# 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: Utkrisht Mishra

Date of completion: 02-01-2022

# 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 | Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz 2.10GHz |
| 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:*

   *I found these items by going into Settings > System > About*

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

## *Software*

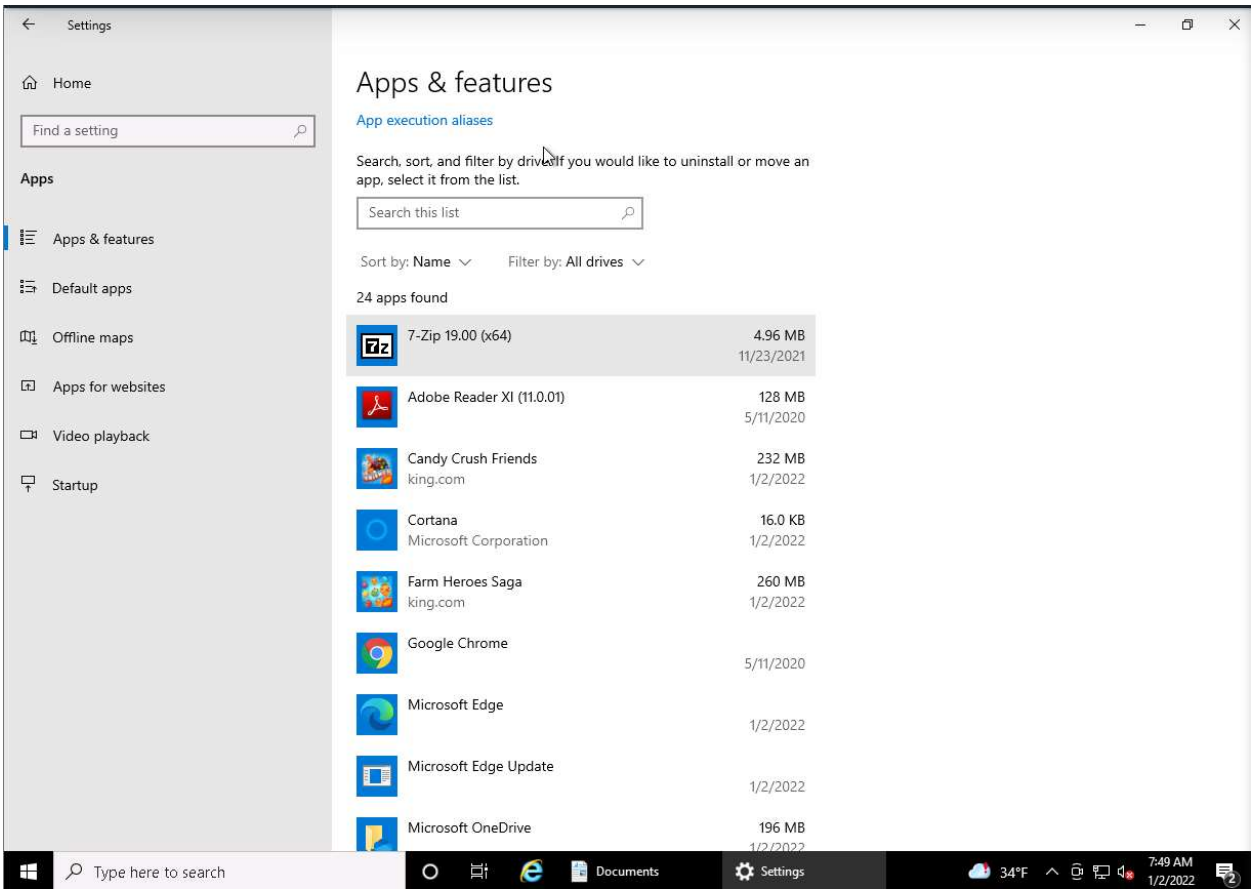
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- 7-Zip 19.00 (x64)
- Adobe reader XI (11.0.01)
- MusicBee 3.3.7367
- Npcap 0.9982
- VNC Server 6.7.1

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

   *I found these items by going into Settings > Apps > Apps & features*




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

*The Center for Internet Security Controls lists this as the 2nd step in securing PC. This step is called Inventory Control Of Software Assets. It fulfills the 2nd step which is Inventory Control Of Software Assets.*

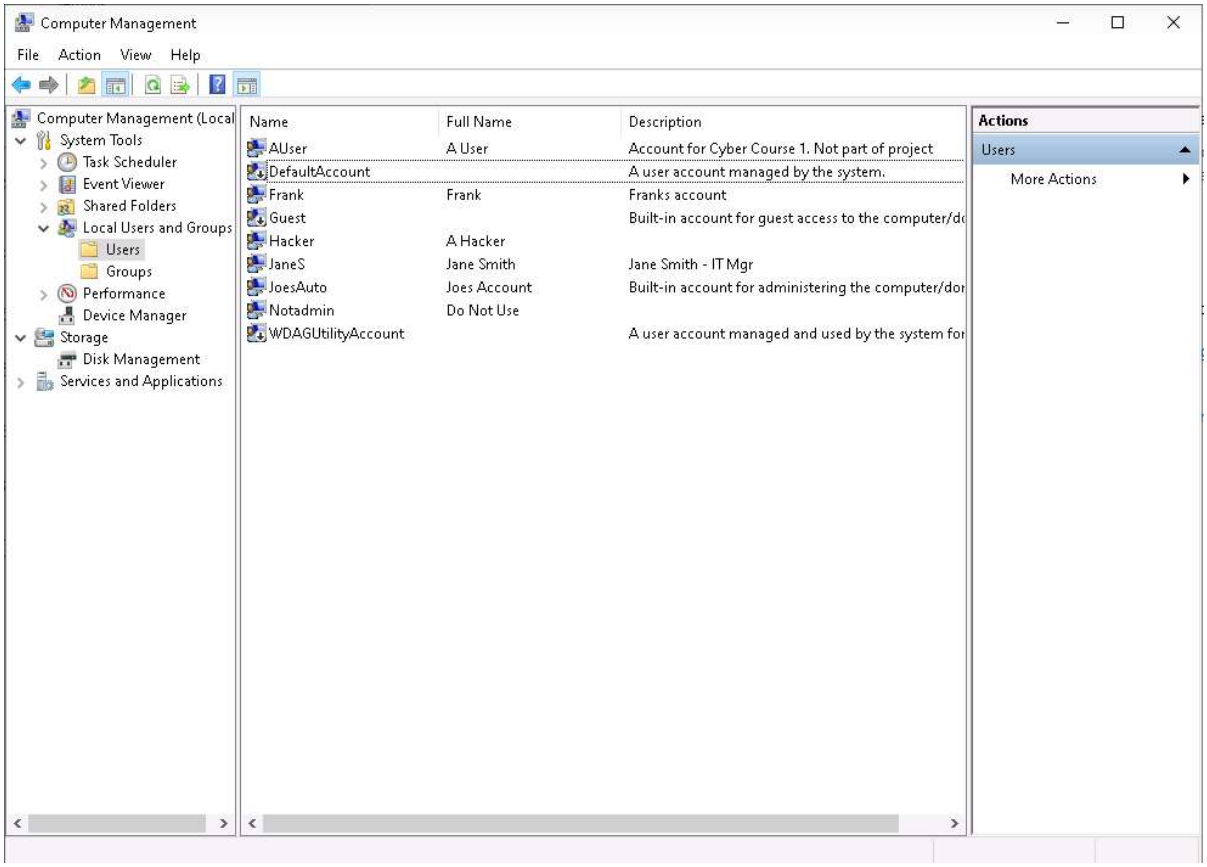
## *Accounts*

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** |
|---|---|---|
| DefaultAccount | - | System Managed Accounts Group |
| Frank | Frank | Remote Desktop Users, Users |
| Guest | - | Guest |
| Hacker | A Hacker | Remote Desktop Users, Users, Administrators |
| JaneS | Jane Smith | Remote Desktop Users, Users, Administrators |
| JoesAuto | Joes Account | Administrators |
| NotAdmin | Do Not Use | Remote Desktop Users, Users |
| WDAGUtilityAccount | - | None |
| | | |

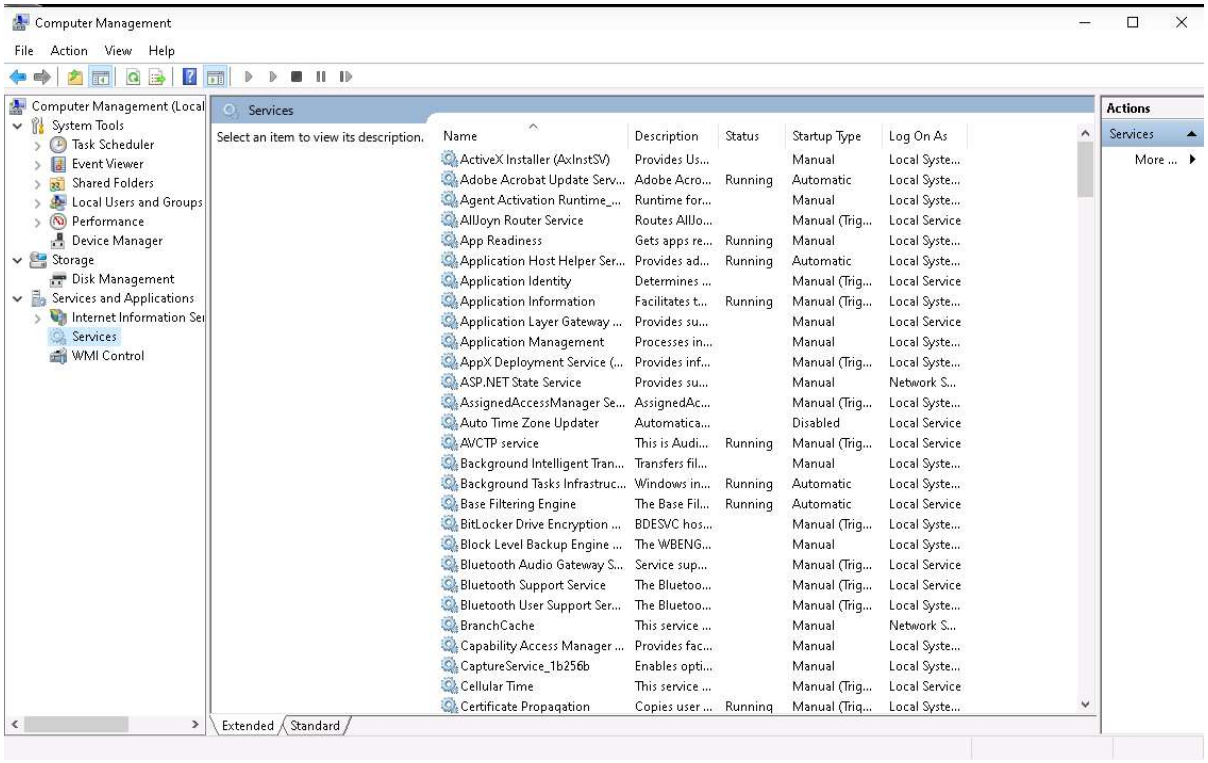
2. *Provide a screenshot of the Local Users.*



## *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.

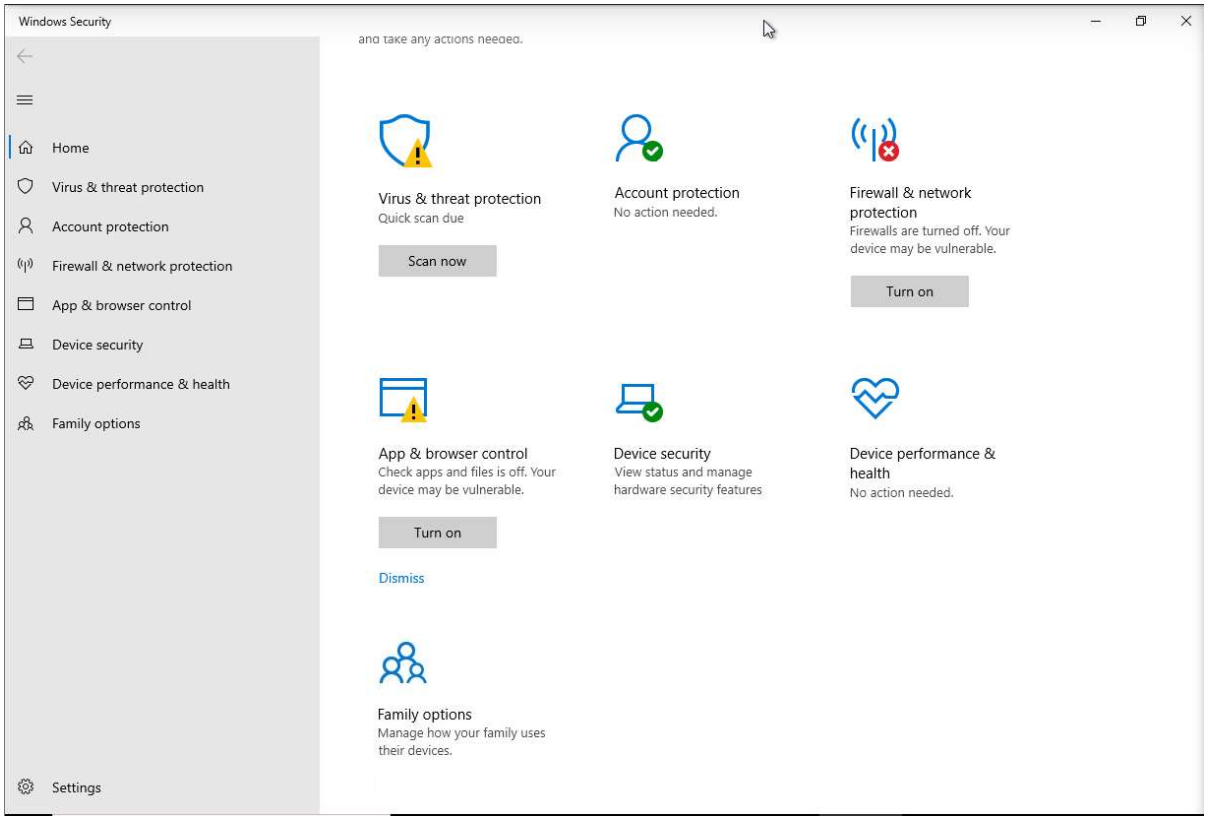
1. *Provide a screenshot of the services running on this PC.*



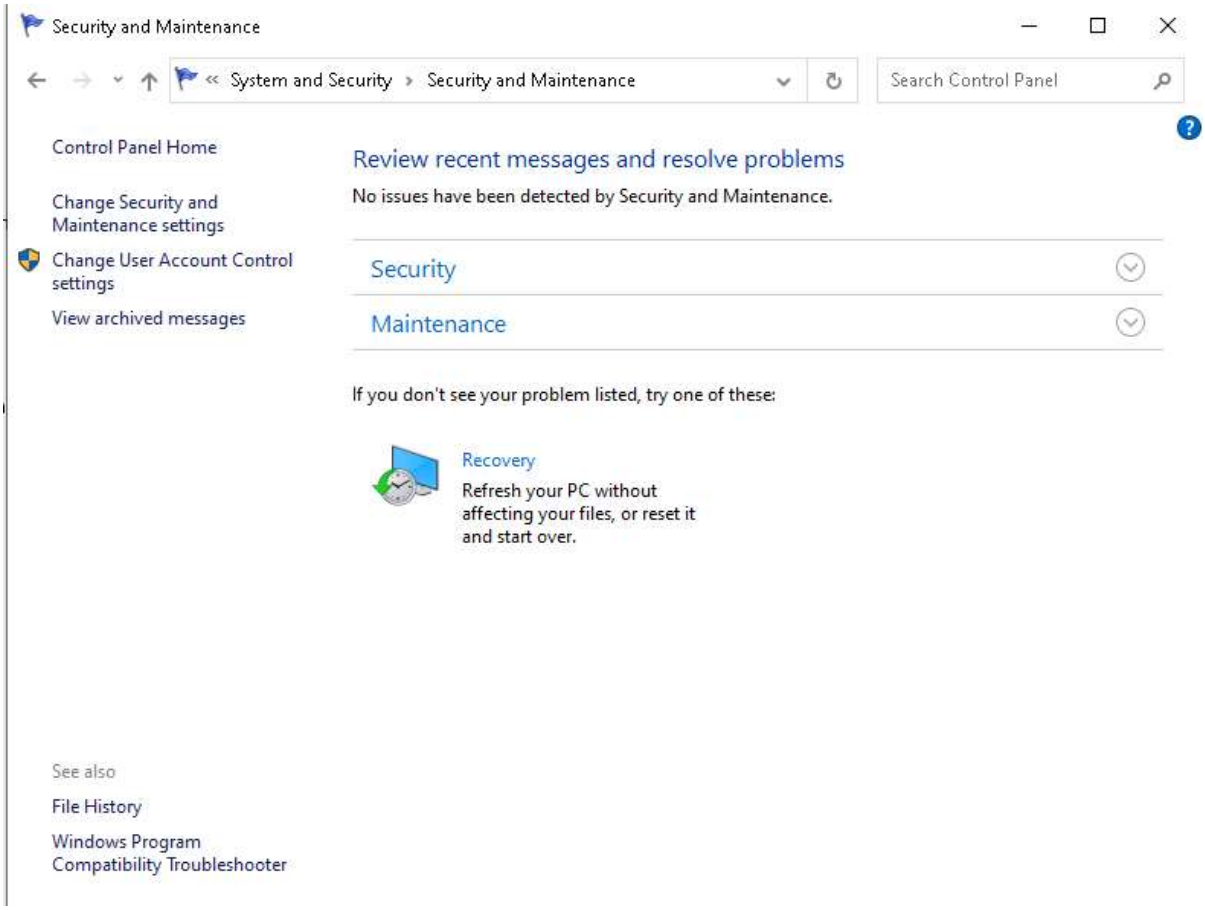
## *Security Services*

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.**

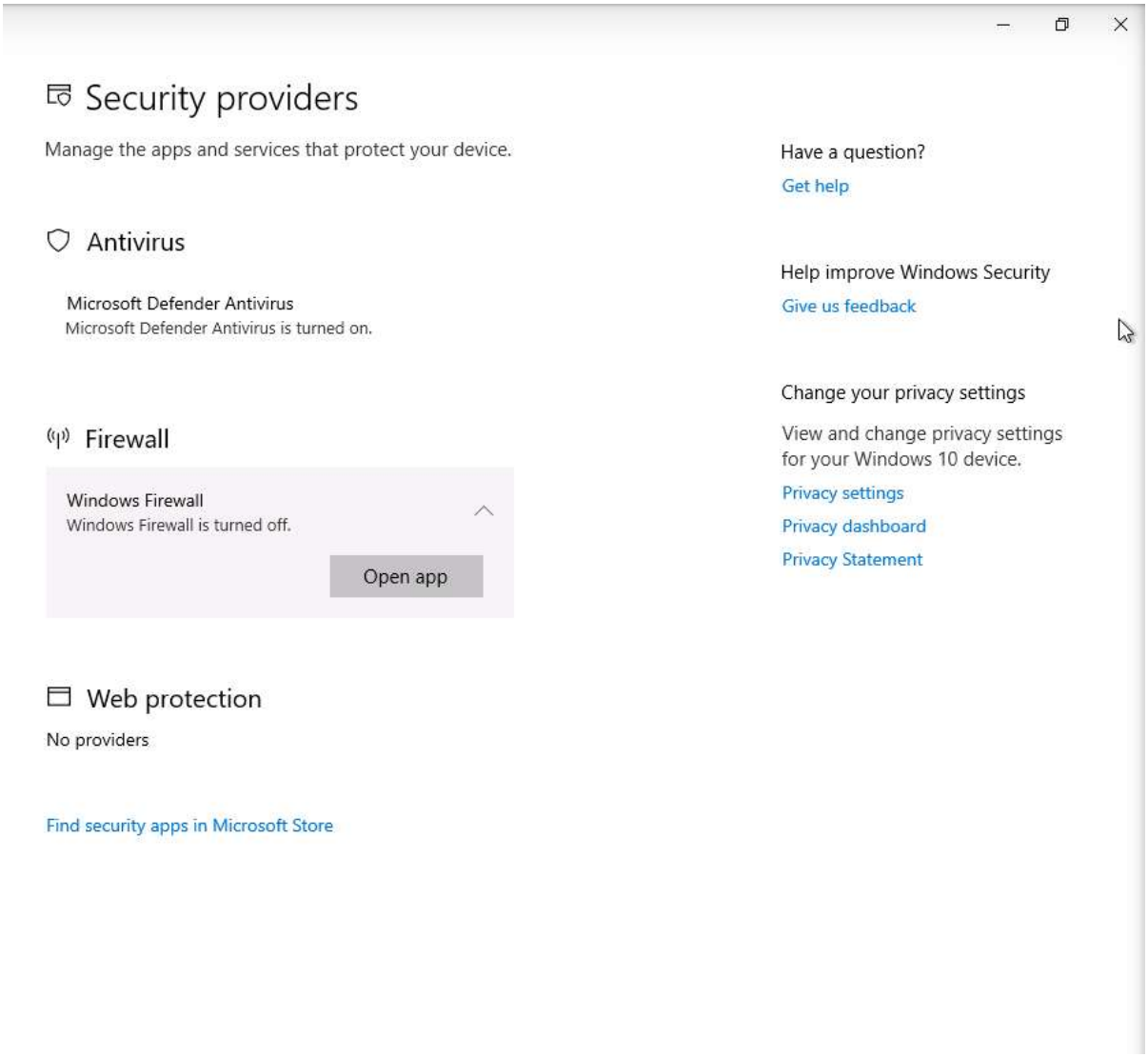
1. *To view a summary of security on Windows 10, start from the **Control Panel**. Use the "Find a setting" bar and search on Windows Defender. You can also search for Windows Defender using the Windows Run bar. Take a screenshot of what you see on the Windows Security screen and include it here:*



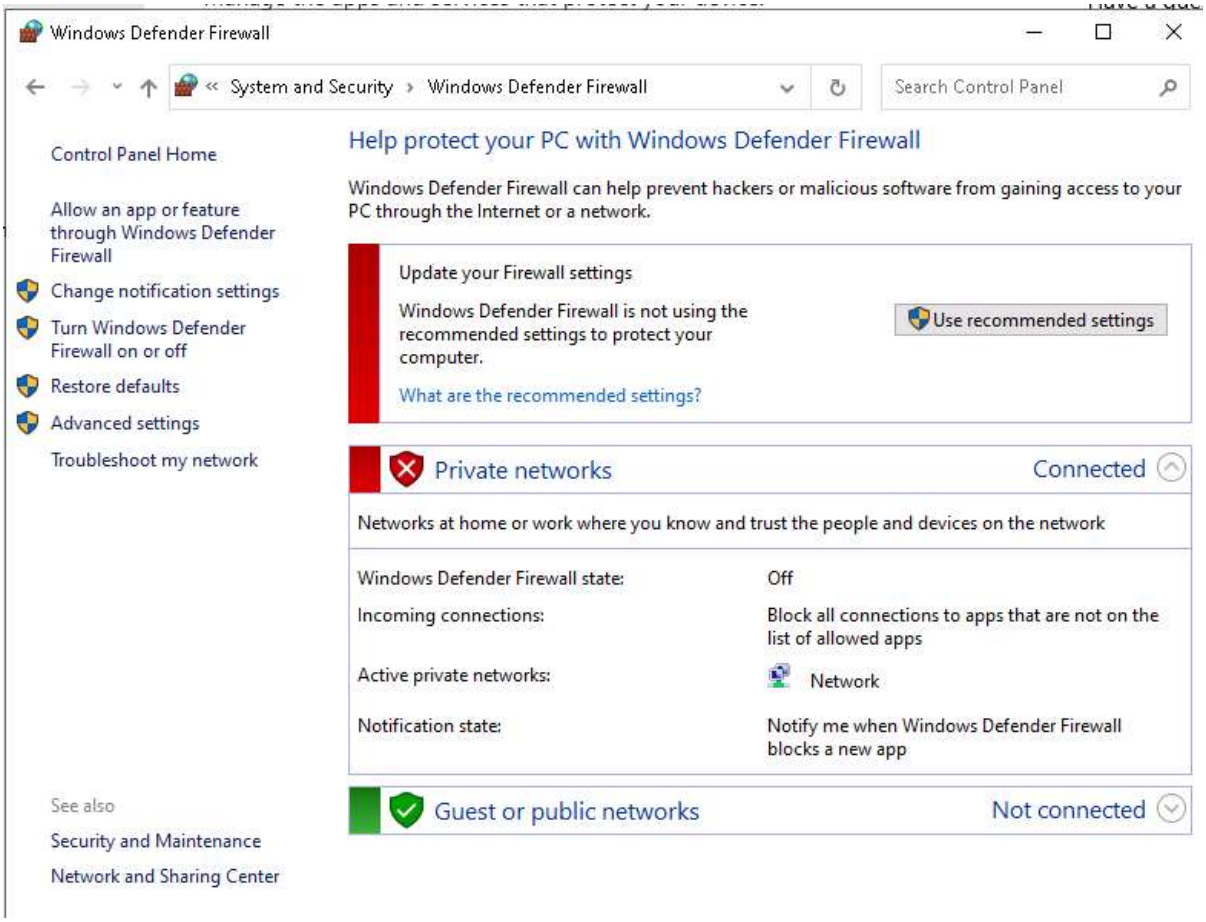
2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve issues."*** *Provide a screenshot of this below:*



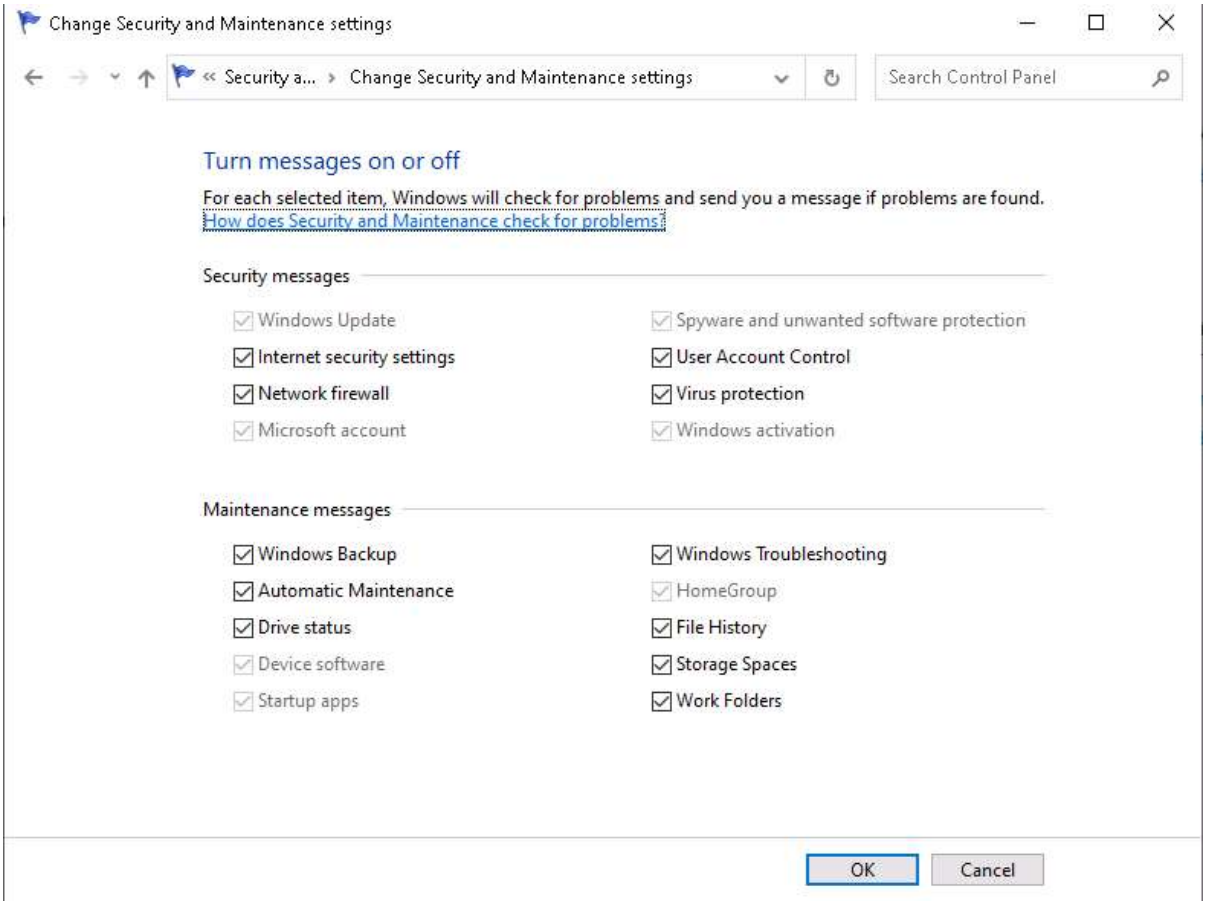
3. *Click on View in Windows Security to see the status there. Provide a screenshot of the **Firewall** settings.*



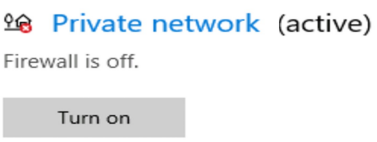
4. *From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:*

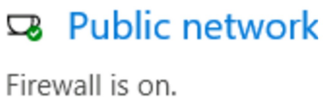
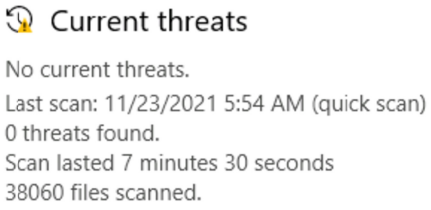
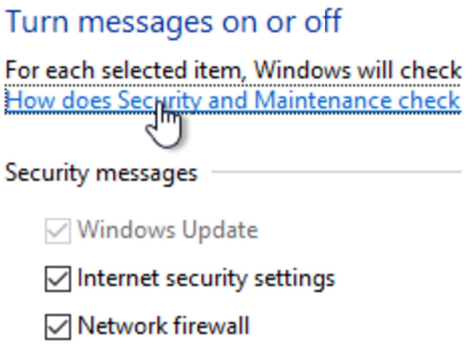
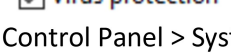


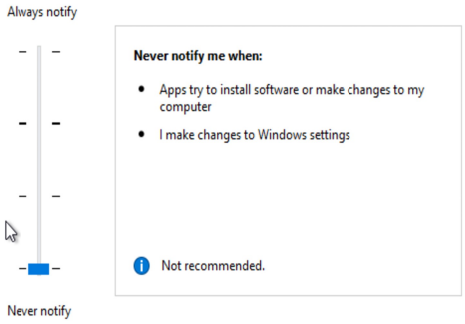
5. *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*




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).*

| **Security Feature** | **Status** |
|---|---|
| Firewall product and status – Private network | Firewall is OFF. Found this in windows security, Firewall & Network Protection<br>  <br>Section. |

| | |
|---|---|
| Firewall product and status – Public network | Firewall is ON. Found this in windows security, Firewall & Network Protection<br>  <br><br>Section. |
| Virus protection product and status | Virus protection is ON. Found this in windows security, Virus & Threat Protection Section.<br>  <br> |
| Internet Security messages | Messages are ON. Found this in Control Panel > System & Security > Security & Maintenance > Change Security & Maintenance Settings |
| Network firewall messages | Messages are ON. Found this in Control Panel > System & Security > Security & Maintenance > Change Security & Maintenance Settings<br>  <br> |
| Virus protection messages | Messages are ON.  <br><br>Found this in Control Panel > System & Security > Security & Maintenance > Change |

| | |
|---|---|
| | Security & Maintenance Settings |
| User Account Control Setting | Never Notify settings were enabled. Found this in Control Panel > System & Security > Security & Maintenance > User Account Control > Change Settings.<br>  |

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.]*

- Firewall for private network is turned off, which can be a major security threat. Disabled firewall permits all data packets to enter and exit the network unrestricted. This includes not just expected traffic, but also malicious data, thereby putting the network at risk.
- There were other unnecessary users like Hacker with Admin rights which puts the whole system at risk as they can modify any security policy and settings in computer.
- User account control settings messages were disabled which implies the computer will never notify if any app try to make changes to computer. If any malicious app makes changes to computer then Joe will not be notified.

# 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?*

*Joe should use the CIS Control to set security policy at his organization. These security controls can be applied to any organization and it is focused on reducing risk and increasing resilience for technical infrastructures.*

2. *What industry baseline do you recommend to Joe?*
   *I would recommend Joe to use the CIS Controls which is the Industry baseline.*

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?

   Joe uses CIS as his baseline, the he'll meet the following basis, fundamental, organizational steps

i. CIS Control 4: Secure Configuration of Enterprise Assets and Software

ii. CIS Control 10: Malware Defenses

## *System and Security*

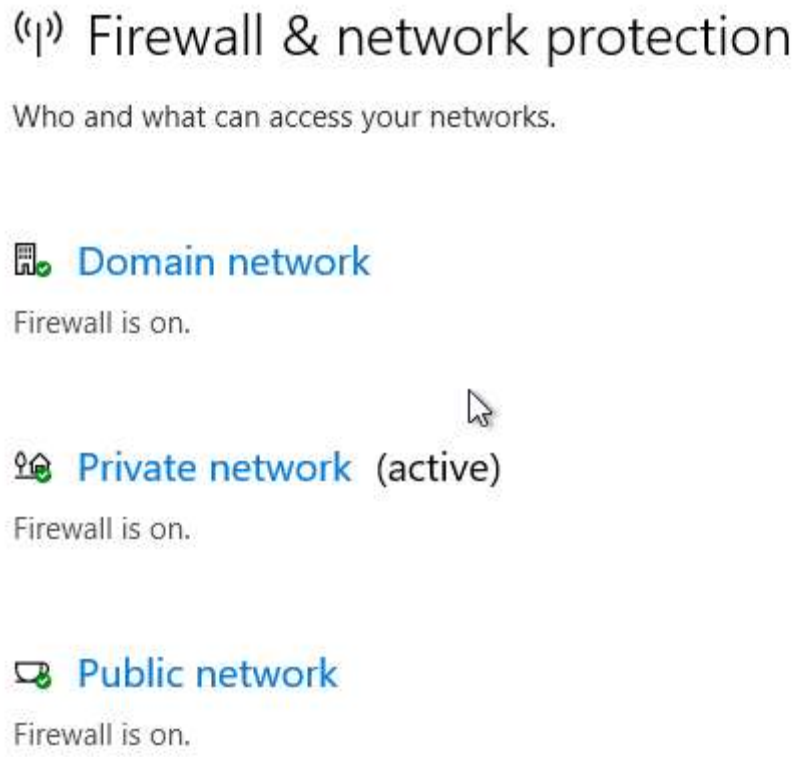
At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

- 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.*
   *To enable firewall for all network access we follow the shown path*
   *Settings > Update & Security > Window Security > Firewall & Network Protection > Turn on Domain Network Protection and Private Network Protection.*
2. *Include screenshots showing the firewall is turned on.*




3. *What protection does this provide?*

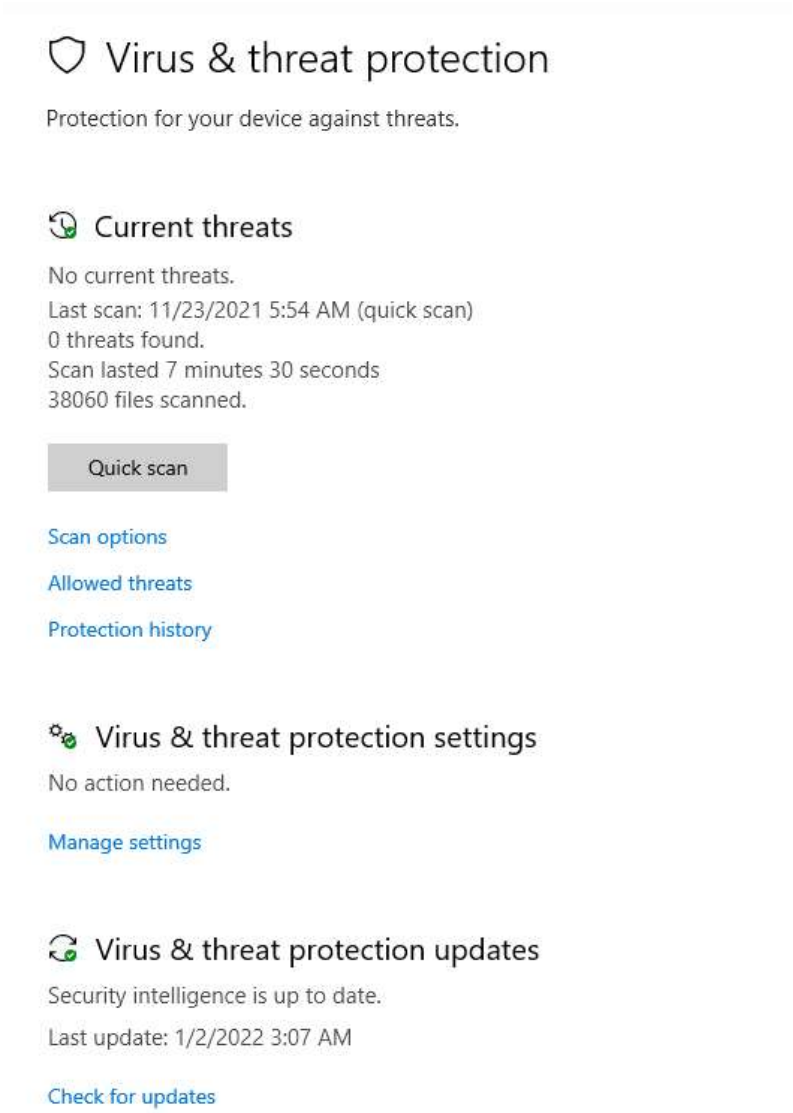
   *This provides protection form malicious network activity. Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.*

**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.

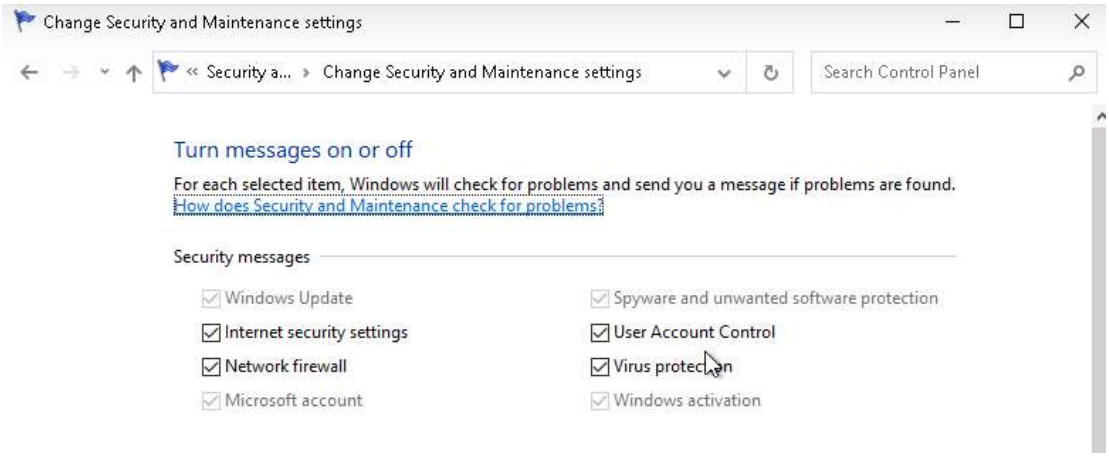
1. *Explain the process you take to do this.*
   *To do the following process we follow the shown path*
   *Settings > Update & Security > Window Security > Virus & Threat protection*
   *there we click the quick scan button to scan for threats at current moment. Also go into Virus & Threat protection settings to ensure Real-time protection is turned on and.*
   *In Virus & threat protection page press cheek for updates under Virus & threat protection updates to ensure Security Intelligence is up to date.*

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.*




3. *Provide at least two risks mitigated by enabling these security settings:*

- By enabling Virus & threat protection, our system will contentiously look for any malicious files in our computes and try to protect us from it by removing them.Alos If there is any virus that managed to sneak into our computer, then a message will be delivered to us informing us about the same.
- By enabling Window Firewall, our computer will ensure that we are protected from any malicious activities on our network.

4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

   i. CIS Critical Security Control 13: Network Monitoring and Defense

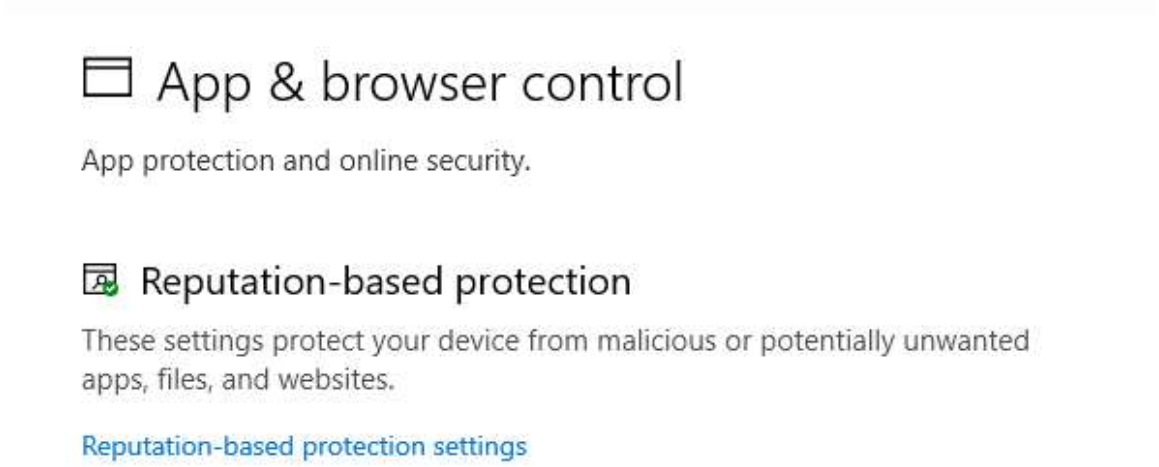
   ii. CIS Critical Security Control 10: Malware Defenses

## 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.*

   *For maximum protection we should enable Reputation-based protection.*




**User Account Control Settings**

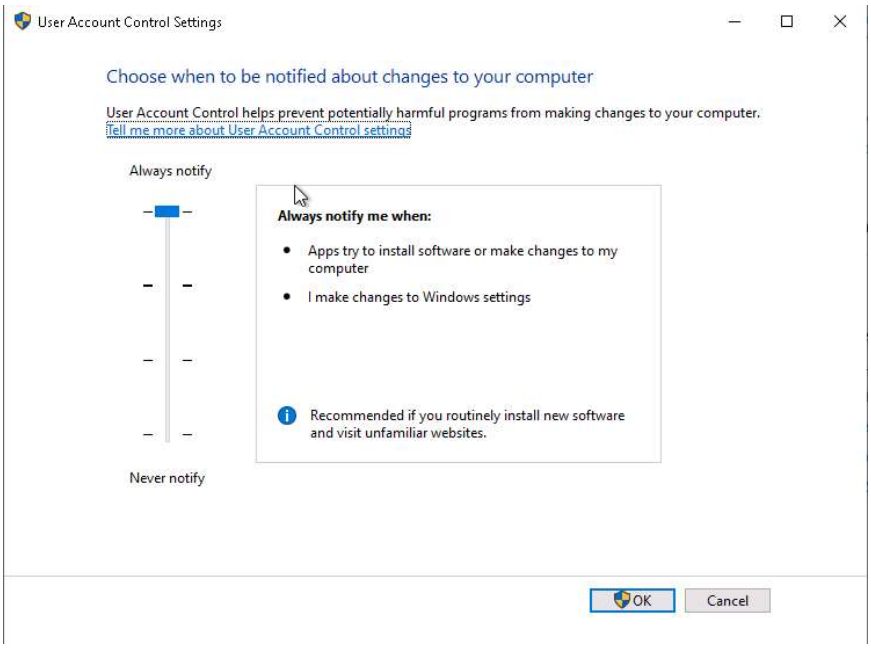
Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer. This is done through the User Account Control Setting.

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

   Never notify

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

   *It should be set to Always notify*




### 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."*
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?*
   *Frank*
   *Hacker*
2. *Bonus questions: What is Hacker's password?*
3. *Explain the steps you take to disable or remove unwanted accounts.*
   *In local User and Groups, under User folder there appears name of users on the computer. Right click on the name you want to remove and select Delete, then a popup will appear confirming if you want to delete the selected user, click Yes, the another popup appears if it is an admin account, asking to delete account, click Yes to delete.*

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

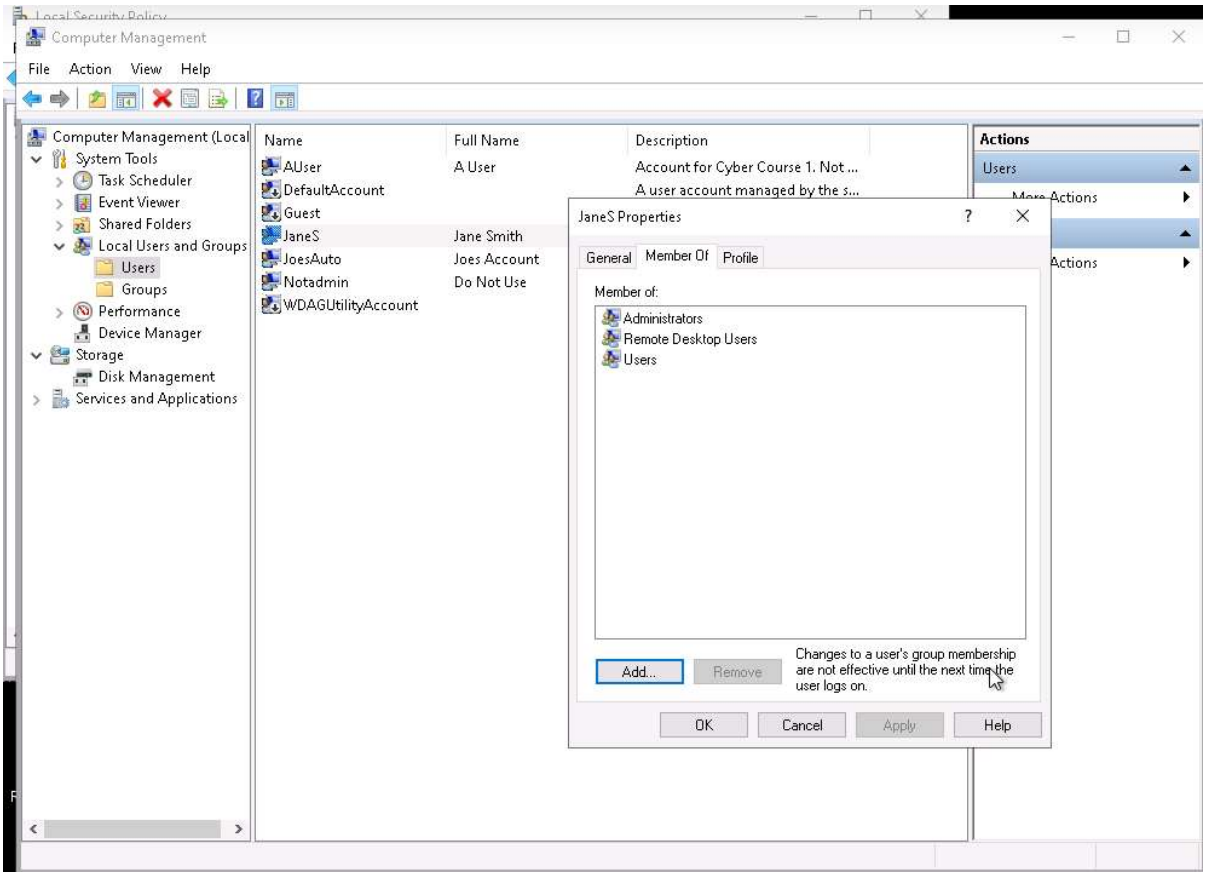
   *Unwanted accounts may get unauthorized access to the PC and perform malicious activities and get sensitive data from PC, therefore it is necessary to remove unwanted or malicious accounts from PC to protect it.*

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?
   Hacker
   JaneS

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

   This could be determined by right clicking the user name and selecting properties, under properties window, there is a “Member of” tab which specifies to which all group does this member belong. If it belongs to Administrator group the there will be Administrator keyword.



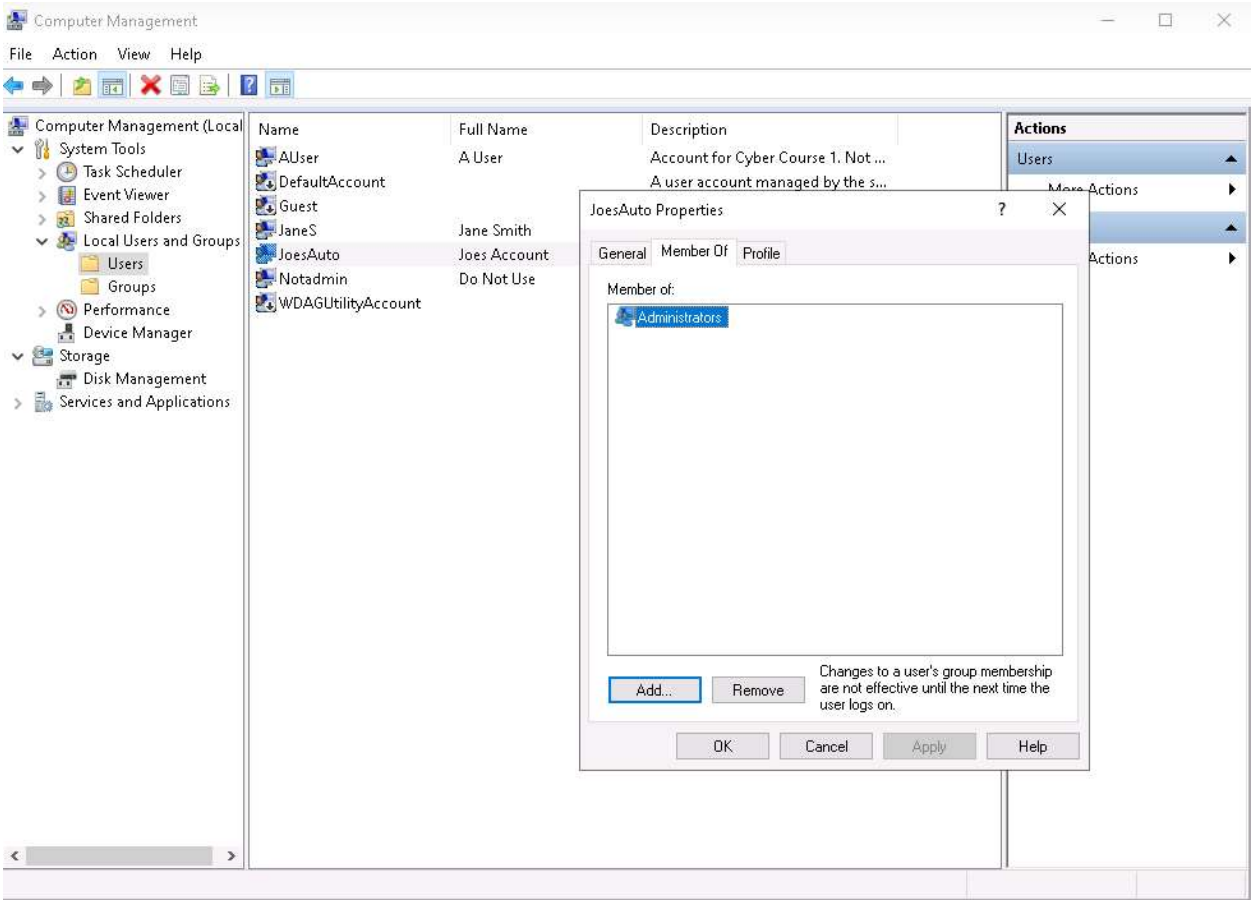

Administrator privileges for too many users are another security challenge.

7. Provide at least three risks associated with users having administrator rights on a PC.

- Higher Risk of Virus/Malware Infections
- Allowing Hackers to Create New User Accounts
- Attacking Other Devices on Your Network

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.*
   *This could be done by right clicking the user name and selecting properties, under properties window, there is a “Member of” tab which specifies to which all group does this member belong. Now to remove Administrator rights, click on administrator and the on bottom there will be a remove button, click on it to remove Administrative Right, Click apply to save the settings.*



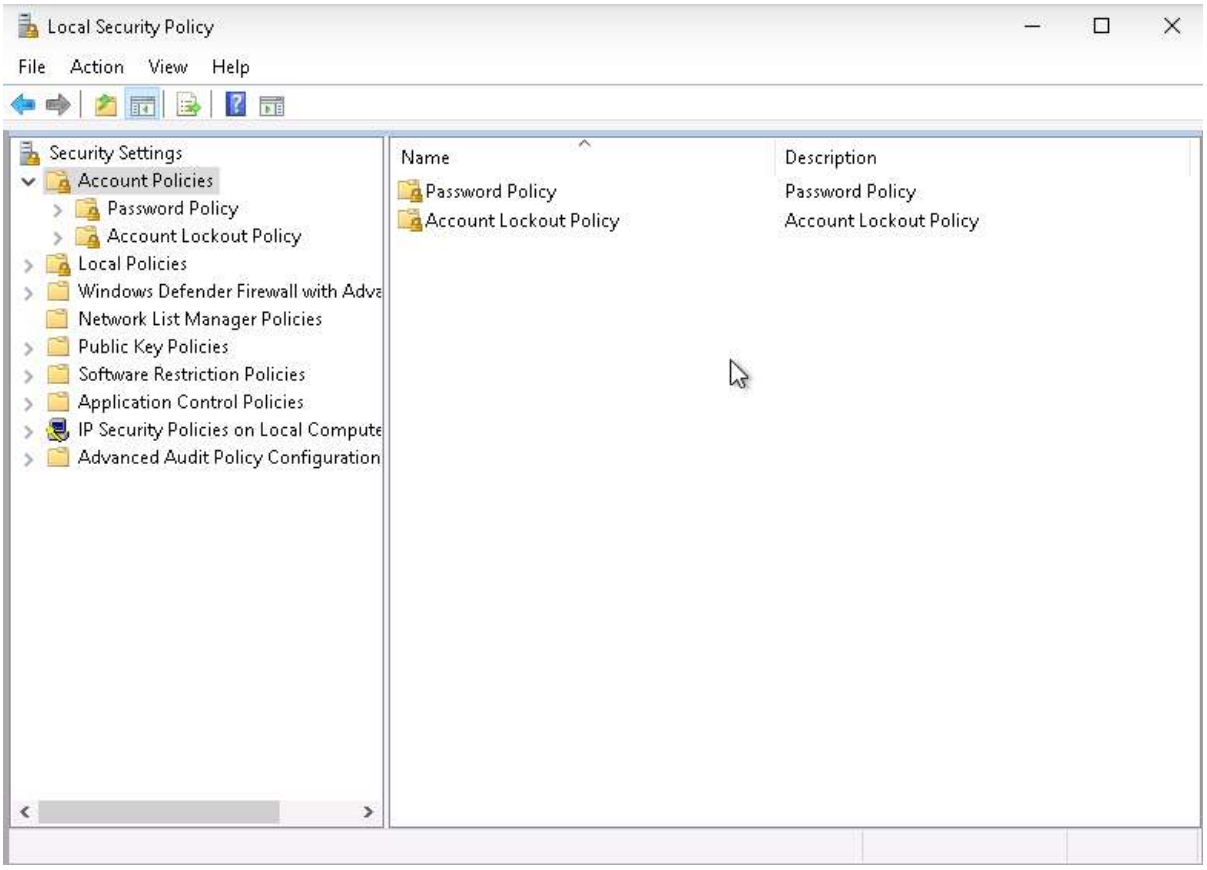

9. *What is the security principle behind this?*
   Least privilege
   Only the minimum necessary rights should be assigned to a subject. Granting more than required permission can allow that user to obtain or change information in unwanted ways. Therefore, careful delegation of access rights can limit attackers from damaging a system.
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

    CIS Critical Security Control 6: Access Control Management

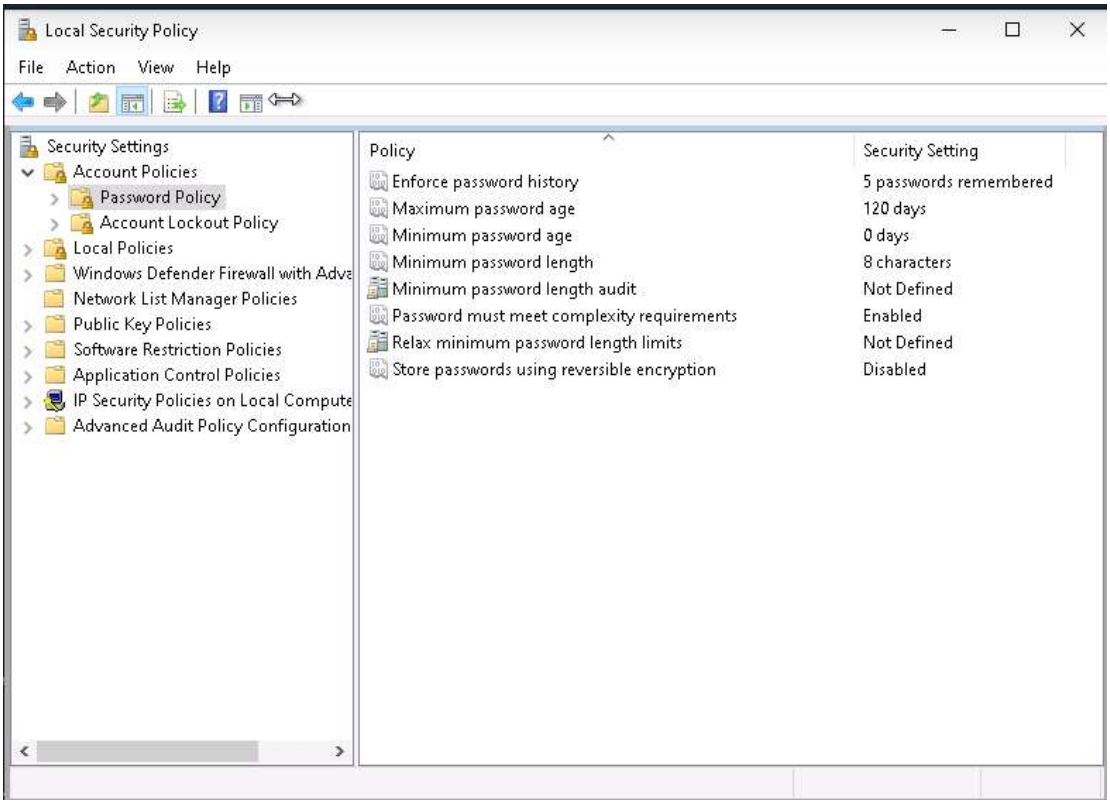
## *Setting Access and Authentication Policies*

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.]*

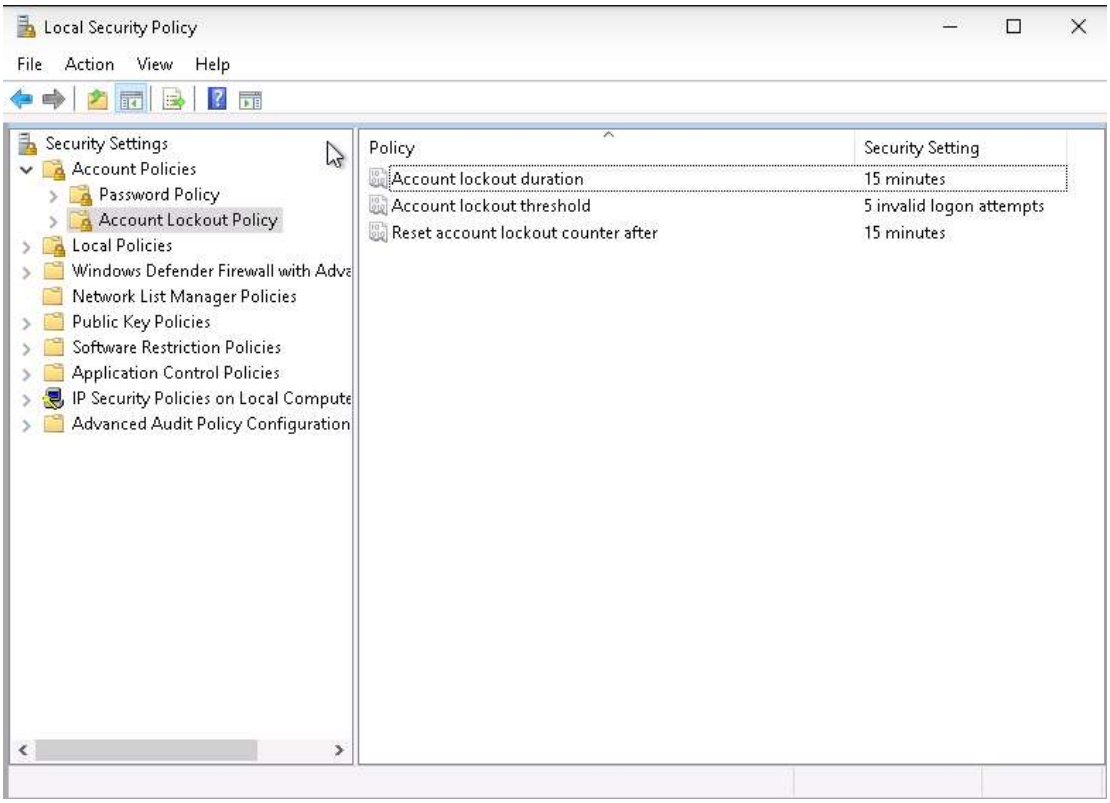


2. Explain the process for setting the password and access control policies locally on a Windows 10 PC. Provide screenshots showing how you set the rules on the PC.
    - Setting the Password Policy:
      To set Password policy, we go into password policy section of account Policy, then we set security settings for various policies as mentioned.



- Setting the Account Lockout Policy:

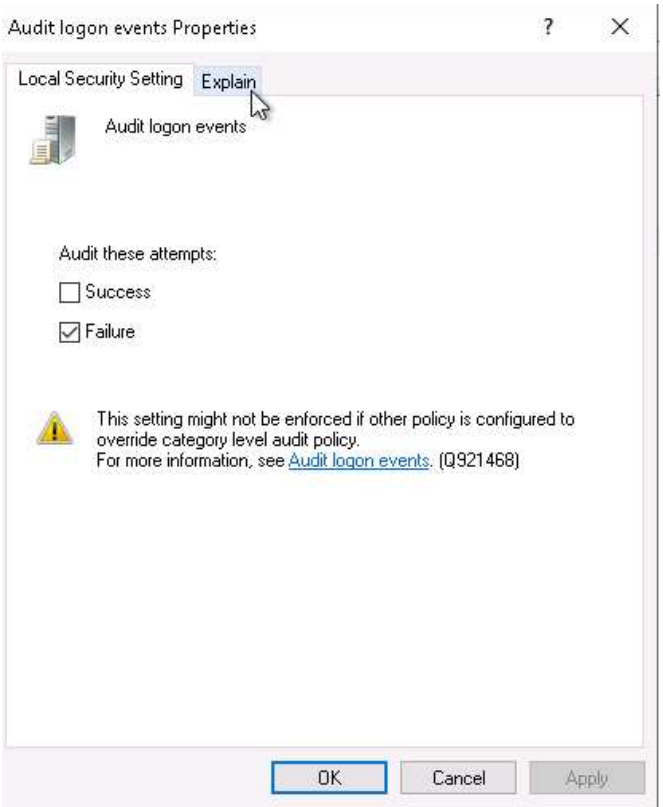
  To set Account lockout policy, we go into Account lockout policy section of account Policy, then we set security settings for various policies as mentioned.

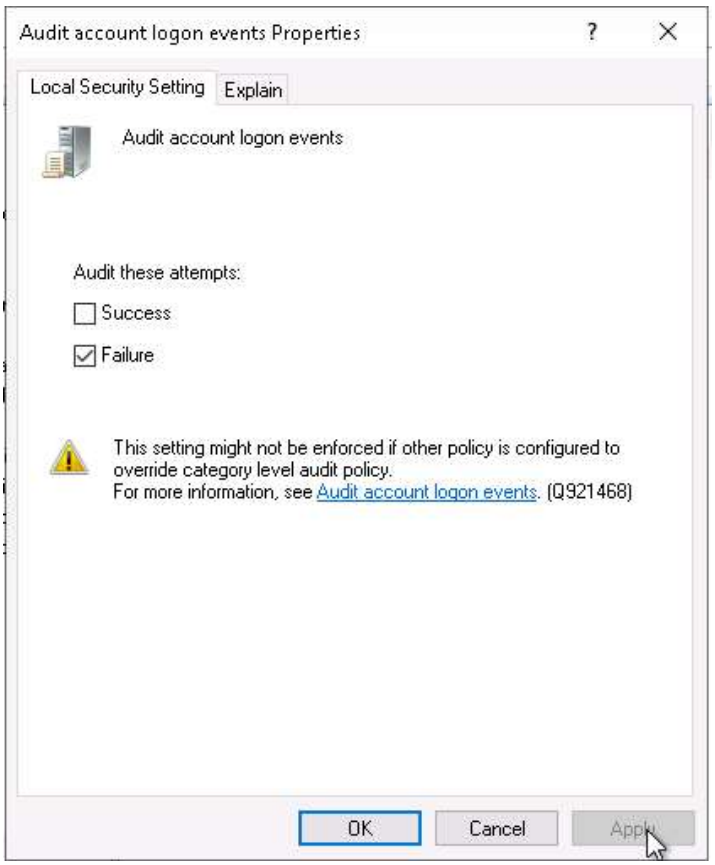


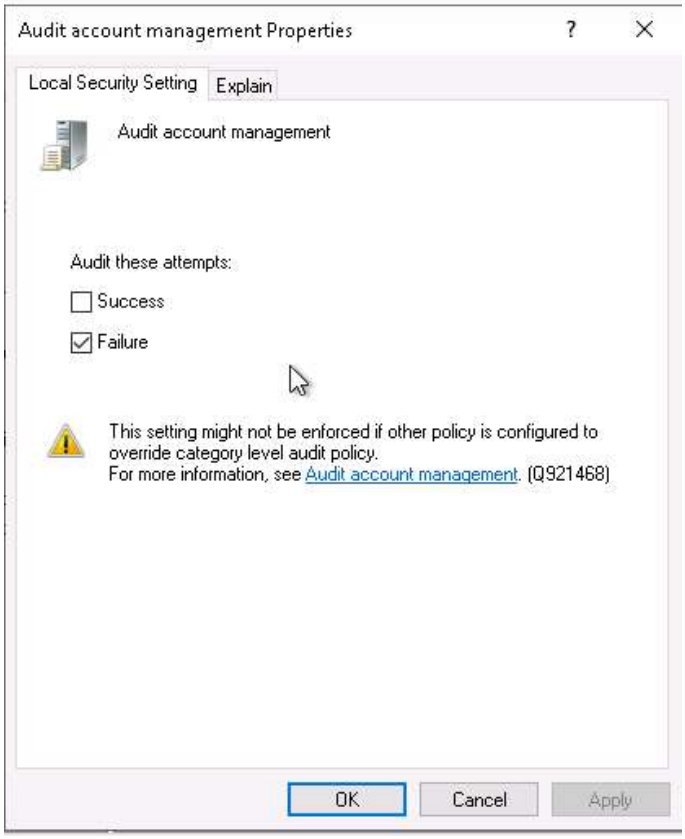

## *Auditing and Logging*

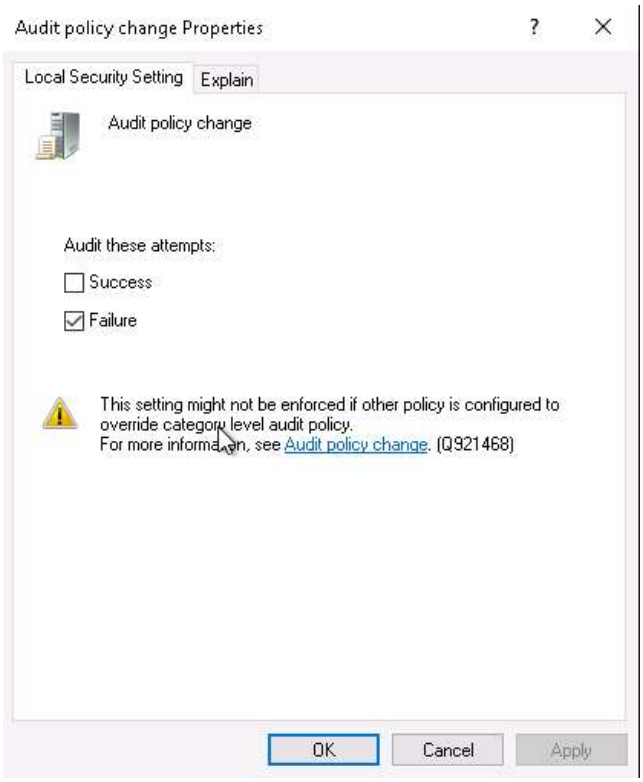
Security best practices like those found in the CIS Controls or NIST Cybersecurity Framework require systems to log events. You need to enable the Audit Policy for Joe's PC to meet these standards.

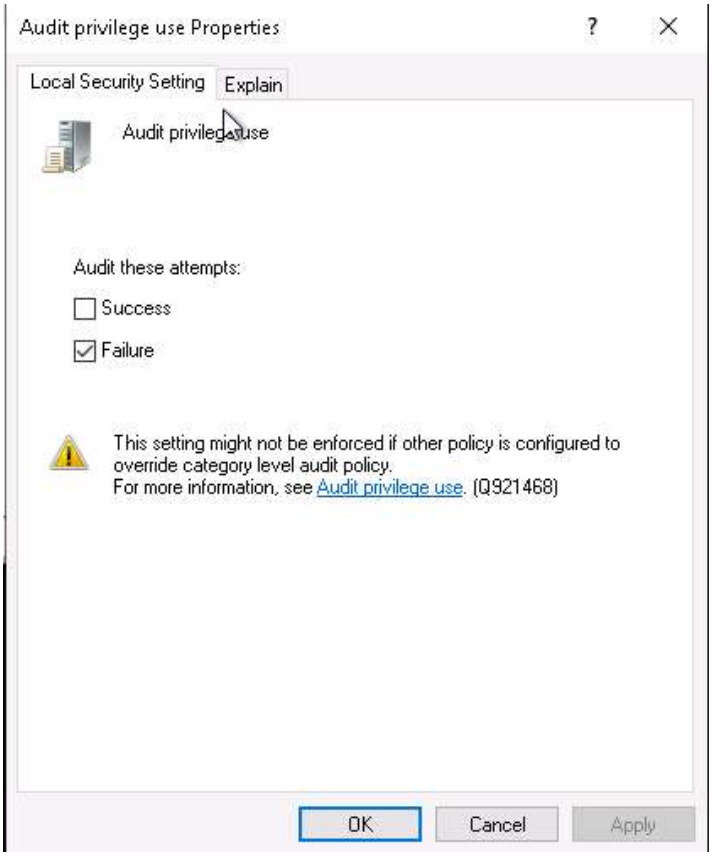
1. From the Local Security Policy window, select Audit Policy and make applicable changes to Joe's PC to enable minimal logging of logon, account, privilege use and policy changes.




Audit account logon events Properties
Local Security Setting
Explain
Audit account logon events
Audit these attempts:
Success
Failure
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)
OK
Cancel
Apply


Audit account management Properties
Local Security Setting
Explain
Audit account management
Audit these attempts:
Success
Failure
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account management. (Q921468)
OK
Cancel
Apply


Audit policy change Properties
Local Security Setting
Explain
Audit policy change
Audit these attempts:
Success
Failure
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit policy change. (Q921468)
OK
Cancel
Apply


Audit privilege use Properties
Local Security Setting
Explain
Audit privilege use
Audit these attempts:
Success
Failure
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit privilege use. (Q921468)
OK
Cancel
Apply

# 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*
- *Hulu*
- *VNC Server & Viewer*

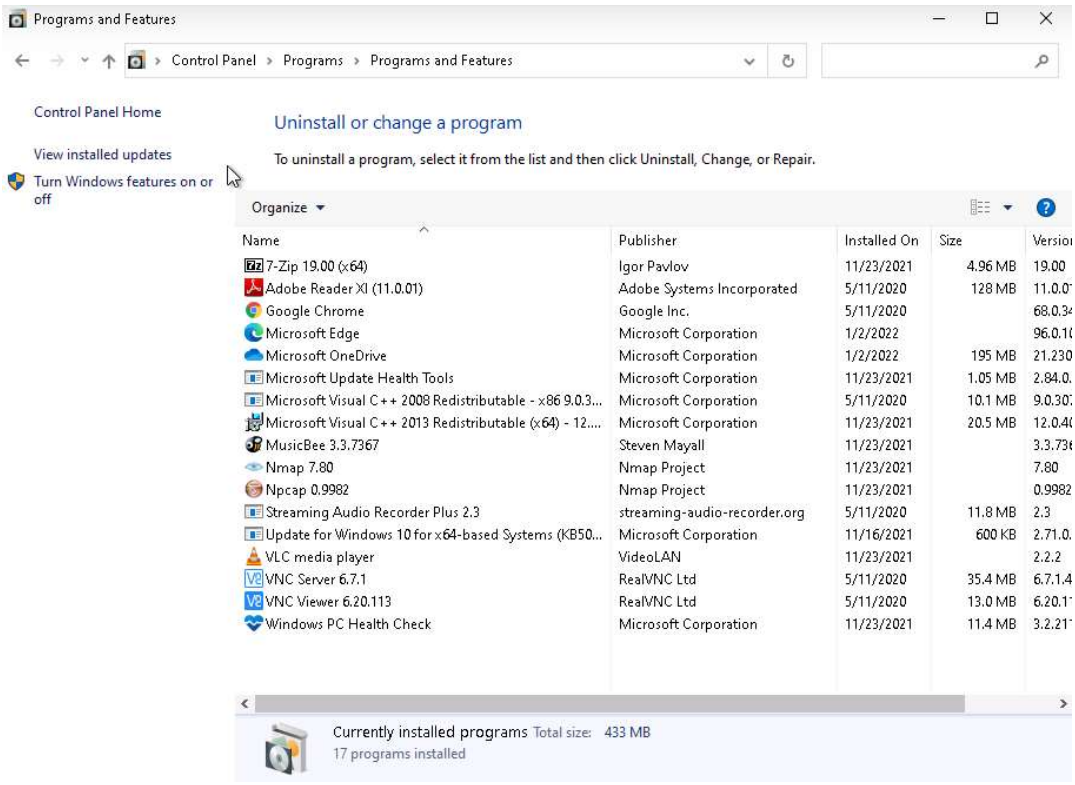
2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*

- *Data Breach From that Application*
- *Remote control access to computer from applications like VNC*
- *Unpatched Security Vulnerabilities*
- *Hidden Backdoor program*

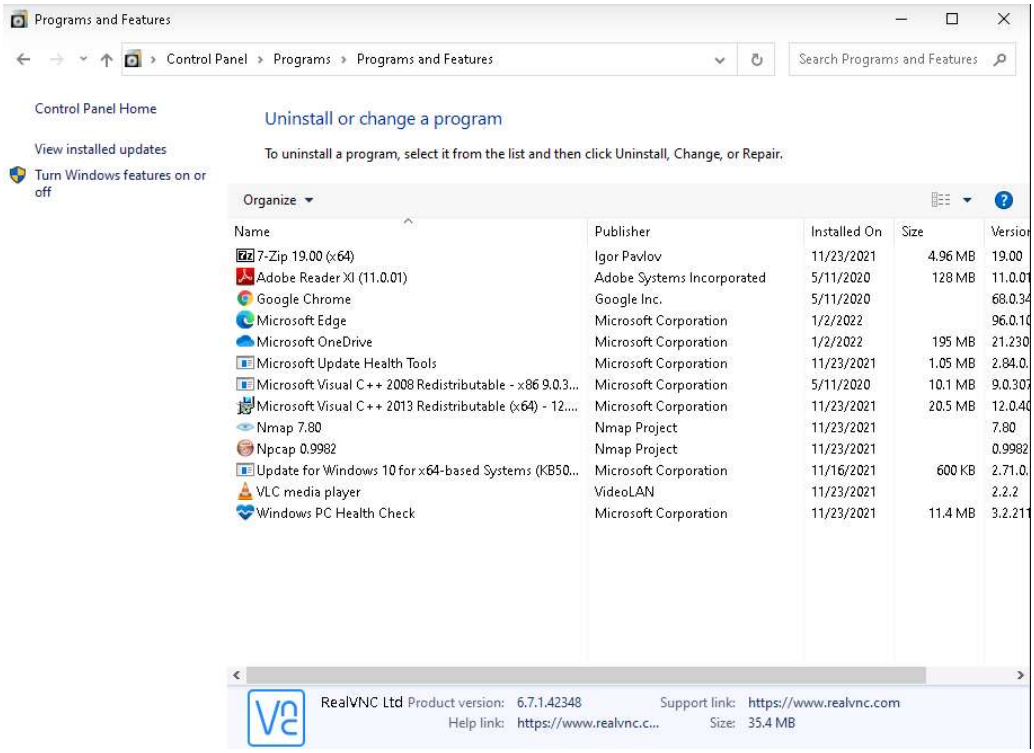
3. *Joe wants you to make sure unneeded applications or programs are no longer on the PC. Explain the steps you take to disable or remove them. Include screenshots to show your work.*

   *To disable or remove them we would go to control panel the select Programs section, then uninstall a program and remove the unnecessary programs.*

   *Program before Removal*



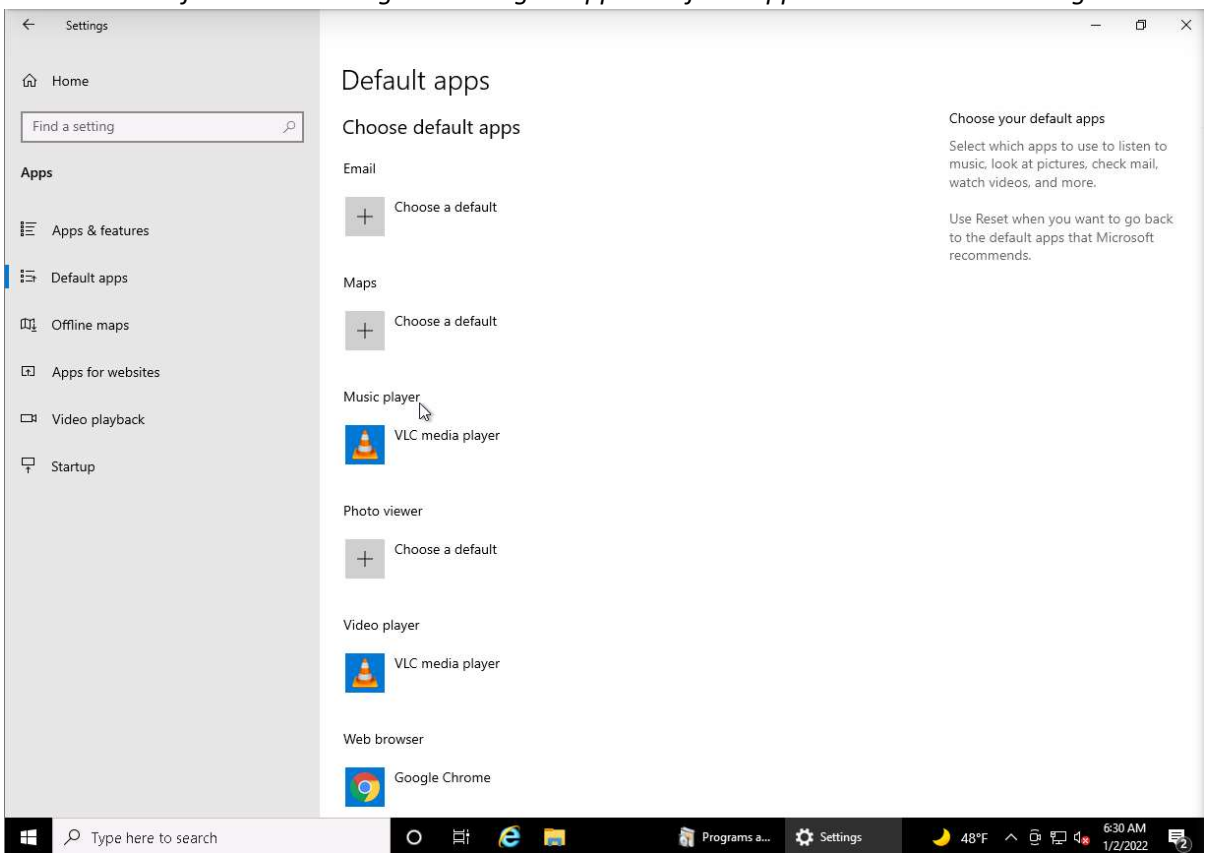

After removing unnecessary Programs



## *Default Browser*

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

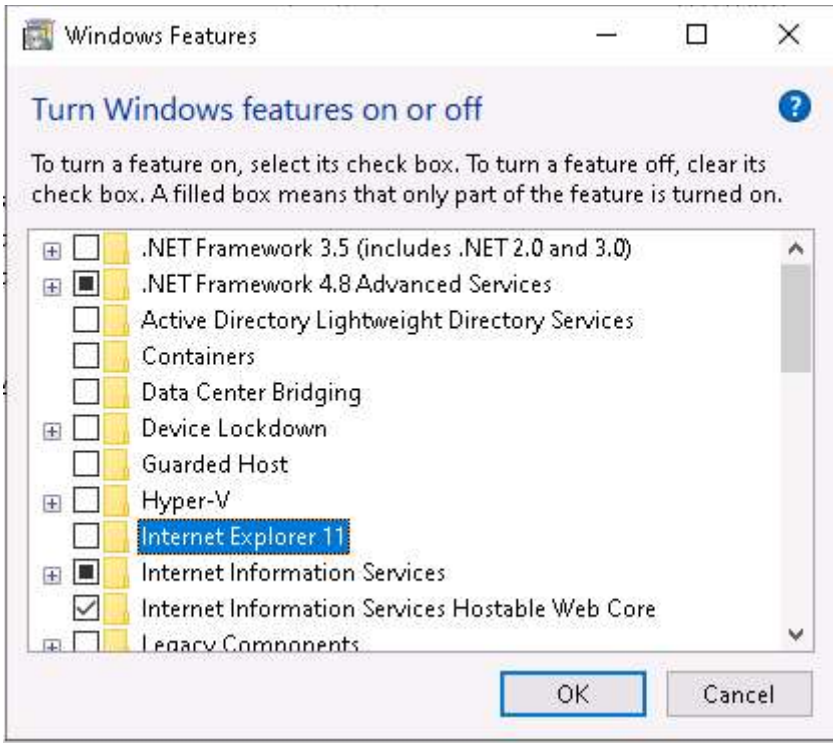
1. *Explain how you set default applications within the Windows 10 operating system. Include screenshots as necessary.*
   *To set default brower we go to Settings > Apps > Default Apps > Web Browser > Google Chrome*




2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
   - As it is no longer supported and no longer receives updates, so it is not patched for latest vulnerabilities.
   - Lack of Support

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**."

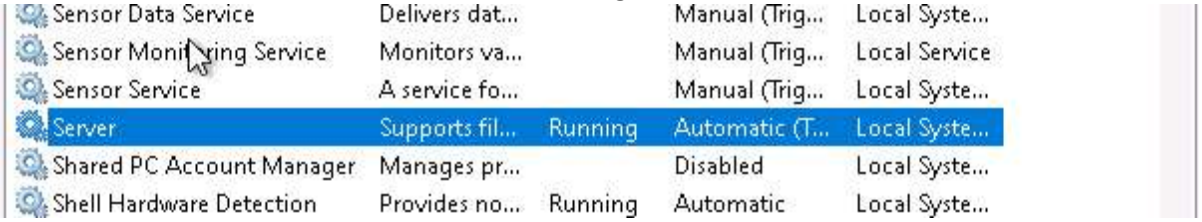
3. *Provide a screenshot showing Internet Explorer 11 is off.*



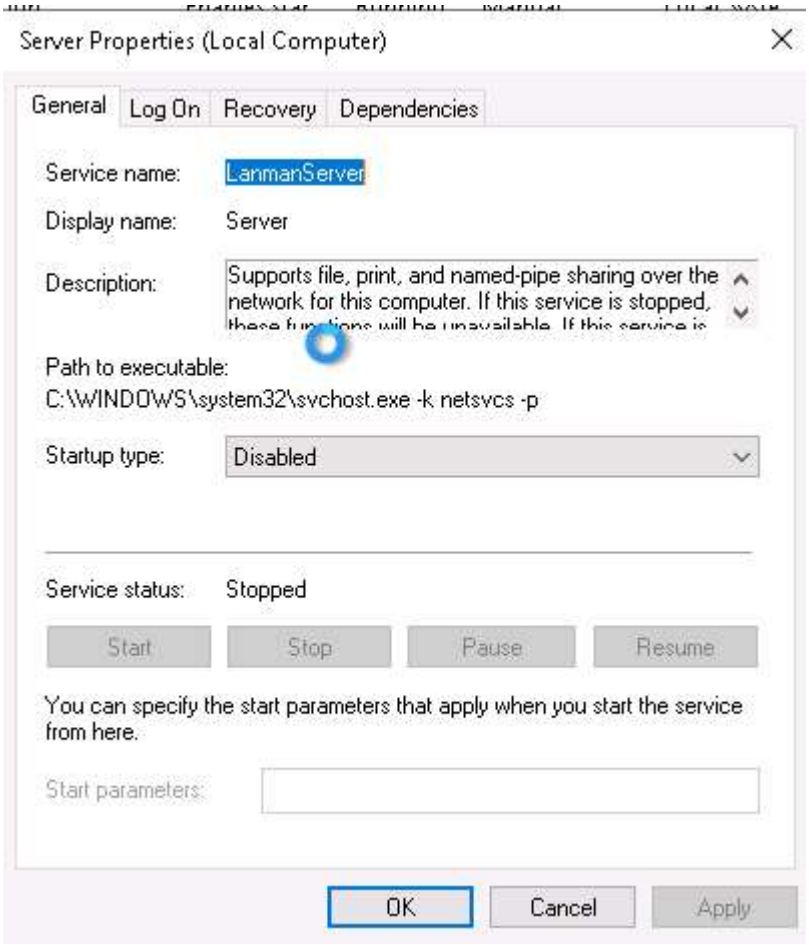

## *Windows Services*

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.
   Next to server service, status is shown as running




2. Advanced users should provide at least two methods for determining a web server is running on a host
3. How do you disable them and make sure they are not restarted?
   Double clicking on server and then in startup type, selecting Disabled and setting the service status to Stopped.

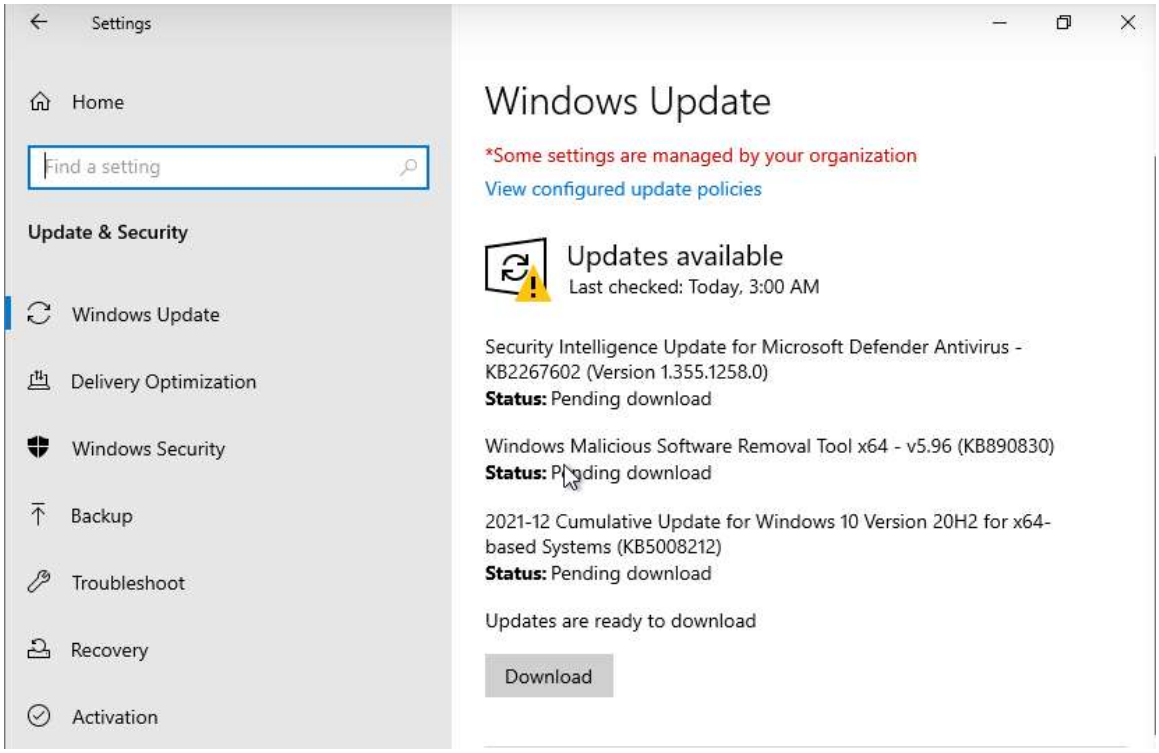



4. Advanced Users: The File Transfer Protocol FTP service is also running on this PC and shouldn't. Explain the process for disabling it and ensuring it is not automatically restarted.

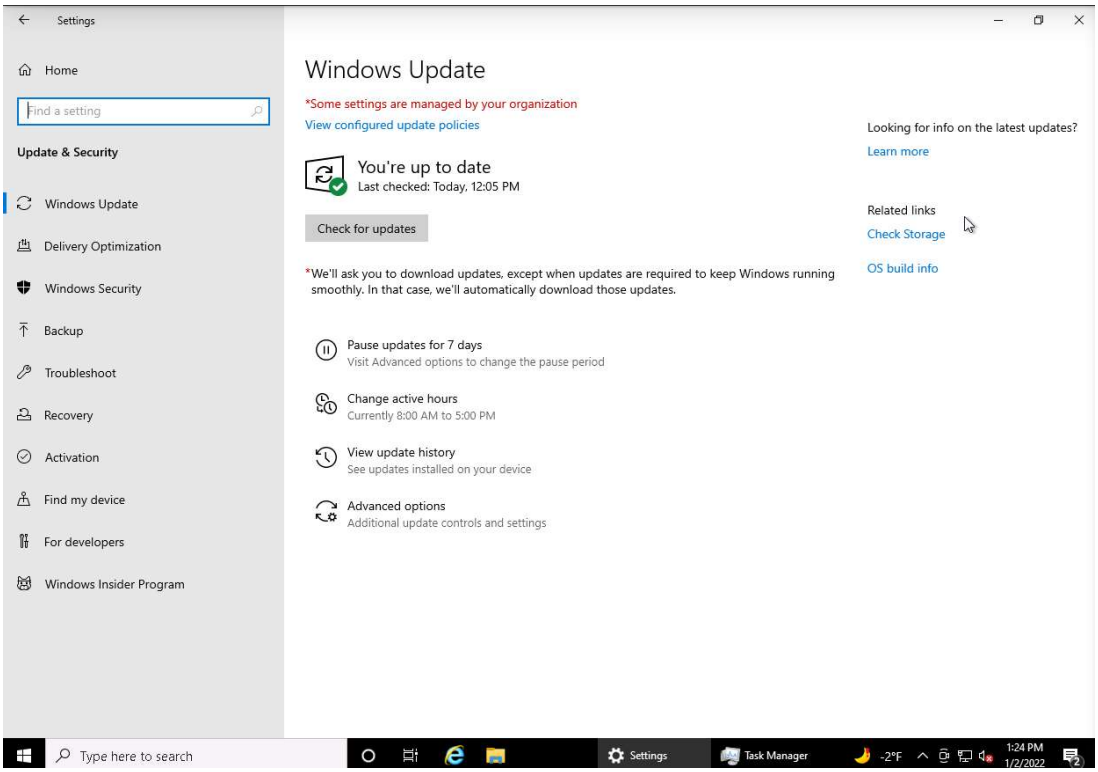
## *Patching and Updates*

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 to Settings > Update & Security > Download Updates/Check for Updates.*




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.

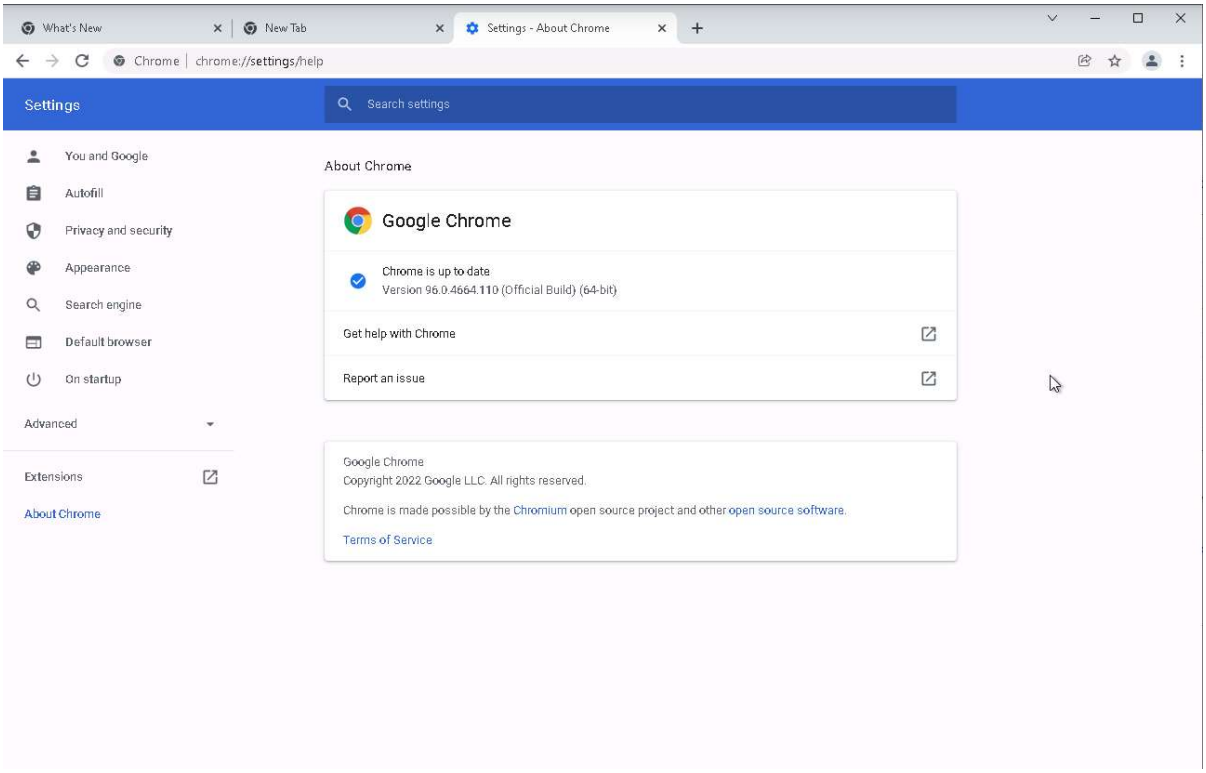
3. *List at least two applications on Joe's PC that are out of date. List them below:*

- Google Chrome
- Acrobat reader XI

4. *Explain the steps you took to determine this information.*
   *Open the desired application, the click on about, check the version and check on internet if any new version is available.*
5. *Explain the steps for updating each of these applications. Include screenshots as needed.*

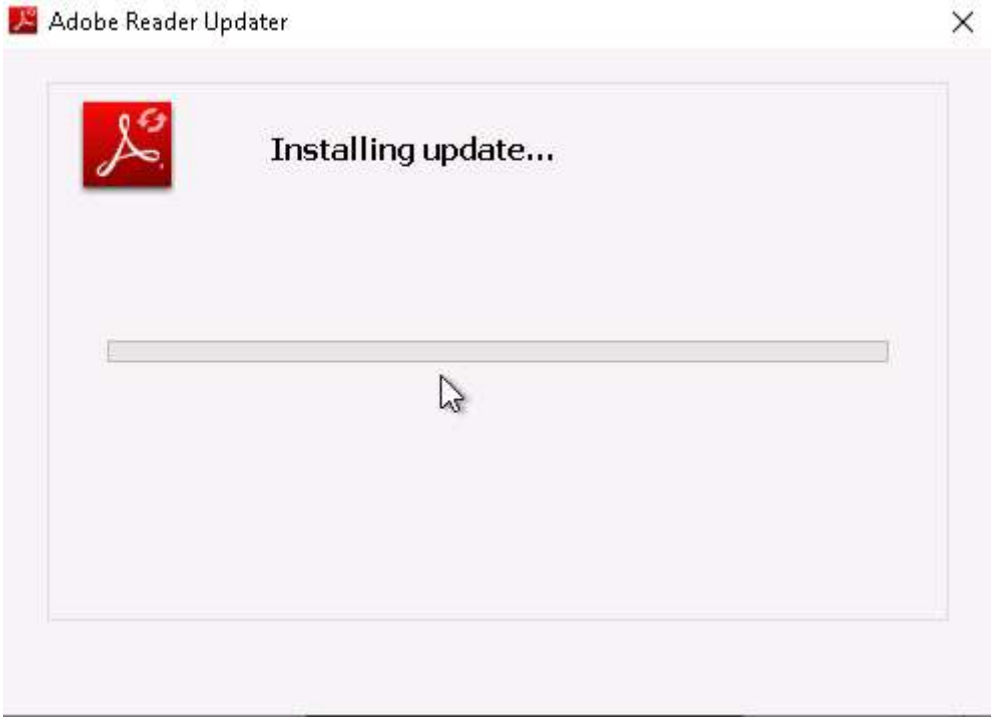
   *Google Chrome*

   *Open Google Chrome, in top right corner click three dots, then select settings, go to about Chrome, it will automatically start checking for updates and update the browser.*



*Adobe reader XI*

*Open the application, in top menu bar click on Help tab, the click on Check for updates, if update is available it will ask you to download it and install it.*



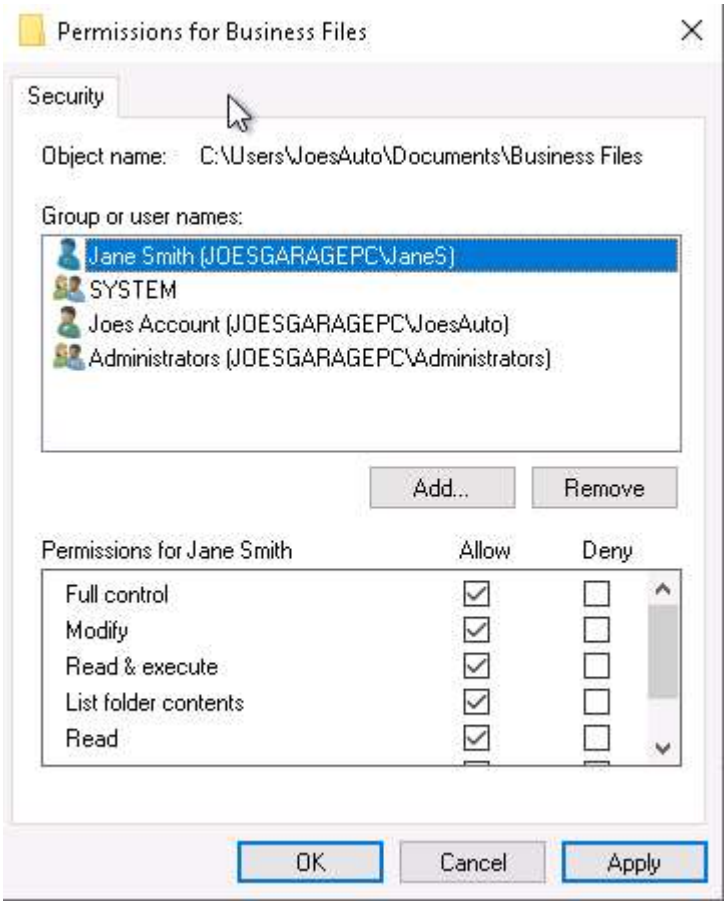

# 5. Securing Files and Folders

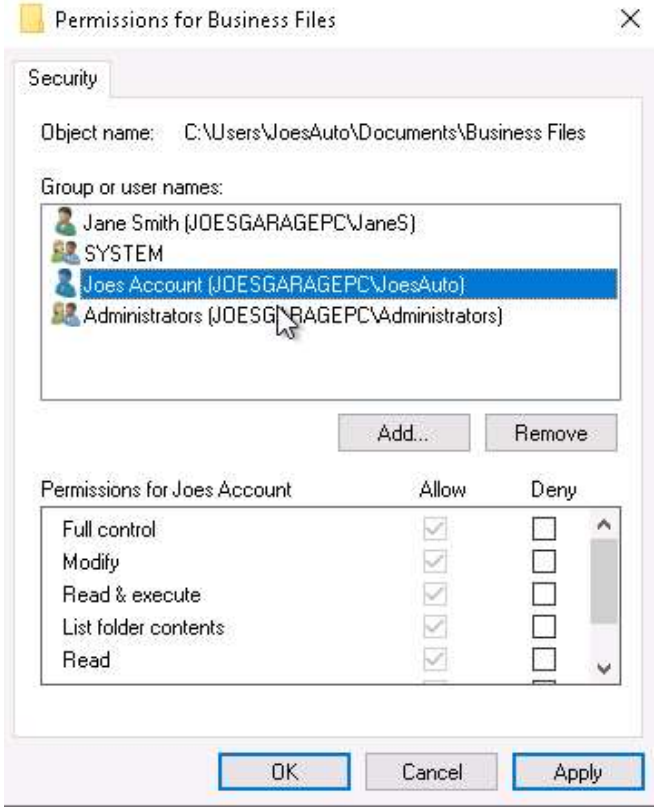
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork."

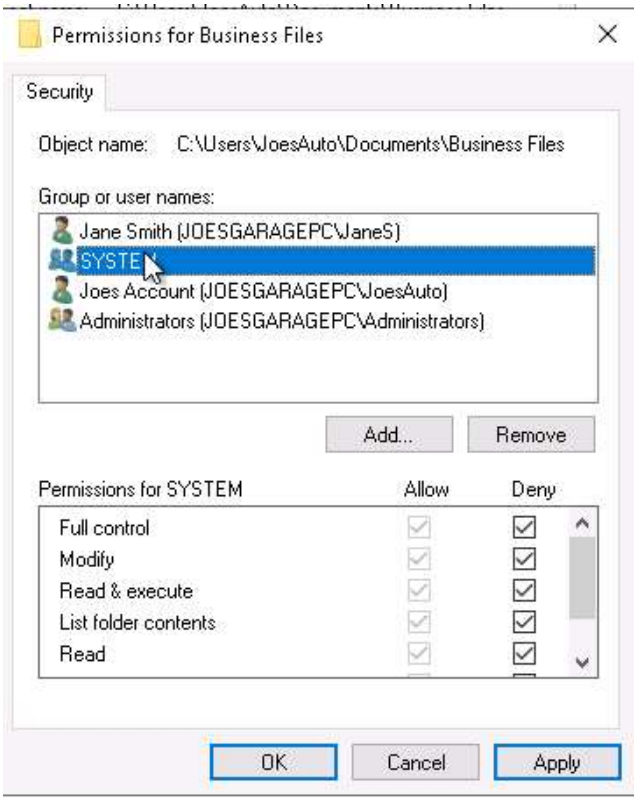
Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

## *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.]*
   *Right click on folder > select properties > go to Securities tab > click on edit button and remove or add users as necessary.*

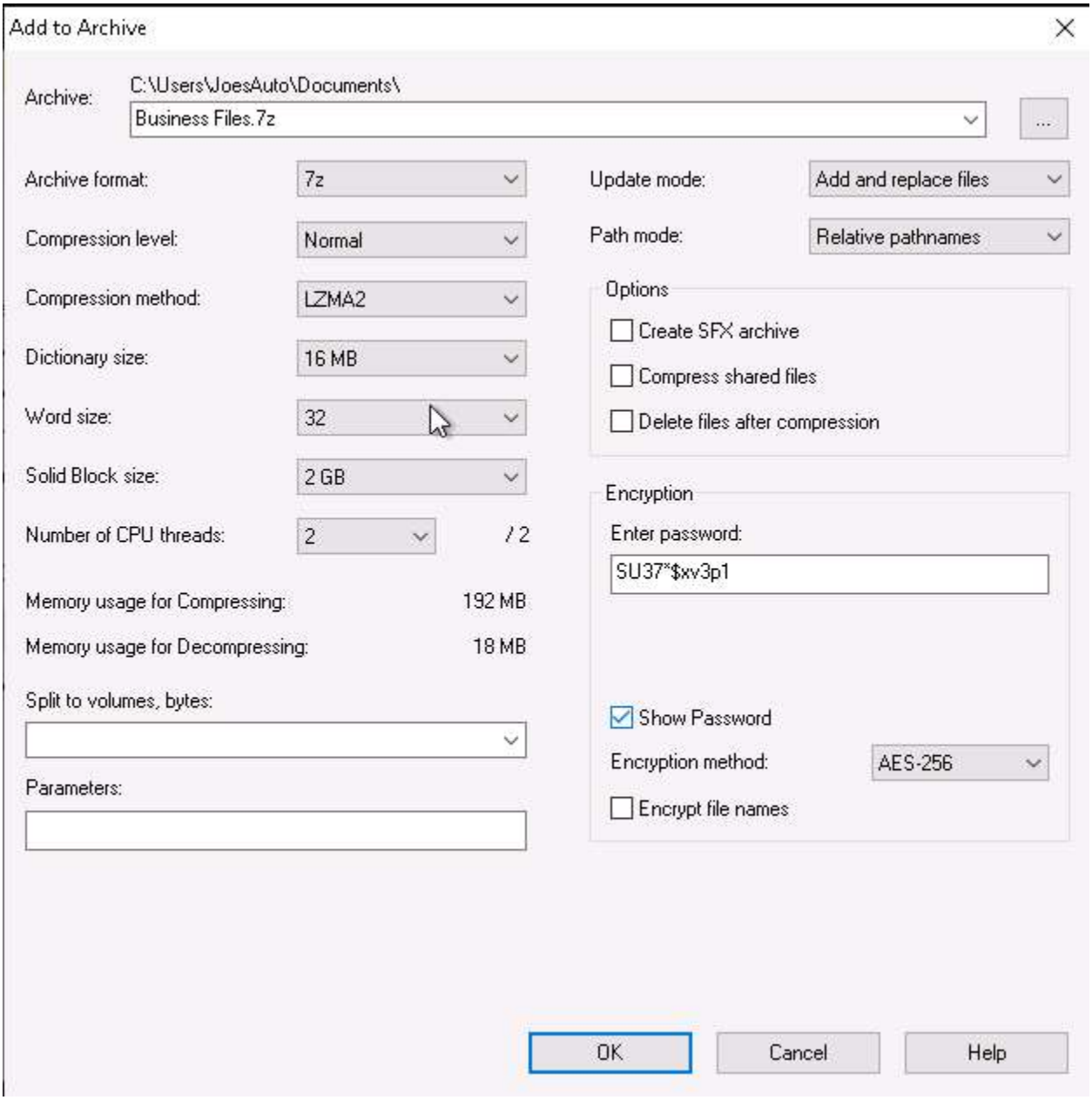

Permissions for Business Files
Security
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
Jane Smith (JOESGARAGEPC\JaneS)
SYSTEM
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
Add...
Remove
Permissions for Jane Smith
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply


Permissions for Business Files
Security
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
Jane Smith (JOESGARAGEPC\JaneS)
SYSTEM
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
Add...
Remove
Permissions for Joes Account
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply

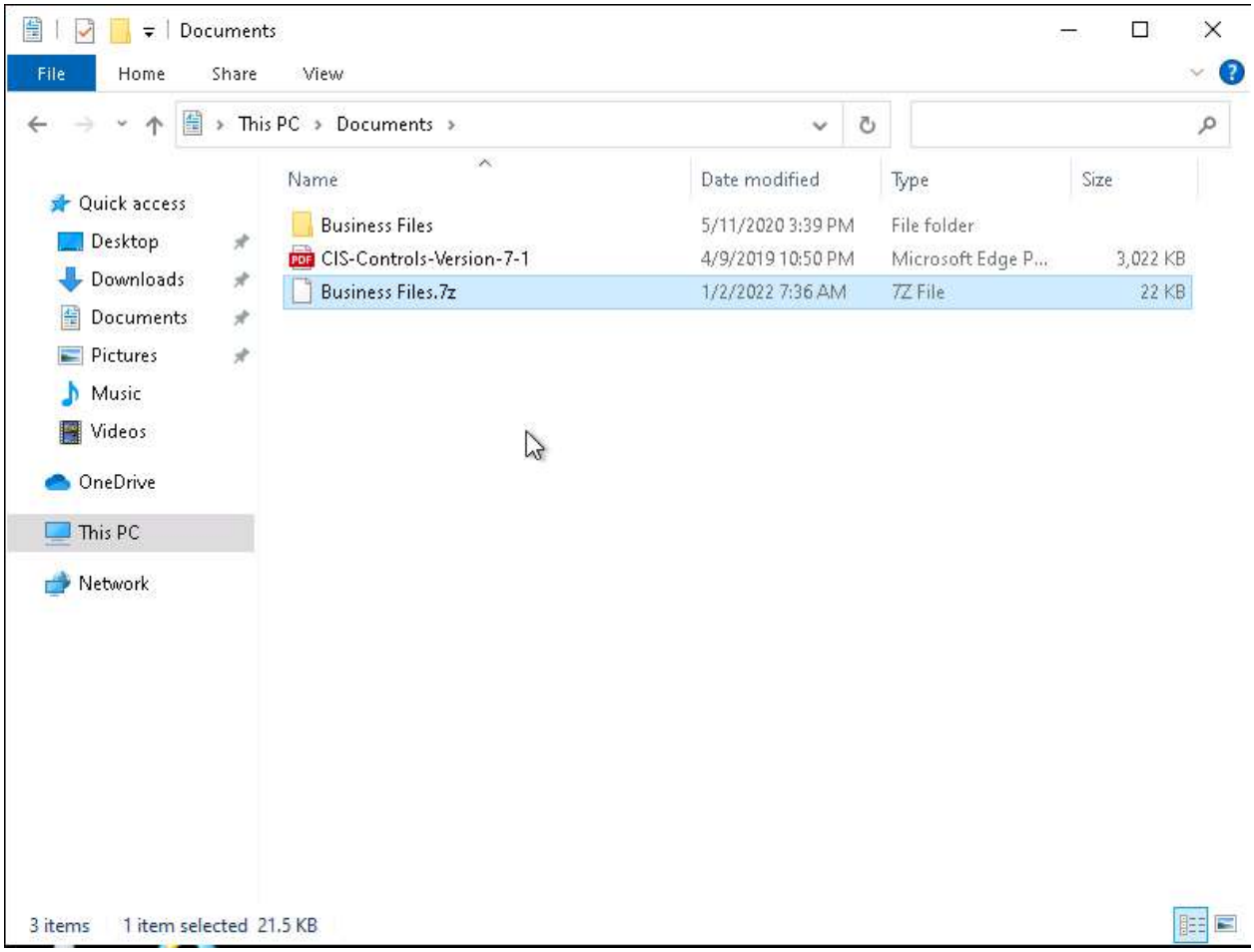

Permissions for Business Files
Security
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
Jane Smith (JOESGARAGEPC\JaneS)
SYSTEM
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
Add...
Remove
Permissions for SYSTEM
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
OK
Cancel
Apply

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.*

*We will open Documents folder, then click on Business Files, right click, select 7-Zip > Add to archive > Under Encryption Area set password and the click Ok*



*Business Files.7z is encrypted*



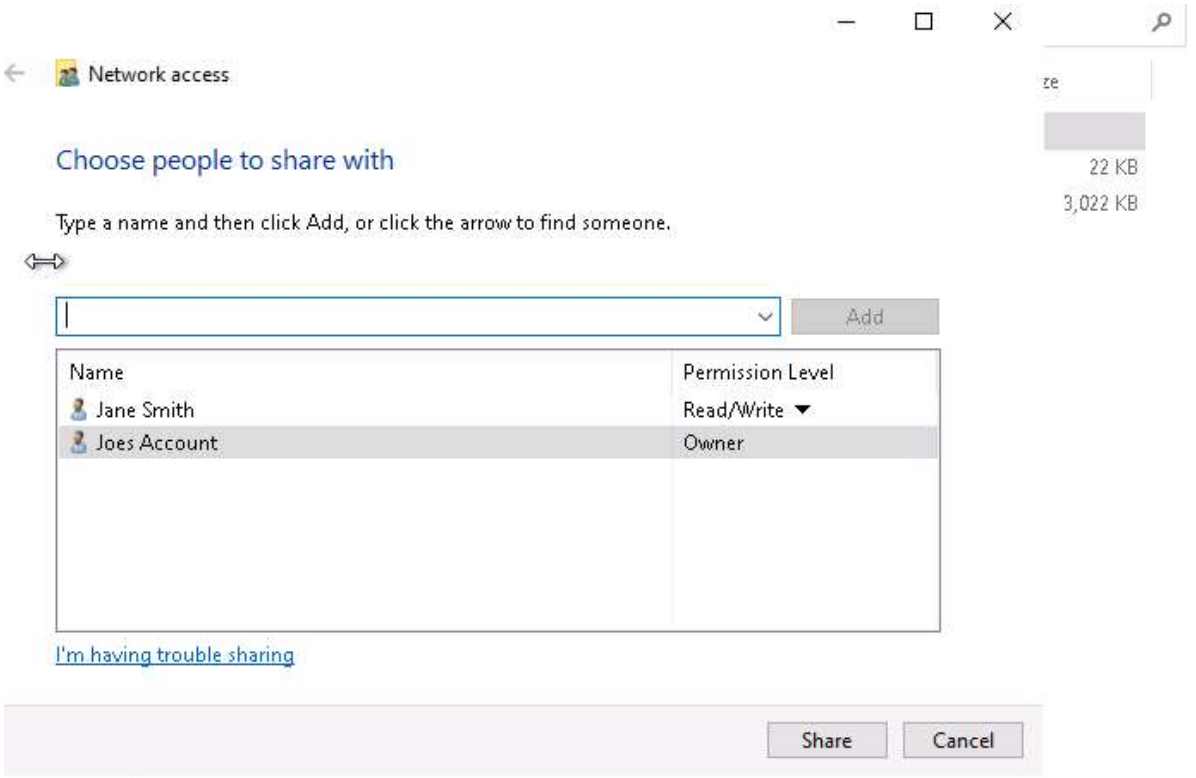

*3. What security fundamental does this provide?*
*It provides Confidentiality. It is the ability to hide information from those people unauthorized to view it. We used encryption to ensure confidentiality of data, so that only authorized users can assess it.*
*4. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?*

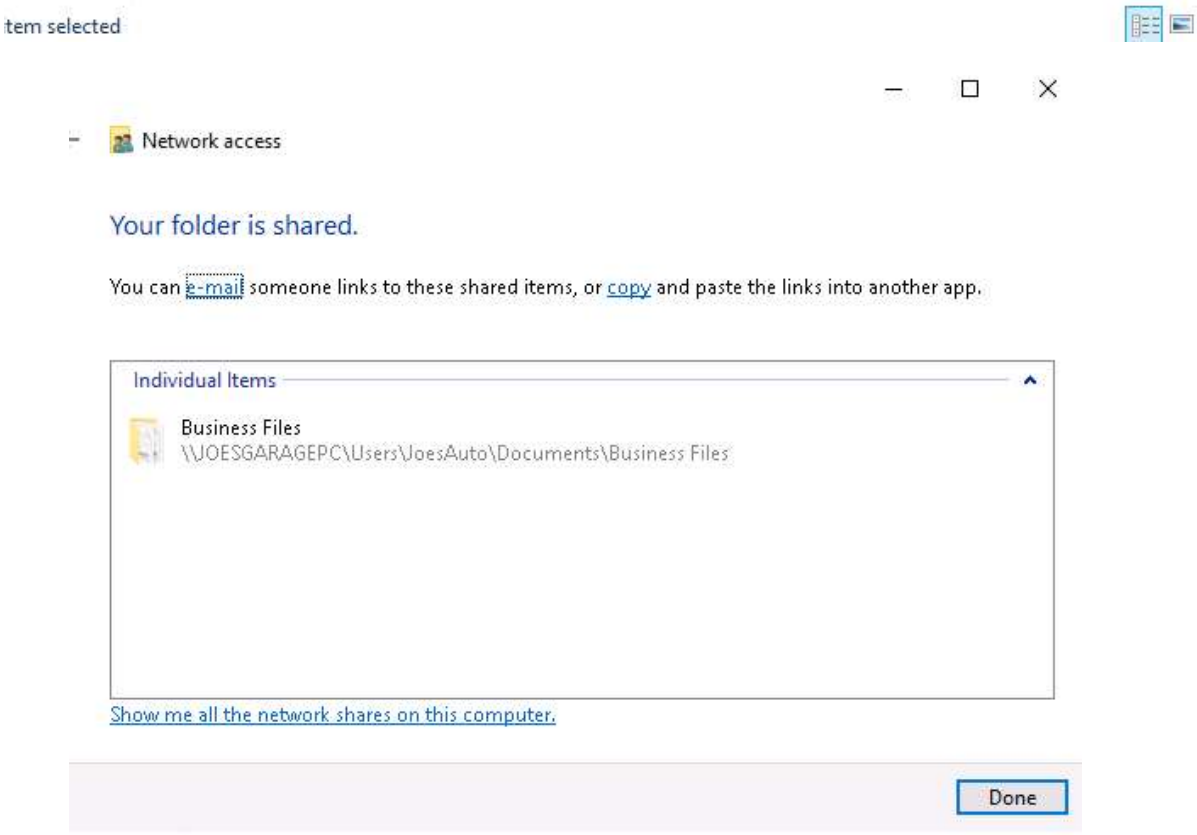
*CIS Control 3: Data protection*

## *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.*
   *Right click on the folder name > Give Access to > Specific people > Add name of Joe and Jane > Press Share*


Network access
Choose people to share with
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
Share
Cancel


Network access
Your folder is shared.
You can e-mail someone links to these shared items, or copy and paste the links into another app.
Individual Items
Business Files
\\JOESGARAGEPC\Users\JoesAuto\Documents\Business Files
Show me all the network shares on this computer.
Done

2. *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.