User Audit Trail Events & Filters

Last Modified on 07/06/2023 2:01 pm EDT

This article provides an overview of the data captured and displayed in the User Audit Trail, along with brief descriptions of the available filters. For a list of important notes, see the User Audit Trail Overview article. For instructions on viewing or exporting the audit trail, see the View & Export the User Audit Trail article.

Columns

The User Audit Trail displays data under the following columns:

- **Time**: The date and time the event occurred, displayed in your current time zone. Note that exported User Audit Trails display the date and time in UTC.
- **Subject:** The name of the user, user group, role, or confidential login that was changed during the event.
- **Event:** The action or change that was made to the subject. See the **Events** section below for more details.
- **Performed By**: The administrator who triggered the event. If the subject is a member of multiple organizations and the events affect all those orgs (e.g., change to the username or email address), the event will be recorded for each of those orgs. If the event was triggered outside of the current org, **External Org User** be displayed in this column.

Events

The following is a summary of the events captured by the audit trail based on the subject type and action. Only header information (e.g., **Update User Group**) is displayed when multiple attributes are changed, but clicking on data from any column on the audit trail will open a palette with more details on the event.

Users

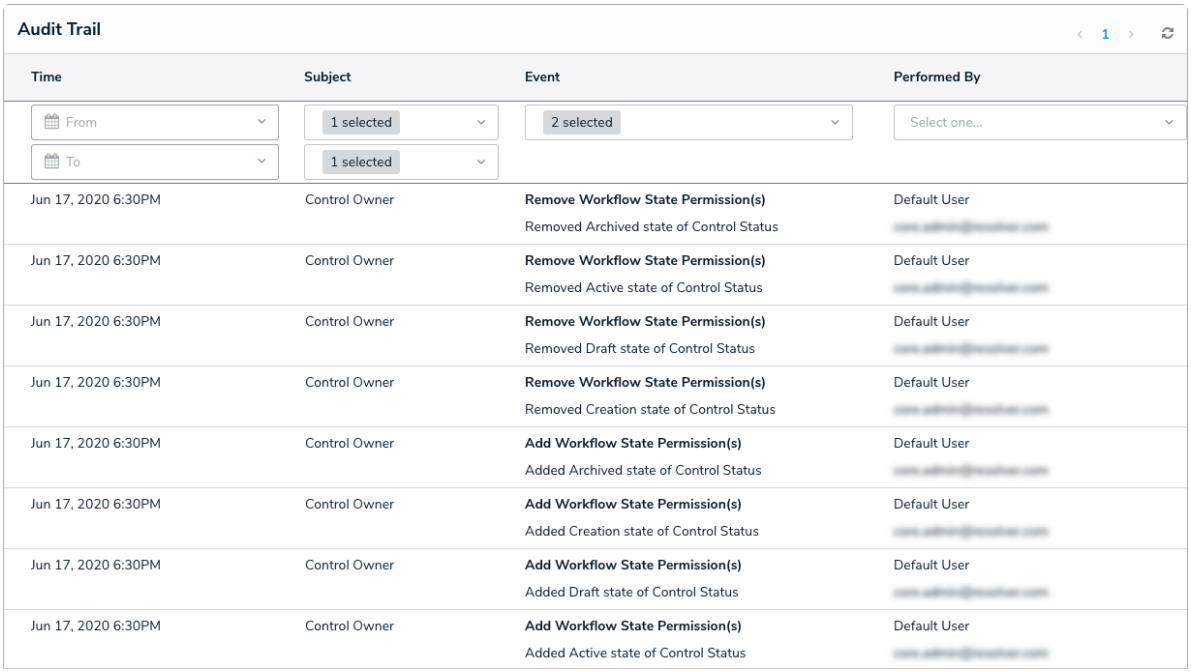
- **Add User**: A user is added to the org.
- **Update User:** One or more user attributes have been changed (e.g., **Admin** or **All Access** permissions enabled or disabled or the user is marked as inactive).
- **Impersonate User:** A user is impersonated by an administrator.
- **Unsuccessful Impersonate User:** An administrator tried to impersonate another user, but their IP address could not be validated under IP authorization control.
- **Regenerate Data Warehouse Password:** A data warehouse password is generated from the user's profile page.
- **Remove User:** A user is deleted from the org.
- **Create API Key:** An API key is created for a specific user.
- **Delete API Key:** An API key is deleted for a specific user.

User Groups

- **Add User Group:** A user group is added to the org.
- **Update User Group:** One or more user group attributes have been modified.
- **Remove User from User Group:** A user is removed from the user group.
- **Delete User Group:** A user group is deleted from the org.

Roles

- **Add Role:** A role is added to the org.
- **Update Role:** One or more role attributes are updated.
- **Add User to Role:** A user is added to a role.
- **Remove User from Role:** A user is removed from the role.
- **Add User Group to Role:** A user group is added to the role.
- **Remove User Group from Role:** A user group is removed from a role.
- **Add Workflow State Permission(s):** An object type is added to the role. This event type is logged for each state in the object type’s workflow, capturing any default form selection and permissions that were added to each state.
- **Remove Workflow State Permission(s):** An object type is removed from a role. This event type is logged for each state in the object type's workflow.
- **Update Workflow State Permission(s):** A workflow state of an object type on a role is updated. This includes any permissions or default form selections for that state that were added or removed.
- **Add Workflow State Trigger:** A trigger is enabled on a state for an object type added to a role.
- **Remove Workflow State Trigger:** A trigger is disabled on a state for an object type added to a role.
- **Delete Role:** A role is deleted from the org.



The User Audit Trail showing Workflow State Permission events.

Logins

- **Add Confidential Login:** A confidential login is added to the org.
- **Update Confidential Login:** One or more confidential login attributes are updated (e.g., hash regeneration or form changes).
- **Regenerate Confidential Login URL:** A confidential login URL is regenerated.
- **Delete Confidential Login:** A confidential login is deleted from the org.
- **Successful Login:** A user successfully logs into the org.
- **Unsuccessful Login:** A user unsuccessfully tried to log into the org. This includes login attempts by users whose IP addresses could not be validated under IP authorization control.
- **Confidential Login:** A login to the org occurred using an confidential login URL.
- **Unsuccessful Confidential Login:** A user tried to access a confidential login URL, but their IP address could not be validated under IP authorization control.
- **Logout:** A user logged out of the org.
- **User Locked Out:** A user is locked out of the environment after too many incorrect password attempts.
- **Change Password:** A user changes their password or sets a new password after activating their account.

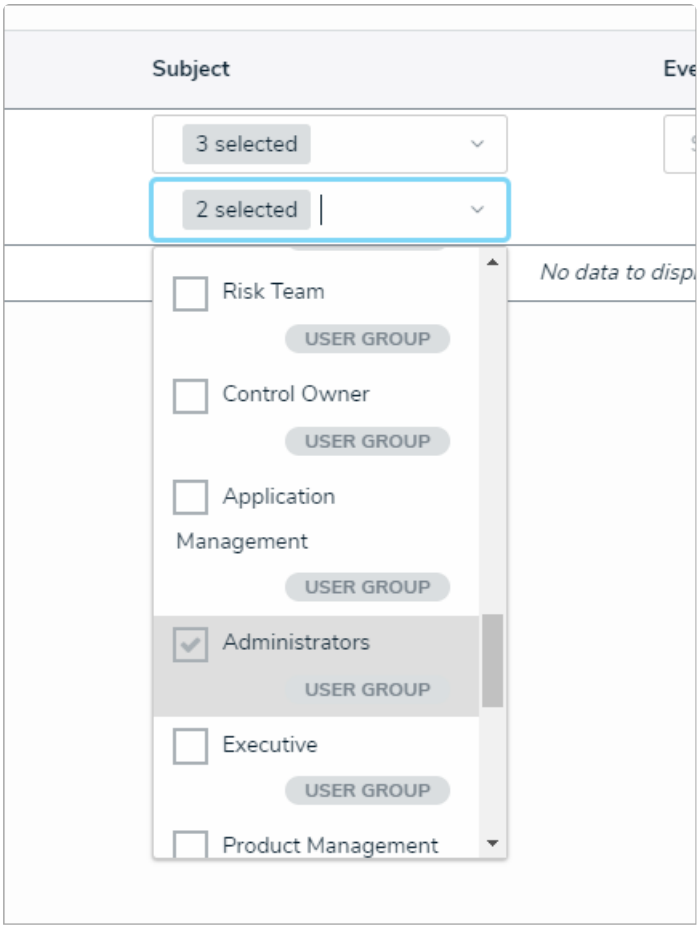
IP Authorization

- **Add to IP Allow List:** An entry is added to the org's IP Allow List.
- **Update IP Allow List Entry:** An entry is updated in the org's IP Allow List.
- **Remove from IP Allow List:** An entry is deleted from the org's IP Allow List.

Filters

The data displayed in the audit trail can be narrowed down by applying one or more of the following filters:

- **Time:** Filters the data based on a **To** and/or **From** date range.
- **Subject:** Filters data based on the subject type, including **User**, **User Group**, **Role**, **Confidential Login**, and **IP Authorization**. Selecting one of these types will then allow you to select additional filters from a secondary dropdown menu. This filter includes active, disabled, and deleted subjects.



The Subject filter.

- **Event:** Filters data based on the event.
- **Performed By:** Filters data based on the administrator who triggered the event. Only active admin users added to the current org appear in this filter.