Nisse-Sec

WinRansomProtect V2.1

User Guide

Offline Anti-Ransomware

Date: Oct 8, 2026

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

Website: 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....5
2. System Requirements....5
2.1 Minimum Requirements....5
2.2 Recommended Requirements....5
3. Installation....5
3.1 Installation Steps....5
3.2 First Launch....6
3.3 Uninstallation....6
4. License & Activation....6
4.1 License Types....7
4.2 Finding Your Machine Code....7
4.3 Getting a License Key....7
4.4 Activating Your License....8
4.5 License Status Display....9
4.6 What Happens When License Expires?....10
5. Protection....10
5.1 Select a Protection Plan....10
5.2 Start Protection....11
5.3 Stop Protection....11
5.4 Protection Status Indicators....12
5.5 Protection Rules....12
5.6 Monitored Locations....14
5.7 Blocked File Types....14
6. Block Log....14
6.1 Log Entry Format....15

6.2 Log Operations 15
7. Settings 15
7.1 Basic Settings 16
7.2 Trusted Zone (Whitelist) 17
8. System Tray 18
8.1 The Tray Icon 18
8.2 Tray Menu Options 18
9. Troubleshooting 19
9.1 Files Not Being Quarantined 19
9.2 Reporting a Bug 19
10. Frequently Asked Questions 19
Q1: Is WinRansomProtect compatible with other antivirus software? 19
Q2: What should I do if I get a false positive? 19
Q3: Can I run WinRansomProtect without administrator privileges? 20
Q4: What happens to quarantined files? 20
Q5: What is the difference between Standard, Enhanced, and Custom Protection? 20
Q6: Can I use the program on multiple computers? 20
Q7: Does the program work on Windows 10/11 Home edition? 20
Q8: Will the program protect me from zero-day ransomware? 20
11. Contact & Support 21
11.1 Contact Information 21
11.2 License & Purchase 21
11.3 Disclaimer 21

1. Introduction

1.1 What is WinRansomProtect?

WinRansomProtect V2.1 is a ransomware protection tool for Windows. It uses signature detection and behavior analysis to protect your files from ransomware and other malware. Everything runs locally on your computer. It does not send your data anywhere and works without an internet connection.

Getting started is simple: pick a protection plan, click **Start Protection**, and it runs quietly in the background.

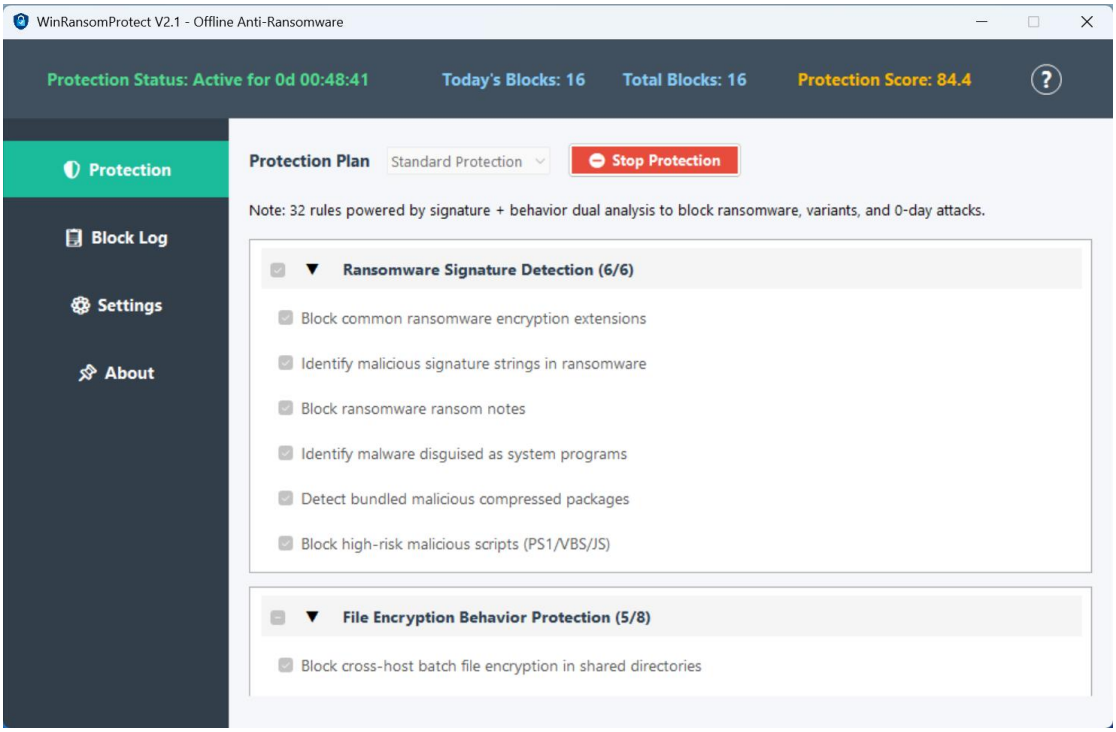


Figure 1: WinRansomProtect Main Window

1.2 Key Features

- Real-time protection: Watches files and processes using 32 detection rules.
- Works offline: No cloud, no data upload, no internet needed.
- Live dashboard: Shows protection status, block counts, and security score.
- Detailed logs: Every blocked event is recorded.
- Whitelist: Exclude trusted files, folders, and processes from scanning.
- License activation: One machine, one code. 14-day trial included.

1.3 How It Works

WinRansomProtect checks for ransomware in four ways:

1. File monitoring: Watches your Desktop, Documents, Downloads, and other important folders.
2. Process monitoring: Watches running programs for suspicious behavior.
3. Signature detection: Matches known ransomware file extensions and markers.
4. Behavior analysis: Detects abnormal patterns, such as mass encryption or rapid file renaming.

2. System Requirements

2.1 Minimum Requirements

- Operating System: Windows 10 version 1607 or later / Windows 11 (32-bit or 64-bit)
- RAM: 4 GB
- Disk Space: 100 MB
- .NET Runtime: .NET Framework 4.8 or later (pre-installed on Windows 10 1903+ and Windows 11)
- Administrator Rights: Required for installation (to install the background service)
- Internet: Not required for activation (offline by email). Required only for update checks and for .NET Framework installation on systems that don't have it.

2.2 Recommended Requirements

- Operating System: Windows 11 (64-bit)
- RAM: 8 GB or more
- Disk Space: 500 MB or more

3. Installation

3.1 Installation Steps

1. Download WinRansomProtect_Setup_V2.1.exe from our website.
2. Double-click the installer. If Windows asks for administrator permission, click Yes.
3. Follow the on-screen steps. The installer will install two components: the UI and a

background Windows service.

4. After installation, launch WinRansomProtect from the desktop shortcut or Start Menu.

3.2 First Launch

When you run the program for the first time:

Step 1: Background service

The installer already installed and started the WinRansomProtect service. It runs in the background with SYSTEM privileges. You do not need to start it manually.

Step 2: Launch the UI

Double-click the desktop shortcut. The UI connects to the service automatically.

Step 3: Trial period

A 14-day trial starts on first launch. All features are available. No credit card required.

3.3 Uninstallation

Before uninstalling, stop protection and exit the program from the tray icon.

Steps:

1. Open Settings → Apps → Installed apps (or Control Panel → Programs and Features).

2. Find WinRansomProtect in the list.

3. Click Uninstall and follow the prompts.

The uninstaller removes the main program, background service, cached data, and the installation folder.

4. License & Activation

WinRansomProtect includes a 14-day free trial that starts on first launch. All features are available during the trial — no credit card, no registration, no internet required.

To continue using the software after the trial ends, you need a license key. See 4.3 for how to obtain one.

4.1 License Types

Type	Duration	Features
Trial	14 days	Full, no restrictions
1-Year	365 days	Full
Permanent	Unlimited	Full

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

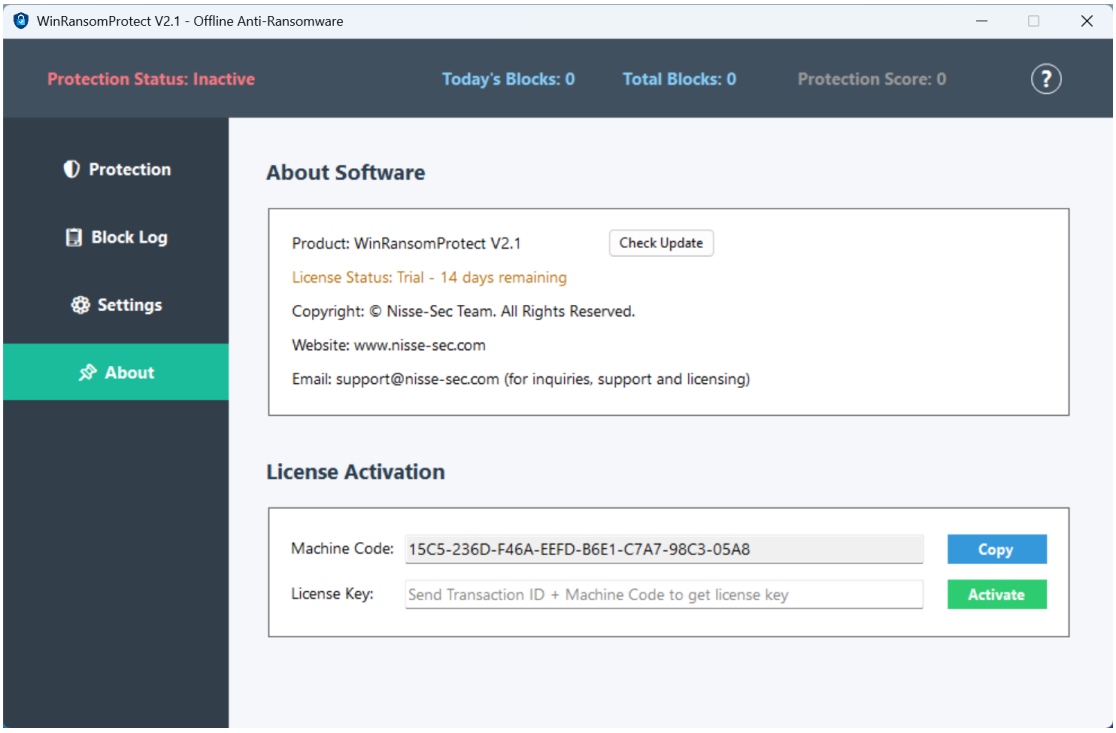


Figure 2: About Page with Machine Code

4.3 Getting a License Key

Activation is done offline by email.

1. Copy your Machine Code (see 4.2).

2. Email it, along with your Transaction ID (shown in your PayPal payment confirmation), to: support@nisse-sec.com

3. You will receive your license key by email.

Once you have the key, proceed to 4.4 Activating Your License.

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

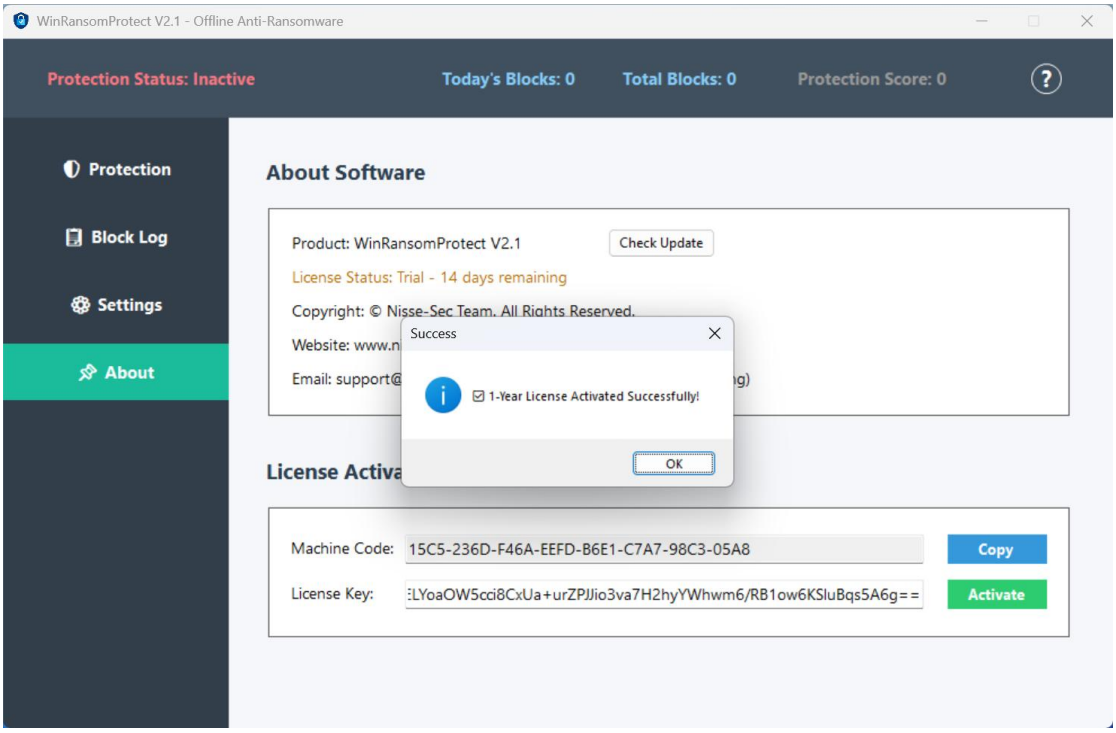


Figure 3: Activating a License

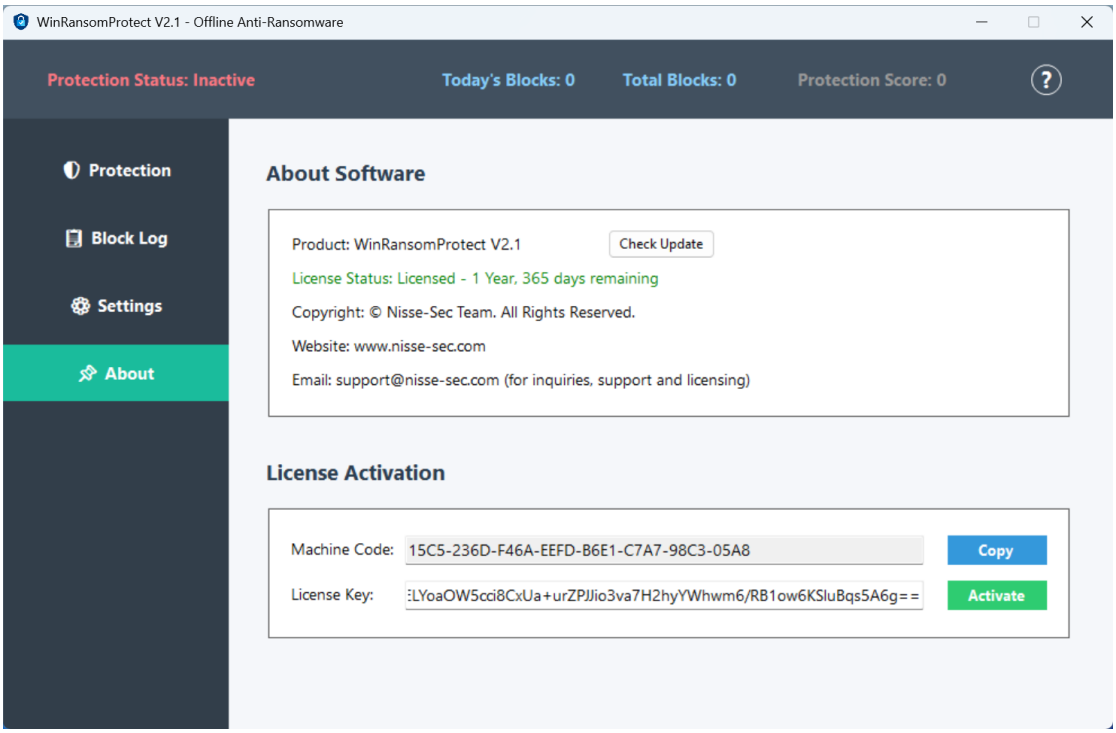


Figure 4: License Status After Activation

Activation Results:

- Success: "1-Year License Activated Successfully!"
- Success: "Permanent License Activated Successfully!"
- Failure: "Invalid license key!" (The key is wrong or incomplete. Check for missing characters.)
- Mismatch: "License key does not match this machine!" (This key was issued for a different computer. Email your current Machine Code to support@nisse-sec.com.)

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:

- Protection stops automatically.
- The Protection, Block Log, and Settings pages are disabled.
- A popup appears, and you are taken to the About page.

To keep using WinRansomProtect, activate or renew your license on the About page.

5. Protection

5.1 Select a Protection Plan

Three protection plans are available: Standard, Enhanced, and Custom. Choose one based on your security requirements.

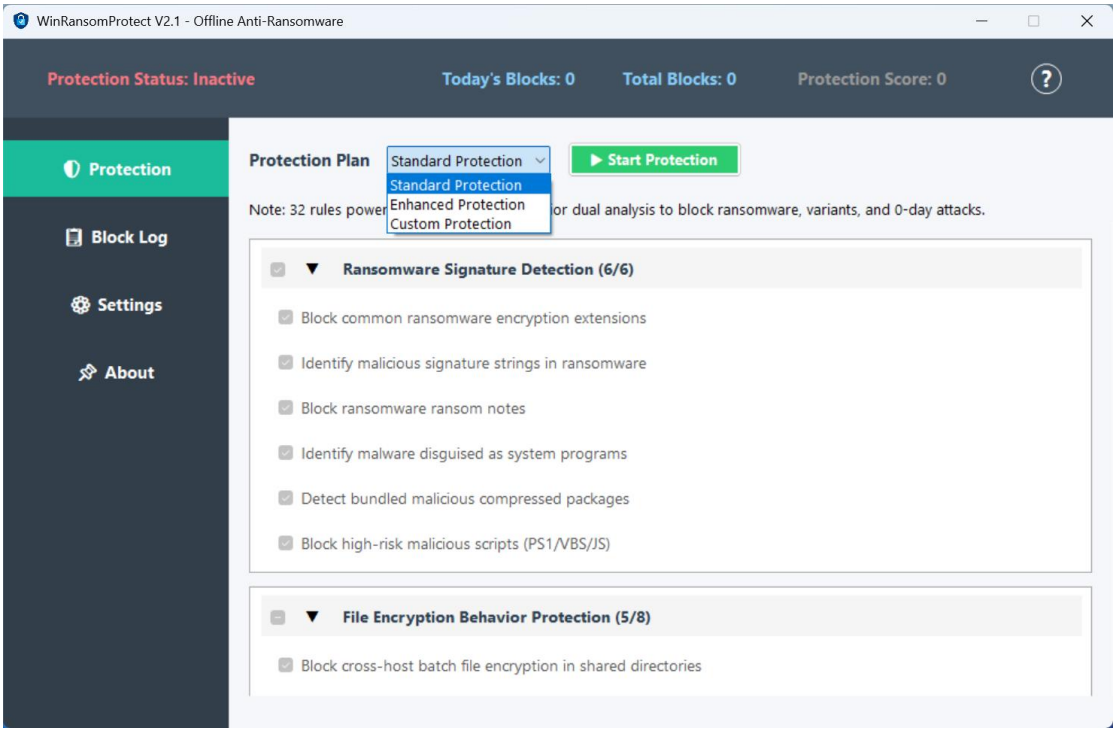


Figure 5: Protection Plan

- **Standard Protection**: 27 rules. Good balance of protection and low false positives. Best for most users.
- **Enhanced Protection**: All 32 rules. Stronger protection, but may produce more false positives. Best for advanced users and high-risk environments.
- **Custom Protection**: Pick any combination of the 32 rules. Best if you want to fine-tune protection yourself.

5.2 Start 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 active:

- The button changes to **Stop Protection**.

- The status bar shows "Active" with an uptime timer.

- The Protection Score reflects your plan: **Standard = 84.4**, **Enhanced = 100**, Custom is calculated from how many rules you enabled.

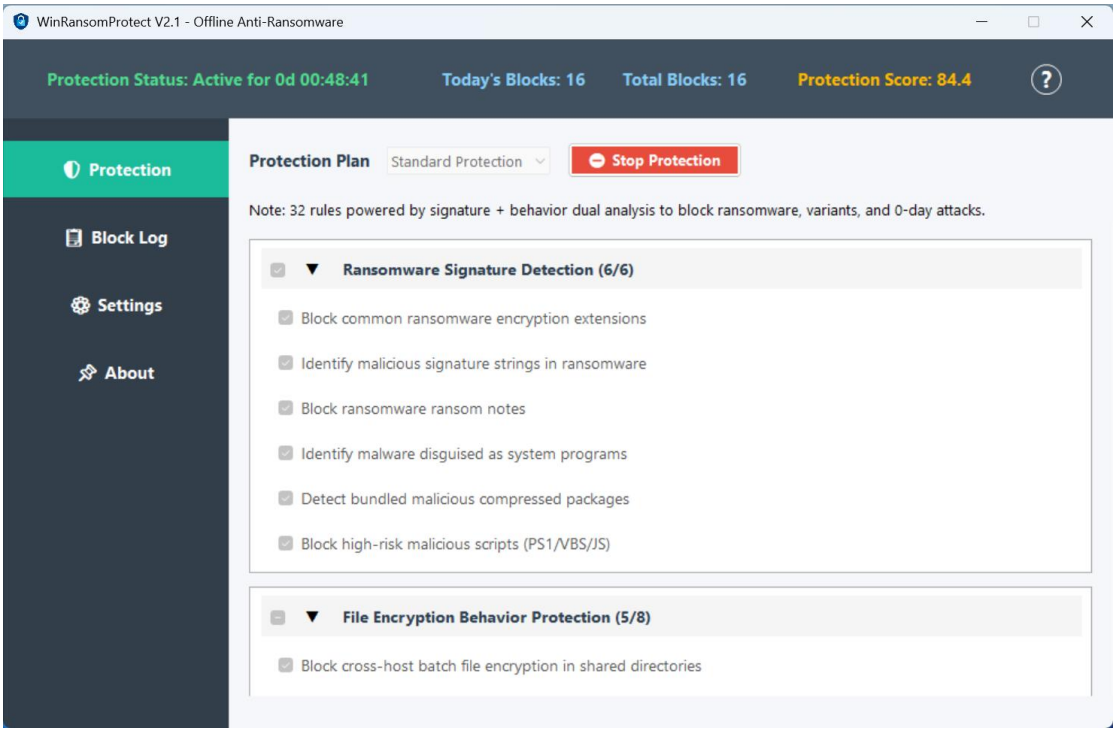


Figure 6: Starting Protection

5.3 Stop Protection

To stop protection:

1. Navigate to the Protection page.

2. Click the **Stop Protection** button.

3. Confirm when prompted.

Once stopped:

- The button changes back to **Start Protection**.
- The status bar shows "Inactive".
- The Protection Score resets to 0.

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

5.4 Protection Status Indicators

The top dashboard shows the following indicators:

- Status:
    - **Active (Green)**: Protection is running.
    - **Inactive (Red)**: Protection is not running.
- **Today's Blocks**: Threats blocked today.
- **Total Blocks**: Cumulative threats blocked since installation.
- **Protection Score**: Real-time score based on your plan: **Standard = 84.4**, **Enhanced = 100**, Custom = calculated from enabled rules.

5.5 Protection Rules

WinRansomProtect has 32 rules across 4 categories. Standard Protection enables 27 of them; rules marked (Enhanced) are only active in the Enhanced and Custom plans.

Ransomware Signature Detection (6 rules):

- Block common ransomware encryption extensions
- Identify malicious signature strings in ransomware
- 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 (may cause false positives, enable cautiously) [Enhanced]

- Monitor high-frequency continuous disk writes (may cause false positives, enable cautiously) [Enhanced]

- Block programs locking a large number of files (may cause false positives, enable cautiously) [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 (may cause false positives, enable cautiously) [Enhanced]

- Block remote injection and process parasitism (may cause false positives, enable cautiously) [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

5.6 Monitored Locations

Monitored Directories:

- Desktop, Documents, Downloads
- Pictures, Videos, Music
- OneDrive
- Startup folder
- Contacts, Favorites, Saved Games
- AppData (Roaming and Local)

Network Resources:

- Mapped network drives (automatically detected)
- Network shares

5.7 Blocked File Types

WinRansomProtect blocks files with extensions commonly used by ransomware, such as:

.wannacry, .locky, .cerber, .zepto, .gandcrab, .ryuk, .revil, .conti, .lockbit, .hive, .blackcat, .blackbyte, .royal, .avaddon, .clop, .pysa .dharma, .djvu, .stop, .enigma, .cryptolocker, .cryptowall, .cry

The list is not exhaustive. Behavior-based detection also covers new ransomware variants that use different extensions.

If a legitimate file or program is being flagged, you can exclude it using the Trusted Zone. See 7.2 Trusted Zone (Whitelist).

6. Block Log

The Block Log provides detailed records of all protection events.

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

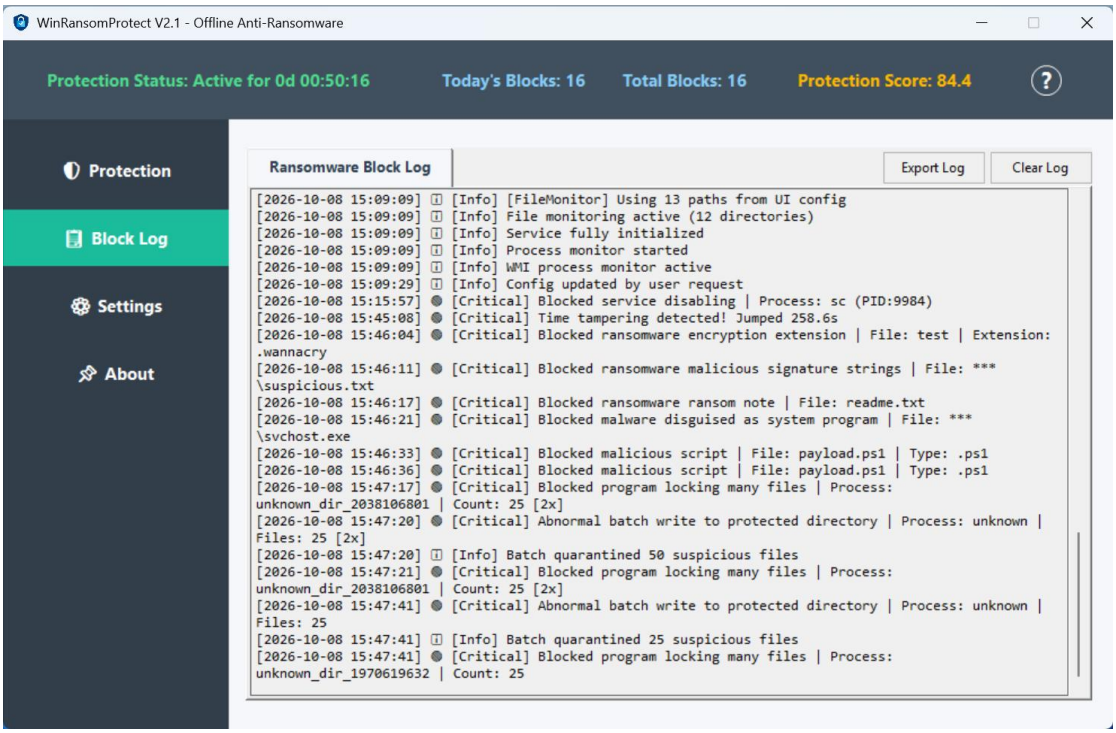


Figure 7: Ransomware Block Log

6.1 Log Entry Format

Each entry shows the time, severity, and event description. Colors:

- **Info (blue)** — normal operations
- **Warning (yellow)** — suspicious activity
- **Error (red)** — operation failed
- **Critical (dark red)** — ransomware blocked

6.2 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

7. Settings

Navigate to the **Settings** page from the left navigation panel. The page is split into two columns:

- **Basic Settings** (left) — configure startup, notifications, quarantine, and

maintenance.

- **Trusted Zone** (right) — manage trusted files, directories, and processes.

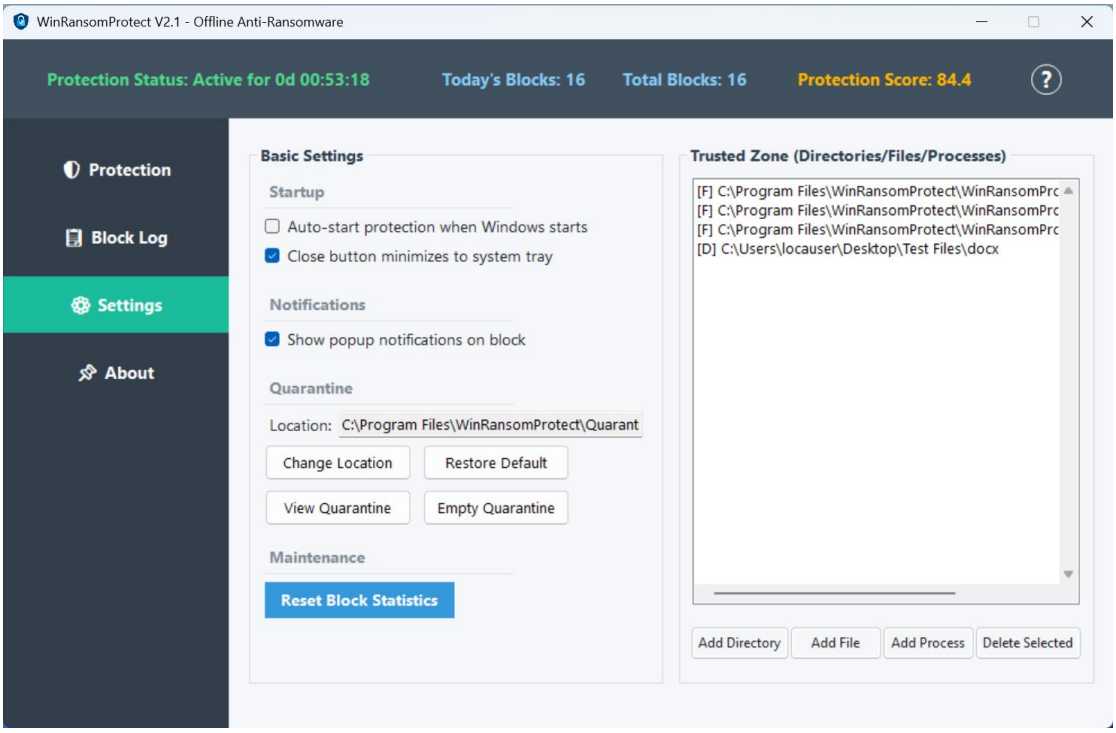


Figure 8: Settings Page (Basic Settings and Trusted Zone)

7.1 Basic Settings

The left column is organized into four groups.

Startup

- Auto-start protection when Windows starts (default: Off)
  Launches the program and starts protection automatically when Windows starts.
- Close button minimizes to system tray (default: On)
  When you click the X button, the window hides to the system tray instead of exiting. The program keeps running in the background.

Notifications

- Show popup notifications on block (default: On)
  Shows a popup in the bottom-right corner when a threat is blocked.

Quarantine

- Location — the folder where suspicious files are stored.
- Change Location — pick a new folder.
- Restore Default — reset to the default quarantine folder.

- View Quarantine — open the quarantine folder in Windows Explorer.
- Empty Quarantine — permanently delete all quarantined files. This cannot be undone.

Maintenance

- Reset Block Statistics — set Today's Blocks and Total Blocks back to 0. This cannot be undone.

7.2 Trusted Zone (Whitelist)

The right column lets you add trusted items so they are not scanned or blocked.

Why use it?

If the program blocks a file you know is safe (a false positive), add it to the Trusted Zone. The program will ignore it from then on.

Types of entries

- File — a specific file, e.g. C:\Tools\my_script.exe
- Directory — a folder (and its subfolders, if enabled)
- Process — a running program, by name, without the .exe extension

Adding an item

1. Click Add Directory, Add File, or Add Process.
2. For a directory or file, browse and select it. For a process, type the name (e.g. my_app).
3. The item appears in the list on the right.

Removing items

- Select one or more — click an item, or hold Ctrl and click to select several.
- Delete — press the Delete key, or click Delete Selected.
- Clear all — right-click the list and choose Clear All.

Notes

- File and directory matching is case-insensitive.
- System directories like C:\Windows and C:\Program Files are trusted by default and do not need to be added.
- Adding a folder does not automatically trust its subfolders unless subdirectory

trust is enabled.

8. System Tray

8.1 The Tray Icon

When WinRansomProtect is running, an icon appears in the system tray (the area at the right end of the taskbar).

Actions:

- Double-click: Restore the main window

- Right-click: Open the context menu

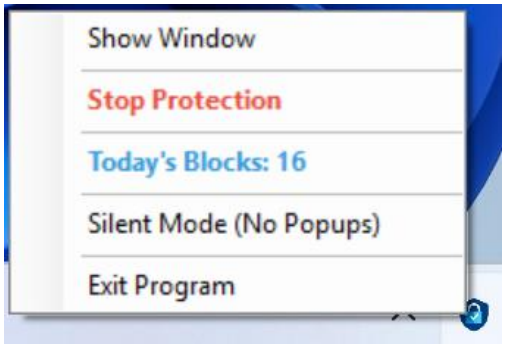


Figure 9: System Tray Context Menu

8.2 Tray Menu Options

- **Show Window** — Restore the main window
- **Start Protection / Stop Protection** — Turn real-time protection on or off. The label changes depending on the current state.
- **Today's Blocks: N** — Number of threats blocked today (read-only)
- **Silent Mode (No Popups)** — Turn popup notifications on or off. When enabled, protection continues running and threats are still blocked, but no popups are shown.
- **Exit Program** —Close WinRansomProtect. If protection is running, you will be asked to confirm.

9. Troubleshooting

9.1 Files Not Being Quarantined

Issue: Suspicious files are detected but not quarantined.

Possible Causes:

1. File is in use — Close the program using it, then try again.

2. File is in a whitelisted location — Check Trusted Zone settings.

3. Quarantine folder inaccessible — Check folder permissions.

4. Protection is stopped — Start protection first.

9.2 Reporting a Bug

To help us fix issues quickly, please include:

1. Version(see the About page)

2. Windows version (Windows 10 or 11)

3. Steps to reproduce

4. Expected result

5. Actual result

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

10. Frequently Asked Questions

Q1: Is WinRansomProtect compatible with other antivirus software?

A: Yes. WinRansomProtect works alongside other antivirus software. It handles ransomware behavior, while traditional antivirus handles known malware. No conflicts have been reported.

Q2: What should I do if I get a false positive?

A: Add the directory, file or process to the Trusted Zone:

1. Navigate to Settings -> Trusted Zone (Whitelist).

2. Add the directory, file or process.

3. The program will ignore it in the future.

Q3: Can I run WinRansomProtect without administrator privileges?

A: The UI runs as a normal user. The background service runs with SYSTEM privileges, which is required for system-level protection. No extra elevation is needed after installation.

Q4: What happens to quarantined files?

A: Suspicious files are copied to the quarantine folder first, then the original is moved to the Recycle Bin. You can restore them from either location.

Q5: What is the difference between Standard, Enhanced, and Custom Protection?

A: WinRansomProtect offers three protection plans:

- **Standard Protection includes 27 pre-configured rules**, covering essential ransomware defenses with minimal false positives.
- **Enhanced Protection includes all 32 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.

Q6: 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.

Q7: Does the program work on Windows 10/11 Home edition?

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

Q8: Will the program protect me from zero-day ransomware?

A: Behavior-based detection can catch zero-day ransomware that has no known signature. No security software can guarantee 100% protection, so keep regular backups.

11. Contact & Support

11.1 Contact Information

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

Email: support@nisse-sec.com

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

11.2 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

5. You will receive your license key by email.

11.3 Disclaimer

WinRansomProtect is intended for legitimate security use only. Misuse is the sole responsibility of the user.

No security software can block every threat. Keep regular backups of important data.