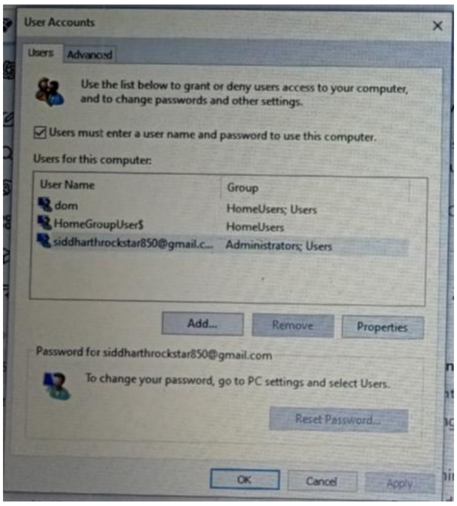
Task 2: Operating System Security Fundamentals (Linux & Windows)

1. OS Environment Windows operating system security settings were used to understand OS-level security controls such as firewall, user accounts, and access control mechanisms.

2. User Accounts and Access Control User accounts and permissions were explored to understand access control mechanisms. Administrator and standard user roles were identified.



User Accounts

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
dom	HomeUsers; Users
HomeGroupUser$	HomeUsers
siddharthrockstar850@gmail.c...	Administrators; Users

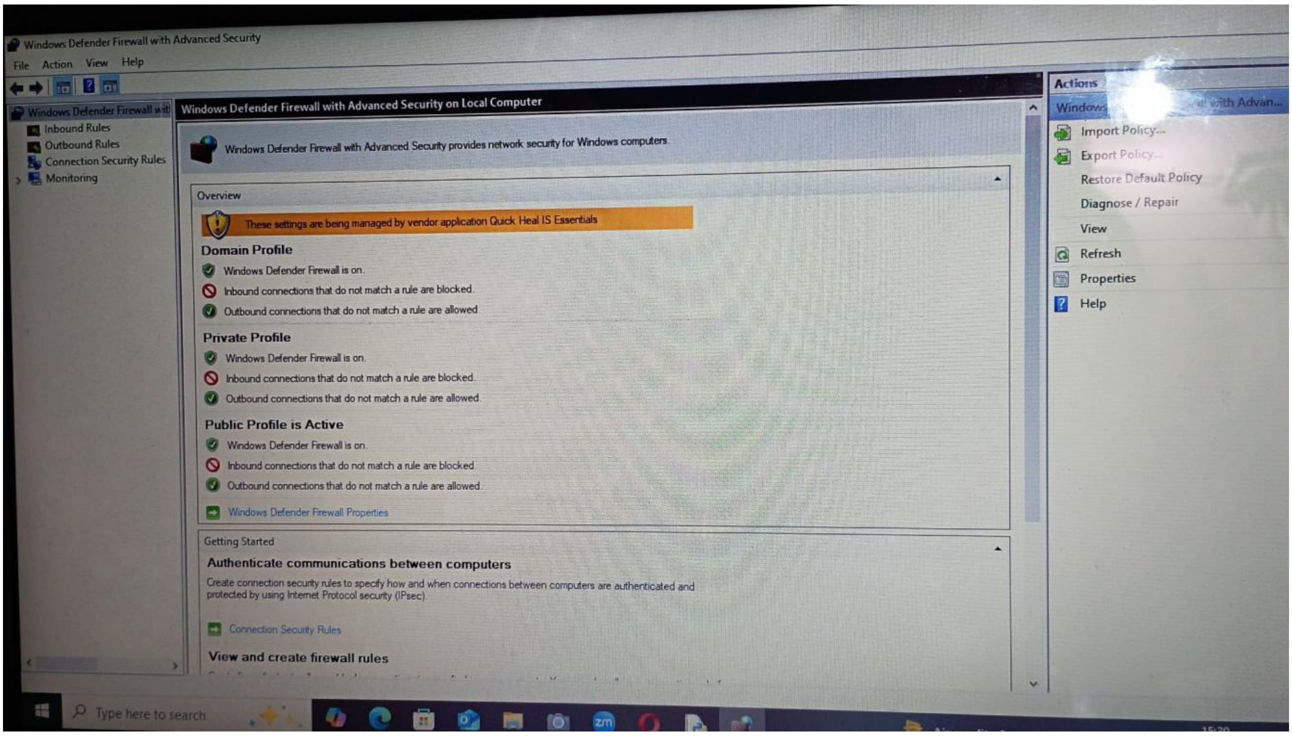
Password for siddharthrockstar850@gmail.com

To change your password, go to PC settings and select Users.

3. File Permissions (Linux – Theoretical) In Linux, file permissions are managed using ls -l to view permissions, chmod to modify permissions, and chown to change ownership.

4. Administrator vs Standard User Administrator users have full system privileges, while standard users have limited access. Using standard users improves security.

 5. Firewall Configuration Windows Defender Firewall was enabled for Domain, Private, and Public profiles to block unauthorized network traffic.



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

These settings are being managed by vendor application Quick Heal IS Essentials

Domain Profile
- ✓ 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.

Private Profile
- ✓ 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.

Public Profile is Active
- ✓ 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.

Windows Defender Firewall Properties

Getting Started

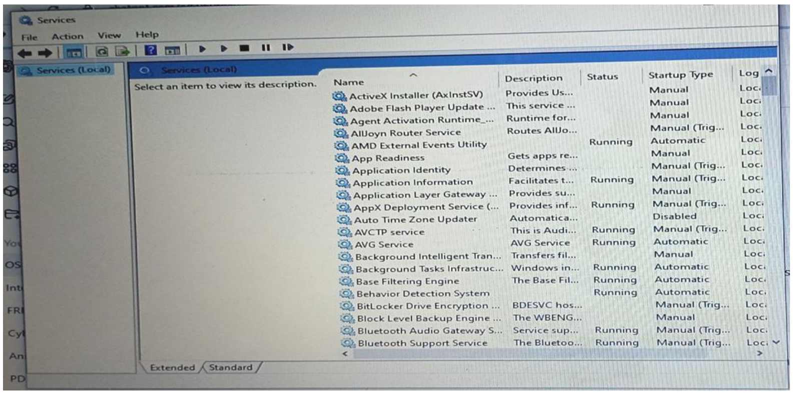
Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

6. Running Processes and Services Running processes and services were identified using Task Manager and Services Manager.



Select an item to view its description.

Name	Description	Status	Startup Type	Log
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Loc:
Adobe Flash Player Update ...	This service ...		Manual	Loc:
Agent Activation Runtime_...	Runtime for...		Manual	Loc:
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Loc:
AMD External Events Utility		Running	Automatic	Loc:
App Readiness	Gets apps re...		Manual	Loc:
Application Identity	Determines ...		Manual (Trig...	Loc:
Application Information	Facilitates t...	Running	Manual (Trig...	Loc:
Application Layer Gateway ...	Provides su...		Manual	Loc:
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Loc:
Auto Time Zone Updater	Automatica...		Disabled	Loc:
AVCTP service	This is Audi...	Running	Manual (Trig...	Loc:
AVG Service	AVG Service	Running	Automatic	Loc:
Background Intelligent Tran...	Transfers fil...		Manual	Loc:
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Loc:
Base Filtering Engine	The Base Fil...	Running	Automatic	Loc:
Behavior Detection System		Running	Automatic	Loc:
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Loc:
Block Level Backup Engine ...	The WBENG...		Manual	Loc:
Bluetooth Audio Gateway S...	Service sup...	Running	Manual (Trig...	Loc:
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trig...	Loc:

7. Disabling Unnecessary Services Unnecessary services increase attack surface and should be disabled if not required.

8. OS Hardening Practices OS hardening includes firewall usage, least privilege, regular updates, strong passwords, and monitoring processes