

# Udacity Cybersecurity Course #1 Project

## Contents

Student Information	2
Scenario	3
1. Reconnaissance	4
2. Securing the PC	6
3. Securing Access	8
4. Securing Applications	10
5. Securing Files and Folders	13
6. Basic Computer Forensics (Advanced)	14
7. Project Completion	15

## 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: Mohammed khaleel

Date of completion: 10/3/2022

## 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

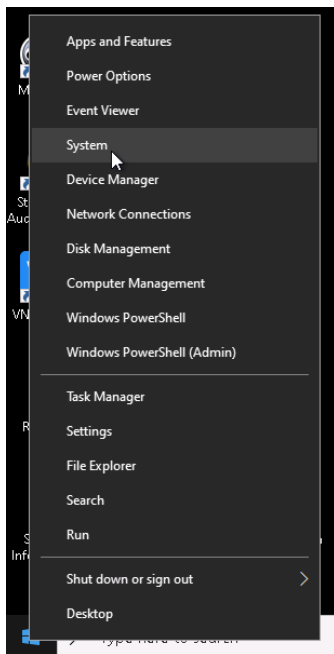
1. Fill in the following table with system information for Joe's PC.

Device Name	JoesGaragePC
Processor	Interl(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHZ-2.59GHZ
Install RAM	4.00 GB
System Type	64-bit operating system, x64-based processor
Windows Edition	Windows 10 Pro
Version	20H2
Installed on	11/23/2021
OS build	19042.1387

2. Explain how you found this information:

To show the Details information for Joe's the best way to get full information pc go click right mouse on windows then click System so there is full details about PC

3. Provide a screenshot showing this information about Joe's PC:



## About

Your PC is monitored and protected.

[See details in Windows Security](#)

## Device specifications

Device name	JoesGaragePC
Processor	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz 2.59 GHz
Installed RAM	4.00 GB
Device ID	E5C64EC4-3404-4D29-8CE1-72C6EF2E1932
Product ID	00331-10000-00001-AA949
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Copy

Rename this PC

## Windows specifications

Edition	Windows 10 Pro
Version	20H2
Installed on	11/23/2021
OS build	19042.1387
Experience	Windows Feature Experience Pack 120.2212.3920.0

Copy

## Software

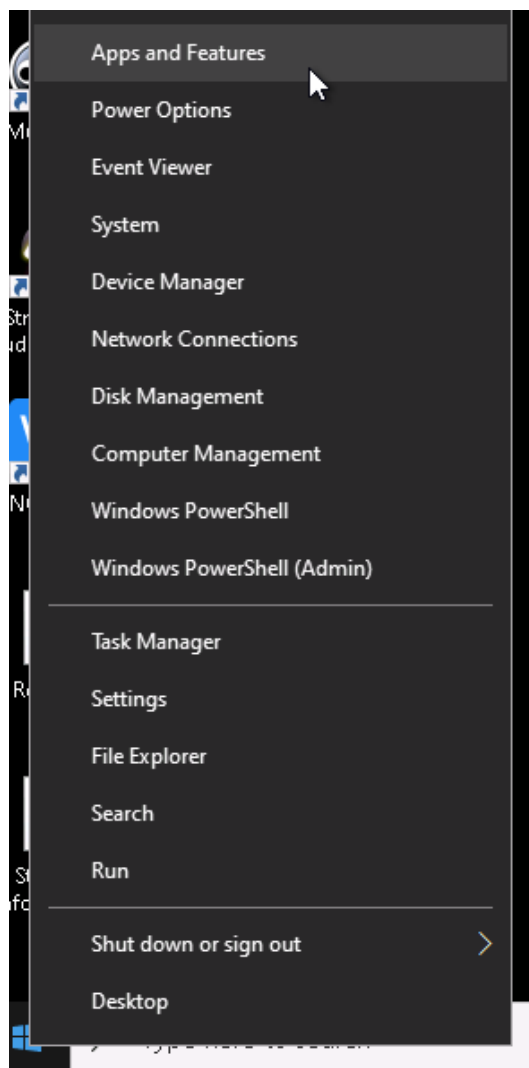
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

1. *List at least 5 installed applications on Joe's computer:*

- MusicBee 3.3.7367
- Nmap 7.80
- Skype
- 7-Zip 19.00
- VLC media Player

2. *Explain how you found this information. Provide screenshots showing this information.*

To check what Joe have application *go click right mouse on windows then click Apps and Features*



## Apps & features

### Choose where to get apps

Installing apps only from Microsoft Store helps protect your device.

Anywhere

## Apps & features

[Optional features](#)

[App execution aliases](#)

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

Search this list

Sort by: Name

Filter by: All drives

24 apps found

	7-Zip 19.00 (x64)	4.96 MB 11/23/2021
	Adobe Reader XI (11.0.01)	128 MB 5/11/2020
	Candy Crush Friends king.com	266 MB 9/25/2022
	Cortana Microsoft Corporation	8.00 KB 11/23/2021
	Farm Heroes Saga king.com	279 MB 9/25/2022

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

*Basic controls: inventory and control of software assets*

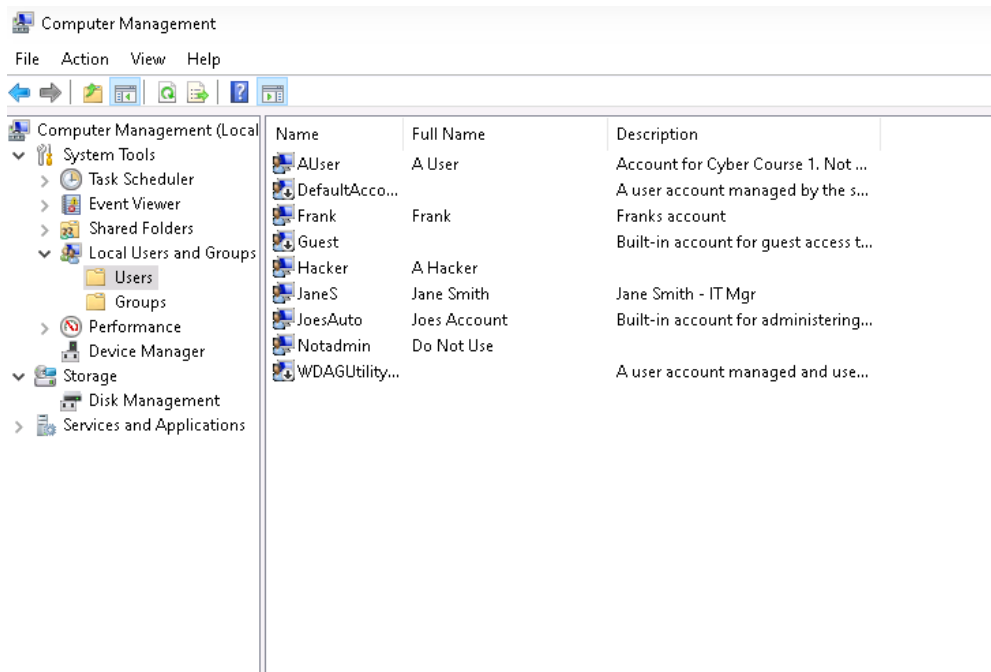
## Accounts

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

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

Account Name	Full Name	Access Level
AUser	A User	Users
DefaultAccount	-	System Managed Accounts Group
Frank	Frank	Remote Desktop Users, Users
Guest	-	Guests
Hacker	A Hacker	Administrators, Remote Desktop Users, Users
JaneS	Jane Account	Administrators, Remote Desktop Users, Users
JoesAuto	Joes Account	Administrators
Notadmin	Do Not Use	Remote Desktop Users, Users
WDAGUtilityAccount	-	-

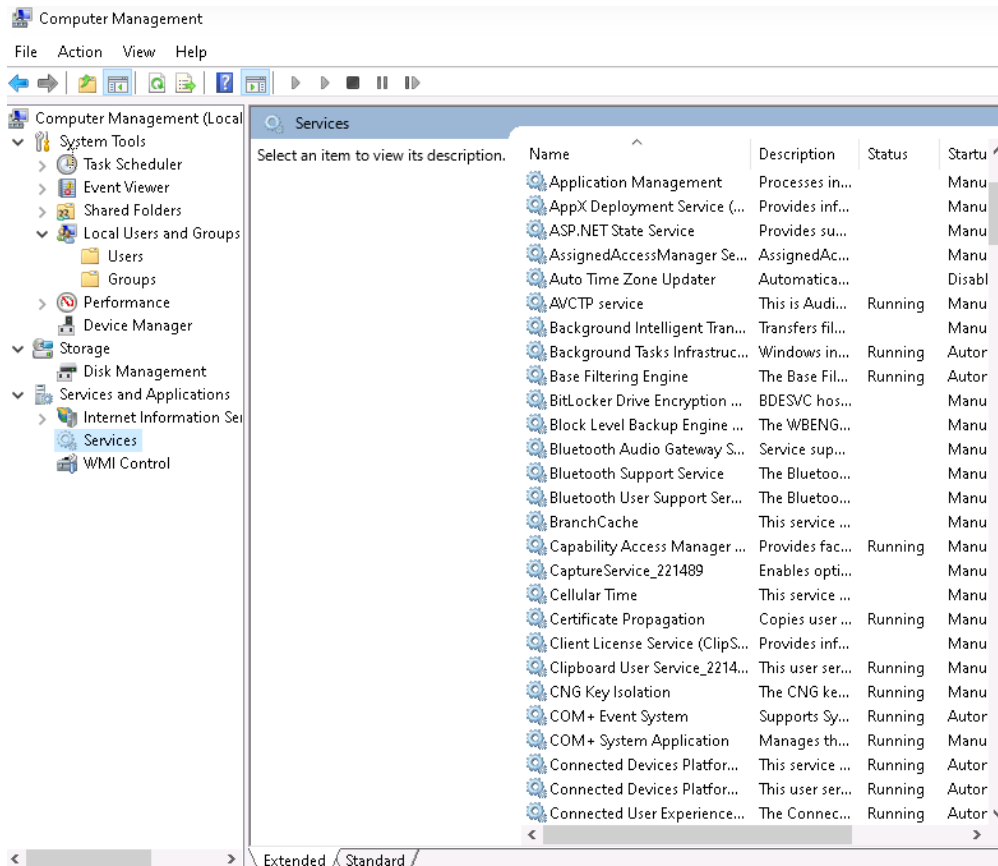
2. Provide a screenshot of the Local Users.



## 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.

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

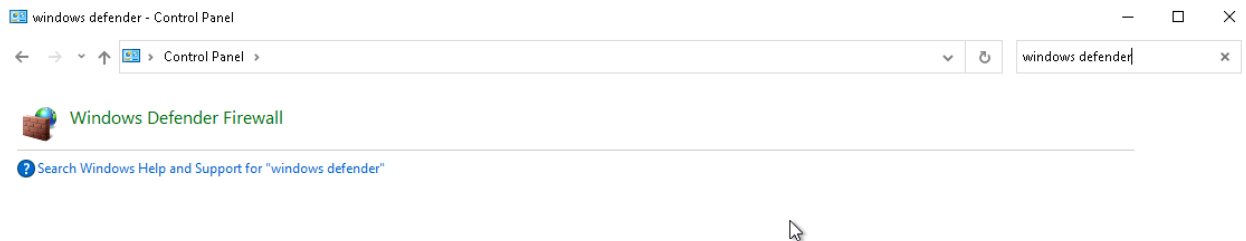




## Security Services

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.**

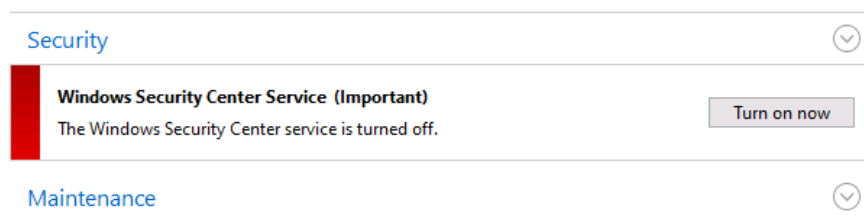
1. To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:



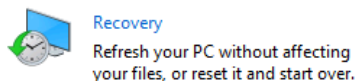
2. The Windows 10 Security settings are also found from the **Control Panel > System and Security > Security and Maintenance**. Start by viewing "Review your computer's status and resolve issues." Provide a screenshot of this below:

[Review recent messages and resolve problems](#)

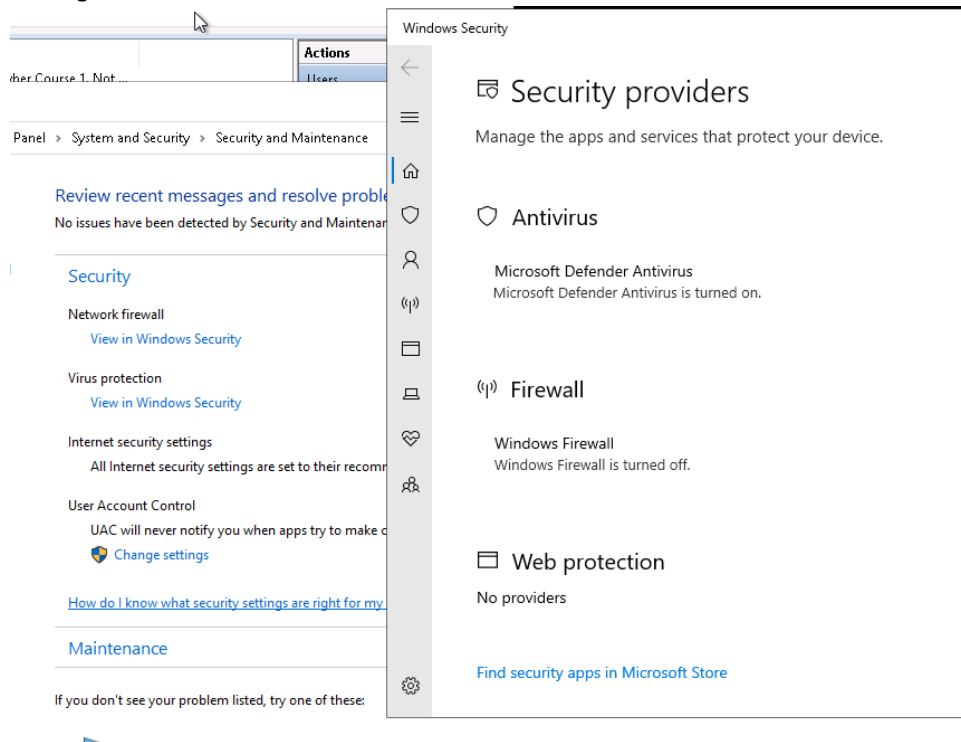
Security and Maintenance has detected one or more issues for you to review.



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



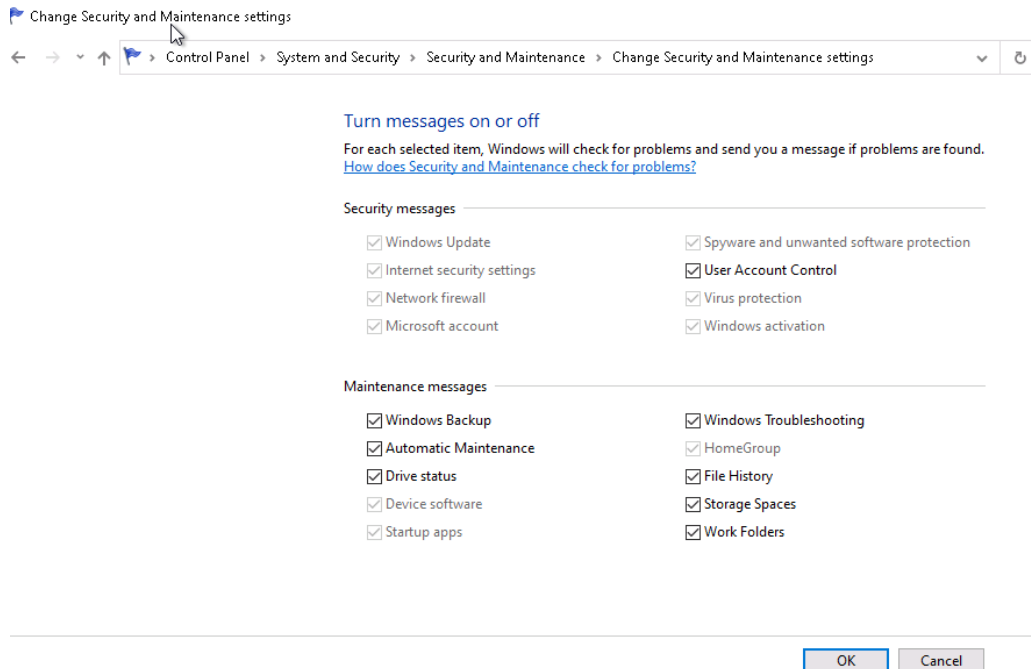
3. Click on **View in Windows Security** to see the status there. Provide a screenshot of the **Firewall** settings.



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

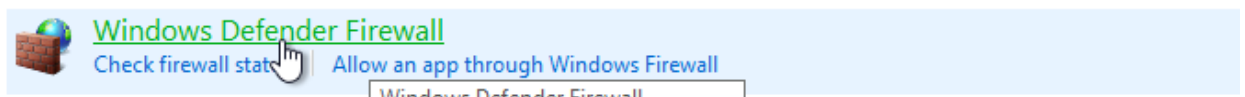


5. *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*



6. *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).*

*To see detail go to Windows Defender Firewall and Security and Maintenance settings and search virus and threat protection*



Security Feature	Status
Firewall product and status – Private network	Off
Firewall product and status – Public network	On
Virus protection product and status	On
Internet Security messages	On
Network firewall messages	On
Virus protection messages	On
User Account Control Setting	On

7. 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.]*

- Limit control of network Ports and protocol because hacker could maybe find some old open port and protocol
- Data Recovery for Ransomware that you can get data if you lost
- Limit privileges that not all people can access whatever they want

## 2. Securing the PC

### **Baselines**

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

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

*Least-Privilege, Only Work-Related Software, Only Use laptop company with limit credential and no personal device*

*Because the company is very important maybe someone could leak information and steal the idea of company*

2. What industry baseline do you recommend to Joe?

*[Hint: Look in the documents folder]*

*I think I would say Identify as NIST Cybersecurity Framework to check all three text file*

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.

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

Basic Controls

### **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.

1. *Explain the process you take to do this.*  
*Go to Control Panel > System and Security > Windows Defender Firewall*
2. *Include screenshots showing the firewall is turned on.*



3. *What protection does this provide?*

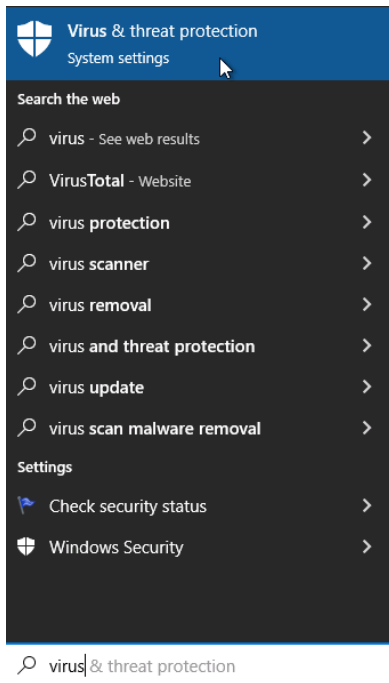
*It's important to turn on this firewall because it provides block all not allowed apps and notify if its block not allowed.*

## 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.

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

Go to windows search then text Virus & threat protection



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



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.

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



## Firewall

Windows Firewall  
Windows Firewall is turned on.

3. *Provide at least two risks mitigated by enabling these security settings:*
  - Detect virus application and stop install
  - Not allowing to connect that firewall limited to connect
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

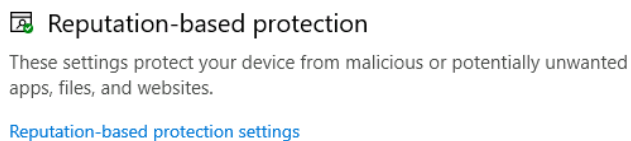
Foundational Controls

## 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.

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



## User Account Control Settings

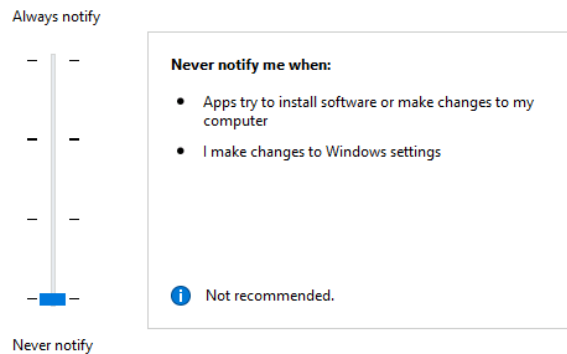
Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer. This is done through the User Account Control Setting.

1. *What is the current UAC setting on Joe's computer?*

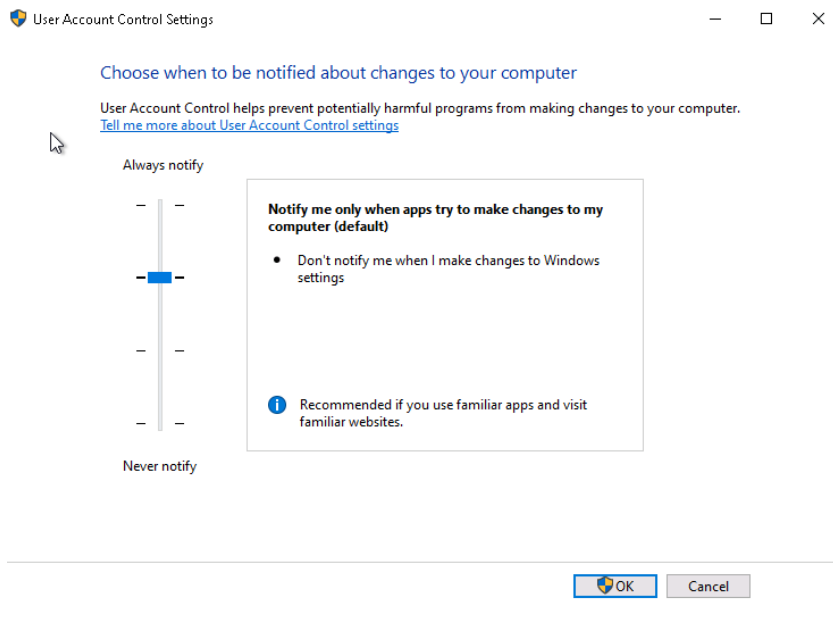
This is available from the above security settings.

[Choose when to be notified about changes to your computer](#)

User Account Control helps prevent potentially harmful programs from making changes to your computer.  
[Tell me more about User Account Control settings](#)



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



## Securing Removable Media

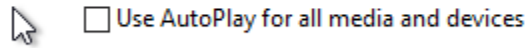
A security best practice is to not allow the use of removable hard drives (USB sticks, Memory Cards, and DVDs). They are needed as part of Joe's backup policy. The next best thing is to make



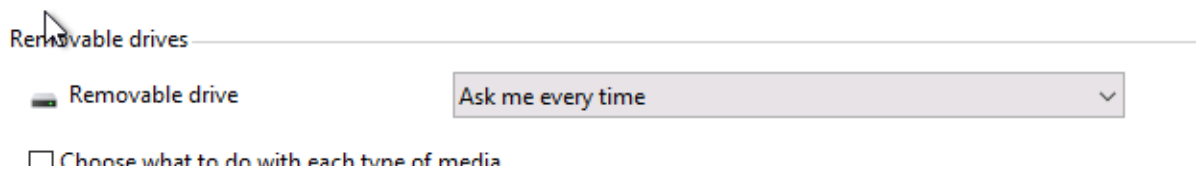
sure that any applications don't automatically start when the media is inserted and the user is asked what should happen. This is set from the Control Panel > Hardware and Sound > Autoplay menu.

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

Choose what happens when you insert each type of media or device



2. 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.

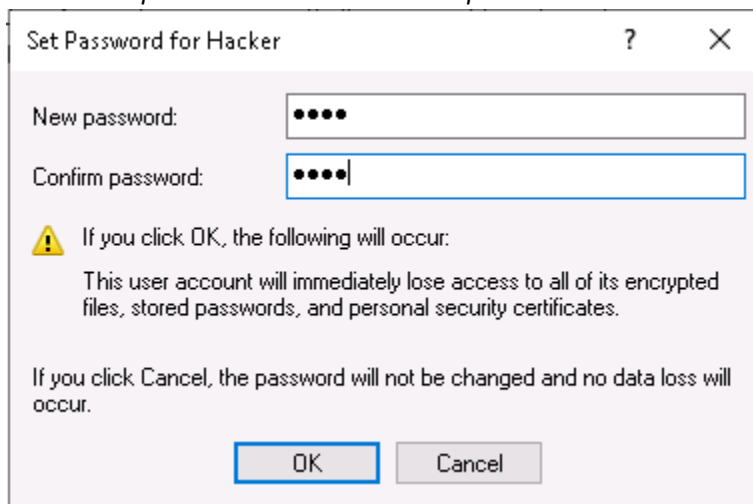
## User Accounts

1. What user accounts should not be there?

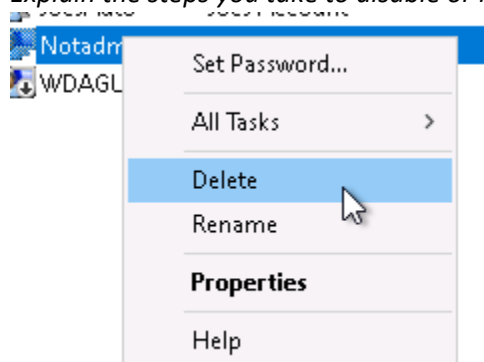
*I think there is nothing user that should not be there*

	AUser	A User	Account for Cyber Course 1. Not ...
	DefaultAcco...		A user account managed by the s...
	Frank	Frank	Franks account
	Guest		Built-in account for guest access t...
	Hacker	A Hacker	
	JaneS	Jane Smith	Jane Smith - IT Mgr
	JoesAuto	Joes Account	Built-in account for administering...
	Notadmin	Do Not Use	
	WDAGUtility...		A user account managed and use...

2. Bonus questions: What is Hacker's password? You can make password for yourself



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



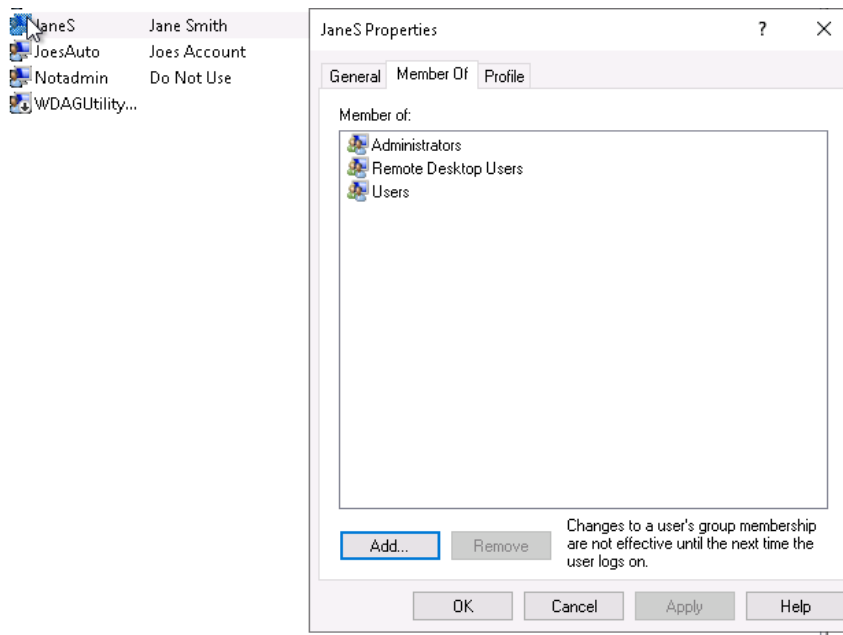
4. Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.

Because if there is an account and for old employees, it could be dangerous may he is using to leak information and steal more account

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

5. Which account(s) have administrator rights that shouldn't?  
Jane Smith and A Hacker
6. Explain how you determined this. Provide screenshots as needed.

Click user > go to Member Of

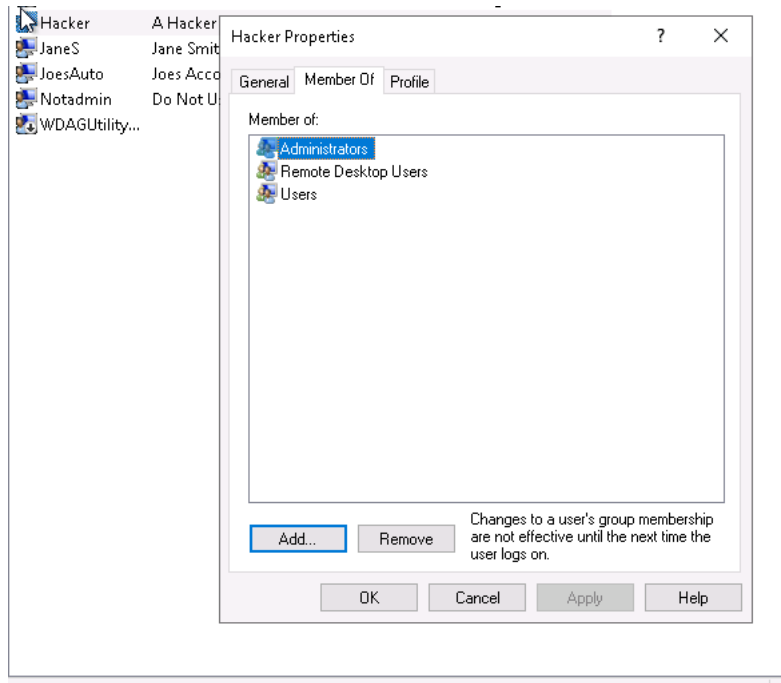


Administrator privileges for too many users are another security challenge.

7. Provide at least three risks associated with users having administrator rights on a PC.
  - Employees will accidentally install malware
  - An application that violation of the license agreement
  - Can control everything in company

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

8. *Explain the process for doing this. Include screenshots to show your work.*  
*click User > go to Member Of > Click Administrators > remove > ok*

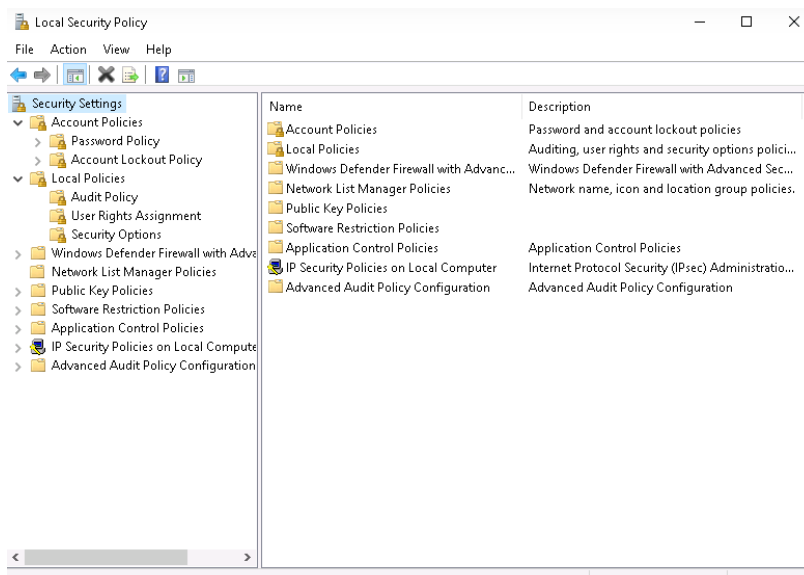


9. *What is the security principle behind this?*  
*Access control and least privilege*
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?  
  
CIS Controls, Basic Controls

## ***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.

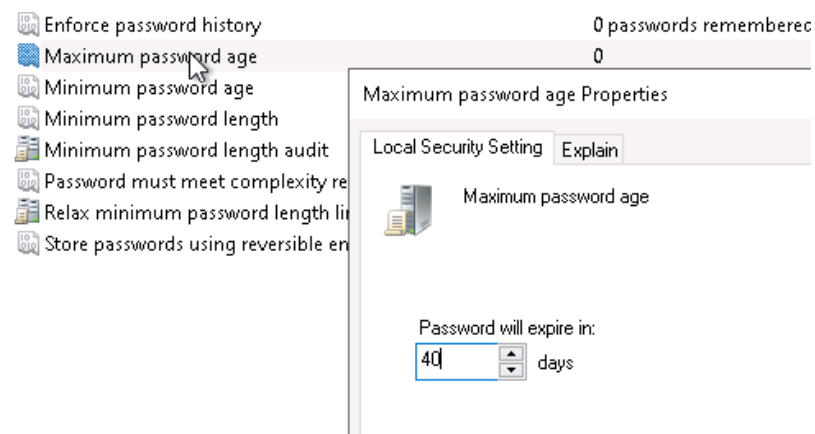
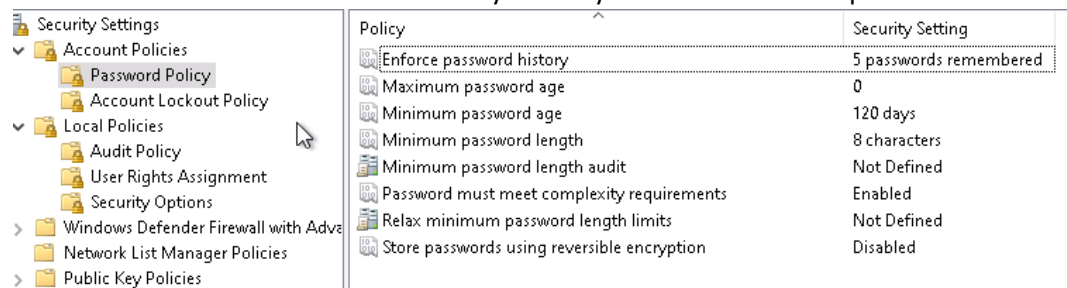
1. *Provide a screenshot of the Local Security Policy window here.*  
*[Note: Local Security Policy is not available on Windows 10 Home edition.]*



2. 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.

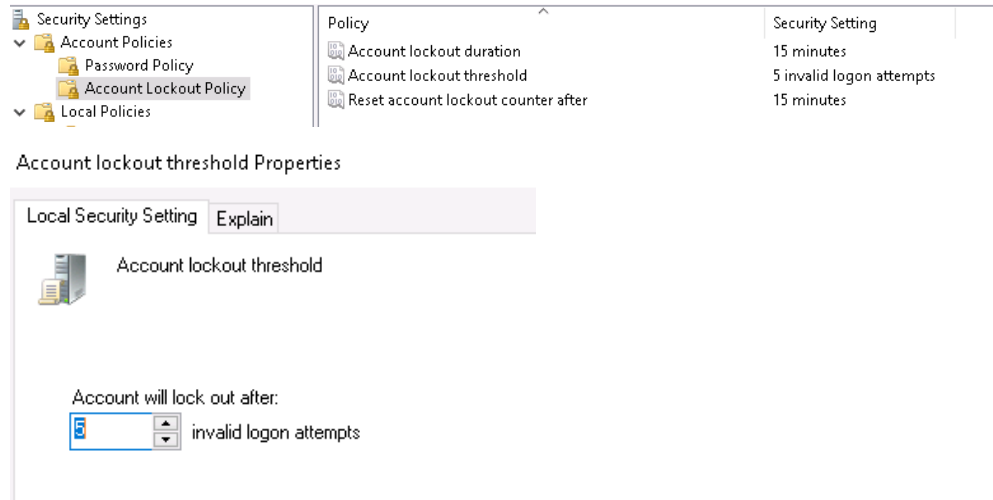
- Setting the Password Policy:

Select Account Policies > Password Policy > then you can set rules like picture two



- Setting the Account Lockout Policy:

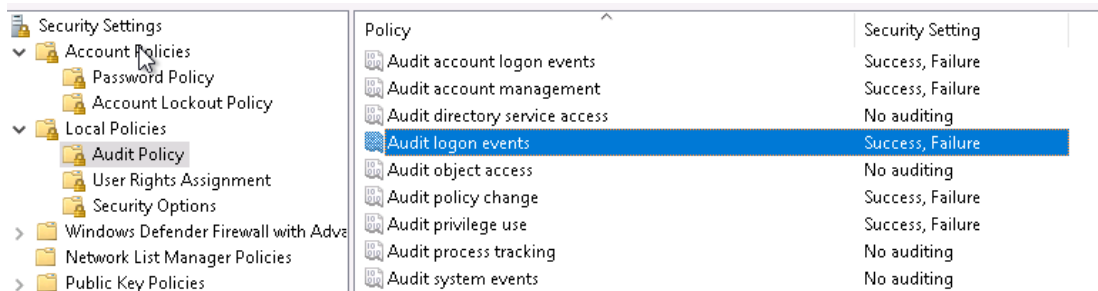
Select Account Policies > Password lockout Policy > then you can set rules like picture two



## 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.

1. 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.
2. Provide a screenshot of your changes here.



## 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.

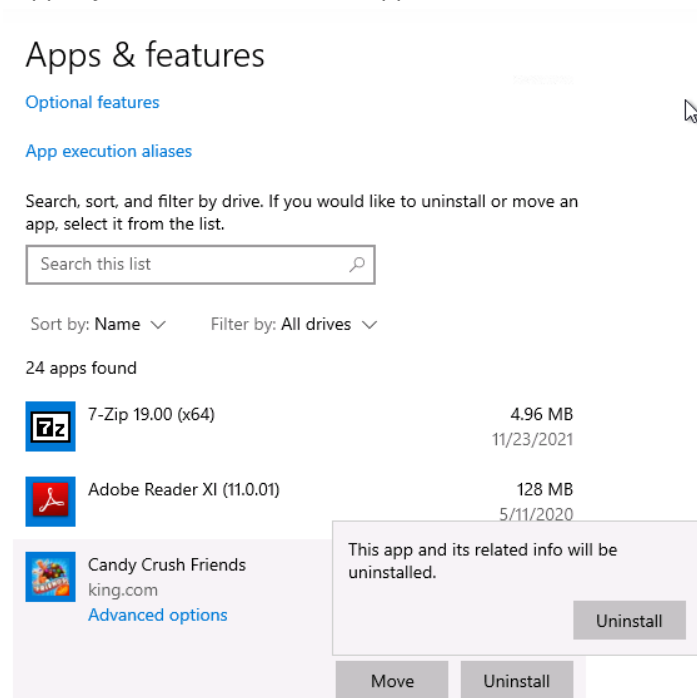
Joe has established the following rules regarding PC applications:

- 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***

1. *List at least three application(s) that violate this policy.*
  - *Candy Crush Friends*
  - *Farm Heroes Saga*
  - *MusicBee*
2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*
  - *Bypass computer or remote access trojan*
  - *Unauthorized access*
  - *Malicious software*
3. *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.*

*Go search App & features > uninstall on application*

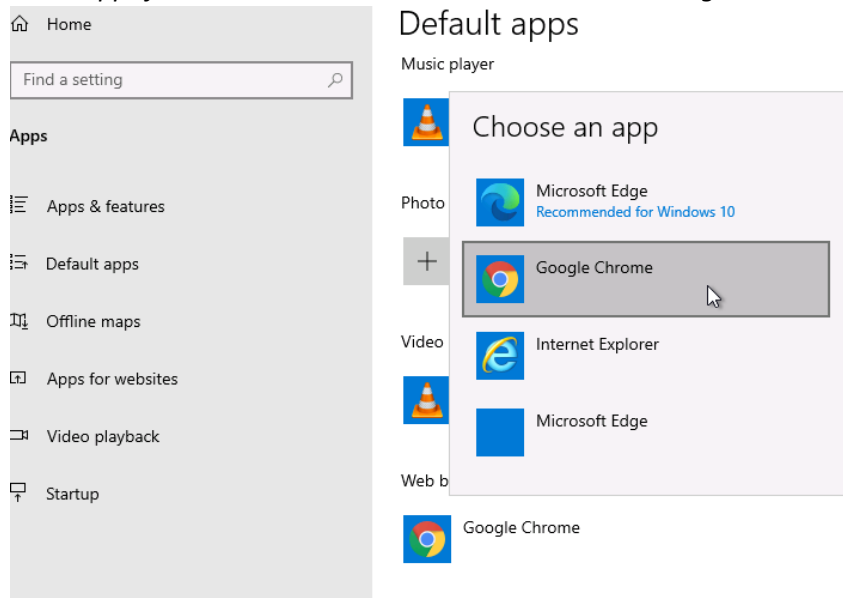


## Default Browser

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

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

Go to Apps for websites > click Web browser > choose Google Chrome

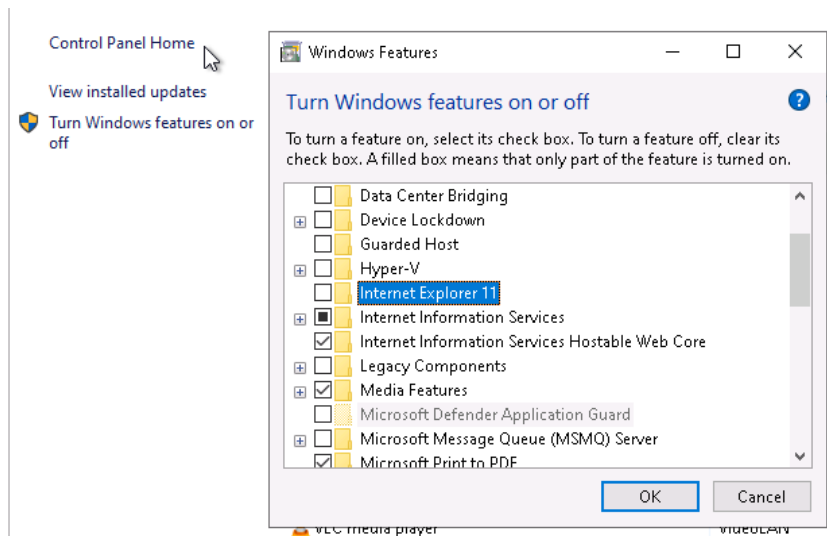


2. Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.
  - There is no update for this application and has many vulnerabilities
  - This appicate has many viruses and hacker can easily access

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.**”

3. Provide a screenshot showing Internet Explorer 11 is off.

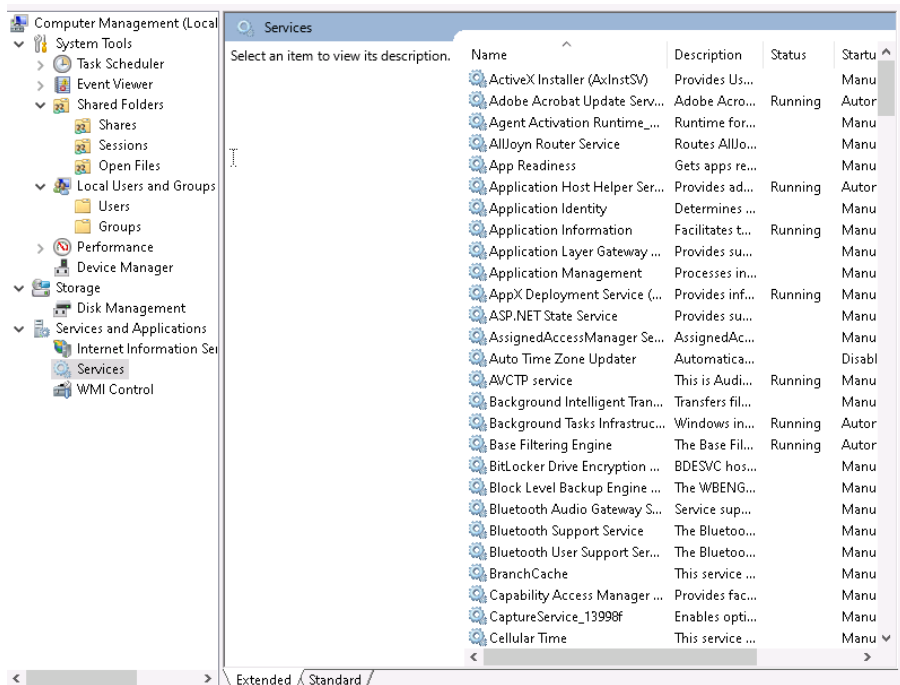




## Windows Services

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.

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

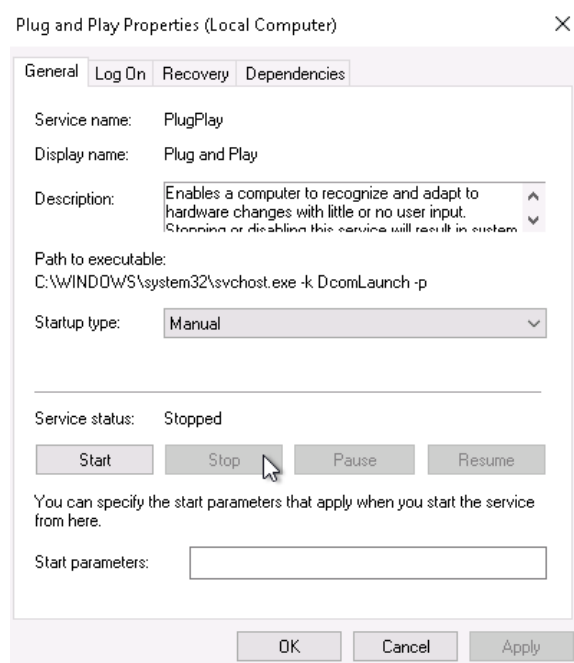


2. Advanced users should provide at least two methods for determining a web server is running on a host

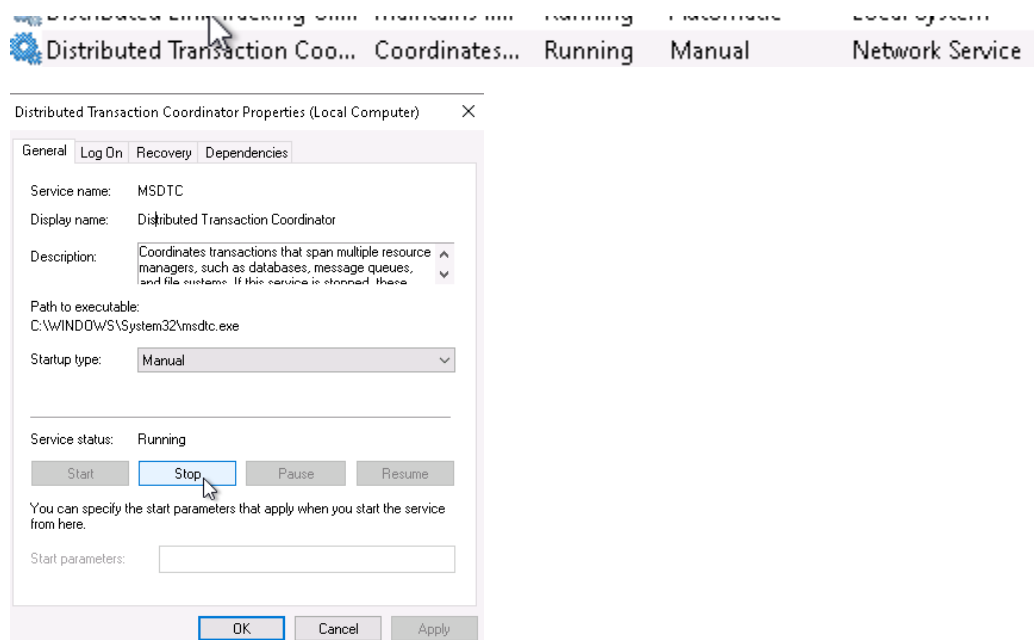
Plug and Play and Performance logs & Alerts

3. How do you disable them and make sure they are not restarted?

Select stop



4. 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.

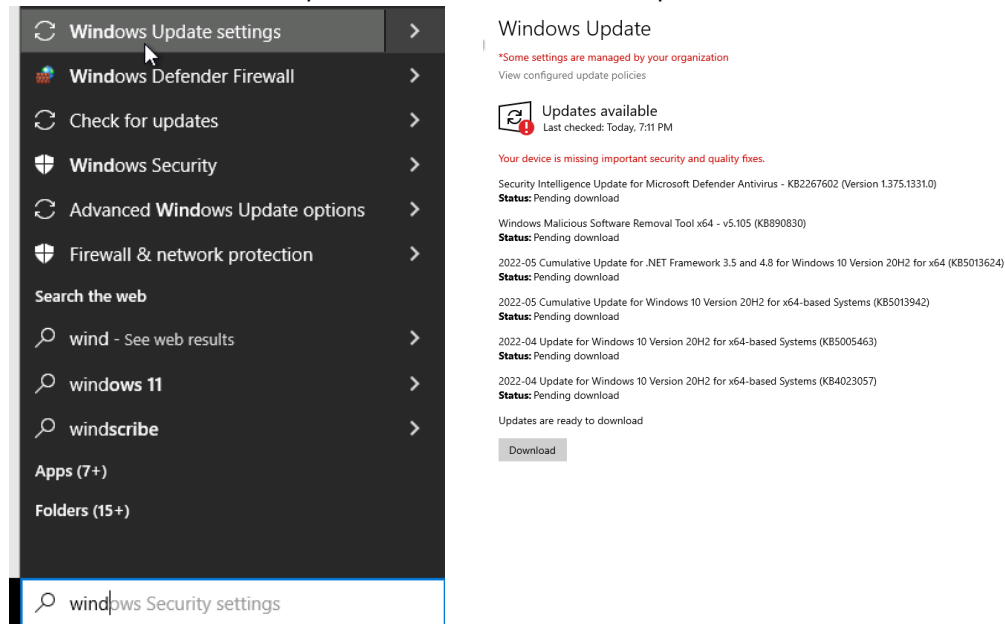


## Patching and Updates

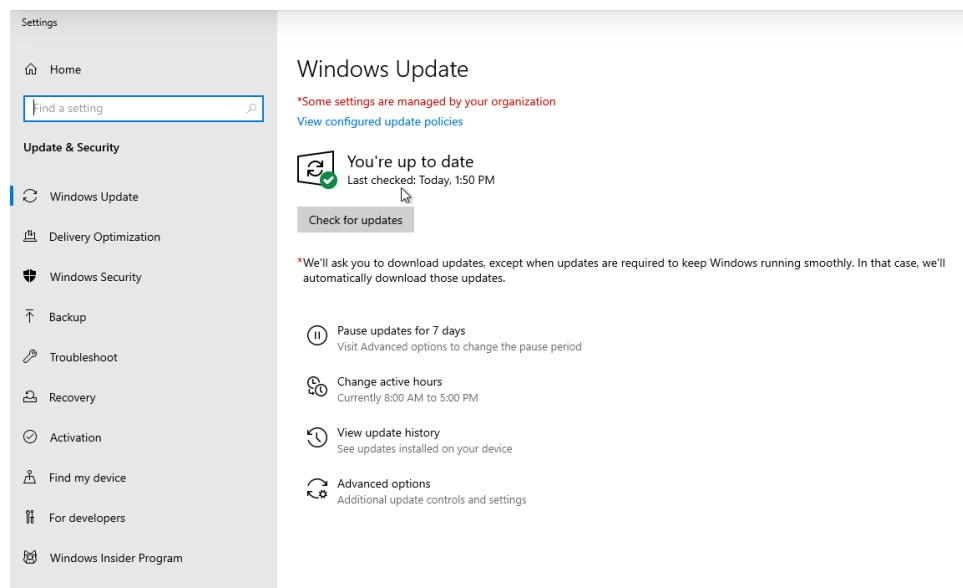
Keeping the operating system current on patches and fixes is a critical part of security. Joe wants his PC to be on the latest version of Windows 10. He also wants you to set it up for automated updates.

1. Explain the process for doing this. Include screenshots as needed.

Go search Windows Update > then click Windows Update



2. 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.



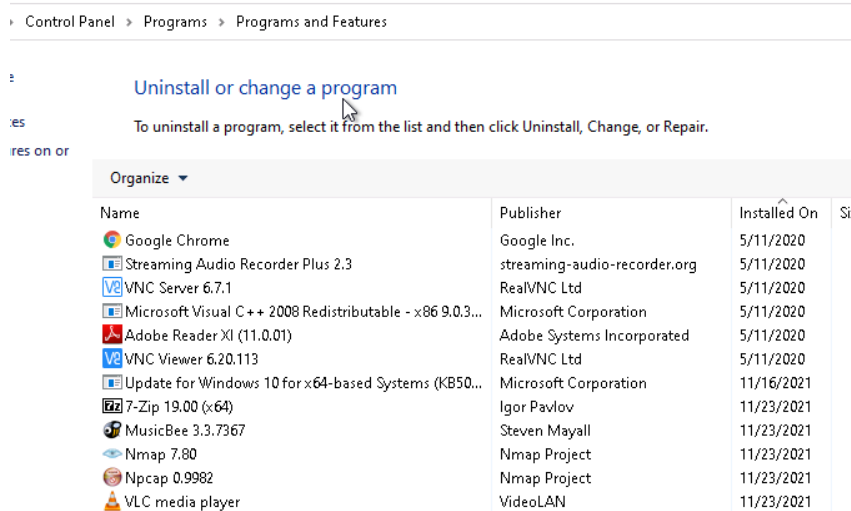
All applications should also be up to date on patches or fixes provided by the manufacturer. Any old versions of software should be uninstalled.

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

- Adobe Reader
- VNC Server

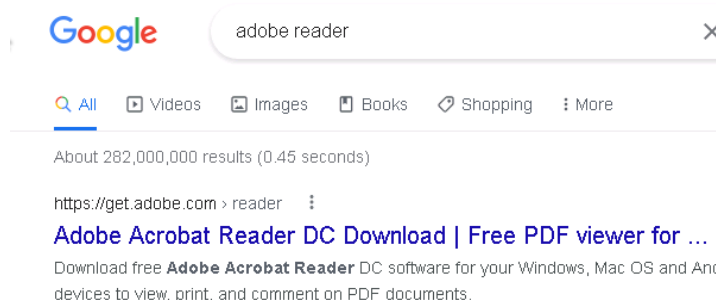
4. Explain the steps you took to determine this information.

Go Control Panel > Programs > Programs and Features > Look Installed On

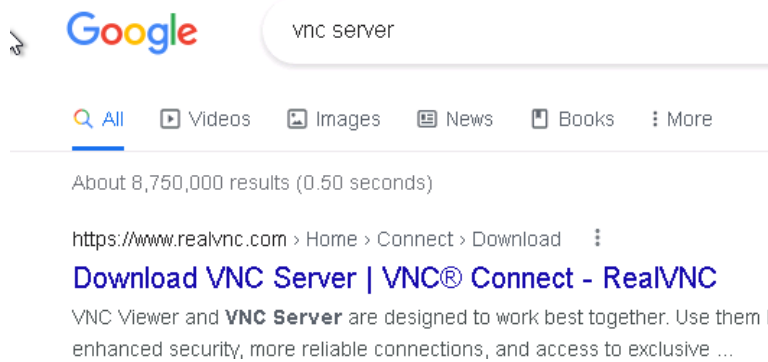


5. Explain the steps for updating each of these applications. Include screenshots as needed.

For Adobe reader first go to google chrome then go search adobe reader and download latest version



For VNC Server first go to google chrome then go search VNC Server and download latest version



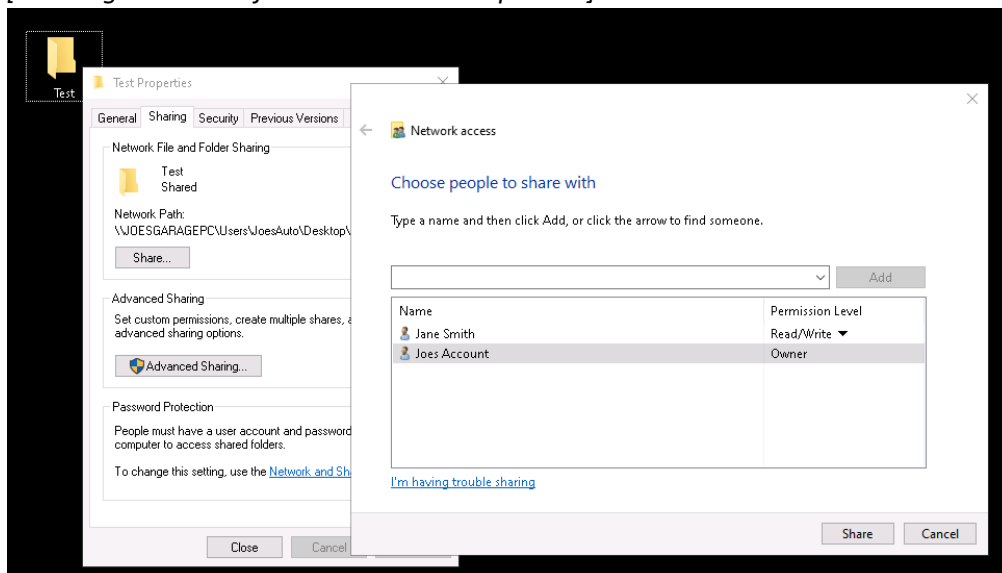
## 5. Securing Files and Folders

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.

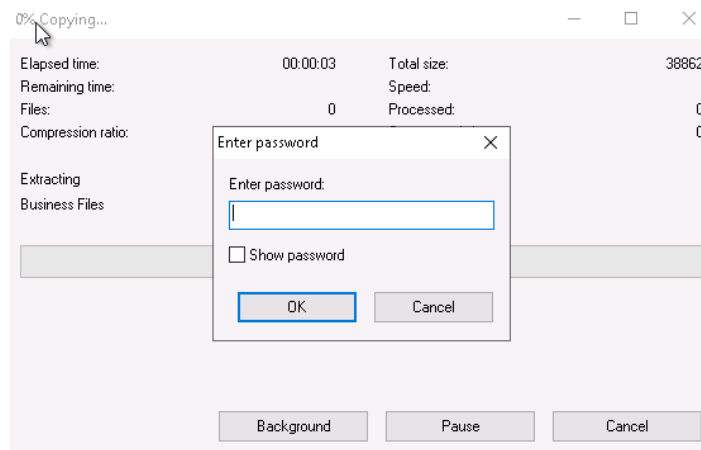
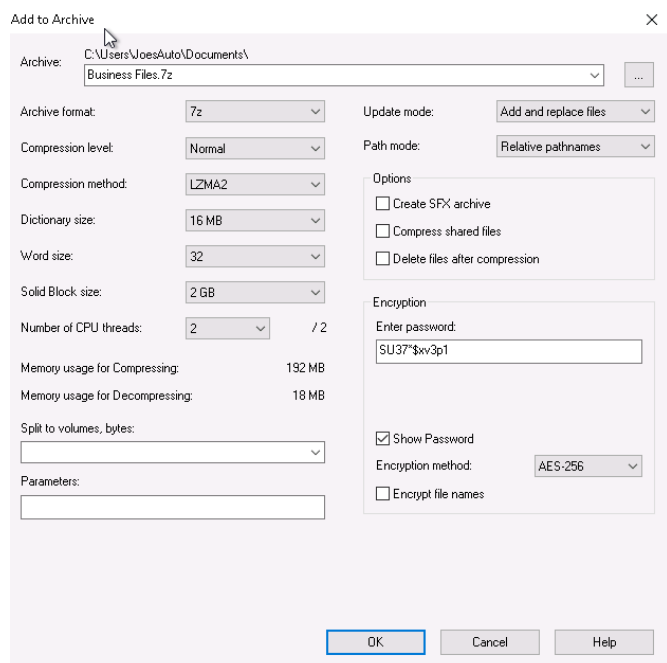
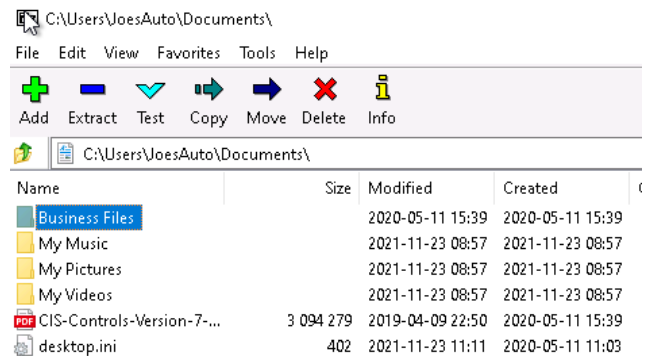
### ***Encrypting files and folders***

1. *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.]*



2. 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.

Go 7-zip application > click Add the file > Enter Password to encrypt > ok



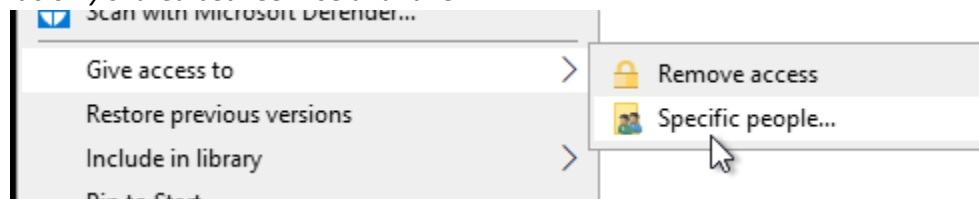
3. What security fundamental does this provide?  
Confidentiality because it is important to keep it secret from unauthorized and only authorized people who has the key
4. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

Foundational Controls - Data Protection

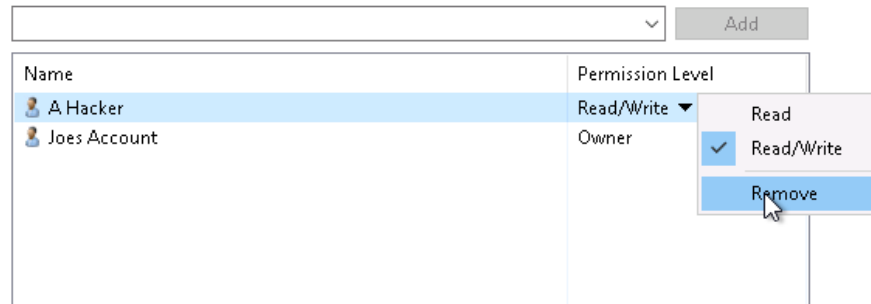
## Shared Folders

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.

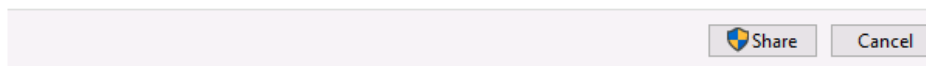
1. Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.



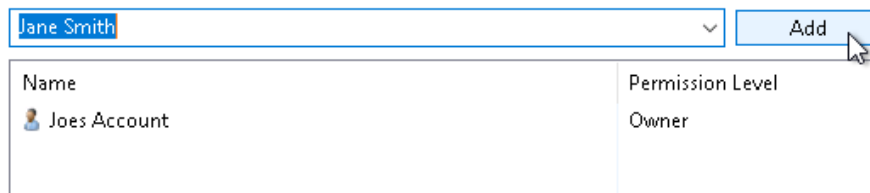
Type a name and then click Add, or click the arrow to find someone.



[I'm having trouble sharing](#)



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

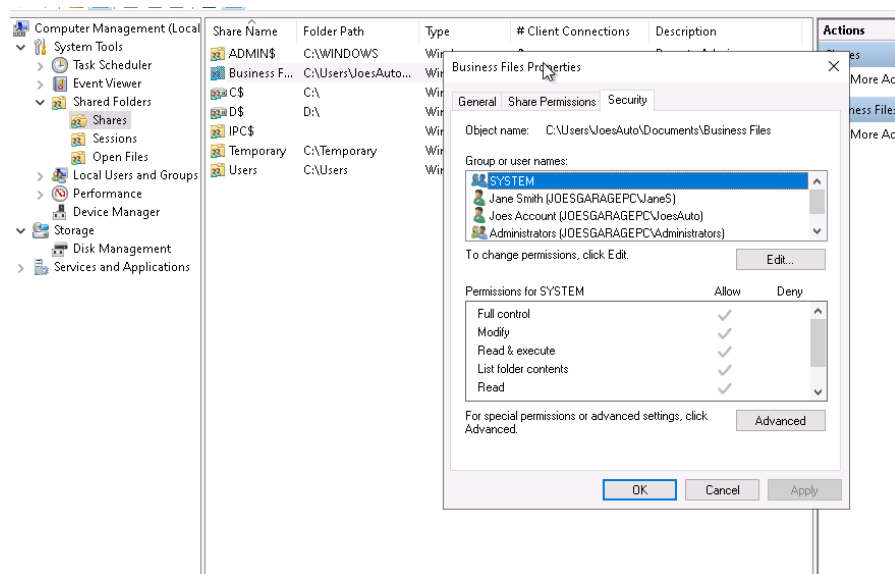


	Add
Name	Permission Level
Jane Smith	Read/Write
Joes Account	Owner

[I'm having trouble sharing](#)

- 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.

*I think this answer*



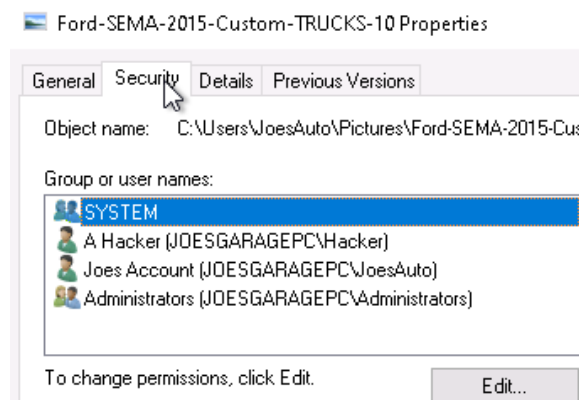
## 6. Basic Computer Forensics (Optional)

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]



Go Picture > properties these photos > go to security

- 132901765.wdp
- Ford-SEMA-2015-custom-TRUCKS-10
- Trucks-Of-SEMA-30



## 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.