



# *Security Log's Training Guide*

*Broadsword Program Office  
Air Force Research Laboratory / IFED  
315-330-4429*

ISSO



Services



- Audit Logs

- Create Audit Report based on:
  - User Name
  - Event Type
  - Date Range
- Archive Audit Logs
- Remove Archived Logs

- Archived Logs

- Query Archived Logs based on:
  - User Name
  - Event Type
  - Date Range

ISSO

• Audit Logs

The purpose of this screen is to allow the ISSO to view, archive, or remove audit information from the Broadsword Sybase Data Base based on user(s), date/time and audit event.

The Audit Log Maintenance screen contains a table of parameters. The first four parameters are used to query for the audit information, the last parameter is used when archiving the audit information.

The screenshot shows the 'Audit Log Maintenance' interface. At the top is a purple header with 'Audit Logs' in yellow. Below it is a black bar with 'Audit Log Maintenance' in white and a 'Help' button on the right. The main area contains a form with the following fields:

- User :** A text input field.
- Start Date :** A text input field with a date/time mask 'YYYYMMDDhhmmss' and the value '19990505182022'.
- End Date :** A text input field with a date/time mask 'YYYYMMDDhhmmss' and the value '19990505182022'.
- Event :** A dropdown menu.
- Archive File Name :** A text input field.

At the bottom of the form are four buttons: 'Audit Report', 'Archive Records', 'Remove Records', and 'Reset'.

Callouts provide the following explanations:

- User :** The user account being queried for audit information.
- Start Date :** The start date/time of the audit information being queried.
- End Date :** The end date/time of the audit information being queried.
- Event :** The audit event being queried.
- Archive File Name :** Name of file to contain audit records being archived. (The directory path is not included in the filename.)
- Audit Report :** Request an audit report for viewing based on the query parameters selected in the parameter table.
- Archive Records :** Archive the records returned from the query based on the parameters selected in the parameter table.
- Remove Records :** Remove the records from the Broadsword Sybase Data Base that are returned from the query based on the parameters selected in the parameter table.
- Reset :** Returns the selections to their previously applied values and automatically applies these changes.

## ISSO

### Audit Logs

#### Example:

The ISSO for our local system wants to get a report on user 'test05'; in particular he wants a record of every log-in attempt by this user. The information filled in on the right specify the correct query. All the ISSO needs to do is click the Audit Report button.

The Audit Log Maintenance screen contains a table of parameters. The first four parameters are used to query for the audit information, the last parameter is used when archiving the audit information.

The user account being queried for audit information.

The end date/time of the audit information being queried.

Name of file to contain audit records being archived. (The directory path is not included in the filename.)

Request an audit report for viewing based on the query parameters selected in the parameter table.

Archive the records returned from the query based on the parameters selected in the parameter table.

Remove the records from the Broadsword Sybase Data Base that are returned from the query based on the parameters selected in the parameter table.

Returns the selections to their previously applied values and automatically applies these changes.

The screenshot shows the 'Audit Log Maintenance' interface. At the top is a purple header with 'Audit Logs' in yellow. Below it is a black bar with 'Audit Log Maintenance' in white and a 'Help' button on the right. The main area contains a form with the following fields:

- User :** A text input field containing 'test05'.
- Start Date :** A date/time input field with a format mask 'YYYYMMDDhhmmss' and the value '19990505182022'.
- End Date :** A date/time input field with a format mask 'YYYYMMDDhhmmss' and the value '19990505182022'.
- Event :** A dropdown menu showing 'User Logged In'.
- Archive File Name :** An empty text input field.

At the bottom of the form are four buttons: 'Audit Report', 'Archive Records', 'Remove Records', and 'Reset'.

## ISSO

### Audit Logs

.....

This is a listing of all the audit events that the ISSO can select for the audit report. The default is All Events.

The screenshot shows the Broadsword web application interface. On the left is a navigation sidebar with the following menu items:

- Searching
  - Search Tools
  - Shopping Cart
  - Order Status
  - Saved Queries
  - Deferred Reservations
- Cataloging
  - Manually
  - With NITF Headers
  - With IPL Data
  - With Templates
  - Catalog Status
- Administration
  - System Status
  - User Maintenance
  - System Statistics
  - System Configuration
- ISSO
  - Audit Logs
  - Archived Logs

The main content area is titled "Audit Logs" and includes "Audit Log Maintenance" and "Help" buttons. It features a search form with a date range selector (YYYYMMDDhhmmss) and a dropdown menu currently set to "All Events". Below the search form are buttons for "Archive Records", "Remove Records", and "Reset".

ISSO

Audit Logs

This screen is the result of clicking on the Audit Report button from the previous page. By clicking on the “View Audit Report” link, the user can view the audit report generated by the criteria specified.

Example: This screen means that the previous request for all log-in information on user test05 up to May 5, 1999 has been processed, and that a report has been generated. To view the report, all the ISSO has to do is click on the “View Audit Report” hyperlink.

**Audit Log Maintenance** Help

User : test05

Start Date : YYYYMMDDhhmmss  
19990505000000

End Date : YYYYMMDDhhmmss  
19990505235959

Event : User Logged In

Archive File Name :

[View Audit Report](#)

Audit Report    Archive Records    Remove Records    Reset

Link to audit report generated using the current search criteria.

ISSO

• Audit Logs

.....

This is a sample audit report generated by the "Audit Log Maintenance" page.

Example:

This is the log generated by the previous request. The header contains all of the log criteria, and the rest contains log entries.

This is the report header. It contains all of the audit log criteria specified in the previous screen.

**Audit Report**

**User: test05 Starting at : 19990505000000 and Ending at : 19990505235959 For Event: LOGIN**

---

<b>Login:</b> test05 <b>IP:</b> 123.456.789	<b>Orig. Login:</b> test05 <b>Gtkpr:</b>	<b>Session Key:</b> 10205
LOGIN @ 19990505185343 : Successful Login from sun Gatekeeper		
<b>Login:</b> test05 <b>IP:</b> 123.456.789	<b>Orig. Login:</b> test05 <b>Gtkpr:</b>	<b>Session Key:</b> 10652
LOGIN @ 19990505194650 : Successful Login from sun Gatekeeper		

This is a sample log entry. Each entry contains the username, IP Address, Gatekeeper, and Session Key, as well as all of the events that were audited.

ISSO

• Audit Logs

.....

This screen is a result of clicking the “Archive Records” button on the “Audit Log Maintenance” page.

Example: Now, let us suppose that the ISSO wants to archive the report that he just generated. By clicking on the “Archive Records” button, the ISSO can archive the report in a file called audit050599.

The screenshot displays the 'Audit Logs' maintenance interface. At the top, there is a purple header with the text 'Audit Logs'. Below this is a black bar with 'Audit Log Maintenance' and a 'Help' button. The main area contains a form with the following fields: 'User' (test05), 'Start Date' (YYYYMMDDhhmmss, 19990505182022), 'End Date' (YYYYMMDDhhmmss, 19990505182022), 'Event' (User Logged In), and 'Archive File Name' (audit050599). Below the form, a message states 'Archived record(s) successfully.'. At the bottom, there are four buttons: 'Audit Report', 'Archive Records', 'Remove Records', and 'Reset'. A diagonal line is drawn over the 'Archive Records' button.

This is the confirmation message from a request to archive a record.

## ISSO

### Audit Logs

Example:

Let's say that the ISSO now wants to remove the audit050599 record. After entering the filename and clicking the "Remove Records" button, this confirmation screen appears. Clicking on the "Remove Records" button again will confirm the removal.

This is the warning displayed when a remove record request is made.

### Audit Logs

#### Audit Log Maintenance Help

User :	test05
Start Date :	YYYYMMDDhhmmss 19990505182022
End Date :	YYYYMMDDhhmmss 19990505182022
Event :	User Logged In
Archive File Name :	audit050599

**WARNING: Verify Record Deletion by Clicking Remove Records Again. These Records will be PERMANENTLY Removed from the System.**

Audit Report    Archive Records    Remove Records    Reset

ISSO

• Audit Logs

Example:

After clicking on the “Remove Records” button, the ISSO receives confirmation that the file audit050599 has been removed.

This page confirms the removal of an archive.

The screenshot displays the 'Audit Log Maintenance' interface. At the top, there is a purple header with 'Audit Logs' in yellow. Below this is a black bar with 'Audit Log Maintenance' in white and a 'Help' button on the right. The main area contains a form with the following fields: 'User' (test05), 'Start Date' (YYYYMMDDhhmmss, 19990505182022), 'End Date' (YYYYMMDDhhmmss, 19990505182022), 'Event' (User Logged In), and 'Archive File Name' (audit050599). Below the form, a message states 'Removed record(s) successfully.' At the bottom, there are four buttons: 'Audit Report', 'Archive Records', 'Remove Records', and 'Reset'. A black arrow points from the 'Remove Records' button to the confirmation message.

This is the confirmation message from a request to remove a record.

## ISSO

- Audit Logs
- Archived Logs

.....

This page displays a listing of all the archived files that the user can select and view.

**Archived Logs**

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input type="checkbox"/>	security_test	19990505113638
<input type="checkbox"/>	diane	19990505175035
<input type="checkbox"/>	audit050599	19990505182550

**Audit Archive Queries** Help

<b>User :</b>	<input style="width: 80%;" type="text"/>
<b>Start Date :</b>	<small>YYYYMMDDhhmmss</small> <input style="width: 80%;" type="text" value="19990505185445"/>
<b>End Date :</b>	<small>YYYYMMDDhhmmss</small> <input style="width: 80%;" type="text" value="19990505185445"/>
<b>Event :</b>	<input style="width: 80%;" type="text"/>

## ISSO

- Audit Logs
- Archived Logs

Example #1:

ISSO selected the archived file audit050599 to query and view *all events* for the user *test05*.

### Archived Logs

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input type="checkbox"/>	security_test	19990505113638
<input type="checkbox"/>	diane	19990505175035
<input checked="" type="checkbox"/>	audit050599	19990505182550

### Audit Archive Queries

User :

Start Date : YYYYMMDDhhmmss

End Date : YYYYMMDDhhmmss

Event :

## ISSO

- Audit Logs
- Archived Logs

Example #2:

ISSO selected the archived file *security\_test* to query and view *user login information* for *all users*.

Note: When the user field is left blank the default is *all users*.

### Archived Logs

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input checked="" type="checkbox"/>	security_test	19990505113638
<input type="checkbox"/>	diane	19990505175035
<input type="checkbox"/>	audit050599	19990505182550

### Audit Archive Queries

User :

Start Date : YYYYMMDDhhmmss

End Date : YYYYMMDDhhmmss

Event :