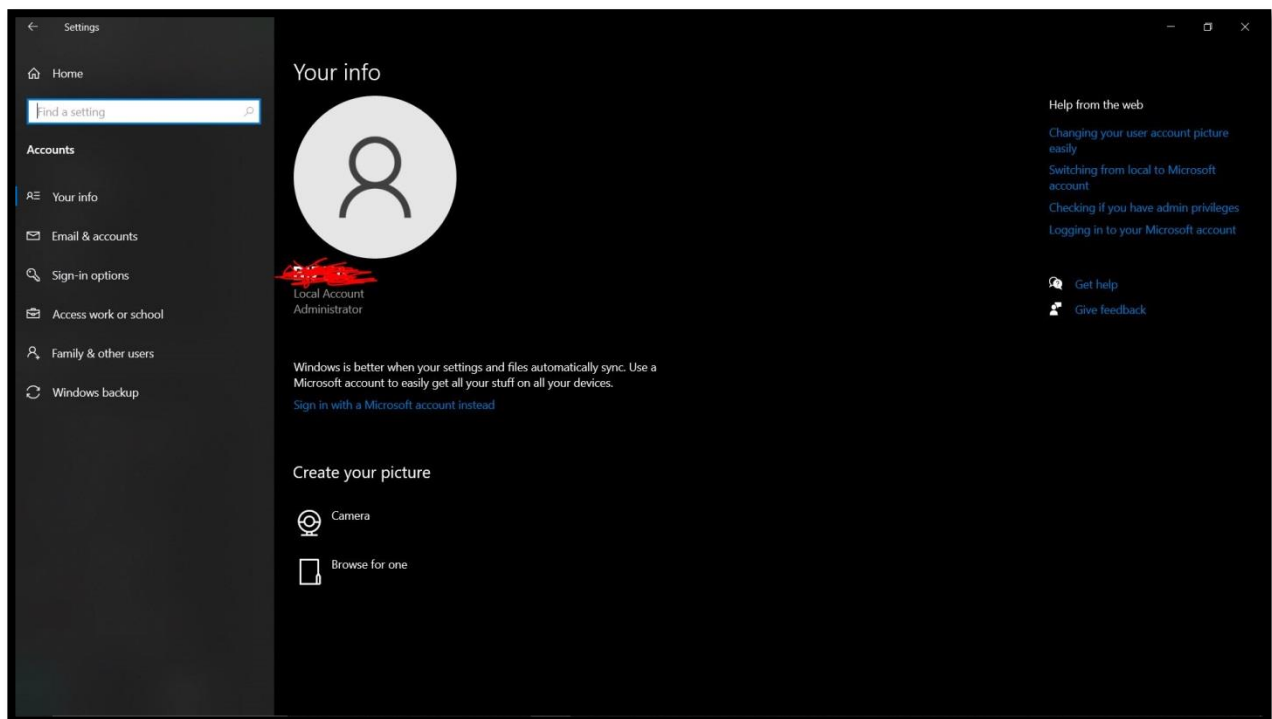


# Operating System Security Checklist – Windows

## 1. User Accounts & Access Control

- Verified administrator and standard user accounts
- Administrator privileges restricted for daily usage
- Standard user recommended for normal activities

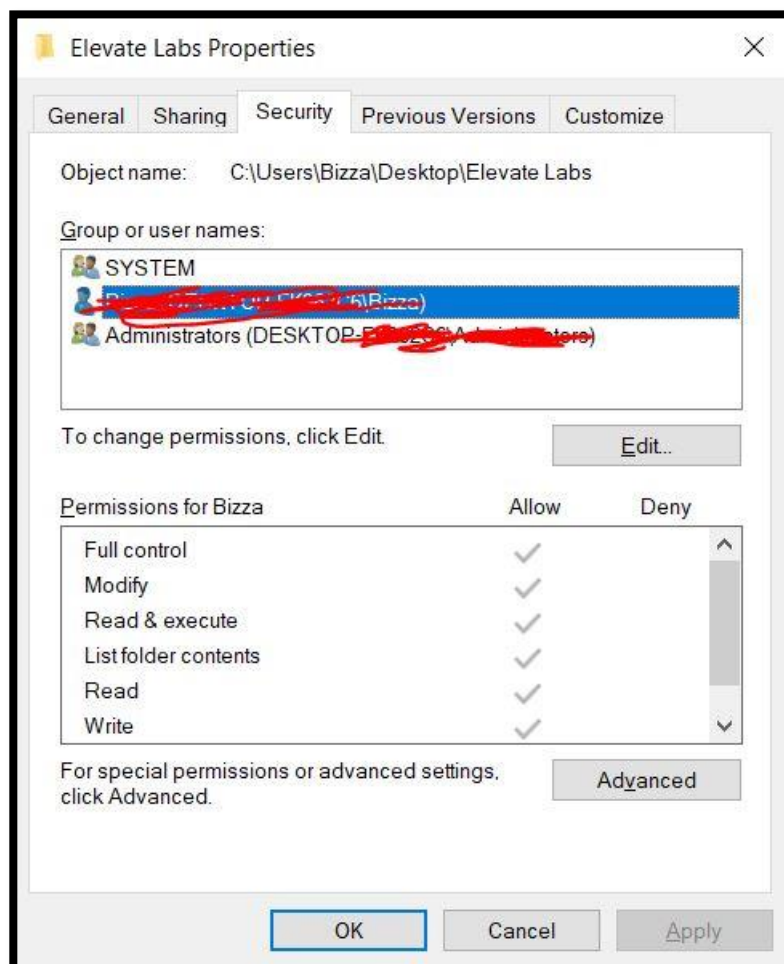


## 2. Administrator vs Standard User

- Administrator used only for system-level changes
- Standard user used for browsing, downloads, and regular work
- Reduced risk of accidental system damage or malware execution

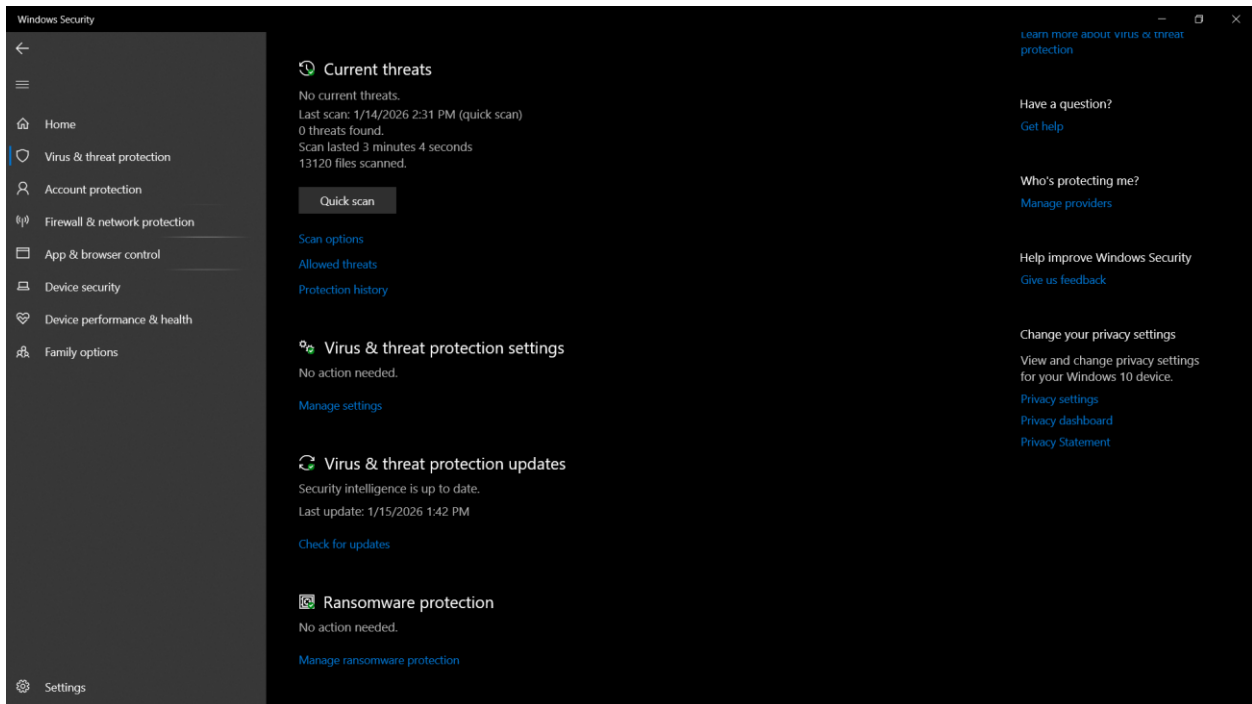
## 3. File & Folder Permissions

- File permissions reviewed using Security tab
- Access rights such as Read, Write, Modify, and Full Control understood
- Sensitive folders restricted to authorized users only



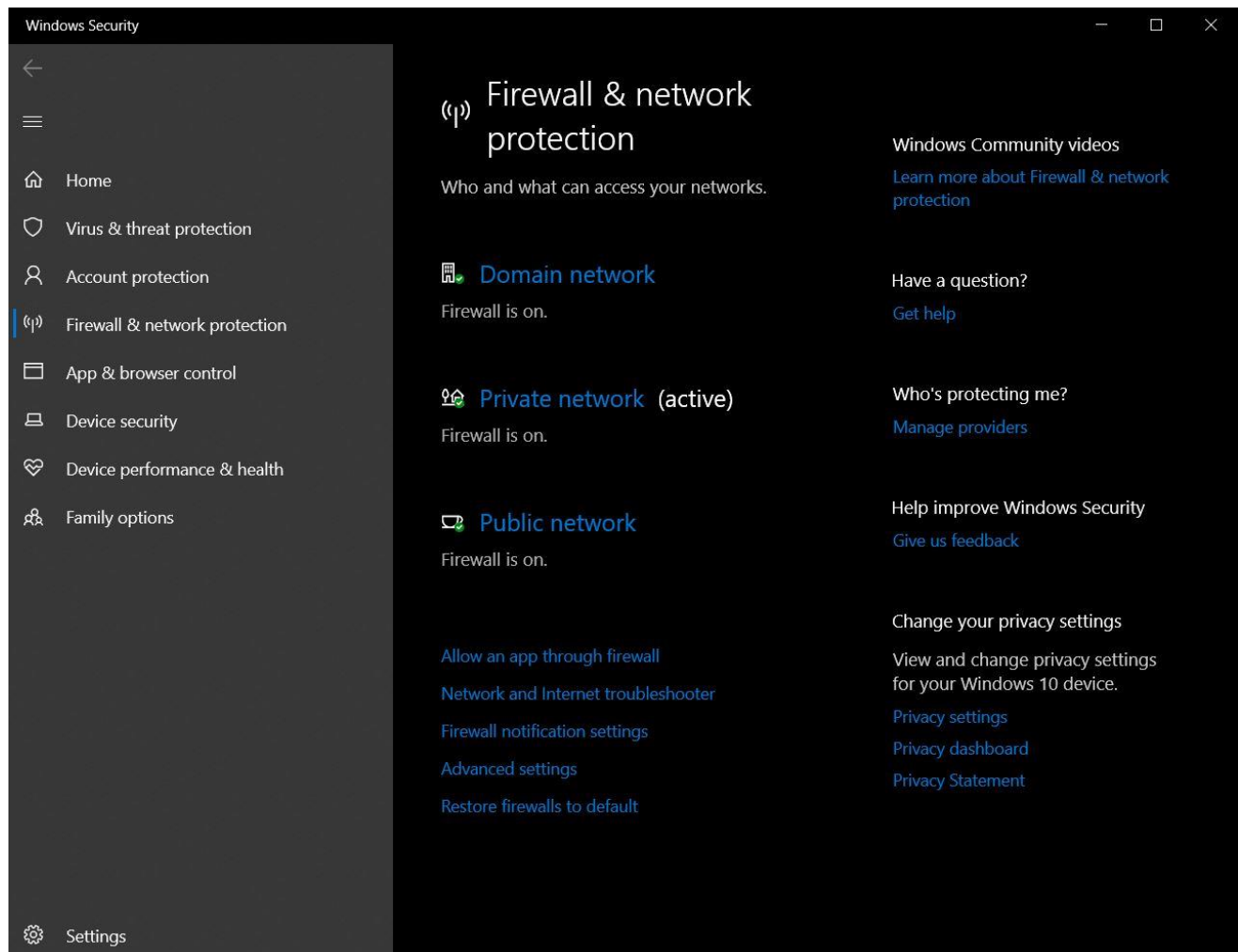
## 4. Windows Defender Security

- Real-time protection enabled
- Virus & threat protection active
- System protected against malware and ransomware
- Cloud-delivered protection enabled for faster threat detection
- Automatic security updates ensured through Windows Update
- Periodic system scans available to detect hidden threats



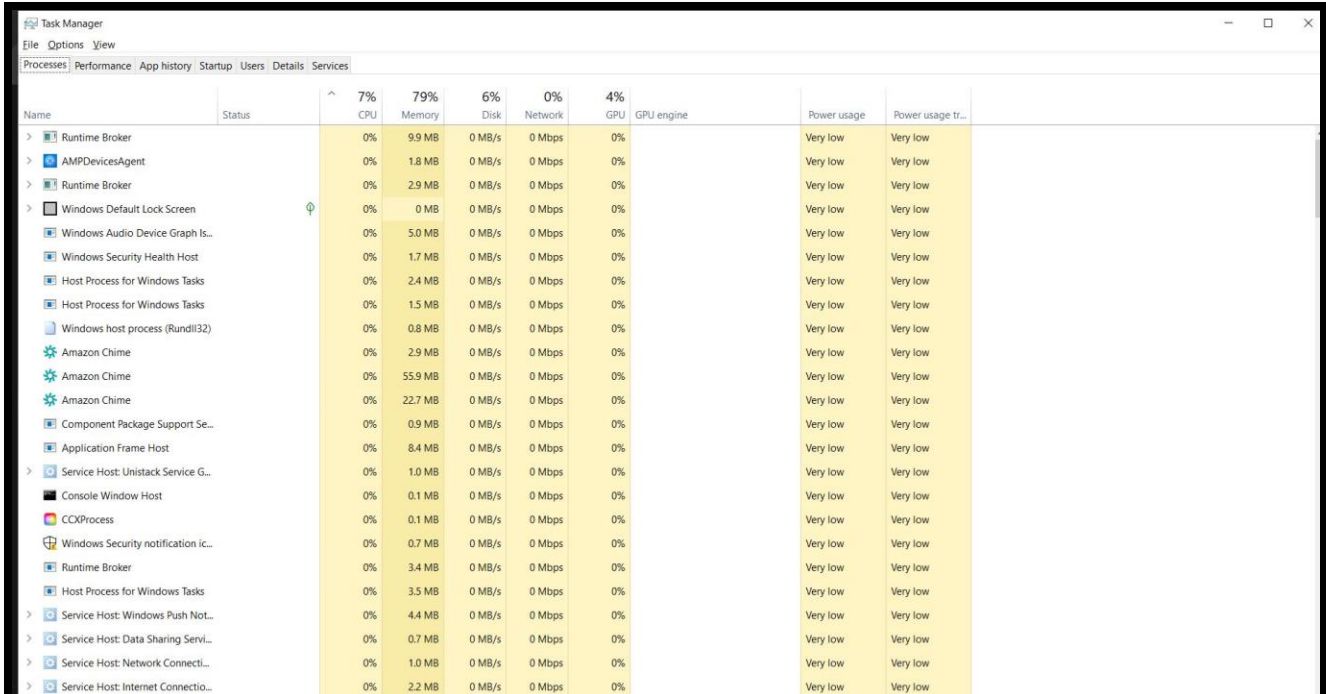
## 5. Firewall Configuration

- Windows Firewall enabled for:
  - Domain Network
  - Private Network
  - Public Network
- Unauthorized network access blocked



## 6. Running Processes Monitoring

- Active processes viewed using Task Manager
- Unknown or suspicious processes identified
- Resource usage monitored
- High CPU or memory usage processes checked regularly
- Background applications reviewed to avoid unnecessary load
- Unwanted startup programs identified and managed



Task Manager									
File Options View									
Processes Performance App history Startup Users Details Services									
Name	Status	7% CPU	79% Memory	6% Disk	0% Network	4% GPU	GPU engine	Power usage	Power usage tr...
Runtime Broker		0%	9.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMPDevicesAgent		0%	1.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Runtime Broker		0%	2.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Default Lock Screen		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Audio Device Graph Is...		0%	5.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Security Health Host		0%	1.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Host Process for Windows Tasks		0%	2.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Host Process for Windows Tasks		0%	1.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows host process (Rundll32)		0%	0.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Amazon Chime		0%	2.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Amazon Chime		0%	55.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Amazon Chime		0%	22.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Component Package Support Se...		0%	0.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Application Frame Host		0%	8.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Uninstall Service G...		0%	1.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Console Window Host		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
CCXProcess		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Security notification ic...		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Runtime Broker		0%	3.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Host Process for Windows Tasks		0%	3.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Windows Push Not...		0%	4.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Data Sharing Servi...		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Network Connecti...		0%	1.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Internet Connecti...		0%	2.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low

## 7. Services Management

- Services reviewed using services.msc
- Unnecessary services identified (e.g., Fax, Remote Registry)
- Reduced attack surface by limiting unused services



## 8. OS Hardening Practices

- System updates applied regularly
- Strong passwords used
- Least privilege principle followed
- Built-in security tools enabled

## Final Outcome

This task helped in understanding how operating system–level security works in Windows and how system hardening reduces security risks.