

DEVIL-GUARD NETWORK MONITOR

Installation & User Manual

Version 1.0.9

Developer	Devilish Services / Devil Software
Platform	Windows 10 / Windows 11 — 64-bit
Framework	Microsoft .NET 10 Desktop Runtime (x64)
Administrator access	Required
Internet access	Required for licensing and software updates

Monitor • Identify • Control • Protect

Contents

Getting Started	Sections 1–8
Dashboard & Network Monitoring	Sections 9–18
Game Ports & Firewall Controls	Sections 19–24
Windows Service & Licensing	Sections 25–30
Web Interface	Sections 31–33
Software Updates	Sections 34–41
Daily Use & Troubleshooting	Sections 42–50
Uninstalling, Support & Quick Start	Sections 51–53

Important: Use firewall, port-blocking and game-kick controls carefully. Blocking required traffic can stop games, voice applications, launchers or Windows services from working normally.

Section 1 — What Devil-Guard Network Monitor Does

Devil-Guard Network Monitor is a Windows utility designed to monitor network activity on a gaming computer and provide controls for connections, game ports, firewall rules and unwanted network traffic. The application combines a desktop dashboard with a background Windows service so monitoring can continue independently of the visible dashboard.

- Network connection monitoring
- Game-related connection monitoring
- Game port management and game port bans
- Windows Firewall integration
- Connection and process information
- Background Windows service
- Automatic licence validation
- Device-bound software licensing
- Built-in software updates with SHA-256 verification
- Local Web UI and desktop dashboard

Section 2 — System Requirements

- Windows 10 or Windows 11, 64-bit
- Microsoft .NET 10 Desktop Runtime for Windows x64
- Administrator access
- Internet connection for licence activation, licence checks and updates

Section 3 — Check Whether .NET 10 Is Installed

Step 1: Right-click the Windows Start button.

Step 2: Open Terminal or PowerShell.

Step 3: Run the command shown below.

Step 4: Look for Microsoft.WindowsDesktop.App 10.x. If version 10 is present, continue with the Network Monitor installation.

```
dotnet --list-runtimes

Microsoft.WindowsDesktop.App 10.
Microsoft.NETCore.App 10.
```

Section 4 — Installing .NET 10

Step 1: Download Microsoft .NET 10 Desktop Runtime for Windows x64 from Microsoft.

Step 2: Run the installer and complete the setup.

Step 3: Restart Windows if prompted.

Step 4: Open PowerShell again and run dotnet --list-runtimes.

Step 5: Confirm that Microsoft.WindowsDesktop.App 10.x is listed.

Section 5 — Installing Devil-Guard Network Monitor

Step 1: Locate the Network Monitor installer.

Step 2: Right-click the installer and choose Run as administrator.

Step 3: Approve the Windows User Account Control prompt by selecting Yes.

Step 4: Wait for the Devil-Guard Network Monitor Setup wizard to open.

Step 5: Follow the setup screens to continue.

```
Devil-Guard-Network-Monitor-1.0.9-Setup.exe
```

Section 6 — Licence Activation

Devil-Guard Network Monitor uses a device-bound software licence. During installation, enter the Devilish Services licence token assigned to Network Monitor.

Step 1: Copy your complete licence token.

Step 2: Paste it into the licence field.

Step 3: Make sure there are no extra spaces before or after the token.

Step 4: Continue the installation and allow the installer to validate the licence.

- Licence token
- Network Monitor product identifier
- Windows device identity / MachineGuid (GDID)
- IPv4 information
- Licence status

Section 7 — Device Binding

A Network Monitor licence is associated with the computer on which it is activated. This helps prevent the same software token being copied to multiple computers. If Network Monitor is moved to another computer, the licence binding may need to be reset through Devilish Services.

Section 8 — Completing Installation

Step 1: Leave the default installation directory unless you have a reason to change it.

Step 2: Click Install.

Step 3: Wait while Setup copies the program files.

Step 4: Allow Setup to install the Network Monitor Windows service.

Step 5: Complete the Setup wizard.

Step 6: Launch Network Monitor.

Section 9 — Starting Network Monitor

Step 1: Open Devil-Guard Network Monitor from the Desktop shortcut or Start Menu.

Step 2: Approve the Administrator/UAC prompt.

Step 3: Wait while the program performs its licence check.

Step 4: The main dashboard opens after validation succeeds.

Section 10 — The Main Dashboard

The main window uses a sidebar for navigation. Select a section from the left side of the Network Monitor window and the selected page appears in the main content area.

- Current network connections
- Network activity
- Processes using the network
- Protected game connections
- Game ports
- Firewall information
- Monitoring/service status

Section 11 — Understanding the Sidebar

The sidebar is the main navigation system. Click a section once to open it. Some pages perform live Windows or network queries, so detailed information may continue loading after the page itself becomes visible.

Section 12 — Network Monitoring

The network monitoring area shows network activity detected on the computer.

- Local IP address
- Remote IP address
- Local port
- Remote port
- Connection protocol
- Connection state
- Associated process

Section 13 — Understanding IP Addresses

Local IP

The address assigned to the computer or local network adapter.

```
192.168.1.20
```

Remote IP

The external computer, game server, website or service your computer is communicating with.

```
203.0.113.45
```

Section 14 — Understanding Ports

Network programs use numbered TCP or UDP ports. A connection may show both a local port and a remote port.

```
80
443
2302
```

```
27015
```

Section 15 — Game Ports

Open Game Ports from the sidebar to view and manage game-related ports and associated firewall information.

- Port number
- Protocol
- Associated game/process
- Rule status
- Firewall status
- Ban/block status

Section 16 — Opening Game Ports

Step 1: Click Game Ports in the sidebar.

Step 2: The Game Ports page opens.

Step 3: Allow a short time for live firewall details to load.

Step 4: Review the listed ports and rules.

Performance: The current Game Ports implementation loads expensive Windows Firewall information separately so a slow firewall query does not need to freeze the entire page.

Section 17 — Refreshing Game Ports

Step 1: Open Game Ports.

Step 2: Click Refresh when you need Network Monitor to re-read current port and firewall information.

Step 3: Wait for the new information to appear.

Refreshing is useful after starting or closing a game, changing firewall rules, adding/removing a game port or applying a ban.

Section 18 — Windows Firewall Information

Network Monitor can query Windows Firewall for rules associated with monitored ports. Large Windows Firewall rule sets may take several seconds to enumerate.

- Rule name
- Enabled/disabled state
- Direction
- Protocol
- Local port
- Remote port

Section 19 — Game Port Bans

Game Port Bans allow a selected game-related port or rule to be restricted. Blocking a required port can prevent multiplayer, server browsing, voice communications or matchmaking from working.

Section 20 — Applying a Game Port Ban

Step 1: Open Game Ports.

Step 2: Locate the required game port.

Step 3: Confirm the port number and protocol.

Step 4: Choose the available block/ban action.

Step 5: Confirm the operation if prompted.

Step 6: Refresh the page and verify that the protection/firewall rule is active.

```
Example: UDP 2302
```

Section 21 — Removing a Game Port Ban

Step 1: Open Game Ports.

Step 2: Locate the blocked rule.

Step 3: Choose the removal/unblock action.

Step 4: Refresh Game Ports.

Step 5: Confirm that the block is no longer active.

Section 22 — Game Kick

Where supported by the installed build, Game Kick functionality can be used with detected game/network activity. Use this control only when you understand which connection, player or session is being affected.

Section 23 — Connection Information

When reviewing network activity, use all available fields rather than judging a connection only by its IP address.

- Process/executable
- Remote IP
- Local IP
- Local/remote port
- Protocol
- Connection state

This helps distinguish traffic belonging to games, Windows, launchers, browsers, voice software, cloud services and update software.

Section 24 — Process Information

Where process information is available, Network Monitor associates network activity with the Windows process responsible for it.

```
game.exe
discord.exe
```

Section 25 — The Network Monitor Windows Service

Network Monitor installs a Windows service so monitoring and licence validation can continue independently of the visible dashboard. The service is normally configured to start with Windows.

Section 26 — Checking the Service

Step 1: Open PowerShell as Administrator.

Step 2: Run Get-Service *Devil*.

Step 3: Locate the Devil-Guard Network Monitor service and check its Status.

```
Get-Service *Devil*
```

You can also open the Windows Services console:

```
services.msc
```

Section 27 — Starting the Service

```
Start-Service DevilGuardNetworkMonitor
```

Section 28 — Stopping the Service

Stop the service only for maintenance or troubleshooting.

```
Stop-Service DevilGuardNetworkMonitor
```

Section 29 — Licence Monitoring

The desktop application validates the software licence when it starts. The background service can also perform periodic licence checks while Network Monitor is running so a disabled or revoked licence does not remain indefinitely active.

Section 30 — Licence Problems

- Invalid token
- Revoked licence
- Disabled licence
- Device mismatch
- Product mismatch
- Account/billing issue
- Temporary network connection problem

Privacy: Do not publish or send your full licence token in screenshots, forum posts or public support messages.

Section 31 — Web Interface

Network Monitor can include a local Web UI, providing browser-based access to monitoring information. Depending on configuration, the Web UI may be restricted to the local computer or made available through an allowed network interface.

Section 32 — Opening the Web Interface

Open a web browser and enter the Network Monitor Web UI address configured for your installation. The exact address depends on the installation and external-access settings.

Section 33 — Web Game Ports

The Web UI Game Ports page is designed to display the page before the expensive Windows Firewall scan finishes. Firewall information is then loaded separately, which helps prevent a slow Windows query from making the entire page appear unresponsive.

Section 34 — Software Updates

Network Monitor contains an automatic update system and checks the Devilish Services Network Monitor update feed for newer releases.

```
https://updates.devilishservices.com/NetworkMonitor/latest.json
```

Section 35 — Downloading an Update

Step 1: Click UPDATE when an update is offered.

Step 2: The update window opens.

Step 3: Network Monitor begins downloading the installer.

Step 4: Watch the progress percentage until it reaches 100%.

```
25%
50%
75%
100%
```

Section 36 — SHA-256 Verification

After the download reaches 100%, Network Monitor verifies the installer using SHA-256. If the calculated value does not match the value published by the update service, the update should not be installed.

Section 37 — Installing the Update

Step 1: Network Monitor prepares the verified update.

Step 2: The Network Monitor service is stopped.

Step 3: The updater waits for locked files to be released.

Step 4: The installer is launched with Administrator privileges.

Step 5: The running application closes.

Step 6: Setup replaces the installed program files.

Step 7: Start Network Monitor again after installation if it does not reopen automatically.

Section 38 — Why the Service Is Stopped During Updates

Windows normally prevents an installer from replacing an executable or DLL that is still being used by another process. Stopping the service reduces the chance of file-lock and access-denied errors during an update.

```
Access to the path is denied
```

Section 39 — Update Download Staging

Each downloaded update uses a unique staging filename so a previous installer that remains locked by Windows cannot prevent a new update from being downloaded and launched.

Section 40 — If an Update Fails

Step 1: Close Network Monitor.

Step 2: Start Network Monitor again as Administrator.

Step 3: Try the update again.

Step 4: Check Windows Defender or third-party security software for blocked/quarantined files.

Step 5: Restart Windows if files remain locked and retry.

Section 41 — Update Log

Network Monitor records diagnostic information for the update process. Include this log when requesting support for update failures.

```
C:\ProgramData\Devilish Services\Devil-Guard\NetworkMonitor\Updates\NetworkMonitor-
WebUpdate.log
```

- Administrator/elevation state
- Service shutdown
- Installer launch
- Installer exit code
- Update exceptions
- File access problems

Section 42 — Recommended Daily Use

Step 1: Start Windows and allow the Network Monitor service to start.

Step 2: Start Network Monitor as Administrator.

Step 3: Confirm that the dashboard loads and licensing succeeds.

Step 4: Start your game.

Step 5: Open Game Ports if you want to review game-related activity.

Step 6: Click Refresh when required.

Step 7: Review detected ports/connections before applying any block or ban.

Step 8: Leave Network Monitor running while gaming if you want live dashboard monitoring.

Section 43 — Troubleshooting — Network Monitor Will Not Start

Step 1: Check that .NET 10 Desktop Runtime is installed.

Step 2: Run Network Monitor as Administrator.

Step 3: Check Internet connectivity.

Step 4: Confirm that the Network Monitor licence is active.

Step 5: Restart Windows and try again.

```
dotnet --list-runtimes
```

Section 44 — Troubleshooting — Game Ports Page Is Slow

Step 1: Allow the page to open.

Step 2: Wait briefly for live firewall information.

Step 3: Use the Refresh button.

Step 4: Test Windows Firewall enumeration from Administrator PowerShell using the command below.

```
Get-NetFirewallRule
```

If this PowerShell command itself is slow, the delay is occurring in Windows Firewall enumeration rather than only in the Network Monitor interface.

Section 45 — Troubleshooting — No Network Connections Appear

- Run Network Monitor as Administrator.
- Confirm the Windows service is running.
- Make sure a network-enabled game/application is running.
- Confirm Windows networking itself is functioning.
- Refresh the selected Network Monitor page.

Section 46 — Troubleshooting — Service Is Not Running

```
Get-Service DevilGuardNetworkMonitor
```

If the service is stopped, run:

```
Start-Service DevilGuardNetworkMonitor
```

If the service immediately stops again, review Windows Event Viewer and the Network Monitor logs.

Section 47 — Troubleshooting — Licence Error

Step 1: Check Internet access.

Step 2: Restart Network Monitor as Administrator.

Step 3: Confirm that the token/licence belongs to Network Monitor.

Step 4: Check that the computer is the device originally activated.

Step 5: Contact Devilish Services if the device binding needs to be reset.

Section 48 — Troubleshooting — Firewall Rule Will Not Apply

- Confirm Network Monitor has Administrator rights.
- Confirm Windows Firewall is enabled.
- Check whether another security package is managing the firewall.
- Confirm the port number is valid.
- Confirm that the selected protocol (TCP/UDP) is correct.

Section 49 — Security Recommendations

Do not automatically block every unfamiliar address or port. Modern Windows systems and games routinely communicate with content-delivery networks, authentication servers, matchmaking services, anti-cheat systems, voice services, cloud services and update servers.

Section 50 — Before Blocking Something

Step 1: Identify the process that owns the connection.

Step 2: Check the local and remote ports.

Step 3: Determine whether the traffic belongs to the game or another legitimate application.

Step 4: Confirm whether the protocol is TCP or UDP.

Step 5: Decide whether the connection is expected.

Step 6: Consider what functionality may stop working if the connection is blocked.

Section 51 — Uninstalling Network Monitor

Step 1: Open Windows Settings.

Step 2: Go to Apps > Installed apps.

Step 3: Find Devil-Guard Network Monitor.

Step 4: Choose Uninstall.

Step 5: Follow the removal wizard and approve Administrator access if requested.

The uninstaller may remove application files, the Network Monitor Windows service and program shortcuts. Review custom firewall rules separately if you intentionally created rules you want removed.

Section 52 — Information to Include With a Support Request

- Network Monitor version
- Network Monitor build number
- Windows version
- Installed .NET version
- A clear description of the problem
- The exact error message
- Relevant screenshot
- Relevant Network Monitor log file

To collect .NET information:

```
dotnet --info
```

Important: Never include your complete software licence token in a public support message or screenshot.

Section 53 — Quick Start Guide

Step 1: Install Microsoft .NET 10 Desktop Runtime x64.

Step 2: Run the Devil-Guard Network Monitor installer as Administrator.

Step 3: Enter your Network Monitor licence token.

Step 4: Complete installation.

Step 5: Start Network Monitor as Administrator.

Step 6: Confirm licence validation succeeds.

Step 7: Confirm the Windows service is running.

Step 8: Start your game.

Step 9: Open Game Ports.

Step 10: Refresh and review the detected game/network activity.

Step 11: Apply blocks or bans only when required.

Step 12: Install software updates when offered.

DEVIL-GUARD NETWORK MONITOR v1.0.9

Devil Software / Devilish Services

Monitor • Identify • Control • Protect