

December 2025

Important Note

Issue in the Audit Trail of QIAcuity® Software Suite versions 3.1 and 3.2

Dear valued customer,

QIAGEN® is dedicated to meeting the needs of our customers, and we are continuously striving to provide you with products and services that enable you to archive outstanding success.

Unfortunately, despite our best efforts, a software issue was discovered that affects the tracking of the audit trail when turning the audit trail on and off in QIAcuity Software Suite versions 3.1 and 3.2.

We would like to inform you about this issue and how you can ensure that your audit trail requirements continue being met.

Description of the issue

The audit trail is a functionality in the QIAcuity Software Suite that supports users in meeting Good Manufacturing Practice (GMP)/Good Laboratory Practice (GLP) regulations and records all user interactions in the QIAcuity Digital PCR System. This functionality can only be activated and deactivated by users having the relevant permissions, such as those provided by the predefined administrator role or by any customer-defined role where the “Turn Audit Trail on and off” permission was assigned to. To meet GMP/GLP requirements, the default setting of the QIAcuity Software Suite has the audit trail tracker switched on, which is indicated in the footer of the QIAcuity Software Suite. In this mode, all activities are tracked and are shown in the audit trail event list.

The issue that has now been identified only affects the deactivation or activation of the audit trail, meaning these events are not recorded.

Despite this specific event not being tracked, all other system events are recorded in the audit trail as expected. The issue is limited solely to the deactivation or activation of the audit trail

tracker and does not affect the logging of any other activity within the QIAcuity Digital PCR System.

Recommended fix

To ensure that no user is able to make changes within the software that are not recorded in the audit trail, we recommend deactivating the predefined administrator role and assigning all users of the previous administrator role a new customer role that no longer has the “Turn Audit Trail on and off” permission. This approach will ensure the integrity of system changes and support ongoing compliance with regulatory requirements.

Step-by-step guidance

The step-by-step instructions on how to implement this workaround within your QIAcuity Software environment are listed below. Following these steps will help maintain a secure and compliant audit trail by limiting the ability to disable tracking only to authorized personnel.

1. Log in as a user with administrator privileges and go to the **Configuration** in the main toolbar.
2. Click **User Management** and check for all users with administrative permission and customized roles that have the permission “Turn Audit Trail on and off”.
3. Go to the **Roles** tab.
4. Define a new role by clicking **New Role** and provide a role name and description.

5. Select “Administrator” as template. Inactivate the “Turn Audit Trail on and off” option and leave all other configurable setting unchanged and save the new role.

System configuration [PC software] 4/5

show descriptions

Registered Instruments

Manage Archive

Manage Lab Automation

Audit Trail configuration

View Audit Trail

Turn Audit Trail on and off

6. Go to the **Users** tab and assign the newly created role to all administrator users. In case no additional administrator users are available, click **New User**.
7. Provide all required information and assign the newly created role.
8. Log out of the application and log in as the new created administrator user.
9. Go to the **User Management** and search the initial administrator user.
10. Deactivate the initial administrator user.

Configuration

Instrument name

Archive

User Management

Audit Trail

Lab Automation

Users

Roles

Users list

New User

Search for users

Search

Show: Active users (2)

Login	Name	Role	Status	Deactivate user
admin	ADMINISTRATOR	ADMINISTRATOR	Active	

In case you have several customized roles with the permission "Turn Audit Trail on and off", edit them accordingly to deactivate this functionality.

Additional information and a detailed description on how to create a new user role and assigning users to the new role can be found in the *QIAcuity User Manual* (www.qiagen.com/QIAcuity).

This recommended fix ensures that no active user is able to change the audit trail tracking configuration. When working under GMP/GLP regulations, note that QIAGEN generally recommends deactivating the predefined administrator role once at least one additional user with administrator rights has been created.

We understand the importance of accurate audit trail functionality for your compliance and operational needs, and we are actively working to resolve this issue in the upcoming software version 3.5. In addition, we confirm that all other events (logs) that happen in the system are correctly displayed within the audit trail event list.

If you have further questions, please contact your local QIAGEN representative or contact our Technical Support Center (www.qiagen.com/support/technical-support).

Best regards,

QIAGEN