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: Filippo Calabrese

Date of completion: August 16, 2024

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.

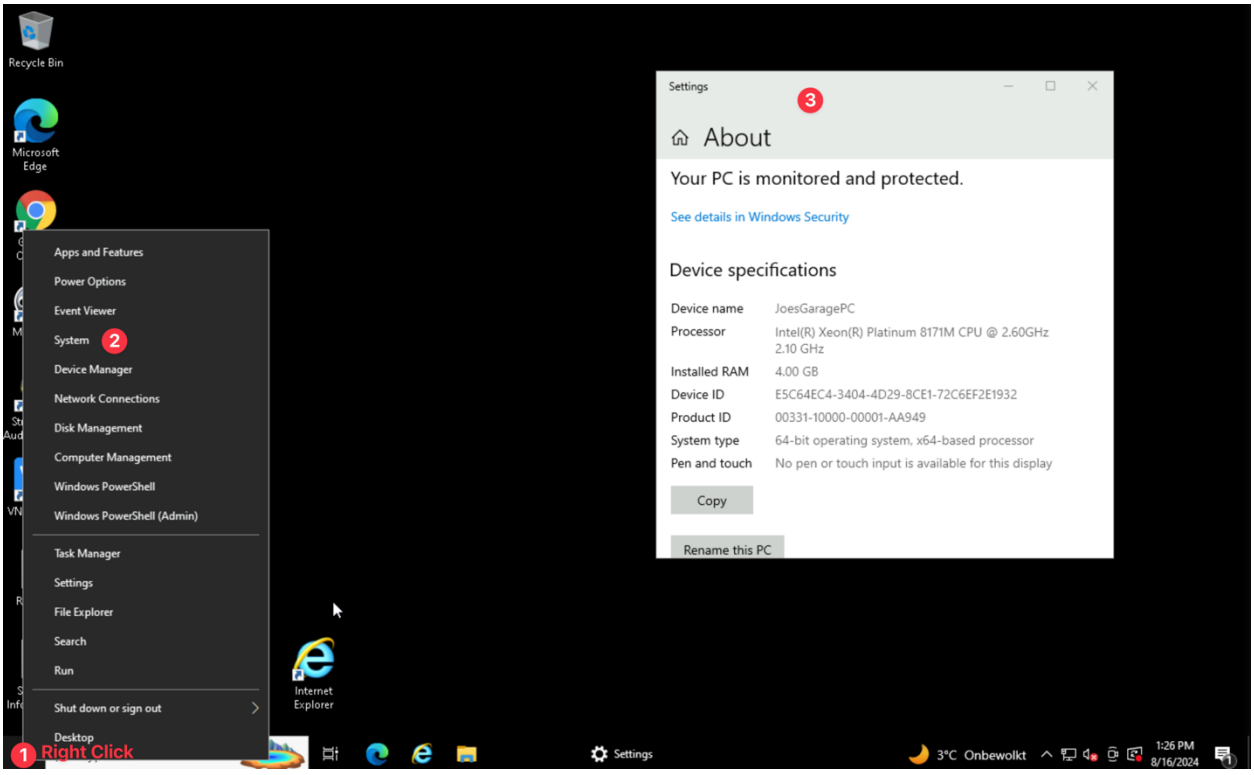
Complete each section below.

Hardware

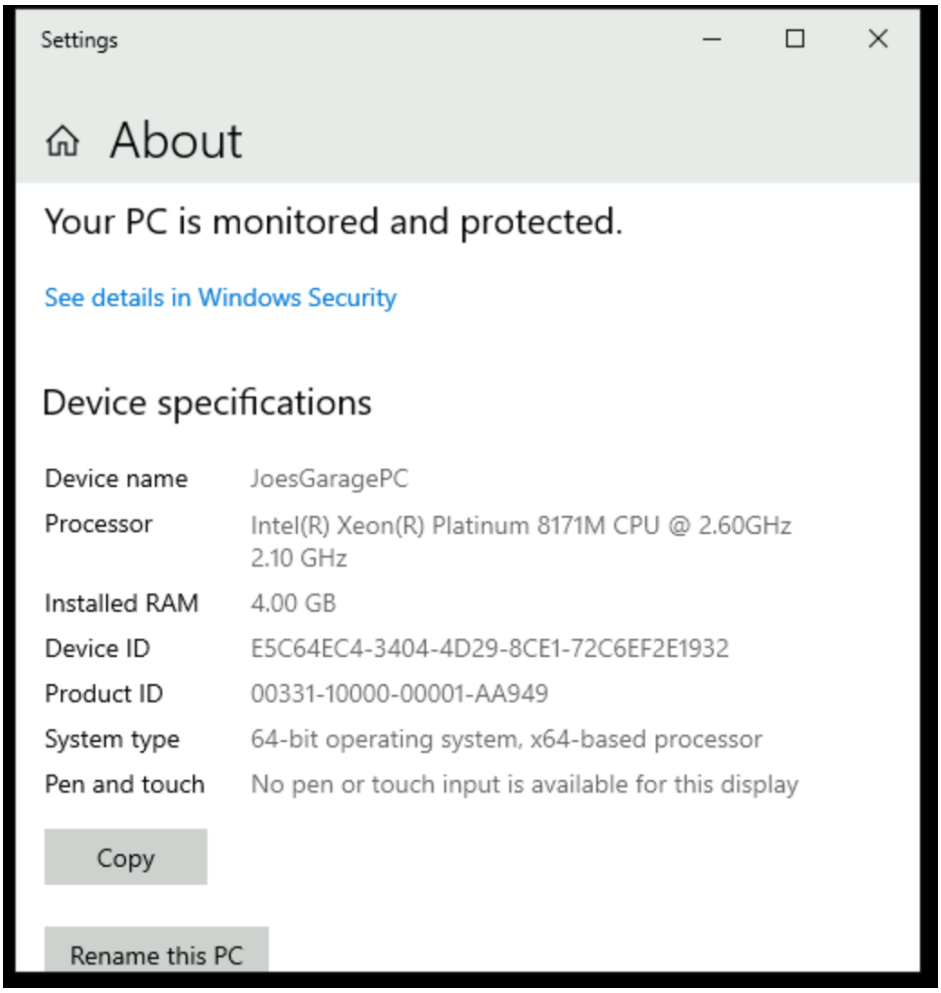
1. *Fill in the following table with system information for Joe's PC.*

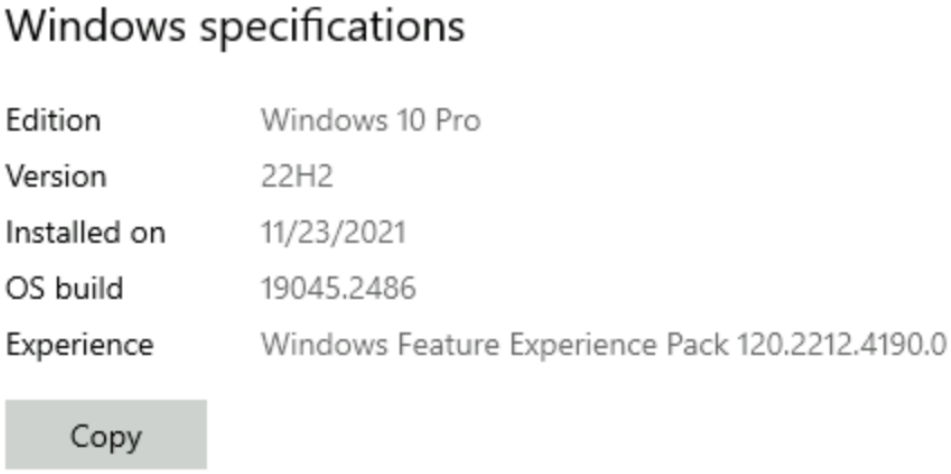
Device Name	JoesGaragePC
Processor	Intel(R) Xeon(R) Platinum 8171M CPU @2.60GHz 2.10GHz
Install RAM	4 GB
System Type	64-bit operating system, x64-based processor
Windows Edition	Windows 10 Pro
Version	22H2
Installed on	11/23/2021
OS build	19045.2486

2. *Explain how you found this information:*



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





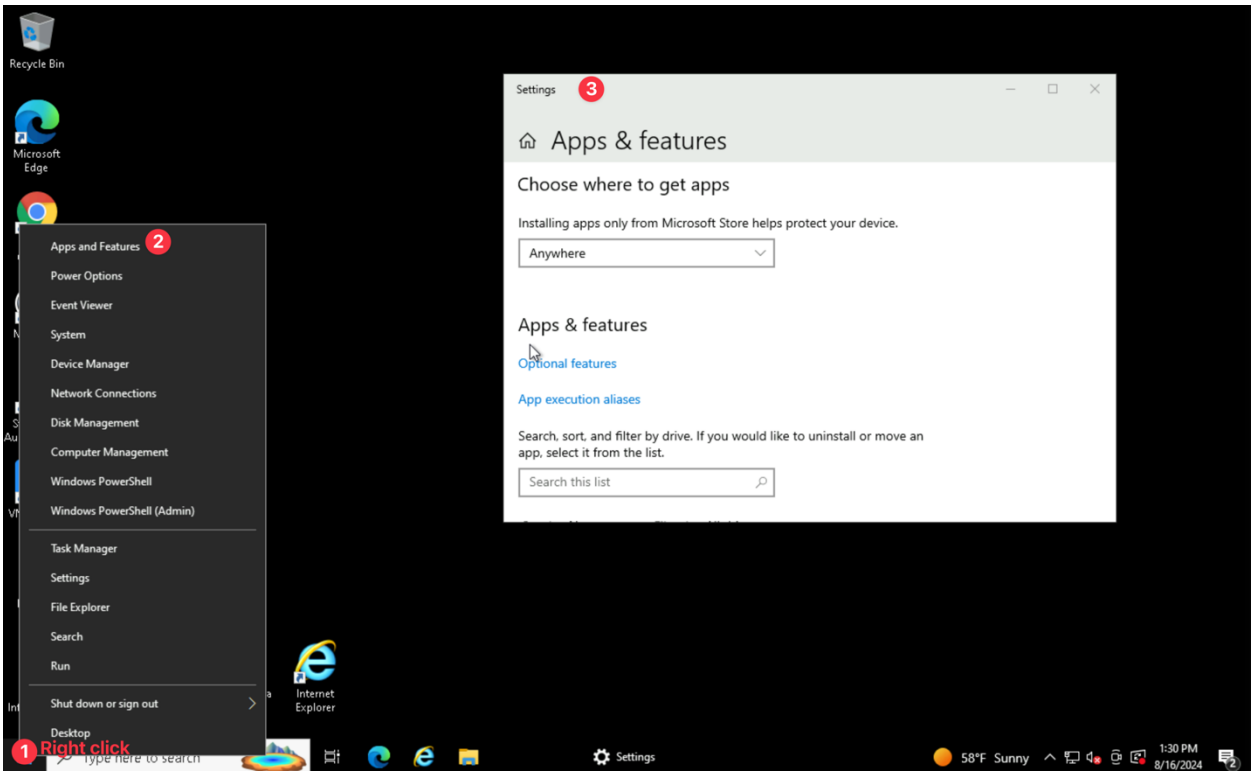
Software

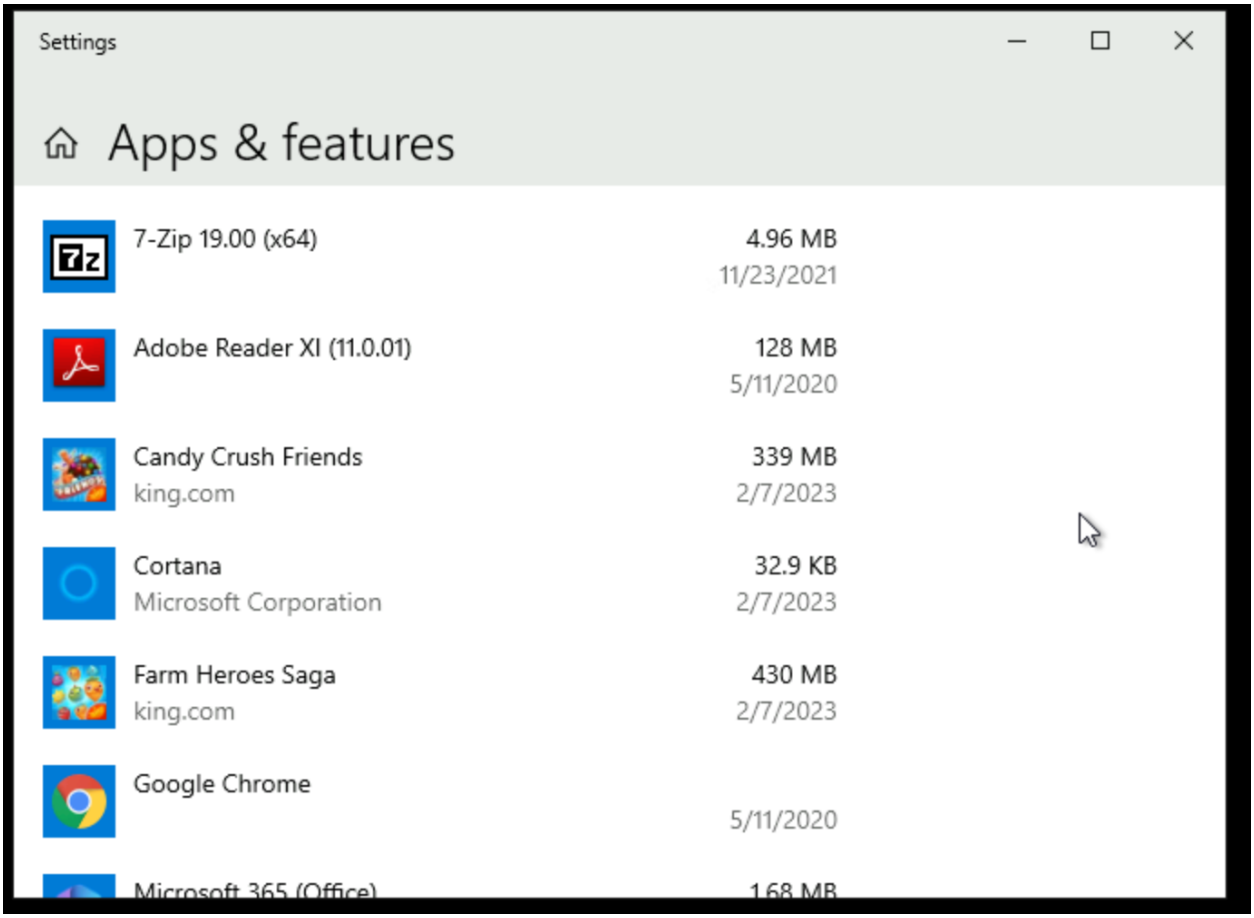
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- 7-Zip 19.00
- Adobe Reader XI (11.0.0.01)
- Candy Crush Friends
- Farm Heroes Saga
- Google Chrome

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





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

   CIS Control 2: Inventory and Control of Software Assets

Accounts

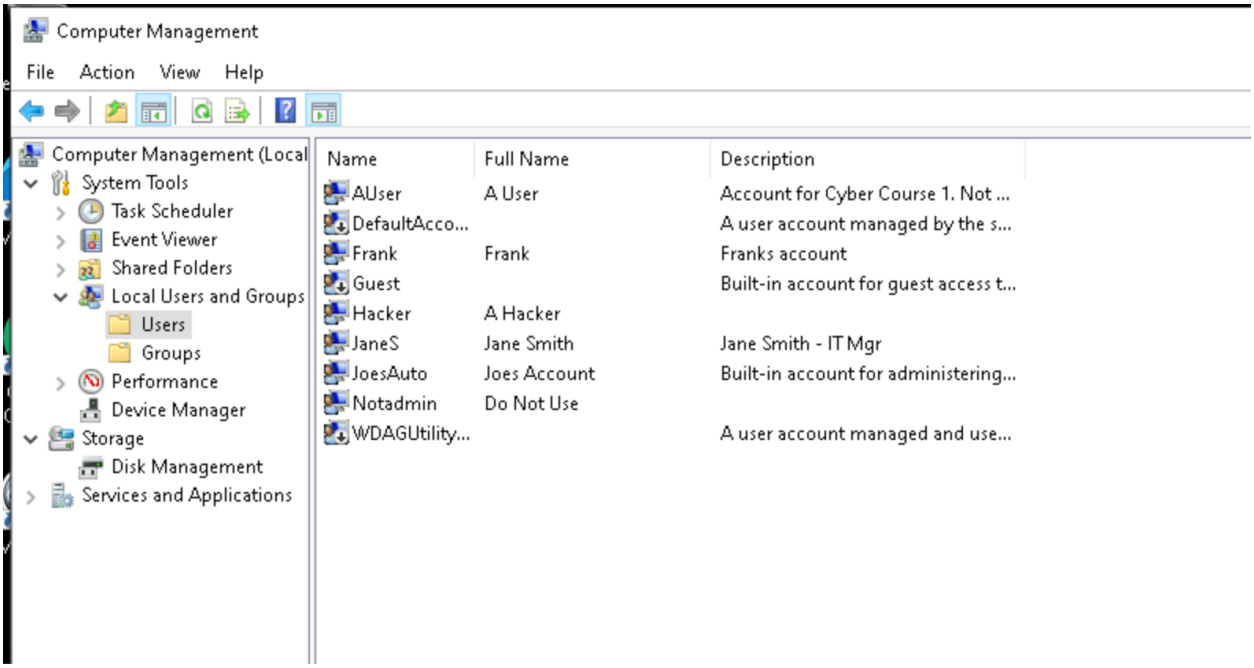
As part of your security assessment, you should know the user accounts that may access the PC.

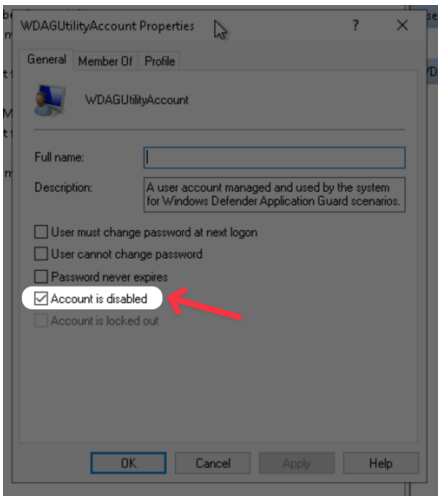
1. *List the names of the accounts found on Joe's PC and their access level.*

Account Name	**Full Name**	**Access Level**
AUser	A User	User
DefaultAccount		User | **Disabled**
Frank	Frank	User
Guest		User | **Disabled**
Hacker	A Hacker	Administrator

JaneS	Jane Smith	Administrator
JoesAuto	Joes Auto	Administrator
Notadmin	Do Not Use	User
WDAGUtilityAccount		User | **Disabled**

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

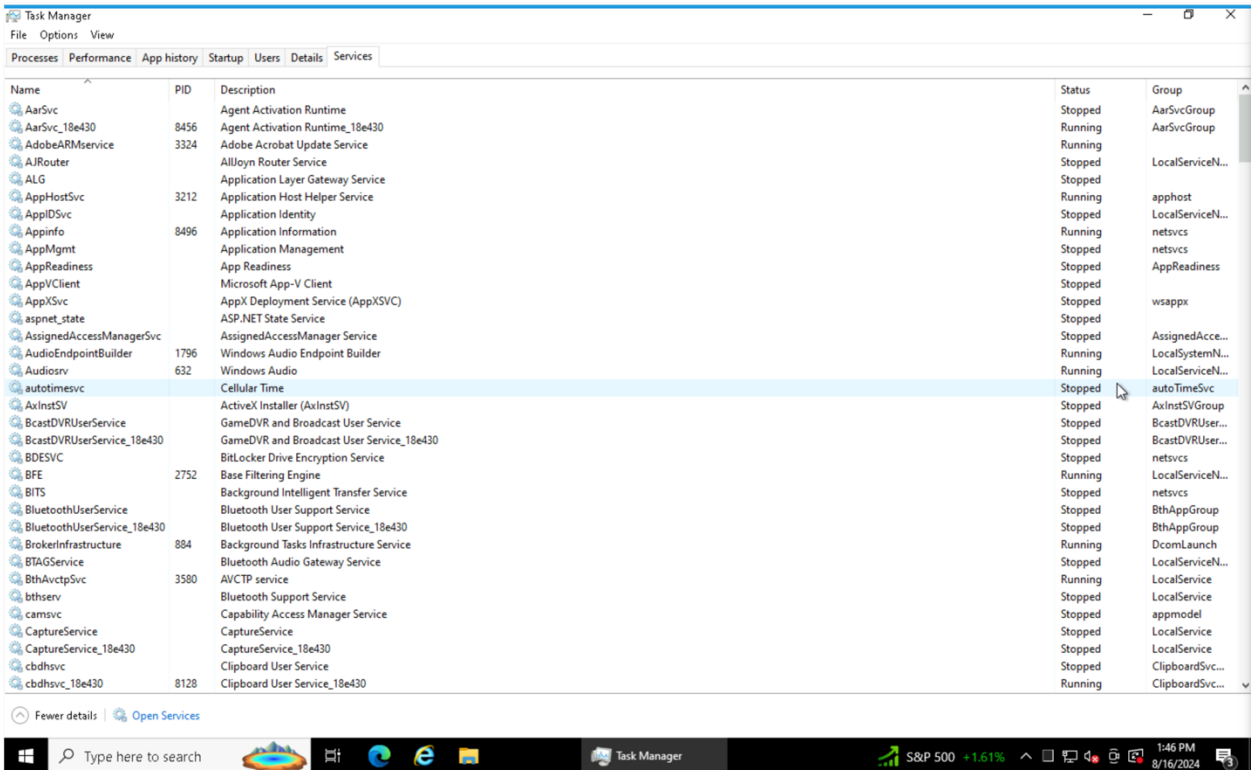




Services

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.*



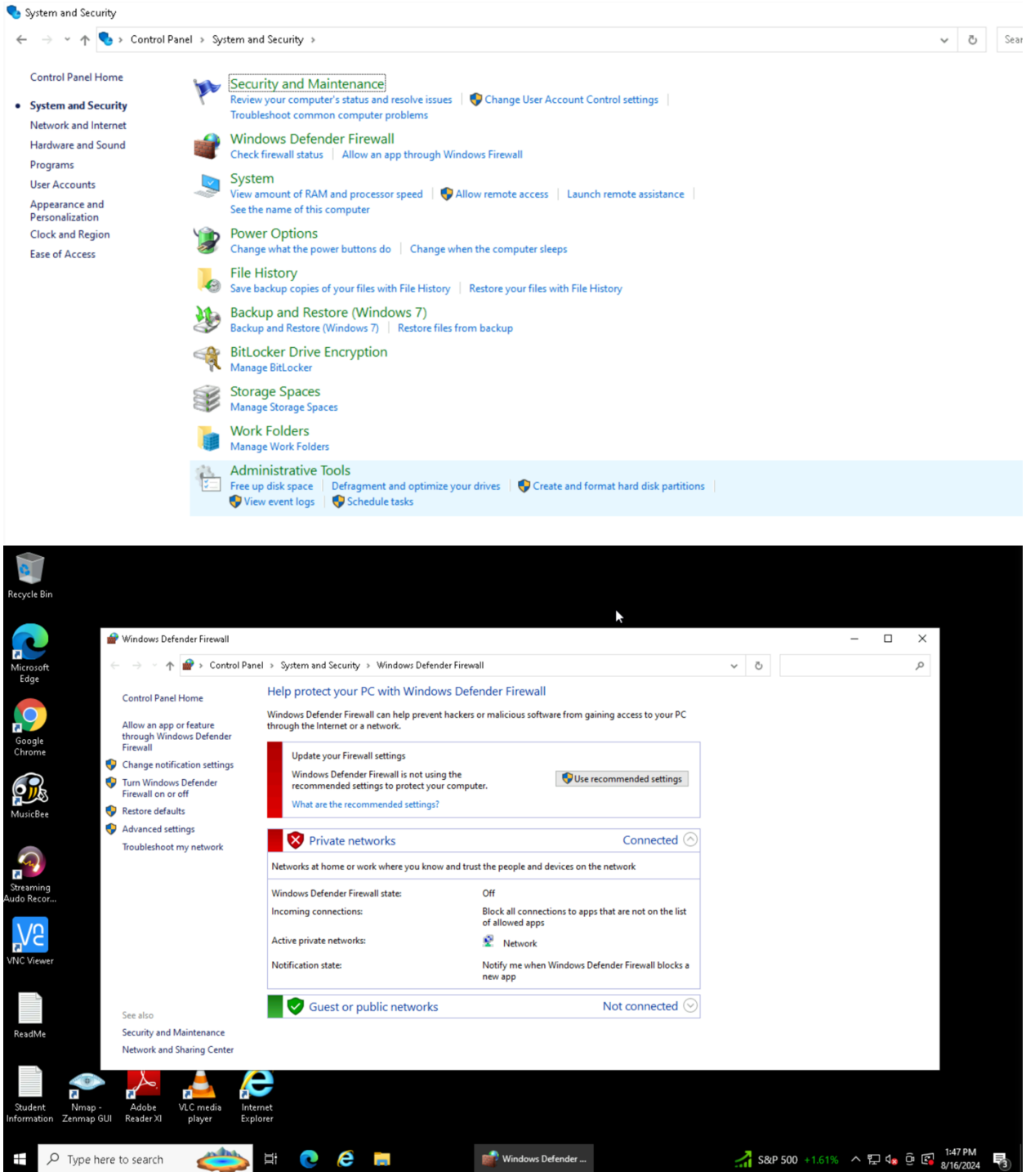
Security Services

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. **Remember 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 for 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:*

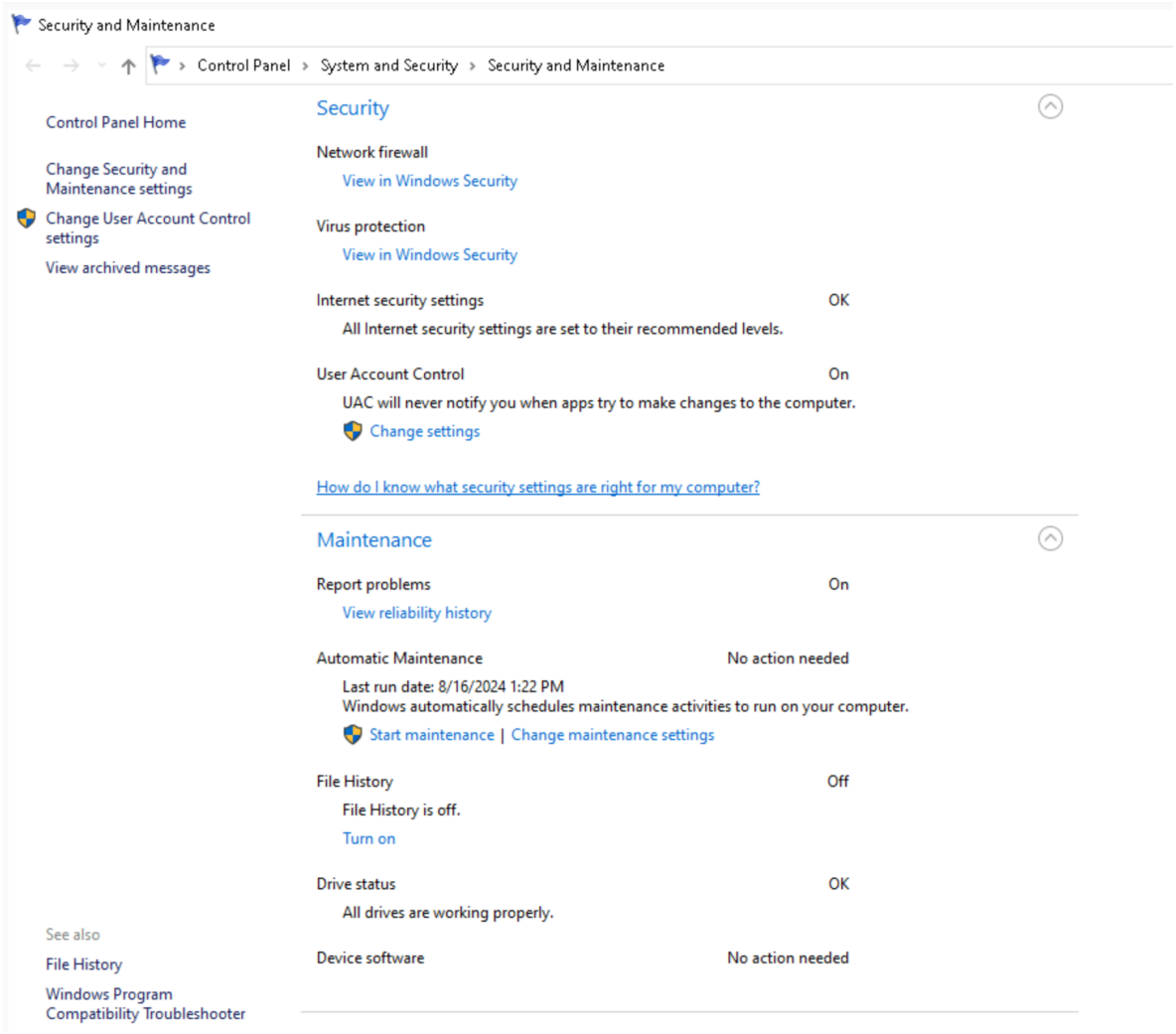
   N:B: As the question is formulated, it is not clear the screenshot you're looking for. I will assume you're asking for "System and Security" interface main screen OR "Windows Defender" main screen.

   Gonna attach both of them 😊

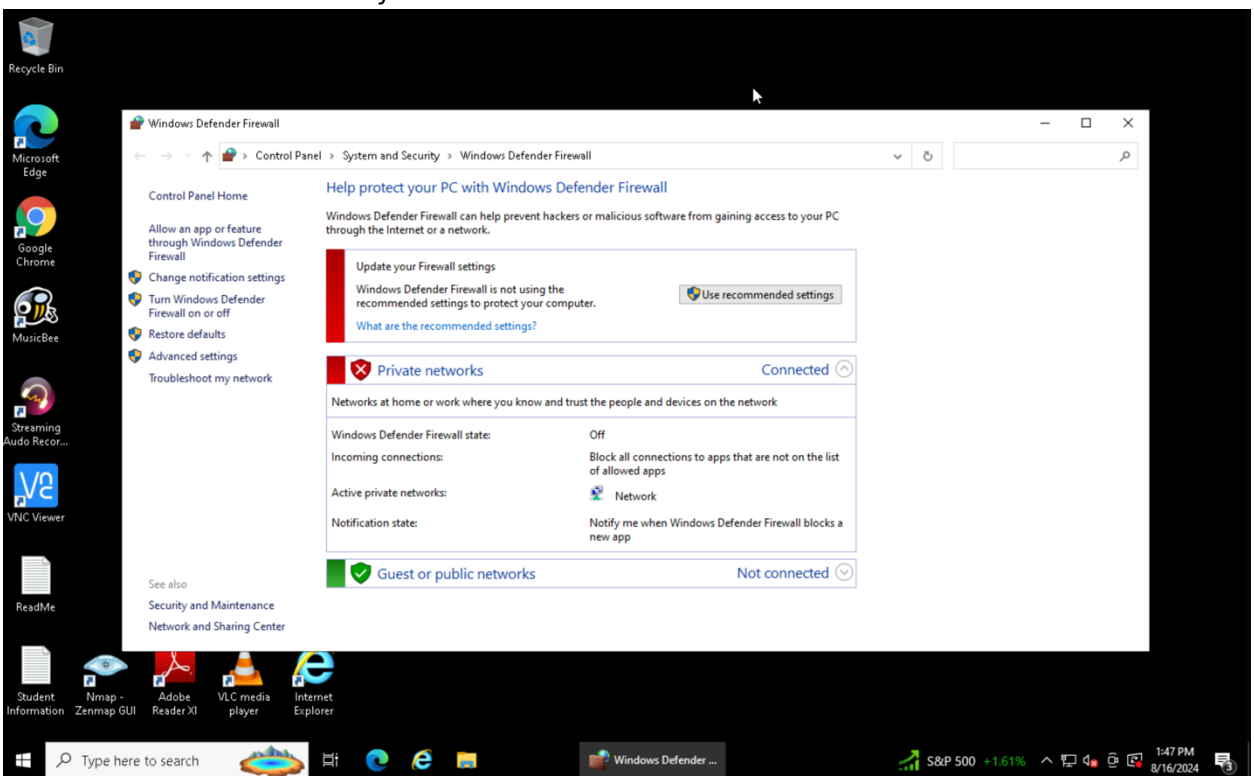


2. *The Windows 10 Security settings are also found from the* ***Control Panel > System and Security > Security and Maintenance****. Start by viewing* ***"Review your computer's status and resolve***

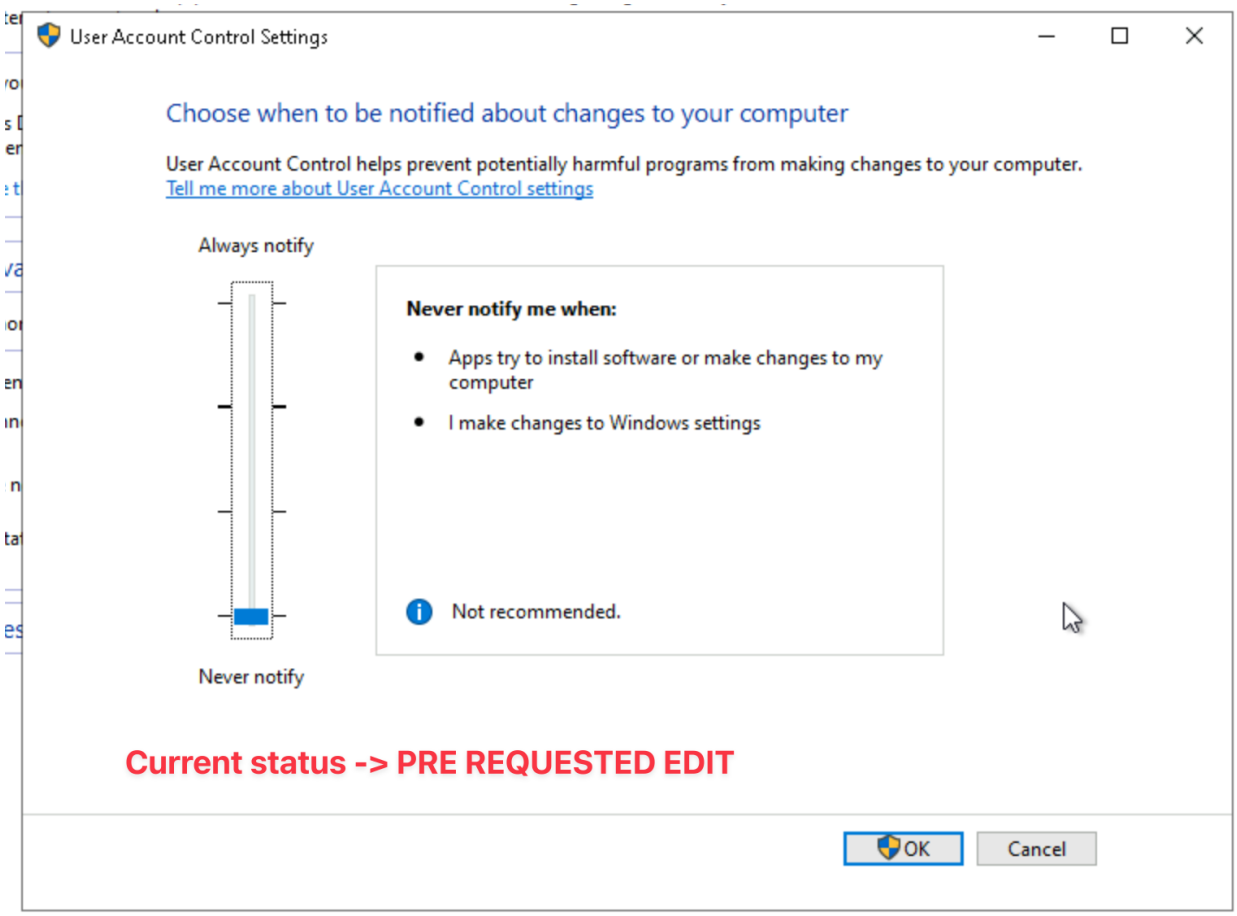
issues." *Provide a screenshot of this below:*



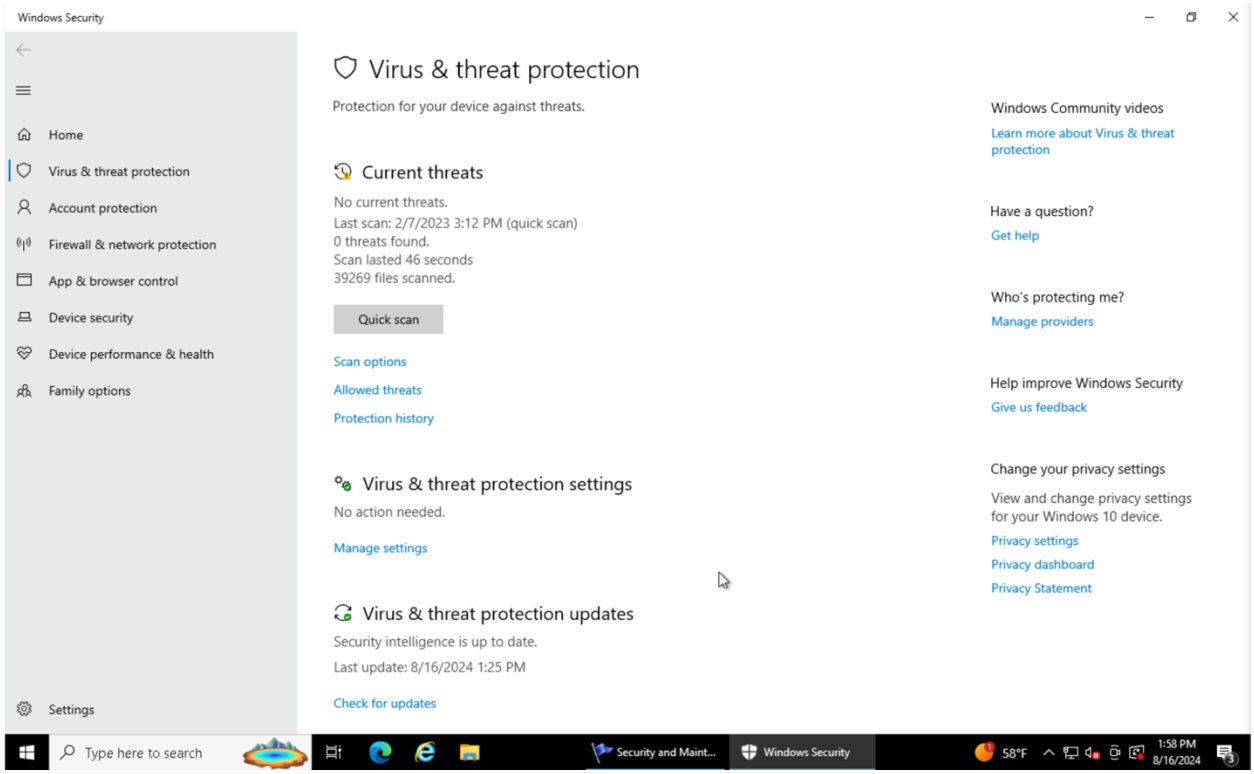
3. *From the **Control Panel**, go to **System and Security**. In that window, select **Windows Defender Firewall**. Provide a screenshot of it here:*



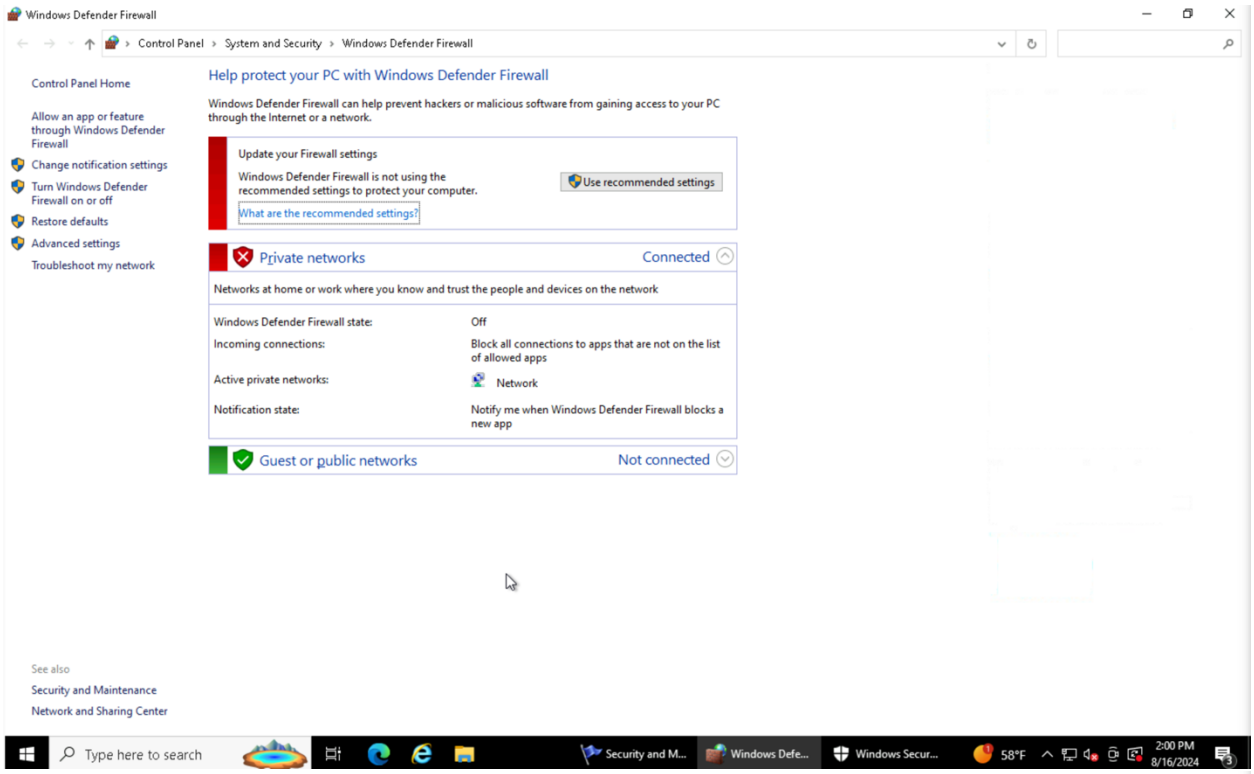
4. *PC users should be notified whenever there is a security or maintenance message. In the Security & Maintenance window, click on Change Security and Maintenance settings and take a screenshot. Paste it here:*

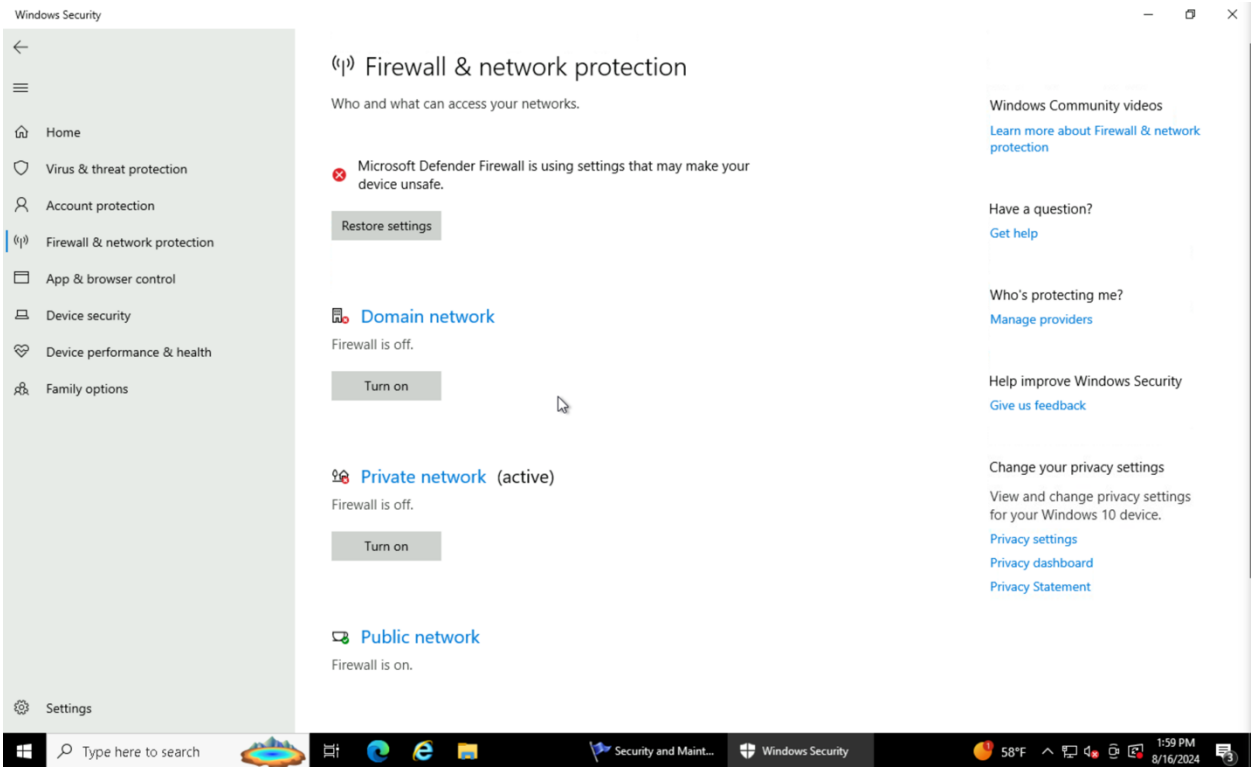

User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Never notify
Never notify me when:
Apps try to install software or make changes to my computer
I make changes to Windows settings
Not recommended.
Current status -> PRE REQUESTED EDIT
OK
Cancel

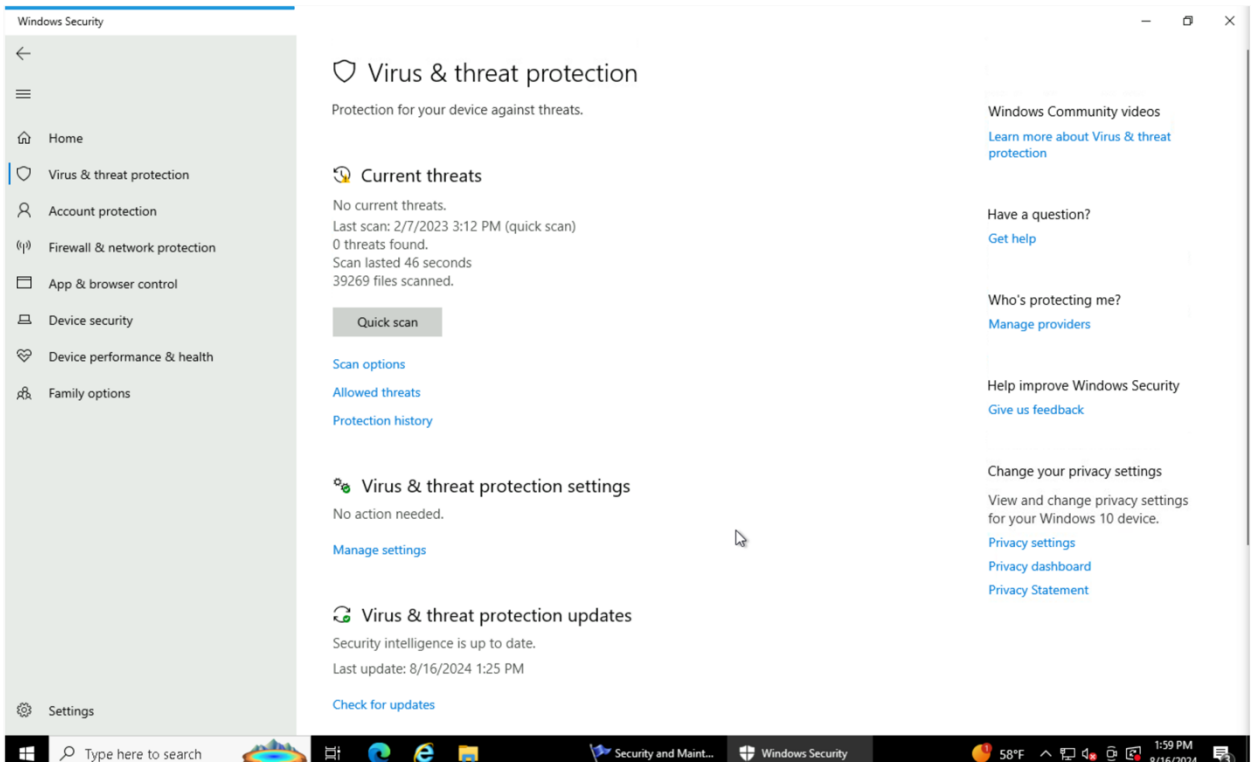
5. *From Control Panel > System and Security > Security and Maintenance>Security>Virus protection. Provide a screenshot for **Virus and threat protection**, here:*

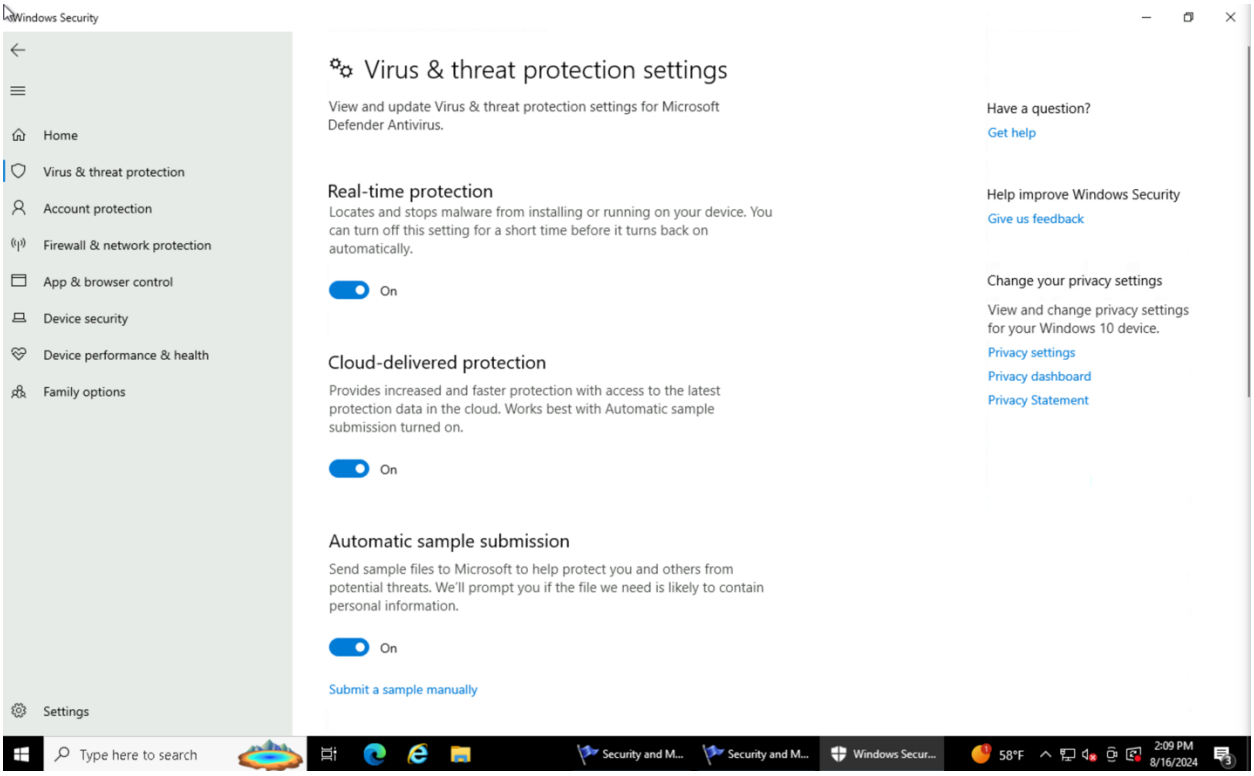


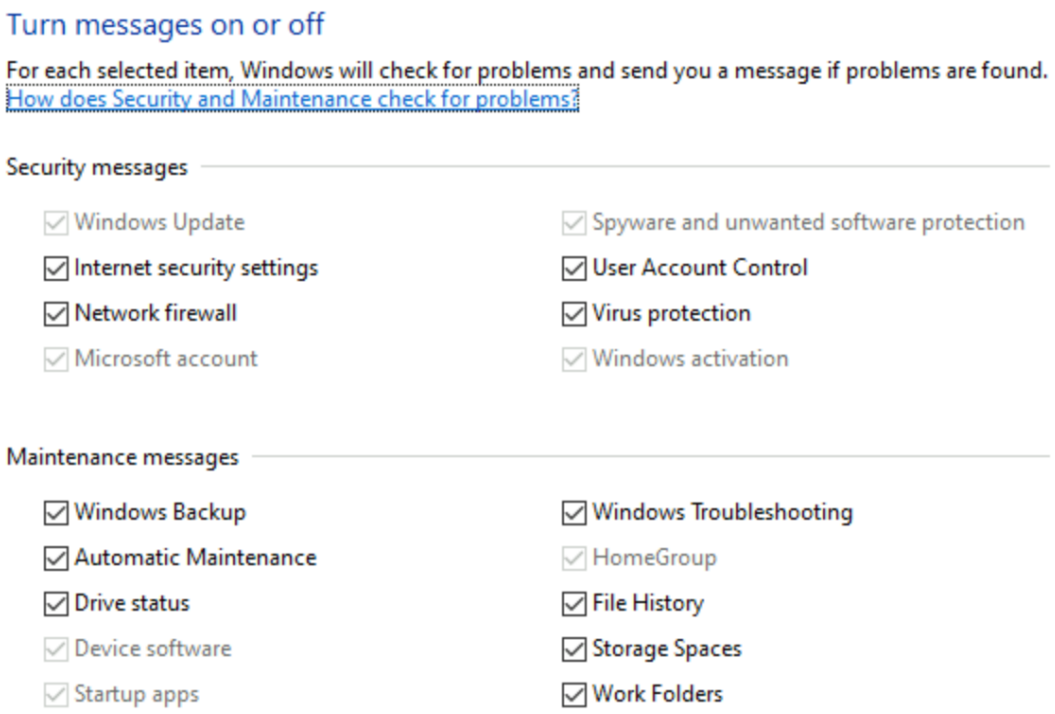
6. *Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).*


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.
Use recommended settings
What are the 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
See also
Security and Maintenance
Network and Sharing Center
Type here to search
Security and M...
Windows Defe...
Windows Secur...
58°F
2:00 PM
8/16/2024


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Firewall & network protection
Who and what can access your networks.
Microsoft Defender Firewall is using settings that may make your device unsafe.
Restore settings
Domain network
Firewall is off.
Turn on
Private network (active)
Firewall is off.
Turn on
Public network
Firewall is on.
Windows Community videos
Learn more about Firewall & network protection
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Type here to search
Security and Maint...
Windows Security
58°F
1:59 PM
8/16/2024


Windows Security
Virus & threat protection
Protection for your device against threats.
Current threats
No current threats.
Last scan: 2/7/2023 3:12 PM (quick scan)
0 threats found.
Scan lasted 46 seconds
39269 files scanned.
Quick scan
Scan options
Allowed threats
Protection history
Virus & threat protection settings
No action needed.
Manage settings
Virus & threat protection updates
Security intelligence is up to date.
Last update: 8/16/2024 1:25 PM
Check for updates
Windows Community videos
Learn more about Virus & threat protection
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Type here to search
Security and Maint...
Windows Security
58°F
1:59 PM
8/16/2024


Windows Security
Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
On
Submit a sample manually
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Type here to search
Security and M...
Security and M...
Windows Secur...
58°F
2:09 PM
8/16/2024



Security Feature	**Status**
Firewall product and status – Private network	Windows Defender - Off
Firewall product and status – Public network	Windows Defender - On
Virus protection product and status	No current threats. No action required. Real time protection is On
Network firewall messages	Recommended settings are not enabled
Virus protection messages	No messages
Internet security	Enabled
User Account Control Setting	Never Notify

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 is disabled for local networks** -> PC would be .vulnerable to attacks over local network
- **Multiple administrator accounts** -> System vulnerability increases. Zero Trust principle fails
- **Useless app installed** -> Increases the attackable terrain on the computer. Increased possibility of malware presence in applications.
- **UCL notification are disabled** -> It is not possible to predict a rapid response to unwanted changes or possible attacks based on user behavior.

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?*
   [Tip: You might find it helpful to take another look at the lessons in the beginning of the course]

   *Joe should use the **Center for Internet Security (CIS) Controls** as the industry standard for setting security policies at his organization.*

   1. ***Comprehensive Coverage**: The CIS Controls provide a comprehensive, prioritized set of actions designed to help organizations defend against common cyber threats. They cover critical areas such as inventory management, secure configurations, access controls, and continuous monitoring.*
   2. ***Widely Recognized**: The CIS Controls are widely recognized and adopted across industries as a best practice framework. They are used by organizations of all sizes to enhance security posture and comply with regulatory requirements.*
   3. ***Regularly Updated**: The CIS Controls are regularly updated to address new and emerging threats, ensuring that Joe's organization remains protected against the latest security challenges.*
   4. ***Actionable and Practical**: The CIS Controls offer clear, actionable guidance that is practical for implementation, making it easier for Joe to enforce and maintain strong security policies.*

***2.** What industry baseline do you recommend to Joe?*

[Hint: Look in the documents folder of the Windows 10 machine]

I recommend that Joe use the CIS Benchmarks as the industry baseline for his organization's security settings.

Justification:

1. ***Standardized Security Settings: CIS Benchmarks provide detailed, consensus-driven security configuration guides. They offer a standardized baseline that helps secure various systems and applications, ensuring they are configured according to best practices.***
2. ***Tailored for Specific Environments: CIS Benchmarks are available for a wide range of platforms, including Windows, Linux, macOS, network devices, and cloud environments. This allows Joe to apply tailored security configurations specific to his organization's environment.***

3. Compliance and Auditing: Adhering to CIS Benchmarks can assist in meeting regulatory compliance requirements. Many auditors and regulatory bodies recognize CIS Benchmarks as a strong foundation for security compliance.

4. Community-Driven: The CIS Benchmarks are developed by a global community of cybersecurity professionals, ensuring they are continuously updated and improved to address the latest threats and vulnerabilities.

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.

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

Accessing the Security and Maintenance aligns with several CIS Controls. Specifically, this action supports CIS Control 5 (ensuring secure configurations for devices), CIS Control 3 (continuous vulnerability management), CIS Control 4 (controlled use of administrative privileges), CIS Control 16 (application software security), and CIS Control 6 (monitoring and analyzing audit logs).

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

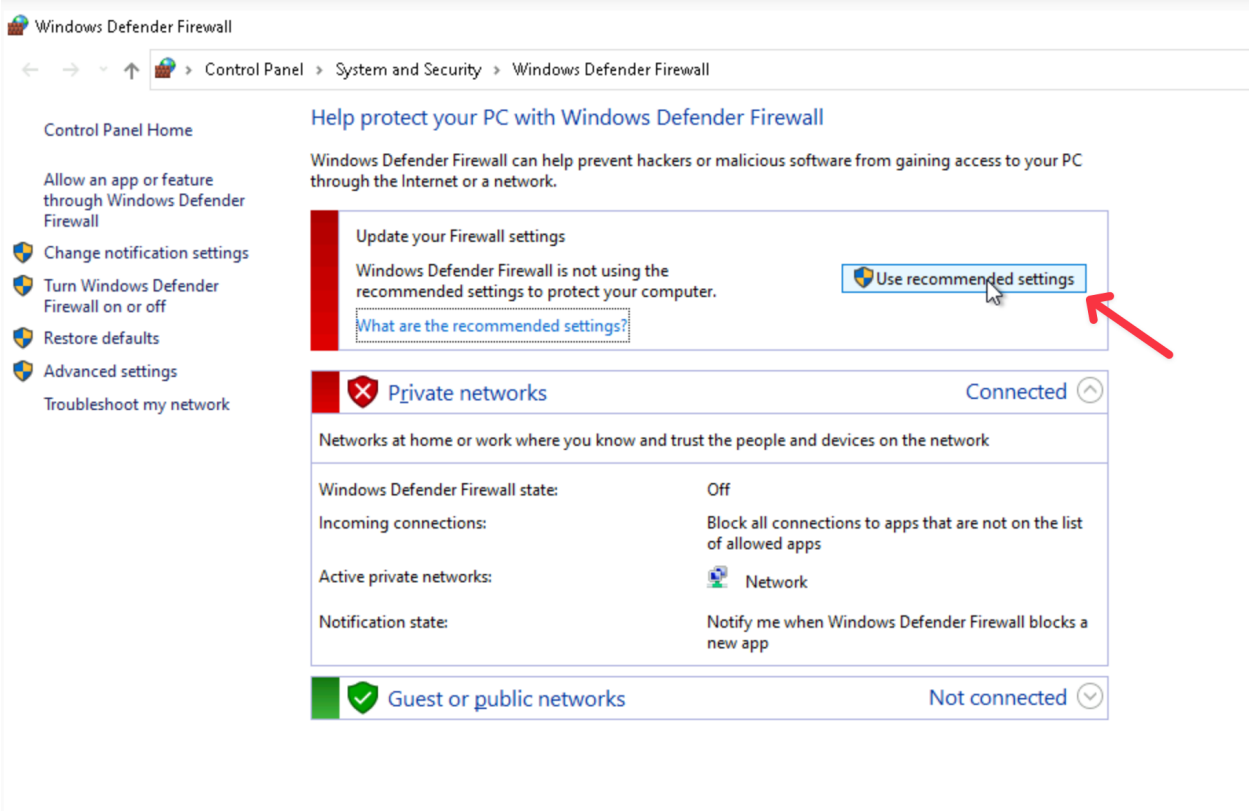
Firewall

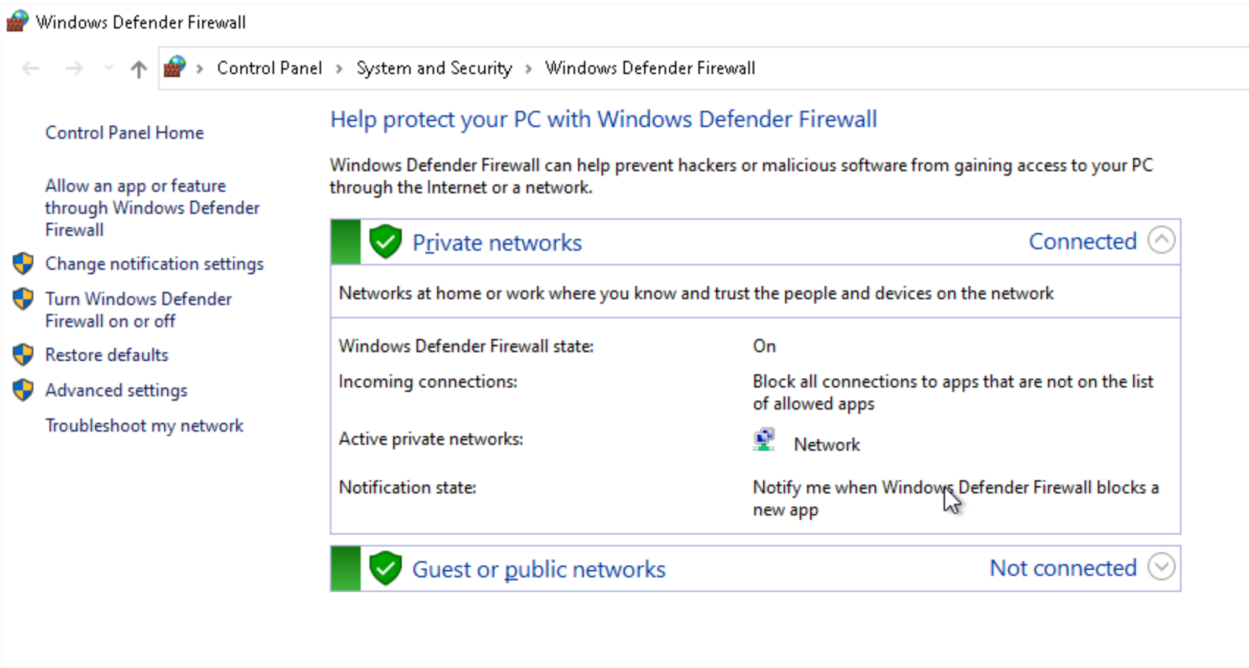
You need to ensure the Windows Firewall is enabled for all network access. You can follow the same steps you used above to check the firewall status

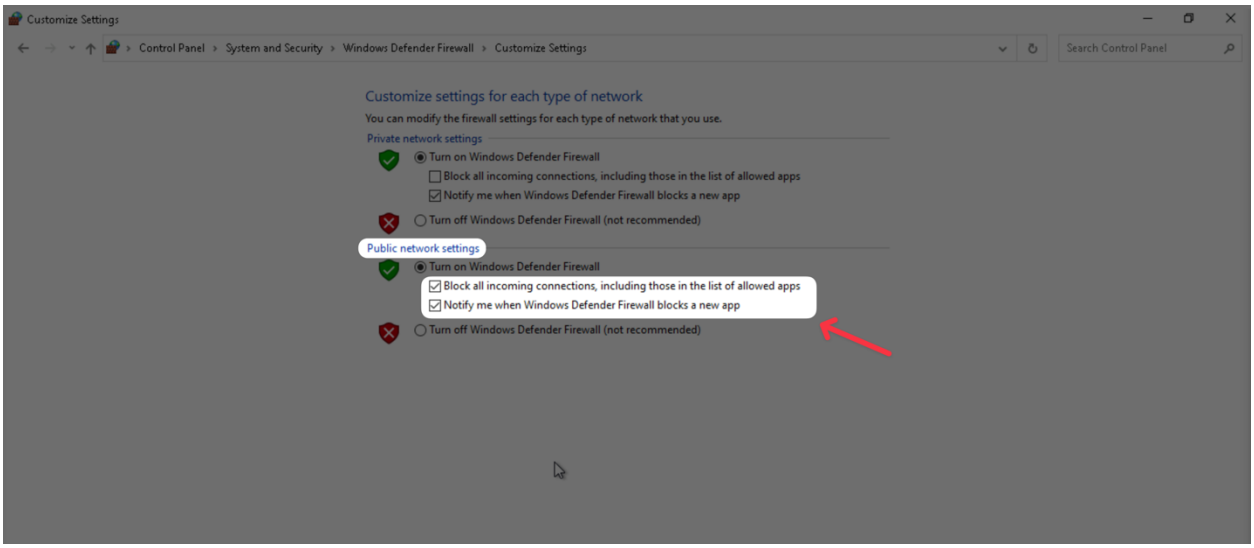
1. *Explain the process you take to do this.*
2. *Include screenshots showing the firewall is turned on.*
3. ***What protection does this provide?***

From the Windows Defender menu I enabled the recommended settings for managing

the firewall on public and private networks. In this way we enabled the firewall for both networks, adding a layer of defense for the PC. I also blocked incoming connections from public networks, in order to further increase the defense in case you use less secure connections, such as at a coffee shop or an airport.







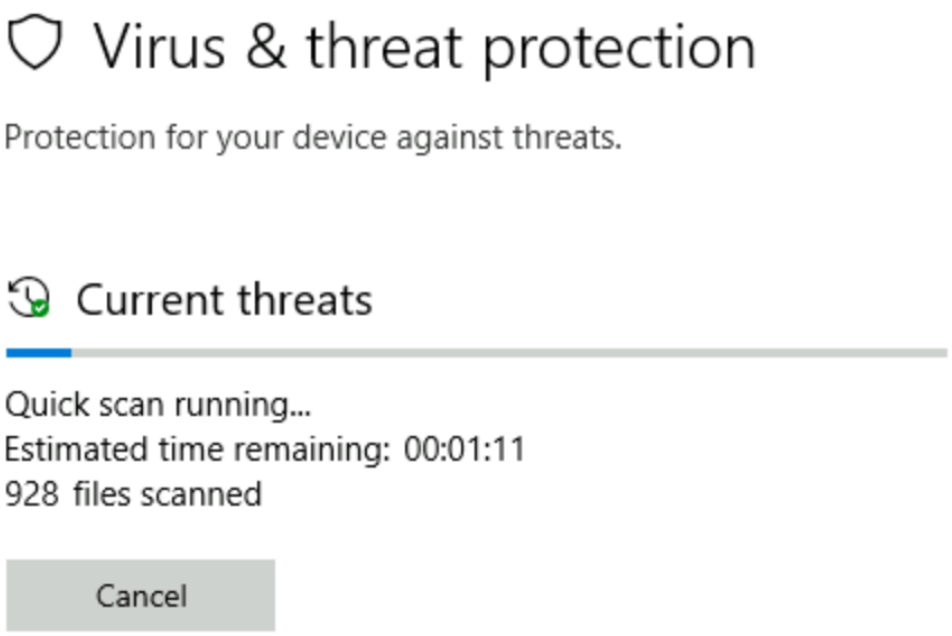
Virus & Threat Protection

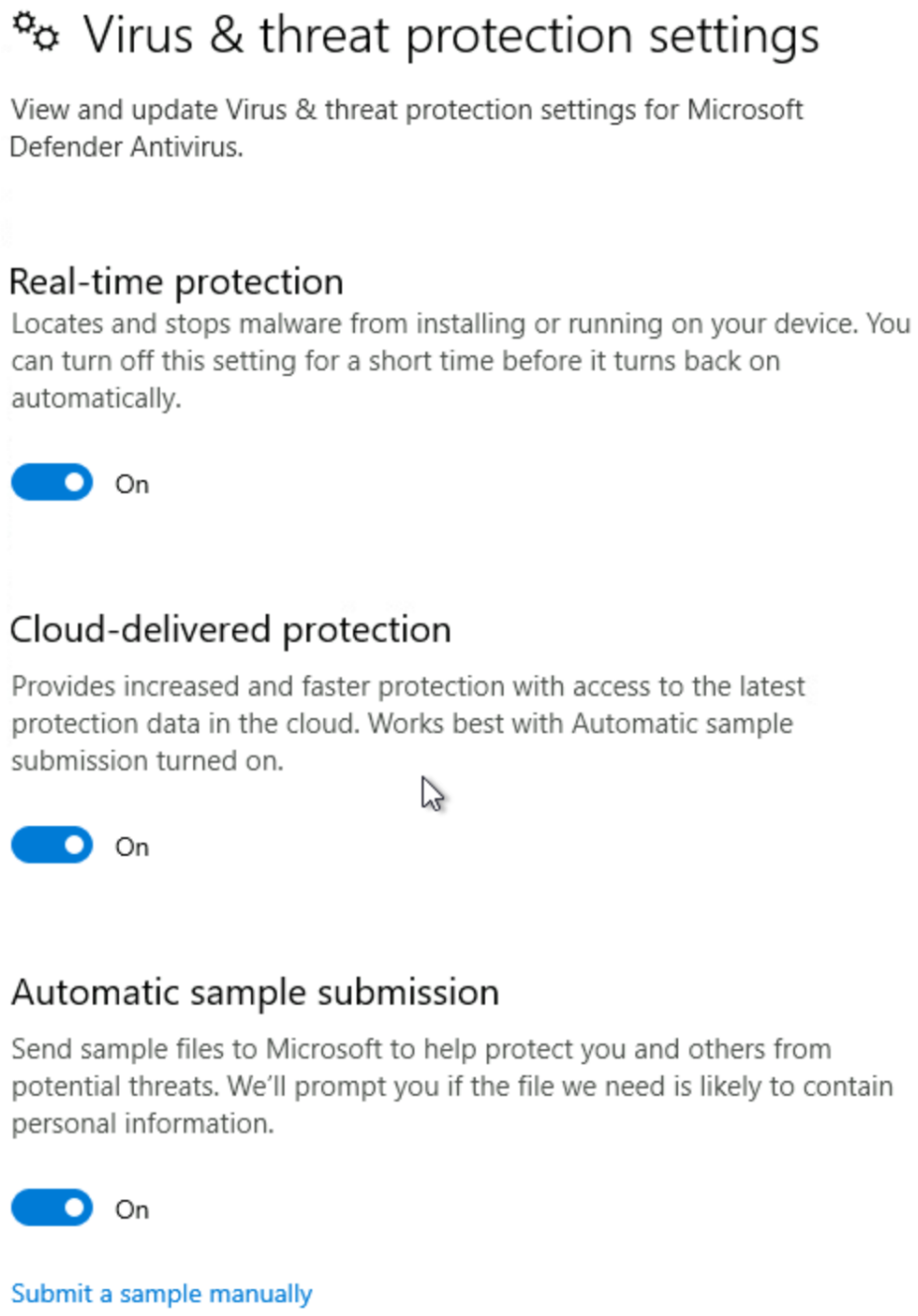
You need to ensure the Windows Defender anti-virus is enabled to always protect against current threats. It should be set to automatically update and continually scan the PC for malicious software. Note: Ignore any alerts about setting up OneDrive.

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

   From the Windows Security panel I moved to the "Virus & Threat protection" item. I checked that the optimal settings had already been set. For added security I also started a file scan.

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


Virus & threat protection
Protection for your device against threats.
Current threats
Quick scan running...
Estimated time remaining: 00:01:11
928 files scanned
Cancel

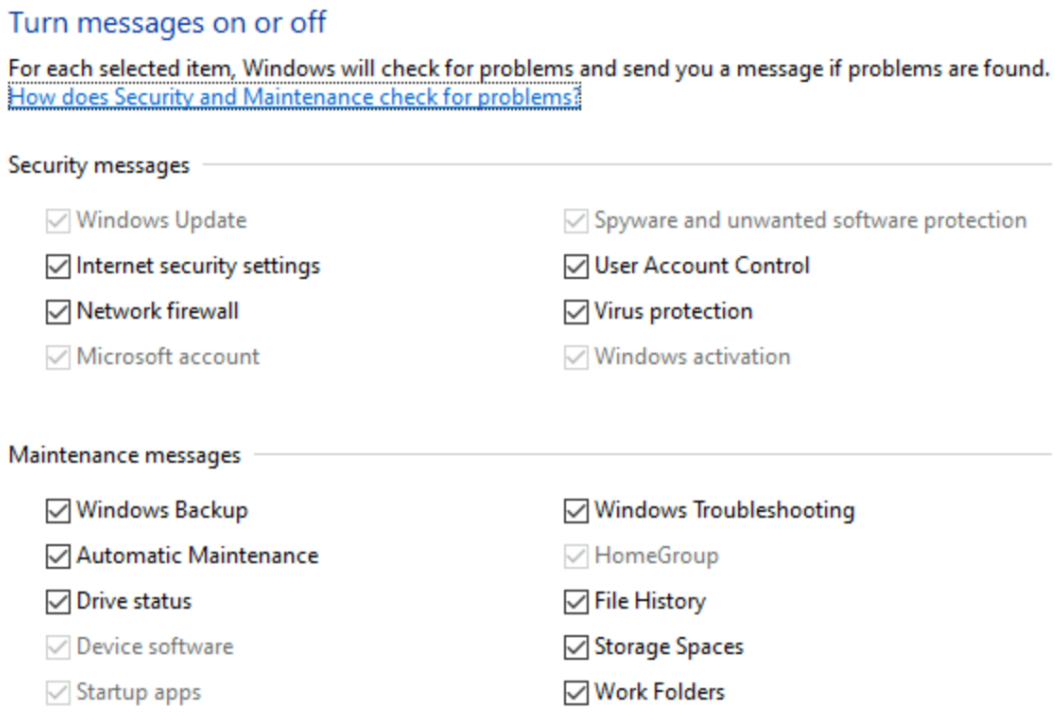


Once you determine that virus & threat protection is on and updated, you need to turn on messages about the Network firewall and Virus protection. Refer to the instructions above for viewing the settings within Security and Maintenance. Review recent messages and resolve problems.

1. *Turn on the Network firewall and Virus protection messages using Change Security and Maintenance Settings.*

Such notifications were already anabled.

2. *Show a screenshot here of them enabled.*



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

- ***Unauthorized Network Access: Enabling the Network firewall ensures that the system monitors and controls incoming and outgoing network traffic based on security rules. This helps prevent unauthorized access to the network and blocks potentially harmful traffic, reducing the risk of network-based attacks.***
- ***Malware and Virus Infections: By turning on Virus protection messages, you ensure that the system regularly monitors for malware and alerts you to any issues. This proactive approach helps to quickly identify and remove viruses or other malicious software, reducing the risk of infections that could compromise system integrity or steal sensitive data.***

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

1. ***CIS Control 4: Controlled Use of Administrative Privileges***

   Ensuring that alerts for critical security functions like the Network firewall and Virus protection are enabled helps maintain control over security configurations, reducing the risk that unauthorized changes could go unnoticed.
2. ***CIS Control 7: Continuous Vulnerability Management***

By enabling messages about Virus protection, you ensure that the system continuously monitors for and alerts you to potential vulnerabilities related to malware. This supports ongoing efforts to identify and mitigate vulnerabilities.

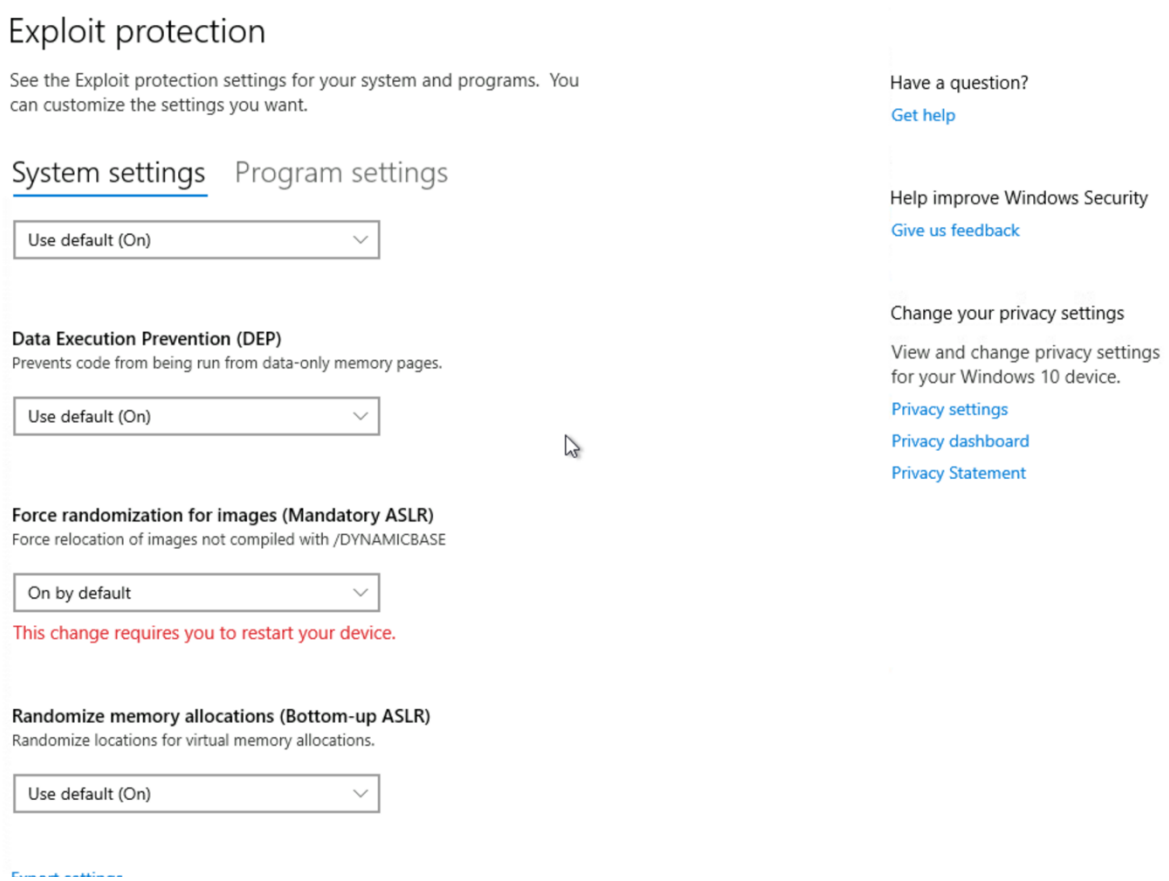
3. ***CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services***

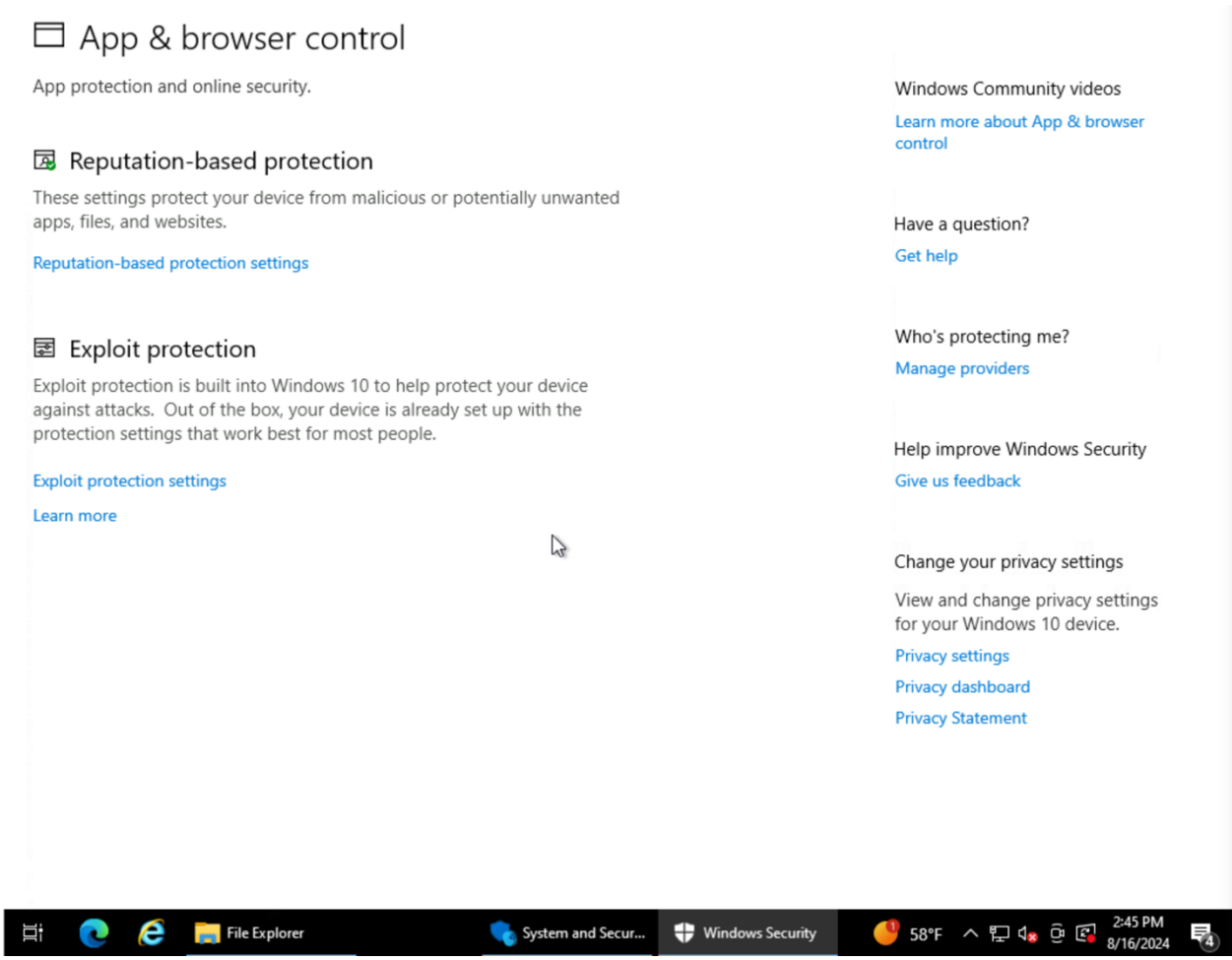
   Enabling the Network firewall ensures that only necessary network ports, protocols, and services are allowed, thereby limiting the attack surface and controlling network traffic as recommended by this control.

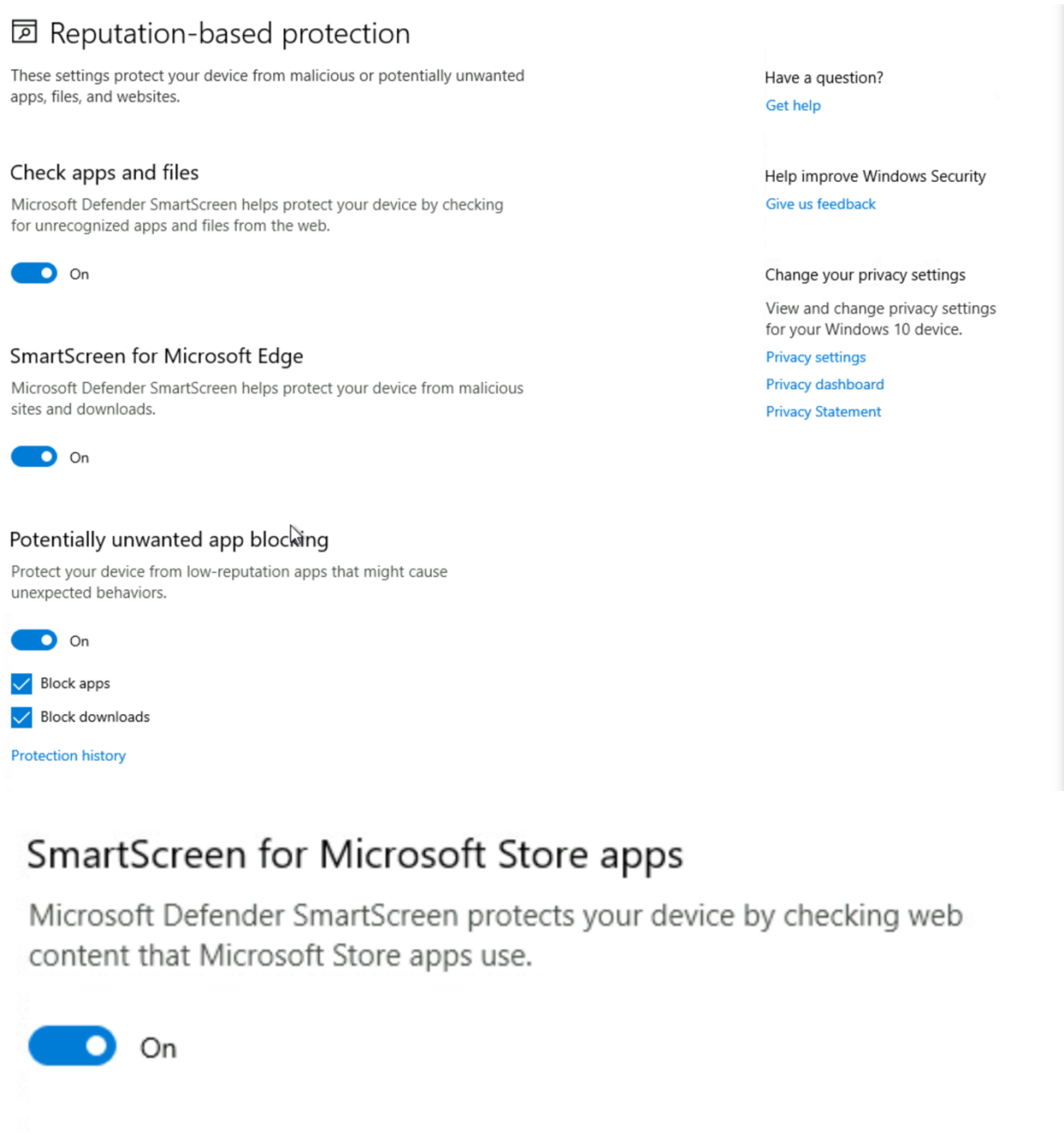
App & Browser Control

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.*




App & browser control
App protection and online security.
Reputation-based protection
These settings protect your device from malicious or potentially unwanted apps, files, and websites.
Reputation-based protection settings
Exploit protection
Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.
Exploit protection settings
Learn more
Windows Community videos
Learn more about App & browser control
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
File Explorer
System and Secur...
Windows Security
58°F
2:45 PM
8/16/2024



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?*

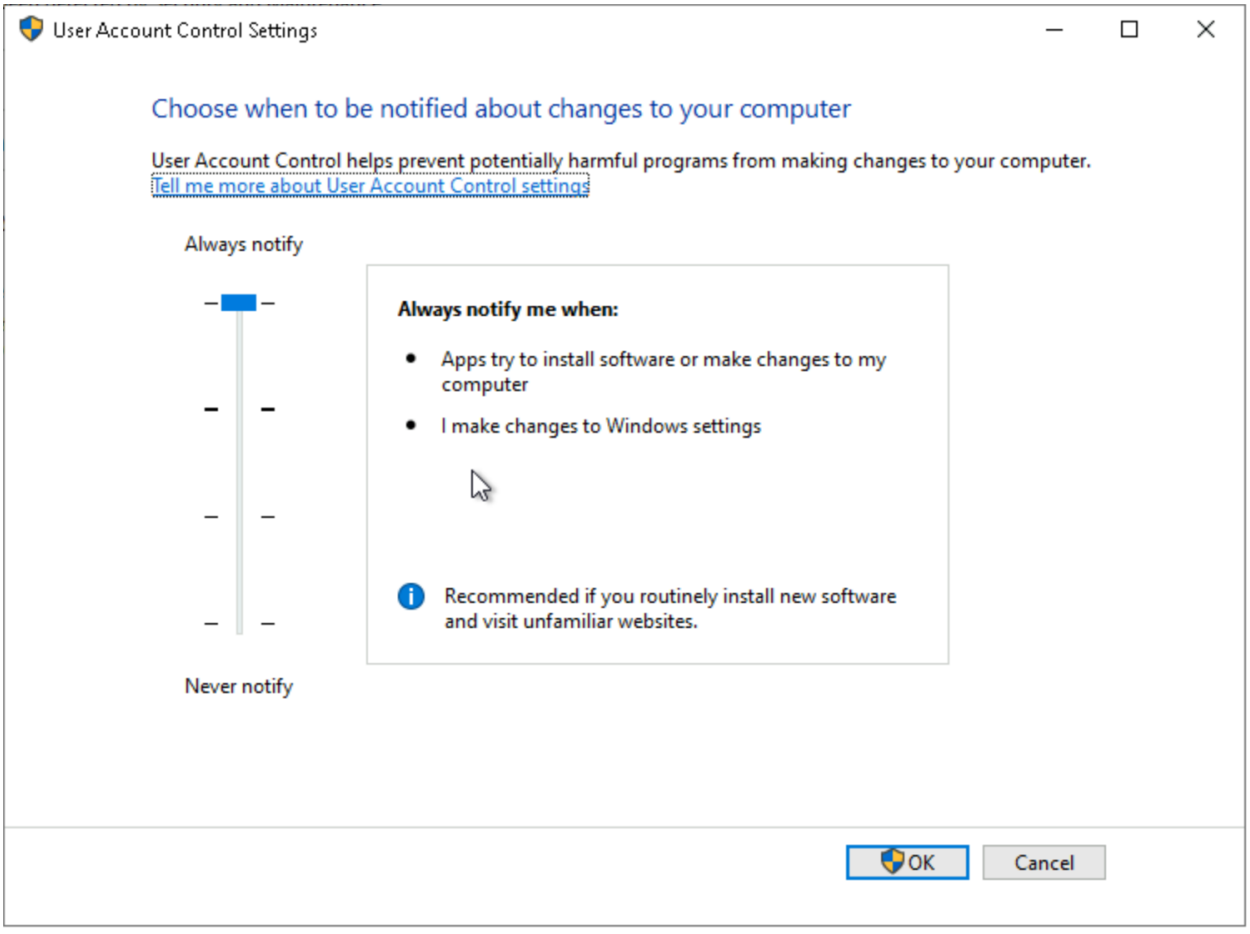
This is available from the above security settings, Control Panel→ User Accounts → Change User Account Control settings.

Current status was Never Notify

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

Configuring the User Account Control (UAC) settings to notify Joe whenever apps try to make changes to his computer aligns with CIS Control 8: Audit Log Management. This control focuses on the collection, management, and review of audit logs to detect suspicious activity and ensure accountability.

By enabling UAC notifications, Joe ensures that any attempt by applications to modify system settings or perform actions that could affect the security or stability of his computer is logged and brought to his attention. This proactive measure helps to detect and prevent unauthorized changes, thereby maintaining the integrity of the system and supporting the auditing and monitoring efforts essential to CIS Control 8.

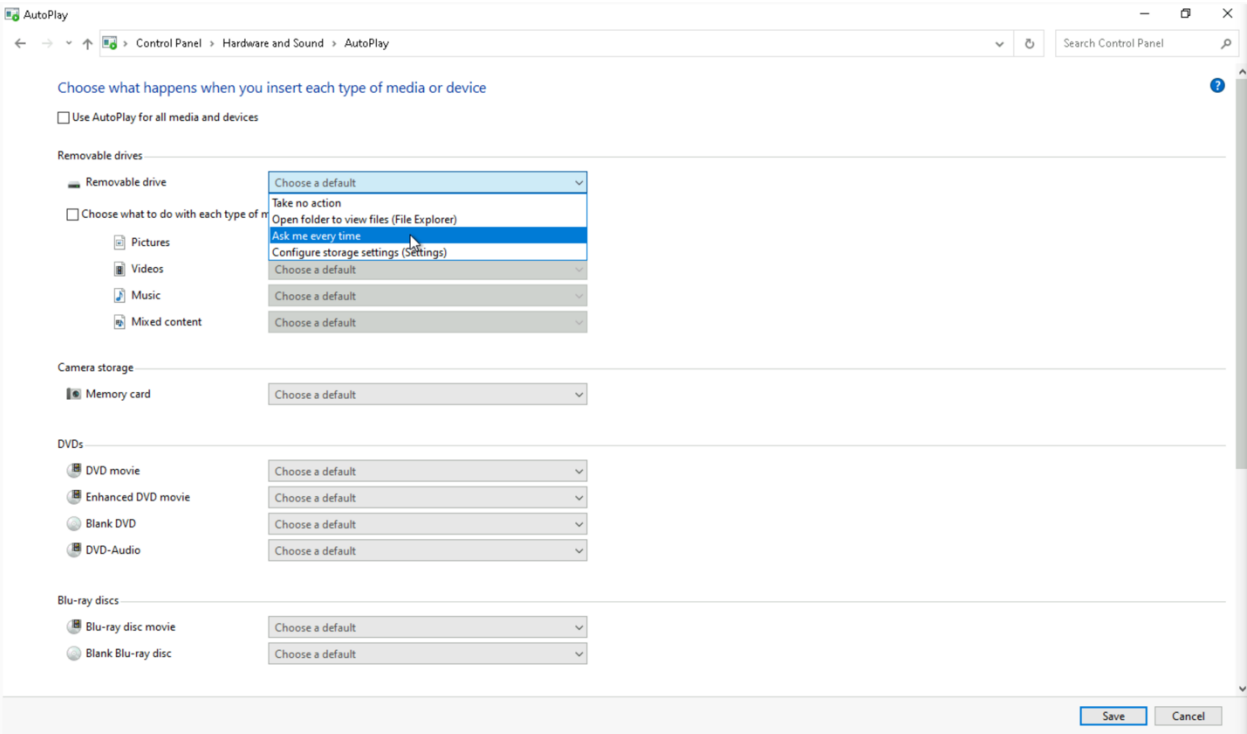


Securing Removable Media

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.*

*Disabling AutoPlay for all media and devices on Joe's computer helps comply with **CIS Control 11: Data Recovery** by reducing the risk of malware infections that could compromise the integrity and availability of backup data. CIS Control 11 focuses on ensuring that data recovery mechanisms are in place and reliable. By setting removable drives to "Ask me every time" and disabling automatic execution of applications, Joe minimizes the chance that malicious software could be introduced via removable media, which could corrupt or destroy critical backup files. This measure helps ensure that Joe's data recovery processes remain secure and effective, safeguarding the integrity of his backup policy.*

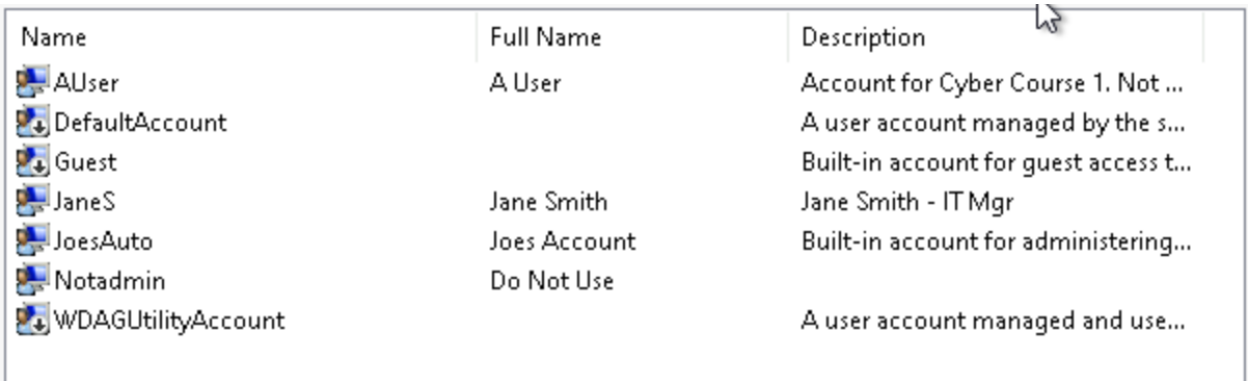


3. Securing Access

Ensuring only specific people have access to 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:

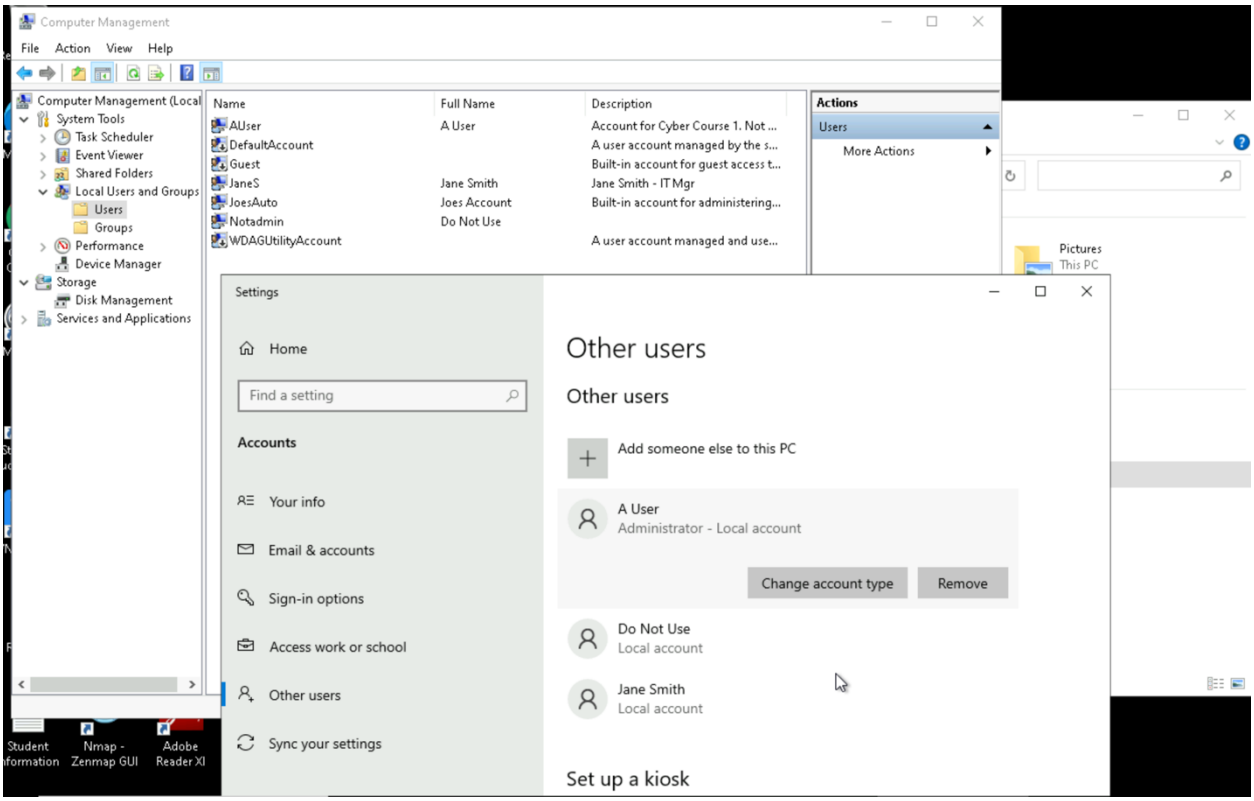
- JoesAuto
- Jane Smith (Joe's assistant)
- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)



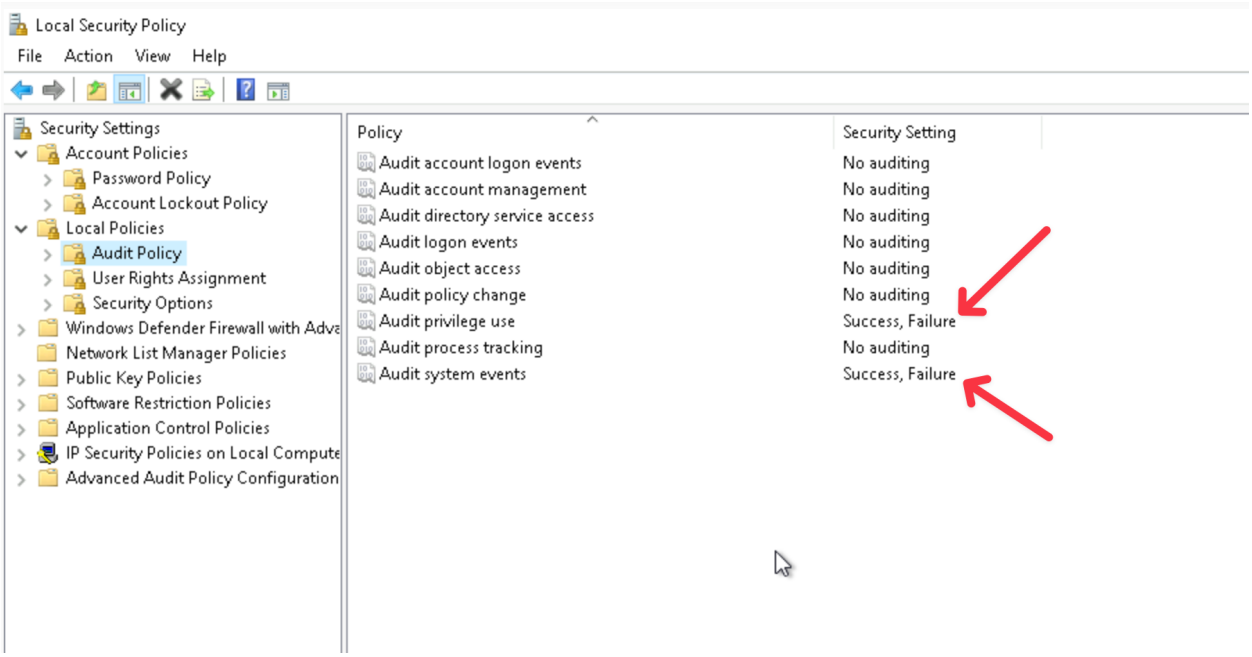
Name	Full Name	Description
AUser	A User	Account for Cyber Course 1. Not ...
DefaultAccount		A user account managed by the s...
Guest		Built-in account for guest access t...
JaneS	Jane Smith	Jane Smith - IT Mgr
JoesAuto	Joes Account	Built-in account for administering...
Notadmin	Do Not Use	
WDAGUtilityAccount		A user account managed and use...

Joe's Auto Access Rules:

- Only JoesAuto and A User should have administrative privileges on this PC.



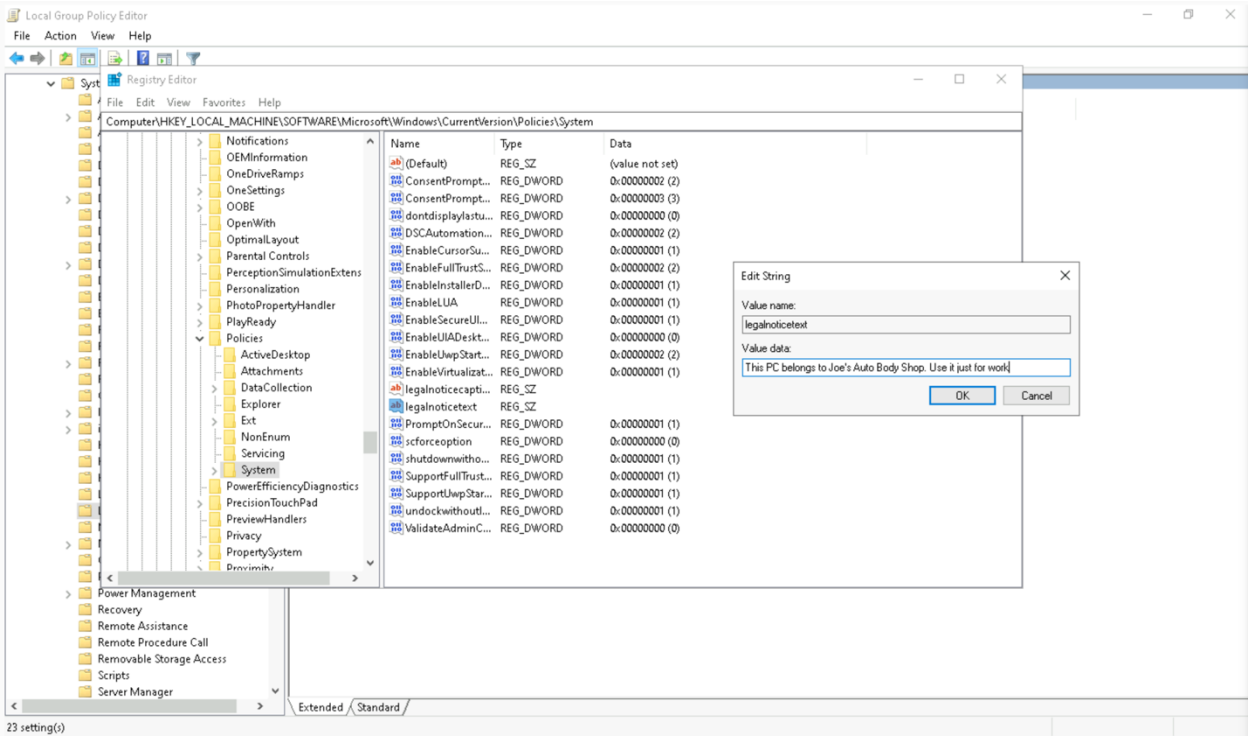
- Joe wants to prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.



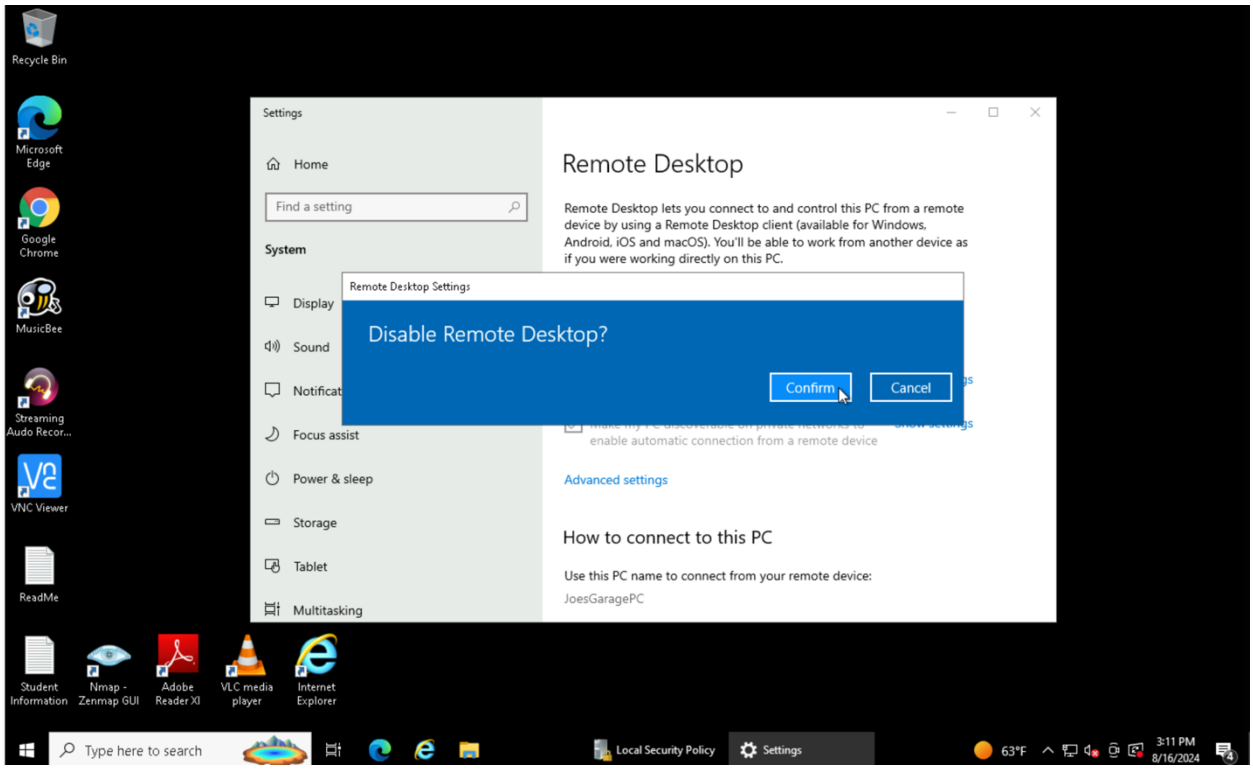
- All valid users should have a password following Joe's password policy below
    - At least 8 characters

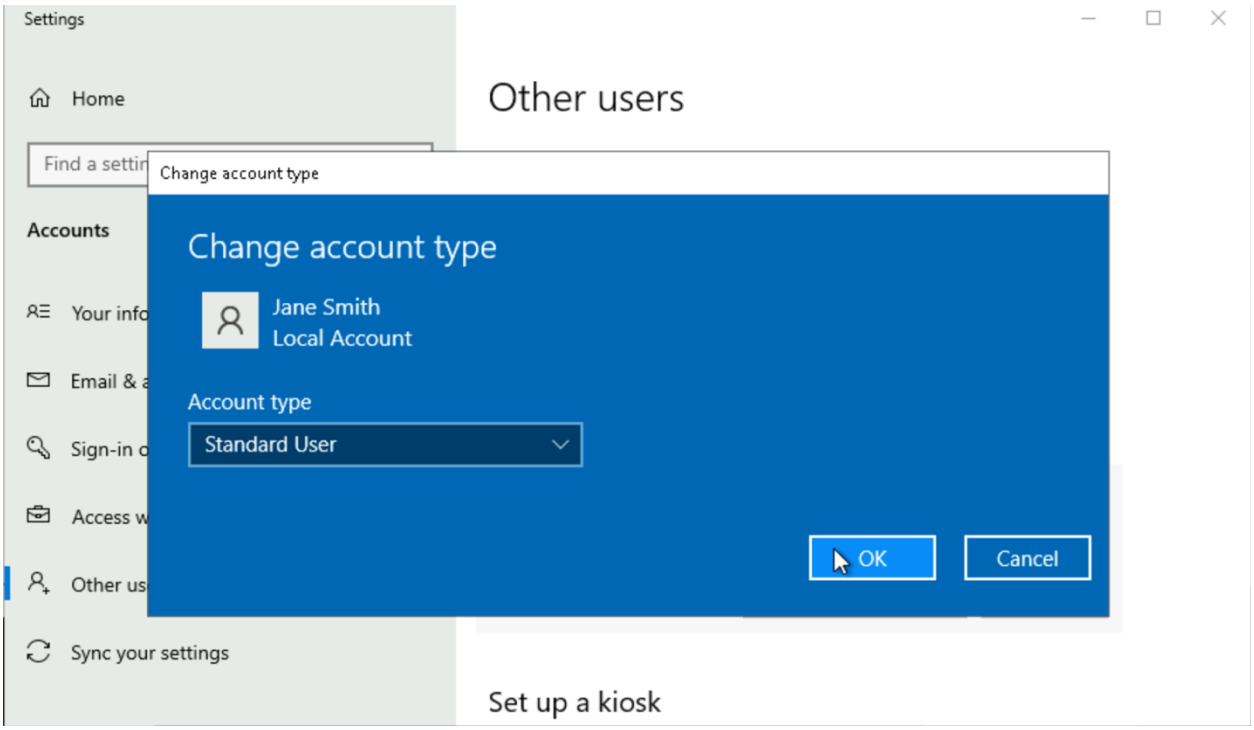
    - Complexity enabled
    - Changed every 120 days
    - Cannot be the same as the previous 5 passwords
- Account should be automatically disabled after 5 unsuccessful login attempts. The account should be locked for 15 minutes and then should automatically unlock.

- 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

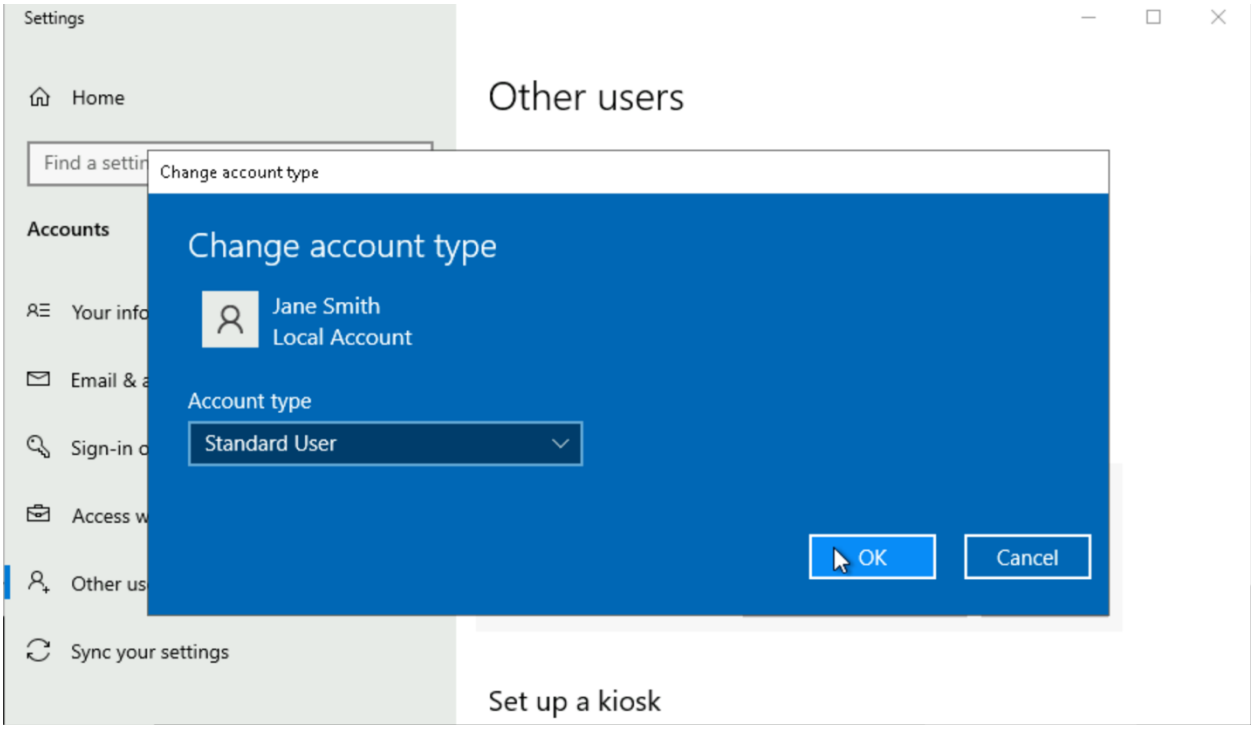
1. *What user accounts should not be there? -> **A Hacker***

2. *Bonus questions: What is Hacker's password? -* ***?***
3. *Explain the steps you take to disable or remove unwanted accounts. -* ***Right click on the account, then select Remove. A prompt will ask for confirmation***
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*

Disabling or removing unneeded accounts from a PC or application is important because it reduces potential entry points for attackers. Unused accounts can be exploited to gain unauthorized access, especially if they have weak or default passwords. These accounts may also increase the risk of insider threats and make it harder to track legitimate activity. By removing them, you minimize vulnerabilities and improve overall security.

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**
6. Explain how you determined this. Provide screenshots as needed. – **From Settings panel I reviewed all accounts. Tourns out that Jane was set as administrator. Double click on the account made me change it to a standard user account as follow:**



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.

- **Malware Installation**: Users with administrator rights can unintentionally install malicious software, which can compromise the entire system.
- **System Configuration Changes**: They can make critical changes to system settings, potentially disrupting system stability or security configurations
- **Unauthorized Access**: If an administrator account is compromised, an attacker can gain full control of the system, accessing sensitive data and executing harmful actions

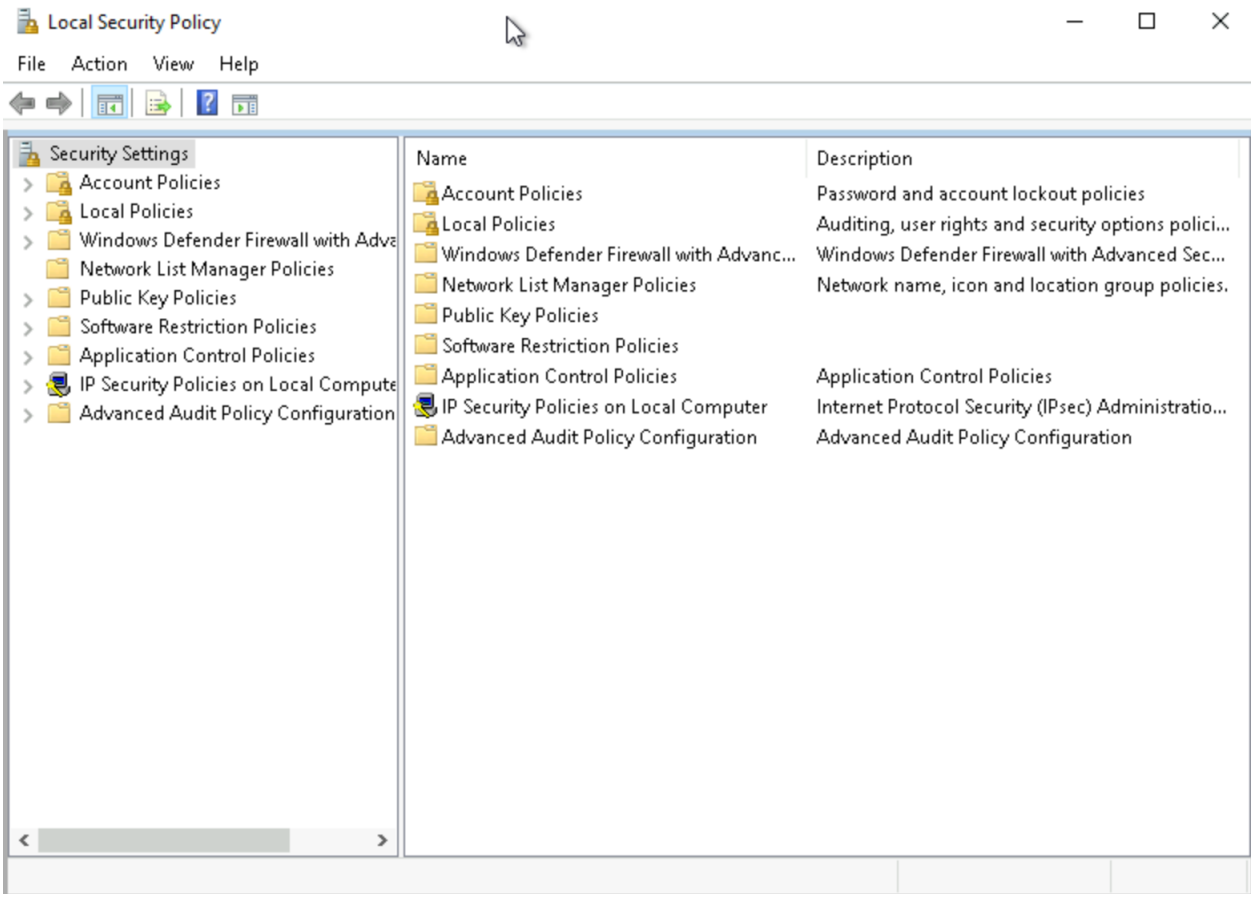
Now you need to remove administrator privileges for any user(s) that should have it.

8. *Explain the process for doing this. Include screenshots to show your work.* – ***Already answered to this question on section before***
9. *What is the security principle behind this?* - ***Principle of Least Privilege***
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill? - ***CIS Control 4: Controlled Use of Administrative Privileges***

Setting Access and Authentication Policies

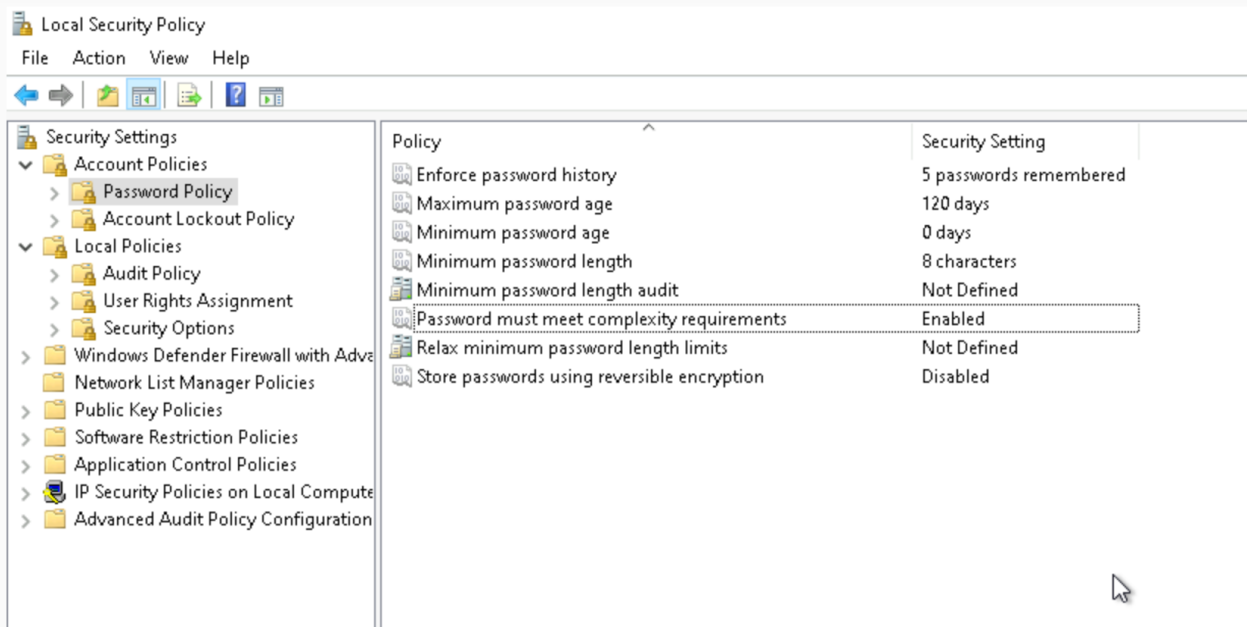
After you talked with Joe about security, he has asked that the access rules outlined above be in place on his PC. These are set using the Local Security Policy function in Windows 10. On the Windows search bar, type "*Local Security Policy*" to access it. Click the > arrow next to both "*Account Policies*"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

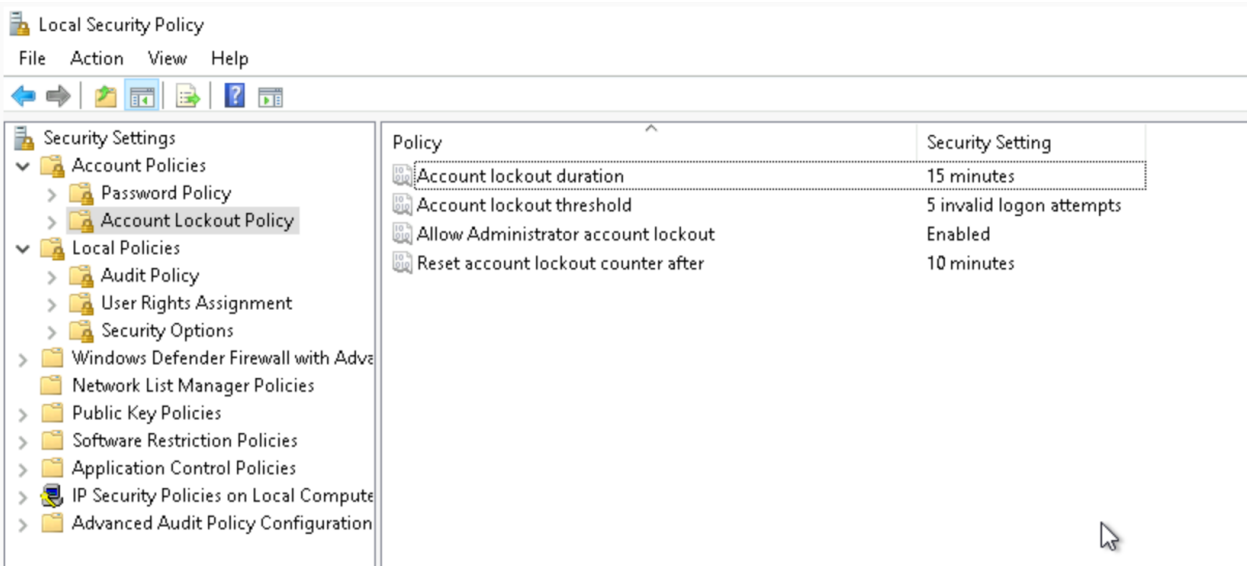
1. *Provide a screenshot of the Local Security Policy window here.*



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:
    - Setting the Account Lockout Policy:

    By accessing the two relevant sections, it is possible to configure the system variables as desired. By clicking on the variable of our interest, a drop-down menu appears that allows us to modify it accordingly

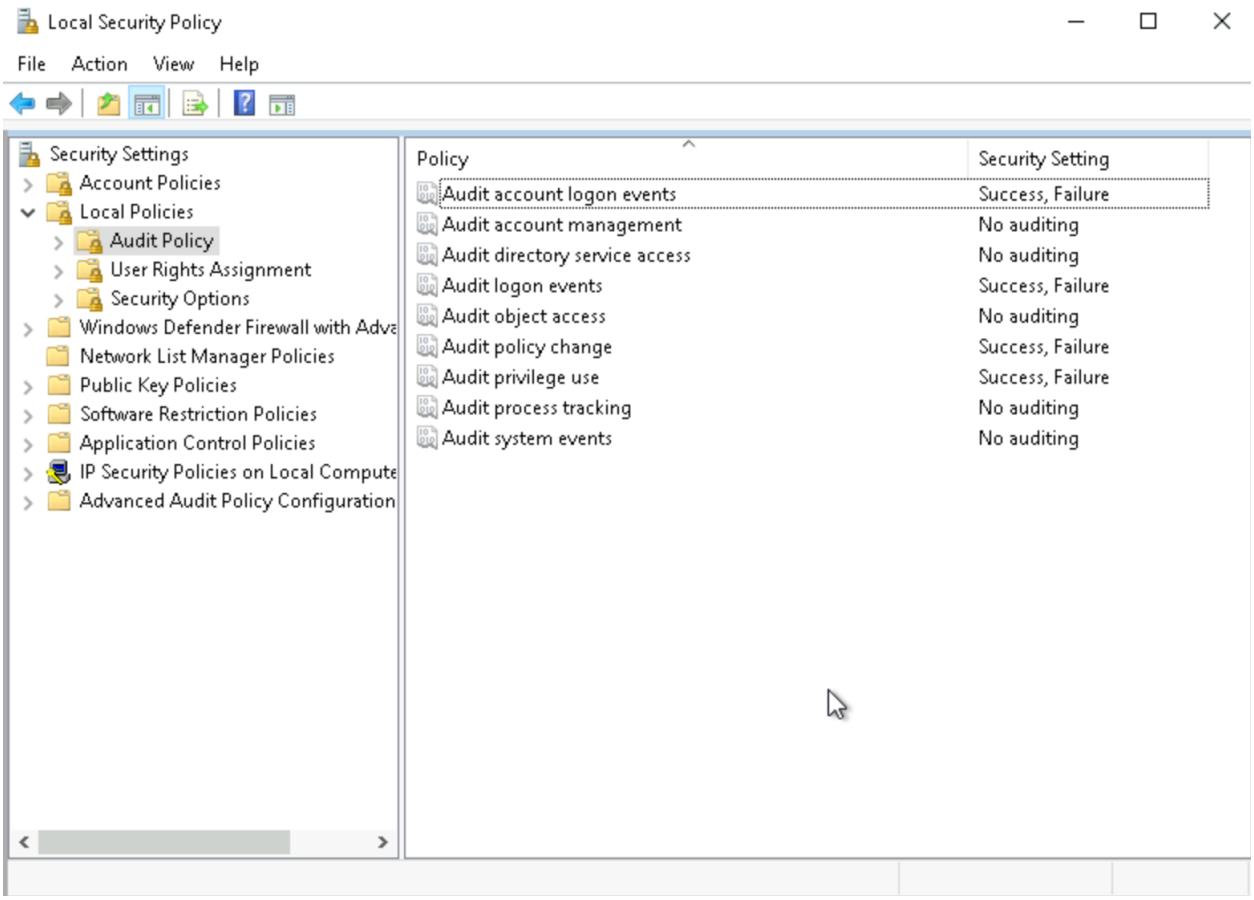




Auditing and Logging

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.*

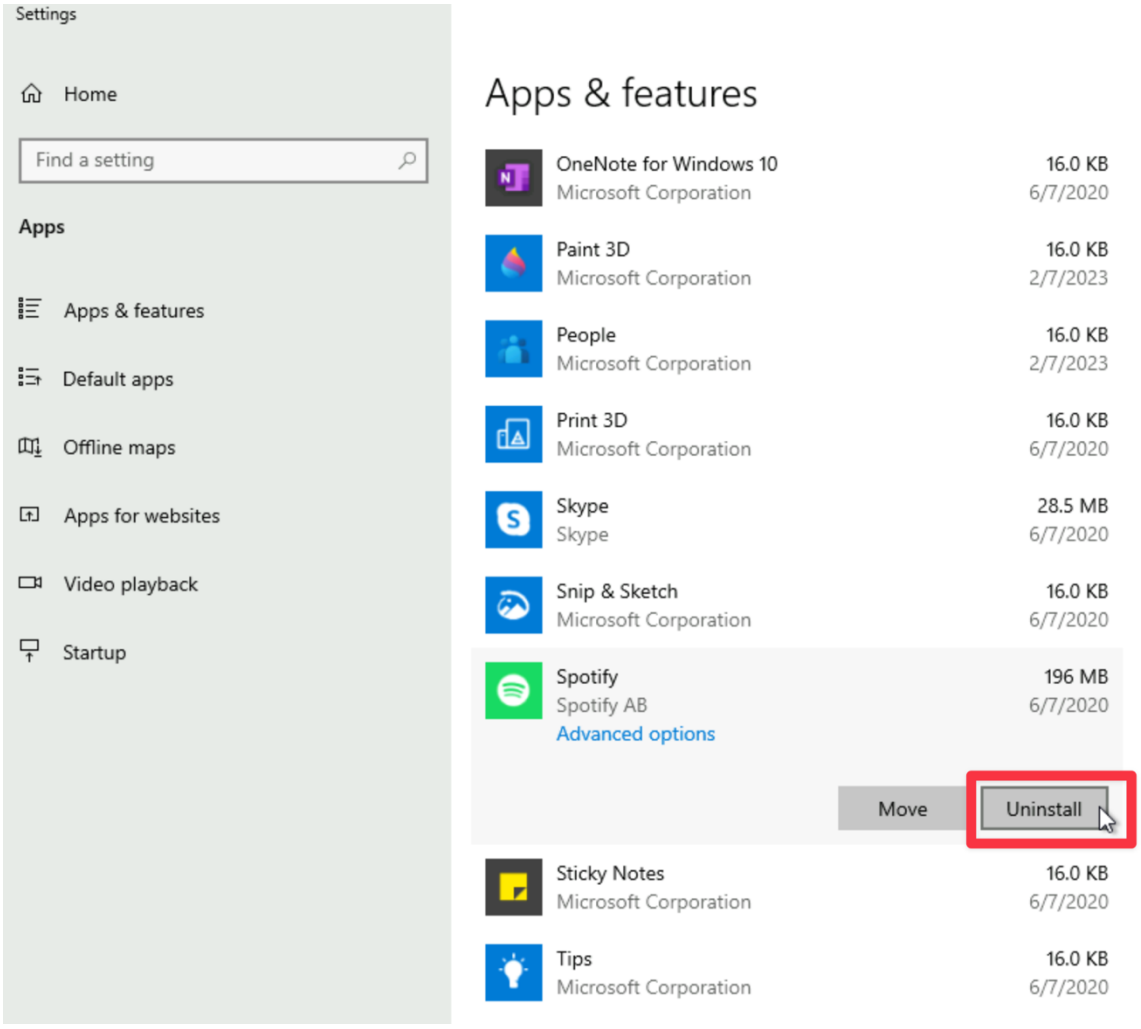
- ***Candy Crush Friends***
- ***Paint 3D***
- ***Spotify***

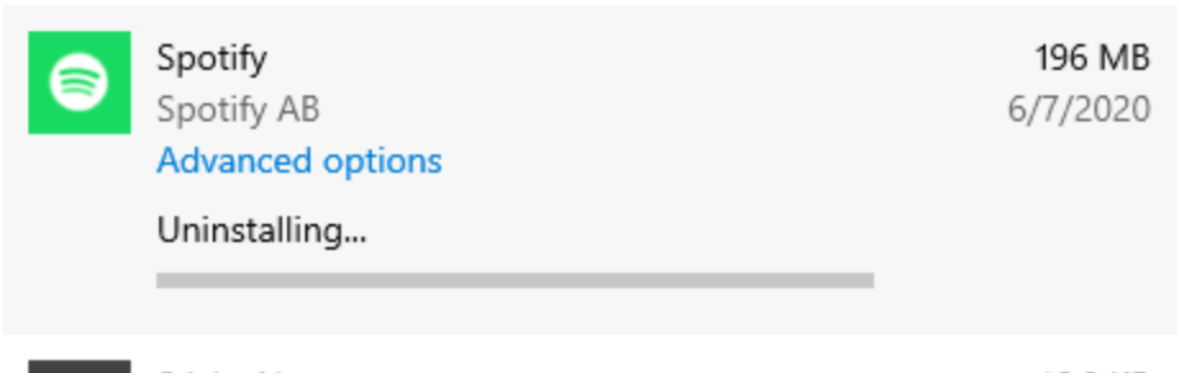
2. *Name at least three vulnerabilities, threats or risks with having unnecessary applications:*

- ***Increased Attack Surface**: Unnecessary applications can introduce additional vulnerabilities that attackers can exploit, increasing the overall risk to the system.*
- ***Outdated Software**: Unused applications are often not updated regularly, making them more susceptible to known security vulnerabilities.*
- ***Resource Drain**: Unnecessary applications can consume system resources, potentially slowing down performance and leaving fewer resources available for essential security processes.*

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.*

Right click on the Windows key -> Applications -> Left click on the application to uninstall -> Follow the wizard. The procedure may vary depending on the application



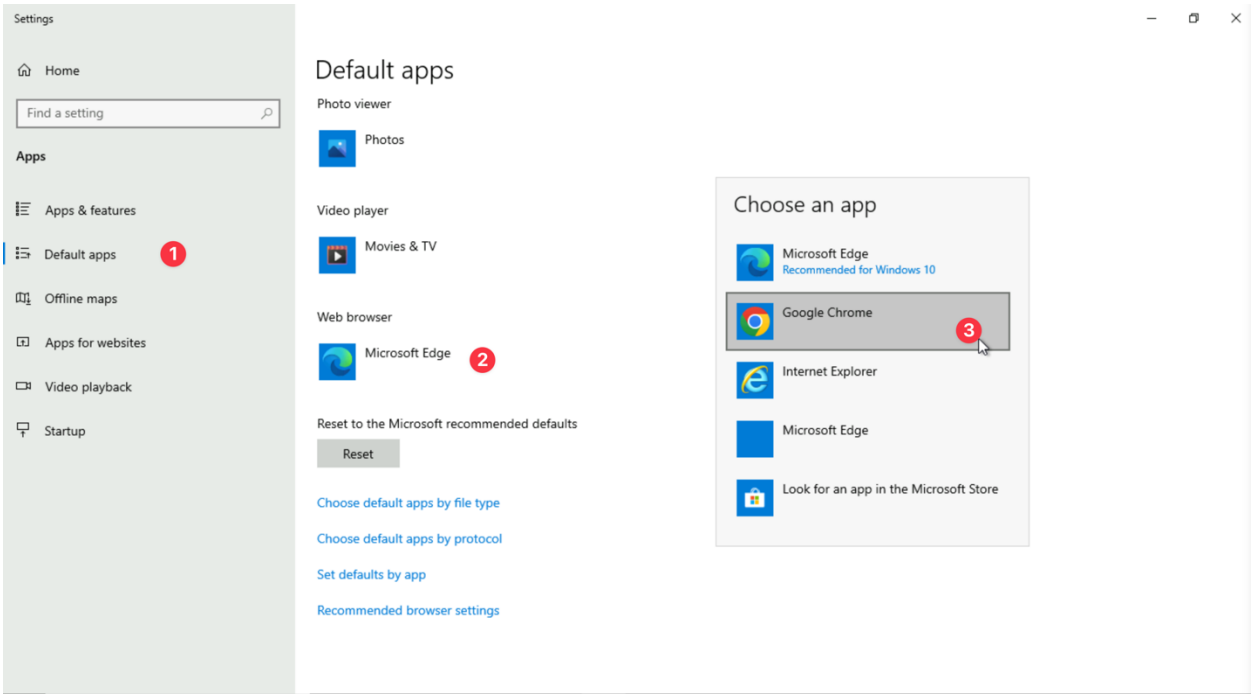


Default Browser

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.*

   Settings -> Default Apps -> Then choose the desired application based on the function

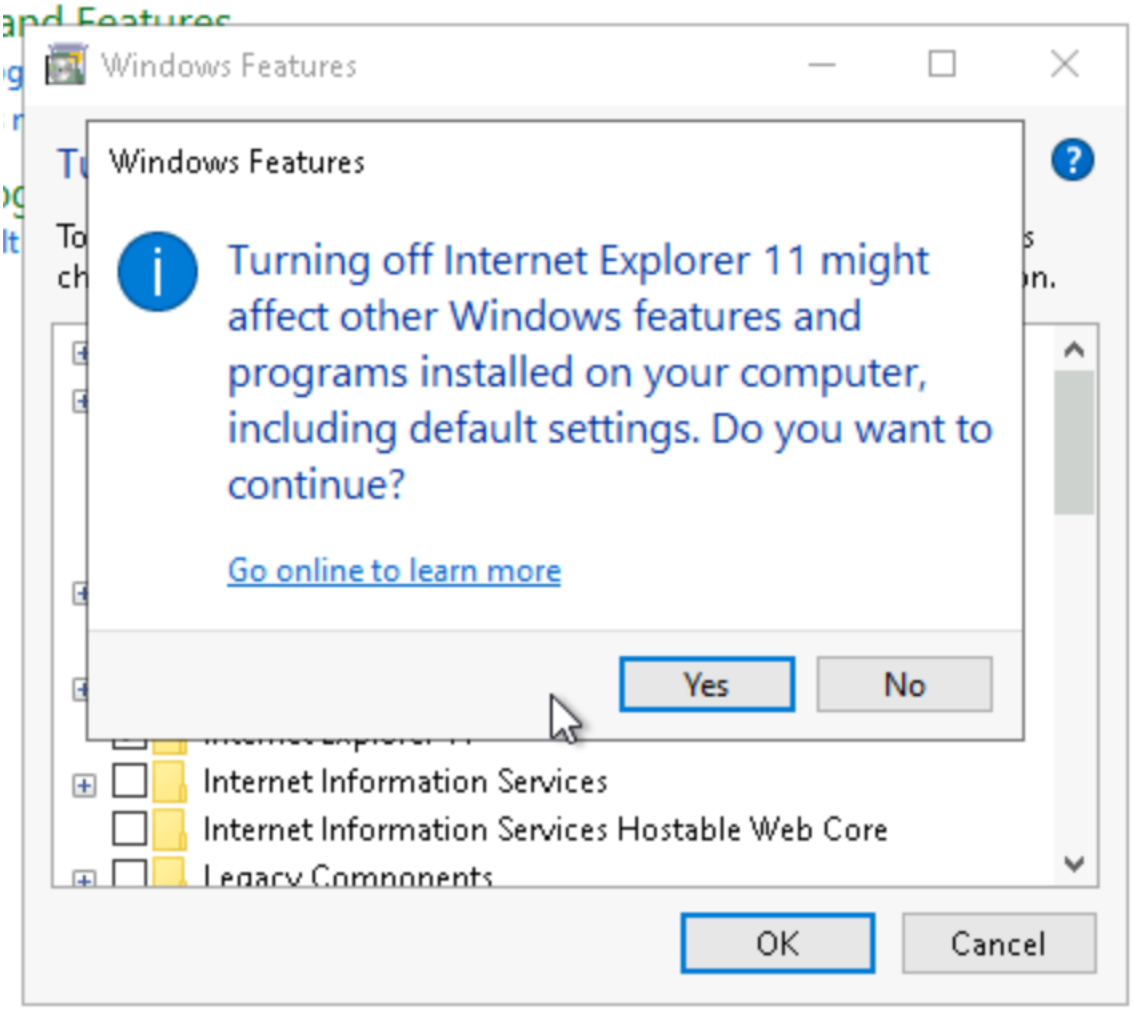


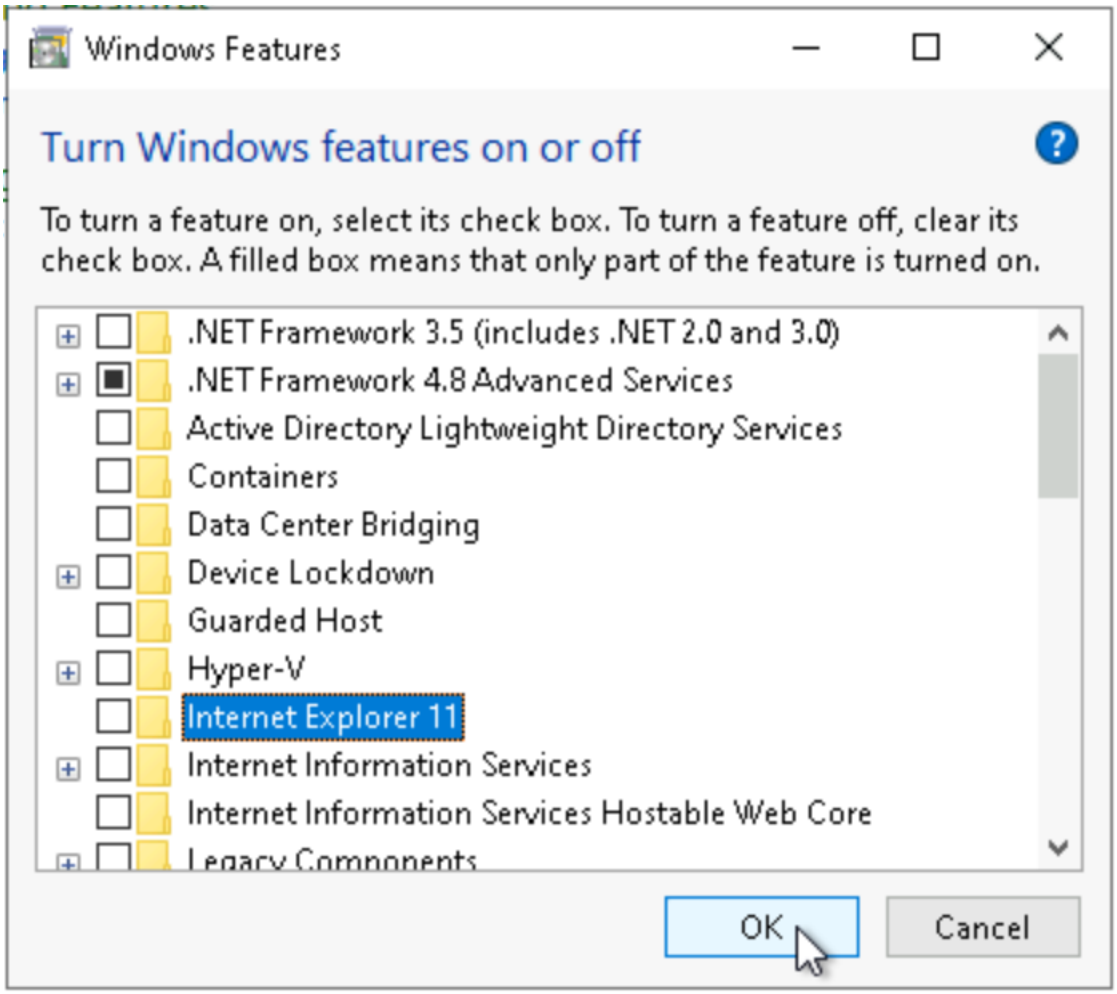
2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
   - **Outdated Security Features**: Internet Explorer is no longer updated with the latest security features, making it more vulnerable to new exploits and attacks. This increases the risk of malware infections and unauthorized access.

- **Known Vulnerabilities**: Since Microsoft has largely discontinued support for Internet Explorer, many of its known vulnerabilities remain unpatched. Attackers can exploit these vulnerabilities to gain control of the system or steal sensitive data.

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.*

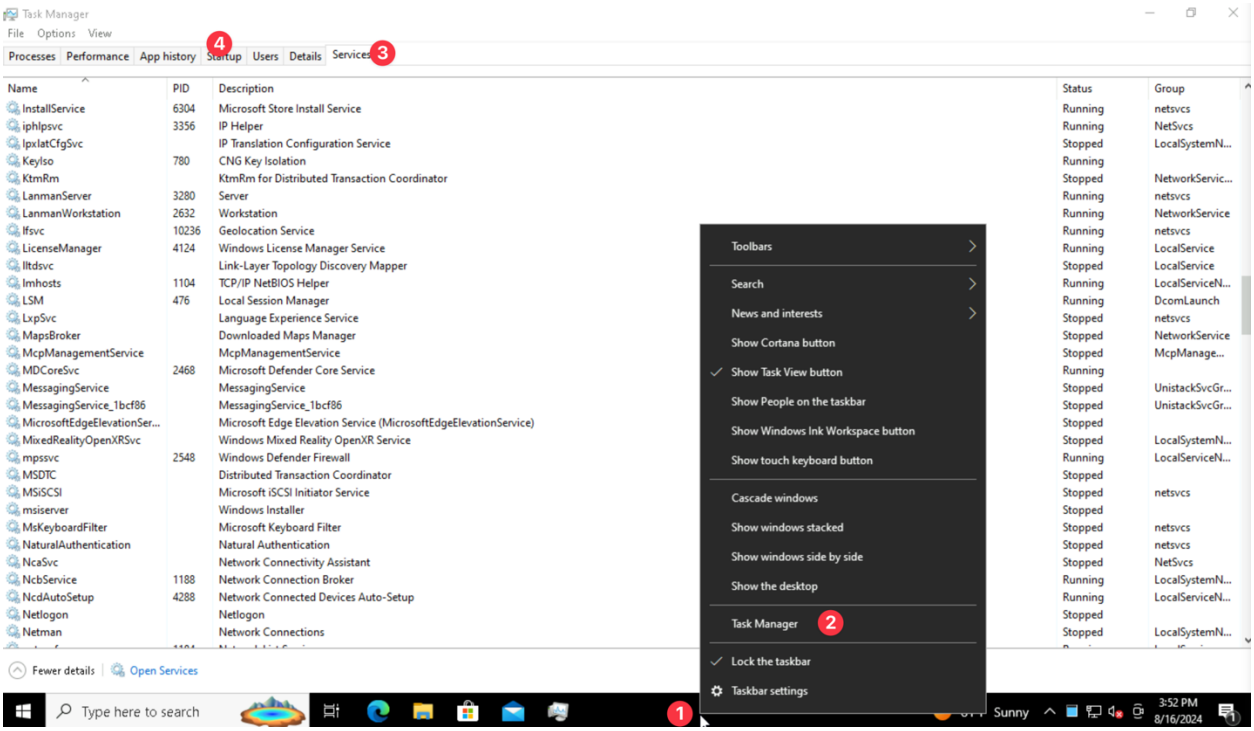




Windows Services

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 -> **You may find an apache/nginx/etc daemon running under Services tab. Otherwise you may run an nMap scan over your localhost to see if any service is listening on ports 80 or 443**
3. How do you disable them and make sure they are not restarted? -> **Point 4 of the previews screenshot. You can disable bootup services from that screen**
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. -> ***Same as above. You can shutdown the FTP service and then remove the bootup daemon from the Startup section***

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.

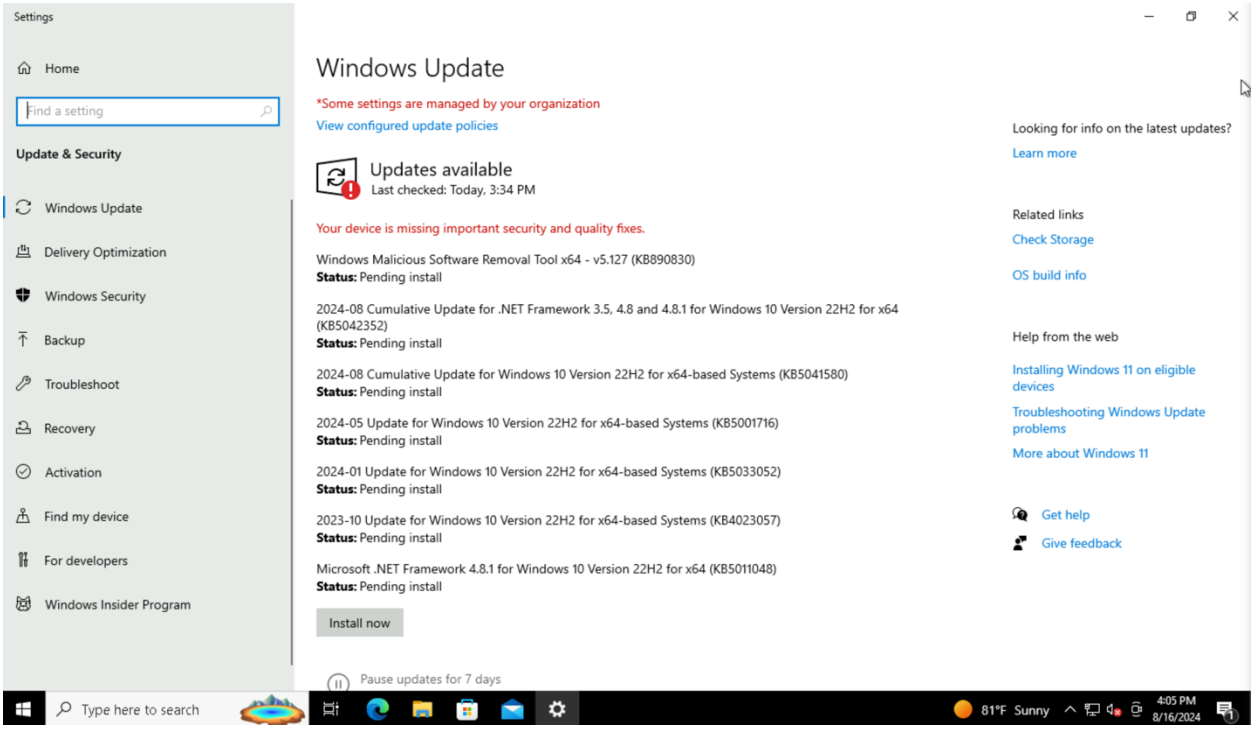
1. *Explain the process for doing this. Include screenshots as needed.*

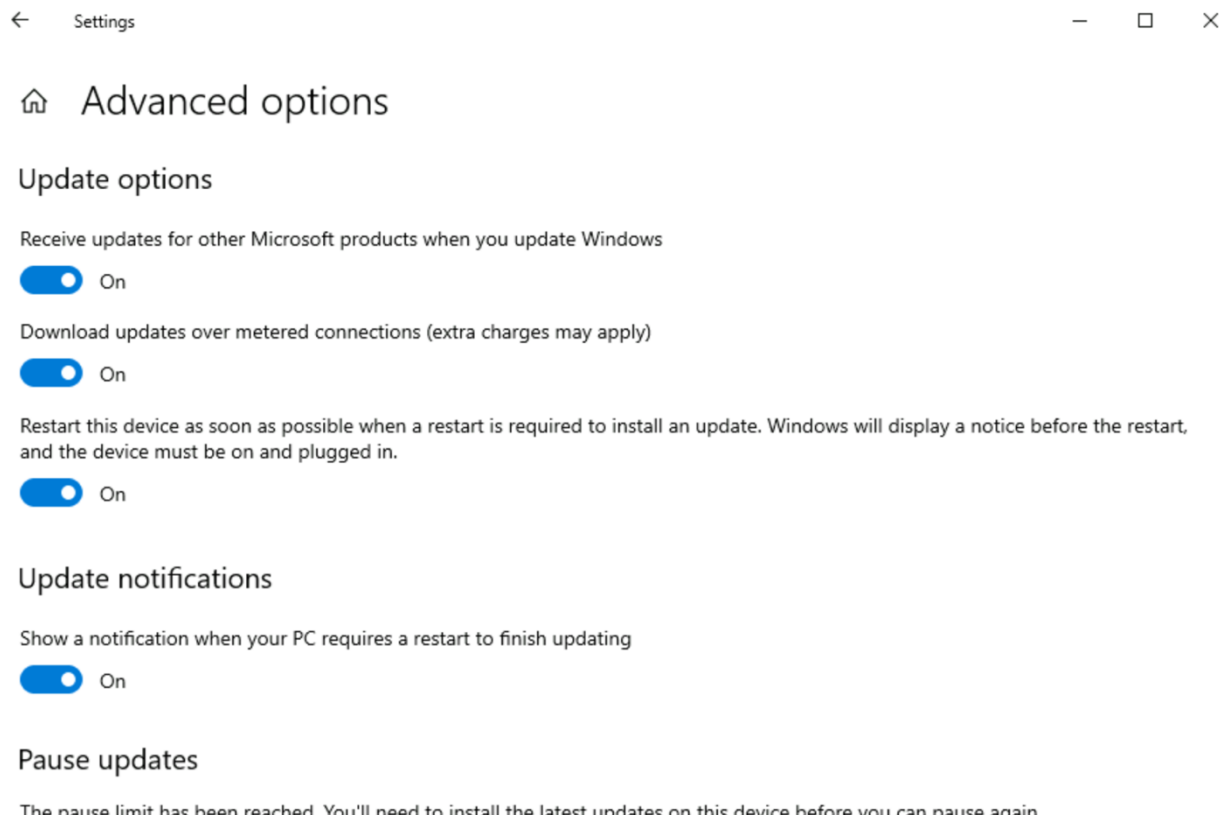
First, we open the Windows Update panel and check for updates for the PC. In our case, several updates are needed, so let's proceed with the relative installation.

While the updates are being installed, let's go to the advanced settings and enable updates for

other Microsoft software, so as to ensure that the PC remains updated on other proprietary Microsoft software.

Finally, let's check that the automatic updates policy is already enabled, as in our case. Otherwise, let's proceed to enable it




Settings
Advanced options
Update options
Receive updates for other Microsoft products when you update Windows
On
Download updates over metered connections (extra charges may apply)
On
Restart this device as soon as possible when a restart is required to install an update. Windows will display a notice before the restart, and the device must be on and plugged in.
On
Update notifications
Show a notification when your PC requires a restart to finish updating
On
Pause updates
The pause limit has been reached. You'll need to install the latest updates on this device before you can pause again

Microsoft .NET Framework 4.8.1 for Windows 10 Version 22H2 for x64 (KB5011048)
Status: Pending install

Windows Update

Windows Malicious Software Removal Tool x64 - v5.127 (KB890830)
Status: Pending install

2024-08 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5042352)
Status: Pending install

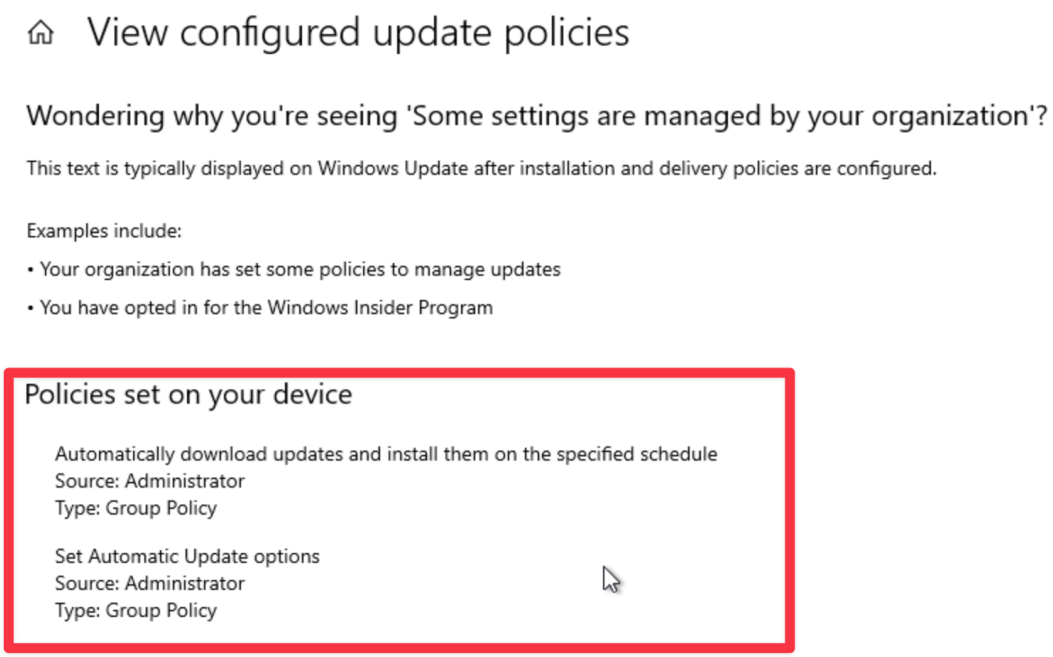
2024-08 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5041580)
Status: Pending install

2024-05 Update for Windows 10 Version 22H2 for x64-based Systems (KB5001716)
Status: Pending install

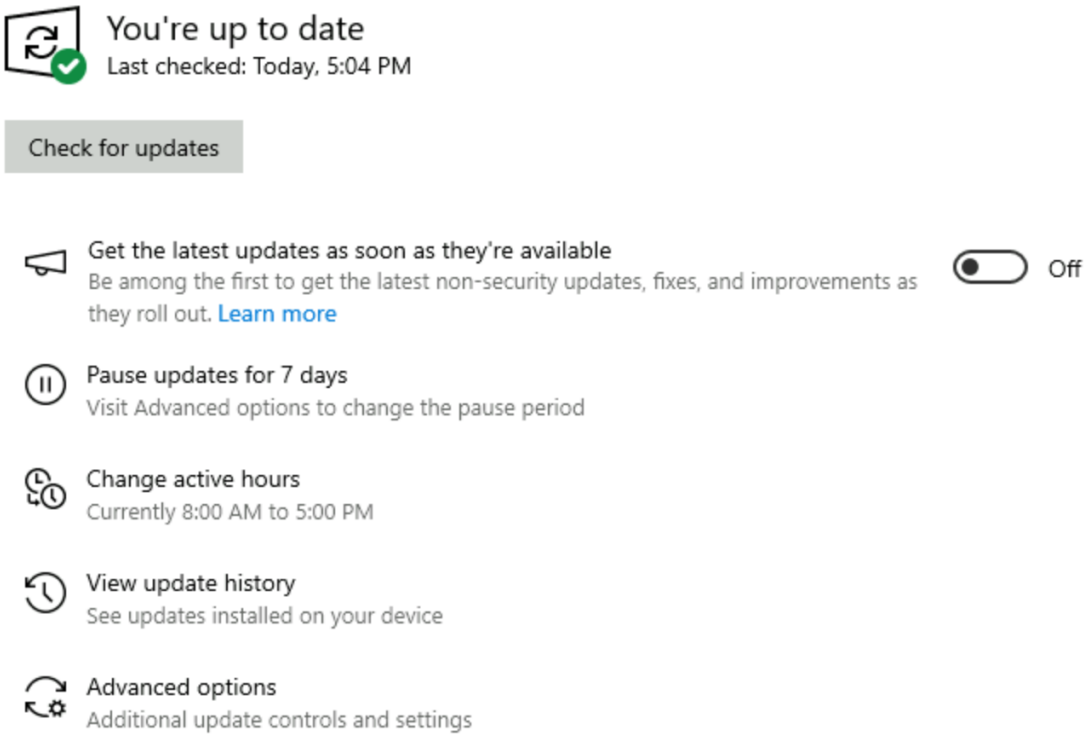
2024-01 Update for Windows 10 Version 22H2 for x64-based Systems (KB5033052)
Status: Pending install

2023-10 Update for Windows 10 Version 22H2 for x64-based Systems (KB4023057)
Status: Pending install

Microsoft .NET Framework 4.8.1 for Windows 10 Version 22H2 for x64 (KB5011048)
Status: Installing - 44%



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.*



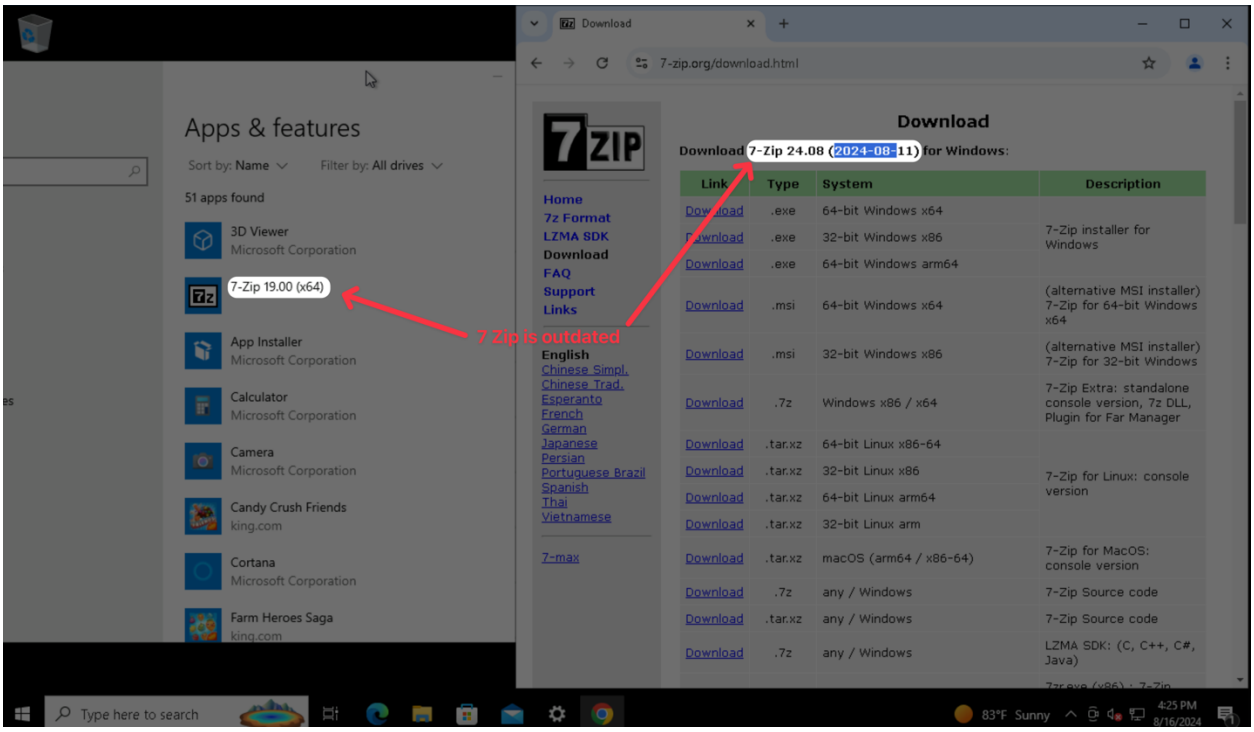
All applications should also be up to date on patches or fixes provided by the manufacturer. Any old versions of software should be uninstalled.

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

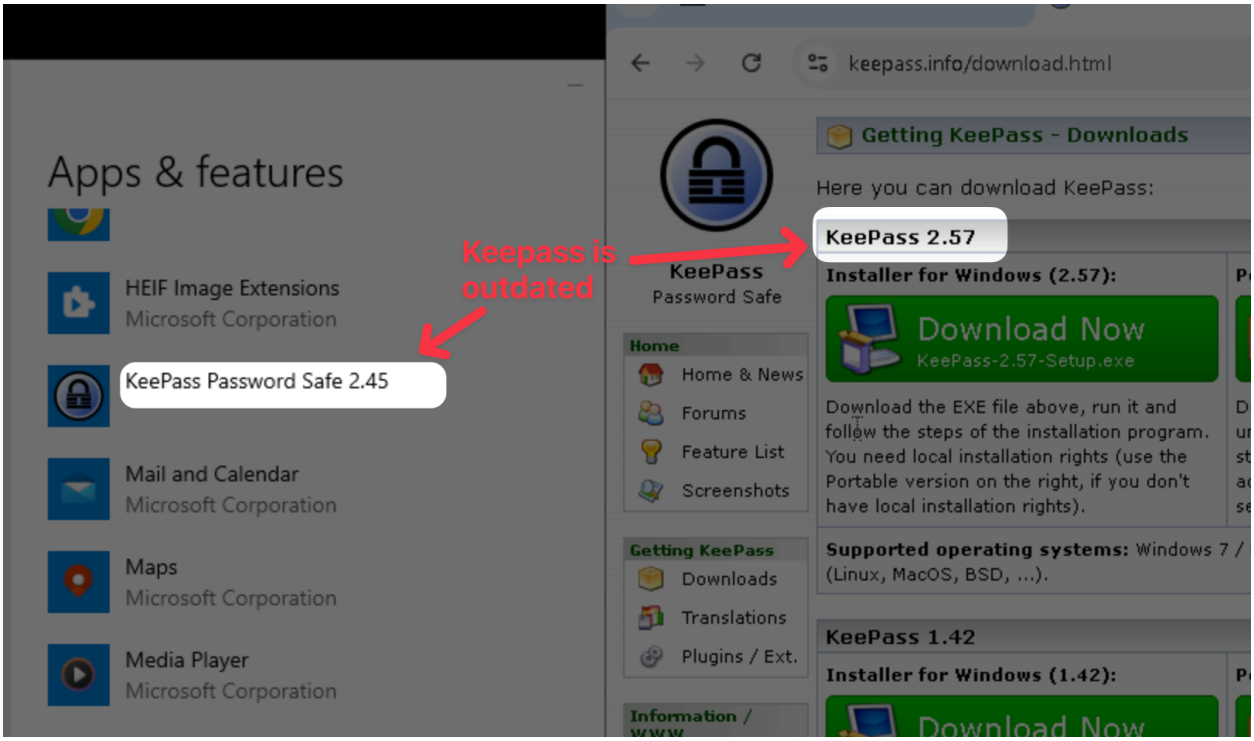
- 7-Zip
- Keepass

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

   Confronting local installed version with newest version available to the 7-Zip website we can determine that the software is outdated:

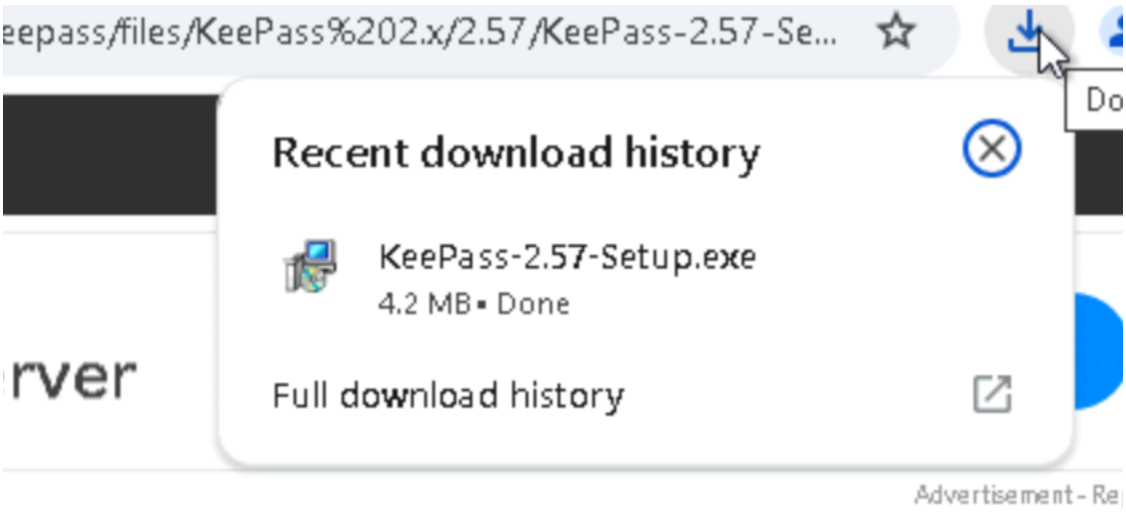


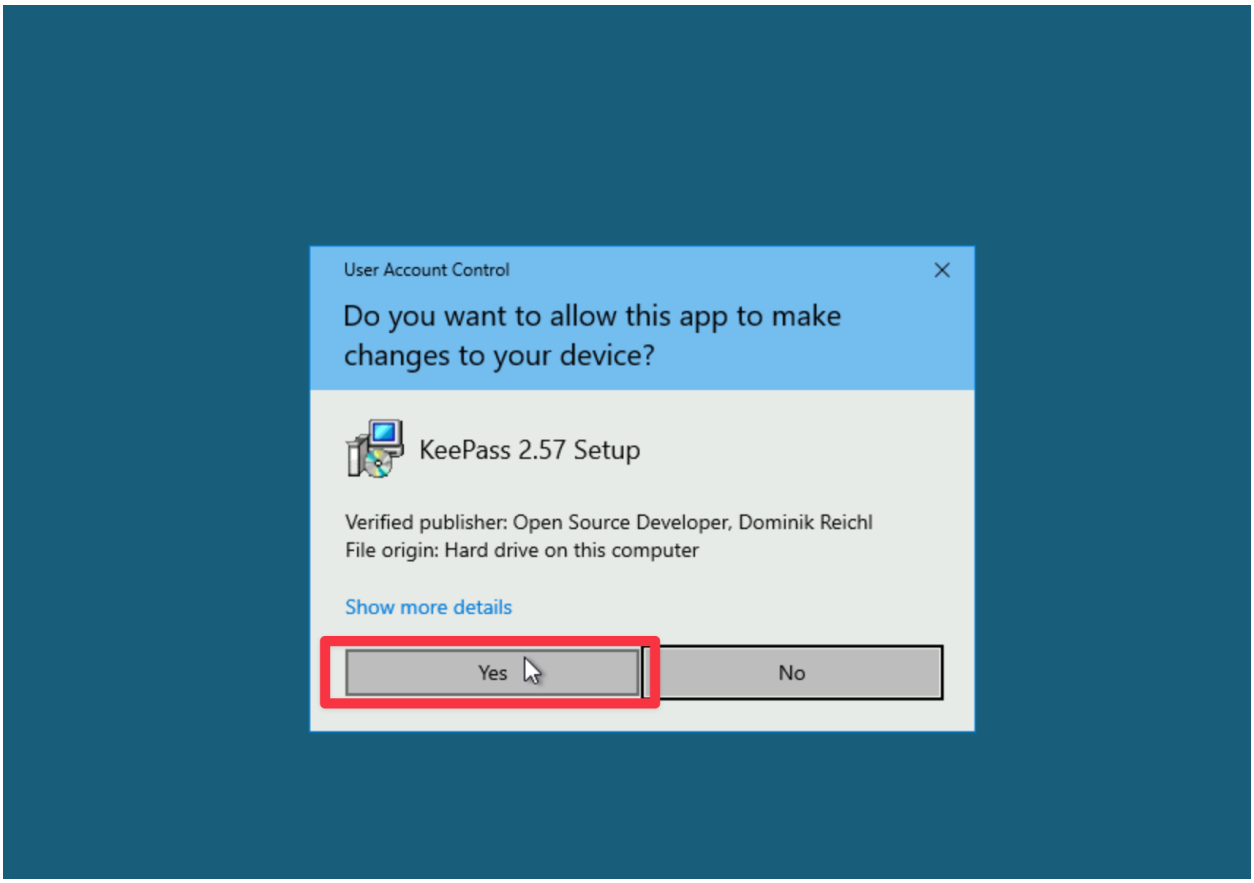
Same apply to KeePass:

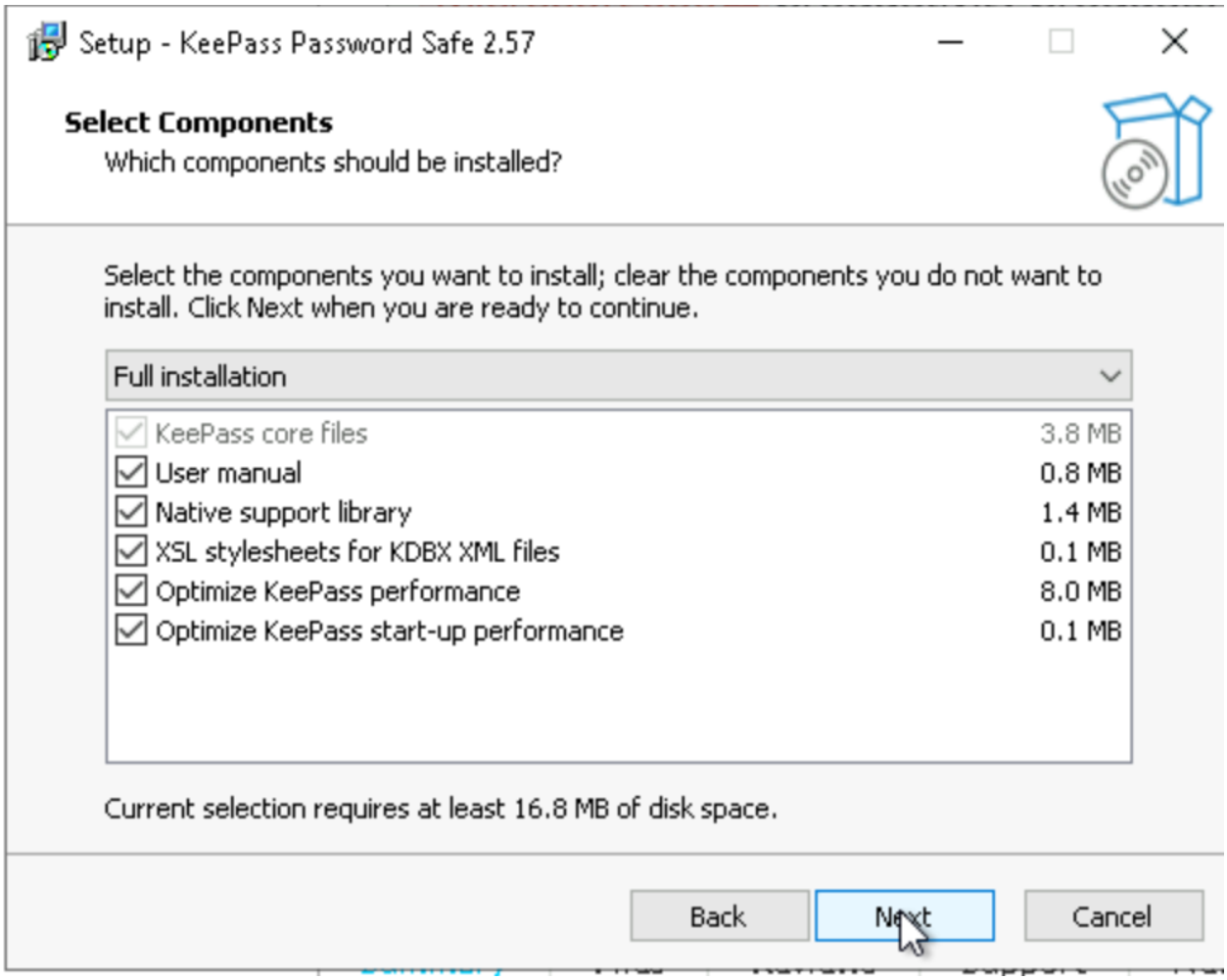


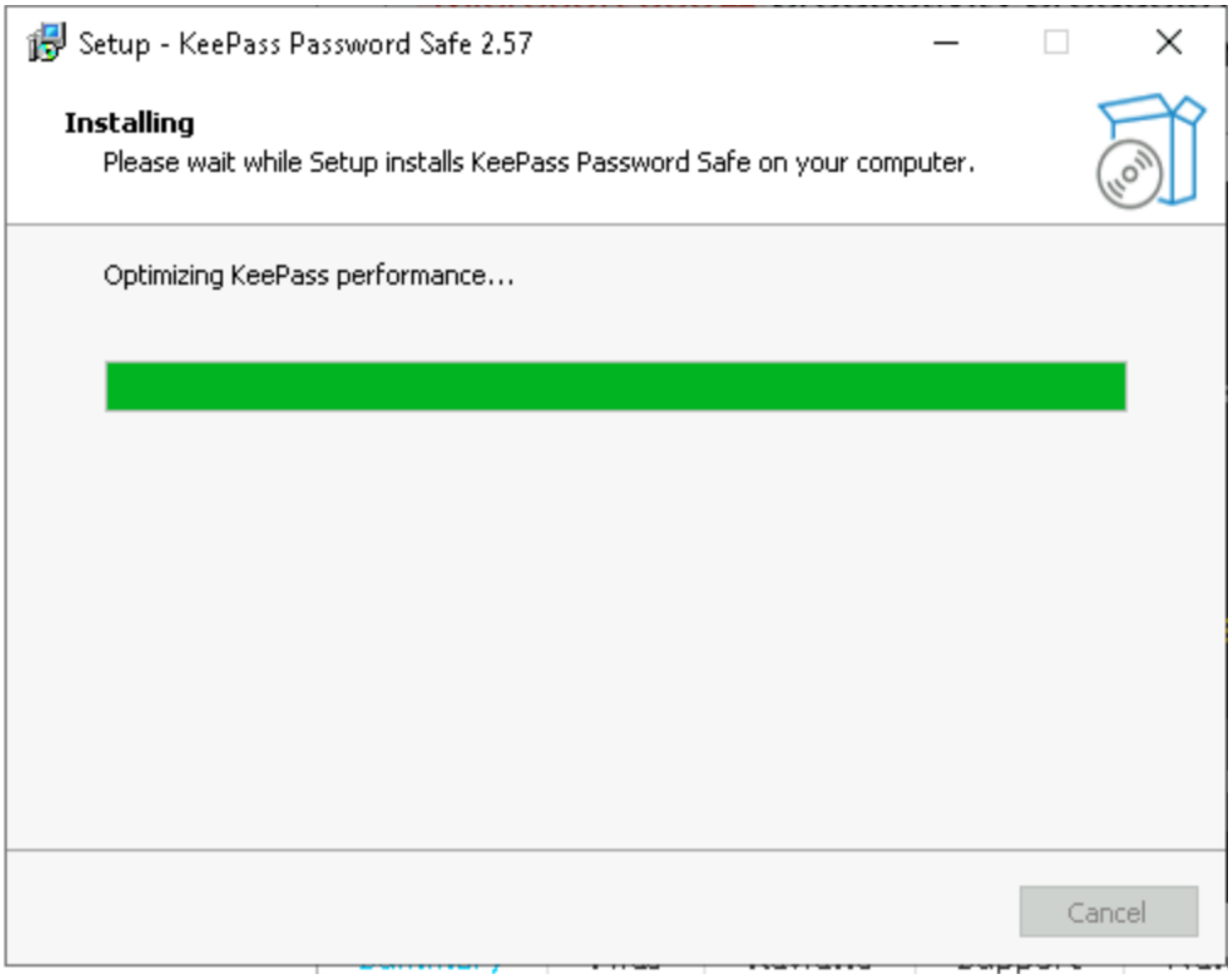
5. *Explain the steps for updating each of these applications. Include screenshots as needed.*

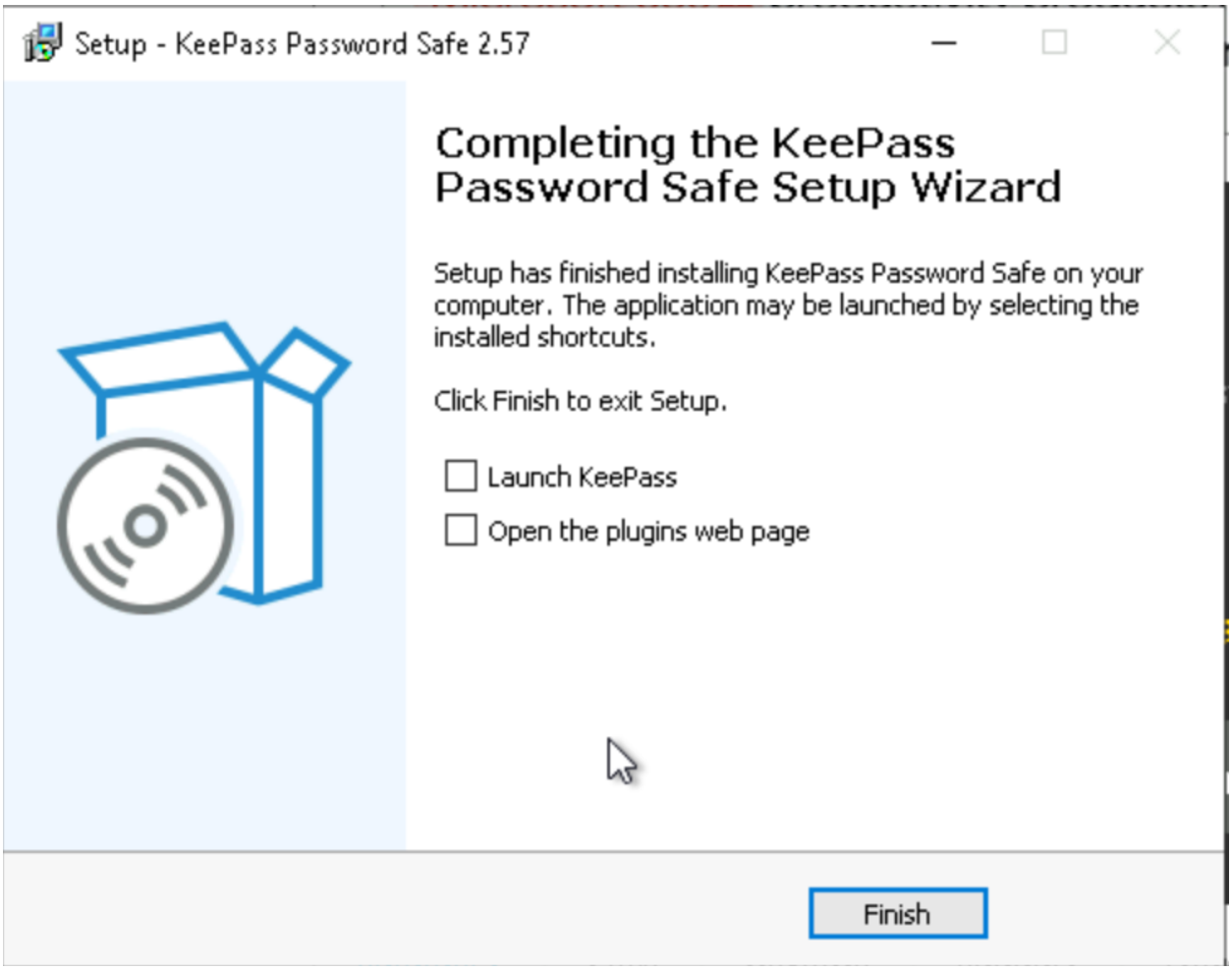
To Update KeePass:


eepass/files/KeePass%202.x/2.57/KeePass-2.57-Se...
Recent download history
KeePass-2.57-Setup.exe
4.2 MB • Done
Full download history
rver
Advertisement - Re

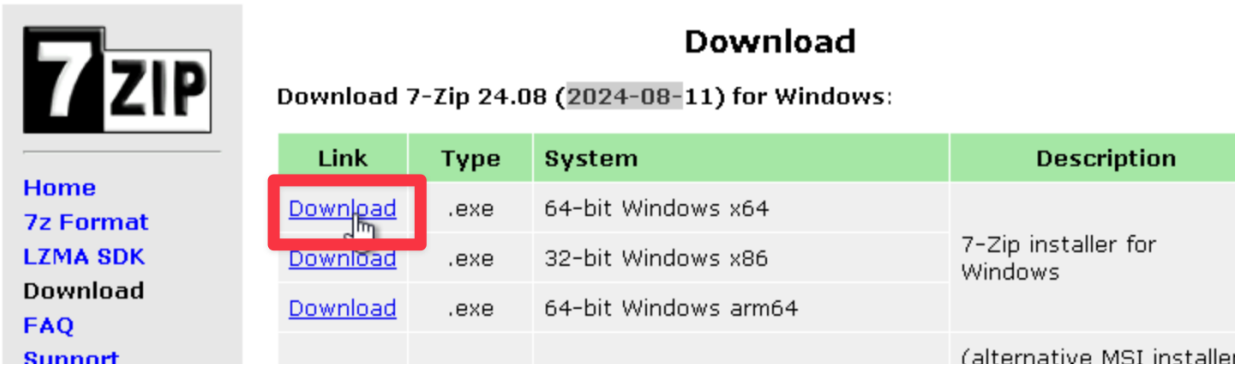

User Account Control
Do you want to allow this app to make changes to your device?
KeePass 2.57 Setup
Verified publisher: Open Source Developer, Dominik Reichl
File origin: Hard drive on this computer
Show more details
Yes
No

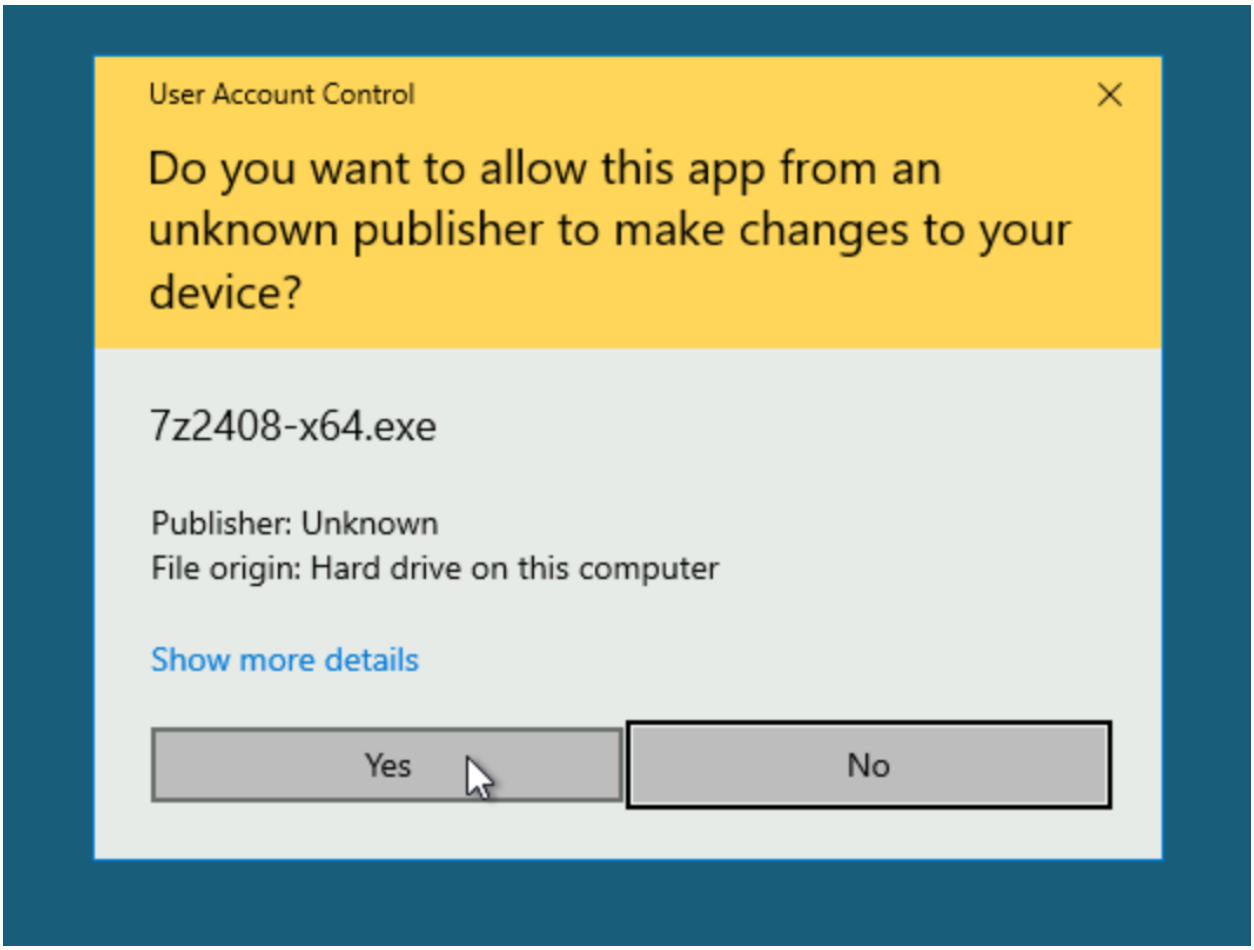

Setup - KeePass Password Safe 2.57
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Full installation
KeePass core files 3.8 MB
User manual 0.8 MB
Native support library 1.4 MB
XSL stylesheets for KDBX XML files 0.1 MB
Optimize KeePass performance 8.0 MB
Optimize KeePass start-up performance 0.1 MB
Current selection requires at least 16.8 MB of disk space.
Back
Next
Cancel

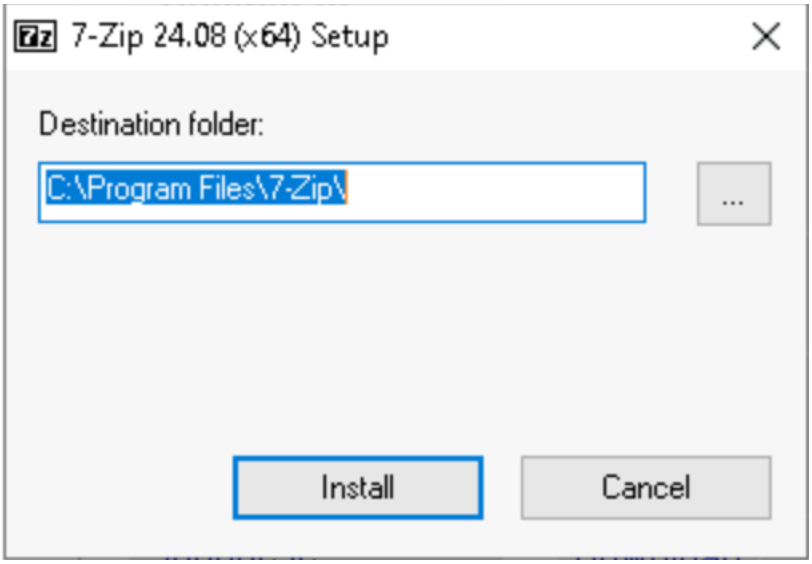

Setup - KeePass Password Safe 2.57
Installing
Please wait while Setup installs KeePass Password Safe on your computer.
Optimizing KeePass performance...
Cancel

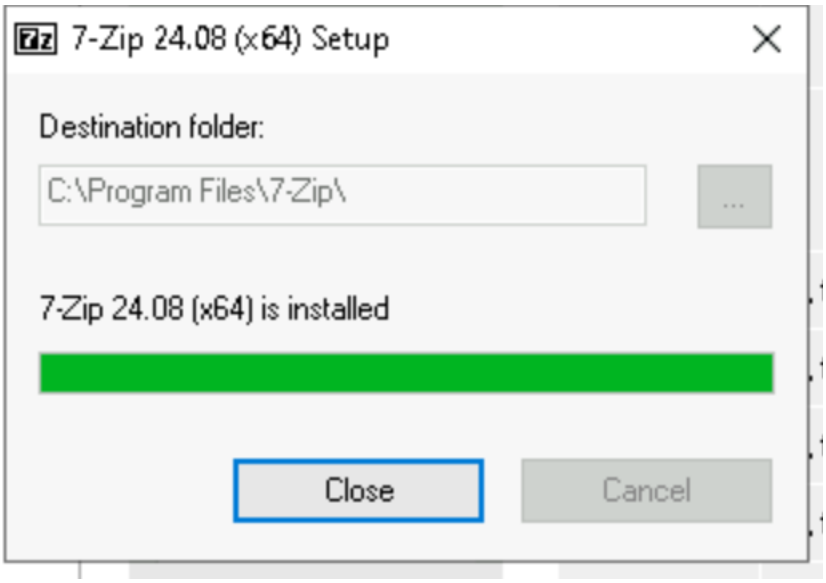


To Update 7 Zip:




User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
7z2408-x64.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
No


7-Zip 24.08 (x64) Setup
Destination folder:
C:\Program Files\7-Zip\
...
Install
Cancel



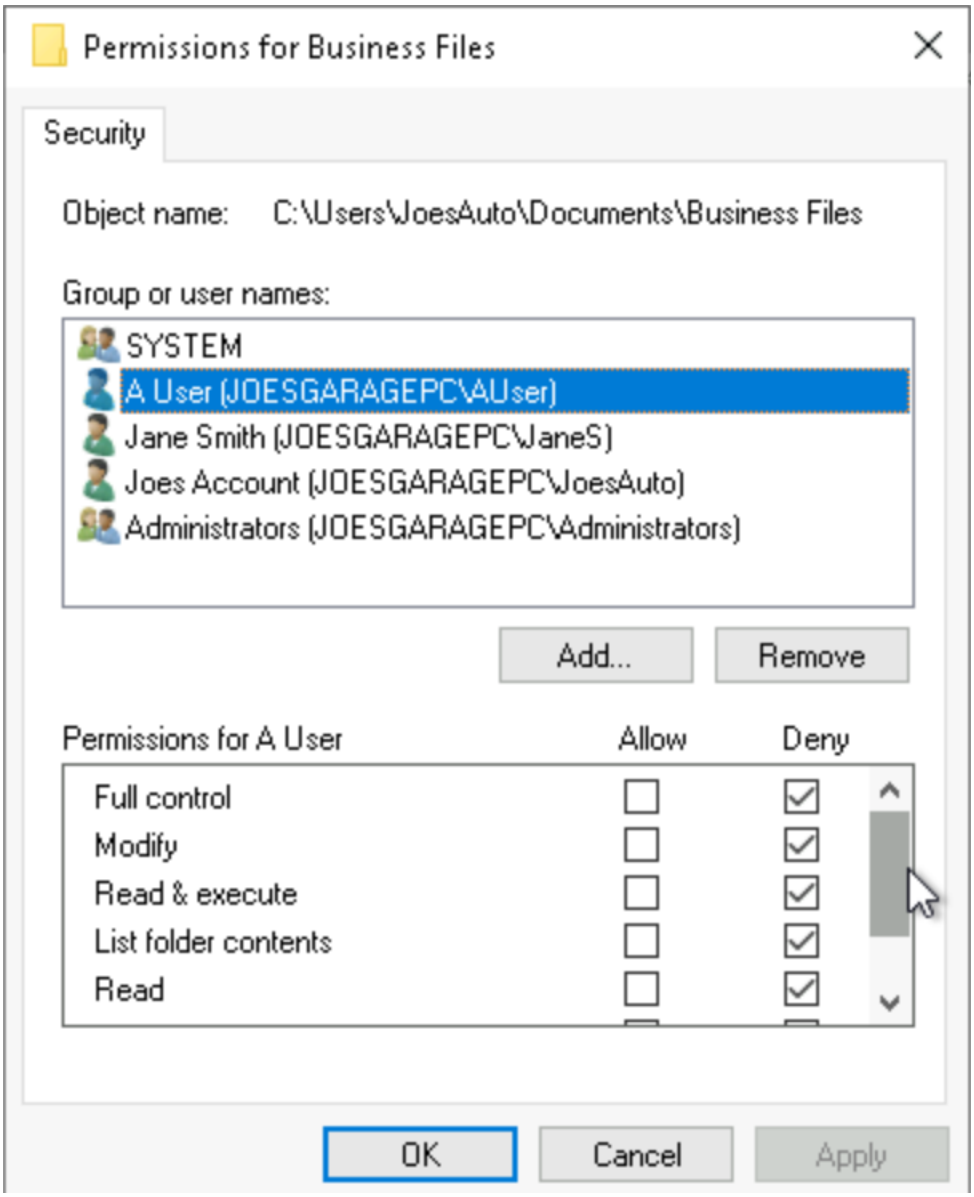
5. Securing Files and Folders

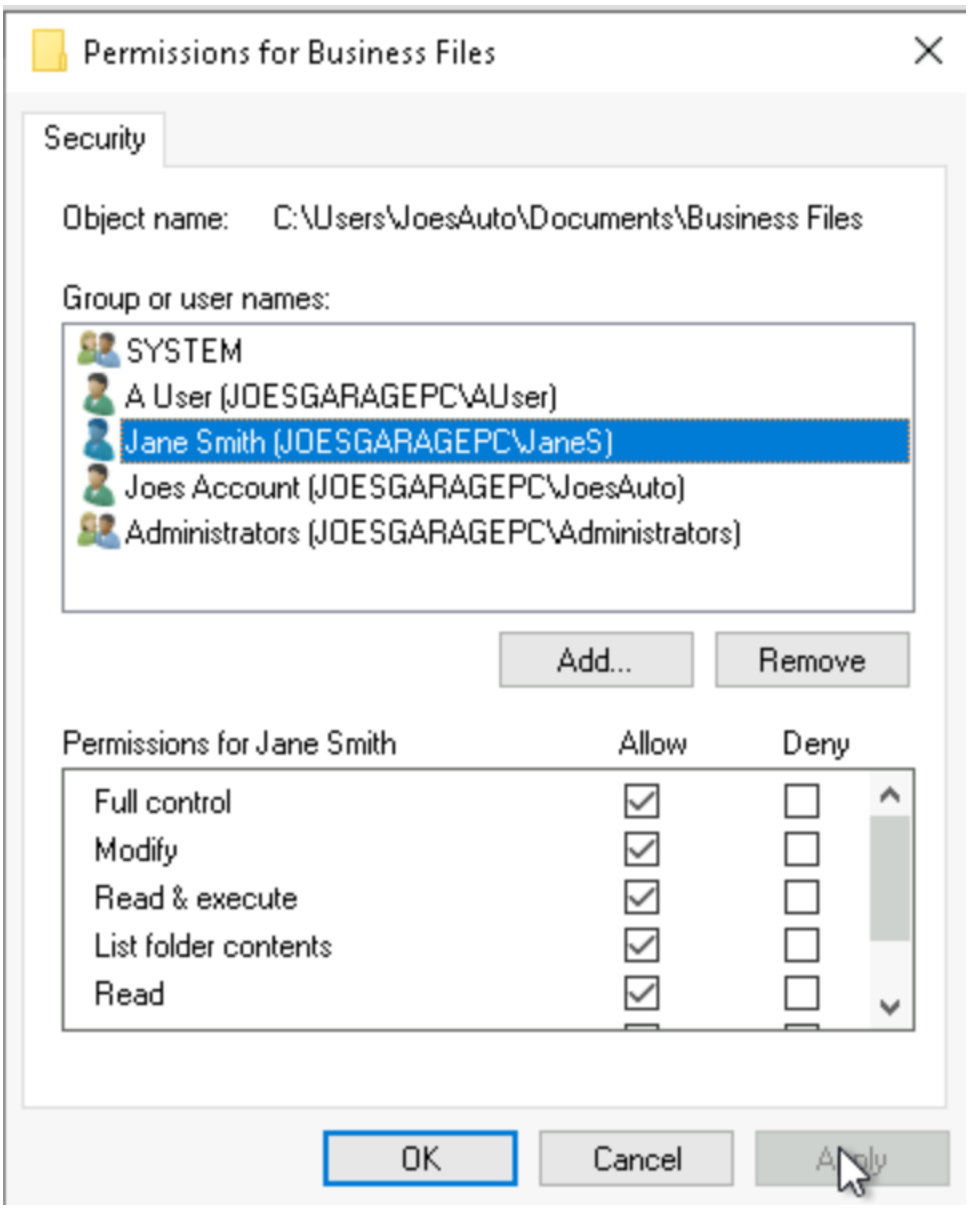
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled “JoesWork.”

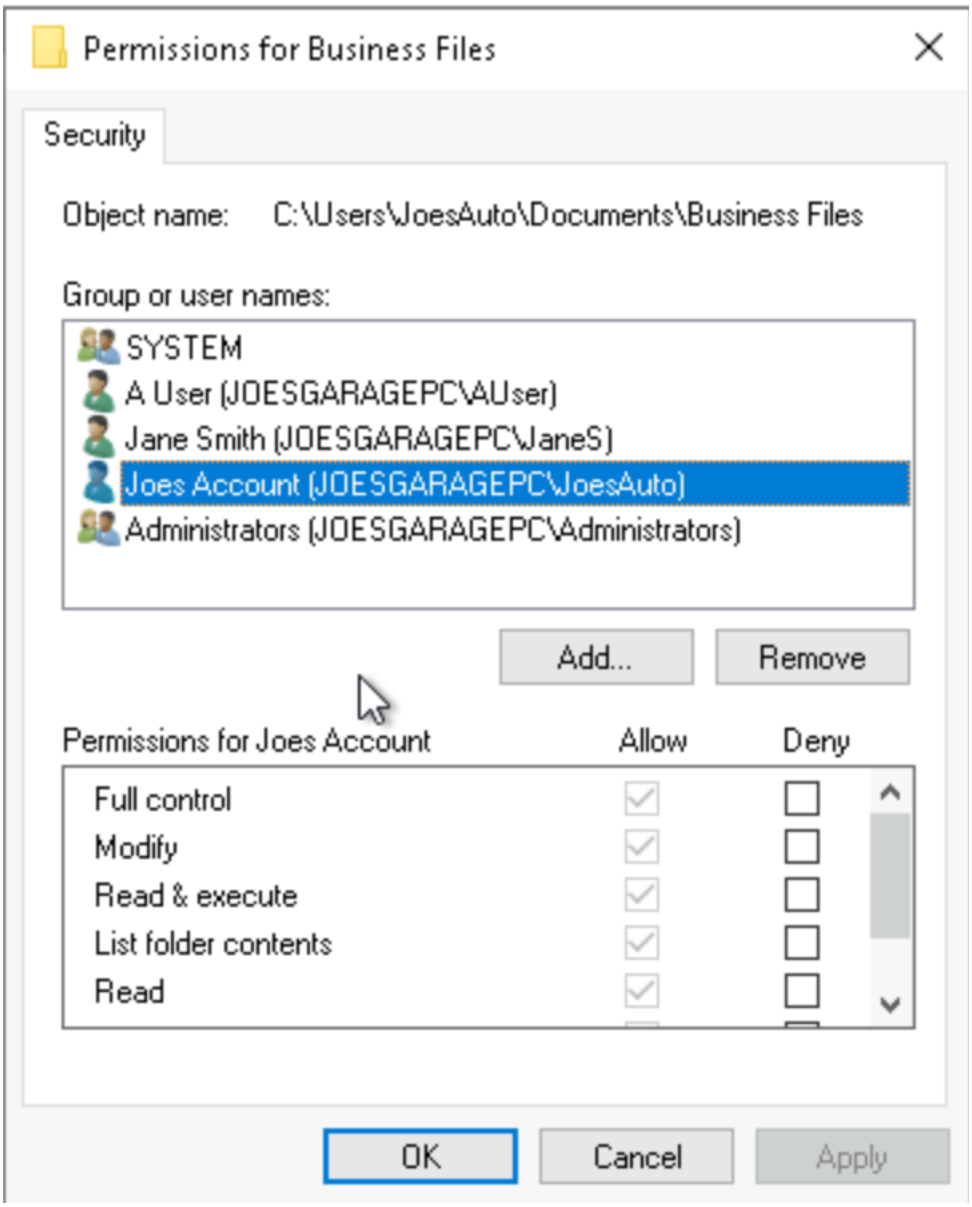
Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

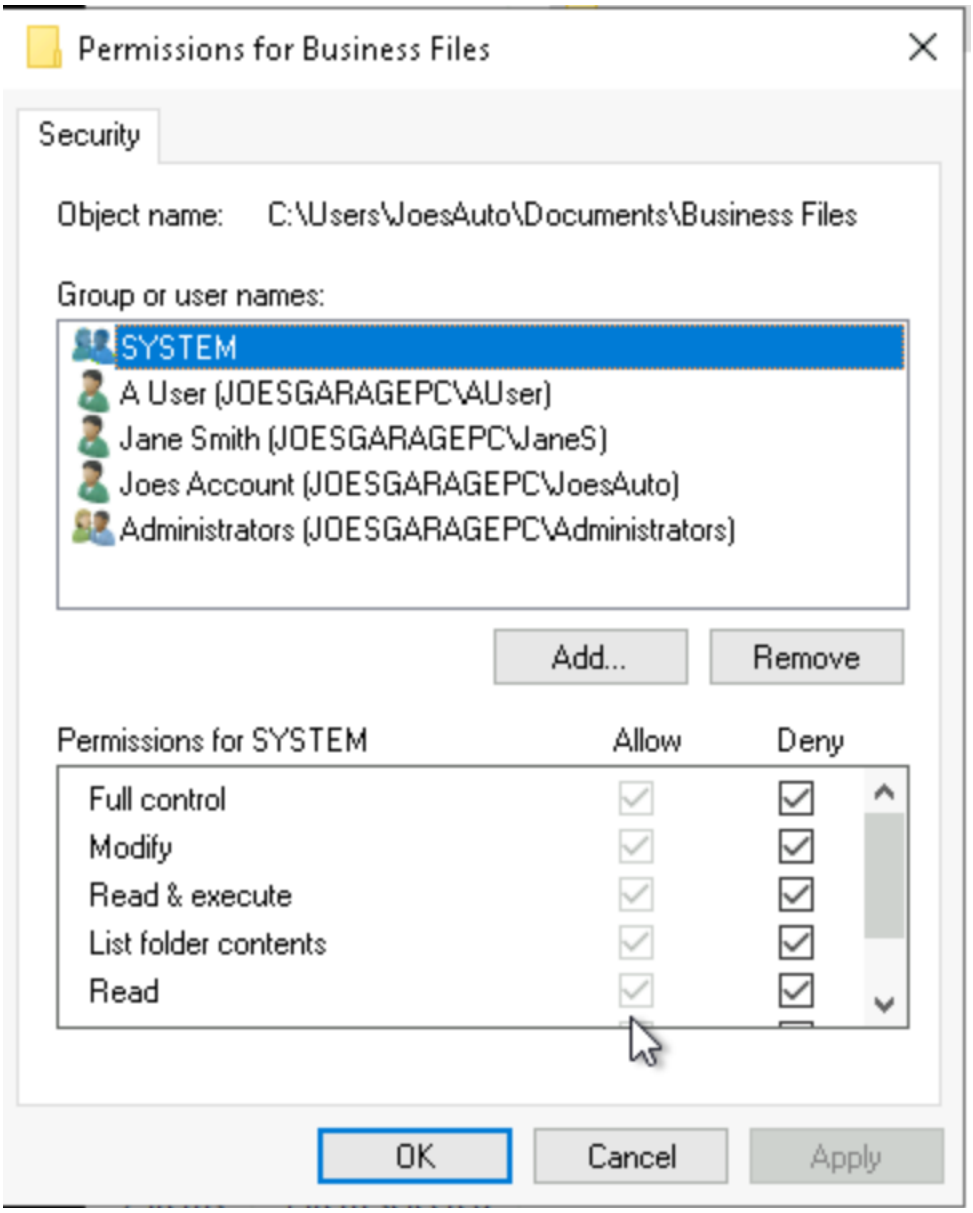
Encrypting files and folders

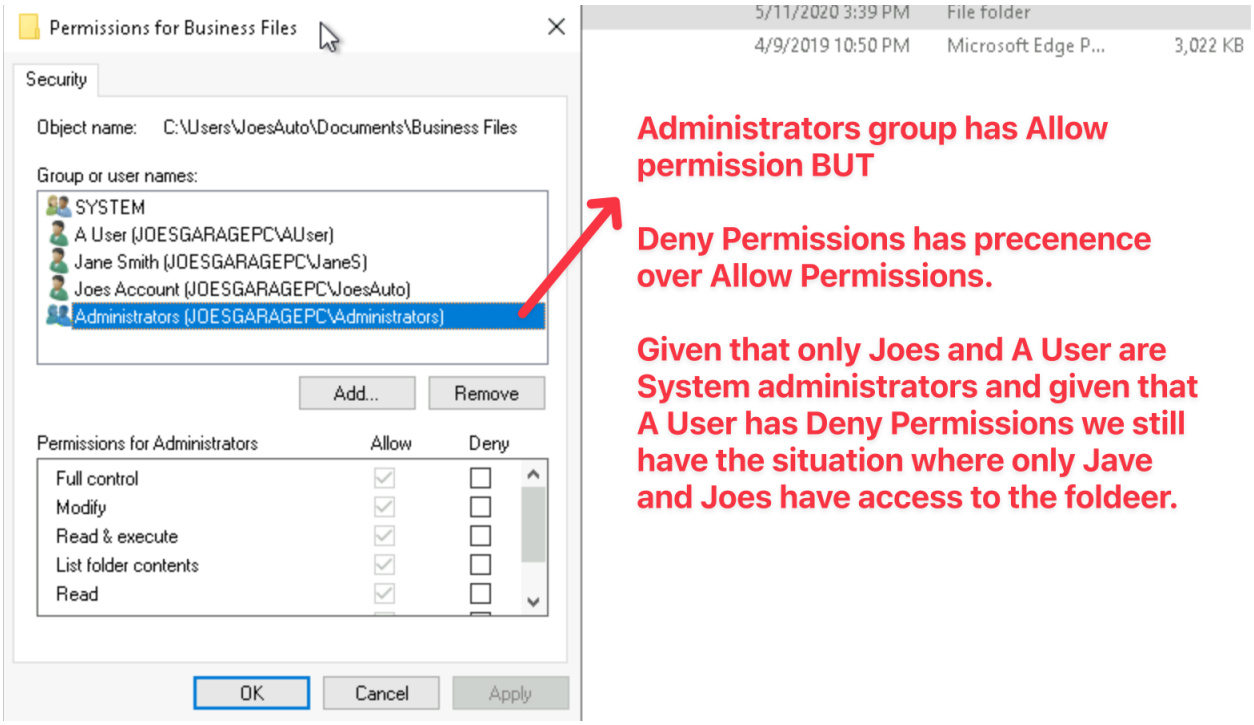
1. *Explain the process for checking this and changing any necessary settings on the file. Include screenshots showing that ONLY Joe and Jane have permissions to change Joe's work files. [Hint: Right-click the folder and select Properties.]*


Permissions for Business Files
Security
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
SYSTEM
A User (JOESGARAGEPC\AUser)
Jane Smith (JOESGARAGEPC\JaneS)
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
Add...
Remove
Permissions for A User
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:
SYSTEM
A User (JOESGARAGEPC\AUser)
Jane Smith (JOESGARAGEPC\JaneS)
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

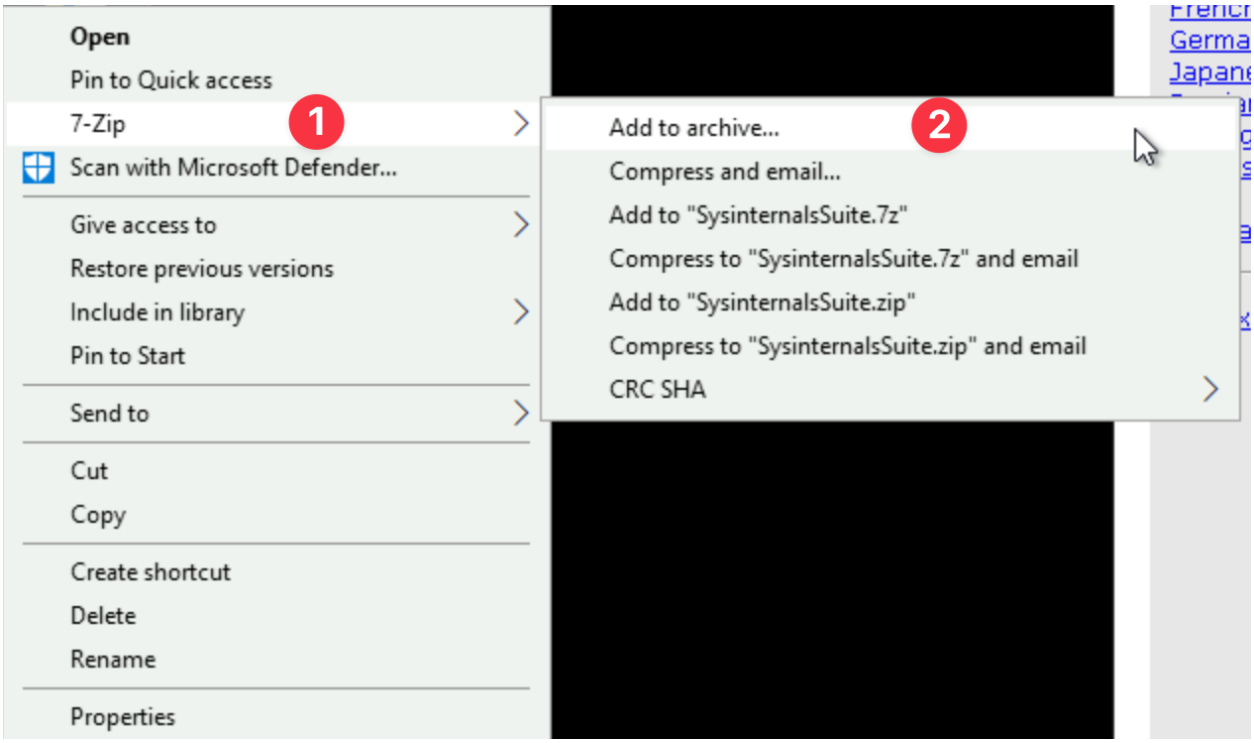

Permissions for Business Files
Security
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
SYSTEM
A User (JOESGARAGEPC\AUser)
Jane Smith (JOESGARAGEPC\JaneS)
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
Add...
Remove
Permissions for Joes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

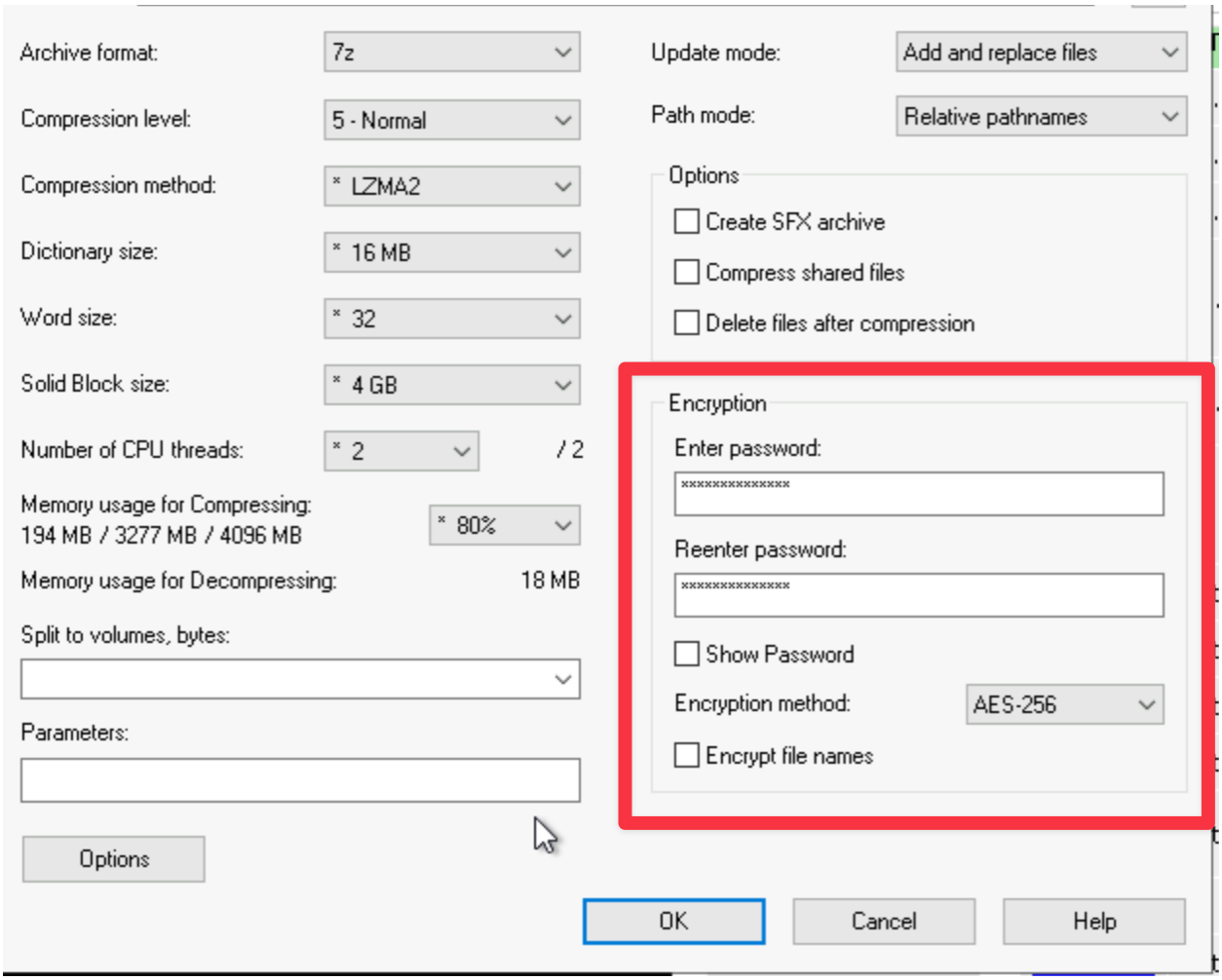

Permissions for Business Files
Security
Object name: C:\Users\JoesAuto\Documents\Business Files
Group or user names:
SYSTEM
A User (JOESGARAGEPC\AUser)
Jane Smith (JOESGARAGEPC\JaneS)
Joes Account (JOESGARAGEPC\JoesAuto)
Administrators (JOESGARAGEPC\Administrators)
Add...
Remove
Permissions for SYSTEM
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.*

   1) Right click on folder to open contextual menu
   2) Go to: 7-Zip -> Add to Archive…
   3) On the window, under Encryption, input the required password twice in order to confirm it. Choose an output directory and then select "OK"
   4) AES-256 is a good algorithm to proceed with. The 256 bits encryption is usually good to empower security.


Open
Pin to Quick access
7-Zip
1
Scan with Microsoft Defender...
Give access to
Restore previous versions
Include in library
Pin to Start
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Add to archive...
2
Compress and email...
Add to "SysinternalsSuite.7z"
Compress to "SysinternalsSuite.7z" and email
Add to "SysinternalsSuite.zip"
Compress to "SysinternalsSuite.zip" and email
CRC SHA



3. *What security fundamentals does this provide?*

   ***Confidentiality**: Encryption ensures that only authorized users with the correct decryption key can access the content of the documents, protecting them from unauthorized access.*

   ***Data Integrity**: By encrypting documents, any unauthorized alterations to the data can be detected, as decryption would fail if the content is tampered with.*

   ***Data Protection**: Encryption safeguards sensitive information, both at rest and in transit, reducing the risk of data breaches.*

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

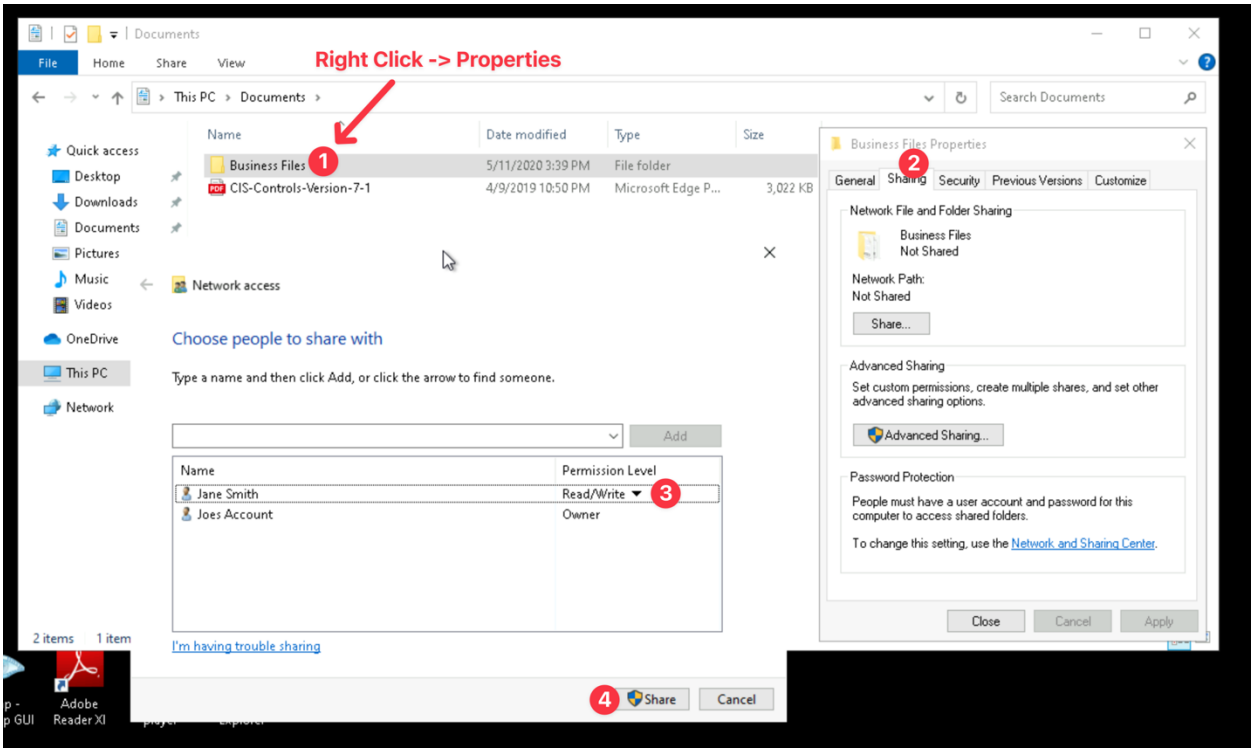
   *Encryption of sensitive documents fulfills **CIS Control 13: Data Protection**. This control focuses on*

the protection of sensitive data through measures such as encryption, ensuring that data remains secure whether it is stored, processed, or transmitted.

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.*



6. 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.