Audit logs

Audit logs provides access to a comprehensive log of administrator activity, for audit purposes. It includes logs for changes to settings, merchants, users, and deployment information.

> **User Access**
>
> A user requires the **System admin** role to view audit logs.

Search audit logs

The most recent audit log entries are shown in the **Audit log list**, by default. The list can be filtered using the following:

- **From** - only entries on or after this date will be shown.
- **To** - only entries before or on this date will be shown.
- **User** - full or partial search on the username of the user who performed the audited entry.
- **Revision type** - type of operation performed on the database entity:
  - **Addition** - new record was added to the database entity.
  - **Modification** - existing record was modified in the database entity.
  - **Deletion** - existing record was removed from the database entity.
- **Entity name** - table in the database that the audit affected.

Select the **Search** button to display the relevant **Audit logs**. Use the ***Clear*** button to reset the search fields.

Audit log list

The **Audit log list** shows a table of **Audit logs** with the amount of log entries returned by the search criteria, along with the following log information:

- **Entity name** - table in the database that the audit affected.

- **Revision type** - type of operation performed on the database entity:
  - **Addition** - new record was added to the database entity.
  - **Modification** - existing record was modified in the database entity.
  - **Deletion** - existing record was removed from the database entity.
- **Revision date** - date and time of the audit log, in dd/mm/yyyy format.
- **User** - username of the user who performed the audited entry.
- **IP** - IP address of the user.

Selecting a log entry from the **Audit log list** will show the **Audit log details**, including the modified ***attribute*** and ***old/new*** values.