

CCP Triaging Alerts 2.0.1

## Triaging Alerts

Date of publish: 2017-11-06

# CLOUDERA

<https://docs.cloudera.com/>

# Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Launch the Alerts User Interface.....4

Getting Started with the Alerts User Interface..... 4

Viewing Alerts..... 6

    Start and Pause Automatic Polling..... 6

    Using the Alerts Table..... 6

        Configure Table Columns.....7

        Set Timestamp to Local Time.....9

        Modify the Alert Data Refresh Rate.....9

        Modify Number of Alert Table Rows..... 10

        Hide Resolved or Dismissed Alerts..... 11

        Display Additional Alerts Information..... 12

    Search Alerts..... 14

    Filter Alerts..... 15

    Manage Alert Status..... 17

    Escalate an Alert..... 21

    Group Alerts..... 24

    Create a Meta Alert.....26

Integrating Third-Party Portals.....28

Save Your Searches..... 29

View Your Recent and Saved Searches.....30

## Launch the Alerts User Interface

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

### Before you begin

- Elasticsearch 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**.

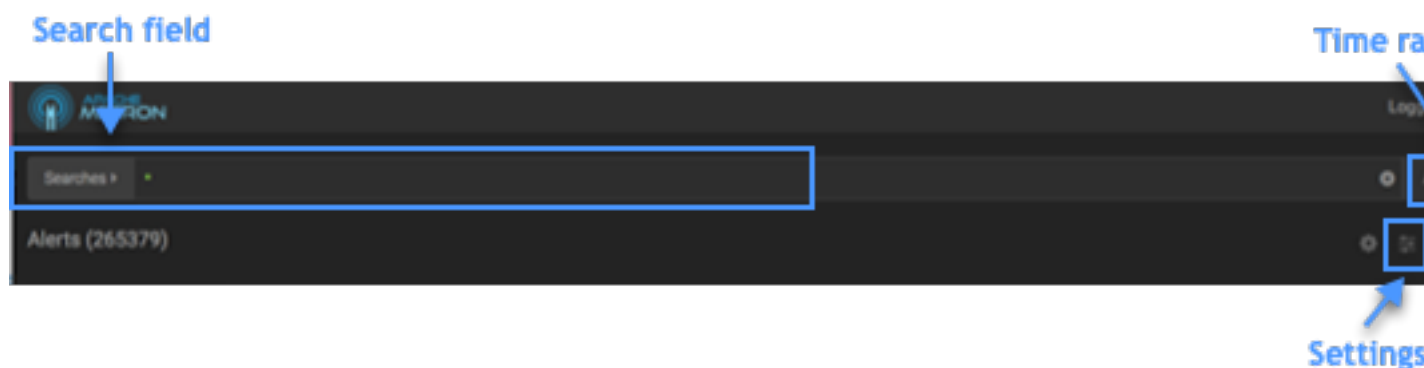


**Note:** There is no login module for the Alerts UI.

## 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.

Tools	Description
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:

**Filter panel**

Alerts (265379)

Group By: 2 source\_type, 10 ip\_dst\_addr, 10 host, 3 enriched\_country

Score	id	timestamp	source_type	ip_dst_addr	enriched_country	ip_src_addr
829ed395-6...	a51eb0bde6	2017-08-31 11:47:55	lsm	192.168.138.158	RU	95.163.121.204
de53d302-b...	25afcc094d	2017-08-31 11:47:55	lsm	192.168.66.1		192.168.66.121
08af55c9-3...	34dc1f9525	2017-08-31 11:47:55	lsm	192.168.138.158	RU	95.163.121.204
13b750ba-0...	a9893694b5	2017-08-31 11:47:55	lsm	192.168.138.158	RU	95.163.121.204
c495a536-0...	2fcb707c67	2017-08-31 11:47:55	lsm	192.168.66.1		192.168.66.121
8168742b-e...	a51f275e99	2017-08-31 11:47:55	lsm	192.168.138.158	FR	62.75.195.236
2270eb9a-6...	ac30f9d14b	2017-08-31 11:47:55	lsm	192.168.138.158	US	72.34.49.86
1a316227-0...	2130c0ea69	2017-08-31 11:47:55	lsm	192.168.138.158	RU	95.163.121.204
b8a5749e-f...	ae8b0b0256	2017-08-31 11:47:55	lsm	192.168.66.1		224.0.0.251
996b18f-c...	d93c95a056	2017-08-31 11:47:55	lsm	192.168.138.158	RU	95.163.121.204
b73646a8-6...	219a89109d	2017-08-31 11:47:58	lsm	192.168.138.158	RU	95.163.121.204
17c3b850-c...	d80e977c6d	2017-08-31 11:47:58	lsm	192.168.66.1		224.0.0.251
76923098-4...	9c39380ad2	2017-08-31 11:47:58	lsm	192.168.138.158	FR	62.75.195.236
9d95bd71-1...	999ed974e6	2017-08-31 11:47:58	lsm	192.168.138.158	RU	95.163.121.204
c8cc34a-b...	329bd7409a	2017-08-31 11:47:58	lsm	192.168.66.1		224.0.0.251
20290982-d...	49b1d3149e	2017-08-31 11:47:58	lsm	192.168.138.158		192.168.138.2
6992e071-4...	f58ebcaf19	2017-08-31 11:47:58	lsm	192.168.138.158	RU	95.163.121.204
5d7a39b4-7...	eead99326f	2017-08-31 11:47:58	lsm	192.168.138.158	RU	95.163.121.204
c0e5c0da-8...	113e5a243a	2017-08-31 11:47:58	lsm	192.168.66.1		192.168.66.121
b60c97c2-0...	635cb68726	2017-08-31 11:47:58	lsm	192.168.138.158	FR	62.75.195.236
8f05f0ed-5...	bcbb0048d2	2017-08-31 11:47:26	lsm	192.168.138.158	FR	62.75.195.236
4e31b79e-9...	63d9f330d8	2017-08-31 11:47:26	lsm	192.168.138.158	RU	95.163.121.204
320ef0d-9...	c986b7c14	2017-08-31 11:47:26	lsm	192.168.66.1		224.0.0.251
767203af-c...	ecb8efc5e9	2017-08-31 11:47:26	lsm	192.168.138.158	RU	95.163.121.204
6ca1b852-6...	d4d5204765	2017-08-31 11:47:26	lsm	192.168.66.1		192.168.66.121

< 1 - 25 of 265379 >

**Table 2: Alerts Table**

Tools	Description
Alerts table	The Alerts table displays the alerts generated by the CCP 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.

Tools	Description
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

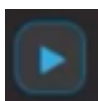
The Alerts user interface defaults to displaying the Alerts table when first opened. You can modify the alerts displayed in the Alerts table to help identify issues.

## 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.

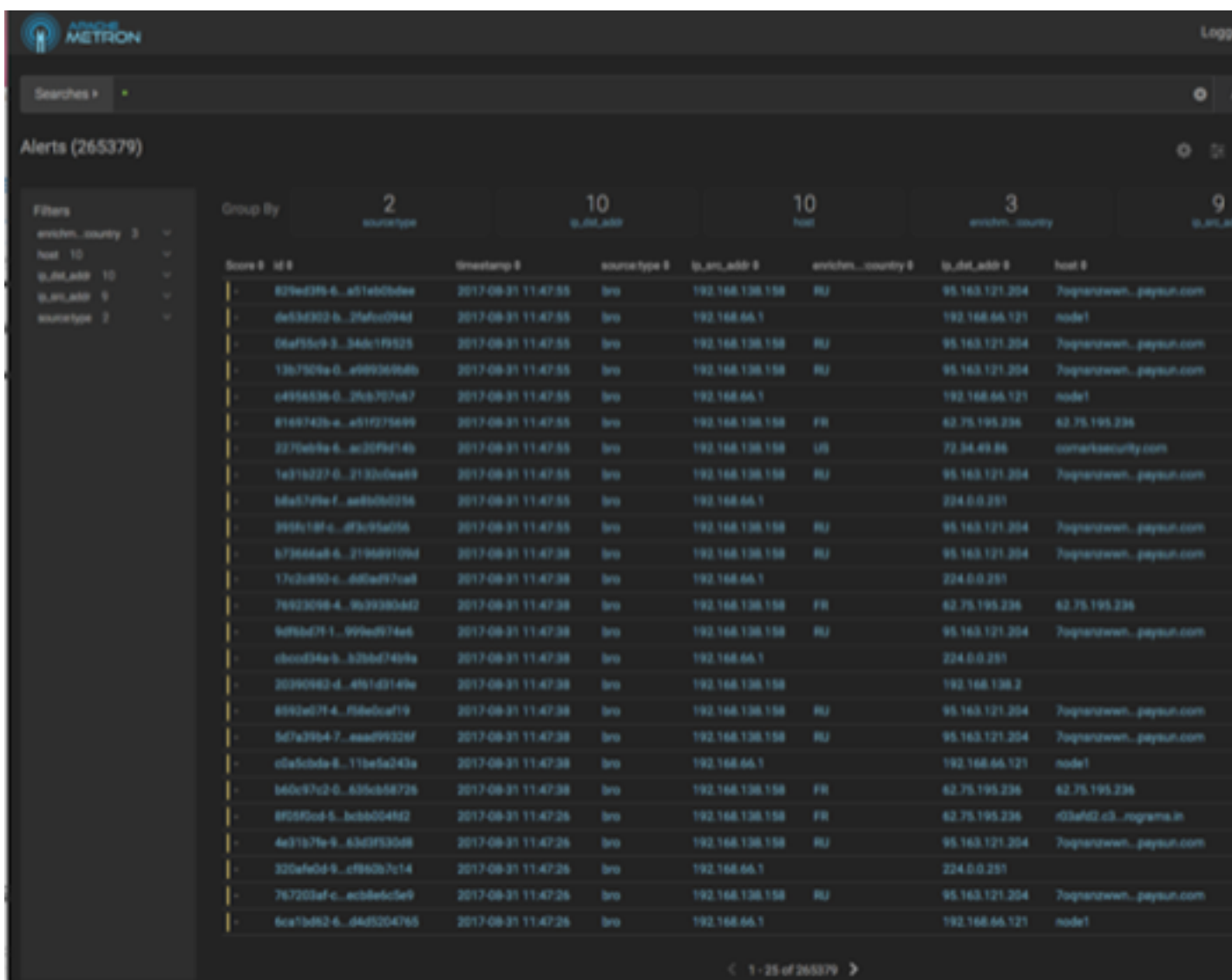
## Using the Alerts Table

The Alerts table displays the alerts generated by the CCP framework. The Alerts UI polls for alerts and refreshes the Alerts table at an interval that you can configure. This polling is paused whenever you open any configuration panels or use the **Searches** field.

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

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:

<b>Red</b>	A score of 69 or higher
<b>Orange</b>	A score between 39 and 69
<b>Yellow</b>	A score below 39



Score	id	timestamp	source_type	ip_addr	enricher...country	ip_addr	host
829e335-6...	a51eb0bde	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
de534302-b...	2fa0c094d	2017-09-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1
06af55c9-3...	34dc1f9325	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
13b7307a-0...	a989369b8b	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
c4956536-0...	2fcb707a67	2017-09-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1
8169742b-e...	a51d275699	2017-09-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236
2270eb9a-6...	ac20f9d14b	2017-09-31 11:47:55	bro	192.168.138.158	US	72.34.49.86	comarkasecurity.com
1e37b227-0...	2132c0eae9	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
5ba57d9e-f...	ae850b0256	2017-09-31 11:47:55	bro	192.168.66.1		224.0.0.251	
3956c18f-c...	d73c95e056	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
b73666a8-6...	219689109d	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
17c3b850-c...	d05ed97ca8	2017-09-31 11:47:55	bro	192.168.66.1		224.0.0.251	
76923098-4...	9c39390d02	2017-09-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236
9d96bd7f-1...	999ed974e6	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
c0cd34a-b...	b2bdf74b9a	2017-09-31 11:47:55	bro	192.168.66.1		224.0.0.251	
20390982-d...	49b1d3149e	2017-09-31 11:47:55	bro	192.168.138.158		192.168.138.2	
8992ed7f-4...	f58ebcaf19	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
5d7a39b4-7...	eead99326f	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
c0a5c0da-8...	119e5a243a	2017-09-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1
b60c97c2-0...	635c358726	2017-09-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236
8f05f0ed-6...	bcb00548d2	2017-09-31 11:47:55	bro	192.168.138.158	FR	62.75.195.236	62.75.195.236
4e31b79e-9...	63d3f930d8	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
320afe0d-9...	c986b7c14	2017-09-31 11:47:55	bro	192.168.66.1		224.0.0.251	
767203af-c...	ecb8efc5e9	2017-09-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7opnanzew...payson.com
6ca73b82-6...	d4d5204765	2017-09-31 11:47:55	bro	192.168.66.1		192.168.66.121	node1

## 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 ✕

<input type="checkbox"/>	Field	Short Name	Type		
<input checked="" type="checkbox"/>	Score		STRING	-	-
<input type="checkbox"/>	AA	<input type="text" value="rename"/>	BOOLEAN	^	v
<input type="checkbox"/>	adapter:geoadapter:begin:ts	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	adapter:geoadapter:end:ts	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	adapter:hostfromjsonlistadapter:begin:ts	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	adapter:hostfromjsonlistadapter:end:ts	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	adapter:threatinteladapter:begin:ts	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	adapter:threatinteladapter:end:ts	<input type="text" value="rename"/>	STRING	^	v
<input checked="" type="checkbox"/>	id	<input type="text" value="rename"/>	STRING	^	v
<input checked="" type="checkbox"/>	timestamp	<input type="text" value="rename"/>	DATE	^	v
<input checked="" type="checkbox"/>	source:type	<input type="text" value="rename"/>	STRING	^	v
<input checked="" type="checkbox"/>	ip_src_addr	<input type="text" value="rename"/>	IP	^	v
<input checked="" type="checkbox"/>	enrichments:geo:ip_dst_addr:country	<input type="text" value="rename"/>	STRING	^	v
<input checked="" type="checkbox"/>	ip_dst_addr	<input type="text" value="rename"/>	IP	^	v
<input checked="" type="checkbox"/>	host	<input type="text" value="rename"/>	STRING	^	v
<input checked="" type="checkbox"/>	alert_status	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	answers	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	bro_timestamp	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	comments	<input type="text" value="rename"/>	OTHER	^	v
<input type="checkbox"/>	dgm:len	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	enrichment:joinbolt:joiner:ts	<input type="text" value="rename"/>	STRING	^	v
<input type="checkbox"/>	enrichments:geo:ip_dst_addr:city	<input type="text" value="rename"/>	STRING	^	v

SAVE
CANCEL

- Select the fields you want to display and unselect the fields you do not want to display.
- 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 is just for display convenience and the changes are not propagated to any system in CCP.



4. You can also configure the order in which the selected columns will appear in the table by using the arrow icons.
5. Click **Save** to save your changes and dismiss the **Configure Table** panel.
- 6.



You can pause the Alerts UI polling by clicking the (pause button).

## Set Timestamp to Local Time

The Alerts user interface timestamp defaults to Coordinated Universal Time (UTC) time. However, you can change the timestamp to reflect your local time.

### Procedure

- 1.



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

A dark gray settings dialog box with the title "Settings" at the top. It contains three sections: "REFRESH RATE" with buttons for 5s, 10s, 15s, 30s, 1m, 10m (selected), and 1h; "ROWS PER PAGE" with buttons for 10, 25 (selected), 50, 100, 250, 500, and 1000; and "HIDE ALERT ENTRIES" with two toggle switches for "HIDE Resolved Alerts" and "HIDE Dismissed Alerts". At the bottom is a "TIMEZONE CONFIGURATION" section with a toggle switch for "Convert timestamps to local time".

2. Click **Convert timestamps to local time**.

## Modify the Alert Data Refresh Rate

You can use the table row settings in the Alerts table to change the refresh rate of the alert data.

Procedure

1.



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. To modify the rate at which the Alerts table is refreshed with new alert information, choose a value under **Refresh Rate**.
- After you modify the refresh rate, you will see a warning indicating that the current alert data is not in sync with your current parameters.



Click the (search) button to refresh the alerts data.

Modify Number of Alert Table Rows

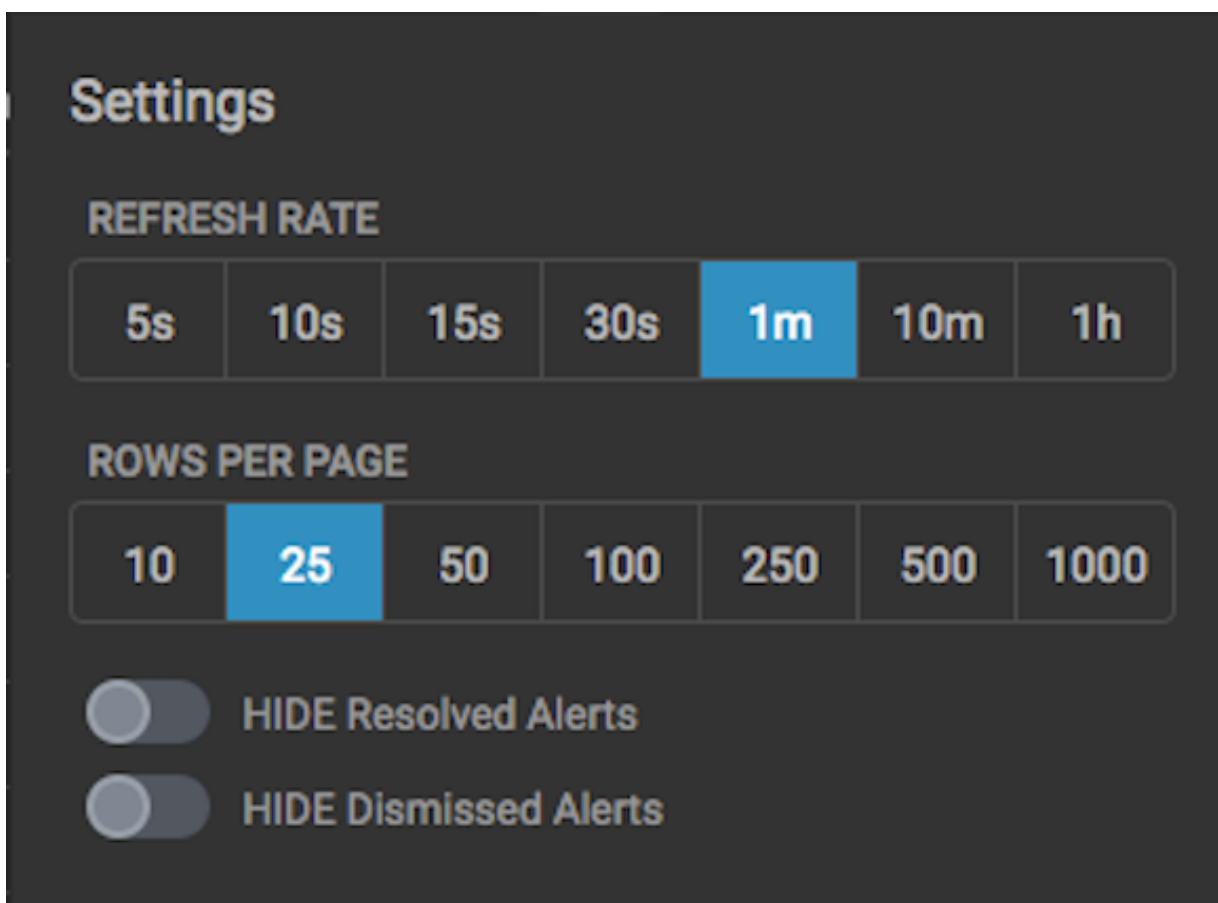
You can use the table row settings in the Alerts table to modify the number of rows that appear in the Alerts table.

Procedure

1.



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



The image shows a 'Settings' dialog box with a dark background. It has two main sections: 'REFRESH RATE' and 'ROWS PER PAGE'. The 'REFRESH RATE' section has buttons for 5s, 10s, 15s, 30s, 1m (selected), 10m, and 1h. The 'ROWS PER PAGE' section has buttons for 10, 25 (selected), 50, 100, 250, 500, and 1000. Below these sections are two toggle switches, both currently turned off, labeled 'HIDE Resolved Alerts' and 'HIDE Dismissed Alerts'.

## 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. 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.

### Hide Resolved or Dismissed Alerts

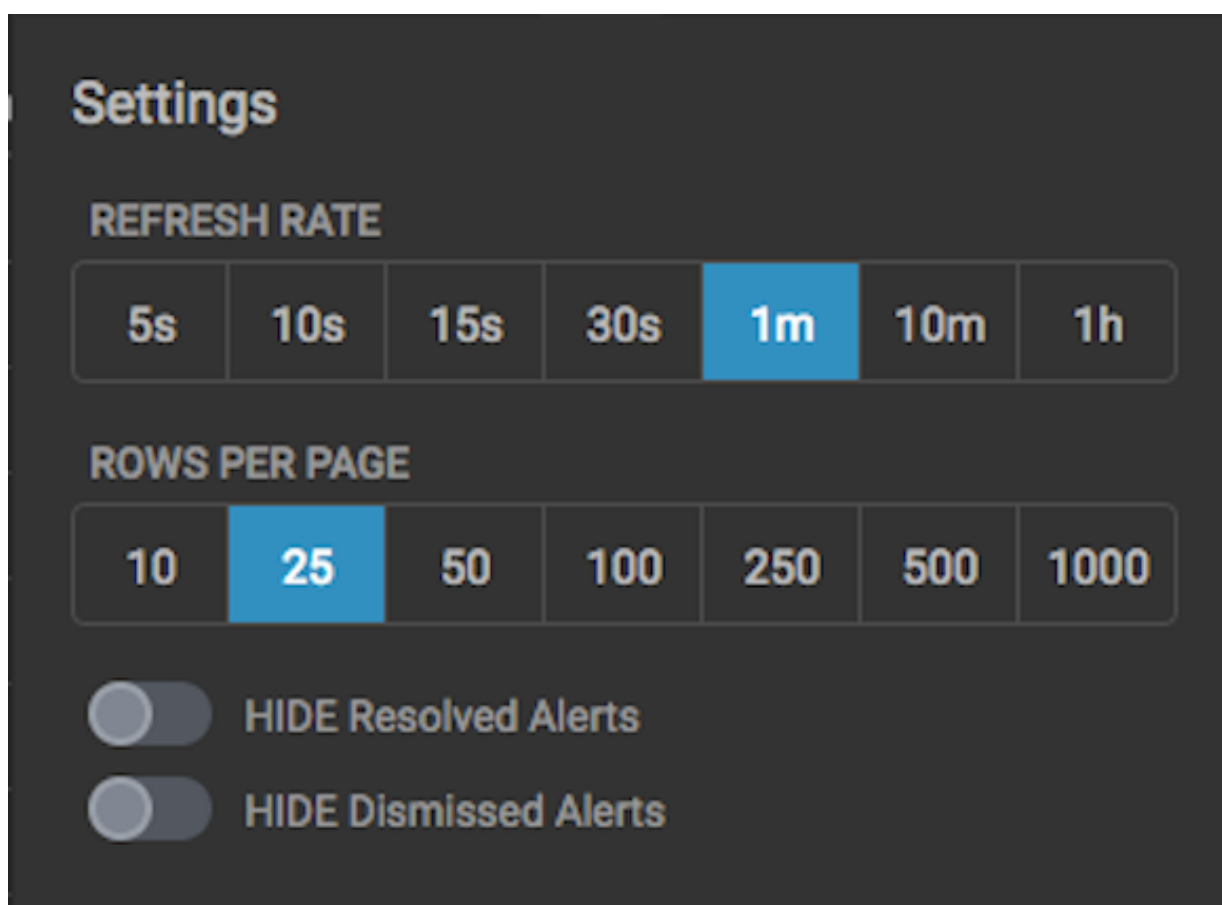
You can use the table row settings in the Alerts table to hide resolved or dismissed alerts.

#### Procedure

- 1.



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



The image shows a settings panel with a dark background. At the top, the word "Settings" is written in a large, bold, light-colored font. Below it, the section "REFRESH RATE" is displayed in a smaller, bold, light-colored font. Under this section, there is a row of seven buttons: "5s", "10s", "15s", "30s", "1m", "10m", and "1h". The "1m" button is highlighted with a blue background. Below the refresh rate section, the section "ROWS PER PAGE" is displayed in a smaller, bold, light-colored font. Under this section, there is a row of seven buttons: "10", "25", "50", "100", "250", "500", and "1000". The "25" button is highlighted with a blue background. At the bottom of the panel, there are two toggle switches. The first toggle is labeled "HIDE Resolved Alerts" and is currently turned off. The second toggle is labeled "HIDE Dismissed Alerts" and is also currently turned off.

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

### 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

OPEN

DISMISS

RESOLVE

ESCALATE

alert_status	OPEN
dgmlen	40
enrichments:geo:ip_sr	Phoenix
c_addr:city	
enrichments:geo:ip_sr	US
c_addr:country	
enrichments:geo:ip_sr	753
c_addr:dmaCode	
enrichments:geo:ip_sr	33.4499
c_addr:latitude	
enrichments:geo:ip_sr	5308655
c_addr:locID	
enrichments:geo:ip_sr	33.4499,-112.0712
c_addr:location_point	
enrichments:geo:ip_sr	-112.0712
c_addr:longitude	
enrichments:geo:ip_sr	85004
c_addr:postalCode	
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

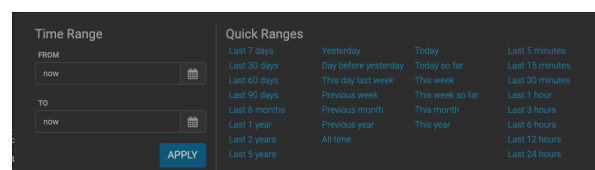
Enables you to enter or choose the start and end dates and times for your search.

The valid date format is: YYYY-MM-DD  
HH:mm:ss.

#### 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.

Searches ▶



## 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 Alerts UI with 147,925 alerts. The left sidebar contains a 'Filters' panel with the following filters applied:

- enrichments:geo\_dst\_addr:country (3)
- host (10)
- ip\_dst\_addr (10)
- ip\_src\_addr (9)
- sourcetype (2)

The main table displays alerts with columns: Score, ID, timestamp, sourcetype, ip\_src\_addr, enrichments:geo\_dst\_addr:country, and ip\_dst\_addr. The table is grouped by sourcetype (2), ip\_dst\_addr (10), host (10), and enrichments:geo\_dst\_addr:country (3).

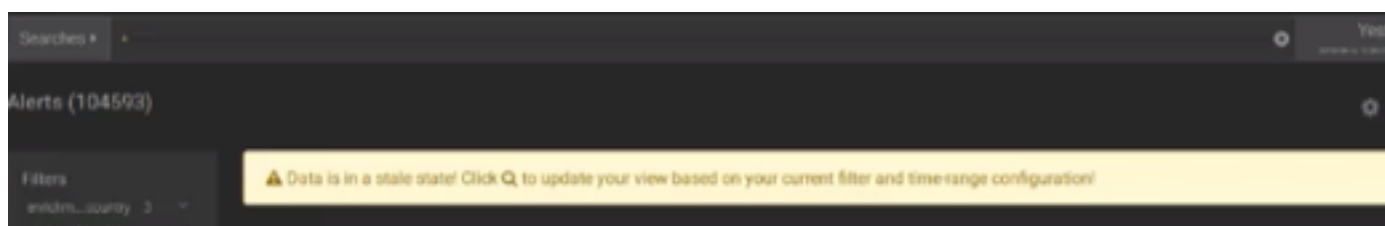
Score	ID	timestamp	sourcetype	ip_src_addr	enrichments:geo_dst_addr:country	ip_dst_addr
10	06af55c9-3...34dc1f9525	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.20
10	829ed3f6-6...a51ab0bdee	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.20
10	de53f302-b...2f4f0c094d	2017-08-31 11:47:55	bro	192.168.66.1		192.168.66.12
10	f8f4a88-8...c938c01be6	2017-08-30 08:07:59	snort	192.168.66.1		192.168.66.12
10	10a83fa3-8...41395e6201	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
10	d83006c0-4...afac68715	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
10	f63236fe-3...2208f599f4	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.12
10	9af4aca9-c...a9914d7655	2017-08-30 12:43:58	bro	192.168.138.158	US	204.152.254.2
10	0b94d0d6-7...fb113e8bce	2017-08-30 12:43:58	bro	192.168.138.158	FR	62.75.195.238
10	5796f8cb-a...7420f2bac2	2017-08-30 12:43:58	bro	192.168.66.1		192.168.66.12
10	3944e90f-b...a6b9d39c39	2017-08-30 12:43:58	bro	192.168.138.158	RU	95.163.121.20
10	90403c32-5...2ecf48d8d8	2017-08-30 12:43:58	bro	192.168.66.1		224.0.0.251
10	88950cee-5...309fao0a78	2017-08-30 12:43:58	bro	192.168.138.158	RU	95.163.121.20
10	60bf112-c...c2619e8a36	2017-08-30 12:43:58	bro	192.168.138.158		192.168.138.2
10	327e865e-1...3c21a1a759	2017-08-30 12:44:06	bro	192.168.138.158	RU	95.163.121.20
10	9eb95f9-5...5ec9069f53	2017-08-30 12:44:06	bro	192.168.138.158	FR	62.75.195.238
10	ca0d424a-6...4f0148306a	2017-08-30 12:44:06	bro	192.168.138.158	FR	62.75.195.238
10	779b607e-2...f1365e19e0	2017-08-30 12:44:06	bro	192.168.138.158	US	72.34.49.86
10	3b22460c-a...b8a14515db	2017-08-30 12:44:06	bro	192.168.138.158		192.168.138.2
10	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.

After you modify the filter, you will see a warning indicating that the current alert data is not in sync with your filter parameters:

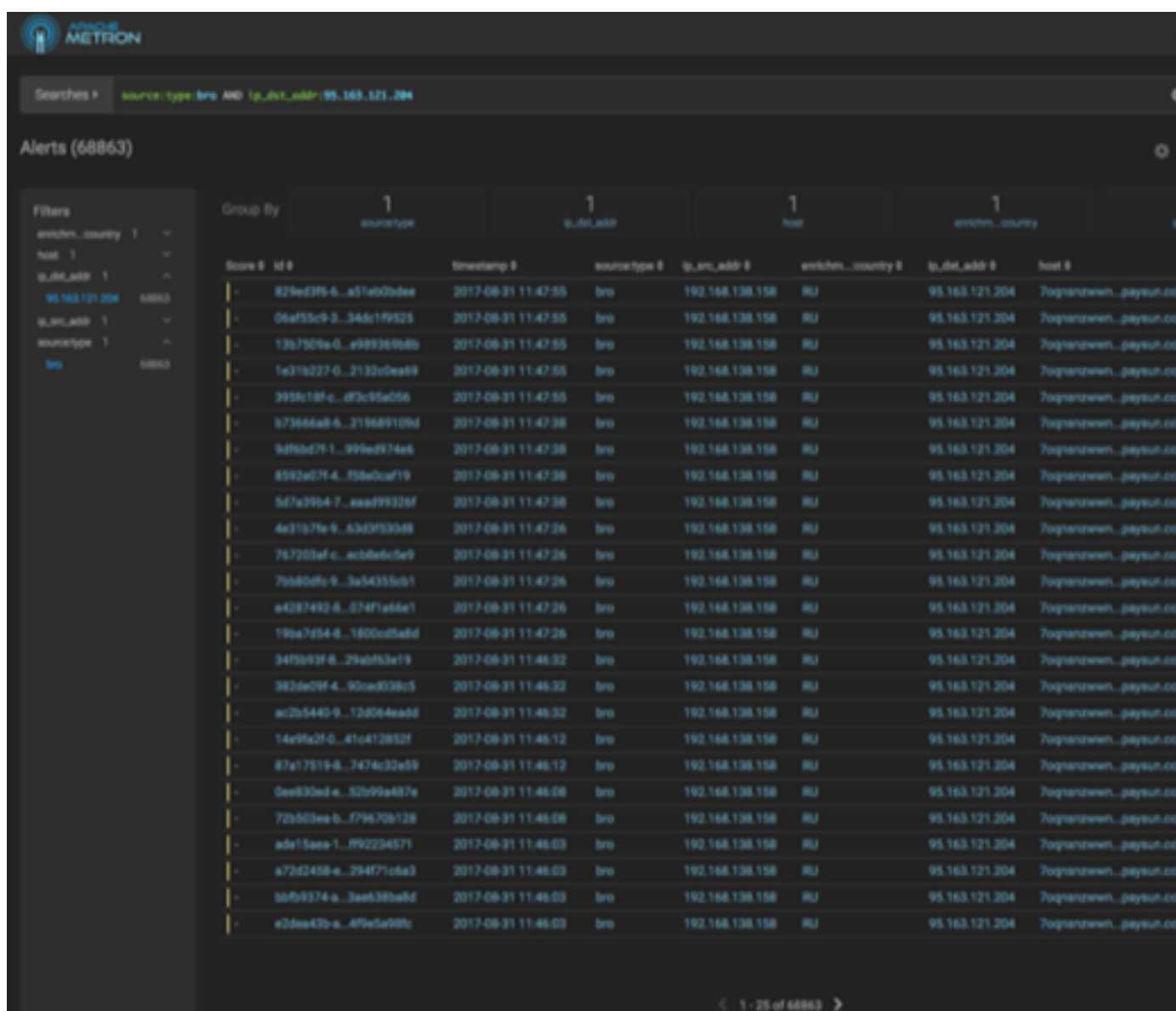


Click the  (search) button to refresh the alerts data.

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.



3. You can also enter alert filters in the **Search** field.



For example:

alert\_status:(NEW OR OPEN)

4.



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

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.

Alerts Information Panel

AVuKz1\_n1LEanKS6qbtb

Status

NEW

OPEN

DISMISS

ESCALATE

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

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.

Alerts Information Panel

AVuKz1\_n1LEanKS6qbtb

Status

NEW

OPEN

DISMISS

ESCALATE

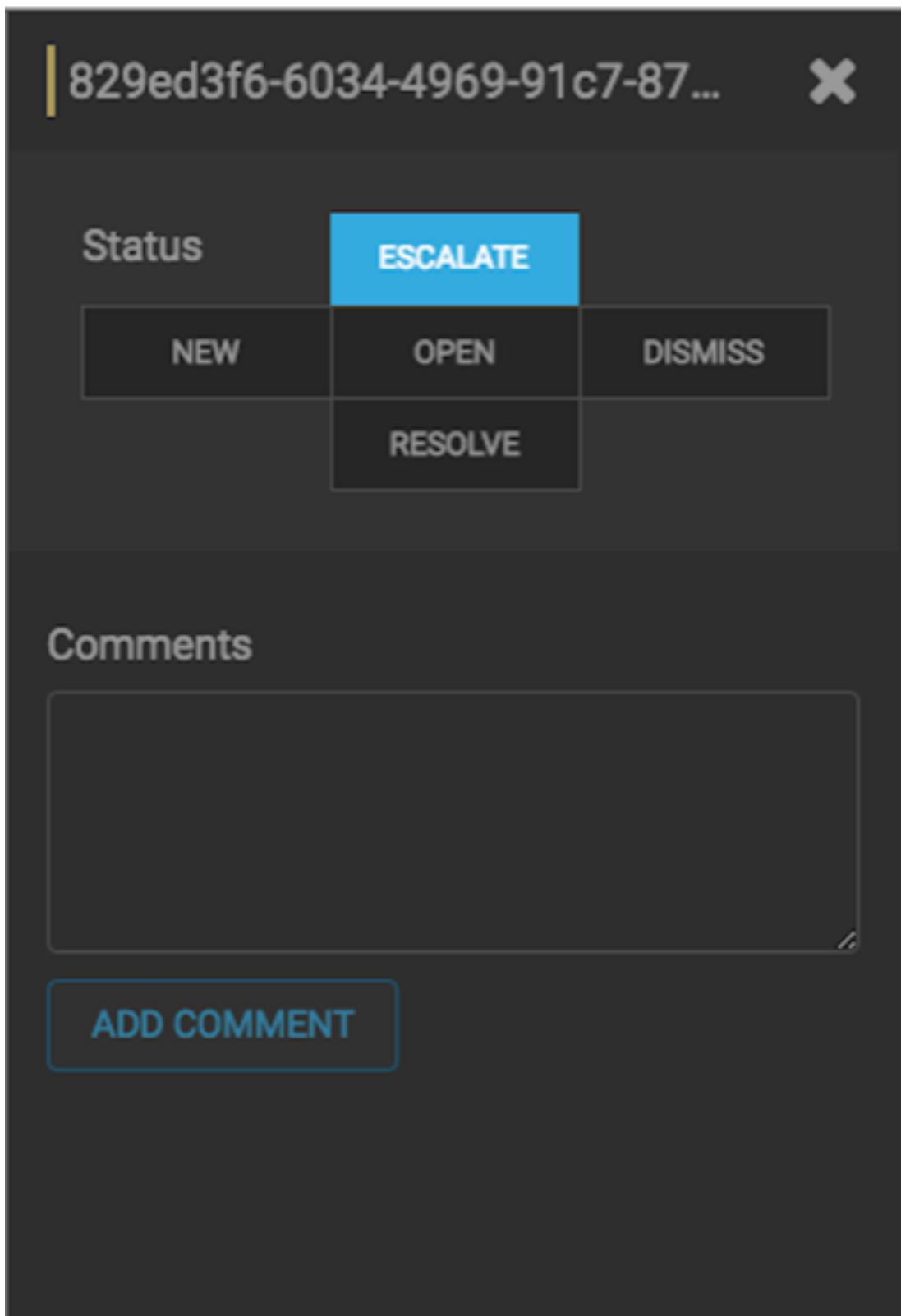
RESOLVE

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

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 triaging 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: 'NEW', 'OPEN', 'DISMISS', and 'RESOLVE'. The 'ESCALATE' button is highlighted in blue and is positioned above the 'OPEN' button. The second section, titled 'Comments', contains a large text input area and an 'ADD COMMENT' button below it.

Status		
	ESCALATE	
NEW	OPEN	DISMISS
	RESOLVE	

Comments

ADD COMMENT

CCP 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.

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**.

## Group Alerts

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

### Procedure

1. 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 Yaf, Snort and Bro.

The Alerts UI displays the total number of alerts in the group below the Alerts total. See **Alerts in Groups (7560)**.

The screenshot shows the Apache Metron Alerts interface. On the left is a navigation menu with options: Alerts, Overview, PCAP, Management, Sensors, and General Settings. The main area displays 'Alerts (7620)' and 'Alerts in Groups (7560)'. Below this, there are filters for enrichm...country (3), ip\_dst\_addr (10), ip\_src\_addr (9), and source.type (3). The 'Group By' section shows three groups: 'source.type' with a count of 3, 'ip\_dst\_addr' with a count of 10, and 'enrichm...country' with a count of 3. The 'source.type' group is selected, showing a tree view with three sub-groups: 'yaf' (ALERTS 2,520), 'snort' (ALERTS 2,520), and 'bro' (ALERTS 2,520). Each group has a severity score icon to its left: a green hexagon with '9' for 'yaf', a red hexagon with '999+' for 'snort', and a green hexagon with '9' for '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+.

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



Alerts (7620)  
Alerts in Groups (7560)

Filters

- enrichm...country 3
- ip\_dst\_addr 10
- ip\_src\_addr 9
- source\_type 3

Group By

- 3 source\_type
- 10 ip\_dst\_addr
- 3 enrichm...country

0 yaf

ALERTS 2,490

Score	guid	timestamp	source_type	ip_src_addr	enrichm...country
-	5114039d-f...515caf9403	2019-08-27 23:16:07	yaf	192.168.66.1	
-	9a3c6e0c-1...429a7b46ad	2019-08-27 23:16:10	yaf	62.75.195.236	
-	9f166103-8...b6a9453d37	2019-08-27 23:16:10	yaf	62.75.195.236	
-	31df241e-b...0db83d741f	2019-08-27 23:16:10	yaf	62.75.195.236	
-	cc691043-5...e7d6070f33	2019-08-27 23:16:13	yaf	192.168.66.1	

3. 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.

4. 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.

5. 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.

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

Alerts (265379)

Filters

- enrichm...country 3
- host 10
- ip\_dst\_addr 10
- ip\_src\_addr 9
- source\_type 2

Group By

- 2 source\_type
- 10 ip\_dst\_addr
- 10 host
- 3 enrichm...country

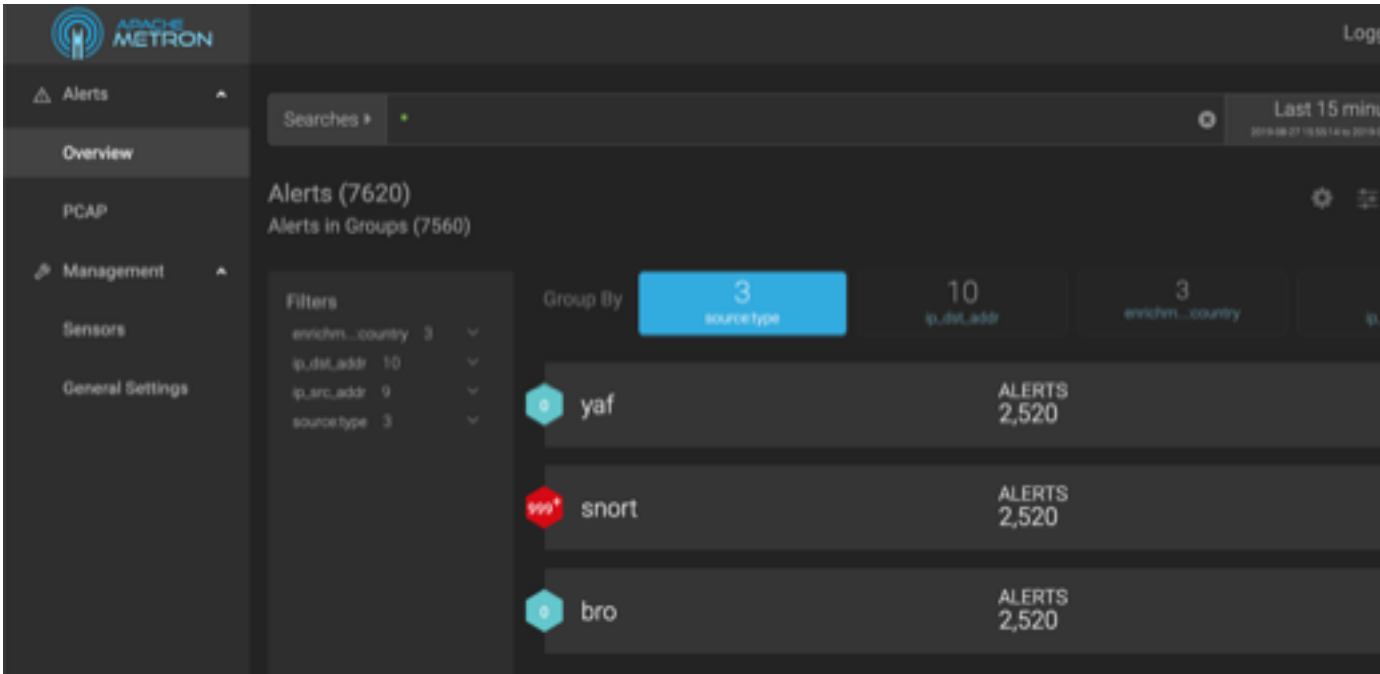
Score	id	timestamp	source_type	ip_src_addr	enrichm...country	ip_dst_addr	host
-	829ed3f5-6...a51eb0bdee	2017-08-31 11:47:55	lms	192.168.138.158	RU	95.163.121.204	7ogranonwn...paysun.o
-	de53d302-b...2fa0c094d	2017-08-31 11:47:55	lms	192.168.66.1		192.168.66.121	node1

## 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

- 1. Click one of the groups listed by **Group By**.  
The **Alerts** table view changes to a tree view listing the values of the groups.



- 2. Use the **Search** and **GroupBy** options to create one or more groups containing alerts on which you want to focus.
- 3.



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.

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

AVuKz1\_n1LEanKS6qbtb

X

Status

ESCALATE

NEW

OPEN

DISMISS

RESOLVE

alert\_status

OPEN

dgmlen

40

enrichments:geoip\_sr

Phoenix

c\_addr:city

enrichments:geoip\_sr

US

c\_addr:country

enrichments:geoip\_sr

753

c\_addr:dmaCode

enrichments:geoip\_sr

33.4499

c\_addr:latitude

enrichments:geoip\_sr

5308655

c\_addr:locID

enrichments:geoip\_sr

33.4499,-112.0712

c\_addr:location\_point

enrichments:geoip\_sr

-112.0712

c\_addr:longitude

enrichments:geoip\_sr

85004

c\_addr:postalCode

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.

## Integrating Third-Party Portals

You can reach other web services to view additional information about the alert data through dynamically created URLs by adding click-through navigation in the Alerts user interface. For example you can view third-party threat intelligence portals or corporate ticketing systems and directories. You can attach click-through navigation to a cell or a row in the Alerts UI table.

### Procedure

1. Change the `isEnabled` property in `/$METRON/web/alerts-ui/assets/context-menu.conf.json` file to `true`:

```
{
  isEnabled: true,
  config: {
    ...
```

2. To attach and configure a menu configuration to a column in the Alerts table, use the field ID to target the particular column.

For example, to configure the "Whois Reputation Service" item for the context menu, add the following information:

```
{
  isEnabled: true,
  config: {
    "host": [
      {
        "label": "Whois Reputation Service",
        "urlPattern": "https://www.whois.com/whois/{}"
      }
    ],
    ...
```

Clicking on the item opens another browser tab and calls the URL in the `urlPattern` config field.

- a) The `{}` at the end of the `urlPattern` is a default placeholder. If you add any available alert property field at the end of the `urlPattern`, the value of the host field replaces the default placeholder.

For example:

```
{
  isEnabled: true,
  config: {
    "host": [
      {
        "label": "Whois Reputation Service",
        "urlPattern": "https://www.whois.com/whois/{ip_src_addr}"
      }
    ],
    ...
```

- b) You can also reference multiple fields and combine default and specific placeholders:

```
{
  isEnabled: true,
  config: {
    "host": [
      {
        "label": "Whois Reputation Service",
        "urlPattern": "https://www.whois.com/whois/{}?srcip={ip_src_addr}&destip={ip_dest_addr}"
      }
    ]
  }
}
```

```

    },
  ],
  ...

```

c) You can also configure multiple menu items to a particular column:

```

{
  isEnabled: true,
  config: {
    "ip_src_addr": [
      {
        "label": "IP Investigation Notebook",
        "urlPattern": "http://zepellin.example.com:9000/notebook/someid?ip={ip_src_addr}"
      },
      {
        "label": "IP Conversation Investigation",
        "urlPattern": "http://zepellin.example.com:9000/notebook/someid?ip_src_addr={ip_src_addr}&ip_dst_addr={ip_dst_addr}"
      }
    ],
    "host": [
      {
        "label": "Whois Reputation Service",
        "urlPattern": "https://www.whois.com/whois/{}?srcip={ip_src_addr}&destip={ip_dest_addr}"
      }
    ],
    ...
  }
}

```

3. To attach and configure a menu configuration to a row in the Alerts table, you can configure for an alert or a meta alert.

To configure for an alert, use the keyword `alertEntry`. For a meta alert, use the keyword `metaAlertEntry`:

```

{
  isEnabled: true,
  config: {
    "alertEntry": [
      {
        "label": "Internal ticketing system",
        "urlPattern": "http://mytickets.org/tickets/{id}"
      }
    ],
    "metaAlertEntry": [
      {
        "label": "MetaAlert specific item",
        "urlPattern": "http://mytickets.org/tickets/{id}"
      }
    ],
    ...
  }
}

```

## Save Your Searches

You can save your Alert searches for future reuse.

**Procedure**

1.



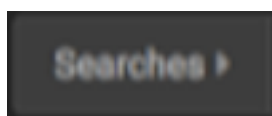
To save a search, click the (save button) next to the **Searches** field.

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

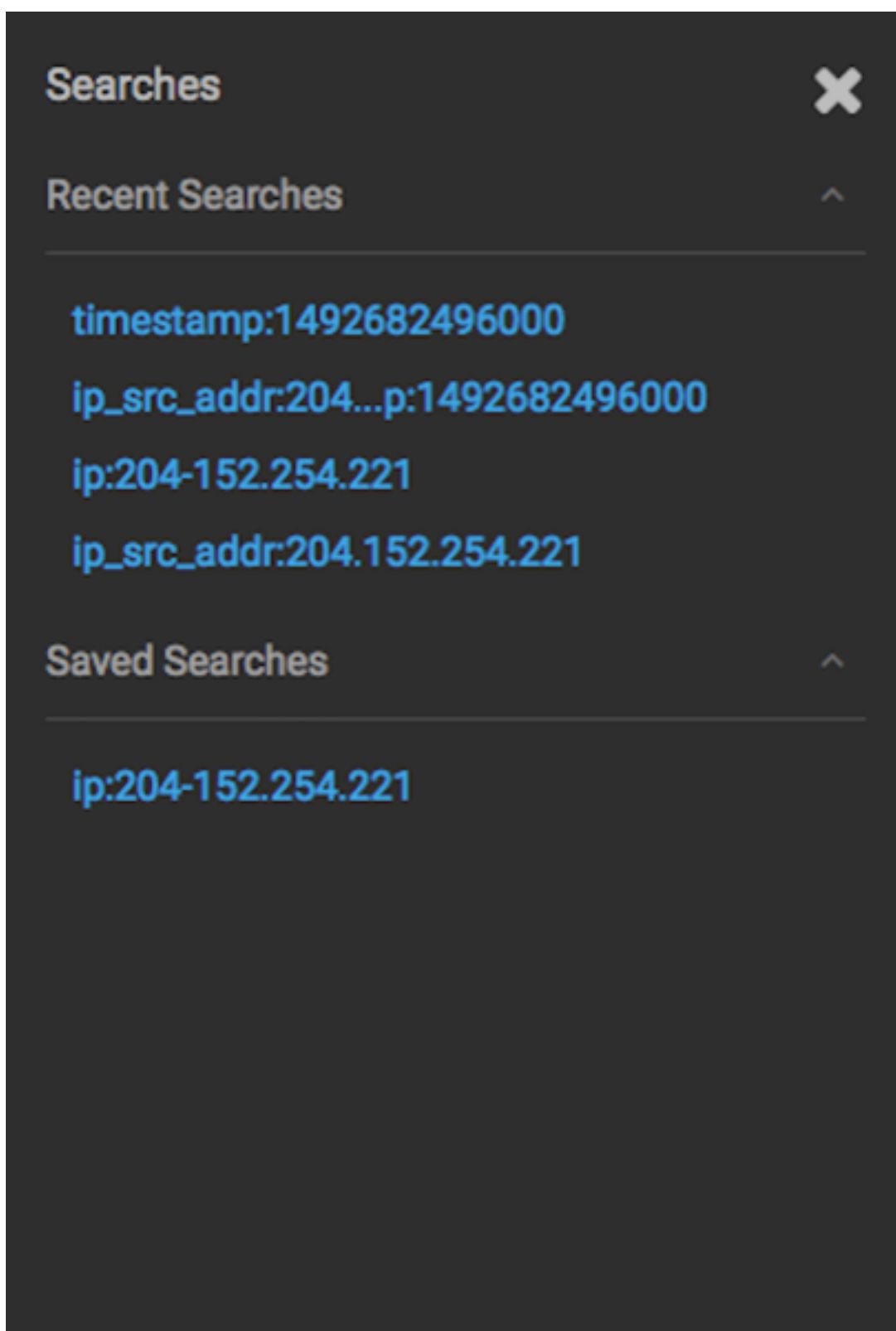
You can view both your recent searches and saved searches in the Alerts UI.

**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.