Fondation Mérieux

Lab Book

LabBook v3.6

LabBook audit log

V1

January 2026

Fondation **Mérieux**
Lutte contre les maladies infectieuses depuis 1967
www.fondation-merieux.org

Table of contents

1. Overview and benefits of the audit log

The audit log is a feature introduced in LabBook version 3.6 to enhance the traceability, security and transparency of operations carried out in the system.

It automatically records all sensitive user actions, such as :

- connections and disconnections,
- operations on users,
- operations on analysis requests
- access to resources,
- parameter or data modifications.

The audit log is an essential tool for :

- monitoring user activities ;
- analyzing incidents and unauthorized access;
- compliance with quality and regulatory requirements (ISO, internal audits, inspections);
- accountability of users according to their role.

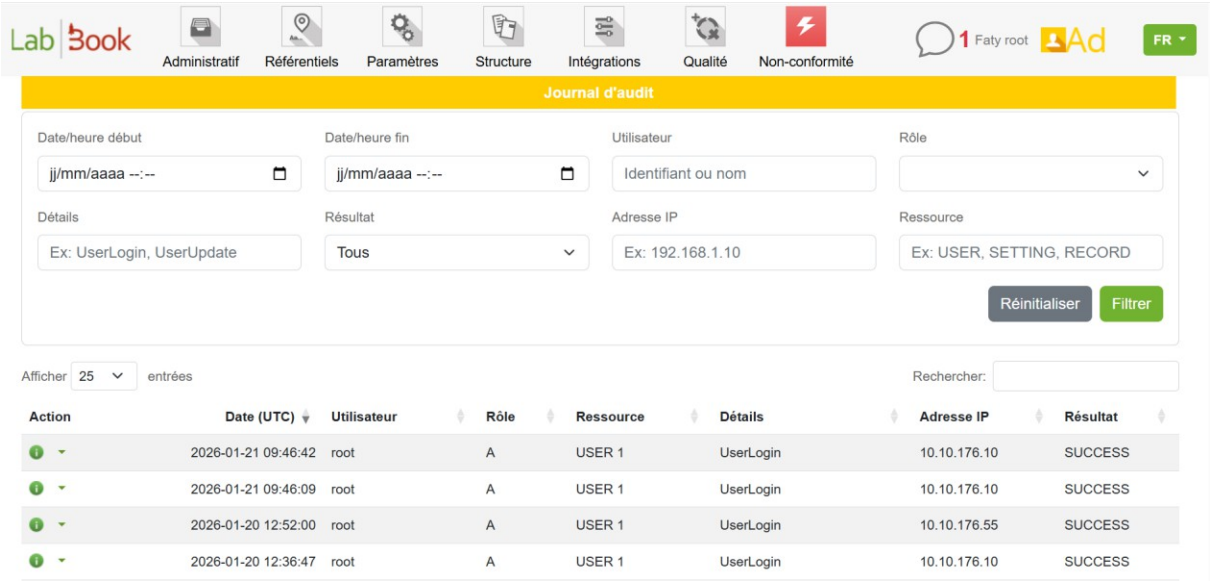
2. Audit log content

Each line of the audit log corresponds to an action performed in LabBook. The following information is displayed:

Column	Description
Date (UTC)	Exact date and time of recorded action, expressed in Universal Time (UTC).
User	Identifier of the user who performed the action (e.g. root).
Role	Role assigned to the user at the time of the action (eg. Administrator).
Resource	Type of resource concerned by the action (e.g. USER, RECORD, SETTING).
Details	Type of action performed (e.g. UserLogin).
IP address	IP address of the machine from which the action was performed.
Result	Action status (SUCCESS or FAILURE).
Action	Button for full event details. event.

3. Example of an audit log line

The Audit Trail function can be accessed from the Quality menu by users with the Administrator (root) profile. For other users, access to this function is conditional on explicit granting of the corresponding rights by the administrator. Once these rights have been granted, the functionality becomes visible and accessible in the Quality menu of their user interface.



Example:

- Date (UTC): 2026-01-21 09:46:42
- User: root
- Role: A (Administrator)
- Resource: USER 1
- Details: UserLogin
- IP address: 10.10.176.10
- Result: SUCCESS

Interpretation

This line indicates that a user with the root account and the Administrator role has successfully logged on to the LabBook system from the IP address 10.10.176.10 at the date and time indicated.

4. Meaning of UserLogin action

The LabBook audit log records different types of actions, depending on the operations performed by users on the system.

UserLogin action" example

The **UserLogin** action corresponds to a user's attempt to connect to the LabBook system. It is systematically logged, whether the connection succeeds or fails, enabling :

- track system accesses ;
- identify suspicious connections;
- analyze authentication problems.

Other types of logged actions

Depending on user rights and functionalities, the audit log may also record other actions. These include

- UserPasswordUpdate: modification of a user's password;→

UserCreate: creation o f a new user account;

- UserUpdate: modification of user information;
- SettingSendReport: send a report from system settings;→ SettingUpdate:

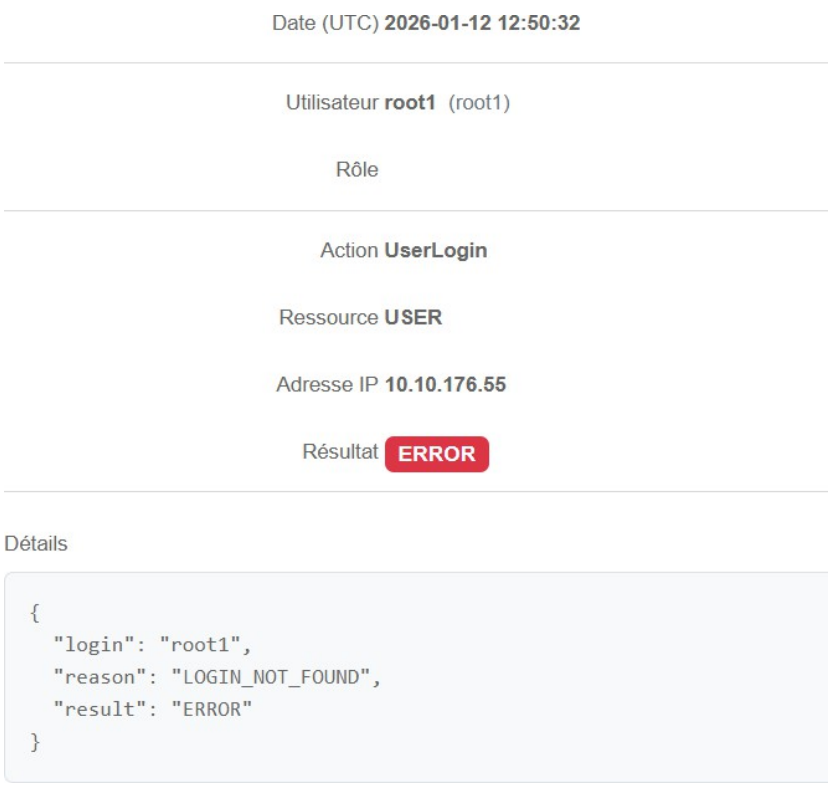
modify configuration settings;

- RecordCreate / RecordUpdate: create or update a file or record.

These actions ensure complete traceability of sensitive operations, reinforce system security and provide reliable information for audits, quality controls or incident investigations.

5. Viewing action details

In the Action column, a View button is available for each log line. Clicking on View takes the user to the Audit Log Detail screen.



This screen displays additional information, including:→ the exact date and time,
→ user and role,→ resource concerned,→ IP address,
→ the result of the action,
→ as well as technical details in structured format (JSON).

Example of details displayed:

```
{
  "login": "root",
  "result": "SUCCESS",
  "id_user": 1
}
```

6. Audit archiving and purging

Audit events are continuously recorded in the LabBook database.

Automatic processing takes place on the 1st day of each month at 02:00 UTC. If the server is unavailable, it is automatically restarted as soon as it becomes accessible again.

When the configured retention period is exceeded, audits prior to the set period are exported to the /storage/resource/audit directory, then deleted from the audit table. This mechanism is applied automatically every month.

By default, the retention period is set to 12 months. In this case, the database permanently contains only audits from the last 12 months, with older audits archived off-base to preserve system performance.

The age can be set from 1 to 60 months maximum.

The retention period can be configured via the field
The retention period can be configured via the "Audit retention age before archiving and purging (in months)" field, accessible from the Administrator interface: Settings → Preferences.

Fondation Mérieux

Fighting infectious diseases since 1967

www.fondation-merieux.org