Configure syslog settings to send system notifications to a remote syslog server

Published: 2018-04-20

The syslog export option enables you to send alerts from an ExtraHop appliance to any remote system that receives syslog input for long-term archiving and correlation with other sources.

Only one remote syslog server can be configured for each ExtraHop appliance.

1. Log into the Admin UI on the ExtraHop appliance.
2. In the Network Settings section, click **Notifications**.
3. In the Destination field, type the IP address of the remote syslog server.
4. From the Protocol drop-down menu, select **TCP** or **UDP**. This option specifies the protocol over which the information will be sent to your remote syslog server.
5. In the Port field, type the port number for your remote syslog server. By default, this value is set to 514.
6. 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
   ```

7. Click **Save**.

Next steps

After you confirm that your new settings are working as expected, preserve your configuration changes through system restart and shutdown events by saving the Running Config file.