SIEM forwarding

- Supported destinations
- Before you begin
- Add a SIEM destination
- Manage destinations

{{< summary-bar feature_name="AI Governance Audit Logs" >}}

Docker can forward audit events to your security information and event management (SIEM) system, letting you centralize Docker governance data alongside other security signals. Docker verifies the endpoint is reachable with the supplied credential before saving.

Supported destinations

Destination	Description
Splunk Cloud (HEC)	Hosted Splunk using the HTTP Event Collector
Dynatrace	Dynatrace Log Management using the Log Ingest API
Datadog	Datadog Logs using the HTTP log intake API
Sumo Logic	Sumo Logic using an HTTP Source
CrowdStrike Falcon Next-Gen SIEM	Falcon Next-Gen SIEM using an HEC / HTTP Event Connector

Before you begin

SIEM forwarding requires Docker Sandboxes 0.39.0 or later. Earlier versions don't deliver audit records to a SIEM destination, even when forwarding is configured. Update Docker Sandboxes before enabling a new destination.

SIEM forwarding requires Docker Cloud delivery to be enabled for your organization. If you haven't already, enable it under **AI Platform** > **Audit logs** > **Audit delivery** before configuring a SIEM

destination. See Configure audit delivery.

Gather the endpoint URL and credential from your SIEM before configuring forwarding. Some destinations require you to create a connector or source first:

- **Splunk Cloud**: HEC ingest URL and an HEC token. Optionally, a Splunk index name. See Splunk documentation.
- **Dynatrace**: Log Ingest API URL and an API token with the `logs.ingest` scope. See Dynatrace documentation.
- **Datadog**: Logs intake URL for your Datadog site and an API key. See Datadog documentation.
- **Sumo Logic**: HTTP Source URL and an auth token from an HTTP Logs & Metrics source. See Sumo Logic documentation.
- **CrowdStrike Falcon Next-Gen SIEM**: API URL and an API key from an HEC / HTTP Event Connector. Append `/raw` to the API URL when you add the destination. See CrowdStrike documentation.

Add a SIEM destination

1. Sign in to Docker Home.
2. Open your organization.
3. Go to **AI Platform** > **Audit logs**.
4. Open **Export & Connectors**.
5. Select **Add destination**.
6. Select your destination and complete the form.
7. Select **Save**.

If verification fails, check that the URL and credential are correct and that the endpoint is accessible from the internet.

Manage destinations

From the **SIEM forwarding** list, select the menu next to a destination to edit or delete it. The edit form lets you update credentials and toggle forwarding on or off for that destination. Deleting a destination permanently removes the endpoint and its stored credential and cannot be undone.

□□□ #2
□ □□□ □□□ 2026-10-31 19:01:19 UTC
□ □□□ □□□ 2026-10-31 19:01:21 UTC