COMPLIANCE ASSESSMENT

Tuesday
02/12/2025

ANSHUL SHUKLA
CBS-0417

Section 1:

Developing a Hardening Strategy

Windows 11 Hardening

1. No full disk encryption (BitLocker unavailable)

Evidence

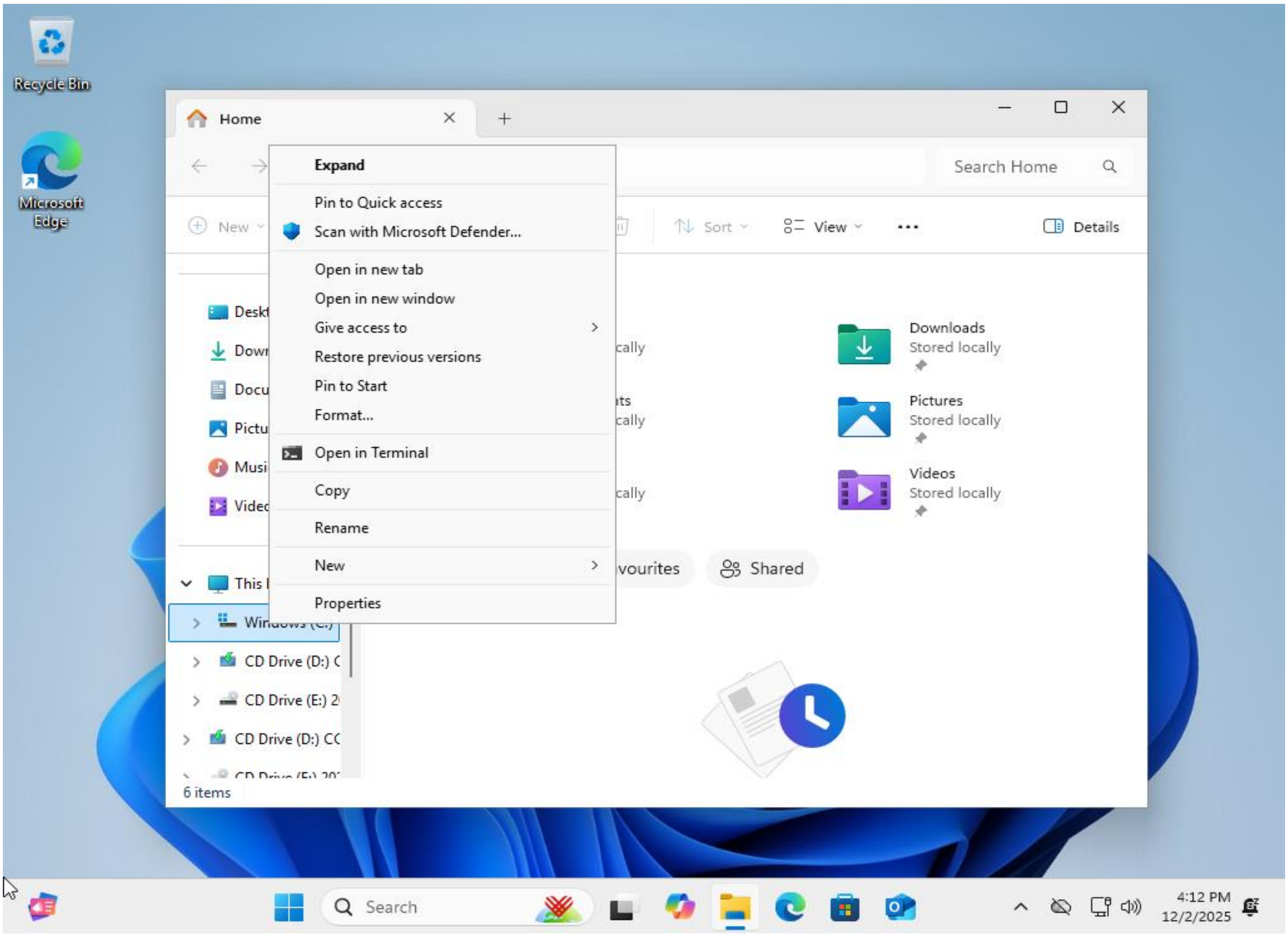
BitLocker management option is not available for the C: drive in Windows 11, and there is no full disk encryption configured on the VM.

Impact

If the system disk is accessed outside the OS, data could be read or copied without authentication, increasing the risk of data leakage.

Remediation

In a production environment, use Windows 11 Pro/Enterprise or hardware that supports BitLocker or device encryption. Enable full disk encryption for the system drive and securely back up recovery keys.



Windows 11 Hardening

2. No local password policy control (gpedit.msc missing)

Evidence

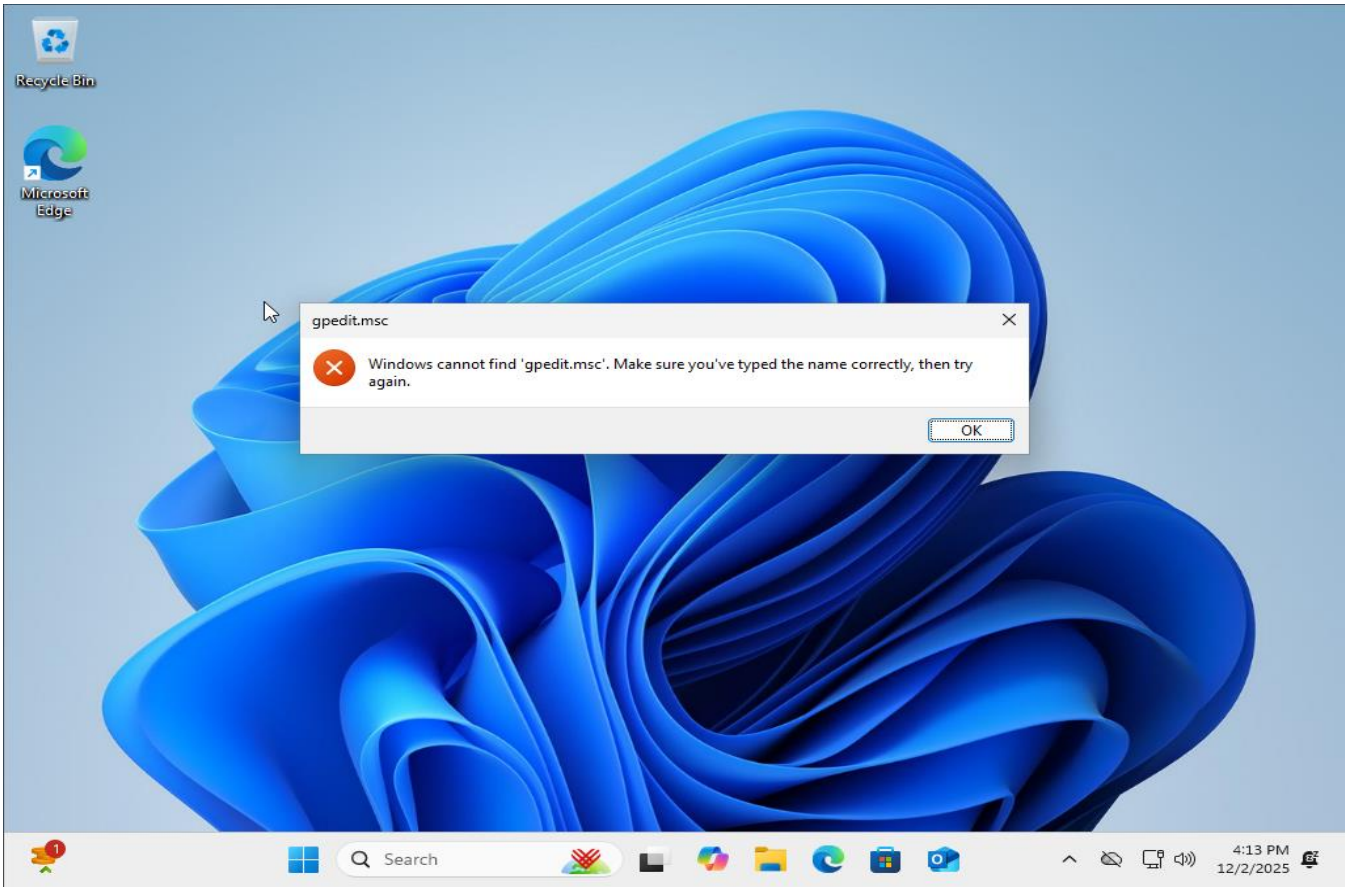
The command gpedit.msc returns an error (“Windows cannot find gpedit.msc”), showing that Local Group Policy Editor is not available. Password policy cannot be configured via the normal security policy UI on this system.

Impact

Without centralized password policy enforcement, users can set weak, short or reused passwords, increasing the risk of account compromise.

Remediation

In a real environment, use Windows 11 Pro/Enterprise joined to a domain so password policies can be enforced via Group Policy / Active Directory. On standalone or Home systems, configure and enforce strong passwords manually (e.g. minimum length, complexity and regular changes).



Windows cannot find 'gpedit.msc'. Make sure you've typed the name correctly, then try again.

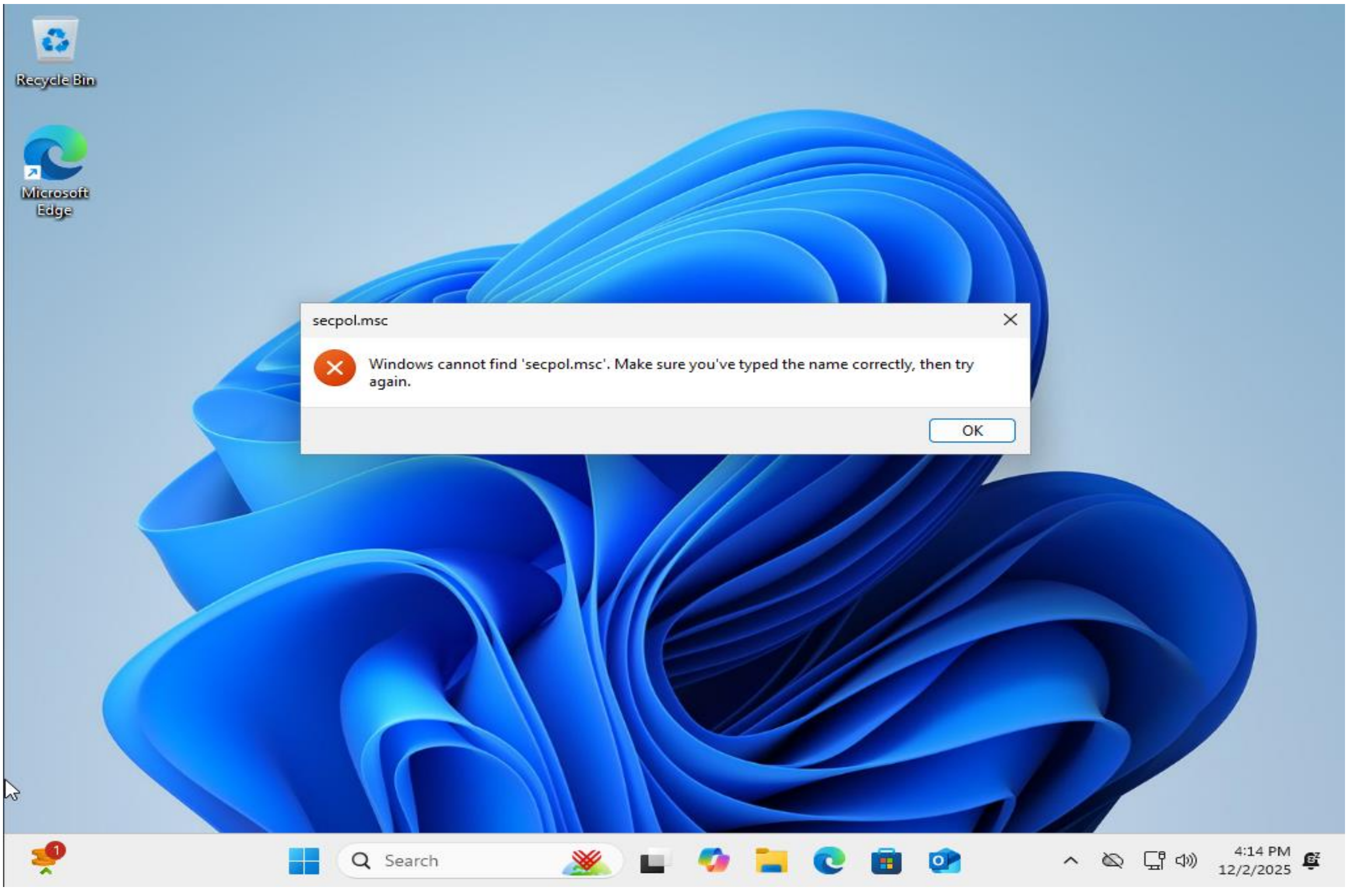
Windows 11 Hardening

3. No audit policy / security policy UI (secpol.msc missing)

Evidence
Running secpol.msc results in “Windows cannot find secpol.msc”, meaning the Local Security Policy console is not available on this Windows 11 Home VM.

Impact
Without easy access to advanced audit settings, it is more difficult to ensure key events (logons, account changes, policy changes) are logged. This reduces the ability to detect and investigate security incidents.

Remediation
Use a Windows edition that supports Local Security Policy or manage audit policies centrally via a domain. Enable auditing for logon events, account management and policy changes. On Home systems, complement with central logging or monitoring tools where possible.



secpol.msc

Windows cannot find 'secpol.msc'. Make sure you've typed the name correctly, then try again.

Windows 11 Hardening

4. AutoPlay not securely configured

Evidence

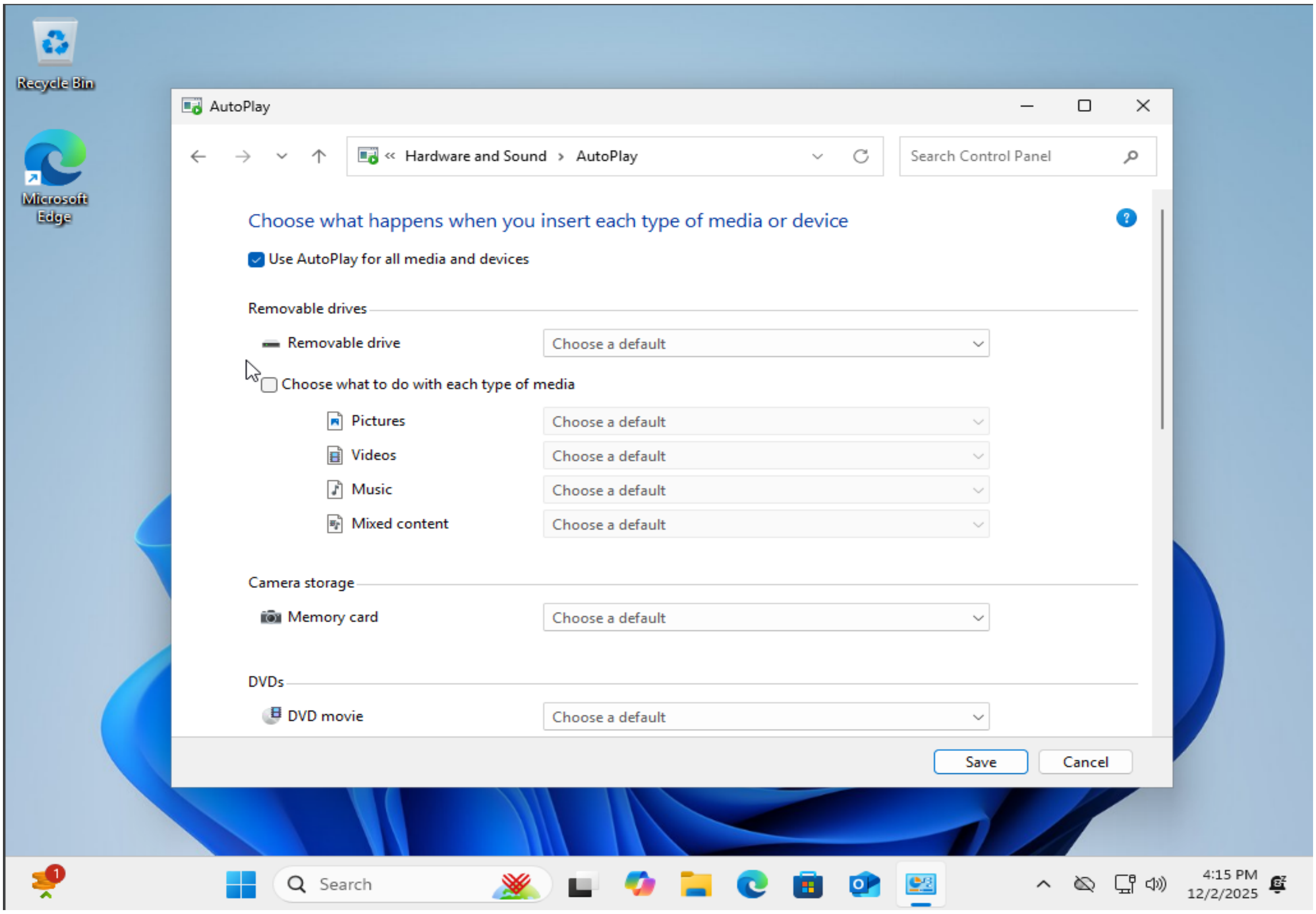
In Control Panel → Hardware and Sound → AutoPlay, removable drives and memory cards are configured with default behavior ("Choose a default") rather than a hardened setting such as "Take no action".

Impact

If removable media automatically opens or runs content, malware on a USB drive can execute more easily when the device is connected.

Remediation

Disable AutoPlay for all media and devices or set removable drives and memory cards to "Take no action" to prevent automatic execution of content from external media.



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

☑ Use AutoPlay for all media and devices

Removable drives

Removable drive	Choose a default

□ 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	Choose a default

DVDs

DVD movie	Choose a default

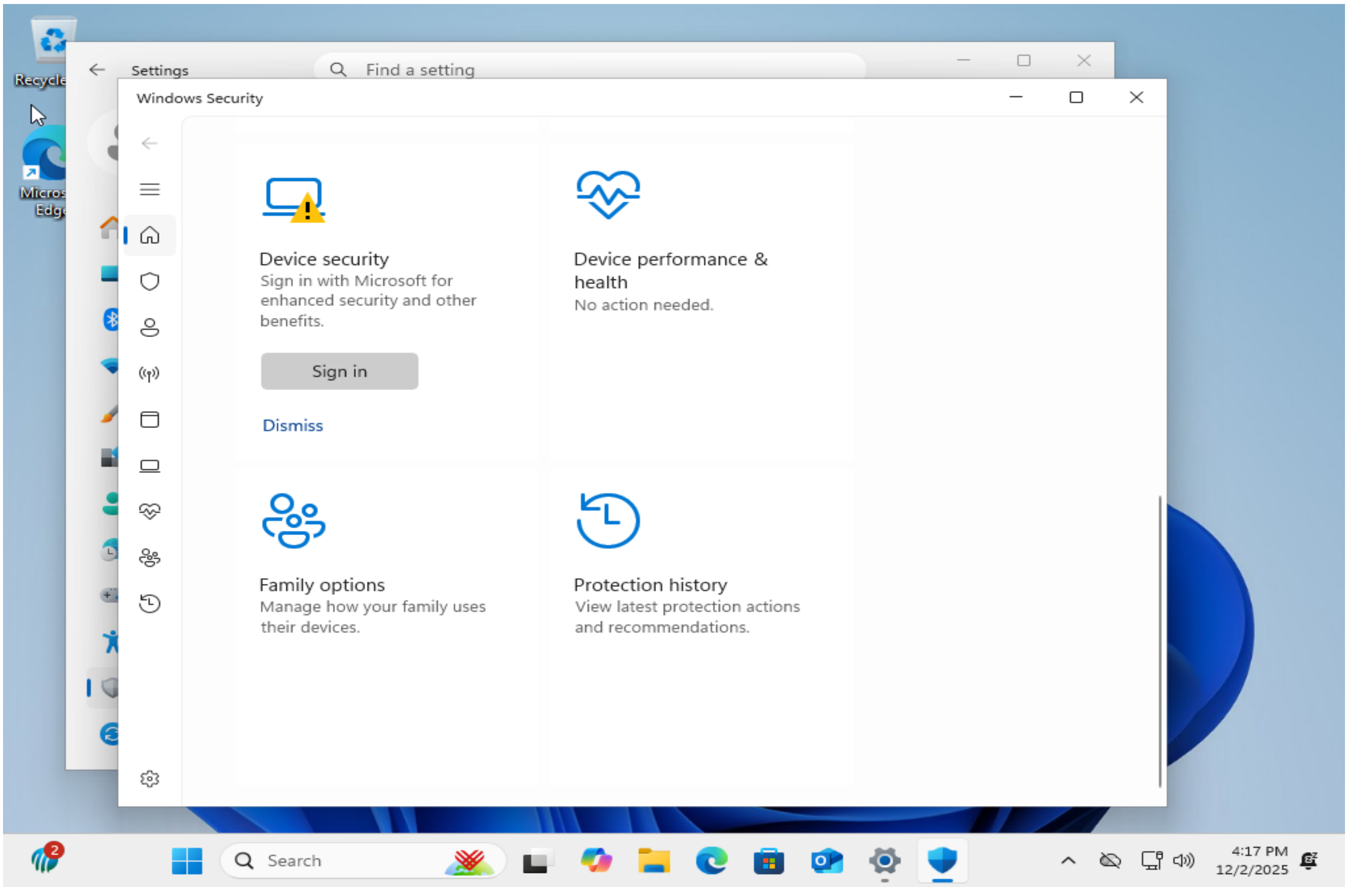
Windows 11 Hardening

5. Device Security warning (not signed in for enhanced security)

Evidence
Windows Security displays a yellow warning on the Device security / Account protection page, prompting “Sign in with Microsoft for enhanced security and other benefits”.

Impact
Without a linked account, some advanced security capabilities, such as cloud-based protection, account protection, and device recovery options, may not be fully available, reducing the overall security posture.

Remediation
Link the device to a Microsoft or organizational account and enable all recommended Windows Security features, including cloud-delivered protection and account protection, according to organizational policy.



Device security
Sign in with Microsoft for enhanced security and other benefits.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Protection history
View latest protection actions and recommendations.

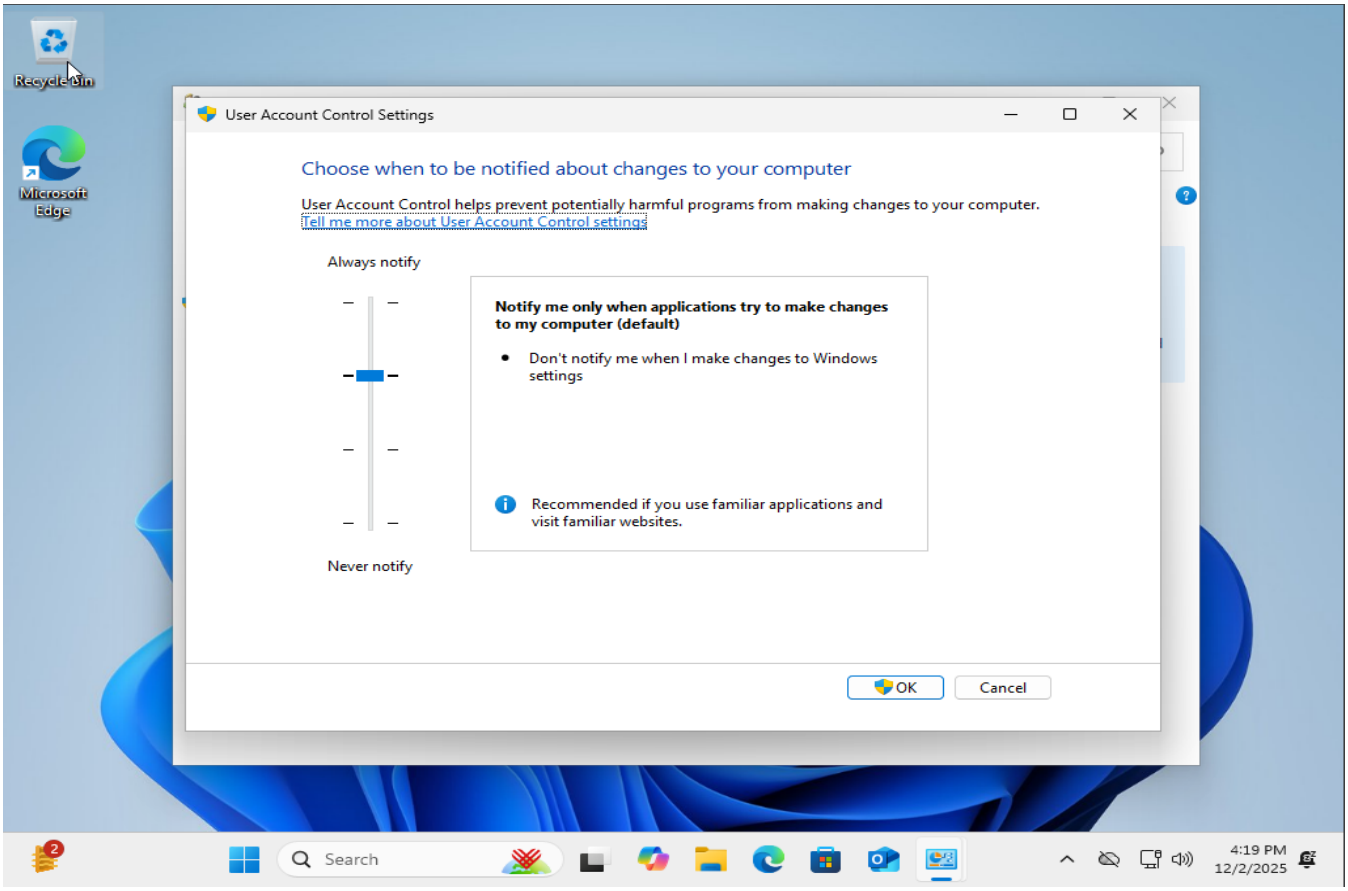
Windows 11 Hardening

6. UAC not set to maximum (hardening choice)

Evidence
UAC is set to the default level (“Notify me only when apps try to make changes to my computer”), which does not prompt when local Windows settings are changed by the logged-in user.

Impact
In high security environments, this can allow configuration changes or certain actions to proceed without an additional approval prompt, slightly lowering the protection against unwanted changes.

Remediation
Increase the UAC level to “Always notify” so that any application or user-driven change to Windows settings triggers a consent prompt, providing stronger protection against unauthorized or accidental changes.



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

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

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

Recommended if you use familiar applications and visit familiar websites.

Never notify

MacOS Hardening

1. Turn on automatic system updates

Configuration: Open System Settings then select General then Software Update. Enable automatic updates for the system and for apps from the App Store.

Rationale: Automatic updates make sure the Mac receives the latest security fixes as soon as they are released. This reduces the time during which known threats can attack the device and it removes the need for users to remember to update on their own.

2. Enable FileVault full disk encryption

Configuration: Open System Settings then select Privacy and Security then FileVault. Turn on FileVault and store the recovery key in a secure company location.

Rationale: Full disk encryption protects all data on the Mac if the device is lost or stolen. A thief can access the hardware but cannot read the data without the login password or the recovery key. This is essential for devices that may leave the office or be used for travel.

3. Require a strong password and a short screen lock time

Configuration: In System Settings select Users and Groups and require strong passwords that use a mix of characters and a suitable length. Then in System Settings select Lock Screen and set the display to lock after a short period such as five or ten minutes and require a password after sleep or screen saver.

Rationale: Strong passwords make it harder for attackers to guess or brute force access to the device. A short lock time limits the chance that someone can use an unattended Mac that is still logged in. Together they protect both local data and access to company accounts.

MacOS Hardening

4. Enable the firewall and limit sharing services

Configuration: In System Settings select Network then Firewall and turn it on. Then open System Settings and review sections such as General and Sharing. Turn off any sharing services that are not required for work such as file sharing screen sharing or remote access tools.

Rationale: The firewall blocks unwanted inbound network connections that could be used to probe or attack the device. Disabling unused sharing services reduces the number of possible entry points for an attacker and follows the idea of least privilege.

5. Use Gatekeeper and allow only trusted apps

Configuration: Open System Settings then select Privacy and Security. Under Security set the Mac to allow apps from the App Store and from identified developers. If a tool is not clearly trusted or approved do not allow it.

Rationale: Gatekeeper checks apps before they run and blocks software that is not from trusted sources. This reduces the risk of users installing malware or unapproved tools that might capture data or weaken other security controls. It also helps standardize the software environment across company devices.

6. Disable automatic login and avoid local admin use for daily work

Configuration: In System Settings select Users and Groups and ensure automatic login is turned off. Set a standard user account for daily work and keep admin access only for support tasks or controlled changes.

Rationale: Automatic login allows anyone with physical access to start the Mac and reach all user data. Using admin rights for normal work makes it easier for malware to gain full control of the system. Requiring a password at startup and reserving admin rights for specific tasks lowers the impact of both misuse and successful attacks.

Section 2:

Create Security Policies

Email Policy

1. Business use of corporate email

Policy item

Company email accounts are provided for business use. Personal use must be limited and must never interfere with work duties or violate company rules.

Why this matters

Keeping email focused on work reduces legal and security risks and helps ensure that business records stay inside the corporate environment rather than scattered across personal accounts.

2. Handling of confidential information

Policy item

Employees must not send confidential or sensitive information by email unless it is strictly required for their job and approved protection is used such as encryption or secure portals.

Why this matters

Email can be intercepted or misdirected so uncontrolled sharing of sensitive data can lead to data leaks loss of customer trust and regulatory issues.

3. Protection against phishing and suspicious emails

Policy item

Employees must not click links open attachments or provide credentials in response to unexpected or suspicious emails. Such messages must be reported to the security or IT team immediately.

Why this matters

Phishing is one of the most common ways attackers steal passwords or install malware. Clear rules on how to treat suspicious messages lower the chance of successful attacks.

Email Policy

4. Use of passwords and multi factor authentication

Policy item

Email accounts must use strong unique passwords and multi factor authentication where available. Passwords must not be shared written down in plain text or reused on other services.

Why this matters

Email is often the recovery point for many other systems. If an attacker controls an email account they can reset many other passwords so strong protection for email access is critical.

5. Restrictions on forwarding and external recipients

Policy item

Automatic forwarding of corporate email to personal accounts is not allowed. Before sending messages outside the company employees must verify that recipients are correct and that the content is appropriate for external sharing.

Why this matters

Forwarding to personal or uncontrolled addresses increases the risk of data leaving the company. Careful control over external recipients helps prevent accidental disclosure of internal information.

BYOD Policy

1. Device registration and technical control

Every personal phone or laptop that connects to company mail or systems must be registered with the IT team first.

IT may install a management tool on the device. This tool can enforce security settings and can remove work data if the device is lost stolen or when the employee leaves the organisation.

Employees must not change or disable these controls while the device is allowed to access company data.

2. Strong access control and screen locking

All devices that access company resources must use a strong unlock method.

Acceptable methods are a long password or PIN or biometric login such as fingerprint or face unlock that is supported by the device.

Screen lock must activate after a short period of inactivity. For example five to ten minutes for laptops and a shorter period for phones.

The device must always require the unlock method after restart and after the screen locks.

3. Encryption and protection of stored data

Data stored on personal devices that holds company information must be encrypted

On Apple and Android smartphones employees must enable device encryption if it is not enabled by default.

On Windows 11 and macOS laptops employees must use full disk encryption where the edition and hardware support this.

Encryption keys and recovery codes must be stored in a secure location that is approved by the company and must not be shared.

BYOD Policy

4. Secure configuration and regular updates

Operating systems and installed apps must be kept up to date.

Automatic update features must be turned on for Apple and Android smartphones and for Windows 11 and macOS laptops.

Employees must not root or jailbreak phones and must not bypass built in security protections.

On laptops staff must install and maintain company approved security software where required such as endpoint protection and secure browsers.

5. Separation of work data and personal data

Where the management tool supports this the company will use a separate work profile or container on smartphones and laptops.

Work mail files and apps must only be stored in this managed area. Personal photos messages and personal apps must remain outside this area.

Employees must not copy or move company data into personal cloud storage personal mail accounts or personal messaging tools.

Backups of work data may only be made to locations approved by the company.

6. Incident reporting and remote response

Employees must report any loss theft or suspected compromise of a personal device that holds company data as soon as possible.

Examples include a lost phone a stolen laptop signs of malware or access by an unknown person.

The company may remotely lock the device or remove work data in order to protect corporate information.

After such an event the device must not be used again for work until IT has confirmed that it is safe.

Section 3:

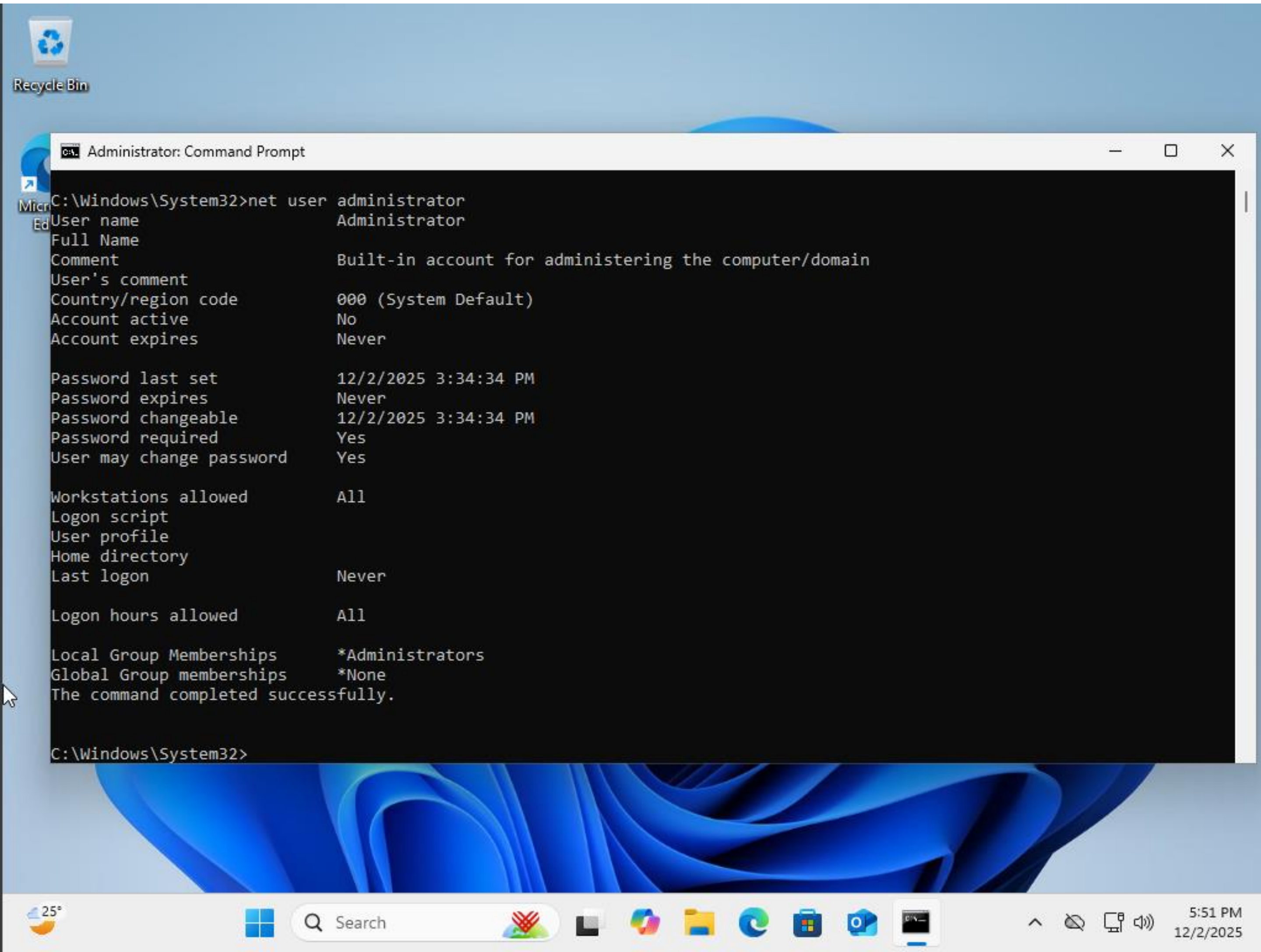
Self Assessment

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	Met
Windows Firewall is enabled	Met
Automatic updates are enabled	Met
User Account Control (UAC) is enabled	Met
Strong password policies are enforced	Not Met
Guest account is disabled	Met
System logging and auditing are enabled	Met
Windows Defender Antivirus is enabled and up to date	Met
Remote Desktop Services are configured securely	Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	Not Met
USB ports are disabled or restricted to authorized devices only	Met
Network access controls are implemented, including VLAN segmentation and port security	Not Met
Remote Registry service is disabled	Met
Windows Updates are configured to download and install updates automatically	Met

Windows Desktop Compliance

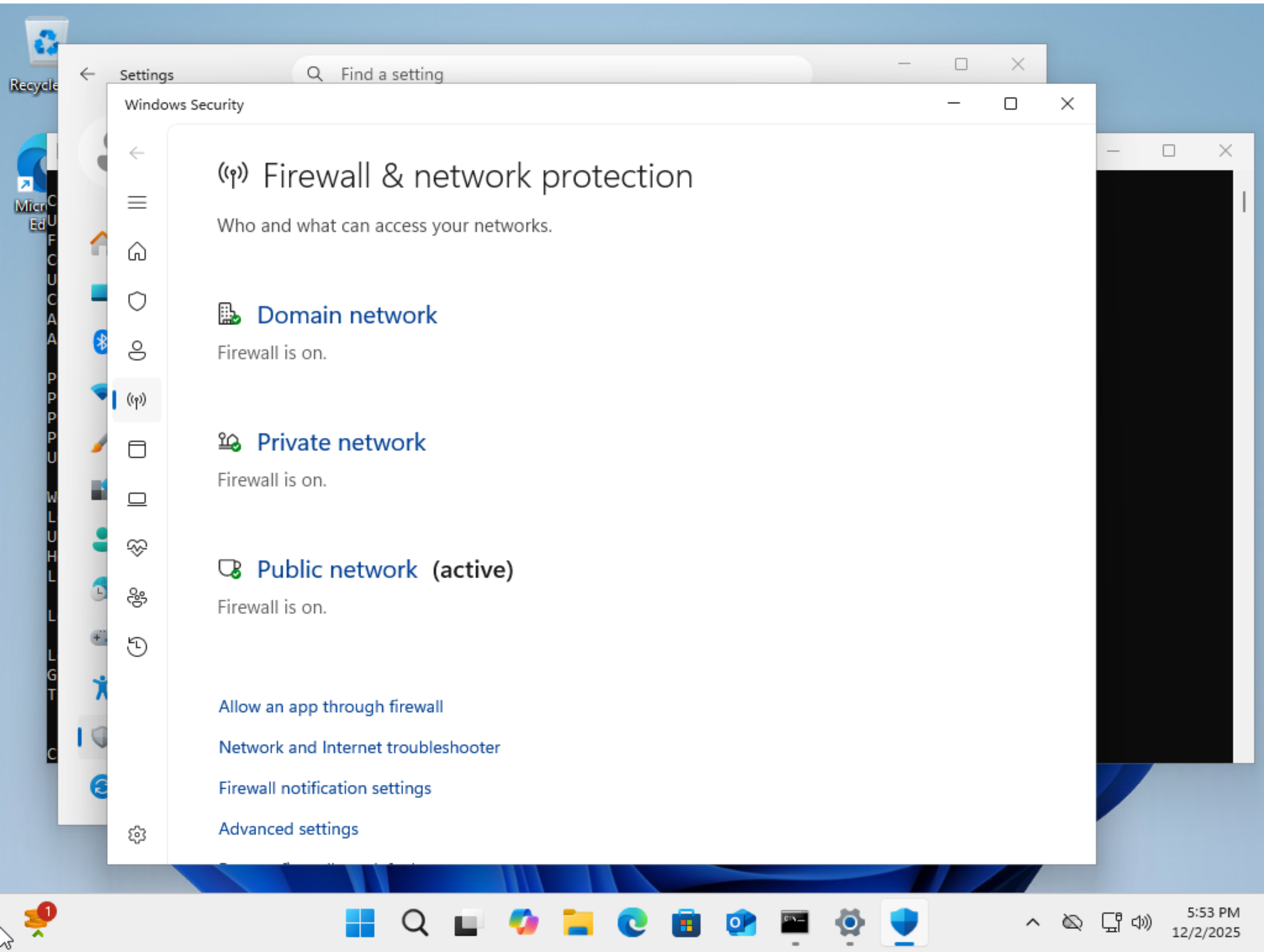
Windows 10 Regulatory Requirement	Met/Not Met
Built-In Administrator account is disabled	Met



```
C:\Windows\System32>net user administrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            12/2/2025 3:34:34 PM
Password expires             Never
Password changeable          12/2/2025 3:34:34 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.


C:\Windows\System32>
```

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Windows Firewall is enabled	Met



Settings
Find a setting
Windows Security

Firewall & network protection

Who and what can access your networks.

Domain network
Firewall is on.

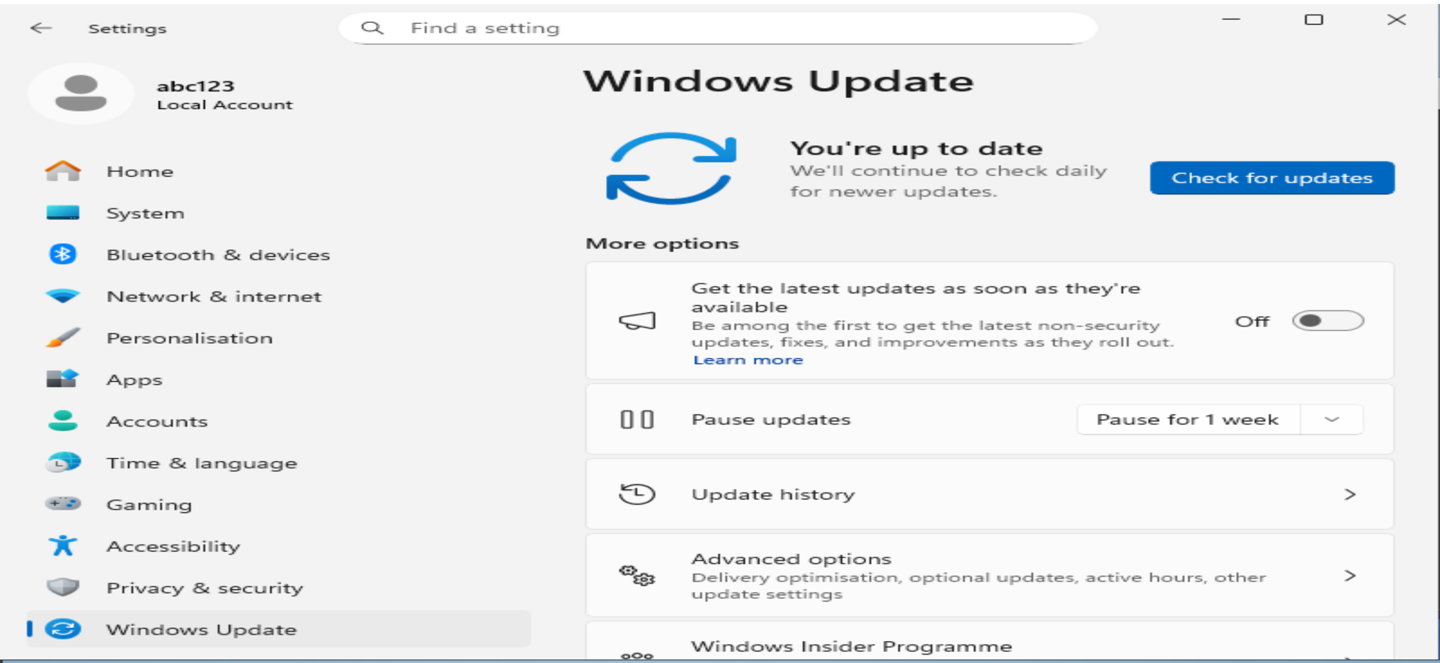
Private network
Firewall is on.

Public network (active)
Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
5:53 PM
12/2/2025

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Automatic updates are enabled	Met



Windows Update

You're up to date
We'll continue to check daily for newer updates.

More options

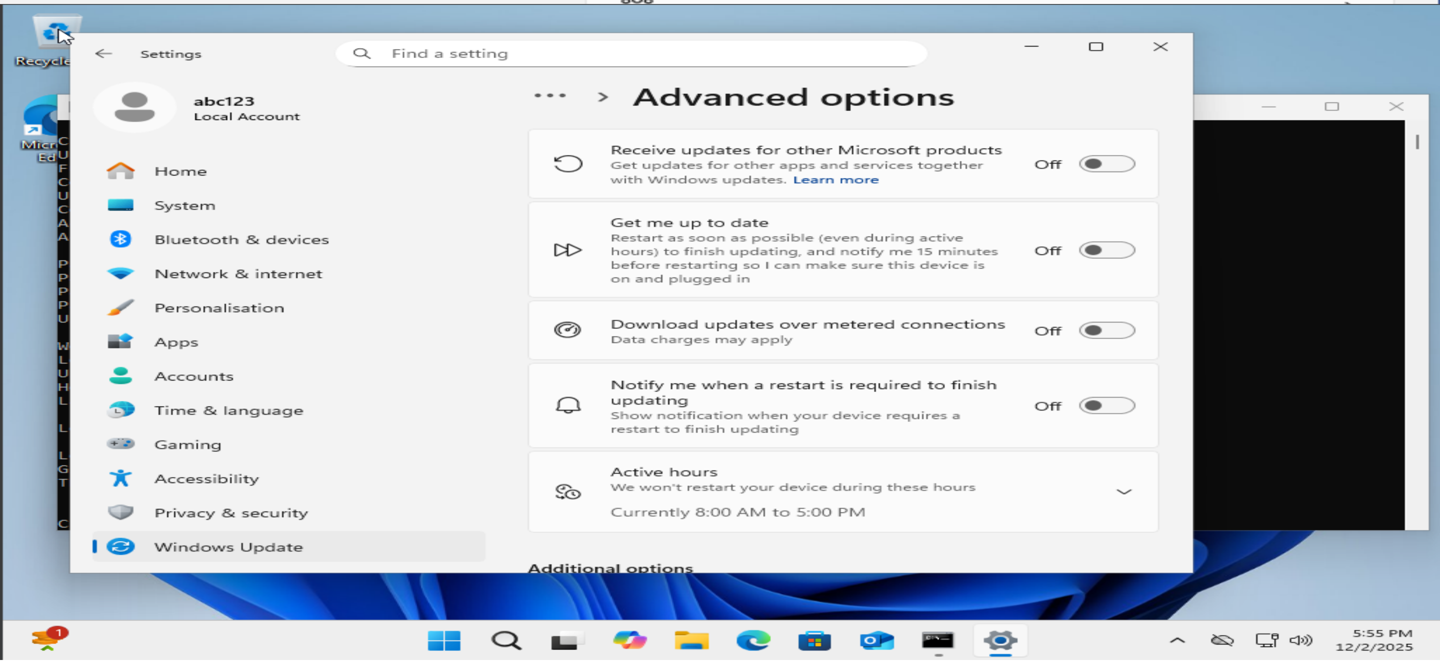
Get the latest updates as soon as they're available
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out.
Off

Pause updates — Pause for 1 week

Update history

Advanced options
Delivery optimisation, optional updates, active hours, other update settings

Windows Insider Programme



Advanced options

Receive updates for other Microsoft products
Get updates for other apps and services together with Windows updates.
Off

Get me up to date
Restart as soon as possible (even during active hours) to finish updating, and notify me 15 minutes before restarting so I can make sure this device is on and plugged in
Off

Download updates over metered connections
Data charges may apply
Off

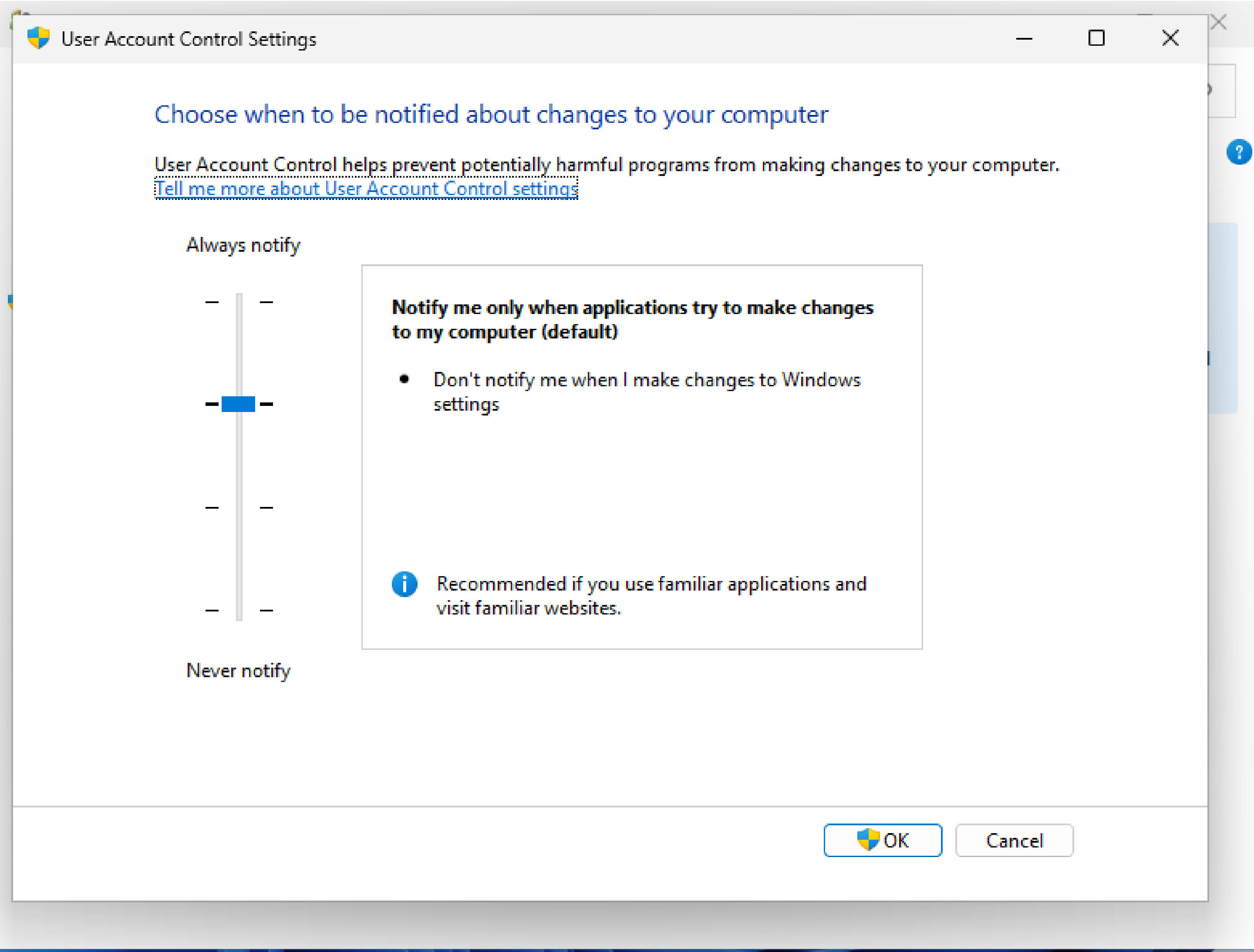
Notify me when a restart is required to finish updating
Show notification when your device requires a restart to finish updating
Off

Active hours
We won't restart your device during these hours
Currently 8:00 AM to 5:00 PM

Additional options

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
User Account Control (UAC) is enabled	Met



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

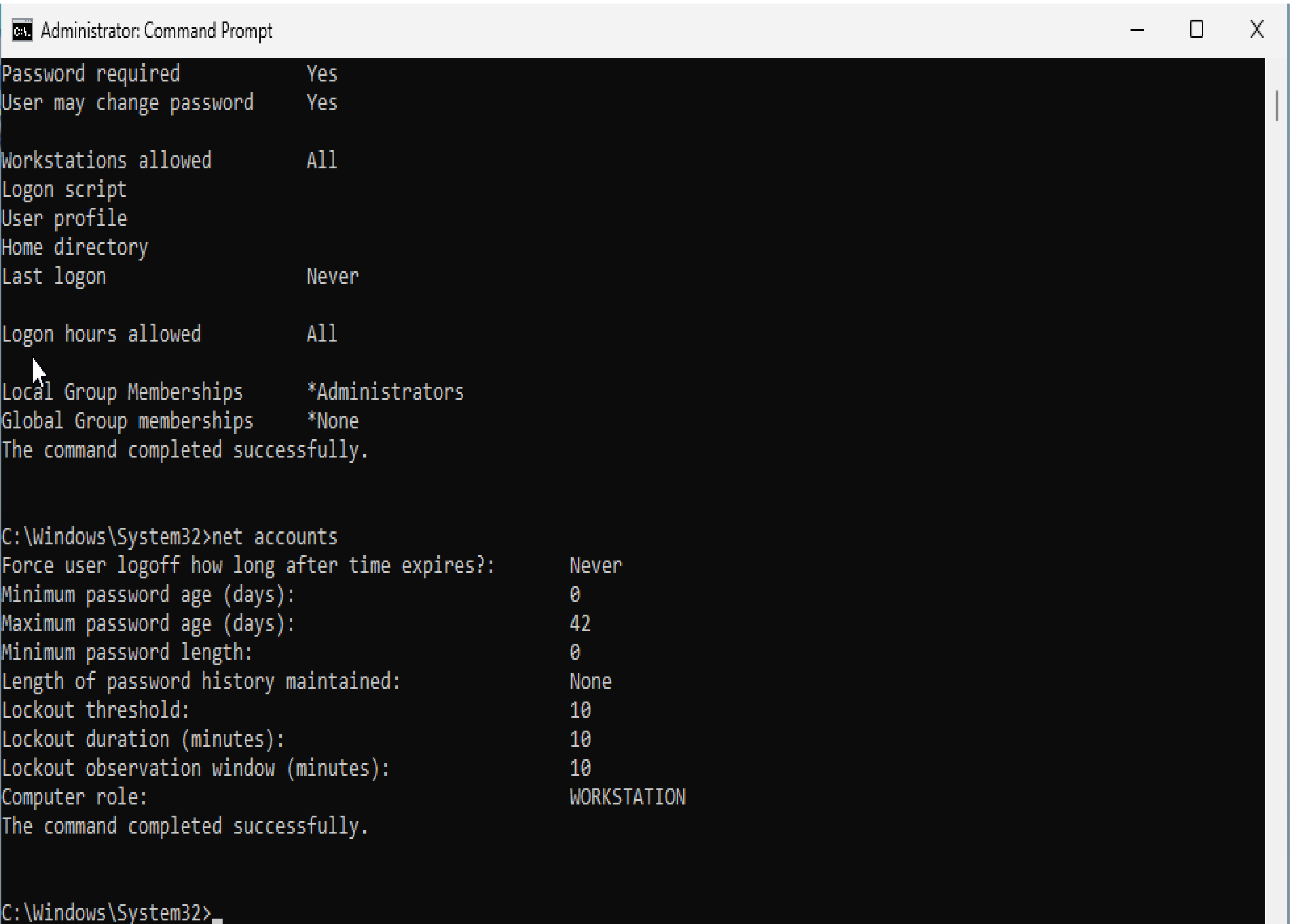
Notify me only when applications try to make changes to my computer (default)

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

Recommended if you use familiar applications and visit familiar websites.

Windows Desktop Compliance

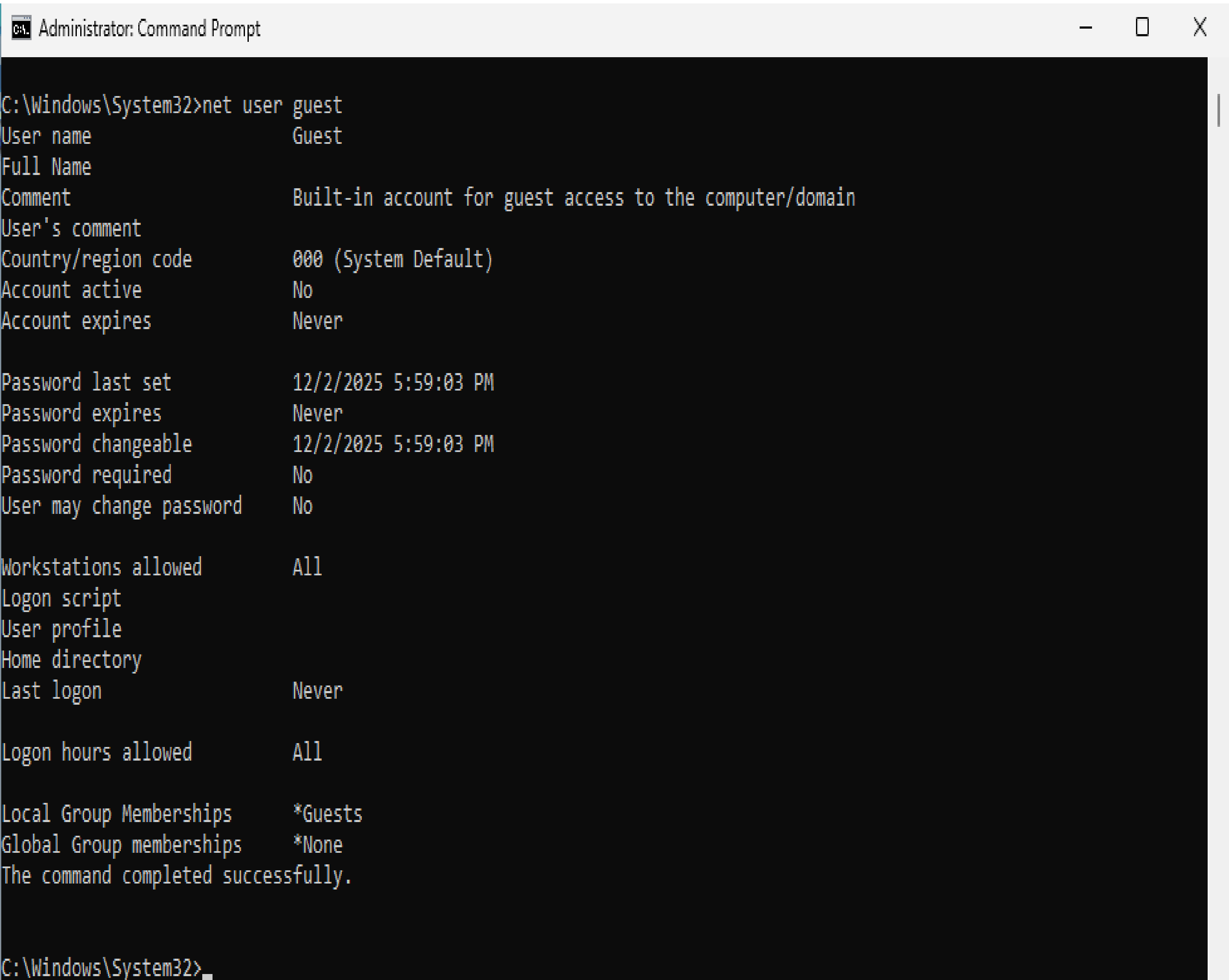
Windows 10 Regulatory Requirement	Met/Not Met
Strong password policies are enforced	Not Met



```
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.


C:\Windows\System32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    10
Lockout duration (minutes):                           10
Lockout observation window (minutes):                 10
Computer role:                                        WORKSTATION
The command completed successfully.


C:\Windows\System32>
```

Windows Desktop Compliance

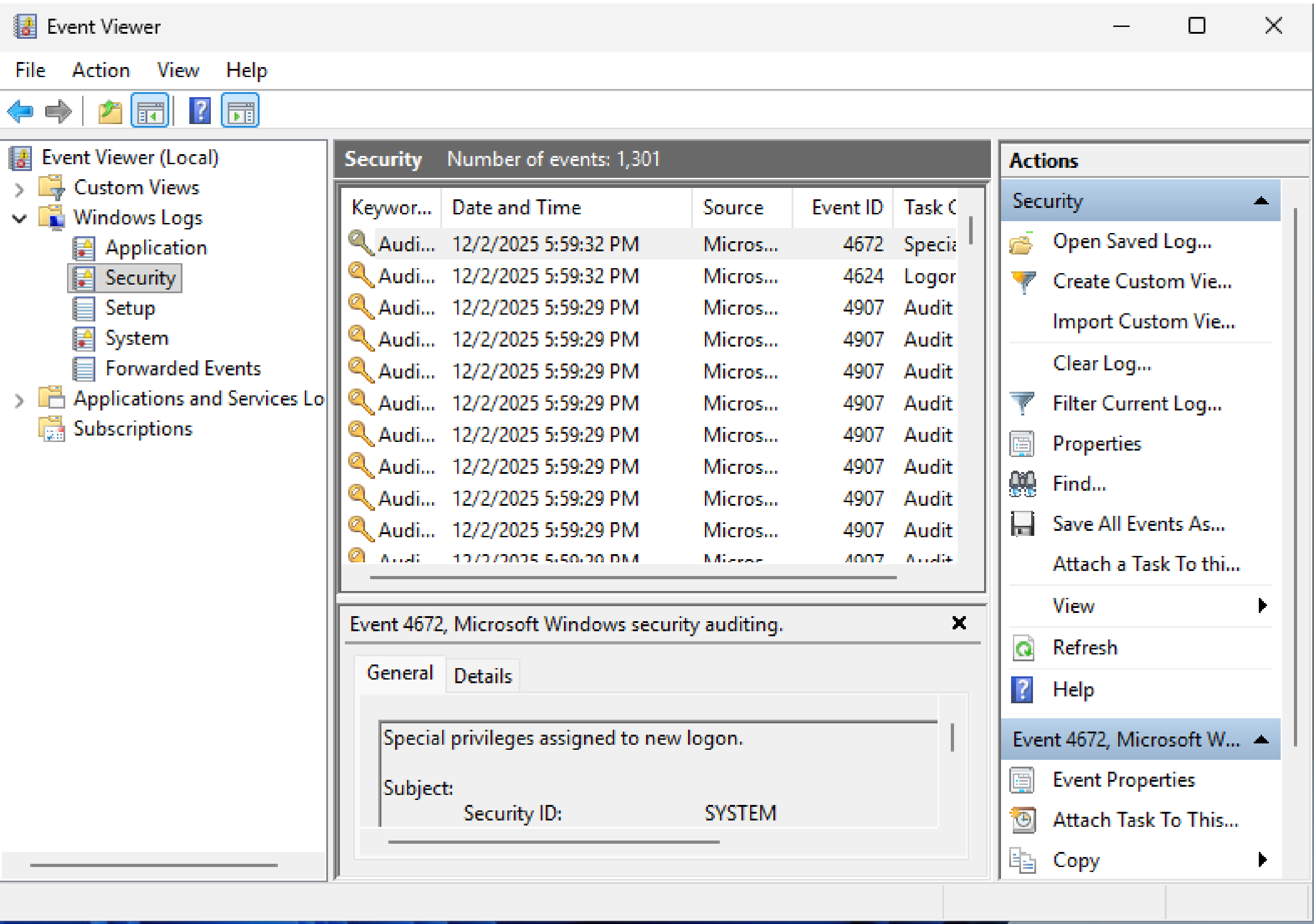
Windows 10 Regulatory Requirement	Met/Not Met
Guest account is disabled	Met



```
C:\Windows\System32>net user guest
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            12/2/2025 5:59:03 PM
Password expires             Never
Password changeable          12/2/2025 5:59:03 PM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Guests
Global Group memberships     *None
The command completed successfully.


C:\Windows\System32>_
```

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
System logging and auditing are enabled	Met



Security Number of events: 1,301

Keywor...	Date and Time	Source	Event ID	Task C
Audi...	12/2/2025 5:59:32 PM	Micros...	4672	Specia
Audi...	12/2/2025 5:59:32 PM	Micros...	4624	Logor
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit
Audi...	12/2/2025 5:59:29 PM	Micros...	4907	Audit

Event 4672, Microsoft Windows security auditing.

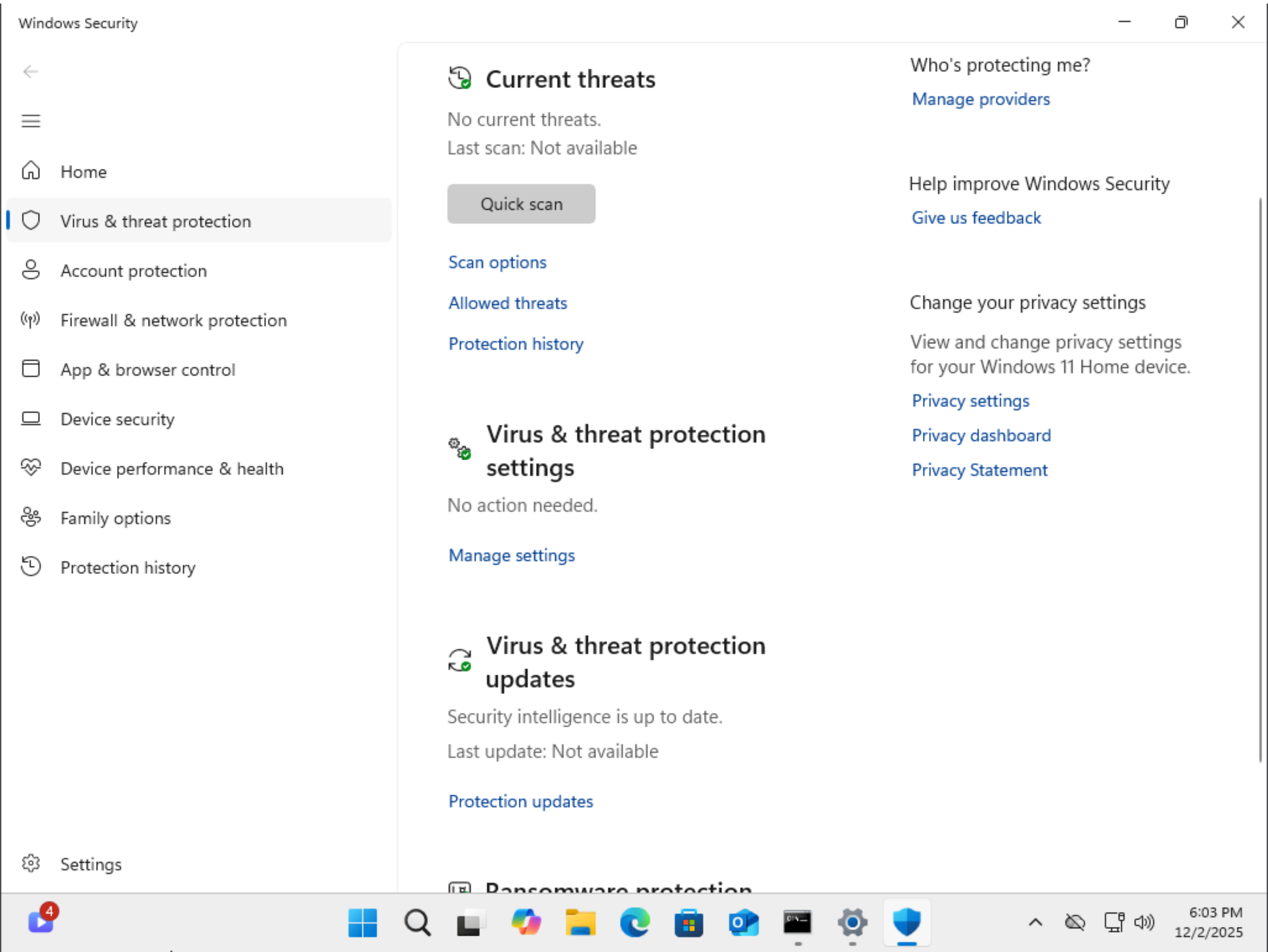
Special privileges assigned to new logon.

Subject:

Security ID: SYSTEM

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Windows Defender Antivirus is enabled and up to date	Met



Current threats

No current threats.

Last scan: Not available

Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

Last update: Not available

Ransomware protection

Who's protecting me?

Help improve Windows Security

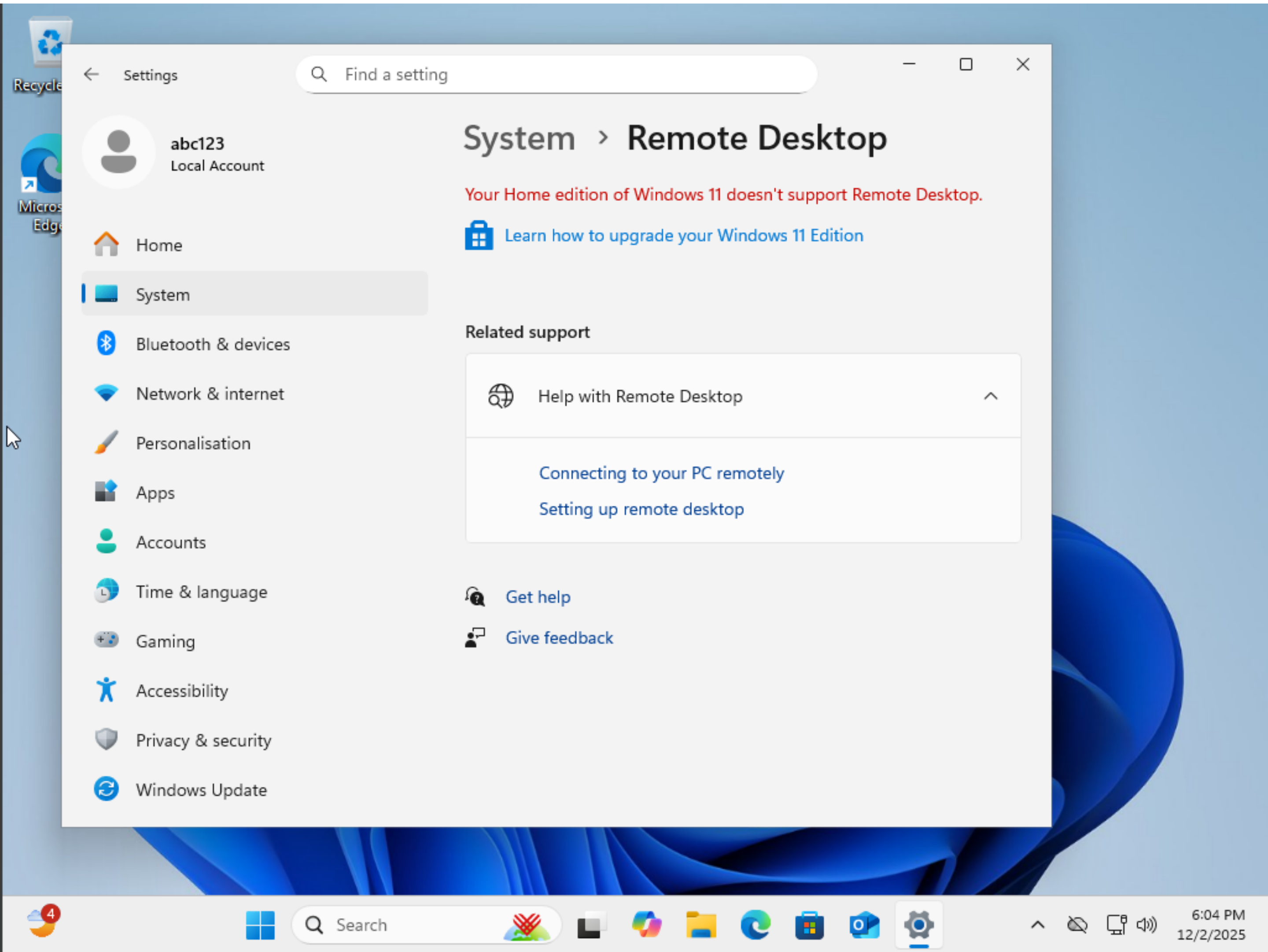
Change your privacy settings

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

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Remote Desktop Services are configured securely	Met

NA the edition does not support Remote Desktop server



System › Remote Desktop

Your Home edition of Windows 11 doesn't support Remote Desktop.

Learn how to upgrade your Windows 11 Edition

Related support

Help with Remote Desktop

Connecting to your PC remotely

Setting up remote desktop

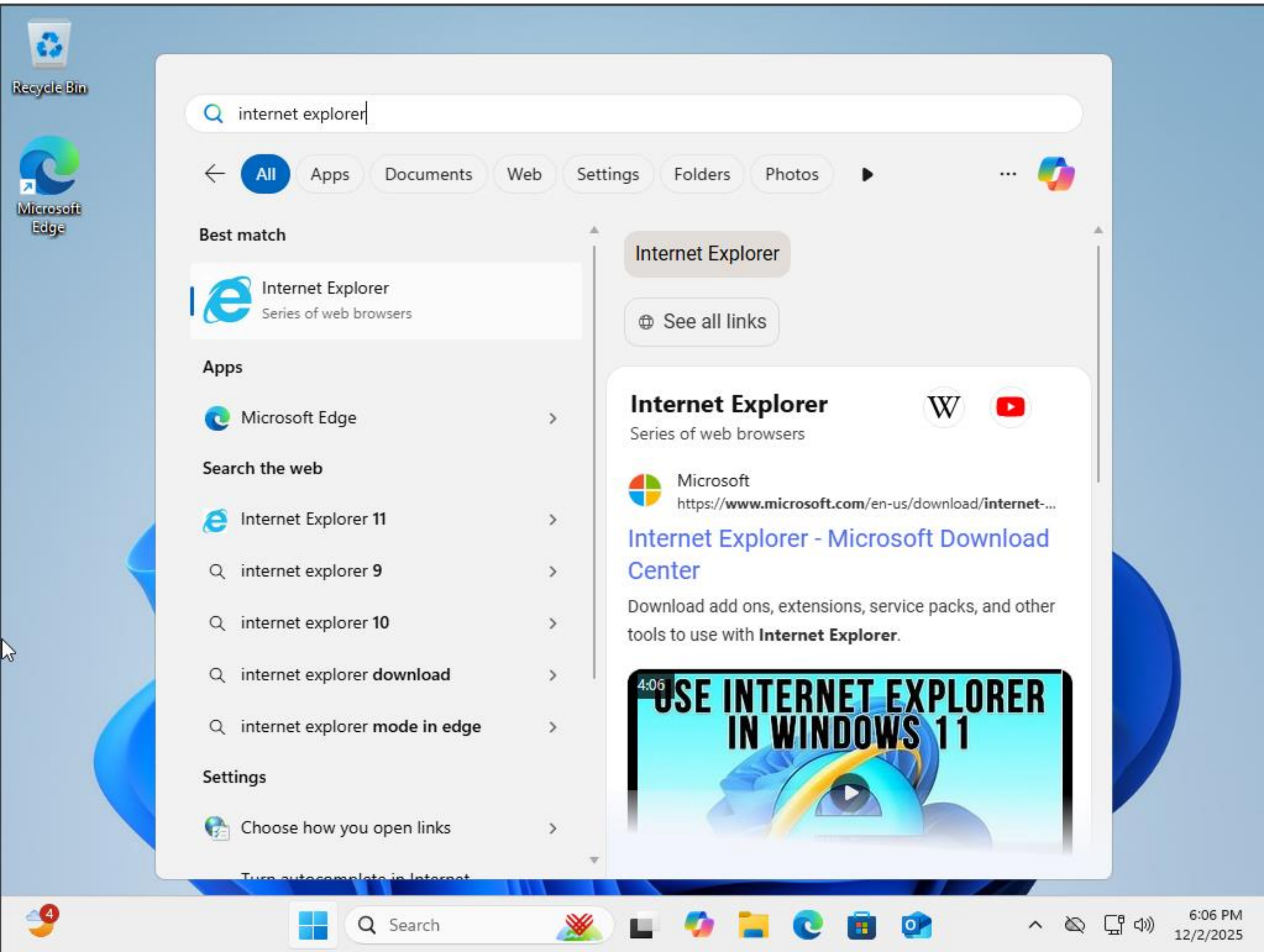
Get help

Give feedback

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Internet Explorer Enhanced Security Configuration (IE ESC) is enabled	Not Met

NA because IE ESC is a server feature and does not apply to a Windows 11 desktop

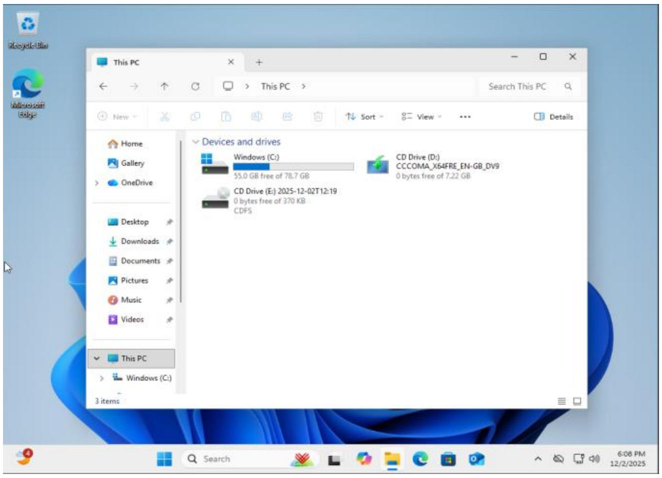


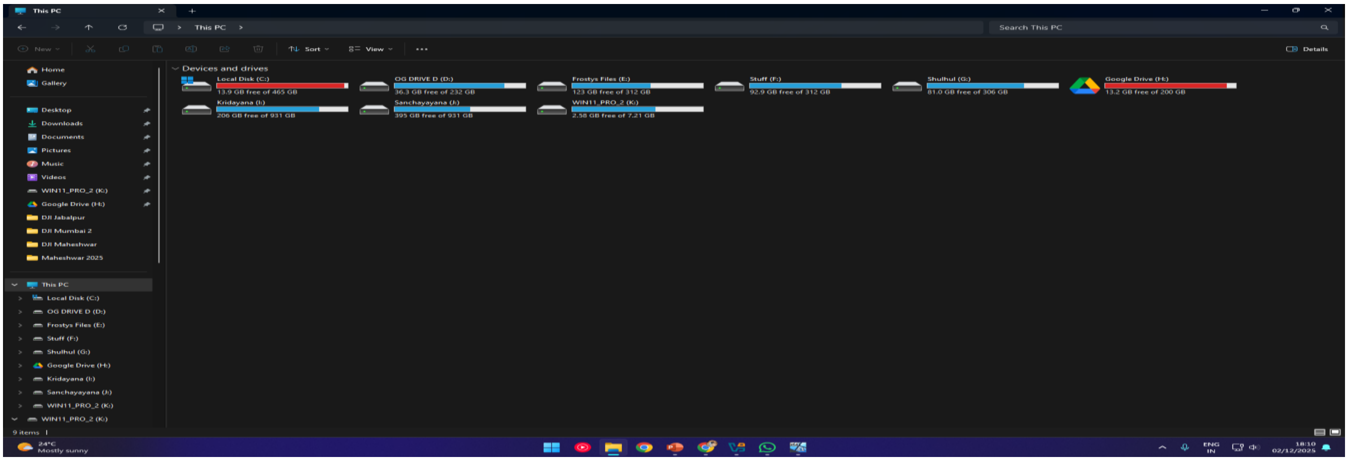
Download add ons, extensions, service packs, and other tools to use with **Internet Explorer**.

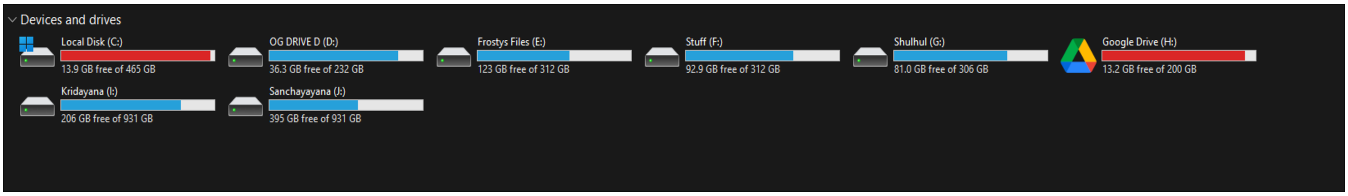
Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
USB ports are disabled or restricted to authorized devices only	Met

The host system detects USB storage but it is not available inside the Windows 11 virtual machine so removable storage is effectively blocked for this desktop



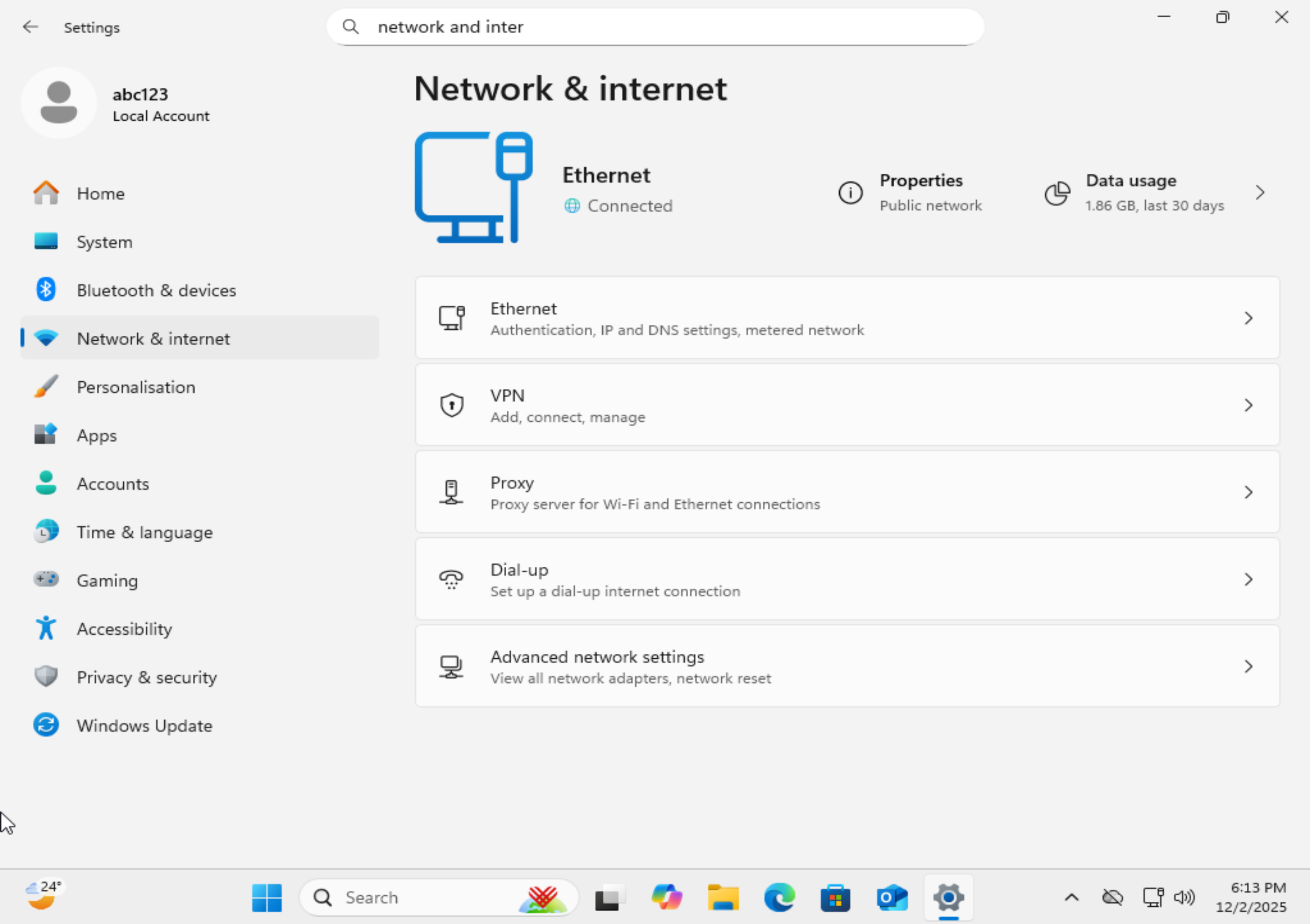




Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Network access controls are implemented, including VLAN segmentation and port security	Not Met

NA: This Windows 11 virtual machine is a client endpoint on a simple VirtualBox virtual network.
VLAN segmentation and switch port security are implemented on network infrastructure devices such as switches and firewalls and cannot be verified or configured from an individual desktop.
Therefore this control is marked Not Applicable for this Windows 11 desktop and is assumed to be handled by the wider network.



Settings

network and inter

abc123
Local Account

Network & internet

Ethernet
Connected

Properties
Public network

Data usage
1.86 GB, last 30 days

Ethernet
Authentication, IP and DNS settings, metered network

VPN
Add, connect, manage

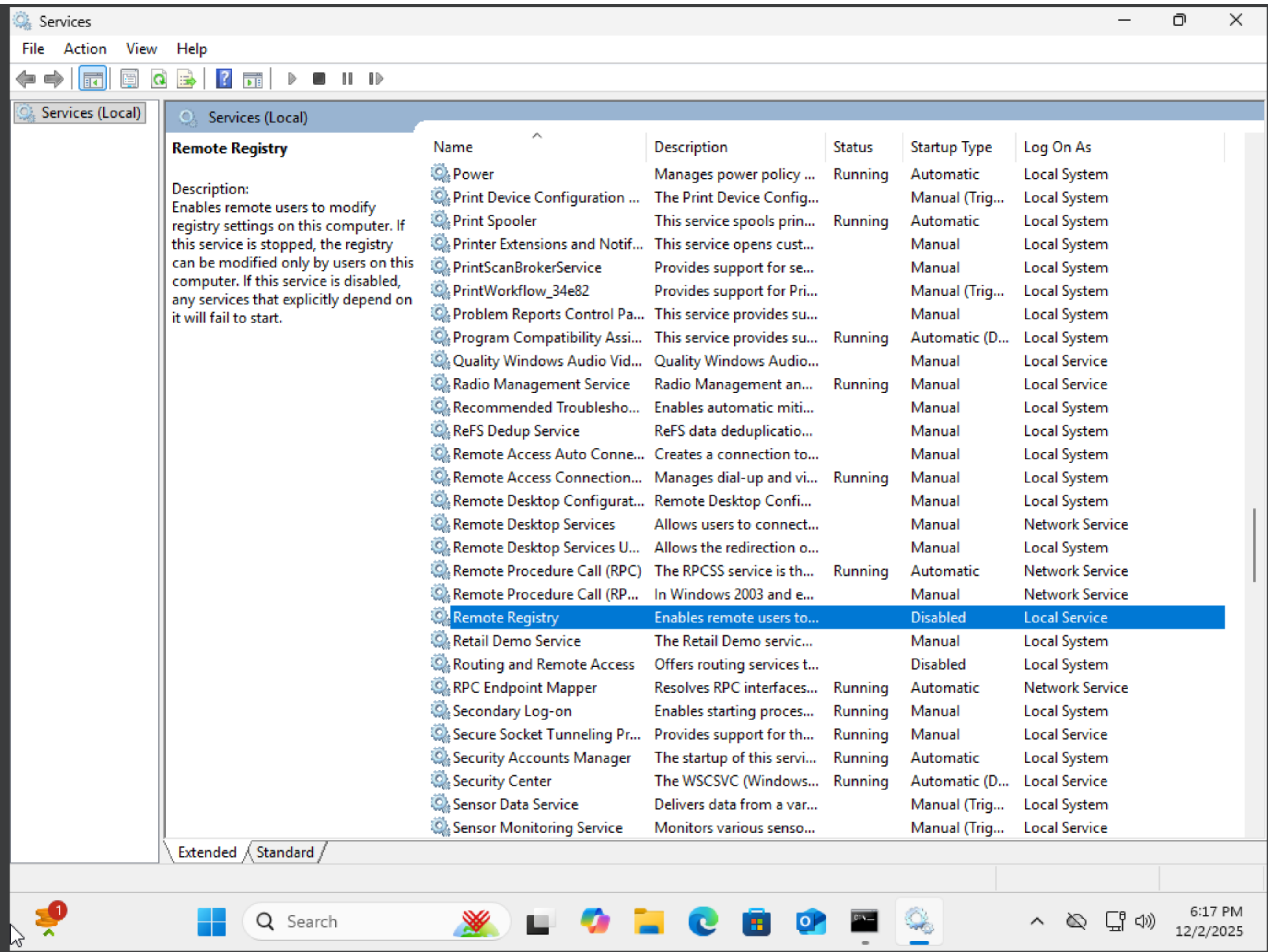
Proxy
Proxy server for Wi-Fi and Ethernet connections

Dial-up
Set up a dial-up internet connection

Advanced network settings
View all network adapters, network reset

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Remote Registry service is disabled	Met



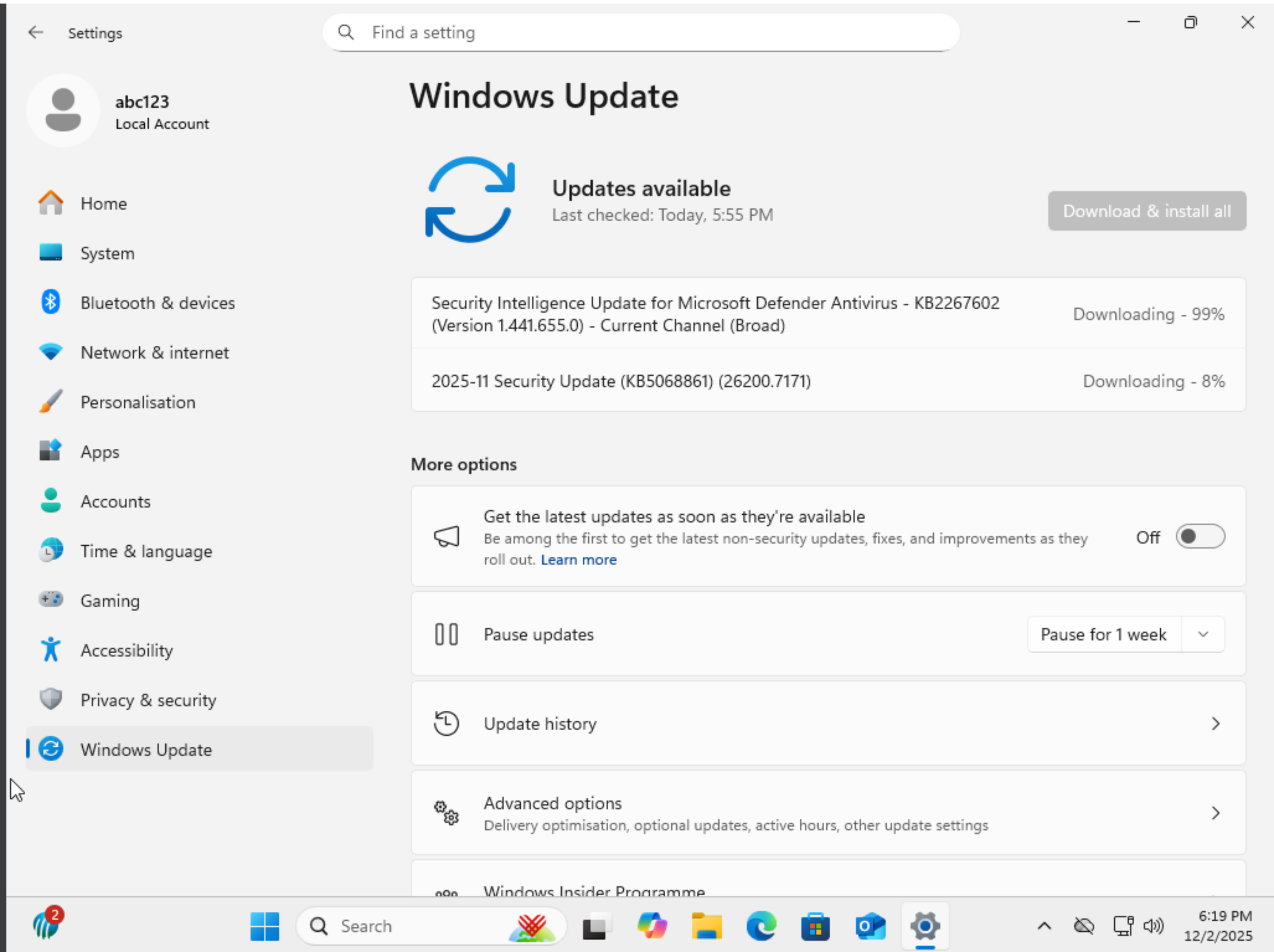
Remote Registry

Description:
Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Power	Manages power policy ...	Running	Automatic	Local System
Print Device Configuration ...	The Print Device Config...		Manual (Trig...	Local System
Print Spooler	This service spools prin...	Running	Automatic	Local System
Printer Extensions and Notif...	This service opens cust...		Manual	Local System
PrintScanBrokerService	Provides support for se...		Manual	Local System
PrintWorkflow_34e82	Provides support for Pri...		Manual (Trig...	Local System
Problem Reports Control Pa...	This service provides su...		Manual	Local System
Program Compatibility Assi...	This service provides su...	Running	Automatic (D...	Local System
Quality Windows Audio Vid...	Quality Windows Audio...		Manual	Local Service
Radio Management Service	Radio Management an...	Running	Manual	Local Service
Recommended Troublesho...	Enables automatic miti...		Manual	Local System
ReFS Dedup Service	ReFS data deduplicatio...		Manual	Local System
Remote Access Auto Conne...	Creates a connection to...		Manual	Local System
Remote Access Connection...	Manages dial-up and vi...	Running	Manual	Local System
Remote Desktop Configurat...	Remote Desktop Confi...		Manual	Local System
Remote Desktop Services	Allows users to connect...		Manual	Network Service
Remote Desktop Services U...	Allows the redirection o...		Manual	Local System
Remote Procedure Call (RPC)	The RPCSS service is th...	Running	Automatic	Network Service
Remote Procedure Call (RP...	In Windows 2003 and e...		Manual	Network Service
Remote Registry	Enables remote users to...		Disabled	Local Service
Retail Demo Service	The Retail Demo servic...		Manual	Local System
Routing and Remote Access	Offers routing services t...		Disabled	Local System
RPC Endpoint Mapper	Resolves RPC interfaces...	Running	Automatic	Network Service
Secondary Log-on	Enables starting proces...	Running	Manual	Local System
Secure Socket Tunneling Pr...	Provides support for th...	Running	Manual	Local Service
Security Accounts Manager	The startup of this servi...	Running	Automatic	Local System
Security Center	The WSCSVC (Windows...	Running	Automatic (D...	Local Service
Sensor Data Service	Delivers data from a var...		Manual (Trig...	Local System
Sensor Monitoring Service	Monitors various senso...		Manual (Trig...	Local Service

Windows Desktop Compliance

Windows 10 Regulatory Requirement	Met/Not Met
Windows Updates are configured to download and install updates automatically	Met



Windows Update

Updates available

Last checked: Today, 5:55 PM

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.441.655.0) - Current Channel (Broad)	Downloading - 99%
2025-11 Security Update (KB5068861) (26200.7171)	Downloading - 8%

More options

Get the latest updates as soon as they're available
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. Learn more — Off

Pause updates — Pause for 1 week

Update history

Advanced options
Delivery optimisation, optional updates, active hours, other update settings

Windows Insider Programme

6:19 PM
12/2/2025

Windows Desktop Compliance

Strong password policies are enforced

Strong password policies are enforced Configure password settings to require at least twelve character passwords that use letters numbers and symbols and prevent reuse through password history set in local security policy or domain group policy

Internet Explorer Enhanced Security Configuration IE ESC is enabled

Internet Explorer Enhanced Security Configuration IE ESC is enabled On systems that still have Internet Explorer enable the enhanced security configuration for all users through Server Manager or group policy or if Internet Explorer is not required remove or disable it and require use of a modern browser

Network access controls are implemented including VLAN segmentation and port security

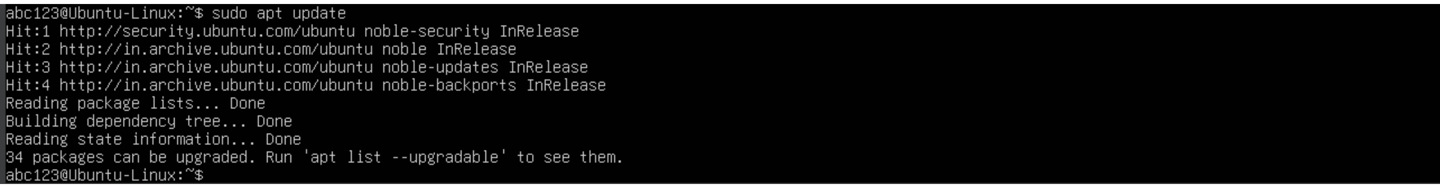
Network access controls are implemented including VLAN segmentation and port security Place this desktop on a secured network that uses separate VLANs and switch port security and restrict traffic with firewall rules so the device can only reach approved networks and services

Linux Compliance

Linux CMMC Requirements	Met/Not Met
Current on security updates	Not Met
Ensure separate partition exists for /var	Not Met
Disable Automounting of drives	Met
Ensure AIDE is installed	Not Met
Ensure daytime services are not enabled	Met
Ensure echo services are not enabled	Met
Ensure tftp server is not enabled	Met
Ensure CUPS is not enabled	Met
Ensure DHCP Server is not enabled	Met
Ensure FTP Server is not enabled	Met
Ensure Samba is not enabled	Met
Ensure TCP Wrappers is installed	Met
Ensure DCCP is disabled	Met
Ensure iptables is installed	Met
Ensure audit log storage size is configured	Not Met
Ensure audit logs are not automatically deleted	Not Met

Linux Compliance

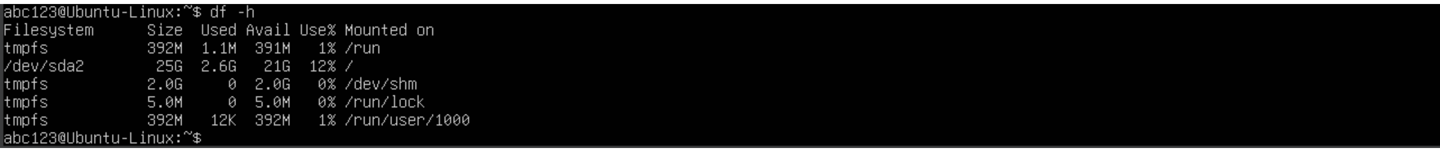
Linux Regulatory Requirement	Met/Not Met
Current on security updates	Not Met



```
abc123@Ubuntu-Linux:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
34 packages can be upgraded. Run 'apt list --upgradable' to see them.
abc123@Ubuntu-Linux:~$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure separate partition exists for /var	Not Met

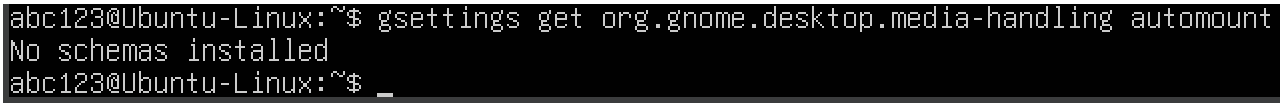


```
abc123@Ubuntu-Linux:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           392M  1.1M  391M   1% /run
/dev/sda2        25G  2.6G   21G  12% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           392M   12K  392M   1% /run/user/1000
abc123@Ubuntu-Linux:~$
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Disable Automounting of drives	Met

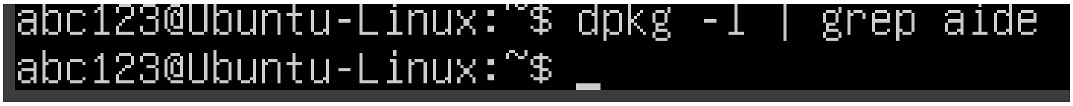
The system does not have a desktop media handling schema so removable drives are not automatically managed by GNOME. Since no automounting feature is present the requirement to disable automount is effectively satisfied.



```
abc123@Ubuntu-Linux:~$ gsettings get org.gnome.desktop.media-handling automount
No schemas installed
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

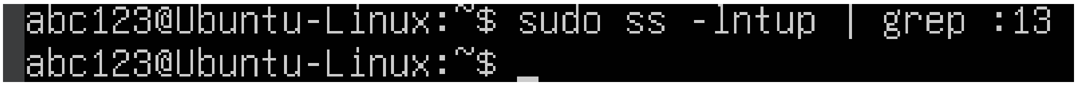
Linux Regulatory Requirement	Met/Not Met
Ensure AIDE is installed	Not Met



```
abc123@Ubuntu-Linux:~$ dpkg -l | grep aide
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

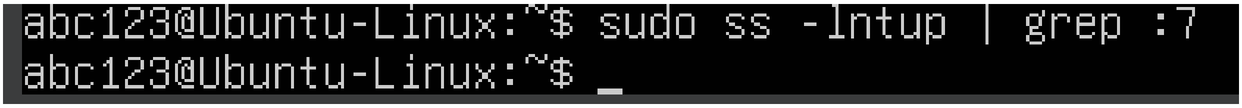
Linux Regulatory Requirement	Met/Not Met
Ensure daytime services are not enabled	Met



```
abc123@Ubuntu-Linux:~$ sudo ss -lntup | grep :13
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

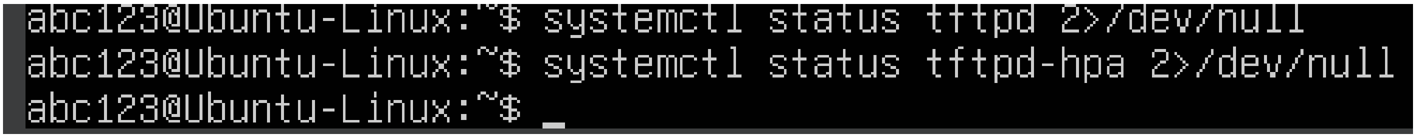
Linux Regulatory Requirement	Met/Not Met
Ensure echo services are not enabled	Met



```
abc123@Ubuntu-Linux:~$ sudo ss -lntup | grep :7
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

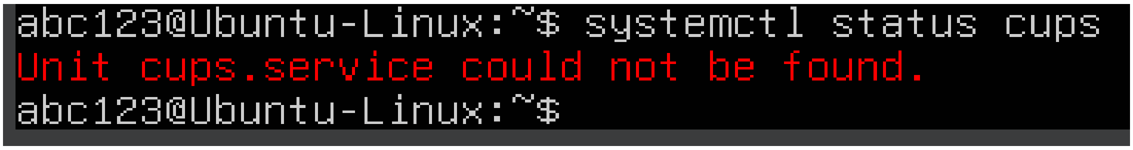
Linux Regulatory Requirement	Met/Not Met
Ensure tftp server is not enabled	Met



```
abc123@Ubuntu-Linux:~$ systemctl status tftpd 2>/dev/null
abc123@Ubuntu-Linux:~$ systemctl status tftpd-hpa 2>/dev/null
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

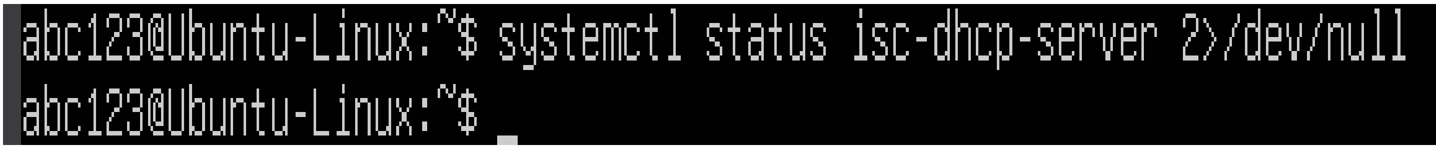
Linux Regulatory Requirement	Met/Not Met
Ensure CUPS is not enabled	Met



```
abc123@Ubuntu-Linux:~$ systemctl status cups
Unit cups.service could not be found.
abc123@Ubuntu-Linux:~$
```

Linux Compliance

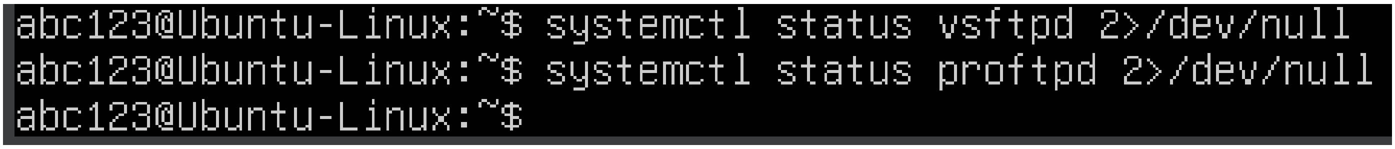
Linux Regulatory Requirement	Met/Not Met
Ensure DHCP Server is not enabled	Met



```
abc123@Ubuntu-Linux:~$ systemctl status isc-dhcp-server 2>/dev/null
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

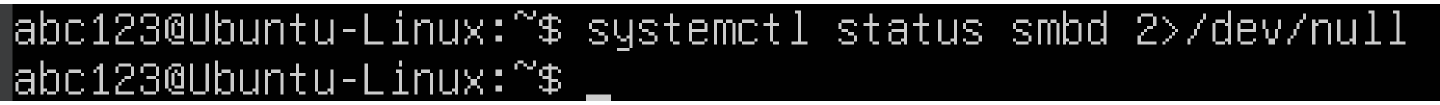
Linux Regulatory Requirement	Met/Not Met
Ensure FTP Server is not enabled	Met



```
abc123@Ubuntu-Linux:~$ systemctl status vsftpd 2>/dev/null
abc123@Ubuntu-Linux:~$ systemctl status proftpd 2>/dev/null
abc123@Ubuntu-Linux:~$
```

Linux Compliance

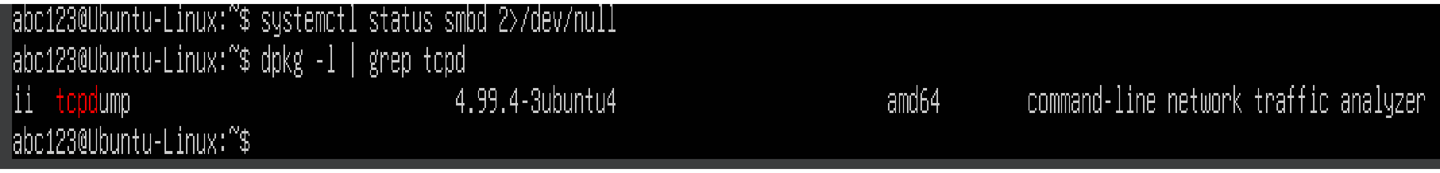
Linux Regulatory Requirement	Met/Not Met
Ensure Samba is not enabled	Met



```
abc123@Ubuntu-Linux:~$ systemctl status smbd 2>/dev/null
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

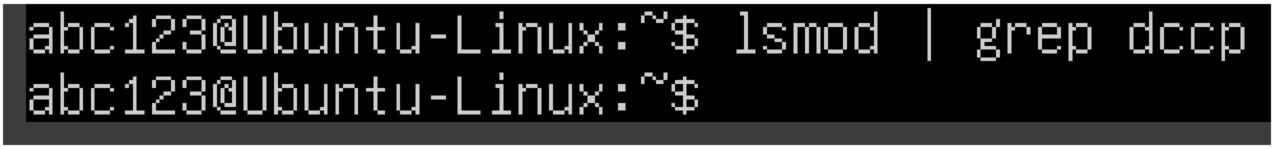
Linux Regulatory Requirement	Met/Not Met
Ensure TCP Wrappers is installed	Met



```
abc123@Ubuntu-Linux:~$ systemctl status smbd 2>/dev/null
abc123@Ubuntu-Linux:~$ dpkg -l | grep tcpd
ii  tcpdump                               4.99.4-3ubuntu4                         amd64        command-line network traffic analyzer
abc123@Ubuntu-Linux:~$
```

Linux Compliance

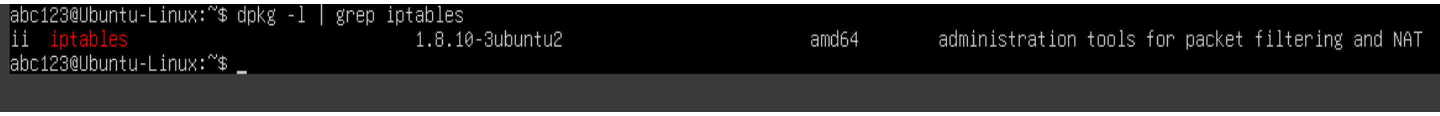
Linux Regulatory Requirement	Met/Not Met
Ensure DCCP is disabled	Met



```
abc123@Ubuntu-Linux:~$ lsmod | grep dccp
abc123@Ubuntu-Linux:~$
```

Linux Compliance

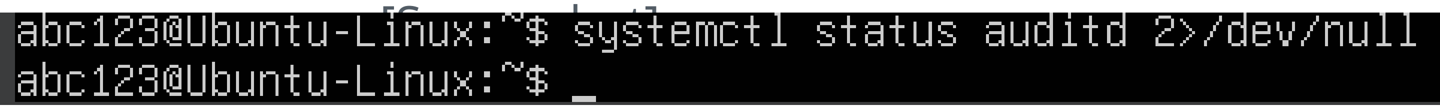
Linux Regulatory Requirement	Met/Not Met
Ensure iptables is installed	Met



```
abc123@Ubuntu-Linux:~$ dpkg -l | grep iptables
ii  iptables                             1.8.10-3ubuntu2                         amd64        administration tools for packet filtering and NAT
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure audit log storage size is configured	Not Met

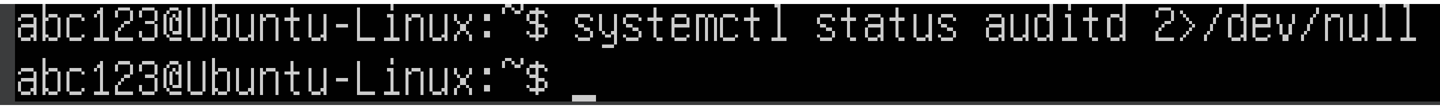


```
abc123@Ubuntu-Linux:~$ systemctl status auditd 2>/dev/null
abc123@Ubuntu-Linux:~$ _
```

Linux Compliance

Linux Regulatory Requirement	Met/Not Met
Ensure audit logs are not automatically deleted	Not Met

It is not met because the iptables package is not installed and the iptables command is not available on this Linux VM so firewall rules cannot be managed using iptables



```
abc123@Ubuntu-Linux:~$ systemctl status auditd 2>/dev/null
abc123@Ubuntu-Linux:~$ _
```

Section 4:

Cloud Management

Windows Server Build Sheet

1. Hardened base image

Use a standard Windows Server image that is fully patched and has only required roles and features installed such as Web Server IIS and no extra tools.

2. Local account and password policy

Create a named admin account and disable direct use of the built in Administrator account. Enforce strong password rules and account lockout settings before the server is exposed.

3. Network security rules

Place the server in a locked down subnet with network security groups or firewalls that allow only required ports such as HTTPS on port 443 from the internet and RDP only from admin networks.

4. Windows Firewall configuration

Enable Windows Defender Firewall on all profiles and create explicit rules that only permit traffic for web services management and monitoring.

5. IIS hardening and site layout

Install IIS with only needed modules. Use a dedicated folder for web content with least privilege NTFS permissions and turn off directory browsing and other unnecessary features.

Windows Server Build Sheet

6. TLS certificate and HTTPS only access

Install a valid TLS certificate for the site and configure IIS bindings so that users connect over HTTPS only. Redirect any HTTP request to HTTPS to protect data in transit.

7. Anti malware and endpoint protection

Enable Microsoft Defender or a company approved endpoint protection agent. Configure real time protection and scheduled scans and ensure definition updates are automatic.

8. Logging and monitoring setup

Turn on detailed IIS logging and Windows event logging. Forward logs to a central log server or SIEM for alerting and long term storage so that incidents can be detected and investigated.

9. Backup and restore plan

Configure regular backups of the server configuration and web content to secure storage in the cloud. Test restore procedures so the site can be recovered quickly after a failure or attack.

10. Least privilege service accounts

Run application pools and background services under dedicated service accounts that have only the rights they need. Avoid using local admin or domain admin accounts for normal application work.

Enhancing Cloud Security with CASB

1. Central visibility of cloud use

Gives one place to see all cloud applications in use including unsanctioned apps. Helps Fed F1rst understand which users and devices access each service.

2. Stronger data loss prevention

Lets the company inspect files and messages going to cloud apps and block or quarantine sensitive data such as customer records or designs that should not leave the network.

3. Fine grained access control

Applies access rules based on user role device type and location. Can allow full access from trusted devices and read only or blocked access from risky locations.

4. Threat detection for cloud activity

Monitors behaviour in cloud apps to spot account takeover malware activity and unusual logins. Can trigger alerts and automatic actions such as forcing a password reset.

5. Support for compliance and audit

Provides detailed logs and reports of who accessed which cloud data and when. Helps demonstrate compliance with security standards and internal policies.