UDACITY

Securing a Business Network

Securing a Business Network

Student Information

Student Name: LUNA DAHAL
Date of completion: 10-09-2025

Securing a Computer System

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.

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: ******

1. Reconnaissance

The first step in securing any system is to know what it is(Hardware), what's on it(Software), what it's used for(Services) and who uses it (Users and Accounts). 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 all sections that follow.

[Please Provide Screenshots as evidence that you completed this step.]

1. A. Hardware

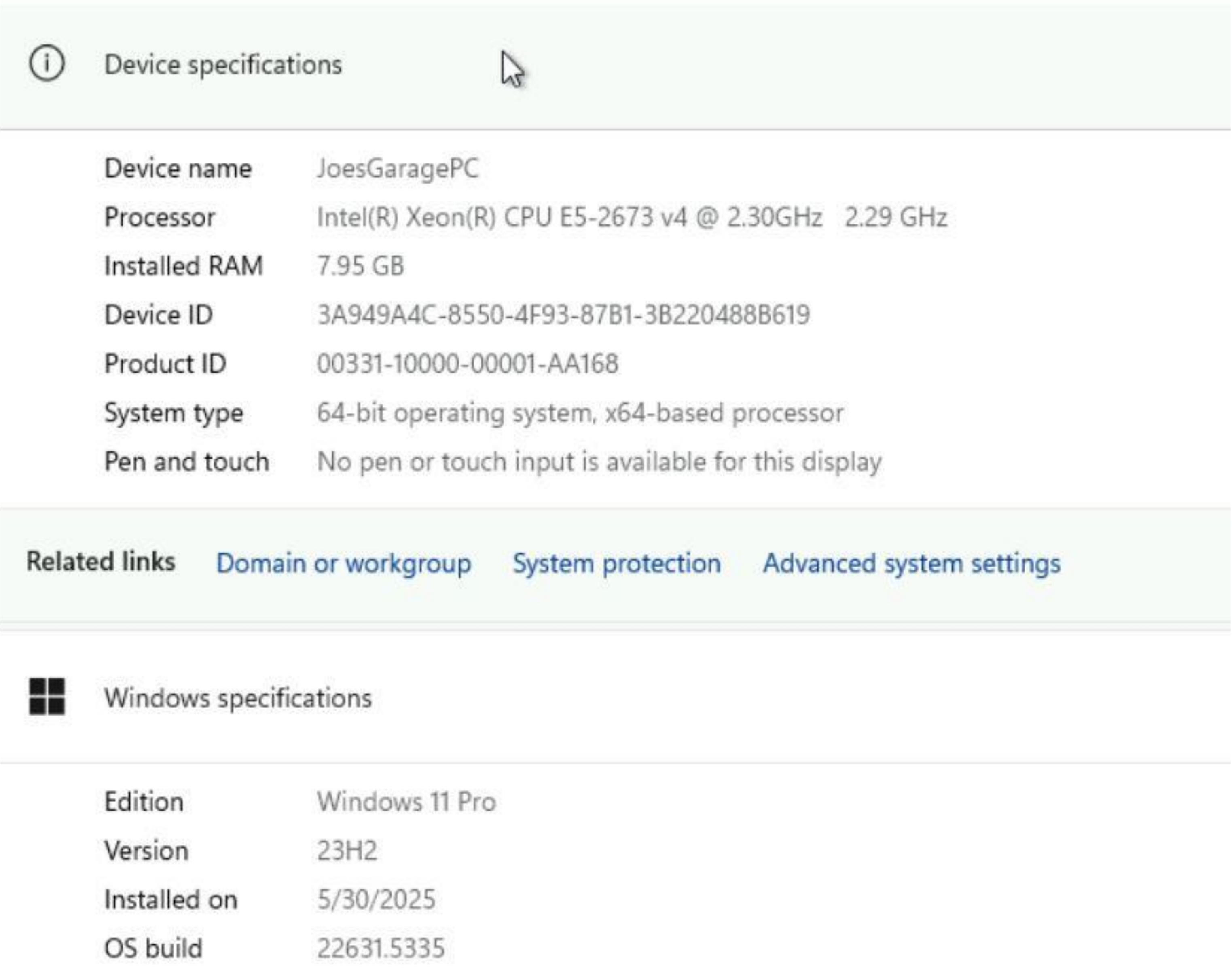
Fill in the following table with system information for Joe's PC.

Device Name	JoesGaragePC
Processor	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz 2.29
Install RAM	7.95 GB
System Type	64-bit operating system, x64-based
Windows Edition	Windows 11 Pro
Version	23H2
Installed on	05-30-2025
OS build	22631.5335

Right-click the Start button > Settings > System > About

[Provide a screenshot in the next slide, showing this information about Joe's PC You may need to duplicate this slide to include all of your screenshots]

Screenshot - Hardware Information



Device specifications

Device name	JoesGaragePC
Processor	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz 2.29 GHz
Installed RAM	7.95 GB
Device ID	3A949A4C-8550-4F93-87B1-3B220488B619
Product ID	00331-10000-00001-AA168
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 11 Pro
Version	23H2
Installed on	5/30/2025
OS build	22631.5335

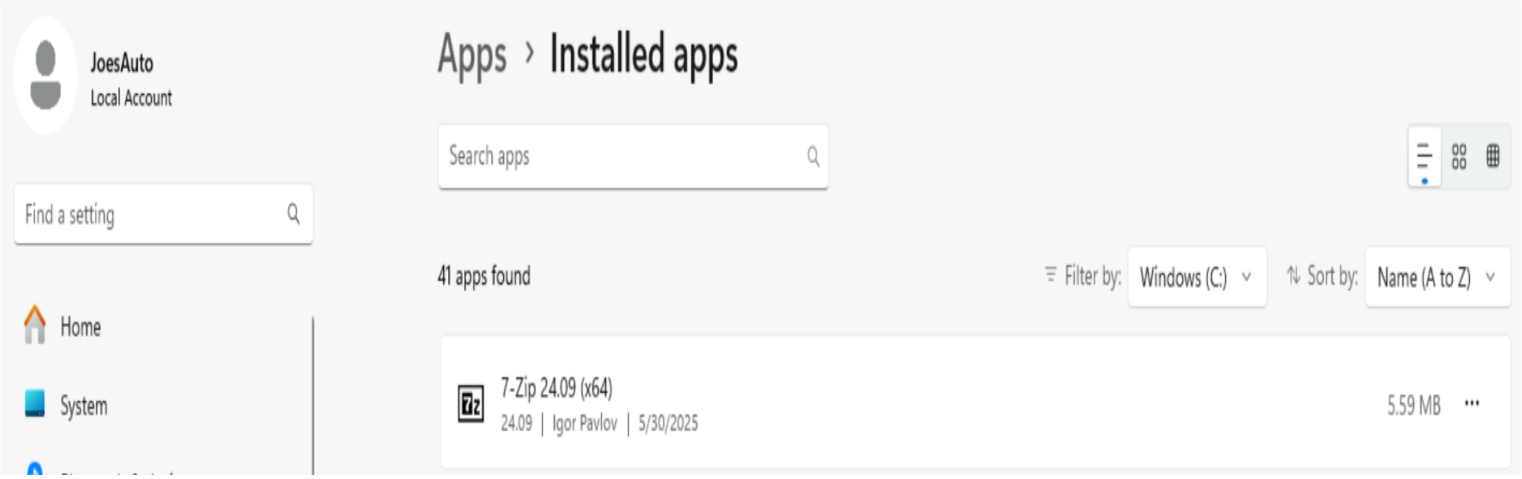
1. B Software Inventory

Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system.
List at least 5 installed applications on Joe's computer:

1.	7-Zip
2.	Google Chrome
3.	Maps
4.	MediaMonkey 2024
5.	Media Player

Right-click the Start button and select Installed Apps
[Provide a screenshot in the next slide, showing this information about Joe's PC]

Screenshot - Software Inventory



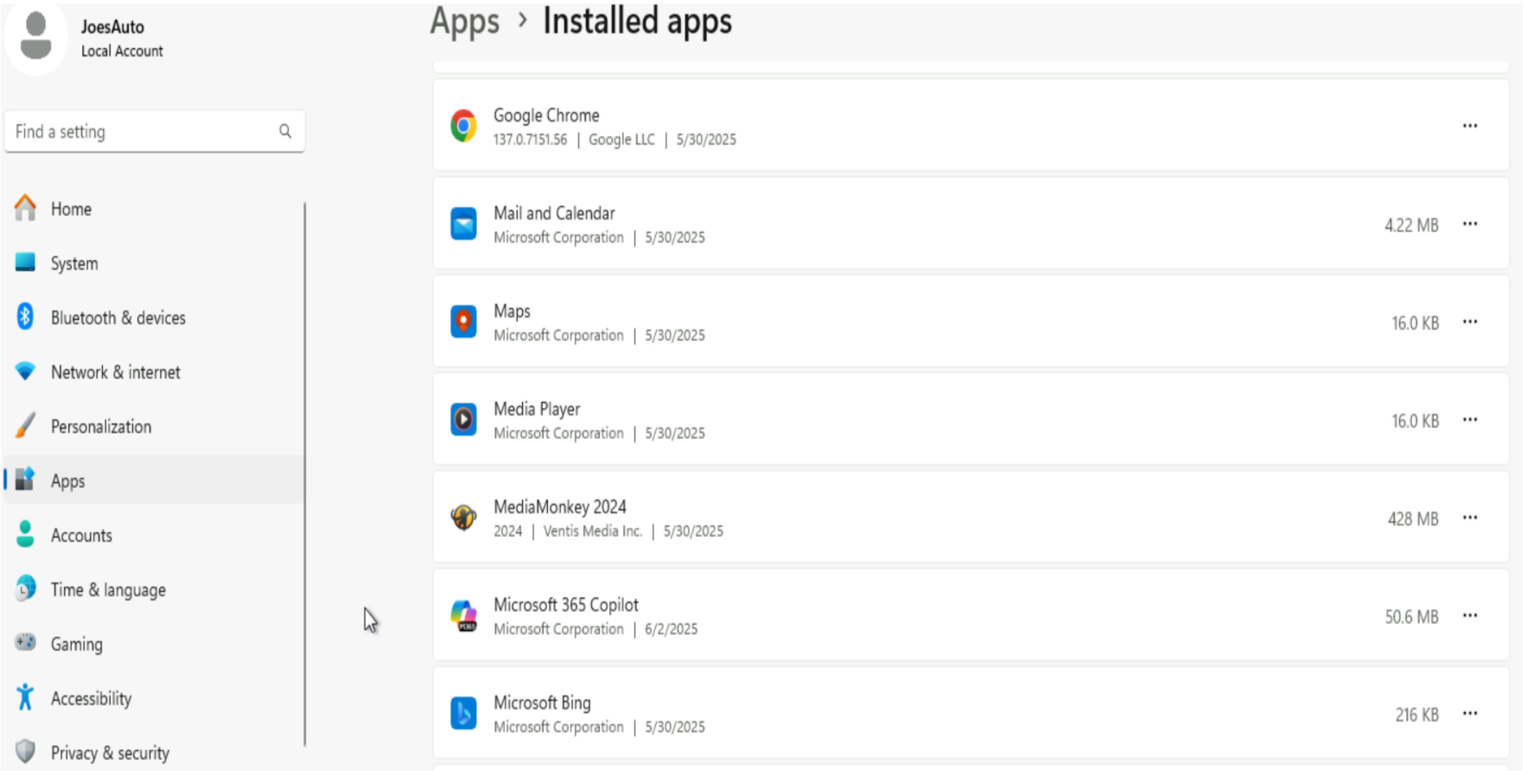
Apps › Installed apps

41 apps found

Filter by: Windows (C:)

Sort by: Name (A to Z)

7-Zip 24.09 (x64)
24.09 | Igor Pavlov | 5/30/2025 — 5.59 MB



Apps › Installed apps

Google Chrome
137.0.7151.56 | Google LLC | 5/30/2025

Mail and Calendar
Microsoft Corporation | 5/30/2025 — 4.22 MB

Maps
Microsoft Corporation | 5/30/2025 — 16.0 KB

Media Player
Microsoft Corporation | 5/30/2025 — 16.0 KB

MediaMonkey 2024
2024 | Ventis Media Inc. | 5/30/2025 — 428 MB

Microsoft 365 Copilot
Microsoft Corporation | 6/2/2025 — 50.6 MB

Microsoft Bing
Microsoft Corporation | 5/30/2025 — 216 KB

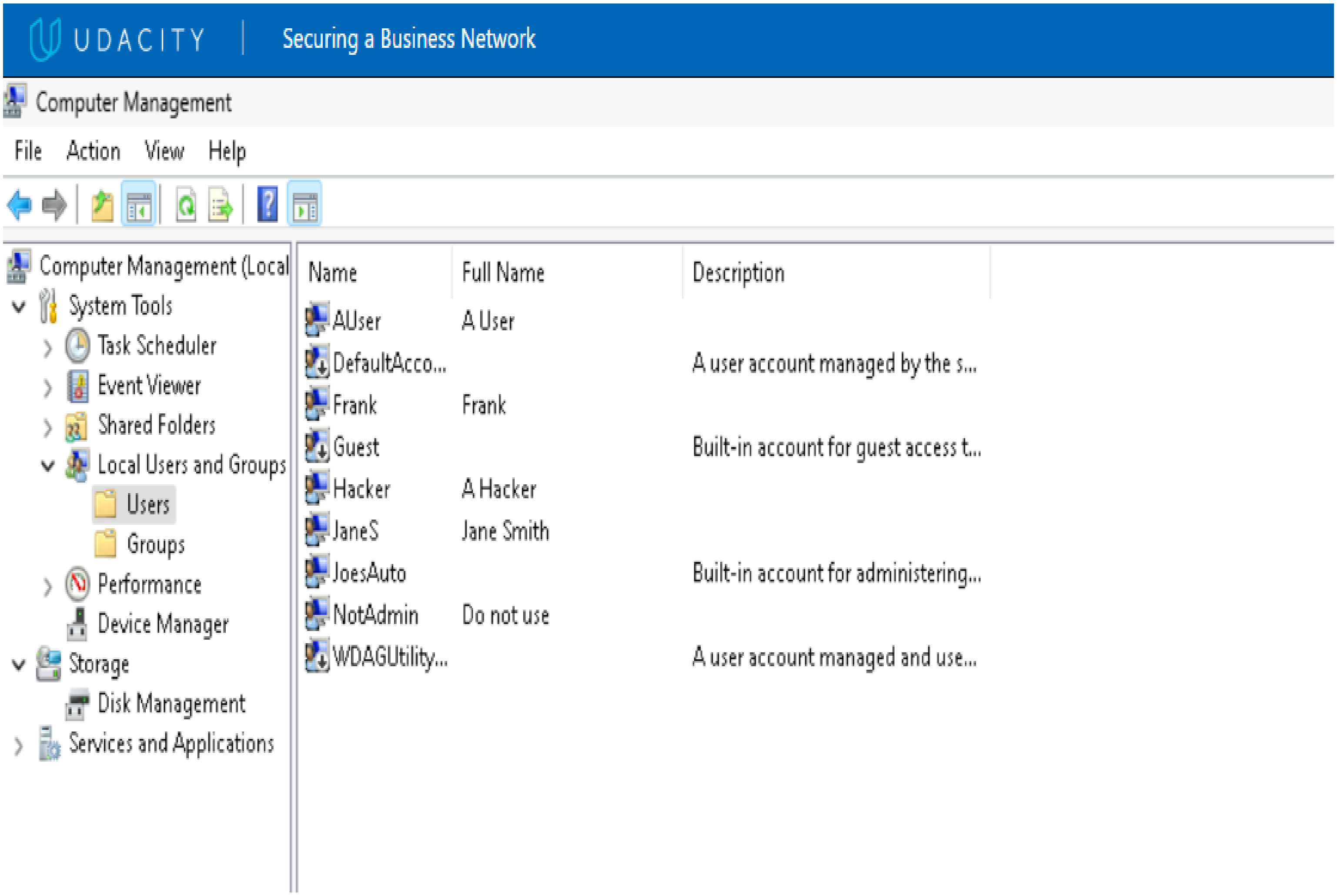
1. C. Accounts

As part of your security assessment, you should know the user accounts that may access the PC. List the names of the accounts found on Joe's PC and their access level.

Account Name	**Full Name**	**Access Level**
Auser	AUser	User
Frank	Frank	User
Hacker	A Hacker	User and Admin
JaneS	Jane Smith	User and Admin
Joes Auto	N/A	Admin

Right-click the Start button> select Computer Management > select Local users and Groups > Users or Use Settings > Accounts > Other users>Add Account
[Provide a screenshot in the next slide, of the Local Users.

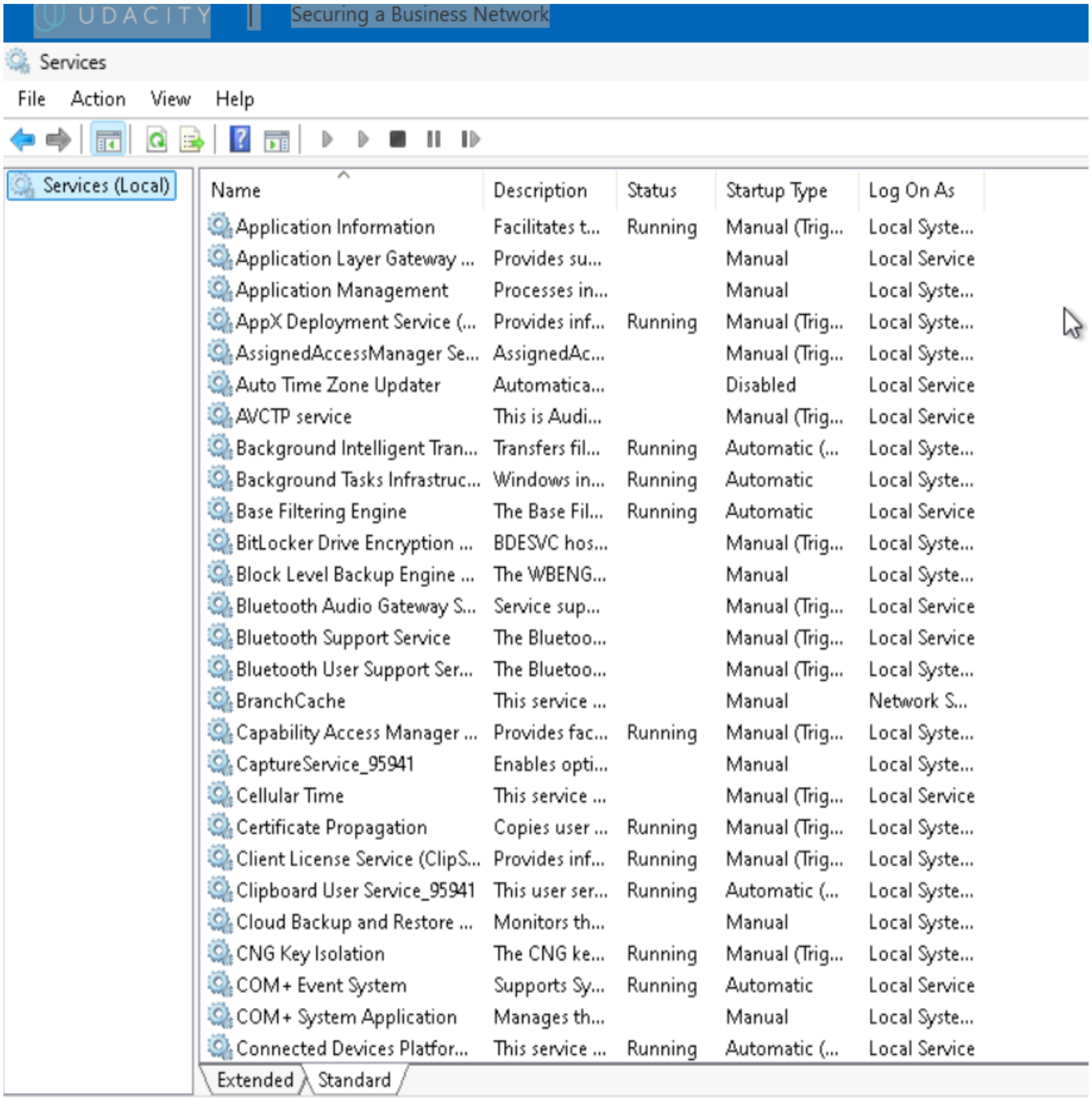
Screenshot - Local Users



Name	Full Name	Description
AUser	A User	
DefaultAcco...		A user account managed by the s...
Frank	Frank	
Guest		Built-in account for guest access t...
Hacker	A Hacker	
JaneS	Jane Smith	
JoesAuto		Built-in account for administering...
NotAdmin	Do not use	
WDAGUtility...		A user account managed and use...

1. D. Services

Services are applications often running in the background. Most of them provide needed functionality for the PC. Some may also be used to violate security policies. Provide a screenshot of the services running on this PC in the space below



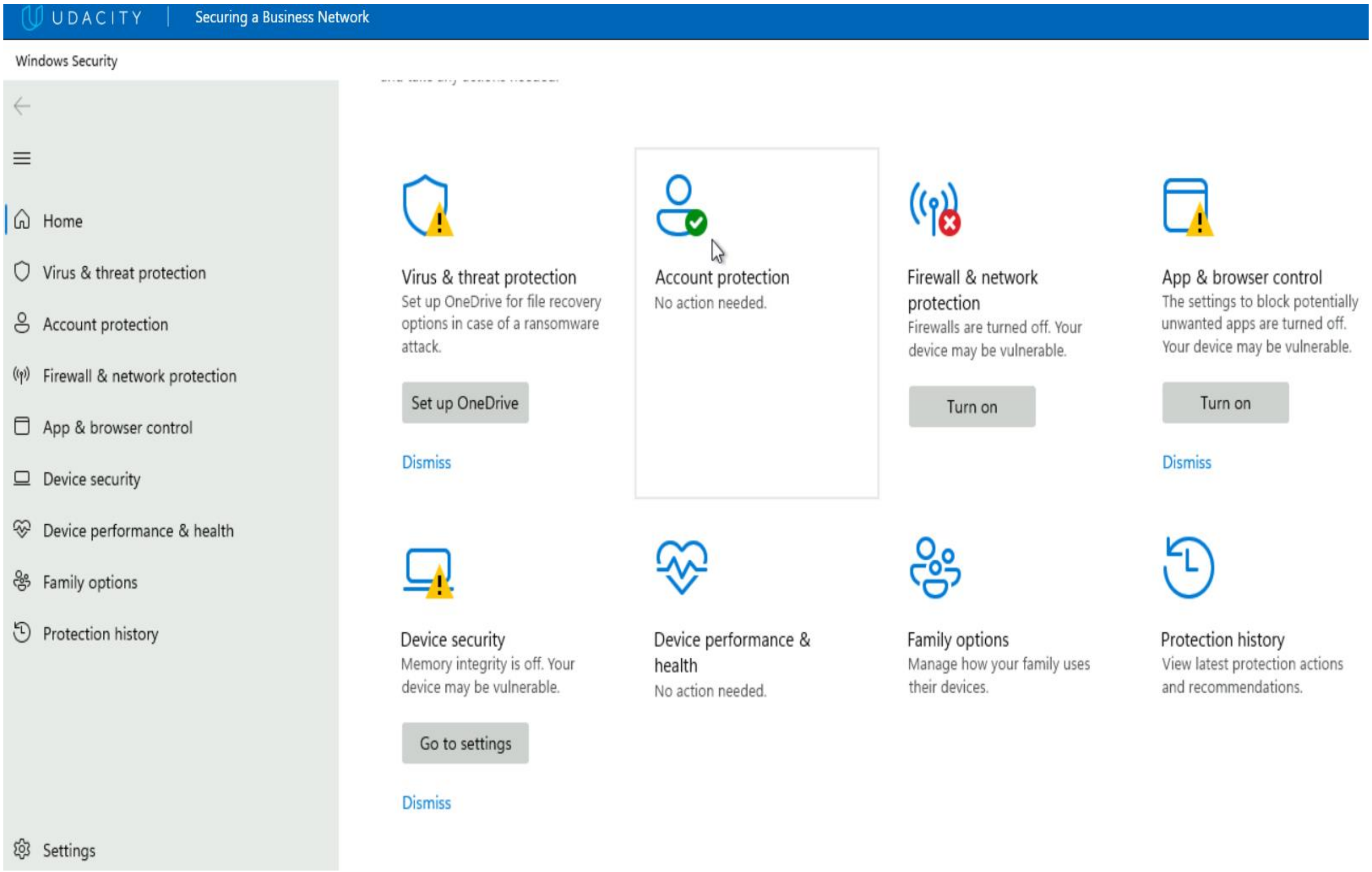
Name	Description	Status	Startup Type	Log On As
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Local Syste...
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
AVCTP service	This is Audi...		Manual (Trig...	Local Service
Background Intelligent Tran...	Transfers fil...	Running	Automatic (...	Local Syste...
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
Bluetooth Audio Gateway S...	Service sup...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...		Manual (Trig...	Local Syste...
BranchCache	This service ...		Manual	Network S...
Capability Access Manager ...	Provides fac...	Running	Manual (Trig...	Local Syste...
CaptureService_95941	Enables opti...		Manual	Local Syste...
Cellular Time	This service ...		Manual (Trig...	Local Service
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Local Syste...
Client License Service (ClipS...	Provides inf...	Running	Manual (Trig...	Local Syste...
Clipboard User Service_95941	This user ser...	Running	Automatic (...	Local Syste...
Cloud Backup and Restore ...	Monitors th...		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...		Manual	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (...	Local Service

Click the Search icon on the taskbar > Type services and select the Services app from the results

1. E. 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 11, Click the Search icon on the taskbar and type Windows Security or Settings > Privacy & Security > Windows Security. Take a screenshot and paste in the subsequent slides. The Windows Security app is the central hub for all major security services in Windows 11.*



Virus & threat protection
Set up OneDrive for file recovery options in case of a ransomware attack.

Account protection
No action needed.

Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.

App & browser control
The settings to block potentially unwanted apps are turned off. Your device may be vulnerable.

Device security
Memory integrity is off. Your device may be vulnerable.

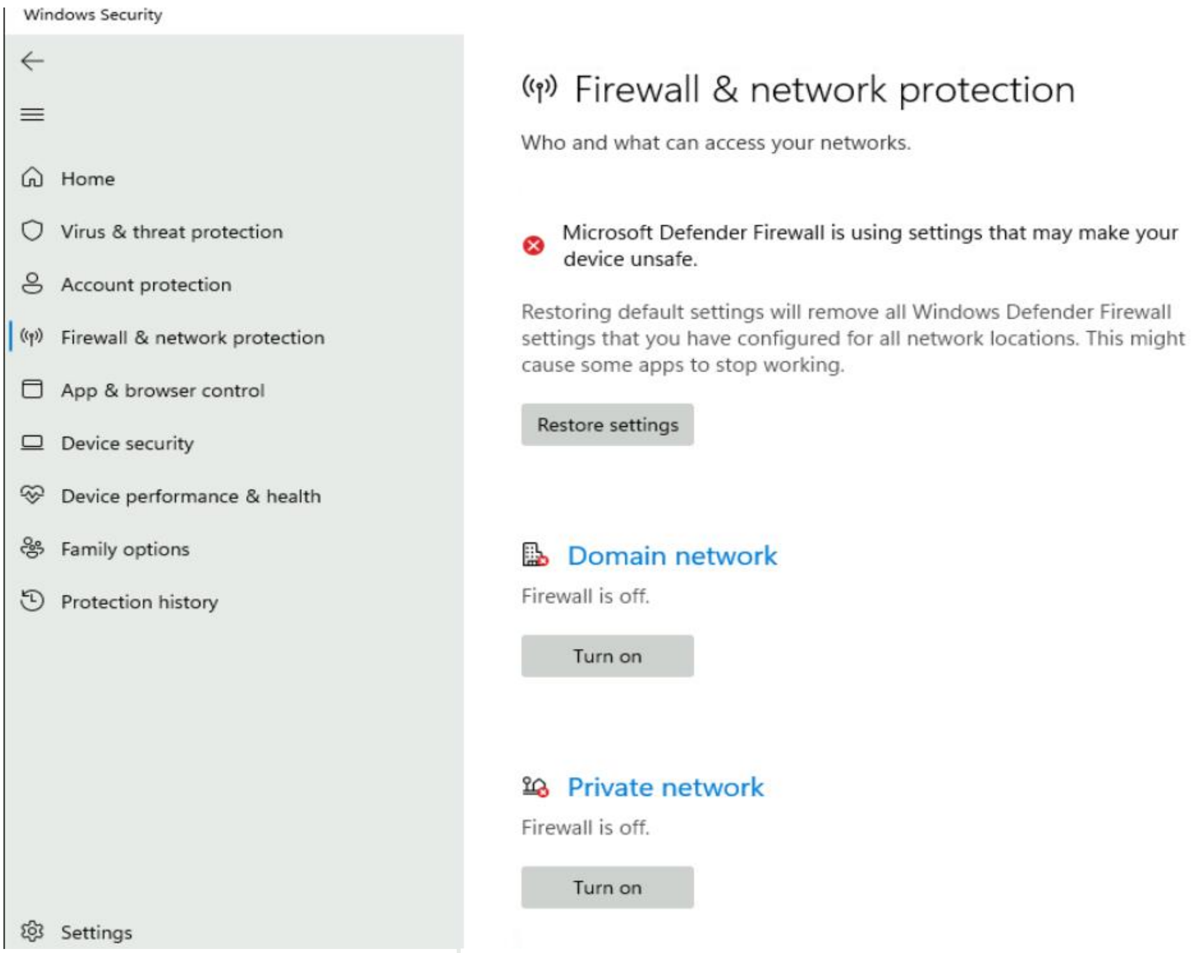
Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Protection history
View latest protection actions and recommendations.

1. E. Security Services - Windows Firewall & network protection .

Click on Firewall & network protection in Windows Security to see the status. Provide a screenshot below:



Firewall & network protection

Who and what can access your networks.

Microsoft Defender Firewall is using settings that may make your device unsafe.

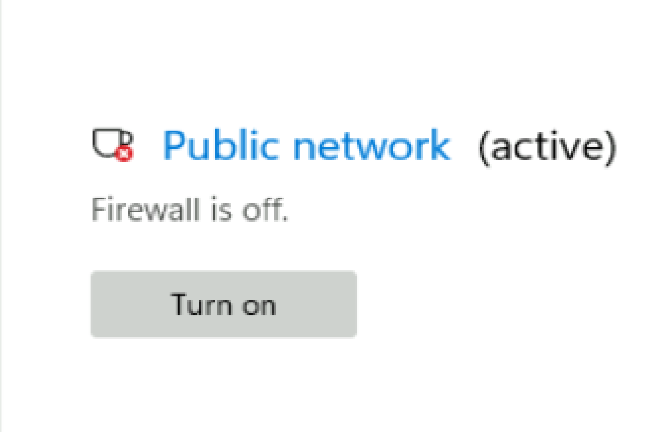
Restoring default settings will remove all Windows Defender Firewall settings that you have configured for all network locations. This might cause some apps to stop working.

Domain network

Firewall is off.

Private network

Firewall is off.

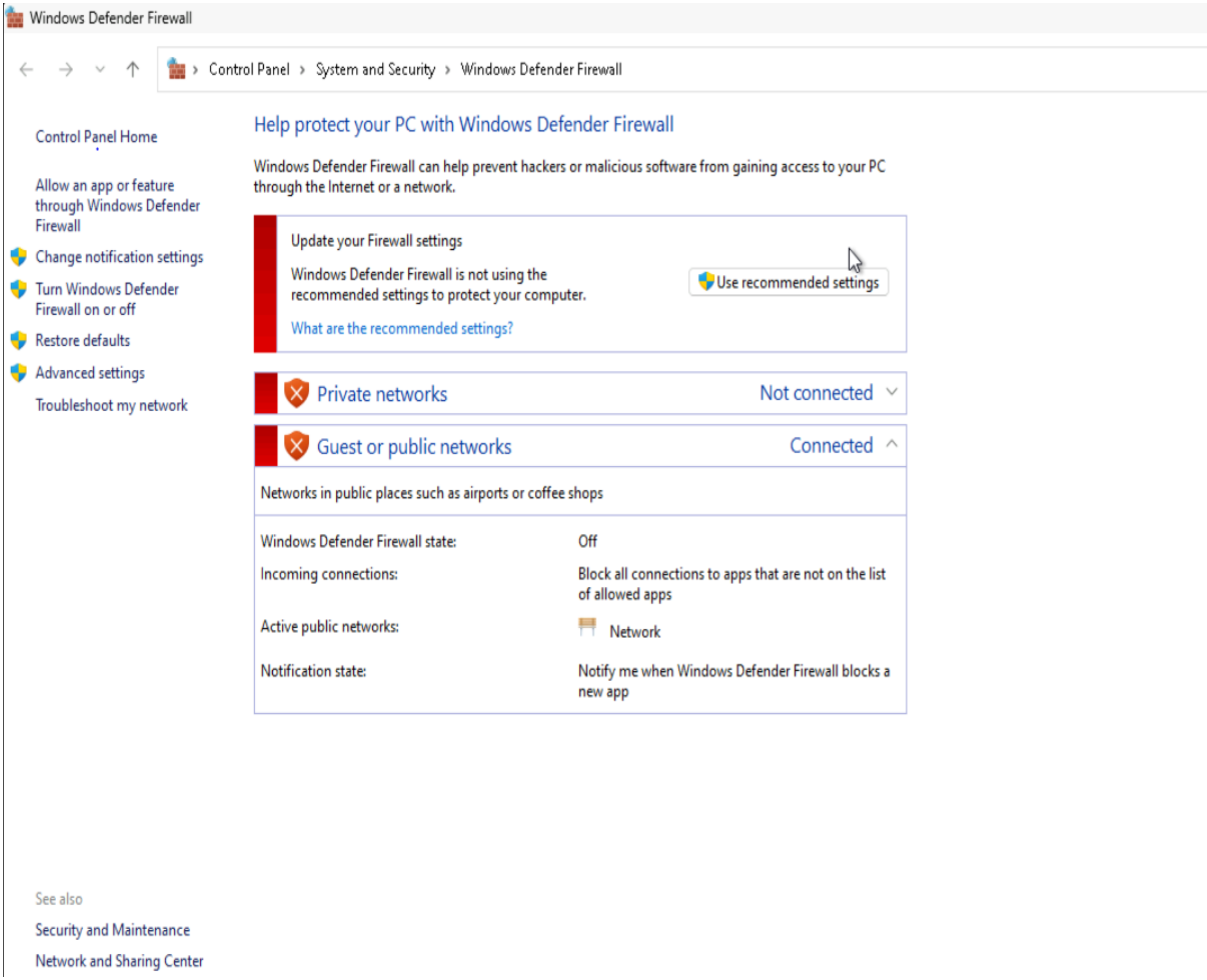


Public network (active)

Firewall is off.

1. E. Security Services - Windows Defender Firewall.

From the Control Panel, go to System and Security > Windows Defender Firewall. Take a screenshot and paste it here:



Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
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 — Not connected

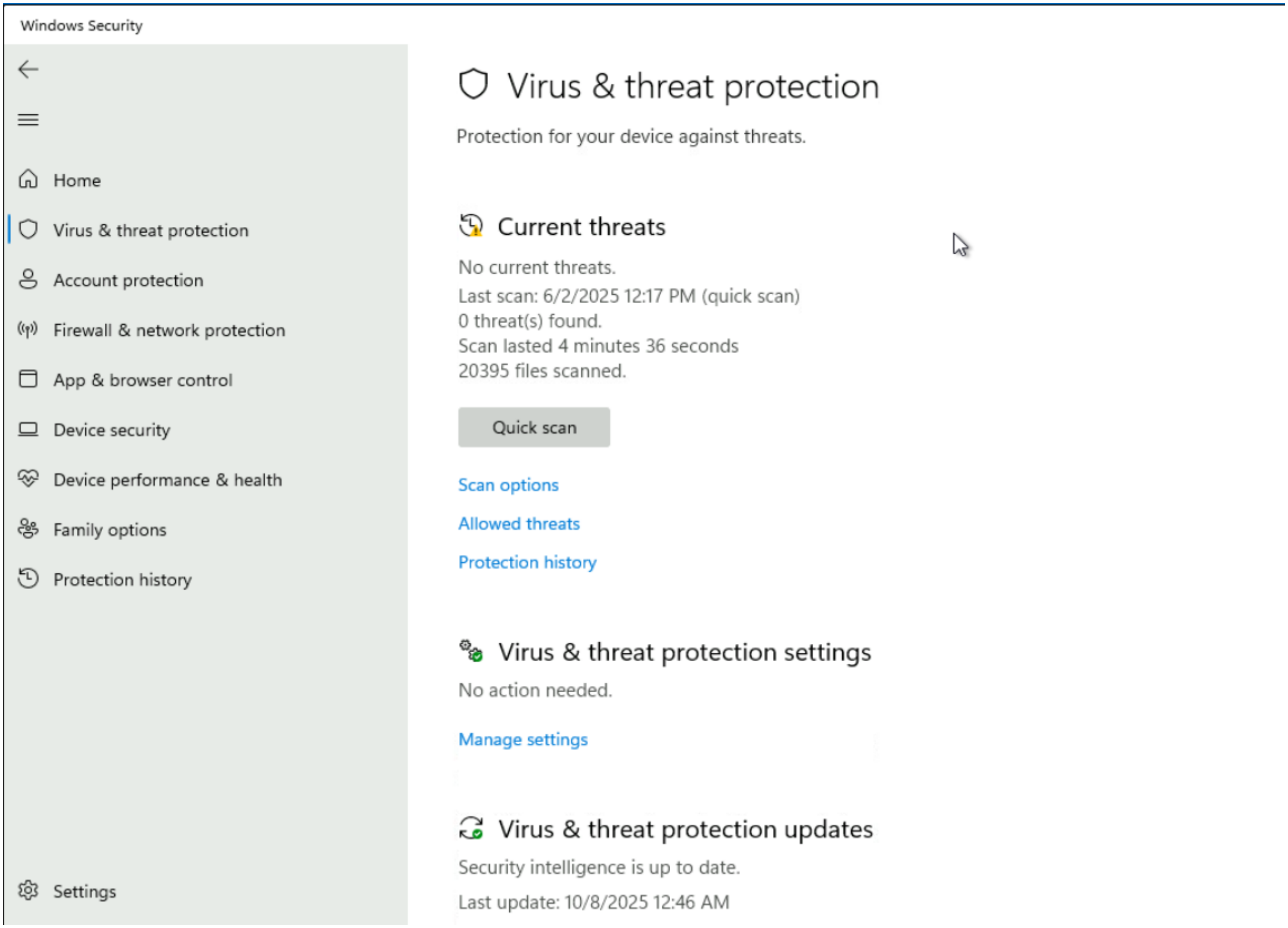
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

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

1. E. Security Services - Virus protection

Click on Virus and Threat Protection in Windows Security to see the status. Provide a screenshot for Virus and threat protection, here:



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 6/2/2025 12:17 PM (quick scan)
0 threat(s) found.
Scan lasted 4 minutes 36 seconds
20395 files scanned.

Virus & threat protection settings

No action needed.

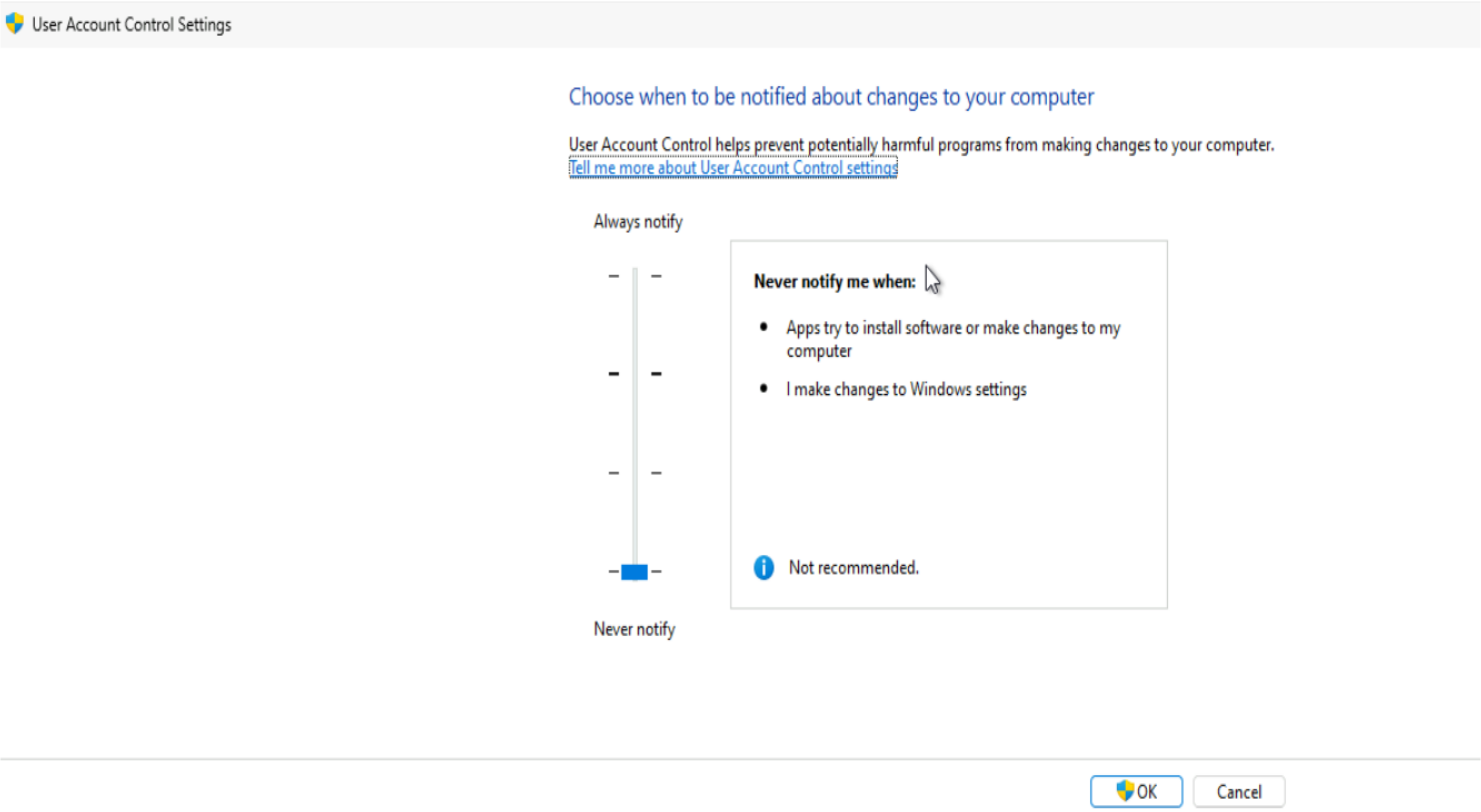
Virus & threat protection updates

Security intelligence is up to date.

Last update: 10/8/2025 12:46 AM

1. E. Security Services - User Account Settings

Click the Search icon on the taskbar > Type User Account Control or UAC and select it. Take a screenshot and 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 me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

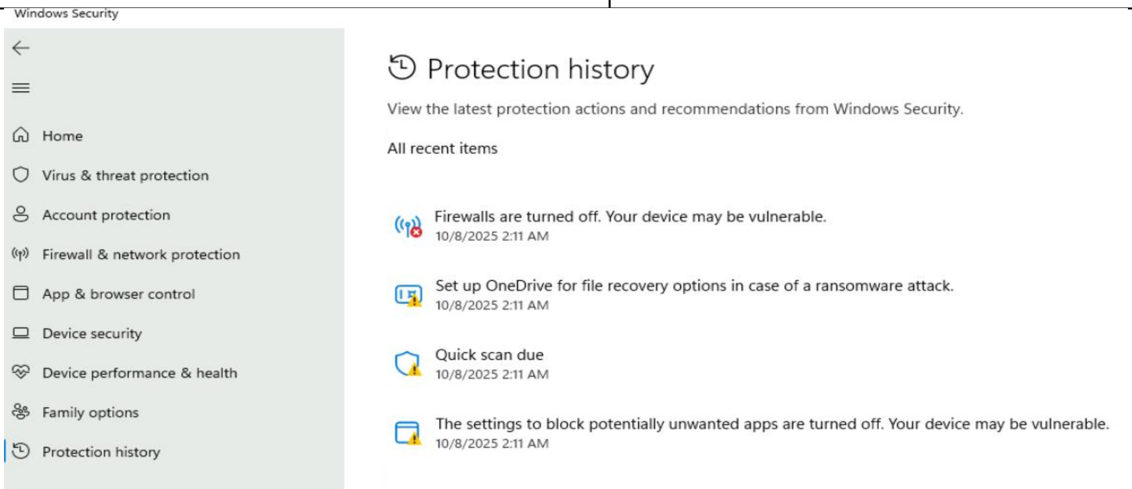
Never notify

Current Setting in UAC is Never Modify.

1. D. Status of the PC’s security settings

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

Security Feature	**Status**
Firewall product and status – Private network	Firewall in Private Network is turned off.
Firewall product and status – Public network	Firewall in Public Network is turned
Virus protection product and status	Quick Scan is due, and device may be vulnerable right now. (sc attached below)
User Account Control Setting	Never modify



Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Firewalls are turned off. Your device may be vulnerable.
10/8/2025 2:11 AM

Set up OneDrive for file recovery options in case of a ransomware attack.
10/8/2025 2:11 AM

Quick scan due
10/8/2025 2:11 AM

The settings to block potentially unwanted apps are turned off. Your device may be vulnerable.
10/8/2025 2:11 AM

1. Reconnaissance Wrap-up

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

Risk and Vulnerabilities with Joe’s PC are Softwares App , Network and Unpatched System

Windows Defender Firewall state is off therefore; hackers and Malicious software can gain access to Joe’s PC through Internet or a network.

Virus & Threat Protection is turned off which means it won’t scan files or detect any suspicious activity.

App Browser and Control are turned off which makes device vulnerable.

User Account Control Setting is set on Never Modify which means harmful programs may make changes to computer

2. Securing the PC

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:

1. Firewall - ensure the Windows Firewall is enabled for all network access.

2. Virus & Threat Protection - ensure the Windows Defender antivirus is enabled to always protect.

3. 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.

4. User Account Control settings - Done through the User Account Control Setting. To prevent potentially harmful programs from making changes and wants to be notified whenever apps try to make changes to his computer.

5. Securing Removable Media – It protects against threats, unauthorized access and non-compliance as well.

2. A. Firewall

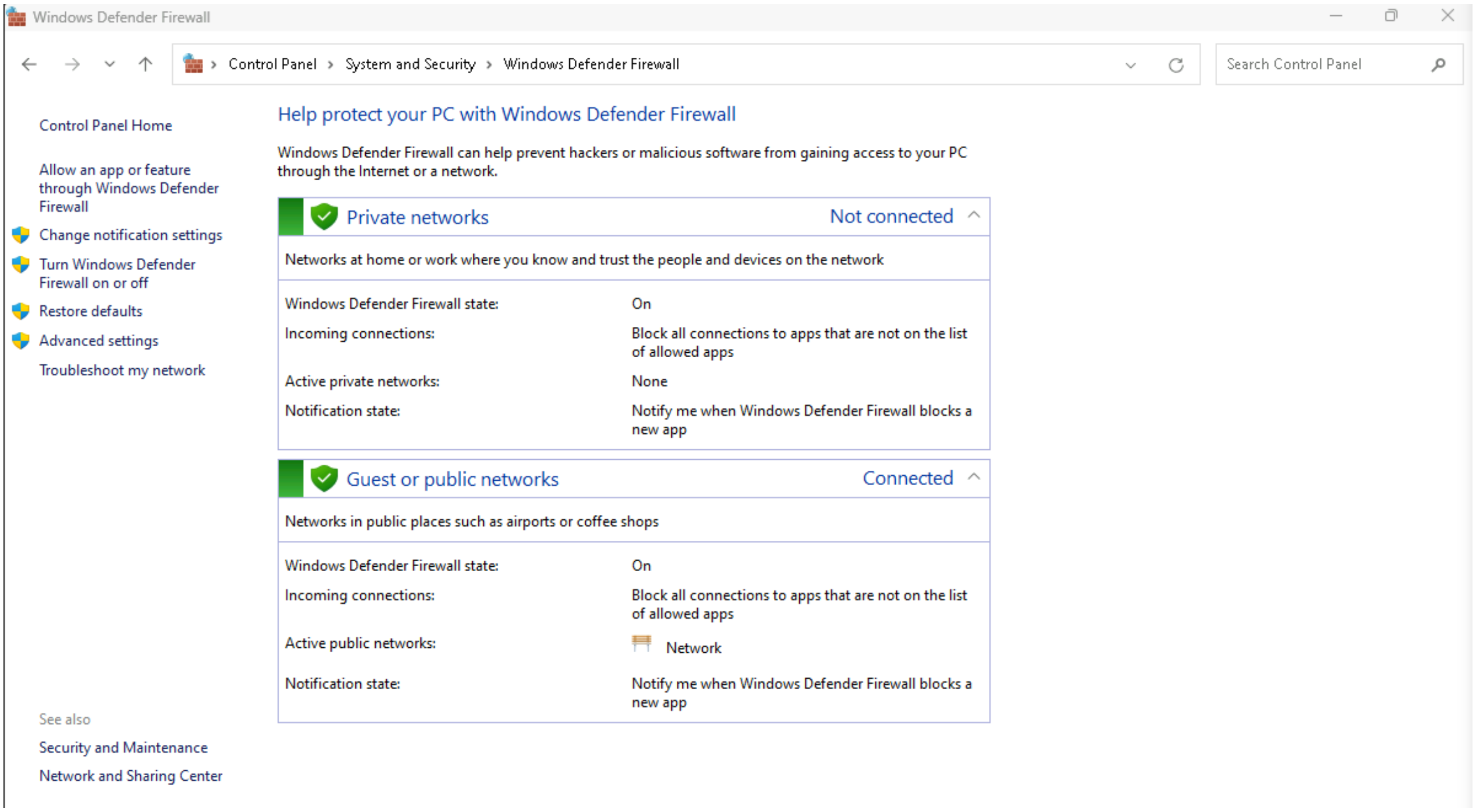
You need to ensure the Windows Firewall is enabled for all network access. Explain the process you take to do this.

⚠ **Important Note:**

Perform this step at the end of your project.

Once you enable the firewall, it may begin **blocking Remote Desktop Protocol (RDP) connections**, which could prevent you from reconnecting to the virtual machine. To avoid losing access, complete all other configurations first. Only **turn the firewall on as your final step** after ensuring all necessary settings and screenshots have been captured.

- Include screenshots showing the firewall is turned on.



Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
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
See also
Security and Maintenance
Network and Sharing Center

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.

Private networks — Not connected

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

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	None
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Connected

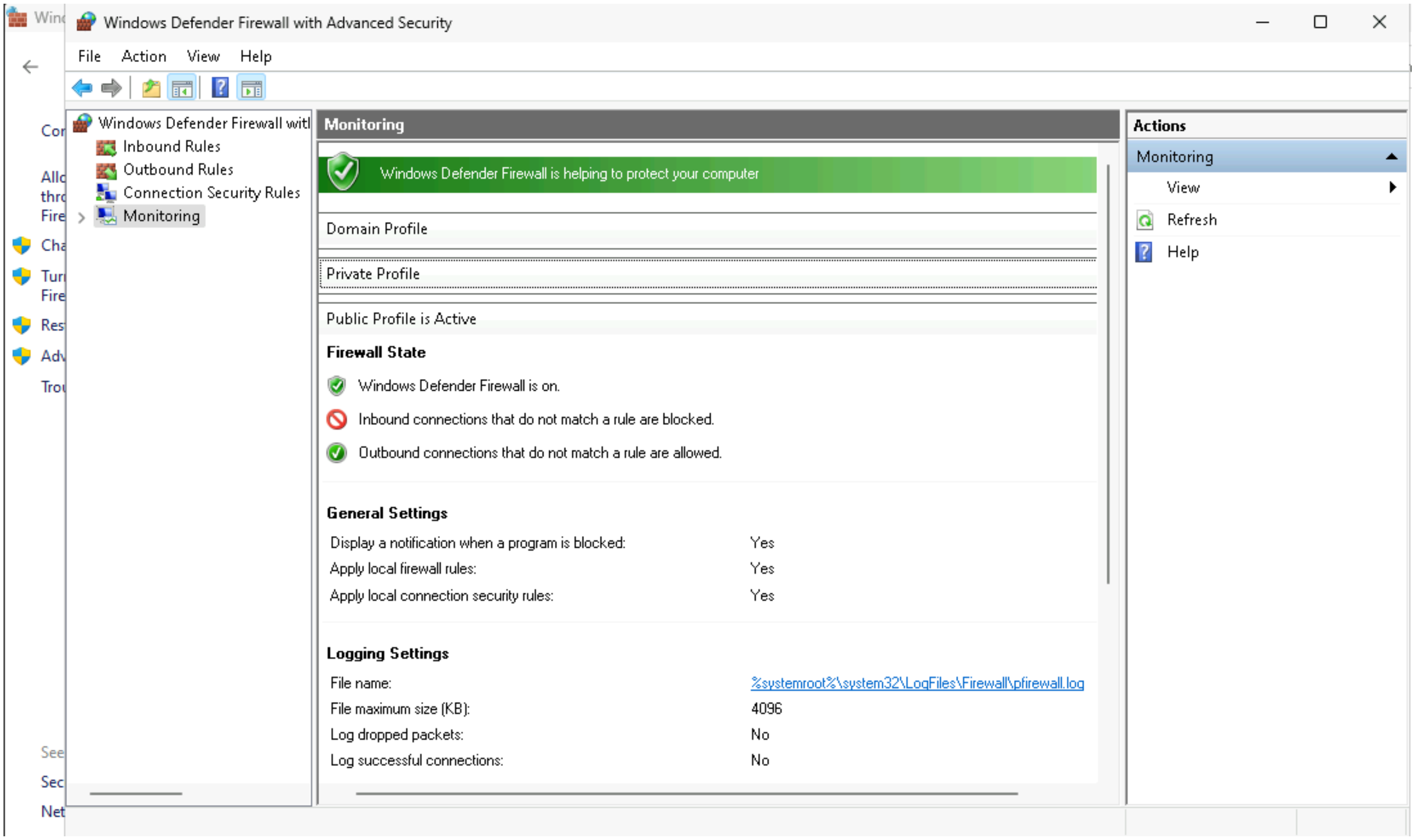
Networks in public places such as airports or coffee shops

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

2. A. Firewall

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

- Include screenshots showing the firewall is turned on.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Monitoring
View
Refresh
Help

Monitoring

Windows Defender Firewall is helping to protect your computer

Domain Profile

Private Profile

Public Profile is Active

Firewall State

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

General Settings

Display a notification when a program is blocked: Yes
Apply local firewall rules: Yes
Apply local connection security rules: Yes

Logging Settings

File name: %systemroot%\system32\LogFiles\Firewall\pfirewall.log
File maximum size (KB): 4096
Log dropped packets: No
Log successful connections: No

2. A. Firewall

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

- What protection does this provide?

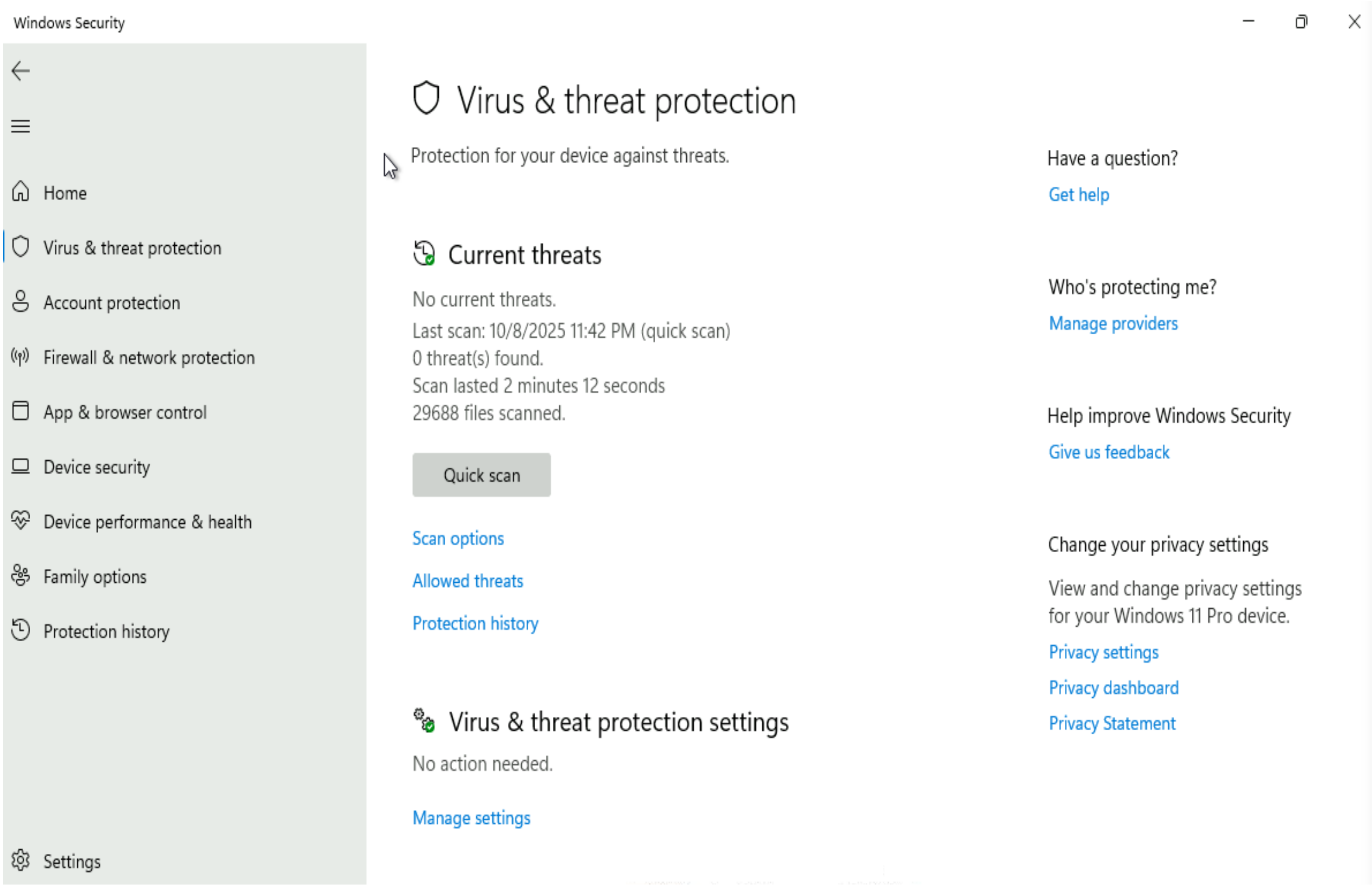
- Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through internet or any network.

- It blocks all the connections to the application that are not on the list of allowed apps.

- It sends notification when Windows Defender Firewall blocks a new app.

2. B. Virus & Threat Protection

You need to ensure the Windows Defender antivirus 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. Include screenshots to confirm that antivirus protection is enabled and a quick scan has been performed.



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 10/8/2025 11:42 PM (quick scan)
0 threat(s) found.
Scan lasted 2 minutes 12 seconds
29688 files scanned.

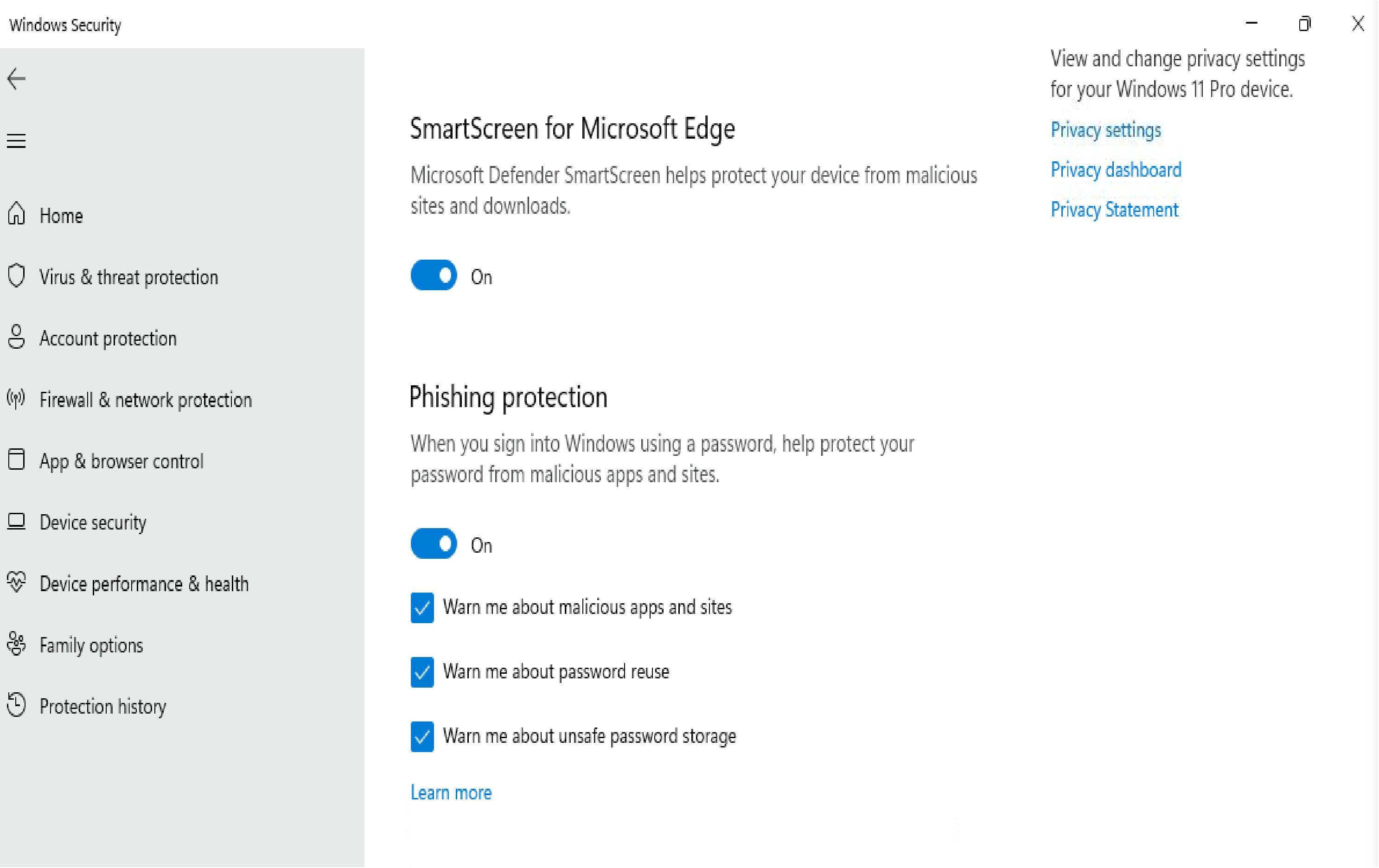
Virus & threat protection settings

No action needed.

View and change privacy settings for your Windows 11 Pro device.

2. C. App & Browser Control

To maximize protection for Joe's PC, enable all reputation-based protection features as follows: Review the settings in App & browser control windows found on the Windows Security page. Use Start > Windows Security> App & browser control> Reputation-based protection settings. Then enable all available protections for maximum security and provide a screenshot of your results, below.



SmartScreen for Microsoft Edge

Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.

On

Phishing protection

When you sign into Windows using a password, help protect your password from malicious apps and sites.

On

☑ Warn me about malicious apps and sites

☑ Warn me about password reuse

☑ Warn me about unsafe password storage

Learn more

View and change privacy settings for your Windows 11 Pro device.

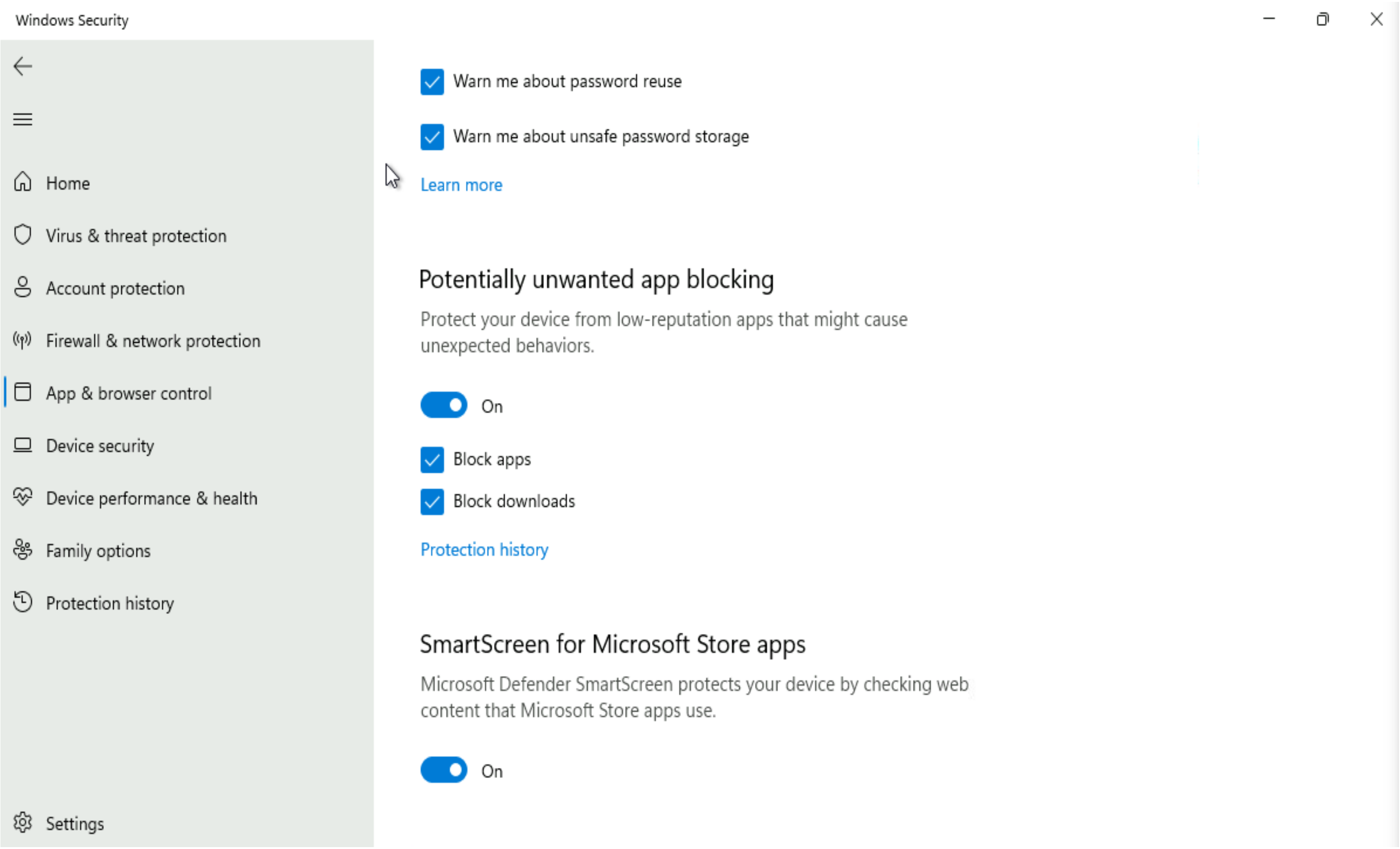
Privacy settings

Privacy dashboard

Privacy Statement

2. C. App & Browser Control

To maximize protection for Joe’s PC, enable all reputation-based protection features as follows: Review the settings in App & browser control windows found on the Windows Security page. Use Start > Windows Security> App & browser control> Reputation-based protection settings. Then enable all available protections for maximum security and provide a screenshot of your results, below.



Windows Security

☑ Warn me about password reuse

☑ Warn me about unsafe password storage

Learn more

Potentially unwanted app blocking

Protect your device from low-reputation apps that might cause unexpected behaviors.

● On

☑ Block apps

☑ Block downloads

Protection history

SmartScreen for Microsoft Store apps

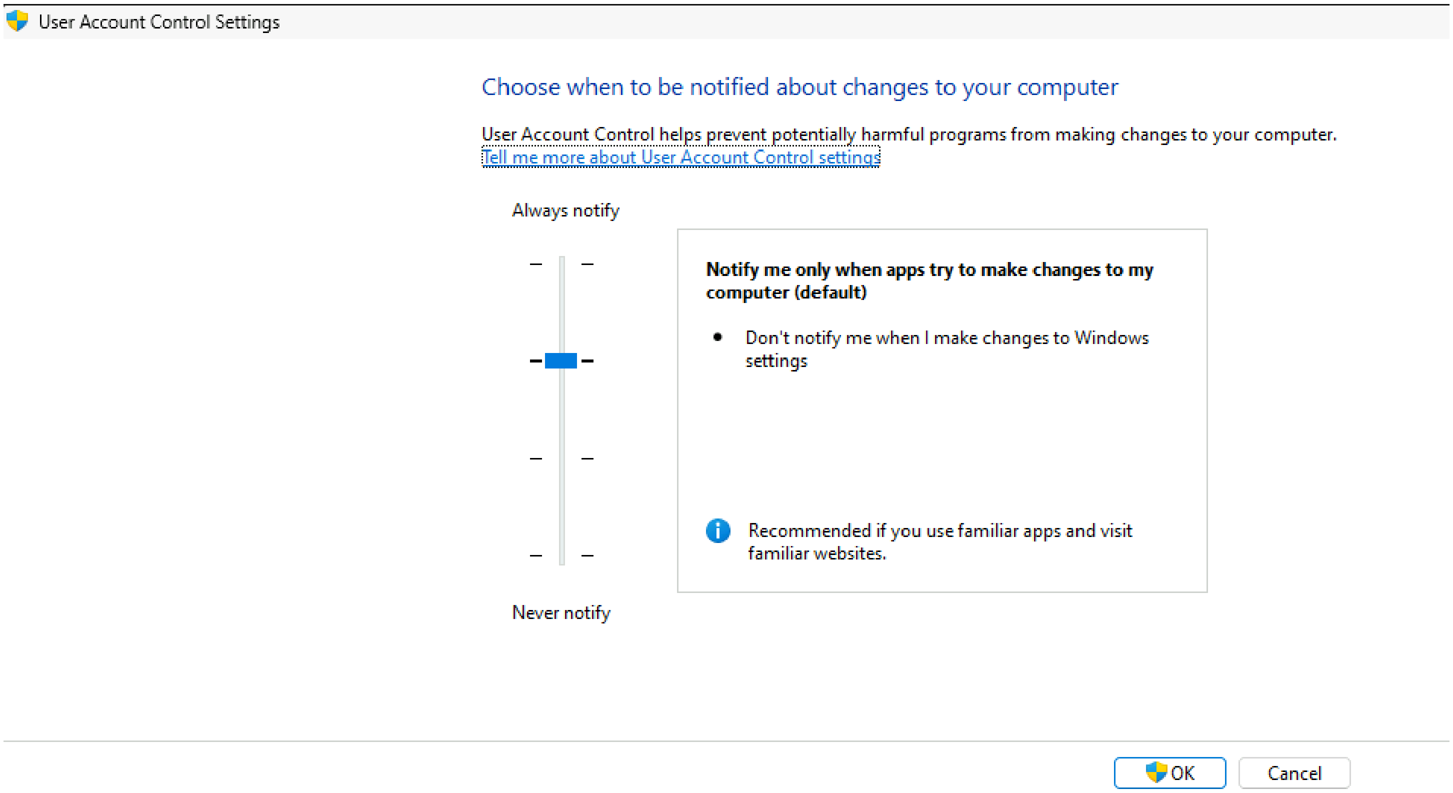
Microsoft Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.

● On

2. D. User Account Control Settings

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

- What is the current UAC setting on Joe's computer?
- Search > type "UAC" > Change User Account Control settings
- What should it be set to? Include a screenshot of the new setting.



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

Notify me only when apps try to make changes to my computer (default)

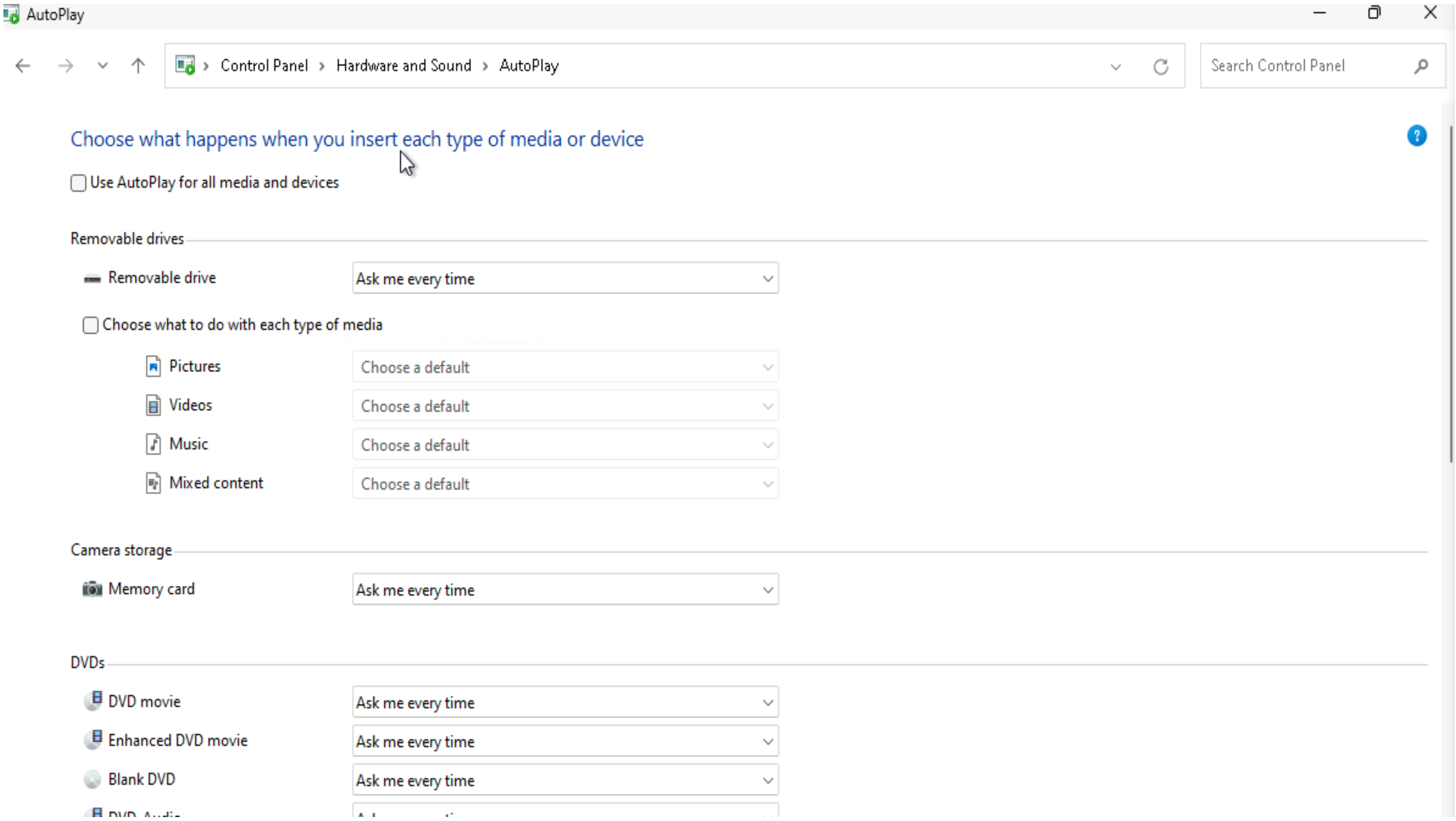
- Don't notify me when I make changes to Windows settings

Recommended if you use familiar apps and visit familiar websites.

2. E. Securing Removable Media

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

- On Joe's computer, go to that function and deselect "Use AutoPlay for all media and devices."
- For the Removable Drive, make the default, "Ask me every time." Include a screenshot of your results.



AutoPlay

Control Panel › Hardware and Sound › AutoPlay

Search Control Panel

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

☐ Use AutoPlay for all media and devices

Removable drives

Removable drive: Ask me every time

☐ Choose what to do with each type of media

Pictures: Choose a default

Videos: Choose a default

Music: Choose a default

Mixed content: Choose a default

Camera storage

Memory card: Ask me every time

DVDs

DVD movie: Ask me every time

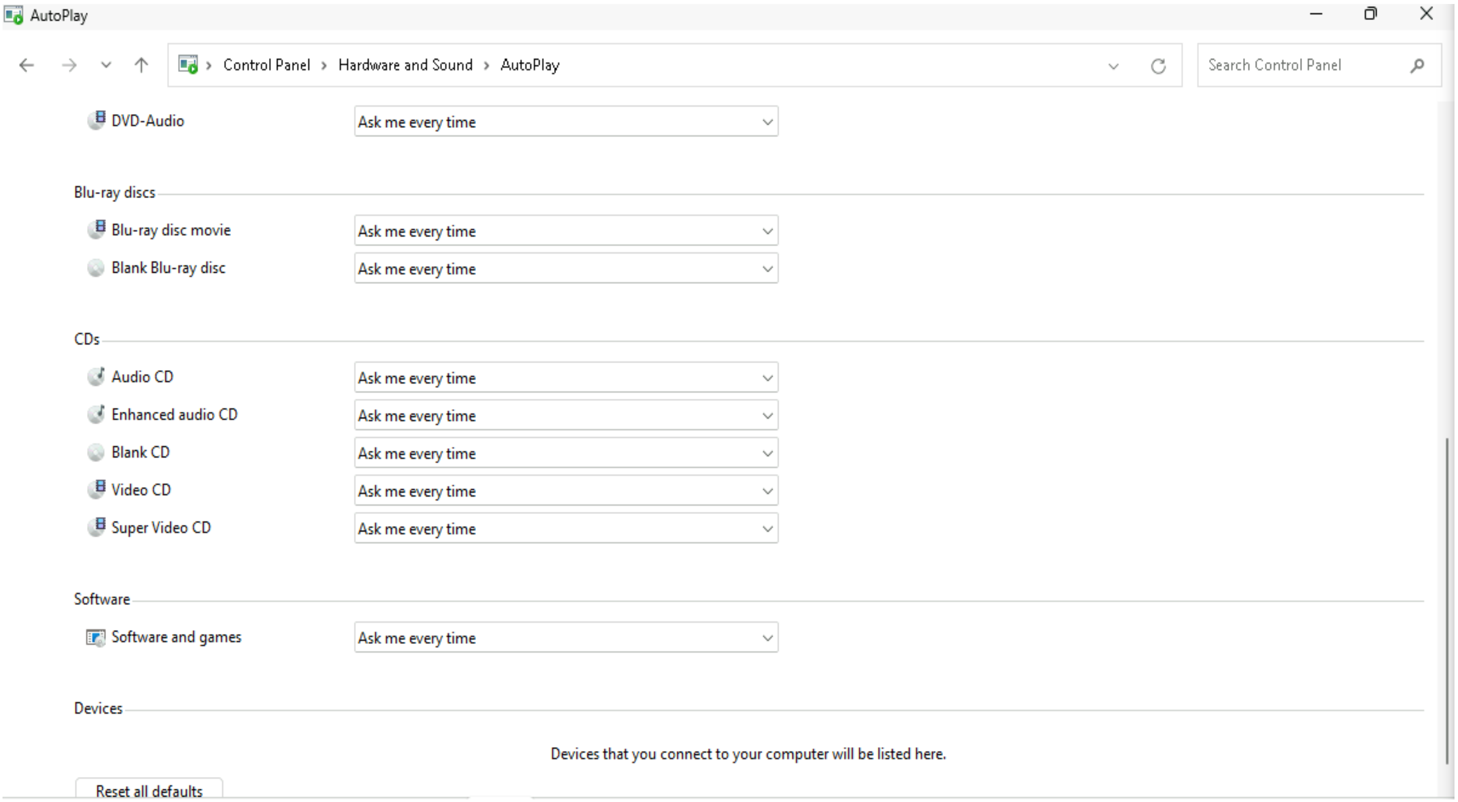
Enhanced DVD movie: Ask me every time

Blank DVD: Ask me every time

2. E. Securing Removable Media

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

- On Joe's computer, go to that function and deselect "Use AutoPlay for all media and devices."
- For the Removable Drive, make the default, "Ask me every time." Include a screenshot of your results.



DVD-Audio: Ask me every time

Blu-ray discs

Blu-ray disc movie: Ask me every time
Blank Blu-ray disc: Ask me every time

CDs

Audio CD: Ask me every time
Enhanced audio CD: Ask me every time
Blank CD: Ask me every time
Video CD: Ask me every time
Super Video CD: Ask me every time

Software

Software and games: Ask me every time

Devices

Devices that you connect to your computer will be listed here.

3. Securing Access

Ensuring only specific people have access to a computer system is necessary. It starts by understanding who should have access and the rules or policies that need to be followed. **Only these accounts should exist on Joe's computer:**

- 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.
- 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.

Joe's password policies:

- 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 and locked for 15 minutes.

3. A. User Accounts

1. What user accounts should not be there?
2. Explain the steps you take to disable or remove unwanted accounts.
3. Why is it important to disable or remove unneeded accounts from a PC or application? Include potential vulnerabilities and risks.

Answers:

1. Frank and Hacker

2. Go to Control Paner → Click on User Accounts → Click on Remove User Accounts under User Accounts → Choose the Account → Click on Delete the Account → Delete Files → Confirm Deletion.

3. To improve Application Security , prevent unauthorized access and data breaches.

3. B. Administrator Privilege

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

1. Which account(s) have administrator rights that shouldn’t?
2. Explain how you determined this. Provide screenshots as needed.
3. Provide at least three risks associated with users having administrator rights on a PC.

Provide screenshots and Answers in the next slide and add slides as needed.

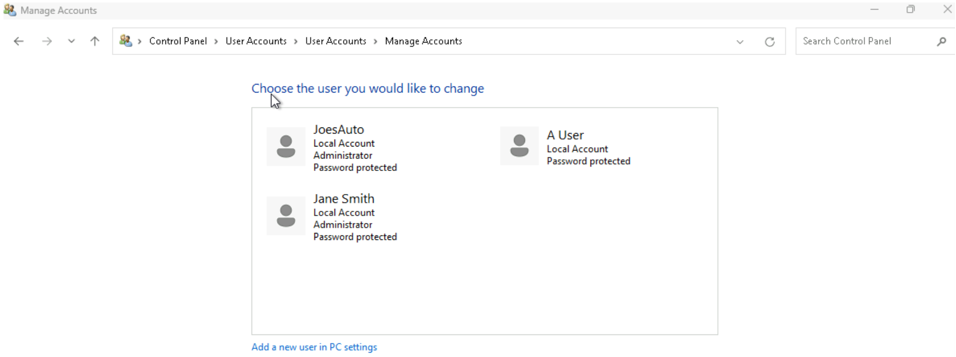
3. B. Administrator Privilege Answers

1 Which account(s) have administrator rights that shouldn't?

Jane Smith who is Joes assistant should not hold administrator privilege.

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

Start → Control Panel → Click on User Account → Click on Manage another Account and the list displays!


Manage Accounts
Control Panel › User Accounts › User Accounts › Manage Accounts
Search Control Panel

Choose the user you would like to change

JoesAuto
Local Account
Administrator
Password protected

A User
Local Account
Password protected

Jane Smith
Local Account
Administrator
Password protected

Add a new user in PC settings

3. B. Administrator Privilege Answers

3.	Provide at least three risks associated with users having administrator rights on a PC. • Unauthorized Software could be installed. • Data breach due to access to all the files and system settings. • Vulnerable to attacks such as ransomware and phishing.

3. C. 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. On the Windows search bar, type “Local Security Policy” to access it. Click the > arrow next to both “Account Policies” and “Local Policies” and review their contents.

- Provide a screenshot of the Local Security Policy window here.[Note: Local Security Policy is not available on Windows Home editions.]
- Provide screenshots in the next slides, showing how you set the rules on the PC

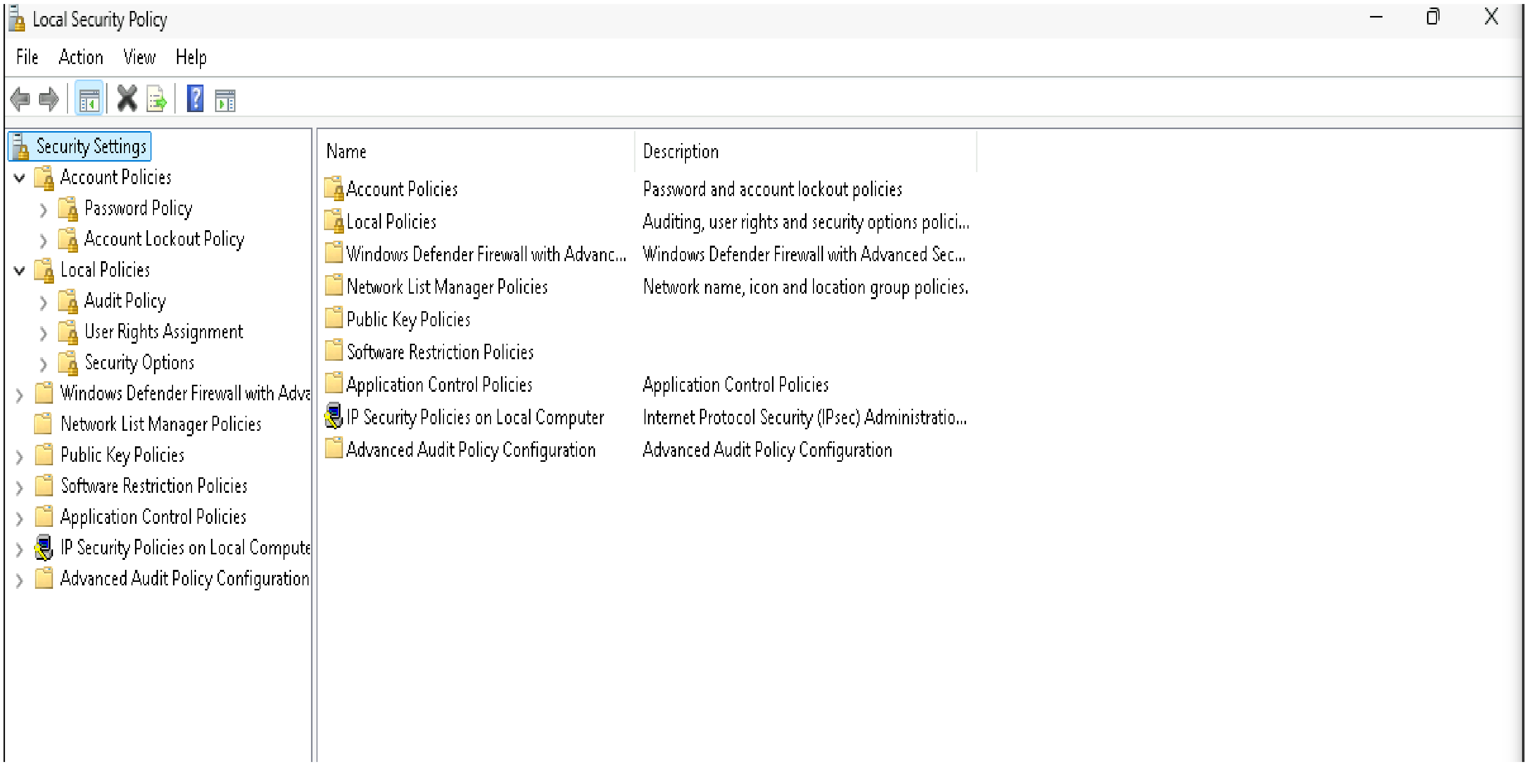
  1. Setting the Password Policy.

  2. Setting the Account Lockout Policy

- Explain the process for setting the password and access control policies locally on a Windows 11 PC.

  Answer: Click on start → search Local Security Policy → Click on Account policies → click on password policy → set the desired length , age etc.→ select ok.

3. C. screenshot of the Local Security Policy window

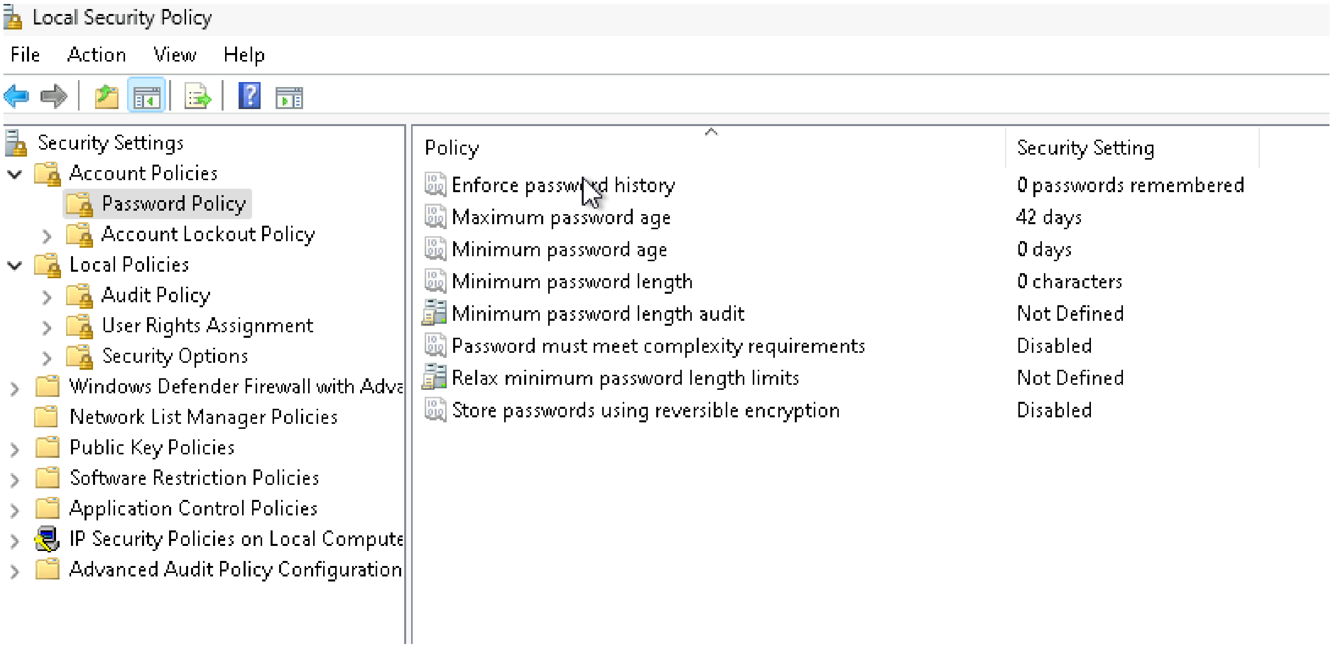


- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction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

3. C. Screenshot of Setting the Password Policy.

Before:



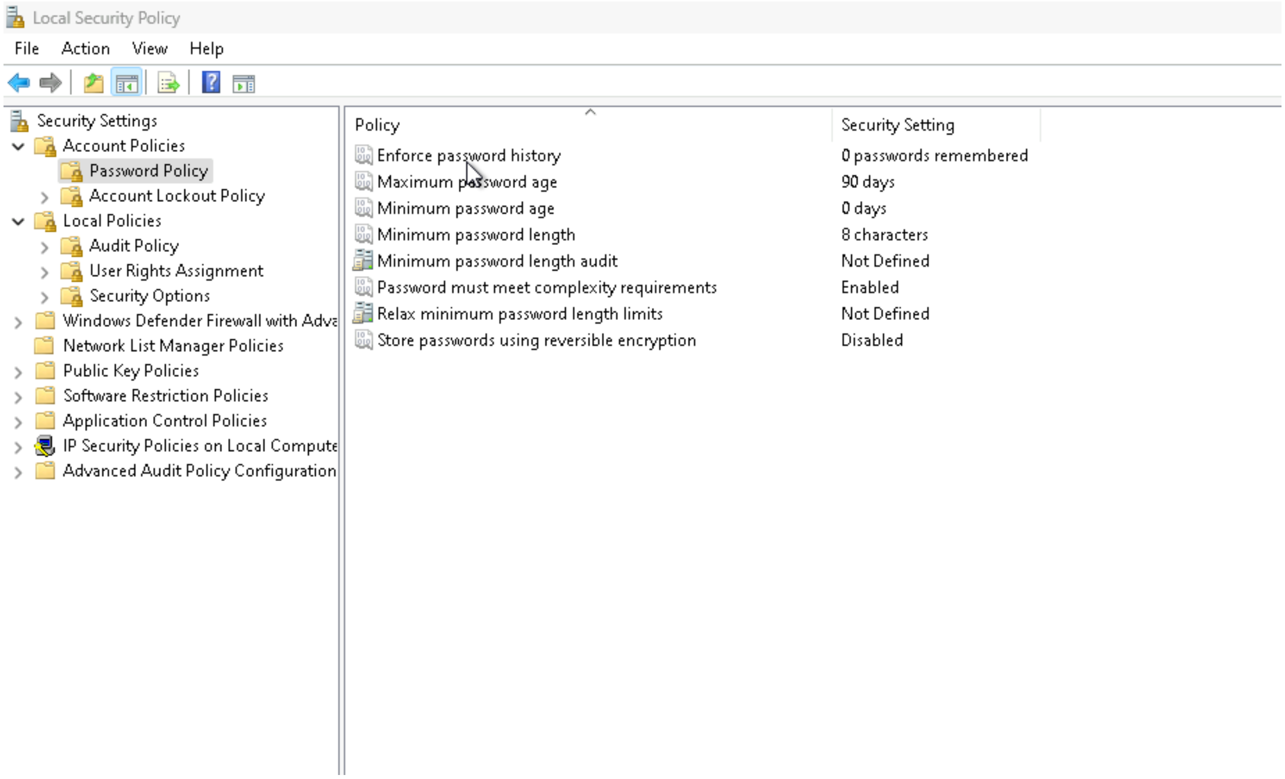
Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies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

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

3. C. Screenshot of Setting the Password Policy.

After:

- Maximum password age set to 90 days.
- Minimum password length to 8 characters.
- Password must meet complexity requirement setting **is enabled**.

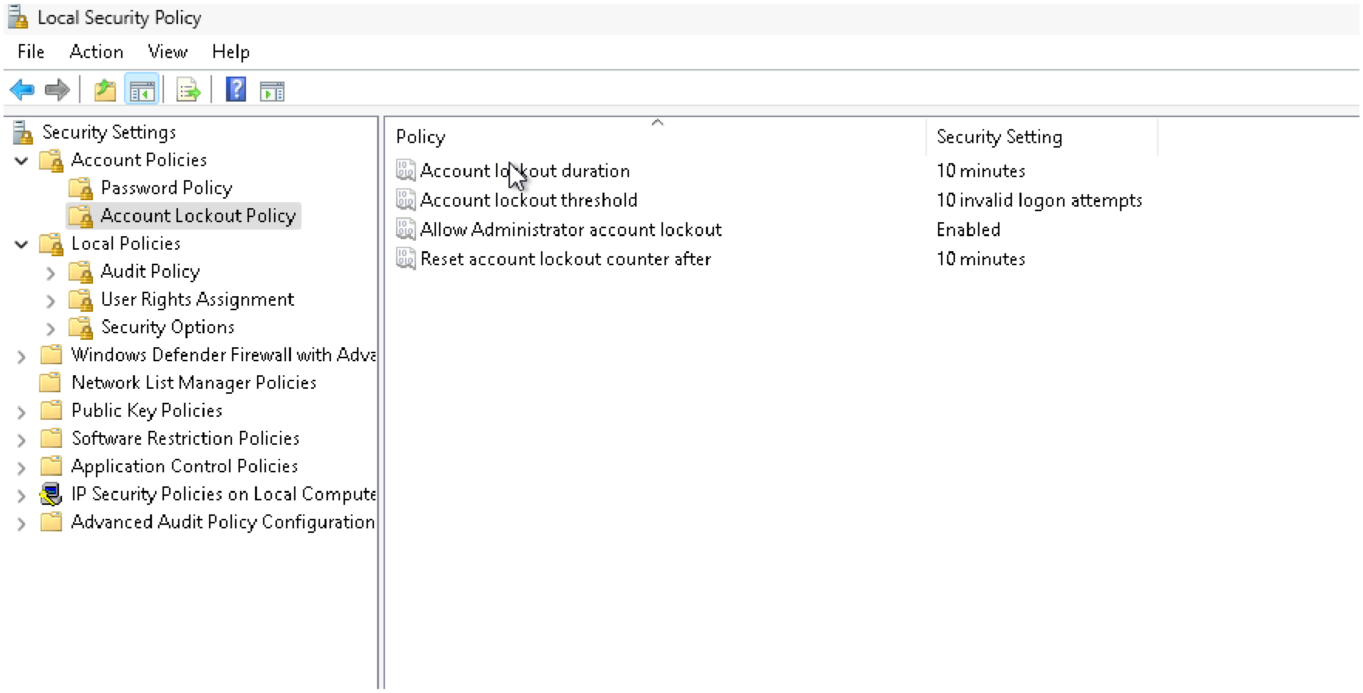


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies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

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	90 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

3. C. Screenshot of the Setting the Account Lockout Policy

Before:

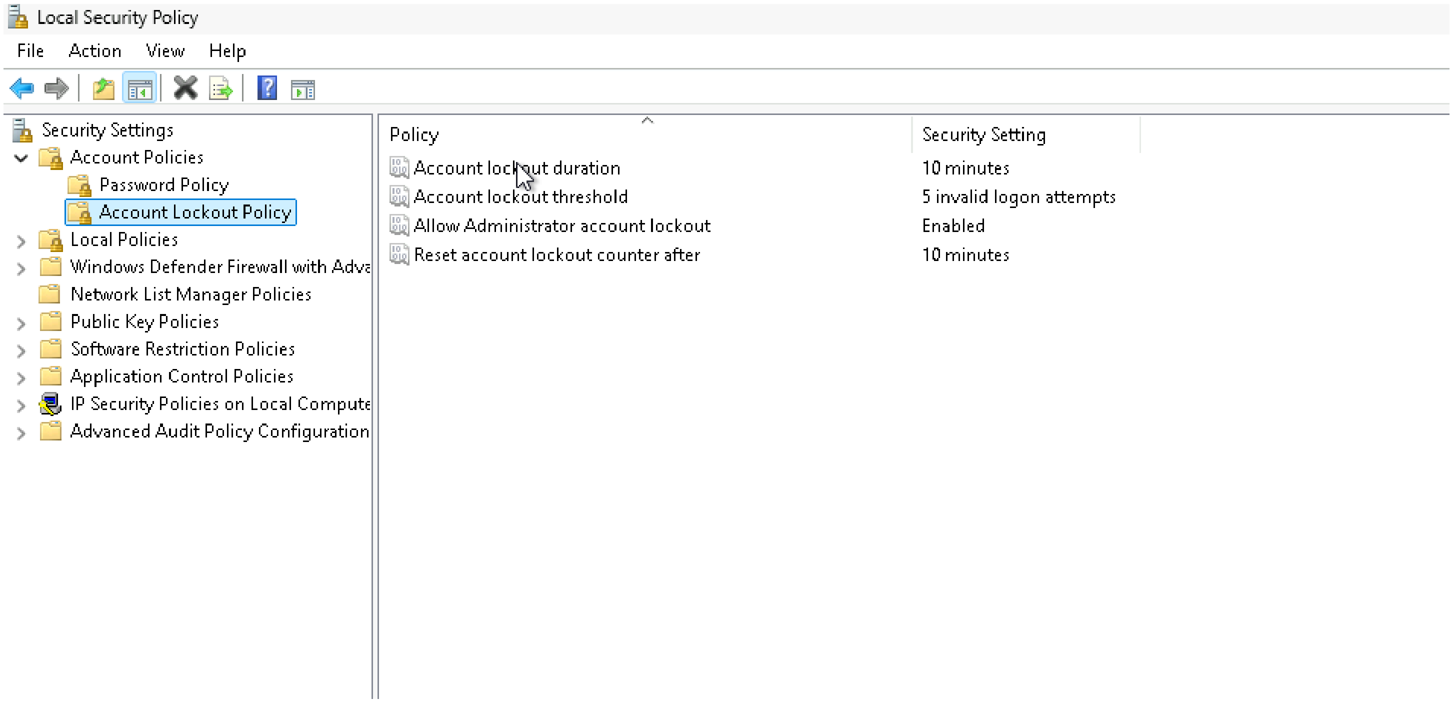

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies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

Policy	Security Setting
Account lockout duration	10 minutes
Account lockout threshold	10 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

3. C. Screenshot of the Setting the Account Lockout Policy

After:

Changed it to 5 logon attempts.



Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
Account lockout duration	10 minutes
Account lockout threshold	5 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

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.

Write your analysis on the next slide.

4. A. Remove unneeded or unwanted applications

Write your analysis below.	

1

Remove unneeded or unwanted applications

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

- *Media Monkey 2024*
- *Solitaire & Casual Games*
- *Xbox*

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

- *Attacks*
- *Phishing and Ransomware*
- *Data breach*

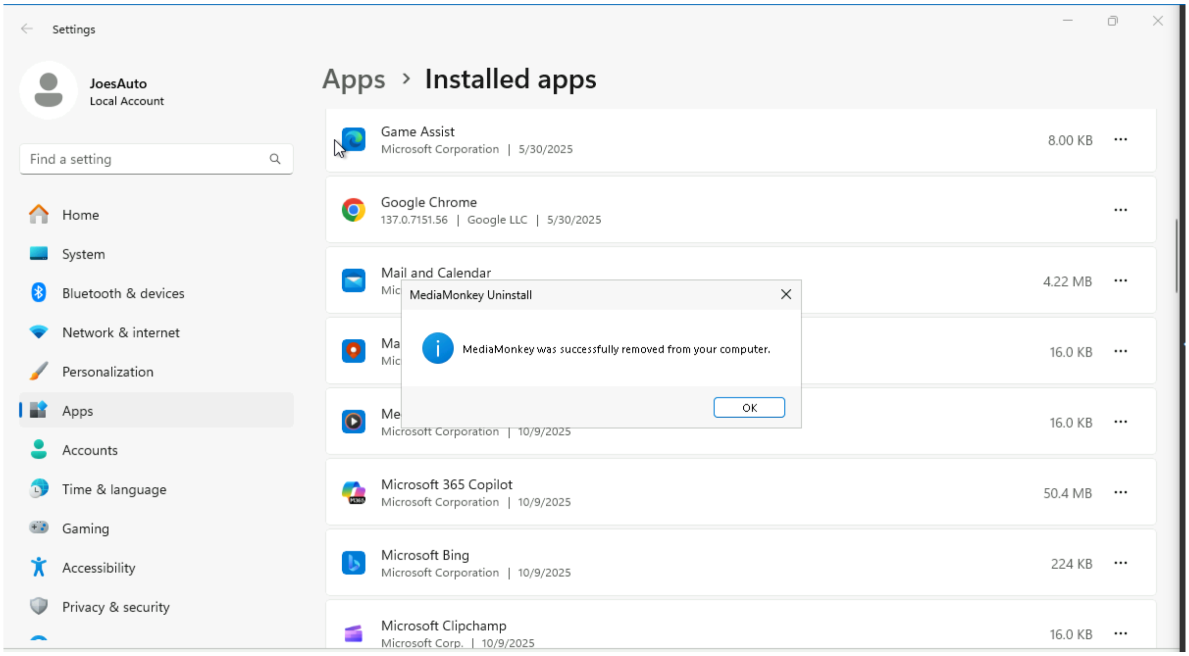
4. A. Remove unneeded or unwanted applications

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.

1

Start → search add or remove programs → click on the three dots of the app you want to be deleted → click uninstall.

Repeat the same steps for all the unneeded applications.



Apps › Installed apps

Game Assist
Microsoft Corporation | 5/30/2025 8.00 KB

Google Chrome
137.0.7151.56 | Google LLC | 5/30/2025

Mail and Calendar
Mic 4.22 MB

Ma
Mic 16.0 KB

Me
Microsoft Corporation | 10/9/2025 16.0 KB

Microsoft 365 Copilot
Microsoft Corporation | 10/9/2025 50.4 MB

Microsoft Bing
Microsoft Corporation | 10/9/2025 224 KB

Microsoft Clipchamp
Microsoft Corp. | 10/9/2025 16.0 KB

MediaMonkey Uninstall

MediaMonkey was successfully removed from your computer.

OK

[I deleted all 3 apps mentioned but it was very quick to capture screenshot of remaining two.]

4. B. Default Browser

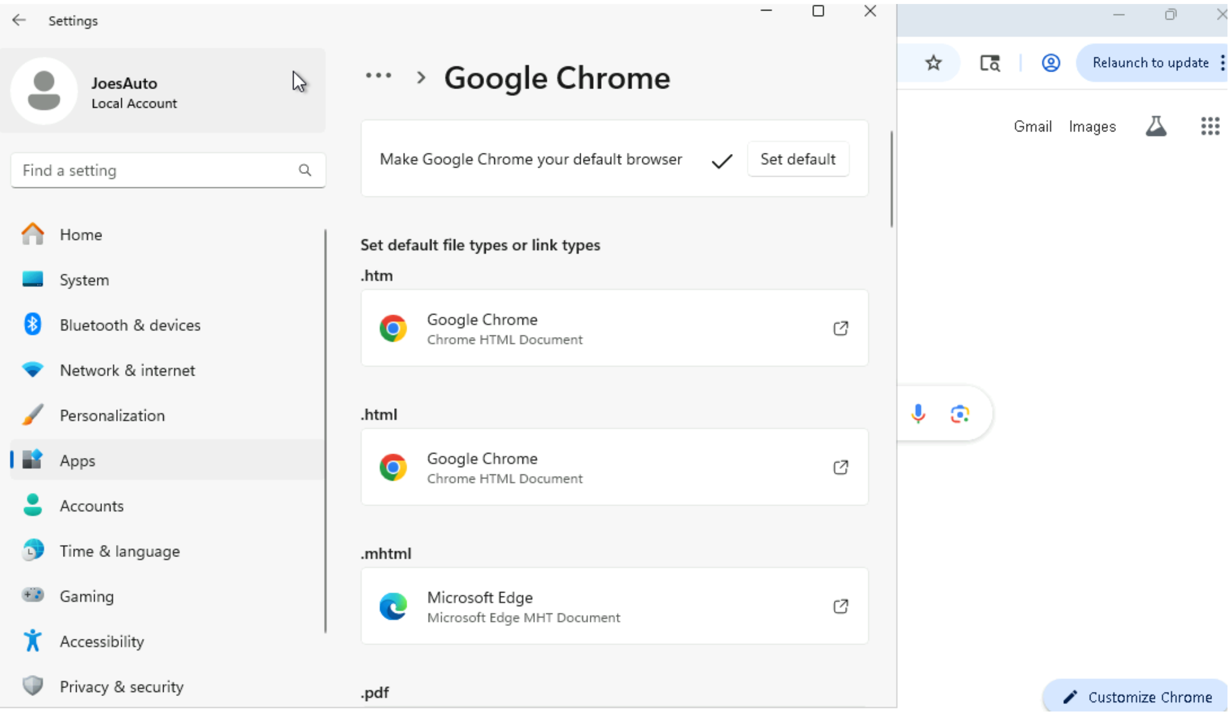
1 *As mentioned in the policy, Joe wants all users to use Chrome as their browser by default.*

1. *Explain how you set default applications within the Windows 11 operating system. Include screenshots as necessary.*

Start → Search chrome → click on three dots → select set chrome as default.

OR,

Start → search apps → click default app → select Google Chrome



··· › Google Chrome

Make Google Chrome your default browser ✓ Set default

Set default file types or link types

.htm
Google Chrome
Chrome HTML Document

.html
Google Chrome
Chrome HTML Document

.mhtml
Microsoft Edge
Microsoft Edge MHT Document

.pdf

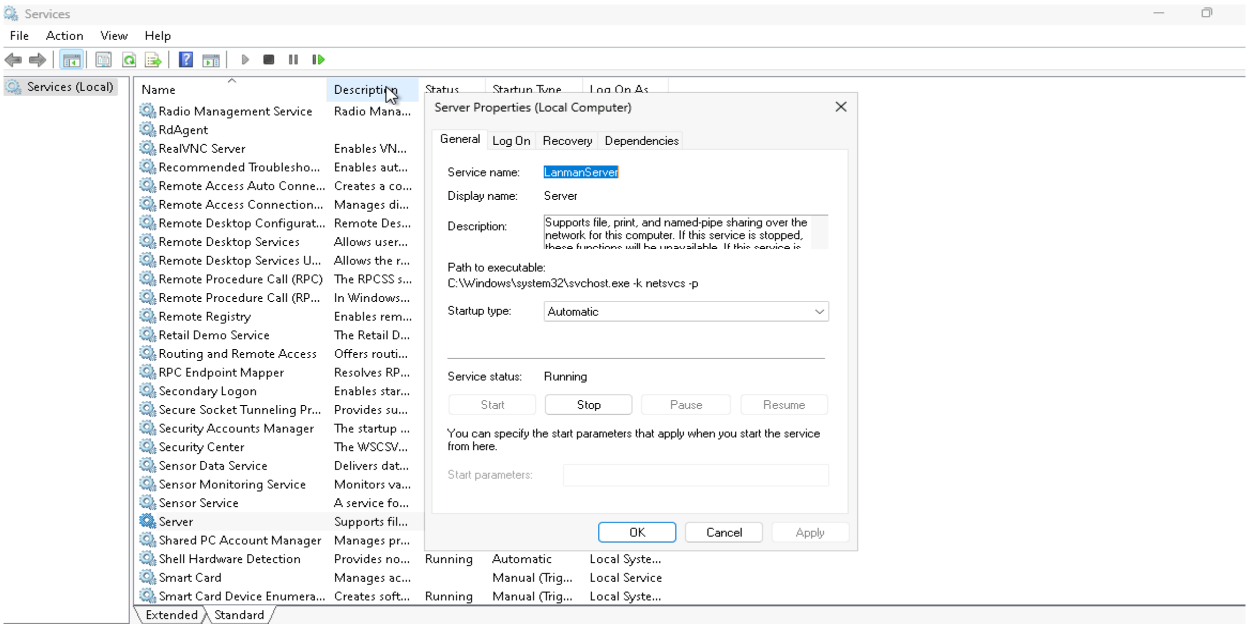
4. C. Windows Services

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. Determine what services were running? Look in the Services window to see if World Wide Web Publishing Service is running. Include screenshots to show that.

1

Server properties on Local Computer is Running.

It support File, print and named-pipe sharing over the network for Joes computer.



Name	Description	Status	Startup Type	Log On As
Radio Management Service	Radio Mana...			
RdAgent				
RealVNC Server	Enables VN...			
Recommended Troublesho...	Enables aut...			
Remote Access Auto Conne...	Creates a co...			
Remote Access Connection...	Manages di...			
Remote Desktop Configurat...	Remote Des...			
Remote Desktop Services	Allows user...			
Remote Desktop Services U...	Allows the r...			
Remote Procedure Call (RPC)	The RPCSS s...			
Remote Procedure Call (RP...	In Windows...			
Remote Registry	Enables rem...			
Retail Demo Service	The Retail D...			
Routing and Remote Access	Offers routi...			
RPC Endpoint Mapper	Resolves RP...			
Secondary Logon	Enables star...			
Secure Socket Tunneling Pr...	Provides su...			
Security Accounts Manager	The startup ...			
Security Center	The WSCSV...			
Sensor Data Service	Delivers dat...			
Sensor Monitoring Service	Monitors va...			
Sensor Service	A service fo...			
Server	Supports fil...			
Shared PC Account Manager	Manages pr...			
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card	Manages ac...		Manual (Trig...	Local Service
Smart Card Device Enumera...	Creates soft...	Running	Manual (Trig...	Local Syste...

Server Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: LanmanServer

Display name: Server

Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is

Path to executable:
C:\Windows\system32\svchost.exe -k netsvcs -p

Startup type: Automatic

Service status: Running

Start | Stop | Pause | Resume

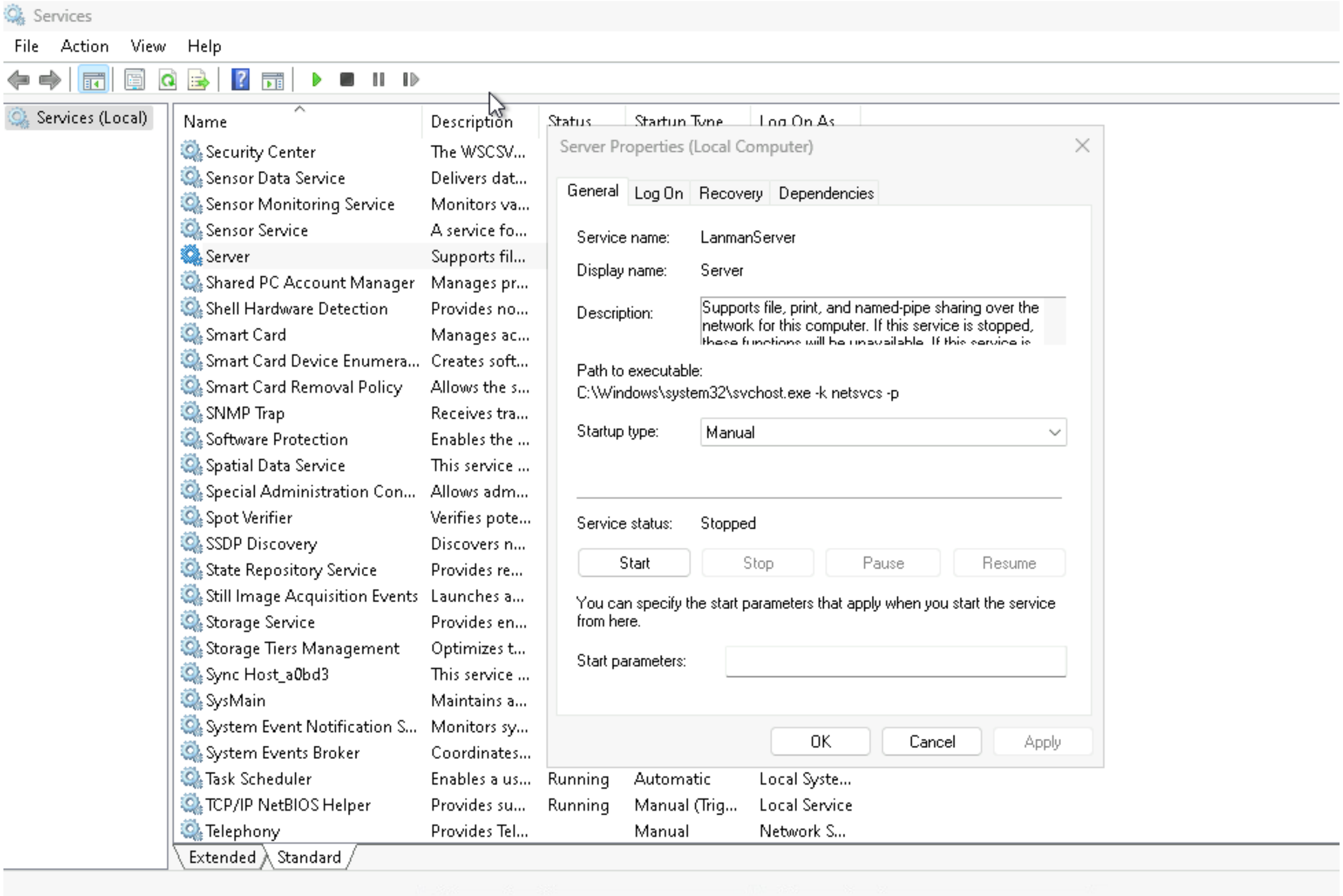
You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

4. C. Screenshot of the Services window

Stopped and set to Manual.



Name	Description	Status	Startup Type	Log On As
Security Center	The WSCSV...			
Sensor Data Service	Delivers dat...			
Sensor Monitoring Service	Monitors va...			
Sensor Service	A service fo...			
Server	Supports fil...			
Shared PC Account Manager	Manages pr...			
Shell Hardware Detection	Provides no...			
Smart Card	Manages ac...			
Smart Card Device Enumera...	Creates soft...			
Smart Card Removal Policy	Allows the s...			
SNMP Trap	Receives tra...			
Software Protection	Enables the ...			
Spatial Data Service	This service ...			
Special Administration Con...	Allows adm...			
Spot Verifier	Verifies pote...			
SSDP Discovery	Discovers n...			
State Repository Service	Provides re...			
Still Image Acquisition Events	Launches a...			
Storage Service	Provides en...			
Storage Tiers Management	Optimizes t...			
Sync Host_a0bd3	This service ...			
SysMain	Maintains a...			
System Event Notification S...	Monitors sy...			
System Events Broker	Coordinates...			
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Telephony	Provides Tel...		Manual	Network S...

Service name: LanmanServer

Display name: Server

Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is

Path to executable:
C:\Windows\system32\svchost.exe -k netsvcs -p

Startup type: Manual

Service status: Stopped

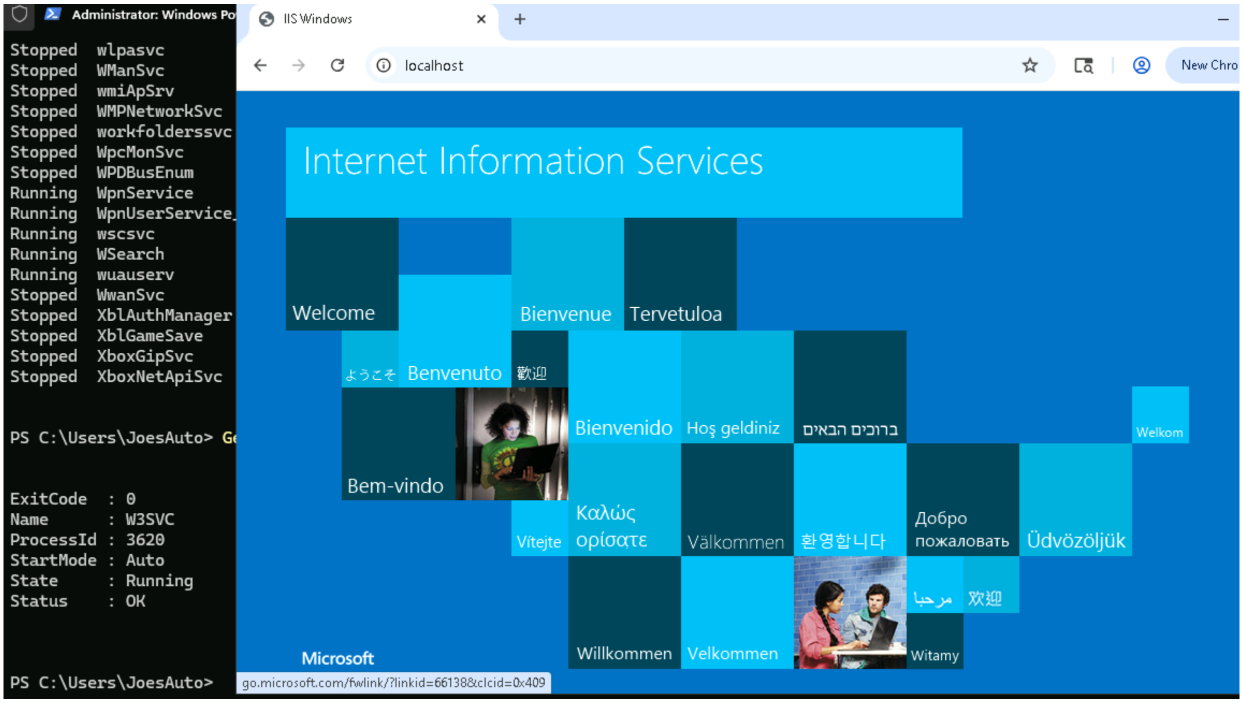
You can specify the start parameters that apply when you start the service from here.

Start parameters:

4. C. Web server status

- Run the Get-Service cmdlet in PowerShell and look for it in the list.
- Run Get-WmiObject Win32_Service -Filter "Name='W3SVC'" in PowerShell shows that a web server is running
- Browsing to http://localhost on the machine should display the site. Include screenshot showing the IIS window on the browser.

1



```
Administrator: Windows Po
Stopped   wlpasvc
Stopped   WManSvc
Stopped   wmiApSrv
Stopped   WMPNetworkSvc
Stopped   workfolderssvc
Stopped   WpcMonSvc
Stopped   WPDBusEnum
Running   WpnService
Running   WpnUserService_
Running   wscsvc
Running   WSearch
Running   wuauserv
Stopped   WwanSvc
Stopped   XblAuthManager
Stopped   XblGameSave
Stopped   XboxGipSvc
Stopped   XboxNetApiSvc


PS C:\Users\JoesAuto> Ge


ExitCode  : 0
Name      : W3SVC
ProcessId : 3620
StartMode : Auto
State     : Running
Status    : OK


PS C:\Users\JoesAuto>
```

5. A. Securing Files and Folders

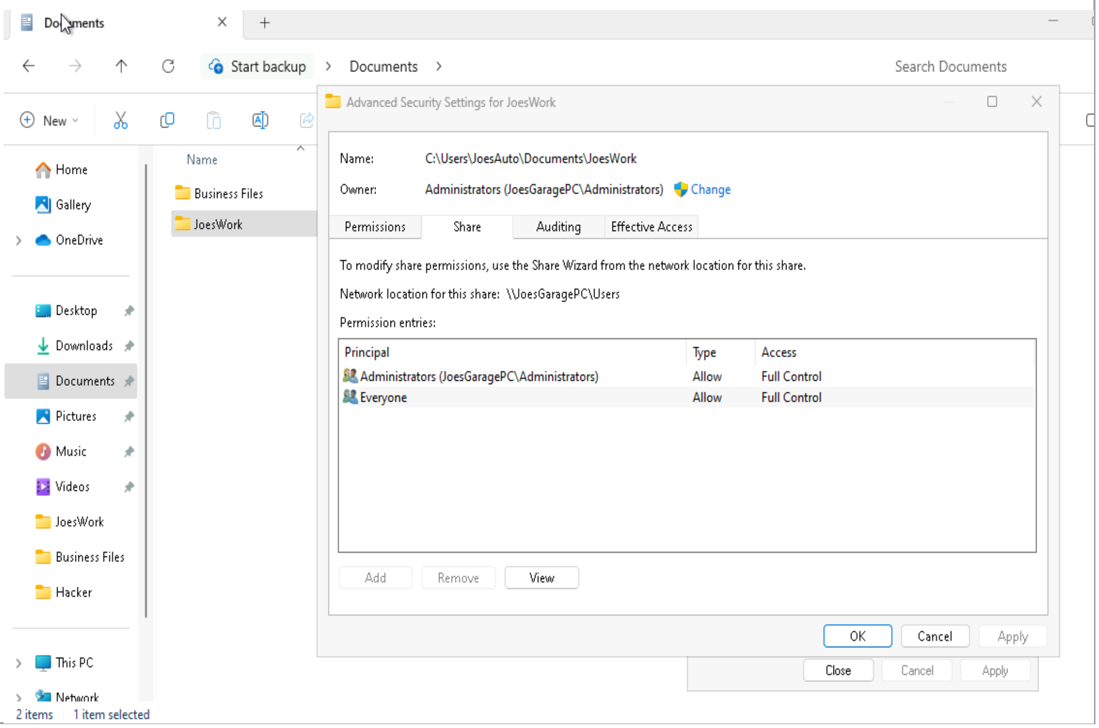
Joe has some work files in his Business folder that he wants to secure since they contain his customer information. They are labeled "JoesWork." Joe suspects that other users on this computer beside him and Jane can see and change his business files. He wants you to check to make sure that only those two users have privileges to view or change the files.

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.]

1

Navigate to folder "JoesWork" → right click → select properties → click on sharing (to view who has access)

The file is shared to everyone, and anyone can view and make changes to it.



Advanced Security Settings for JoesWork

Name: C:\Users\JoesAuto\Documents\JoesWork

Owner: Administrators (JoesGaragePC\Administrators) Change

Permissions | Share | Auditing | Effective Access

To modify share permissions, use the Share Wizard from the network location for this share.

Network location for this share: \\JoesGaragePC\Users

Permission entries:

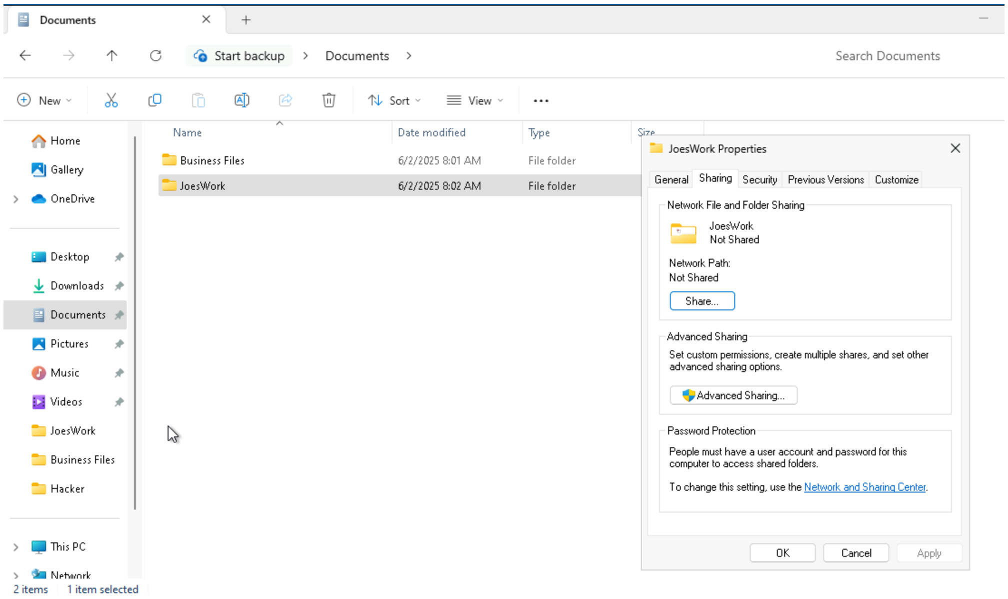
Principal	Type	Access
Administrators (JoesGaragePC\Administrators)	Allow	Full Control
Everyone	Allow	Full Control

Add | Remove | View

OK | Cancel | Apply

5. A. Securing Files and Folders

1 *More screenshot of unprotected files.*



Name	Date modified	Type	Size
Business Files	6/2/2025 8:01 AM	File folder	
JoesWork	6/2/2025 8:02 AM	File folder	

2 items 1 item selected

JoesWork Properties

Network File and Folder Sharing

JoesWork
Not Shared

Network Path:
Not Shared

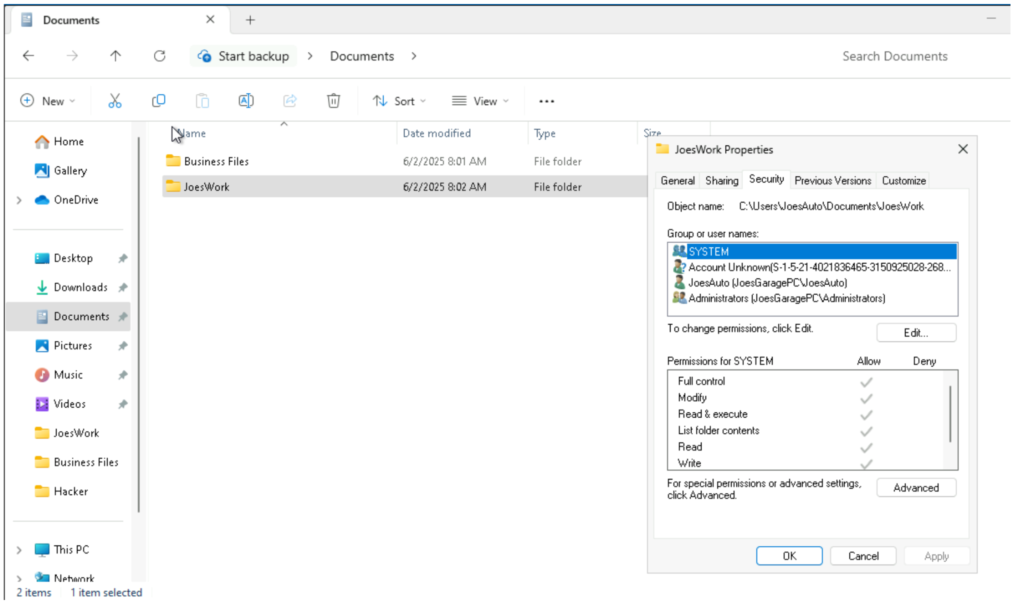
Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.



Name	Date modified	Type	Size
Business Files	6/2/2025 8:01 AM	File folder	
JoesWork	6/2/2025 8:02 AM	File folder	

2 items 1 item selected

JoesWork Properties

Object name: C:\Users\JoesAuto\Documents\JoesWork

Group or user names:

SYSTEM
Account Unknown(S-1-5-21-4021836465-3150925028-268...
JoesAuto (JoesGaragePC\JoesAuto)
Administrators (JoesGaragePC\Administrators)

To change permissions, click Edit.

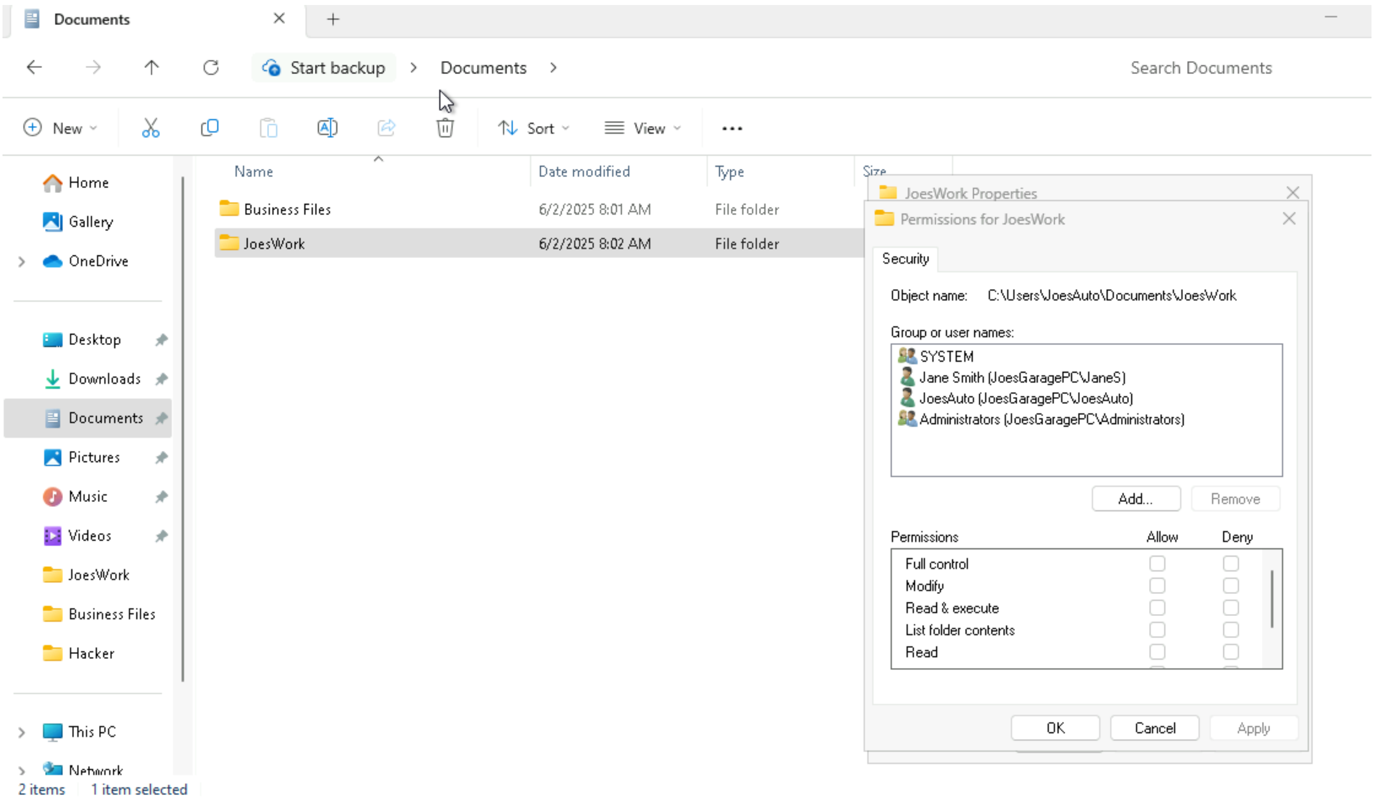
Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

5. A. Securing Files and Folders

1

Changed the setting → shared with Jane and removed everyone.



Name	Date modified	Type	Size
Business Files	6/2/2025 8:01 AM	File folder	
JoesWork	6/2/2025 8:02 AM	File folder	

Object name: C:\Users\JoesAuto\Documents\JoesWork

Group or user names:

- SYSTEM
- Jane Smith (JoesGaragePC\JaneS)
- JoesAuto (JoesGaragePC\JoesAuto)
- Administrators (JoesGaragePC\Administrators)

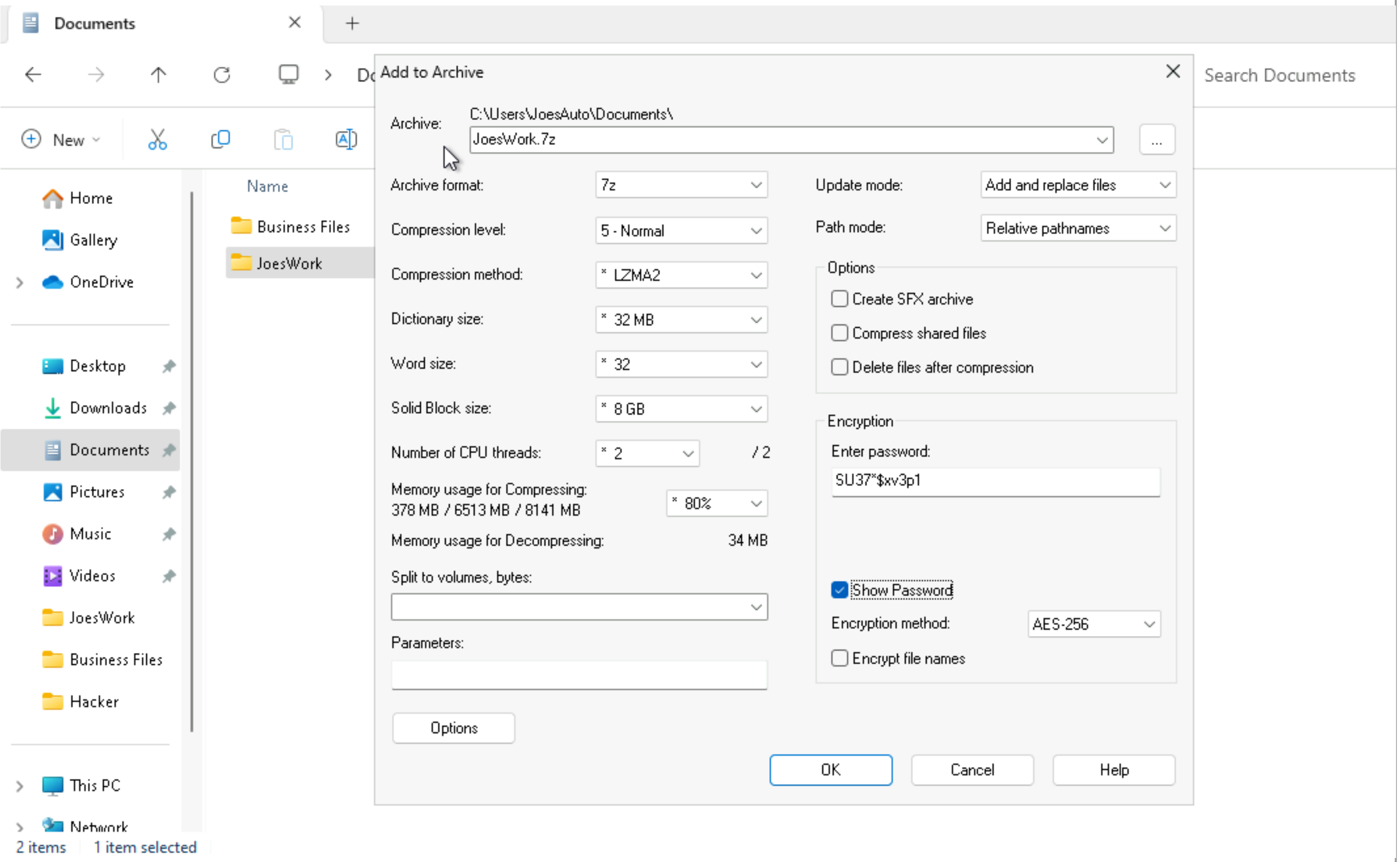
Permissions	Allow	Deny
Full control	☐	☐
Modify	☐	☐
Read & execute	☐	☐
List folder contents	☐	☐
Read	☐	☐

5. B. Securing Files and Folders

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.

3. What security fundamentals does this provide?

2. *Right click on the folder “JoesWork” under document → show more options → Click on 7-zip → Add to archive → Encrypt with password → select ok.*



Archive: C:\Users\JoesAuto\Documents\
JoesWork.7z

Archive format: 7z
Compression level: 5 - Normal
Compression method: * LZMA2
Dictionary size: * 32 MB
Word size: * 32
Solid Block size: * 8 GB
Number of CPU threads: * 2 / 2
Memory usage for Compressing: 378 MB / 6513 MB / 8141 MB * 80%
Memory usage for Decompressing: 34 MB
Split to volumes, bytes:
Parameters:

Update mode: Add and replace files
Path mode: Relative pathnames

Options
□ Create SFX archive
□ Compress shared files
□ Delete files after compression

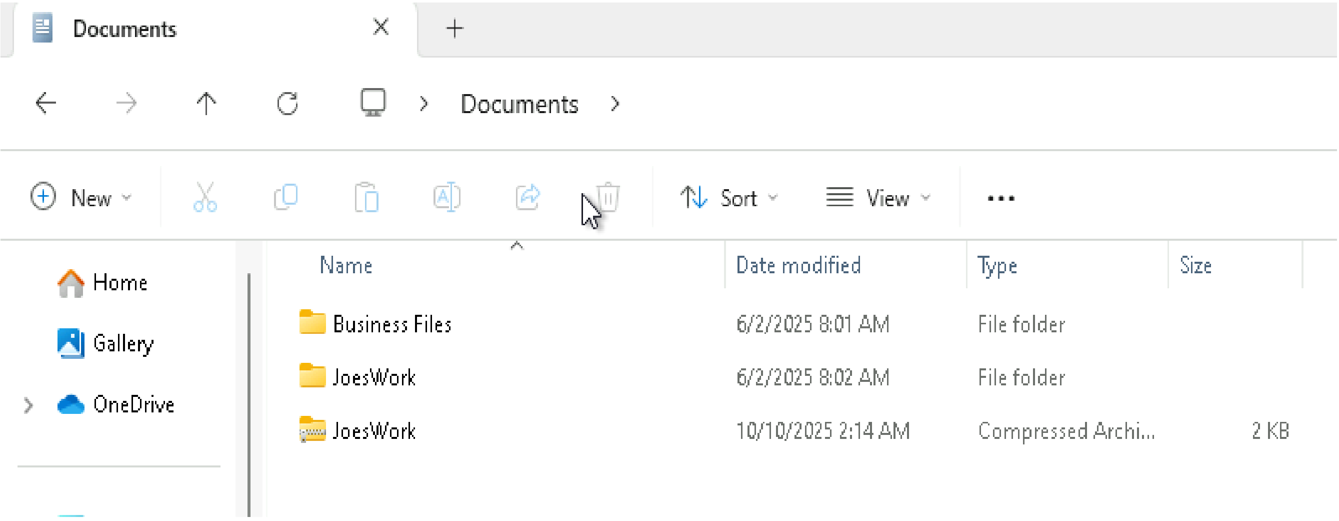
Encryption
Enter password:
SU37*$xv3p1
☑ Show Password
Encryption method: AES-256
□ Encrypt file names

5. B. Securing Files and Folders

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.

3. What security fundamentals does this provide?

2. *It should create a separate zipped file.*



Name	Date modified	Type	Size
Business Files	6/2/2025 8:01 AM	File folder	
JoesWork	6/2/2025 8:02 AM	File folder	
JoesWork	10/10/2025 2:14 AM	Compressed Archi...	2 KB

5. B. Securing Files and Folders

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.

3. What security fundamentals does this provide?

3.	*It provides CIA → Confidentiality , Integrity and Availability.* *It is highly confidential, the data is trust-worthy, and they are accessible for the authorized users when they need them.*

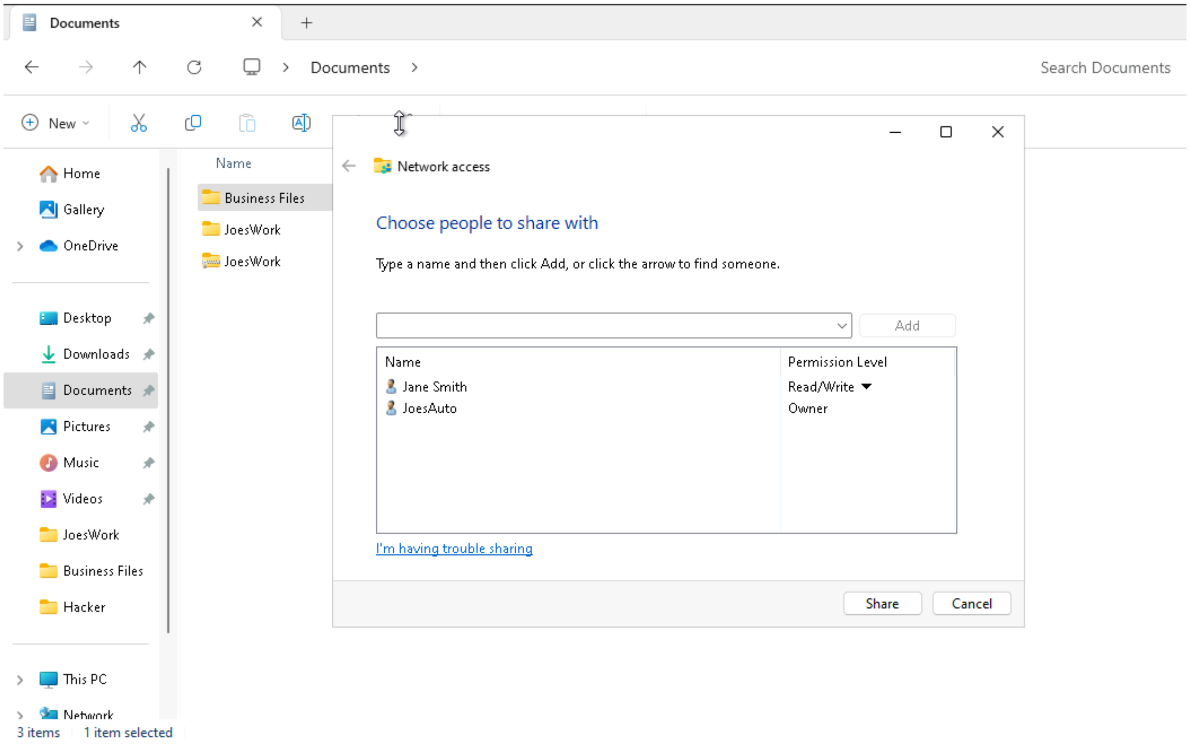
5. C. Securing Files and Folders

4. Shared Folders

Shared folders are a common way to make files available to multiple users. There's a folder under Documents called "Business Files" that Joe wants shared with his administrator Jane. Explain how you would do that and provide a screenshot showing how you can do it. Make sure it's only shared between Joe and Jane.

1

Right click on the folder "Business Files" under documents → show more options → Click on give access → select specific people → Click on the drop down → select JaneSmith → click the drop down on permission level → select Read/Write → select share.



Network access

Choose people to share with

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

Name	Permission Level
Jane Smith	Read/Write ▾
JoesAuto	Owner

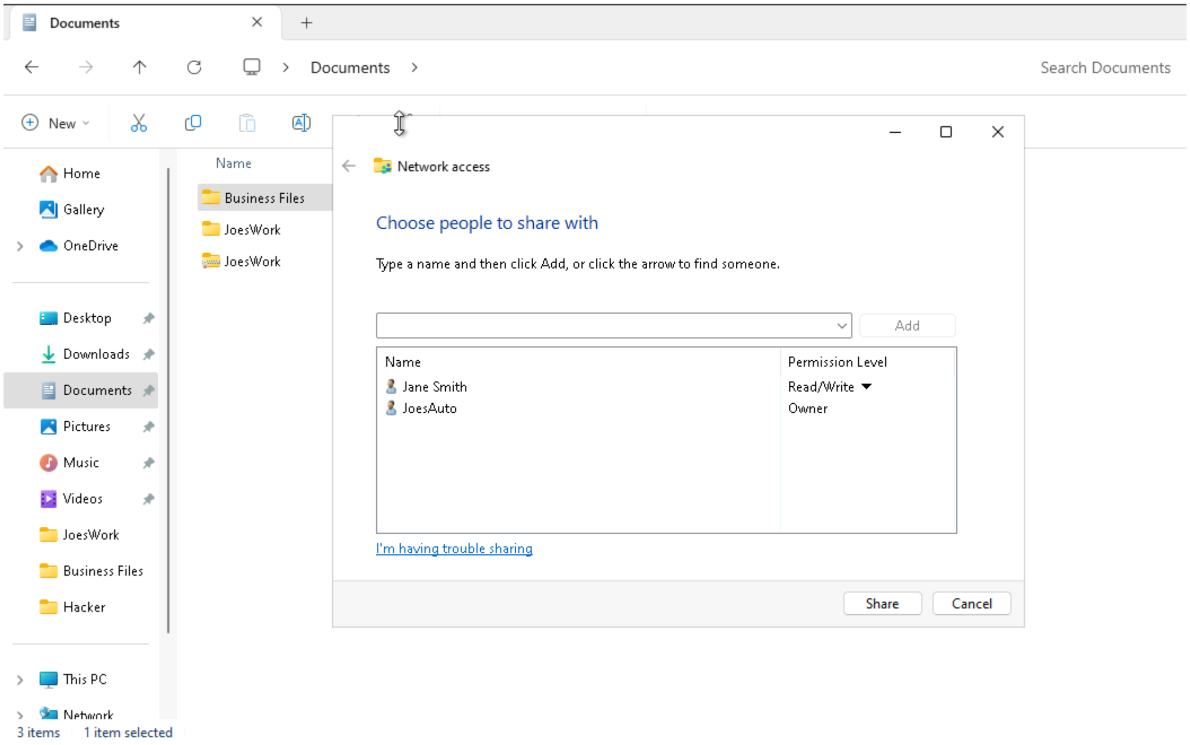
I'm having trouble sharing

5. C. Securing Files and Folders

4. Shared Folders

Shared folders are a common way to make files available to multiple users. There’s a folder under Documents called “Business Files” that Joe wants shared with his administrator Jane. Explain how you would do that and provide a screenshot showing how you can do it. Make sure it’s only shared between Joe and Jane.

1 *Right click on the folder “Business Files” under documents → show more options → Click on give access → select specific people → Click on the drop down → select JaneSmith → click the drop down on permission level → select Read/Write → select share.*



Choose people to share with

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

Name	Permission Level
Jane Smith	Read/Write ▾
JoesAuto	Owner