ATLORIA

Reviewing Security and Audit Controls

August 26, 2026

Opening the Security Area and Understanding What You Can Review

In Atloria, the **Security & Audit** area is available from the **Admin** workspace. Open the main signed-in area, go to **Admin**, and then select **Security & Audit**. The page opens with a clear header labeled **Security & Audit** and supporting text that describes it as the place for **security logs and audit trail management**. This tells you that the screen is meant for review and investigation rather than day-to-day content editing.

The page is presented as an administrative review screen. From the information currently shown in the interface, this area is focused on viewing security-related information rather than changing settings directly on the same page. In other words, you should expect to inspect records, logs, and activity history here, not manage project content or edit documentation. If you need broader administrative navigation, see Using the Admin Workspace.

When you open **Security & Audit**, look first at the page title and the main content panel beneath it. Atloria uses this screen to surface audit-related information for administrators. Based on the page labeling, the types of information associated with this area include:

- Audit trail records
- Security logs
- Sensitive activity history
- Administrative review information

Because this is an audit-focused screen, the most important details to look for are the people involved, the action that occurred, and when it happened. In audit views, these details are typically presented together so you can understand the sequence of events quickly.

[SCREENSHOT: Security & Audit page in the Admin workspace showing the page header and main review area]

At the moment, the visible interface emphasizes that this area is for monitoring and audit review. If you are looking for user or permission management actions, start from the other cards in **Admin**, such as **Users & Permissions**, and return to **Security & Audit** when you need to review what happened afterward.

Reviewing Audit Logs and Security Events

From the **Admin** workspace, open **Security & Audit** to review security-related activity. This page is labeled for **security logs and audit trail management**, so it is the right place to look when you need to check whether an important action took place and who performed it.

When Atloria presents an audit log or event history list, read each record as a short summary of one action. The most useful details to identify in each row are usually:

What to look for	Why it matters
Event type	Tells you what kind of action happened
User or **actor**	Shows who performed the action
Date and **time**	Helps you place the event in sequence
Affected item	Shows what project, setting, or record was involved
Status or **result**	Indicates whether the action succeeded or failed

Start by scanning the most recent entries first. If the list includes filtering controls, narrow the results to the activity you are investigating. Common review patterns include checking a specific day, focusing on one person, or isolating a type of event such as access activity or administrative changes.

If Atloria lets you open a single event, select the record to view its full details. The detail view is where you confirm exactly what changed, which item was affected, and whether the action completed successfully. This is especially helpful when a short row in the list only gives you a summary.

[SCREENSHOT: Audit log list with event rows showing action, actor, time, affected item, and result]

Use this screen as a fact-checking tool. Rather than relying on memory or chat messages, review the event list directly and compare the event time, the person involved, and the action recorded in Atloria.

Checking Sensitive Activity and Access Changes

The **Security & Audit** area is especially useful when you need to review actions that could affect access, trust, or administrative control. In Atloria, this includes activity such as permission-related changes, role updates, sign-in activity, and important configuration changes when those records are shown in the audit trail.

When you review sensitive activity, focus on three questions:

1. **Who performed the action?** Check the actor or user listed on the event.
2. **What was affected?** Look for the target user, project, setting, or other affected item.
3. **Did it succeed?** Use the status or result shown in the record.

If a record involves access changes, compare the person who made the change with the person or item that was changed. For example, one person may update another user's access, or an administrator may change a project-level setting. Reading both the actor and the affected item together helps you avoid misreading the event.

For login-related or access-related records, pay close attention to result indicators. A successful action and a denied or failed attempt can look similar at a glance unless you check the status carefully. If Atloria shows badges, labels, or result text, use those markers to separate normal activity from attempts that did not complete.

A timeline or recent activity list is also helpful when you are looking for unusual patterns. Several similar changes in a short period, repeated access attempts, or multiple permission-related updates close together may deserve a closer look.

[SCREENSHOT: Security event details highlighting actor, affected user or item, and success or failure status]

If you need to confirm whether an access-related change was expected, compare the event timing with known team activity, such as onboarding, role updates, or project administration work described in Managing User Access and Administrative Permissions.

Using Filters, Search, and Event Details to Investigate Activity

When you are investigating a specific issue in **Security & Audit**, the fastest approach is to narrow the event list before opening individual records. In Atloria, start with the search box or filter controls if they are available on the audit screen. Search for a person's name, a resource name, or a known action so you are not reviewing unrelated entries.

A good investigation usually follows this order:

1. Set the **time range** to the period when the activity likely happened.
2. Apply a **user** or **actor** filter if you know who may have performed the action.
3. Add an **event type**, **category**, or **severity** filter if the list is too broad.
4. Sort by **most recent** activity to bring the latest records to the top.
5. Open the matching event to inspect the full detail view.

Changing the time window is especially important. If you only review today's activity, you may miss the earlier event that explains the current issue. Expand the date range when needed so you can compare recent actions with earlier changes.

Once you find a likely match, open the event details. The summary row may only show the action name and time, while the detail panel can include supporting information such as the source of the action, session-related context, changed values, or other identifying details. That extra context is what helps you decide whether the activity was expected or unusual.

[SCREENSHOT: Security & Audit filters and an opened event detail panel]

If you are comparing several related events, keep the list sorted in a consistent way while you open records one by one. That makes it easier to follow the sequence of changes and spot the first event that triggered the rest.

Understanding What Security Information Is Available in the UI

In Atloria, the **Security & Audit** page is designed to show review information directly in the interface. The page title and description make clear that administrators use it for **security logs** and **audit trail management**. That means the UI is intended to help you inspect what happened, when it happened, and who was involved.

The kinds of security information administrators can review in the interface include:

- Audit events
- Security-related activity history
- Access-related records
- Permission or role-related changes when they are captured in the audit trail
- Sensitive configuration updates when those records are surfaced on the page

Across audit-style records, the most useful fields are usually the same even when the event types differ:

Common field	What it tells you
Timestamp	When the action happened
Actor	Who performed the action
Action	What happened
Target	Which user, project, or item was affected
Source	Where the action came from, when shown
Result	Whether the action succeeded, failed, or was denied

It is also important to separate **current settings** from **historical records**. A settings screen shows the current state of access or configuration. The **Security & Audit** area, by contrast, is about past activity and review history. If you want to see who changed something, use the audit view. If you want to change the current setup, move to the relevant administration screen instead.

The visible Atloria interface for this page currently presents **Security & Audit** as a review destination. If you need broader reporting or usage trends, compare it with **Analytics & Insights**, which is a separate area in **Admin** and is currently marked as coming soon. For related administrative context, see Monitoring Administrative Analytics and Activity.

Resolving Common Gaps When Reviewing Security Activity

If the **Security & Audit** area does not show what you expect, the issue is often related to scope, filters, or where the action was recorded. Start by checking the screen carefully before assuming the event is missing.

- **No events appear in the audit list**
  - Check the selected date range first.
  - Clear any active filters that may be hiding results.
  - Confirm you are in the correct administrative area and reviewing the right workspace.
  - Refresh the page and reopen **Security & Audit** if the list looks incomplete.
- **A specific user action is missing**
  - Look for a different event category if the screen separates access activity from settings changes.
  - Search by the user’s name and then search again by the affected item.

    - Expand the time range in case the action happened earlier than expected.
    - Check whether the action belongs in another administrative area, such as **Users & Permissions**, with the audit trail only showing the recorded result afterward.

- **Event details seem incomplete**
    - Open the individual event instead of relying on the summary row.
    - Review whether the list view is only showing a short description.
    - Compare multiple related events to piece together the full sequence.
- **You cannot open the Security section**
    - Confirm that your account has the administrative access needed to use **Security & Audit**.
    - If you can reach **Admin** but not this page, your permissions may be limited to other administrative sections.

[SCREENSHOT: Empty or filtered Security & Audit state with filter controls visible]

When you still cannot find the activity you need, cross-check the related administrative workflow. For example, a permission update may be easier to understand after reviewing the user management steps in Managing User Access and Administrative Permissions.

Overview

- **Security & Audit** is the Atloria admin area for reviewing security logs and audit trail information.
- You reach it from the **Admin** workspace after signing in.
- The page is presented as a review screen, with a header labeled **Security & Audit** and supporting text about **security logs and audit trail management**.
- Use this area when you need to confirm:
    - who performed an action
    - what item or setting was affected
    - when the action happened
    - whether the action succeeded or failed
- This screen is best suited for investigation and verification, not for making routine content changes.

- When available, focus on audit details such as:
  - event type
  - actor
  - timestamp
  - affected item
  - result or status
- For broader administrative navigation, use the other cards in **Admin**, including:
  - **Users & Permissions**
  - **Organizations**
  - **Documents**
  - **Projects**
  - **Analytics**
- If you need to understand the full admin navigation before reviewing audit records, read Using the Admin Workspace.
- If your goal is to inspect permission-related changes specifically, pair this screen with Managing User Access and Administrative Permissions.

Prerequisites

- You must be able to sign in to Atloria.
- Your account must have access to the **Admin** workspace.
- To open **Security & Audit**, you need the appropriate administrative permissions for audit-related review.
- Before you start, it helps to know:
  - the approximate date and time of the activity you want to review
  - the name of the person involved, if known
  - the project, setting, or item that may have been affected
- If you are investigating a permission or access issue, gather any related details from the team first so you can search the audit records more quickly.
- For sign-in help, see Signing In to Atloria and Solving Access Problems.
- If you are unsure whether you have the right level of access, review Managing Organization and Admin Settings or Managing User Access and Administrative Permissions.