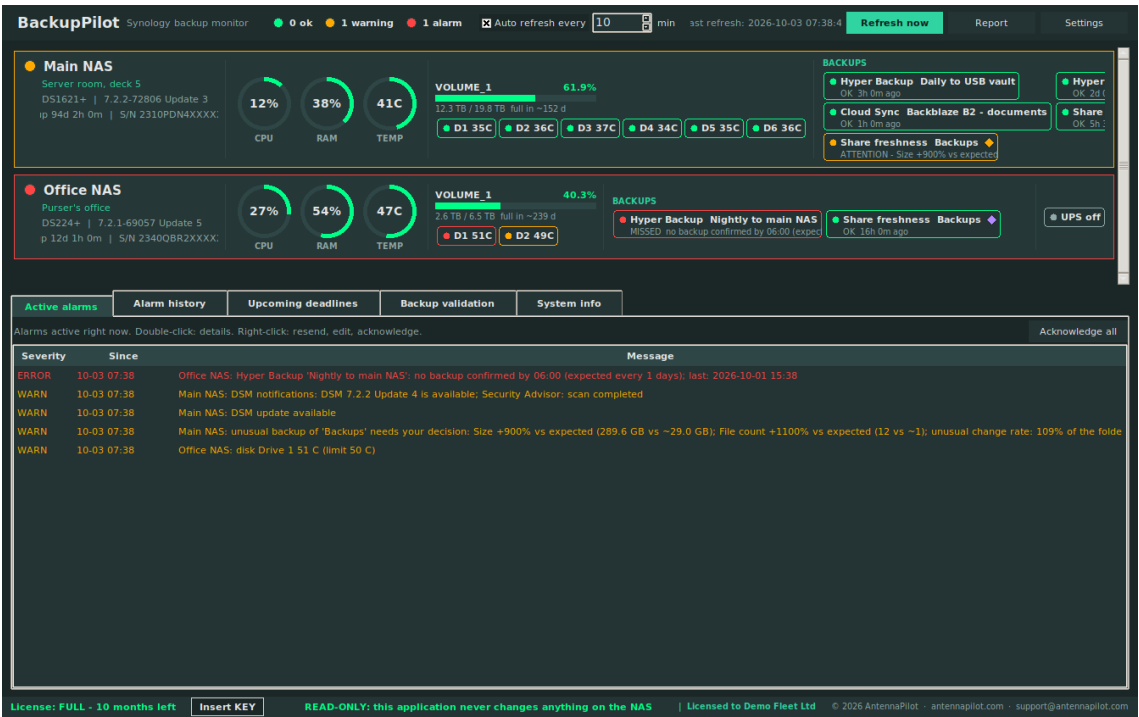


BackupPilot

Synology backup monitor

User Manual

Application version 1.2 · Document version 1.2 · 03 October 2026



AntennaPilot · <https://antennapilot.com> · support@antennapilot.com

Synology, DiskStation, RackStation, DSM, Hyper Backup, Active Backup for Business, Cloud Sync and Synology Drive are trademarks or registered trademarks of Synology Inc. BackupPilot is an independent product of AntennaPilot and is not affiliated with, endorsed by or sponsored by Synology Inc. All other trademarks are the property of their respective owners.

Contents

1. Introduction	4
2. What BackupPilot does - and what it does not	4
What it does	4
What it does not do	5
2A. How it compares	6
3. Requirements and installation	7
Installation	7
4. Preparing the NAS	7
5. First start and licensing	8
6. Quick start	8
7. The dashboard	9
Top bar	9
One row per NAS	9
Bottom tabs	10
8. Settings	12
8.1 NAS connection	12
8.2 Backup monitors	13
8.3 Other alarms	14
8.4 Notifications	15
8.5 Thresholds	16
8.6 Smart validation	17
8.7 Startup & service	18
9. Backup monitors - how the rule works	19
10. Alarms	20
10A. Smart backup validation	22
How a run is measured	22
How it is judged	22
Your decision	23
Extra signals	25
What it cannot do (by design)	25
11. E-mail notifications	26
12. Backup report	26
13. Trends	31
14. Running permanently	32
A) Desktop application with autostart	32
B) Background service (no user logged on)	32

Maintenance window 32

15. Files, data and the read-only guarantee 32

Read-only guarantee 32

Privacy 33

16. Troubleshooting 34

17. Support, bug reports and updates 34

Appendix A. DSM APIs used (read-only) 36

Appendix B. Glossary 36

Copyright and trademarks 36

1. Introduction

BackupPilot is a Windows desktop application that watches the backups of one or more Synology NAS units and answers one question continuously: **did the backup happen, in time?** It connects to each NAS through the official DSM Web API, reads the state of every backup source it can find, compares it with the rules you define (how often, by what time of day) and raises an alarm - sound, e-mail, dashboard - when a backup window is missed. It also watches the health of the NAS itself: volumes, disks, S.M.A.R.T., temperatures, DSM notifications, security scan and updates.

It is designed for environments where somebody is responsible for backups but is not watching a console all day: ships, remote sites, small IT departments, managed fleets of NAS units. The whole application is a single executable; nothing is installed on the NAS and nothing is ever written to it.

Who this manual is for

IT officers, administrators and operators who install and run BackupPilot. Basic familiarity with Synology DSM (creating a user, finding the shared folders) is assumed.

2. What BackupPilot does - and what it does not

What it does

- Detects automatically the backup sources present on each NAS: Hyper Backup tasks, Active Backup for Business tasks, Snapshot Replication plans, Cloud Sync connections, Synology Drive ShareSync connections and Btrfs snapshots of shared folders.
- Watches shared folders written by external backup software (Veeam, Windows Server Backup, Acronis, robocopy, rsync...) - the newest file in the folder is treated as the last confirmed backup.
- Lets you define, per source, a **backup monitor**: a backup must be confirmed every N hours/days and, optionally, by a given time of day. The rule is re-checked every minute.
- **Smart backup validation** for watched folders: every backup run is measured (files, bytes, average size, change rate, file types, names) and compared with the confirmed history of that folder using robust statistics; full and incremental runs are separated automatically. Unusual runs ask for your decision; hard facts (0 bytes, empty files, ransomware extensions, changed canary files, failed content checks) are alarms. Rejected backups move the RPO clock back to the last good one.
- Raises alarms when a window is missed or when a task reports an error, with sound on the computer and e-mail (Outlook or SMTP), repeat reminders and escalation to a second address.
- Monitors NAS health: volume status and usage, disk status, S.M.A.R.T. and temperature, system temperature, CPU/RAM, UPS, DSM notifications, Security Advisor, DSM update availability.
- Keeps a history: every alarm with the time it appeared and cleared, periodic samples for 90 days, every confirmed backup time.
- Produces a backup report (screen, PDF, print, e-mail with PDF attached) for all devices or one device, and can send it weekly.
- Shows 30-day trends of volume usage and disk temperatures, with a linear forecast of when a volume will be full.
- Runs permanently: start with Windows, system tray with balloon notifications, or a background job (Windows Task Scheduler) that needs no logged-on user.
- Is strictly read-only on the NAS, enforced by a whitelist of DSM API methods inside the program.

What it does not do

- It does **not** perform backups, restore data, start or stop tasks, change settings or delete anything on the NAS. It only reads.
- It does not restore files to test them, and it cannot compare a backup with the source server (both would need write access or an agent). Smart validation tells you when a backup stops looking like the previous ones and lets you check canary files and format signatures; keep the integrity check / restore test of your backup software for the final proof.
- It does not replace DSM's own notifications; it complements them with deadline logic, history and reports. DSM's active notifications are shown and can be alarmed on, but they are managed in DSM.
- It does not monitor NAS units of other brands, and it does not monitor backup software directly (only through what it leaves on the NAS).
- It does not need, use or send any cloud service. Nothing leaves your computer except the e-mails you configure and, if enabled, a daily version check on antennapilot.com.
- It does not run on the NAS. It runs on a Windows computer that can reach the NAS over the network.

2A. How it compares

The table compares what each kind of tool documents **as shipped**, without custom scripting. Columns: **Synology built-in** - DSM notifications, Hyper Backup / Active Backup task reports and alerts, and Synology Active Insight (cloud service); **Generic monitors** - SNMP/API suites such as PRTG, Zabbix or Checkmk with Synology templates; **Backup-software monitors** - tools that watch the backup application itself, such as Veeam ONE, the Acronis console alerts or Backup Radar.

Capability	Synology built-in	Generic monitors	Backup-software monitors	BackupPilot
Job finished / failed notification	Yes	Via SNMP traps or logs	Yes	Yes, with appear / clear history
Alarm when no successful backup exists by a deadline ('every day by 06:00'), including jobs that never ran	Partly - Active Insight flags abnormal Hyper Backup tasks; no per-source deadline rule	Custom scripting	Yes, for the supported backup products (e.g. 'no successful backup in N days', 'no results')	Yes, per source, every N hours/days and optional deadline, re-checked every minute
Backups written by third-party software into NAS shared folders	No	Folder size / age sensors	Only for their own product	Yes - watched folders, independent of the software that writes
Plausibility of each backup run vs its confirmed history (size, files, average size, change rate, file types, names; full / incremental classes)	No	Thresholds only, no history-based verdict	Product-specific job statistics	Yes - smart validation, robust statistics
Operator verdicts that shape the trend (normal / exception / new normal / rejected) with quarantine and audit trail	No	No	Not as a built-in workflow	Yes
RPO measured from the last good backup after a rejection	No	No	Partly (last successful job)	Yes
Canary (sentinel) files, ransomware extension and format-signature checks on the backup content	No	No	Some products, for their own backups	Yes, optional, read-only
NAS health: volumes, disks, S.M.A.R.T., temperatures, DSM notifications, Security Advisor, DSM updates	Yes; centralised in Active Insight	Yes	No	Yes, thresholds and alarms ON / OFF
Several NAS units, mixed DSM versions, one screen	Active Insight - cloud, Synology Account	Yes - monitoring server	Not the NAS itself	Yes - local, no cloud
Report with charts, per device	Active Insight reports (cloud)	Yes, generic	Yes	Yes - screen, PDF, print, weekly e-mail with PDF
Escalation, maintenance windows, acknowledge, repeat reminders	Notifications only	Yes	Yes	Yes
Read-only guarantee enforced in the program (method whitelist)	n/a	Depends on the credentials given	Depends on the product	Yes, with a blocked-call counter
Restore test / comparison with the source server	Hyper Backup integrity check	No	Yes, for their own product	No - read-only by design
Footprint	Included with DSM; Active Insight is a cloud service	Monitoring server	Server or cloud service	One executable on a Windows PC

Based on publicly documented features in October 2026. Products change; check the current documentation of each tool before a purchase decision.

What is original to BackupPilot: the deadline rule per backup source; watched folders that turn any third-party backup written to a Synology NAS into a monitored source; smart validation of each run against its confirmed history with four operator decisions, quarantine and a capped adaptive tolerance; canary files as direct proof that the job copies what it should; device states that refuse to claim 'all backups OK' without a rule; a read-only guarantee you can audit; every finding explained in words.

3. Requirements and installation

Item	Requirement
Computer	Windows 10 or 11, 64-bit. About 150 MB of disk space. Permanent power if it is the monitoring station.
Network	TCP access from the computer to each NAS on the DSM port: 5001 (HTTPS, default) or 5000 (HTTP). VPN connections are fine. Self-signed NAS certificates are accepted.
NAS	Synology DSM 6.2 or 7.x. Any model: 2-bay home units up to rack models. Backup packages are optional; without them BackupPilot still watches folders, snapshots and health.
E-mail (optional)	Microsoft Outlook (desktop) installed and configured, or an SMTP server (Office 365, Gmail app password, company mail server).
License	One activation key per computer, bound to the machine fingerprint. A 24-hour demo with one NAS is available once per computer.

Installation

- Run **BackupPilot_setup.exe** and follow the installer. The program is installed per computer; settings and history are kept per Windows user in %APPDATA%\BackupPilot.
- Start BackupPilot from the Start menu. The license window appears (chapter 5).
- To update, install the new version over the old one; settings, history and license are kept. Help > Check for updates tells you when a new version is published.

4. Preparing the NAS

Create a dedicated account on each NAS for BackupPilot. Do not use your personal administrator account.

- DSM > Control Panel > User & Group > Create. Name it for example **monitor**, choose a strong password.
- Group: storage, S.M.A.R.T., Hyper Backup tasks, Cloud Sync and ShareSync are only readable by members of **administrators**. For the full picture add the account to that group. A non-administrator account still works; unreadable sections are marked 'restricted' on the dashboard.
- Do **not** enable 2-step verification on this account: BackupPilot logs in automatically at every refresh and cannot type a one-time code.
- Recommended: Control Panel > Security > Account - allow this account only from the IP address of the monitoring computer.
- If Auto Block is enabled, put the monitoring computer on the allow list, so a temporary wrong password does not lock it out.
- For watched folders (file freshness) the account needs read permission on the shared folder.
- Check the DSM ports under Control Panel > Login Portal if you changed the defaults.

BackupPilot never changes anything on the NAS, whatever the rights of the account. The read-only guarantee is enforced inside the program (chapter 15).

5. First start and licensing

At the first start the license window is shown. Two choices:

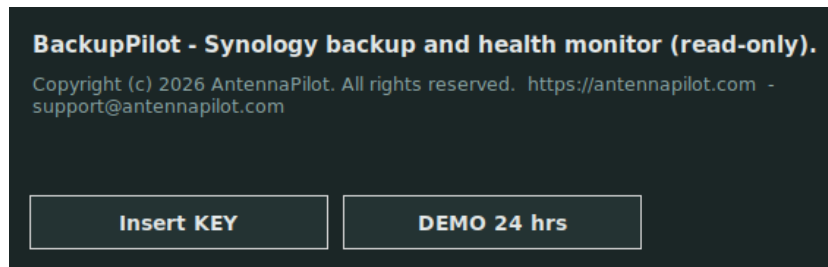


Figure 5.1 - License window: Insert KEY or start the 24-hour demo

- **DEMO 24 hrs** - a one-time trial with all features and one NAS. It can be used only once per computer; moving the system clock backwards disables it.
- **Insert KEY** - paste the activation key received from support. The key is bound to the machine fingerprint shown in the window (figure 5.2). Use *Send email request* to open a pre-filled e-mail to support@antennapilot.com, or copy the fingerprint and send it yourself.

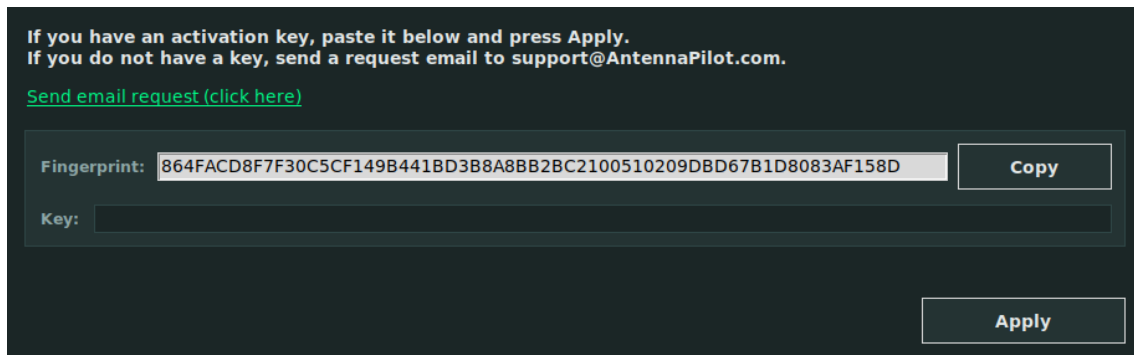


Figure 5.2 - Insert KEY: the machine fingerprint and the key field

Keys cannot be transferred between computers and are not valid for other AntennaPilot products. The status bar of the main window always shows the license state (FULL - N days/months left, Permanent, DEMO - time left) and the **Insert KEY** button; the text embedded in the key (for example the licensee name) appears in every window title and in the footer of reports and e-mails. If the license expires while the application runs, monitoring pauses and the Insert KEY window opens.

6. Quick start

- Create the monitoring account on the NAS (chapter 4).
- Open **Settings** (toolbar). In *NAS connection* fill in display name, host or IP, port, user, password and - optionally - a location/description. Press **Connect & detect**. Model, DSM version, backup sources, shared folders, volumes and disks are read from the NAS.
- If an external server writes its backups into a shared folder, tick that folder under *Watched shared folders*. A ticked folder gets a monitor immediately (every 1 day).
- Tab *Backup monitors*: for each source set how often a backup must be confirmed and by what time of day, and which channels (sound, e-mail) to use. Press **Apply to source**.
- Tab *Notifications*: enter the recipient address(es), choose Outlook or SMTP, press **Send test email**.
- Press **Save & close**. The dashboard polls the NAS every N minutes (toolbar) and re-checks the deadlines every minute.
- Optional: tab *Other alarms* for health alarms (all off by default), tab *Startup & service* to run permanently, toolbar **Report** for the backup report.

7. The dashboard

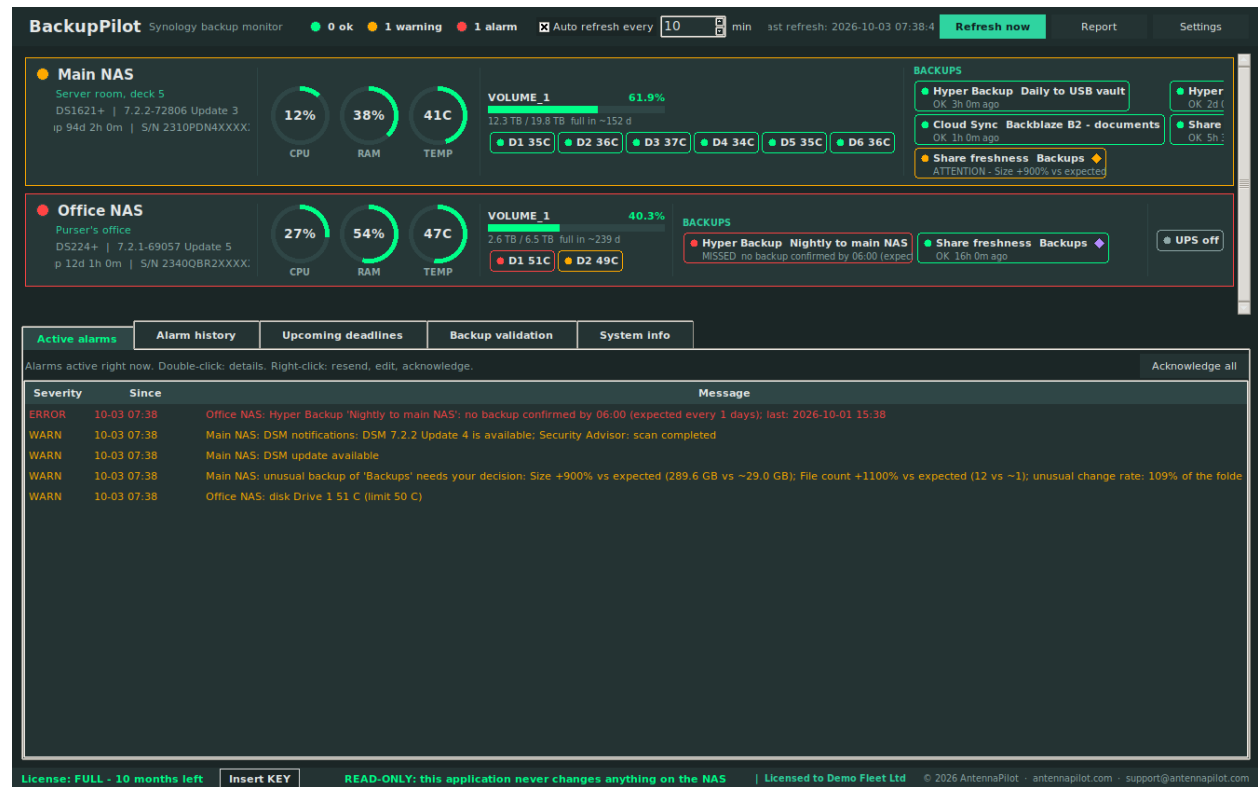


Figure 7.1 - Main window with two NAS units (demo data)

Top bar

- Counters: number of NAS units that are **ok**, with a **warning** or with an **alarm**.
- Auto refresh every N min** and **Refresh now**. Backup deadlines are re-evaluated every minute regardless of the refresh interval.
- Last refresh time and countdown to the next one. When a new version is available a notice appears here.
- Report** opens the backup report (chapter 12), **Settings** the configuration (chapter 8).

One row per NAS

Zone	Content
Identity	Status LED, display name, location, model, DSM version, uptime, serial number. The row border turns amber or red with the state.
System	Rings for CPU load, RAM usage and system temperature. Amber 10 units before the threshold, red at the threshold.
Storage	One bar per volume (used %, used/total, 'full in ~N d' linear estimate when there are enough samples; click for trends) and one chip per disk with its temperature; red when status or S.M.A.R.T. is not normal.
Backups	One chip per backup source. Green: monitored and confirmed in time (with 'OK Nh ago'). Red: window missed or task error. Grey: not monitored. Amber 'NEW': detected at a refresh, no monitor yet. Watched folders carry the validation badge (diamond) at the right end of the chip - see the legend in chapter 10A; click the chip for the runs and the tolerance chart.
Extra	UPS state, number of active DSM notifications (click for the list), 'restricted' when the account cannot read some sections, 'maintenance' during a maintenance window.

LED colours

Colour	Meaning
Green	Every monitored source confirmed; no selected alarm active.
Amber	A warning is active (temperature, usage, DSM notification, update available...).
Red	A backup window was missed, a task reports an error, or the NAS is unreachable.
Grey	Not refreshed yet.

Every element has a tooltip: rest the mouse on a ring, a bar, a chip or a button for the current values, the thresholds and what the element means.

Bottom tabs

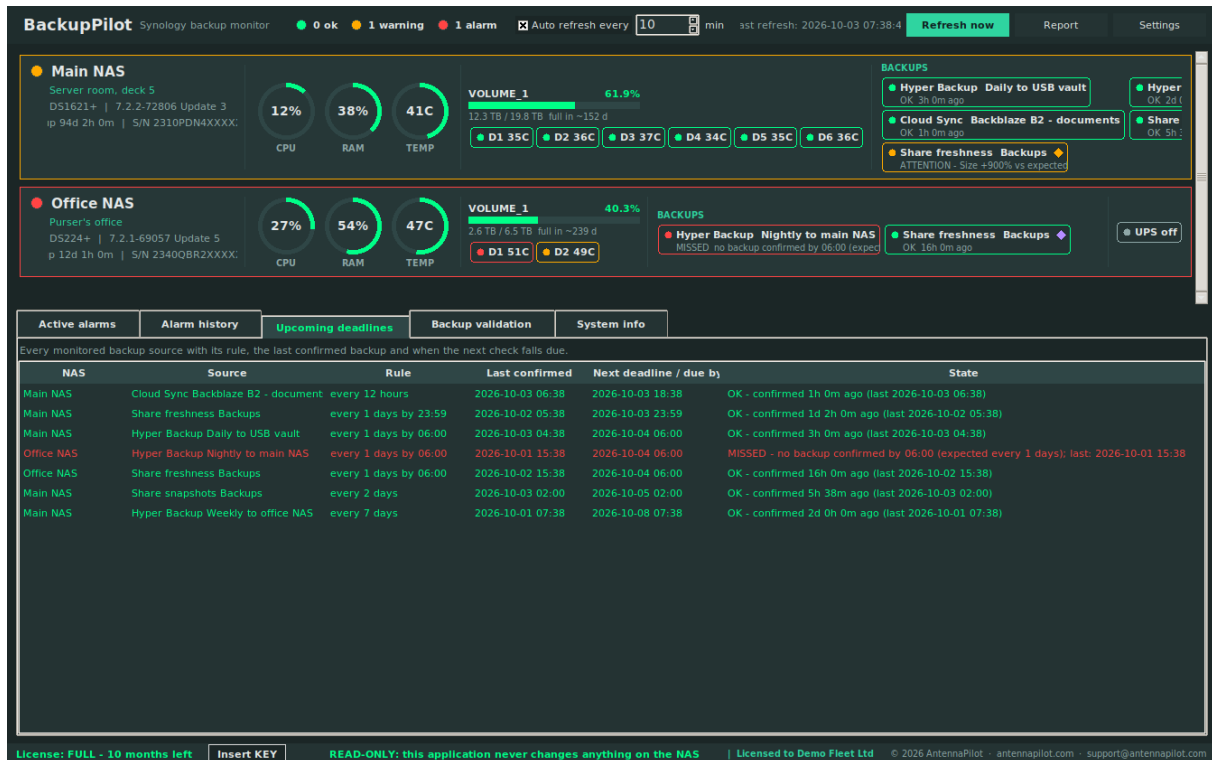
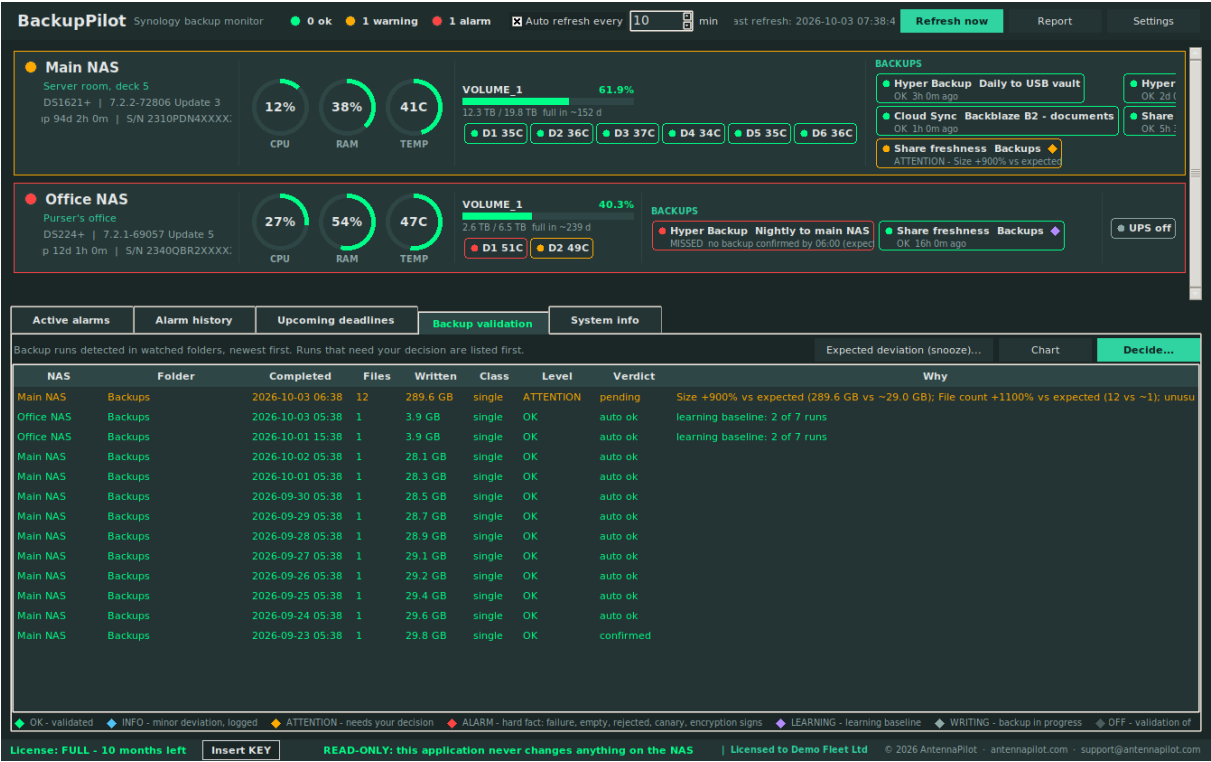


Figure 7.2 - Upcoming deadlines: every monitored source with its rule, last confirmed backup and next deadline

- **Active alarms** - what is wrong right now. Double-click: details. Right-click: Details, Resend by e-mail, Edit the rule in Settings, Acknowledge. *Acknowledge all* clears the list; a condition that persists is not re-alarmed until it ends and returns.
- **Alarm history** - every alarm with the time it appeared and the time it cleared. One alarm is one row; a persisting condition is never logged twice. Right-click: Details, Resend, Edit, Delete. Buttons: Delete cleared, Delete all.
- **Upcoming deadlines** - the monitored sources sorted by urgency, with the rule, the last confirmed backup, the next deadline and the verdict.
- **Backup validation** - every backup run detected in watched folders, newest first, with level, verdict and the reasons in words; runs waiting for your decision come first (chapter 10A).
- **System info** - version, license, e-mail configuration, escalation, report schedule, autostart, background service, data folder, read-only guard counter.



8. Settings

The Settings window has the list of NAS units on the left and tabs on the right. **Apply** saves and keeps the window open (the dashboard refreshes behind it); **Save & close** saves and closes; **Close** discards the changes made since the last Apply. The main window cannot be closed or minimized to tray while Settings is open.

8.1 NAS connection

Settings read-only access to every NAS

NAS UNITS

- Main NAS
- Office NAS

NAS connection | Backup monitor | Other alarm | Notification | Threshold | Smart validation | Startup & service

CONNECTION

Display name: Main NAS Host / IP: 10.0.10.21

Port: 5001 User: monitor

☒ Use HTTPS (recommended) Password: *****

Location / description: Server room, deck 5

Connect & detect

DETECTED BACKUP SOURCES

Type	Name	NAS status	Last confirmed
Hyper Backup	Daily to USB vault	none / done	2026-10-03 04:38
Hyper Backup	Weekly to office NAS	none / done	2026-10-01 07:38
Cloud Sync	Backups to documents	update	2026-10-03 06:38

MAINTENANCE WINDOW (ALARMS SHOWN BUT NOT NOTIFIED)

☒ Enabled from 02:00 to 04:00 ☐ Mo ☐ Tu ☐ We ☐ Th ☐ Fr ☐ Sa ☒ Su

WATCHED SHARED FOLDERS - FILE FRESHNESS AND SNAPSHOTS

Tick the shared folders to watch. For each one BackupPilot reads (read-only) the newest file time - for backups written by an external server - and, if the NAS has Btrfs snapshots on that folder, the newest snapshot. Only ticked folders are queried, one call per folder. Drag the divider above to resize this area.

- ☒ Backups
- ☐ Documents
- ☐ Photos
- ☐ Public
- ☐ Software

A ticked folder is monitored right away (every 1 day). Adjust the interval, the deadline and the channels in the next tab. **Backup monitors >**

Buttons: Add, Remove, Help, Close, Apply, Save & close

© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com

Figure 8.1 - NAS connection: credentials, detected sources, maintenance window, watched folders

- **Display name, Host / IP, Port, User, Password, Location / description.** Passwords are stored encrypted with Windows DPAPI, bound to your Windows user.
- **Connect & detect** logs in (read-only), reads model, DSM version, installed packages, backup sources, shared folders, volumes and disks. Run it again after changes on the NAS.
- **Detected backup sources** - what the NAS reports: type, name, status, last confirmed time.
- **Maintenance window** - between the two times, on the ticked days, alarms are evaluated and shown but not notified. Useful for planned reboots.
- **Watched shared folders** - tick the folders where external software writes its backups, or that have snapshots you want to watch. Only ticked folders are queried (one call per folder). A ticked folder gets a monitor immediately (every 1 day, no deadline); the button *Backup monitors >* takes you to it.
- If no backup source is found, a window lists the backup-related APIs and packages present on the NAS, so you can see whether a backup package is installed.

8.2 Backup monitors

Settings read-only access to every NAS

NAS UNITS

Main NAS
Office NAS

Add Remove

Help

NAS connectio **Backup monitor** Other alarm Notification Threshold Smart validatio Startup & servic

Select a source, set how often a backup must be confirmed and by what time, then press Apply to source.

Type	Name	Last confirmed	Monitor	Every	Deadline	Channels
Hyper Backup	Daily to USB vault	2026-10-03 04:38	ON	1 days	06:00	sound e-mail
Hyper Backup	Weekly to office NAS	2026-10-01 07:38	ON	7 days	-	sound e-mail
Cloud Sync	Backblaze B2 - documents	2026-10-03 06:38	ON	12 hours	-	e-mail
Share snapshots	Backups	2026-10-03 02:00	ON	2 days	-	e-mail
Share freshness	Backups	-	ON	1 days	23:59	sound e-mail

☒ Monitor this source

A backup must be confirmed every days

By this time of day (HH:MM, optional)

When missed, alert with ☒ Sound ☒ E-mail

Editing: Hyper Backup 'Daily to USB vault'

© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com

Figure 8.2 - Backup monitors: one rule per source

- Select a source. Tick **Monitor this source**, set **every N hours/days** and, optionally, **by this time of day** (type 6, 2359 or 23:59 - it is completed to HH:MM). Choose **Sound** and/or **E-mail**. Press **Apply to source** (or **Apply to all sources**).
- E-mail can only be ticked when it is configured in Notifications; otherwise it is greyed out.
- Right-click a source: enable/disable, apply, copy name, delete the monitor settings, remove the source. Double-click toggles the monitor.
- New sources appearing on the NAS are picked up automatically at every refresh and shown as NEW on the dashboard until you set their monitor.

8.3 Other alarms

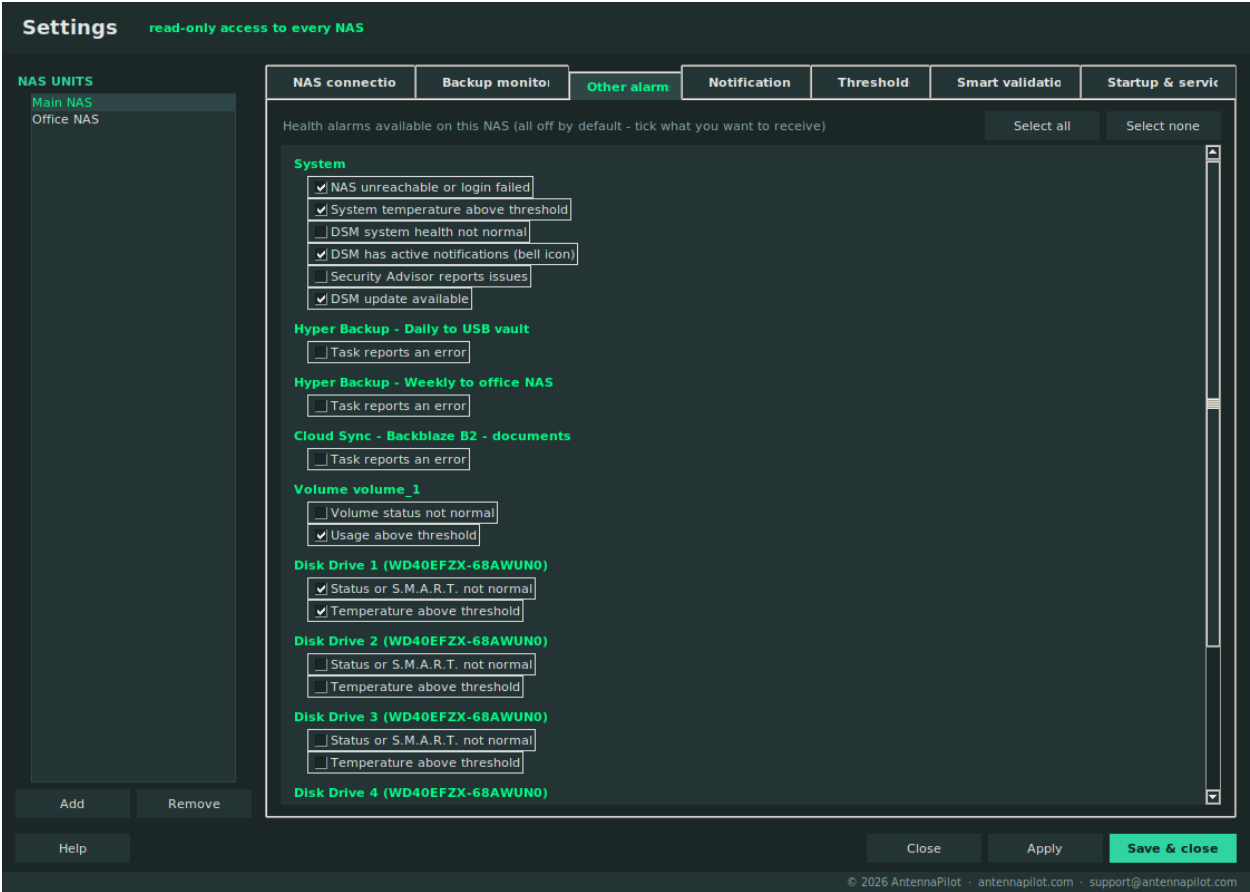


Figure 8.3 - Health alarms available on this NAS, all off by default

The list is built from what the NAS exposes: System (unreachable, temperature, DSM health, DSM notifications, Security Advisor, DSM update), every backup task ('task reports an error'), every volume (status, usage above threshold), every disk (status / S.M.A.R.T., temperature above threshold). Tick only what you want to receive. The list is refreshed at every poll; your choices are kept.

8.4 Notifications

Settings read-only access to every NAS

NAS UNITS

- Main NAS
- Office NAS

Notification:

RECIPIENTS AND CHANNELS

Send alarms to (comma separated)

☒ Sound on this computer (default)

Repeat reminder for active alarms every (hours, 0 = off)

SEND USING

☒ Outlook application on this computer ☐ SMTP server

SMTP host Port

User Password

From address ☒ STARTTLS (port 587); port 465 uses SSL

ESCALATION, REPORT AND UPDATES

Escalate unresolved alarms after (hours, 0 = off) to

Weekly report: schedule and recipients are set in Tools > Backup report.

☒ Check antennapilot.com for updates daily

E-MAIL CONTENT

Write the subject and the body in your own words and insert the values you want (NAS name, source, message...) from the list on the right; the preview shows the result with sample values. Alarm e-mails are sent as HTML with a colour band per severity. The footer with the copyright is fixed.

Subject

Body

Insert a value:

Preview

Subject: [BackupPilot] ERROR | Main NAS | Hyper Backup - 1

Main NAS: Hyper Backup 'Daily to USB': no backup confirmed by 06:00 (expected every 1 days)

© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com

Figure 8.4 - Recipients, channel, escalation, e-mail content

- **Send alarms to** - one or more addresses, comma separated. **Sound on this computer** is the default for health alarms (monitors have their own switch).
- **Repeat reminder** - 0 = notify once per alarm; N = re-send active alarms every N hours until they clear.
- **Send using**: Outlook application on this computer (uses the configured Outlook profile; Outlook is started if needed) or SMTP server (host, port 587 STARTTLS or 465 SSL, user, password, sender).
- **Escalation** - if an alarm is still active after N hours, a second e-mail goes to the escalation address (for example the superintendent).
- **Check for updates daily** - reads a small version file from antennapilot.com; nothing is sent.
- **E-mail content** - subject and body templates with placeholders {app} {nas} {severity} {source} {message} {time} {site} {support}. The footer (product, web site, support address, copyright, licensee) is fixed. **Send test email** verifies the channel.

8.5 Thresholds

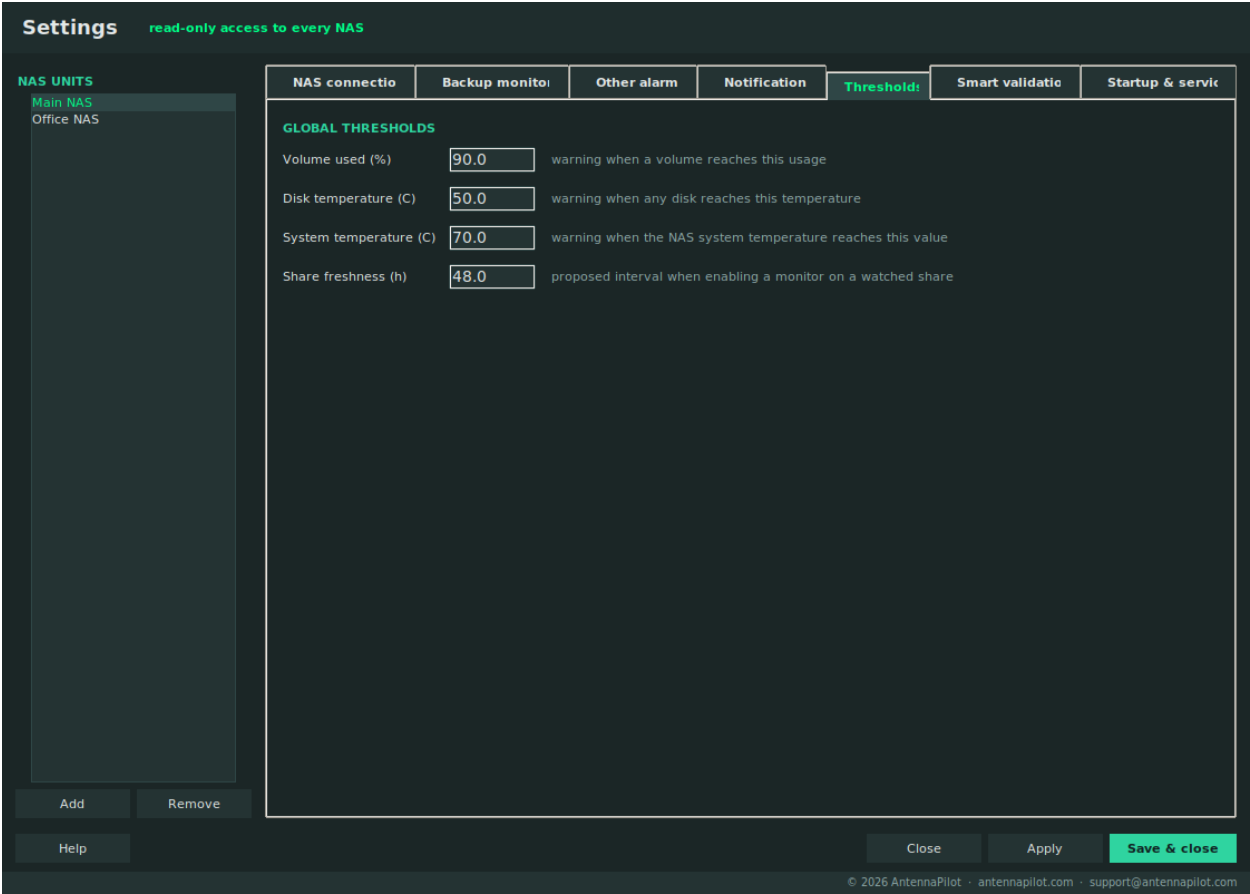


Figure 8.5 - Global thresholds

Threshold	Default	Effect
Volume used (%)	90	Warning when a volume reaches this usage; amber on the dashboard 10 points earlier.
Disk temperature (C)	55	Warning when any disk reaches this temperature.
System temperature (C)	70	Warning when the NAS system temperature reaches this value, or when DSM itself reports a temperature
Share freshness (h)	48	Proposed interval when a monitor is enabled on a watched folder.

8.6 Smart validation

Settings read-only access to every NAS

NAS UNITS

- Main NAS
- Office NAS

Smart validation

SMART BACKUP VALIDATION (WATCHED FOLDERS)

Every backup run written into a watched folder is measured (files, bytes, average file size, change rate, file types, names) and compared with the confirmed history of that folder. Full and incremental runs are told apart automatically. A run outside the tolerance band is not an alarm: it asks for your decision (confirm / exception / new normal / reject). Hard facts - 0 bytes, empty files, suspicious extensions, a changed canary file - are alarms. Everything stays read-only on the NAS.

☒ Enable smart validation

Learning runs Quiet period (min)

Tolerance factor Max tolerance

INFO band (%) Escalate after (h)

Max files scanned Folder depth

CONTENT CHECKS (OPTIONAL - DOWNLOADS A FEW SMALL FILES PER RUN, STILL READ-ONLY)

☐ Verify file signatures and entropy on a stratified sample max files max size (MB)

VALIDATION ALARMS (ON / OFF)

Which findings may raise a WARNING (needs your decision) or an ALARM. Switched off = logged only.

☒ Size outside the tolerance band **ATTENTION** ☒ File count outside the band **ATTENTION**

☒ Average file size outside the band **ATTENTION** ☒ Unusual change rate **ATTENTION**

☒ New / suspicious file types **ATTENTION / ALARM** ☒ File names off the usual pattern **INFO**

☒ Empty files written **ATTENTION / ALARM** ☒ Canary file missing or changed **ALARM**

☐ Start time shifted by more than 2 hours **INFO** ☒ Escalate unanswered decisions **ALARM**

☒ Rejected backup - RPO from last good backup **ALARM**

CANARY (SENTINEL) FILES FOR THE SELECTED NAS

Place 2-3 small files with known content in the source of the backup; list them here as paths inside the watched folder (one per line, 'folder/file.ext'). At every run BackupPilot checks that they exist in the backup with the same size and hash as first seen. Reset the reference after you change them on purpose.

Watched folder NAS: Main NAS

only_on_main.txt

Buttons: Add, Remove, Help, Close, Apply, Save & close

© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com

Figure 8.6 - Smart validation: learning, tolerance, content checks, alarms ON/OFF, canary files, legend

- **Enable smart validation** - master switch for all watched folders.
- **Learning runs** (7), **Quiet period** (15 min), **Tolerance factor** (2.0 = half to double), **Max tolerance** (3.0, ceiling of the adaptive band), **INFO band** (25%), **Escalate after** (24 h), **Max files scanned**, **Folder depth**.
- **Content checks** - optional: a stratified sample of each run (newest, largest, a few small files, up to the configured size) is downloaded up to 64 KB and checked against the format signature; text files with very high entropy look encrypted.
- **Validation alarms ON/OFF** - each finding can be switched off (logged only). The label next to each one tells the level it produces: INFO, ATTENTION (needs your decision) or ALARM.
- **Canary (sentinel) files** - per watched folder of the selected NAS: paths of 2-3 files with known content that must appear unchanged in the backup. 'Reset reference' after you change them on purpose.
- **Legend** - the colours of the validation badge, identical on the dashboard, in reports and in e-mails.

8.7 Startup & service

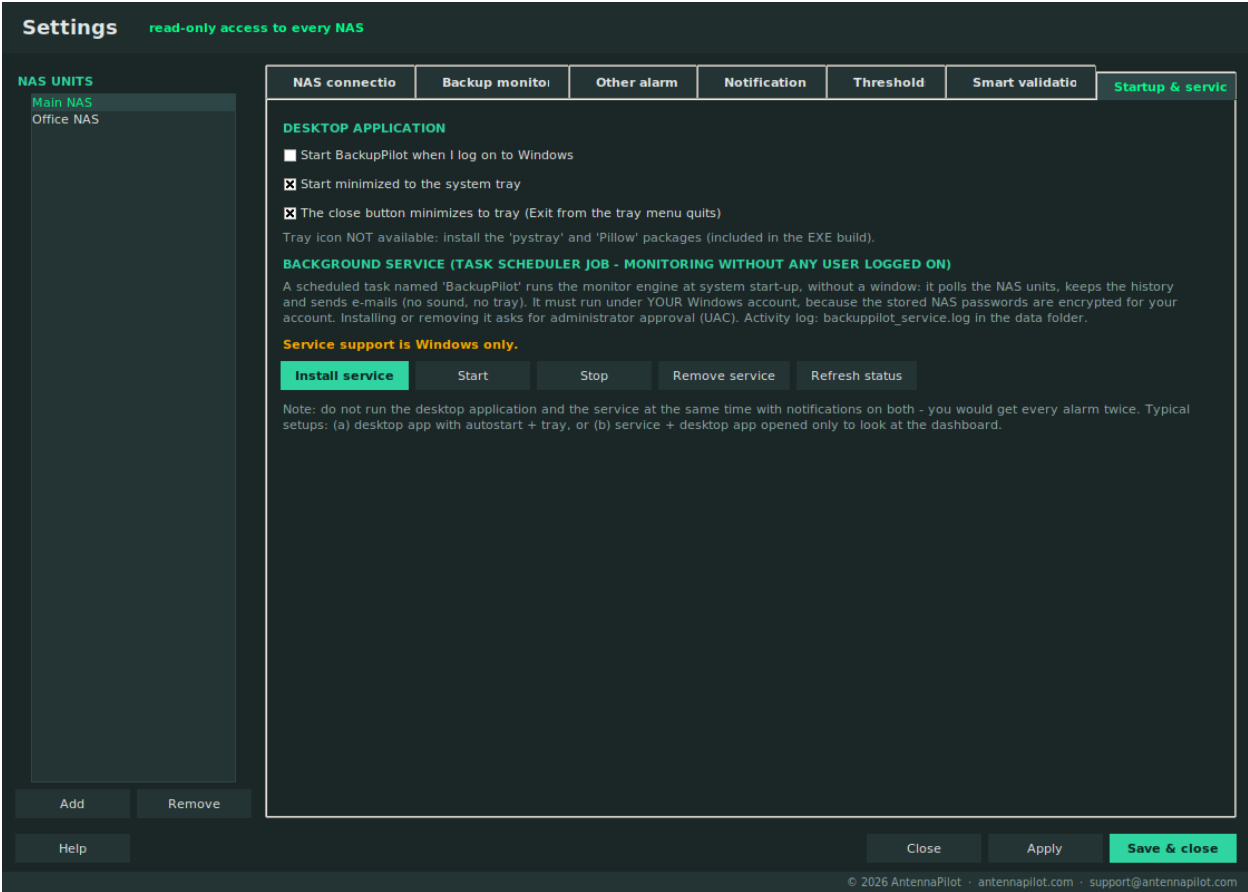


Figure 8.7 - Autostart, tray and background service

Described in chapter 14.

9. Backup monitors - how the rule works

A monitor is attached to one backup source and has three settings: **every N hours/days**, an optional **deadline** (time of day) and the **channels**.

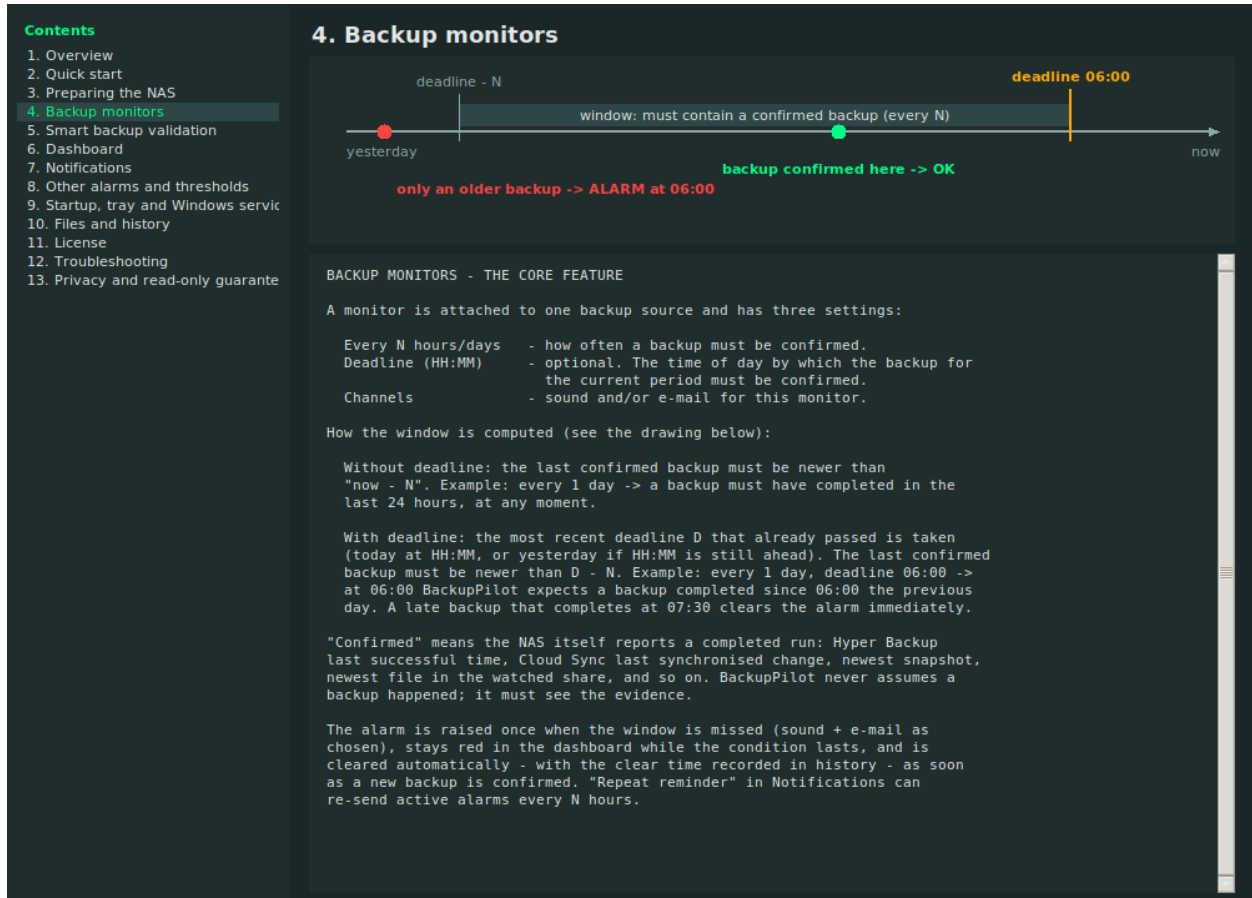


Figure 9.1 - The built-in help chapter with the timeline drawing

Without deadline (rolling window)

The last confirmed backup must be newer than $\text{now} - N$. Example: every 12 hours - at any moment a backup must have completed in the last 12 hours.

With deadline

The most recent deadline D that already passed is taken (today at HH:MM, or yesterday if HH:MM is still ahead). The last confirmed backup must be newer than $D - N$. Example: every 1 day by 06:00 - at 06:00 BackupPilot expects a backup completed since 06:00 the previous day. A late backup that completes at 07:30 clears the alarm immediately.

Rule	Means
every 1 day by 06:00	Nightly backup. Checked at 06:00 every morning; a backup finished between yesterday 06:00 and now is required.
every 1 day by 23:59	A backup must be written every calendar day. The check happens at midnight.
every 7 days, no deadline	Weekly backup, checked continuously: the last confirmed backup must be less than 7 days old.
every 4 hours, no deadline	Frequent sync (Cloud Sync, ShareSync): something must have been synchronised in the last 4 hours.

What 'confirmed' means

BackupPilot never assumes a backup happened; it must see the evidence reported by the NAS: Hyper Backup last successful run, Active Backup last backup time, Snapshot Replication plan time, Cloud Sync last synchronised change, ShareSync last activity, the newest snapshot of a folder, the newest file inside a watched folder.

The alarm is raised once when the window is missed (sound + e-mail as chosen), stays red while the condition lasts, and clears automatically - with the clear time recorded in history - as soon as a new backup is confirmed.

10. Alarms

An alarm has a severity (ERROR or WARN), a key (what it is about), a message and a lifetime: it appears when the condition starts and clears when it ends. Backup monitors raise ERROR alarms; health rules raise WARN (thresholds) or ERROR (status not normal, unreachable, task error).

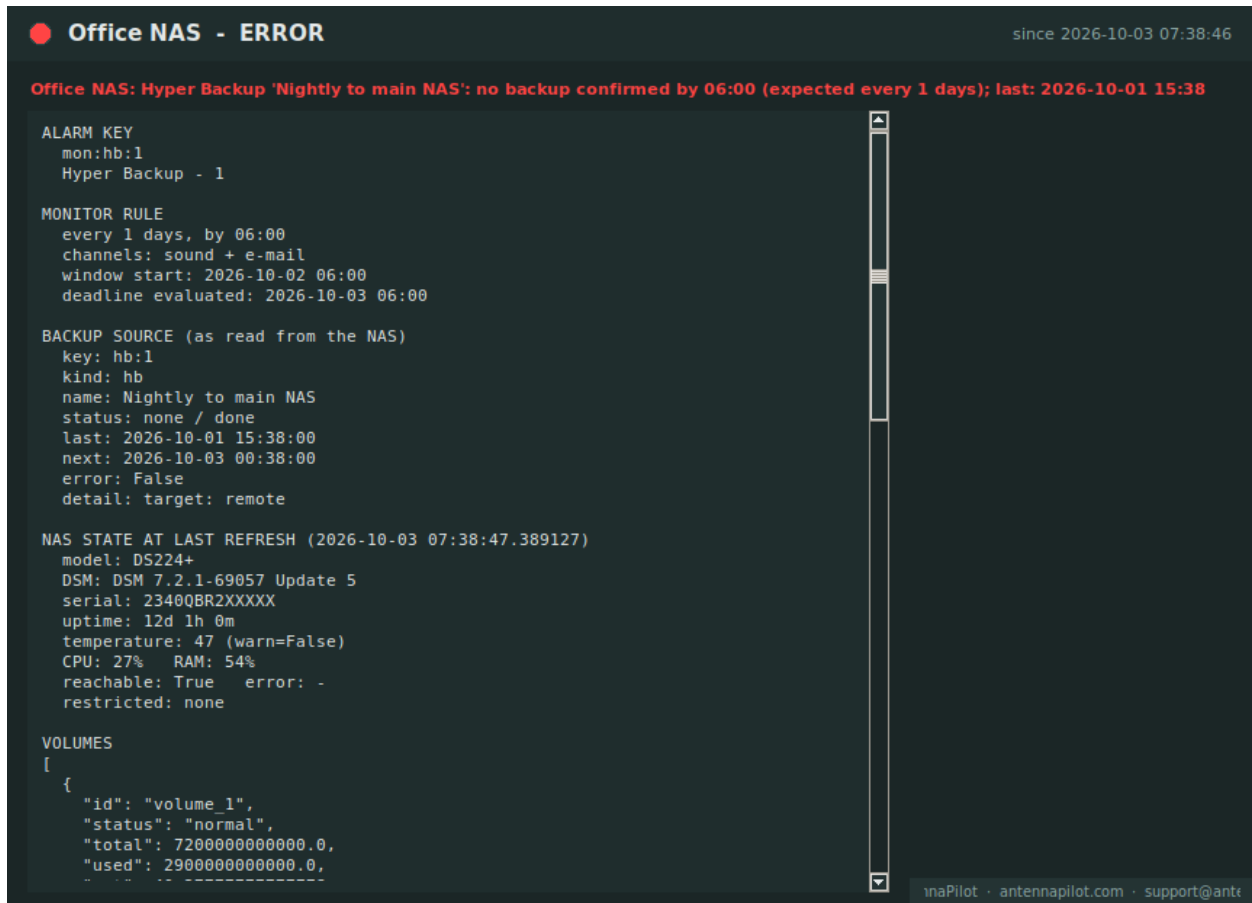


Figure 10.1 - Alarm details: the rule, the source and all data read from the NAS at the last refresh

- **Details** (double-click) shows the monitor rule with the evaluated window, the backup source as read from the NAS with raw data, the NAS state, volumes, disks, DSM notifications, all sources and the detection debug.
- **Acknowledge** removes an alarm from the active list; the history row is marked cleared. A condition that is still present is not re-alarmed until it ends and comes back.
- **Resend by e-mail** sends the alarm again to the configured addresses; **Edit the rule** opens Settings directly on the relevant NAS, tab and source.
- When the NAS is unreachable, the last known sources are kept and the monitors keep evaluating on them; the row shows 'showing last known data'.
- DSM notifications (the bell icon in DSM) are listed by clicking the chip on the row; they are DSM's own messages and are dismissed in DSM.

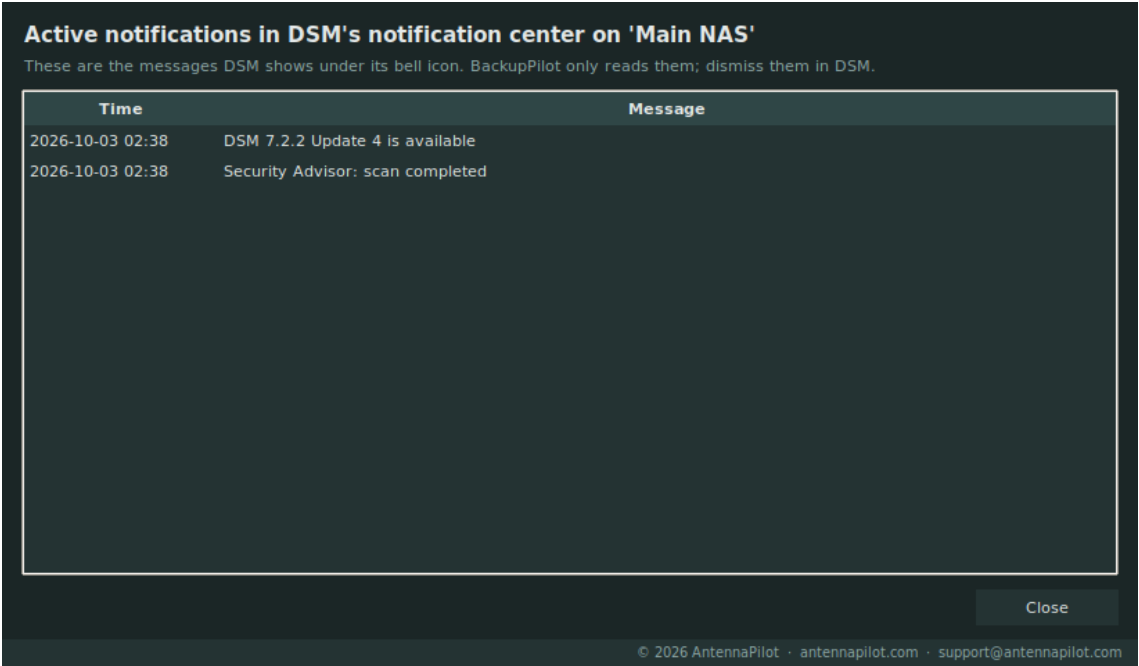


Figure 10.2 - Active DSM notifications of a NAS

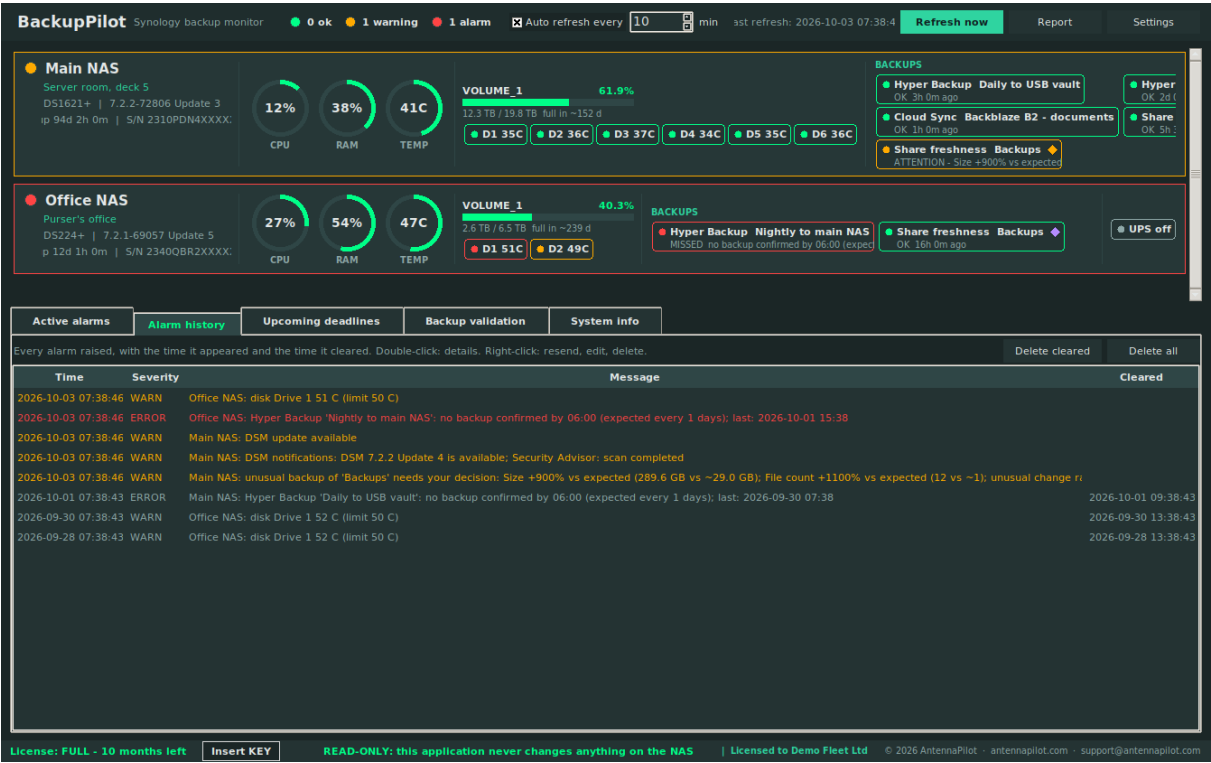


Figure 10.3 - Alarm history

10A. Smart backup validation

A freshness check tells you that something was written in the watched folder. It cannot tell you that a job which failed after writing a 2 KB log file is broken, or that a backup is half the usual size. Smart validation adds that judgement - and keeps the human in the loop. Everything stays read-only on the NAS.

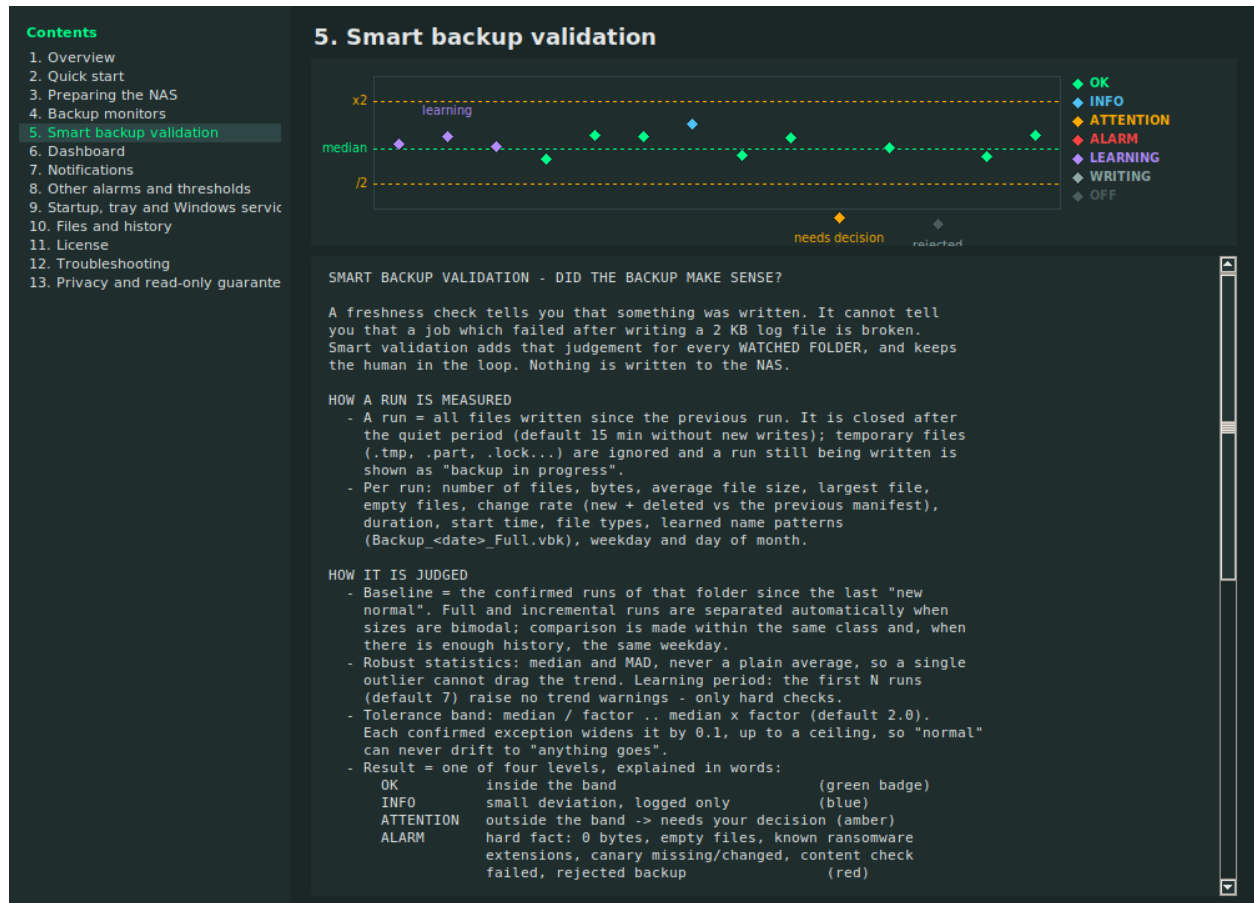


Figure 10A.1 - Built-in help: runs, tolerance band, decisions and the badge legend

How a run is measured

- A run = all files written since the previous run. It is closed after the quiet period (default 15 min without new writes); temporary files (.tmp, .part, .lock...) are ignored and a run still being written is shown as 'backup in progress'.
- Per run: number of files, bytes, average file size, largest file, empty files, change rate (new + deleted files vs the previous manifest), duration, start time, file types, learned name patterns (Backup_<date>_Full.vbk), weekday and day of month.

How it is judged

- Baseline = the confirmed runs of that folder since the last 'new normal'. Full and incremental runs are separated automatically when sizes are bimodal; the comparison is made within the same class and, when there is enough history, the same weekday.
- Robust statistics: median and MAD, never a plain average, so one outlier cannot drag the trend. The first N runs (default 7) raise no trend warnings - only hard checks.
- Tolerance band = median / factor .. median x factor. Each confirmed exception widens it by 0.1, up to a ceiling, so 'normal' can never drift to 'anything goes'.
- Every finding is explained in words, e.g. *Size -62% vs expected (12.4 GB vs ~33 GB); file count -80%; usual for this class and weekday: ~33 GB (median of 9 runs).*

Badge	Level	Meaning
OK	OK	Inside the band - validated.
INFO	INFO	Small deviation, only logged (under the INFO band).

Badge	Level	Meaning
◆	ATTENTION	Outside the band - the run is quarantined and asks for your decision (WARNING on the dashboard and by e-mail).
◆	ALARM	Hard fact: 0 bytes, all files empty, known ransomware extensions, canary file missing or changed, content check failed, backup rejected by the operator.
◆	LEARNING	Baseline still being built (fewer than N runs).
◆	WRITING / OFF	A run is in progress / validation switched off.

Your decision

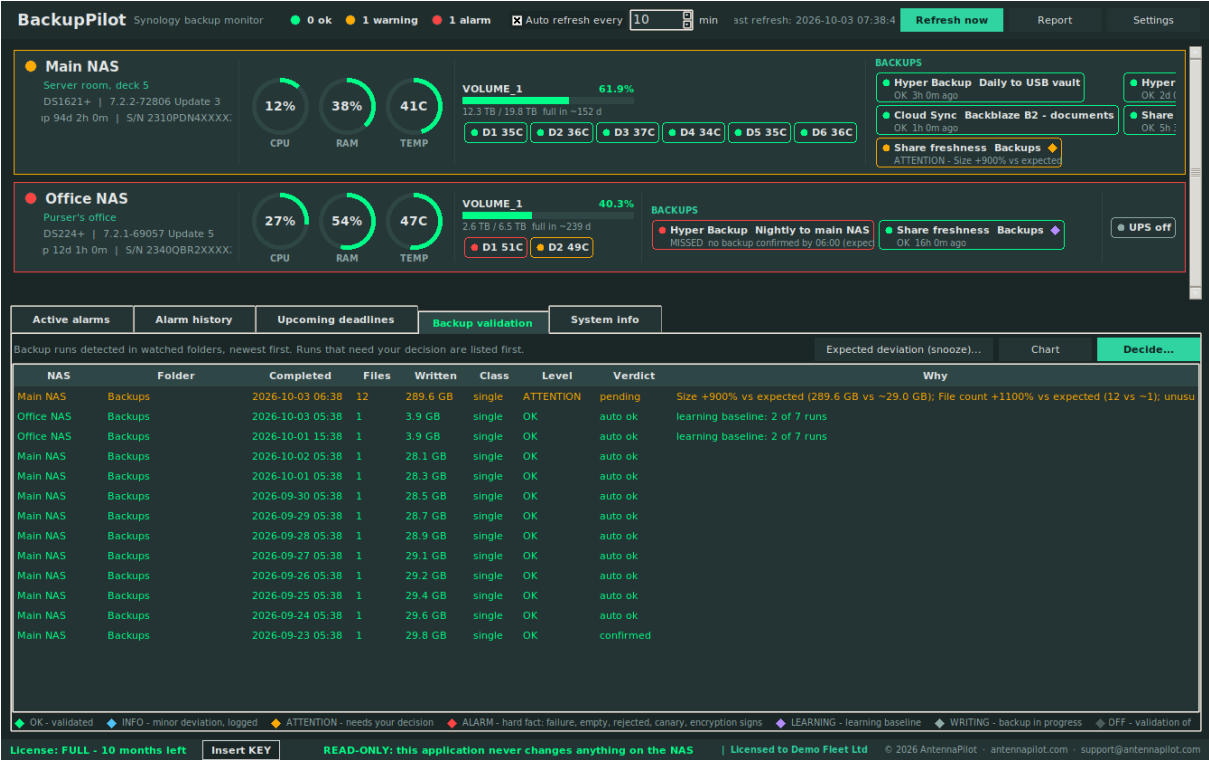


Figure 10A.2 - Backup validation tab: runs newest first, pending decisions on top, legend at the bottom

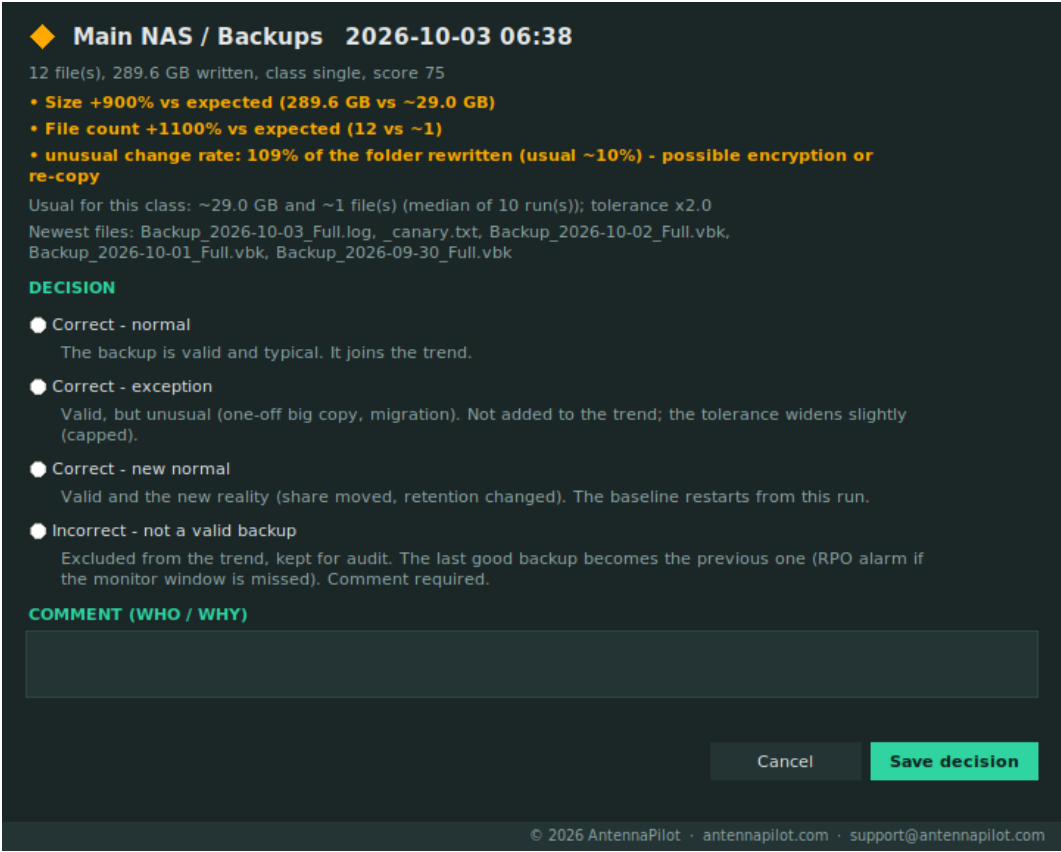


Figure 10A.3 - Decision window: the finding in words, the usual values, four choices and the mandatory comment for a rejection

Decision	Effect on the trend
Correct - normal	The backup is valid and typical; it joins the baseline.
Correct - exception	Valid but one-off (a big manual copy, a migration). Not added to the baseline; the tolerance widens by 0.1, capped.
Correct - new normal	Valid and the new reality (share moved, retention changed). The baseline restarts from this run. If three runs in a row deviate the same way, this is the decision to consider.
Incorrect	Not a valid backup. Excluded from the trend, kept for audit, comment required. The last GOOD backup becomes the previous one, so the monitor window (RPO) is measured from there: a missed window is an alarm even though the deviation itself was only a warning.

- Quarantine: until you decide, the run is not part of the trend. After 'Escalate after' hours without a decision the warning becomes an alarm.
- Decisions are stored with your Windows user name, time and comment, and appear in the chart (rejected runs in grey, exceptions in blue).
- 'Expected deviation (snooze)' marks a source for N days (migration, re-full): deviations are logged as INFO instead of asked.
- Anti-fatigue: one open question per source; reminders follow the normal reminder interval.

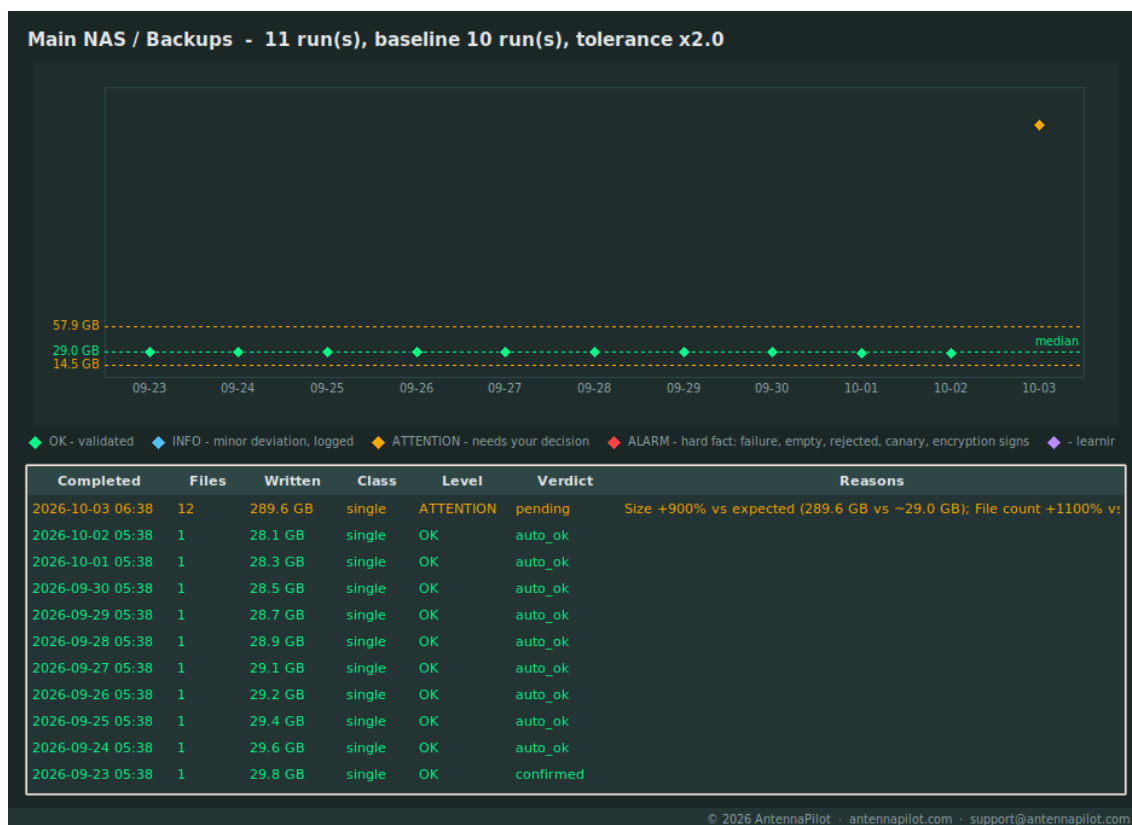


Figure 10A.4 - Runs of one folder with the median and the tolerance band; the amber point waits for a decision

Extra signals

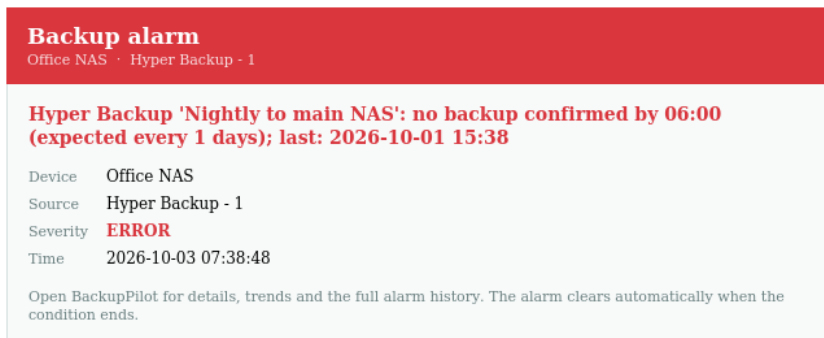
- **Canary files:** 2-3 sentinel files with known content placed in the source. BackupPilot checks that they appear in the backup with the same size and hash as first seen - the most direct proof that the job copies what it should.
- **Ransomware signs:** known extensions (.locked, .enc...), file types never seen before in that folder, a change rate near 100% when it is usually low and, with content checks on, format signatures (a PDF must start with %PDF, Office files as ZIP) and the entropy of text files.
- **Content checks** are optional and bounded: a stratified sample (newest, largest, a few small files) is downloaded up to 64 KB each - still read-only.

What it cannot do (by design)

It does not restore files to test them and it cannot compare the backup with the source server; both would need write access or an agent. Keep the integrity check and restore test of your backup software for the final proof. BackupPilot tells you when its result stops looking like the previous ones, and shows you why.

11. E-mail notifications

Alarm e-mails are sent as HTML (with a plain-text alternative): a band coloured by severity, the message, device, source, severity, time and location. The subject is *[BackupPilot] ERROR | device | source* by default and can be changed with the templates.



© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com | Licensed to Demo Fleet Ltd

Synology, DiskStation, RackStation, DSM, Hyper Backup, Active Backup for Business, Cloud Sync and Synology Drive are trademarks or registered trademarks of Synology Inc. BackupPilot is an independent product of AntennaPilot and is not affiliated with, endorsed by or sponsored by Synology Inc. All other trademarks are the property of their respective owners.

Figure 11.1 - Alarm e-mail (HTML)

- **Reminder** e-mails repeat active alarms every N hours (Notifications > Repeat reminder).
- **Escalation** e-mails go to the escalation address when an alarm is still active after N hours.
- **Resent** e-mails are sent manually from the alarm's context menu.
- In a maintenance window no e-mail or sound is sent; the alarm is still shown.
- The e-mail channel is only used when it is configured (recipient and, for SMTP, a server host). Otherwise it is greyed out everywhere.

12. Backup report

The toolbar button **Report** opens the report on screen: KPI header (devices, backups confirmed now, without backup monitor, missed windows and other alarms in the period), then one card per device with its state, backup sources (rule, last confirmed, confirmed/missed counts, verdict), missed windows and alarms of the period, storage with a linear 'full in ~N days' estimate, 30-day charts of volume usage and disk temperatures, disks with S.M.A.R.T., active DSM notifications, and - for watched folders - the backup validation section: level badge, latest runs with their verdicts and the finding in words, with the legend. The e-mail version counts the runs waiting for your decision.

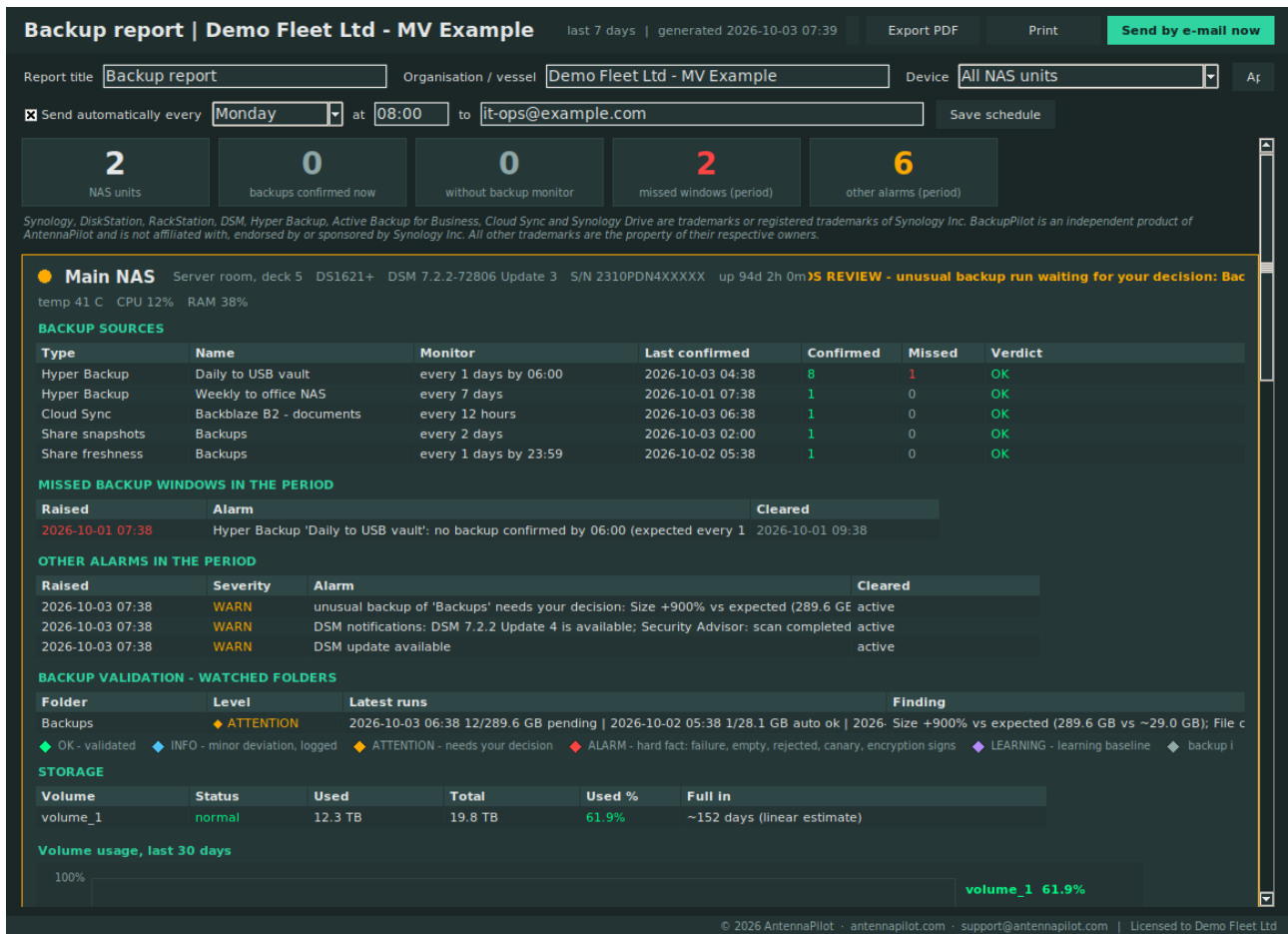


Figure 12.1 - Report on screen

Device states in the report

State	Meaning
BACKUPS CONFIRMED	Every monitored source has a confirmed backup inside its window at this moment.
BACKUP MISSED	At least one monitored source is outside its window, or a missed-window alarm is still active.
NO BACKUP MONITOR	Sources may be detected but no monitor is set, so nothing can be confirmed. The report never claims a backup is fine without a rule.
NOT REACHABLE	The last poll failed (with the reason).
NO DATA YET	The device has not been polled in this session.

- **Report title** and **Organisation / vessel** are editable and appear on screen, in the PDF and in the e-mail subject. **Device** selects all units or one device.
- **Export PDF** asks where to save the PDF and opens it. **Print** asks where to save it, then sends it to the default printer.
- **Send by e-mail now** sends an HTML summary (alarms first) with the PDF attached; you are asked whether to keep a copy of the PDF.
- **Send automatically every** weekday / time / recipients - the weekly e-mail attaches the PDF without saving anything on disk.
- Only data read from the NAS and from the history is shown; the only estimate is the storage forecast, marked as a linear estimate.



Figure 12.2 - PDF report, summary page



Figure 12.3 - PDF report, one page per device

Backup report

Demo Fleet Ltd - MV Example

Last 7 days · generated 2026-10-03 07:38 · read-only monitoring of Synology NAS units

2	0	0	2	6
NAS units	backups confirmed now	without backup monitor	missed windows (period)	other alarms (period)

Main NAS

Server room, deck 5 DS1621+ DSM 7.2.2-72806 Update 3

NEEDS REVIEW - unusual backup run waiting for your decision: Backups

Raised	Severity	Alarm	Cleared
2026-10-01 07:38	ERROR	Hyper Backup 'Daily to USB vault': no backup confirmed by 06:00 (expected every 1 days); last: 2026-09-30 07:38	2026-10-01 09:38
2026-10-03 07:38	WARN	unusual backup of 'Backups' needs your decision: Size +900% vs expected (289.6 GB vs ~29.0 GB); File count +1100% vs expected (12 vs ~1); unusual change rate: 109% of the folder rewritten (usual ~10%) - possible encryption or re-copy	STILL ACTIVE
2026-10-03 07:38	WARN	DSM notifications: DSM 7.2.2 Update 4 is available; Security Advisor: scan completed	STILL ACTIVE
2026-10-03 07:38	WARN	DSM update available	STILL ACTIVE

Backup source	Monitor	Last confirmed	Confirmed	Missed	Verdict
Hyper Backup Daily to USB vault	every 1 days by 06:00	2026-10-03 04:38	8	1	OK
Hyper Backup Weekly to office NAS	every 7 days	2026-10-01 07:38	1	0	OK
Cloud Sync Backblaze B2 - documents	every 12 hours	2026-10-03 06:38	1	0	OK
Share snapshots Backups	every 2 days	2026-10-03 02:00	1	0	OK
Share freshness Backups	every 1 days by 23:59	2026-10-02 05:38	1	0	OK

Backup validation	Level	Latest runs	Finding
Backups	ATTENTION	2026-10-03 06:38 - 12 files / 289.6 GB - pending 2026-10-02 05:38 - 1 files / 28.1 GB - auto ok 2026-10-01 05:38 - 1 files / 28.3 GB - auto ok	Size +900% vs expected (289.6 GB vs ~29.0 GB); File count +1100% vs expected (12 vs ~1)

Storage: volume_1 61.9% (12.3 TB / 19.8 TB) - full in ~152 days (linear estimate) · Disks: 6 total, 0 with problems

Office NAS

Purser's office DS224+ DSM 7.2.1-69057 Update 5

BACKUP MISSED - 1 of 2 monitored source(s) not confirmed

Raised	Severity	Alarm	Cleared
2026-10-03 07:38	ERROR	Hyper Backup 'Nightly to main NAS': no backup confirmed by 06:00 (expected every 1 days); last: 2026-10-01 15:38	STILL ACTIVE
2026-09-28 07:38	WARN	disk Drive 1 52 C (limit 50 C)	2026-09-28 13:38
2026-09-30 07:38	WARN	disk Drive 1 52 C (limit 50 C)	2026-09-30 13:38
2026-10-03 07:38	WARN	disk Drive 1 51 C (limit 50 C)	STILL ACTIVE

Backup source	Monitor	Last confirmed	Confirmed	Missed	Verdict
Hyper Backup Nightly to main NAS	every 1 days by 06:00	2026-10-01 15:38	8	1	MISSED
Share freshness Backups	every 1 days by 06:00	2026-10-02 15:38	1	0	OK

Backup validation	Level	Latest runs	Finding
Backups	LEARNING	2026-10-03 05:38 - 1 files / 3.9 GB - auto ok 2026-10-01 15:38 - 1 files / 3.9 GB - auto ok	learning baseline: 2 of 7 runs

Storage: volume_1 40.3% (2.6 TB / 6.5 TB) - full in ~239 days (linear estimate) · Disks: 2 total, 0 with problems

◆ 1 backup run(s) wait for your decision in BackupPilot (Backup validation tab).

Validation badge: ◆ green validated · blue minor deviation · amber needs your decision · red hard fact (failure, empty, rejected, canary, encryption signs) · purple learning baseline

Full report with charts in the attached PDF.

© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com | Licensed to Demo Fleet Ltd
Synology, DiskStation, RackStation, DSM, Hyper Backup, Active Backup for Business, Cloud Sync and Synology Drive are trademarks or registered trademarks of Synology Inc. BackupPilot is an independent product of AntennaPilot and is not affiliated with, endorsed by or sponsored by Synology Inc. All other trademarks are the property of their respective owners.

Figure 12.4 - Report e-mail body (the PDF is attached)

13. Trends

Tools > Trends, or click a volume bar on the dashboard. Volume usage and disk temperatures over the last 30 days, from the samples database. The 'full in ~N days' forecast is a linear fit of the last samples; it is shown only when the volume is growing and the result is under 10 years.

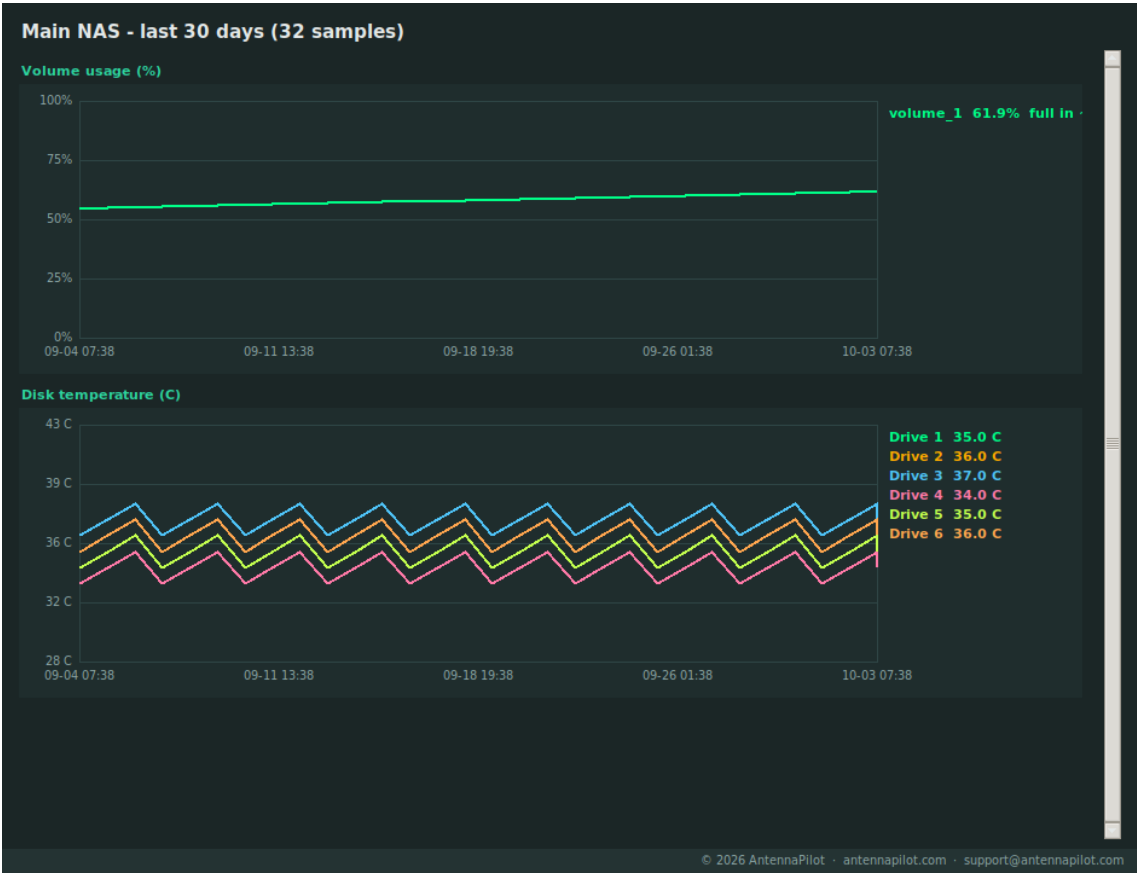


Figure 13.1 - Trends window

14. Running permanently

Monitoring only works while the engine runs. Settings > Startup & service offers two ways:

A) Desktop application with autostart

- **Start BackupPilot when I log on to Windows** - added to the user's Run key; no administrator rights needed.
- **Start minimized to the system tray and The close button minimizes to tray.** The tray icon shows alarms as balloons; right-click it for Open / Refresh / Settings / Exit. Exit from the tray menu quits.
- Requirement: a user must be logged on (the lock screen is fine).

B) Background service (no user logged on)

- A Windows Task Scheduler job named **BackupPilot** runs the monitor engine at system start-up, 'run whether user is logged on or not', without a window: it polls the NAS units, keeps the history and sends e-mails (no sound, no tray).
- It must run under **your** Windows account, because the NAS passwords are encrypted for your account. **Install service** asks for your Windows password and for administrator approval (UAC), creates the task with a 1-minute delay after boot and starts it.
- **Start, Stop, Remove service** and **Refresh status** manage the same job; it is also visible in Task Scheduler. Its activity is written to `backuppilot_service.log` in the data folder.
- Open the desktop application any time to look at the dashboard; it reads the same settings and history. Do not keep notifications on in both at the same time, or every alarm arrives twice.
- Command line: `BackupPilot.exe --headless` runs the engine without a window; `--tray` starts minimized.

Maintenance window

Per NAS (Settings > NAS connection): between the two times, on the ticked days, alarms are evaluated and displayed but no sound or e-mail is sent. Useful for planned reboots and DSM updates.

15. Files, data and the read-only guarantee

File (in %APPDATA%\BackupPilot)	Content
<code>backuppilot_config.json</code>	Settings. NAS passwords and the SMTP password are encrypted with Windows DPAPI, bound to your Windows user.
<code>backuppilot_history.db</code>	SQLite: alarms (with cleared time), samples (90 days), confirmed backup times per source, validation runs with decisions, folder manifests, canary references.
<code>backuppilot_error.log</code>	Internal errors, if any. Help > Report a bug attaches its tail.
<code>backuppilot_service.log</code>	Heartbeat of the background engine.
<code>backuppilot_bugreport_*.txt</code>	Full text of a bug report prepared with Help > Report a bug.

Read-only guarantee

Every call to the DSM API goes through one function in the program that checks the method name against a whitelist of read methods (`list`, `get`, `getinfo`, `status`, `load_info`, `query`, `list_conn`, `get_recently_change`, `notify/load`, `system_get...`). Any other method is refused before it is sent, logged, and counted in System info. The application therefore cannot start, stop, modify or delete anything on the NAS, even by mistake, whatever the rights of the account.

Privacy

- Credentials never leave the computer; there is no cloud component and no telemetry.
- The only outgoing connections are: the NAS units, your mail server or Outlook, and - if enabled - a daily read of a small version file on antennapilot.com.
- TLS certificate validation is relaxed to accept the self-signed certificates most NAS units use; use a trusted network or VPN.
- Reports and bug reports contain NAS names, models, serial numbers and alarm texts; review them before sending outside your organisation.

16. Troubleshooting

Symptom	What to check
NAS unreachable (no API answer)	Wrong host/port, firewall, HTTPS/HTTP mismatch. Check DSM > Control Panel > Login Portal for the real ports. Try the other port.
Login failed: Wrong user or password (400)	Check the credentials. DSM may block the IP after several failures (Auto Block).
Login failed: 2FA code required (403)	Disable 2-step verification on the monitoring account.
Sections marked 'restricted'	The account lacks permission. Add it to 'administrators' or accept the reduced view.
No backup source found	No backup package is installed and no snapshots exist. Tick the folder where backups are written under Watched shared folders. The detection window lists the APIs and packages found.
A monitor shows 'last: -'	The NAS never reported a completed run for that source. For Cloud Sync the time comes from recently changed files; a connection with no changes yet has no evidence.
Outlook error	Outlook must be installed with a configured profile. Allow the security prompt the first time. Otherwise use SMTP.
The weekly report / alarms arrive twice	Both the desktop application and the background service are running with notifications on. Use one, or turn notifications off in the other.
Red banner at the top of the window	An internal error was caught and written to backuppilot_error.log; the application keeps running. Click to dismiss; use Help > Report a bug if it repeats.
Settings do not persist	Settings are saved per Windows user in %APPDATA%\BackupPilot; check that the folder is writable (a message is shown if saving fails).

17. Support, bug reports and updates

- **Help > Help contents** - the built-in manual with illustrations (figure 17.1).
- **Help > Check for updates** - compares the installed version with the version published on antennapilot.com and offers the installer download.
- **Help > Report a bug / request support** - opens your e-mail client with a message to support@antennapilot.com already filled in (version, Windows, license state and fingerprint, e-mail method, service state, every NAS with model/DSM/sources/monitors, active alarms, the last lines of the error log). The full text is also copied to the clipboard and saved in the data folder.
- **Tools > Export diagnostics** - a JSON snapshot of the last readings for support.
- **Help > About** - version, license, fingerprint.

Contents

- Overview
- Quick start
- Preparing the NAS
- Backup monitors
- Smart backup validation
- Dashboard**
- Notifications
- Other alarms and thresholds
- Startup, tray and Windows service
- Files and history
- License
- Troubleshooting
- Privacy and read-only guarantee

6. Dashboard

- GREEN - all backups confirmed, nothing selected is active
- AMBER - warning active (temperature, usage, DSM notification)
- RED - backup window missed or error active
- GREY - not refreshed yet

THE DASHBOARD

Top bar: overall status (number of NAS units OK / warning / error), last refresh time and next automatic refresh.

Each NAS has a card:

- Header - status LED, name, model, DSM version, serial, uptime.
- System - gauges for CPU, RAM and system temperature.
- Backups - one row per backup source: LED, type, name, NAS status, last confirmed time and the monitor verdict (e.g. "confirmed 3h ago" or "MISSED - no backup by 06:00").
- Storage - a gauge per volume (used %) and per disk (temperature, with the S.M.A.R.T. status underneath).
- Extra - UPS, USB disks, DSM notifications, Security Advisor, update.

LED colours (legend below):

- GREEN - all monitors confirmed, no selected alarm active.
- AMBER - a warning is active (temperature, usage, DSM notification...).
- RED - a backup window was missed or an error is active.
- GREY - not refreshed yet.

Gauge colours turn amber 10 units before the threshold and red at the threshold or when a status is not normal.

Bottom: four tabs - Active alarms, Alarm history, Upcoming deadlines (every monitored source with its rule, last confirmed backup and the next deadline, sorted by urgency) and System info (version, license, e-mail, service, data folder). The NAS rows above take only the height they need; the rest of the window goes to the tabs.

- Double-click an alarm - details window with the rule, the backup source and all data read from the NAS at the last refresh (volumes, disks, notifications, raw task data, detection debug).
- Right-click an alarm - Details, Resend by e-mail, Edit the rule in Settings, Acknowledge (active) / Delete (history).
- Acknowledge all - clears the active list; a condition that is still present is not re-alarmed until it ends

Figure 17.1 - Built-in help

Appendix A. DSM APIs used (read-only)

API	Method	Used for
SYNO.API.Info / SYNO.API.Auth	query / login, logout	Discover available APIs; session
SYNO.DSM.Info	getinfo	Model, DSM version, serial, uptime, temperature
SYNO.Core.System.Utilization	get	CPU and RAM load
SYNO.Core.Package	list	Installed packages
SYNO.Storage.CGI.Storage	load_info	Volumes, disks, S.M.A.R.T., temperatures
SYNO.Core.Share / .Snapshot	list	Shared folders; snapshots of watched folders
SYNO.FileStation.List	list, getinfo	Files of watched folders (manifest, runs), canary files
SYNO.FileStation.Download	download (first 64 KB / 5 MB)	Optional content checks and canary hash - read only
SYNO.Backup.Task	list, status (offline)	Hyper Backup tasks
SYNO.ActiveBackup.Task	list	Active Backup for Business tasks
SYNO.DR.Plan	list	Snapshot Replication plans
SYNO.CloudSync	list_conn, get_recently_change	Cloud Sync connections and last change
SYNO.SynologyDriveShareSync.Connection	list	Drive ShareSync connections
SYNO.Core.DSMNotify	notify (load)	Active DSM notifications
SYNO.Core.System.SystemHealth	get	DSM health
SYNO.Core.SecurityScan.Status	system_get	Security Advisor summary
SYNO.Core.Upgrade	status	DSM update availability
SYNO.Core.ExternalDevice.UPS / .Storage.USB	get / list	UPS state, USB devices

Appendix B. Glossary

Term	Meaning
Backup source	Anything on the NAS that evidences a backup: a task, a sync connection, snapshots of a folder, or the newest file in a watched folder.
Monitor	The rule attached to a source: every N hours/days, optional deadline, channels.
Window	The period in which a confirmed backup must exist for the monitor to be satisfied.
Confirmed	The NAS reported a completed backup at a given time; BackupPilot does not assume it.
Watched folder (share freshness)	A shared folder whose newest file time is used as the last confirmed backup - for external backup software.
Acknowledge	Remove an active alarm from the list without clearing the underlying condition; it is not re-alarmed until it ends and returns.
Run	The set of files written into a watched folder since the previous run, closed after the quiet period.
Baseline / band	The confirmed runs used as reference and the tolerance interval (median / factor .. median x factor) around their median.
Canary file	A sentinel file with known content placed in the source; it must appear unchanged in the backup.
Fingerprint	A code derived from the computer's hardware and Windows installation, to which the license key is bound.

Copyright and trademarks

© 2026 AntennaPilot · antennapilot.com · support@antennapilot.com. All rights reserved. This document describes BackupPilot 1.2; later versions may differ.

Synology, DiskStation, RackStation, DSM, Hyper Backup, Active Backup for Business, Cloud Sync and Synology Drive are trademarks or registered trademarks of Synology Inc. BackupPilot is an independent product of AntennaPilot and is not affiliated with, endorsed by or sponsored by Synology Inc. All other trademarks are the property of their respective owners.