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 

(Archive Management) to manage archive requests and create a recording request.
- Click 

(Search Management) to manage and view search rules and results.

Related Topics

Log on to Application Audit

Archive Management

Search Management

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

Archive Management

Search Management

Archive Management

Archive Management allows you to manage archive requests and create recording requests.

You can 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. From here, you can also create an archive request.
- **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 **Filter** allows for filtering within the tables by entering text. Multiple text items may be used when separated by a space.

 Clicking **Menu** allows for selecting a menu of Functions.

 Clicking **Clear** clears all fields on the page when creating a search rule.

Table columns

The following tables include the column headings:

Active Archives

- **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

VTAM 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.

To create an archive request

1. Click ☰ and select *Create Archive* from the menu list. The Create Archive Request page appears.
2. In the **Name** field, enter a name for your archive request. This will be appended onto the Base Dataset Name field when the dataset is saved to the mainframe.
3. 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 a filter type, and then 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 **Archive 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 customize both the Initial dataset size, as well as the Increment dataset size.

SIEM tab

1. Click the **SIEM** tab.
2. Under the **SIEM** tab, you can choose to push data to SIEM when an archive dataset switch occurs. You can also choose to send an email notification if the push to SIEM fails.

Archive Actions

Only those action items that are valid for the selected archive are displayed and enabled.

Active

- Clicking **Switch** allows the data captured to be set and ready to be sent to SIEM.
- Clicking **Stop** stops the record function.
- Clicking **Open** allows the viewing of the archive definition.
- Clicking **Duplicate** clones the definition as a template for defining a new one.
- Clicking **Schedule Switch** allows the times that a switch will occur to be modified, regardless of how full the file segment is.
- Clicking **Show Queued Searches** displays the **Queued Searches** defined for that archive.

Inactive

- Clicking **Delete** deletes the reference to the selected archive.
- Clicking **Open** allows the viewing of the archive definition.
- Clicking **Duplicate** clones the definition as a template for defining a new one.
- Clicking **Restart** restarts an inactive archive.
- Clicking **Show Queued Searches** displays the **Queued Searches** defined for that archive.

Related Topics

Welcome to Application Audit

Log on to Application Audit

Search Management

Search Management

The Search Management page allows you to create, modify, save, and access search rules, as well as submit search requests. You can specify complex search conditions for locating VTAM 3270 sessions based on the content of output window data within the selected archive. You can make this search request private (for yourself only), or, with the proper authorization, you can make a public search request that any authorized user can use.

To create a search rule

1. From the rules tab of the Search Management page, click **Add**. The Search Rule page appears.
2. Type a name for your search rule in the **Name** text box. Names must follow valid ISPF naming conventions. The name can be alphanumeric, up to eight characters in length, and must start with a letter.
3. Choose to make the search request either Private or Public by clicking the **Public** button. Private search requests can be viewed by the originator only. Public search requests can be viewed by all authorized users.

    Only users with Global Recording Administrator authority on the mainframe are authorized to create global search requests. If you do not have Global Recording Administrator authority, this field does not appear on your window.

4. The information on which you can search is located in an archive that has previously been created. Select an archive from the Archive list.
5. Select a **Search scope**: Inputs, Outputs, or Both.
   - **Inputs** displays user-entered input keystrokes.
   - **Outputs** displays hits on target text on output screens (transmitted from the application to a user's terminal).
   - **Both** displays both inputs and outputs.
6. Specify a date and time range on which to search by completing the **Start date**, **Start time**, **End date**, and **End time**. This limits the archive search to a specific time period rather than the entire archive repository set. Be sure the toggle switch is in the **On** position in order to enable this field.
7. Specify filters by User ID, Application ID, or Terminal ID. This limits the archive search to specific IDs.
8. Specify search criteria by typing the information that you want to search for in the **Search String** text box and click **Save**. The search string will now appear in the search table.

   You can create more advanced search strings by clicking the **Advanced** button. The search strings are executed in the order they appear in the list. The combined search strings create a search rule.
   - Select an **Operator** from the list. The list contains standard relational operators.
   - If you add more than one search string, select **AND** or **OR** from the list by clicking .
   - The right and left parentheses ( ) can be used to build conditional searches.
   - **Row** specifies to search only this row. Zero (0) is the valid wildcard character.
   - **Column** specifies to search only this column through the number of columns specified in Length. Zero (0) is the valid wildcard character.
   - **Length** is the length of the search string padded with blanks. Zero (0) is the valid wildcard character.
9. **Submit**, **Save**, or **Queue** your new search rule:
   - Click **Submit** to save your search rule, start your search immediately and create your report. A message will appear giving a date and time when the report was submitted. When execution is complete, the report will appear in the tree view. You may need to

click the refresh button in the tree view to refresh the Reports list with your report when it has finished executing.

- Click **Queue** to save your search rule and queue your report for later submission.
- Click **Save** to save your search rule for future use. It will be saved with the name you entered in the **Request Name** field. After it is saved, it will appear in the tree view with either a local rule icon or a global rule icon depending on the choice you made when you created the rule.
- Click  (**Clear**) to clear all fields and start over without saving the search rule.

Related Topics

Welcome to Application Audit

Log on to Application Audit

Archive Management