Configure a syslog target for an open data stream

Published: 2024-04-01

You can export data on an ExtraHop system to any system that receives syslog input (such as Splunk, ArcSight, or Q1 Labs) for long-term archiving and comparison with other sources.

- 1. Log in to the Administration settings on the ExtraHop system through https://extrahop-hostname-or-IP-address>/admin.
 - Repeat these steps on each sensor in your environment.
- 2. In the System Configuration section, click **Open Data Streams**.
- 3. Click **Add Target**.
- 4. From the Target Type drop-down menu, select **Syslog**.
- 5. In the Name field, type a name to identify the target.
- 6. In the Host field, type the hostname or IP address of the remote syslog server.
- 7. In the Port field, type the port number of the remote syslog server.
- 8. From the Protocol drop-down menu, select one of the following protocols over which to transmit data:
 - TCP
 - UDP
 - SSL/TLS
- 9. Optional: Select **Local Time** to send syslog information with timestamps in the local time zone of the ExtraHop system. If this option is not selected, timestamps are sent in GMT.
- 10. Optional: Select **Length-prefix framing** to prepend the number of bytes in a message to the beginning of each message. If this option is not selected, the end of each message is delimited by a trailing newline.
- 11. Optional: In the **Batch min bytes** field, type the minimum number of bytes to send to the syslog server at a time.
- 12. Optional: In the **Concurrent connections** field, type the number of concurrent connections to send messages over.
- 13. Optional: If you selected the **SSL/TLS** protocol, specify certificate options.
 - a) If the Syslog server requires client authentication, specify a TLS client certificate to send to the server in the **Client certificate** field.
 - b) If you specified a client certificate, specify the private key of the certificate in the **Client key** field.
 - c) If you do not want to verify the certificate of the Syslog server, select **Skip server certificate** verification.
 - d) If you want to verify the certificate of the Syslog server, but the certificate has not been signed by a valid Certificate Authority (CA), specify trusted certificates to verify the server certificate with in the **CA certificates (optional)** field. Specify the certificates in PEM format. If this option is not specified, the server certificate is validated with the built-in list of valid CA certificates.
- 14. Optional: Click **Test** to establish a connection between the ExtraHop system and the remote syslog server and send a test message to the server.
 - The dialog box displays a message that indicates whether the connection succeeded or failed. If the test fails, edit the target configuration and test the connection again.
- 15. Click Save.

Next steps

Create a trigger that specifies what syslog message data to send and initiates the transmission of data to the target. For more information, see the Remote.Syslog & class in the ExtraHop Trigger API Reference &.