



WinSystemHarden V1.3

User Guide

Offline System Hardening

Version: 1.3

Date: Sep 22, 2026

Copyright: © Nisse-Sec Team. All Rights Reserved.

Website: www.nisse-sec.com

Email: support@nisse-sec.com

Table of Contents

1. Introduction.....	3
1.1 What is WinSystemHarden?	3
1.2 Key Features	3
2. System Requirements.....	4
3. Installation & First Launch	4
3.1 Installation	4
3.2 First Launch	4
4. Hardening	5
4.1 Overview	5
4.2 Hardening Plans.....	6
4.3 Hardening Categories	6
4.4 Applying Hardening	8
4.5 Pending Restart State.....	10
5. Rollback.....	10
6. Log View	14
7. Troubleshooting.....	14
7.1 Common Issues.....	14
7.2 Reporting a Bug.....	15
8. FAQ	15
9. Contact & Support	17

1. Introduction

1.1 What is WinSystemHarden?

WinSystemHarden V1.3 is a free, offline system hardening tool for Windows. It offers 29 security measures inspired by CIS benchmarks and NSA Windows security recommendations, reducing your attack surface by disabling vulnerable protocols and services, and enforcing security policies.

The Standard plan applies 20 essential measures. The Deep plan applies all 29.

It works entirely offline — no cloud dependency, no data upload. No account, no license, no telemetry.

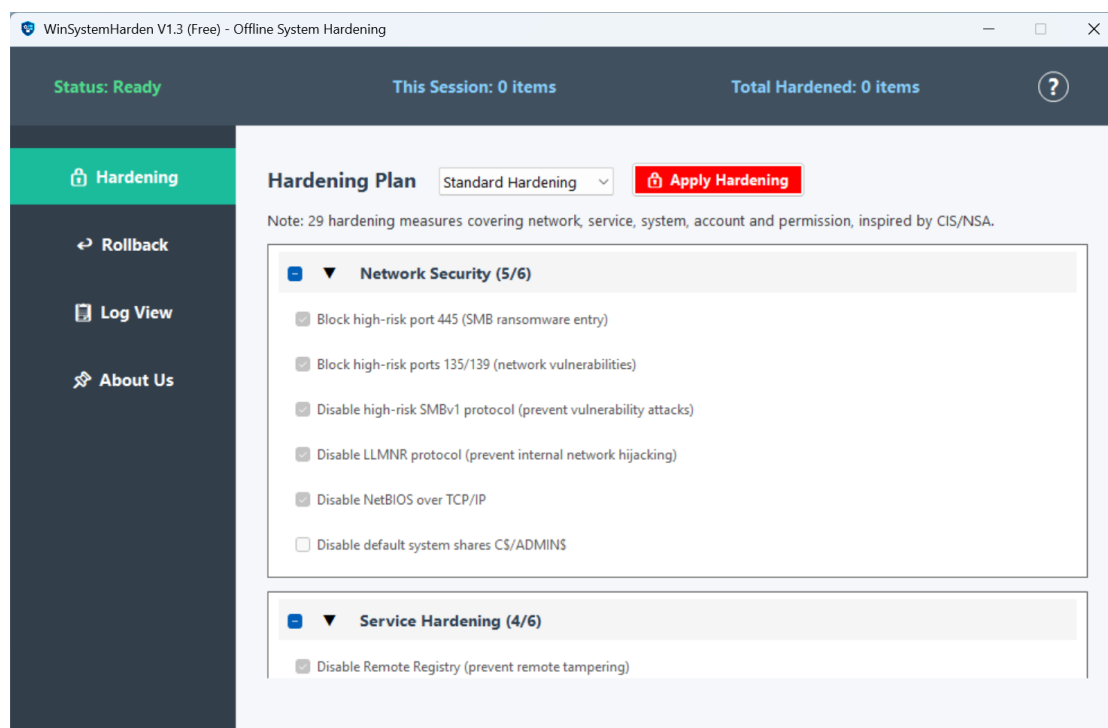


Figure 1: WinSystemHarden Main Window

1.2 Key Features

- ✓ 29 Hardening Measures — Covering network, services, system, account, and permission security
- ✓ Three Hardening Plans - Standard (20 items), Deep (29 items), and Custom
- ✓ One-Click Rollback — Revert any hardening operation with a single click
- ✓ Offline Operation — No cloud, no data upload, no telemetry
- ✓ 100% Free — No trial, no license, no expiration

2. System Requirements

- ✓ Operating System: Windows 10 / 11 (32-bit or 64-bit)
- ✓ RAM: 4 GB
- ✓ Disk Space: 100 MB
- ✓ .NET Runtime: .NET 8.0 Desktop Runtime
- ✓ Administrator Rights: Required
- ✓ Internet: Optional (only for update check)

3. Installation & First Launch

3.1 Installation

- 1) Download the installer (WinSystemHarden_Setup_V1.3.exe) from our website
- 2) Double-click the installer to run it
- 3) Follow the on-screen instructions to complete the installation
- 4) Launch WinSystemHarden from the desktop shortcut or Start Menu

3.2 First Launch

On launch, the program will automatically request administrator elevation. This is required because hardening operations modify system settings. Click "Yes" when prompted.

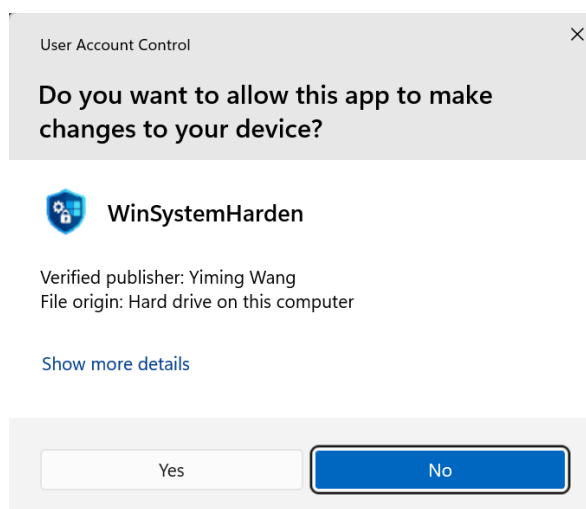


Figure 2: Administrator Privilege Request

The program creates a data folder at %ProgramData%\WinSystemHarden for storing

configuration and logs. You don't need to interact with this folder directly.

4. Hardening

4.1 Overview

The Hardening module provides 29 security measures organized into five categories:

- ✓ Network Security - Block dangerous ports, disable vulnerable protocols
- ✓ Service Hardening - Disable high-risk services
- ✓ System Hardening - Enable DEP, ASLR, SEHOP; disable AutoRun
- ✓ Account Policy - Enable UAC, password complexity, auto lock screen
- ✓ Permission Management - Lock critical files and directories

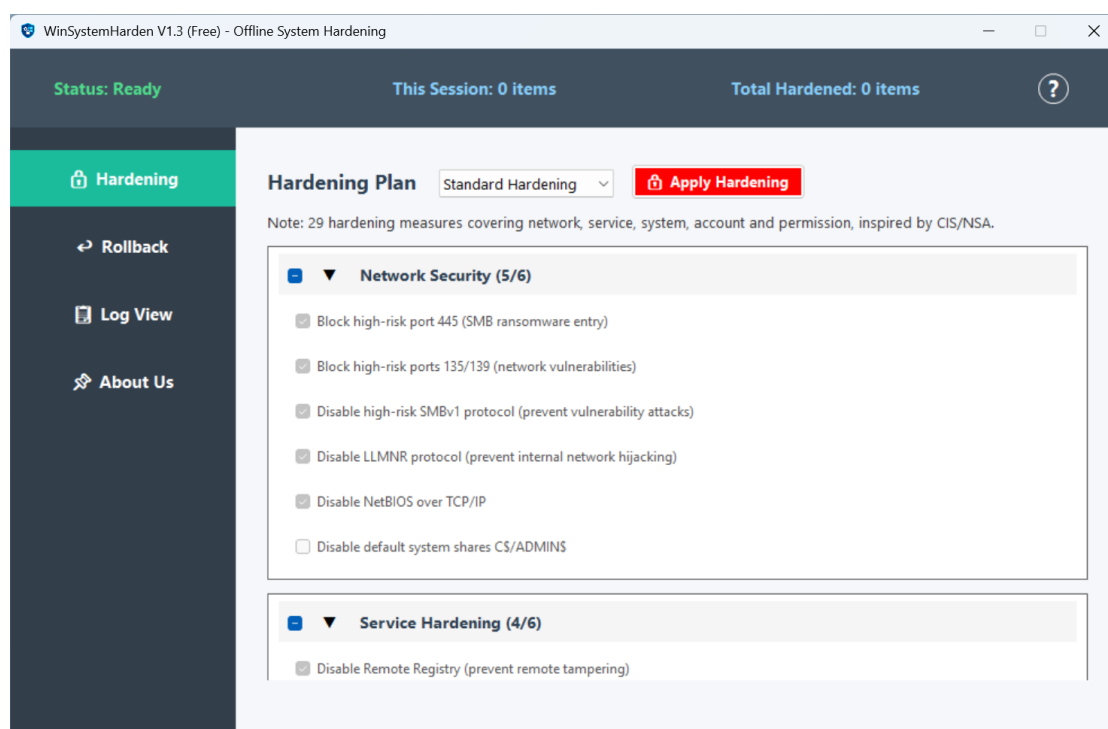


Figure 3: Hardening Page

4.2 Hardening Plans

WinSystemHarden offers three hardening plans:

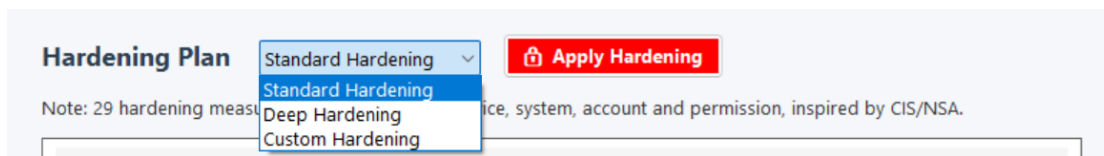


Figure 4: Hardening Plans

- ✓ Standard Hardening - 20 essential security measures across 5 categories. Safe for all systems. Recommended for most users.
- ✓ Deep Hardening - All 29 measures, including default share disabling, WSH disabling, UPnP disabling, PowerShell execution policy reset, password complexity, and auto lock screen. May affect some applications. Recommended for advanced users or high-security environments.
- ✓ Custom Hardening - Manually select individual hardening items. Full control over which security measures to apply.

4.3 Hardening Categories

Network Security (6 items)

- ✓ Block high-risk port 445 (SMB ransomware entry)
- ✓ Block high-risk ports 135/139 (network vulnerabilities)
- ✓ Disable high-risk SMBv1 protocol (prevent vulnerability attacks)
- ✓ Disable LLMNR protocol (prevent internal network hijacking)
- ✓ Disable NetBIOS over TCP/IP
- ✓ Disable default system shares C\$/ADMIN\$

Service Hardening (6 items)

- ✓ Disable Remote Registry (prevent remote tampering)
- ✓ Disable Telnet Service (high-risk remote tool)

- ✓ Disable Windows Remote Assistance
- ✓ Disable Windows Script Host (WSH)
- ✓ Disable UPnP (prevent internal network scanning)
- ✓ Disable System Diagnostic Tracking Service

System Hardening (7 items)

- ✓ Harden critical registry key permissions
- ✓ Limit NTP time correction (prevent time drift abuse)
- ✓ Enable security audit policy
- ✓ Disable USB/CD-ROM AutoRun
- ✓ Enable Data Execution Prevention (DEP)
- ✓ Enable ASLR memory randomization
- ✓ Enable SEHOP structured exception handling protection

Account Policy (7 items)

- ✓ Enable UAC (prevent privilege escalation)
- ✓ Reset PowerShell execution policy to RemoteSigned
- ✓ Restrict anonymous access to named pipes and shares
- ✓ Disable Guest account
- ✓ Disable anonymous SAM account enumeration
- ✓ Enable password complexity security policy
- ✓ Enable 5-minute auto lock screen (prevent unattended access)

Permission Management (3 items)

- ✓ Prevent regular users from modifying Hosts file
- ✓ Prevent writing to startup directory
- ✓ Lock backup directory against deletion

4.4 Applying Hardening

To apply hardening:

- ✓ Navigate to the Hardening page
- ✓ Select a hardening plan from the dropdown menu
 - Standard Hardening: 20 high-value, low-impact items
 - Deep Hardening: all 29 items
 - Custom Hardening: manually select items
- ✓ Click the red Apply Hardening button
- ✓ Confirm the hardening dialog
- ✓ Wait for the progress bar to complete
- ✓ Review the results summary

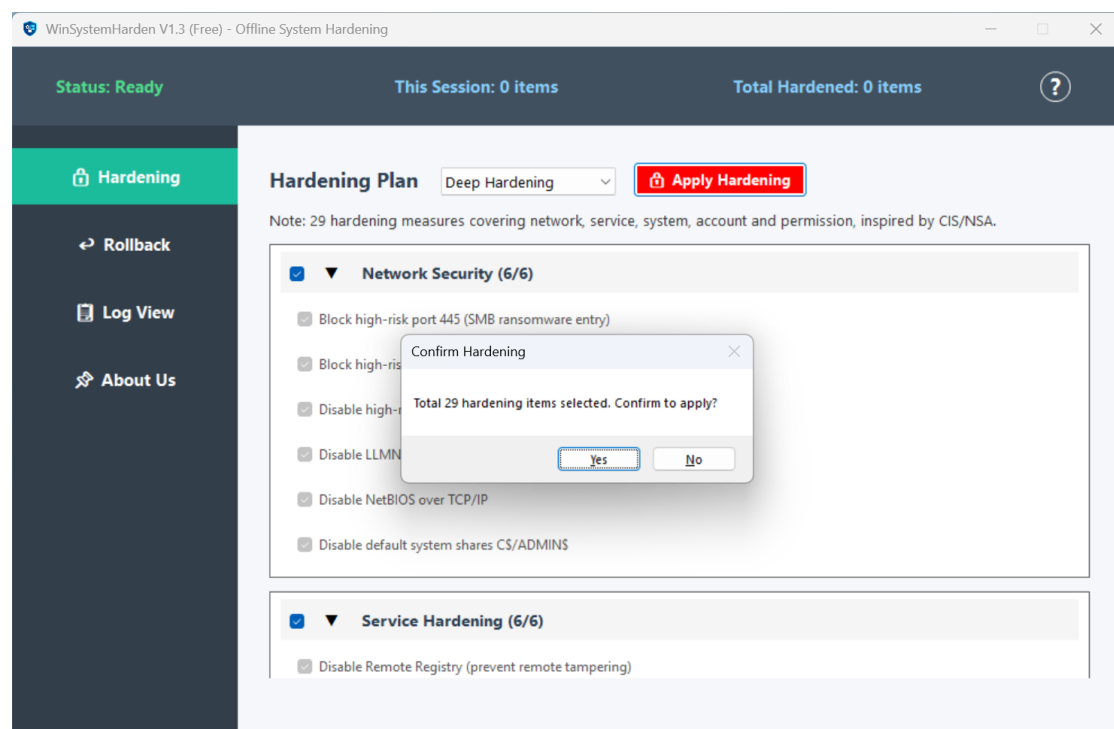


Figure 5: Confirm Hardening Dialog

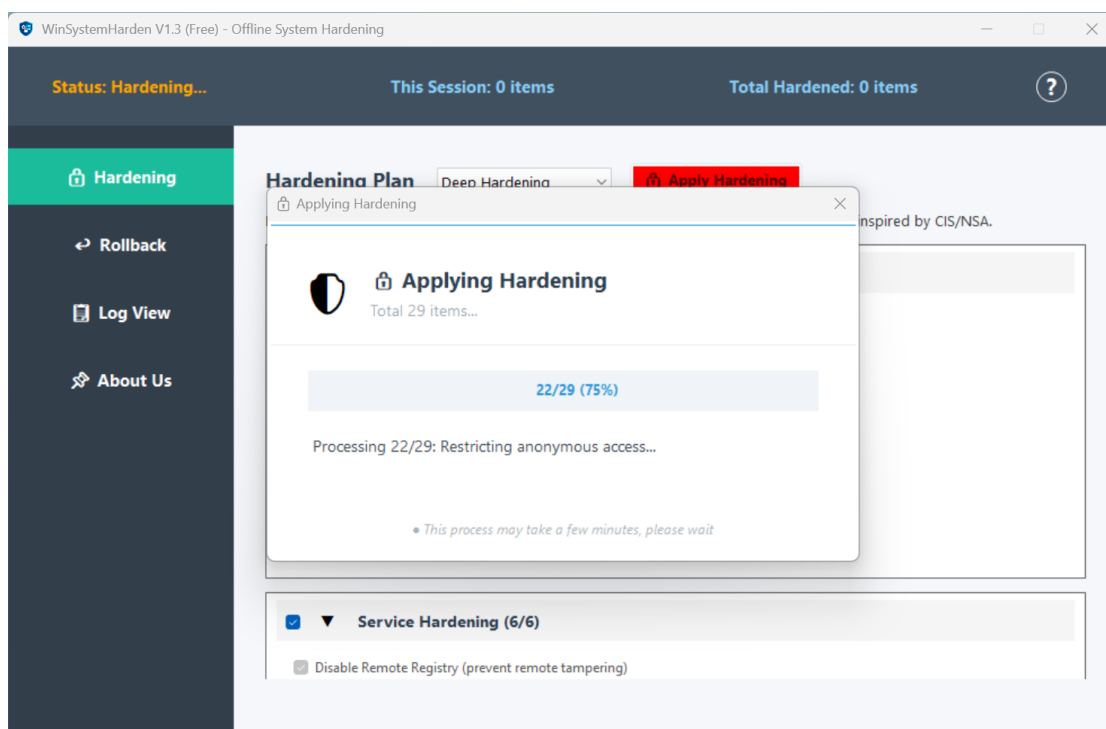


Figure 6: Hardening Progress

The operation may take a few minutes. Each hardening item is applied sequentially.

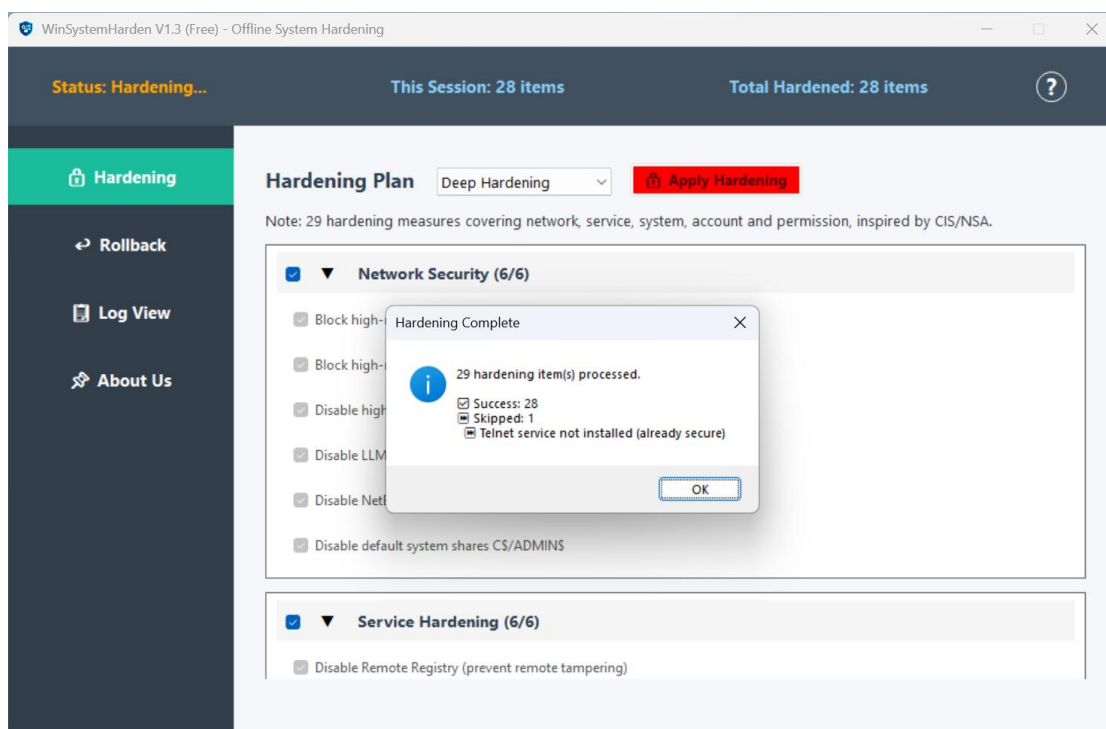


Figure 7: Hardening Completion Results

4.5 Pending Restart State

Some hardening measures require a computer restart to take full effect. When this happens, a dialog appears asking if you want to restart now or later.

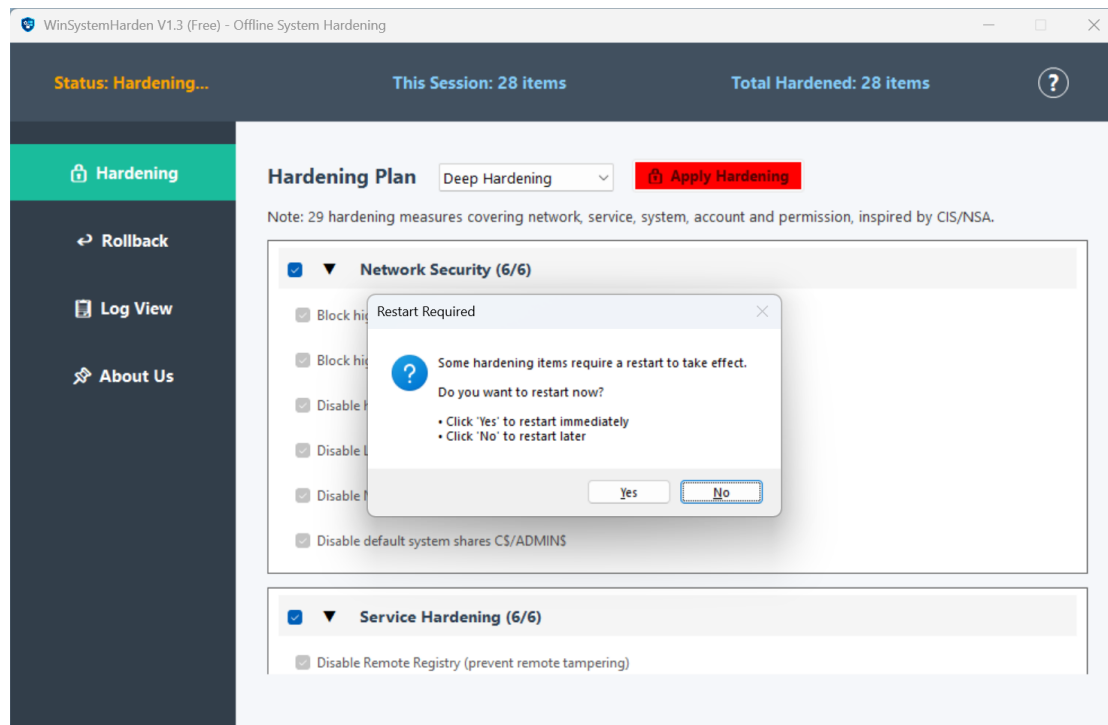


Figure 8: Hardening Restart Required

If you choose "No", the program enters a "Pending Restart" state — hardening and rollback operations are blocked until you restart your computer. After reboot, the state is cleared automatically.

5. Rollback

Every hardening operation is recorded. You can roll back hardening at any time to restore previous system settings.

To roll back:

- ✓ Navigate to the Rollback page
- ✓ Select a hardening time point to roll back to
- ✓ Click Confirm Rollback
- ✓ Wait for the progress bar to complete

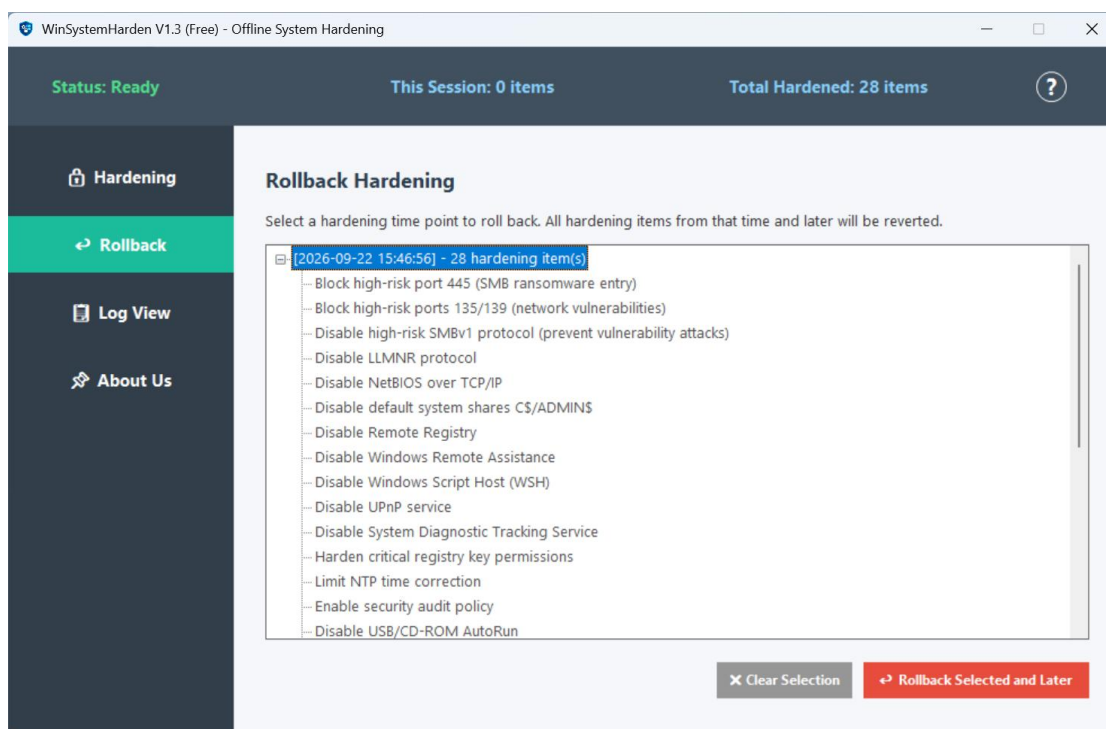


Figure 9: Rollback Selection Dialog

Note: All hardening items from the selected time point and later will be reverted.

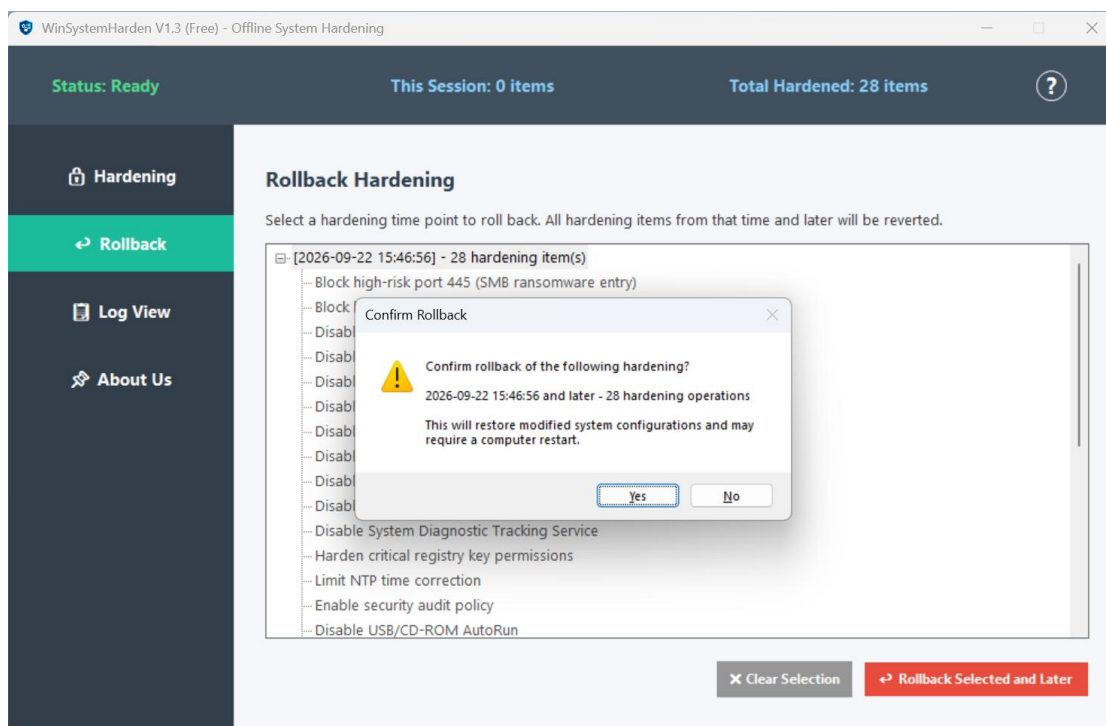


Figure 10: Rollback Confirmation Dialog

After rollback, a summary dialog shows the success count and any failed items.

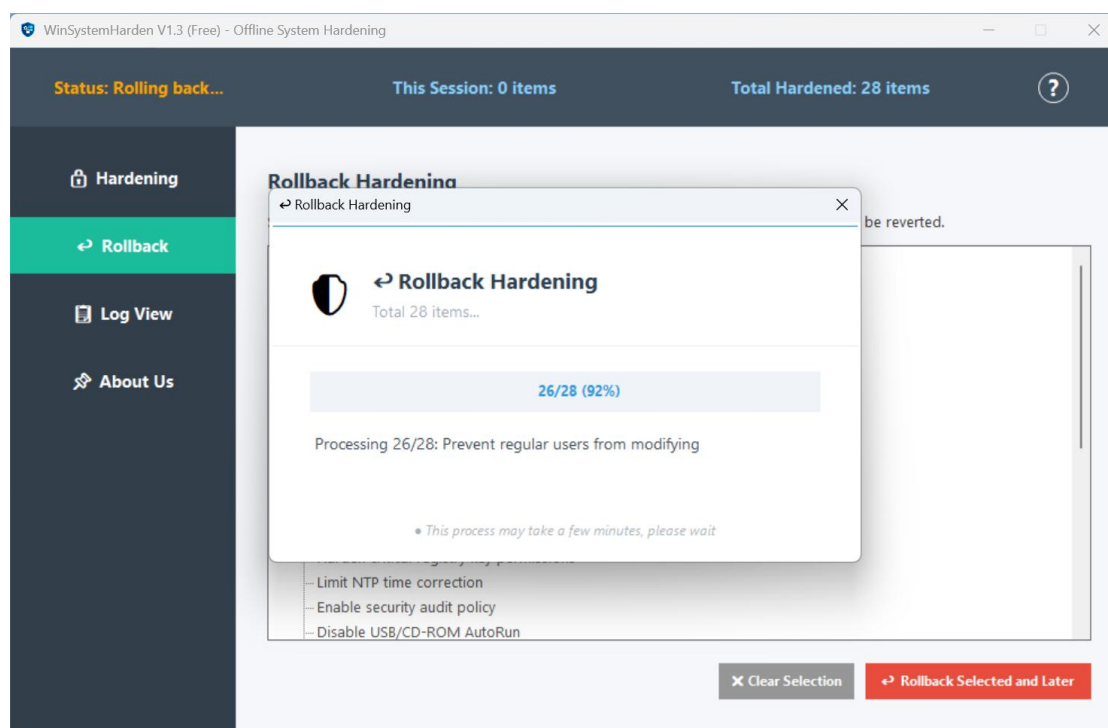


Figure 11: Rollback Progress

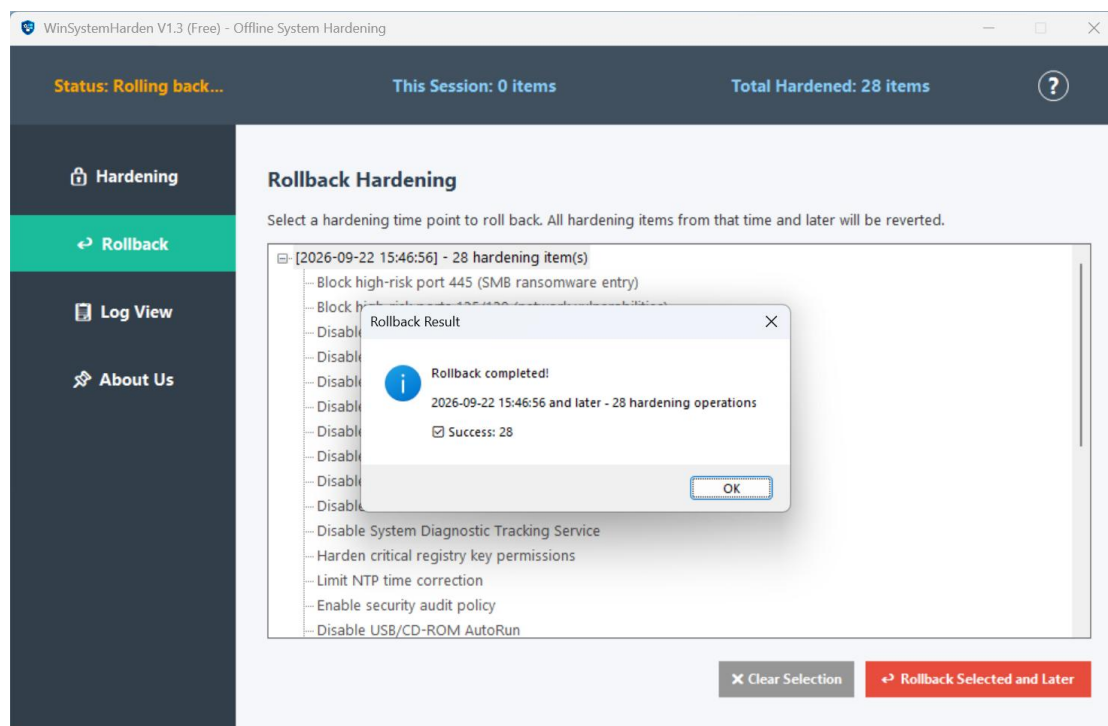


Figure 12: Rollback Result

Some rollback operations may require a computer restart to take effect. You will be prompted to restart.

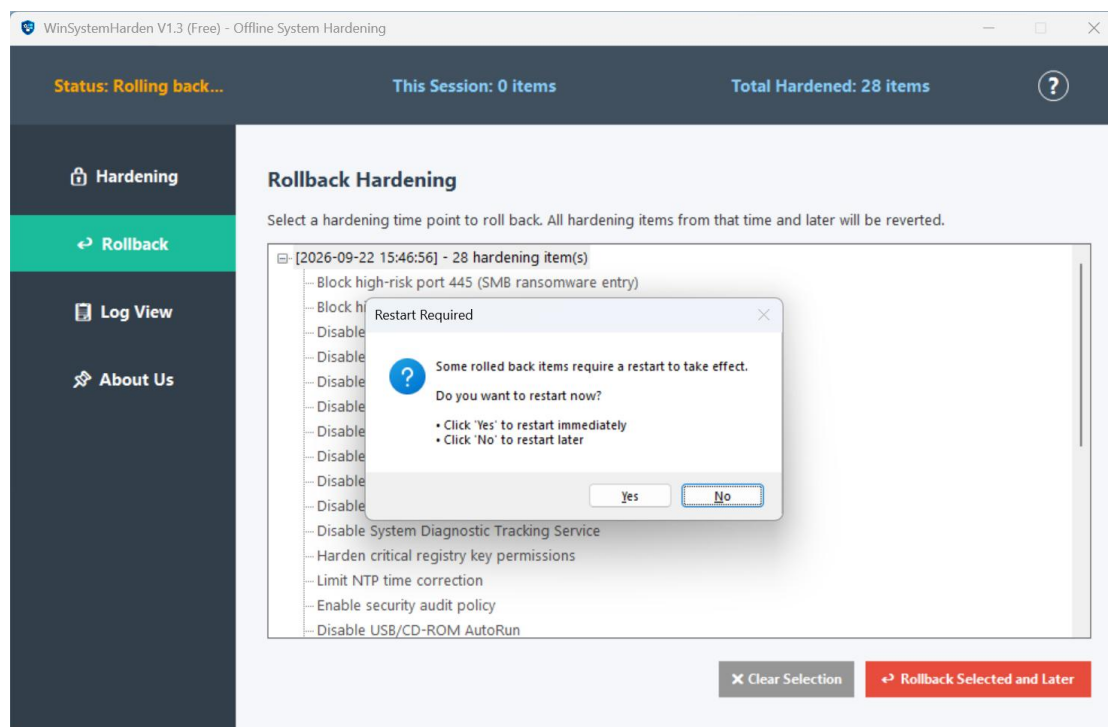


Figure 13: Rollback Restart Required

If you choose "No", the program enters a "Pending Restart" state — hardening and rollback operations are blocked until you restart your computer. After reboot, the state is cleared automatically.

6. Log View

The Log View page provides detailed records of all hardening and rollback operations.

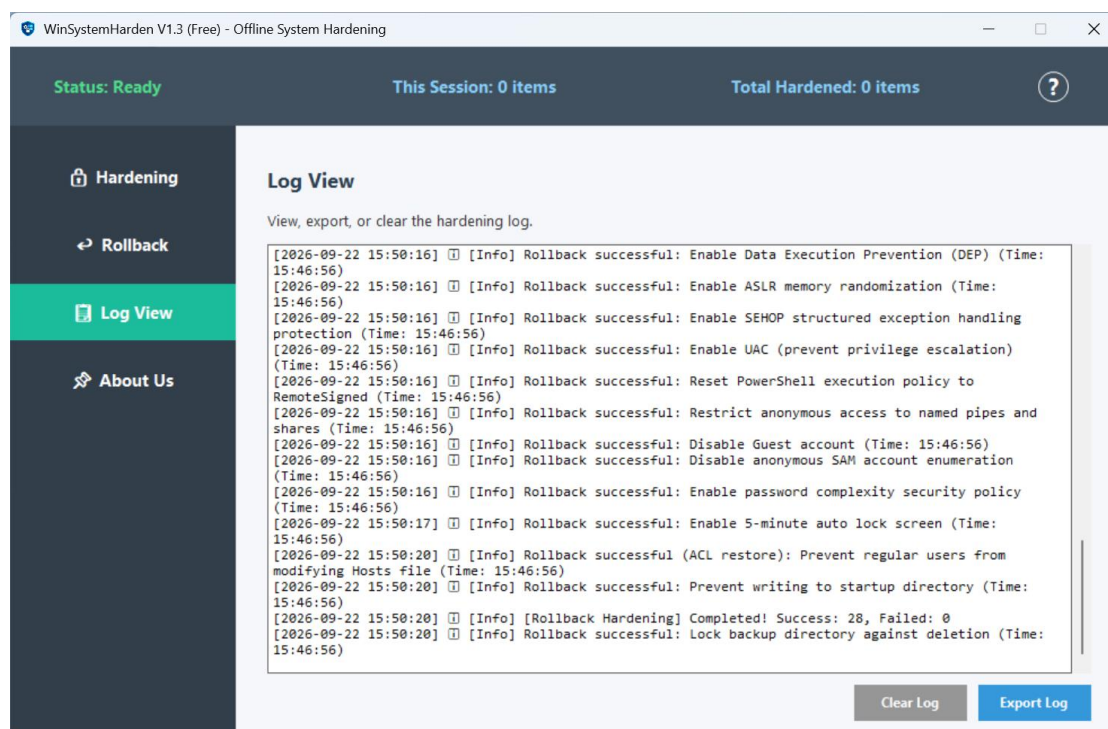


Figure 13: Log View Page

Each log entry includes:

- ✓ Timestamp
- ✓ Severity level (Info, Warning, Error, Critical)
- ✓ Event description

Note: Debug-level entries are not written to the log file.

Operations:

- ✓ Export Log: Export as TXT or CSV
- ✓ Clear Log: Clear all entries (cannot be undone)

7. Troubleshooting

7.1 Common Issues

"Please run this program as administrator"

If the UAC elevation prompt does not appear automatically, right-click WinSystemHarden.exe → Run as administrator → Click Yes when prompted by UAC.

Hardening operation fails

Possible causes: not running as admin, Windows feature missing, permission denied, or system files locked by another program.

To diagnose:

- ✓ Check the Log View for error messages
- ✓ Note which specific item failed
- ✓ Contact support with the error details

7.2 Reporting a Bug

Please include:

- ✓ Version (check the About page)
- ✓ Windows Version (Windows 10 or 11?)
- ✓ Steps to Reproduce
- ✓ Expected Result
- ✓ Actual Result

Send bug reports to: support@nisse-sec.com

8. FAQ

Q1: Is WinSystemHarden really free?

A: Yes. WinSystemHarden is completely free, with no trial period, no license key, and no expiration. It is a standalone tool that applies the same hardening engine we use on our own machines.

Q2: Will WinSystemHarden slow down my computer?

A: No. WinSystemHarden only applies configuration changes. It does not run in the background and does not consume CPU or memory after hardening completes.

Q3: Can I undo hardening?

A: Yes. Every hardening operation is recorded, and you can roll back any time point from the Rollback page.

Q4: Can I run WinSystemHarden without administrator privileges?

A: No. Administrator privileges are required for hardening operations to modify system settings.

Q5: Does WinSystemHarden work on Windows 10/11 Home edition?

A: Yes. WinSystemHarden works on all Windows 10/11 editions (Home, Pro, and Enterprise).

Q6: What is the difference between Standard, Deep, and Custom

Hardening?

A:

- ✓ Standard Hardening applies 20 essential measures. Safe for all systems.
- ✓ Deep Hardening applies all 29 measures. May affect some applications.
- ✓ Custom Hardening lets you select individual measures.

Q7: Will hardening affect my applications?

A: Most applications work fine after hardening. Some legacy applications may rely on protocols or services that hardening disables (e.g., SMBv1, NetBIOS). If an application stops working after hardening, roll back the corresponding measure.

Q8: Does WinSystemHarden collect any data?

A: No. WinSystemHarden works entirely offline and does not collect or transmit any data. Configuration and logs are stored locally at %ProgramData%\WinSystemHarden.

Q9: Can I use WinSystemHarden on multiple computers?

A: Yes. WinSystemHarden is free, so you can install it on any number of computers.

Q10: How often should I apply hardening?

A: Once is usually enough. Windows updates may reset some settings, so you can re-

apply hardening periodically or after major updates.

9. Contact & Support

- ✓ Website: www.nisse-sec.com
- ✓ Email: support@nisse-sec.com

Disclaimer

For legitimate security use only. This tool is intended for use on systems you own or are authorized to manage. Provided "as is", without warranty of any kind — use at your own risk.

WinSystemHarden applies system configuration changes inspired by CIS benchmarks and NSA recommendations. No hardening tool can guarantee complete security. Always maintain regular backups of your important data.

Copyright © 2026 Nisse-Sec Team. All rights reserved.