

# Secure Health- Final Cybersecurity Audit Report

## 1. Introduction

This project provides a complete cybersecurity audit and basic infrastructure for **SecureCart Health**, a small healthcare-related organisation. The goal of the audit was to review the company's security posture, identity risks, and implement controls to improve protection across the network.

During this audit, I reviewed password policies, account lockout settings, audit logs, remote-access configurations, and firewall rules. I then implemented security enhancements to mitigate vulnerabilities and enhance the company's overall defences.

## 2. Company Background

SecureCart Health is a healthcare support service that maintains sensitive patient-related data such as customer information, internal staff accounts, and operational systems. Because healthcare data is considered sensitive, the company needs to maintain strong cybersecurity practices.

Although SecureCart Health is small, it still faces common security risks like weak passwords, unauthorised access attempts, and insecure network services. This project focuses on simple and effective controls to protect the organisation.

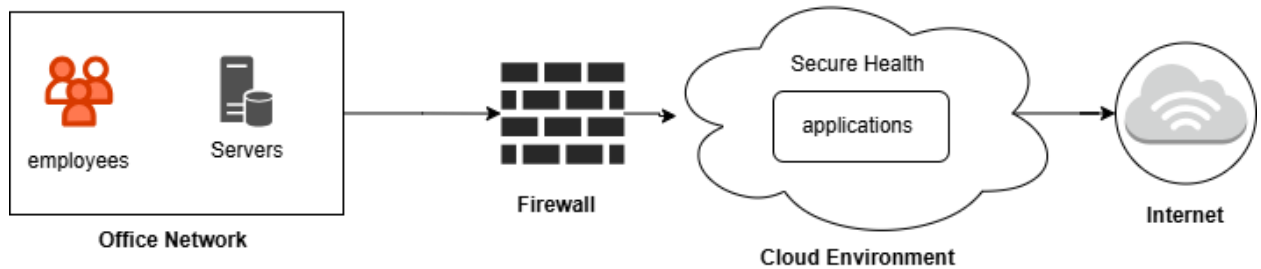
## 3. Project Scope

The scope of this project includes:

- Reviewing the organisation's existing security posture
- Identifying key risks and vulnerabilities
- Applying five security controls inside the virtual environment
- Documenting changes with screenshots
- Providing future recommendations for the organisation

This project does **not** include penetration testing, data recovery, advanced incident response, or cloud architecture design.

#### 4. Network Diagram



#### 5. Project Objectives

- Strengthen user authentication
- Reduce the risk of unauthorised access
- Improve system visibility through logging
- Limit the number of exposed network services
- Create clear documentation showing implemented security controls.

#### 6. Tools Used

- Windows Server 2022 (Domain Controller)
- Windows 11 Client
- Group Policy Management
- Event Viewer
- Windows Defender Firewall
- Virtual Box or VMware environment

#### 7. Identified Risks and Vulnerabilities

During the audit, I identified five key security risks that could affect SecureCart Health:

##### **Risk 1: Weak or Easy-to-Guess Passwords**

Users may select passwords that are too short or predictable, which increases the chance of unauthorised access.

**Risk 2: Brute-Force Login Attempts**

Attackers can try passwords repeatedly until they find the right one if no limit is set.

**Risk 3: Lack of Logon/Logoff Tracking**

Without proper logging, the organisation cannot detect suspicious login behaviour or investigate incidents.

**Risk 4: Unsafe or Unnecessary Ports Open**

Leaving insecure ports (like FTP or HTTP) open exposes the system to attacks/

**Risk 5: Too Many Remote Services Enabled**

Unneeded remote access services increase the attack surface and create entry points for attackers.

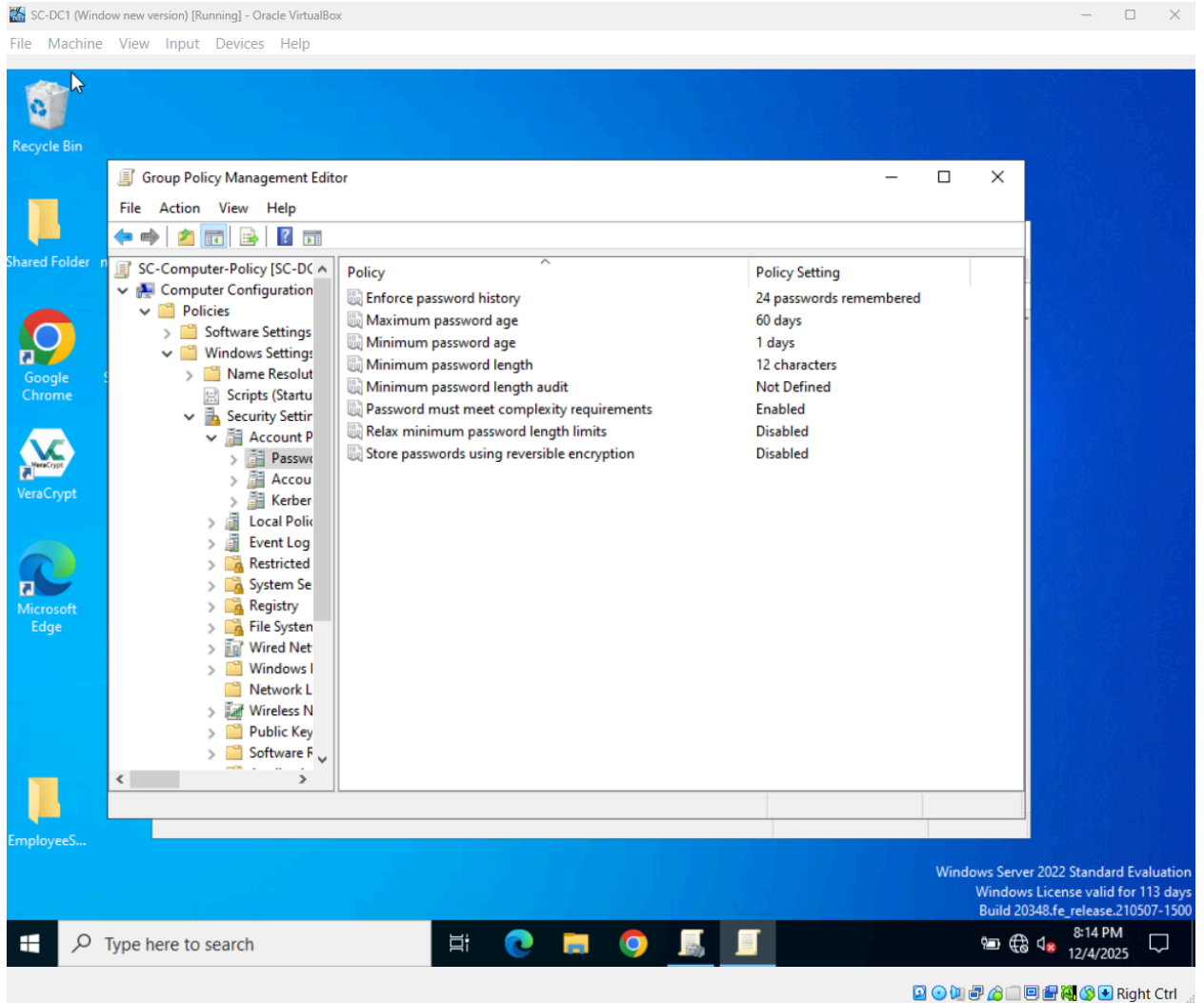
**8. Security Controls Implemented & Evidence**

To reduce these risks, I applied five security controls in the virtual environment. Each control includes a screenshot from the environment showing the applied configuration.

## Control 1: Strong Password Policy

### Risk Addressed: Weak Passwords

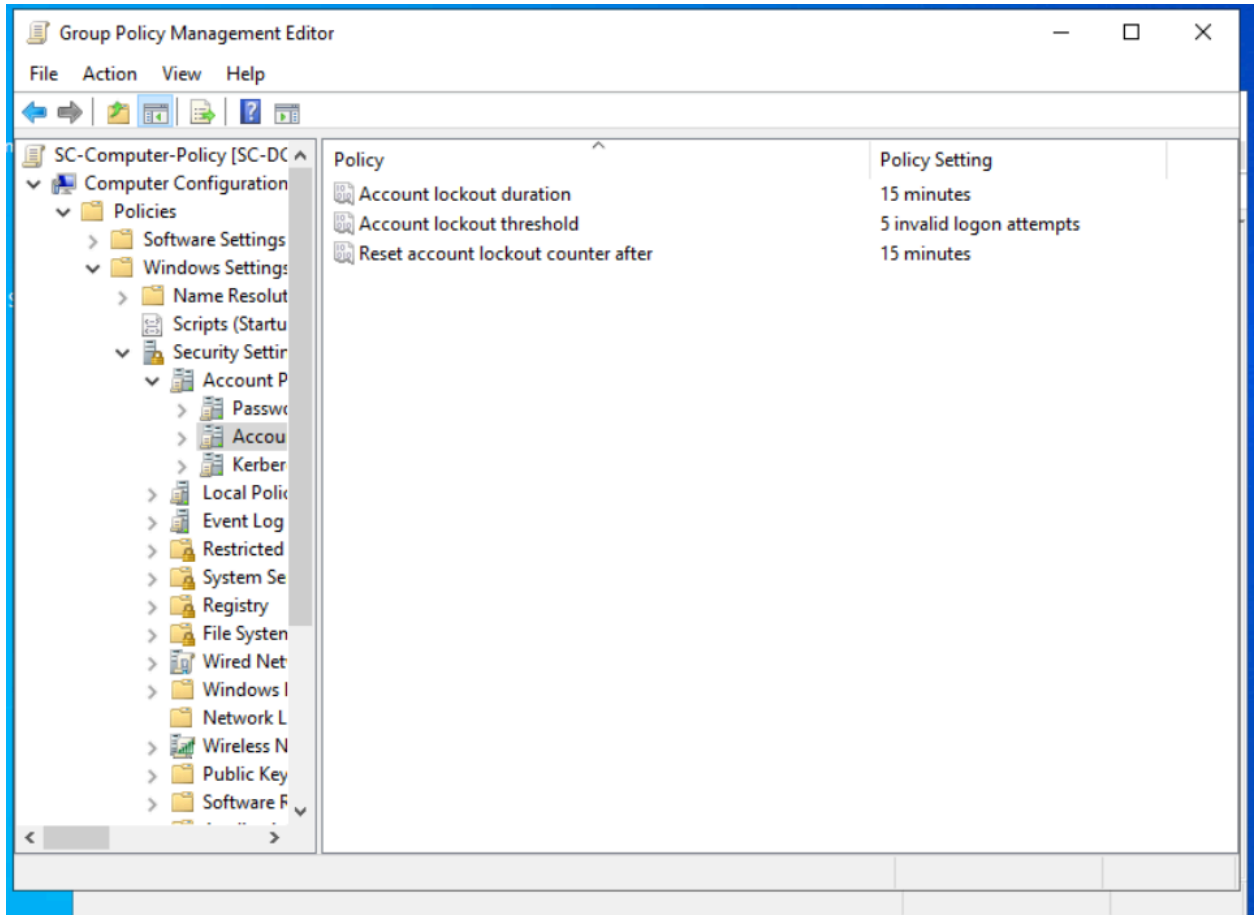
I configured a stronger password policy requiring complexity, minimum length, and password history.



## Control 2: Account Lockout Policy

**Risk Addressed:** Brute Force attacks

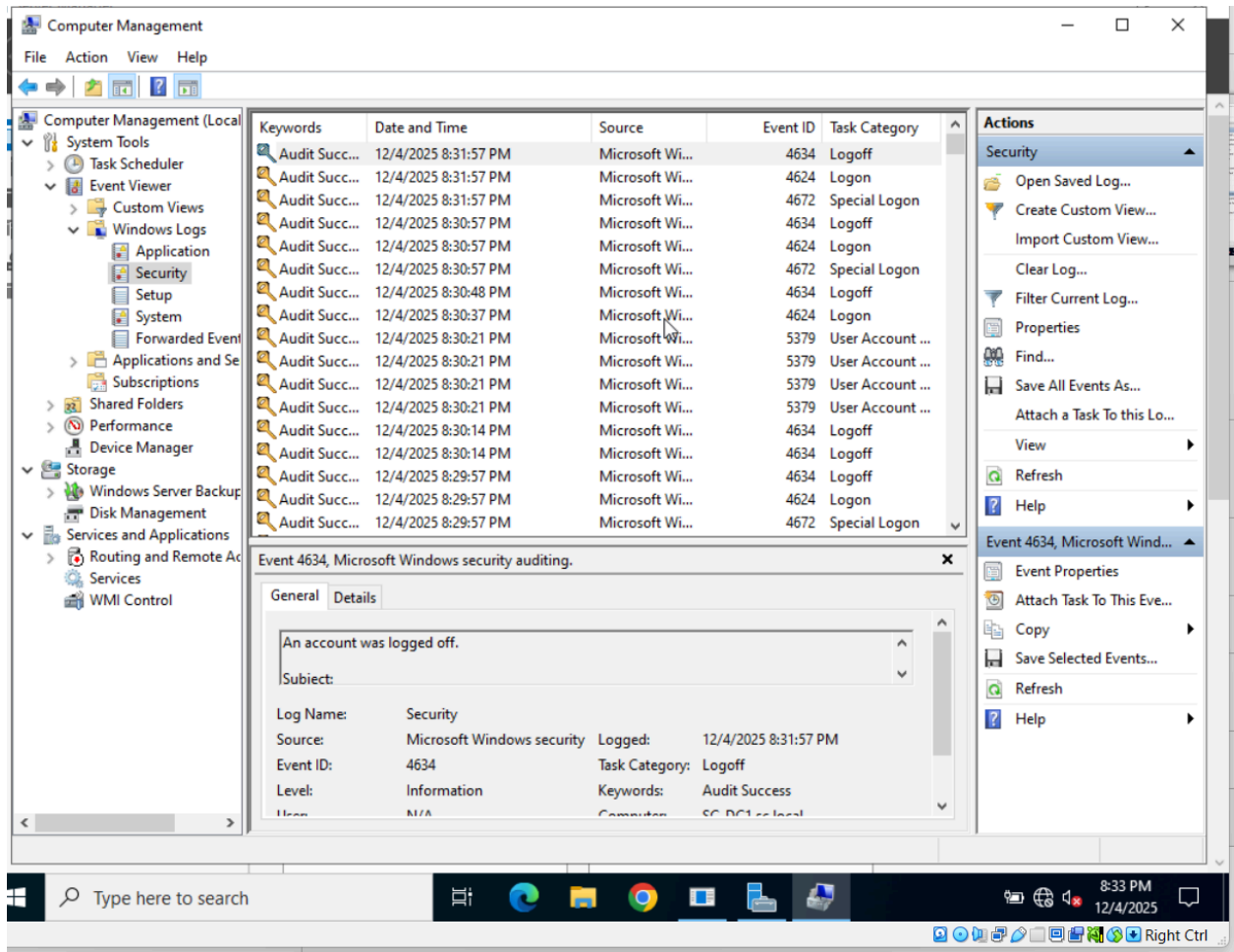
I set the account lockout threshold to five failed attempts, with a 15-minute lockout duration.



### Control 3: Logon/Logoff Auditing

**Risk Addressed:** No Security visibility

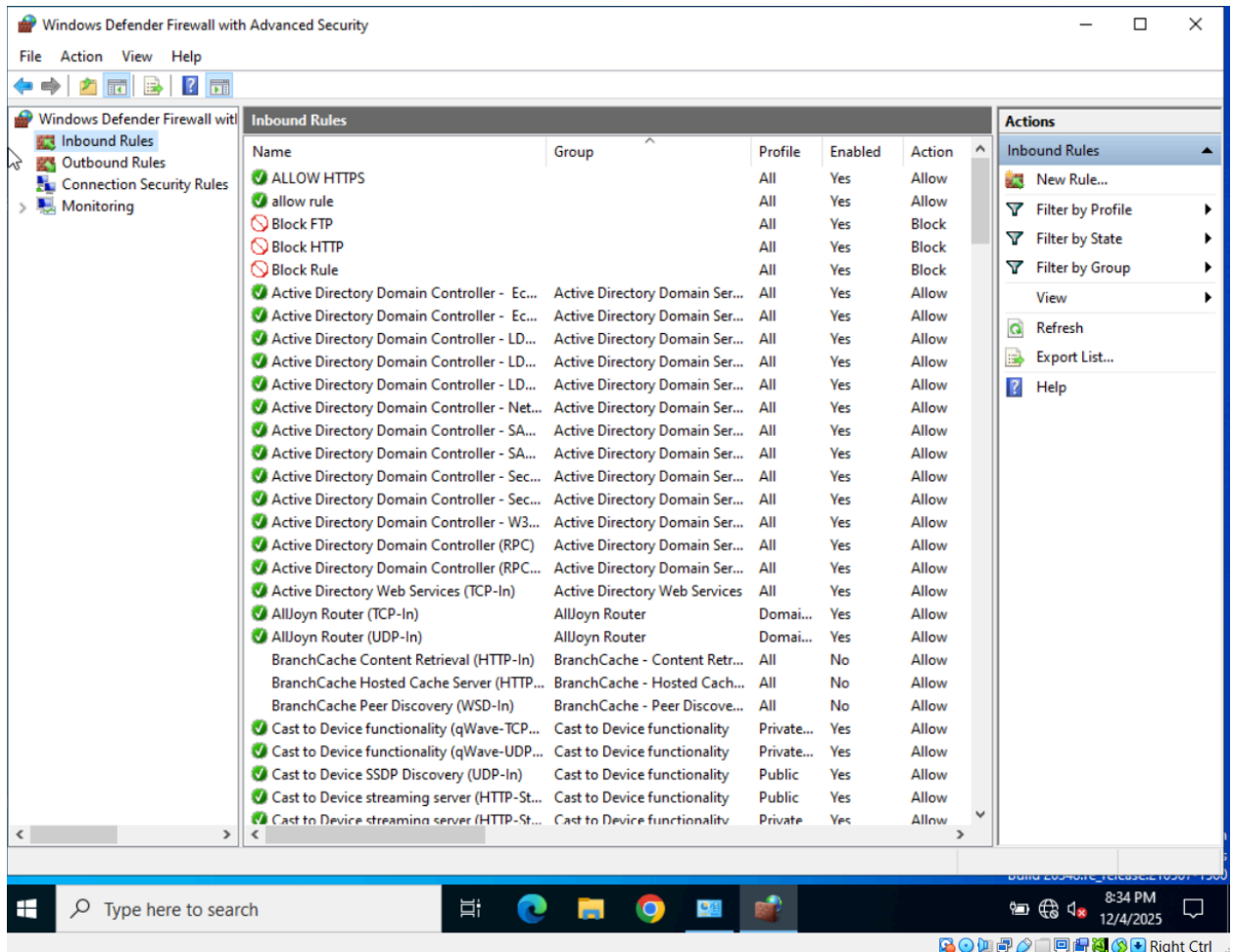
I enabled auditing so logon and logoff events are recorded in Event Viewer.



## Control 4: Firewall Hardening - Custom Allow/Block Rules

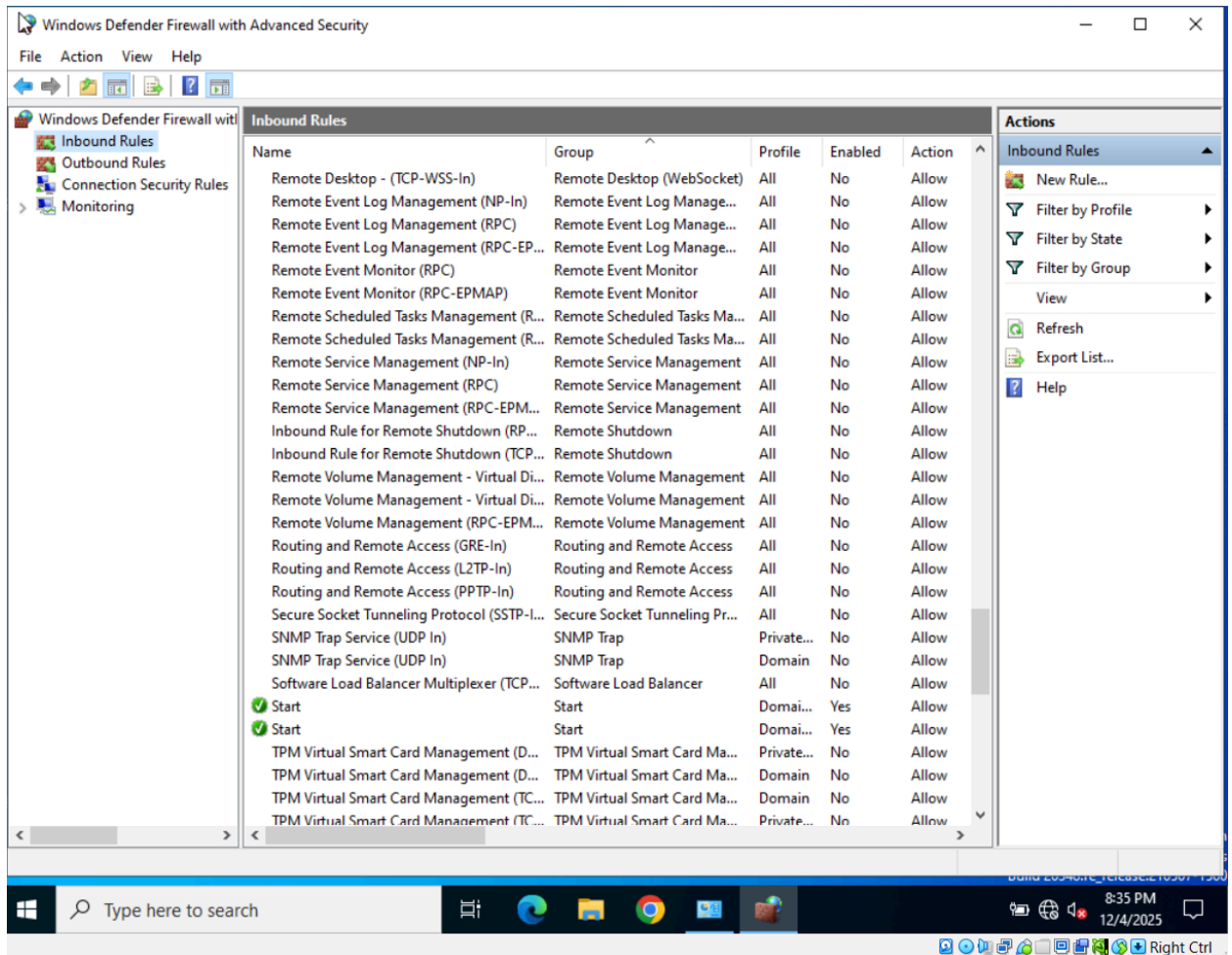
**Risk Addressed:** Unsafe ports left open

I blocked insecure services like FTP and HTTP, and allowed only HTTPS traffic for secure communication.



**Control 5: Remote Access Rules Review****Risk Addressed:** Too many remote services enabled

I reviewed the inbound firewall rules to make sure only necessary remote access features were enabled.



## **9. Results & Analysis**

The implemented controls significantly improved SecureCart Health's security posture:

- Stronger passwords make credential compromise harder
- Brute-force attempts are now limited
- Security logs provide visibility into account activity
- Firewall rules reduce the number of available attack points
- Remote access services are now properly controlled

These changes create a more secure and manageable environment for the organisation.

## **10. Conclusion & Recommendations**

This cybersecurity audit helped SecureCart Health strengthen its basic security controls. While these updates greatly reduce the organisation's risks, continuous improvement is important.

### **Recommended Next Steps:**

- Provide annual Cybersecurity awareness training
- Review password and account policies every 90 days
- Regularly monitor security logs
- Implement centralised log management or a SIEM
- Continue to remove or disable unused services

Overall, the organisation is now much better protected against common threats.