

# COMPLIANCE ASSESSMENT



*Deekshith A*

# Project Scenario

# Overview

In the swiftly evolving digital age, Fed F1rst Control Systems stands at the cusp of a significant transformation, pushing the boundaries of cybersecurity to safeguard its technological frontier. As the organization embarks on integrating cutting-edge tools and technologies, from Windows environments to the inclusion of MacBooks, and ventures deeper into the cloud, the role of a security engineer has never been more pivotal. Amidst this backdrop, you, as a security engineer, are thrust into the heart of this transformation.

Your mission: to navigate the complexities of digital security, ensuring that every technological advancement—be it through securing desktop environments, fortifying email communications, or aligning with stringent cybersecurity standards—translates into a fortified defense against the cyber threats of tomorrow. Your efforts will not only secure Fed F1rst's digital assets but also shape the very foundation of its future in the digital realm.

Welcome to the forefront of cybersecurity at Fed F1rst Control Systems, where your expertise is the key to unlocking a secure, innovative future.

# Section 1:

## Developing a Hardening Strategy

# Windows 10 Hardening

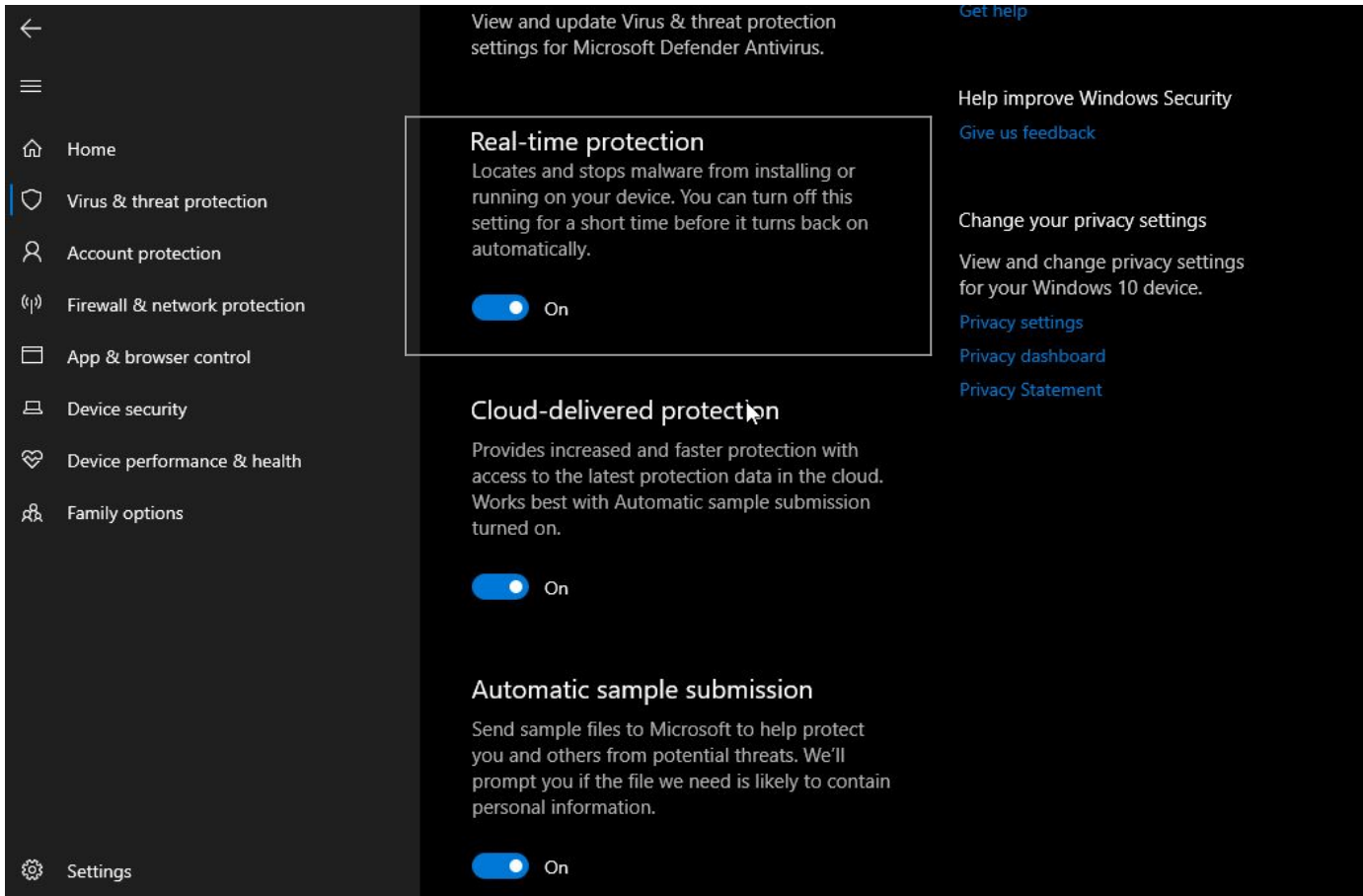
## System Updates



Setting Up Auto System Update For Security Purpose and Minimizing Attack Surface.

# Windows 10 Hardening

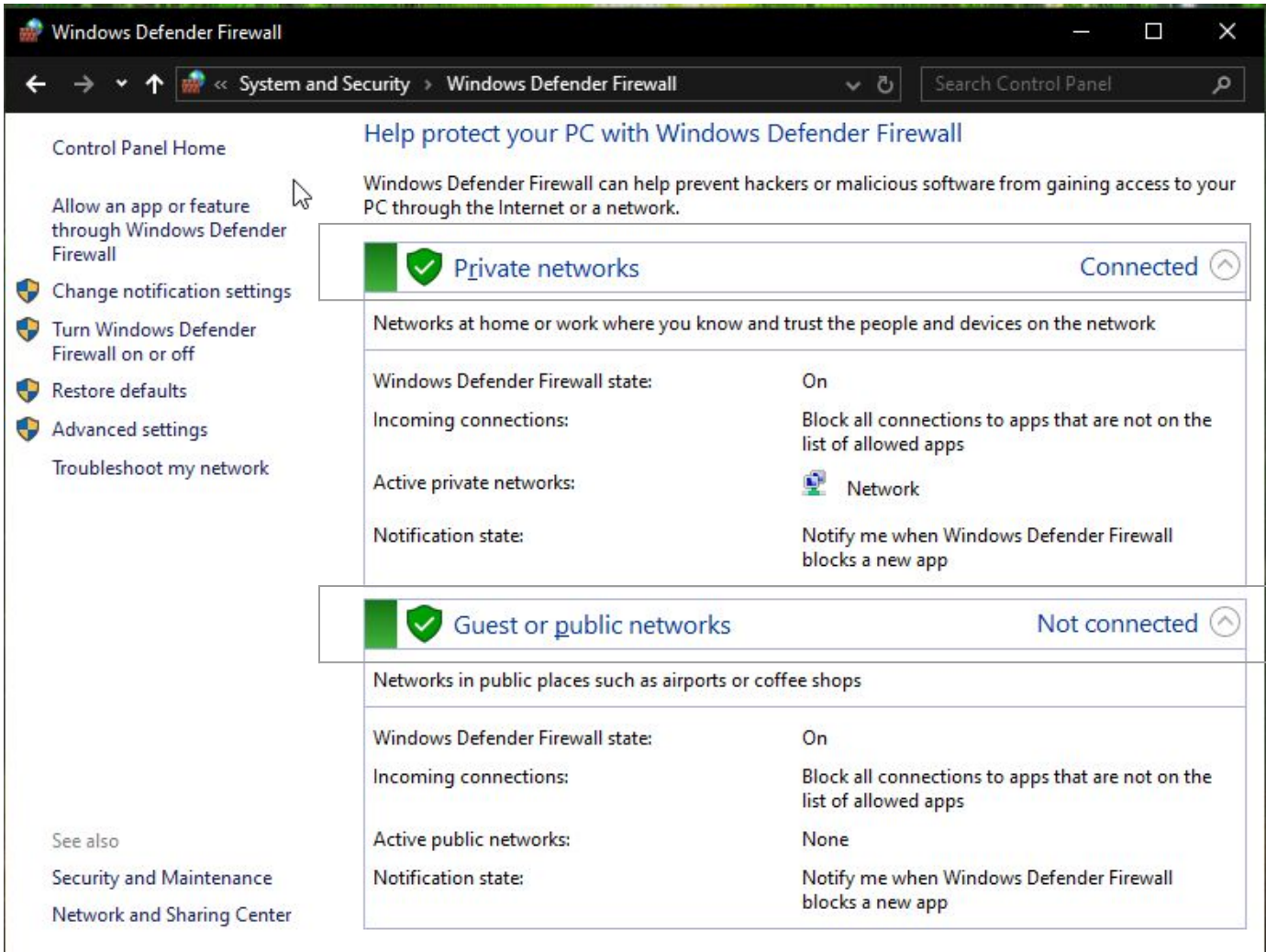
## Antivirus Status



Real-time Protection(Windows Defender) Helps to prevent the creation and Malware Spreading

# Windows 10 Hardening

## Firewall Settings



The screenshot shows the Windows Defender Firewall control panel window. The title bar reads "Windows Defender Firewall". The breadcrumb navigation shows "System and Security > Windows Defender Firewall". The main heading is "Help protect your PC with Windows Defender Firewall". Below this, a description states: "Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network." The left sidebar contains links: "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", and "Troubleshoot my network". The main content area displays two network profiles: "Private networks" (Connected) and "Guest or public networks" (Not connected). Each profile has a description, the firewall state, incoming connections, active networks, and notification state.

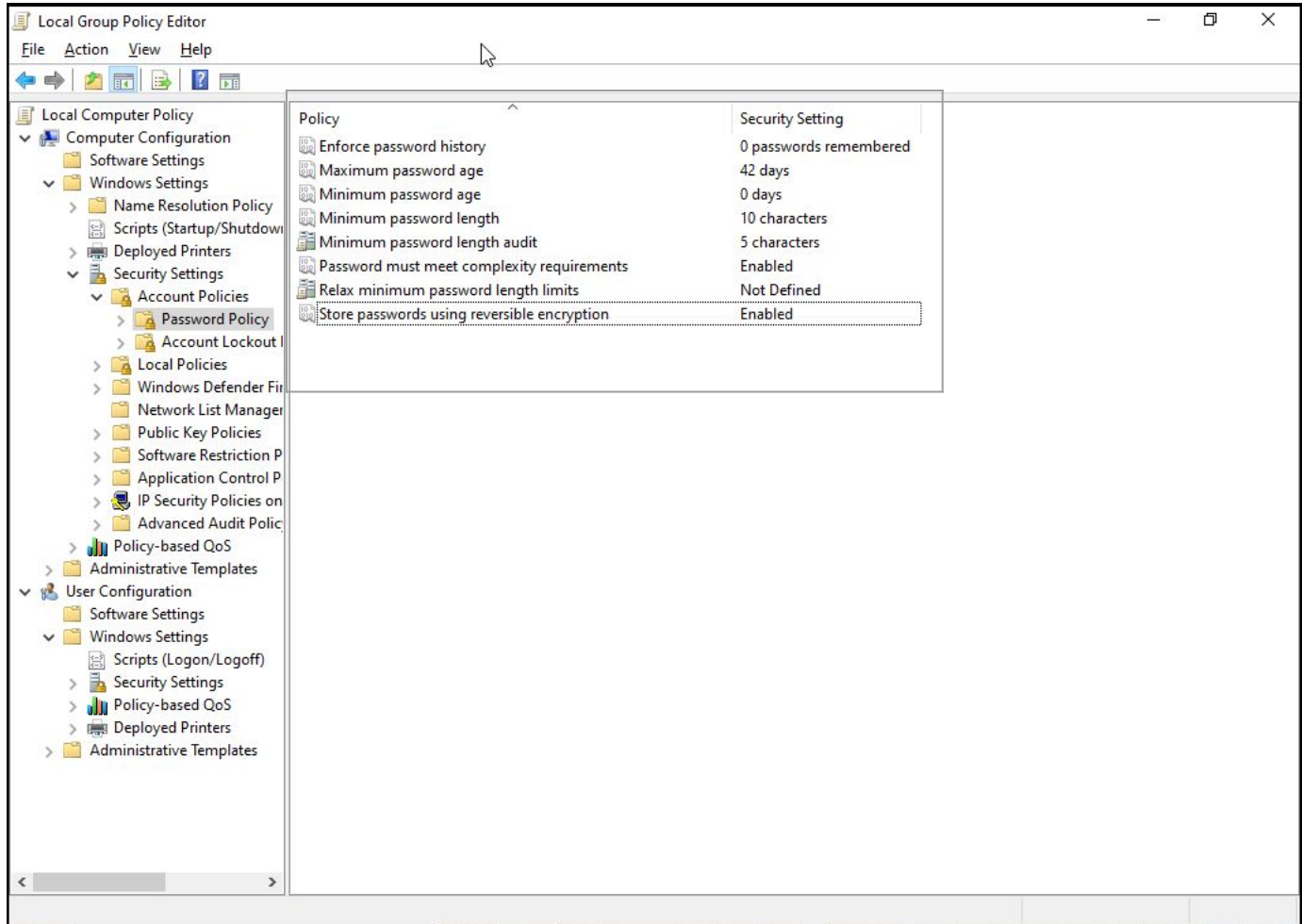
Network Profile	Connection Status	Description	Windows Defender Firewall state	Incoming connections	Active networks	Notification state
Private networks	Connected	Networks at home or work where you know and trust the people and devices on the network	On	Block all connections to apps that are not on the list of allowed apps	Network	Notify me when Windows Defender Firewall blocks a new app
Guest or public networks	Not connected	Networks in public places such as airports or coffee shops	On	Block all connections to apps that are not on the list of allowed apps	None	Notify me when Windows Defender Firewall blocks a new app

See also  
Security and Maintenance  
Network and Sharing Center

## Configuring The Firewall To both Public and Private Networks

# Windows 10 Hardening

## Password Policies

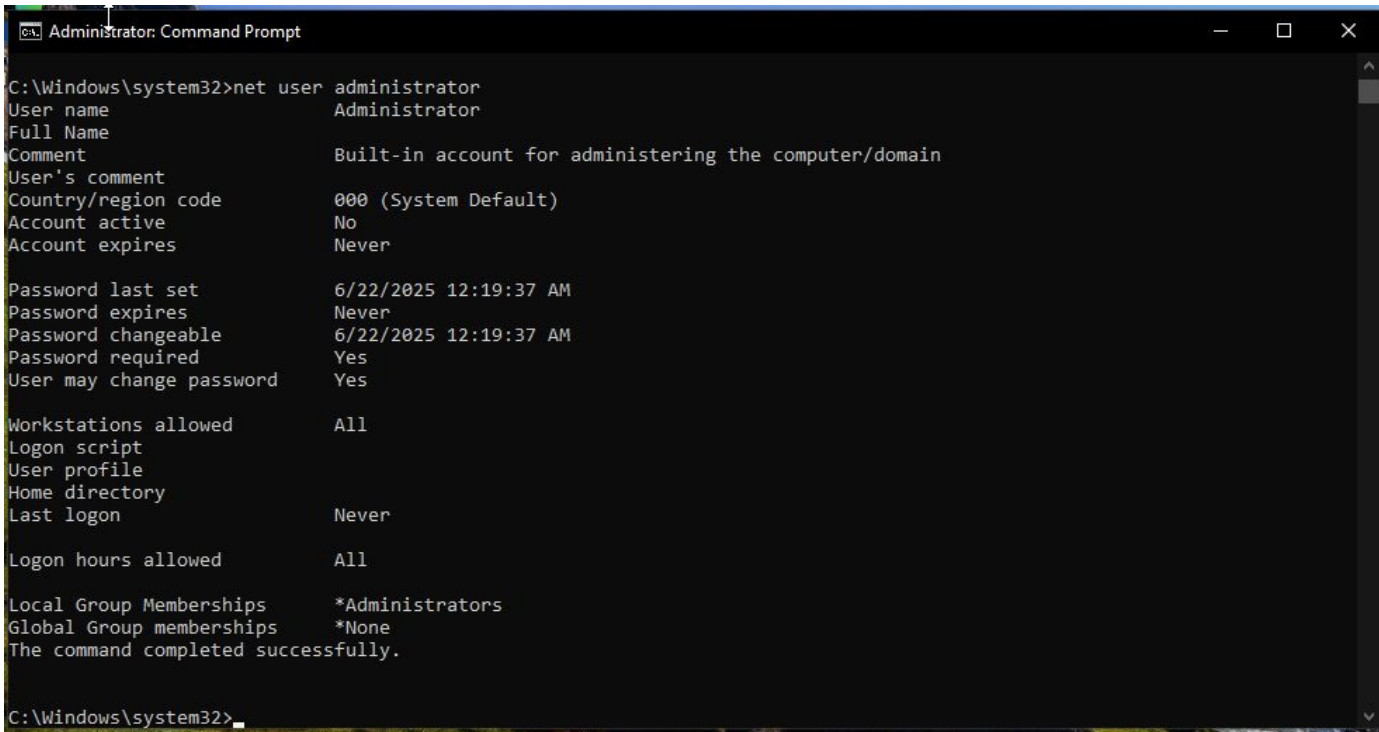


Ensure the Implementation of Strong Password Policies



# Windows 10 Hardening

## Administrator Account Settings

A screenshot of a Windows 10 Administrator Command Prompt window. The title bar reads "Administrator: Command Prompt". The command prompt shows the command "C:\Windows\system32>net user administrator" and its output. The output lists various user properties for the built-in administrator account, including name, full name, comment, password settings, and group memberships. The command completed successfully.

```
C:\Windows\system32>net user administrator
User name                Administrator
Full Name                Built-in account for administering the computer/domain
Comment
User's comment
Country/region code      000 (System Default)
Account active           No
Account expires          Never

Password last set        6/22/2025 12:19:37 AM
Password expires         Never
Password changeable      6/22/2025 12:19:37 AM
Password required        Yes
User may change password Yes

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

Logon hours allowed      All

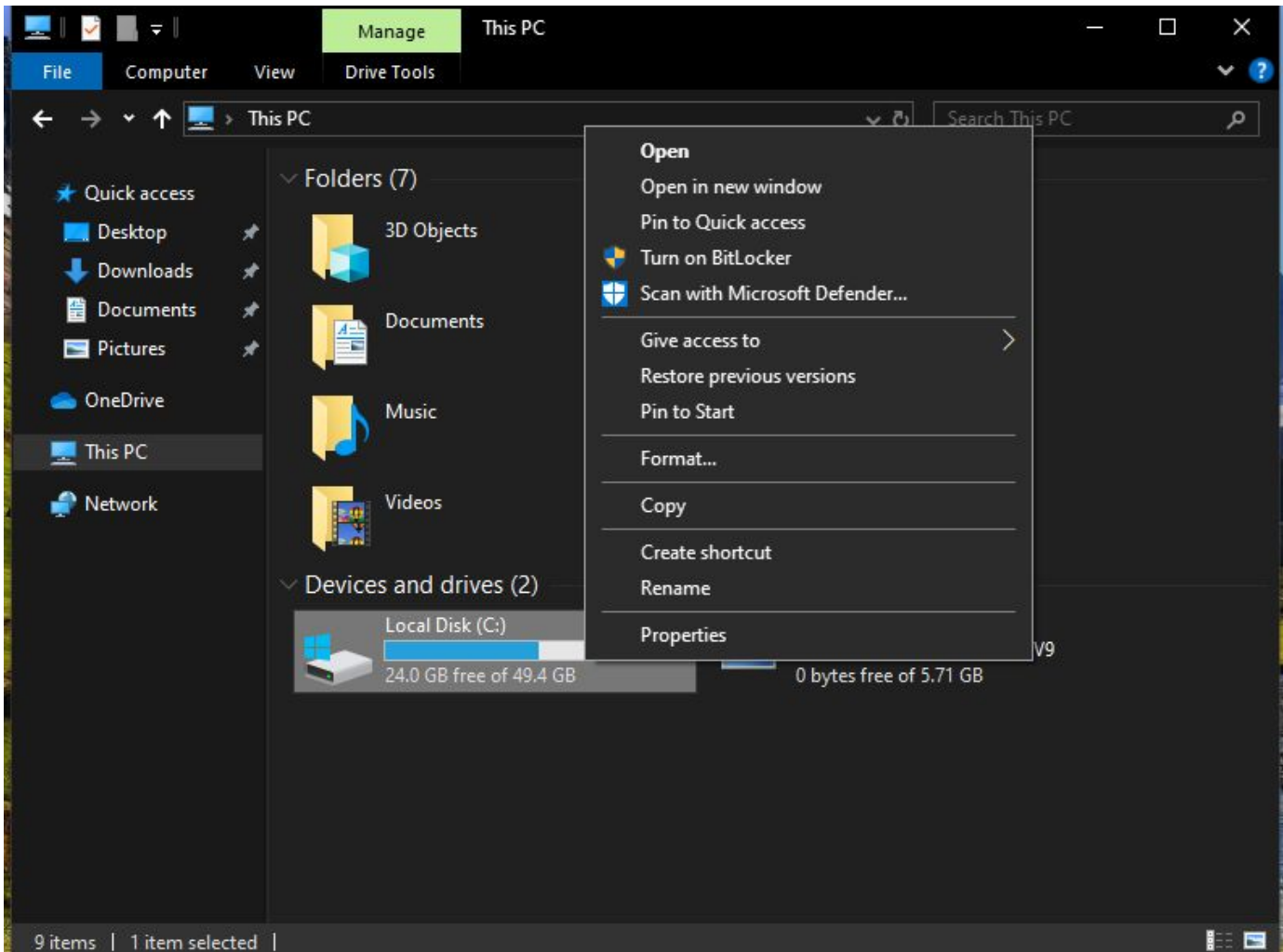
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.

C:\Windows\system32>
```

Change Admin Account Name and set a strong password  
Also Disable if Admin Privileges are not necessary

# Windows 10 Hardening

## BitLocker Drive Encryption



Enable Bitlocker with a strong password for all drives present in the system

# MacOS Hardening

## **1. Enable FileVault (Full Disk Encryption)**

FileVault encrypts the entire hard drive, protecting all data at rest. If a MacBook is lost or stolen, unauthorized users cannot access the data without the login credentials. This is crucial for safeguarding confidential business and customer information and ensuring compliance with data protection regulations.

## **2. Set Up a Mobile Device Management (MDM) Solution**

An MDM allows IT administrators to remotely manage, configure, and secure MacBooks. It enforces security policies, deploys updates, tracks assets, and remotely wipes devices if lost or compromised. This central management is essential for maintaining consistency, security compliance, and operational efficiency.

## **3. Enforce Secure Login Policies (Strong Passwords & FileVault Recovery Key)**

Require strong passwords (complexity and length) and associate a FileVault recovery key with the MDM for account recovery. This protects against brute-force and unauthorized access. Password policies ensure that users follow best practices for authentication security.

# MacOS Hardening

## **4. Disable Automatic Login and Guest Access**

Disabling automatic login ensures users authenticate each time the device is started, reducing the risk of unauthorized access. Disabling guest access prevents anonymous users from logging in and potentially misusing the system or network resources.

## **5. Enable Firewall and Limit Incoming Connections**

macOS includes a built-in firewall that can block unwanted incoming connections. Enabling it and configuring it to allow only necessary services limits exposure to network-based attacks, especially when devices are used on public or untrusted networks.

## **6. Apply System and Security Updates Automatically**

Enabling automatic updates ensures that all critical patches for macOS, firmware, and native apps are applied promptly. This protects against known vulnerabilities and exploits, helping maintain system integrity and reducing the risk of targeted attacks.

# Section 2:

## Create Security Policies

# Email Policy

- |   |
|---|
| <ul style="list-style-type: none"><li>• Employees must use work email accounts to send, receive, or store any work-related information only.</li></ul>  |
| <ul style="list-style-type: none"><li>• Employees must not open email attachments or click on hyperlinks unless they are from a verified and trusted source.</li></ul>  |
| <ul style="list-style-type: none"><li>• All sensitive data (e.g., financial, personal, or client information) must be encrypted before being transmitted via email.</li></ul>   |
| <ul style="list-style-type: none"><li>• Employees must use complex passwords for accessing corporate email accounts and must not reuse passwords across multiple services.</li></ul>  |
| <ul style="list-style-type: none"><li>• Employees must promptly report any suspicious or phishing emails to the IT/security team using designated procedures (e.g., marking as phishing or forwarding to a security mailbox).</li></ul> |

# BYOD Policy

- |  |
|--|
| <ul style="list-style-type: none"><li>● All BYOD devices must be enrolled in the company-approved Mobile Device Management (MDM) system before accessing corporate resources.</li></ul>  |
| <ul style="list-style-type: none"><li>● Devices must be protected with biometric authentication (e.g., Face ID, fingerprint) or complex passwords. Auto-lock must be enabled with a timeout of no more than 5 minutes of inactivity.</li></ul>         |
| <ul style="list-style-type: none"><li>● <b>iOS/macOS:</b> FileVault and built-in encryption must be turned on.</li><li>● <b>Android:</b> Full-disk encryption must be enabled.</li><li>● <b>Windows 10/11:</b> BitLocker must be activated.</li></ul>  |
| <ul style="list-style-type: none"><li>● Only company-approved applications should be used for email, file sharing, messaging, and VPN access. A secure container or work profile must be used to separate corporate data from personal apps.</li></ul> |
| <ul style="list-style-type: none"><li>● Rooted Android devices or jailbroken iPhones are strictly prohibited from accessing corporate systems.</li></ul>   |
| <ul style="list-style-type: none"><li>● Employees must immediately report lost, stolen, or compromised devices to the IT Security Team. The company reserves the right to initiate a remote wipe of corporate data if needed.</li></ul>                |

# 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	Not 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	NA(Not Applicable)
USB ports are disabled or restricted to authorized devices only	Not Met
Network access controls are implemented, including VLAN segmentation and port security	NA(Not Applicable)
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

```
Windows PowerShell
PS C:\Users\d33> Get-LocalUser

Name           Enabled Description
-----
Administrator   False Built-in account for administering the computer/domain
d33             True
DefaultAccount  False A user account managed by the system.
Guest           False Built-in account for guest access to the computer/domain
WDAGUtilityAccount False A user account managed and used by the system for Windows Defender Application Guard scen...
```

```
Windows PowerShell
PS C:\Users\d33> Get-LocalUser

Name           Enabled Description
-----
Administrator   False Built-in account for administering the computer/domain
d33             True
DefaultAccount  False A user account managed by the system.
Guest           False Built-in account for guest access to the computer/domain
WDAGUtilityAccount False A user account managed and used by the system for Windows Defen

PS C:\Users\d33>
```

Command : Get-LocalUser

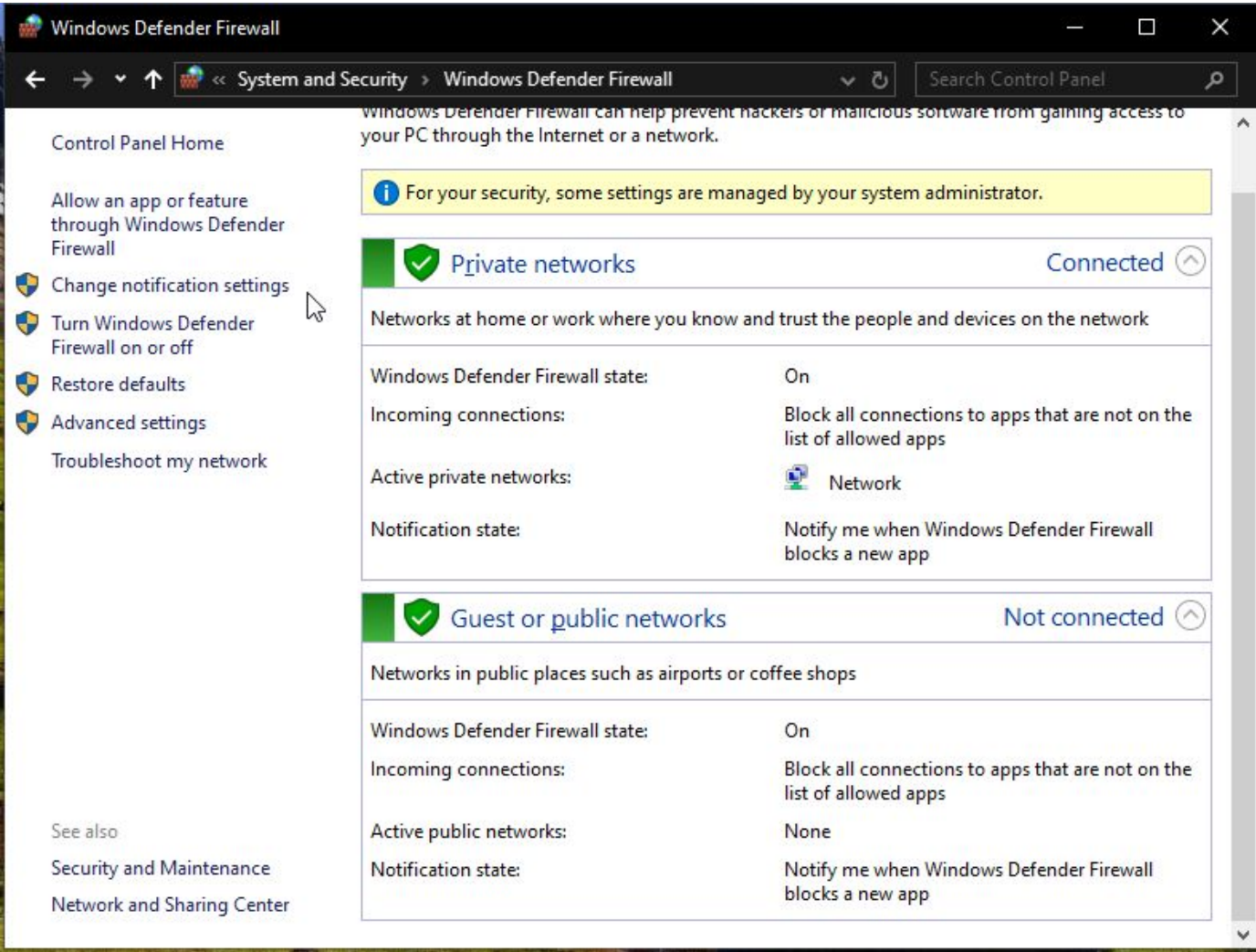
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

Met/Not Met

Windows Firewall is enabled

Met



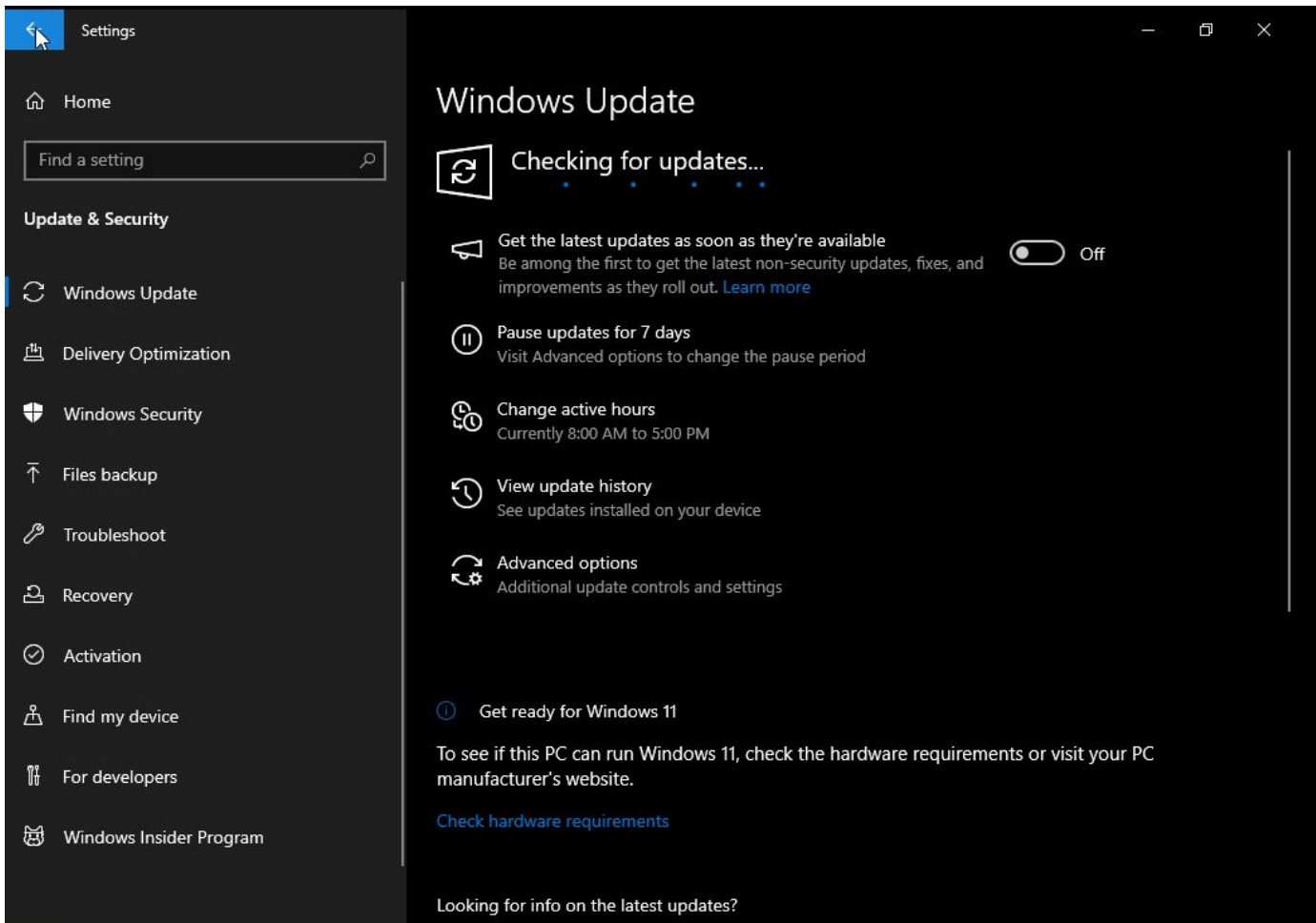
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

Met/Not Met

Automatic updates are enabled

Met



Updates will Automatically downloaded when connected to the internet and will be installed in the inactive hours or can also be installed manually.

# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

Met/Not Met

User Account Control (UAC) is enabled

Met

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

**Always notify me when:**

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

i

Recommended if you routinely install new software and visit unfamiliar websites.

OK

Cancel

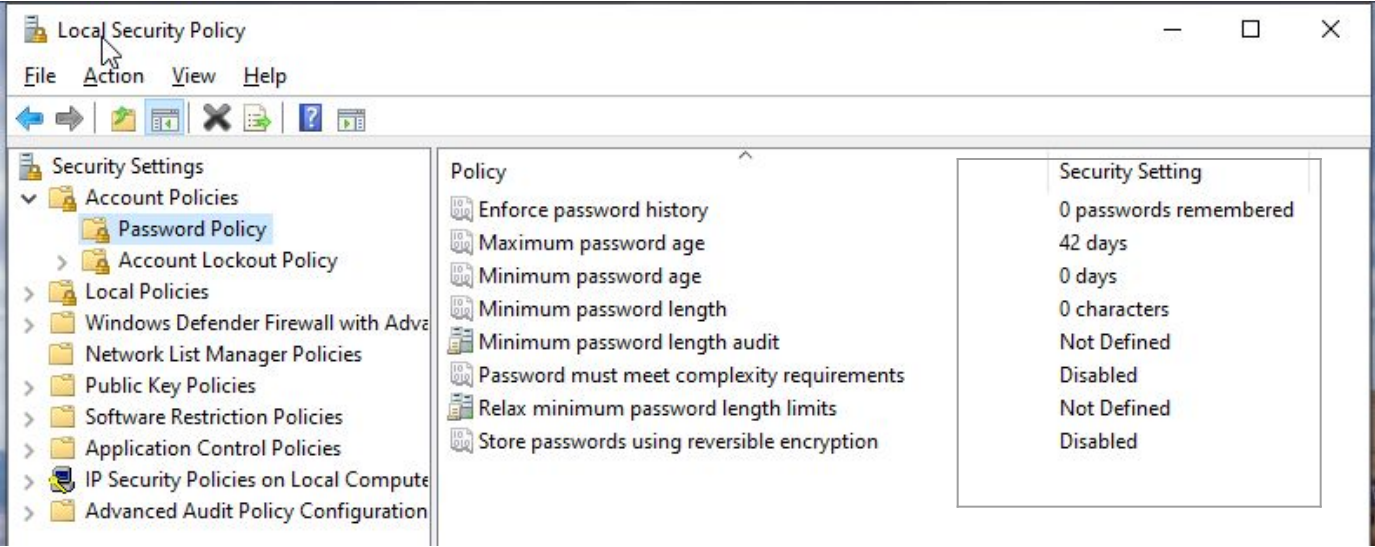
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

## Met/Not Met

Strong password policies are enforced

Not Met



# Windows Desktop Compliance

Windows 10 Regulatory Requirement

Met/Not Met

Guest account is disabled

Met

```
Windows PowerShell
PS C:\Users\d33> Get-LocalUser

Name           Enabled Description
-----
Administrator  False  Built-in account for administering the computer/domain
d33            True   A user account managed by the system.
DefaultAccount  False  Built-in account for guest access to the computer/domain
Guest          False  Built-in account for guest access to the computer/domain
WDAGUtilityAccount False  A user account managed and used by the system for Windows Defender Application Guard scen...
```

```
Windows PowerShell
PS C:\Users\d33> Get-LocalUser

Name           Enabled Description
-----
Administrator  False  Built-in account for administering the computer/domain
d33            True   A user account managed by the system.
DefaultAccount  False  Built-in account for guest access to the computer/domain
Guest          False  Built-in account for guest access to the computer/domain
WDAGUtilityAccount False  A user account managed and used by the system for Windows Defender Application Guard scen...

PS C:\Users\d33>
```

Command Get-LocalUser



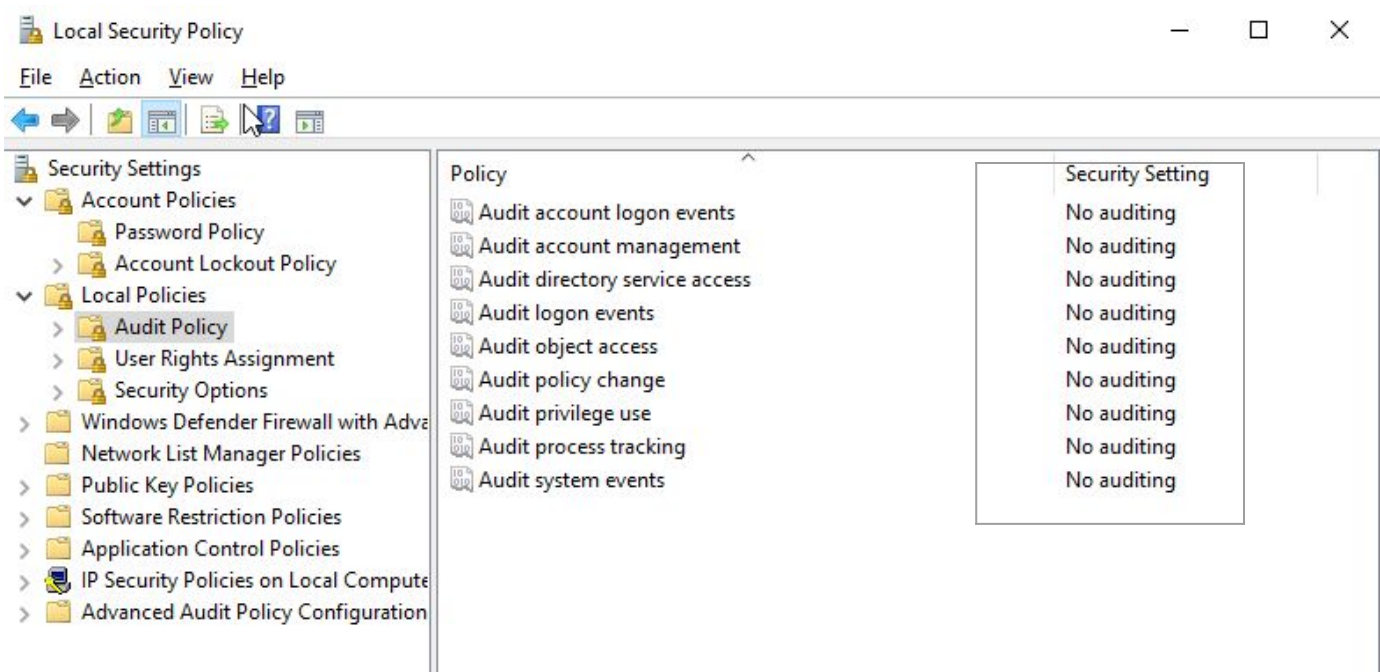
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

## Met/Not Met

System logging and auditing are enabled

Not Met





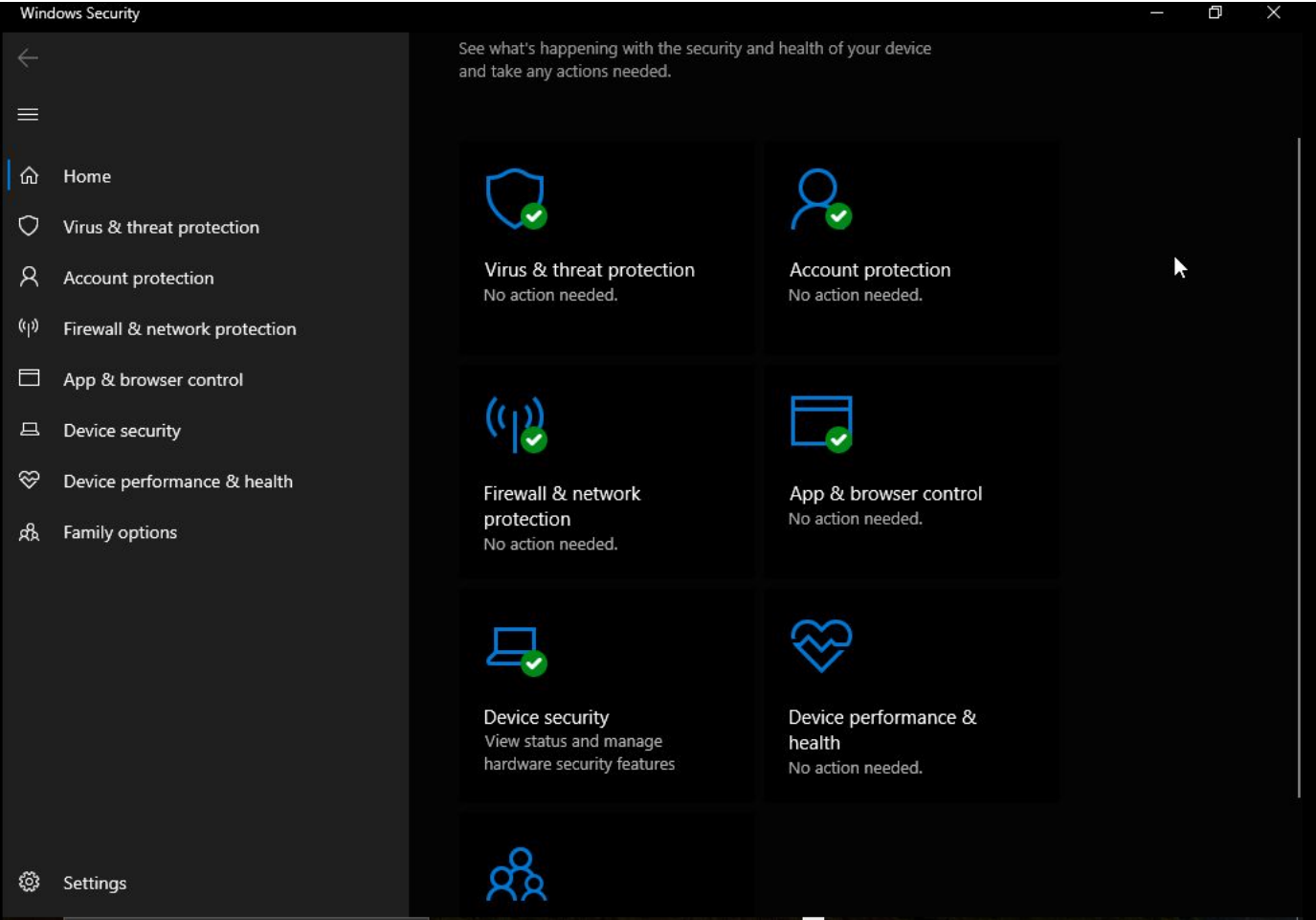
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

## Met/Not Met

Windows Defender Antivirus is enabled and up to date

Met



Updates For Windows Security Comes with the system updates therefore keeping the system up to date is recommended for the latest windows security

# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

Met/Not Met

Remote Desktop Services are configured securely

Met

```
PS C:\Users\d33> Get-ItemProperty -Path 'HKLM:\System\CurrentControl
Set\Control\Terminal Server' -Name fDenyTSConnections
fDenyTSConnections : 1
PSPath              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_M
achine\Software\Microsoft\Terminal Server
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_M
achine\Software\Microsoft\Terminal Server
PSChildName         : Terminal Server
PSDrive             : HKLM
PSProvider          : Microsoft.PowerShell.Core\Registry

PS C:\Users\d33>
```

### Command:

```
"Get-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\'
-Name fDenyTSConnections"
```

Determines RDP(remote desktop protocol) is blocked.

**RDP is disabled by default; if you enable it you must configure Network Level Authentication (NLA) and strong encryption.**

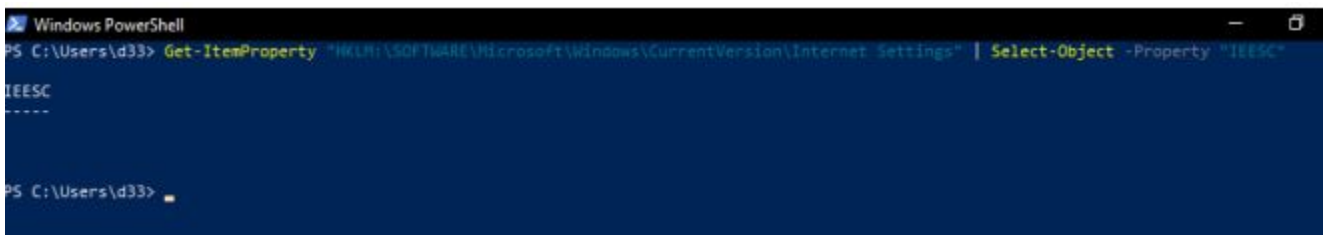
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

## Met/Not Met

Internet Explorer Enhanced Security Configuration (IE ESC) is enabled

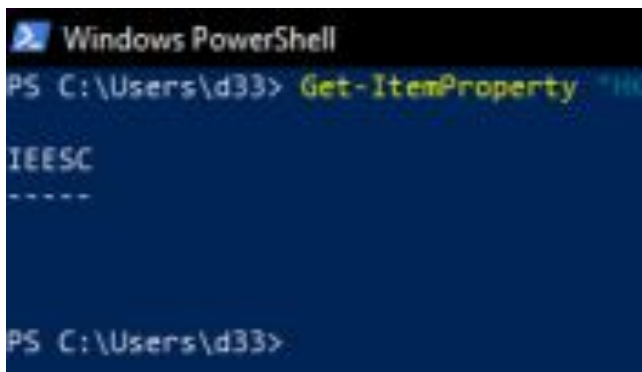
NA(Not Applicable)



```
Windows PowerShell
PS C:\Users\d33> Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings" | Select-Object -Property "IEESC"

IEESC
-----

PS C:\Users\d33>
```



```
Windows PowerShell
PS C:\Users\d33> Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings" | Select-Object -Property "IEESC"

IEESC
-----

PS C:\Users\d33>
```

No Objects are Shown confirming IE ESC is not present

**Command:** Get-ItemProperty  
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings" |  
Select-Object -Property "IEESC"

**NOTE:IE ESC is a feature of Windows Server, not Windows 10 client.**

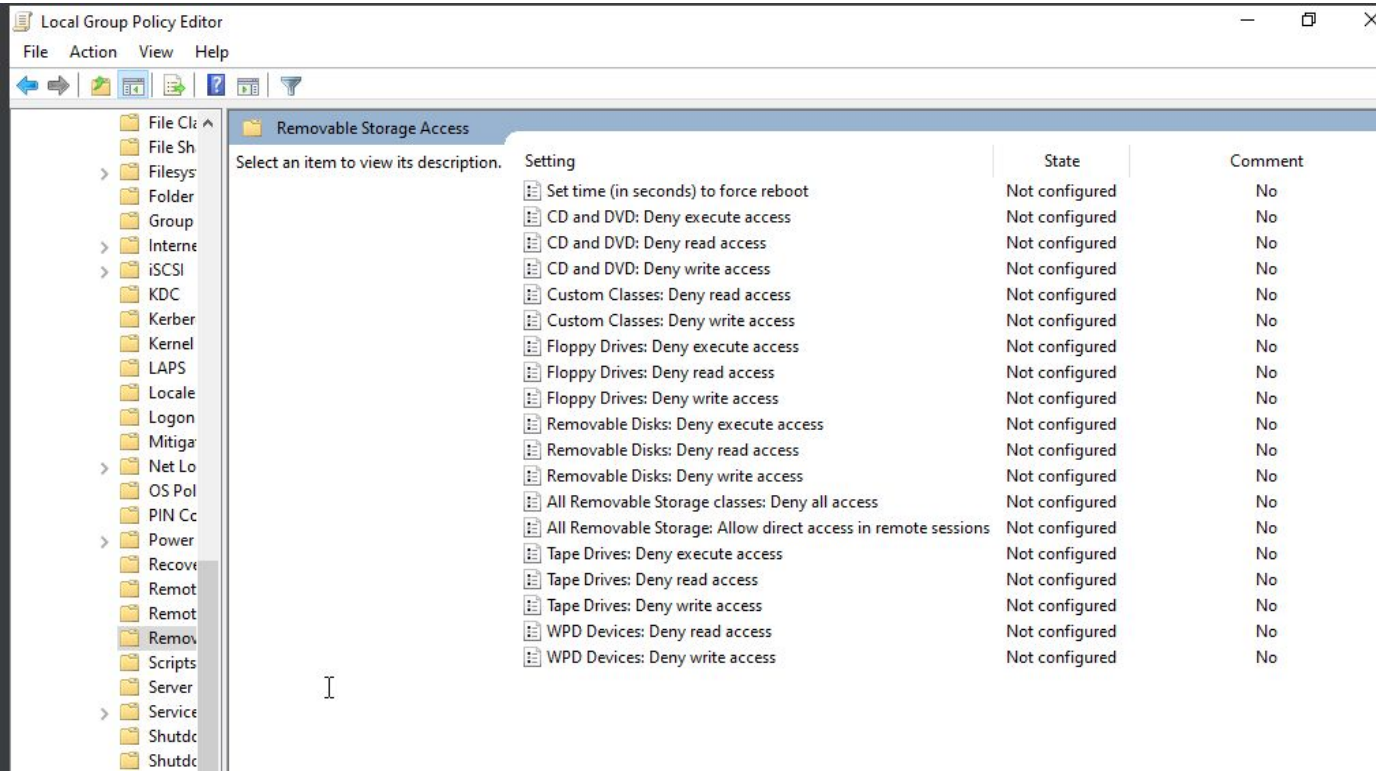
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

Met/Not Met

USB ports are disabled or restricted to authorized devices only

Not Met



# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

## Met/Not Met

Network access controls are implemented, including VLAN segmentation and port security

NA(Not Applicable)

```
PS C:\Users\d33> Get-NetAdapterAdvancedProperty
```

Name	DisplayName	DisplayValue	RegistryKeyword	RegistryValue
Ethernet	Flow Control	Rx & Tx Enabled	*FlowControl	{3}
Ethernet	Interrupt Moderation	Enabled	*InterruptMo...	{1}
Ethernet	IPv4 Checksum Offload	Rx & Tx Enabled	*IPChecksumO...	{3}
Ethernet	Jumbo Packet	Disabled	*JumboPacket	{1514}
Ethernet	Large Send Offload (IPv4)	Enabled	*LsoV1IPv4	{1}
Ethernet	Priority & VLAN	Priority & VLAN Enabled	*PriorityVLA...	{3}
Ethernet	Receive Buffers	256	*ReceiveBuffers	{256}
Ethernet	Link Speed & Duplex	Auto Negotiation	*SpeedDuplex	{0}
Ethernet	TCP Checksum Offload (IPv4)	Rx & Tx Enabled	*TCPChecksum...	{3}
Ethernet	Transmit Buffers	512	*TransmitBuf...	{512}
Ethernet	UDP Checksum Offload (IPv4)	Rx & Tx Enabled	*UDPChecksum...	{3}
Ethernet	Adaptive Inter-Frame Spacing	Enabled	AdaptiveIFS	{1}
Ethernet	Interrupt Moderation Rate	Adaptive	ITR	{65535}
Ethernet	Locally Administered Address	--	NetworkAddress	{--}
Ethernet	Number of Coalesce Buffers	128	NumCoalesceB...	{128}

Network access controls and port security Should be configured in the routers .

# Windows Desktop Compliance

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

```
PS C:\Users\d33> Get-Service RemoteRegistry

Status      Name            DisplayName
-----      -
Stopped     RemoteRegistry  Remote Registry
```

Command : Get-Service RemoteRegistry

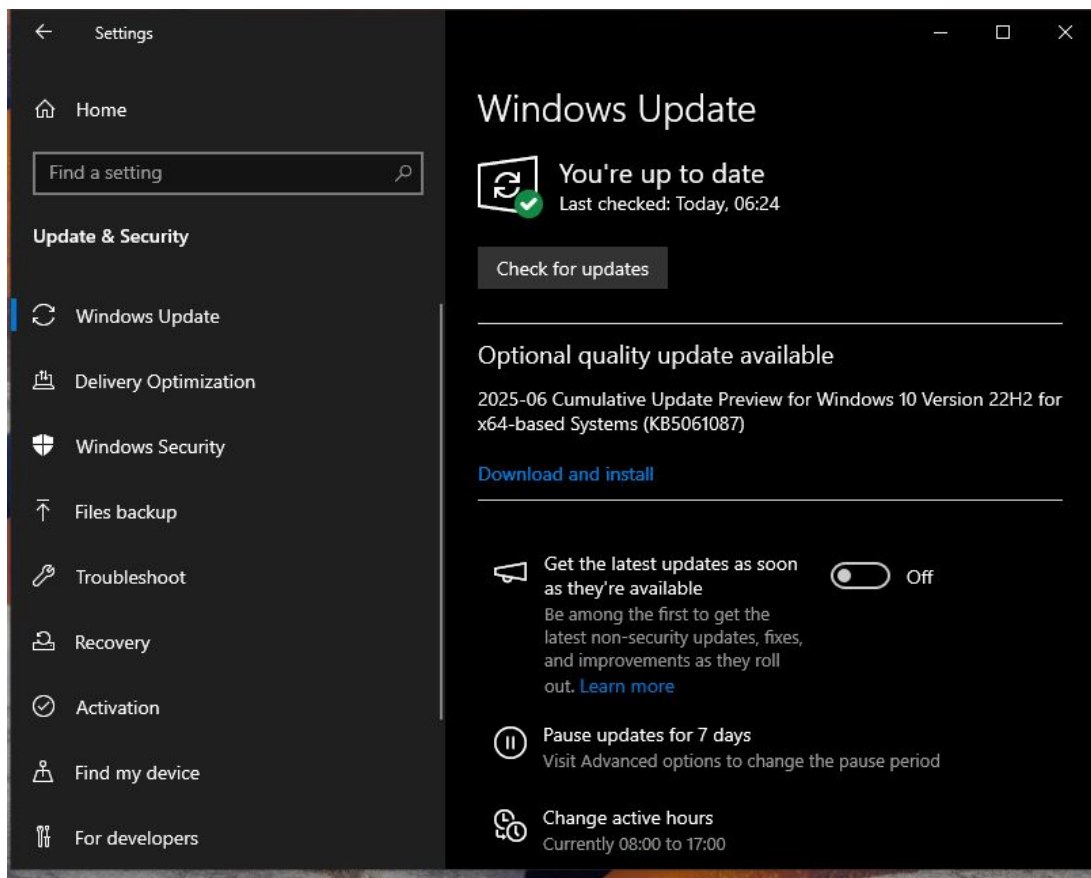
# Windows Desktop Compliance

## Windows 10 Regulatory Requirement

Met/Not Met

Windows Updates are configured to download and install updates automatically

Met



Updates Will Be Automatically Download as soon as they are released and Will Be Automatically Installed During Inactive hours.

# Windows Desktop Compliance

## Remediation

Strong password policies: Configure the system with Strong Password Policies

System logging and auditing : Enable and configure auditing

Ports Restriction: Disable Unnecessary ports (physical)

USB ports restricted to authorized devices only: Identify and allow device by hardware ID



# Linux Compliance

Linux CMMC Requirements	Met/Not Met
Current on security updates	Met
Ensure separate partition exists for /var	Not Met
Disable Automounting of drives	Not 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	Not 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	Not 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

Machine OS : Ubuntu 24..04.2 LTS (Nobel Numbet)

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Current on security updates

Met

```
d33@d33-VirtualBox: ~  
d33@d33-VirtualBox:~$ sudo apt update ; sudo apt upgrade  
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  
2 packages can be upgraded. Run 'apt list --upgradable' to see them.  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Calculating upgrade... Done  
The following upgrades have been deferred due to phasing:  
  libfprint-2-2 libfprint-2-tod1  
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

Command : `sudo apt update ; sudo apt upgrade`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure separate partition exists for /var

Not Met

```
d33@d33-VirtualBox:~$ grep -E '\s/var\s' /etc/fstab
d33@d33-VirtualBox:~$
```

```
d33@d33-VirtualBox:~$ ls /mnt
d33@d33-VirtualBox:~$
```

Command :

```
grep -E '\s/var\s' /etc/fstab
ls /mnt
```

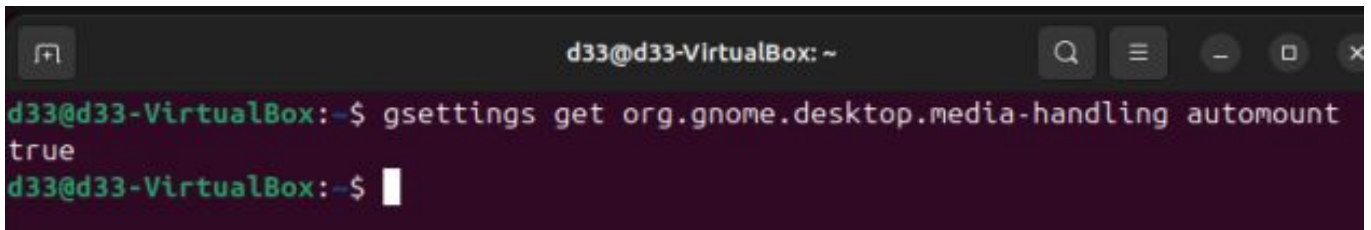
# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Disable Automounting of drives

Not Met



```
d33@d33-VirtualBox: ~  
d33@d33-VirtualBox:~$ gsettings get org.gnome.desktop.media-handling automount  
true  
d33@d33-VirtualBox:~$
```

Command :

`gsettings get org.gnome.desktop.media-handling automount`

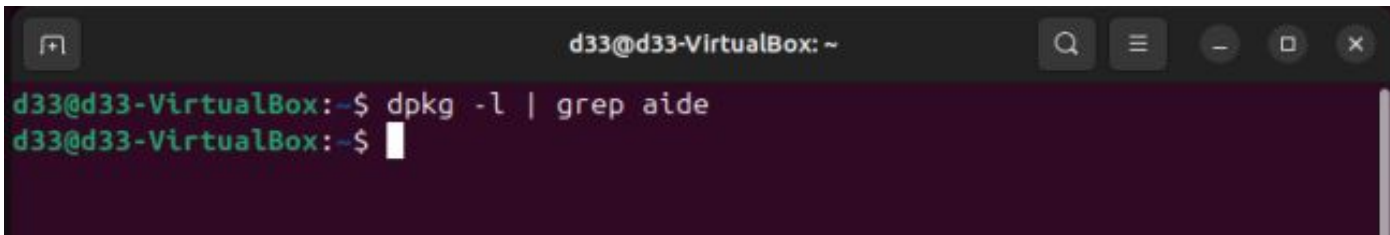
# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure AIDE is installed

Not Met

A terminal window titled 'd33@d33-VirtualBox: ~' with search, menu, and window control icons in the title bar. The terminal shows the command 'dpkg -l | grep aide' being entered and executed. The prompt is 'd33@d33-VirtualBox:~\$' and the output is empty, with a cursor on the next line.

```
d33@d33-VirtualBox:~$ dpkg -l | grep aide
d33@d33-VirtualBox:~$
```

Command : `dpkg -l | grep aide`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure daytime services are not enabled

Met

```
d33@d33-VirtualBox:~$ systemctl is-enabled daytime.socket
not-found
d33@d33-VirtualBox:~$
```

Command : `systemctl is-enabled daytime.socket`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure echo services are not enabled

Met

```
d33@d33-VirtualBox:~$ systemctl is-enabled echo-server
not-found
d33@d33-VirtualBox:~$
```

Command : systemctl is-enabled echo-server

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure tftp server is not enabled

Met

```
d33@d33-VirtualBox:~$ systemctl is-enabled tftpd.socket  
not-found  
d33@d33-VirtualBox:~$
```

Command : systemctl is-enabled tftpd.socket



# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure CUPS is not enabled

Not Met

```
d33@d33-VirtualBox:~$ systemctl is-enabled cups
enabled
d33@d33-VirtualBox:~$
```

Command : systemctl is-enabled cups

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure DHCP Server is not enabled

Met

```
ensured  
d33@d33-VirtualBox:~$ systemctl is-enabled isc-dhcp-server  
not-found  
d33@d33-VirtualBox:~$
```

Command : `systemctl is-enabled isc-dhcp-server`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure FTP Server is not enabled

Met

```
d33@d33-VirtualBox:~$ systemctl is-enabled vsftpd  
not-found  
d33@d33-VirtualBox:~$
```

Command : `systemctl is-enabled vsftpd`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure Samba is not enabled

Met

```
d33@d33-VirtualBox:~$ systemctl is-enabled smbd  
not-found  
d33@d33-VirtualBox:~$
```

Command : systemctl is-enabled smbd

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure TCP Wrappers is installed

Not Met

```
d33@d33-VirtualBox:~$ which /usr/sbin/tcpd
d33@d33-VirtualBox:~$
```

Command : `which /usr/sbin/tcpd`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure DCCP is disabled

Met

```
d33@d33-VirtualBox:~$ lsmod | grep dccp  
d33@d33-VirtualBox:~$
```

Command : `lsmod | grep dccp`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure iptables is installed

Met

```
d33@d33-VirtualBox:~$ dpkg -l | grep iptables
ii  iptables                1.8.10-3ubuntu2
    amd64                 administration tools for packet filtering and NAT
d33@d33-VirtualBox:~$
```

Command : `dpkg -l | grep iptables`

# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure audit log storage size is configured

Not Met

```
d33@d33-VirtualBox:~$ inspect /etc/audit/audit.conf
terminate called after throwing an instance of 'boost::filesystem::filesystem_error'
  what():  boost::filesystem::canonical: No such file or directory: "/etc/audit/audit.conf"
Aborted (core dumped)
d33@d33-VirtualBox:~$
```

Command : inspect /etc/audit/audit.conf



# Linux Compliance

## Linux Regulatory Requirement

## Met/Not Met

Ensure audit logs are not automatically deleted

Not Met

```
d33@d33-VirtualBox:~$ inspect /etc/audit/audit.conf
terminate called after throwing an instance of 'boost::filesystem::filesystem_error'
  what():  boost::filesystem::canonical: No such file or directory: "/etc/audit/audit.conf"
Aborted (core dumped)
d33@d33-VirtualBox:~$
```

Command : `inspect /etc/audit/audit.conf`

# Section 4:

## Cloud Management

# Windows Server Build Sheet

## 1. Operating System Version

Specify the exact OS build for consistency and patch management.  
*Example: Windows Server 2022 Datacenter, Build 20348.825*

## 2. Cloud Network Configuration

Define VPC/subnet, public IP allocation, and security group rules.  
*Example: Allow TCP 80/443 inbound, restrict RDP to specific IPs*

## 3. Web Server Role Installation

Ensure IIS or equivalent is installed and configured.  
*Example: Install-WindowsFeature -Name Web-Server -IncludeManagementTools*

## 4. Patch Management Setup

Enable automatic updates or integrate with WSUS/Azure Update Management.  
*Example: Windows Update for Business with 7-day deferral*

## 5. Firewall Configuration

Apply local Windows Firewall rules in addition to cloud-based controls.  
*Example: Allow only inbound HTTP/HTTPS, block FTP*

# Windows Server Build Sheet

## 6. Administrator Account Hardening

Rename default admin account and enforce password complexity.  
*Example: Rename "Administrator" to "ServerAdmin2025"*

## 7. Antivirus and Endpoint Protection

Install and configure antivirus (e.g., Microsoft Defender for Endpoint).  
*Example: Enable Defender Real-time Protection & Cloud-delivered Protection*

## 8.Web Content and Root Folder Setup

Define location and structure for hosting web content.  
*Example: Root content at `C:\inetpub\wwwroot\FedFirstPortal`*

## 9.Logging and Monitoring Integration

Connect server to central logging and monitoring tools.  
*Example: Enable Windows Event Forwarding and Azure Monitor agent*

## 10. [Build Sheet Item]

Implement regular backup of critical data and configurations.  
*Example: Daily snapshot with 7-day retention using Azure Backup*

# Enhancing Cloud Security with CASB

- **Visibility into Cloud Usage**

- CASBs provide deep visibility into all sanctioned and unsanctioned (shadow IT) cloud services used across the organization.
- By identifying unauthorized applications or risky user behavior, the company can eliminate blind spots, enforce approved tools, and reduce potential data leakage points.

- **Data Loss Prevention (DLP) Enforcement**

- CASBs enforce DLP policies to monitor, classify, and prevent sensitive data from being shared inappropriately across cloud platforms.
- Protects confidential company data (e.g., engineering plans, financial records) from accidental or malicious exposure, helping to maintain compliance with regulations like GDPR and HIPAA.

- **Threat Protection**

- CASBs use advanced threat detection techniques such as anomaly detection and behavior analytics to identify malware, compromised accounts, or suspicious activity.
- Improves early detection of insider threats and external attacks, enabling rapid response before damage occurs within critical cloud-hosted services.

# Enhancing Cloud Security with CASB

- **Access Control and Policy Enforcement**
  - CASBs allow granular control over who can access what data, under what conditions (e.g., location, device type, role).
  - Ensures only authorized users and devices access cloud resources, reducing the risk of unauthorized access from stolen credentials or unsecured endpoints.
- **Compliance Monitoring and Reporting**
  - CASBs offer continuous monitoring and automated reporting to help meet regulatory and internal compliance requirements.
  - Simplifies audits and proves adherence to industry standards (ISO 27001, PCI-DSS, etc.), minimizing legal and reputational risks.