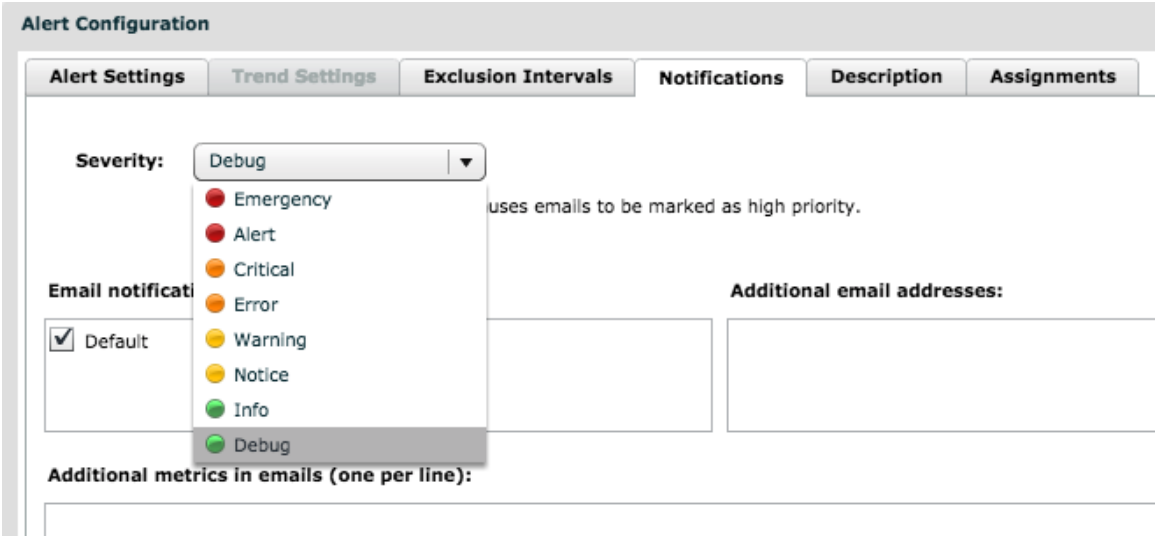
Alerts FAQ

Published: 2020-02-22

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 is independent from notifications; you do not have to configure notifications to configure the severity level of an alert.

The severity level is displayed in email notifications, SNMP traps, and on the Alerts page. The severity status is also reflected in activity maps and geomaps.

- On an activity map, the color of a device corresponds to the most severe alert status for all alerts assigned to the device.
- On a geomap, the color of a data point corresponds to the most severe alert for all alerts tracking the same metric.

What information will I get in an alert email notification?

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. Descriptions over 255 characters are truncated, which is indicated by an ellipses.

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

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

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

Detection title

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

Risk score (ExtraHop Reveal(x) only)

The risk score that indicates the severity of the detection.

Protocol

The watched protocol over which the detection 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.

Alert descriptions support Markdown, which is a simple formatting syntax that converts plain text into HTML. When placed before or around text, certain non-alphabetic characters specify what HTML styling to apply to the text. For example, place double asterisks (**) before and after text you want to display as bold. For more information, see Add Markdown to an alert description.

How do I view alert configuration assignments?

There are two ways to view alert configuration assignments: from a source or from an alert configuration.

View which alert configurations are assigned to a source

Open the source and click **Assignments** or **Alerts** from the top-right corner of the page.

The window displays the following information:

- Alert configurations directly assigned to the source.
- Alert configurations globally assigned to the source.
- The status of the alert configuration and whether the configuration is disabled.

View which sources an alert configuration is assigned to

Open the alert configuration you want and click the **Assignments** tab.

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.

  If the alert has been assigned globally to all applications or devices, you cannot remove the assignment from the individual source.
- Open the alert configuration you want and click the **Assignments** tab. Click the remove (X) icon next to each source you want to remove the assignment from.

How are metrics calculated for alert configurations assigned to a device 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.

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.