

WinRansomProtect V1.0.2

User Guide

Protect your data from ransomware with multi-layered defense

Version: 1.0.2

Date: July 28, 2026

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

Website: <https://www.nisse-sec.com>

Email: support@nisse-sec.com

Table of Contents

1. Introduction	4
1.1 What is WinRansomProtect?	4
1.2 Key Features	4
1.3 How It Works	4
2. System Requirements.....	5
2.1 Minimum Requirements	5
2.2 Recommended Requirements.....	5
3. Installation & First Launch.....	5
3.1 Installation.....	5
3.2 First Launch	6
4. License & Activation.....	7
4.1 License Types.....	7
4.2 Finding Your Machine Code.....	7
4.3 Getting a License Key	8
4.4 Activating Your License.....	8
4.5 License Status Display	9
4.6 What Happens When License Expires?	9
5. Protection Module	10
5.1 Overview	10
5.2 Protection Plans	11
5.3 Starting Protection	11
5.4 Protection Status Indicators	12
5.5 What Protection Monitors	13
5.6 Blocked File Types	14
5.7 Stopping Protection.....	14
6. Hardening Module	14
6.1 Overview	14
6.2 Hardening Plans	15
6.3 Applying Hardening.....	16
6.4 Rolling Back Hardening.....	19
6.5 Pending Restart State	24
7. Log Center	24
7.1 Overview	24
7.2 Log Types.....	24
7.3 Log Entry Format.....	25
7.4 Log Operations	26
8. Settings & Whitelist.....	26
8.1 Basic Settings.....	26
8.2 Quarantine Management.....	27
8.3 Whitelist (Trusted Zone).....	27
9. System Tray.....	29
9.1 Accessing the System Tray.....	29
9.2 Tray Menu Options.....	29

9.3 Silent Mode	29
10. Troubleshooting	30
10.1 Common Issues	30
10.2 Reporting a Bug.....	31
11. Frequently Asked Questions.....	31
Q1: Is WinRansomProtect compatible with other antivirus software?	31
Q2: Will WinRansomProtect slow down my computer?	31
Q3: What should I do if I get a false positive?.....	32
Q4: Can I run WinRansomProtect without administrator privileges?.....	32
Q5: What happens to quarantined files?	32
Q6: What is the difference between Standard, Enhanced, and Custom Protection?	32
Q7: Does WinRansomProtect offer different hardening levels?	33
Q8: Can I use the program on multiple computers?	33
Q9: Does the program work on Windows 10/11 Home edition?	33
Q10: Will the program protect me from zero-day ransomware?.....	33
12. Contact & Support.....	33
12.1 Contact Information	33
12.2 License & Purchase.....	34
12.3 Disclaimer.....	34

1. Introduction

1.1 What is WinRansomProtect?

WinRansomProtect V1.0.2 is a comprehensive ransomware protection and system hardening tool for Windows. It employs a multi-layered defense strategy combining signature-based detection, behavioral analysis, and system hardening to protect your data from ransomware attacks and other malware threats. The system hardening module applies 32 security measures following CIS benchmarks and NSA recommendations, reducing the attack surface by disabling vulnerable protocols, services, and enforcing security policies.

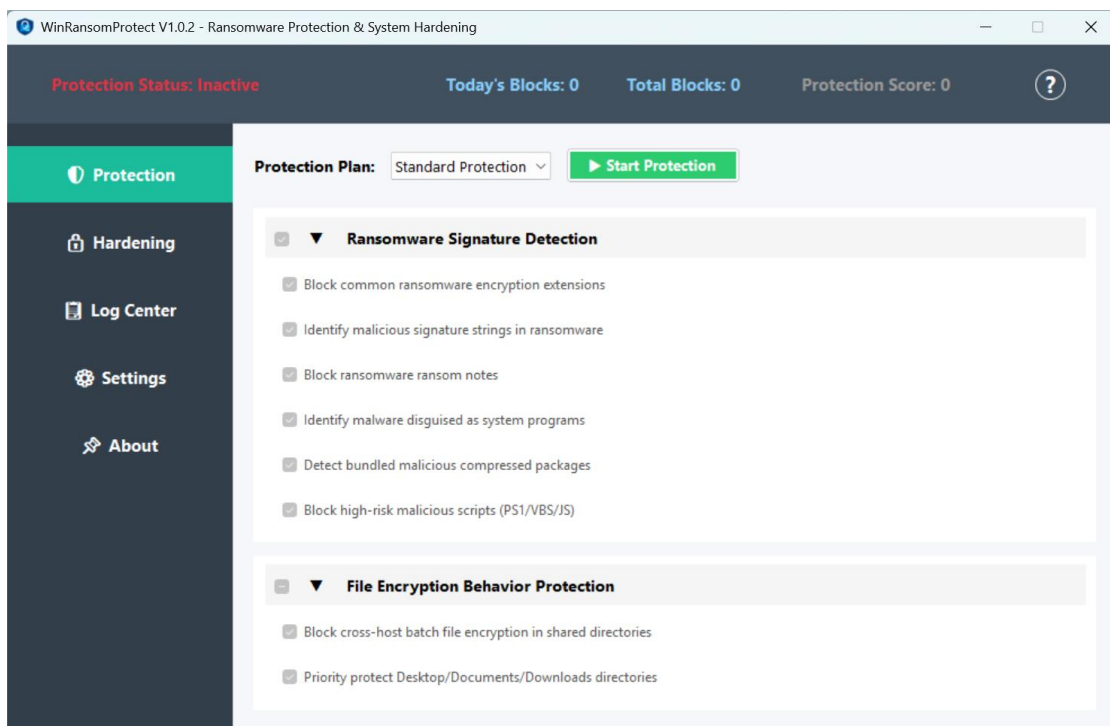


Figure 1: WinRansomProtect Main Window

1.2 Key Features

- Real-time Protection — Signature + behavior dual analysis across 30 detection rules to detect and block ransomware
- System Hardening — Security measures following industry-standard best practices
- Live Dashboard — Real-time protection status, block counts, and security score
- Comprehensive Logging — Detailed logs for both protection events and hardening operations
- Flexible Configuration — Whitelist trusted files, directories, and processes
- License System — One-machine-one-code activation with trial support

1.3 How It Works

WinRansomProtect operates at multiple levels:

1. File System Monitoring — Watches critical user directories for suspicious file operations
2. Process Analysis — Monitors running processes for ransomware-like behavior
3. Signature Detection — identifies known ransomware patterns and extensions across 30 detection rules
4. Behavioral Analysis — Detects abnormal activity patterns indicative of ransomware
5. System Hardening — Applies security configurations to prevent attacks

2. System Requirements

2.1 Minimum Requirements

Operating System: Windows 10 / 11 (32-bit or 64-bit), Windows Server 2016 / 2019 / 2022

RAM: 4 GB

Disk Space: 100 MB

.NET Runtime: .NET 8.0 Desktop Runtime (x86 or x64, matching your system architecture)

Administrator Rights: Required

Internet: Required for license activation and updates

2.2 Recommended Requirements

Operating System: Windows 11 (64-bit) (other Windows versions may work but are not officially recommended)

RAM: 8 GB or more

Disk Space: 500 MB or more

3. Installation & First Launch

3.1 Installation

WinRansomProtect is distributed as an installer package for easy setup.

1. Download the installer ([`WinRansomProtect\\_Setup\\_V1.0.2.exe`](#)) from our website
2. Double-click the installer to run it
3. Follow the on-screen instructions to complete the installation
4. Launch WinRansomProtect from the desktop shortcut or Start Menu

3.2 First Launch

When you run the program for the first time:

Step 1: Administrator Privileges

The program will automatically request administrator elevation. This is required for:

- Real-time file monitoring
- Process protection
- System hardening
- Registry protection

IMPORTANT: Without administrator privileges, protection features will not work. Click "Yes" when prompted.

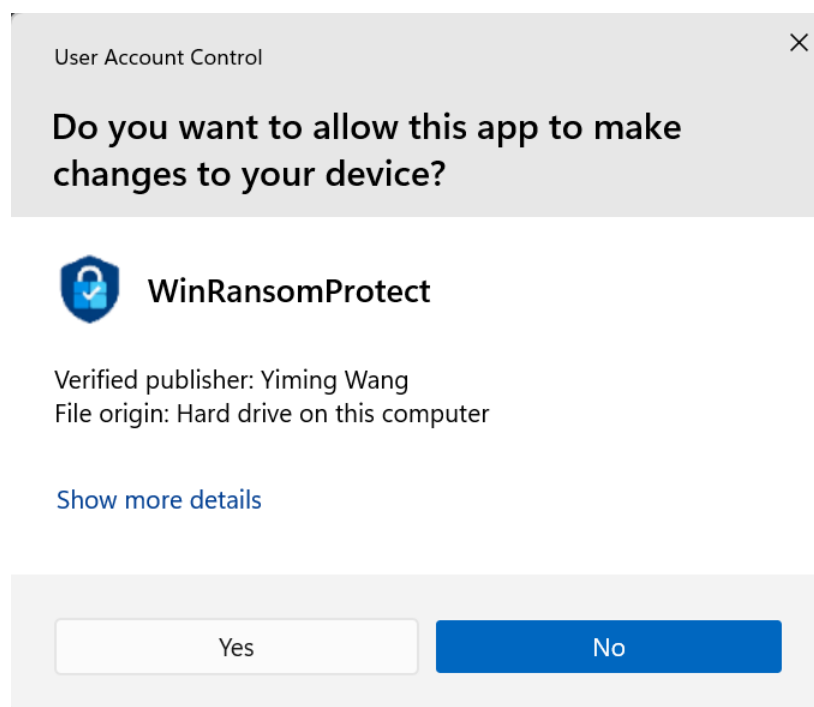


Figure 2: Administrator Privilege Request

Step 2: Trial Period

A 14-day free trial starts automatically upon first launch:

- Full features available
- No credit card required
- Trial tracking is tamper-resistant

Step 3: Data Directory

The program creates a data folder for storing configuration and logs.

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

Step 4: Single Instance

Only one instance of WinRansomProtect can run at a time. If you try to launch a second instance, you'll see:

"Program already running, please do not open again!"

4. License & Activation

4.1 License Types

Trial: 14 days, Full features, no restrictions

1-Year: 365 days, Full features

Permanent: Unlimited, Full features

4.2 Finding Your Machine Code

Your machine code uniquely identifies your computer and is required for license activation.

To find your machine code:

1. Navigate to the About page (click the "About" button in the left navigation panel)
2. Locate the "Machine Code" field
3. Click the Copy button to copy it to your clipboard

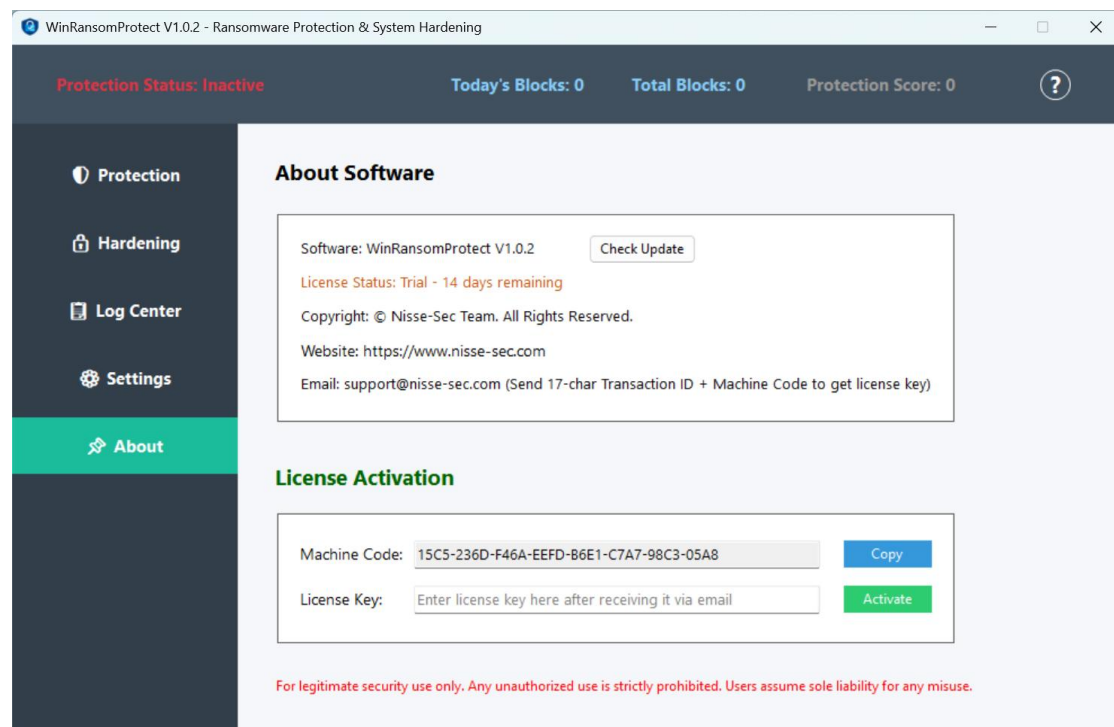


Figure 3: About Page with Machine Code

4.3 Getting a License Key

1. Copy your machine code
2. Email it along with your 17-character Transaction ID to: support@nisse-sec.com
3. You will receive an activation key via email (typically within 24 hours)

4.4 Activating Your License

1. Navigate to the About page
2. Paste your license key into the "License Key" field
3. Click the Activate button

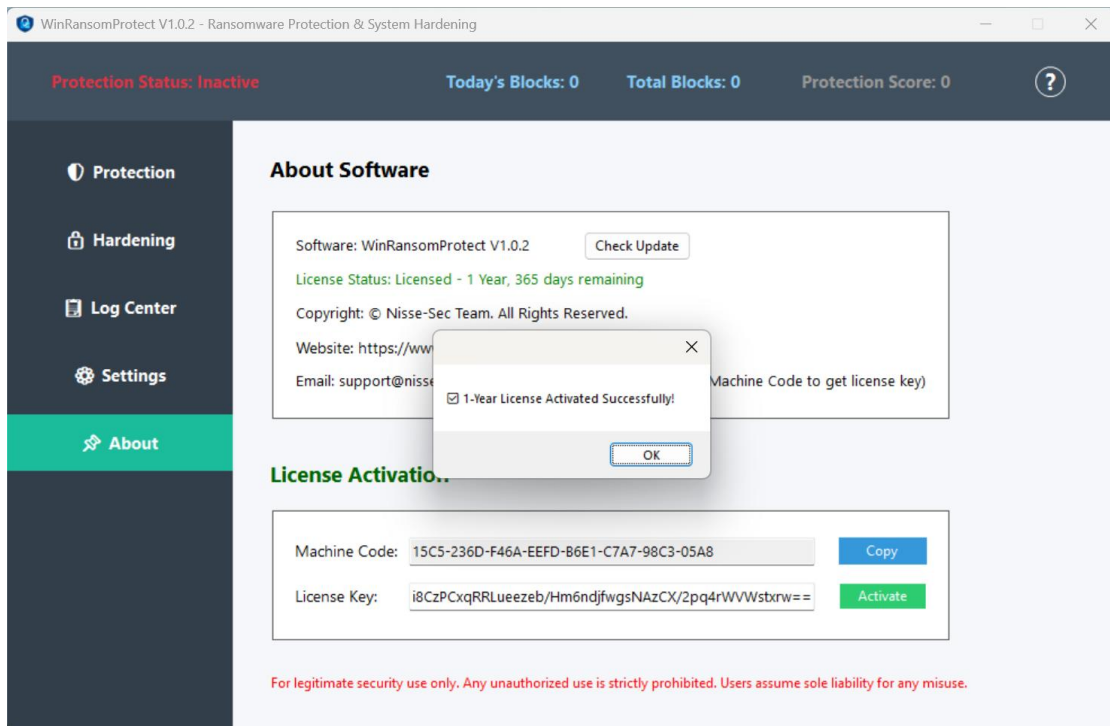


Figure 4: License Activation Interface

Activation Results:

Success: "1-Year License Activated Successfully!"

Success: "Permanent License Activated Successfully!"

Failure: "Invalid license key!"

Mismatch: "License key does not match this machine!"

4.5 License Status Display

The license status is displayed at the top of the About page:

Trial (active): "Trial - X days remaining" (Orange)

Trial (expired): "Expired - Trial period has ended" (Red)

1-Year Licensed: "Licensed - 1 Year, X days remaining" (Green)

Permanent: "Licensed - Permanent" (Green)

Expired (licensed): "Expired - Please renew" (Red)

4.6 What Happens When License Expires?

When your license expires:

- All protection features stop automatically
- Navigation buttons (Protection, Hardening, Log, Settings) are disabled
- A popup notification appears

- You are redirected to the About page for activation

IMPORTANT: To continue using WinRansomProtect, please renew your license before it expires.

5. Protection Module

5.1 Overview

The Protection module provides multiple detection rules organized into four categories:

- Ransomware Signature Detection — Known ransomware patterns
- File Encryption Behavior Protection — Ransomware-like behavior
- Malicious Process Behavior Blocking — Suspicious process activity
- System Runtime Control — System integrity protection

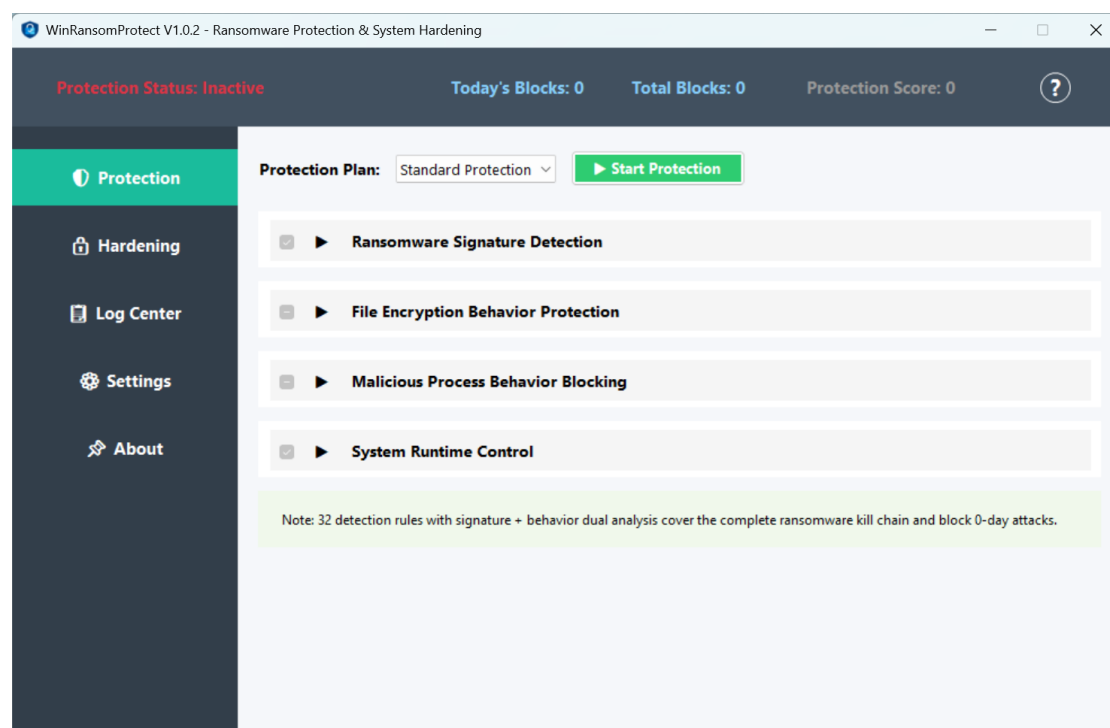


Figure 5: Protection rules

5.2 Protection Plans

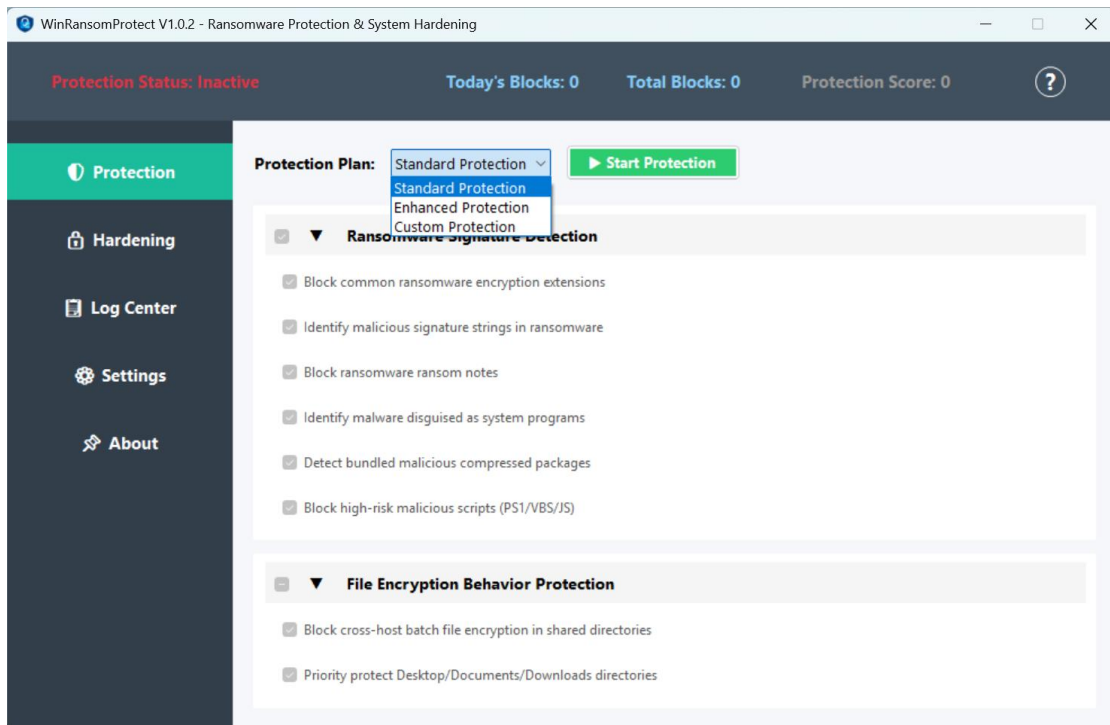


Figure 6: Protection Rules

Standard Protection: 27 core detection rules covering ransomware signatures, file encryption behavior, malicious process blocking, and system runtime control. Offers balanced protection with minimal false positives. Recommended for most users.

Enhanced Protection: 32 detection rules including advanced behavioral analysis (cloud sync monitoring, high-frequency disk writes, file locking detection, DLL injection detection, scheduled task monitoring, etc.). Provides maximum protection but may increase false positives. Recommended for advanced users or high-risk environments.

Custom Protection: Manually enable or disable individual detection rules (32 rules available). Gives you full control over what threats to monitor. Suitable for advanced users who want fine-tuned protection.

5.3 Starting Protection

To start protection:

1. Navigate to the Protection page from the left panel
2. Select a protection plan from the dropdown menu: Standard Protection, Enhanced Protection, or Custom Protection
3. Click the Start Protection button

Once protection is active, the **Protection Status** will display "Active" with an uptime timer.

The **Protection Score** reflects your selected plan: **Standard Protection** scores 84.4, **Enhanced Protection** scores 100, and **Custom Protection** scores are automatically calculated based on the enabled rules. To stop protection at any time, simply click the **Stop Protection** button.

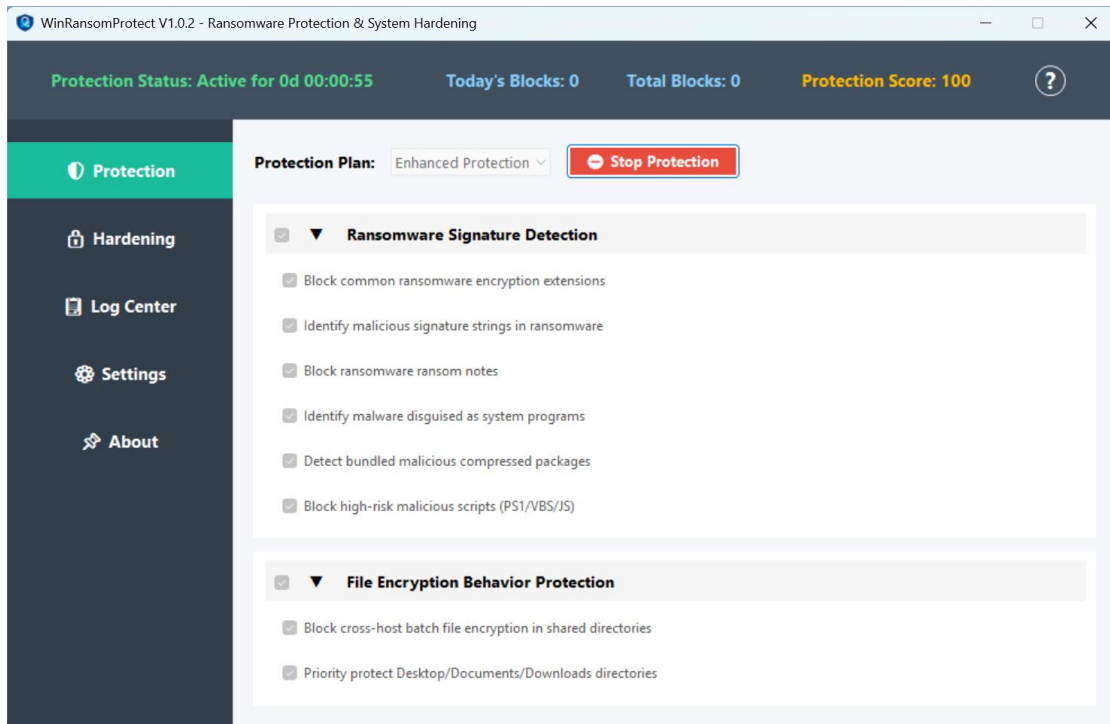


Figure 7: Starting Protection

5.4 Protection Status Indicators

The main dashboard provides clear visual indicators of your protection status:

- **Active (Green)** – Protection is actively monitoring your system. The timer shows how long protection has been running (e.g., Active for 0d 00:00:55).
- **Inactive (Red)** – Protection is not running. Click **Start Protection** to activate.
- **Stopped (Hardening) (Orange)** — Protection has been temporarily stopped for system hardening or rollback operations. It will be automatically restored after the operation completes. **Note:** If you choose to restart immediately, you need to manually launch the program and click **Start Protection** after reboot.

The dashboard also displays:

- **Today's Blocks** – Number of threats blocked today
- **Total Blocks** – Cumulative threats blocked since installation
- **Protection Score** – A real-time security score based on your selected protection plan (84.4 for Standard, 100 for Enhanced, auto-calculated for Custom)

5.5 What Protection Monitors

WinRansomProtect uses signature + behavior dual analysis across 32 detection rules in 4 categories:

Ransomware Signature Detection (6 rules):

- Block known ransomware encryption extensions
- Identify malicious signature strings
- Block ransomware ransom notes
- Identify malware disguised as system programs
- Detect bundled malicious compressed packages
- Block high-risk malicious scripts (PS1/VBS/JS)

File Encryption Behavior Protection (8 rules):

- Block cross-host batch file encryption in shared directories
- Priority protect Desktop/Documents/Downloads directories
- Block mass file encryption in short time
- Block batch rename and batch delete of documents
- Monitor abnormal batch hidden file generation
- Monitor abnormal batch file modifications in cloud sync directories (Enhanced)
- Monitor high-frequency continuous disk writes (Enhanced)
- Block programs locking a large number of files (Enhanced)

Malicious Process Behavior Blocking (8 rules):

- Block malicious system backup deletion commands
- Block suspicious script file execution
- Block WMIC remote command lateral movement
- Block malicious invocation of system tools
- Block PowerShell/CMD malicious parameter execution
- Block malicious creation/modification of scheduled tasks
- Block suspicious DLL injection into process memory (Enhanced)
- Block remote injection and process parasitism (Enhanced)

System Runtime Control (10 rules):

- Protect volume shadow copies from malicious deletion
- Real-time intercept high-entropy encrypted suspicious files
- Prevent malicious Hosts file tampering
- Prevent malicious system time modification
- Protect critical system configuration from tampering
- Block abnormal disk unmounting and formatting
- Real-time block malicious system service disabling
- Block malicious system restore point deletion
- Prevent drive letter and partition permission malicious modification
- Prevent Group Policy critical configuration tampering (Enhanced)

Monitored Directories:

- Desktop, Documents, Downloads
- Pictures, Videos, Music
- OneDrive
- Startup folder
- Contacts, Favorites

Network Resources:

- Mapped network drives (automatically detected)
- Network shares

Trusted Zone (Whitelist)

To reduce false positives, you can add trusted files, directories, or processes to the whitelist. Items in the whitelist are automatically excluded from protection scans. See Section 8.3 for details.

5.6 Blocked File Types

The program blocks files with extensions commonly used by ransomware, including but not limited to:

.wannacry, .locky, .cerber, .zepto, .gandcrab, .ryuk, .revil, .conti, .lockbit, .hive, .blackcat, .blackbyte, .royal, .avaddon, .clon, .pysa, .dharma, .djvu, .stop, .enigma, .cryptolocker, .cryptowall, .cry, .ncry, .encrypted, .encrypt, .ransom, .filelock, .crypt, .cryptor, .btc, .bitcoin, .locked

And many more. The list is continuously updated.

5.7 Stopping Protection

To stop protection:

1. Navigate to the Protection page
2. Click the red Stop Protection button

Note: Stopping protection leaves your system vulnerable. Only stop if necessary.

6. Hardening Module

6.1 Overview

System Hardening applies 32 comprehensive security measures to strengthen your Windows system against attacks. These measures follow industry-standard security guidelines (CIS benchmarks and NSA recommendations).

Network Security: Block dangerous ports, disable vulnerable protocols

Service Hardening: Disable high-risk services

System Hardening: Enable DEP, ASLR, CFG, SEHOP, etc.

Account Policy: Enable UAC, password complexity, auto lock screen

Permission Management: Lock critical files and directories

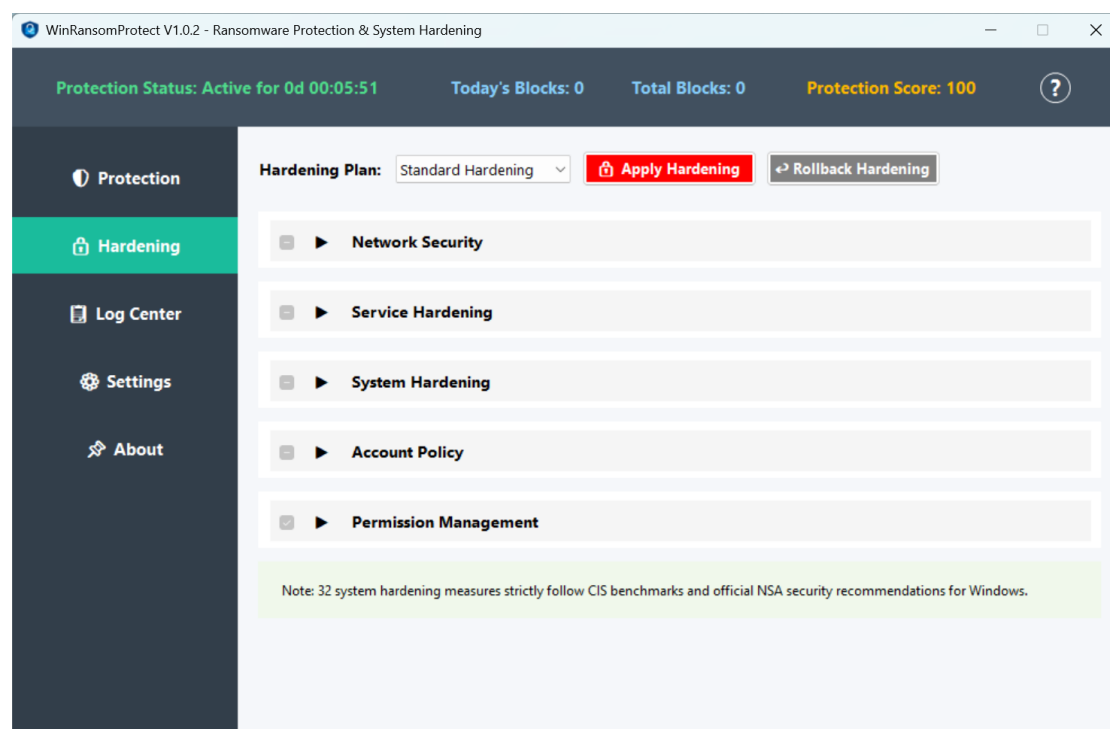


Figure 8: System Hardening Page

6.2 Hardening Plans

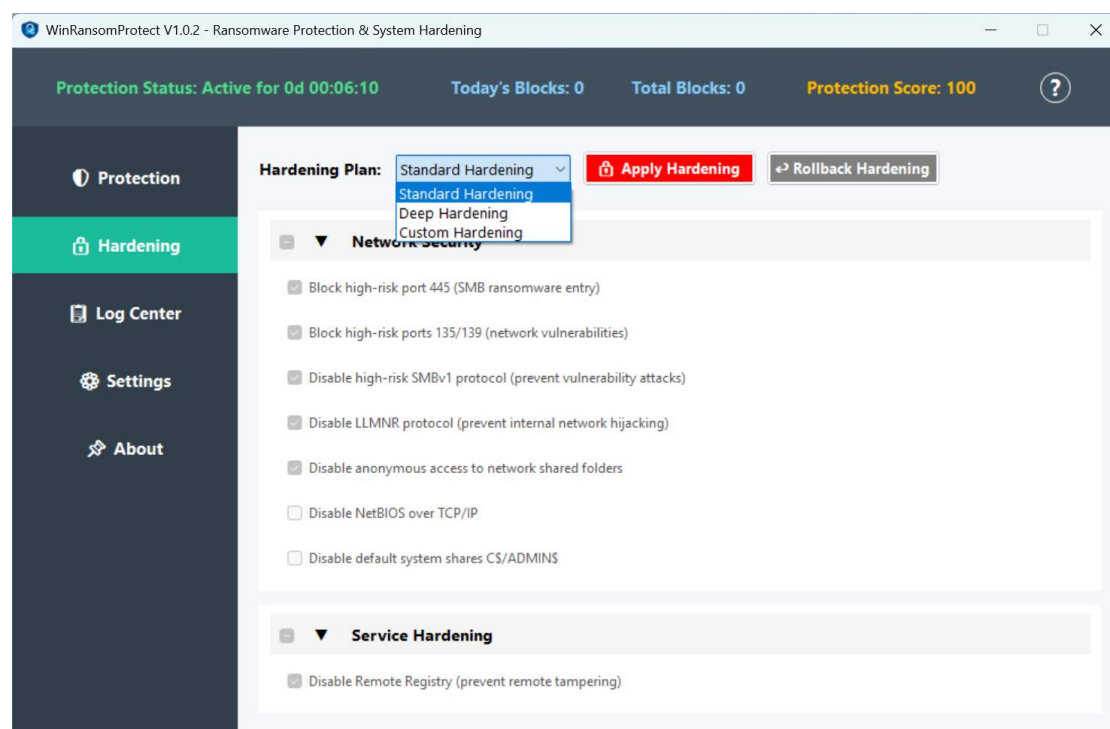


Figure 9: Hardening Plans

Standard Hardening: Essential security measures across 5 categories (24 items). Safe for all systems. Recommended for most users.

Deep Hardening: Maximum security across all 32 items (includes NetBIOS disabling, default shares disabling, WSH disabling, SAM enumeration disabling, password complexity, auto lock screen, and more). May affect some applications. Recommended for advanced users or high-security environments.

Custom Hardening: Full control over individual hardening items. Lets you select exactly which security measures to apply.

6.3 Applying Hardening

To apply hardening:

1. Navigate to the Hardening page
2. Select a hardening plan from the dropdown menu
3. Click the red Apply Hardening button
4. Review the **confirm Hardening** dialog and click **Yes**

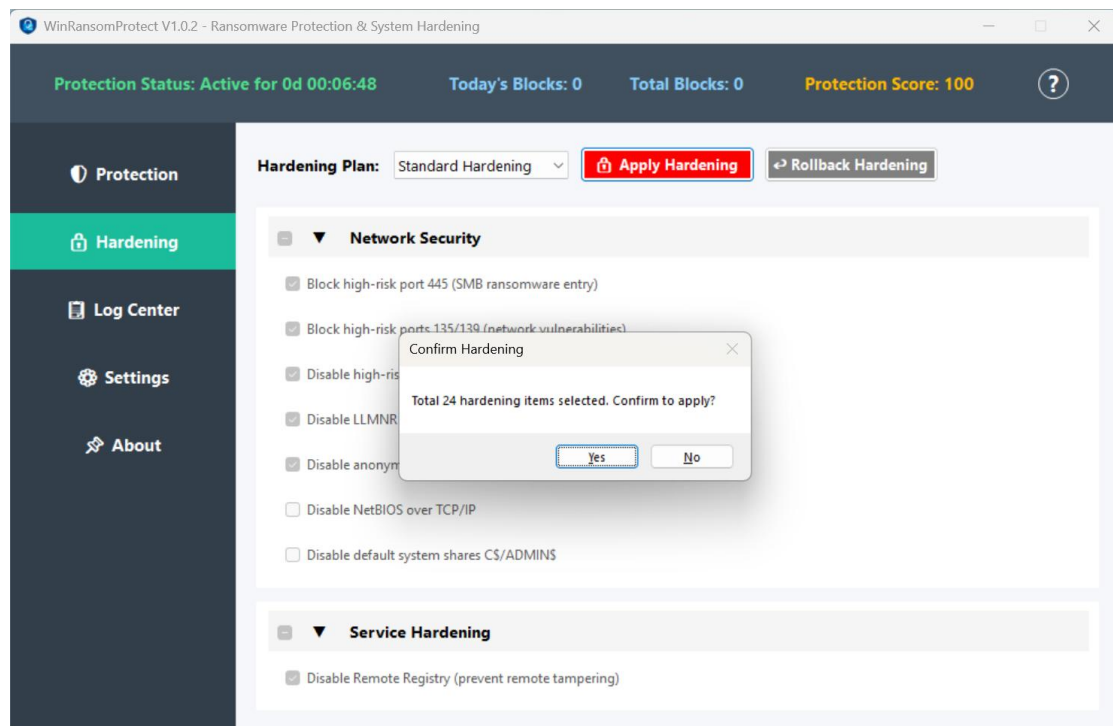


Figure 10: Confirm Hardening dialog

5. Review the **Stop Protection** dialog and click **Yes**

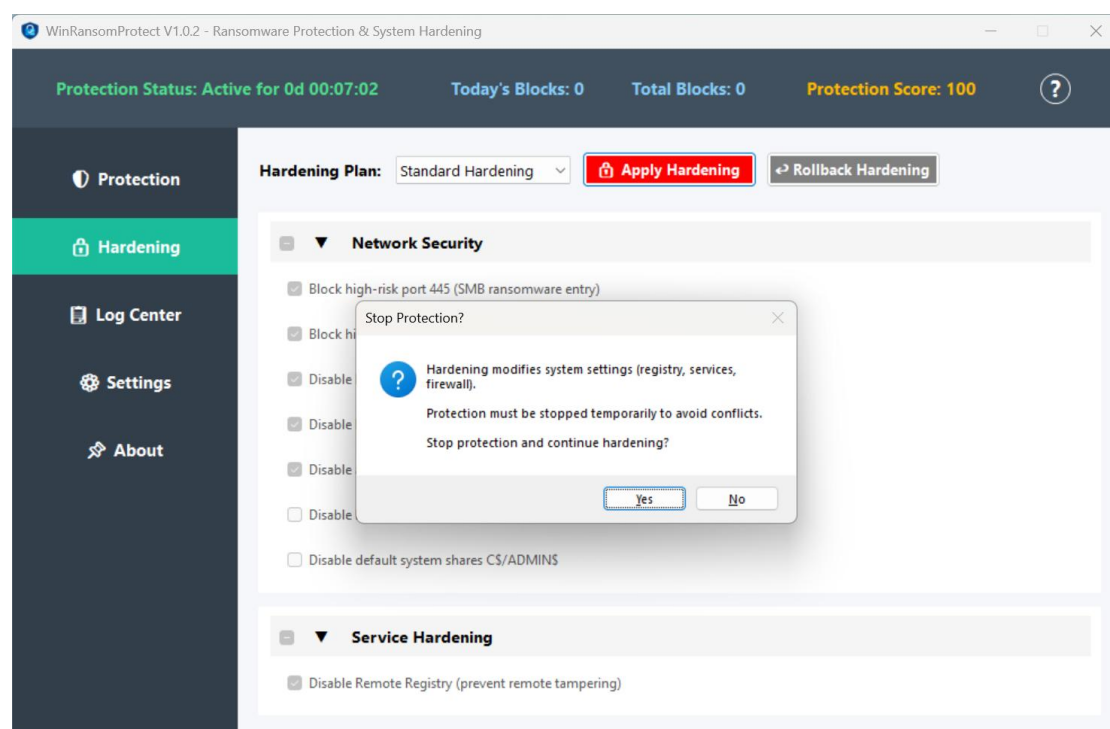


Figure 11: Stop Protection dialog

Important: Protection is automatically stopped during hardening

When you apply hardening, the program will temporarily stop protection to avoid conflicts with system modifications. After the hardening process completes:

- **If no restart is required:** Protection is automatically restored.
- **If a restart is required and you choose "No":** Protection is automatically restored.
- **If you choose "Yes" to restart:** The system will restart immediately to apply the hardening changes. After reboot, you need to manually launch WinRansomProtect and click Start Protection to resume protection.

During the process:

- A progress bar shows the status
- Each hardening item is applied sequentially
- The operation may take a few minutes

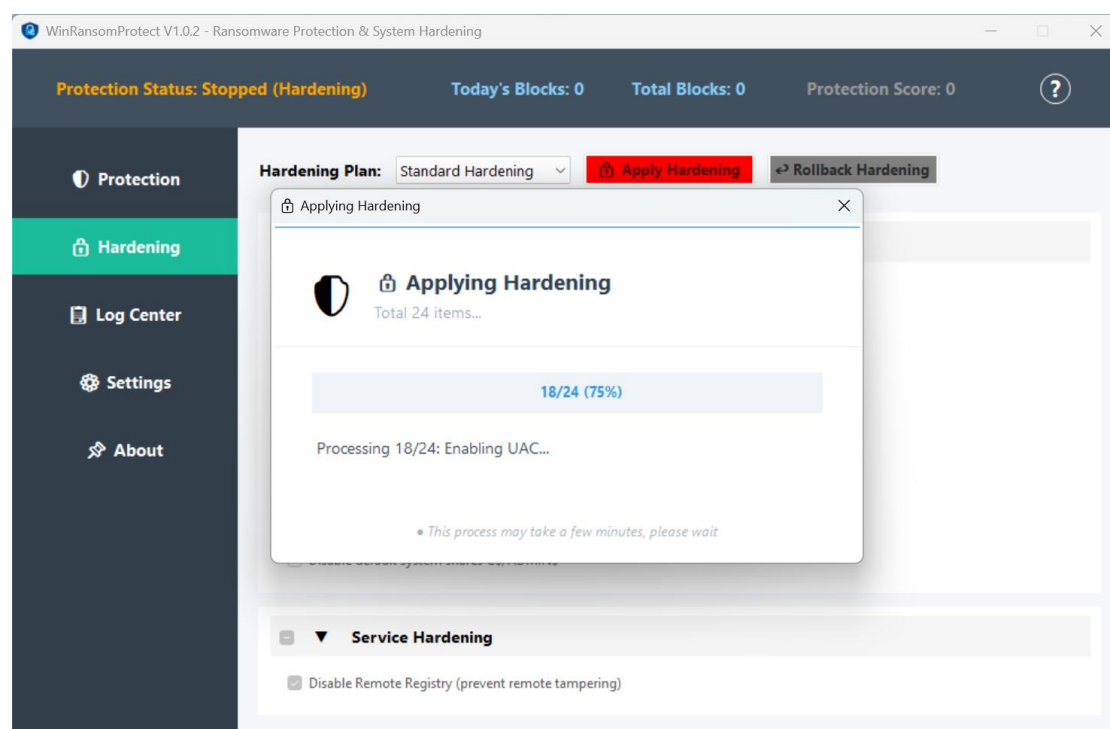


Figure 12: Hardening Progress Indicator

Once the hardening process completes, a summary dialog will appear showing the results.

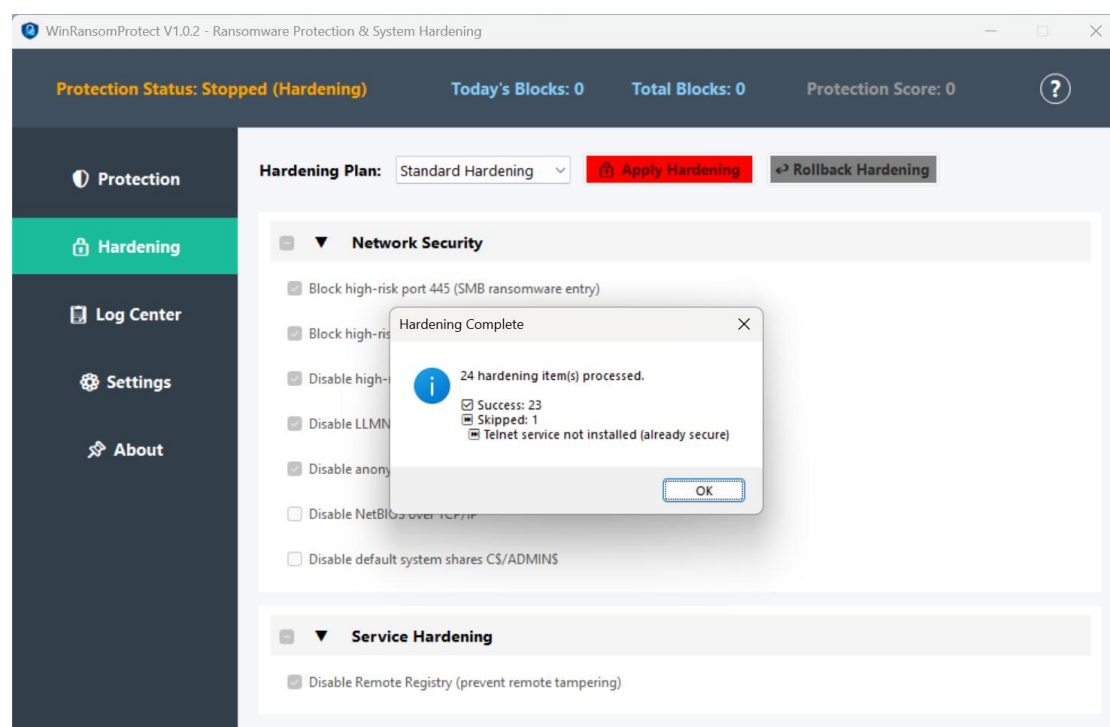


Figure 13: Hardening Completion Results

After Hardening completes, you will see:

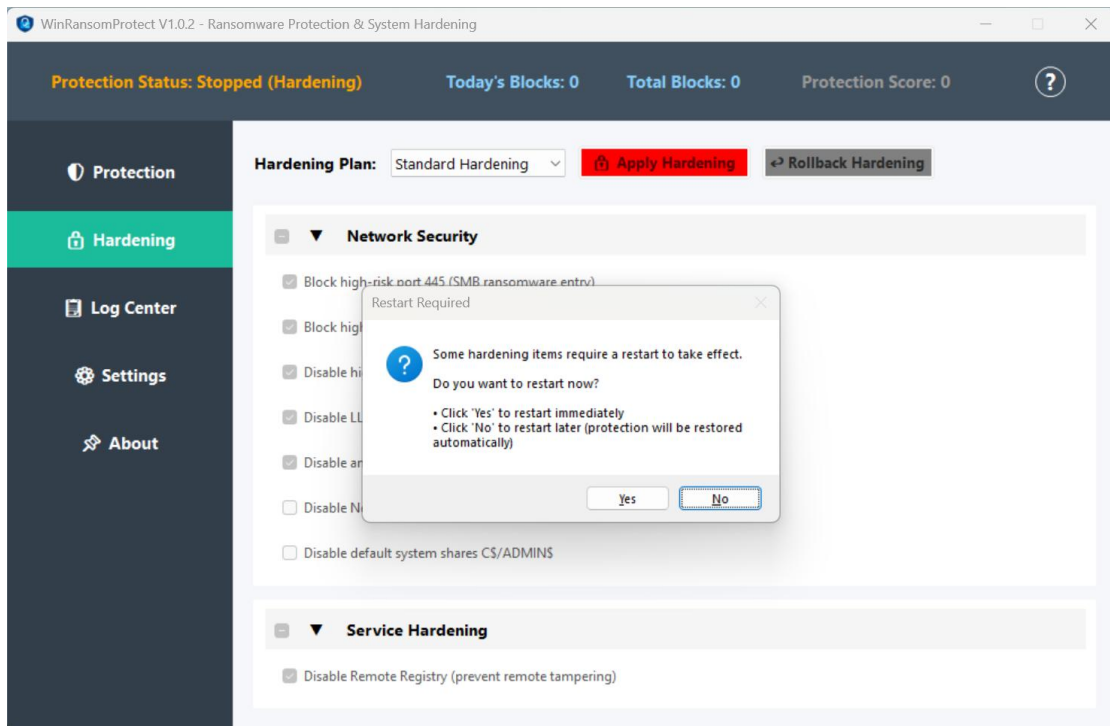


Figure 14: Restart Required Dialog

Some hardening items require a restart to take effect.

Do you want to restart now?

- Click 'Yes' to restart immediately
- Click 'No' to restart later"

Yes: System restarts immediately. After reboot, launch the program and click **Start Protection** to resume protection.

No: Program continues running. Protection is automatically restored, but hardening and rollback operations are blocked until you restart your computer.

6.4 Rolling Back Hardening

If a hardening measure causes issues, you can roll it back:

To roll back:

1. Click the gray Rollback Hardening button
2. Select a time point to roll back to
3. Confirm to restore previous settings

Important: Protection is automatically stopped during rollback

Similar to applying hardening, the program will temporarily stop protection during rollback operations to avoid conflicts. After the rollback completes:

- **If no restart is required:** Protection is automatically restored.
- **If a restart is required and you choose "No":** Protection is automatically restored.
- **If you choose "Yes" to restart:** Protection will resume automatically after the system reboots and you manually start the program.

You do not need to manually start protection after rollback—the program handles this automatically.

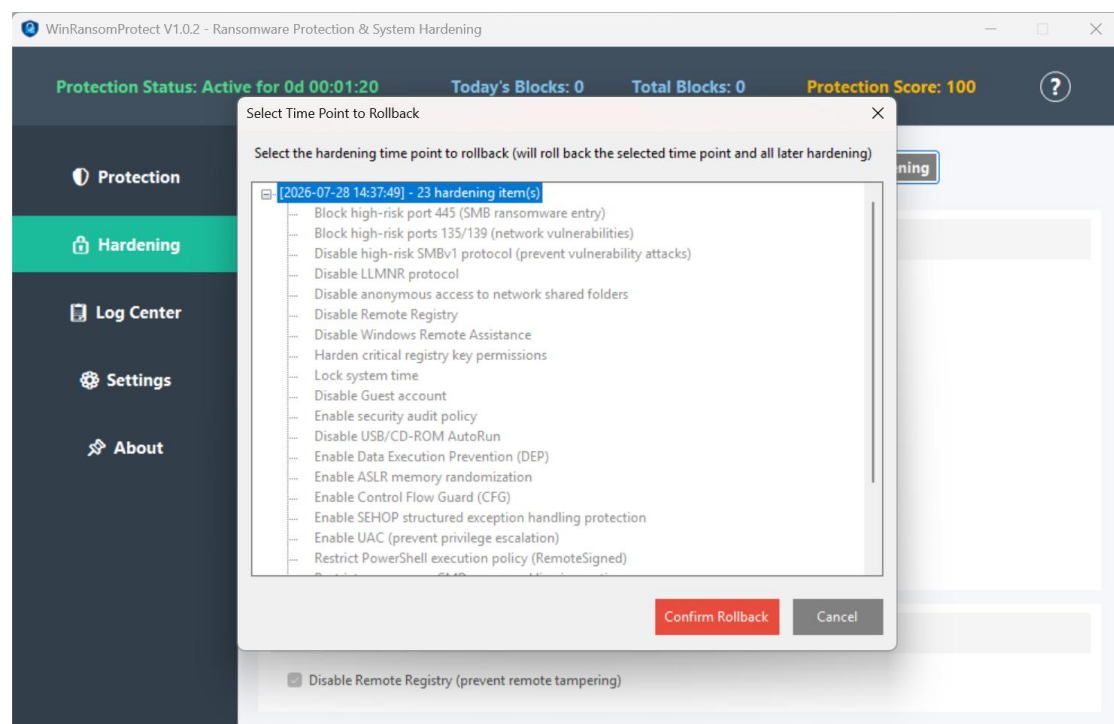


Figure 15: Rollback Selection Dialog

After selecting a restore point, a confirmation dialog appears. Click **Yes** to confirm the rollback operation.

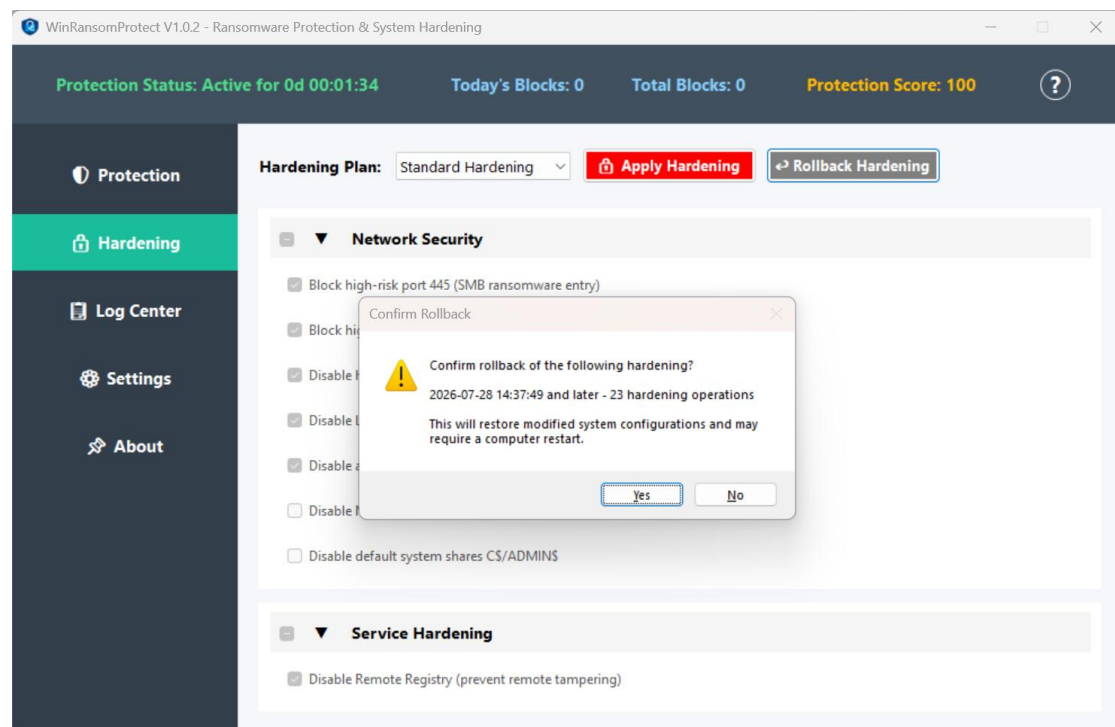


Figure 16: Rollback Confirmation Dialog

Review the **Stop Protection** dialog and click **Yes**

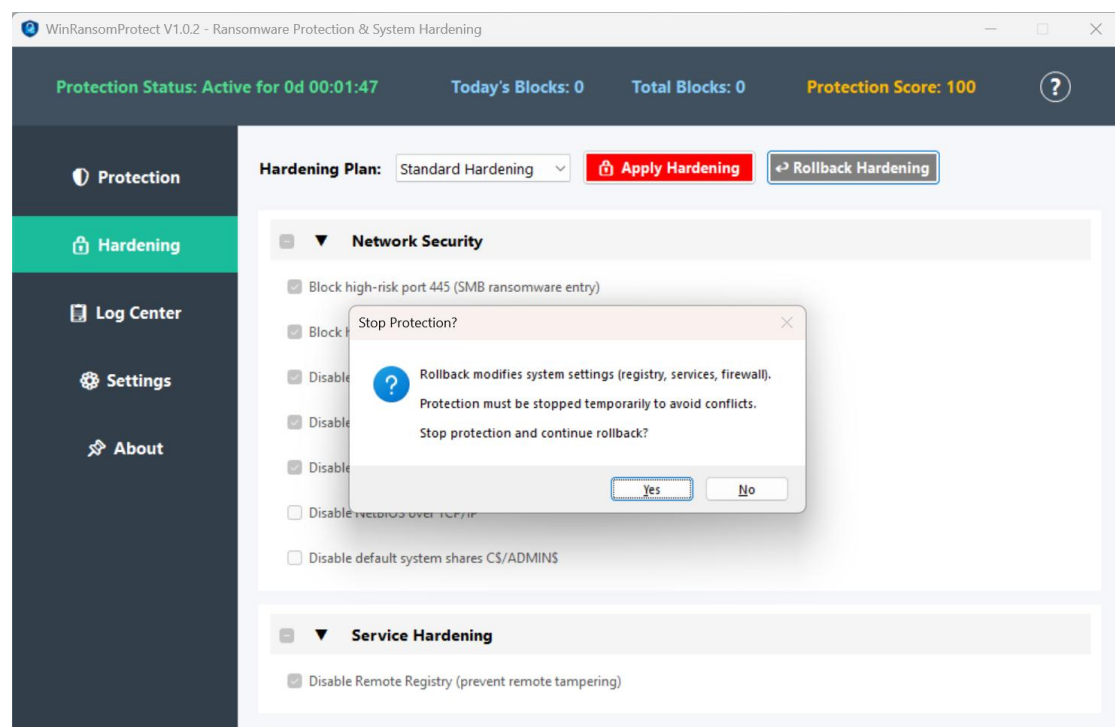


Figure 17: Stop Protection dialog

Important: Protection is automatically stopped during rollback

When you roll back hardening, the program will temporarily stop protection to avoid conflicts with system modifications. After the rollback process completes:

- **If no restart is required:** Protection is automatically restored.
- **If a restart is required and you choose "No":** Protection is automatically restored.
- **If you choose "Yes" to restart:** The system will restart immediately to apply the rollback changes. After reboot, you need to manually launch WinRansomProtect and click Start Protection to resume protection.

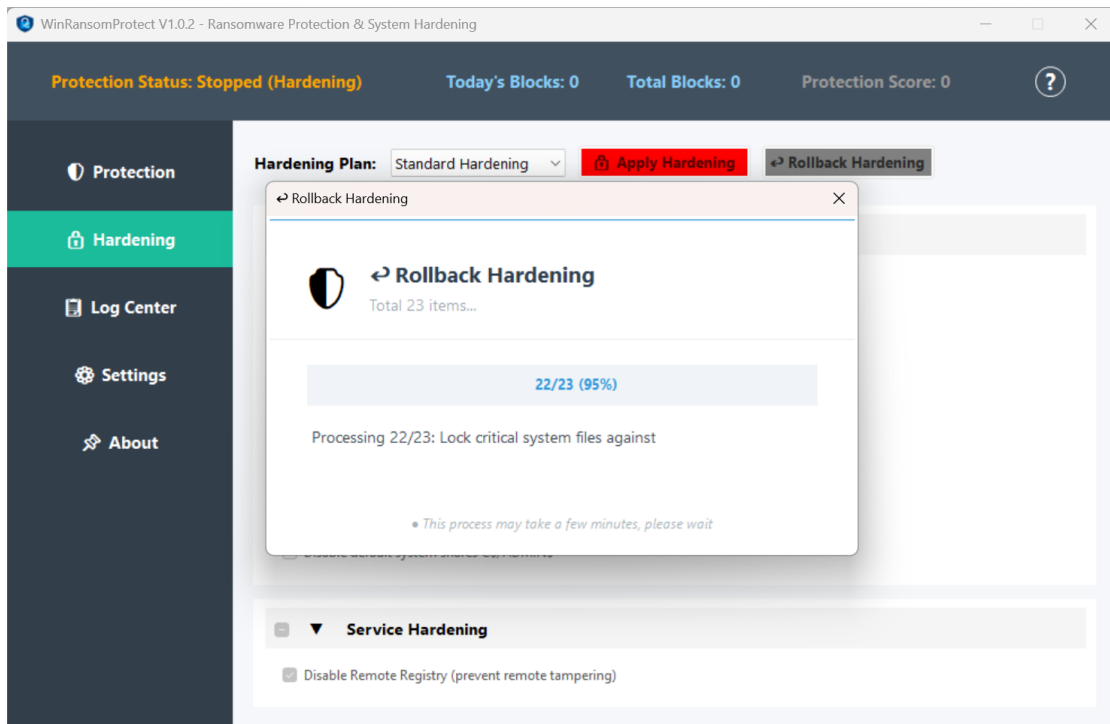


Figure 18: Rollback Progress Indicator

Once the rollback process finishes, a summary dialog shows the outcome, including how many items were successfully restored and whether any errors occurred.

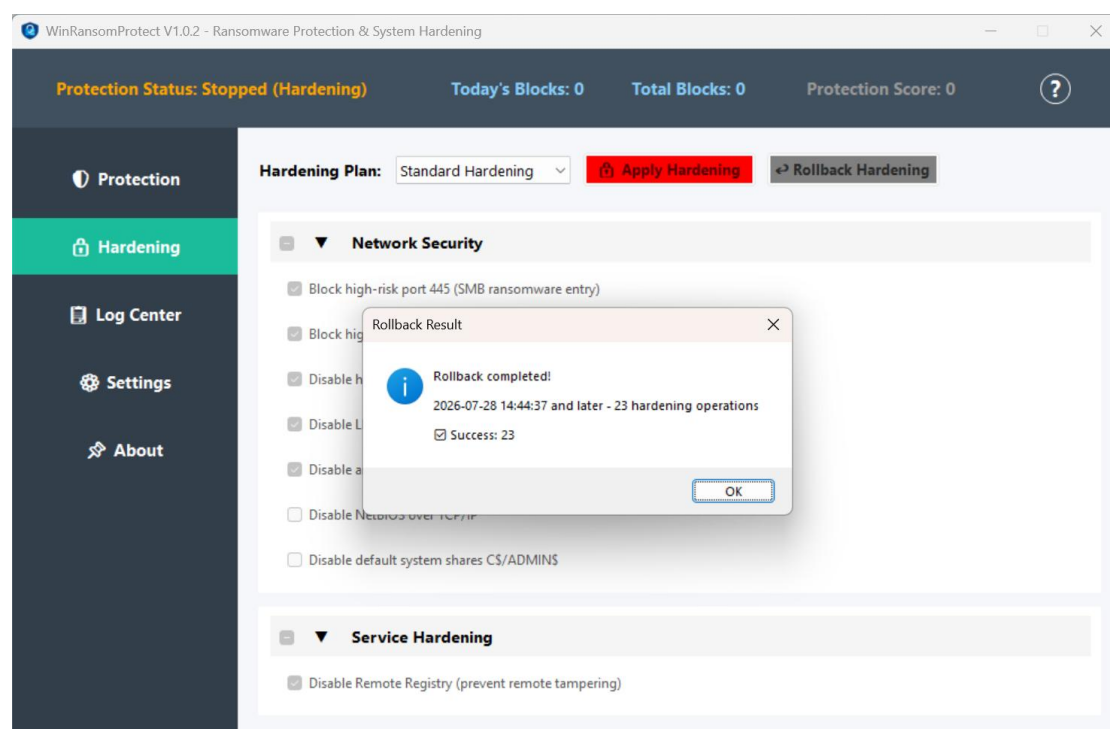


Figure 19: Rollback Completion Results

After rollback completes, you will see:

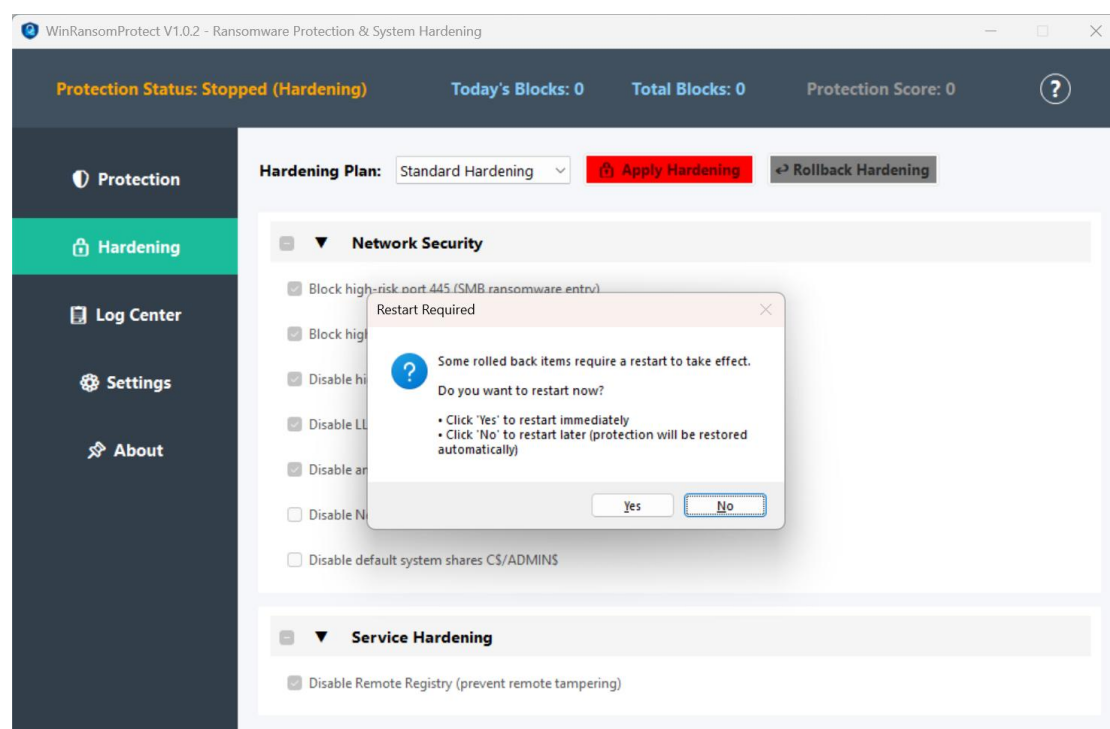


Figure 20: Restart Required Dialog

Some rolled back items require a restart to take effect.

Do you want to restart now?

- Click 'Yes' to restart immediately
- Click 'No' to restart later"

Yes: System restarts immediately. After reboot, launch the program and click **Start Protection** to resume protection.

No: Program continues running. Protection is automatically restored, but hardening and rollback operations are blocked until you restart your computer.

6.5 Pending Restart State

When you choose "No" during the restart confirmation dialog, the program enters a pending restart state:

- **Protection Status:** Displays "Stopped (Hardening)" in orange
- **Hardening/Rollback:** All hardening and rollback operations are blocked
- **Resolution:** Restart your computer to clear this state

The pending restart state is automatically detected and cleared when:

- You restart your computer
- The program detects the system has been rebooted since the pending state was set

Once the system restarts, all hardened items take full effect, and you can perform additional hardening or rollback operations normally.

7. Log Center

7.1 Overview

The Log Center provides detailed records of all protection and hardening events.

7.2 Log Types

Ransomware Protection Log: Real-time protection events. Check what threats were blocked.

System Hardening Log: Hardening operations history. Track what was changed.

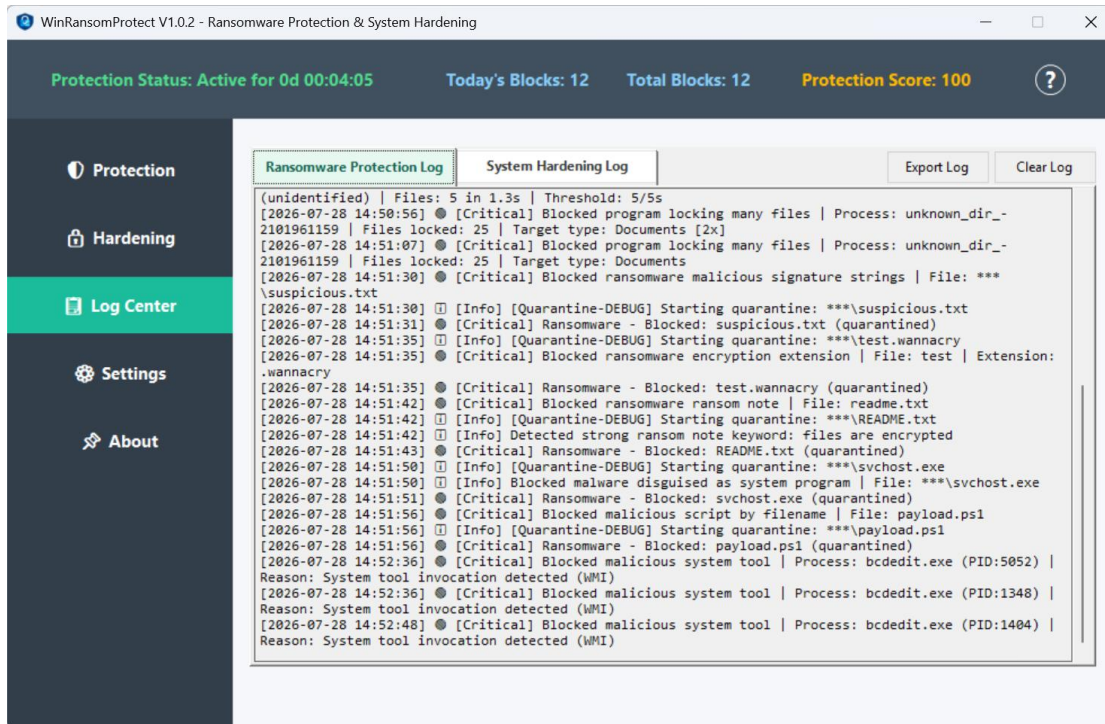


Figure 21: Log Center—Ransomware Protection Log

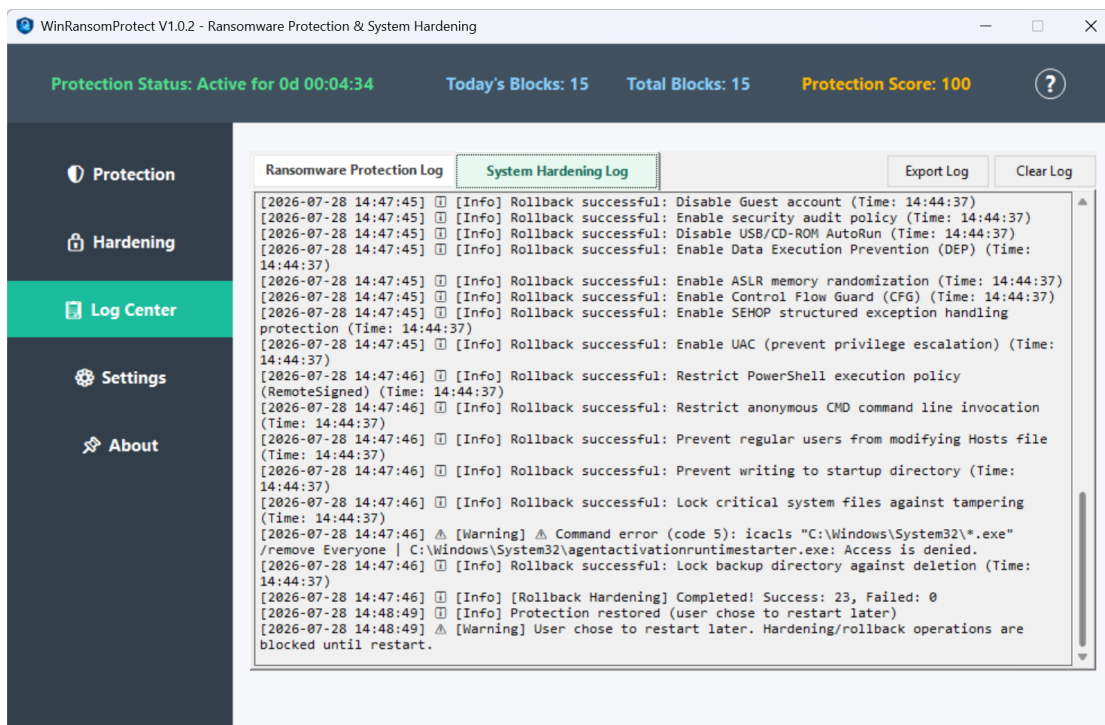


Figure 22: Log Center—System Hardening Log

7.3 Log Entry Format

Each log entry includes:

- Timestamp

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

Color Coding:

Info (Blue): Normal operations

Warning (Yellow): Suspicious activity detected

Error (Red): Operation failed

Critical (Dark Red): Ransomware blocked

7.4 Log Operations

Export Log: Export as TXT or CSV

Clear Log: Clear all entries (cannot be undone)

Auto-scroll: Automatically scrolls to show latest entries

8. Settings & Whitelist

8.1 Basic Settings

Navigate to the Settings page to configure the program.

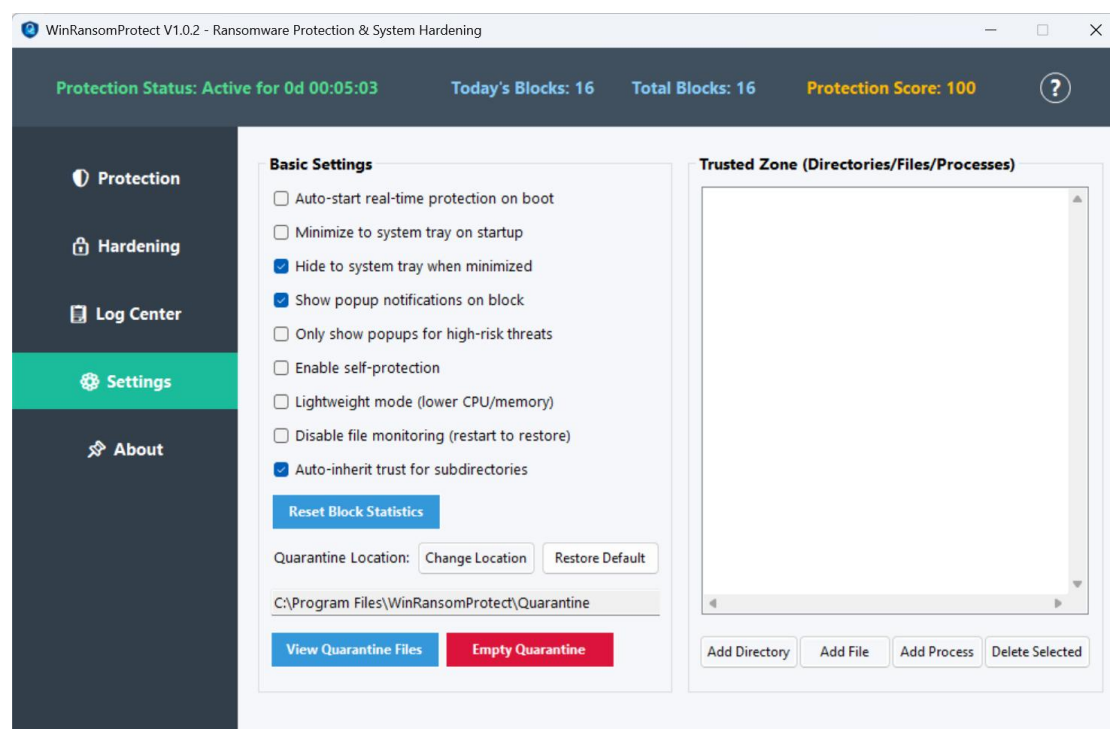


Figure 23: Settings Page

Setting (Default) - Description

Auto-start on boot (Off) - Launch program automatically with Windows
Minimize to tray on startup (Off) - Start program minimized
Hide to tray when minimized (On) - Minimize to system tray instead of taskbar
Show popup notifications (On) - Show alerts when threats are blocked
Only show high-risk alerts (Off) - Only notify for critical threats
Enable self-protection (Off) - Prevent unauthorized termination
Lightweight mode (Off) - Lower CPU/memory usage
Disable file monitoring (Off) - Pause real-time file monitoring
Auto-inherit trust for subdirectories (On) - Trust subdirectories of whitelisted folders

8.2 Quarantine Management

Quarantine Location:

- A dedicated folder where suspicious files are safely stored
- You can change this location in Settings

Operations:

Change Location: Select a new quarantine folder
Restore Default: Reset to default location
View Quarantine Files: Open in Windows Explorer
Empty Quarantine: Permanently delete all quarantined files

8.3 Whitelist (Trusted Zone)

Add trusted items to prevent false positives.

Types of Whitelist Entries:

File: Trust a specific file (e.g., C:\Tools\my_script.exe)
Directory: Trust a folder (and optionally subfolders)
Process: Trust an executable by name (e.g., my_app)

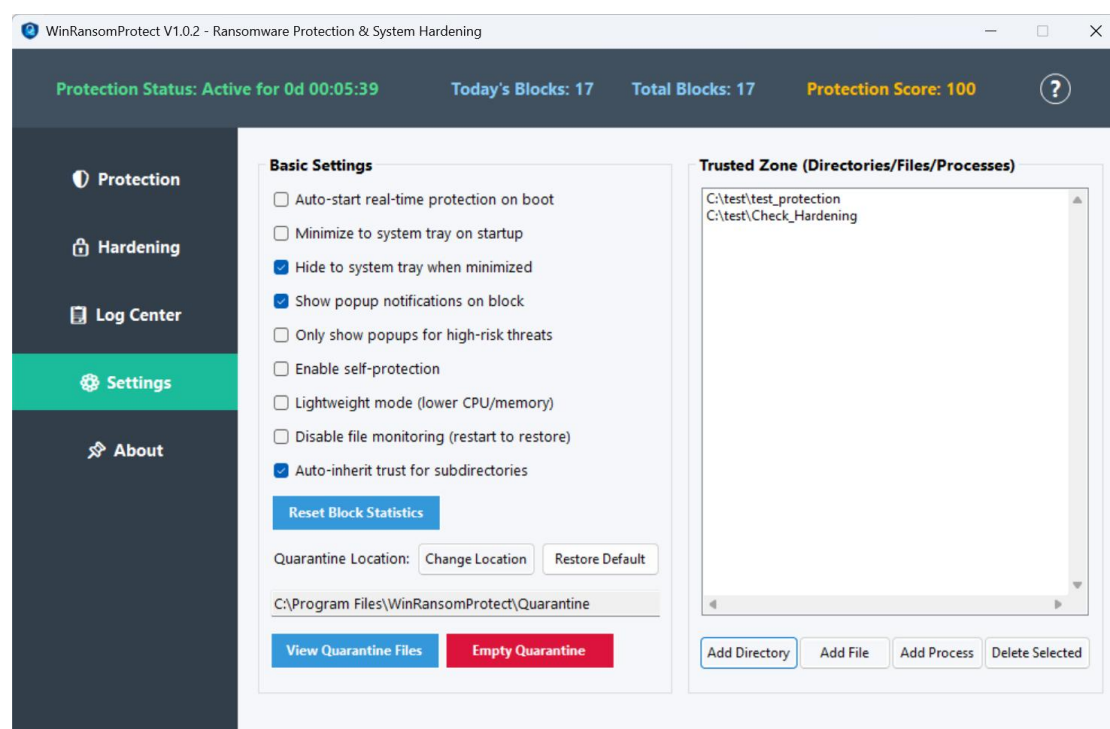


Figure 24: Whitelist Management

How to Add Items:

1. Click the appropriate button:
 - Add File — Browse and select files
 - Add Directory — Browse and select folders
 - Add Process — Enter process name (no .exe extension)
2. The item appears in the list

How to Remove Items:

- Select: Click or Ctrl+Click to select multiple items
- Delete: Press the Delete key or click Delete Selected
- Clear All: Right-click -> Clear All

How Subdirectory Trust Works:

Auto-inherit trust for subdirectories (On): All subdirectories are automatically trusted

Auto-inherit trust for subdirectories (Off): Only the exact directory is trusted

9. System Tray

9.1 Accessing the System Tray

When WinRansomProtect is running, an icon appears in the system tray (near the clock).

Actions:

Double-click: Restore the main window

Right-click: Open the context menu

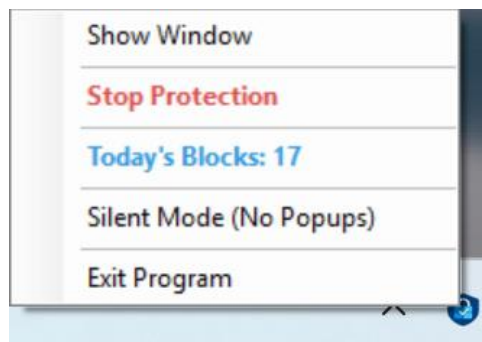


Figure 25: System Tray Context Menu

9.2 Tray Menu Options

Show Window: Restore the main window

Start/Stop Protection: Toggle real-time protection on/off

Today's Blocks: Show number of blocks today (read-only)

Silent Mode (No Popups): Toggle popup notifications on/off

Exit Program: Close WinRansomProtect

9.3 Silent Mode

When Silent Mode is enabled:

- Protection continues running
- Threats are still blocked
- No popup notifications are shown

Tip: Enable Silent Mode if you find notifications distracting, but still want protection.

10. Troubleshooting

10.1 Common Issues

"Program already running"

Issue: A message says "Program already running, please do not open again!"

Solution:

- Check the system tray for the WinRansomProtect icon
- If found, the program is already running
- If not found, it may be hidden. Restart your computer.

"Please run this program as administrator"

Issue: The program says it needs administrator privileges.

Solution:

1. Right-click WinRansomProtect.exe
2. Select Run as administrator
3. Click Yes when prompted by UAC

"No protection items selected"

Issue: Cannot start protection because no rules are selected.

Solution:

1. Navigate to the Protection page
2. Select Standard Protection plan, or
3. Select Custom Protection and manually check at least one rule
4. Try starting protection again

Hardening operation fails

Issue: The hardening operation fails with an error.

Possible Causes & Solutions:

Not running as admin -> Run as administrator

Windows feature missing -> Install required Windows features

Permission denied -> Check user permissions

System files locked -> Close other programs and retry

To diagnose:

1. Check the Hardening Log for error messages
2. Note which specific item failed
3. Contact support with the error details

Files not being quarantined

Issue: Suspicious files are detected but not quarantined.

Possible Causes & Solutions:

File is in use by another program -> Close the program and try again

File is in a whitelisted location -> Check whitelist settings

Quarantine folder inaccessible -> Check folder permissions

Protection is stopped -> Start protection

10.2 Reporting a Bug

To help us fix issues quickly, please include:

1. Version: Check the About page
2. Windows Version: Windows 10 or 11?
3. Steps to Reproduce: What did you do?
4. Expected Result: What should have happened?
5. Actual Result: What actually happened?

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

11. Frequently Asked Questions

Q1: Is WinRansomProtect compatible with other antivirus software?

A: Yes, WinRansomProtect is designed to work alongside existing antivirus solutions. It focuses specifically on ransomware protection and system hardening, complementing traditional antivirus software.

Q2: Will WinRansomProtect slow down my computer?

A: The program uses minimal system resources. For lower resource usage, enable Lightweight Mode in Settings.

Resource usage typically:

- CPU: < 1% (idle)
- Memory: ~50-100 MB
- Disk: Minimal

To enable Lightweight Mode:

1. Navigate to Settings
2. Check "Lightweight mode (lower CPU/memory)"
3. The change takes effect immediately

Q3: What should I do if I get a false positive?

A: Add the false positive to the whitelist:

1. Navigate to Settings -> Whitelist
2. Add the file, directory, or process
3. The program will ignore it in the future

Q4: Can I run WinRansomProtect without administrator privileges?

A: No. Administrator privileges are required for:

- Real-time file monitoring
- Process protection
- System hardening
- Registry protection

Q5: What happens to quarantined files?

A: Quarantined files are:

1. Copied to the quarantine folder
2. Removed from their original location
3. Stored safely for potential recovery

To restore: Move the file back manually from the quarantine folder.

Q6: What is the difference between Standard, Enhanced, and Custom Protection?

A: WinRansomProtect offers three protection plans:

Standard Protection includes 24 pre-configured rules covering essential ransomware defenses with minimal false positives. It is recommended for most users.

Enhanced Protection includes all 30 rules, adding advanced behavioral analysis for maximum security. It may increase false positives and is best suited for advanced users or high-risk environments.

Custom Protection allows you to manually enable or disable individual rules, giving you full control over what threats to monitor. It is designed for power users who want fine-tuned protection.

Q7: Does WinRansomProtect offer different hardening levels?

A: Yes. WinRansomProtect provides three hardening plans:

Standard Hardening includes 24 essential security measures across 5 categories. It is safe for all systems and recommended for most users.

Deep Hardening applies all 32 hardening measures for maximum security. It may affect some applications and is recommended for advanced users.

Custom Hardening lets you manually select individual hardening measures for full control.

All hardening measures follow CIS benchmarks and NSA security recommendations.

Q8: Can I use the program on multiple computers?

A: Each license key is one-machine-one-code and cannot be transferred between computers. Each computer requires its own license.

Q9: Does the program work on Windows 10/11 Home edition?

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

Q10: Will the program protect me from zero-day ransomware?

A: Yes. WinRansomProtect uses behavioral analysis to detect ransomware-like activity, which is effective against zero-day and unknown ransomware variants.

12. Contact & Support

12.1 Contact Information

Website: <https://www.nisse-sec.com>

Email: support@nisse-sec.com

Update Check: Click "Check Update" on the About page

12.2 License & Purchase

To purchase a license or renew an existing one:

1. Visit our website: <https://www.nisse-sec.com>
2. Complete your order
3. Receive your transaction ID via email
4. Email your transaction ID + machine code to support@nisse-sec.com

12.3 Disclaimer

For legitimate security use only. Any unauthorized use is strictly prohibited. Users assume sole liability for any misuse.

WinRansomProtect is designed to protect against ransomware and malware threats. While we strive for 100% effectiveness, no security software can guarantee complete protection. Always maintain regular backups of your important data.