Alerts FAQ

Published: 2025-01-22

Here are some answers to frequently asked questions about alerts.

Where can I find alerts generated by the ExtraHop system?

While the Alerts page provides quick access to all alerts, there are indicators and links to alerts throughout the ExtraHop system.

- On a dashboard, you can add an Alerts widget that displays up to 40 recent alerts.
- On the Overview page for a device, device group, or application, view an Alerts chart.
- On an activity map, the color of a device corresponds to the most severe alert status for all alerts assigned to the device.

Can I add custom text to email notifications?

There is no text field for custom messages in email notifications. However, information can be added to the **Description** field in the alert settings, 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.

In addition, the **Description** field supports Markdown, which is a simple formatting syntax that converts plain text into HTML. When placed before or around text, certain non-alphabetic characters specify which HTML styling to apply to the text. For example, place double asterisks (**) before and after the text that you want to display as bold. The following table shows common Markdown formats that are supported in the text box.

Format	Description	Example
Headings	Place a number sign (#) and a space before your text to format headings. The level of heading is determined by the amount of number signs.	`#### Example H4 heading`
Unordered lists	Place a single asterisk (*) before your text. If possible, put each list item on a separate line.	`* First example` `* Second example`
Ordered lists	Place a the number 1 and period (1.) before your text for each line item; Markdown will automatically increment the list number. If possible, put each list item on a separate line.	`1. First example` `1. Second example`
Bold	Place double asterisks before and after your text.	`**bold text**`
Italics	Place an underscore before and after your text.	`_italicized text_`

Format	Description	Example
Hyperlinks	Place link text in brackets before the URL in parentheses. Or type your URL. Links to external websites open in a new browser tab. Links within the ExtraHop system, such as dashboards, open in the current browser tab.	`[Visit our home page](https://www.extrahop.com)` `https://www.extrahop.com`
Blockquotes	Place a right angle bracket and a space before your text.	`On the ExtraHop website:` `> Access the live demo and review case studies.`
Monospace font	Place a backtick (`) before and after your text.	`` `example code block` ``
Emojis	Copy and paste an emoji image into the text box. See the Unicode Emoji Chart website for images. Markdown syntax does not support emoji shortcodes.	

How can I see which alerts are assigned to a source?

You can find alert assignments from the Overview page for a source.

- From a Device Overview page, click **Edit Assignments**.
- From a Device Group Overview page, click **Assignments** from the top-right corner.
- From an Application or Network Overview page, click **Alerts** from the top-right corner.

A window that contains the following alert assignment information is displayed:

- Alert configurations directly assigned to the source.
- Alert configurations assigned through a device group.
- Alert configurations globally assigned to the source.
- Alert configuration status.

From the window that contains the alert information, you can remove an alert assignment from the source by clicking the remove (X) icon next to the alert name. If the alert has been assigned globally to all applications or devices, you cannot remove the assignment from an individual source.

How are metrics calculated for alert configurations assigned to a device group?

If you assign an alert 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 of the members of a group, you can create an application that consolidates the devices into a single metric source, and then assign the alert to that application.

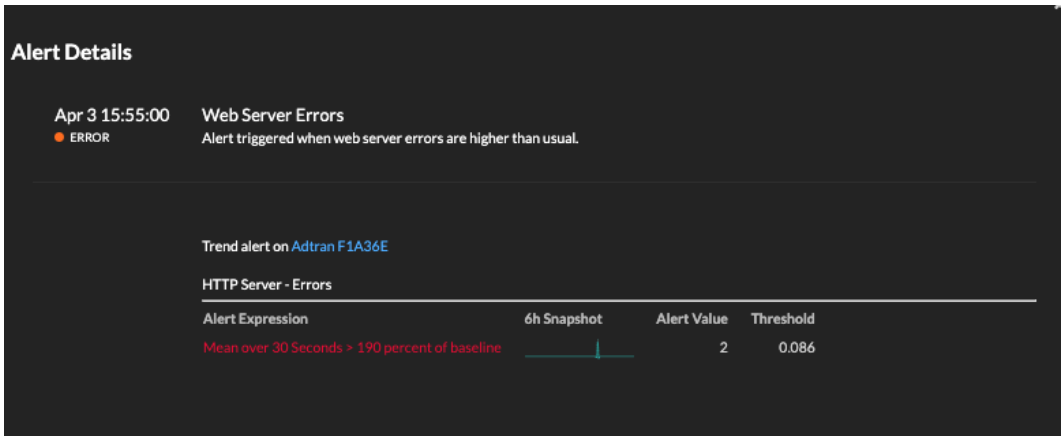
How are trends calculated?

The ExtraHop system calculates trends by looking at historical data and establishing a baseline. Trend alerts are well suited for metrics where meaningful thresholds are difficult to define, such as errors.

Trend alerts are generated when a metric is outside of the normal trend learned by the system. For example, you can configure a trend alert that generates alerts when a spike (75th percentile) in HTTP web

server processing time lasts longer than 10 minutes, and where the metric value of the processing time is 100% higher than the trend.

When viewing a trend alert, the Snapshot sparkline and the Alert Value represent the value of the monitored metric as computed according to the configured alert condition, which is displayed as the Threshold.



In most cases, historical data is available and trend alerts are active as soon as they are enabled. However, if you configure a trend alert that requires more historical data than your appliance currently has, the appliance calculates the trend with whatever data is available.

Why can't I see an alert in the Alerts table?

If you added an alert from a console, you must log in to that system to see and configure the alert.