Alerts FAQ

Published: 2018-04-20

Here are some answers to frequently asked questions about alerts.

How do I set the alert severity level?

You set the alert severity level on the Notifications tab of the Alert Configuration window.

The severity level you set for an alert is displayed in the Alert History, in emails, and in SNMP traps. You do not have to configure email notifications or SNMP traps to set the severity level.

What alert information is sent in email notifications?

All email notifications provide the following information:

Alert Name

The name specified for the alert.

Alert Comment

The description specified for the alert, if one was provided.

Alert Time

The time the alert conditions were met and the alert was generated.

Alert Source

The name of the metric source and any additional information available, such as the MAC address and IP address for devices.

Alert Source URL

A URL to the specific protocol page of the alert source.

If an anomaly alert email contains multiple protocols, the email also provides a URL to the Overview page of the alert source.

Email notifications for anomaly alerts also include the anomalies observed that met alert conditions. Each anomaly listed includes the following information:

Anomaly title

The name of the anomaly that occurred. Click the anomaly title to go to the specific anomaly in the Alerts section of the ExtraHop Web UI.

Protocol

The watched protocol over which the anomaly occurred.

Metric

The metric that had an abnormal value.

Value

The value of the metric.

Expected Range

The range of values that represent a normal level of activity.

Deviation

The quantity calculated to indicate the extent of change from an expected range.

Email notifications for threshold and trend alerts also provide the following information:

Alert Expression

The sequence of values that specified when to issue the alert.

Value

For threshold alerts, the value of the metric when the threshold was crossed. For trend alerts, a value of 1 indicates that the alert expression was true.

Can I customize text in email notifications?

There is no text field for custom messages in email notifications. However, information can be added to the Description tab of the Alert Configuration window, and that text appears in the email. For example, the text could direct your team to take action, such as restarting devices, when they receive emails for specific alerts.

If I assign an alert configuration to a device group, does it look at metrics on each device or does it look at the consolidated metrics of the group?

If you assign an alert configuration to a device group, it is equal to assigning the alert to each device in the group. If you want to aggregate metrics across all the members of the group, you can create an application that consolidates the devices into a single metric source, and then assign the alert to that application.

Can I assign an alert configuration to an activity group?

You cannot assign an alert configuration to an activity group. However, you can create a custom device group and specify an activity criteria, such as AAA Clients, as the dynamic group type.

How do I remove an alert configuration assignment?

There are two methods for removing an alert configuration assignment:

- Open the source the alert configuration is assigned to and click **Assignments** from the top-right corner of the page. On the Alerts tab, click the remove (X) icon next to each assignment you want to remove from the source.
- Open the alert configuration you want and click the **Assignments** tab to view which sources the alert configuration is assigned to. Click the remove (X) icon next to each source you want to remove the assignment from.

How are trends calculated?

Appliances calculate trends by looking at historical data. Therefore, in most cases, trend alerts are active as soon as they are assigned. Even if you configure a trend alert to reference more historical data than your appliance currently has, the appliance will still attempt to calculate the trend with whatever data is currently available.

Trend-based alerts are triggered when a network statistic is outside of the normal trend learned by the system. Trend-based alerts are well suited for metrics such as errors where meaningful thresholds are difficult to define. Trend-based alerts need historical data to define a trend, so these alerts will be generated once the Discover appliance has collected enough data to establish a baseline.