SCOM Pulse

Quick Start

Document 1.3 · 14 September 2026

You already run Operations Manager. SCOM Pulse is a browser front end for the parts of it you touch every day — the alert queue, object health, maintenance windows, overrides, and most of the Administration pane — plus a few things the console has never given you, like a queryable audit trail of operator actions and a page that explains exactly why somebody is read-only. It installs on one Windows server — a dedicated one or a management server — in about ten minutes, needs nothing on anyone's desktop, and runs a full 30-day trial with no key.

What you get that the console makes hard

The job	What you do today	In Pulse
Find what matters in 60 open alerts	Sort by severity, then age, then read	**Smart rank** orders by likely importance — severity, age, repeat count, and whether the object is in a group you pinned to the Overview
Work one alert	Alert properties, Health Explorer, the object, then hunt for the knowledge article	**One panel**: description, why it fired, product knowledge, current health, the full event timeline, the other open alerts on that host, and the actions
Explain why someone is read-only	Work backwards through user roles, scopes and group membership	`/Pulse/Access` prints every test the decision ran, what each resolved to, and the reason each one failed
See every override in the management group	Hunt pack by pack, workflow by workflow	**One list** — what changed, the target, the pack holding it, when, and the author's description
Prove what your team did and what SCOM said back	The alert's own history, one alert at a time	**Audit trail**: every action submitted, who asked, per-target outcome, filterable and exportable as JSONL
Check operational database retention and grooming	Global settings, then SQL for the sizes	**Retention, measured size and last-groomed time on one screen**, editable with confirmation
Work out whether a maintenance schedule is sane	A schedule list	**Table and calendar**, upcoming occurrences, the timezone stated, and a history of what actually ran

The job	What you do today	In Pulse
Let an operator acknowledge 20 alerts	Watch a wall of failures	**Per-target outcomes** — which succeeded, which SCOM refused, and why

None of this is a second monitoring system. Every alert, object, override and maintenance window is SCOM's own, and anything you change here the Operations console shows too.

Get it running

1. On a Windows Server 2016+ machine with .NET 4.6.2+, run **`SCOMPulse-<version>.msi`**. The Operations console is not required. If Windows warns that the publisher is not recognised, choose **More info**, check that it reads **AMTM Tech Inc**, and choose **Run anyway** — a new release carries no download history yet.
2. Accept the licence and installation folder. Confirm the management server and service account, then enter its password. Setup suggests the local SCOM Data Access account when available. Advanced options cover website placement, certificates and storage.
3. Click **Next**, then **Install**. Setup installs IIS when needed, configures Pulse and verifies its SCOM connection. Leave **Open SCOM Pulse** selected on the final page.
4. Open Pulse. There is no welcome screen and nothing to set up: an authorized person lands on their dashboard. Your SCOM Administrator role is what makes you a SCOM Pulse administrator, and your team gets in through the SCOM user roles they already hold. Somebody whose roles give no monitoring access sees an **Access status** page instead, saying why and whom to ask.

The 30-day trial starts by itself and is the full product. Thirteen setup steps run in front of you, ending with "*Connected to management group …*". Full detail, including unattended install, is in the *Installation Guide*.

> **Note — Nothing to install for users — one policy to push**
>
> Users browse to it and are signed in by Windows Authentication. There is no client and no agent change. For Edge and Chrome to sign people in **without a password box**, push one browser policy naming the site — almost always needed with an HTTPS address. **Settings** → **Access** shows the exact settings for your address, ready to copy; see *Sign people in without a password box* in the *Installation Guide*.
>
> A management pack **does** ship in the box, at `C:\Program Files\SCOM Pulse\ManagementPacks` — but setup does not import it and Pulse runs perfectly well without it. It adds SCOM-side monitoring *of Pulse*: product discovery, an alert when the service stays down, a bounded restart, and warnings before the licence expires. Import it when you are ready; see the *Installation Guide*.

Ten minutes that tell you whether it is worth it

Do these in order. Each one is something you would struggle to do as quickly in the console.

1 — Look at the alert queue you already have

Open **Alerts**. It opens on active alerts grouped by severity and sorted by **Smart rank**.

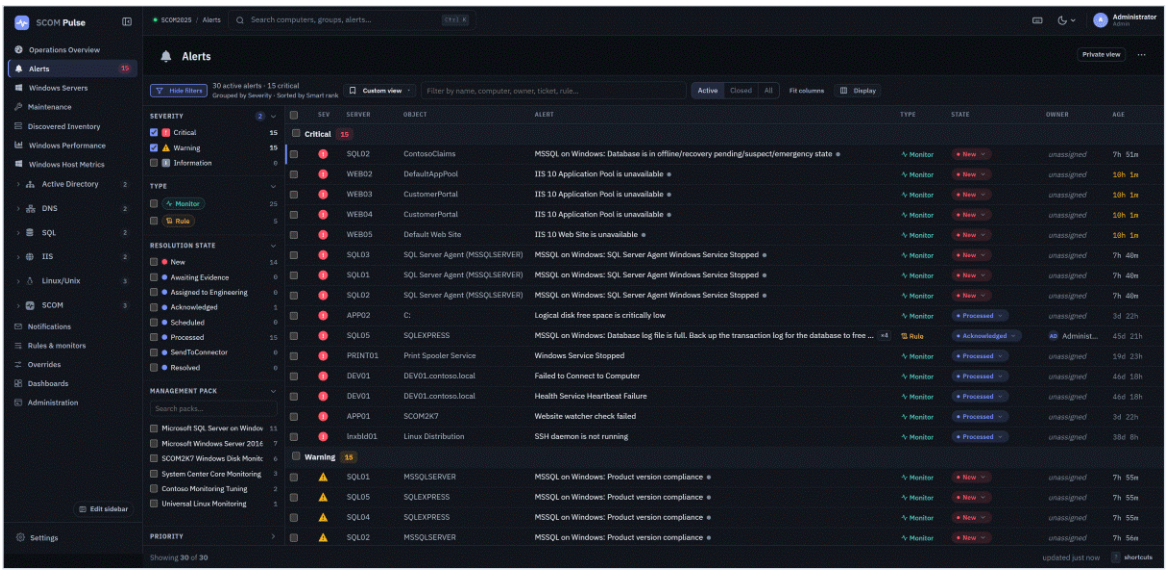


Figure 1 The Alert Center. The filter rail counts every facet as you narrow; the heading counts what matched, which is not the same as the rows on screen. **Server** is the computer the alert is on, even when SCOM names only a database or a web site.

The filter rail is the point: severity, monitor versus rule, resolution state, **management pack**, priority and age, each with a live count. Tick **Rule** and one noisy pack and you have your tuning list in about five seconds.

2 — Open one alert and see how much is in one place

Click any row.

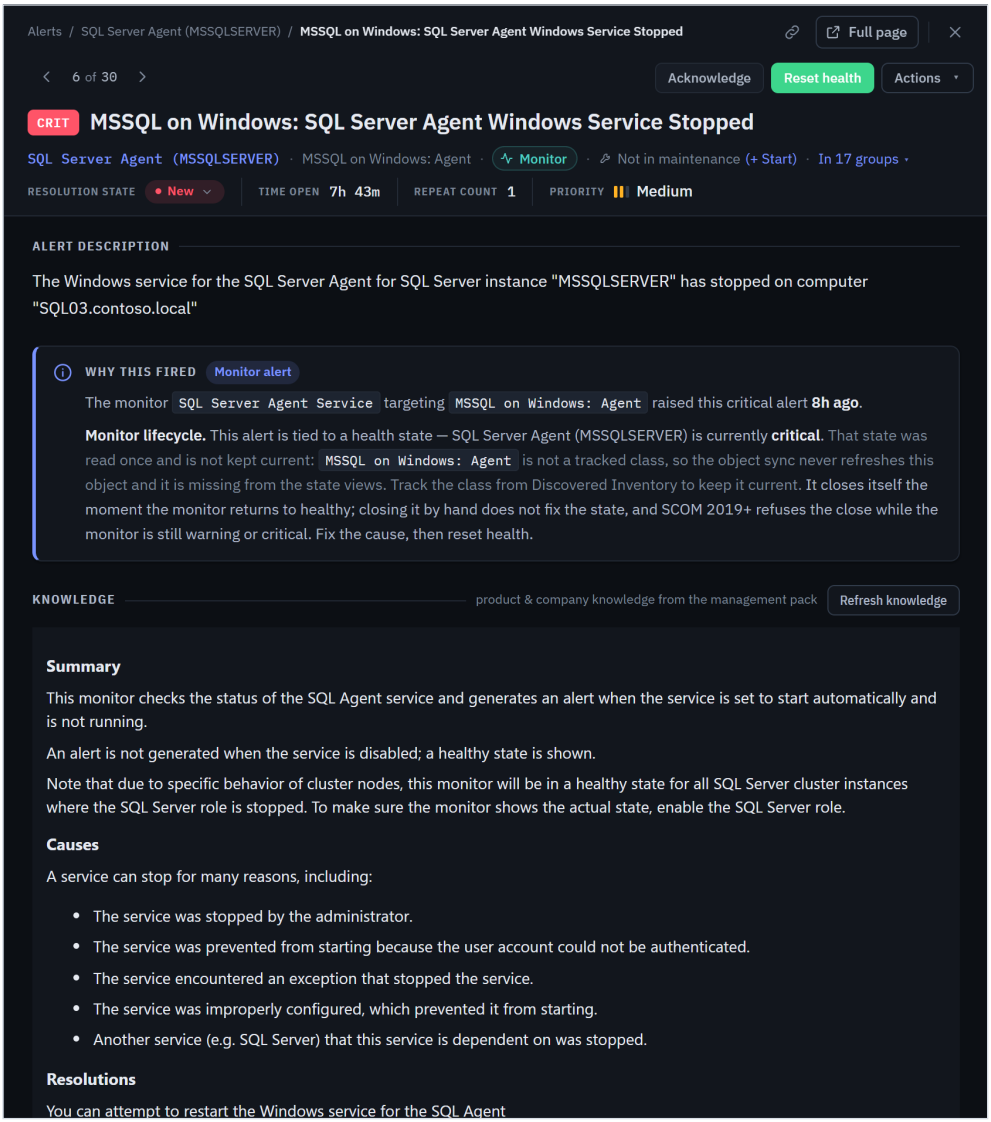


Figure 2 One alert, one panel — **WHY THIS FIRED** spells out the lifecycle consequence, and the management pack's own knowledge is right underneath it.

WHY THIS FIRED is worth dwelling on. It names the rule or monitor, and then states the consequence: a monitor alert "*closes itself the moment the monitor returns to healthy; closing it by hand does not fix the state, and SCOM 2019+ refuses the close while the monitor is still warning or critical.*"

You know that. Your level-one operators demonstrably do not, which is why they close monitor alerts all day. This puts the answer on the alert, in front of the person about to get it wrong.

Below it, without leaving the panel: the pack's **Summary / Causes / Resolutions** knowledge, current health with the four aspects, the event timeline showing who changed what and when, the other open alerts on the same host, and **NEXT STEPS** — put it in maintenance, run a task, create an override.

3 — Ask why somebody is read-only

Open **`/Pulse/Access`**. Any signed-in person can open it for themselves.

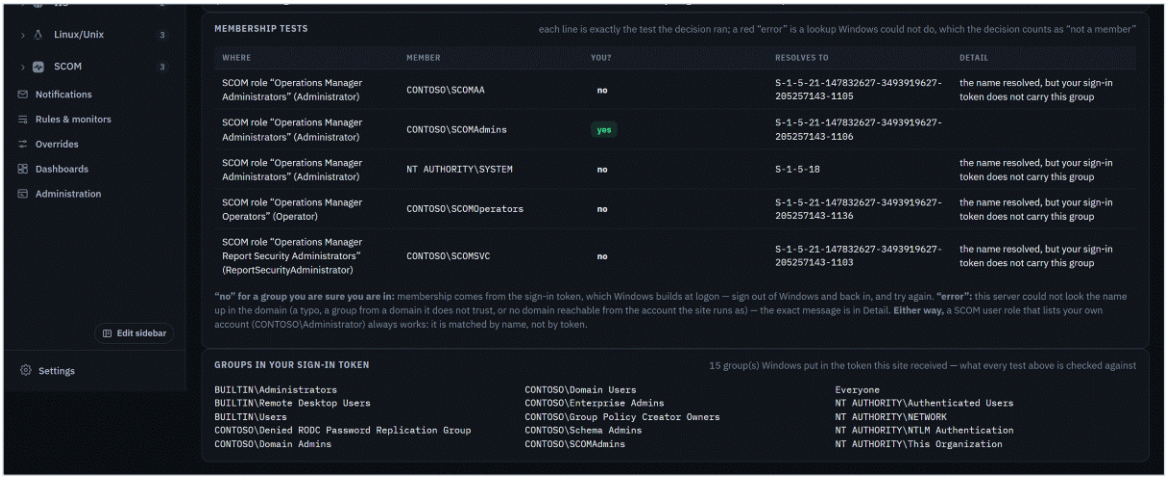


Figure 3 Every membership test behind an access decision, with the reason each one failed. SIDs are covered here.

The page names the SCOM user roles the sign-in matched, the effective profile and the scope, then tests every member of every SCOM user role against the sign-in. Each row is a test that actually ran. "*the name resolved, but your sign-in token does not carry this group*" ends the usual argument immediately — and so does the note that membership comes from the **Windows logon token**, so the person has to sign out of Windows and back in, not just restart the browser.

Send somebody this page instead of debugging their user roles for twenty minutes.

4 — Audit your maintenance windows

Open **Maintenance**. These are SCOM's own schedules, shared with the console.

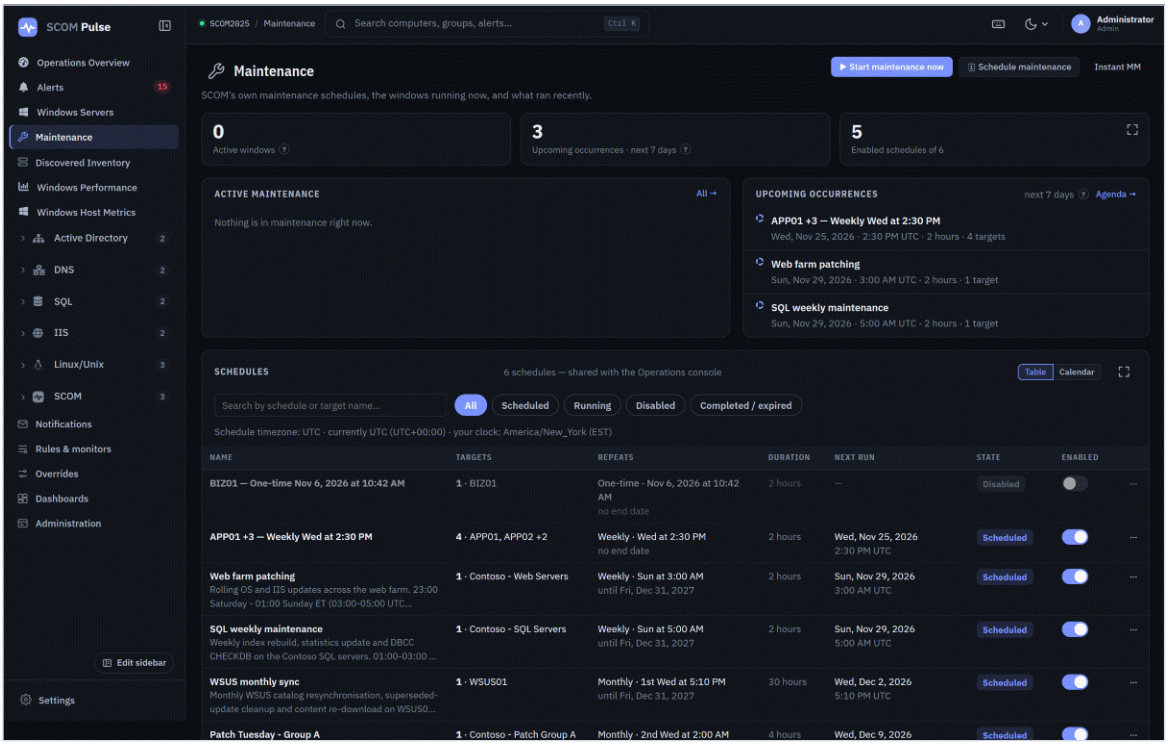


Figure 4 Active windows, upcoming occurrences, the schedule table, and a history of what actually ran.

Two things to check on your own estate right now:

- The **REPEATS** and **NEXT RUN** columns, against the schedule's name. In the management group used for this guide a schedule named **2AM Patch window** was set to **Weekly · Sun at 2:00 PM**. The name had been wrong for a long time and nothing in the console makes that obvious.
- **RECENT HISTORY** against **UPCOMING OCCURRENCES**. An upcoming occurrence is a projection from the recurrence, not proof anything ever ran.

The timezone is stated on the page, and it is the **service host's** — worth knowing before you argue about an hour.

5 — Do some administration without the console

Open **Administration**. Eleven tabs: Agents, Management packs, Run As, Pools & connectors, User roles, Groups, Watchers, Operational database, Data warehouse, Audit, Shares. Notification channels and subscribers are on the **Notifications** page, beside the subscriptions that use them; **Channels & subscribers** → in the tab strip leads there.

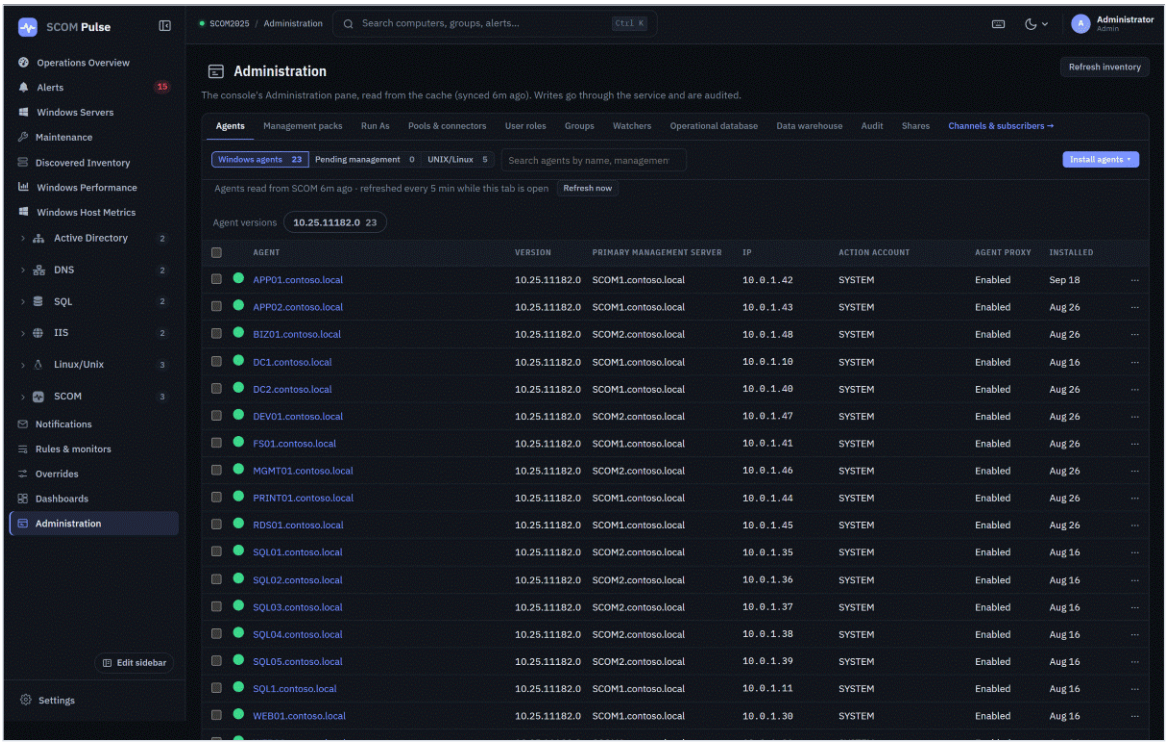


Figure 5 Agents, with health, version, primary management server, action account and proxy setting — and discovery, install, repair, reassign and uninstall behind the row menu.

The two tabs most SCOM administrators will care about first are **Operational database** and **Data warehouse** — retention, measured sizes, last-groomed times, the staging backlog, and a comparison of your warehouse retention against both the Microsoft defaults and the published community preset, with nothing written until you confirm.

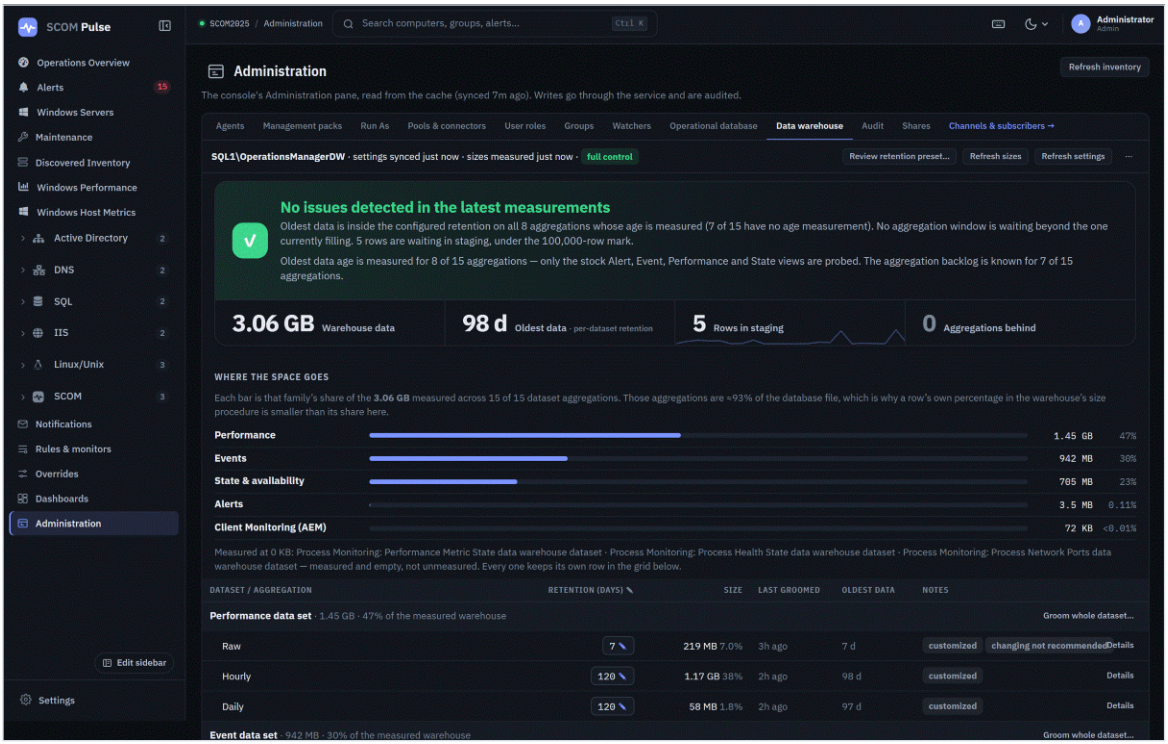


Figure 6 The warehouse: where the space actually goes, what is measured, and what is not.

> **Important — It is honest about what it does not know**
>
> The warehouse page distinguishes *measured*, *measured at zero* and *not measured*, and says how many aggregations fall into each. A number you have not measured is never shown as a healthy zero.

6 — Look at the audit trail

Administration → **Audit**. Every action queued through Pulse: who asked, what, on which target, and what the service reported back, with per-target detail and an export.

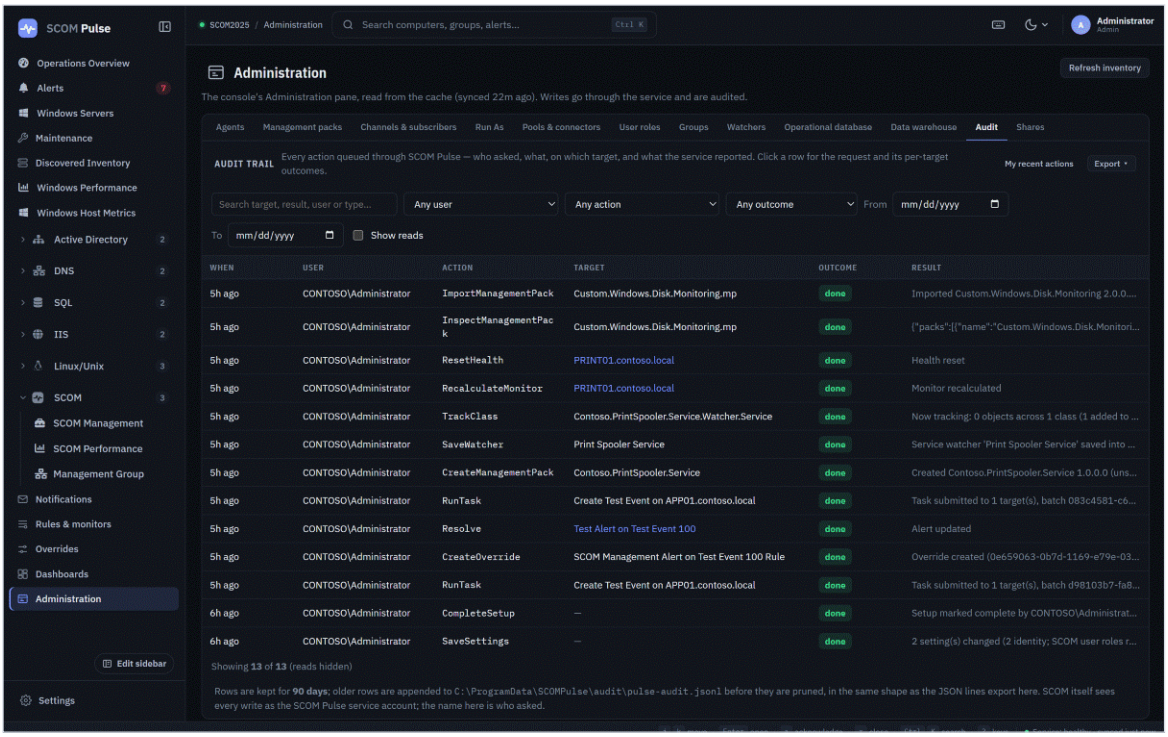


Figure 7 The audit trail, filterable by user, action, outcome and date.

> **Note — Your name, SCOM's name**
>
> Every write reaches SCOM as the Pulse **service account**, and Pulse separately records who asked. So SCOM's *Modified By* shows the service account while the audit trail and the alert timeline show the person. Expect that, and use the audit trail when somebody asks who did what.

What stays in the Operations console

Pulse does not pretend to replace it. These remain console work:

- Management pack authoring and sealing; distributed application design.
- Complex group formulas, sealed and Default-pack group edits.
- **Editing** company knowledge — Pulse displays it.
- Run As **credential** creation and password rotation.
- Network device and UNIX/Linux discovery; UNIX/Linux agent lifecycle; agent upgrade and UR patching; gateway and management-server deployment.
- Connector configuration, and SCOM/SSRS reporting.

Six things to know before you roll it out

1. **Access is SCOM's, and only SCOM's.** Your existing SCOM user roles determine access to supported SCOM operations in Pulse. There are no Pulse role lists and nothing to configure before people sign in: a person's **SCOM user roles** decide what they see and what they may do, the same answer the Operations console gives, and it works the same on SCOM 2016, 2019, 2022 and 2025. A Read-Only Operator sees the role's scope and cannot act. An Operator works alerts, maintenance, tasks in the role's task scope, diagnostics and recoveries. An Advanced Operator adds overrides on objects and groups; an Author adds class-wide overrides and group authoring; and a **SCOM Administrator** is the only kind of SCOM Pulse administrator. On SCOM 2022 and later, a Read-Only Administrator also reads the whole **Administration** page and changes nothing, and a custom role made from Delegated Administrator changes exactly what was ticked for it in the console — repairing agents, say, and nothing else. Permissions are per role and never added together: several roles add up for seeing, but a person acts only where the role that grants the action reaches — read-only over everything plus Operator over the SQL group means seeing everything and acting on SQL. And **signing in is not a grant**: a person in no SCOM user role can sign in and sees no monitoring data at all. To give someone access, add them to a SCOM user role, in the console or under **Administration → User roles**; Pulse picks the change up within about a minute, and a person newly added to an AD group must sign out of Windows and back in.
2. **Operators have their own notifications, and SCOM decides the rest.** There is no Pulse setting for it: anyone with the Operator profile or better can create subscriptions that notify **themselves**, through channels you configured, without ever seeing or editing a channel. Everyone's subscriptions,

subscribers and channels need a role that administers notifications — the SCOM Administrator profile, or a Delegated Administrator role with **Notification Management**.

3. **Three stores, three retentions.** Pulse's SQLite cache, the SCOM operational database, and the warehouse. A Pulse backup covers **only the first**. Lowering a SCOM retention deletes data at the next grooming run and raising it back recovers nothing.
4. **Back up with the command, never by copying the file** — `PulseService.exe -backup-db`. WAL sidecars and a live writer make a file copy unreliable. Keep `action.key` with the backup; it is not inside it.
5. **Check the transport.** The Settings status strip tells you plainly if the site is on plain HTTP. Windows Authentication over unencrypted HTTP is not what you want in production — rerun **Configure SCOM Pulse** and pick a certificate.
6. **Push the browser policy before you announce the address.** Edge and Chrome sign people in with Windows by themselves reliably only when a policy on the PC names the site; without it, most people opening an HTTPS address meet a grey password box on day one. **Settings → Access → Signing in without a password box** has the values for your address, ready to copy into a group policy.

Where things are

I want to…	Go to
Work the alert queue	**Alerts** — `/Pulse/Alerts`
Object state, monitor tree, active overrides	**Discovered Inventory** → object → **Health**
Chart a counter	**Discovered Inventory** → object → **Performance**
Maintenance windows and schedules	**Maintenance**
Run an agent task	Object → **Tasks** → □ **Run task…**
Search 4,400 rules and monitors	**Rules & monitors** — `/Pulse/Workflows`
Every override in the management group	**Overrides**
Agents, MPs, Run As, roles, groups, retention, audit	**Administration** — `/Pulse/Admin`
Pulse's own configuration	**Settings** — `/Pulse/Settings`
Why am I read-only	**`/Pulse/Access`**

Keyboard: `Ctrl+K` search · `j` / `k` move · `Enter` open · `a` acknowledge · `r` close · `?` every shortcut this build supports.

Read next

- **SCOM Pulse Installation Guide** — MSI, Configure field by field, unattended install, upgrade, repair, recovery.
- **SCOM Pulse User Guide** — every operator procedure in full, for the people who will live in it.
- **SCOM Pulse Administration Guide** — the access model, all five Settings tabs, SCOM administration, the two SCOM databases, sharing and audit, backup and recovery.