Alerts

Published: 2021-09-01

Alerts make it easy to learn when important events occur, such as security detections on high-priority devices or Software License Agreement (SLA) violations. Configured alert conditions determine when an alert is generated.

Alert conditions are a combination of settings, such as a time interval, metric value, and metric calculations that occur on assigned data sources. Threshold or trend alerts are based on the value of the monitored metric. Detection alerts are based on specified protocols and detection categories.

Configuring alerts

Configure an alert to monitor for certain conditions and generate alerts when those conditions are met on the assigned data sources.

Threshold alerts

Threshold-based alerts are generated when a monitored metric crosses a defined value within a specified time interval.

Create a threshold alert to monitor occurrences such as error rates that surpass a comfortable percentage or SLA-violations. Learn how to configure a threshold alert.

Trend alerts

Trend-based alerts are generated when a monitored metric deviates from the normal trends observed by the system. Trend alerts are more complex than threshold alerts and are useful for monitoring metric trends such as unusually high round-trip times or storage servers experiencing abnormally low traffic, which might indicate a failed backup.

Create a trend alert to monitor when a metric deviates from normal behavior and where thresholds are difficult to define. Learn how to configure a trend alert.

Detection alerts

Detection alerts are generated when a detection on a specified protocol or detection category occurs. Detections are unexpected deviations from normal patterns in device or application behavior or notable activity in your environment. See Detections for more information.

Create a detection alert to monitor when detections occur in higher risk categories such as actions on objective or exfiltration. Learn how to configure a detection alert.

In addition, you can configure an alert with the following options:

- Set an exclusion interval to suppress alerts during certain time periods, such as a maintenance window.
- Configure notifications to receive an email when an alert is generated.

Viewing alerts

The Alerts page displays a list of all alerts generated during the specified time interval. Select from the filters at the top of the page to adjust the list or click an alert name to view details about the alert.

Select from the filters at the top of the page to adjust the list or click an alert name to view details about the alert.

Source Type

Filter alerts assigned to applications or devices.

Severity

Filter alerts by severity level.

Alert Type

Filter by threshold, trend, or detection alerts.

Site

Filter by connected sites. Command appliances and Reveal(x) only.

The Alerts page displays the following information about each alert:

Severity

A color-coded indicator of the alert severity level. You can set the following severity levels: Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug.

Alert name

The name of the configured alert. Click the alert name to view alert details.

Source

The name of the data source on which the alert conditions occurred. Click the source name to navigate to the source Overview page.

Time

The time of the most recent occurrence of the alert conditions.

Alert type

Indicates a trend, threshold, or detection alert.

For more information about viewing alerts, see the following topics

- Add an Alerts widget to a dashboard
- Alerts FAQ