Send audit log data to a remote syslog server

Published: 2024-04-01

The audit log collects data about ExtraHop system operations, broken down by component. The log stored on the system has a capacity of 10,000 entries, and entries older than 90 days are automatically removed. You can view these entries in the Administration settings, or you can send the audit log events to a syslog server for long-term storage, monitoring, and advanced analysis. All logged events are listed in the table below.

The following steps show you how to configure the ExtraHop system to send audit log data to a remote syslog server.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Status and Diagnostics section, click **Audit Log**.
3. Click **Configure Syslog Settings**.
4. In the Destination field, type the IP address of the remote syslog server.
5. From the Protocol drop-down menu, select **TCP** or **UDP**. This option specifies the protocol over which the information is sent to your remote syslog server.
6. In the Port field, type the port number for your remote syslog server. By default, this value is set to 514.
7. Click **Test Settings** to verify that your syslog settings are correct. If the settings are correct, you should see an entry in the syslog log file on the syslog server similar to the following:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

8. Click **Save**.
9. Optional: Modify the format of syslog messages.

   By default, syslog messages are not compliant with RFC 3164 or RFC 5424. However, you can format syslog messages to be compliant by modifying the running config.

   a) Click **Admin**.
   b) Click **Running Config (Unsaved Changes)**.
   c) Click **Edit Config**.
   d) Add an entry under `auditlog_rsyslog` where the key is `rfc_compliant_format` and the value is either `rfc5424` or `rfc3164`.

      The `auditlog_rsyslog` section should look similar to the following code:

      ```
      "auditlog_rsyslog": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```

   e) Click **Update**.
   f) Click **Done**.

10. Optional: Modify the timezone referenced in syslog timestamps.

    By default, syslog timestamps reference UTC time. However, you can modify timestamps to reference the ExtraHop system time by modifying the running config.

    a) Click **Admin**.
    b) Click **Running Config (Unsaved Changes)**.
    c) Click **Edit Config**.

d) Add an entry under `auditlog_rsyslog` where the key is `syslog_use_localtime` and the value is `true`.

The `auditlog_rsyslog` section should look similar to the following code:

```
    "auditlog_rsyslog": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

e) Click **Update**.

f) Click **Done**.

Next steps

After you confirm that your new settings are working as expected, preserve your configuration changes by saving the running configuration file.

Audit log events

The following events on an ExtraHop system generate an entry in the audit log.

Category	Event
Agreements	• A EULA or POC agreement is agreed to
API	• An API key is created • An API key is deleted • A user is created. • A user is modified.
Sensor Migration	• A sensor migration is started • A sensor migration succeeded • A sensor migration failed
Browser sessions	• A specific browser session is deleted • All browser sessions are deleted
Cloud Services	• Status of a connected sensor is retrieved
Console	• A sensor connects to a console • A sensor disconnects from a console • An ExtraHop recordstore or packetstore establishes a tunneled connection to a console • Console information is set • A console nickname is set • Enable or disable a sensor • The sensor is remotely viewed • A license for a sensor is checked by a console • A license for a sensor is set by a console
Dashboards	• A dashboard is created • A dashboard is renamed • A dashboard is deleted

Category	Event
	• A dashboard permalink, also known as a short code, is modified • Dashboard sharing options are modified
Datastore	• The extended datastore configuration is modified • The datastore is reset • A datastore reset completed • Customizations are saved • Customizations are restored • Customizations are deleted
Detections	• A detection status is updated • A detection assignee is updated • Detection notes are updated • An external ticket is updated • A tuning rule is created • A tuning rule is deleted • A tuning rule is modified • A tuning rule description is updated • A tuning rule is enabled • A tuning rule is disabled • A tuning rule is extended
Exception files	• An exception file is deleted
ExtraHop recordstore records	• All ExtraHop recordstore records are deleted
ExtraHop recordstore cluster	• A new ExtraHop recordstore node is initialized • A node is added to an ExtraHop recordstore cluster • A node is removed from an ExtraHop recordstore cluster • A node joins an ExtraHop recordstore cluster • A node leaves an ExtraHop recordstore cluster • A sensor or console is connected to an ExtraHop recordstore • A sensor or console is disconnected from an ExtraHop recordstore • An ExtraHop recordstore node is removed or missing, but not through a supported interface
ExtraHop Update Service	• A detection category is updated • A detection definition is updated • A detection trigger is updated • A ransomware definition is updated • Detection metadata is updated • Expanded detection content is updated
Firmware	• Firmware is upgraded

Category	Event
Global Policies	• Global policy for device group edit control is updated
Integrations	• An integration is updated
License	• A new static license is applied • License server connectivity is tested • A product key is registered with the license server • A new license is applied
Login to the ExtraHop system	• A login succeeds • A login fails
Login from SSH or REST API	• A login succeeds • A login fails
Modules	• NDR module access control is enabled • NPM module access control is enabled
Network	• A network interface configuration is edited • The hostname or DNS setting is changed • A network interface route is changed
Offline capture	• An offline capture file is loaded
PCAP	• A packet capture (PCAP) file is downloaded
Remote Access	• Remote access for ExtraHop Support Team is enabled • Remote access for ExtraHop Support Team is disabled • Remote access for ExtraHop Atlas Analysts is enabled • Remote access for ExtraHop Atlas Analysts is disabled • Remote access for ExtraHop Support is enabled • Remote access for ExtraHop Support is disabled
RPCAP	• An RPCAP configuration is added • An RPCAP configuration is deleted
Running Config	• The running configuration file changes
SAML Identity Provider	• An identity provider is added • An identity provider is modified • An identity provider is deleted
SAML login	• A login succeeds

Category	Event
	• A login fails
SAML privileges	• A privilege level is granted • A privilege level is denied
SSL decryption	• An SSL decryption key is saved
SSL session keys	• A PCAP session key is downloaded
Support account	• The support account is disabled • The support account is enabled • The support SSH key is regenerated
Support Script	• A default support script is running • A past support script result is deleted • A support script is uploaded
Syslog	• Remote syslog settings are updated
System and service status	• The system starts up • The system shuts down • The system is restarted • The bridge, capture, or portal process is restarted • A system service is enabled (such as SNMP, web shell, management, SSH) • A system service is disabled (such as SNMP, web shell, /management, SSH)
System time	• The system time is set • The system time is changed • The system time is set backwards • NTP servers are set • The time zone is set • A manual NTP synchronization is requested
System user	• A user is added • User metadata is edited • A user is deleted • A user password is set • A user other than the `setup` user attempts to modify the password of another user • A user password is updated
Threat briefings	• A threat briefing is archived • A threat briefing is restored
ExtraHop packetstore	• A new ExtraHop packetstore is initialized • A sensor or console is connected to an ExtraHop packetstore

Category	Event
	• A sensor or console is disconnected from an ExtraHop packetstore • An ExtraHop packetstore is reset
Trends	• A trend is reset
Triggers	• A trigger is added • A trigger is edited • A trigger is deleted
User Groups	• A local user group is created • A local user group is deleted • A local user group is enabled • A local user group is disabled