Search an Audit Log Online

To search an audit log, complete the following steps:

To search an audit log, complete the following steps:

- 1. From the **Administration** tab, select **Audit**. The *Search Audit Logs* page appears.
- 2. Enter your search criteria.

Under Search Criteria, optional

- Select a Module type
- Enter a User
- Select an OTC Endpoint
- Enter the From and To date and time ranges, required
- Select a **Keyword**, required
- Select a Category Name, required
- Enter the Terminal ID
- Enter the Batch ID
- Select an Event Type
- Select an Operation Mode



Application Tips

- Module drop-down options vary by user role. Module options include Administration, Check Capture, Check Processing, Card Processing, and Deposit Processing.
- The **From** and **To Created On Date** must be entered in **MM/DD/YYYY** format and cannot exceed 30 days.
- The Keyword and Category Name drop-down options vary by user role.
 Operation Mode options include All, Online, or Offline.



Event Types are categories of events that are recorded by the audit log.

Table 1. Event Types

Event Type	Description
All	Includes all event types in the audit log
Error	Error entries are created when the system is unable to complete an action.
Informational	Information entries are general records of the activity that has happened while using OTCnet.
Warning	Warning entries are created to inform the user when events of note have taken place. This includes cancelling an action, deleting information from the system and inactive users.

3. Select **Search**. The *Search Results* table appears as shown in Figure 1.

Figure 1. Audit Log Output

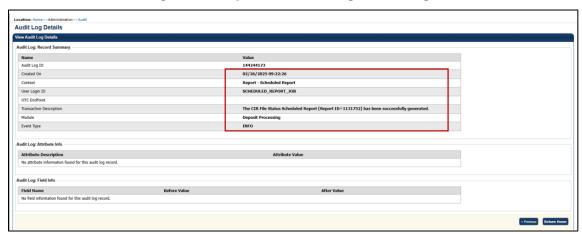




Application Tips

- Run a search (select a module type, FROM and TO dates, and a keyword).
 - The search results include all activities in the system that you have access to view.
 - Run additional searches, the Search Results table repopulates with the results of the new search.
- Select **Download** to download the search results.
- Select Print Audit Log Records to print a formatted audit log record.
- If the audit log records contain Personally Identifiable Information (PII) the data is masked.
- An entry in the audit log will appear each time a user submits a request to generate
 a CIR file status report asynchronously, when the scheduled report is successfully
 generated, and when the user successfully downloads the generated report.
- 4. Select the **Audit Log ID** hyperlink to view additional details for an individual audit log entry. The *View Audit Log Details* page appears as shown in Figure 2.

Figure 2: Sample View Audit Log Details Page





Additional Buttons

- Select **Previous** to return to the previous page.
- Select **Return Home** to the OTCnet Home Page.