

## Triaging Alerts

**Date of Publish:** 2019-04-09



# Contents

- Launch the Alerts User Interface..... 3**
- Getting Started with the Alerts User Interface..... 3**
- Viewing Alerts.....4**
  - Start and Pause Automatic Polling..... 4
  - Using the Alerts Table..... 5
    - Configure Table Columns..... 6
    - Configure Table Row Settings..... 7
    - Configure Alerts Window Refresh Rate..... 8
    - Display Additional Alerts Information..... 9
  - Search Alerts..... 11
  - Filter Alerts..... 11
  - Manage Alert Status..... 13
  - Escalate an Alert..... 17
  - Group Alerts..... 20
  - Create a Meta Alert..... 21
- Save Your Searches..... 23**
- View Your Recent and Saved Searches..... 23**

## Launch the Alerts User Interface

When an event violates your threat intelligence thresholds, you are sent an alert that you can view in the Hortonworks Cybersecurity Platform (HCP) Alerts user interface, enabling you to evaluate the severity of the violation and manage it accordingly. The Alerts user interface is bundled with HCP and installed with the Ambari management pack.

### Before you begin

- Elasticsearch or Solr must be up and running and should have alerts populated by HDP topologies.
- The Alerts UI defaults to port 4201. If you are already using port 4201 for another purpose, you must change the default port for the Alerts UI to another port number.

### Procedure

1. Display the **Ambari** user interface.
2. In the Services pane, select **Metron**.
3. From the **Quick Links** menu, choose **Alerts UI**.

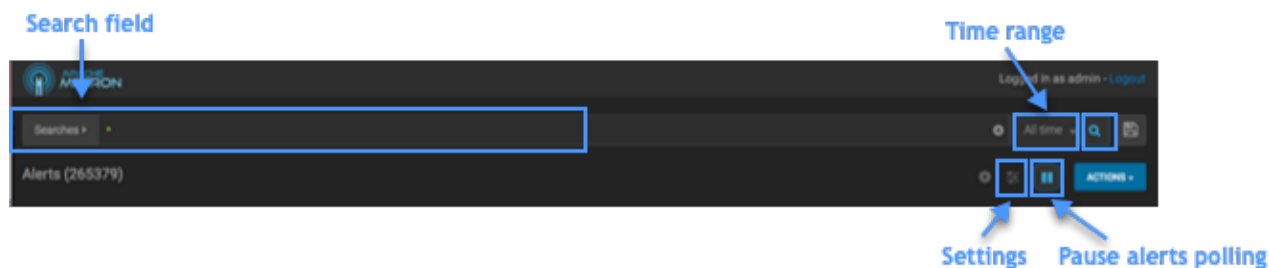


**Note:** There is no login module for the Alerts UI.

## Getting Started with the Alerts User Interface

The Alerts user interface provides mechanisms for viewing alerts, searching and filtering alerts, grouping alerts to facilitate management, and changing alert status. The Alerts user interface defaults to displaying the Alerts table when first opened.

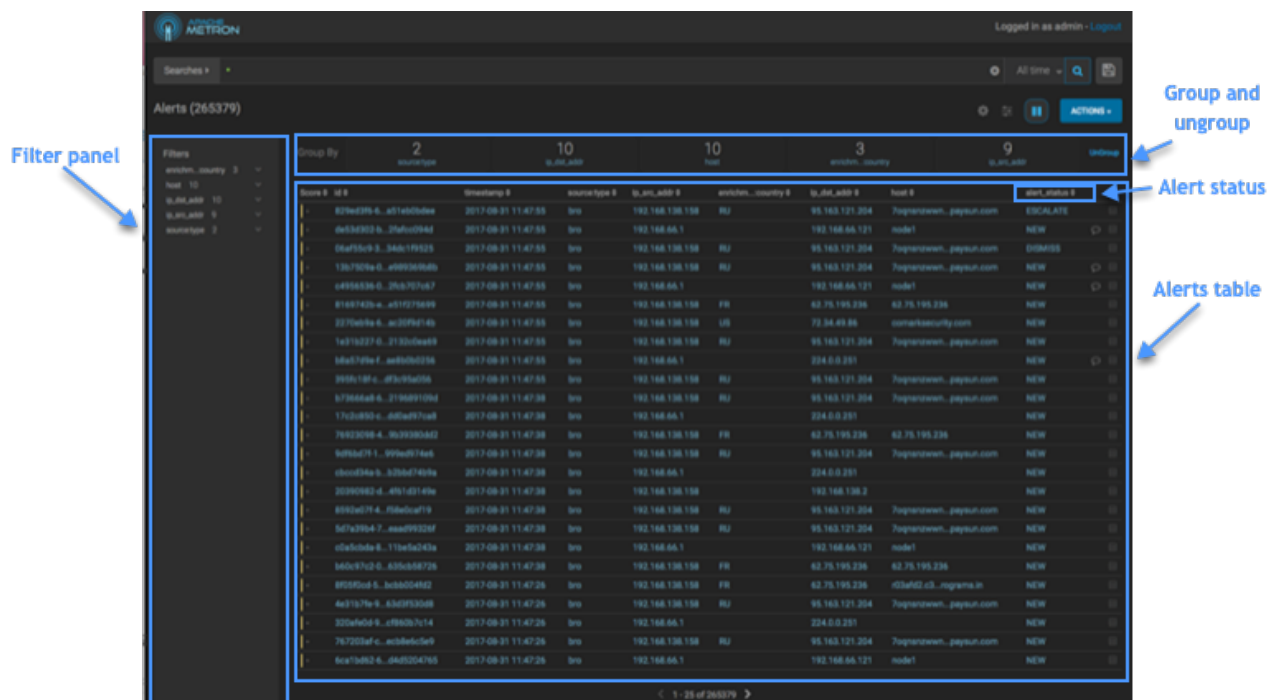
You can use the Alerts user interface tool bar to perform searches and manage the Alerts UI settings.



**Table 1: Alerts UI Tool Bar**

Tools	Description
Search field	You can search for alerts using the search bar above the Alerts table. The search tool follows the Lucene syntax which supports a rich query language.
Settings	You can configure the table row settings in the Alerts table to modify the appearance of the Alerts table and the refresh rate.
Pause alerts	You can pause the Alerts UI polling while you adjust settings or focus on current alerts.
Time range	You can set the time range over which to perform alert polling or choose one of the predefined quick ranges.

You can use the Alerts table to view and manage alerts:



**Table 2: Alerts Table**

Tools	Description
Alerts table	The Alerts table displays the alerts generated by the HCP framework. The Alerts UI polls for alerts and refreshes the Alerts table at an interval that you can configure.
Filters	The Alerts UI currently provides five filters that you can apply to alerts. You can use these filters to refine the list of alerts and collect additional information on the alerts.
Alert status	You can change the status of or dismiss an alert.
Group By	You can group alerts so you can apply filters, status, etc. on multiple alerts at a time.
Meta Alerts	The meta alert feature enables you to create a system entity that contains a collection of filtered alerts.

## Viewing Alerts

The Alerts user interface defaults to displaying the Alerts table when first opened. You can modify the alerts displayed in the Alerts table to help identify issues.

### Start and Pause Automatic Polling

The automatic polling in the Alerts UI defaults to a paused state when you first log in. To start automatic polling, you must click the play button.

### Procedure

1. To start automatic polling, click the



(play) button.

Polling is also paused whenever you open any configuration panels or use the **Searches** field.

2. To manually pause automatic polling, click the



(pause) button.

## Using the Alerts Table

The Alerts table displays the alerts generated by the HCP framework. The Alerts UI polls for alerts and refreshes the Alerts table at an interval that you can configure.

By default, the alerts table shows the recent alerts at the top. For example, alerts are sorted descending on timestamp.

The Alerts table also provides the threat intelligence score for each alert. Next to the score is a bar that indicates the severity of the score:

**Red**

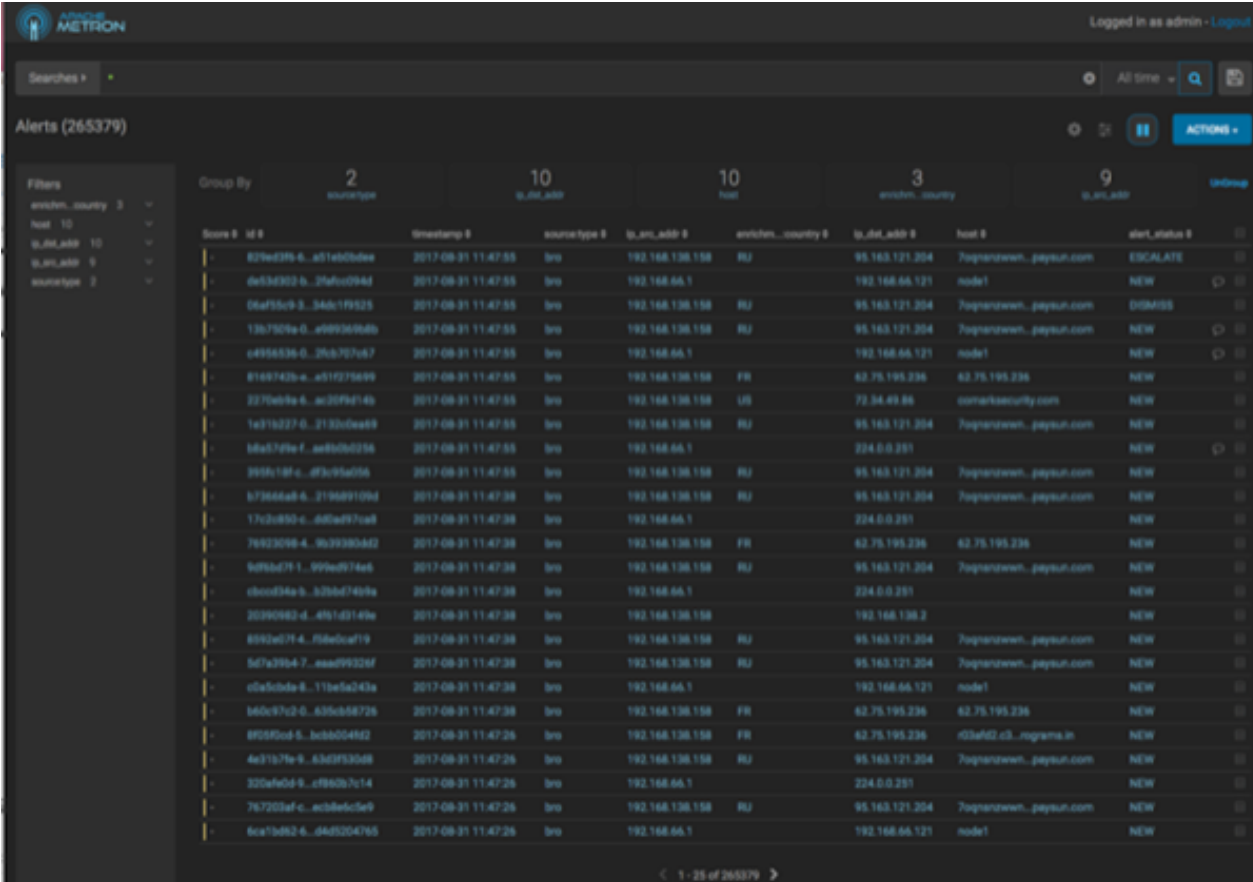
A score of 69 or higher

**Orange**

A score between 39 and 69

**Yellow**

A score below 39



Alerts (265379)

Filters:   
 enrich\_country: 3   
 host: 10   
 ip\_int\_addr: 10   
 ip\_ext\_addr: 0   
 sourcetype: 2

Group By:   
 2 sourcetype   
 10 ip\_int\_addr   
 10 host   
 3 enrich\_country   
 9 ip\_ext\_addr   
 UnGroup

Score	ID	timestamp	sourcetype	ip_int_addr	enrich_country	ip_ext_addr	host	alert_status
82	62f6d3f9-6...a51e60bde	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	ESCALATE
81	de53d922-b...2f6fcd94d	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1	NEW
80	06af35b9-3...34dc1f9d25	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	DISMISS
79	13b750fa-0...e9993d96d9	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
78	e4956536-0...35cb707a67	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1	NEW
77	8169742b-e...a51d275699	2017-08-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
76	2270e9a6-6...ac30f9d14b	2017-08-31 11:47:55	bro	192.168.138.158	US	72.34.49.86	comcastsecurity.com	NEW
75	1a31b227-0...2130cd6a69	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
74	b6a579fa-f...ae8dc6d256	2017-08-31 11:47:55	bro	192.168.66.1		224.0.0.251		NEW
73	395bc18f-c...d93c95a056	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
72	b73666a6-6...2196d9109d	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
71	17c2b830-e...d80ad97ca8	2017-08-31 11:47:55	bro	192.168.66.1		224.0.0.251		NEW
70	76923098-4...9c39380dd2	2017-08-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
69	9d95a67f-1...995ed974e6	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
68	cb0ed34a-b...32b6d749fa	2017-08-31 11:47:55	bro	192.168.66.1		224.0.0.251		NEW
67	20290962-d...4961d3149e	2017-08-31 11:47:55	bro	192.168.138.158		192.168.138.2		NEW
66	8992a07f-4...f08edcaef9	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
65	5d7a39b4-7...eead99326f	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
64	c0a5c0da-8...11b6a243a	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1	NEW
63	b6dc97c2-0...635cd68726	2017-08-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
62	89050ed-5...bcb600482	2017-08-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236	NEW
61	4e31b7fe-9...63d9f33d68	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
60	32c6a6d-9...c096097c14	2017-08-31 11:47:55	bro	192.168.66.1		224.0.0.251		NEW
59	767203af-c...ac0b6efc9f	2017-08-31 11:47:55	bro	192.168.138.158	RJ	95.165.121.204	7ogpnczwen...paypal.com	NEW
58	6ca1b862-6...d4d3204765	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1	NEW

1 - 25 of 265379

## Configure Table Columns

You can configure the table columns in the Alerts table to customize the type of information you display. You can modify the information that shows in each column, the title of the column, and the order in which the columns are displayed.

### Procedure

1. Click




























(gear icon).

The Alerts UI displays the Configure Table that lists all the columns available across all the valid search indexes.

Configure Table Columns

Filter list of available fields

VISIBLE			AVAILABLE	
	Short Name	Type		Type
	Score	STRING		AA BOOLEAN
	guid	STRING		acks INTEGER
	timestamp	DATE		actions KEYWORD
	source.type	STRING		active_dns_requests INTEGER
	ip_src_addr	IP		active_files INTEGER
	enrichments:geo:ip_dst_addr:country	STRING		active_icmp_conns INTEGER
	ip_dst_addr	IP		active_tcp_conns INTEGER
	host	STRING		active_timers INTEGER
	alert_status	STRING		active_udp_conns INTEGER
				adapter:geoadapter.begin.ts DATE
				adapter:geoadapter.end.ts DATE
				adapter:hostfromjsonlistadapter.begin.ts DATE
				adapter:hostfromjsonlistadapter.end.ts DATE
				adapter:threatinteladapter.begin.ts DATE
				adapter:threatinteladapter.end.ts DATE
				addl KEYWORD

- In the AVAILABLE column, use the add button next to a field to create an Alerts table column for that field.
- In the VISIBLE column, use the remove button next to a field to remove the corresponding column from the Alerts table.
- You can rename the column titles by entering a new name in the **Short Name** column.  
For example, 'enrichments:geo:ip\_dst\_addr:country' can be renamed to 'Dst Country'.  
This name is just for display convenience and the changes are not propagated to any system in HCP.
- You can also configure the order in which the selected columns will appear in the table by using the arrow icons.
- Click **Save** to save your changes and dismiss the **Configure Table** panel.

## Configure Table Row Settings

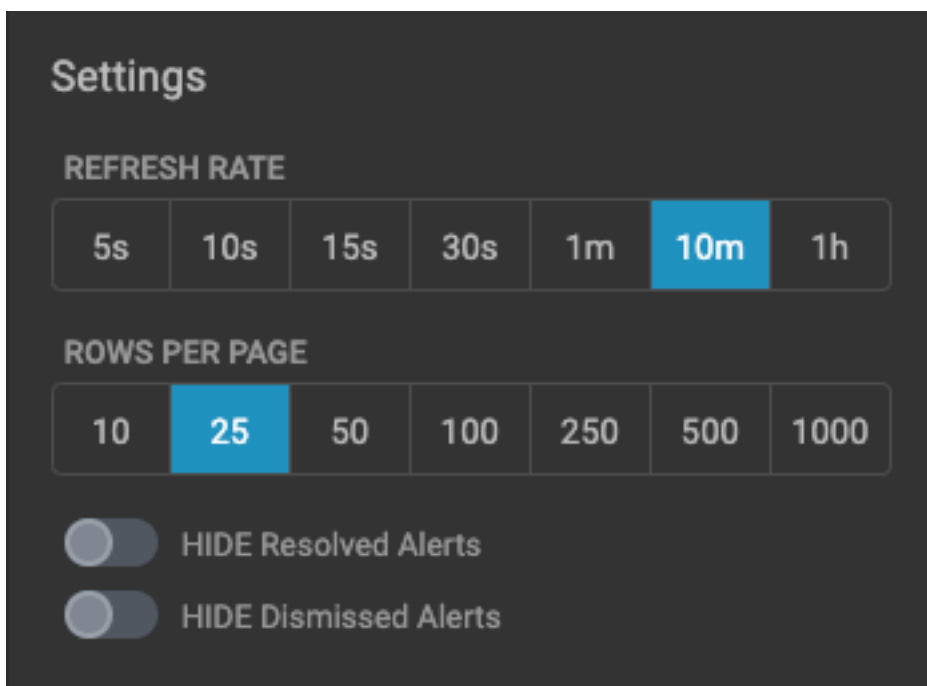
You can modify the table row settings in the Alerts table to to modify the appearance of the Alerts table.

### Procedure

- Click the



(slides icon) at the top of the table to display the Settings dialog box.



2. To modify the number of rows displayed in the Alerts table, choose a value under **Rows Per Page**.



**Note:** The number of rows that are visible in the Alerts table is restricted by the size of your browser window.

3. To hide resolved alerts or dismissed alerts, click the slide button next to the appropriate action.

### Configure Alerts Window Refresh Rate

The default refresh rate for the Alerts table defaults to 10 minutes. You can modify the default rate to suit your needs.

#### Procedure

1. To modify the rate at which the Alerts table is refreshed with new alert information, , click the



(slides icon) at the top of the table to display the Settings dialog box.



**Settings**

**REFRESH RATE**

5s 10s 15s 30s 1m **10m** 1h

**ROWS PER PAGE**

10 **25** 50 100 250 500 1000

☐ HIDE Resolved Alerts

☐ HIDE Dismissed Alerts

2. Choose a value under **Refresh Rate**.

### Display Additional Alerts Information

In addition to displaying alert information in the Alerts table, you can display all the information about the alert in Elasticsearch in a separate panel.

#### Procedure

1. Select an alert by clicking on empty space in the alert row.  
The Alerts UI displays a panel listing all available data in Elasticsearch about the alert.

AVuKz1\_n1LEanKS6qbtb

Status

NEW

ESCALATE

OPEN

DISMISS

RESOLVE

alert_status	OPEN
dgmLen	40
enrichments:geo:ip_sr c_addr:city	Phoenix
enrichments:geo:ip_sr c_addr:country	US
enrichments:geo:ip_sr c_addr:dmaCode	753
enrichments:geo:ip_sr c_addr:latitude	33.4499
enrichments:geo:ip_sr c_addr:locID	5308655
enrichments:geo:ip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_sr c_addr:longitude	-112.0712
enrichments:geo:ip_sr c_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f- b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

2. The Status states at the top of the panel display the current status of the alert.

## Search Alerts

You can search for alerts using the search bar above the Alerts table. The search tool follows the Lucene syntax which supports a rich query language.

### Procedure

1. To search on an item that is displayed in the Alerts table, simply click on the item and it will display in the **Searches** field.

Searches Field



2. You can also directly type in the **Searches** field to enter search criteria.  
For example, you can enter source:type:snort.
3. To remove an item in the **Searches** field, mouse over the information in the **Searches** field until an **x** appears at the end of the text. Click on the **x** to remove the search filter and the operator following or preceding it.
4. To clear the entire **Searches** field, click the **x** at the end of the field.
5. You can specify the time range of your search by using the time range selector on the far right of the **Searches** field.



#### Note:

The time-range selector is not available if you put a timestamp in the **Searches** field.

The time-range button defaults to **All time** which displays all alerts corresponding to the Searches parameters. To customize the time range, click the time-range drop-down menu and select one of the following:

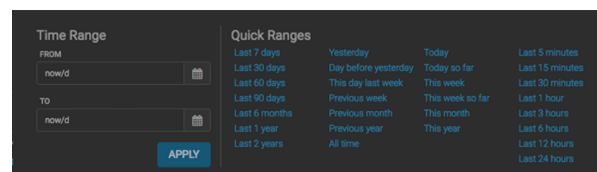
#### Time Range

Enables you to choose the start and end dates and times for your search.

#### Quick Ranges

Provides a list of pre-specified time ranges that you can choose.

#### Time Selector Dialog Box



After you make your choice, the time-selector label will reflect your selection.



## Filter Alerts

The Alerts UI currently provides five filters that you can apply to alerts. You can use these filters to refine the list of alerts and collect additional information on the alerts. These filters are listed in the **Filters** panel on the left of the **Alerts** window.

## Procedure

1. Click one of the filters in the **Filters** panel on the left of the window.

The Filter expands to list all of the facet values contained in the filter. For example, in the following figure, the **enrichments:geo\_dst\_addr:country** filter contain the countries Russia, France, and USA.

The screenshot shows the Apache Metron Alerts interface. On the left, the **Filters** panel is expanded for the **enrichments:geo\_dst\_addr:country** filter, showing three facet values: **RU** (3769), **FR** (27187), and **US** (17649). The main **Alerts (147925)** table is grouped by **source.type** (2 groups), **ip\_dst\_addr** (10 groups), **host** (10 groups), and **enrichments:geo\_dst\_addr:country** (3 groups). The table columns are: **Score**, **id**, **timestamp**, **source.type**, **ip\_src\_addr**, **enrichments:geo\_dst\_addr:country**, and **ip\_dst\_addr**. The right sidebar shows the **Status** section with buttons for **NEW**, **OPEN**, **DISMISS**, and **RESOLVE**, and a **Comments** section with an **ADD COMMENT** button.

Score	id	timestamp	source.type	ip_src_addr	enrichments:geo_dst_addr:country	ip_dst_addr
-	06e95c9-3...34dc1f925	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.20
-	829ed3f6-6...a51eb0bde	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.20
-	de33d302-b...2fa0c094d	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.12
10	6644a88-8...c958cd1be5	2017-08-30 08:07:59	snort	192.168.66.1		192.168.66.12
-	10a83fa3-8...41395e6201	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
-	483004c0-4...afcc68715	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
-	f63236fe-3...2208f9994	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.12
-	9ef44ca9-c...a9914d7655	2017-08-30 12:43:58	bro	192.168.138.158	US	204.152.254.2
-	08f9d0b6-7...fb113e0ce	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
-	578f8db-e...7420f2ba2	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.12
-	3964e90f-b...a09439c39	2017-08-30 12:43:58	bro	192.168.138.158	RU	95.163.121.20
-	90403c32-0...2ecf46b68	2017-08-30 12:43:58	bro	192.168.66.1		224.0.0.251
-	88950cae-5...359faa0a78	2017-08-30 12:43:58	bro	192.168.138.158	RU	95.163.121.20
-	605fe112-c...c2619a8a36	2017-08-30 12:43:58	bro	192.168.138.158		192.168.138.2
-	327e865e-1...3c21a1a799	2017-08-30 12:44:06	bro	192.168.138.158	RU	95.163.121.20
-	9ebf8379-5...5ec9069f53	2017-08-30 12:44:06	bro	192.168.138.158	FR	62.75.195.238
-	ca0d424a-6...40146306a	2017-08-30 12:44:06	bro	192.168.138.158	FR	62.75.195.238
-	779b607e-2...f1365e19a0	2017-08-30 12:44:06	bro	192.168.138.158	US	72.34.49.86
-	3b22460c-a...3ba14515db	2017-08-30 12:44:06	bro	192.168.138.158		192.168.138.2
-	e56c2754-b...737a2ecbde	2017-08-30 12:44:06	bro	192.168.66.1		224.0.0.251



### Note:

The UI displays the number of alerts corresponding to each facet next to the facet.

2. You can continue to apply filters to the alerts displayed in the **Alerts** window to further refine the alerts list.

As you select filters and facets, they are displayed in the **Searches** field.

For example, in the following figure, we've applied the **source.type** filter with the **bro** facet and then the **ip\_dst\_addr** filter with the IP address 95.163.121.204.

Searches: source: type: bpo AND ip\_dst\_addr: 95.168.121.204

Alerts (68863)

Filters: evictem\_country: 1, host: 1, ip\_dst\_addr: 95.168.121.204, source\_type: 1, bpo: 68863

Score	ID	Timestamp	source_type	ip_dst_addr	evictem_country	ip_dst_addr	host	evictem_country	ip_dst_addr	host	alert_status
829ed3f6-6...	a51e03bdee	2017-08-31 11:47:55	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	ESCALATE
06af55c9-9...	346c1f9325	2017-08-31 11:47:55	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	DISMISS
13b7909e-0...	a993695db	2017-08-31 11:47:55	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
1e31a227-0...	2132c0e69	2017-08-31 11:47:55	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
395fc18f-c...	d73c95a056	2017-08-31 11:47:55	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
679466a8-6...	21948910bd	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
9d9bd7f-1...	999e9374e6	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
8592a07f-4...	f58d0caf19	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
5d7a3964-7...	aaad7932bf	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
4e31b79e-9...	63d9f530a8	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
767202af-c...	ac58efc5b9	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
76b86dfc-9...	3a54355cb1	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
e4287492-8...	074f1a64e1	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
78ba7d54-8...	1805d0fadd	2017-08-31 11:47:58	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
34f5b93f-8...	29a0f53e19	2017-08-31 11:48:02	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
382de09f-4...	90c0d33b05	2017-08-31 11:48:02	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
ac2b5440-9...	12d054eadd	2017-08-31 11:48:02	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
149f9a2f-0...	41a412850f	2017-08-31 11:48:12	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
87a17519-8...	7474c32e59	2017-08-31 11:48:12	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
0ee030ed-e...	52b99a497e	2017-08-31 11:48:08	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
72a503ee-b...	f79670b128	2017-08-31 11:48:08	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
ade15aea-1...	f9c2234571	2017-08-31 11:48:03	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
a72d2458-e...	294771c6a3	2017-08-31 11:48:03	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
3a5b9374-e...	3aeb38badd	2017-08-31 11:48:03	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW
e3dee43b-e...	4ffef9e98c	2017-08-31 11:48:03	bpo	192.168.138.158	RU	95.168.121.204	7ogranznewm_payout.com	RU	95.168.121.204	7ogranznewm_payout.com	NEW

- To clear filters that have been populated to the **Searches** field, click



(delete icon) at the end of the **Searches** field.

## Manage Alert Status

You can manage one or more alerts at a time using the **ACTIONS** menu. You can use the **ACTIONS** to change the status of or dismiss an alert.

### Procedure

- Select an alert by clicking on empty space in the alert row.

The Alerts UI displays a panel listing the status of the alert all available data in Elasticsearch about the alert.

AVuKz1\_n1LEanKS6qbtb

Status

NEW

OPEN

DISMISS

RESOLVE

ESCALATE

alert_status	OPEN
dgmlen	40
enrichments:geo:ip_sr c_addr:city	Phoenix
enrichments:geo:ip_sr c_addr:country	US
enrichments:geo:ip_sr c_addr:dmaCode	753
enrichments:geo:ip_sr c_addr:latitude	33.4499
enrichments:geo:ip_sr c_addr:locID	5308655
enrichments:geo:ip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_sr c_addr:longitude	-112.0712
enrichments:geo:ip_sr c_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f- b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

The current alert status is highlighted.




**Note:**

To manage more than one alert at a time, click the check boxes at the end of alert rows, then select the action you want to perform from the ACTIONS menu.

2. Click the new status you want to apply to the alert, then dismiss the panel.
3. You can also add a comment to this action by clicking



(Comment button), entering your comment in the **Comments** field, and clicking **ADD COMMENT**.

829ed3f6-6034-4969-91c7-87... 

Status

NEW

OPEN

DISMISS

RESOLVE

ESCALATE

Comments

ADD COMMENT



The Alerts UI indicates that an alert has one or more comments by displaying



(comment icon) next to the alert status in the **Alerts** window.



**Note:**

You cannot add a comment to an alert contained in a meta alert. You can only add comments to the meta alert.

4. To delete a comment, click the comment to delete, then click the trash can icon.  
Click OK in the **Confirmation** dialog box.

## Escalate an Alert

You can escalate one or more alerts at a time to create an event that can be tracked by an external ticketing system.

### Procedure

1. Select an alert by clicking on empty space in the alert row.

The Alerts UI displays a panel listing the status of the alert all available data in Elasticsearch about the alert.

AVuKz1\_n1LEanKS6qbtb

Status

NEW

OPEN

DISMISS

RESOLVE

ESCALATE

alert_status	OPEN
dgmlen	40
enrichments:geo:ip_sr c_addr:city	Phoenix
enrichments:geo:ip_sr c_addr:country	US
enrichments:geo:ip_sr c_addr:dmaCode	753
enrichments:geo:ip_sr c_addr:latitude	33.4499
enrichments:geo:ip_sr c_addr:locID	5308655
enrichments:geo:ip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_sr c_addr:longitude	-112.0712
enrichments:geo:ip_sr c_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f- b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

The current alert status is highlighted.



**Note:**  
To manage more than one alert at a time, click the check boxes at the end of alert rows, then select the action you want to perform from the ACTIONS menu.

2. Click **Escalate**.

The screenshot shows a dark-themed user interface for managing alerts. At the top, there is a header bar with a yellow vertical bar on the left, a truncated alert ID '829ed3f6-6034-4969-91c7-87...' in the center, and a close button (X) on the right. Below the header, the main content area is divided into two sections. The first section, titled 'Status', contains a grid of buttons. The 'ESCALATE' button is highlighted in blue and is positioned above the 'OPEN' button. Other buttons in the grid include 'NEW', 'DISMISS', and 'RESOLVE'. The second section, titled 'Comments', features a large, empty text input area with a small cursor icon at the bottom right. Below the input area is a blue button labeled 'ADD COMMENT'.

Status		
NEW	ESCALATE	DISMISS
	OPEN	
	RESOLVE	

Comments

ADD COMMENT

HCP writes the event to a Kafka escalation topic. An external orchestration software can pick up the event from the topic and use the API to create an incident or append to an existing incident.

- You can also add a comment to this action by clicking



(Comment button), entering your comment in the **Comments** field, and clicking **ADD COMMENT**.

## Group Alerts

You can group alerts so you can apply filters, status, etc. to multiple alerts at a time.

### Procedure

- Click one of the groups listed by **Group By**.

The **Alerts** table view changes to a tree view listing the values of the groups.

In the following example, the group is source.type and the values are Snort and Bro.



**Note:** The icon to the left of the value provides the cumulative severity score for all the alerts in the value. If the score exceeds 999, then the value displays as 999+.

- Click one of the values to list the alerts for that value.

- You can click an alert to add it to the Searches field.



**Note:** Searches will search through all the groups, not just the group containing the alert.

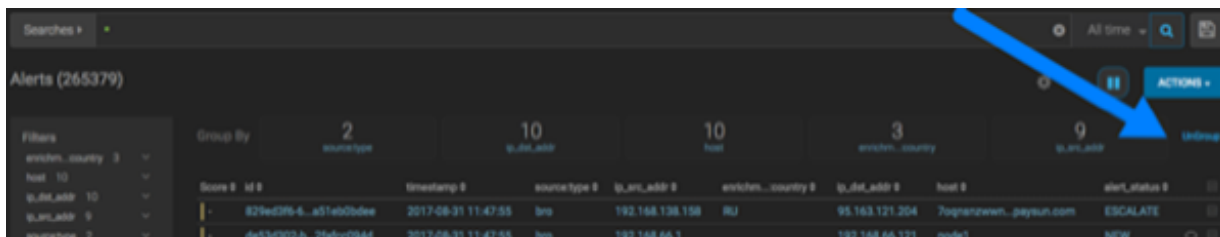
- All features that are available for the Alerts table are available for the tree view.

For example, if you apply an action, such as Escalate, to an alert, it will apply to all alerts within the group. Similarly, if you search for a parameter, it will search all alerts within the group.

- You can continue to refine your alerts by applying additional groups.

You can change the order in which the groups are applied to the alerts by clicking and dragging the groups on the **Groups By** line.

- To ungroup your alerts and return to the Alerts window, click Ungroup which is located on the far right of the list of groups.



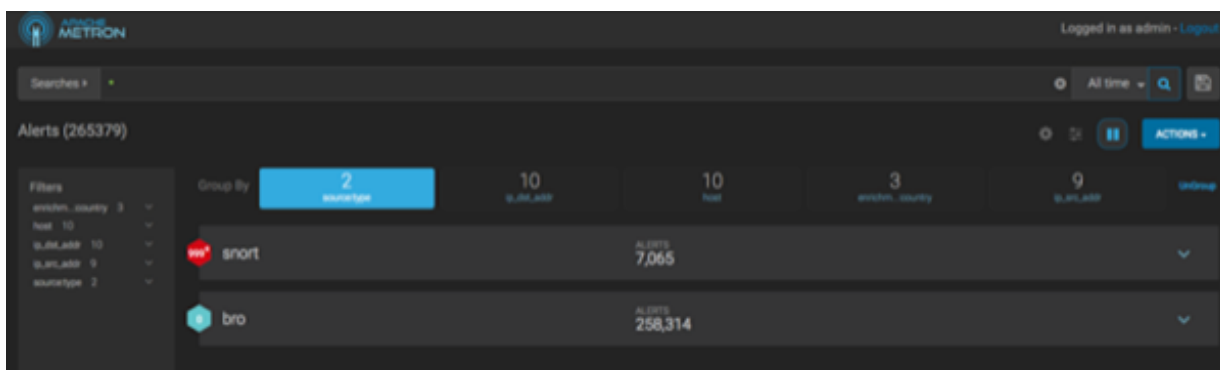
## Create a Meta Alert

The meta alert feature enables you to create a save a group of filtered alerts. Like the group feature, you can group filtered alerts that pertain to an incident. However, with meta alert, you can save your grouping, creating a system entity, to view it later. Also, when you filter alerts, if a relevant alert is contained in a meta alert, the entire meta alert will be included in the filter results.

### Procedure

- Click one of the groups listed by **Group By**.

The **Alerts** table view changes to a tree view listing the values of the groups.



- Use the **Search** and **GroupBy** options to create one or more groups containing alerts on which you want to focus.
- When you have selected a group of alerts that you want to focus on, click



(meta alert icon), then confirm that you wish to create a meta alert with the selected alerts.

The meta alert disappears from the tree view. You can still see the meta alert in the alerts table view.

- You can rename your meta alert by completing the following steps:
  - Display the Alerts UI display panel by clicking on empty space in the meta alert row.

Alerts Information Panel

AVuKz1\_n1LEanKS6qbtb

Status

NEW

ESCALATE

OPEN

DISMISS

RESOLVE

alert_status	OPEN
dgmlen	40
enrichments:geoip_sr c_addr:city	Phoenix
enrichments:geoip_sr c_addr:country	US
enrichments:geoip_sr c_addr:dmaCode	753
enrichments:geoip_sr c_addr:latitude	33.4499
enrichments:geoip_sr c_addr:locID	5308655
enrichments:geoip_sr c_addr:location_point	33.4499,-112.0712
enrichments:geoip_sr c_addr:longitude	-112.0712
enrichments:geoip_sr c_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	Seba8dec-278f-4f9f- b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

- b) Click the current meta alert name at the top of the panel and enter your new meta alert name.
- c) Dismiss the panel by clicking the X in the upper right corner of the panel.

## Save Your Searches

You can save your Alert searches for future reuse.

### Procedure

1. To save a search, click the



(save button) next to the **Searches** field.

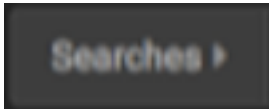
2. When prompted, enter a name for the saved search parameters, then click **Save**.  
This will save both the search parameters and the column configurations.

## View Your Recent and Saved Searches

You can view both your recent searches and saved searches in the Alerts UI.

### Procedure

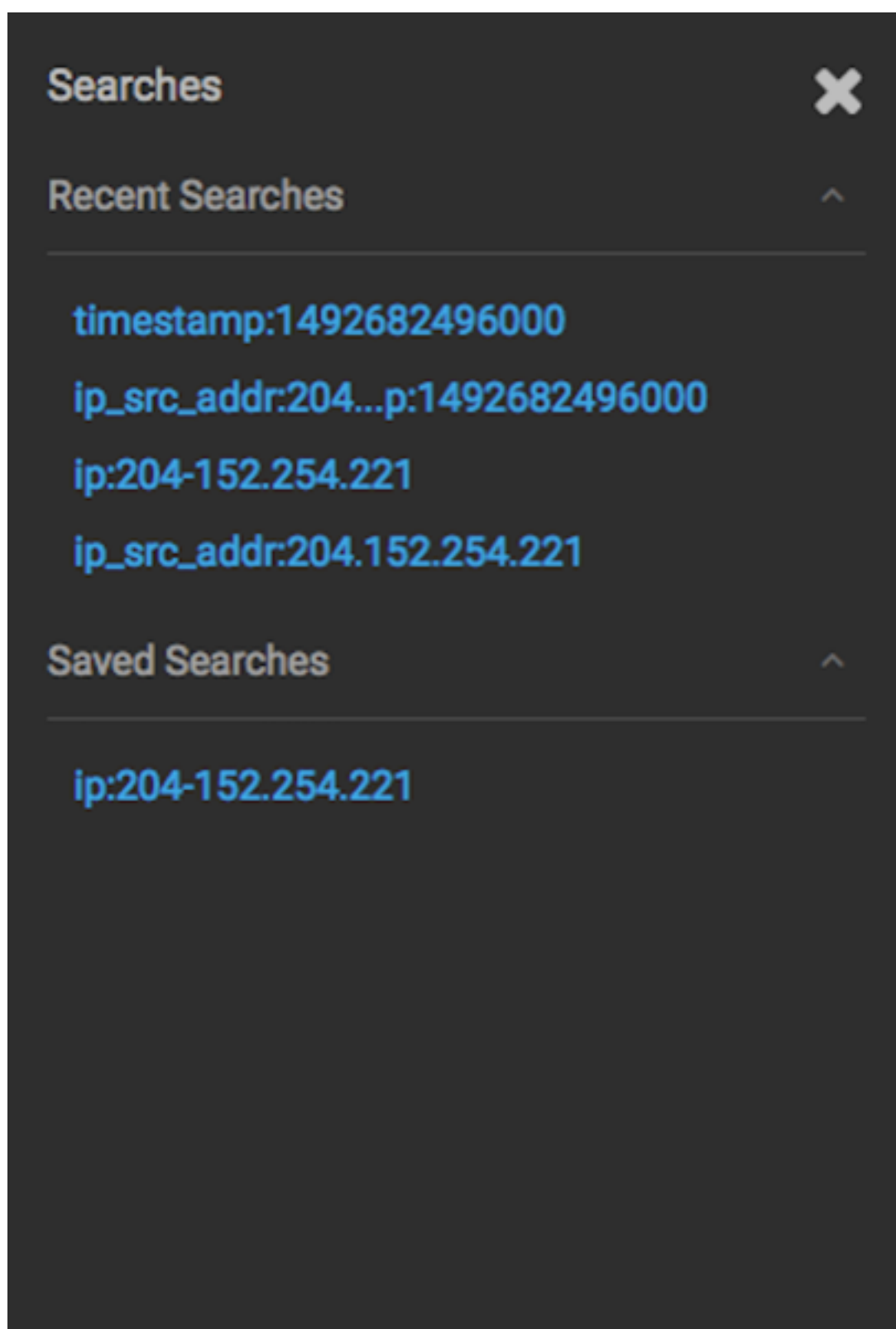
Click the



button to the left of the **Searches** field.

The Alerts UI displays the Searches panel.

Searches Panel



The **Searches** panel lists two types of searches:

**Recent Searches**

This is a list of your most recent searches.

To display the saved search, simply click on the search name.



**Saved Searches**

The Alerts UI saves a maximum of ten of your most recent searches.

This is a list of your saved searches.

To display the saved search, simply click on the search name.

You can delete any of these saved searches by clicking the trash can icon that becomes visible when you mouse over each saved search.