


# Configure Addy anomaly alert settings

Published: 2018-11-09

You can configure anomaly alert settings that monitor when an anomaly, detected by the ExtraHop Addy™ service, has occurred on specific protocols. When the conditions configured in the alert settings are met, the ExtraHop system generates an anomaly alert, which you can view in the Alert History.

Anomaly alerts are useful for monitoring unusual behavior that you want to be notified of right away. For example, if you are worried about spikes in SSH sessions on specific servers, you can configure alert settings to watch for anomalies that occur over SSH and assign the alert configuration to SSH servers.

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon  and then click **Alerts**.
3. Click **New** to open the Alert Configuration window.
4. Enter a unique name for the alert configuration in the **Name** field.
5. From the **Alert Type** section, click Anomaly.
6. Click the **Source Type** list and select the data source for the alert configuration. The alert configuration can be assigned only to the type of source selected.
7. Select one of the following [Addy anomaly category](#) options:

<b>Option</b>	<b>Description</b>
<b>Any category</b>	Watches for anomalies on assigned sources that occur over any Addy category.
<b>Specific categories</b>	Watches for anomalies on assigned sources that occur only within specified Addy categories.  Click <b>Select Categories</b> to specify one or more categories, such as Database and Network Infrastructure.

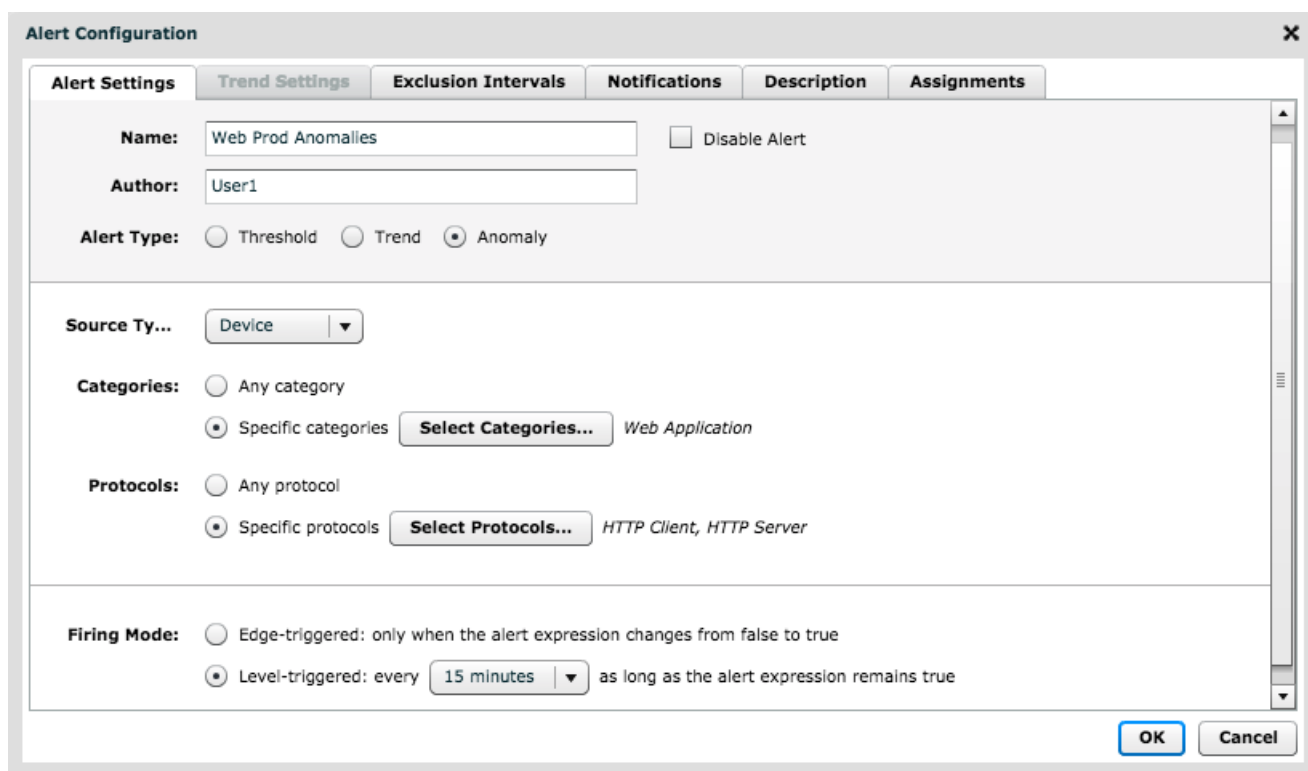
8. Select one of the following protocols options:

<b>Option</b>	<b>Description</b>
<b>Any protocol</b>	Watches for anomalies on assigned sources that occur over any protocol.
<b>Specific protocols</b>	Watches for anomalies on assigned sources that occur only over specified protocols.  Click <b>Select Protocols</b> to specify one or more categories, such as HTTP Client and HTTP Server.

9. Select one of the following firing modes:

<b>Option</b>	<b>Description</b>
<b>Edge-Triggered</b>	Generates an alert only once when the alert conditions are true. The alert is generated again only if conditions are true after the metric value has returned to normal conditions twice.
<b>Level-Triggered</b>	Generates alerts continuously while the alert conditions are true for the specified time period.

10. Click **OK**.



The image shows a screenshot of the 'Alert Configuration' dialog box in the ExtraHop interface. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: 'Alert Settings', 'Trend Settings', 'Exclusion Intervals', 'Notifications', 'Description', and 'Assignments'. The 'Alert Settings' tab is active. The configuration fields are as follows:

- Name:** Web Prod Anomalies
- Author:** User1
- Alert Type:** Radio buttons for Threshold, Trend, and Anomaly (selected).
- Source Ty...:** Device (dropdown menu)
- Categories:** Radio buttons for Any category and Specific categories (selected). A 'Select Categories...' button is next to it, with 'Web Application' listed below.
- Protocols:** Radio buttons for Any protocol and Specific protocols (selected). A 'Select Protocols...' button is next to it, with 'HTTP Client, HTTP Server' listed below.
- Firing Mode:** Radio buttons for Edge-triggered (only when the alert expression changes from false to true) and Level-triggered (selected). The Level-triggered option includes a dropdown menu set to '15 minutes' and the text 'as long as the alert expression remains true'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

### Next steps

- Alerts cannot be generated until you [assign an alert configuration to a source](#).
- [Assign an exclusion interval to an alert](#) to suppress alerts during specific times.
- [Add a notification to an alert configuration](#) to receive emails or SNMP traps when an alert is generated.