

# Audit and Syslog

The following topics describe how to audit activity on your system:


- System log, on page 1
- About system auditing, on page 3


# System log

The System Log (syslog) page provides you with system log information for the appliance.

### System audit capabilities

You can audit activity on your system in two ways. The appliances that are part of the system generate an audit record for each user interaction with the web interface, and also record system status messages in the system log.

The system log displays each message generated by the system. These items are listed in order:

- The date that the message was generated.
- The time that the message was generated.
- The host that generated the message.
- The message itself.

## View the system log

View system log information that is local to your system to monitor and troubleshoot system events and activities.

System log information is local. For example, you **cannot** use the Firewall Management Center to view system status messages in the system logs on your managed devices.

You can filter messages using most syntax accepted by the UNIX file search utility Grep. This includes using Grep-compatible regular expressions for pattern matching.

**Before you begin**

To view system statistics, ensure you have Admin or Maintenance privileges in the Global domain.

### Procedure

**Step 1** Choose **System** (⚙) > **Monitoring** > **Syslog**.

**Step 2** To search for specific message content in the system log:

a) Enter a word or query in the filter field as described in Syntax for system log filters, on page 2.

Only Grep-compatible search syntax is supported.

Examples:

- To search for all log entries that contain the user name "Admin," use `Admin`.
- To search for all log entries that are generated on November 27, use `Nov[[:space:]]*27` or `Nov.*27` (but not `Nov 27` or `Nov*27`).
- To search for all log entries that contain authorization debugging information on November 5, use `Nov[[:space:]]*5.*AUTH.*DEBUG`.

b) To make your search case-sensitive, select **Case-sensitive**.

By default, filters are not case-sensitive.

c) To search for all system log messages that do **not** meet the criteria you entered, select **Exclusion**.

d) Click **Go**.

## Syntax for system log filters

This table shows the regular expression syntax you can use in System Log filters.

***Table 1: System log filter syntax***

| Syntax Component | Description | Example |
|---|---|---|
| . | Matches any character or white space | `Admi.` matches `Admin`, `AdmiN`, `Admi1`, and `Admi` |
| `[[:alpha:]]` | Matches any alphabetic character | `[[:alpha:]]dmin` matches `Admin`, `bdmin`, and |
| `[[:upper:]]` | Matches any uppercase alphabetic character | `[[:upper:]]dmin` matches `Admin`, `Bdmin`, and |
| `[[:lower:]]` | Matches any lowercase alphabetic character | `[[:lower:]]dmin` matches `admin`, `bdmin`, and |
| `[[:digit:]]` | Matches any numeric character | `[[:digit:]]dmin` matches `0dmin`, `1dmin`, and |
| `[[:alnum:]]` | Matches any alphanumeric character | `[[:alnum:]]dmin` matches `1dmin`, `admin`, `2dmin`, |
| `[[:space:]]` | Matches any white space, including tabs | `Feb[[:space:]]29` matches logs from Februar |
| * | Matches zero or more instances of the character or expression it follows | `ab*` matches `a`, `ab`, `abb`, `ca`, `cab`, and `cabb`<br>`[ab]*` matches anything |
| ? | Matches zero or one instances | `ab?` matches `a` or `ab` |

| Syntax Component | Description | Example |
|---|---|---|
| \ | Allows you to search for a character typically interpreted as regular expression syntax | `alert\?` matches `alert?` |

# About system auditing

The appliances that are part of the system generate an audit record for each user interaction with the web interface.

**Related Topics**

Standard reports

# Audit records

Firewall Management Center logs read-only auditing information for user activity. Audit logs appear in a standard event view that allows you to view, sort, and filter audit log messages based on any item in the audit view. You can easily delete audit information, generate reports, and review detailed records of the changes that users make.

### Audit record storage and limitations

The audit log stores a maximum of 100,000 entries. When the number of audit log entries exceeds 100,000, the appliance prunes the oldest records from the database to reduce the number to 100,000.

The audit logs do not display the user or the source IP for login errors:

- When wrong password is used, the source IP is not displayed.
- When the user account does not exist, both source IP and the user are not displayed.
- If the attempt for an LDAP user fails, no audit log is triggered.

**Related Topics**

Guidelines for SSO configuration on Firewall Management Center

## View audit records

Monitor system activities and configuration changes by reviewing audit records.

Accessing audit records allows you to track events, system changes, and configuration activity for Firewall Management Center. You can use predefined workflows or create custom views that display only the information relevant to your needs.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

**Before you begin**

Ensure you have admin privileges.

### Procedure

**Step 1** Access the audit log from **System** (⚙) > **Monitoring** > **Audit**.

**Step 2** If no events are visible, adjust the time range to include the desired events.

For more information, see Event time constraints.

**Note** Events that were generated outside the appliance's configured time window (whether global or event specific) may appear in an event view if you constrain the event view by time. This can occur even if you configured a sliding time window for the appliance.

**Step 3** You have these choices:

The choices are applicable only based on the results of the search constraints. For example, when you search for **Health Events**, the resulting view page displays **Workflow** option. Similarly, only when you are in the **Vulnerabilities** table view, the option to view (**View** (👁)) specific vulnerability is displayed.

| Action | Link to topic |
|---|---|
| To learn more about the contents of the columns in the table. | Refer to System log, on page 1. |
| To sort and constrain events on the current workflow page. | Refer to Use table view pages. |
| To navigate between pages in the current workflow, keeping the current constraints, click the appropriate page link at the top left of the workflow page. | Refer to Use workflows. |
| To drill down to the next page in the workflow. | Refer to Use drill-down pages. |
| To constrain on a specific value, click a value within a row. If you click a value on a drill down page, you move to the next page and constrain on the value. Note that clicking a value within a row in a table view constrains the table view and does **not** drill down to the next page.<br>**Tip**<br>Each table view includes **Table View** in its page name. | See Event view constraints for more information. |
| To delete audit records, check the check boxes next to events you want to delete, then click **Delete**, or click **Delete All** to delete all events in the current constrained view. | - |
| To bookmark the current page, click **Bookmark This Page** so you can quickly return to it. | For more information, see Bookmarks. |

| Action | Link to topic |
|---|---|
| To navigate to the bookmarked management page, click **View Bookmarks**. | For more information, see Bookmarks. |
| To generate reports based on the data in the current view, click **Create Reports**. | For more information, see Create a report template from an event view. |
| To compare system changes recorded in the audit log, click **Compare** next to applicable events in the **Message** column. | For more information, see Use audit log to examine changes, on page 6. |

### Related Topics

Event view constraints

## Audit log workflow fields

This table describes the audit log fields that can be viewed and searched.

***Table 2: Audit log fields***

| Field | Description |
|---|---|
| Time | Time and date that the appliance generated the audit record. |
| User | User name of the user that triggered the audit event. |
| Subsystem | The full menu path the user followed to generate the audit record. For example, **System** (⚙) > **Monitoring** > **Audit** is the menu path to view the audit log.<br>In a few cases where a menu path is not relevant, the Subsystem field displays only the event type. For example, **Login** classifies user login attempts. |
| Message | The action the user performed or the button the user clicked on the page.<br>For example, `Page View` signifies that the user simply viewed the page indicated in the Subsystem, while `Save` means that the user clicked the **Save** button on the page.<br>Changes made to the system appear with a **Compare icon** that you can click to see a summary of the changes. |
| Source IP | IP address associated with the host used by the user.<br>Note: When searching this field you must type a specific IP address; you cannot use IP ranges when searching audit logs. |
| Domain | The current domain of the user when the audit event was triggered. This field is only present if you have ever configured the Firewall Management Center for multitenancy. |
| Configuration Change<br>(search only) | Specifies whether to view audit records of configuration changes in the search results. (`yes` or `no`) |

| Field | Description |
|---|---|
| Count | The number of events that match the information that appears in each row. Note that the Count field appears only after you apply a constraint that creates two or more identical rows. This field is not searchable. |

**Related Topics**

Event searches

## The audit events table view

You can customize the layout of the audit events table view or filter events by specific field value.

Use these options to customize the audit events table view:

- You can change the layout of the event view, or constrain the events in the view by a field value.
- To disable a column, click **Close** (✕) in the desired column heading. Click **Apply** in the pop-up window. When you disable a column, it is disabled for the duration of your session (unless you add it back later).

**Note** When you disable the first column, the Count column is added.

- To hide or show other columns, or to add a disabled column back to the view, select or clear the appropriate check boxes before you click **Apply**.
- Clicking a value within a row in a table view constrains the table view and does not drill down to the next page in the workflow.

**Tip** Table views always include "Table View" in the page name.

**Related Topics**

Use workflows

## Use audit log to examine changes

You can use the audit log to view detailed reports about changes made to your system. These reports show the current configuration and compare it to the most recent configuration before a supported change.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

**Before you begin**

You must have admin privileges to access and use the audit log features.

**Procedure**

**Step 1** Choose **System** (⚙) > **Monitoring** > **Audit**.

**Step 2** In the audit log, find the event you want to review. Click **Compare** next to the log entry in the **Message** column.

**Step 3** On the **Compare Configurations** page, review the highlighted differences between the previous and current configurations.

- Blue indicates that the highlighted setting is different in the two configurations. The difference is noted in red text.
- Green indicates that the highlighted setting appears in one configuration but not the other.
- The audit event type, timestamps, and user who made the change appear in the title bar for each configuration.

**Tip** You can navigate through changes individually by clicking **Previous** or **Next** above the title bar. If the change summary is more than one page long, you can also use the scroll bar on the right to view additional changes.

## Suppress audit records

Suppress audit records for specific types of user interactions that your auditing policy does not require monitoring.

If your auditing policy does not require that you audit specific types of user interactions with the system, you can prevent those interactions from generating audit records. For example, by default, each time a user views the online help, the system generates an audit record. If you do not need to keep a record of these interactions, you can automatically suppress them.

To configure audit event suppression, you must have access to an appliance's `admin` user account, and you must be able to either access the appliance's console or open a secure shell.

**Caution** Make sure that only authorized personnel have access to the appliance and to its `admin` account.

### Before you begin

You must have admin privileges to perform this procedure.

### Procedure

In the `/etc/sf` directory, create one or more `AuditBlock` files in the following form, where type is one of the types described in Audit block types, on page 8:

`AuditBlock.`*`type`*

**Note** If you create an `AuditBlock.type` file for a specific type of audit message, but later decide that you no longer want to suppress them, you must delete the contents of the `AuditBlock.type` file, but leave the file itself on the system.

## Audit block types

Each audit block type requires content in a specific format, as described in the following table. Ensure you use the correct capitalization for file names, because the contents are case sensitive.

**Note** When you add an `AuditBlock` file, an audit record with a subsystem of `Audit` and a message of `Audit Filter type Changed` is added to the audit events. For security reasons, this audit record **cannot** be suppressed.

***Table 3: Audit block types***

| Type | Description |
|---|---|
| Address | Create a file named `AuditBlock.address` and include, one per line, each IP address that you want to suppress from the audit log. You can use partial IP addresses provided that they map from the beginning of the address. For example, the partial address `10.1.1` matches addresses from `10.1.1.0` through `10.1.1.255`. |
| Message | Create a file named `AuditBlock.message` and include, one per line, the message substrings that you want to suppress.<br>Note that substrings are matched so that if you include `backup` in your file, all messages that include the word `backup` are suppressed. |
| Subsystem | Create a file named `AuditBlock.subsystem` and include, one per line, each subsystem that you want to suppress.<br>Note that substrings are **not** matched. You must use exact strings. See Audited subsystems, on page 8 for a list of subsystems that are audited. |
| User | Create a file named `AuditBlock.user` and include, one per line, each user account that you want to suppress. You can use partial string matching provided that they map from the beginning of the username. For example, the partial username `IPSAnalyst` matches the user names `IPSAnalyst1` and `IPSAnalyst2`. |

## Audited subsystems

This table lists audited subsystems.

*Table 4: Subsystem names*

| Name | Includes user interactions with... |
|---|---|
| Admin | Administrative features such as system and access configuration, time synchronization, backup and restore, device management, user account management, and scheduling |
| Alerting | Alerting functions such as email, SNMP, and syslog alerting |
| Audit Log | Audit event views |
| Audit Log Search | Audit event searches |
| Command Line | Command line interface |
| Configuration | Email alerting |
| contextual cross-launch | External resources added to the system or accessed from dashboards and event views |
| COOP | Continuity of operations feature |
| Date | Date and time range for event views |
| Default Subsystem | Options that do not have assigned subsystems |
| Detection & Prevention Policy | Menu options for intrusion policies |
| Error | System-level errors |
| eStreamer | eStreamer configuration |
| EULA | Reviewing the end user license agreement |
| Events | Intrusion and discovery event views |
| Events Reviewed | Reviewed intrusion events |
| Events Search | Any event search |
| Failed to install rule update **rule_update_id** | Installing rule updates |
| Header | Initial presentation of the user interface after a user logs in |
| Health | Health monitoring |
| Health Events | Health monitoring event views |
| Help | Online help |
| High Availability | Establishing and handling Firewall Management Centers in high availability pairs |
| IDS Impact Flag | Impact flag configuration for intrusion events |

| Name | Includes user interactions with... |
|---|---|
| IDS Policy | Intrusion policies |
| IDSRule sid:**sig_id** rev:**rev_num** | Intrusion rules by SID |
| Install | Installing updates |
| Intrusion Events | Intrusion events |
| Login | Web interface login and logout functions |
| Logout | Web interface logout functions |
| Menu | Any menu option |
| Configuration export > **config_type** > **config_name** | Importing configurations of a specific type and name |
| Permission Escalation | User role escalation |
| Preferences | User preferences, such as the time zone for a user account and individual event preferences |
| Policy | Any policy, including intrusion policies |
| Register | Registering devices on a Firewall Management Center |
| RemoteStorageDevice | Configuring remote storage devices |
| Reports | Report listing and report designer features |
| Rules | Intrusion rules, including the intrusion rules editor and the rule importation process |
| Rule Update Import Log | Viewing the rule update import log |
| Rule Update Install | Installing rule updates |
| Session Expiration | Web interface session timeouts |
| Status | Syslog, as well as host and performance statistics |
| System | Various system-wide settings |
| Task Queue | Viewing background process status |
| Users | Creating and modifying user accounts and roles |

## About sending audit logs to an external location

To send audit logs to an external location from the Firewall Management Center, see:

- Audit logs
- Audit log certificates