



<https://verifone.cloud/docs/portal/reports/audit-log>

Updated: 04-Sep-2025

Audit Log

Overview

The Audit Log allows merchants to monitor activities undertaken by their teams to minimize the risk of fraudulent actions, money laundering actions, or actions that might cause reputational or any other damage.

For this purpose, an **Audit Log report** is introduced.

The Audit Log is a record that displays the merchant's team's actions within the Verifone Central dashboard. The Audit Log report shows the activities performed by a user that results in data change.

Audit Logs are useful whether you want to manage cases, perform user activity analysis, or conduct a specific survey.

Availability

Only users with a **Merchant Admin** role can access the **Audit Log** section in Verifone Central. Events are recorded only when the users are logged in to Verifone Central.

Benefits

The Verifone Audit Log aims to improve companies' security and risk management.

Using the Audit Log functionality, merchants will be able to:

- Access and find out the precise reasons for activities that affected specific operations or procedures
- Keep the company safe with full visibility over daily activities made by users
- Gain insight into fraudulent or unauthorized activities with the potential to damage the company's operations and/or reputation

Access Audit Log in Verifone Central

1. Log in to your [Verifone Central](#) account.
2. Navigate to *Commerce > Reporting* and then click on **Audit Log**.

Commerce

Optimize commerce operations with a comprehensive suite of payment tools, designed to streamline transactions and maximize revenue. Stay on top of financial performance with detailed reporting on sales and revenue, and never miss a payment with reliable payment deliverables.

Report

Payment

Order

3D Se

Settle

Repo

Gene

Audit

3. You have the option to search directly by entering an Item ID in the *Search by Item ID* box or you can use filters to refine recorded events (detailed in step 4).
 - Enter an item ID in the *Search by Item ID* box.
 - Search by Item ID
 - In an event, the *Item ID* serves as the identifier through which we can uniquely distinguish the event. This ID varies based on the type of event. For instance:
 - In an organization change event, the Organization ID serves as the Item ID.
 - In a payment action event, the transaction ID serves as the Item ID.
 - In a POI update event, the POI ID serves as the Item ID.
 - In an user update event, the User ID serves as the Item ID.
4. You can filter recorded events per time interval, organizations, user, and event type.

Audit Log Search and Filters

- Click on **Organizations** to filter the results according to the organization(s) you are part of, by selecting the needed organization(s) from the main dropdown menu, or by selecting one of the below three options:
 - **Name** - use the name of the desired organization or part of the name.

- **Organization ID** - use the organization ID, that can be found under *Administration > Organizations*.
 - **Business Identifier Value** - use the business identifier value, that can be found under *Administration > Organizations*.
 - Click on **User** to filter results according to the users (and their emails) on your organization(s). You can also filter to show your inactive users:
Audit Log Filter by User
 - Click on **Event type** and select a specific action, for example, *User updated*. The following types of events are displayed in the Audit Log report:
 - **Business information related events** (such as entity created, POI deleted or payment provider contract updated)
 - **User management related events** (such as new user created, existing user deleted, user is updated)
 - **User interaction events** (such as user account changes are executed, password is changed)
 - **Payment action events** (such as capture, authorization or refund) - used on eCommerce platforms
 - Click the **Apply** button. This action will filter all the user activities under the *User updated event type*.
event type filter
5. After setting the desired filters, click on a report line to see more detailed information on the logged event. Selecting a report line will make available the *Event Details* of the *Event type*.

Audit Log

Search by Item ID

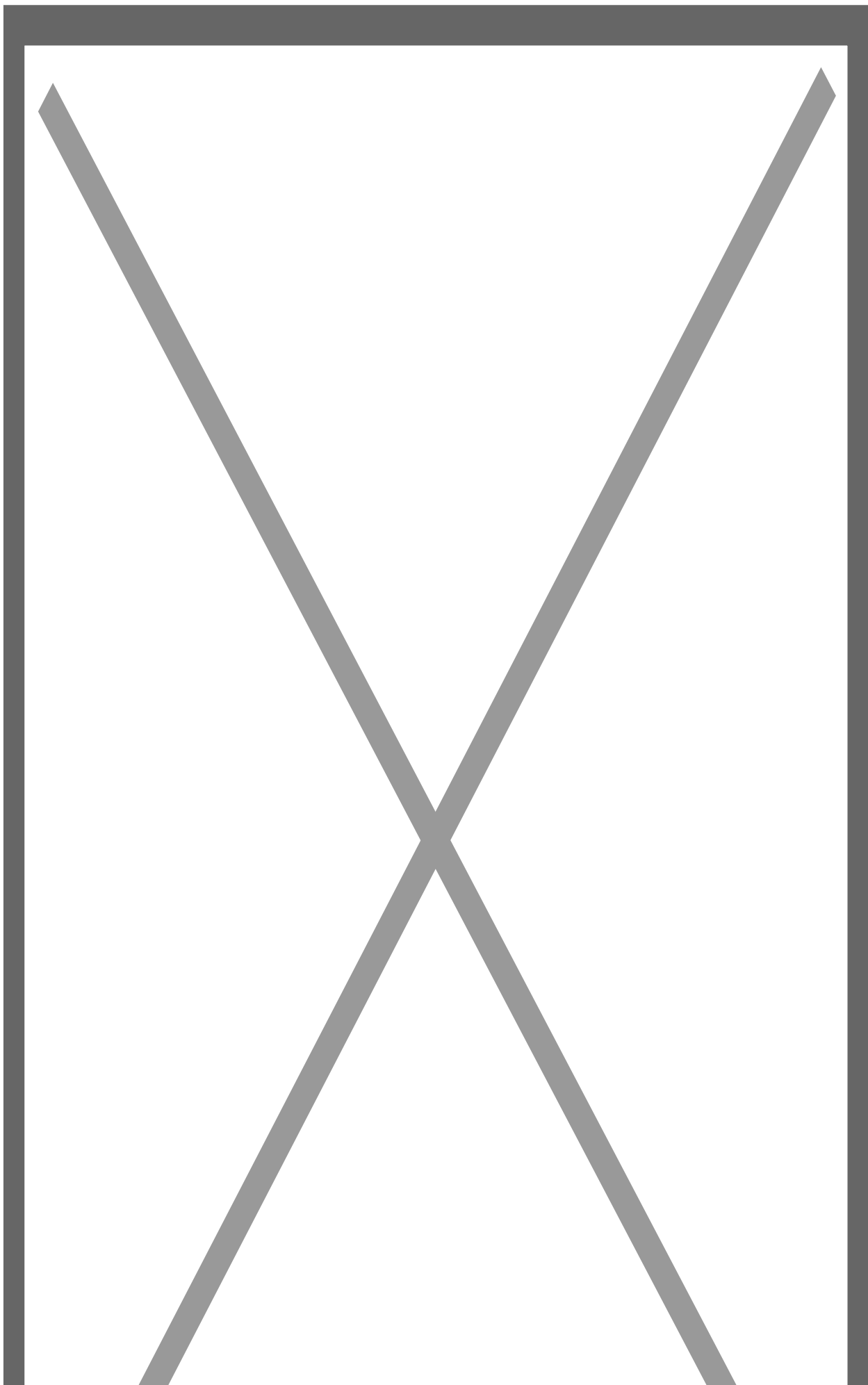
7/4/2023 — 7/11/2023 ▾ Organizations (+100) ▾ User ▾ Event type (+1) ▾ Clear

1 - 2 of 2 Audit logs

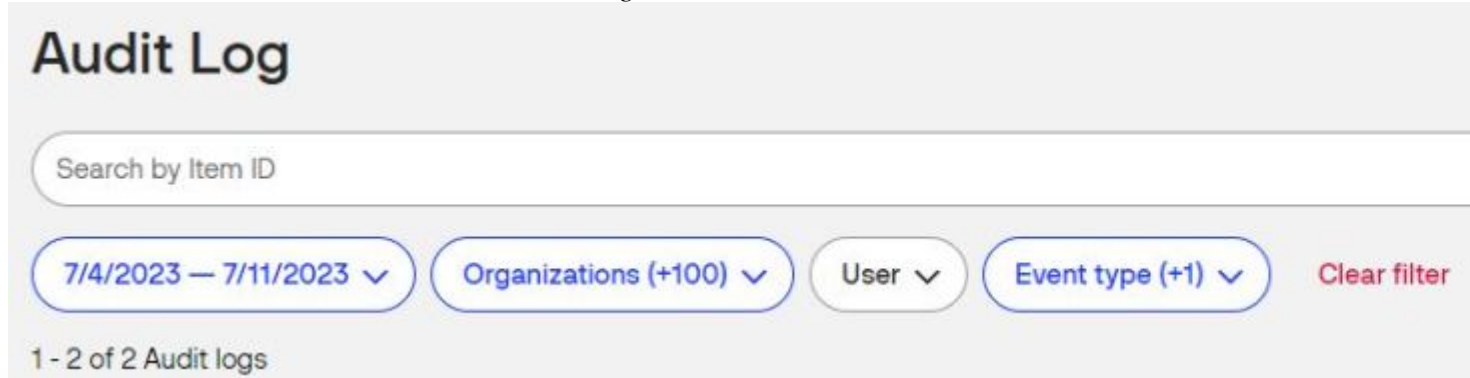
Date and Time ▴▾	Event type	User	User email address
7/5/2023, 12:23:10	User created	Test	qaams.verifone.admin@v
7/5/2023, 11:05:51	User created	—	—

Results per page 10 ^

6. The *Event Details* window shows detailed information on the logged event.



7. To reset all the filters and return to the *Audit Log* menu, click **Clear filter**.



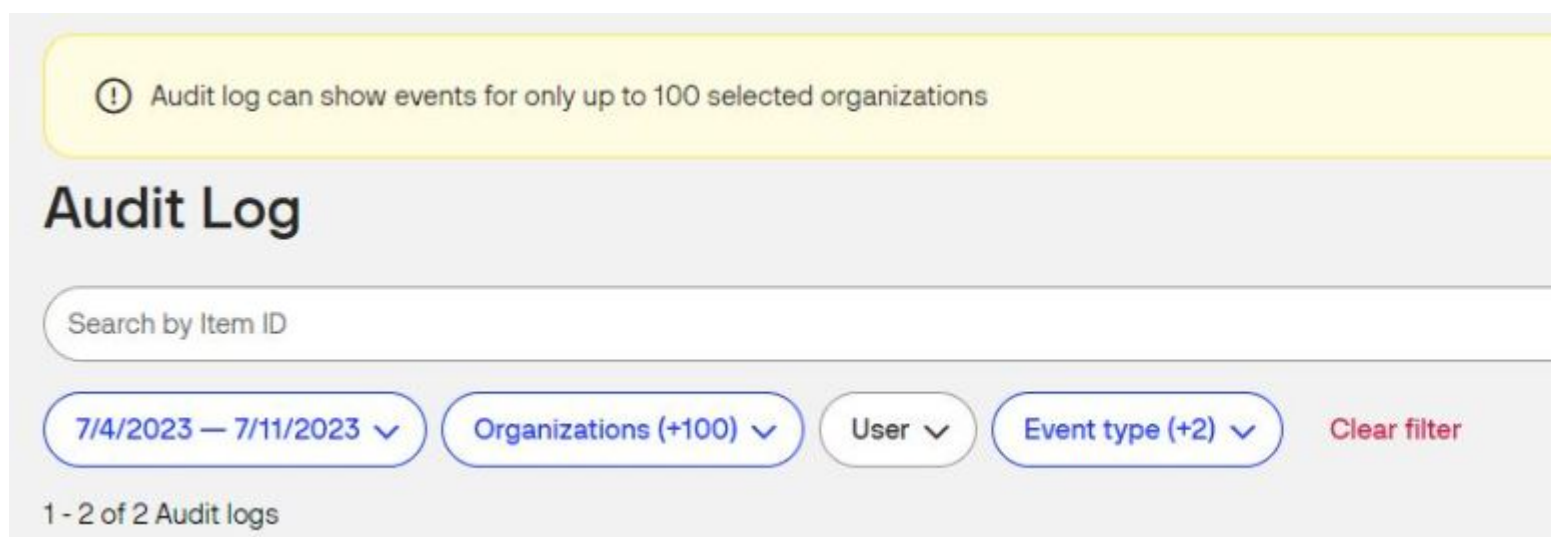
The screenshot shows the 'Audit Log' header. Below it is a search bar labeled 'Search by Item ID'. There are four filter buttons: '7/4/2023 — 7/11/2023' with a dropdown arrow, 'Organizations (+100)' with a dropdown arrow, 'User' with a dropdown arrow, and 'Event type (+1)' with a dropdown arrow. To the right of these buttons is a red 'Clear filter' button. At the bottom left, it says '1 - 2 of 2 Audit logs'.

All the rest of the desired report lines from the *Audit Log* section behave similarly.

Selecting multiple organizations

Audit log now supports multi-selection in the organization filters. When selecting an organization, automatically its children organizations are also selected recursively.

Only up to 100 organizations can be selected at the same time.



The screenshot shows the 'Audit Log' interface with a yellow warning banner at the top that says 'Audit log can show events for only up to 100 selected organizations'. Below the banner, the 'Audit Log' header is visible. The search bar is labeled 'Search by Item ID'. There are four filter buttons: '7/4/2023 — 7/11/2023' with a dropdown arrow, 'Organizations (+100)' with a dropdown arrow, 'User' with a dropdown arrow, and 'Event type (+2)' with a dropdown arrow. To the right of these buttons is a red 'Clear filter' button. At the bottom left, it says '1 - 2 of 2 Audit logs'.

Audit Log parameters

The following table describes the fields that appear in the Audit log page:

Parameter	Description
Date and time	Time stamp, when an action was undertaken
Event type	What kind of action was undertaken by the user
User	The name of the Verifone Central user, who has undertaken the action
User email address	E-mail of the user in the Verifone Central application
User status	Status of the user's account in the Verifone Central application
Organization	An organization assigned to the user to make actions with

Parameter	Description
Item ID	Identifier through which we can uniquely distinguish the event
User ID	Verifone Central identifier number assigned to the user

Event types

The following types of events are displayed in the Audit Log report:

- **Business information related events** (such as entity created, POI deleted or payment provider contract updated)
- **User management related events** (such as new user created, existing user deleted, user is updated)
- **User interaction events** (such as user account changes are executed, password is changed)
- **Payment action events** (such as capture, authorization or refund) - used on eCommerce platforms