Configure audit delivery

- Before you begin
- Configure delivery
- Configure retention
- Audit delivery change history

Organization owners and users with a custom role that includes AI Governance audit permissions can configure where Docker writes audit events. Two delivery destinations are available and can be used independently or together:

- **Local disk**: The sandbox daemon writes audit events to the local disk on each host.
- **Docker Cloud**: Audit events are sent to Docker's cloud platform, enabling the hosted log view, CSV export, and SIEM forwarding.

Before you begin

Your organization needs:

- A Docker AI Governance plan
- An enforced organization governance policy
- Organization owner access, or a custom role with AI Governance audit permissions

Only users who have an AI Governance license and are governed by the enforced organization policy send Docker Sandboxes audit data.

Configure delivery

To configure audit delivery:

1. Sign in to Docker Home.
2. Open your organization.
3. Go to **AI Platform** > **Audit logs**.

4. Open **Audit Delivery**.
5. Choose one or both delivery modes:
   - **Local disk** writes audit records to JSON Lines files on each host.
   - **Docker Cloud** stores audit records in Docker Cloud for hosted search, CSV export, and SIEM forwarding.
6. Save your changes.

Cloud delivery is on by default when AI Governance is enabled. To keep records local to your hosts, turn off **Docker Cloud** and keep **Local disk** on.

Organizations that used local audit logging before hosted audit logs were available start with cloud delivery off until an owner opts in.

Configure retention

When **Docker Cloud** is selected, you can also configure how long cloud-stored events are retained:

Field	Description	Default
Searchable retention (days)	How long events stay searchable in the hosted audit log view.	90 days
Archive retention (days)	How long events are kept in long-term archive storage.	90 days

Archive retention must be greater than or equal to searchable retention.

Retention reductions apply going forward. They don't delete records that were already retained under a longer retention window.

Audit delivery change history

Docker keeps a record of every change made to your organization's audit delivery settings. Each entry captures the timestamp, the user who made the change, and the delivery configuration that was set. Use this history to audit configuration changes and verify when delivery modes or retention windows were modified.

Open **History** to review delivery and retention changes for your organization. History entries show who made the change, when it happened, and the before and after values.

□□□ #2
□ □□□ □□□ 2026-10-31 19:01:07 UTC
□ □□□ □□□ 2026-10-31 19:01:08 UTC