

DEVIL SOFTWARE
SERVER MONITOR

User Manual

Version 1.3.3

Installation • Licensing • Monitoring • Updates • Portable Edition

Contents

1. Introduction
2. System requirements
3. Installing Server Monitor
4. First-run licence activation
5. Dashboard overview
6. Adding and editing servers
7. How monitoring works
8. Availability and scan history
9. Automatic updates
10. Portable edition
11. Data, database and logs
12. Troubleshooting
13. Security and operational notes
14. Uninstalling
15. Quick reference

1. Introduction

Devil Software Server Monitor is a Windows desktop application for monitoring remote servers, VPS systems and network services from a single dashboard. It performs scheduled reachability checks, records the results in SQLite, displays reply times in milliseconds, and keeps a history of availability for each configured server.

- ICMP ping checks with reply time shown as MS REPLY.
- TCP service checks, including the built-in hidden checks for port 8, SSH on port 22 and RDP on port 3899, plus additional configured ports.
- Per-server availability bars and percentages calculated from saved scan history.
- SQLite storage for servers, settings and scan history.
- Automatic update checking on startup and after each scan.
- Installed and portable editions with separate licence identities.
- System tray access and modern dark dashboard.

Important
A failed ICMP ping does not always mean a server is offline. Firewalls may block ping. Server Monitor also uses configured TCP checks to help determine reachability.

2. System requirements

Requirement	Details
Operating system	Windows 10/11 or Windows Server, 64-bit

Requirement	Details
Architecture	x64
.NET runtime	Not required for the self-contained installer/portable build
Network	Outbound network access to monitored hosts and the licensing/update services
Permissions	Standard user for normal operation; administrator approval may be required for installation or updates
Storage	Small local footprint plus SQLite history growth over time

3. Installing Server Monitor

3.1 Installer edition

1. Download ServerMonitor-Setup.exe from the Devilish Services download portal.
2. Run the installer. Approve the Windows elevation prompt if it appears.
3. Complete the installation. The application is installed under Program Files and creates its data directory under ProgramData.
4. Launch Server Monitor from the Start Menu or desktop shortcut if created.

Installed data location
C:\ProgramData\Devil Software\Server Monitor\

4. First-run licence activation

Server Monitor uses the Devilish Services token system. The installed and portable editions are treated as separate licensed products.

Edition	Licensed filename	Use this token
Installed	ServerMonitor-Setup.exe	Token generated for the installer product
Portable	ServerMonitor-Portable.zip	Token generated for the portable product

1. Start Server Monitor.
2. When the activation window appears, paste the activation token generated for the correct edition.
3. Submit the activation. The software contacts the Devilish Services licensing service and validates the token against the machine and product.
4. If activation succeeds, the dashboard opens and the licence is stored securely for later launches.

Product mismatch
If you see “activation failed: product mismatch”, verify that the token was generated for the exact edition you are running. Installer and portable tokens are not interchangeable. If a failed mismatch disabled the licence on the website, reset the binding and re-enable it before trying again.

5. Dashboard overview

The dashboard provides an at-a-glance view of the monitored infrastructure. The top summary cards show total monitors, online count, offline count, overall availability and average ping. The server table focuses on the information most useful during daily operation.

Column	Meaning
SERVER	Friendly name assigned to the monitored system.
AVAILABILITY	Per-server red/green history bars plus online percentage, calculated from saved scans.
IP ADDRESS	Configured IP address used for monitoring when present.
MS REPLY	ICMP reply time in milliseconds. “No reply” means ping did not respond.
STATUS	Current Online, Offline, Waiting or Disabled state.

The Host Name is still stored in the database and available in the Add/Edit Server dialog, but it is intentionally hidden from the main table to give more space to availability information.

6. Adding and editing servers

6.1 Add a server

1. Click + Add server from the dashboard or sidebar.
2. Enter a clear Server Name.
3. Enter an IP Address and/or Host Name. The IP address is preferred when present; the host name can be used when an IP is not entered.
4. Configure any additional TCP ports that should be tested.
5. Keep the server enabled if it should participate in scheduled scans.
6. Save the server.

6.2 Edit a server

Select a server row and click Edit, or double-click the row. Change the required fields and save. The next scan uses the new configuration.

6.3 Delete a server

Select the server and click Delete. The monitor entry is removed. Existing scan history may remain in the database for historical reporting.

7. How monitoring works

Server Monitor runs scheduled scans at the configured interval (normally every five minutes). A manual scan can also be started with Scan now.

- Ping: sends an ICMP request and records the round-trip time in milliseconds when a reply is received.
- TCP port 8: hidden health-check port; scanned but not displayed as a dashboard column.

- SSH (22): scanned in the background and recorded, but not shown as a separate dashboard column.
- RDP (3899): scanned in the background and recorded, but not shown as a separate dashboard column.
- Additional ports: any user-configured ports are scanned and stored without adding extra table columns.
- Online decision: the monitor can still regard a host as reachable when ping is blocked but a configured TCP service responds.

Scan timing
The bottom status area shows the last completed scan and the countdown to the next scheduled scan. Update checks are also performed after scans.

8. Availability and scan history

Availability is calculated from the scan results saved for each server. Green bars represent successful/online observations and red bars represent failed/offline observations. The percentage shown in each row is specific to that server.

8.1 Opening history

1. Select History from the left navigation.

2. Use the search box to filter by server name, host name or IP address.

3. Review timestamp, server identity, status and MS reply for previous scans.

The dashboard intentionally hides Last Check and individual port columns to keep the main view uncluttered. Detailed scan information remains stored in SQLite.

9. Automatic updates

Server Monitor checks for software updates automatically when the application starts and after each scan. The update check is silent when no new version is available.

1. When a newer version is detected, a green Update button appears in the dashboard header.

2. Click the update button and confirm the installation when prompted.

3. A progress dialog displays the download and verification process.

4. The installer download is verified using its SHA-256 value from the update manifest.

5. Server Monitor launches the verified installer directly and closes itself.

6. Inno Setup updates the installed files and restarts Server Monitor when complete.

Update service
The application checks the Devilish Services update endpoint at updates.devilishservices.com/server-monitor/. Do not manually replace files while an update is running.

10. Portable edition

The portable edition is distributed as ServerMonitor-Portable.zip. Extract the ZIP to a writable folder and run ServerMonitor.exe from that folder.

- The portable package contains portable.flag so the application automatically selects the portable licence identity.
- Use a token generated specifically for ServerMonitor-Portable.zip.
- Do not remove portable.flag unless you intentionally want the application to stop identifying itself as the portable edition.
- Copying the portable build to another computer may trigger the licence system's machine-binding rules.

11. Data, database and logs

Server definitions, settings and scan history are stored in SQLite. This avoids the need to install SQL Server, MySQL or another external database.

11.1 Installed edition data

Database/data directory
C:\ProgramData\Devil Software\Server Monitor\

The database is preserved during normal application upgrades. Installer updates should not overwrite or delete the existing SQLite database.

11.2 Backup recommendation

For important monitoring history, periodically back up the Server Monitor data directory while the application is closed. Keeping a copy of the SQLite database provides the easiest recovery path after disk failure or accidental deletion.

12. Troubleshooting

Problem	What to check
Server shows Offline	Confirm the IP/hostname, firewall rules, routing and that at least one monitored service is reachable. Ping may be blocked independently of TCP.
MS REPLY says No reply	The server did not answer ICMP. This alone does not prove that the server is down.
Activation failed: product mismatch	Use a token generated for the exact edition. Installer and portable products have different identities.
Licence disabled after mismatch	Reset binding/re-enable the licence in the download portal, then activate with the corrected build/token.
Update button never appears	Confirm internet access and that the update manifest is reachable. The app checks at startup and after scans.
Update download is locked	Current releases use unique update filenames to avoid reusing an installer file that another process still has open.
Portable licence rejected	Verify portable.flag is present and the token belongs to ServerMonitor-Portable.zip.
No servers appear	Add at least one server and confirm it is enabled.

13. Security and operational notes

- Only monitor systems and services you are authorised to access.
- TCP checks only test whether a connection can be established; they do not authenticate to SSH or RDP.
- Keep activation tokens private. If a token is exposed publicly, revoke or replace it through the licence portal.
- Allow the application to update through the official update endpoint instead of downloading executables from untrusted sources.
- Back up the SQLite database if scan history is operationally important.

14. Uninstalling

1. Open Windows Settings > Apps > Installed apps.
2. Locate Devil Software Server Monitor.
3. Choose Uninstall and follow the prompts.
4. If you also want to remove historical monitoring data, remove the Server Monitor data directory only after confirming that you no longer need the SQLite database.

15. Quick reference

Task	Action
Run a scan	Click Scan now.
Add a server	Click + Add server.
Edit a server	Select a row and click Edit, or double-click it.
Delete a server	Select a row and click Delete.
View history	Select History in the sidebar.
Find a server	Use the dashboard search box.
Install an update	Click the green Update button when it appears.
Open data folder	Select Data folder in the sidebar.
Check availability	Read the red/green availability bars and percentage in each server row.
Check latency	Read MS REPLY; lower values generally indicate faster network response.

Support and product information

Product: Devil Software Server Monitor

Manual version: 1.3.3

Developer: Devil Software / Devilish Services

Download portal: downloads.devilishservices.com

Update service: updates.devilishservices.com/server-monitor/