Application Audit Web User Guide

Table of Contents

Welcome to Application Audit

The purpose of Application Audit is to record application activity for auditing purposes.

With Application Audit, you can create search requests from which reports are created using data on the mainframe. Users and help desk personnel can access the reports and information they need from the mainframe in a format that they are more familiar with.

From the Application Audit home page, choose one of the following:

- Click 

(Record) to create a recording request.
- Click 

(Recordings) to manage recording requests.

Related Topics

Log on to Application Audit

Record

Recordings

Log on to Application Audit

To use Application Audit, establish a host connection. Host Connection Logon allows you to establish or change host connections within Application Audit to one of those connections defined in CES.

The Host Connection Logon fields include:

- **Host connections** – Select a host connection from the drop down menu. The connections listed include those which were created in CES.
- **Authentication** – Select an authentication method from the drop down. Possible values include:
  - **User/ID Password** – Always valid. With this selected, both the User name and Password fields are *enabled*. In User name, enter the name of the user. In Password, enter the password of the user.
  - **Passticket** – Present only when CES is installed on USS. With this selected, only the User name is *enabled*.
- **User name** – Enter the user name.
- **Password** – Enter the password for the user name.

Related Topics

Welcome to Application Audit

Record

Recordings

Record

Application Audits Record page allows you to create a recording request.

To create a record request

Record Request

1. In the **Name** field, enter a name for your recording. This will be appended onto the Base Dataset Name field when the dataset is saved to the mainframe.

2. In the **Description** field, enter a description for your recording.

Target tab

1. Click the **Target** tab.

2. Under **Network Traffic**, you can select the type of traffic to target:

   - 3270
   - TCP
   - MQ

3. Under **Activity**, if you've chosen to target 3270 traffic in your recording, you can further filter the activity being recorded by clicking **Add**. From the **Activity Filter** dialog box, select an Application, User ID, and Terminal. Click **OK**.

Datasets tab

1. Click the **Datasets** tab.

2. Under **Name** (Base Dataset Name), enter a name for the dataset. Recording data is stored in archive datasets. Your user ID will need authority to create datasets under this High Level Qualifier (HLQ). The recordings Name will be appended to the base dataset name. A sequence number is appended to the base dataset name when each archive segment is created. Each new dataset will be automatically incremented by one uniquely identifying the segment.

   Example
   For example, you could enter the following as your recording name.

   Name: USER

   Base Dataset Name: HLQ.AUDIT

   Once submitted, the first dataset below will be created, with the following being created as they are necessary

   HLQ.AUDIT.USER.#0000001

   HLQ.AUDIT.USER.#0000002

   HLQ.AUDIT.USER.#0000003

3. Under **Daily Switch Schedule**, you can choose to establish a daily switch schedule. To do so, set the switch to **On** and establish a start time, end time, and switch interval. You can further choose

to apply the schedule to weekdays only by setting that switch as well. When the switch interval is turned off, dataset switching will be performed when the dataset reaches its capacity. A switch can also be performed manually at any time.

4. Under **Recording Dataset Conflicts**, determine which action you would like to perform if the dataset exists. You can choose to cancel the recording or delete the dataset.

5. Under **Archive Size**, choose a size for the base dataset of either Small, Medium, Large, or Custom. With Custom, you may choose size by Type, Primary, and Secondary quantities.

SIEM tab

1. Click the **SIEM** tab.
2. Under the **SIEM** tab, you can choose to push data to SIEM when the recording data is archived. You can also choose to send an email notification if the push fails.

Related Topics

Welcome to Application Audit

Log on to Application Audit

Recordings

Recordings

The **Recordings** tab allows you to view two types of recording requests:

- **Active** - Displays a list of currently active recordings, active sessions for a recording, and archived activity that has been sent to SIEM for each recording.
- **Inactive** - Displays a list of inactive recordings and archived activity that has been sent to SIEM for each recording.

View recording requests

- To view active recordings, click the **Active** tab.
- To view inactive recordings, click the **Inactive** tab.

Toolbar functions

Depending on the recording request tab, the toolbar allows you to perform the following functions:


Clicking **Refresh** allows the screen content to refresh.


Clicking **Switch** allows the data captured to be set and ready to be sent to SIEM.


Clicking **Stop** stops the record function.


Clicking **Open** begins a new record.


Clicking **Duplicate** duplicates the input from a previous record request.


Clicking **Filter** allows for filtering within the tables by entering text. Multiple text items may be used when separated by a space.

Table Columns

The tables include the following column headings, depending on the table being viewed.

Recordings

- **Name** - Identifies the name of the recording.
- **Description** - Identifies the description of the recording.
- **Type** - Identifies the recording by type—either 3270, TCP/IP, or MQ.

- **Sessions** - Identifies the number of sessions in the recording.
- **Start Time** - Identifies the start time for the item listed.
- **Duration** - Identifies the duration for each item in a given list.
- **Base Dataset** - Identifies the base datasets used to archive recordings.
- **Last Segment Time** - Identifies the time for the last segment.

Active Sessions

3270

- **User ID** - Identifies the user IDs for active sessions within a recording.
- **Terminal** - Identifies the terminals for active sessions within a recording.
- **Application** - Identifies the applications for active sessions within a recording.
- **Start Time** - Identifies the start time for the item listed.
- **Transaction** - Identifies the number of transactions contained in an active session within a recording.
- **Lost** - Identifies the number of transactions that were not recorded.

MQ

- **Queue Manager** - Identifies the queue manager captured.
- **Queue Object** - Identifies the queue object name.
- **Start time** - Identifies the start time for the item listed.
- **Last Update Time** - Identifies the time for the active session.
- **Bytes** - Identifies the size of the data in the active session.

TCP

- **Server Address** - Identifies the TCP/IP server address of the capture.
- **Server Port** - Identifies the server port of the active session.
- **Client Address** - Identifies the client address for the active session.
- **Client Port** - Identifies the client port for the active session.
- **Start time** - Identifies the start time for the active session.
- **Last Update Time** - Identifies the last update time for the active session.
- **Bytes** - Identifies the size of the data captures in the active session.

Archived Activity

- **Start Time** - Identifies the start time for the item listed.
- **End Time** - Identifies the end time for the item listed.
- **Duration** - Identifies the duration for each item in a given list.

- **SIEM Status** - Identifies whether or not the SIEM transfer failed, succeeded, or is unknown for the archived activity.

Related Topics

Welcome to Application Audit

Log on to Application Audit

Record