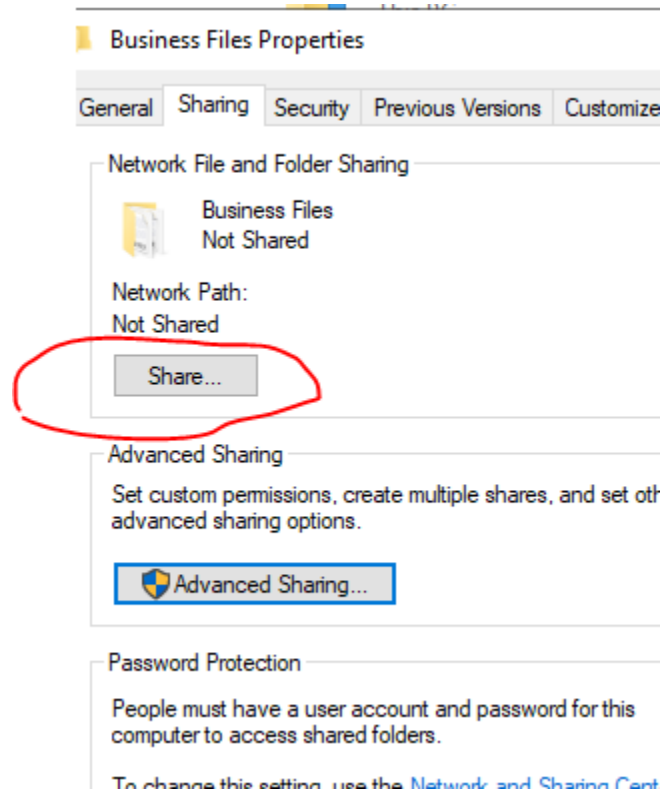
Maintenance, Monitoring, and Analysis of Audit Logs.

## Shared Folders

Shared folders are a common way to make files available to multiple users. There's a folder under Joe's documents called "Business Files" that Joe wants shared with his administrator Jane.

- Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.



*If Joe wants to share the document "Business Files" with Jane then I would go to file explorer. I would click on "Business Files", then right click on the properties. I would then click on the sharing tab, and click on share.*



## Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Add

Name	Permission Level
 A Hacker	Read/Write ▼
 Joes Account	Owner

[I'm having trouble sharing](#)

Share Cancel

I would type Jane's name into and then press Add. Once its added then I would click on the share button.

- For advanced students: Joe wants to make sure there are no other folders shared on the PC. Explain how you view all shared files and folders on a Windows 10 PC. Include a screenshot as proof.

## 6. Basic Computer Forensics (Optional)

Joe has asked that you investigate his PC to see if there are any other files left behind by previous unwanted users that may show they wanted to harm Joe's business. Look through the unwanted users' folders and list suspicious files. General students should document three issues and advanced students at least five issues. Include a brief explanation of their contents and their risks. [Hint: there is a "Hacker" in the PC]

- 
- 

## 7. Project Completion

Take the following steps when you are done answering the challenges and securing Joe's PC:

- Save your answer template as both a Word document and PDF. Make sure your name and date are on it.

- Shutdown the virtual Windows 10 PC.
- Submit the PDF to Udacity for review.