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: Wiam Almokhtar

Date of completion: 16/10/2022

Resubmission: 17/10/2022

Resubmission for feedback on: securing access – user accounts- question 10

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.*

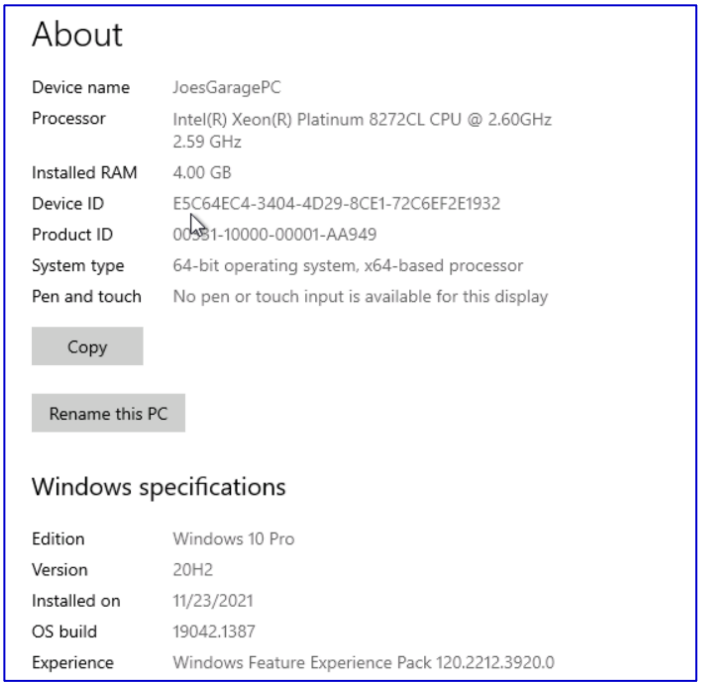
Device Name	JoesGaragePC
Processor	Intel® Xeon® Platinum 8272CL CPU @ 2.60GHz
Install RAM	4.00 GB
System Type	64-bit
Windows Edition	Windows 10 Pro
Version	20H2
Installed on	11/23/2021
OS build	19042.1387

2. *Explain how you found this information:*

   I obtained the information using 2 ways:

   1- Search 'system information' > Enter> System Summary
   2- Windows> Settings> System> About

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



About

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

Windows specifications

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

Software

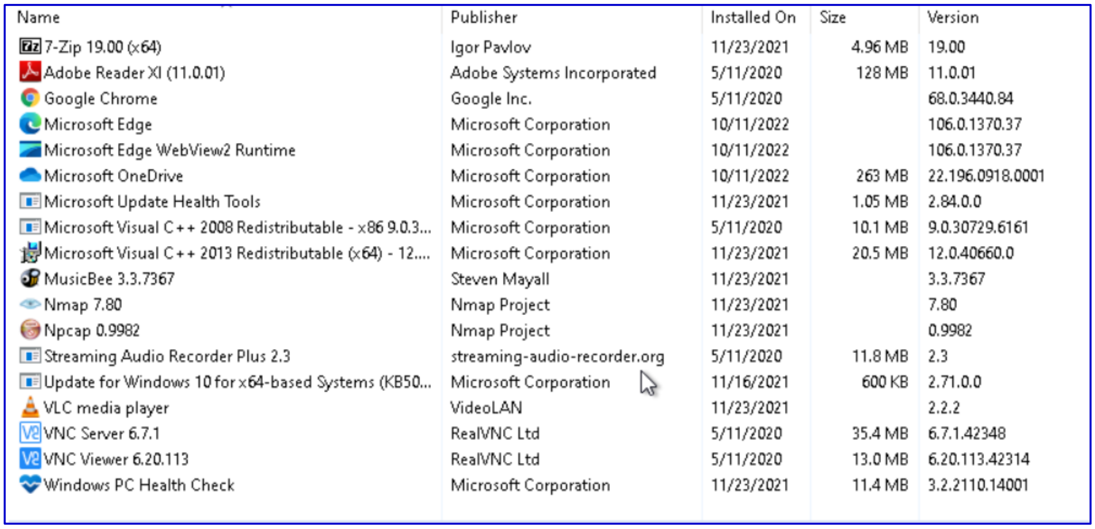
Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.

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

- 7-Zip
- Adobe Reader XI
- Google Chrome
- Microsoft Edge
- Nmap

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

   Control panel > programs > programs and feature



Name	Publisher	Installed On	Size	Version
7-Zip 19.00 (x64)	Igor Pavlov	11/23/2021	4.96 MB	19.00
Adobe Reader XI (11.0.01)	Adobe Systems Incorporated	5/11/2020	128 MB	11.0.01
Google Chrome	Google Inc.	5/11/2020		68.0.3440.84
Microsoft Edge	Microsoft Corporation	10/11/2022		106.0.1370.37
Microsoft Edge WebView2 Runtime	Microsoft Corporation	10/11/2022		106.0.1370.37
Microsoft OneDrive	Microsoft Corporation	10/11/2022	263 MB	22.196.0918.0001
Microsoft Update Health Tools	Microsoft Corporation	11/23/2021	1.05 MB	2.84.0.0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	5/11/2020	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x64) - 12....	Microsoft Corporation	11/23/2021	20.5 MB	12.0.40660.0
MusicBee 3.3.7367	Steven Mayall	11/23/2021		3.3.7367
Nmap 7.80	Nmap Project	11/23/2021		7.80
Npcap 0.9982	Nmap Project	11/23/2021		0.9982
Streaming Audio Recorder Plus 2.3	streaming-audio-recorder.org	5/11/2020	11.8 MB	2.3
Update for Windows 10 for x64-based Systems (KB50...	Microsoft Corporation	11/16/2021	600 KB	2.71.0.0
VLC media player	VideoLAN	11/23/2021		2.2.2
VNC Server 6.7.1	RealVNC Ltd	5/11/2020	35.4 MB	6.7.1.42348
VNC Viewer 6.20.113	RealVNC Ltd	5/11/2020	13.0 MB	6.20.113.42314
Windows PC Health Check	Microsoft Corporation	11/23/2021	11.4 MB	3.2.2110.14001

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

   Inventory and Control of Software Assets

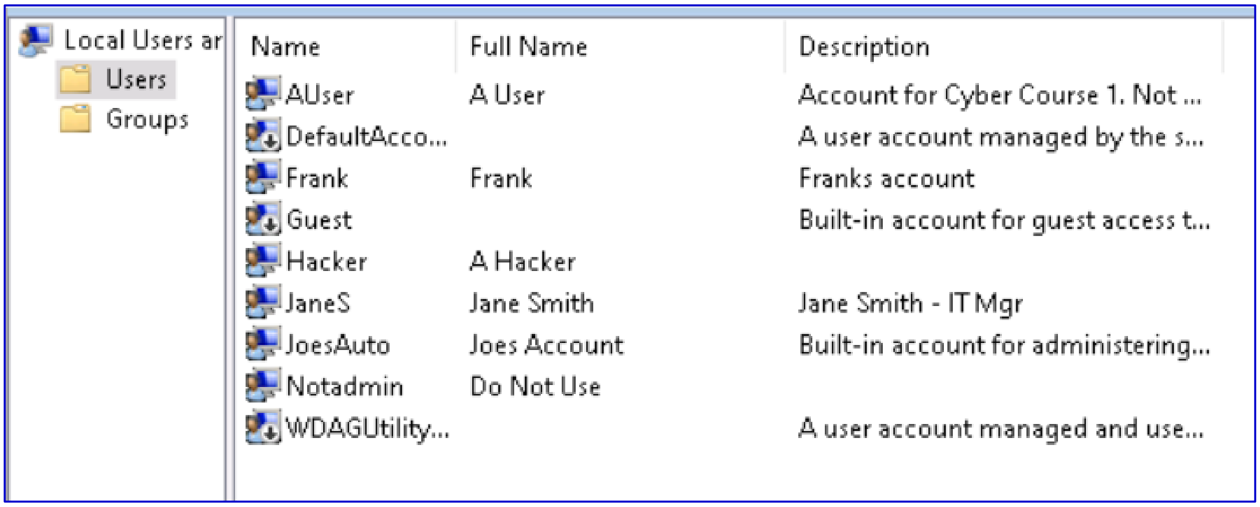
Accounts

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
JoesAuto	Joes Account	Administrator
A User	A User	Standard
Hacker	A Hacker	Administrator
Notadmin	Do Not Use	Administrator
Frank	Frank	Standard
JaneS	Jane Smith	Administrator
DefaultAccount	-	-
WDAGUtilityAccount	-	-
Guest	-	Guest

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

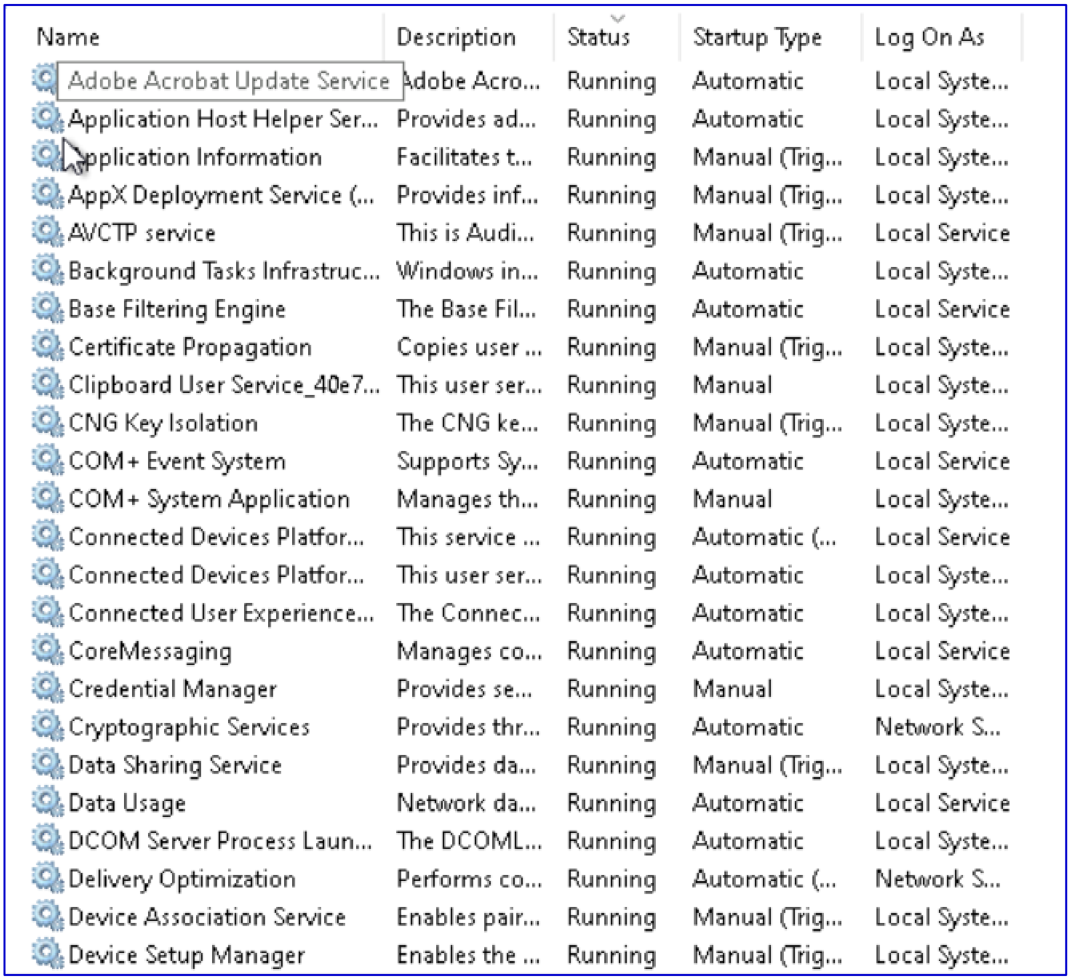


Name	Full Name	Description
AUser	A User	Account for Cyber Course 1. Not ...
DefaultAcco...		A user account managed by the s...
Frank	Frank	Franks account
Guest		Built-in account for guest access t...
Hacker	A Hacker	
JaneS	Jane Smith	Jane Smith - IT Mgr
JoesAuto	Joes Account	Built-in account for administering...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

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.*

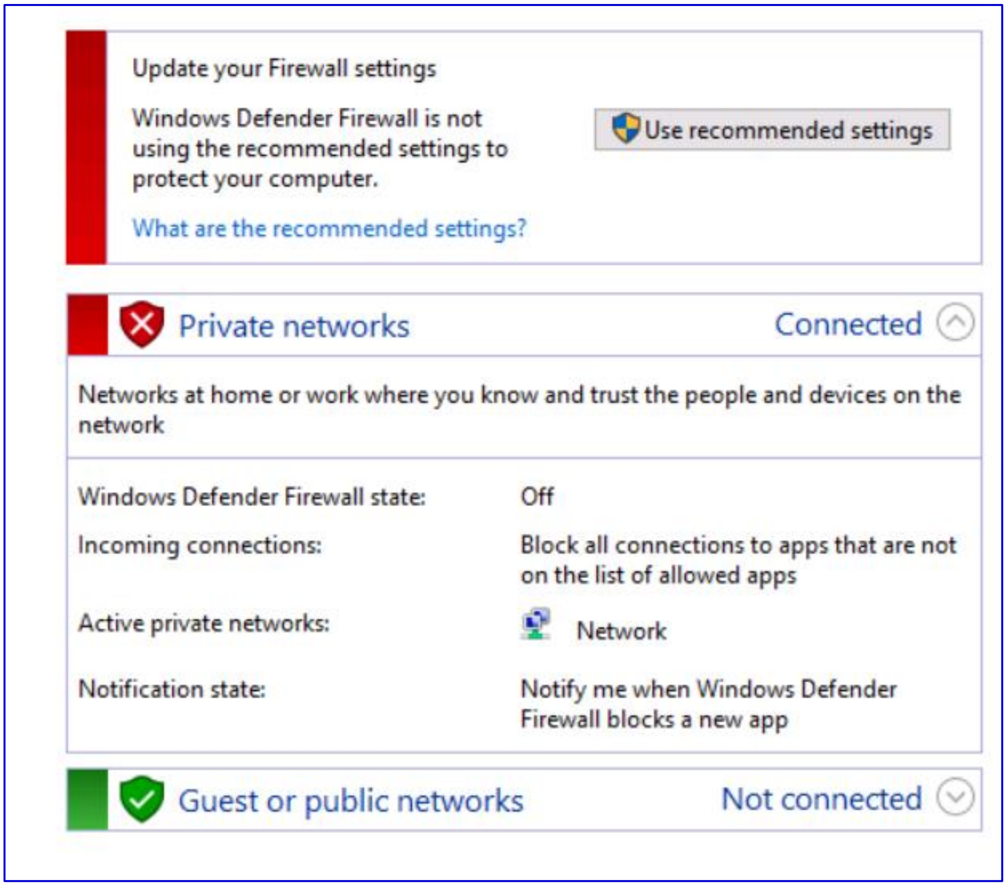


Name	Description	Status	Startup Type	Log On As
Adobe Acrobat Update Service	Adobe Acro...	Running	Automatic	Local Syste...
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Local Syste...
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Local Syste...
Clipboard User Service_40e7...	This user ser...	Running	Manual	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (...	Local Service
Connected Devices Platfor...	This user ser...	Running	Automatic	Local Syste...
Connected User Experience...	The Connec...	Running	Automatic	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
Data Sharing Service	Provides da...	Running	Manual (Trig...	Local Syste...
Data Usage	Network da...	Running	Automatic	Local Service
DCOM Server Process Laun...	The DCOML...	Running	Automatic	Local Syste...
Delivery Optimization	Performs co...	Running	Automatic (...	Network S...
Device Association Service	Enables pair...	Running	Manual (Trig...	Local Syste...
Device Setup Manager	Enables the ...	Running	Manual (Trig...	Local Syste...

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:*



Update your Firewall settings

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

What are the recommended settings?

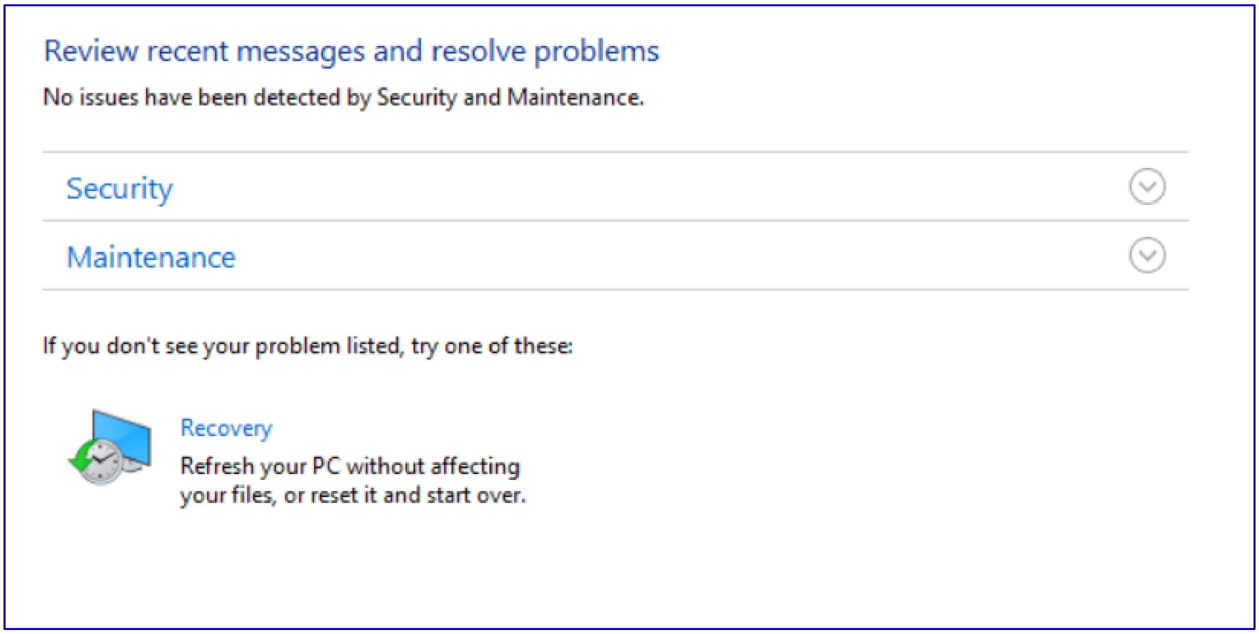
Private networks — Connected

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

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



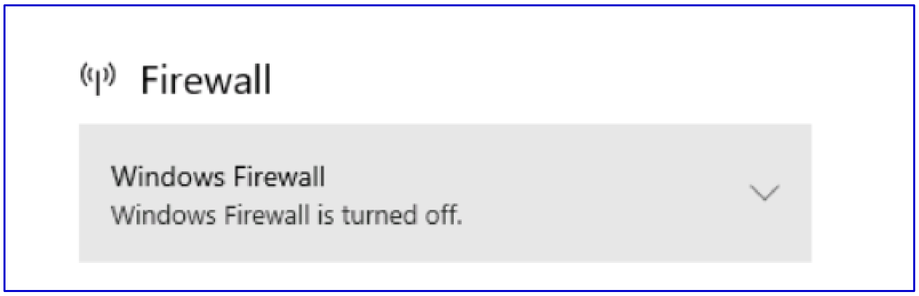
Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

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

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

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

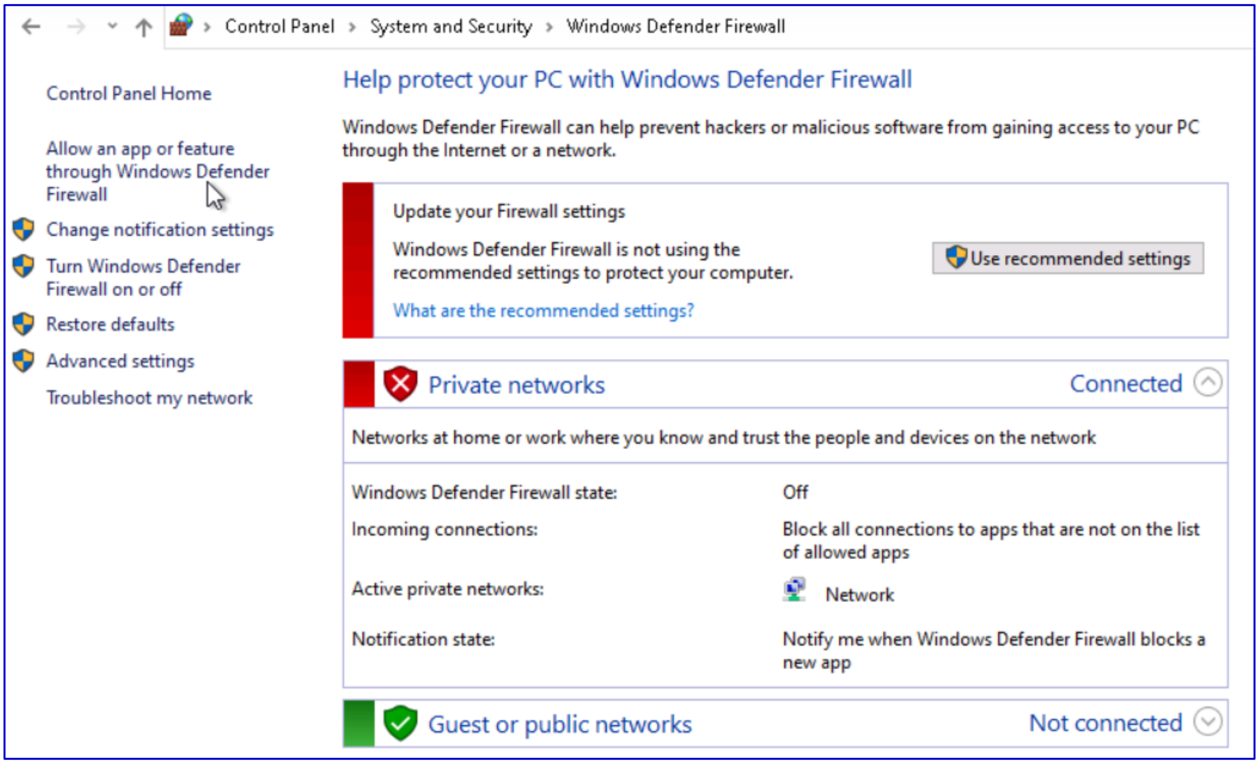


Firewall

Windows Firewall

Windows Firewall is turned off.

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


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
Use recommended settings

Help protect your PC with Windows Defender Firewall

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

Update your Firewall settings

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

What are the recommended settings?

Private networks — Connected

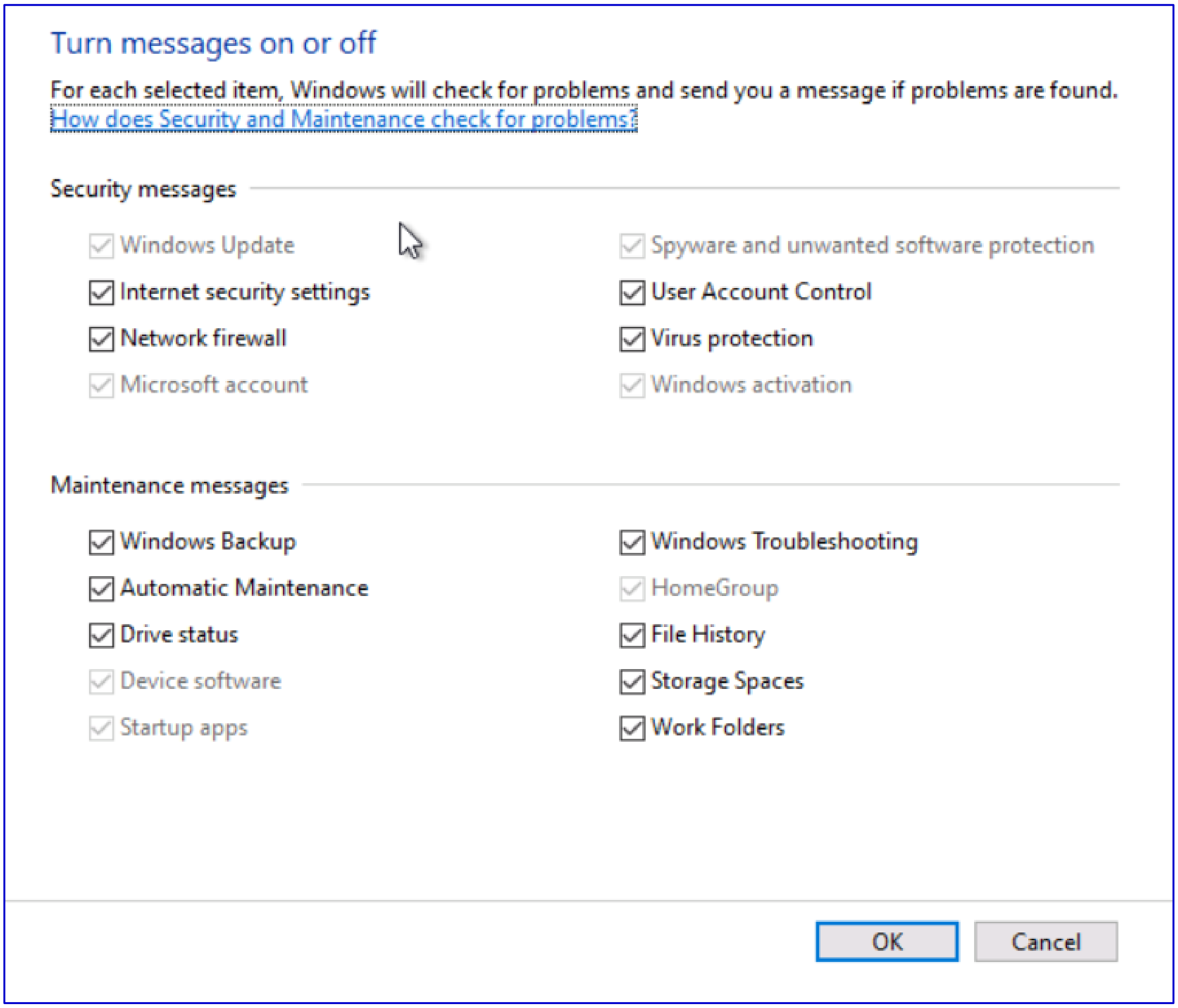
Networks at home or work where you know and trust the people and devices on the network

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

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:



Turn messages on or off

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

Security messages

☑ Windows Update
☑ Internet security settings
☑ Network firewall
☑ Microsoft account

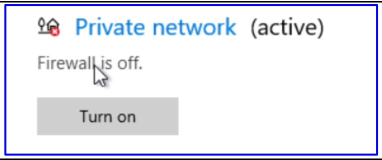
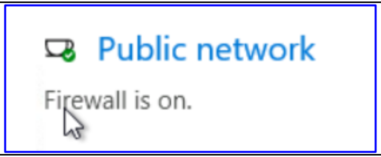
☑ Spyware and unwanted software protection
☑ User Account Control
☑ Virus protection
☑ Windows activation

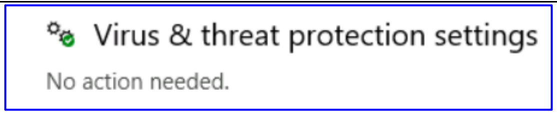
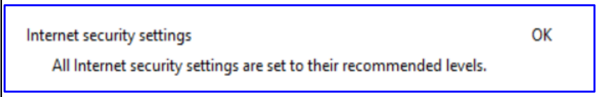
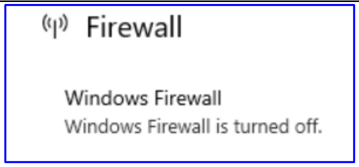
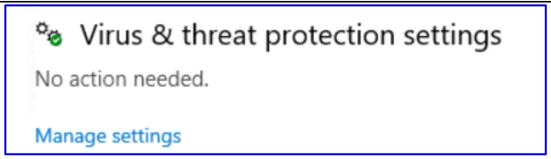
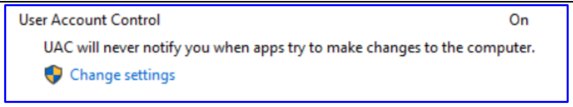
Maintenance messages

☑ Windows Backup
☑ Automatic Maintenance
☑ Drive status
☑ Device software
☑ Startup apps

☑ Windows Troubleshooting
☑ HomeGroup
☑ File History
☑ Storage Spaces
☑ Work Folders

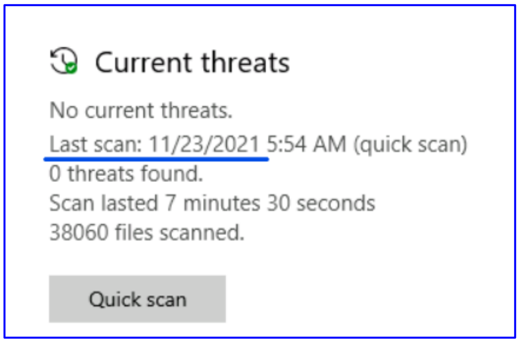
6. *Document the status of the PC's security settings listed below. Include the process you used to determine this information along with any screenshots. At this point, you are only documenting what you find. Do not make changes (yet).*

Security Feature	Status	Process used	Screenshot
Firewall product and status – Private network	off	Setting> updates &privacy> windows security> firewall & network protection	 Private network (active) Firewall is off.
Firewall product and status – Public network	on	Setting> updates &privacy> windows security> firewall & network protection	 Public network Firewall is on.

Virus protection product and status	No action needed	Setting> updates &privacy> windows security> virus & threat protection	 Virus & threat protection settings No action needed.
Internet Security messages	OK	Control panel > system and security> security and maintenance> expand security tap	 Internet security settings OK All Internet security settings are set to their recommended levels.
Network firewall messages	Windows Firewall is turned off	Control panel > system and security> security and maintenance> expand security tap> click view in windows security	 Firewall Windows Firewall Windows Firewall is turned off.
Virus protection messages	No action needed	Setting> updates &privacy> windows security> virus & threat protection	 Virus & threat protection settings No action needed. Manage settings
User Account Control Setting	On but no notification when apps try to make changes	Control panel > system and security> security and maintenance> expand security tap	 User Account Control On UAC will never notify you when apps try to make changes to the computer. Change settings

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 turned off on private network and that could cause attacks from the internet by unauthorized access on network traffic.
- A malicious app may try to make changes to the computer and no notification will be sent.
- The last scan happened a long time ago, so new undiscovered threats may be present.



Current threats

No current threats.
Last scan: 11/23/2021 5:54 AM (quick scan)
0 threats found.
Scan lasted 7 minutes 30 seconds
38060 files scanned.

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?*
   NIST because it provides many guidelines and recommendations for computer security.
2. *What industry baseline do you recommend to Joe?*
   [Hint: Look in the documents folder]

   CIS because it provides easy-to-implement and well-defined steps that could be followed to ensure the security of the system.

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?

   CIS Critical Security Control 2: Inventory and Control of Software Assets

   Because we're managing everything on the network.

System and Security

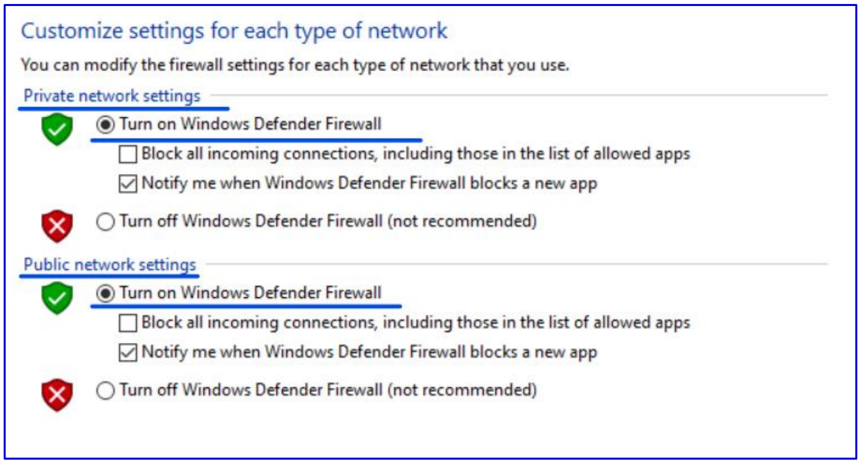
At this point, you need to enable security services for this PC. Pick at least 3 of the following 5 areas to secure in order to satisfactorily meeting the project requirements:

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

Firewall (chosen)

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

1. *Explain the process you take to do this.*
   Windows search> windows defender firewall> enter> Turn windows defender firewall on or off
2. *Include screenshots showing the firewall is turned on*



Customize settings for each type of network

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

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

.

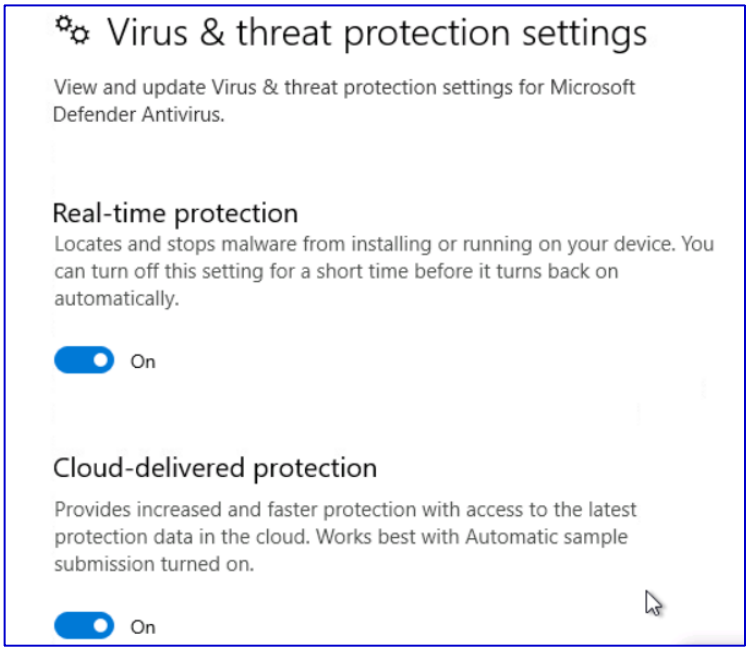
3. *What protection does this provide?*

   Network protection. It prevents malicious websites from harming computer system through the network

Virus & Threat Protection (chosen)

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.*
   Setting> updates &privacy> windows security> virus & threat protection
2. *Include screenshots to confirm that anti-virus is enabled.*



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

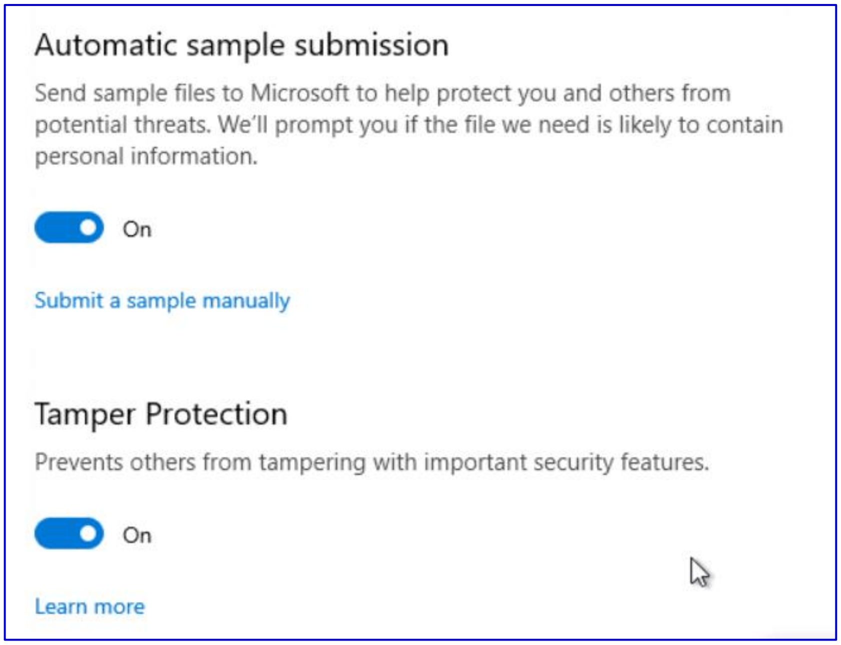
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

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

Tamper Protection

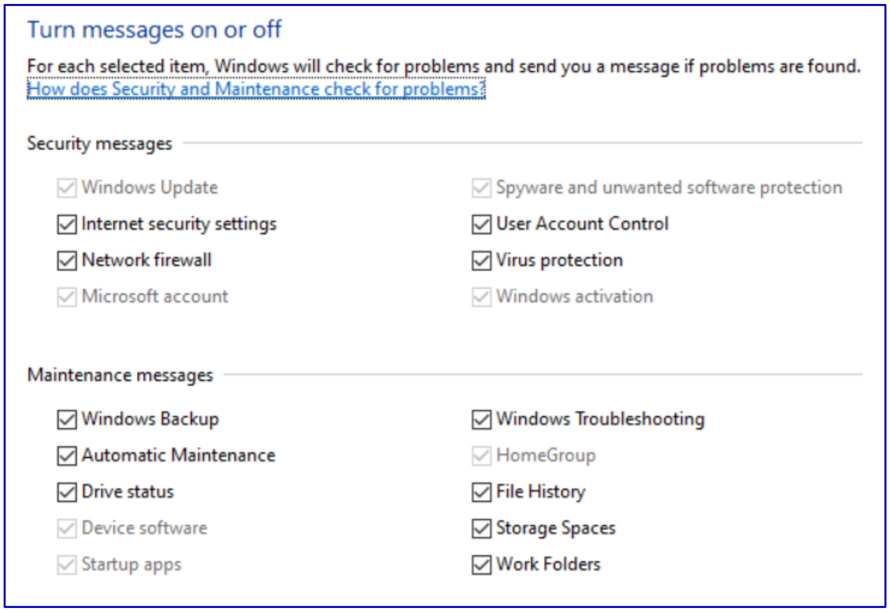
Prevents others from tampering with important security features.

● On

Learn more

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.*



Turn messages on or off

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

Security messages

☑ Windows Update
☑ Internet security settings
☑ Network firewall
☑ Microsoft account

☑ Spyware and unwanted software protection
☑ User Account Control
☑ Virus protection
☑ Windows activation

Maintenance messages

☑ Windows Backup
☑ Automatic Maintenance
☑ Drive status
☑ Device software
☑ Startup apps

☑ Windows Troubleshooting
☑ HomeGroup
☑ File History
☑ Storage Spaces
☑ Work Folders

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

- Virus protection: any apps or files containing a signature of a known virus will be blocked and the user will be alerted of their existence
- Firewall: Attempts of attacks from malicious websites on the network will be blocked.

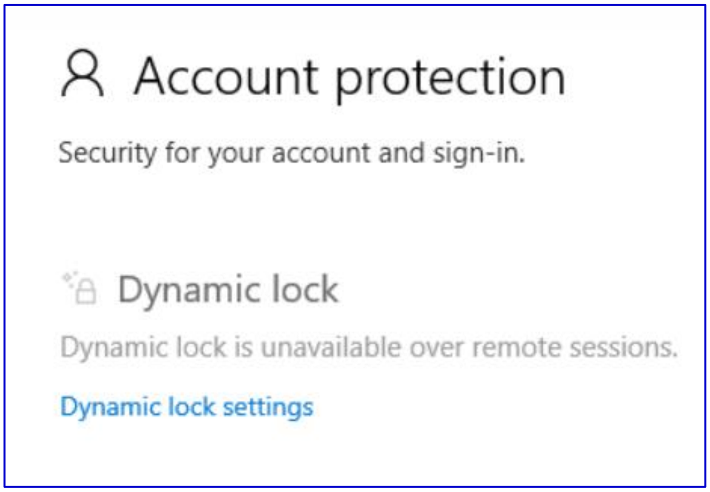
4. *From the CIS baseline controls, provide the controls satisfied by completing this.*

   - Inventory and Control of Software Assets: through turning on firewall
   - Malware Defenses: through virus scan
   - Application Software Security: through virus scan

App & Browser Control (chosen)

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.*



Account protection

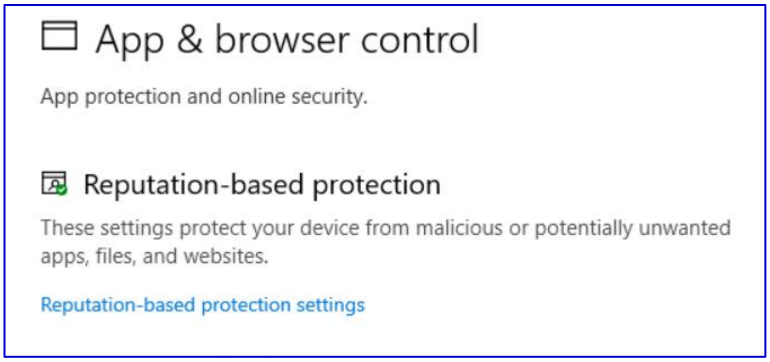
Security for your account and sign-in.

Dynamic lock

Dynamic lock is unavailable over remote sessions.

Dynamic lock settings

I believe that Joe can use the Dynamic Lock feature if he tends to walk around the shop and forgets to lock his PC. This will lock it automatically to prevent any tampering.



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

I turned on the settings for reputation-based protection to further enhance the security of Joe's PC by blocking any app that is known to be malicious.

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.

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

Securing Removable Media

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

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

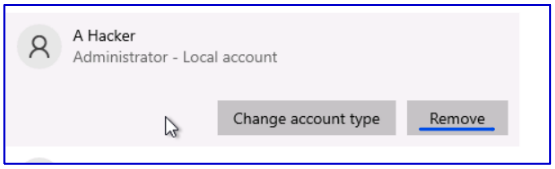
- JoesAuto
- Jane Smith (Joe’s assistant)
- A User - Used for exercises (Not used in this project)
- Notadmin - Built-in administrator account (Not used for this project)
- Windows built-in accounts: Guest, DefaultAccount, and WDAGUtility (Not used for this project)

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 and Hacker
2. *Bonus questions: What is Hacker’s password?*
3. *Explain the steps you take to disable or remove unwanted accounts.*
   Settings> accounts> other users> Add, edit, or remove other users> click on the user> click remove



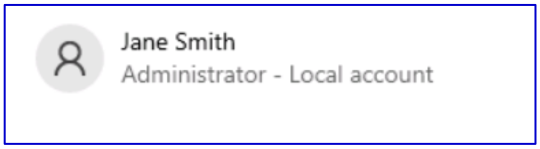
4. *Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.*

    - If they can be accessed remotely, that means the user might still have access to the PC and can perform malicious tasks or just consume resources.
    - If unneeded accounts are not checked frequently that means an attacker gains access to them and it won’t be noticed. The attacker can then snoop on activities to perform a larger attack on the system.

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?
   Any account other than joe's and A User's accounts
6. Explain how you determined this. Provide screenshots as needed.

   Who should have admin rights is determined according to Joe's access rules.
   Jane smith has administrator rights when she shouldn't, this can be seen from:
   settings> accounts> other users



Jane Smith
Administrator - Local account

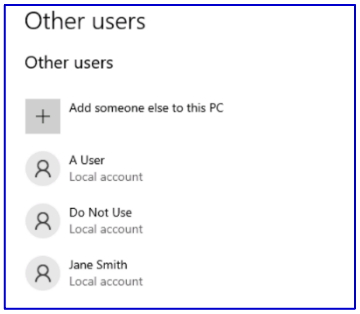
Administrator privileges for too many users are another security challenge.

7. Provide at least three risks associated with users having administrator rights on a PC.
   If many users have administrator rights, the following changes can occur frequently which will make the system harder to manage and be kept safe.

- Installing software that can harm the system
- Deleting or modifying important files
- Adding unnecessary users to the system

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.*
   settings> accounts> other users> add someone else to this pc> settings> accounts> (lusrmgr[local users and groups]) window> click user>double click on Jane S> click on member of tab> click on administrator> click remove
   or settings> accounts> other users>change account type> change to local account
   now Jane doesn't have access rights



Other users

Other users

+ Add someone else to this PC

A User
Local account

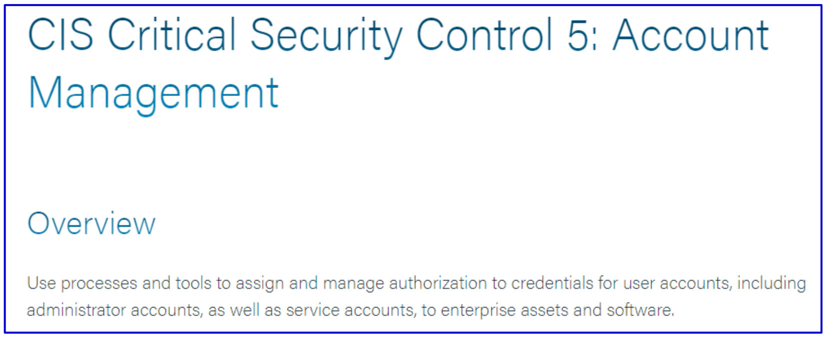
Do Not Use
Local account

Jane Smith
Local account

9. *What is the security principle behind this?*
   Least privilege principle. Jane can perform her assistance-related tasks without admin rights, so she shouldn't have admin rights.
10. The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?

Account management step

I was given feedback regarding this answer and a hint that says it’s step 4.
I did some research to correct my answer and I found that CIS version 7 has step 4 as “ Controlled Use of Administrative privileges”.
However, CIS version 8 does not have that step but has step 5 as “Account management step” which has a similar purpose as shown in the following image.



CIS Critical Security Control 5: Account Management

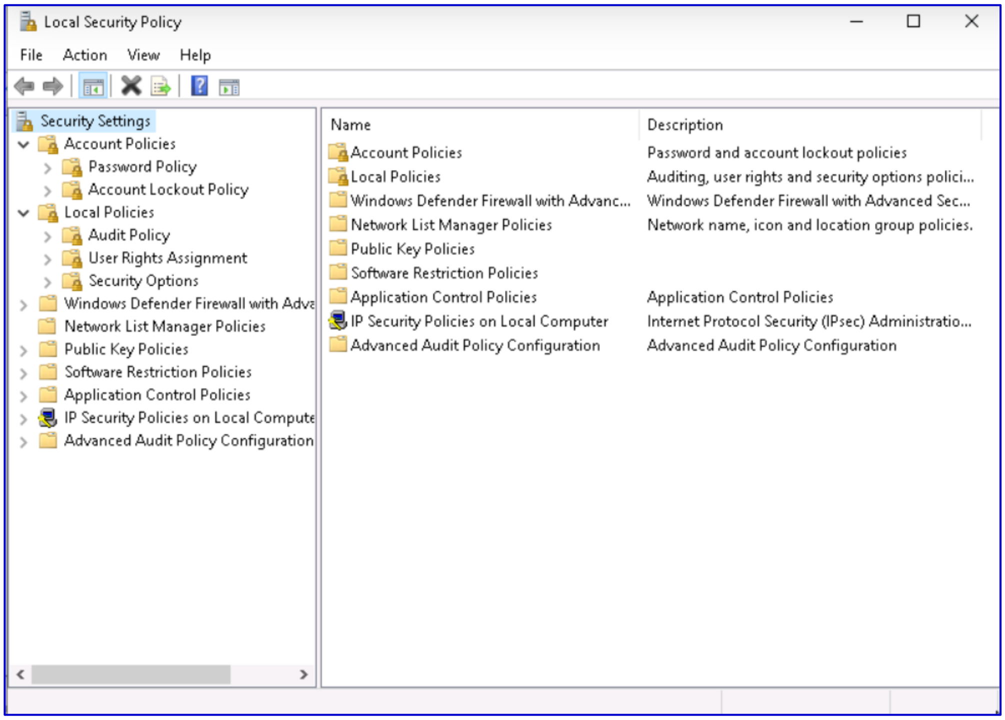
Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

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.*

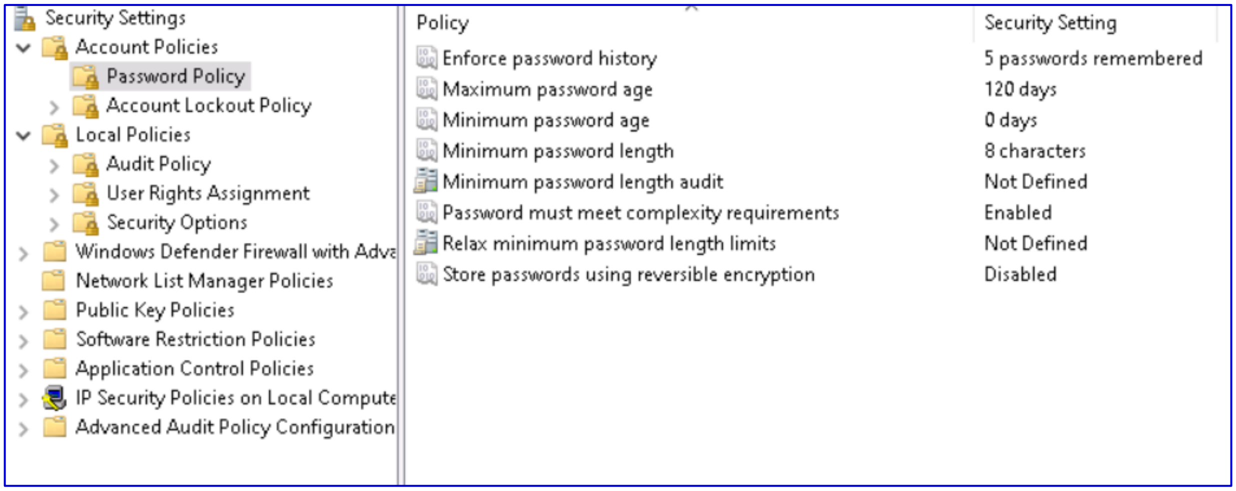


- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

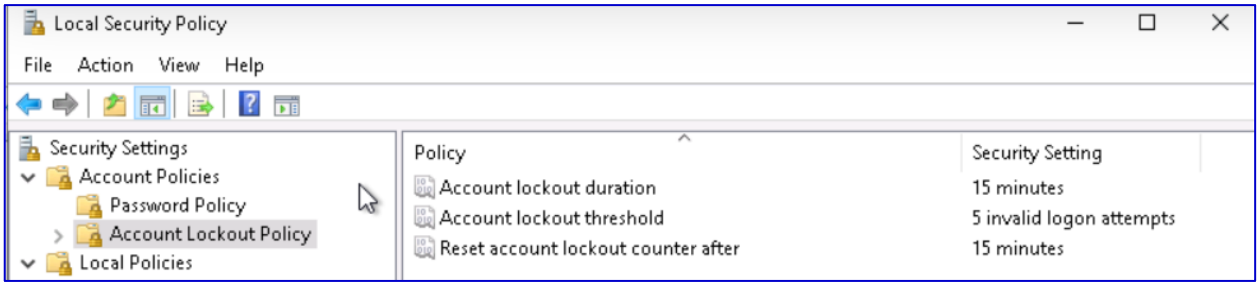
[Note: Local Security Policy is not available on Windows 10 Home edition.]

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:
     change the required fields in Password Policy


Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	5 passwords remembered
Maximum password age	120 days
Minimum password age	0 days
Minimum password length	8 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

   - Setting the Account Lockout Policy:
     change the required fields in Account Lockout Policy



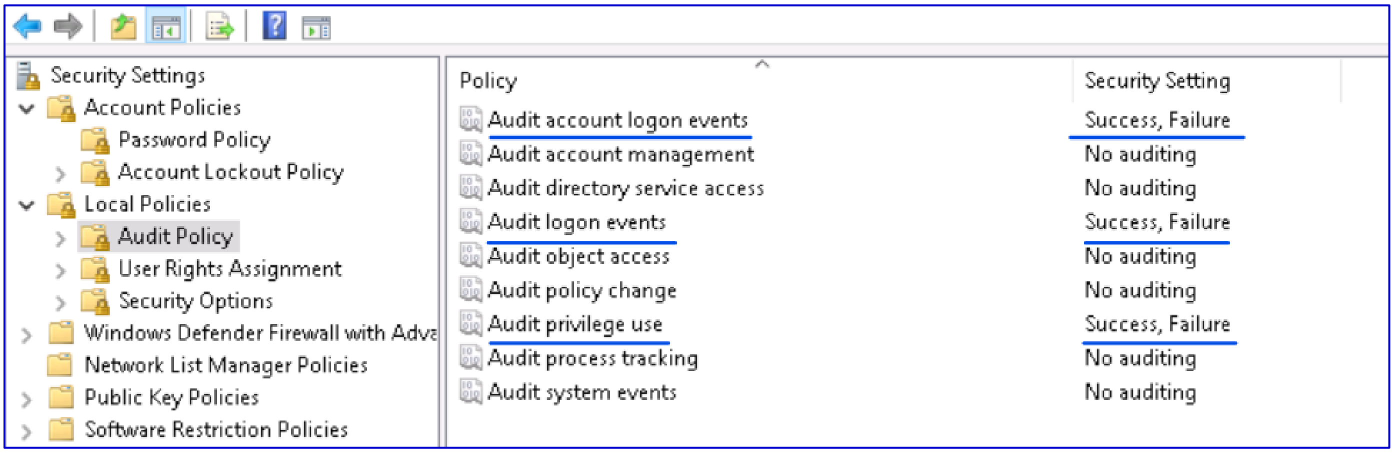
Policy	Security Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

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.



Security Settings
- Account Policies
  - Password Policy
  - Account Lockout Policy
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Defender Firewall with Adva
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	No auditing

4. Securing Applications

As part of the inventory process, you determined computer programs or applications on the PC. The next step is to decide which ones are needed for business and which ones should be removed. Unneeded programs could be vulnerable to attacks and allow unauthorized access into the computer. They also consume system resources and could also violate licensing agreements.

Joe has established the following rules regarding PC applications:

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

Remove unneeded or unwanted applications

1. *List at least three application(s) that violate this policy.*

- Candy crush friends
- Farm heroes saga
- MusicBee

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

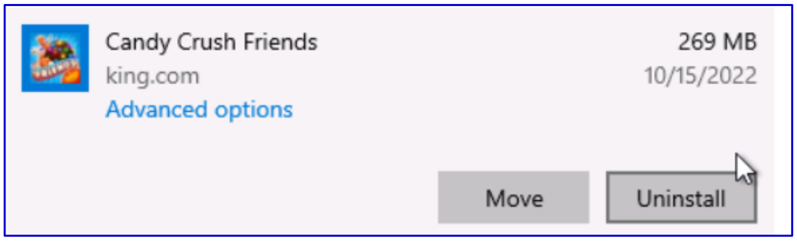
- They could be installed from an unsafe source
- They may not be used often so they’re not updated which makes them vulnerable to attacks
- They consume computer resources such as CPU and memory which are needed to perform tasks. The more unnecessary apps there are, the higher the possibility that the system will crash due to the lack of resources.

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.*

Settings>apps> Apps& Features > select app > click remove

Or

Control Panel> programs> click on program> click uninstall (this doesn't show all apps)

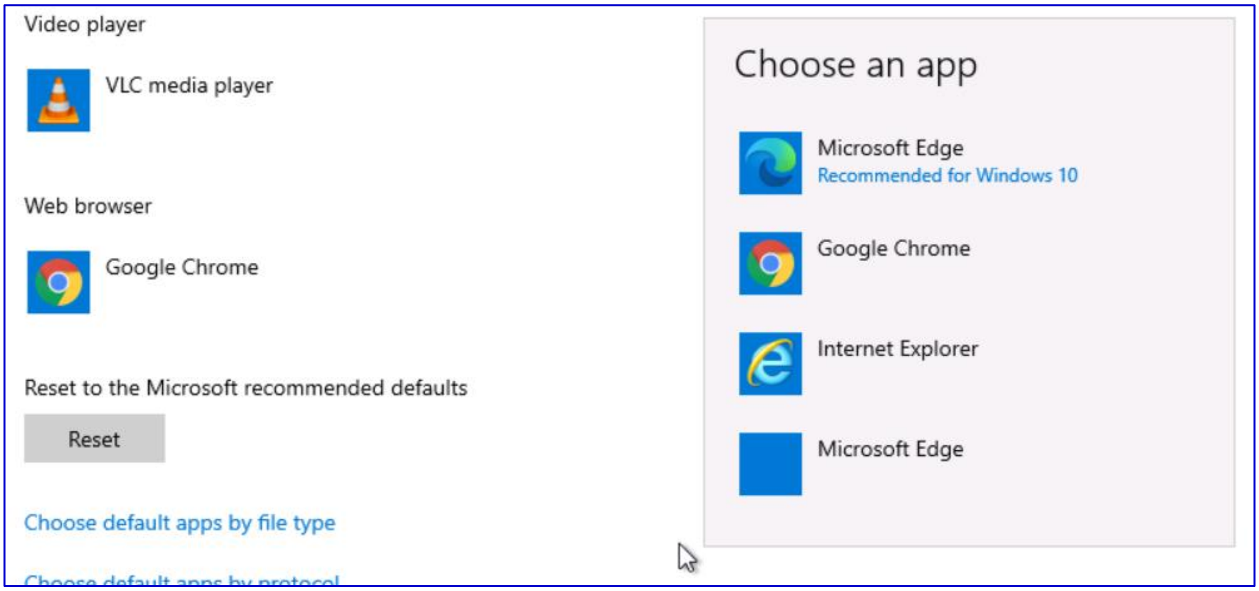


Default Browser

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.*

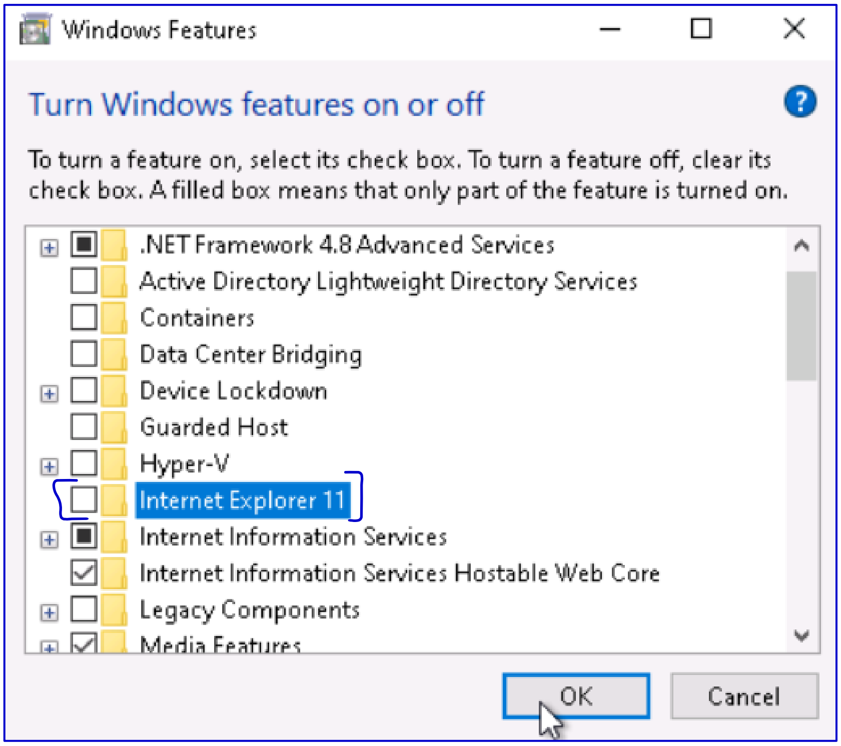
Settings> apps> default apps > click on the icon under "web browser" > choose chrome


Video player
VLC media player
Web browser
Google Chrome
Reset to the Microsoft recommended defaults
Reset
Choose default apps by file type
Choose default apps by protocol
Choose an app
Microsoft Edge
Recommended for Windows 10
Google Chrome
Internet Explorer
Microsoft Edge

2. *Why should Internet Explorer be disabled from Windows PCs? Provide at least two risks or vulnerabilities associated with it.*
    - Lack of support: vulnerabilities remain unpatched for a long time
    - Vulnerabilities are more than what Microsoft care to patch now that there's Microsoft Edge

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 Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

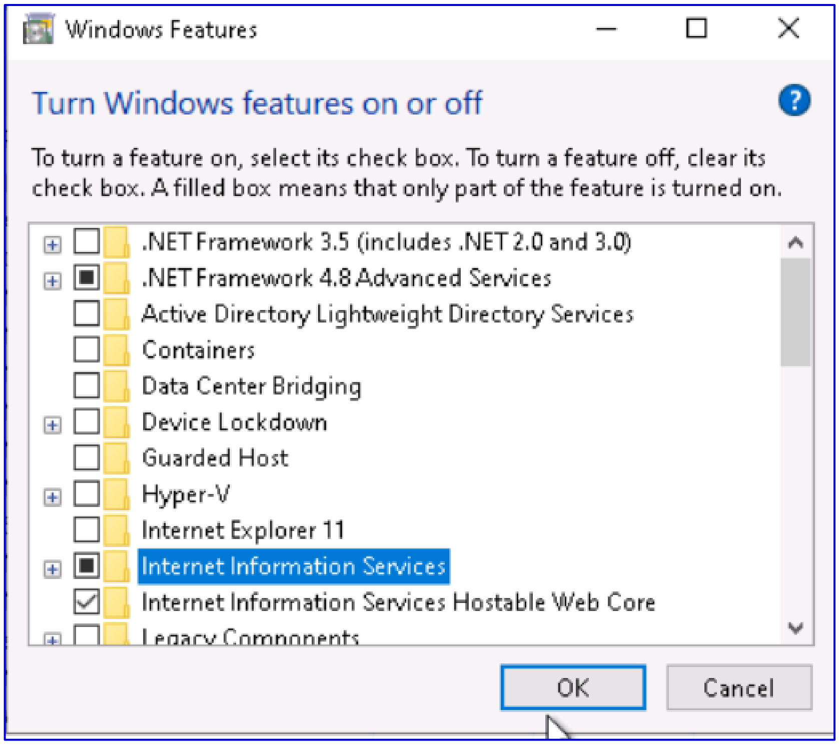
- ⊞ ■ .NET Framework 4.8 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Data Center Bridging
- ⊞ □ Device Lockdown
- □ Guarded Host
- ⊞ □ Hyper-V
- □ Internet Explorer 11
- ⊞ ■ Internet Information Services
- ☑ Internet Information Services Hostable Web Core
- ⊞ □ Legacy Components
- ⊞ ☑ Media Features

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.

   Control Panel> programs> programs and features> turn windows features on or off



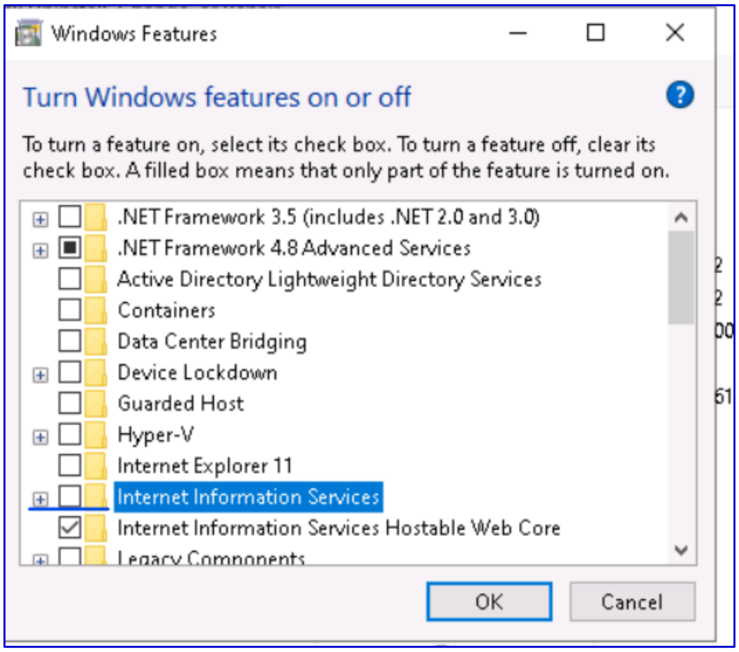
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.8 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Data Center Bridging
- □ Device Lockdown
- □ Guarded Host
- □ Hyper-V
- □ Internet Explorer 11
- ■ Internet Information Services
- ☑ Internet Information Services Hostable Web Core
- □ Legacy Components

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?

By clicking the box next to the option

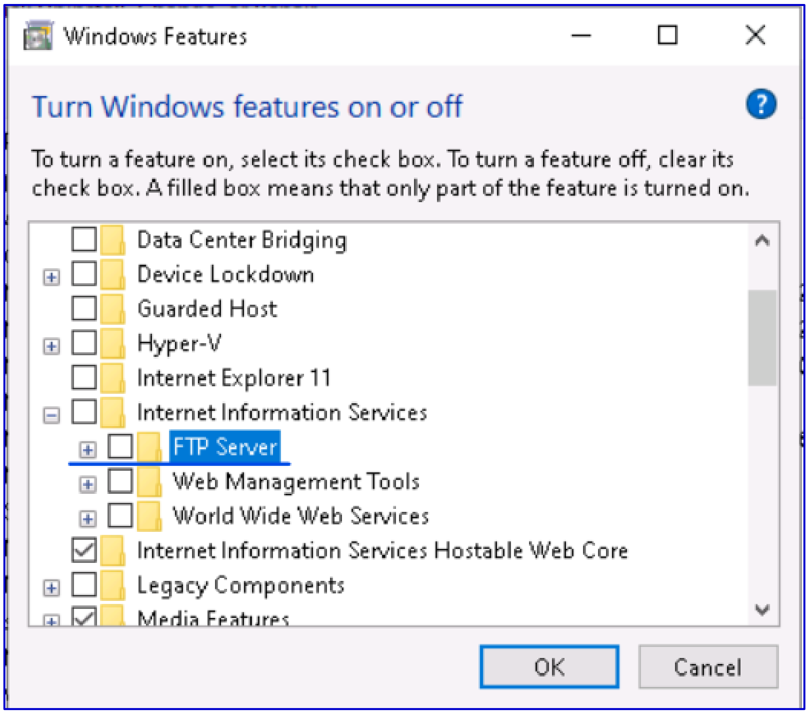


Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.8 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Data Center Bridging
- □ Device Lockdown
- □ Guarded Host
- □ Hyper-V
- □ Internet Explorer 11
- □ Internet Information Services
- ☑ Internet Information Services Hostable Web Core
- □ Legacy Components

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.



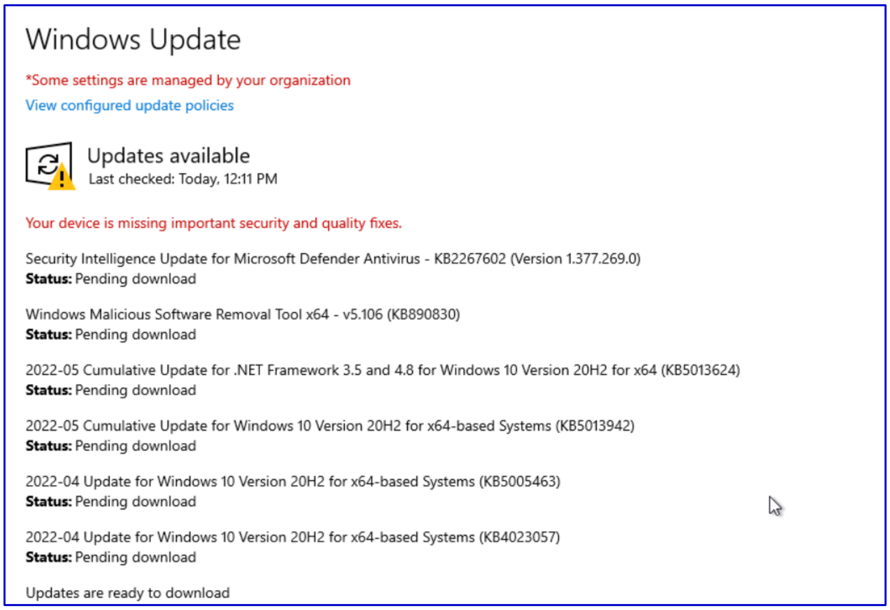
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Data Center Bridging
- ⊞ □ Device Lockdown
- □ Guarded Host
- ⊞ □ Hyper-V
- □ Internet Explorer 11
- ⊟ □ Internet Information Services
  - ⊞ □ FTP Server
  - ⊞ □ Web Management Tools
  - ⊞ □ World Wide Web Services
- ☑ Internet Information Services Hostable Web Core
- ⊞ □ Legacy Components
- ⊞ ☑ Media Features

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.*
   Setting> updates& security > Windows Updates



*Some settings are managed by your organization

View configured update policies

Updates available
Last checked: Today, 12:11 PM

Your device is missing important security and quality fixes.

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.377.269.0)
Status: Pending download

Windows Malicious Software Removal Tool x64 - v5.106 (KB890830)
Status: Pending download

2022-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for x64 (KB5013624)
Status: Pending download

2022-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5013942)
Status: Pending download

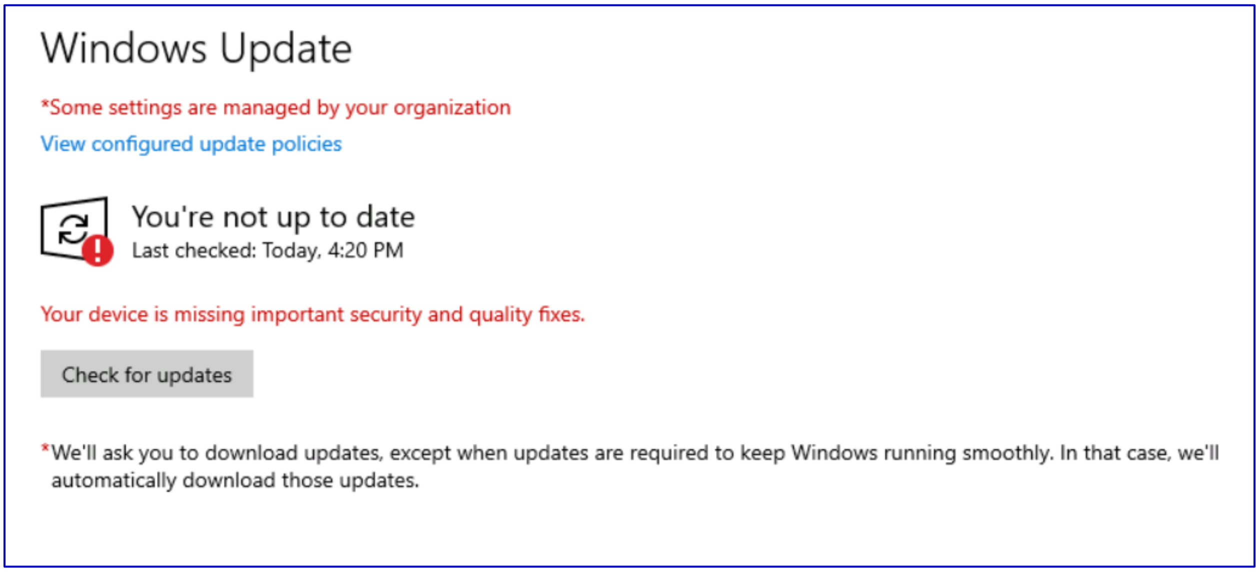
2022-04 Update for Windows 10 Version 20H2 for x64-based Systems (KB5005463)
Status: Pending download

2022-04 Update for Windows 10 Version 20H2 for x64-based Systems (KB4023057)
Status: Pending download

Updates are ready to download

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.*

Restarting after first set of updates



Windows Update

*Some settings are managed by your organization

View configured update policies

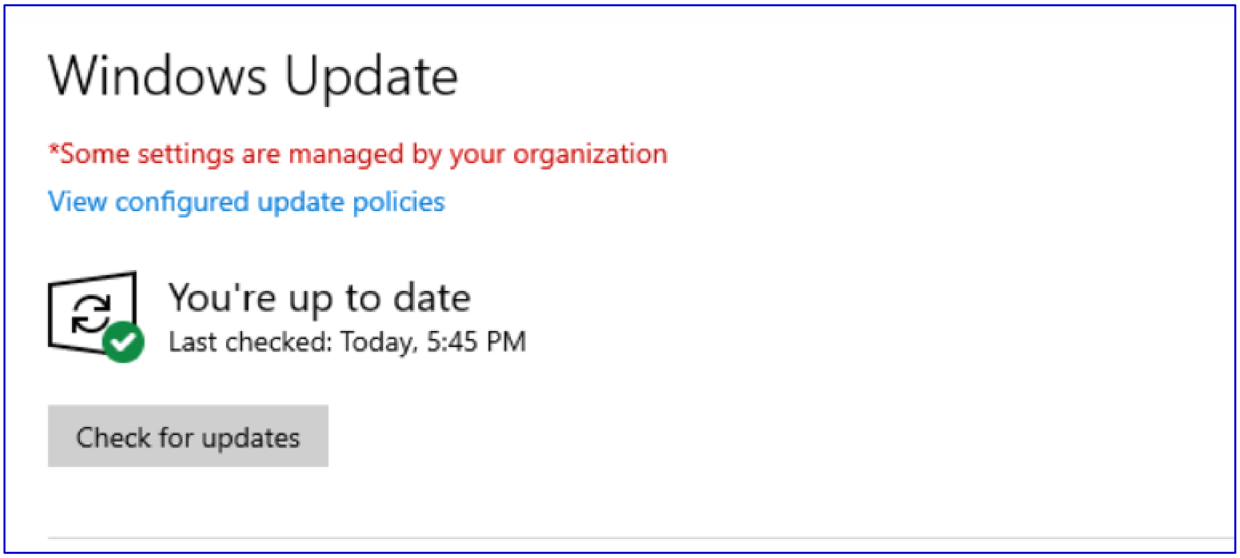
You're not up to date

Last checked: Today, 4:20 PM

Your device is missing important security and quality fixes.

*We'll ask you to download updates, except when updates are required to keep Windows running smoothly. In that case, we'll automatically download those updates.

After updating for the second time



Windows Update

*Some settings are managed by your organization

View configured update policies

You're up to date

Last checked: Today, 5:45 PM

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

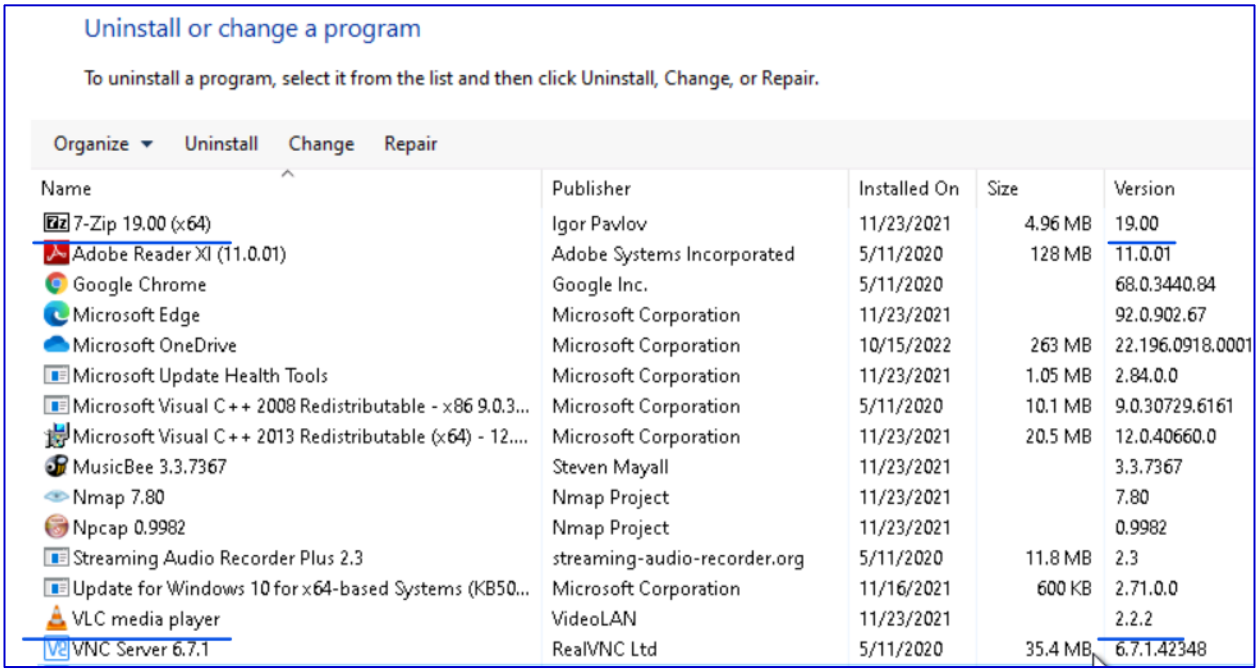
3. *List at least two applications on Joe's PC that are out of date. List them below:*

- 7-Zip
- VLC media player

4. *Explain the steps you took to determine this information.*
   I checked the version in Joe's PC then compared it to the latest version I found in the publisher's website
5. *Explain the steps for updating each of these applications. Include screenshots as needed.*

   1- Removed the applications

   Applications' version before updates

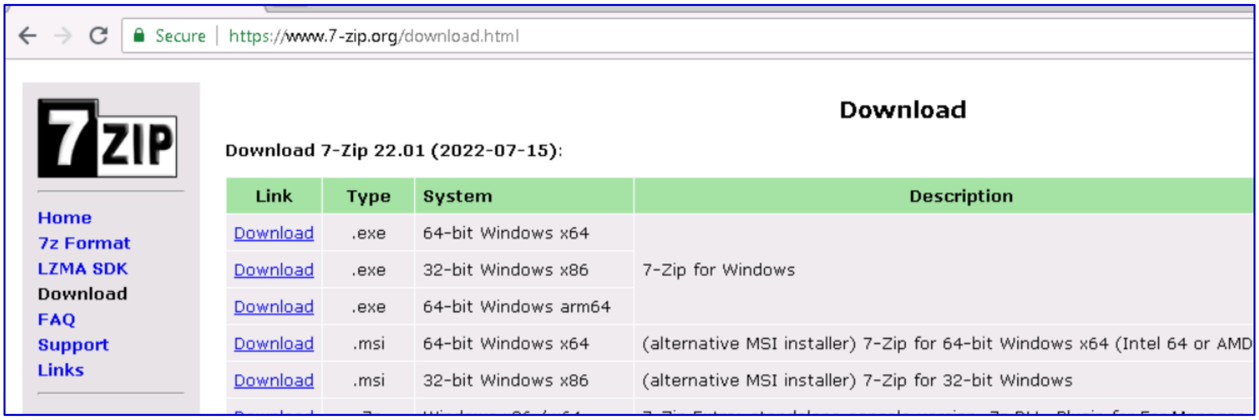


Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
7-Zip 19.00 (x64)	Igor Pavlov	11/23/2021	4.96 MB	19.00
Adobe Reader XI (11.0.01)	Adobe Systems Incorporated	5/11/2020	128 MB	11.0.01
Google Chrome	Google Inc.	5/11/2020		68.0.3440.84
Microsoft Edge	Microsoft Corporation	11/23/2021		92.0.902.67
Microsoft OneDrive	Microsoft Corporation	10/15/2022	263 MB	22.196.0918.0001
Microsoft Update Health Tools	Microsoft Corporation	11/23/2021	1.05 MB	2.84.0.0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	5/11/2020	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x64) - 12....	Microsoft Corporation	11/23/2021	20.5 MB	12.0.40660.0
MusicBee 3.3.7367	Steven Mayall	11/23/2021		3.3.7367
Nmap 7.80	Nmap Project	11/23/2021		7.80
Npcap 0.9982	Nmap Project	11/23/2021		0.9982
Streaming Audio Recorder Plus 2.3	streaming-audio-recorder.org	5/11/2020	11.8 MB	2.3
Update for Windows 10 for x64-based Systems (KB50...	Microsoft Corporation	11/16/2021	600 KB	2.71.0.0
VLC media player	VideoLAN	11/23/2021		2.2.2
VNC Server 6.7.1	RealVNC Ltd	5/11/2020	35.4 MB	6.7.1.42348

   2- Download the latest version of 7-zip from the official publisher's website and launch it



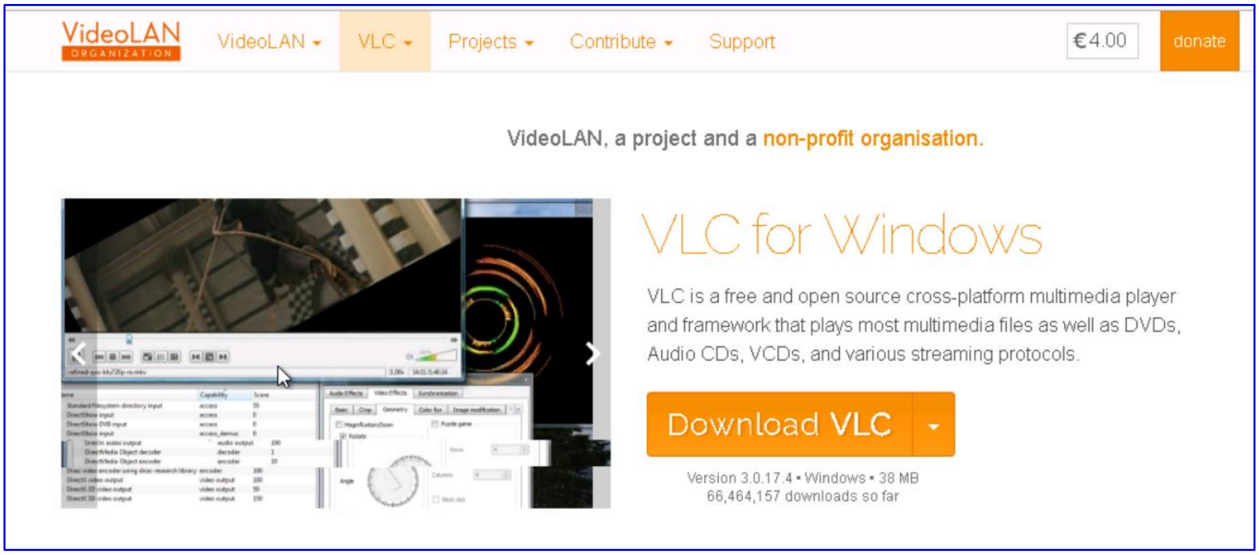
Secure | https://www.7-zip.org/download.html

Download

Download 7-Zip 22.01 (2022-07-15):

Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip for Windows
Download	.exe	32-bit Windows x86	
Download	.exe	64-bit Windows arm64	
Download	.msi	64-bit Windows x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64 (Intel 64 or AMD
Download	.msi	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows

   3- Download the latest version of VLC from the official publisher's website and launch it



VideoLAN, a project and a non-profit organisation.

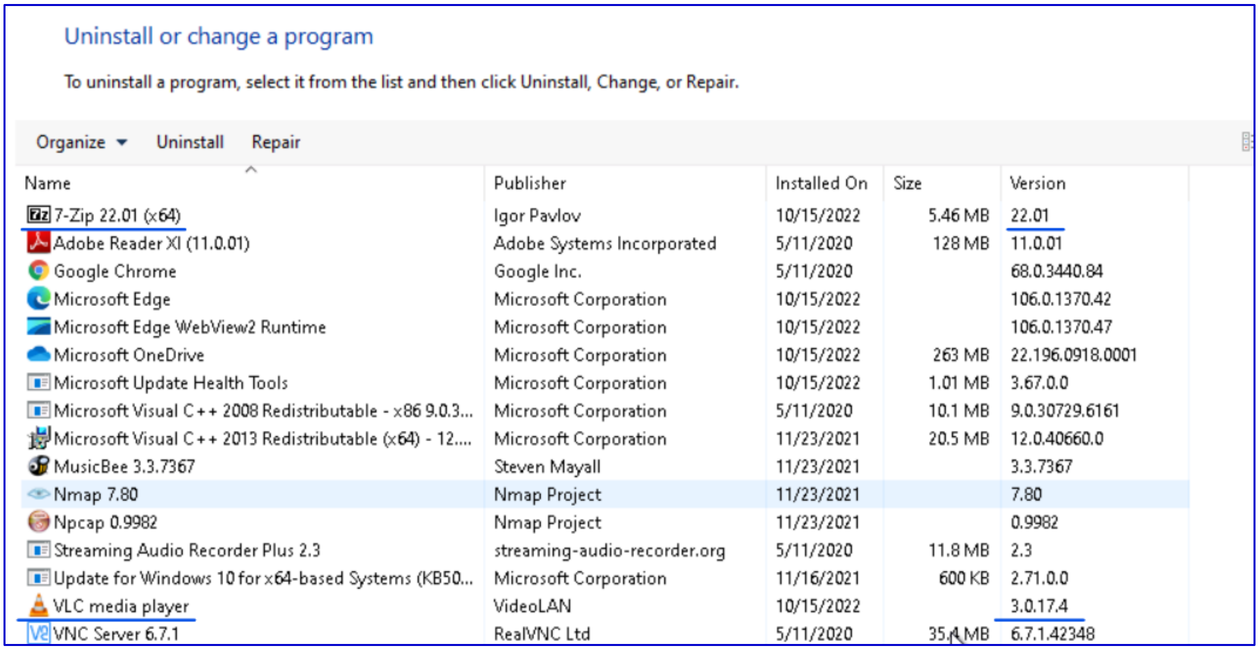
VLC for Windows

VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs, and various streaming protocols.

Download VLC

Version 3.0.17.4 • Windows • 38 MB
66,464,157 downloads so far

4- Apps after update



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
7-Zip 22.01 (x64)	Igor Pavlov	10/15/2022	5.46 MB	22.01
Adobe Reader XI (11.0.01)	Adobe Systems Incorporated	5/11/2020	128 MB	11.0.01
Google Chrome	Google Inc.	5/11/2020		68.0.3440.84
Microsoft Edge	Microsoft Corporation	10/15/2022		106.0.1370.42
Microsoft Edge WebView2 Runtime	Microsoft Corporation	10/15/2022		106.0.1370.47
Microsoft OneDrive	Microsoft Corporation	10/15/2022	263 MB	22.196.0918.0001
Microsoft Update Health Tools	Microsoft Corporation	10/15/2022	1.01 MB	3.67.0.0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	5/11/2020	10.1 MB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x64) - 12....	Microsoft Corporation	11/23/2021	20.5 MB	12.0.40660.0
MusicBee 3.3.7367	Steven Mayall	11/23/2021		3.3.7367
Nmap 7.80	Nmap Project	11/23/2021		7.80
Npcap 0.9982	Nmap Project	11/23/2021		0.9982
Streaming Audio Recorder Plus 2.3	streaming-audio-recorder.org	5/11/2020	11.8 MB	2.3
Update for Windows 10 for x64-based Systems (KB50...	Microsoft Corporation	11/16/2021	600 KB	2.71.0.0
VLC media player	VideoLAN	10/15/2022		3.0.17.4
VNC Server 6.7.1	RealVNC Ltd	5/11/2020	35.4 MB	6.7.1.42348

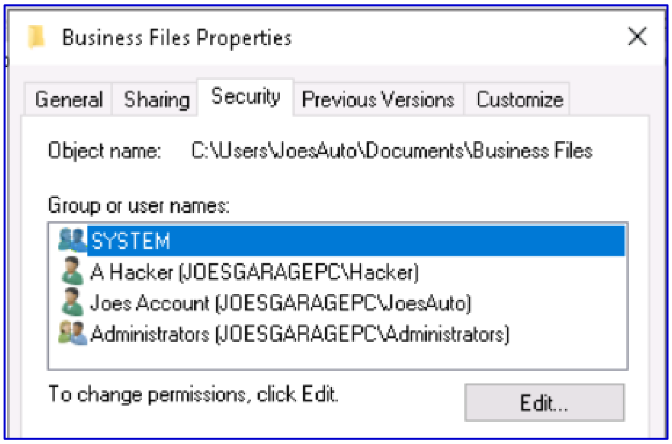
5. Securing Files and Folders

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.]*
   search for folder name> right click on Business Files folder> properties> security tab



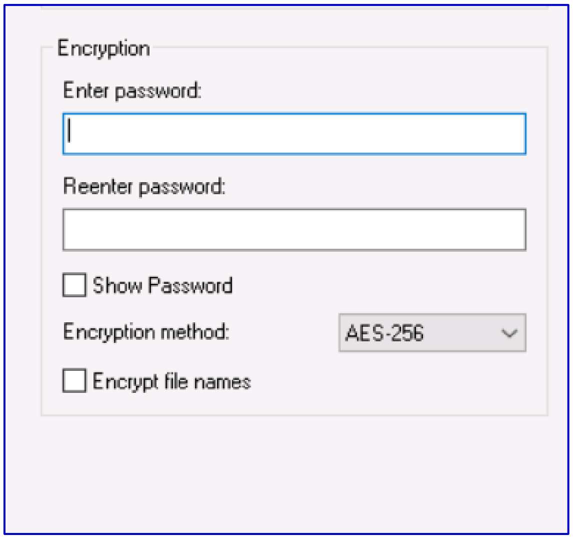
Object name: C:\Users\JoesAuto\Documents\Business Files

Group or user names:

- SYSTEM
- A Hacker (JOESGARAGEPC\Hacker)
- Joes Account (JOESGARAGEPC\JoesAuto)
- Administrators (JOESGARAGEPC\Administrators)

To change permissions, click Edit.

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.*
   Right click on folder> 7-zip> add to archive> type the password in the enter password under encryption section.
   I recommend AES with a key length of 256bit because it's a reliable encryption method



Encryption

Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

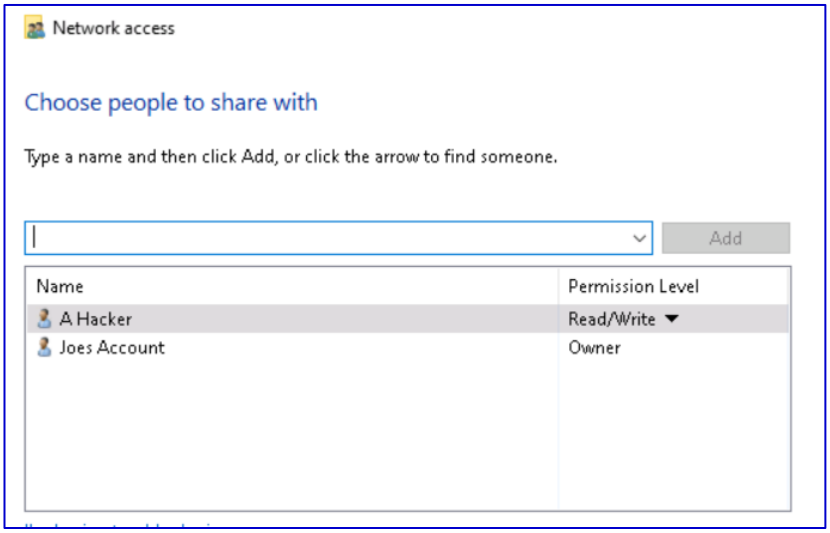
□ Encrypt file names

3. *What security fundamental does this provide?*
   Confidentiality because now files are encrypted can only be viewed by users who have the password
4. *The Center for Internet Security Controls lists this as one of their steps for security. Which step does this fulfill?* 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.*
   Go to documents> right click on "business files" folder> properties> sharing tab> click on share
   Currently, A Hacker has read/rights permissions



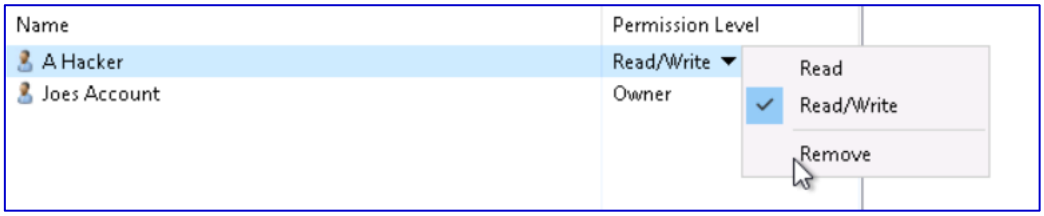
Network access

Choose people to share with

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

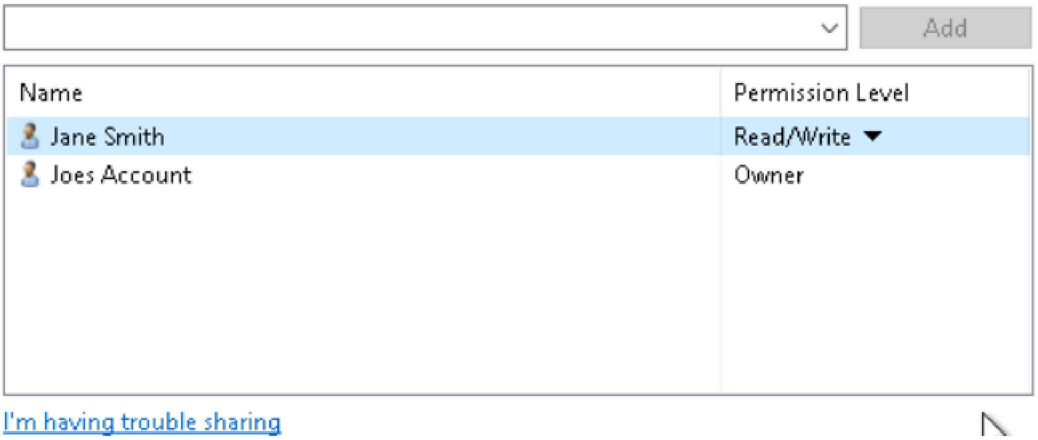
Name	Permission Level
A Hacker	Read/Write ▼
Joes Account	Owner

Click on hacker> click remove



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

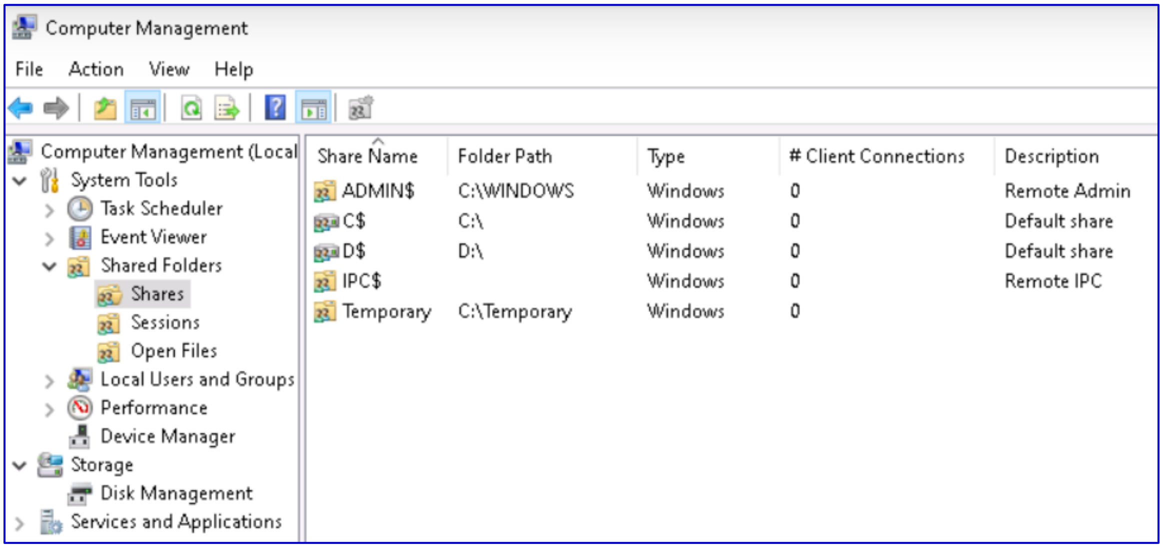
To add jane: click on the arrow near add> choose jane from drop-down menu> change permission to read/write



Name	Permission Level
Jane Smith	Read/Write
Joes Account	Owner

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.*

   Right click on windows icon> computer management> shared folders

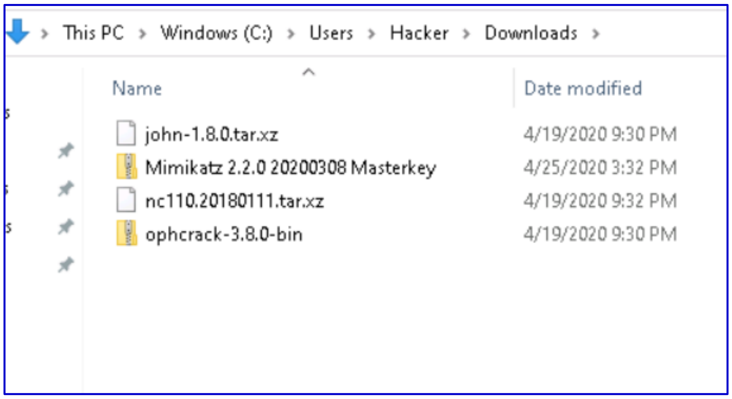


Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\WINDOWS	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
D$	D:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
Temporary	C:\Temporary	Windows	0	

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]

Going to file explorer> this pc> users> AHacker> downloads

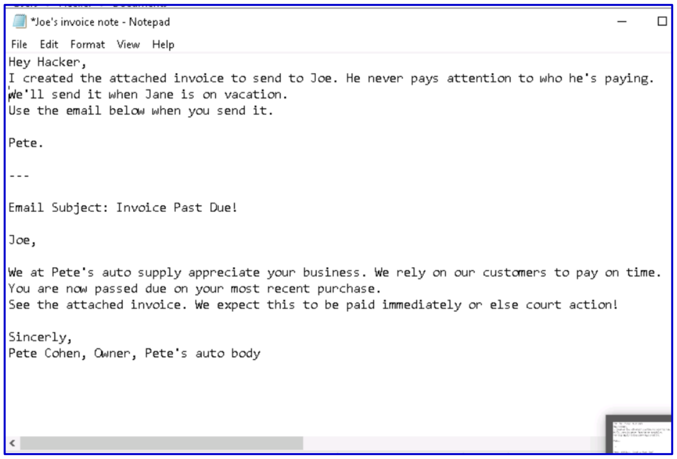


This PC › Windows (C:) › Users › Hacker › Downloads ›

Name	Date modified
john-1.8.0.tar.xz	4/19/2020 9:30 PM
Mimikatz 2.2.0 20200308 Masterkey	4/25/2020 3:32 PM
nc110.20180111.tar.xz	4/19/2020 9:32 PM
ophcrack-3.8.0-bin	4/19/2020 9:30 PM

- There’s an Ophcrack program folder. Ophcrack is used to crack password using rainbow tables. The user Hacker might have used this to know the passwords used by other users.
- There’s also a folder for Mimikatz which is an exploitation tool for extracting passwords saved in memory in windows systems

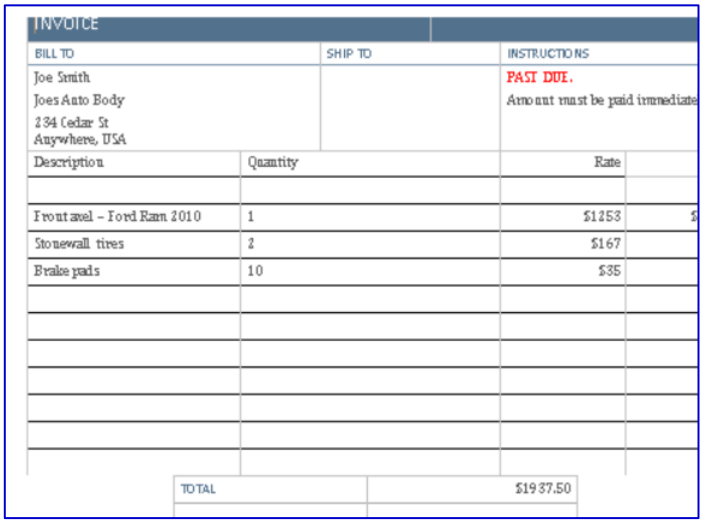
By going to hacker documents I found this note



*Joe's invoice note - Notepad

```
Hey Hacker,
I created the attached invoice to send to Joe. He never pays attention to who he's paying.
We'll send it when Jane is on vacation.
Use the email below when you send it.

Pete.

---

Email Subject: Invoice Past Due!

Joe,

We at Pete's auto supply appreciate your business. We rely on our customers to pay on time.
You are now passed due on your most recent purchase.
See the attached invoice. We expect this to be paid immediately or else court action!

Sincerly,
Pete Cohen, Owner, Pete's auto body
```

And this is a snapshot of the invoice



INVOICE

BILL TO	SHIP TO	INSTRUCTIONS
Joe Smith Joes Auto Body 234 Cedar St Anywhere, USA		PAST DUE. Amount must be paid immediate

Description	Quantity	Rate	
Front axel – Ford Ram 2010	1	$1253	$
Stonewall tires	2	$167	
Brake pads	10	$35	

TOTAL	$1937.50

- The hacker used phishing to trick Joe into sending him money by pretending he is a legitimate business contacting Joe via email

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.