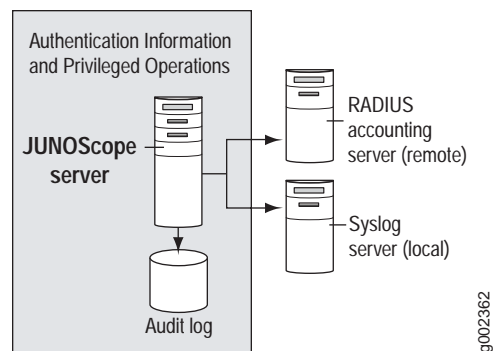


Chapter 22

Monitoring the Audit Log

This chapter describes how to monitor authentication activity and privileged operation events in the audit log. JUNOScope auditable events are stored in the JUNOScope database and are subsequently sent to the system log server and an optional RADIUS accounting server if one is configured (see Figure 6).

Figure 6: JUNOScope Security-Enhanced Sensitive Data Logging



Authentication activity events include the following:

- User logs in
- Login attempt failures because of an invalid username and/or password
- User logs out
- User session times out

Privileged operation events are user actions that change information in the JUNOScope system or in the network. Privileged events include the following:

- Configuration is committed on a device from the Configuration Editor
- Configuration is archived from a device
- Configuration is restored to a device
- User account is created
- User account is deleted

- User password is changed
- Device is added
- Device is deleted
- Label association is changed
- Access method is changed
- Authentication information is changed

Each audit record includes the date and time, event category, event type, username, and client IP address.

In addition to the internal audit log, audit events are also forwarded to the local syslog server and the configured RADIUS server (if any) as RADIUS accounting messages.

You must have superuser permission to view the audit log.

This chapter includes the following topic:

- [Displaying the Audit Log on page 223](#)

Displaying the Audit Log

The audit log displays JUNOScope authentication and privileged operation events by date and time, event category, event type, username, and client IP address. You can select filters to specify which records you want to see.

To display the Audit Log, follow these steps:

1. From the JUNOScope main window, click Monitor > Audit Log. The Audit Log Filters dialog box appears.

The screenshot shows the JUNOScope interface with the 'Audit Log' filter dialog box open. The dialog has a sidebar on the left with 'Operations', 'Status', and 'Audit Log' (selected). The main area has 'Monitor' and 'Audit Log' tabs. Below the tabs is the text 'Select Event Category, Type or User name' and 'Filters to apply to query:'. The filter rules are as follows:

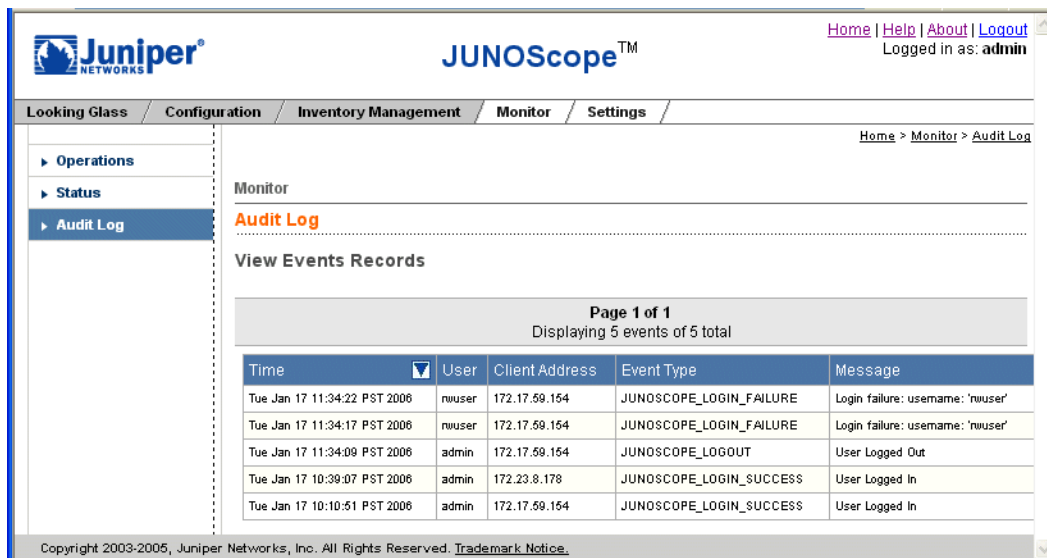
Filter Rule
Limit to 10 rows per page
Sort results by Time
Refresh Events every Never
Event Category ALL
Event Type ALL
<input type="checkbox"/> Updated in last 0 seconds
<input type="checkbox"/> Associated with user admin

An 'OK' button is located at the bottom left of the dialog.

2. Select a filter rule to select the audit log records that you want to view:
 - Limit to *number* of rows per page drop-down list box—Select how many record rows you want to display per audit log page: 10, 25, 50, or 100. The default is 10.
 - Sort results by *column-name* drop-down list box—Select the column of data by which the audit log records will be sorted in the table: Time, Username, Client address, Event type, or Message. The default is Time.
 - Refresh Events every *interval* drop-down list box—Select when the audit log data will be updated in the table: from Never up to 1 hour. The default is Never.

- Event Category drop-down list box—Select the events category to display: All, Authentication, or Privileged Operations. Authentication activities include user login success, failure, logout, and session timeout. Privileged operations are changes of information in the system or in the network, such as restoring a configuration to a device or changing a user password. The default is All.
- Event Type drop-down list box—This list box is dynamically populated based on the event category that you selected. For example, if you select the authentication event category, all authentication event message types appear in this drop-down list box.
- Updated in last time period check box, text box, and drop-down list box—Select the audit log records that have been updated in the last specified length of time. You can select n seconds, minutes, hours, or days. Where n represents the time you specify. The default is 0 seconds.
- Associated with user drop-down list box—Select records that are associated with a specified username.

3. Click OK. The Audit Log dialog box appears.



Each audit record includes the date and time, event category, event type, username, and client IP address. The records are initially sorted by time in descending order so that the most recent events are at the top of the list. See Table 17.

Table 17: Audit Log Columns

Column Name	Description
Time	<p>The date and time that the event was logged. The format for date and time is <i>dow mon dd hh:mm:ss zzz yyyy</i>.</p> <p>Where:</p> <ul style="list-style-type: none"> ■ <i>dow</i> is the day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). ■ <i>mon</i> is the month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec). ■ <i>dd</i> is the day of the month (01 through 31), as two decimal digits. ■ <i>hh</i> is the hour of the day (00 through 23), as two decimal digits. ■ <i>mm</i> is the minute within the hour (00 through 59), as two decimal digits. ■ <i>ss</i> is the second within the minute (00 through 61), as two decimal digits. ■ <i>zzz</i> is the time zone (and may reflect Daylight Saving Time). If time zone information is not available, then <i>zzz</i> is empty; that is, it consists of no characters at all. ■ <i>yyyy</i> is the year, as four decimal digits.
User	The name of the user who performed that action that was logged. The default user is admin.
Client Address	The IP address of the client from which the action occurred.
Event Type	The title of the system log message that is logged.
Message	The description of the system log message that is logged.

