![tracelink NETWORK FOR GREATER GOOD]

TRACELINK UNIVERSITY

Home
Resources
TraceLink University

Monitor audit trail data

System Administrators and Application Administrators must assign users the **Member - Standard Audit Trail Access** role to access the Audit Trail Events menu item to export audit trail data which provides visibility into the exact date and time that a particular user made a change, the data that was updated, and where the change occurred (e.g. which application, whether the user touched the UI).

Export audit trail data

Export audit trail data

System Administrators and Application Administrators can export audit trail data to investigate specific events.

1. Select Administration in the main menu.
2. Select Audit Trail.
3. Select the Export ⬇ icon to generate and export an audit trail file.
4. Fill in the following fields in the Export Audit Trail section:
   a. Audit Start Date field – drop-down – Select a specific start date range from the calendar to view specific audit trail date or type the date.
   b. Audit End Date field – drop-down – Select a specific end date range from the calendar to view specific audit trail date or type the date.
5. Select Export.

A notification displays when the file is ready, and the file downloads automatically.

Tips

- Select View Audit Trail to Filter and download audit trail reports on a separate screen.

Filter audit trail reports

Filter and download audit trail reports

1. Select Administration in the main menu.
2. Select Audit Trail.
3. Select View Audit Trail.

4. Fill in a date range to filter the audit trails results.

5. Select Apply.

   The results display in the table.

   ### See the information that displays in the table
   - Date Generated – The date that a user generated the audit trail export.
   - Start Date – The audit trail export includes data starting from this date.
   - End Date – The audit trail export includes data until this date.
   - File Name – The file name of the audit trail exported file.

6. Select the Download ⊕ icon in the appropriate row to download the document.

   ### See the columns that display in the Audit Trail CSV file
   - **eventDate** – The date and time the event occurred in GMT.
   - **performedBy** – The email address of the integration user, integration principal, or company user performing the action. The integration user or integration principal allows a company to assign roles and configure an

app without assigning a specific user to apply the changes. The integration user or integration principal does not exist in the TraceLink SSO, and this user cannot log into the UI.

- **performedByCompany** – The company of the user performing the action or an identifier of the Company for events initiated via API or B2B exchanges using an integration user or integration principal.
- **supportAccessAccount** – The email address of the TraceLink Support Representative performing an action on behalf of the performedBy user.
- **functionalArea** – The app that the event occurred within.
- **businessObjectType** – The part of the app that the event occurred within.
- **businessObject** – The specific object within the businessObjectType that the user updated (e.g. if a user is a businessObjectType, then the user's email is the businessObjectjsmith@company.com, Location 2350014).
- **action** – The action the user performed (e.g. Create, Modify, Delete).
- **modifiedData** – The data field that the user updated, which includes one of the following explanations:
  - Identifies the field name, the old value, and the new value in the following format: [FieldName]: [oldValue or --], [newValue or --]
  - Text that describes the change (e.g. Login, Logout, Password Changed, Invitation Sent)
  - For B2B message exchange, the file name provided.
- **reasonforChange** – The reason for an update if the app requires a reason for change for that update. For example, if a user adds or removes administrator access.

Tips

- See specific help centers for each app for more information about the events that are included for that app.

Related Content

Add B2B connections

Application Administrators can create and update Opus B2B connections using AS2, SFTP, and SMTP protocols.
View More

View B2B messages

Application Administrators and members with standard access can filter and view the B2B messages for AS2 , SFTP and SMTP connection types.
View More

Configure TraceLink for Multienterprise Information Network Tower

Unlike other Opus apps, Multienterprise Information Network Tower must be configured on Track & Trace Services because Multienterprise Information Network Tower supports asynchronous messages, which are not yet available on the Opus Platform.
View More