Configure an HTTP target for an open data stream

Published: 2025-02-08

You can export data on an ExtraHop system to a remote HTTP server 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 **HTTP**.
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 HTTP server.
7. In the Port field, type the port number of the remote HTTP server.
8. From the Type drop-down menu, select one of the following protocols:
   - **HTTP**
   - **HTTPS**
9. If you selected HTTPS, select **Skip certificate verification** to bypass certificate verification of encrypted data. Data can be verified by trusted certificates that you upload to the ExtraHop system.

   Note: Secure connections to the HTTPS ODS server can be verified through trusted certificates that you upload to the ExtraHop system.
10. Select **Multiple connections** to enable concurrent requests through multiple connections, which can improve throughput speed.
11. In the Additional HTTP Header field, type an additional HTTP header.

    The format for the additional header is *Header* : *Value*.

    Note: Headers configured in a trigger take precedence over an additional header. For example, if the Additional HTTP Header field specifies `Content-Type: text/plain` but a trigger script for the same ODS target specifies `Content-Type: application/json`, then `Content-Type: application/json` is included in the HTTP request.
12. Optional: From the Authentication drop-down menu, select the type of authentication from the following options.

Option	Description
Basic	Authenticates through a username and password.
Amazon AWS	Authenticates through Amazon Web Services.
Microsoft Azure Storage	Authenticates through Microsoft Azure.
Microsoft Entra ID	Authenticates through Microsoft Entra ID (v1.0). **Note:** Microsoft identity platform (v2.0) is not supported.
CrowdStrike	Authenticates through CrowdStrike.

13. Select **Connect through global proxy** to send requests through the global proxy server configured for the ExtraHop system.
14. Optional: Click **Test** to establish a connection between the ExtraHop system and the remote HTTP 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. Optional: Send a test request to the remote HTTP server.

    The request is for testing purposes only; it is not included in any trigger scripts.

    a) From the Method drop-down menu, select one of the following HTTP request methods:

    - **DELETE**
    - **GET**
    - **HEAD**
    - **OPTIONS**
    - **PUT**
    - **POST**
    - **TRACE**

    b) In the Options field, specify the parameters of the HTTP request in the following format:

```
    "headers": {},
    "payload": "",
    "path": "/"
}
```

    The parameters are defined as follows:

    headers

    The headers of the HTTP request. You must specify headers as an array, even if you specify only one header. For example:

```
"headers": {"content-type":["application/json"]},
```

    path

    The path that the HTTP request will be applied to.

    payload

    The payload of the HTTP request.

    c) Click **Test** to establish a connection between the ExtraHop system and the remote server and send the request.
    The dialog box displays a message that indicates whether the request succeeded or failed, and displays any requested content.

16. Click **Save**.

Next steps

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