

# **BroadWorks Dashboards and Discovery**

## Kibana Dashboards Installation Instructions

Document Version 1.0

## Content

This document contains instructions to configure Kibana and import the sample visualizations contains in file "BroadWorks Dashboards x.x".

These instructions assume that Elasticsearch is installed, functional and collecting data from BroadWorks. Kibana should also be installed with its default configuration.

## Table of Contents

1. Create the Index Patterns on Kibana.....	4
2. Configure lucene string parser .....	8
3. Change calculated_callduration format (optional).....	10
4. Import Dashboards .....	11
5. Start Dashboards.....	11

## 1. Create the Index Patterns on Kibana

Upon entering a new instance of Kibana the following screen will be presented prompting you to configure the index patterns:

**Configure an index pattern**

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☒ Index contains time-based events

☐ Use event times to create index names [DEPRECATED]

**Index name or pattern**

Patterns allow you to define dynamic index names using \* as a wildcard. Example: logstash-\*

logstash-\*

☒ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-\** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

Unable to fetch mapping. Do you have indices matching the pattern?

### a. Configure `bwcd*` index pattern as follows:

**Configure an index pattern**

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☒ Index contains time-based events

☐ Use event times to create index names [DEPRECATED]

**Index name or pattern**

Patterns allow you to define dynamic index names using \* as a wildcard. Example: logstash-\*

bwcd\*

☒ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-\** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

Time-field name ⓘ refresh fields

starttime

Create

Click “Create”:

The screenshot shows the Kibana Settings page for the **bwlog\*** index pattern. The left sidebar shows the navigation menu with 'Indices' selected. The main content area displays the index pattern **bwlog\*** and a table of fields.

Fields (52):

name	type	format	analyzed	indexed	controls
siptouser	string			✓	
apacheresponsemicroseconds	string			✓	
logtimestamp	date			✓	
usscmd	string			✓	
_source	_source				
impto	string			✓	
siptype	string			✓	
psociduration	string			✓	
psocitransactionid	string			✓	
ocitransaction	string			✓	
apacheremoteip	string			✓	
correlationid	string			✓	
apacheuri	string			✓	
ussroomid	string			✓	
psocitransaction	string			✓	
usssrc	string			✓	
ocictargetid	string			✓	

b. Configure bwlog\* index pattern. Click “+Add New”:

The screenshot shows the Kibana Settings page for configuring the **bwlog\*** index pattern. The left sidebar shows the navigation menu with 'Indices' selected. The main content area displays the configuration form.

**Configure an index pattern**

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☒ Index contains time-based events

☐ Use event times to create index names [DEPRECATED]

**Index name or pattern**

Patterns allow you to define dynamic index names using \* as a wildcard. Example: logstash-\*

**bwlog\***

☐ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-\** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

**Time-field name** refresh fields

logtimestamp

**Create**

Click “Create”:

Discover

Visualize

Dashboard

Settings

Indices

Advanced

Objects

Status

About

Index Patterns

★ bwcdt\*

bwlog\*

+ Add New

bwlog\*

★

This page lists every field in the **bwlog\*** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API.

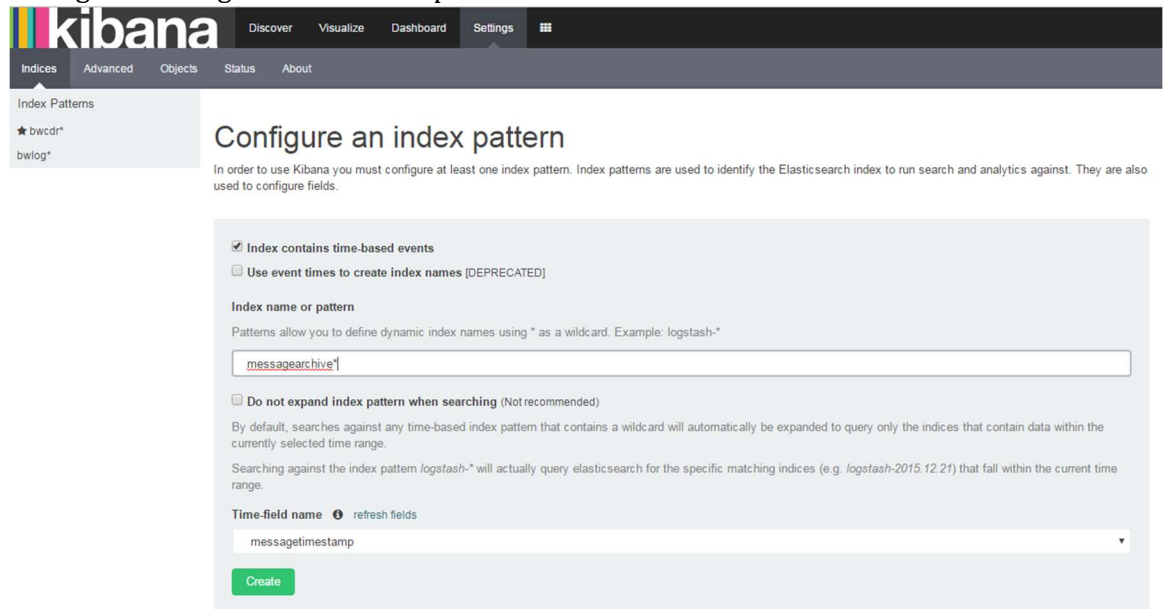
Filter

Fields (52)

Scripted fields (0)

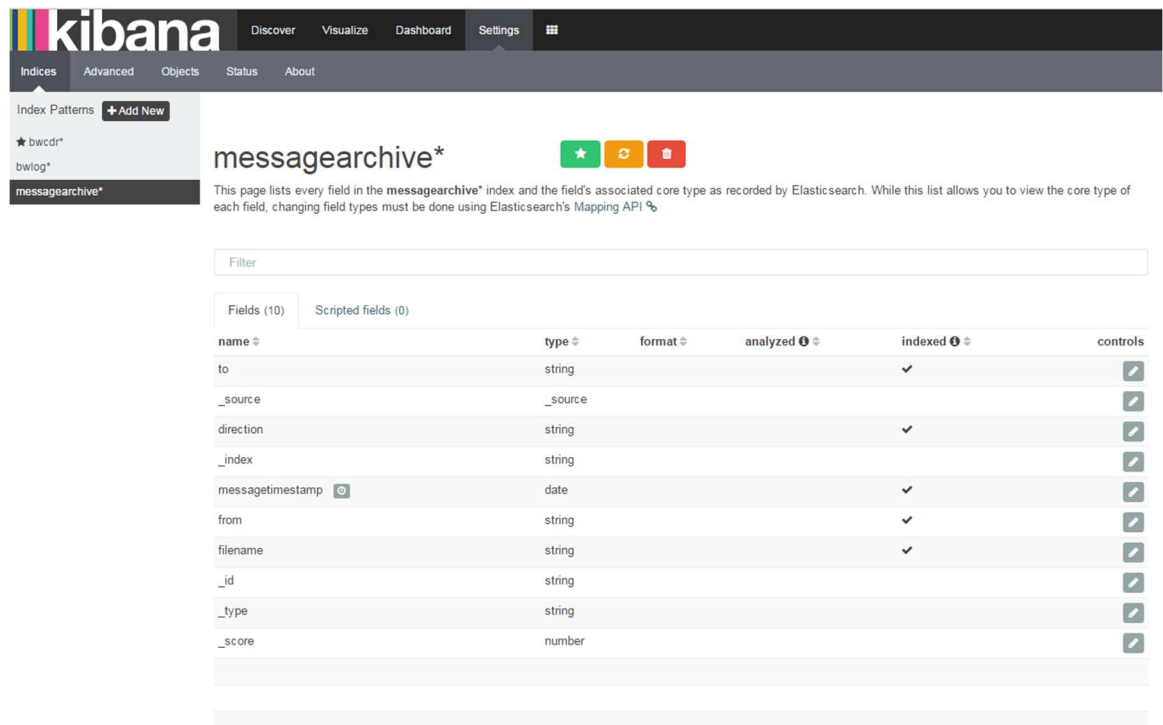
name	type	format	analyzed	indexed	controls
siptouser	string			✓	
apacheresponsemicroseconds	string			✓	
logtimestamp	date			✓	
usscmd	string			✓	
_source	_source				
impto	string			✓	
siptype	string			✓	
psociduration	string			✓	
psocitransactionid	string			✓	
ocitransaction	string			✓	
apacheremoteip	string			✓	
correlationid	string			✓	
apacheuri	string			✓	
ussroomid	string			✓	
psocitransaction	string			✓	
usssrc	string			✓	
ocictargetid	string			✓	

- c. Configure messagearchive\* index pattern. Click “+Add New”:



The screenshot shows the Kibana 'Configure an index pattern' page. The left sidebar has 'Indices' selected, with 'Index Patterns' expanded. Below it are '★ bwcdr\*' and 'bwlog\*'. The main content area is titled 'Configure an index pattern' and includes a description: 'In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.' The configuration options are: 'Index contains time-based events' (checked), 'Use event times to create index names [DEPRECATED]' (unchecked), 'Index name or pattern' (text input with 'messagearchive\*'), 'Do not expand index pattern when searching (Not recommended)' (unchecked), and 'Time-field name' (dropdown menu with 'messagetimestamp' selected). A green 'Create' button is at the bottom.

Click “Create”:

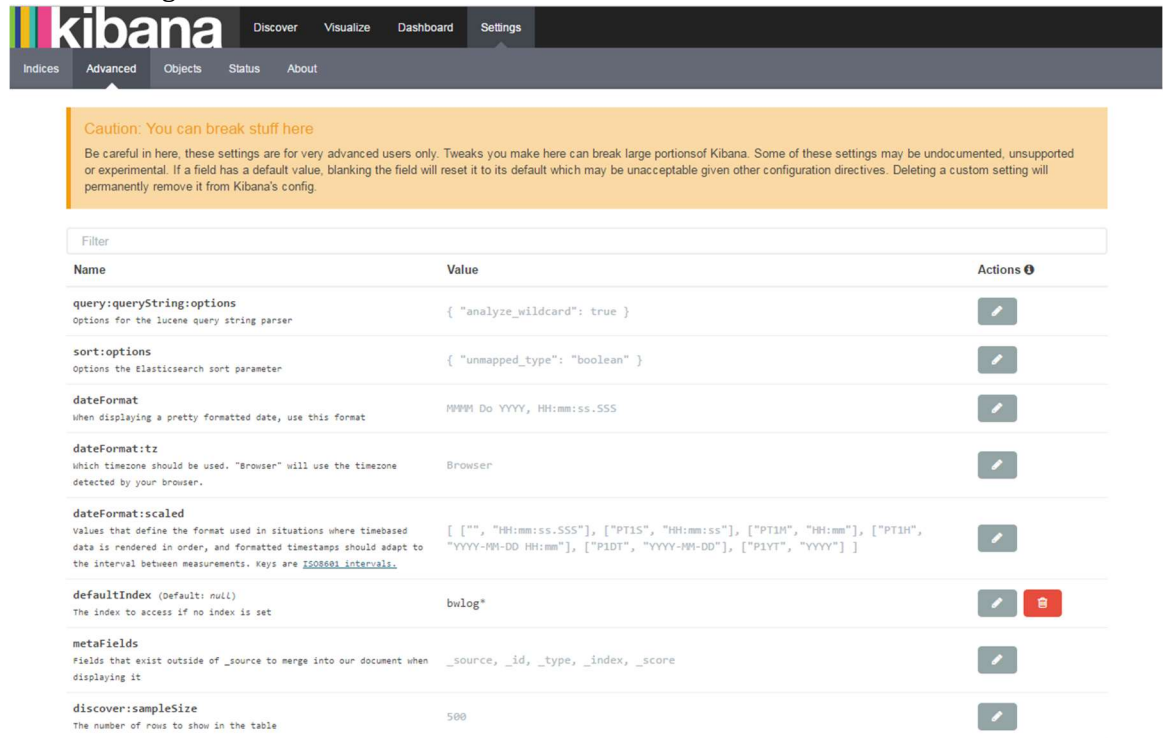


The screenshot shows the Kibana 'messagearchive\*' index pattern page. The left sidebar has 'Indices' selected, with 'Index Patterns' expanded. Below it are '★ bwcdr\*', 'bwlog\*', and 'messagearchive\*'. The main content area is titled 'messagearchive\*' and includes a description: 'This page lists every field in the messagearchive\* index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API %'. Below the description is a table of fields.

name	type	format	analyzed	indexed	controls
to	string			✓	
_source	_source				
direction	string			✓	
_index	string				
messagetimestamp	date			✓	
from	string			✓	
filename	string			✓	
_id	string				
_type	string				
_score	number				

## 2. Configure lucene string parser

### a. Click “Settings”, click “Advanced”

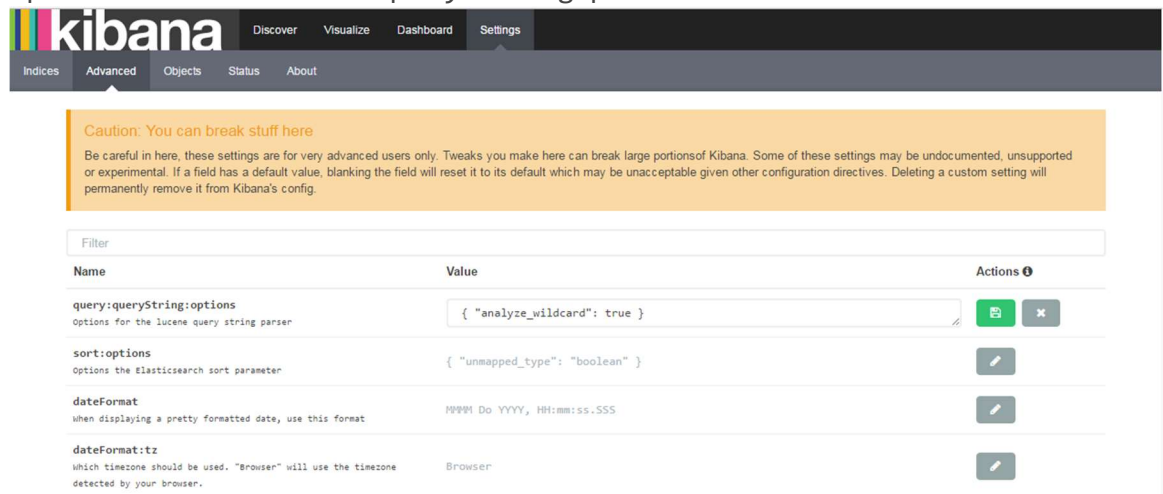


The screenshot shows the Kibana Settings page with the 'Advanced' tab selected. A warning banner at the top states: 'Caution: You can break stuff here. Be careful in here, these settings are for very advanced users only. Tweaks you make here can break large portions of Kibana. Some of these settings may be undocumented, unsupported or experimental. If a field has a default value, blanking the field will reset it to its default which may be unacceptable given other configuration directives. Deleting a custom setting will permanently remove it from Kibana's config.'

Name	Value	Actions
<b>query:queryString:options</b> options for the lucene query string parser	{ "analyze_wildcard": true }	
<b>sort:options</b> options the Elasticsearch sort parameter	{ "unmapped_type": "boolean" }	
<b>dateFormat</b> when displaying a pretty formatted date, use this format	MMM Do YYYY, HH:mm:ss.SSS	
<b>dateFormat:tz</b> which timezone should be used. "Browser" will use the timezone detected by your browser.	Browser	
<b>dateFormat:scaled</b> values that define the format used in situations where timebased data is rendered in order, and formatted timestamps should adapt to the interval between measurements. Keys are <a href="#">ISO8601 intervals</a> .	[ "", "HH:mm:ss.SSS", ["PT1S", "HH:mm:ss"], ["PT1H", "HH:mm"], ["PT1H", "YYYY-MM-DD HH:mm"], ["P1DT", "YYYY-MM-DD"], ["P1YT", "YYYY"] ]	
<b>defaultIndex</b> (Default: null) The index to access if no index is set	bwlog*	
<b>metaFields</b> Fields that exist outside of _source to merge into our document when displaying it	_source, _id, _type, _index, _score	
<b>discover:sampleSize</b> The number of rows to show in the table	500	

### b. Click Edit icon for query:queryString:options (Default: { "analyze\_wildcard": true })

Options for the lucene query string parser

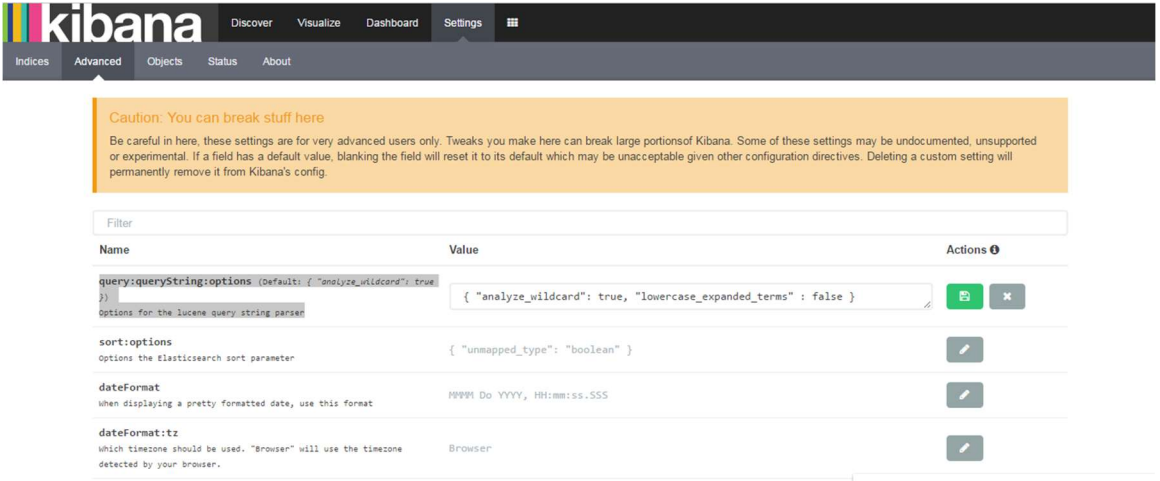


This screenshot shows the same Kibana Settings page, but the 'query:queryString:options' setting is now being edited. The value field contains the JSON object { "analyze\_wildcard": true }, and the Actions column shows a green 'Save' icon and a red 'Cancel' icon, along with the edit icon.

Name	Value	Actions
<b>query:queryString:options</b> options for the lucene query string parser	{ "analyze_wildcard": true }	
<b>sort:options</b> options the Elasticsearch sort parameter	{ "unmapped_type": "boolean" }	
<b>dateFormat</b> when displaying a pretty formatted date, use this format	MMM Do YYYY, HH:mm:ss.SSS	
<b>dateFormat:tz</b> which timezone should be used. "Browser" will use the timezone detected by your browser.	Browser	



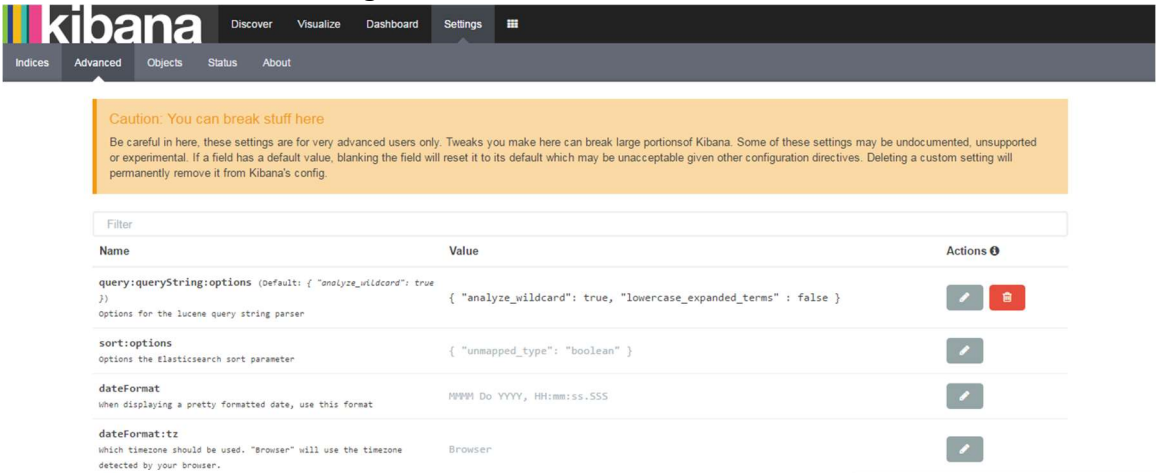
Enter the following value: { "analyze\_wildcard": true, "lowercase\_expanded\_terms" : false } and click the Save icon



The screenshot shows the Kibana Settings page. At the top, there is a navigation bar with the Kibana logo and tabs for Discover, Visualize, Dashboard, Settings, and a hamburger menu. Below the navigation bar, there is a sub-navigation bar with links for Indices, Advanced, Objects, Status, and About. A yellow warning box is present, stating: "Caution: You can break stuff here. Be careful in here, these settings are for very advanced users only. Tweaks you make here can break large portions of Kibana. Some of these settings may be undocumented, unsupported or experimental. If a field has a default value, blanking the field will reset it to its default which may be unacceptable given other configuration directives. Deleting a custom setting will permanently remove it from Kibana's config." Below the warning box, there is a table with the following settings:

Name	Value	Actions
query:queryString:options (Default: { "analyze_wildcard": true }) options for the lucene query string parser	{ "analyze_wildcard": true, "lowercase_expanded_terms" : false }	[Save] [X]
sort:options options the Elasticsearch sort parameter	{ "unmapped_type": "boolean" }	[Edit]
dateFormat when displaying a pretty formatted date, use this format	YYYY Do YYYY, HH:mm:ss.SSS	[Edit]
dateFormat:tz which timezone should be used. "browser" will use the timezone detected by your browser.	Browser	[Edit]

Which results in the following screen:



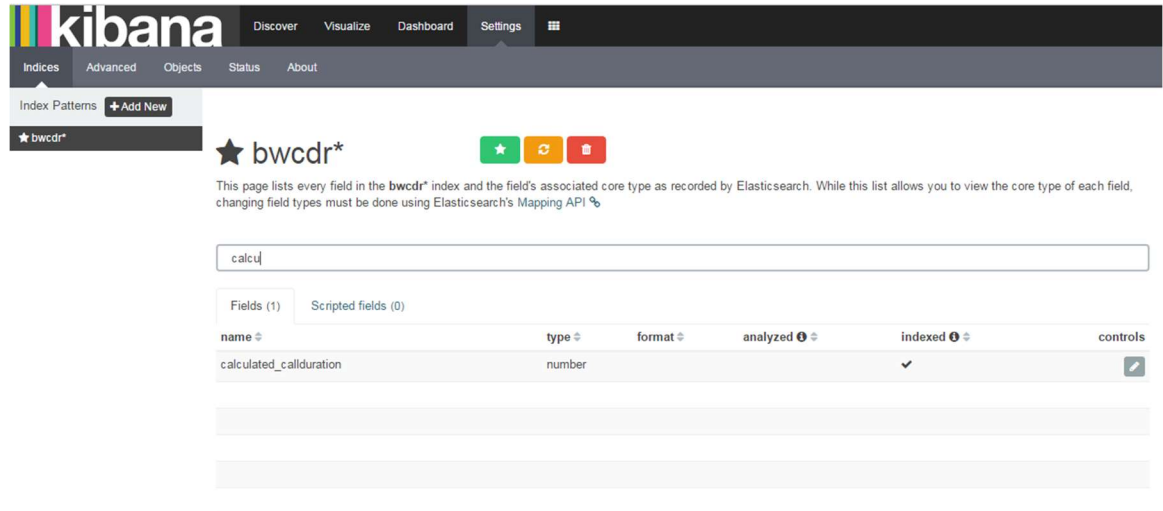
The screenshot shows the Kibana Settings page after saving the configuration. The navigation bar and sub-navigation bar are the same as in the previous screenshot. The yellow warning box is still present. The table now shows the following settings:

Name	Value	Actions
query:queryString:options (Default: { "analyze_wildcard": true }) options for the lucene query string parser	{ "analyze_wildcard": true, "lowercase_expanded_terms" : false }	[Edit] [Delete]
sort:options options the Elasticsearch sort parameter	{ "unmapped_type": "boolean" }	[Edit]
dateFormat when displaying a pretty formatted date, use this format	YYYY Do YYYY, HH:mm:ss.SSS	[Edit]
dateFormat:tz which timezone should be used. "browser" will use the timezone detected by your browser.	Browser	[Edit]

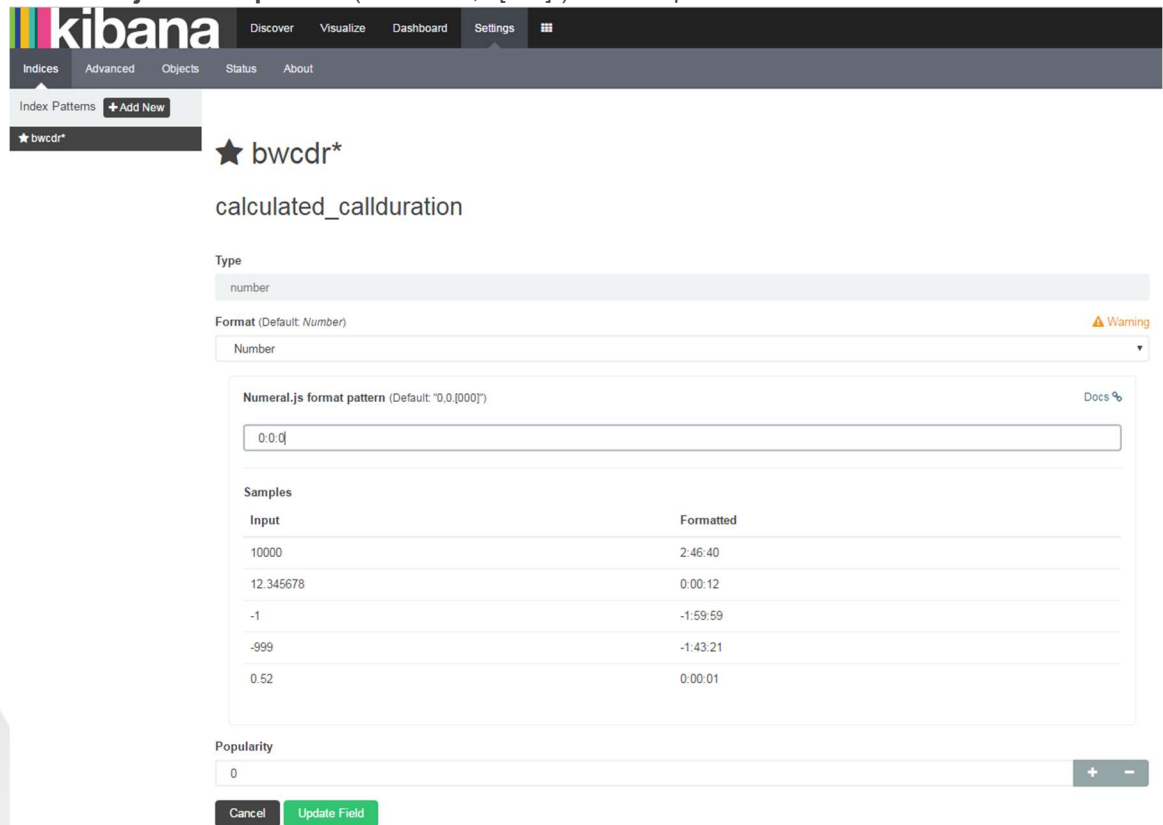
### 3. Change calculated\_callduration format (optional).

By default the calculated\_callduration will be displayed in seconds. To display in hours:minutes:seconds (hh:mm:ss):

- Click “Settings”, then “Indices”, and start entering “calcu” in filter box:

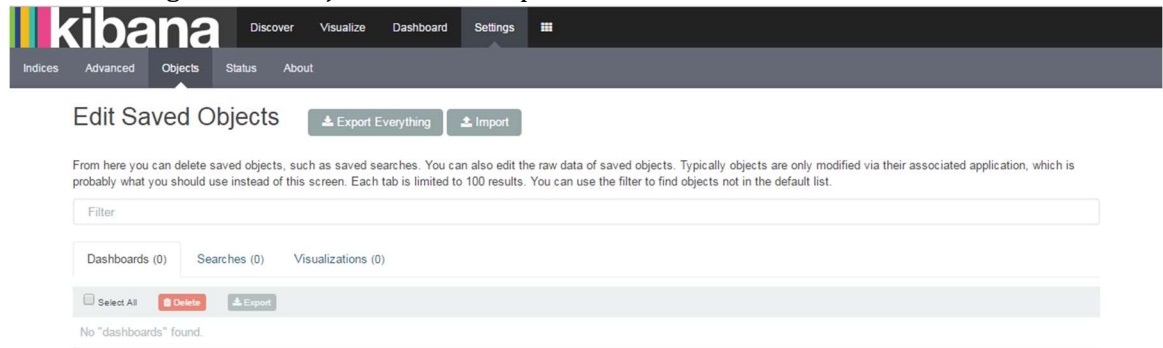


- Click the edit icon under “controls” and enter “0:0:0” in the edit box below “Numeral.js format pattern (Default: “0,0.[000]”)”. Click “Update Field”

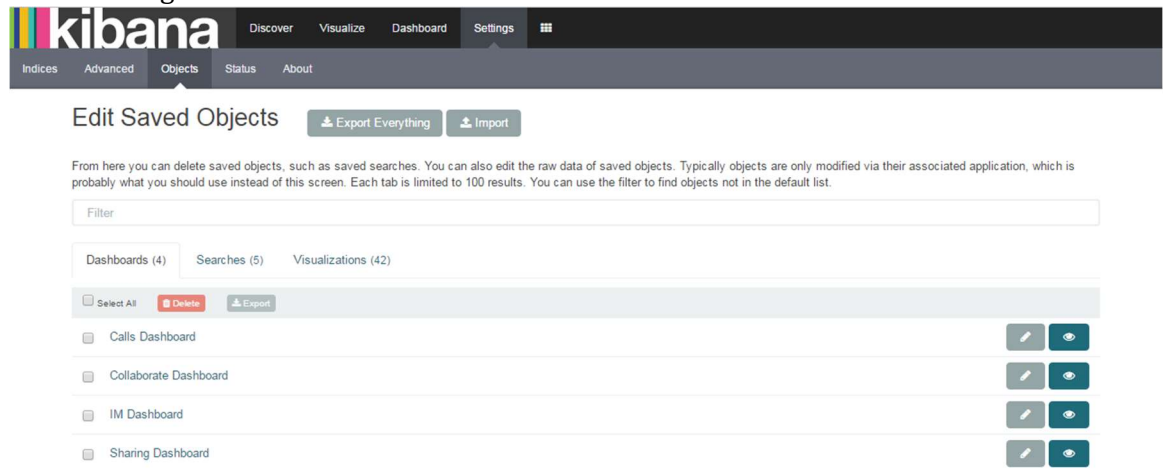


## 4. Import Dashboards

- Go to “Settings”, click “Objects”, Click “Import”

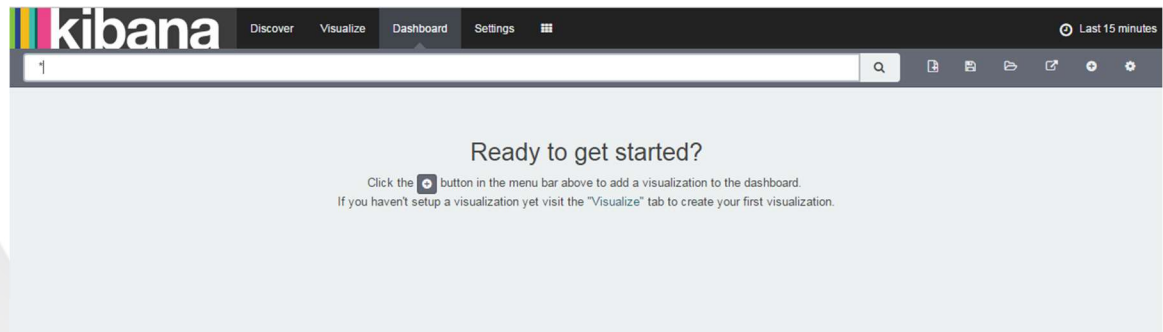


- Locate file “Broadworks Dashboards 1.0”, click Open. When import completes, the following screen should result:

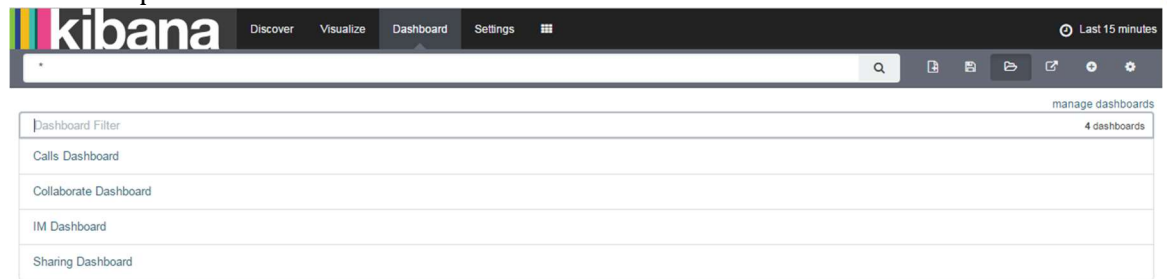


## 5. Start Dashboards

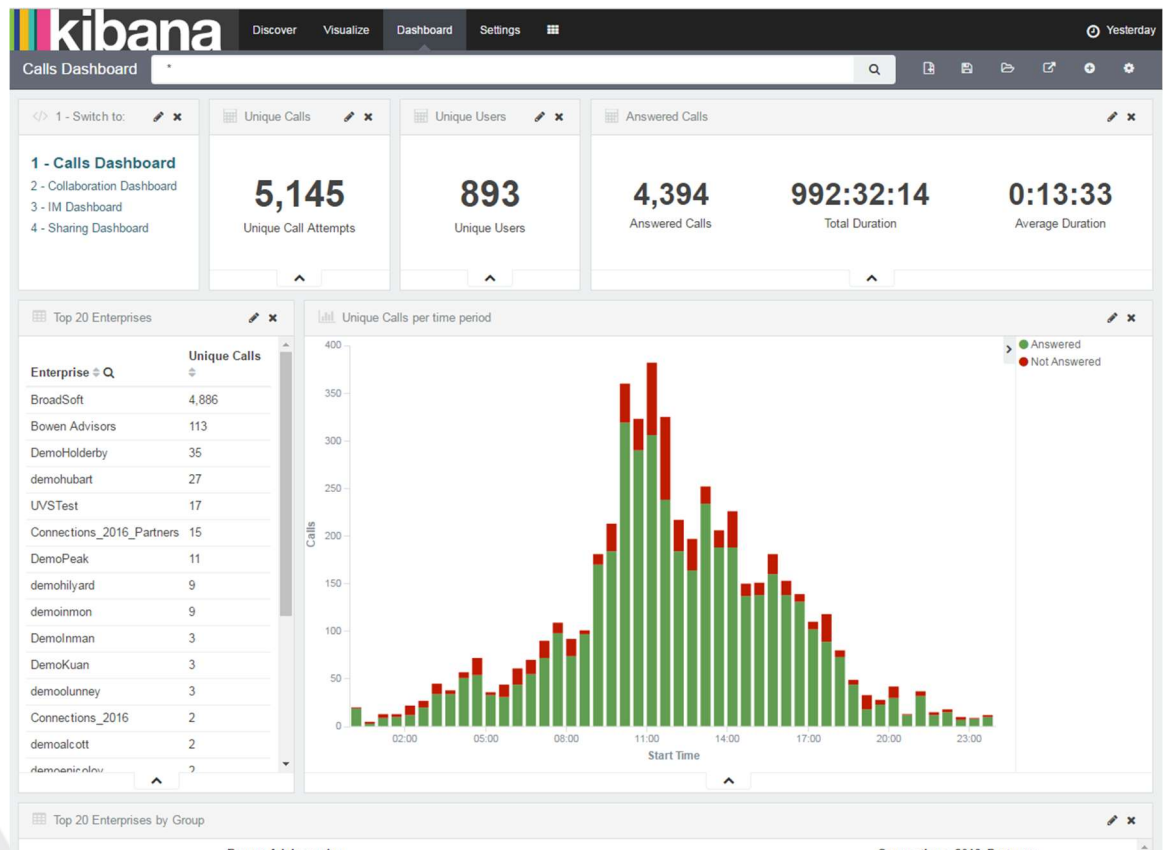
- Click “Dashboard”



- b. Click file open icon:



- c. Click “Calls Dashboard”



And you're done! You can switch dashboards by selecting it in the upper left menu.