User Audit Trail Events & Filters

Last Modified on 11/05/2025 11:48 am EST

Overview

This article provides an overview of the data captured and displayed in the **User Audit Trail**, along with brief descriptions of the available filters.

> ***Note:***
> *The **User Audit Trail** supports a data retention period, allowing organizations to define how long User Audit Trail data should be kept to ensure compliance with data privacy and retention policies. Please contact Resolver Support if you are interested in enabling this on your Org.*

User Account Requirements

The user must have Administrator permissions in order to access the ***Admin Overview*** screen.

Related Information/Setup

For a list of important notes regarding the **User Audit Trail**, please refer to the User Audit Trail Overview article.

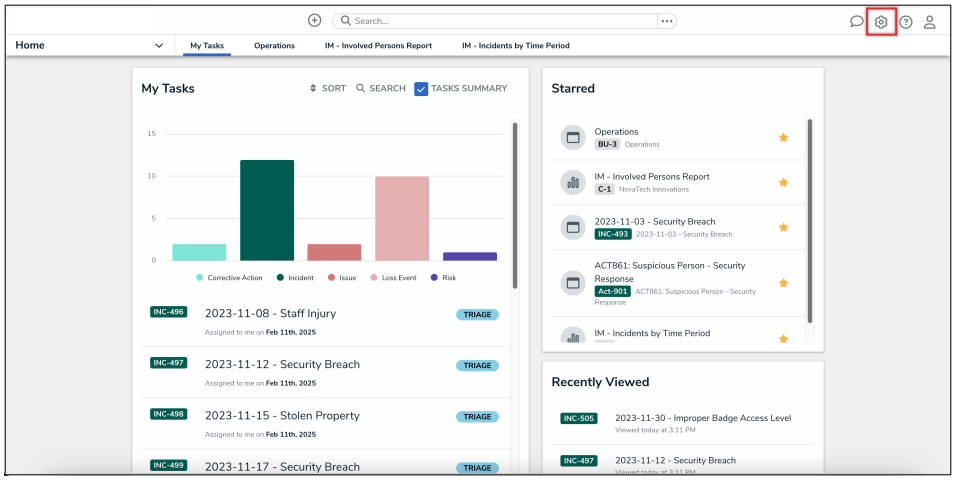
Please refer to the View the User Export Trail article for information on viewing the **User Audit Trail**.

Please refer to the Export the User Audit Trail article for information on exporting the **User Audit Trail**.

For further information on enabling a data retention period for the **User Audit Trail**, please refer to the Enabling the User Audit Trail Data Retention Period article.

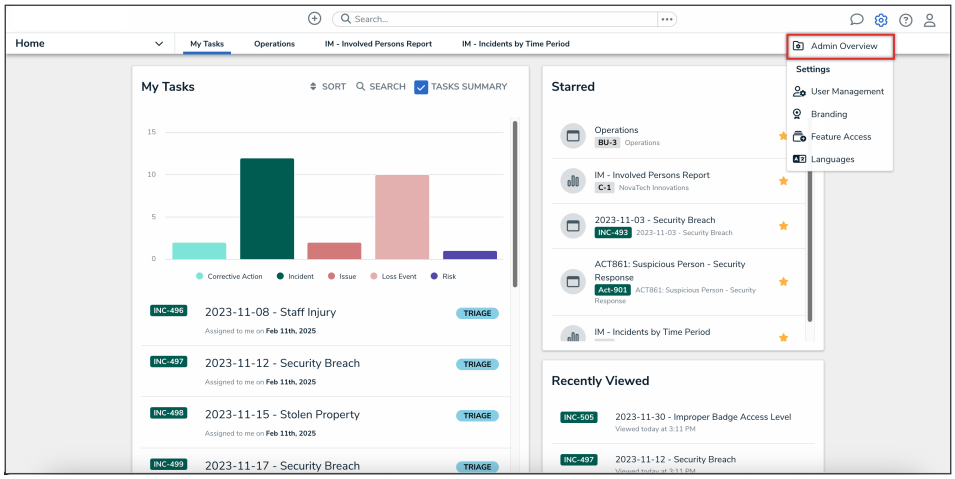
Navigation

1. From the ***Home*** screen, click the **Administration** icon.



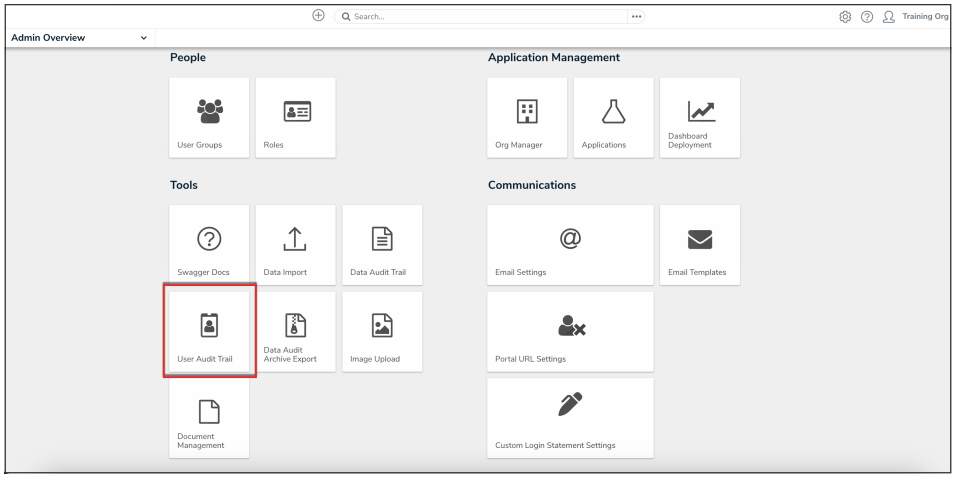
Administration Icon

2. From the Administrator settings menu, click the **Admin Overview** link.



Administrator Settings Menu

3. From the ***Admin Overview*** screen, click the **User Audit Trail** tile under the **Tools** section.



User Audit Trail Tile

Columns in the User Audit Trail

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:***
  > 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 in the User Audit Trail

The following is a summary of the events captured by the User 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. If you enabled the **Portal URL Access** toggle switch when you created the user, the User Audit Trail will list the user type as **Portal URL Access**. If an advanced permissions user is added, it will specify which type of advanced permission.
- **Update User:** One or more user attributes have been changed (e.g., **Admin, Portal URL Access,** or **All Data 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.

- **Add User to Advanced Permission:** An advanced permission is added to a user.
- **Remove User from Advanced Permission:** An advanced permission is removed from a user.
- **Reset User MFA:** An Administrator resets MFA for a user.
- **Multi-factor Authentication Setup Complete:** A user sets up MFA on their account.
- **Add User Email Change Request:** A request is sent to change the email address for a user.
- **Cancel User Email Change Request:** A request that was sent to change the email address for a user is cancelled.
- **Add Admin to Org:** A Resolver user is added to the Org to assist with a Support request, with approval. Please see the Account Access article for further information.
- **Expire Admin from Org:** A Resolver user's access expires and removed from the Org. Please see the Account Access article for further information.

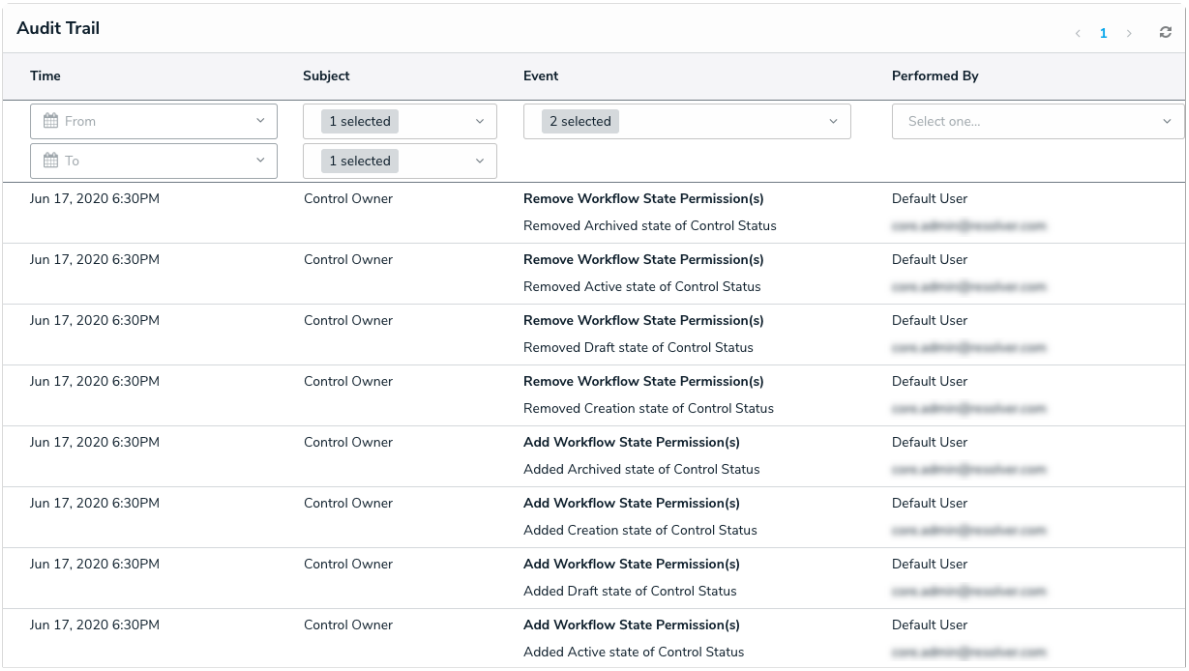
User Groups

- **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 Portal URL:** A Portal URL is added to the Org.
- **Update Portal URL:** One or more Portal URLs attributes are updated (e.g., regeneration, form changes, or Secure Access Portal landing page).
- **Regenerate Portal URL:** A Portal URL is regenerated.
- **Delete Portal URL:** A Portal URL 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.
- **Portal URL Login:** A login to the Org occurred using a Portal URL.
- **Secure Access Portal Login**: A login to the Org occurred using a Secure Access Portal URL.
- **Unsuccessful Secure Access Portal Login:** A user tried to access a Secure Access Portal, but their IP address could not be validated under IP authorization control.
- **Unsuccessful Portal URL Login:** A user tried to access a Portal 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.

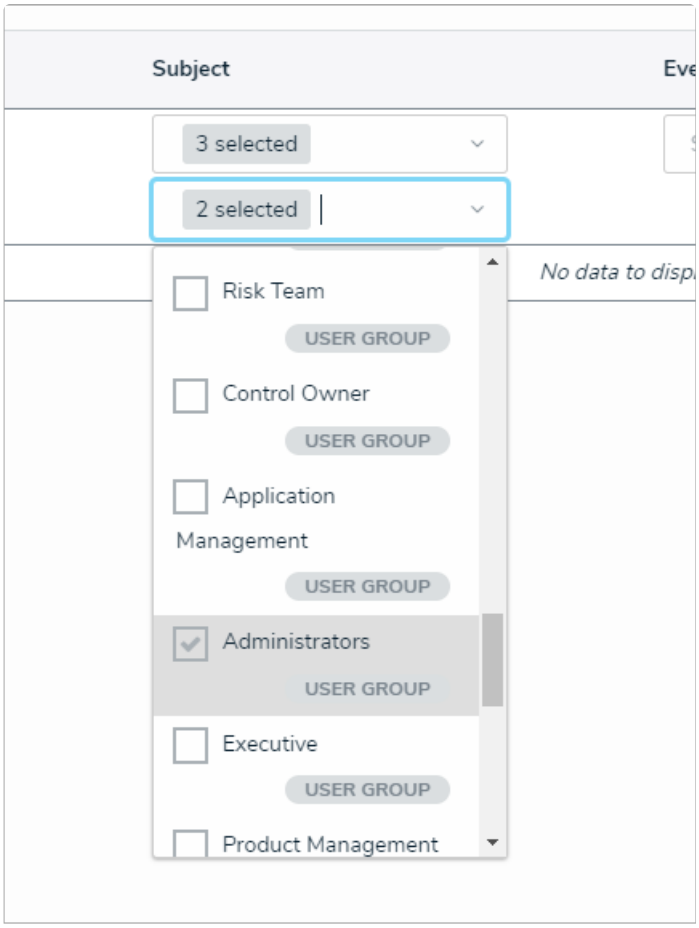
Feature Flags

- **Update Feature Flag:** One of the following features is self-enabled on an Org:
    - Enable Document Management (*fileAttachment_v2*)
    - Allow Editing Online via Microsoft Office (*officeOnlineIntegration*)
    - Enable AI-Generated Regulatory Summarization (*reqSummarization*)
    - Enable AI-Recommended Controls (*controlSuggestions*)
    - Enable Requirement Similarity (*similarity*)
    - Enable Portal Agent (*universalAutomatedIngestion_v2*)

Filters in the User Audit Trail

The data displayed in the User 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.