


Configure Addy anomaly alert settings

Published: 2018-07-17

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:

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

8. Select one of the following protocols options:

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

9. Select one of the following firing modes:

Option	Description
Edge-Triggered	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.
Level-Triggered	Generates alerts continuously while the alert conditions are true for the specified time period.

10. Click **OK**.

Alert Configuration

Alert Settings | Trend Settings | Exclusion Intervals | Notifications | Description | Assignments

Name: Web Prod Anomalies Disable Alert

Author: User1

Alert Type: Threshold Trend Anomaly

Source Ty...: Device

Categories: Any category
 Specific categories **Select Categories...** Web Application

Protocols: Any protocol
 Specific protocols **Select Protocols...** HTTP Client, HTTP Server

Firing Mode: Edge-triggered: only when the alert expression changes from false to true
 Level-triggered: every 15 minutes as long as the alert expression remains true

OK **Cancel**

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.