

Send audit log data to a remote syslog server

Published: 2021-08-31

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**.

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 system generate an entry in the audit log.

| Category | Event |
|---------------------|--|
| Agreements | <ul style="list-style-type: none"> • A EULA or POC agreement is agreed to |
| API | <ul style="list-style-type: none"> • An API key is created • An API key is deleted • A user is created. • A user is modified. |
| Appliance Migration | <ul style="list-style-type: none"> • An appliance migration is started • An appliance migration succeeded • An appliance migration failed |
| Browser sessions | <ul style="list-style-type: none"> • A specific browser session is deleted • All browser sessions are deleted |
| Cloud Services | <ul style="list-style-type: none"> • Status of a connected sensor is retrieved |

| Category | Event |
|---------------------------|---|
| 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 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 |
| 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 |
| 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 |
| Detections | <ul style="list-style-type: none"> • An investigation status is updated • An investigation assignee is updated • Investigation notes are updated • An external ticket is updated • A detection rule is added • A detection rule description is updated • A detection rule is enabled • A detection rule is disabled • A detection rule is extended |
| Exception files | <ul style="list-style-type: none"> • An exception file is deleted |
| Explore appliance records | <ul style="list-style-type: none"> • All Explore appliance records are deleted |
| 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 |

| Category | Event |
|------------------------------|---|
| | <ul style="list-style-type: none"> • A Discover or Command appliance is connected to an Explore appliance • A Discover or Command appliance is disconnected from an Explore appliance • An Explore node is removed or missing, but not through a supported interface |
| ExtraHop Update Service | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • Firmware is upgraded |
| Global Policies | <ul style="list-style-type: none"> • Global policy for detections access is updated |
| 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 |
| Login to the ExtraHop system | <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 |
| 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 |
| Offline capture | <ul style="list-style-type: none"> • An offline capture file is loaded |
| PCAP | <ul style="list-style-type: none"> • A packet capture (PCAP) file is downloaded |
| Remote Access | <ul style="list-style-type: none"> • 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. |

| Category | Event |
|---------------------------|---|
| RPCAP | <ul style="list-style-type: none"> An RPCAP configuration is added An RPCAP configuration is deleted |
| Running Config | <ul style="list-style-type: none"> The running configuration file changes |
| SAML Identity Provider | <ul style="list-style-type: none"> An identity provider is added An identity provider is modified An identity provider is deleted |
| SAML login | <ul style="list-style-type: none"> A login succeeds A login fails |
| SAML privileges | <ul style="list-style-type: none"> A privilege level is granted A privilege level is denied |
| SSL decryption | <ul style="list-style-type: none"> An SSL decryption key is saved |
| SSL session keys | <ul style="list-style-type: none"> A PCAP session key is downloaded |
| Support account | <ul style="list-style-type: none"> The support account is disabled The support account is enabled The support SSH key is regenerated |
| 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 |
| Syslog | <ul style="list-style-type: none"> Remote syslog settings are updated |
| System and service status | <ul style="list-style-type: none"> 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 | <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 |
| System user | <ul style="list-style-type: none"> A user is added User metadata is edited A user is deleted A user password is set |

| Category | Event |
|-----------------------------|---|
| | <ul style="list-style-type: none"> • A user other than the <code>setup</code> user attempts to modify the password of another user • A user password is updated |
| Trace appliance | <ul style="list-style-type: none"> • A new Trace appliance is initialized. • A Discover or Command appliance is connected to a Trace appliance. • A Discover or Command appliance is disconnected from a Trace appliance |
| Trace appliance packetstore | <ul style="list-style-type: none"> • A Trace appliance packetstore is reset |
| Trends | <ul style="list-style-type: none"> • A trend is reset |
| Triggers | <ul style="list-style-type: none"> • A trigger is added • A trigger is edited • A trigger is deleted |
| User Groups | <ul style="list-style-type: none"> • A local user group is created • A local user group is deleted • A local user group is enabled • A local user group is disabled |