

# SilentHelm Configuration Guide

**Applies to:** SilentHelm Windows tray build (local-first). **Updated:** January 05, 2026

This guide explains every setting available in **SilentHelm.config.json** and how to tune it for home users or IT teams. It also includes examples for common scenarios and notes about safe testing.

## Where the config lives

By default, SilentHelm stores data under your local app data directory (for example: %LOCALAPPDATA%\SilentHelm\). The config file is: `SilentHelm.config.json`.

## Editing and applying changes

Edit the JSON file with a text editor (Notepad is fine). Then use the tray menu: **Reload** to apply changes without restarting the app. If you make a JSON syntax mistake, SilentHelm will keep using the last valid configuration.

**Windows path escaping in JSON:** when you write a Windows path in JSON, you must escape backslashes. Example: `C:\\\\SilentHelm_Test` (represents `C:\SilentHelm_Test`).

## 1) Monitoring toggles

Setting	Type	Default	What it does / notes
<code>enableProcessMonitor</code>	bool	True	Enables the process monitor loop (collects process/command-line based signals).
<code>enableDirMonitorDesktop</code>	bool	True	Watches Desktop for file activity (create/rename/modify/delete).
<code>enableDirMonitorDocuments</code>	bool	True	Watches Documents for file activity.
<code>enableDirMonitorDownloads</code>	bool	True	Watches Downloads for file activity (useful for malware/ransomware staging).

## 2) Extra watched directories (extraWatchDirs)

Use **extraWatchDirs** to monitor additional folders beyond Desktop/Documents/Downloads. Ideal for shared folders, dev build folders, test sandboxes, or server data directories.

**Format:** a single string containing one or more directories separated by `;` or `|`.

```
{
  "extraWatchDirs": "C:\\\\SilentHelm_Test;D:\\\\Shares\\\\Finance"
}
```

Equivalent example using pipe: `C:\\\\SilentHelm_Test|D:\\\\Shares\\\\Finance`

**Reload behavior:** Adding a new directory starts monitoring immediately after tray -> Reload. Removing a directory stops its monitor thread (full removal support is implemented).

## 3) Mass file-change detection (file burst)

Setting	Type	Default	What it does / notes
<code>burstWindowSeconds</code>	int	30	Time window (seconds) for counting file changes within a watched folder.
<code>burstThreshold</code>	int	50	How many changes within the window triggers a file-burst signal.

fileBurstIncidentSeverity	int	80	Severity assigned to a file-burst incident (0-100). Recommended: 75-90.
---------------------------	-----	----	---

Tip: If you work with large repos or frequently extract big archives to Downloads, raise **burstThreshold** to reduce noise.

## 4) Process heuristics

Setting	Type	Default	What it does / notes
enableProcessHeuristics	bool	True	Turns on process scoring rules (for example suspicious command-line patterns).
processSuspiciousScoreThreshold	int	60	Score needed to trigger a suspicious-process incident. Lower = more sensitive, higher = fewer alerts.

Recommendation: start with 60-70. If you see too many alerts from developer tools or automation scripts, increase the threshold.

## 5) Directory + file heuristics (names/extensions)

Setting	Type	Default	What it does / notes
enableDirFileHeuristics	bool	True	Turns on file-name/extension heuristics inside watched folders.
ransomNoteHeuristicsEnabled	bool	True	Detects ransom-note style filenames (for example README_DECRYPT).
encryptedExtHeuristicsEnabled	bool	True	Detects encrypted-looking extensions or known bad extension patterns (config-driven in code).
dirFileHeuristicIncidentSeverity	int	65	Severity assigned to dir/file heuristic incidents.

In the report, SilentHelm shows the folder and (when available) the specific file that matched the heuristic.

## 6) Canary files

Setting	Type	Default	What it does / notes
enableCanaryFiles	bool	True	Creates and monitors canary files inside each watched folder. Touching a canary is a high-confidence signal.
canaryIncidentSeverity	int	90	Severity assigned to canary incidents. Recommended: 90-100 (often Critical).
canaryWarmupSeconds	int	10	Startup grace period to ignore canary events created by SilentHelm itself.
canaryFileNames	string	SilentHelm_DO_NOT_TOUCH.txt   Important_Backup_DO_NOT_DELETE.txt	Pipe-separated list of canary file names. These are created in each watched folder.

```
{
  "enableCanaryFiles": true,
  "canaryIncidentSeverity": 95,
  "canaryWarmupSeconds": 10,
  "canaryFileNames":
  "SilentHelm_DO_NOT_TOUCH.txt | Important_Backup_DO_NOT_DELETE.txt | canary.txt"
}
```

Testing canaries safely: edit or rename a canary file in a watched folder. This should generate a Critical/High incident and update the tray tooltip.

## 7) Incident rate limiting

Setting	Type	Default	What it does / notes
<code>incidentRateLimitSeconds</code>	int	60	Minimum time between incident bundle creation. Prevents incident spam during noisy events. Default: 60 seconds.

Note: Rate limiting affects incident bundle creation, not logging. You can still see underlying activity in `SilentHelm.log.jsonl`.

# Example configurations

## A) Home user (balanced)

```
{
  "enableProcessMonitor": true,
  "enableDirMonitorDesktop": true,
  "enableDirMonitorDocuments": true,
  "enableDirMonitorDownloads": true,
  "burstWindowSeconds": 30,
  "burstThreshold": 60,
  "fileBurstIncidentSeverity": 80,
  "enableProcessHeuristics": true,
  "processSuspiciousScoreThreshold": 65,
  "enableDirFileHeuristics": true,
  "ransomNoteHeuristicsEnabled": true,
  "encryptedExtHeuristicsEnabled": true,
  "dirFileHeuristicIncidentSeverity": 65,
  "enableCanaryFiles": true,
  "canaryIncidentSeverity": 95,
  "canaryWarmupSeconds": 10,
  "canaryFileNames": "SilentHelm_DO_NOT_TOUCH.txt|Important_Backup_DO_NOT_DELETE.txt",
  "incidentRateLimitSeconds": 60
}
```

## B) IT workstation (more sensitive)

```
{
  "processSuspiciousScoreThreshold": 55,
  "burstThreshold": 45,
  "fileBurstIncidentSeverity": 85,
  "canaryIncidentSeverity": 98,
  "incidentRateLimitSeconds": 45,
  "extraWatchDirs": "D:\\Work\\Shared;E:\\Projects"
}
```

This snippet shows only the differences you would apply on top of your base config.

## C) Developer machine (reduce false positives)

```
{
  "burstThreshold": 90,
  "processSuspiciousScoreThreshold": 75,
  "incidentRateLimitSeconds": 90,
  "extraWatchDirs": "C:\\SilentHelm_Test"
}
```

If you frequently run build systems or scripts that touch many files quickly, increase thresholds to avoid noise.

**Support tip:** When filing a bug report, include the report HTML, the last 200 lines of SilentHelm.log.jsonl, and the relevant incident folder under Incidents\.