

Collect L7 records


Published: 2018-04-20

You can collect L7 records to store on your Explore appliance, which show details from individual messages or transactions over L7 protocols. These types of records require triggers.

Before you begin

- You must connect your Explore appliances to your Discover appliance before you can collect L7 records. See [Connect the Explore appliance to Discover and Command appliances](#).
- These instructions assume some familiarity with ExtraHop Triggers. New users can learn about triggers in our [Triggers Walkthrough](#).

In the following example, you will learn how to collect records for any device that sends or receives an HTTP response. First, we will write a trigger to collect information from the built-in HTTP record type. Then, we will assign the trigger to a web server. Finally, we will verify that the records are being sent to the Explore appliance.

1. Log into the Web UI on your Discover appliance.
2. Click the System Settings icon , and then click **Triggers**.
3. Click **New** to launch the Trigger Configuration window.
4. In the Configuration tab, complete your information, similar to the following example:

- **Name:** HTTP Responses
- **Author:** ExtraHop
- **Description:** This trigger collects HTTP responses.
- **Debugging:** Select the checkbox to enable debugging.
- **Events:** HTTP_RESPONSE

5. Click the **Editor** tab.
6. Type the following example code in the text box:

```
HTTP.commitRecord()  
debug ("committing HTTP responses")
```

This code generates records for the HTTP record type when the HTTP_RESPONSE event occurs and corresponds to the built-in record format for HTTP.

7. Click **Save and Close**. Next, assign this trigger to a web server.
8. Click **Metrics** from the top menu and then click **Devices** in the left pane.
9. Search for an active web server that you want to collect records for. For this example, we will select a web server called `web-sea-example`.
10. Select the checkbox next to the web server (such as `web-sea-example`).
11. Click **Assign Trigger** from the menu above the table.
12. From the list, select the checkbox next to the trigger we previously created named HTTP Responses, and then click **Assign Triggers**.
Records that meet your criteria are now sent to your connected Explore appliance. Wait a few minutes for records to be collected, and then verify that your records are being collected in the next step.
13. Click **Records** from the top menu to launch a query. If you do not see any HTTP records, wait a few minutes and try again. If no records appear after five minutes, review your configuration or contact [ExtraHop Support](#).

Next steps

- [Collect and store custom records](#)

- [Query for stored records from a Discover or Command appliance](#)
- [Commit a custom record to monitor suspicious port activity](#)