

Send audit log data to a remote syslog server

Published: 2018-04-20

The ExtraHop appliance audit log provides 90 days of lookback data about the operations of the system, broken down by component. You can view the audit log entries in the Admin UI 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 Audit log events table below.

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

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Status and Diagnostics section, click **Audit Log**.
3. Click **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**.

Next steps

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

Audit log events

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

| Category | Event |
|-------------------------------|--|
| Login from Web UI or Admin UI | <ul style="list-style-type: none"> • A login succeeds • A login fails |
| Login from SSH or REST API | <ul style="list-style-type: none"> • A login succeeds. • A login fails. |
| Running Config | The running configuration file changes |
| Support Script | <ul style="list-style-type: none"> • A default support script is running • A past support script result is deleted • A support script is uploaded |
| System and service status | <ul style="list-style-type: none"> • The system starts up • The system shuts down • The system is restarted |

| Category | Event |
|-------------------|--|
| | <ul style="list-style-type: none"> • 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) |
| Network | <ul style="list-style-type: none"> • A network interface configuration is edited • The hostname or DNS setting is changed • A network interface route is changed |
| Browser sessions | <ul style="list-style-type: none"> • A specific browser session is deleted • All browser sessions are deleted |
| Support account | <ul style="list-style-type: none"> • The support account is disabled • The support account is enabled • The support key is regenerated |
| System time | <ul style="list-style-type: none"> • 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 |
| Firmware | <ul style="list-style-type: none"> • Firmware is upgraded • Archived firmware is deleted |
| License | <ul style="list-style-type: none"> • 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 |
| Command appliance | <ul style="list-style-type: none"> • A Discover appliance connects to a Command appliance • A Discover appliance disconnects from a Command appliance • An Explore or Trace appliance establishes a tunneled connection to a Command appliance • Command appliance information is set • A Command nickname is set • Enable or disable a Discover appliance • The Discover appliance Web UI is remotely viewed • A license for a Discover appliance is checked by a Command appliance • A license for a Discover appliance is set by a Command appliance |
| Agreements | A EULA or POC agreement is agreed to |

| Category | Event |
|-----------------|--|
| SSL decryption | An SSL decryption key is saved |
| Appliance user | <ul style="list-style-type: none"> A user is added User metadata is edited A user is deleted A user password is set A user other than the <code>setup</code> user attempts to modify the password of another user A user password is updated |
| API | <ul style="list-style-type: none"> An API key is created An API key is deleted |
| Triggers | <ul style="list-style-type: none"> A trigger is added A trigger is edited A trigger is deleted |
| Dashboards | <ul style="list-style-type: none"> A dashboard is created A dashboard is renamed A dashboard is deleted A dashboard permalink, also known as a short code, is modified Dashboard sharing options are modified |
| Trends | A trend is reset |
| PCAP | A packet capture (PCAP) is downloaded |
| RPCAP | <ul style="list-style-type: none"> An RPCAP configuration is added An RPCAP configuration is deleted |
| Syslog | Remote syslog settings are updated |
| Support account | <ul style="list-style-type: none"> The support account is enabled The support account is disabled |
| Atlas | <ul style="list-style-type: none"> The Atlas Remote UI account is enabled The Atlas Remote UI account is disabled The connection to the Atlas Service is reset A Discover appliance disconnects from the Atlas Service |
| Datastore | <ul style="list-style-type: none"> The extended datastore configuration is modified The datastore is reset A datastore reset completed Customizations are saved Customizations are restored Customizations are deleted |
| Offline capture | An offline capture is loaded |
| Exception files | An exception file is deleted |

| Category | Event |
|-----------------------------|--|
| Explore cluster | <ul style="list-style-type: none"> • A new Explore node is initialized • A node is added to an Explore cluster • A node is removed from an Explore cluster • A node joins an Explore cluster • A node leaves an Explore cluster • A Discover or Command appliance is paired to an Explore appliance • A Discover or Command appliance is unpaired from an Explore appliance • An Explore node is removed or missing, but not through a supported interface |
| Explore appliance records | All Explore appliance records are deleted |
| Trace appliance | <ul style="list-style-type: none"> • A new Trace appliance is initialized. • A Discover or Command appliance is paired to a Trace appliance. • A Discover or Command appliance is disconnected from a Trace appliance. |
| Trace appliance packetstore | A Trace appliance packetstore is reset. |