


Find and filter anomalies

Published: 2018-04-18

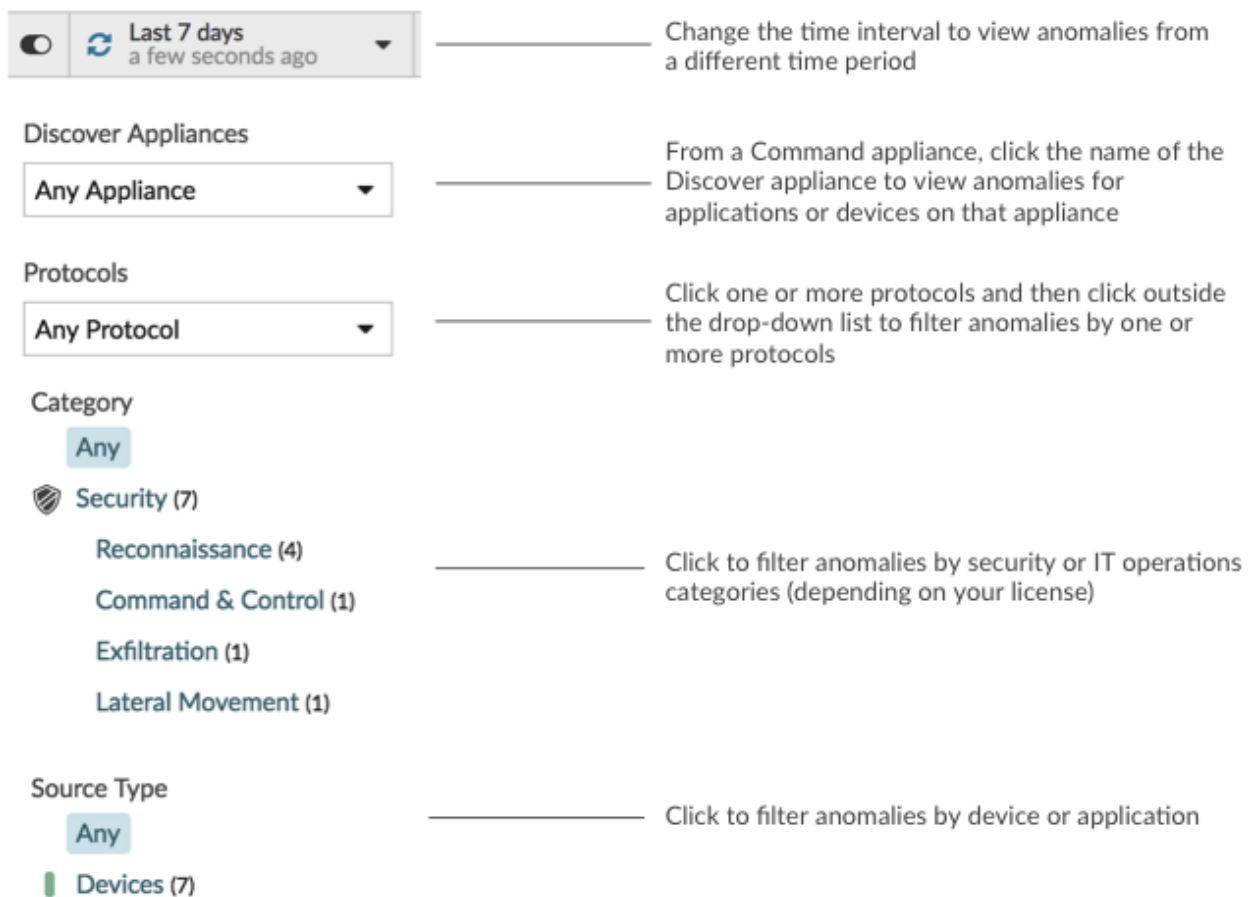
After activating Addy, a top menu item appears for anomalies. To browse anomalies detected by Addy, log into the Web UI and click **Anomalies** at the top of the page. You can then filter anomalies by time interval, protocol, category, applications, or devices. Anomalies are sorted by their start time and the most recent anomaly is listed first.

 **Note:** Configuring an anomaly alert from the Alerts page lets you monitor alerts or receive email notifications when a specific anomaly is detected. For more information, see the following topics:

- [Configure Addy anomaly alert settings](#)
- [Add a notification to an alert configuration](#) to receive emails when an anomaly is generated
- Monitor alerts from the [Alert History](#) page

The following steps show you how to find and filter anomalies:

1. Log into the Web UI on the Discover appliance, Command appliance, or ExtraHop Reveal(x) and then click **Anomalies** at the top of the page.
A list of anomalies for the current time interval appears. If the list is empty, then Addy has not detected anomalies for the selected time interval.
2. In the left pane, filter anomalies by selecting the options as shown in the following figure:



The screenshot shows the filter pane for anomalies with the following options and callouts:

- Time Interval:** A dropdown menu currently set to "Last 7 days a few seconds ago". Callout: "Change the time interval to view anomalies from a different time period".
- Discover Appliances:** A dropdown menu currently set to "Any Appliance". Callout: "From a Command appliance, click the name of the Discover appliance to view anomalies for applications or devices on that appliance".
- Protocols:** A dropdown menu currently set to "Any Protocol". Callout: "Click one or more protocols and then click outside the drop-down list to filter anomalies by one or more protocols".
- Category:** A list of categories with counts: "Any", "Security (7)", "Reconnaissance (4)", "Command & Control (1)", "Exfiltration (1)", and "Lateral Movement (1)". Callout: "Click to filter anomalies by security or IT operations categories (depending on your license)".
- Source Type:** A list of source types with counts: "Any" and "Devices (7)". Callout: "Click to filter anomalies by device or application".

Next steps

- [Investigate anomalies with Addy](#) 