

Information Assurance Audit Report

Author: Norman Shatto

Date: 10/24/2025

System: Windows 11 Enterprise Lab

Framework: NIST 800-53

Introduction:

This report summarizes the findings from a security control audit performed on the Windows 11 Enterprise evaluation environment. The goal of this assessment was to verify that key information assurance controls are functioning as intended, aligned with NIST 800-53 and CIS Critical Security Controls. Evidence was collected through direct observation, system commands, and screenshots.

Scope:

The scope of this audit includes selected NIST 800-53 controls related to user account management, password policies, firewall configuration, patch management, event logging, and configuration management. The assessment focuses on verifying whether each control is implemented, operational, and documented appropriately.

Methodology:

Each control was reviewed using Windows built-in administrative tools such as PowerShell, Command Prompt, Event Viewer, Local Security Policy (where available), and Windows Update settings. Screenshots were captured as evidence of compliance or non-compliance. Each control was assigned a compliance status (Pass/Fail) and a corresponding recommendation.

Controls Tested:

Control	Description	Result	Evidence	Recommendation
AC-2	Account Management	Pass	Screenshot of local user	Review accounts quarterly
IA-5	Password Policy	Pass	Screenshot of net accounts	Increase minimum length to 12 characters
AC-7	Account Lockout	Fail	Screenshot of lockout threshold	Enable lockout after 5 failed attempts
SC-7	Firewall Configuration	Pass	Screenshot of firewall settings	Maintain firewall enabled on all profiles
AU-2	Audit Logging	Pass	Screenshot of event viewer	Review logs monthly for anomalies
SI-2	Patch Management	Pass	Screenshot of Windows update	Auto-updates enabled
CM-2	Baseline Configuration	Pass	Screenshot of system info results	Review baseline after major updates
AC-11	Session Timeout	Pass	Screenshot of power settings	Ensure screen locks after 15 minutes idle time

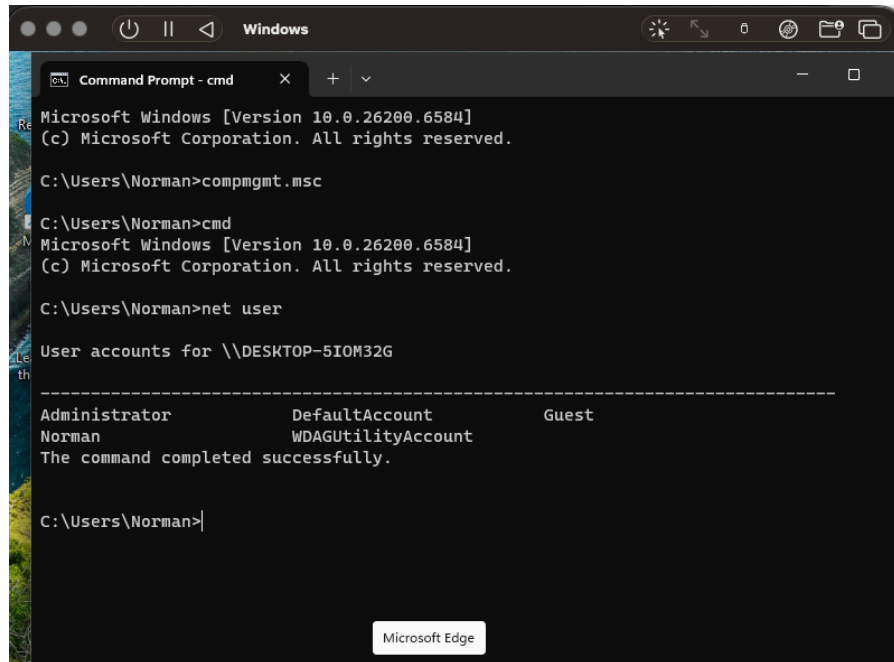
Results:

Overall, the Windows Enterprise system meets most tested security controls. The environment demonstrates compliance in areas such as password management, firewall configuration, and event logging. One area for improvement is enforcing an account lockout policy to mitigate brute-force attack risks. Documentation and continuous monitoring are recommended to maintain compliance and operational security.

Evidence Appendix:

The following screenshots were collected during the audit. Each corresponds to the control ID listed in the “Controls Tested” section.

1. AC-2 Account Management



A screenshot of a Windows Command Prompt window. The window title is "Command Prompt - cmd". The prompt shows the user is logged in as "Norman" on a Windows 10 system (version 10.0.26200.6584). The user has executed the command `compmgmt.msc`, which opens the Local Security Policy console. The user then executes `net user`, which displays the user accounts for the local machine `\\DESKTOP-5IOM32G`. The output shows three accounts: Administrator, DefaultAccount, and Guest. The command completed successfully.

```
Microsoft Windows [Version 10.0.26200.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Norman>compmgmt.msc

C:\Users\Norman>cmd
Microsoft Windows [Version 10.0.26200.6584]
(c) Microsoft Corporation. All rights reserved.

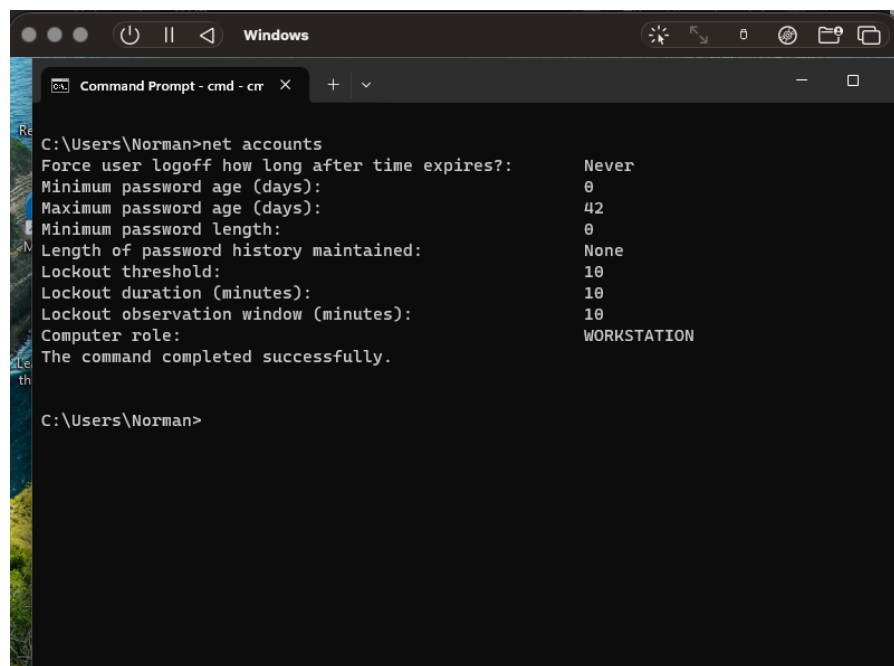
C:\Users\Norman>net user

User accounts for \\DESKTOP-5IOM32G

-----
Administrator      DefaultAccount      Guest
Norman              WDAGUtilityAccount
The command completed successfully.

C:\Users\Norman>
```

2. IA-5 Password Policy

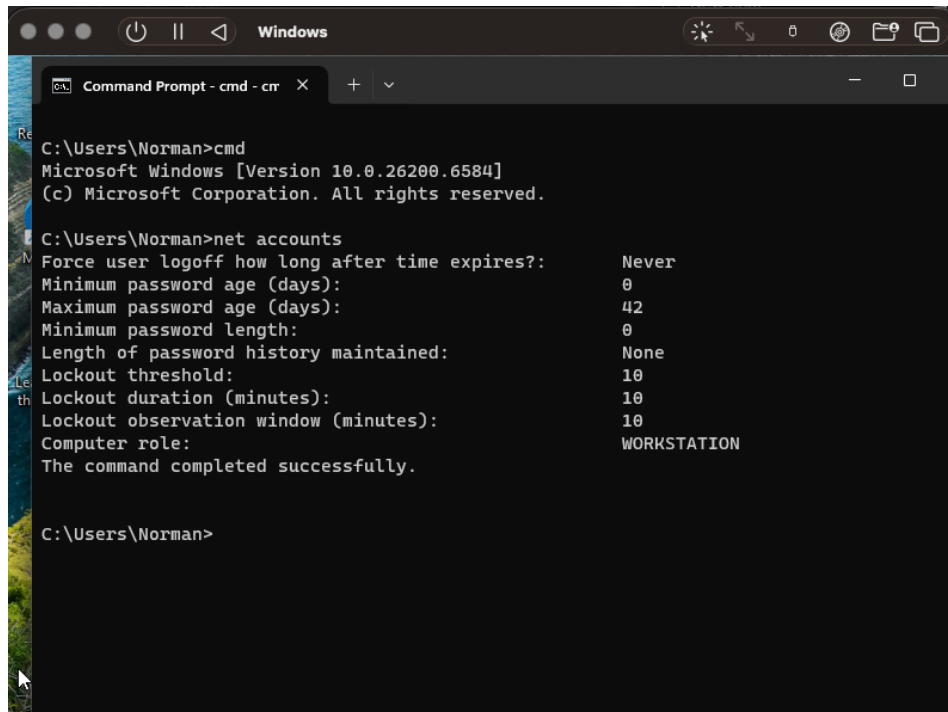


A screenshot of a Windows Command Prompt window. The window title is "Command Prompt - cmd - crr". The prompt shows the user is logged in as "Norman" on a Windows 10 system (version 10.0.26200.6584). The user has executed the command `net accounts`, which displays the current password policy settings for the local machine `\\DESKTOP-5IOM32G`. The output shows the following settings: 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), and Computer role (WORKSTATION). The command completed successfully.

```
C:\Users\Norman>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:\Users\Norman>
```

3. AC-7 Lockout Policy

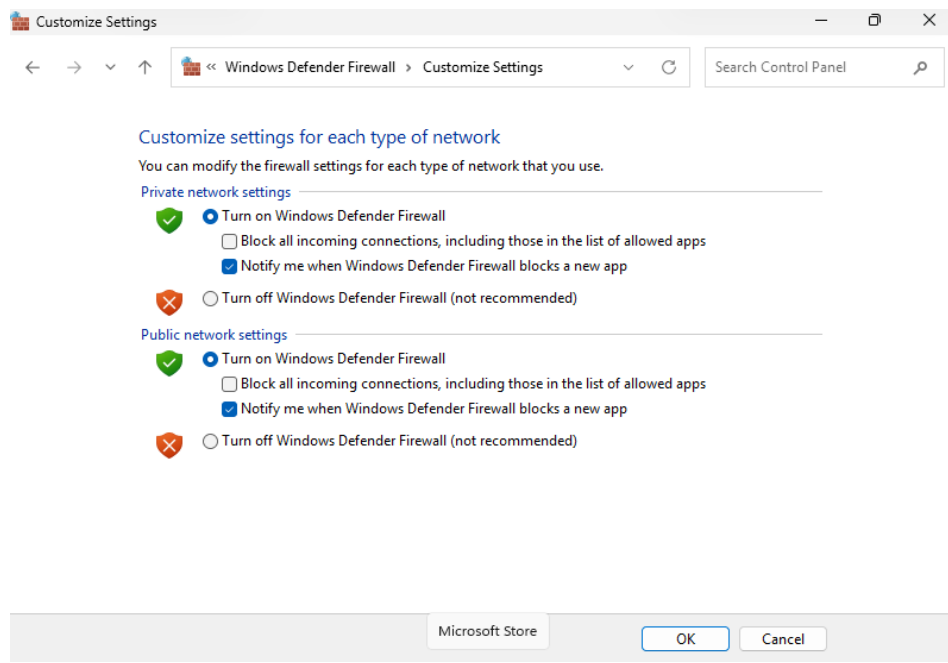


```
C:\Users\Norman>cmd
Microsoft Windows [Version 10.0.26200.6584]
(c) Microsoft Corporation. All rights reserved.

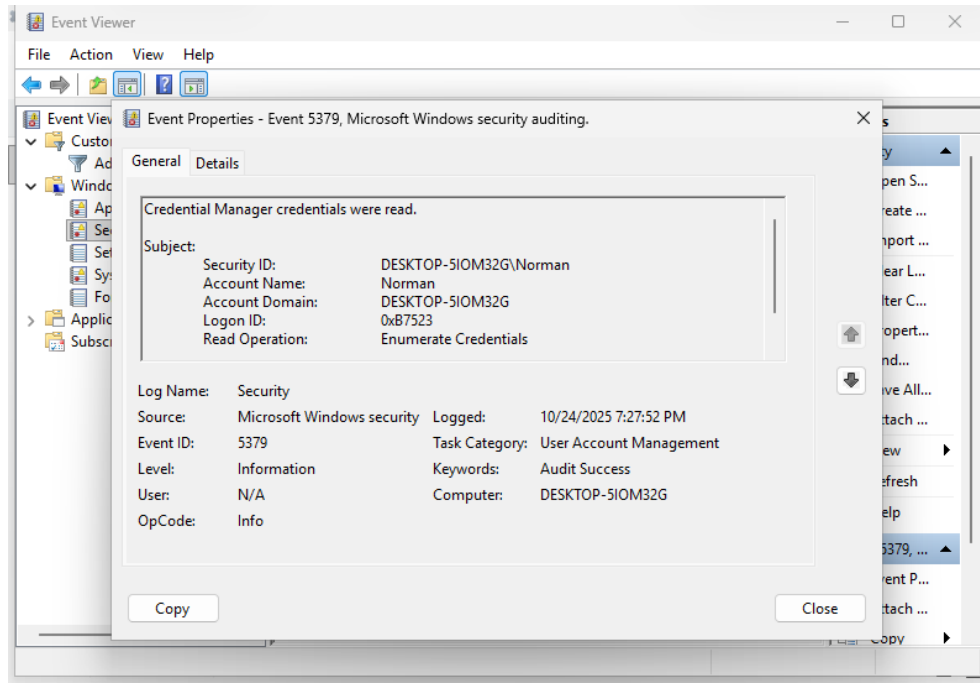
C:\Users\Norman>net accounts
Force user logoff how long after time expires?:      Never
Minimum password age (days):                        0
Maximum password age (days):                       42
Minimum password length:                            0
Length of password history maintained:            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

C:\Users\Norman>
```

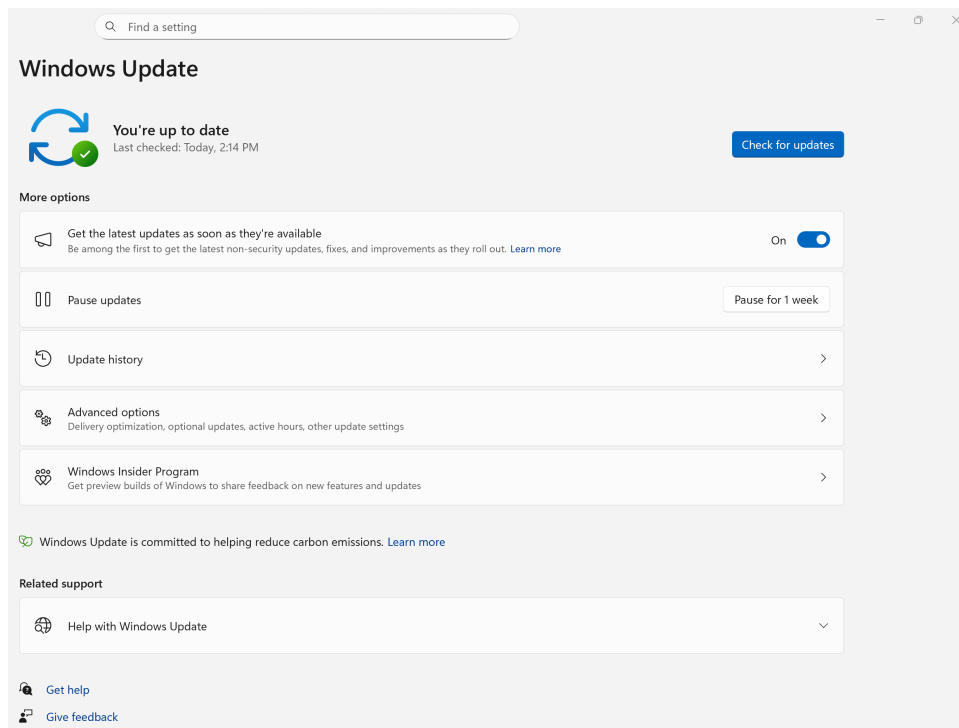
4. SC-7 Firewall



5. AU-2 Audit Logging



6. SI-2 Patch Management



7. CM-2 Configuration

```
Command Prompt
Microsoft Windows [Version 10.0.26200.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Norman>systeminfo

Host Name:                DESKTOP-5IOM32G
OS Name:                  Microsoft Windows 11 Home
OS Version:               10.0.26200 N/A Build 26200
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         Norman
Registered Organization:   N/A
Product ID:                00326-10000-00000-AA239
Original Install Date:     10/24/2025, 6:09:29 PM
System Boot Time:          10/24/2025, 9:58:02 PM
System Manufacturer:       QEMU
System Model:              QEMU Virtual Machine
System Type:               ARM64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: ARMv8 (64-bit) Family 8 Model 0 Revision 0 QEM
U ~1000 Mhz
BIOS Version:              EFI Development Kit II / OVMF 0.0.0, 2/6/2015
Windows Directory:         C:\WINDOWS
System Directory:           C:\WINDOWS\system32
Boot Device:                \Device\HarddiskVolume1

Boot Device:                \Device\HarddiskVolume1
System Locale:               en-us;English (United States)
Input Locale:               en-us;English (United States)
Time Zone:                  (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:      4,087 MB
Available Physical Memory:  2,084 MB
Virtual Memory: Max Size:   5,495 MB
Virtual Memory: Available:  3,905 MB
Virtual Memory: In Use:     1,590 MB
Page File Location(s):      C:\pagefile.sys
Domain:                     WORKGROUP
Logon Server:                \\DESKTOP-5IOM32G
Hotfix(s):                   4 Hotfix(s) Installed.
                           [01]: KB5066613
                           [02]: KB5054156
                           [03]: KB5065426
                           [04]: KB5064531
Network Card(s):            N/A
Virtualization-based security: Status: Not enabled
                             App Control for Business policy: Enforced
                             App Control for Business user mode policy: Audit
                             Security Features Enabled:
Hyper-V Requirements:       A hypervisor has been detected. Features required for
Hyper-V will not be displayed.

C:\Users\Norman>
```

8. AC-11 Session Timeout

