

# SentinelX System Hardening Report

Operating System: windows  
Hardening Level: strict  
Operation: scan  
Timestamp: 2025-12-10T17:18:30+05:30

## System Information

Edition: Windows 11 Home Single Language  
Version: 25H2  
Installed on: 11-11-2025  
OS Build: 26200.7309  
Architecture: amd64  
Computer Name: DESKTOP-H1VKPHE  
Domain: WORKGROUP  
Manufacturer: HP  
Model: OMEN by HP Gaming Laptop 16-xd0xxx  
Processor: AMD Ryzen 7 7840HS w/ Radeon 780M Graphics  
Ram Memory: 15.29 GB

## Summary

Total Checks: 75  
Passed: 29  
Failed: 46  
Warnings: 0

**Compliance: 38.67%**

## Detailed Results

### Category: Account Policies / Password Policy

Check ID: WIN\_001  
Description: Enforce password history is set to 24 or more passwords  
**Status: failed**  
Current Value: 2 passwords  
Expected Value: 24 or more  
Remediation: net accounts /uniquepw:24

---

### Category: Account Policies / Password Policy

Check ID: WIN\_002  
Description: Maximum password age is set to 60 or fewer days, but not 0  
**Status: failed**  
Current Value: Not set (0)  
Expected Value: 30 days (but not 0)  
Remediation: net accounts /maxpwage:30

---

### Category: Account Policies / Password Policy

Check ID: WIN\_003  
Description: Minimum password age is set to 1 or more day(s)  
**Status: failed**  
Current Value: 0 days  
Expected Value: 3 day(s)  
Remediation: net accounts /minpwage:3

---

**Category: Account Policies / Password Policy**

Check ID: WIN\_004

Description: Minimum password length is set to 14 or more character(s)

**Status: failed**

Current Value: 0 (not set)

Expected Value: 20 or more character(s)

Remediation: net accounts /minpwlen:20

---

**Category: Account Policies / Password Policy**

Check ID: WIN\_005

Description: Password must meet complexity requirements is set to Enabled

**Status: failed**

Current Value: Not configured

Expected Value: true (Enabled)

Remediation: secedit /configure /db %windir%\security\database\secedit.sdb /cfg %windir%\security\templates\hisecws.inf /areas SECURITYPOLICY

---

**Category: Account Policies / Password Policy**

Check ID: WIN\_006

Description: Store passwords using reversible encryption is set to Disabled

**Status: passed**

Current Value: Not configured

Expected Value: Disabled

Remediation: reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v ClearTextPassword /t REG\_DWORD /d 0 /f

---

**Category: Account Policies / Account Lockout Policy**

Check ID: WIN\_007

Description: Account lockout duration is set to 15 or more minute(s)

**Status: failed**

Current Value: 10 minutes

Expected Value: 60 or more minute(s)

Remediation: net accounts /lockoutduration:60

---

**Category: Account Policies / Account Lockout Policy**

Check ID: WIN\_008

Description: Account lockout threshold is set to 5 or fewer invalid logon attempt(s), but not 0

**Status: failed**

Current Value: 10 attempts

Expected Value: 3 or fewer (but not 0)

Remediation: net accounts /lockoutthreshold:3

---

**Category: Account Policies / Account Lockout Policy**

Check ID: WIN\_009

Description: Reset account lockout counter after is set to 15 or more minute(s)

**Status: failed**

Current Value: 10 minutes

Expected Value: 60 or more minute(s)

Remediation: net accounts /lockoutwindow:60

---

**Category: User Rights Assignment**

Check ID: WIN\_010

Description: Access Credential Manager as a trusted caller is set to No One

**Status: failed**

Current Value: Not configured

Expected Value: S-1-0-0

Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

**Category: User Rights Assignment**

Check ID: WIN\_011

Description: Access this computer from the network is set to Administrators, Authenticated Users

**Status: failed**

Current Value: Not configured  
Expected Value: S-1-5-32-544  
Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

#### Category: User Rights Assignment

Check ID: WIN\_012  
Description: Act as part of the operating system is set to No One  
**Status: failed**  
Current Value: Not configured  
Expected Value: S-1-0-0  
Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

#### Category: User Rights Assignment

Check ID: WIN\_013  
Description: Allow log on locally is set to Administrators, Users  
**Status: failed**  
Current Value: Not configured  
Expected Value: S-1-5-32-544  
Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

#### Category: User Rights Assignment

Check ID: WIN\_014  
Description: Allow log on through Remote Desktop Services is set to Administrators  
**Status: failed**  
Current Value: Not configured  
Expected Value: S-1-5-32-544  
Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

#### Category: User Rights Assignment

Check ID: WIN\_015  
Description: Back up files and directories is set to Administrators  
**Status: failed**  
Current Value: Not configured  
Expected Value: S-1-5-32-544  
Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

#### Category: User Rights Assignment

Check ID: WIN\_016  
Description: Change the system time is set to Administrators, LOCAL SERVICE  
**Status: failed**  
Current Value: Not configured  
Expected Value: S-1-5-32-544  
Remediation: secedit /configure /db secedit.sdb /cfg policy.cfg /areas USER\_RIGHTS

---

#### Category: Security Options / Accounts

Check ID: WIN\_017  
Description: Accounts: Block Microsoft accounts is set to Users cannot add or log on with Microsoft accounts  
**Status: failed**  
Current Value: Not Set  
Expected Value: 3  
Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v NoConnectedUser /t REG\_DWORD /d 3 /f

---

#### Category: Security Options / Accounts

Check ID: WIN\_018  
Description: Accounts: Guest account status is set to Disabled  
**Status: passed**  
Current Value: Disabled  
Expected Value: Disabled  
Remediation: net user Guest /active:no

---

### Category: Security Options / Accounts

Check ID: WIN\_019

Description: Accounts: Limit local account use of blank passwords to console logon only is set to Enabled

Status: passed

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v LimitBlankPasswordUse /t REG\_DWORD /d 1 /f

---

### Category: Security Options / Accounts

Check ID: WIN\_020

Description: Accounts: Rename administrator account is configured

Status: passed

Current Value: Renamed

Expected Value: Not 'Administrator' (e.g., Administrator)

Remediation: Rename via Local Security Policy or Group Policy

---

### Category: Security Options / Accounts

Check ID: WIN\_021

Description: Accounts: Rename guest account is configured

Status: passed

Current Value: Renamed

Expected Value: Not 'Guest' (e.g., Guest)

Remediation: Rename via Local Security Policy or Group Policy

---

### Category: Security Options / Interactive Logon

Check ID: WIN\_022

Description: Interactive logon: Don't display last signed-in is set to Enabled

Status: failed

Current Value: Disabled

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v DontDisplayLastUserName /t REG\_DWORD /d 1 /f

---

### Category: Security Options / Interactive Logon

Check ID: WIN\_023

Description: Interactive logon: Require Domain Controller authentication to unlock workstation is set to Enabled

Status: failed

Current Value: Not Set

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v RequireDomainControllerAuthentication /t REG\_DWORD /d 1 /f

---

### Category: Security Options / Interactive Logon

Check ID: WIN\_024

Description: Interactive logon: Smart card removal behavior is set to Lock Workstation or Force logoff

Status: failed

Current Value: Not Set

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ScRemoveOption /t REG\_DWORD /d 1 /f

---

### Category: Security Options / Network Access

Check ID: WIN\_025

Description: Network access: Allow anonymous SID/Name translation is set to Disabled

Status: failed

Current Value: Not Set

Expected Value: Disabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v LSAAnonymousNameLookup /t REG\_DWORD /d 0 /f

---

### Category: Security Options / Network Access

Check ID: WIN\_026

Description: Network access: Do not allow anonymous enumeration of SAM accounts is set to Enabled

Status: passed

Current Value: Enabled  
Expected Value: Enabled  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v RestrictAnonymousSAM /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Network Access

Check ID: WIN\_027  
Description: Network access: Do not allow anonymous enumeration of SAM accounts and shares is set to Enabled  
**Status: failed**  
Current Value: Disabled  
Expected Value: Enabled  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v RestrictAnonymous /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Network Access

Check ID: WIN\_028  
Description: Network access: Restrict anonymous access to Named Pipes and Shares is set to Enabled  
**Status: failed**  
Current Value: Disabled  
Expected Value: Enabled  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v RestrictAnonymous /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Network Access

Check ID: WIN\_029  
Description: Network access: Restrict clients allowed to make remote calls to SAM is configured  
**Status: failed**  
Current Value: Not Set  
Expected Value: O:BAG:BAD:(A;;RC;;;BA)  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v RestrictRemoteSAM /t REG\_DWORD /d O:BAG:BAD:(A;;RC;;;BA) /f

---

#### Category: Security Options / Network Security

Check ID: WIN\_030  
Description: Network security: Allow Local System to use computer identity for NTLM is set to Enabled  
**Status: failed**  
Current Value: Not Set  
Expected Value: Enabled  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v UseMachineId /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Network Security

Check ID: WIN\_031  
Description: Network security: Allow PKU2U authentication requests to this computer to use online identities is set to Disabled  
**Status: failed**  
Current Value: Not Set  
Expected Value: Disabled  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\pku2u" /v AllowOnlineID /t REG\_DWORD /d 0 /f

---

#### Category: Security Options / Network Security

Check ID: WIN\_032  
Description: Network security: Configure encryption types allowed for Kerberos is configured  
**Status: failed**  
Current Value: Not Set  
Expected Value: 2147483640  
Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" /v SupportedEncryptionTypes /d 2147483640 /f

---

#### Category: Security Options / Network Security

Check ID: WIN\_033  
Description: Network security: Do not store LAN Manager hash value on next password change is set to Enabled  
**Status: passed**  
Current Value: Enabled  
Expected Value: Enabled  
Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v NoLMHash /t REG\_DWORD /d 1 /f

---

**Category: Security Options / Network Security**

Check ID: WIN\_034

Description: Network security: LAN Manager authentication level is set to Send NTLMv2 response only. Refuse LM & NTLM

**Status: failed**

Current Value: Not Set

Expected Value: 5

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v LmCompatibilityLevel /t REG\_DWORD /d 5 /f

---

**Category: Security Options / Network Security**

Check ID: WIN\_035

Description: Network security: Minimum session security for NTLM SSP based clients is configured

**Status: failed**

Current Value: 536870912

Expected Value: 537395200

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0" /v NtlmMinClientSec /t REG\_DWORD /d 537395200 /f

---

**Category: User Account Control**

Check ID: WIN\_036

Description: User Account Control: Admin Approval Mode for the Built-in Administrator account is set to Enabled

**Status: failed**

Current Value: Not Set

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v FilterAdministratorToken /t REG\_DWORD /d 1 /f

---

**Category: User Account Control**

Check ID: WIN\_037

Description: User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop is set to Disabled

**Status: passed**

Current Value: Disabled

Expected Value: Disabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableUIADesktopToggle /t REG\_DWORD /d 0 /f

---

**Category: User Account Control**

Check ID: WIN\_038

Description: User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode is set to Prompt for consent on

**Status: failed**

Current Value: 5

Expected Value: 2

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin /t REG\_DWORD /d 2 /f

---

**Category: User Account Control**

Check ID: WIN\_039

Description: User Account Control: Behavior of the elevation prompt for standard users is set to Automatically deny elevation requests

**Status: failed**

Current Value: 3

Expected Value: Disabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorUser /t REG\_DWORD /d 0 /f

---

**Category: User Account Control**

Check ID: WIN\_040

Description: User Account Control: Detect application installations and prompt for elevation is set to Enabled

**Status: passed**

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableInstallerDetection /t REG\_DWORD /d 1 /f

---

**Category: User Account Control**

Check ID: WIN\_041

Description: User Account Control: Only elevate UIAccess applications that are installed in secure locations is set to Enabled

**Status: passed**

Current Value: Enabled  
Expected Value: Enabled  
Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableSecureUIAPaths /t REG\_DWORD /d 1 /f

---

#### Category: User Account Control

Check ID: WIN\_042

Description: User Account Control: Run all administrators in Admin Approval Mode is set to Enabled

**Status: passed**

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG\_DWORD /d 1 /f

---

#### Category: User Account Control

Check ID: WIN\_043

Description: User Account Control: Switch to the secure desktop when prompting for elevation is set to Enabled

**Status: passed**

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v PromptOnSecureDesktop /t REG\_DWORD /d 1 /f

---

#### Category: User Account Control

Check ID: WIN\_044

Description: User Account Control: Virtualize file and registry write failures to per-user locations is set to Enabled

**Status: passed**

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableVirtualization /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Microsoft Network Client

Check ID: WIN\_045

Description: Microsoft network client: Digitally sign communications (always) is set to Enabled

**Status: failed**

Current Value: Not Set

Expected Value: Enabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" /v RequireSecuritySignature /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Microsoft Network Client

Check ID: WIN\_046

Description: Microsoft network client: Digitally sign communications (if server agrees) is set to Enabled

**Status: passed**

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" /v EnableSecuritySignature /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Microsoft Network Server

Check ID: WIN\_047

Description: Microsoft network server: Digitally sign communications (always) is set to Enabled

**Status: failed**

Current Value: Not Set

Expected Value: Enabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v RequireSecuritySignature /t REG\_DWORD /d 1 /f

---

#### Category: Security Options / Microsoft Network Server

Check ID: WIN\_048

Description: Microsoft network server: Digitally sign communications (if client agrees) is set to Enabled

**Status: failed**

Current Value: Disabled

Expected Value: Enabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v EnableSecuritySignature /t REG\_DWORD /d 1 /f

---

### Category: Security Options / Microsoft Network Server

Check ID: WIN\_049

Description: Microsoft network server: Disconnect clients when logon hours expire is set to Enabled

**Status: passed**

Current Value: Enabled

Expected Value: Enabled

Remediation: reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v EnableForcedLogoff /t REG\_DWORD /d 1

---

### Category: Security Options / System

Check ID: WIN\_050

Description: Turn off Autoplay is set to Enabled: All drives

**Status: failed**

Current Value: Not Set

Expected Value: 255

Remediation: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoDriveTypeAutoRun /t REG\_DWORD /d

---

### Category: Audit Policies

Check ID: WIN\_051

Description: Audit Account Lockout is set to Success and Failure

**Status: passed**

Current Value: Success

Expected Value: Success, Failure

Remediation: auditpol /set /subcategory:"Account Lockout" /success:enable /failure:enable

---

### Category: Audit Policies

Check ID: WIN\_052

Description: Audit Logon is set to Success and Failure

**Status: passed**

Current Value: Success and Failure

Expected Value: Success, Failure

Remediation: auditpol /set /subcategory:"Logon" /success:enable /failure:enable

---

### Category: Audit Policies

Check ID: WIN\_053

Description: Audit Logoff is set to Success

**Status: passed**

Current Value: Success

Expected Value: Success

Remediation: auditpol /set /subcategory:"Logoff" /success:enable /failure:enable

---

### Category: Audit Policies

Check ID: WIN\_054

Description: Audit Account Management is set to Success and Failure

**Status: failed**

Current Value: Not configured

Expected Value: Success, Failure

Remediation: auditpol /set /subcategory:"Account Management" /success:enable /failure:enable

---

### Category: Audit Policies

Check ID: WIN\_055

Description: Audit Directory Service Access is set to Failure

**Status: failed**

Current Value: Not configured

Expected Value: Success, Failure

Remediation: auditpol /set /subcategory:"Directory Service Access" /success:enable /failure:enable

---

### Category: Audit Policies

Check ID: WIN\_056

Description: Audit Object Access is set to Success and Failure

**Status: failed**



Current Value: Not configured  
Expected Value: Success, Failure  
Remediation: auditpol /set /subcategory:"Object Access" /success:enable /failure:enable

---

#### Category: Audit Policies

Check ID: WIN\_057  
Description: Audit Policy Change is set to Success and Failure  
**Status: failed**  
Current Value: Not configured  
Expected Value: Success, Failure  
Remediation: auditpol /set /subcategory:"Policy Change" /success:enable /failure:enable

---

#### Category: Audit Policies

Check ID: WIN\_058  
Description: Audit Privilege Use is set to Failure  
**Status: failed**  
Current Value: Not configured  
Expected Value: Success, Failure  
Remediation: auditpol /set /subcategory:"Privilege Use" /success:enable /failure:enable

---

#### Category: Audit Policies

Check ID: WIN\_059  
Description: Audit System Events is set to Success and Failure  
**Status: failed**  
Current Value: Not configured  
Expected Value: Success, Failure  
Remediation: auditpol /set /subcategory:"System" /success:enable /failure:enable

---

#### Category: Windows Firewall

Check ID: WIN\_060  
Description: Windows Firewall: Domain: Firewall state is set to On (recommended)  
**Status: passed**  
Current Value: On  
Expected Value: On  
Remediation: netsh advfirewall set domainprofile state on

---

#### Category: Windows Firewall

Check ID: WIN\_061  
Description: Windows Firewall: Private: Firewall state is set to On (recommended)  
**Status: passed**  
Current Value: On  
Expected Value: On  
Remediation: netsh advfirewall set privateprofile state on

---

#### Category: Windows Firewall

Check ID: WIN\_062  
Description: Windows Firewall: Public: Firewall state is set to On (recommended)  
**Status: passed**  
Current Value: On  
Expected Value: On  
Remediation: netsh advfirewall set publicprofile state on

---

#### Category: Windows Firewall

Check ID: WIN\_063  
Description: Windows Firewall: Domain: Inbound connections is set to Block (default)  
**Status: passed**  
Current Value: Block  
Expected Value: Block  
Remediation: netsh advfirewall set domainprofile firewallpolicy BlockInbound,AllowOutbound

---

### Category: Windows Firewall

Check ID: WIN\_064

Description: Windows Firewall: Private: Inbound connections is set to Block (default)

**Status: passed**

Current Value: Block

Expected Value: Block

Remediation: netsh advfirewall set privateprofile firewallpolicy BlockInbound,AllowOutbound

---

### Category: Windows Firewall

Check ID: WIN\_065

Description: Windows Firewall: Public: Inbound connections is set to Block (default)

**Status: passed**

Current Value: Block

Expected Value: Block

Remediation: netsh advfirewall set publicprofile firewallpolicy BlockInbound,AllowOutbound

---

### Category: Windows Firewall

Check ID: WIN\_066

Description: Windows Firewall: Domain: Outbound connections is set to Allow (default)

**Status: failed**

Current Value: Allow

Expected Value: Block

Remediation: netsh advfirewall set domainprofile firewallpolicy BlockInbound,BlockOutbound

---

### Category: Windows Firewall

Check ID: WIN\_067

Description: Windows Firewall: Private: Outbound connections is set to Allow (default)

**Status: failed**

Current Value: Allow

Expected Value: Block

Remediation: netsh advfirewall set privateprofile firewallpolicy BlockInbound,BlockOutbound

---

### Category: Windows Firewall

Check ID: WIN\_068

Description: Windows Firewall: Public: Outbound connections is set to Allow (default)

**Status: failed**

Current Value: Allow

Expected Value: Block

Remediation: netsh advfirewall set publicprofile firewallpolicy BlockInbound,BlockOutbound

---

### Category: System Services

Check ID: WIN\_069

Description: Base Cryptographic Provider is set to Enabled

**Status: passed**

Current Value: Running

Expected Value: Running

Remediation: sc config CryptSvc start= running

---

### Category: System Services

Check ID: WIN\_070

Description: DHCP Client is set to Enabled (if using DHCP)

**Status: passed**

Current Value: Running

Expected Value: Running

Remediation: sc config Dhcp start= running

---

### Category: System Services

Check ID: WIN\_071

Description: DNS Client is set to Enabled

**Status: passed**

Current Value: Running  
Expected Value: Running  
Remediation: sc config Dnscache start= running

---

**Category: System Services**

Check ID: WIN\_072  
Description: Network Location Awareness is set to Enabled  
**Status: failed**  
Current Value: Disabled  
Expected Value: Running  
Remediation: sc config NlaSvc start= running

---

**Category: System Services**

Check ID: WIN\_073  
Description: Windows Time is set to Enabled  
**Status: failed**  
Current Value: Disabled  
Expected Value: Running  
Remediation: sc config W32Time start= running

---

**Category: System Services**

Check ID: WIN\_074  
Description: Windows Firewall is set to Enabled  
**Status: passed**  
Current Value: Running  
Expected Value: Running  
Remediation: sc config MpsSvc start= running

---

**Category: System Services**

Check ID: WIN\_075  
Description: Remote Registry is set to Disabled  
**Status: passed**  
Current Value: Disabled  
Expected Value: Disabled  
Remediation: sc config RemoteRegistry start= disabled

---