


Add a notification to an alert

Published: 2017-08-09Z

You can add notifications to an alert configuration that will email specified addresses when an alert is generated. You can also send notifications to an SNMP listener.

Before you begin

Configure alert settings before you add notifications to an alert as described in [Configure threshold alert settings](#) and [Configure trend alert settings](#).

1. Log into the Web UI on the ExtraHop Discover or Command appliance.
2. Click the System Settings icon  and then click **Alerts**.
3. Open the alert you want, and then click the **Notifications** tab.
4. Configure the following notification options:

Severity

Specifies the severity level of the generated alert. The severity level is represented by color in emails and in the [Alert History](#).

Send SNMP Trap

Specifies whether notifications are sent to an SNMP listener. Users with administration privileges can [configure the SNMP listener](#) in the ExtraHop Admin UI.

Email notification groups

Specifies email groups that can receive alert notifications. The Default group is checked by default. Users with administration privileges can [configure additional email groups](#) in the ExtraHop Admin UI.

Additional email addresses

Specifies email addresses that are not included in a selected groups but should receive notifications.

Additional metrics in emails

Specifies additional metrics to include in the notification email. Enter the metric names, one per line, into the window or click the **Find metric...** button to search for a metric.

5. Click **OK**.

Email notifications will include the following information:

Alert Name

The name specified for the alert.

Alert Comment

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

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.

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.