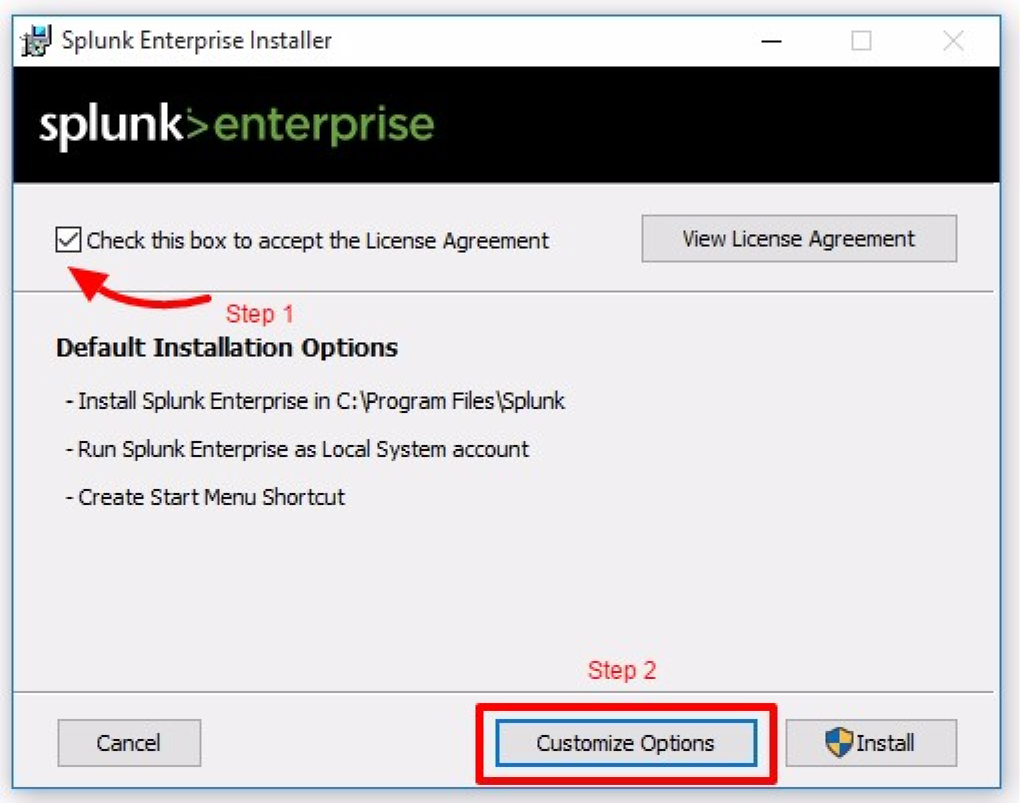
Chapter 1: Splunk in Action


Splunk Enterprise Installer

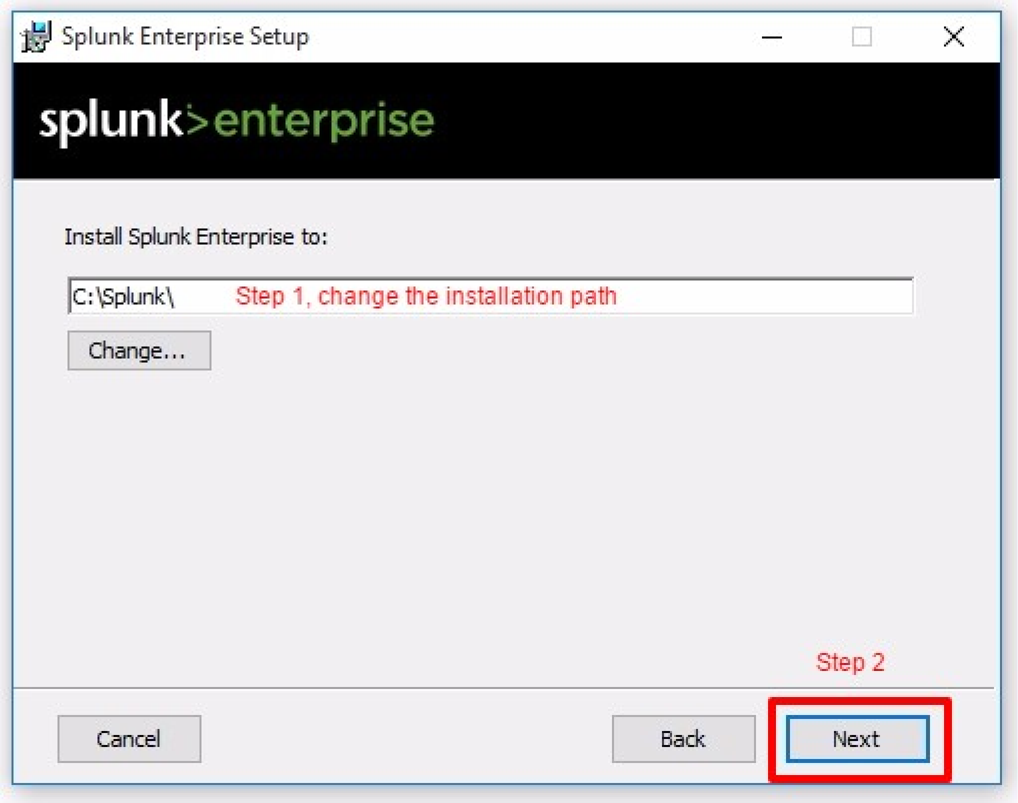
☑ Check this box to accept the License Agreement

Step 1

Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

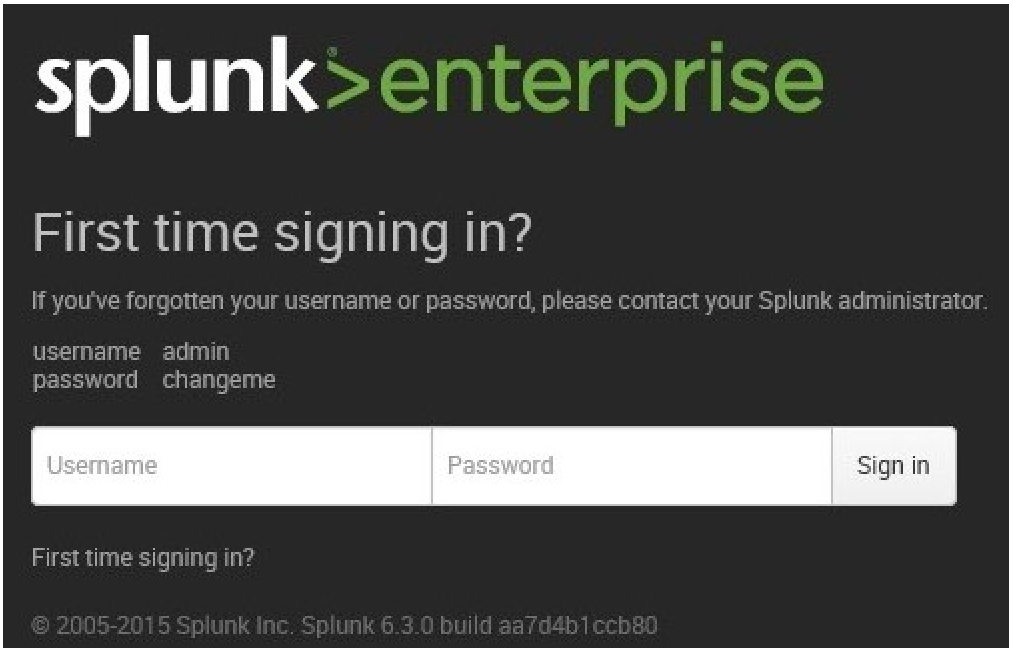
Step 2


Splunk Enterprise Setup

Install Splunk Enterprise to:

C:\Splunk\ Step 1, change the installation path

Step 2

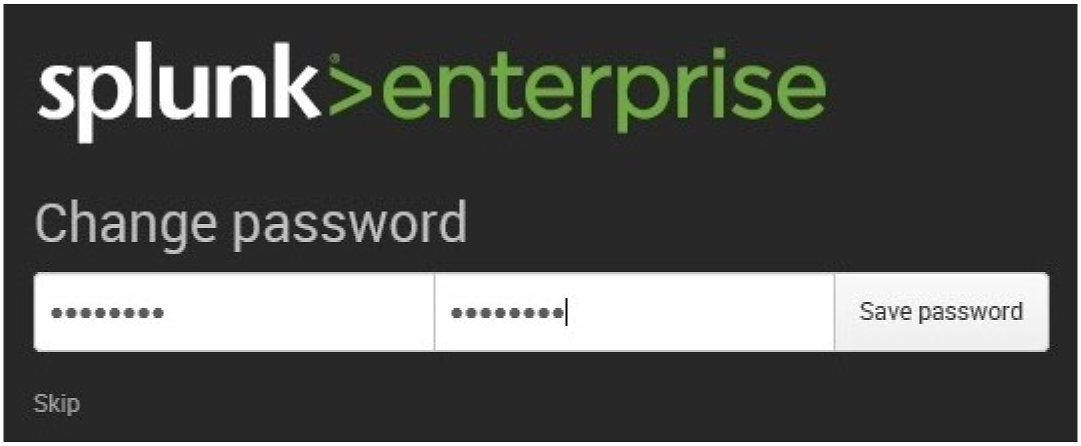


First time signing in?

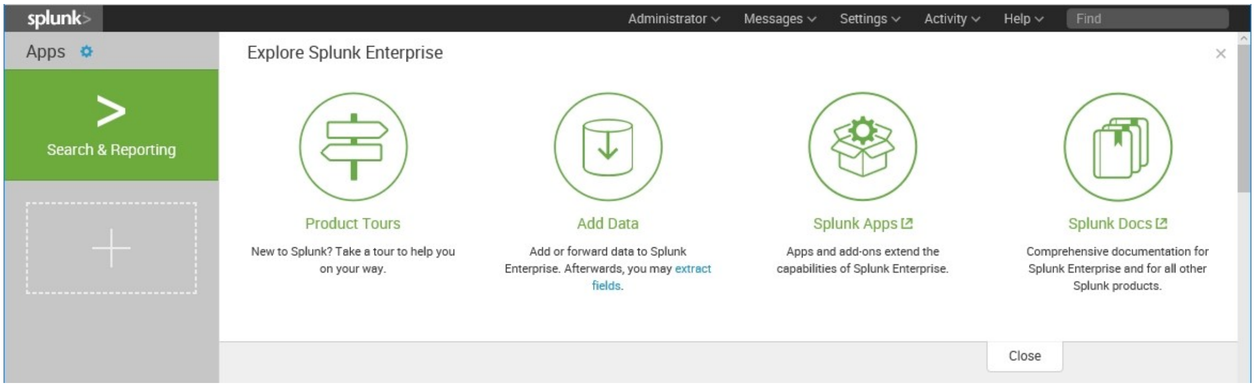
If you've forgotten your username or password, please contact your Splunk administrator.

username	admin
password	changeme

© 2005-2015 Splunk Inc. Splunk 6.3.0 build aa7d4b1ccb80



Change password



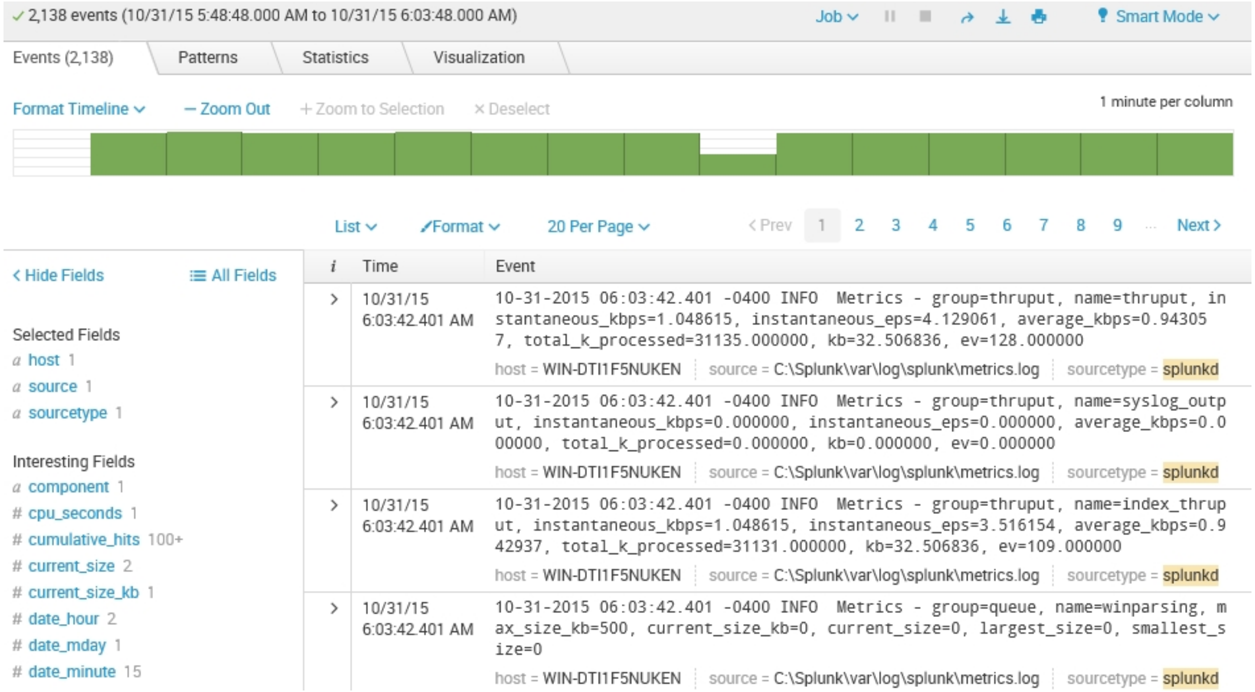
Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

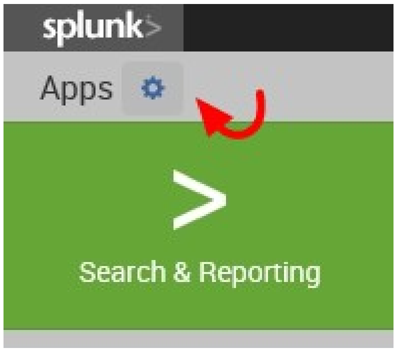


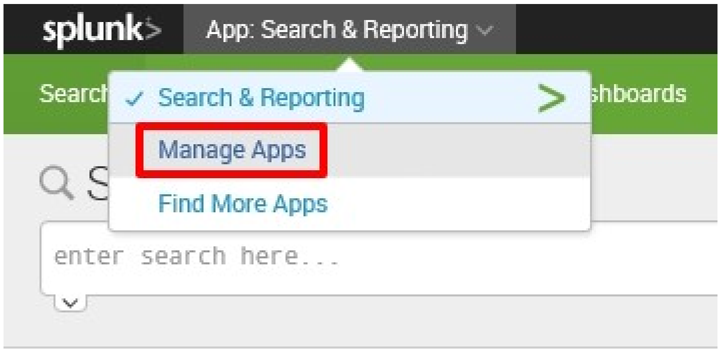
✓ 2,138 events (10/31/15 5:48:48.000 AM to 10/31/15 6:03:48.000 AM)

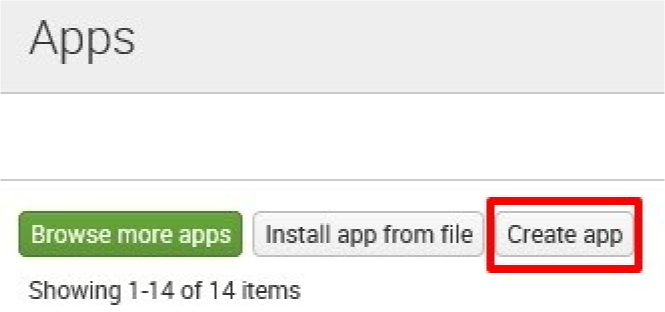
Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
a component 1
# cpu_seconds 1
# cumulative_hits 100+
# current_size 2
# current_size_kb 1
# date_hour 2
# date_mday 1
# date_minute 15

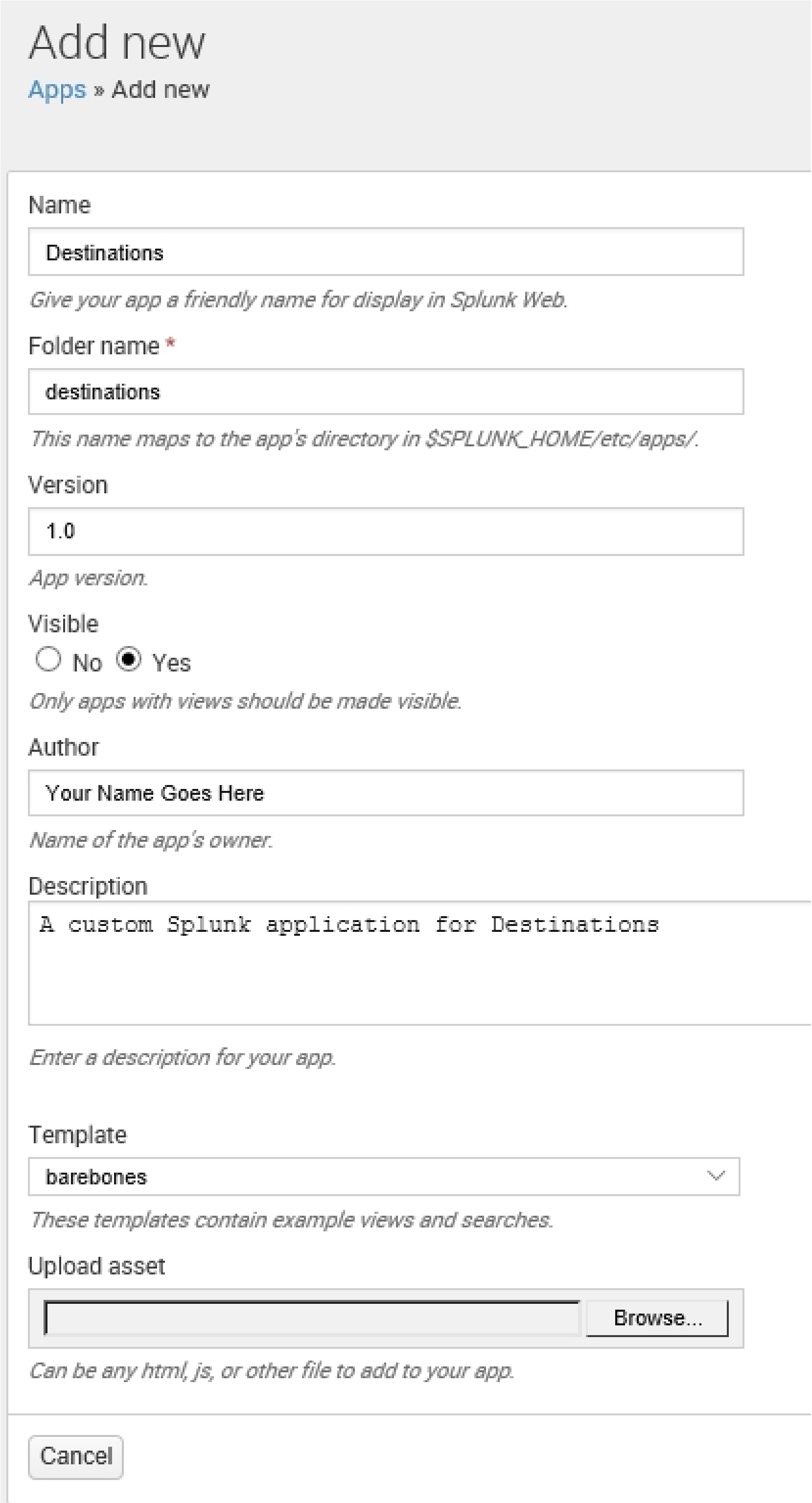
Time	Event
10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=thruput, instantaneous_kbps=1.048615, instantaneous_eps=4.129061, average_kbps=0.943057, total_k_processed=31135.000000, kb=32.506836, ev=128.000000 host = WIN-DTI1F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=syslog_output, instantaneous_kbps=0.000000, instantaneous_eps=0.000000, average_kbps=0.000000, total_k_processed=0.000000, kb=0.000000, ev=0.000000 host = WIN-DTI1F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=index_thruput, instantaneous_kbps=1.048615, instantaneous_eps=3.516154, average_kbps=0.942937, total_k_processed=31131.000000, kb=32.506836, ev=109.000000 host = WIN-DTI1F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=queue, name=winparsing, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=0, smallest_size=0 host = WIN-DTI1F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd







Apps
Browse more apps
Install app from file
Create app
Showing 1-14 of 14 items



Add new

Apps » Add new

Name

Destinations

Give your app a friendly name for display in Splunk Web.

Folder name *

destinations

This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.

Version

1.0

App version.

Visible

○ No ● Yes

Only apps with views should be made visible.

Author

Your Name Goes Here

Name of the app's owner.

Description

```
A custom Splunk application for Destinations
```

Enter a description for your app.

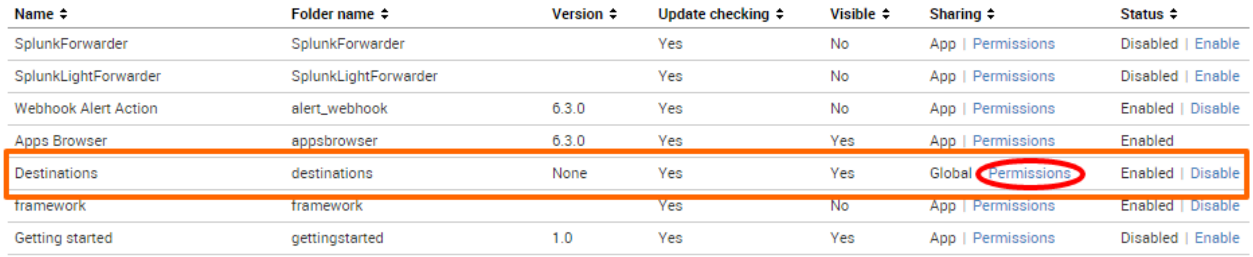
Template

barebones

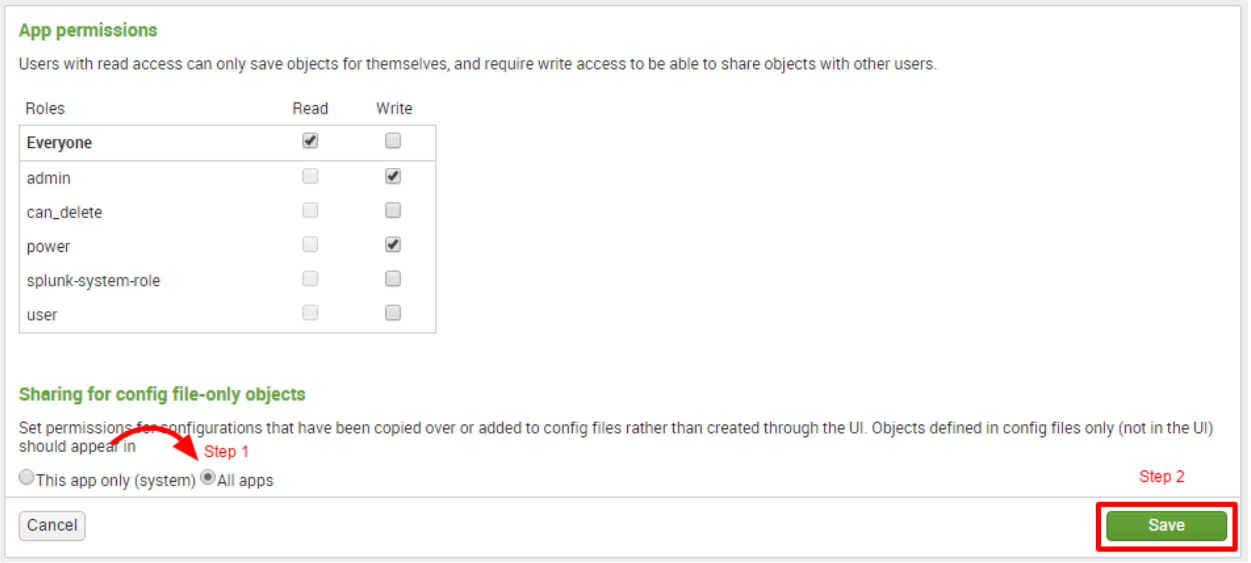
These templates contain example views and searches.

Upload asset

Can be any html, js, or other file to add to your app.



Name ⬍	Folder name ⬍	Version ⬍	Update checking ⬍	Visible ⬍	Sharing ⬍	Status ⬍
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable
Webhook Alert Action	alert_webhook	6.3.0	Yes	No	App | Permissions	Enabled | Disable
Apps Browser	appsbrowser	6.3.0	Yes	Yes	App | Permissions	Enabled
Destinations	destinations	None	Yes	Yes	Global | Permissions	Enabled | Disable
framework	framework		Yes	No	App | Permissions	Enabled | Disable
Getting started	gettingstarted	1.0	Yes	Yes	App | Permissions	Disabled | Enable



App permissions

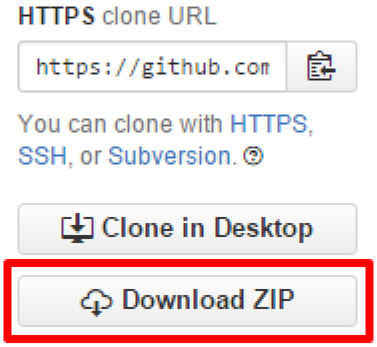
Users with read access can only save objects for themselves, and require write access to be able to share objects with other users.

Roles	Read	Write
Everyone	☑	☐
admin	☐	☑
can_delete	☐	☐
power	☐	☑
splunk-system-role	☐	☐
user	☐	☐

Sharing for config file-only objects

Set permissions for configurations that have been copied over or added to config files rather than created through the UI. Objects defined in config files only (not in the UI) should appear in

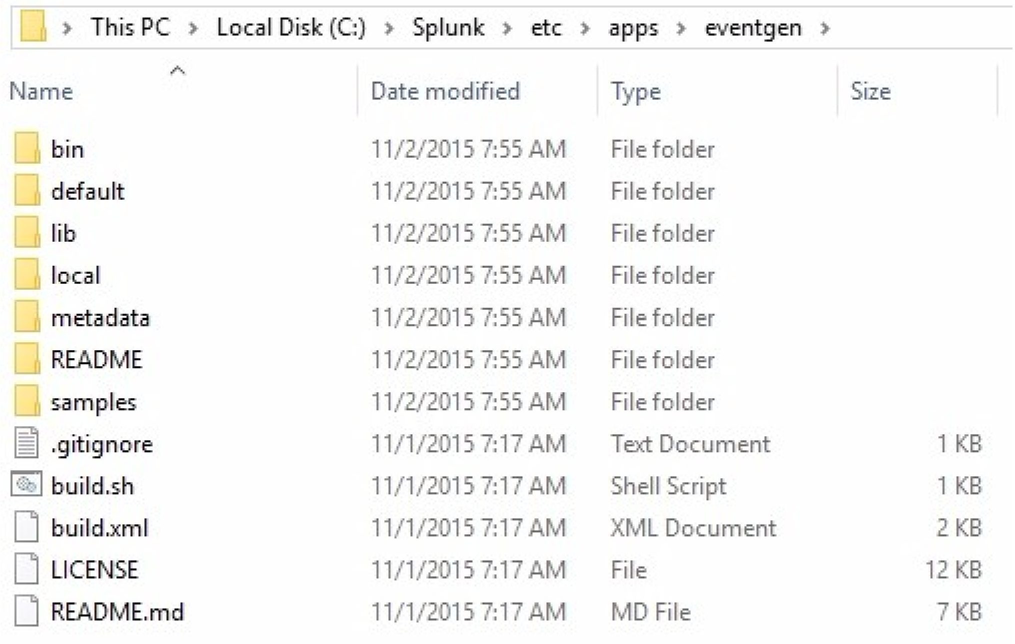
○ This app only (system) ● All apps



HTTPS clone URL

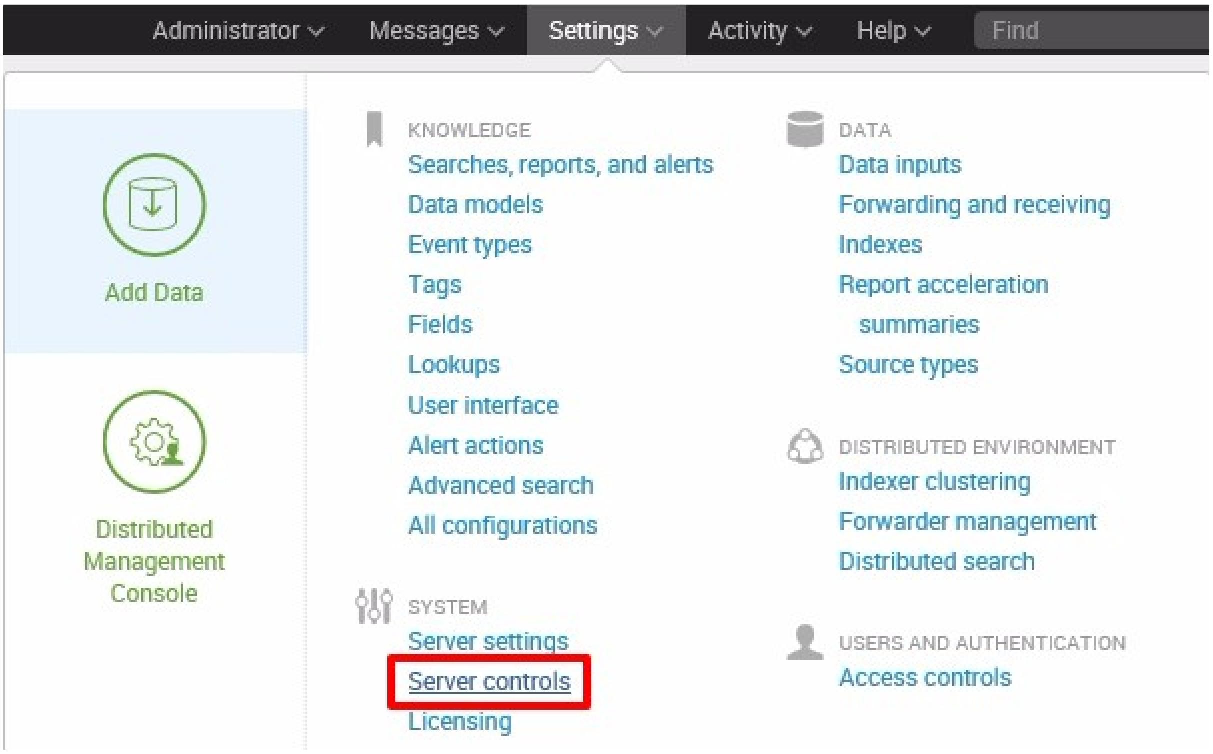
https://github.com

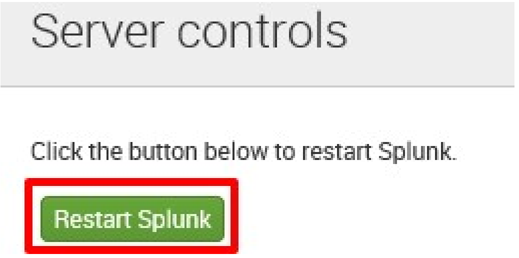
You can clone with HTTPS, SSH, or Subversion.



This PC › Local Disk (C:) › Splunk › etc › apps › eventgen ›

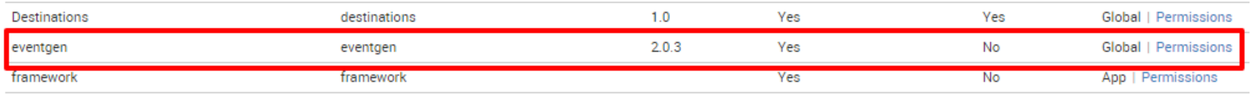
Name	Date modified	Type	Size
bin	11/2/2015 7:55 AM	File folder	
default	11/2/2015 7:55 AM	File folder	
lib	11/2/2015 7:55 AM	File folder	
local	11/2/2015 7:55 AM	File folder	
metadata	11/2/2015 7:55 AM	File folder	
README	11/2/2015 7:55 AM	File folder	
samples	11/2/2015 7:55 AM	File folder	
.gitignore	11/1/2015 7:17 AM	Text Document	1 KB
build.sh	11/1/2015 7:17 AM	Shell Script	1 KB
build.xml	11/1/2015 7:17 AM	XML Document	2 KB
LICENSE	11/1/2015 7:17 AM	File	12 KB
README.md	11/1/2015 7:17 AM	MD File	7 KB



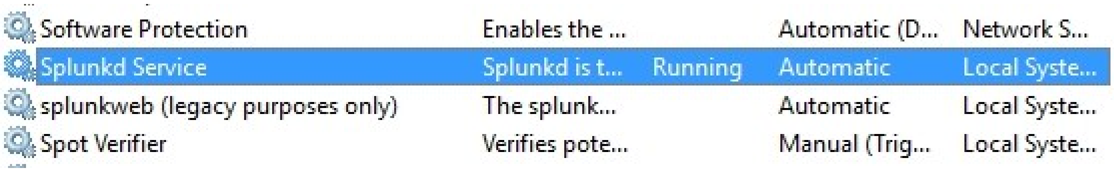


Server controls

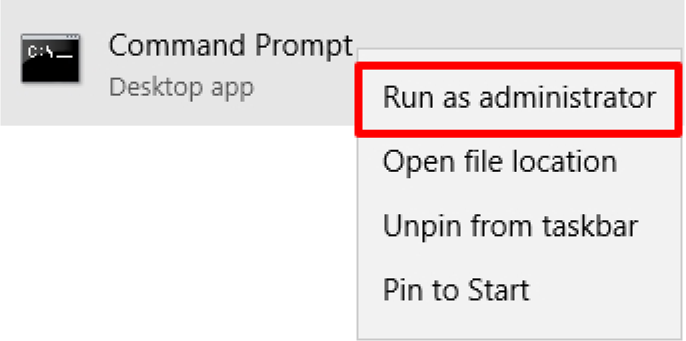
Click the button below to restart Splunk.

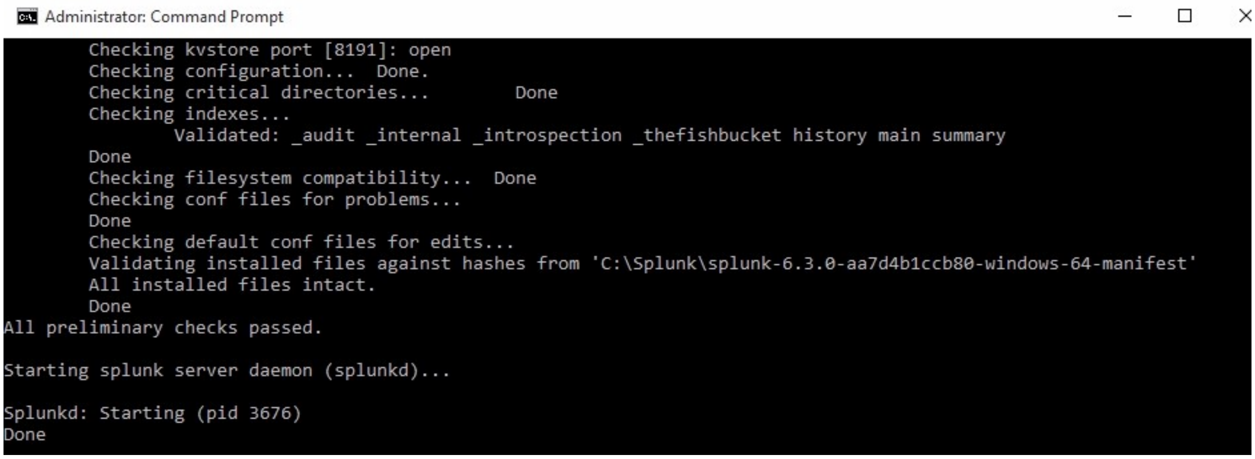


Destinations	destinations	1.0	Yes	Yes	Global | Permissions
eventgen	eventgen	2.0.3	Yes	No	Global | Permissions
framework	framework		Yes	No	App | Permissions

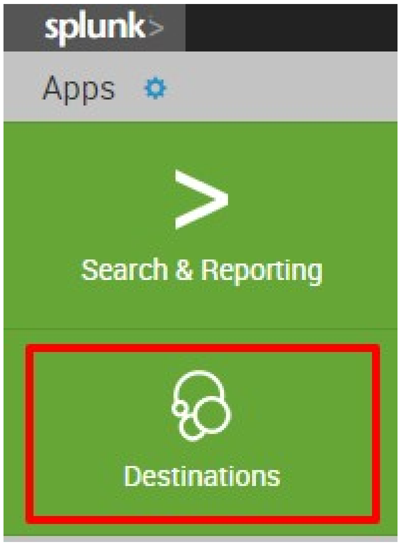


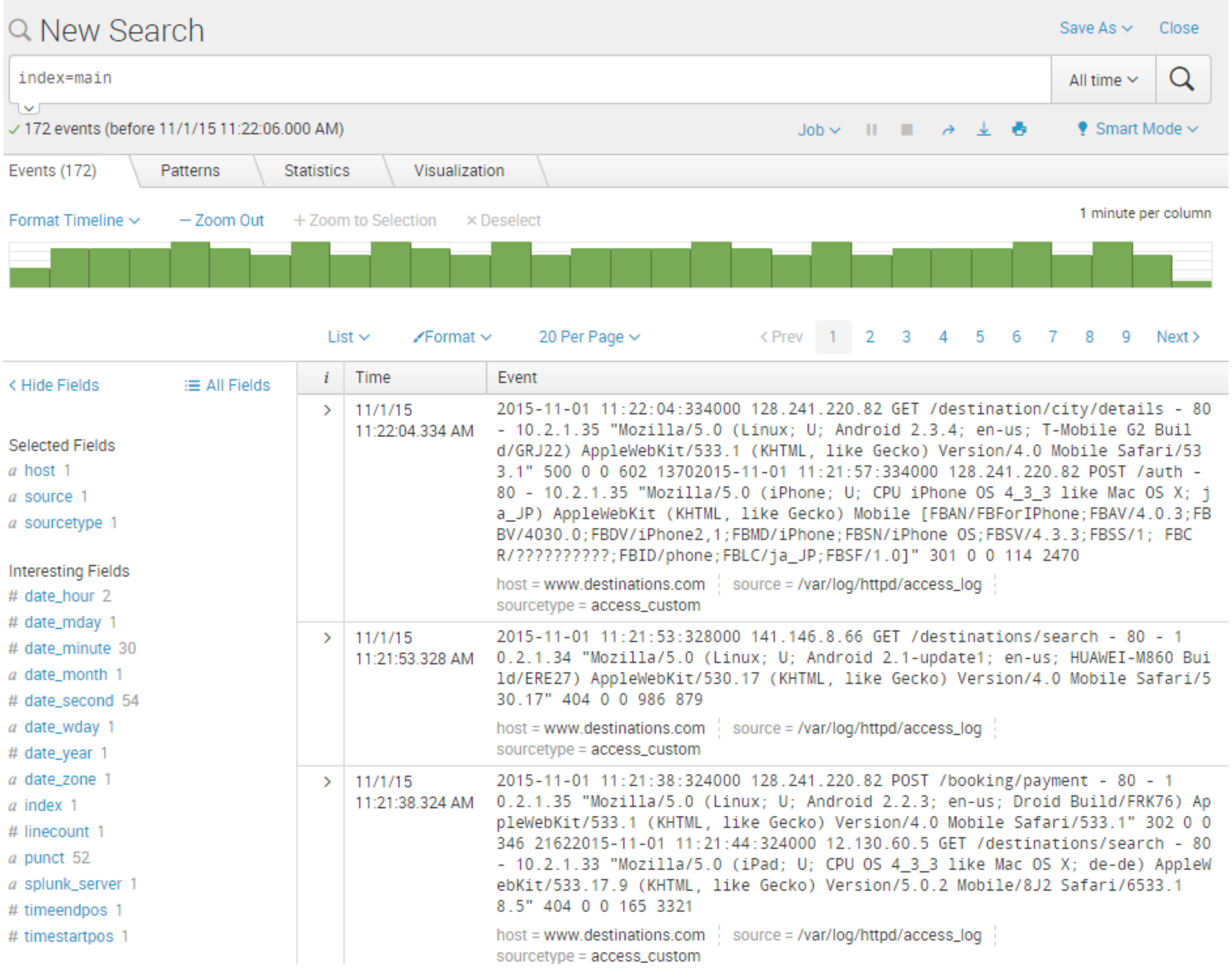
Software Protection	Enables the ...		Automatic (D...	Network S...
Splunkd Service	Splunkd is t...	Running	Automatic	Local Syste...
splunkweb (legacy purposes only)	The splunk...		Automatic	Local Syste...
Spot Verifier	Verifies pote...		Manual (Trig...	Local Syste...





```
        Checking kvstore port [8191]: open
        Checking configuration...  Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspection _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from 'C:\Splunk\splunk-6.3.0-aa7d4b1ccb80-windows-64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Splunkd: Starting (pid 3676)
Done
```





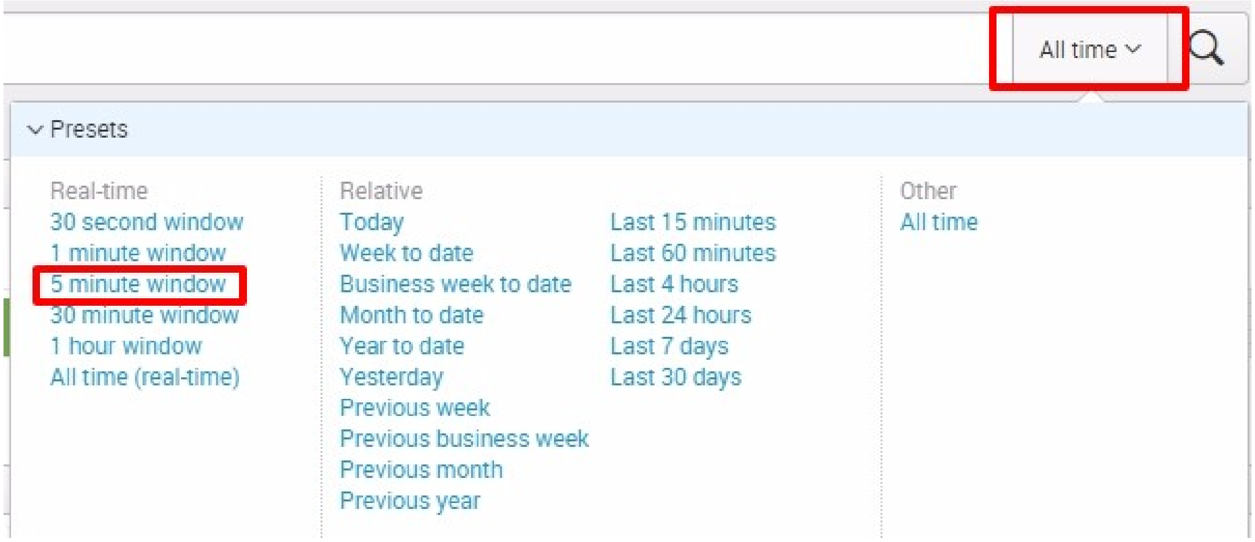
```
index=main
```

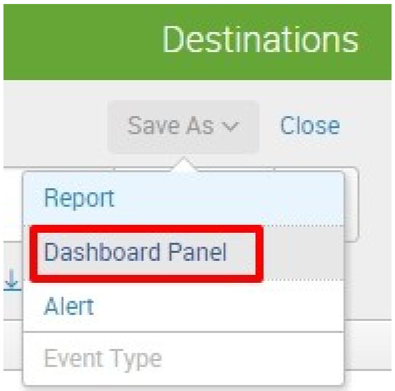
✓ 172 events (before 11/1/15 11:22:06.000 AM)

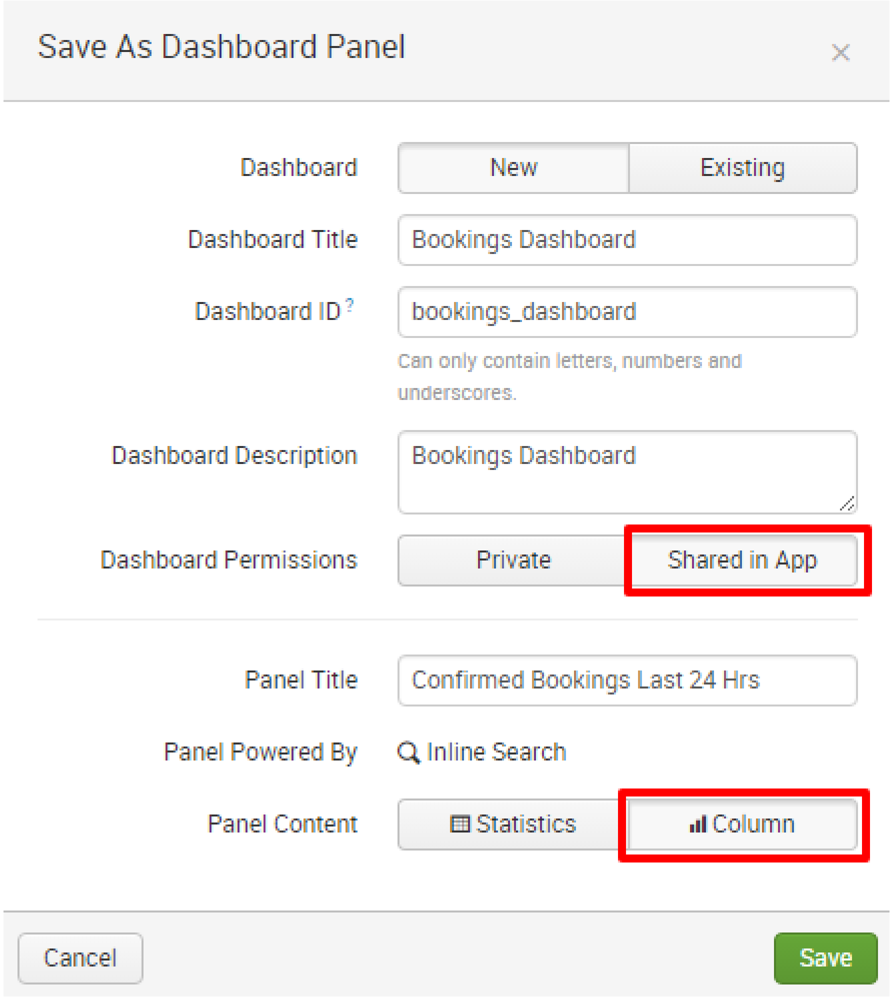
Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
# date_hour 2
# date_mday 1
# date_minute 30
a date_month 1
# date_second 54
a date_wday 1
# date_year 1
a date_zone 1
a index 1
# linecount 1
a punct 52
a splunk_server 1
# timeendpos 1
# timestartpos 1

Time	Event
11/1/15 11:22:04.334 AM	2015-11-01 11:22:04:334000 128.241.220.82 GET /destination/city/details - 80 - 10.2.1.35 "Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; T-Mobile G2 Build/GRJ22) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" 500 0 0 602 13702015-11-01 11:21:57:334000 128.241.220.82 POST /auth - 80 - 10.2.1.35 "Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3_3 like Mac OS X; ja_JP) AppleWebKit (KHTML, like Gecko) Mobile [FBAN/FBForIPhone;FBAV/4.0.3;FBBV/4030.0;FBDV/iPhone2,1;FBMD/iPhone;FBSN/iPhone OS;FBSV/4.3.3;FBSS/1; FBCR/??????????;FBID/phone;FBLC/ja_JP;FBSF/1.0]" 301 0 0 114 2470 host = www.destinations.com source = /var/log/httpd/access_log sourcetype = access_custom
11/1/15 11:21:53.328 AM	2015-11-01 11:21:53:328000 141.146.8.66 GET /destinations/search - 80 - 10.2.1.34 "Mozilla/5.0 (Linux; U; Android 2.1-update1; en-us; HUAWEI-M860 Build/ERE27) AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Mobile Safari/530.17" 404 0 0 986 879 host = www.destinations.com source = /var/log/httpd/access_log sourcetype = access_custom
11/1/15 11:21:38.324 AM	2015-11-01 11:21:38:324000 128.241.220.82 POST /booking/payment - 80 - 10.2.1.35 "Mozilla/5.0 (Linux; U; Android 2.2.3; en-us; Droid Build/FRK76) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" 302 0 0 346 21622015-11-01 11:21:44:324000 12.130.60.5 GET /destinations/search - 80 - 10.2.1.33 "Mozilla/5.0 (iPad; U; CPU OS 4_3_3 like Mac OS X; de-de) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8J2 Safari/6533.18.5" 404 0 0 165 3321 host = www.destinations.com source = /var/log/httpd/access_log sourcetype = access_custom


All time
Presets
Real-time
30 second window
1 minute window
5 minute window
30 minute window
1 hour window
All time (real-time)
Relative
Today
Week to date
Business week to date
Month to date
Year to date
Yesterday
Previous week
Previous business week
Previous month
Previous year
Last 15 minutes
Last 60 minutes
Last 4 hours
Last 24 hours
Last 7 days
Last 30 days
Other
All time


Destinations
Save As
Close
Report
Dashboard Panel
Alert
Event Type



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Bookings Dashboard

Dashboard ID: bookings_dashboard

Can only contain letters, numbers and underscores.

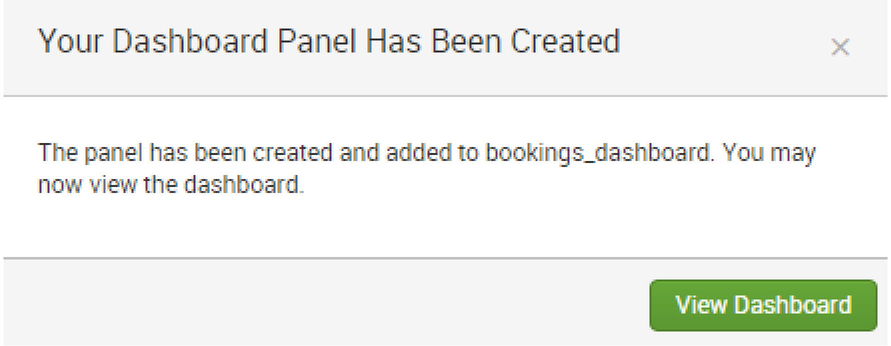
Dashboard Description: Bookings Dashboard

Dashboard Permissions: Private | Shared in App

Panel Title: Confirmed Bookings Last 24 Hrs

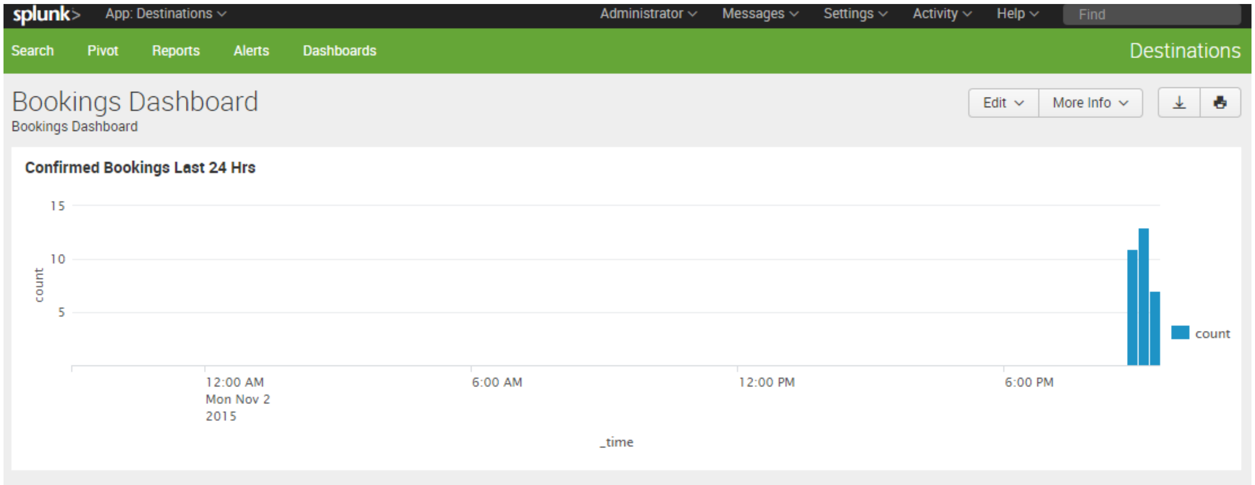
Panel Powered By: Inline Search

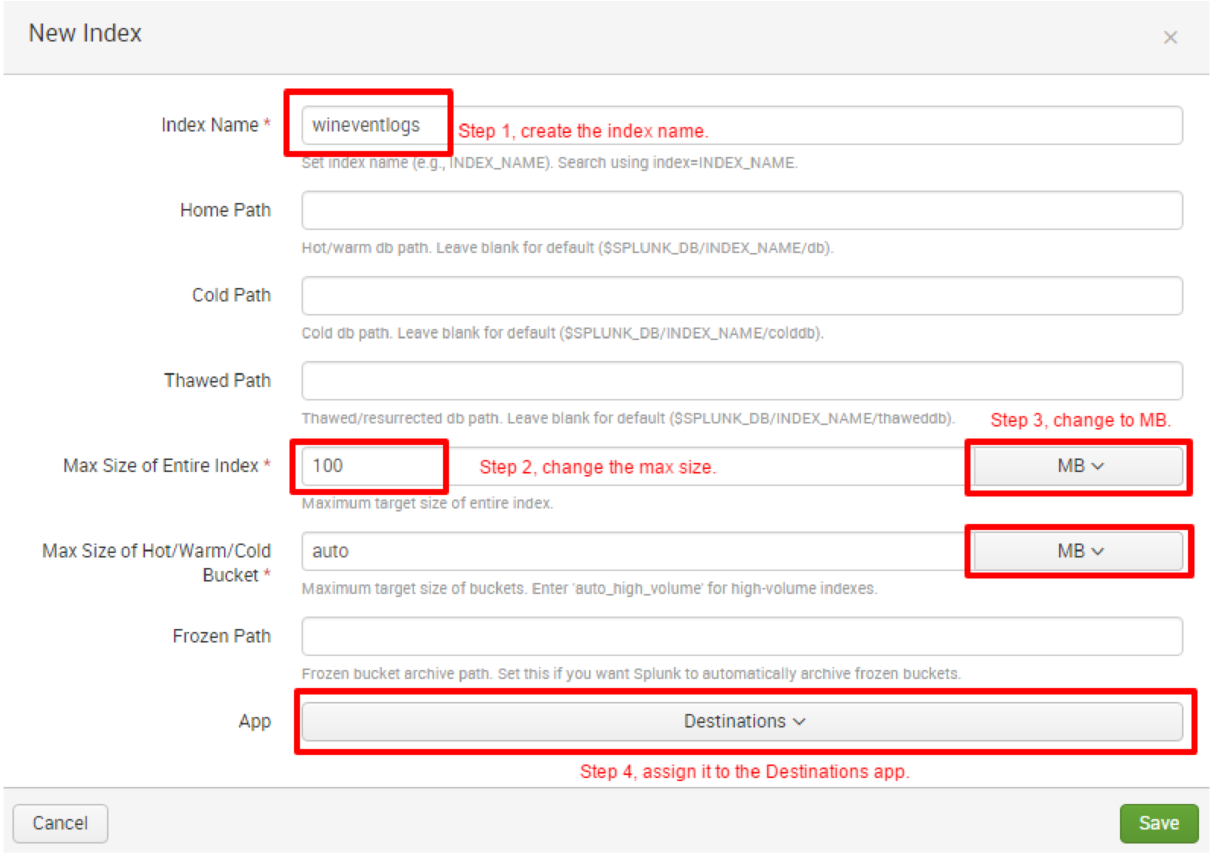
Panel Content: Statistics | Column



Your Dashboard Panel Has Been Created

The panel has been created and added to bookings_dashboard. You may now view the dashboard.


splunk>
App: Destinations
Administrator
Messages
Settings
Activity
Help
Find
Search
Pivot
Reports
Alerts
Dashboards
Destinations
Bookings Dashboard
Bookings Dashboard
Edit
More Info
Confirmed Bookings Last 24 Hrs
15
10
5
count
count
12:00 AM
Mon Nov 2
2015
6:00 AM
12:00 PM
6:00 PM
_time



New Index

Index Name * wineventlogs

Step 1, create the index name.

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Home Path

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path

Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Step 3, change to MB.

Max Size of Entire Index * 100 MB

Step 2, change the max size.

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket * auto MB

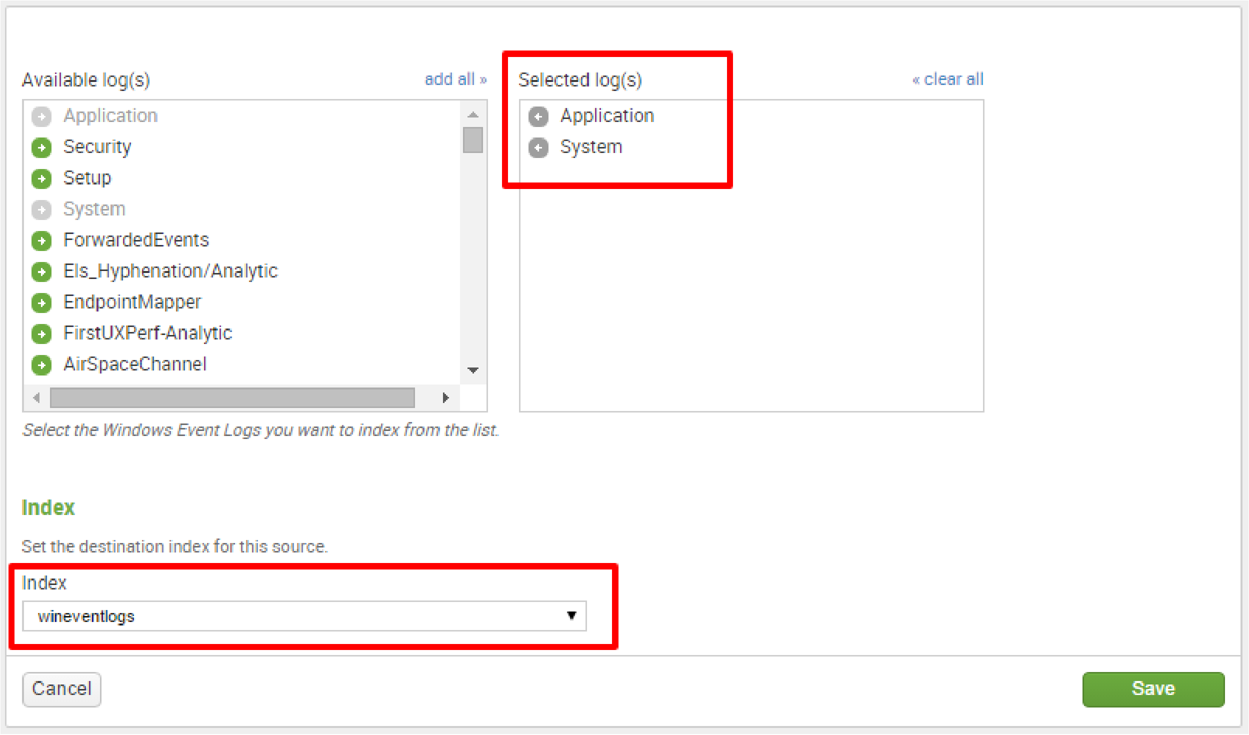
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Destinations

Step 4, assign it to the Destinations app.



Available log(s)

- Application
- Security
- Setup
- System
- ForwardedEvents
- Els_Hyphenation/Analytic
- EndpointMapper
- FirstUXPerf-Analytic
- AirSpaceChannel

Selected log(s)

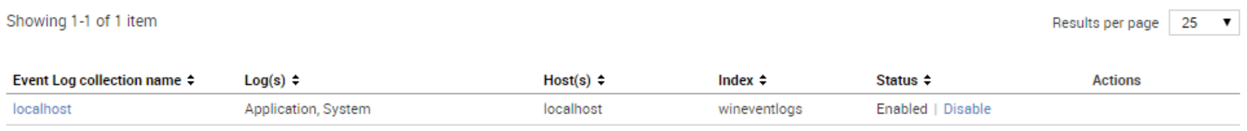
- Application
- System

Select the Windows Event Logs you want to index from the list.

Index

Set the destination index for this source.

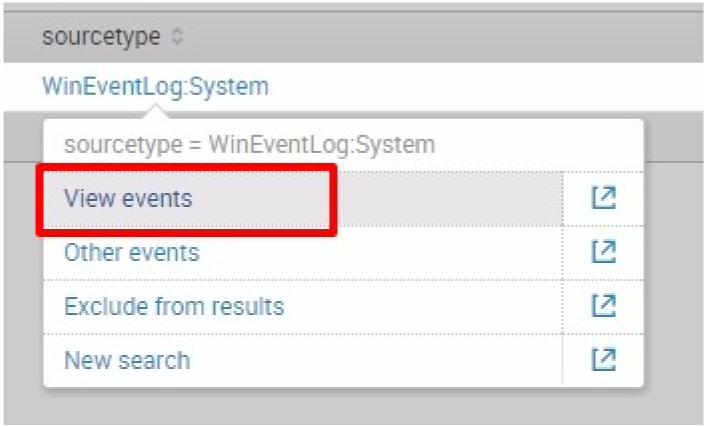
Index: wineventlogs

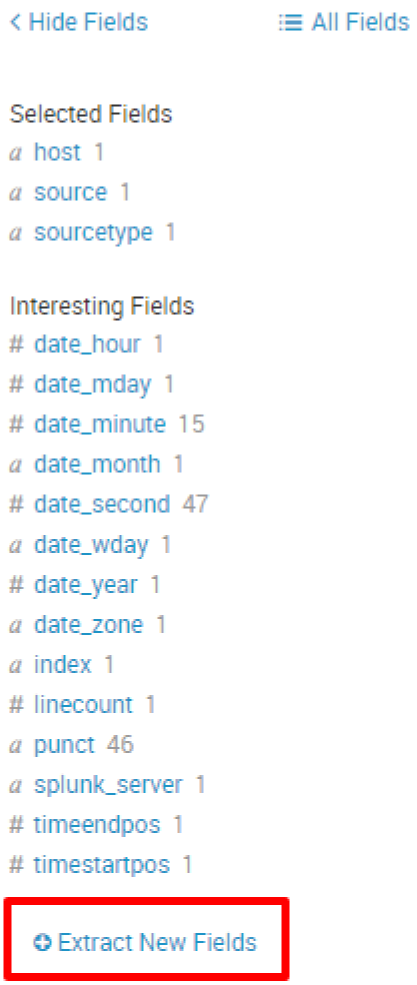


Showing 1-1 of 1 item

Results per page 25 ▼

Event Log collection name ⬍	Log(s) ⬍	Host(s) ⬍	Index ⬍	Status ⬍	Actions
localhost	Application, System	localhost	wineventlogs	Enabled | Disable	





< Hide Fields ☰ All Fields

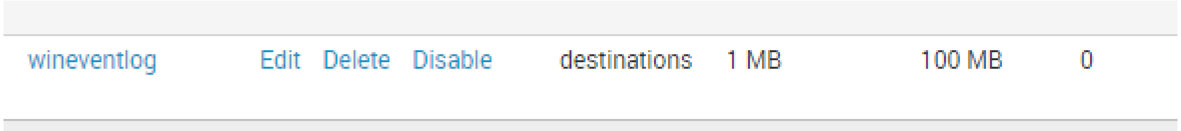
Selected Fields

a	host	1
a	source	1
a	sourcetype	1

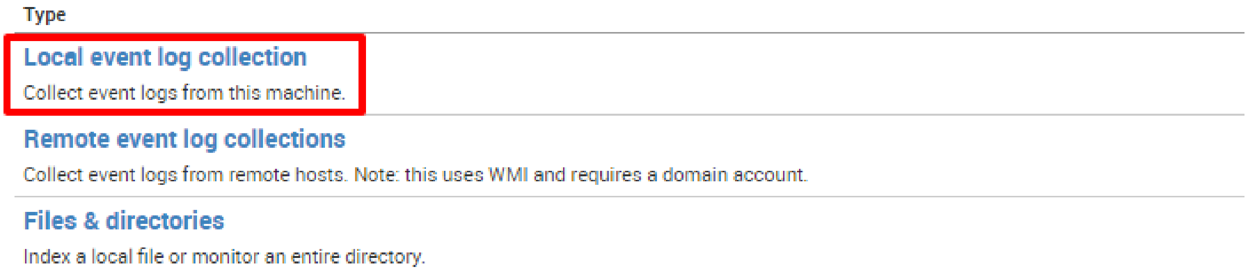
Interesting Fields

#	date_hour	1
#	date_mday	1
#	date_minute	15
a	date_month	1
#	date_second	47
a	date_wday	1
#	date_year	1
a	date_zone	1
a	index	1
#	linecount	1
a	punct	46
a	splunk_server	1
#	timeendpos	1
#	timestartpos	1

⊕ Extract New Fields



wineventlog	Edit Delete Disable	destinations	1 MB	100 MB	0

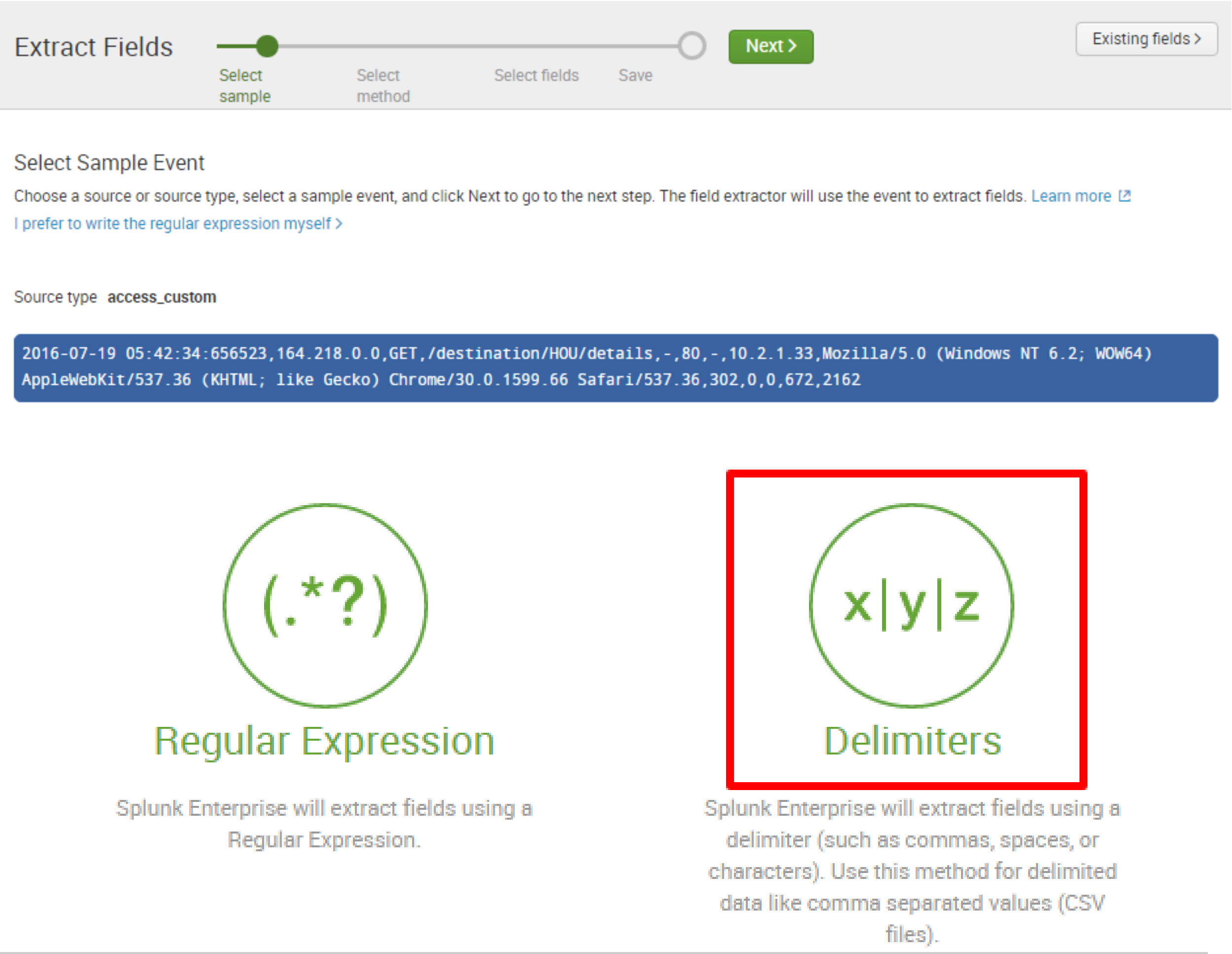


Type

Local event log collection
Collect event logs from this machine.

Remote event log collections
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & directories
Index a local file or monitor an entire directory.



Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. Learn more

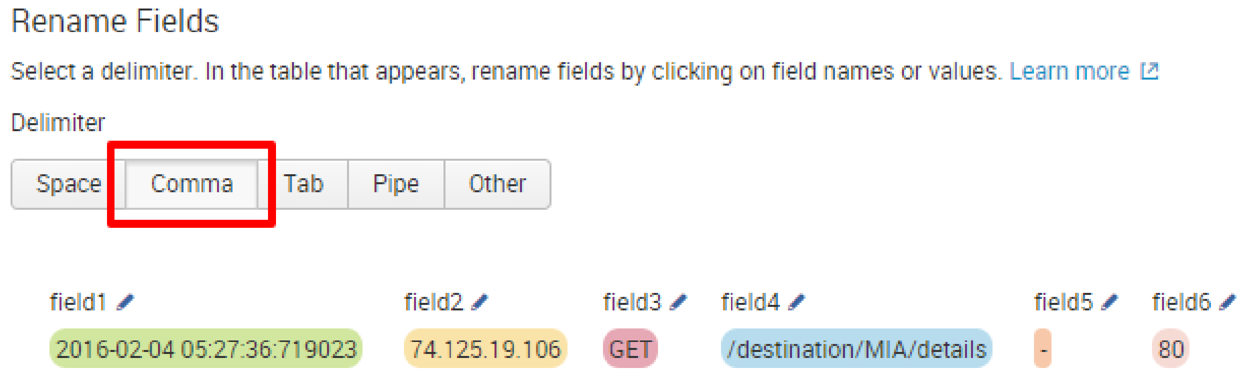
I prefer to write the regular expression myself >

Source type **access_custom**

```
2016-07-19 05:42:34:656523,164.218.0.0,GET,/destination/HOU/details,-,80,-,10.2.1.33,Mozilla/5.0 (Windows NT 6.2; WOW64)
AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.66 Safari/537.36,302,0,0,672,2162
```

Splunk Enterprise will extract fields using a Regular Expression.

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

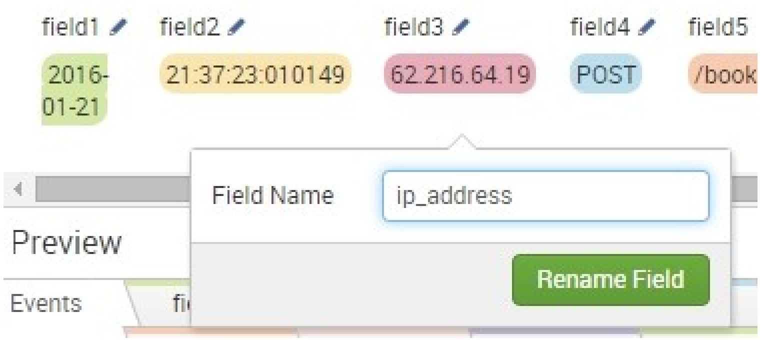


Rename Fields

Select a delimiter. In the table that appears, rename fields by clicking on field names or values. Learn more

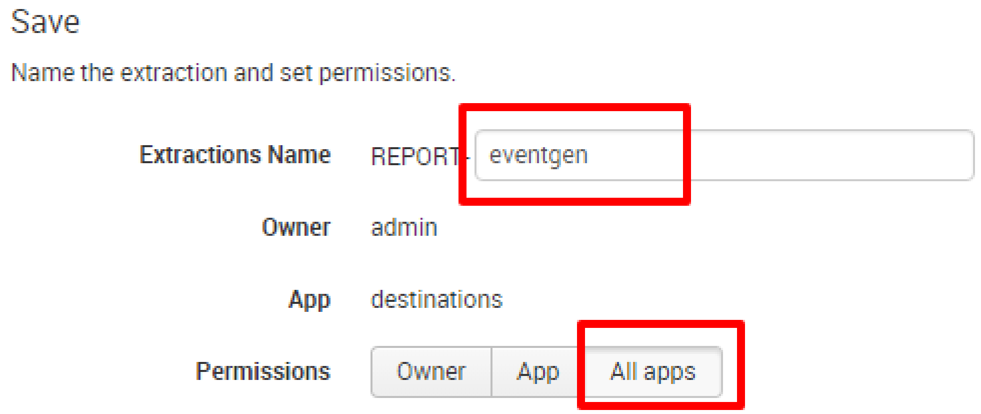
Delimiter

field1	field2	field3	field4	field5	field6
2016-02-04 05:27:36:719023	74.125.19.106	GET	/destination/MIA/details	-	80



field1	field2	field3	field4	field5
2016-01-21	21:37:23:010149	62.216.64.19	POST	/book

Field Name: ip_address



Save

Name the extraction and set permissions.

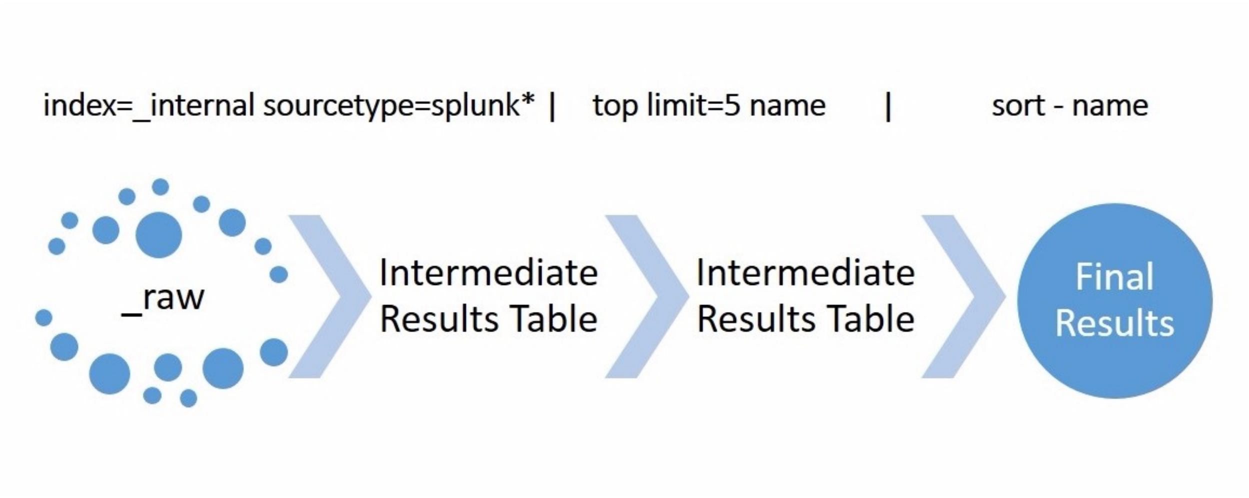
Extractions Name REPORT- eventgen

Owner admin

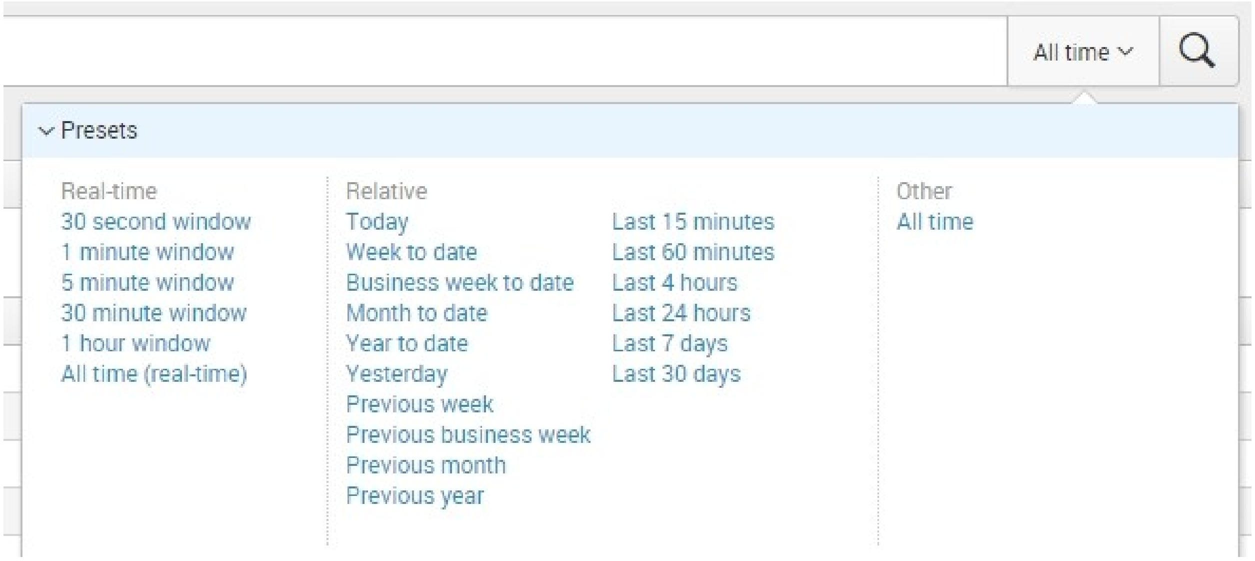
App destinations

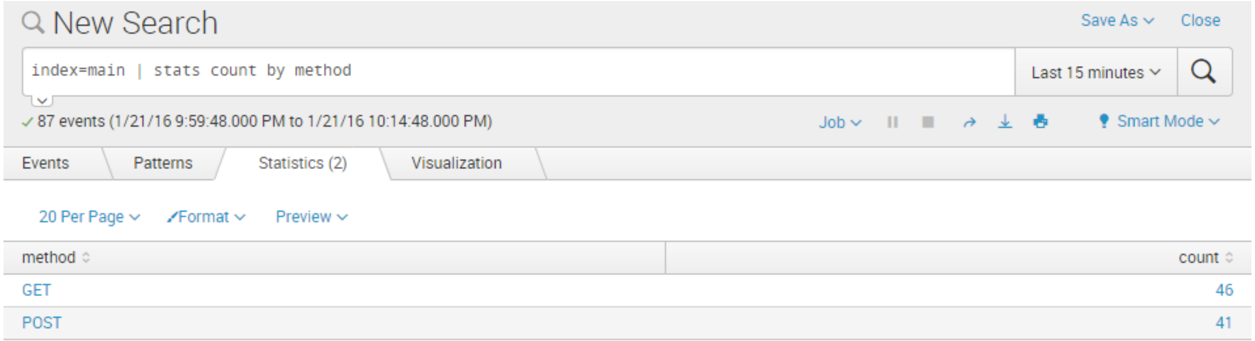
Permissions Owner | App | All apps

Chapter 3: Search Processing Language



```
index=_internal sourcetype=splunk* |   top limit=5 name   |   sort - name
```

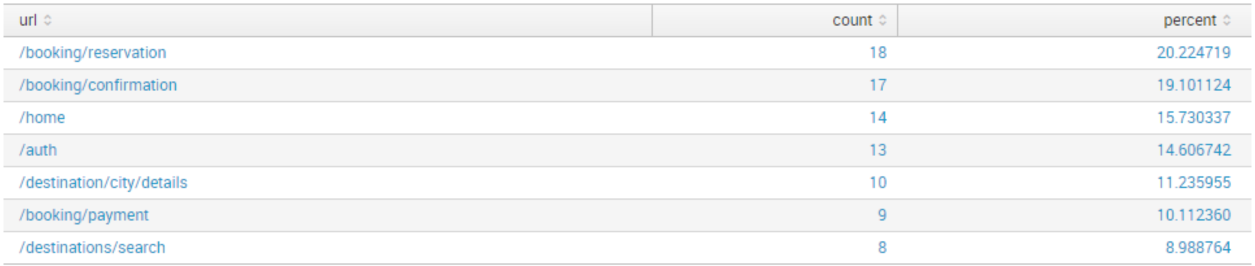




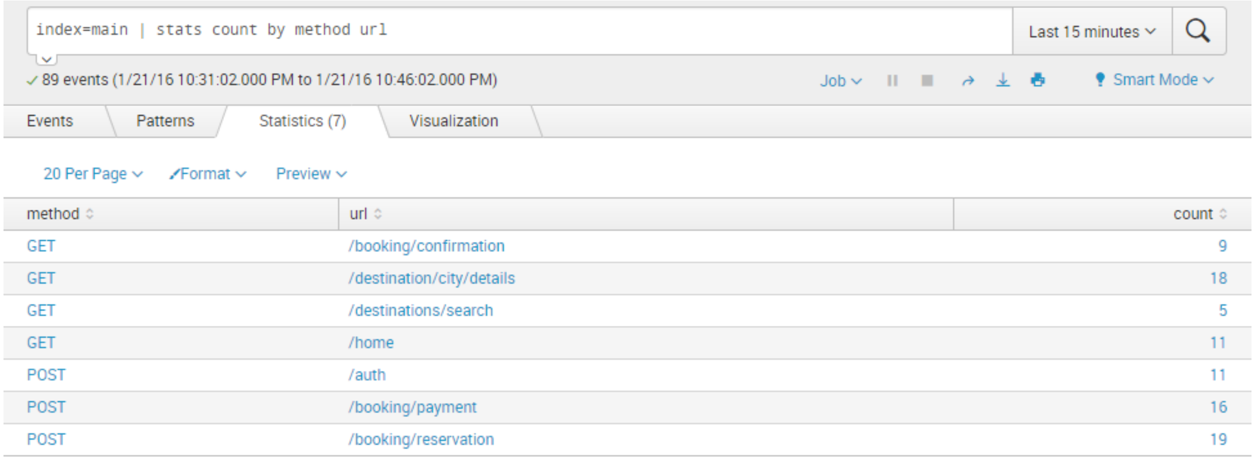
```
index=main | stats count by method
```

✓ 87 events (1/21/16 9:59:48.000 PM to 1/21/16 10:14:48.000 PM)

method	count
GET	46
POST	41



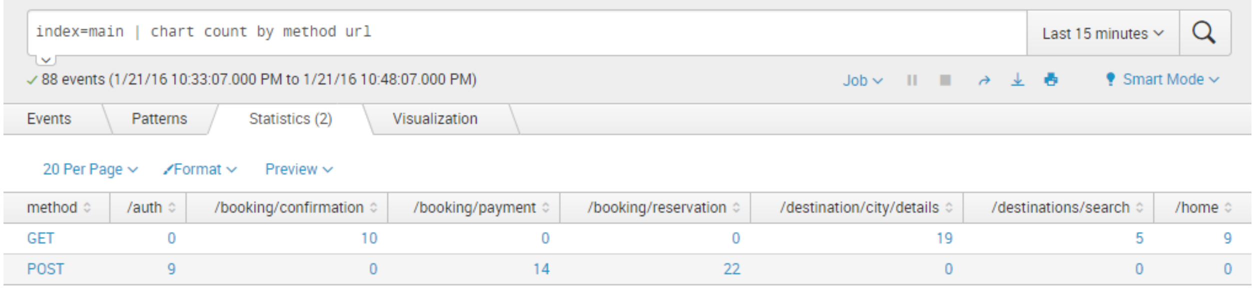
url	count	percent
/booking/reservation	18	20.224719
/booking/confirmation	17	19.101124
/home	14	15.730337
/auth	13	14.606742
/destination/city/details	10	11.235955
/booking/payment	9	10.112360
/destinations/search	8	8.988764



```
index=main | stats count by method url
```

✓ 89 events (1/21/16 10:31:02.000 PM to 1/21/16 10:46:02.000 PM)

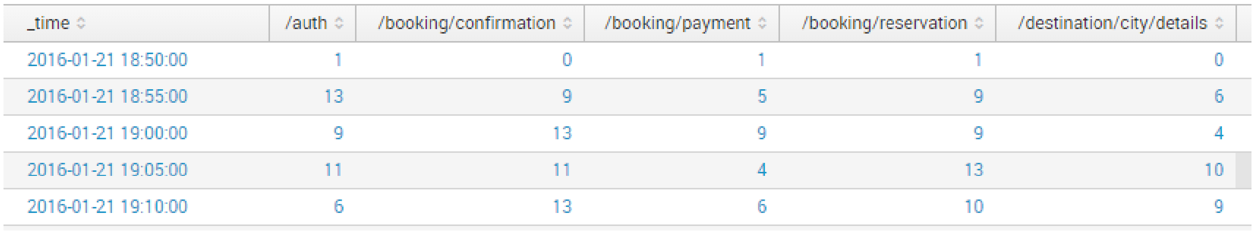
method	url	count
GET	/booking/confirmation	9
GET	/destination/city/details	18
GET	/destinations/search	5
GET	/home	11
POST	/auth	11
POST	/booking/payment	16
POST	/booking/reservation	19



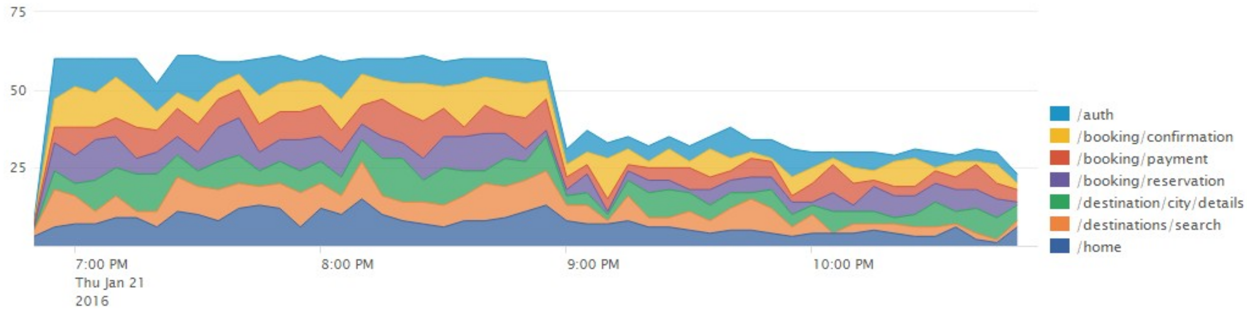
```
index=main | chart count by method url
```

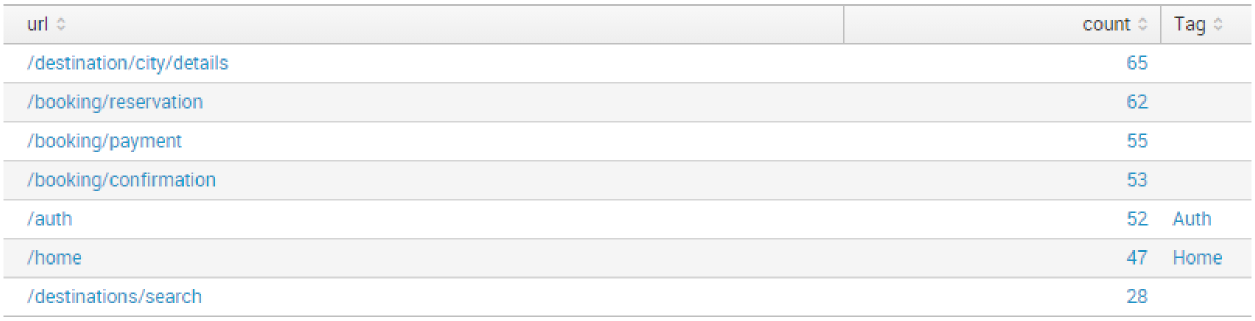
✓ 88 events (1/21/16 10:33:07.000 PM to 1/21/16 10:48:07.000 PM)

method	/auth	/booking/confirmation	/booking/payment	/booking/reservation	/destination/city/details	/destinations/search	/home
GET	0	10	0	0	19	5	9
POST	9	0	14	22	0	0	0

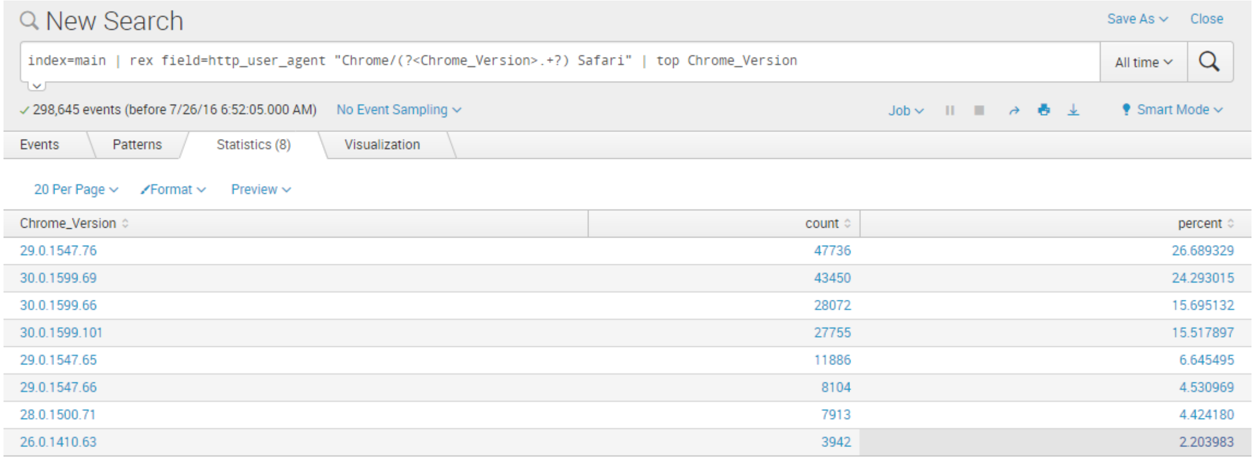


_time	/auth	/booking/confirmation	/booking/payment	/booking/reservation	/destination/city/details
2016-01-21 18:50:00	1	0	1	1	0
2016-01-21 18:55:00	13	9	5	9	6
2016-01-21 19:00:00	9	13	9	9	4
2016-01-21 19:05:00	11	11	4	13	10
2016-01-21 19:10:00	6	13	6	10	9





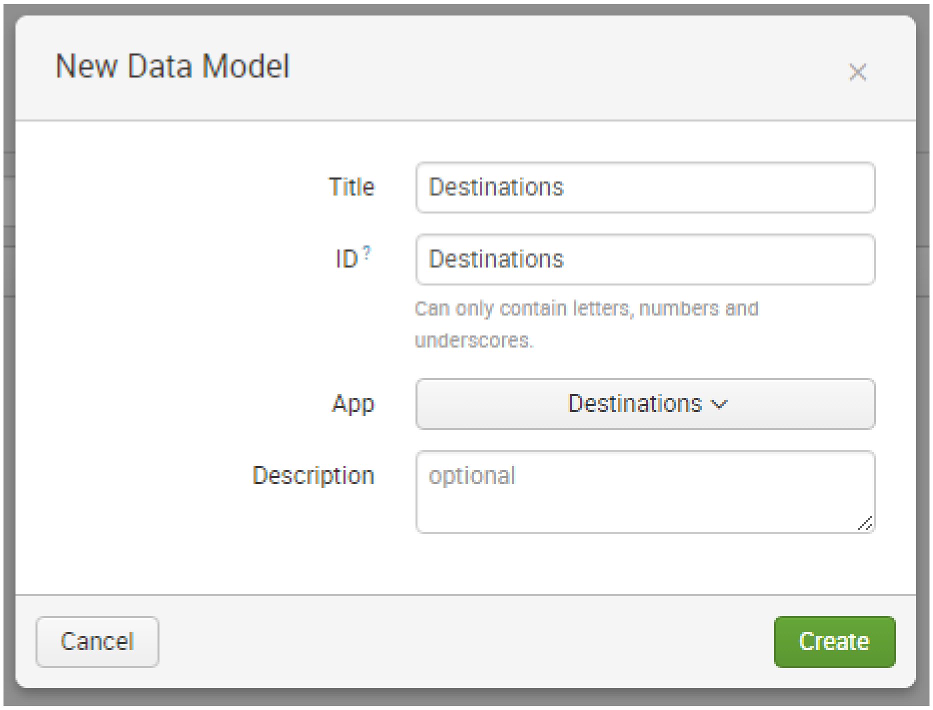
url	count	Tag
/destination/city/details	65	
/booking/reservation	62	
/booking/payment	55	
/booking/confirmation	53	
/auth	52	Auth
/home	47	Home
/destinations/search	28	



```
index=main | rex field=http_user_agent "Chrome/(?<Chrome_Version>.+?) Safari" | top Chrome_Version
```

✓ 298,645 events (before 7/26/16 6:52:05.000 AM) No Event Sampling

Chrome_Version	count	percent
29.0.1547.76	47736	26.689329
30.0.1599.69	43450	24.293015
30.0.1599.66	28072	15.695132
30.0.1599.101	27755	15.517897
29.0.1547.65	11886	6.645495
29.0.1547.66	8104	4.530969
28.0.1500.71	7913	4.424180
26.0.1410.63	3942	2.203983



New Data Model

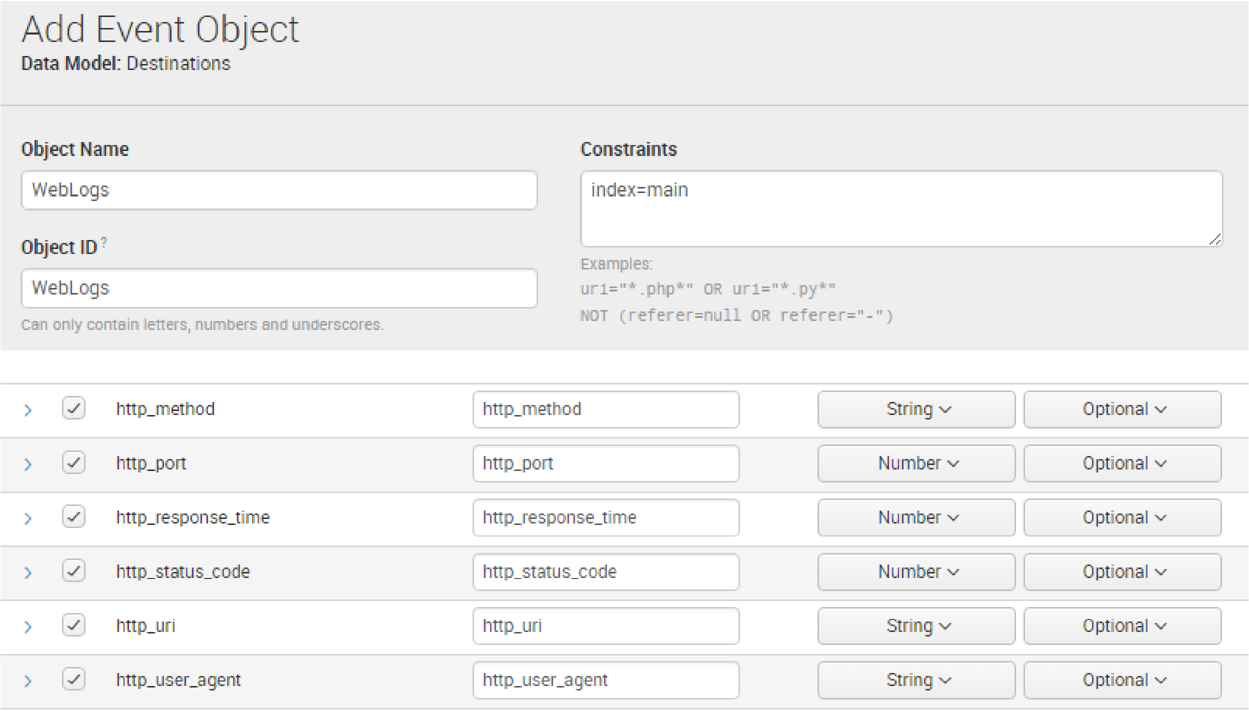
Title: Destinations

ID: Destinations

Can only contain letters, numbers and underscores.

App: Destinations

Description: optional



Add Event Object

Data Model: Destinations

Object Name: WebLogs

Object ID: WebLogs

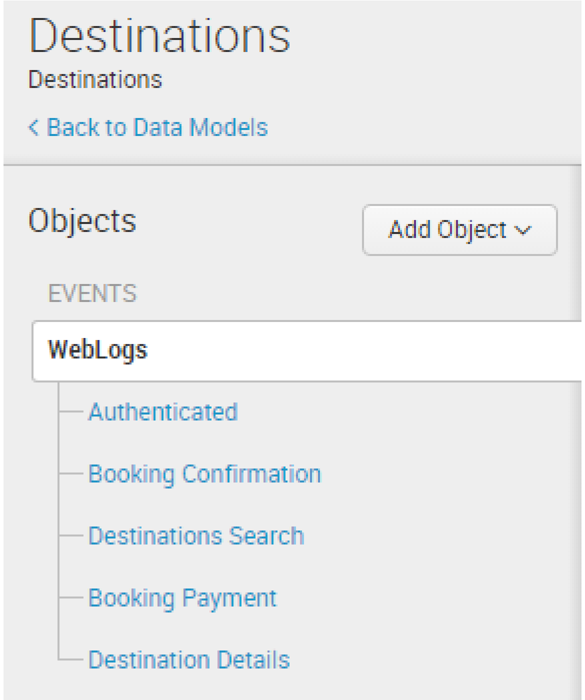
Can only contain letters, numbers and underscores.

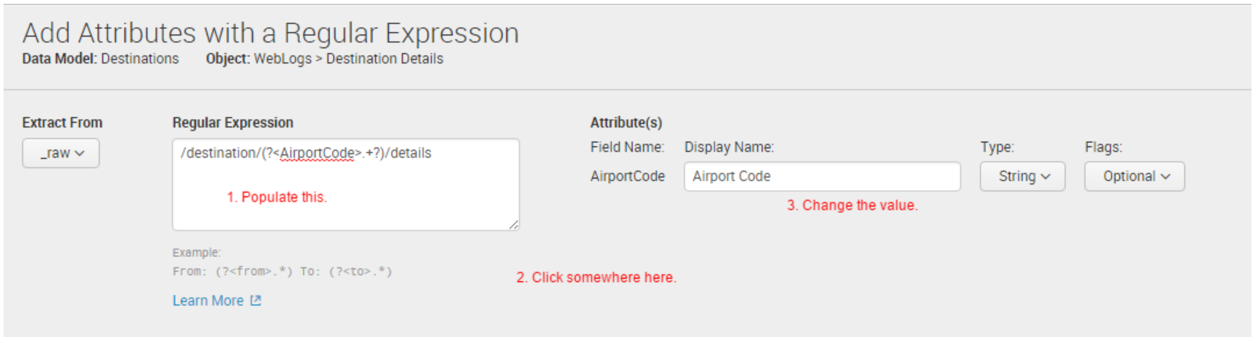
Constraints: index=main

Examples:

```
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer="-")
```

☑	http_method	http_method	String	Optional
☑	http_port	http_port	Number	Optional
☑	http_response_time	http_response_time	Number	Optional
☑	http_status_code	http_status_code	Number	Optional
☑	http_uri	http_uri	String	Optional
☑	http_user_agent	http_user_agent	String	Optional





Add Attributes with a Regular Expression

Data Model: Destinations **Object:** WebLogs > Destination Details

Extract From: _raw

Regular Expression: /destination/(?<AirportCode>.+?)/details

1. Populate this.

Example:
From: (?<from>.*) To: (?<to>.*)

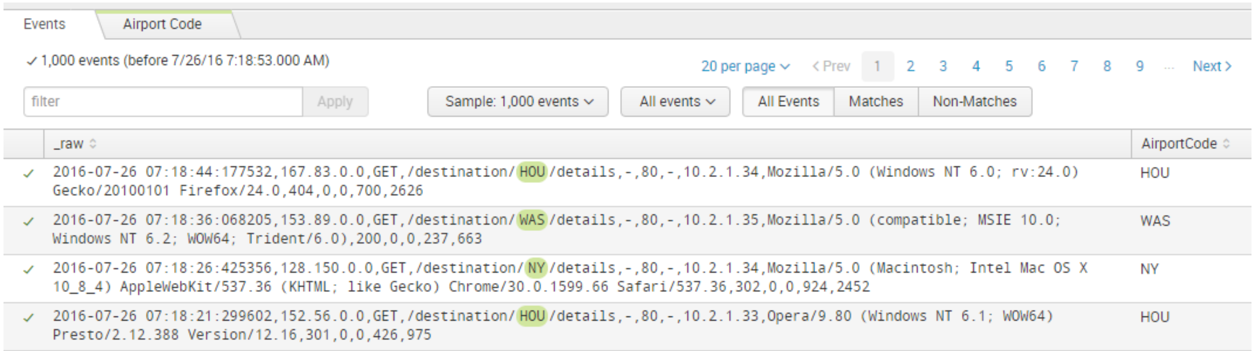
Learn More

Attribute(s)

Field Name: AirportCode Display Name: Airport Code Type: String Flags: Optional

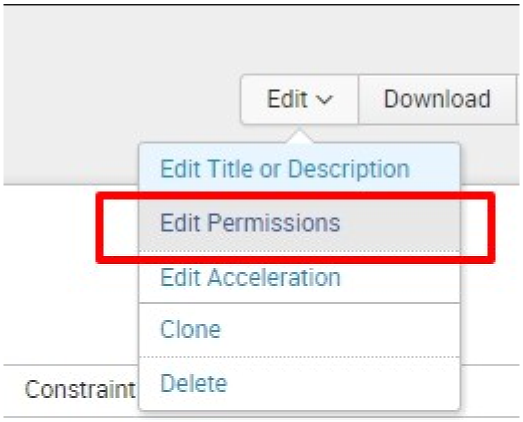
3. Change the value.

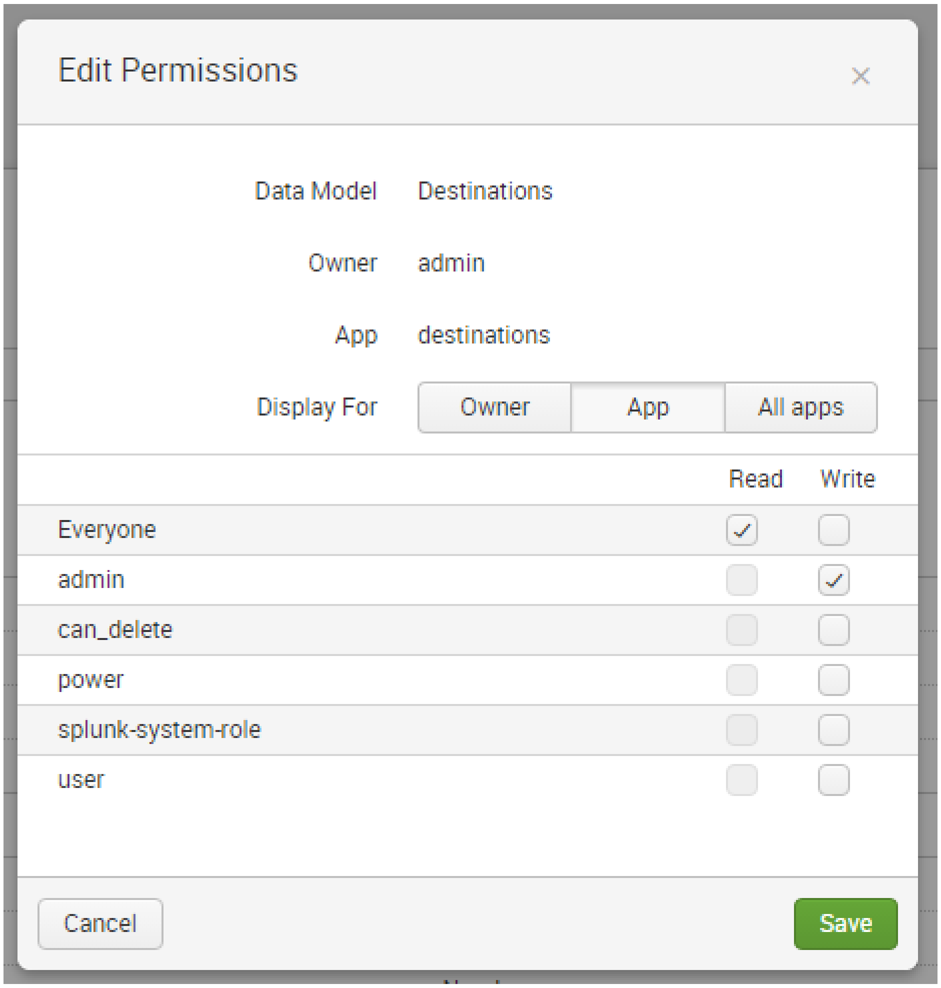
2. Click somewhere here.



✓ 1,000 events (before 7/26/16 7:18:53.000 AM)

	_raw	AirportCode
✓	2016-07-26 07:18:44:177532,167.83.0.0,GET,/destination/HOU/details,-,80,-,10.2.1.34,Mozilla/5.0 (Windows NT 6.0; rv:24.0) Gecko/20100101 Firefox/24.0,404,0,0,700,2626	HOU
✓	2016-07-26 07:18:36:068205,153.89.0.0,GET,/destination/WAS/details,-,80,-,10.2.1.35,Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0),200,0,0,237,663	WAS
✓	2016-07-26 07:18:26:425356,128.150.0.0,GET,/destination/NY/details,-,80,-,10.2.1.34,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.66 Safari/537.36,302,0,0,924,2452	NY
✓	2016-07-26 07:18:21:299602,152.56.0.0,GET,/destination/HOU/details,-,80,-,10.2.1.33,Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.16,301,0,0,426,975	HOU





Edit Permissions

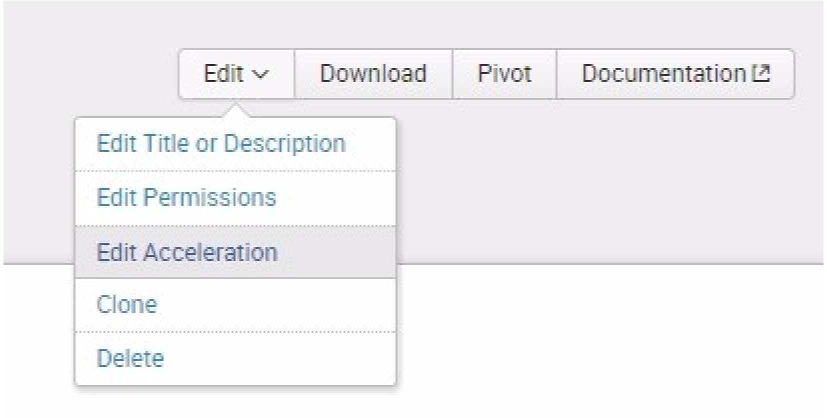
Data Model: Destinations

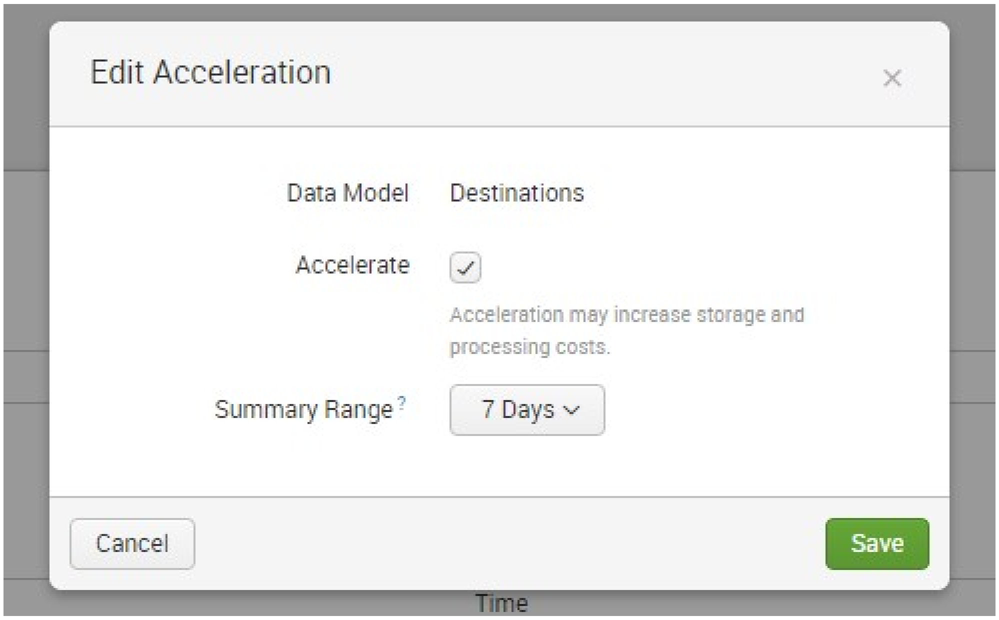
Owner: admin

App: destinations

Display For: Owner | App | All apps

	Read	Write
Everyone	☑	□
admin	□	☑
can_delete	□	□
power	□	□
splunk-system-role	□	□
user	□	□



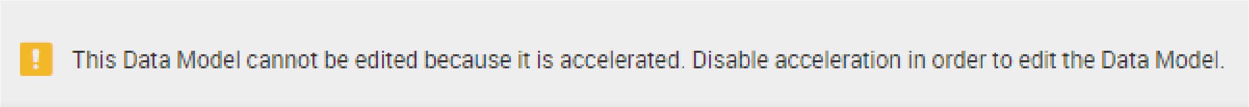

Edit Acceleration

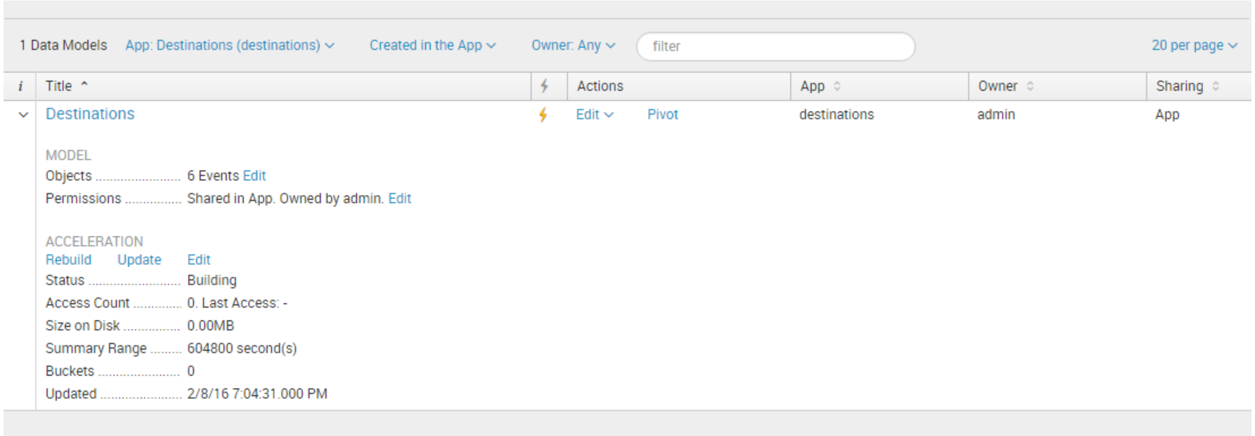
Data Model Destinations

Accelerate ☑

Acceleration may increase storage and processing costs.

Summary Range 7 Days


This Data Model cannot be edited because it is accelerated. Disable acceleration in order to edit the Data Model.

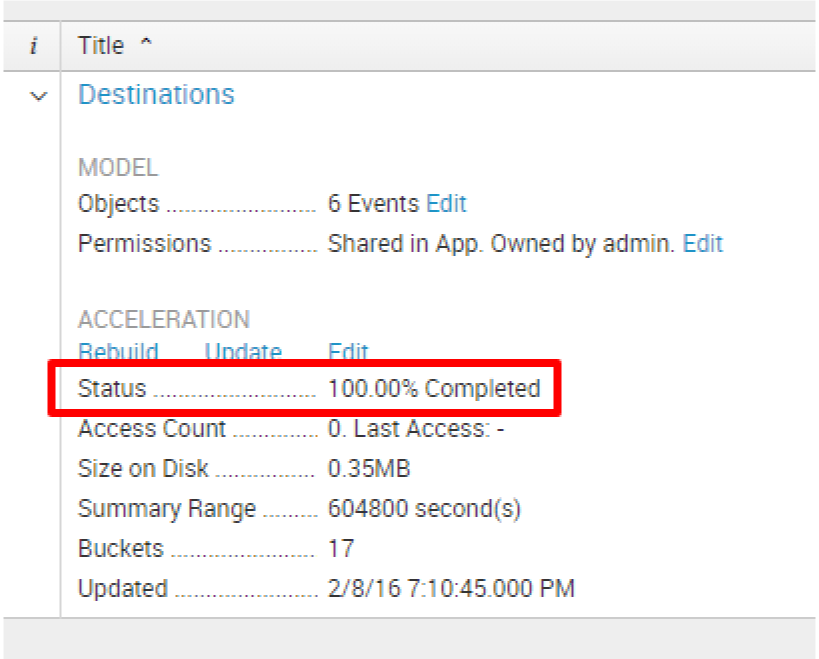


1 Data Models App: Destinations (destinations) Created in the App Owner: Any filter 20 per page

i	Title ^	⚡	Actions		App	Owner	Sharing
⌄	Destinations	⚡	Edit	Pivot	destinations	admin	App

MODEL
Objects .... 6 Events Edit
Permissions .... Shared in App. Owned by admin. Edit

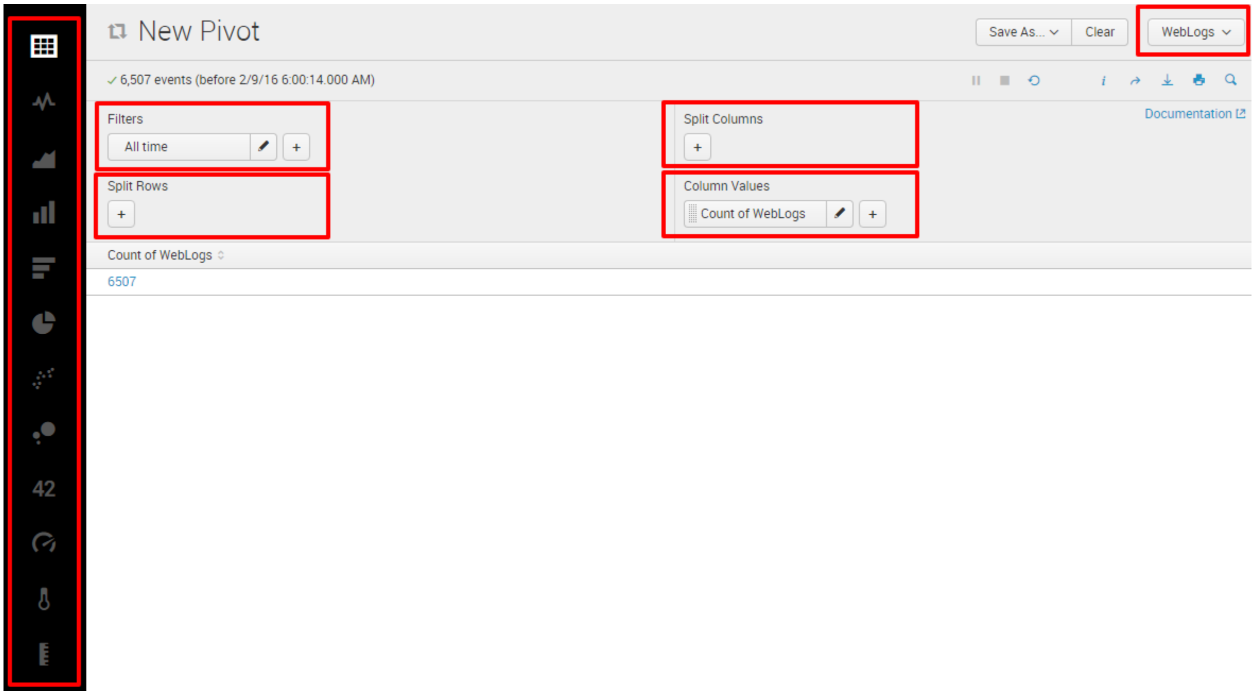
ACCELERATION
Rebuild Update Edit
Status .... Building
Access Count .... 0. Last Access: -
Size on Disk 0.00MB
Summary Range .... 604800 second(s)
Buckets 0
Updated .... 2/8/16 7:04:31.000 PM



i	Title ^
⌄	Destinations

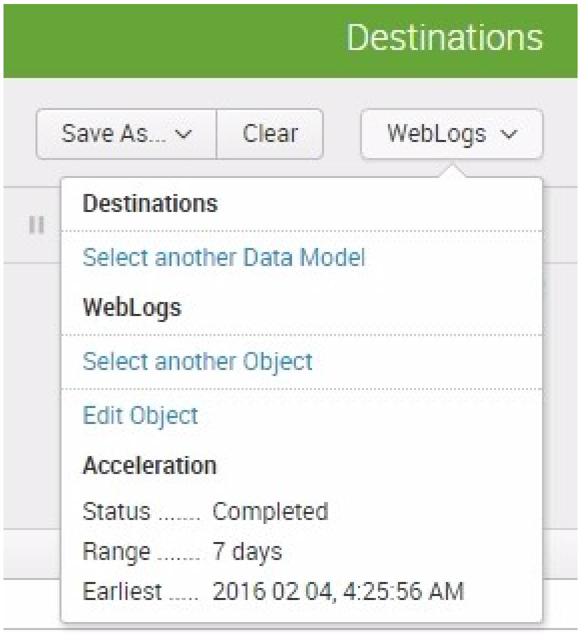
MODEL
Objects .... 6 Events Edit
Permissions .... Shared in App. Owned by admin. Edit

ACCELERATION
Rebuild Update Edit
Status .... 100.00% Completed
Access Count .... 0. Last Access: -
Size on Disk 0.35MB
Summary Range .... 604800 second(s)
Buckets 17
Updated .... 2/8/16 7:10:45.000 PM

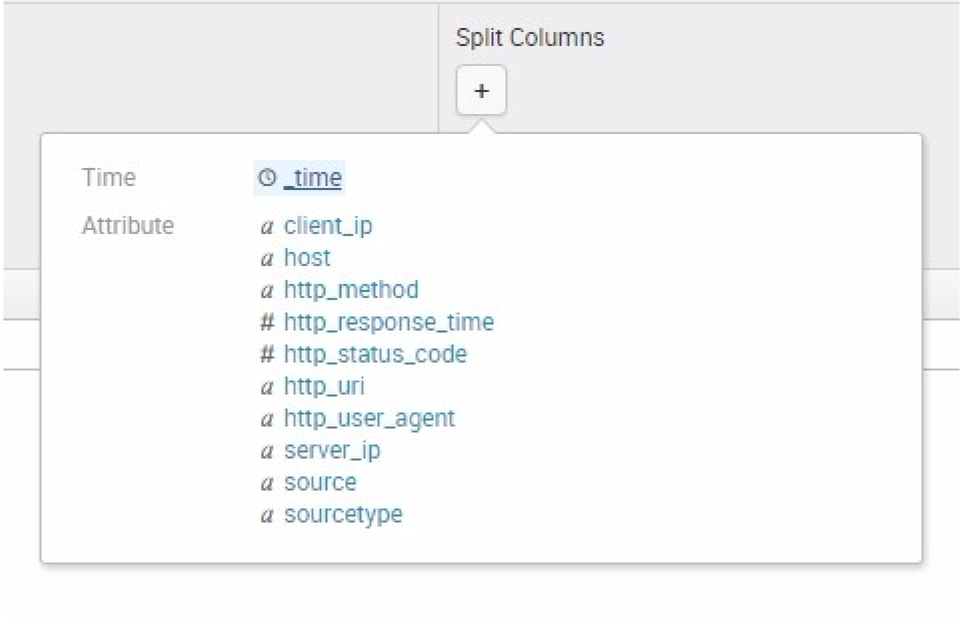


✓ 6,507 events (before 2/9/16 6:00:14.000 AM)

Count of WebLogs
6507



Status .... Completed
Range .... 7 days
Earliest ..... 2016 02 04, 4:25:56 AM

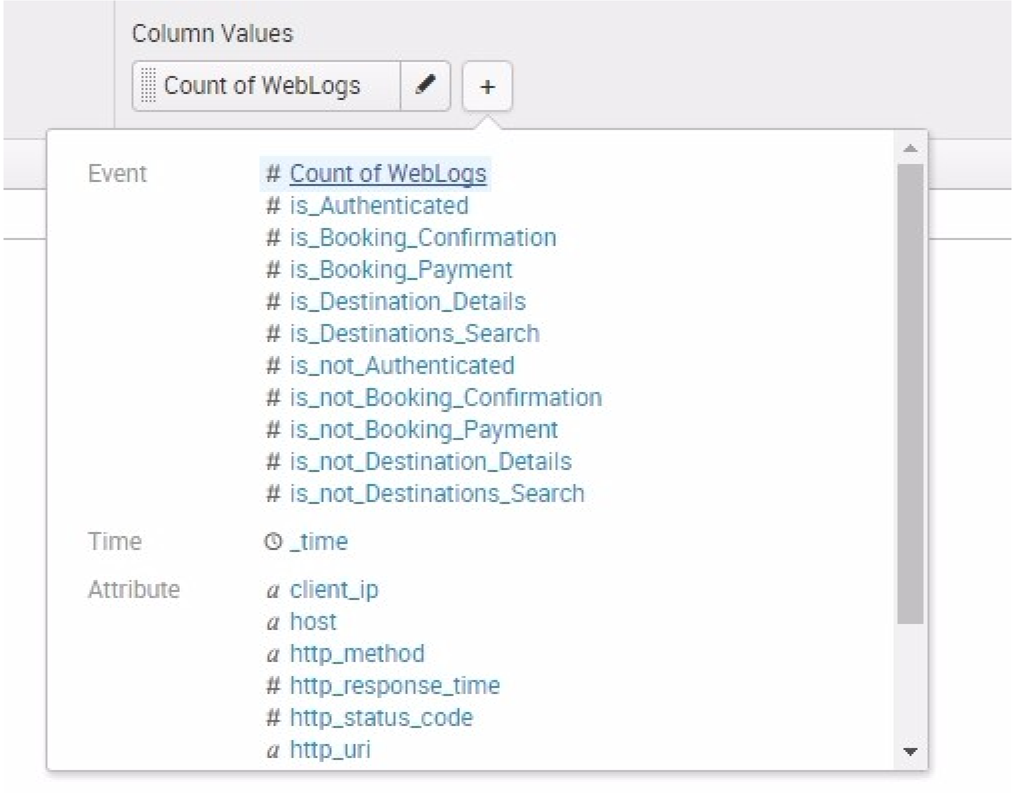


Split Columns

+

Time ◷ _time

Attribute
- a client_ip
- a host
- a http_method
- # http_response_time
- # http_status_code
- a http_uri
- a http_user_agent
- a server_ip
- a source
- a sourcetype



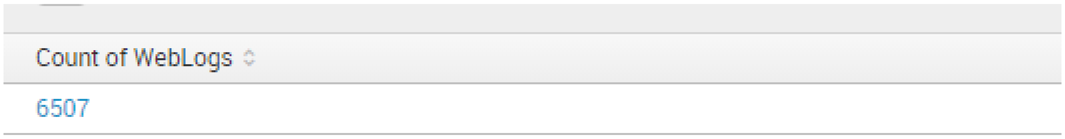
Column Values

Count of WebLogs ✎ +

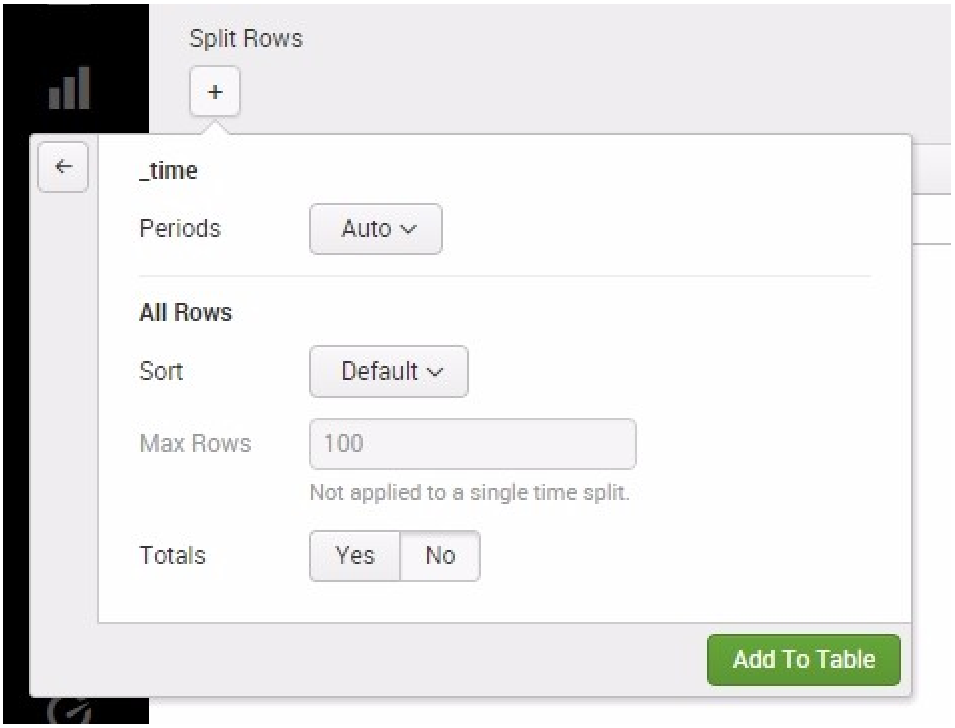
Event
- # Count of WebLogs
- # is_Authenticated
- # is_Booking_Confirmation
- # is_Booking_Payment
- # is_Destination_Details
- # is_Destinations_Search
- # is_not_Authenticated
- # is_not_Booking_Confirmation
- # is_not_Booking_Payment
- # is_not_Destination_Details
- # is_not_Destinations_Search

Time ◷ _time

Attribute
- a client_ip
- a host
- a http_method
- # http_response_time
- # http_status_code
- a http_uri



Count of WebLogs
6507



Split Rows

_time

Periods: Auto

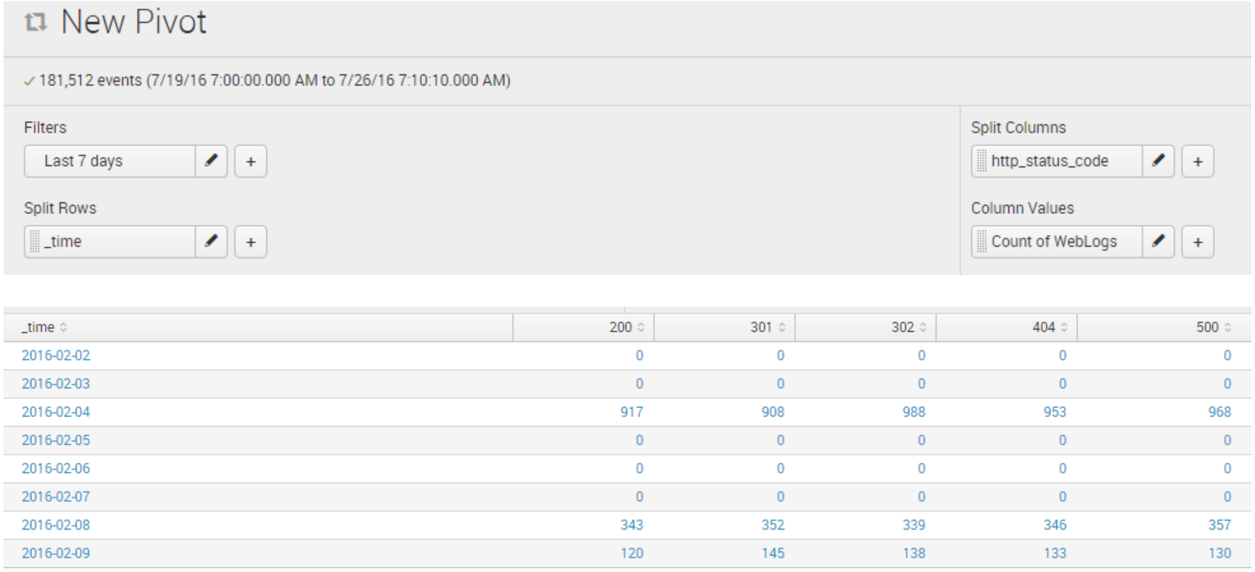
All Rows

Sort: Default

Max Rows: 100

Not applied to a single time split.

Totals: Yes | No



New Pivot

✓ 181,512 events (7/19/16 7:00:00.000 AM to 7/26/16 7:10:10.000 AM)

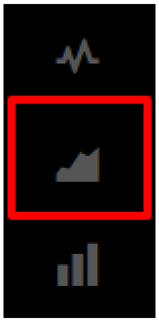
Filters: Last 7 days

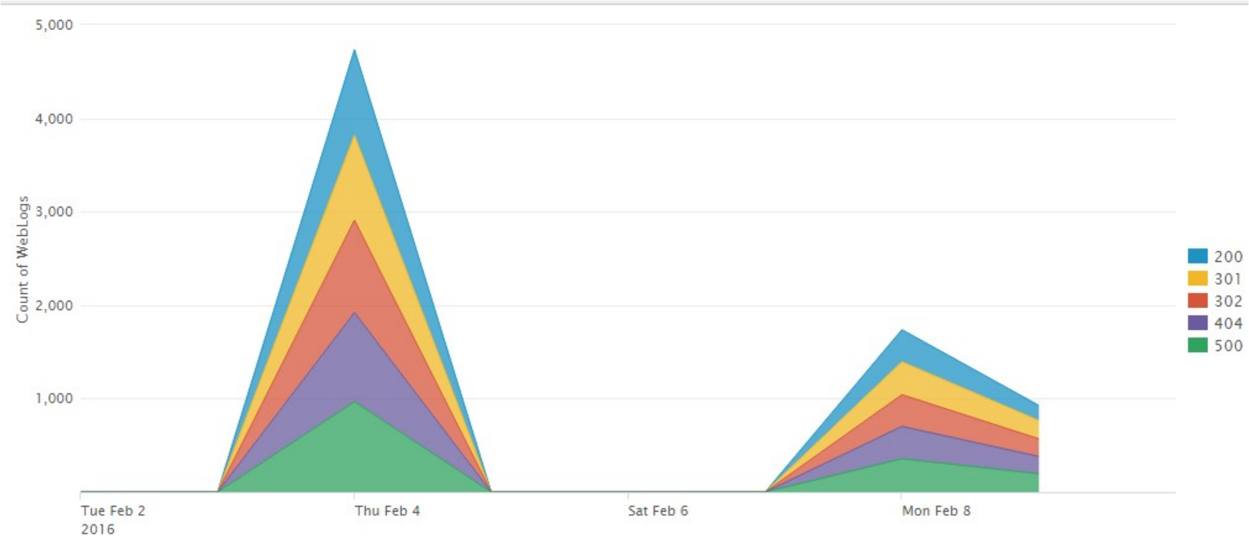
Split Rows: _time

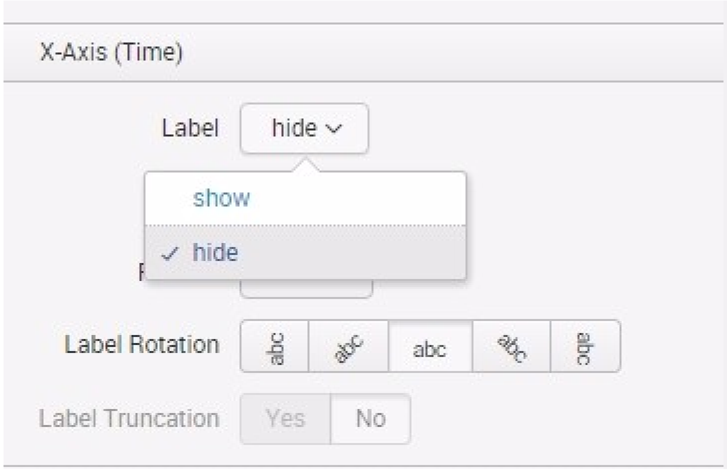
Split Columns: http_status_code

Column Values: Count of WebLogs

_time	200	301	302	404	500
2016-02-02	0	0	0	0	0
2016-02-03	0	0	0	0	0
2016-02-04	917	908	988	953	968
2016-02-05	0	0	0	0	0
2016-02-06	0	0	0	0	0
2016-02-07	0	0	0	0	0
2016-02-08	343	352	339	346	357
2016-02-09	120	145	138	133	130





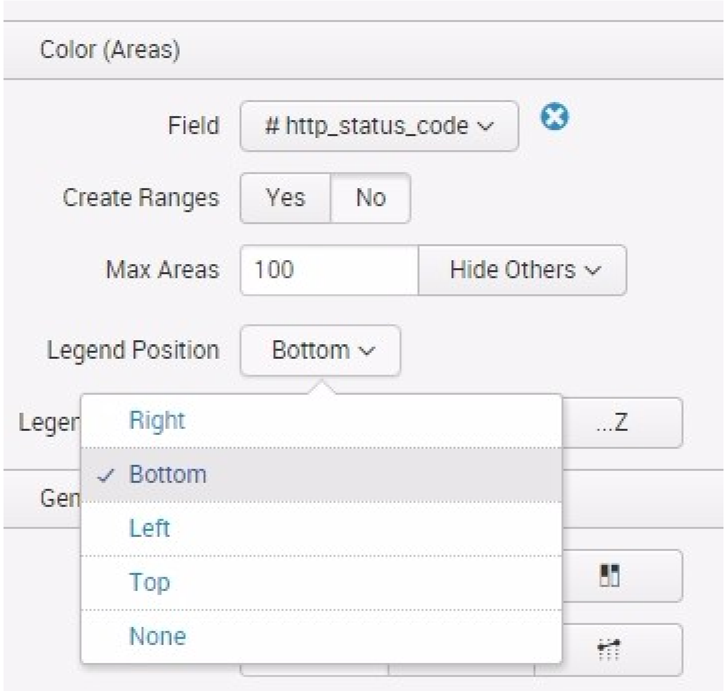

X-Axis (Time)

Label: hide

show

✓ hide

Label Truncation: Yes No



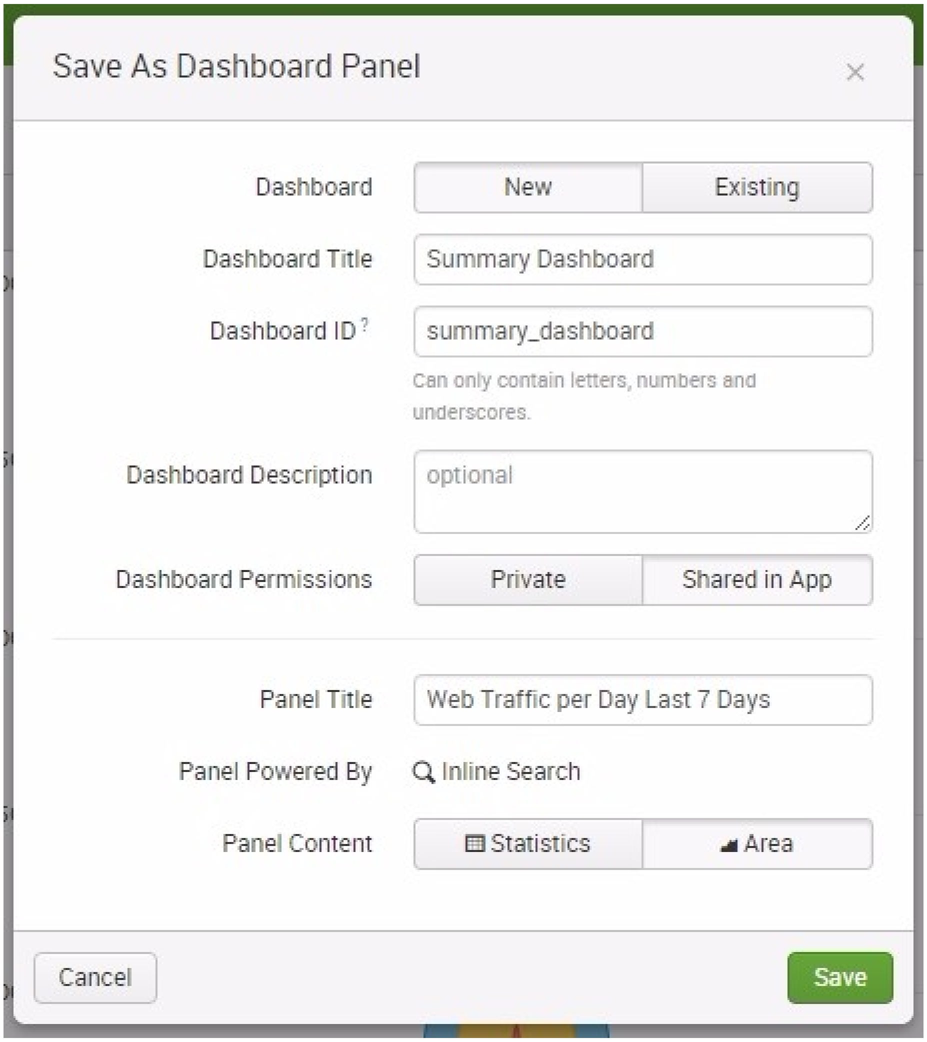
Color (Areas)

Field: # http_status_code

Create Ranges: Yes No

Max Areas: 100 Hide Others

Legend Position: Bottom



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Summary Dashboard

Dashboard ID ?: summary_dashboard

Can only contain letters, numbers and underscores.

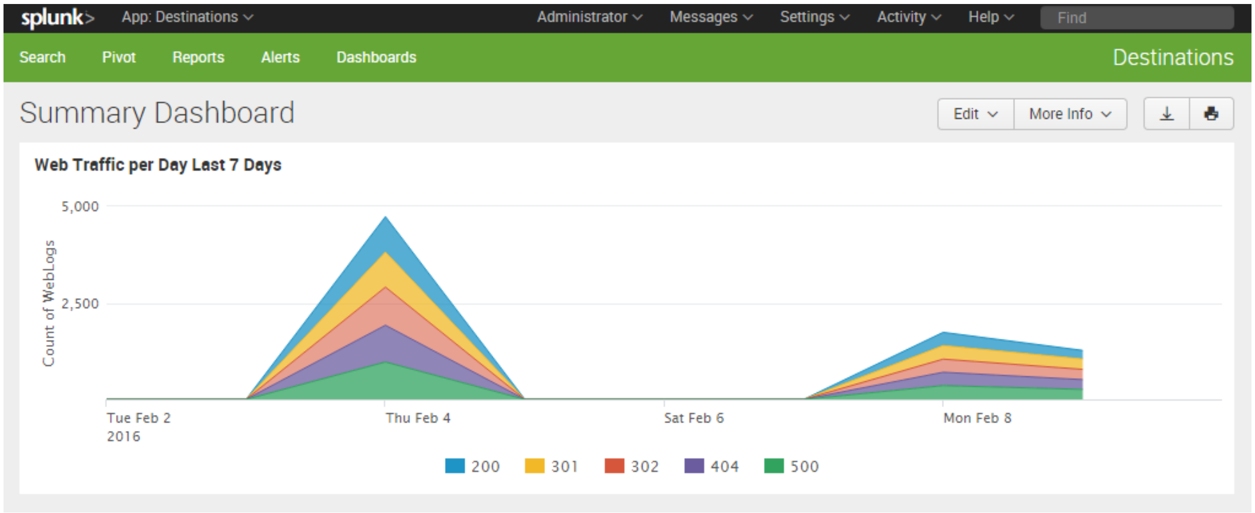
Dashboard Description: optional

Dashboard Permissions: Private | Shared in App

Panel Title: Web Traffic per Day Last 7 Days

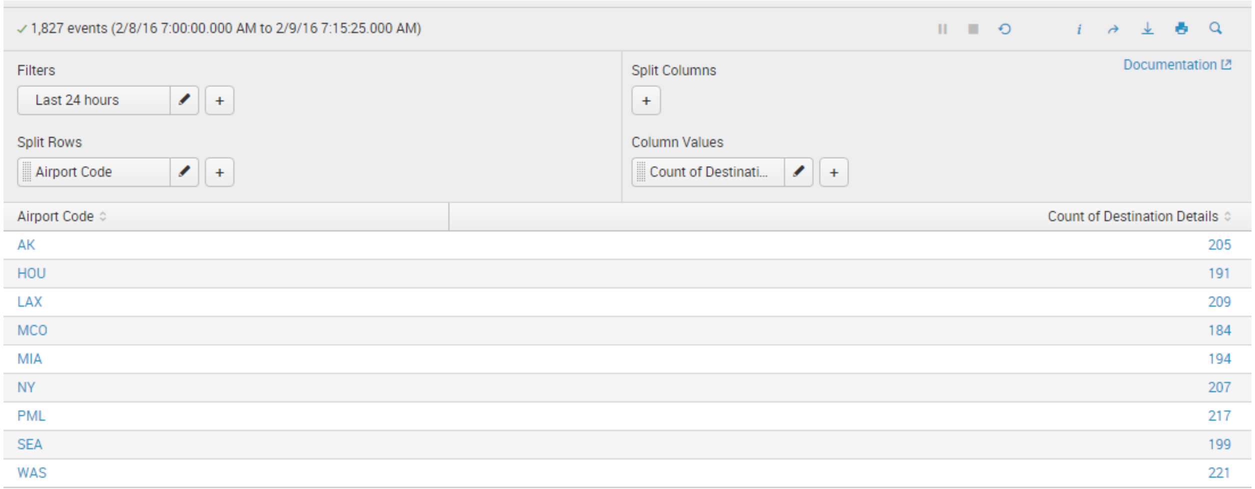
Panel Powered By: Inline Search

Panel Content: Statistics | Area



Summary Dashboard

Web Traffic per Day Last 7 Days



✓ 1,827 events (2/8/16 7:00:00.000 AM to 2/9/16 7:15:25.000 AM)

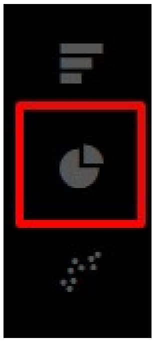
Filters: Last 24 hours

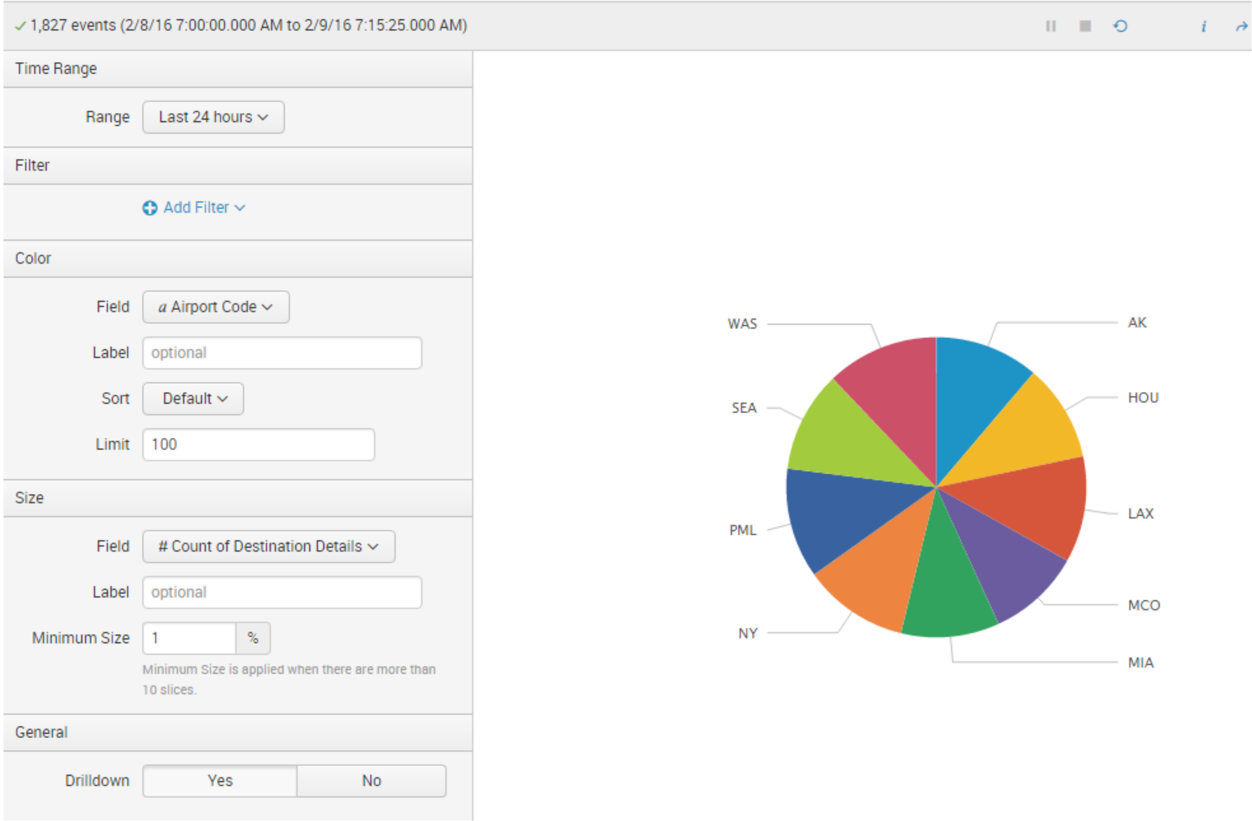
Split Columns

Split Rows: Airport Code

Column Values: Count of Destinati...

Airport Code	Count of Destination Details
AK	205
HOU	191
LAX	209
MCO	184
MIA	194
NY	207
PML	217
SEA	199
WAS	221





✓ 1,827 events (2/8/16 7:00:00.000 AM to 2/9/16 7:15:25.000 AM)

Time Range

Range: Last 24 hours

Filter

Add Filter

Color

Field: *a* Airport Code

Label: optional

Sort: Default

Limit: 100

Size

Field: # Count of Destination Details

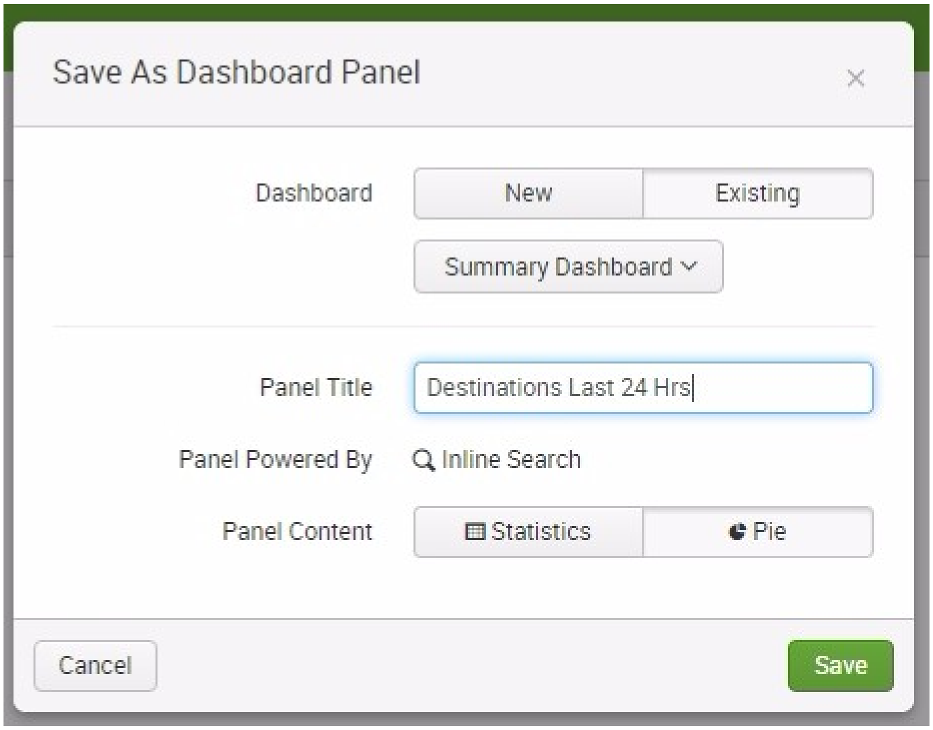
Label: optional

Minimum Size: 1 %

Minimum Size is applied when there are more than 10 slices.

General

Drilldown: Yes No



Save As Dashboard Panel

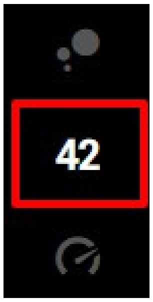
Dashboard: New Existing

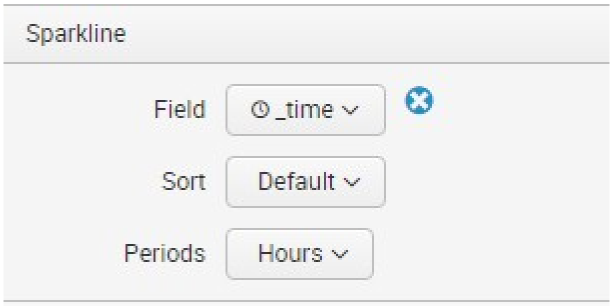
Summary Dashboard

Panel Title: Destinations Last 24 Hrs

Panel Powered By: Inline Search

Panel Content: Statistics Pie

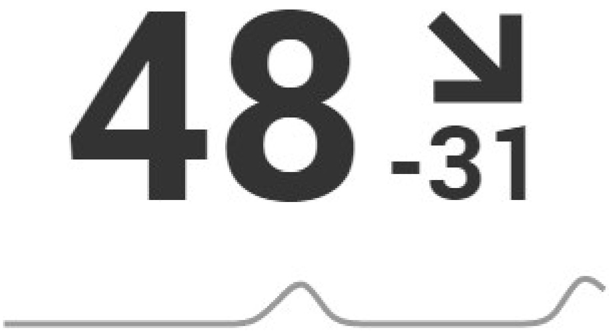


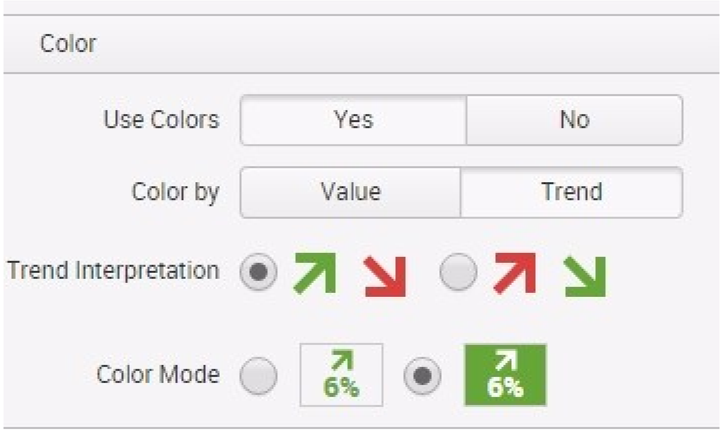

Sparkline

Field ◷ _time ⌄

Sort Default ⌄

Periods Hours ⌄



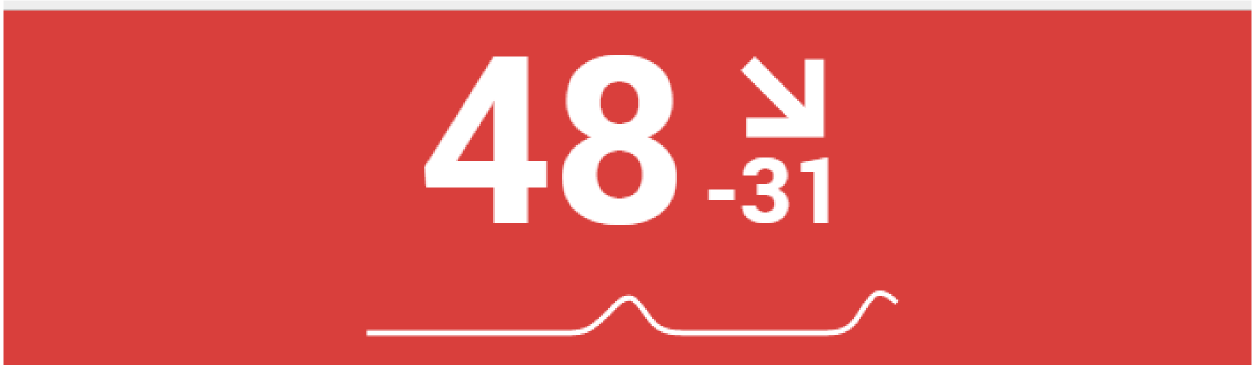

Color

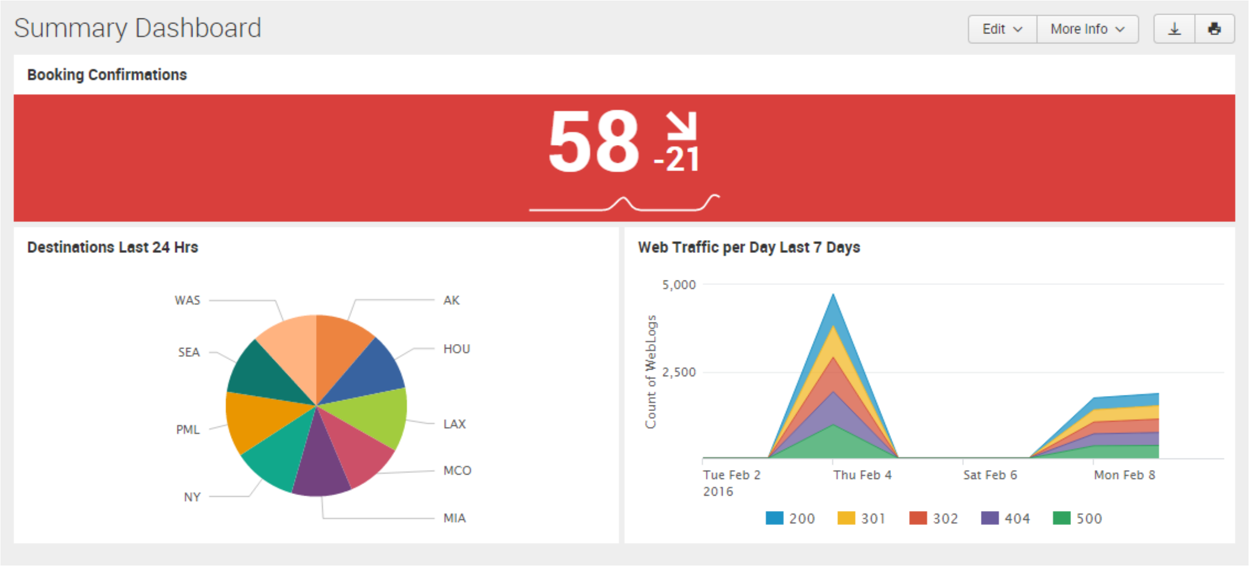
Use Colors: Yes | No

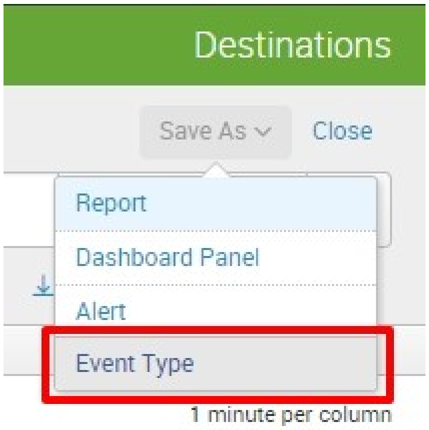
Color by: Value | Trend

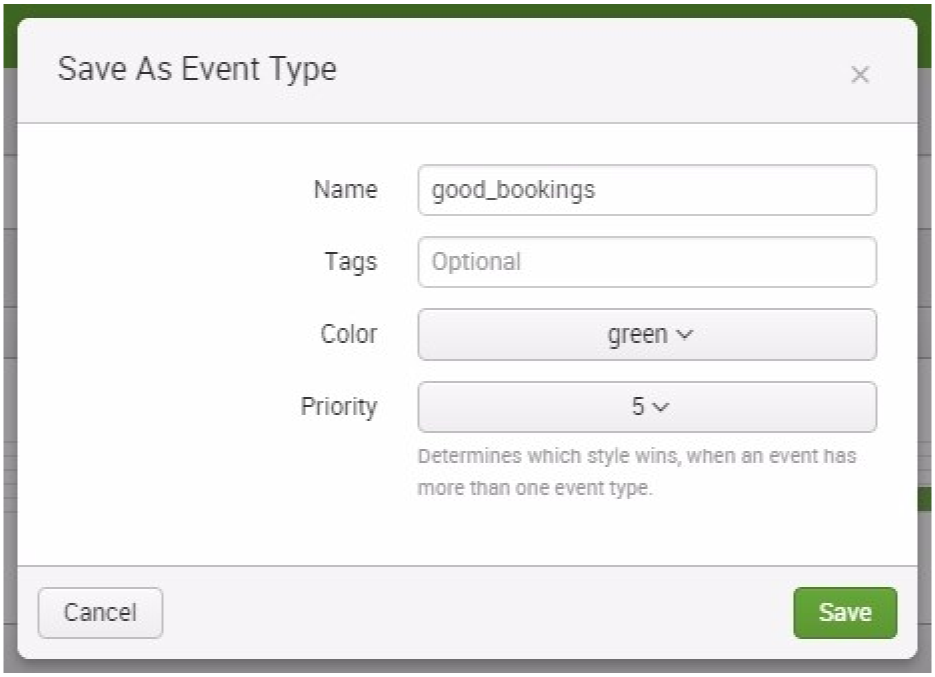
Trend Interpretation ● ↗ ↘ ○ ↗ ↘

Color Mode ○ ↗ 6% ● ↗ 6%


48
-31


Summary Dashboard
Edit
More Info
Booking Confirmations
58
-21
Destinations Last 24 Hrs
WAS
AK
SEA
HOU
PML
LAX
MCO
NY
MIA
Web Traffic per Day Last 7 Days
5,000
2,500
Count of WebLogs
Tue Feb 2
2016
Thu Feb 4
Sat Feb 6
Mon Feb 8
200
301
302
404
500




Save As Event Type

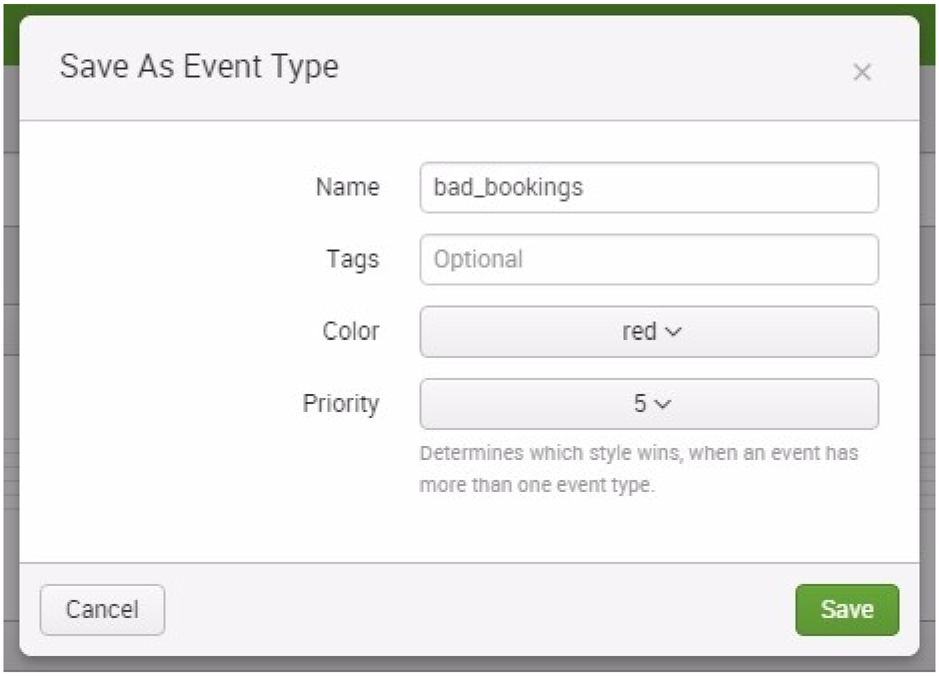
Name: good_bookings

Tags: Optional

Color: green

Priority: 5

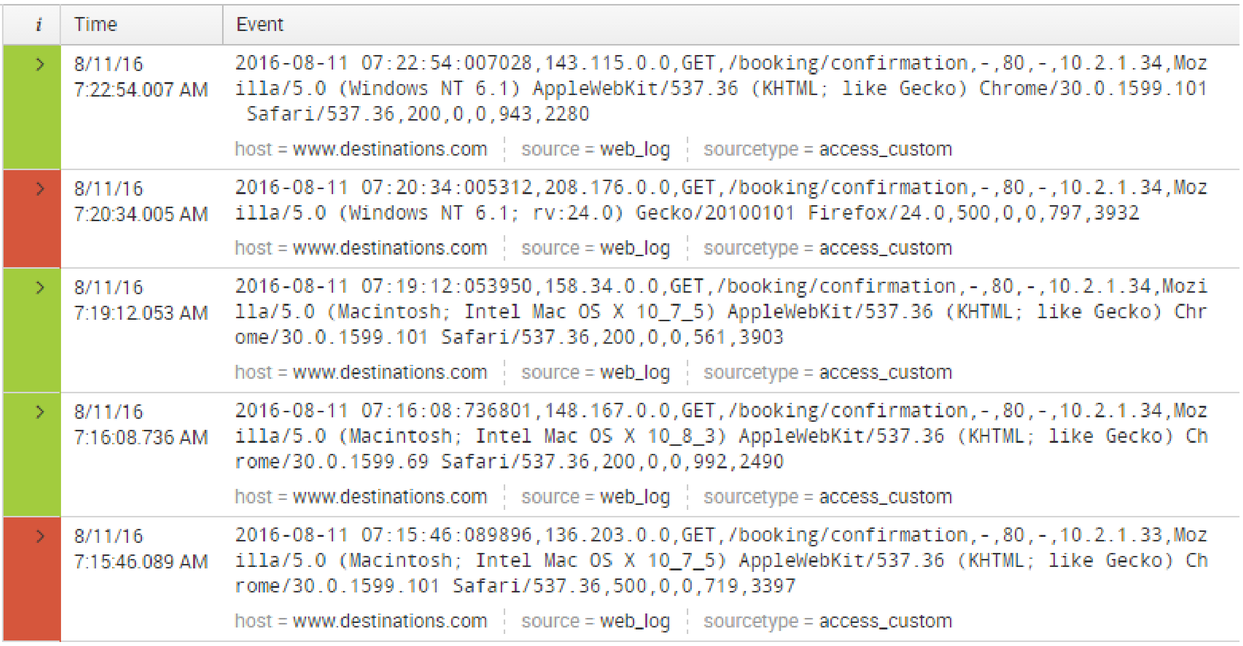
Determines which style wins, when an event has more than one event type.



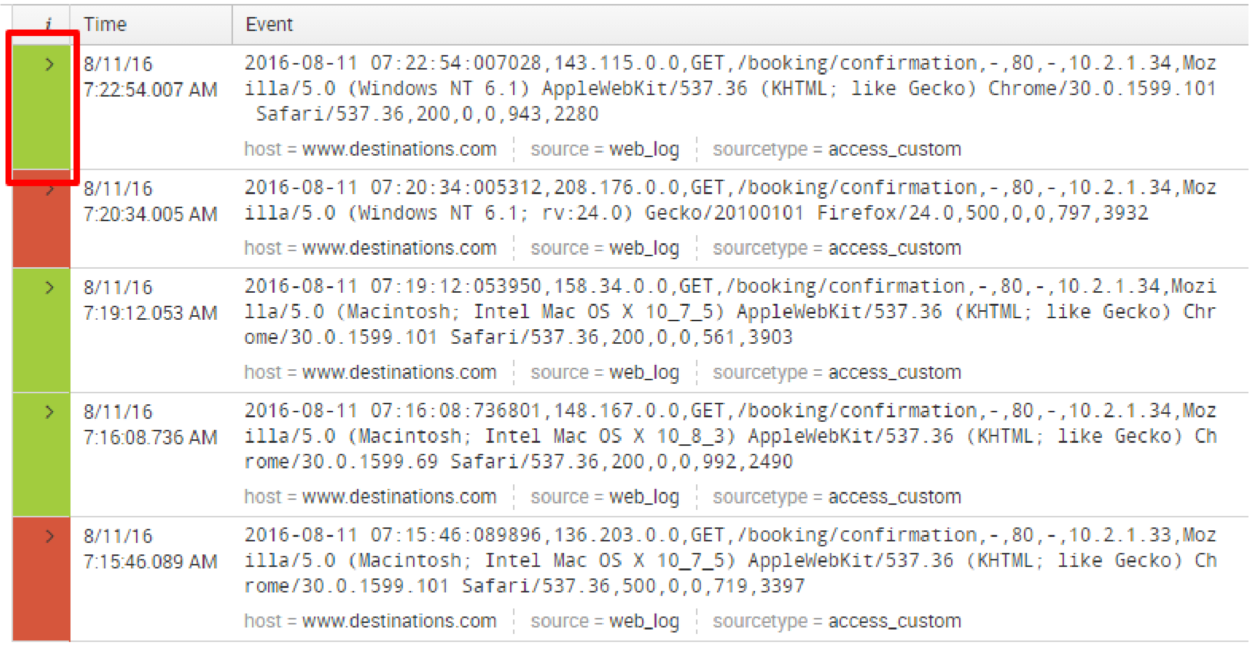
Save As Event Type

Name	bad_bookings
Tags	Optional
Color	red
Priority	5

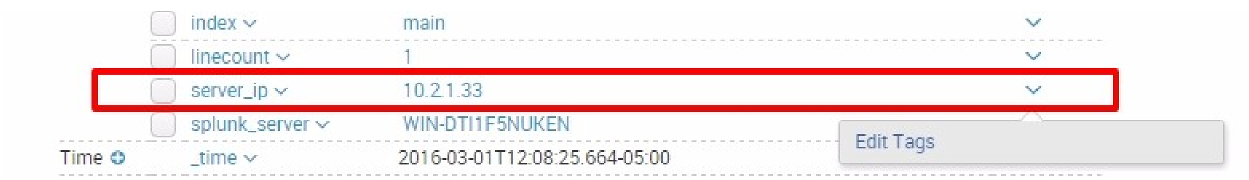
Determines which style wins, when an event has more than one event type.



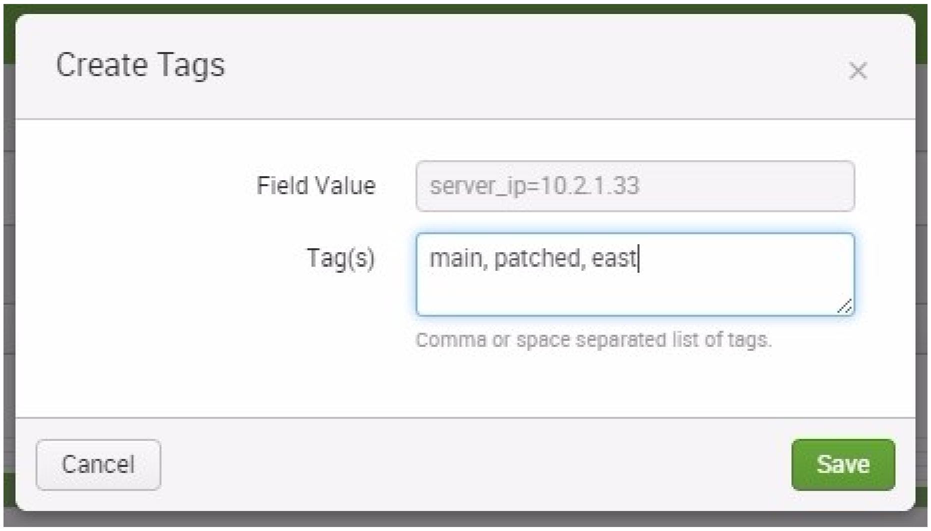
i	Time	Event
🟩 >	8/11/16 7:22:54.007 AM	2016-08-11 07:22:54:007028,143.115.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36,200,0,0,943,2280 host = www.destinations.com ⁝ source = web_log ⁝ sourcetype = access_custom
🟥 >	8/11/16 7:20:34.005 AM	2016-08-11 07:20:34:005312,208.176.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0,500,0,0,797,3932 host = www.destinations.com ⁝ source = web_log ⁝ sourcetype = access_custom
🟩 >	8/11/16 7:19:12.053 AM	2016-08-11 07:19:12:053950,158.34.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36,200,0,0,561,3903 host = www.destinations.com ⁝ source = web_log ⁝ sourcetype = access_custom
🟩 >	8/11/16 7:16:08.736 AM	2016-08-11 07:16:08:736801,148.167.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.69 Safari/537.36,200,0,0,992,2490 host = www.destinations.com ⁝ source = web_log ⁝ sourcetype = access_custom
🟥 >	8/11/16 7:15:46.089 AM	2016-08-11 07:15:46:089896,136.203.0.0,GET,/booking/confirmation,-,80,-,10.2.1.33,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36,500,0,0,719,3397 host = www.destinations.com ⁝ source = web_log ⁝ sourcetype = access_custom



i	Time	Event
🟩 >	8/11/16 7:22:54.007 AM	2016-08-11 07:22:54:007028,143.115.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36,200,0,0,943,2280 host = www.destinations.com ¦ source = web_log ¦ sourcetype = access_custom
🟥 >	8/11/16 7:20:34.005 AM	2016-08-11 07:20:34:005312,208.176.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0,500,0,0,797,3932 host = www.destinations.com ¦ source = web_log ¦ sourcetype = access_custom
🟩 >	8/11/16 7:19:12.053 AM	2016-08-11 07:19:12:053950,158.34.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36,200,0,0,561,3903 host = www.destinations.com ¦ source = web_log ¦ sourcetype = access_custom
🟩 >	8/11/16 7:16:08.736 AM	2016-08-11 07:16:08:736801,148.167.0.0,GET,/booking/confirmation,-,80,-,10.2.1.34,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.69 Safari/537.36,200,0,0,992,2490 host = www.destinations.com ¦ source = web_log ¦ sourcetype = access_custom
🟥 >	8/11/16 7:15:46.089 AM	2016-08-11 07:15:46:089896,136.203.0.0,GET,/booking/confirmation,-,80,-,10.2.1.33,Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36,500,0,0,719,3397 host = www.destinations.com ¦ source = web_log ¦ sourcetype = access_custom



	□	index ⌄	main
	□	linecount ⌄	1
	□	server_ip ⌄	10.2.1.33
	□	splunk_server ⌄	WIN-DTI1F5NUKEN
Time ⊕		_time ⌄	2016-03-01T12:08:25.664-05:00

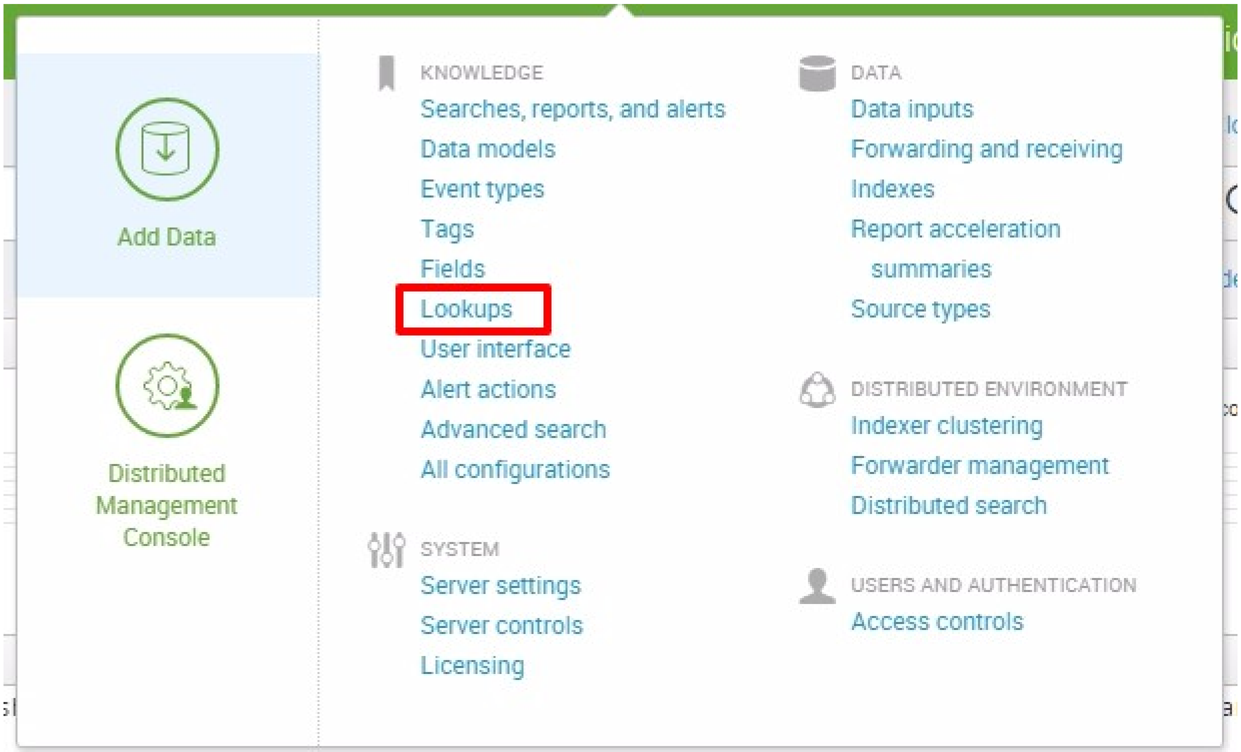


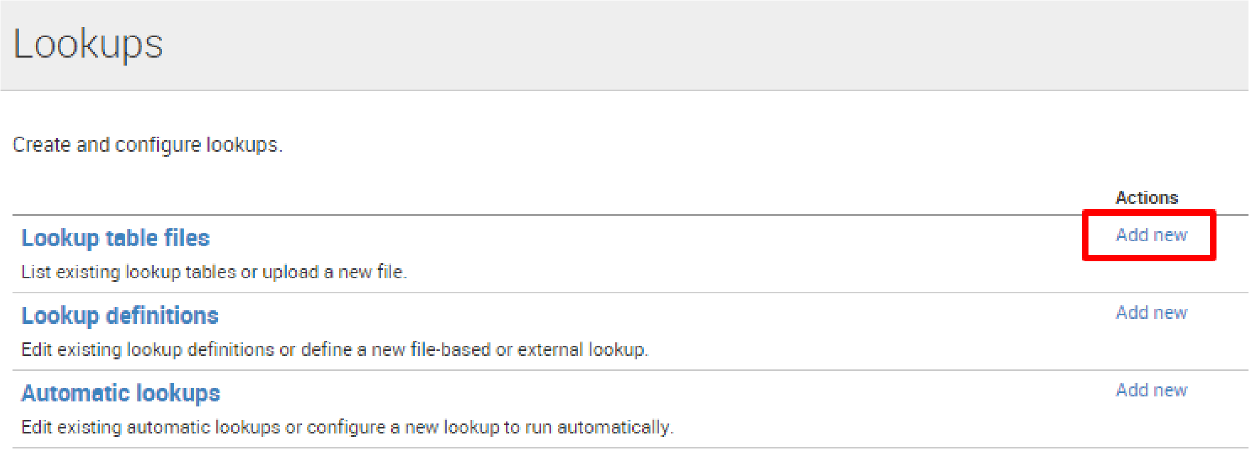
Create Tags

Field Value: server_ip=10.2.1.33

Tag(s): main, patched, east

Comma or space separated list of tags.

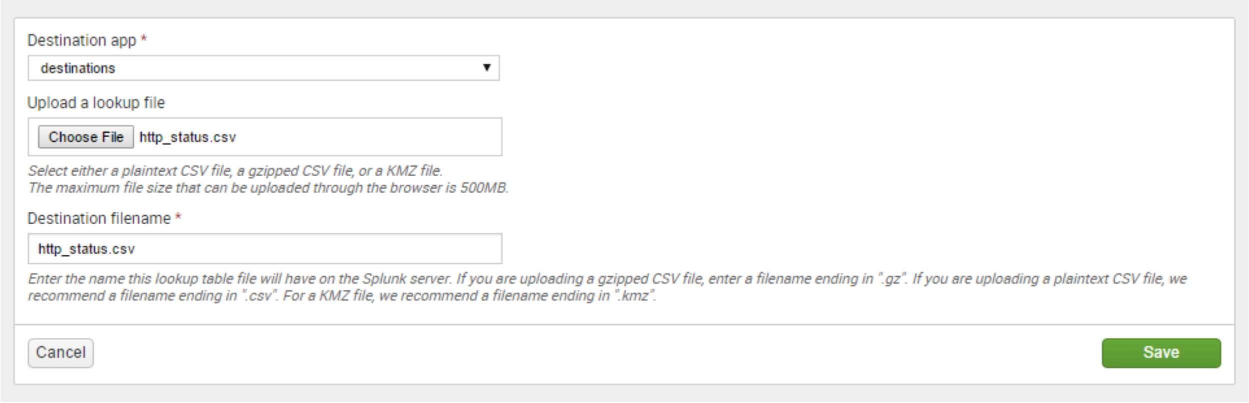

Add Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls



Lookups

Create and configure lookups.

	Actions
Lookup table files List existing lookup tables or upload a new file.	Add new
Lookup definitions Edit existing lookup definitions or define a new file-based or external lookup.	Add new
Automatic lookups Edit existing automatic lookups or configure a new lookup to run automatically.	Add new



Destination app *

destinations ▾

Upload a lookup file

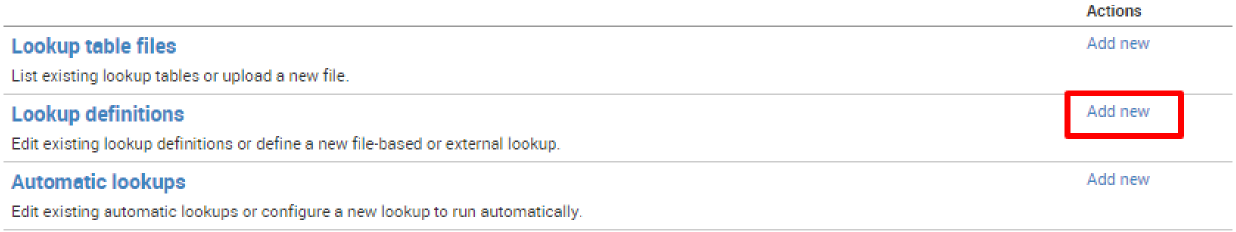
Choose File http_status.csv

Select either a plaintext CSV file, a gzipped CSV file, or a KMZ file.
The maximum file size that can be uploaded through the browser is 500MB.

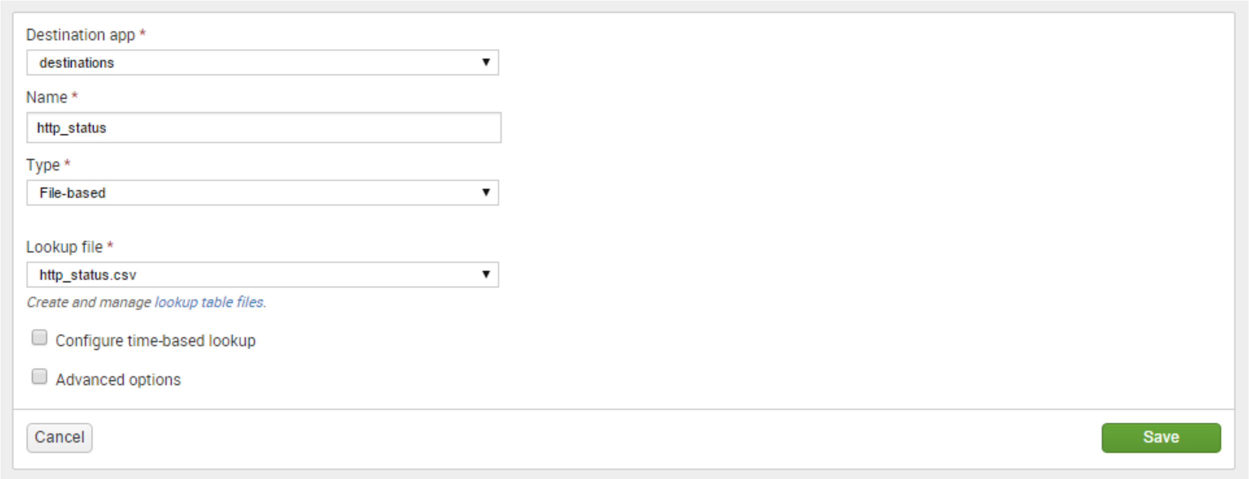
Destination filename *

http_status.csv

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv". For a KMZ file, we recommend a filename ending in ".kmz".



	Actions
Lookup table files List existing lookup tables or upload a new file.	Add new
Lookup definitions Edit existing lookup definitions or define a new file-based or external lookup.	Add new
Automatic lookups Edit existing automatic lookups or configure a new lookup to run automatically.	Add new

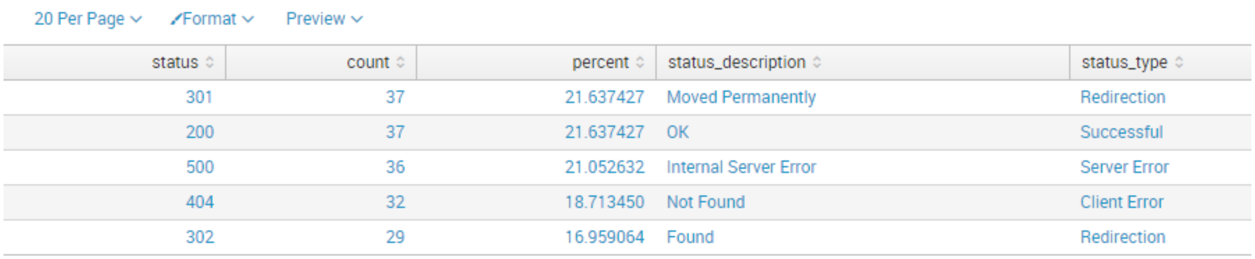


Destination app *	destinations
Name *	http_status
Type *	File-based
Lookup file *	http_status.csv

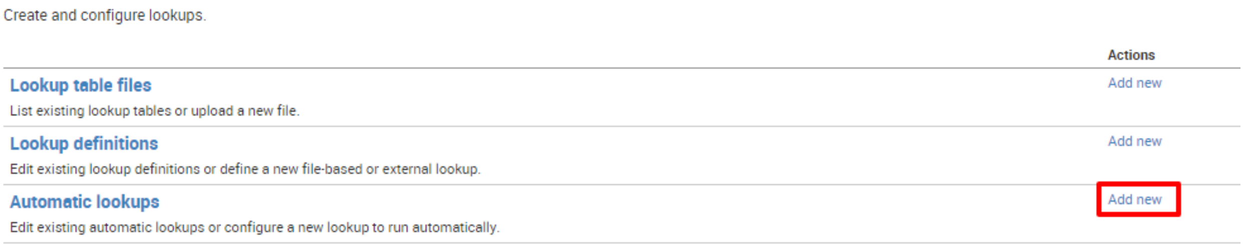
Create and manage lookup table files.

□ Configure time-based lookup

□ Advanced options

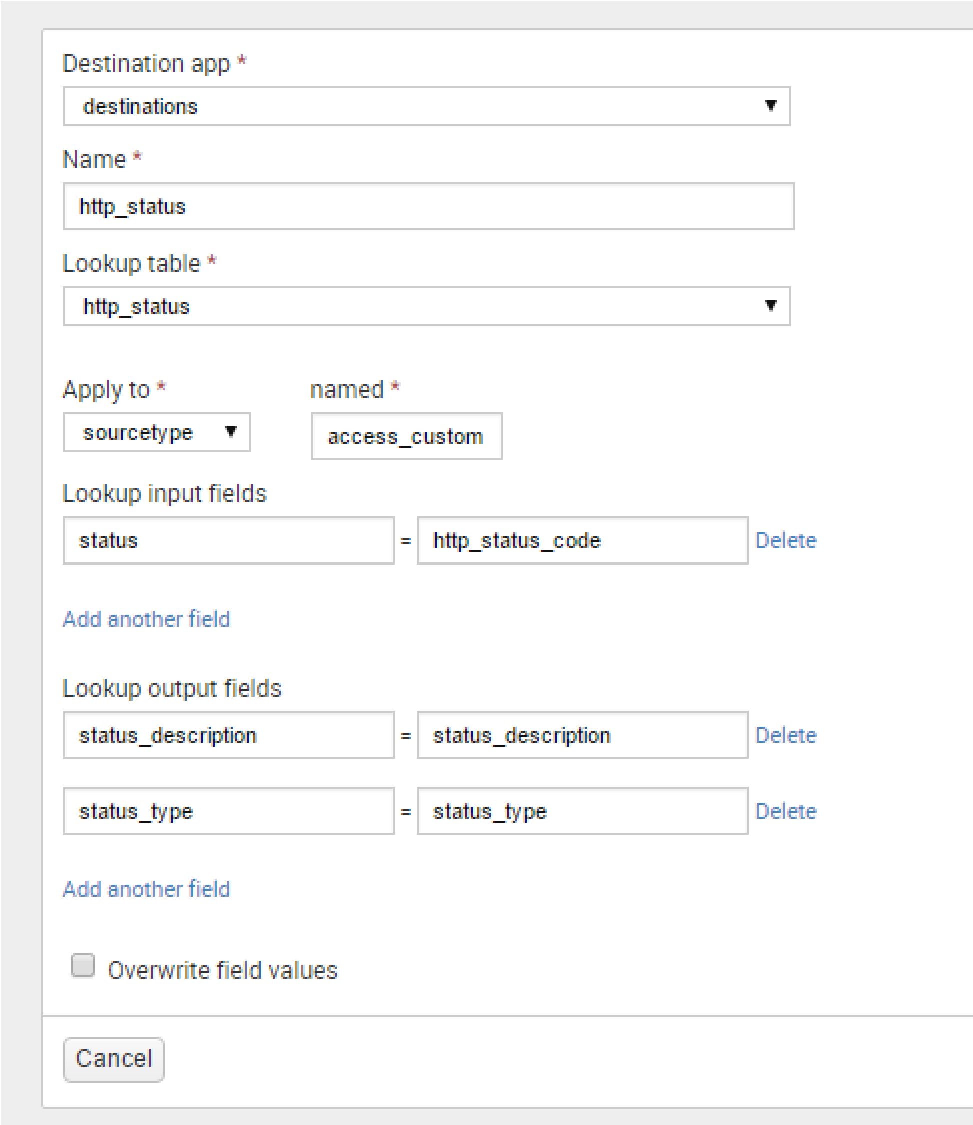


status	count	percent	status_description	status_type
301	37	21.637427	Moved Permanently	Redirection
200	37	21.637427	OK	Successful
500	36	21.052632	Internal Server Error	Server Error
404	32	18.713450	Not Found	Client Error
302	29	16.959064	Found	Redirection



Create and configure lookups.

	Actions
Lookup table files List existing lookup tables or upload a new file.	Add new
Lookup definitions Edit existing lookup definitions or define a new file-based or external lookup.	Add new
Automatic lookups Edit existing automatic lookups or configure a new lookup to run automatically.	Add new



Destination app *
destinations

Name *
http_status

Lookup table *
http_status

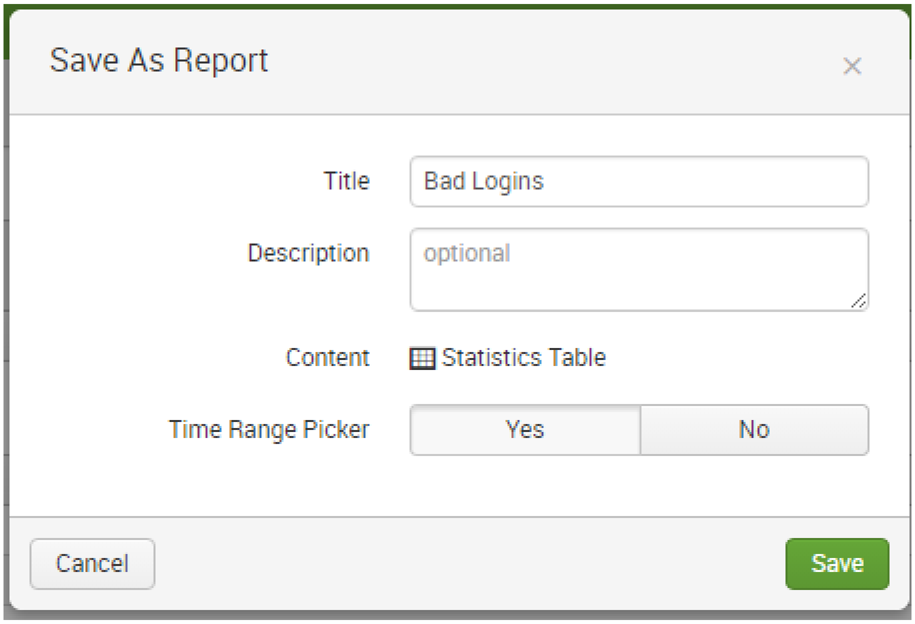
Apply to *
sourcetype

named *
access_custom

Lookup input fields
status = http_status_code

Lookup output fields
status_description = status_description
status_type = status_type

□ Overwrite field values

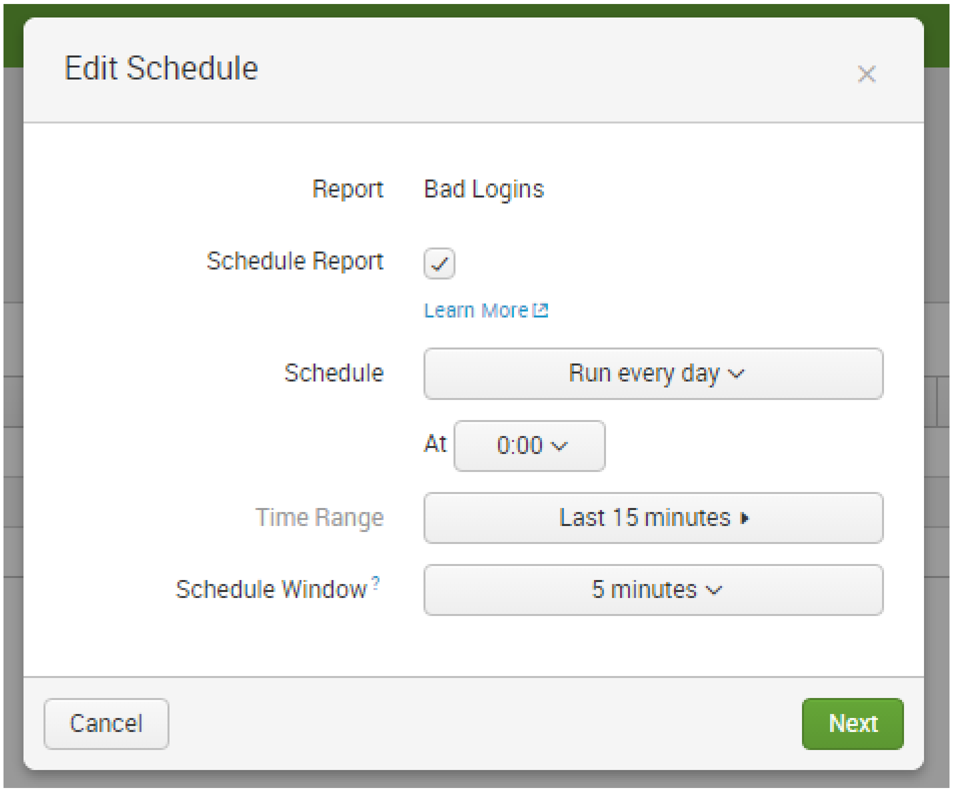

Save As Report

Title: Bad Logins

Description: optional

Content: Statistics Table

Time Range Picker: Yes | No


Edit Schedule

Report: Bad Logins

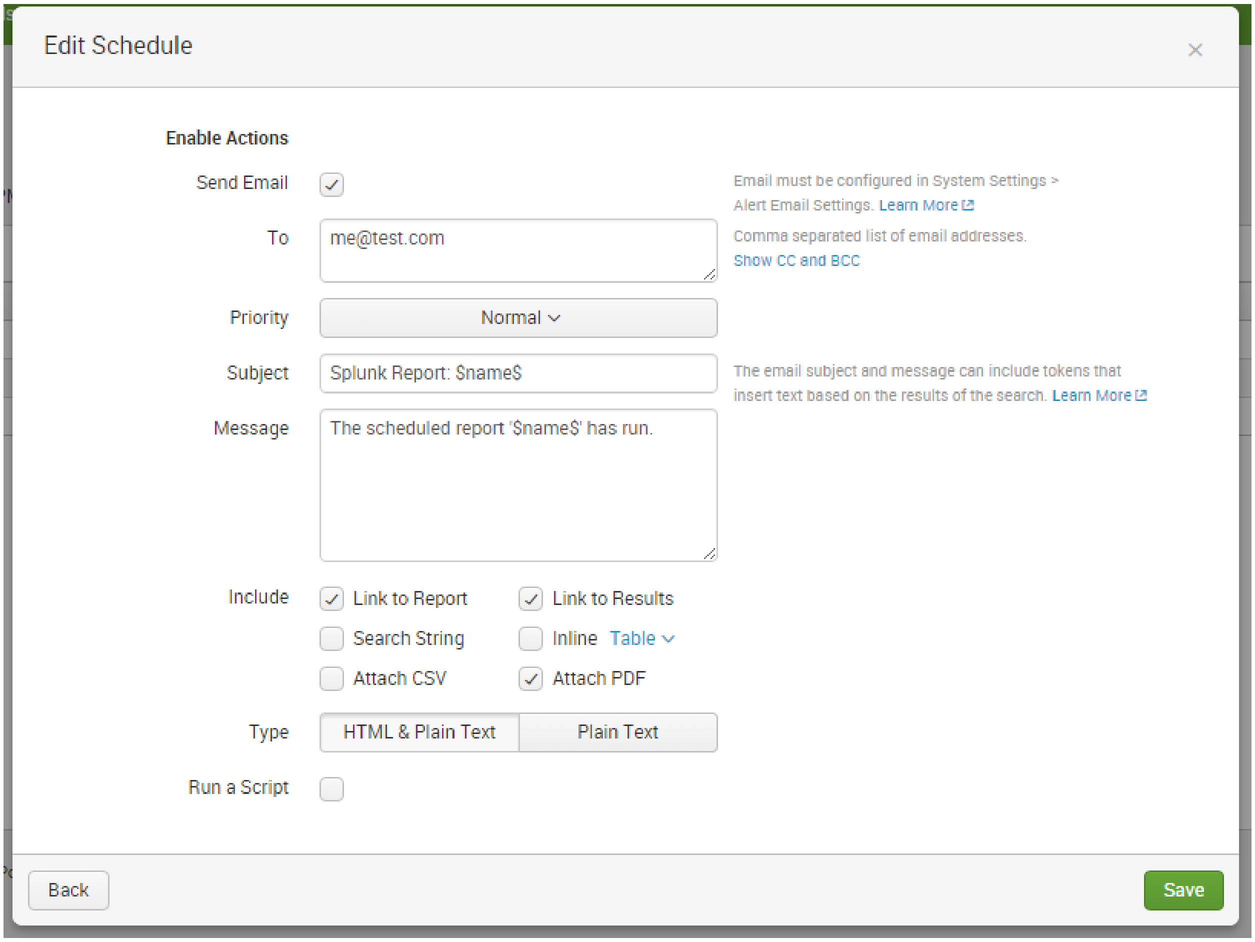
Schedule Report: ☑

Schedule: Run every day

At: 0:00

Time Range: Last 15 minutes

Schedule Window: 5 minutes



Edit Schedule ×

Enable Actions

Send Email ☑ — Email must be configured in System Settings > Alert Email Settings. Learn More

To: me@test.com — Comma separated list of email addresses. Show CC and BCC

Priority: Normal

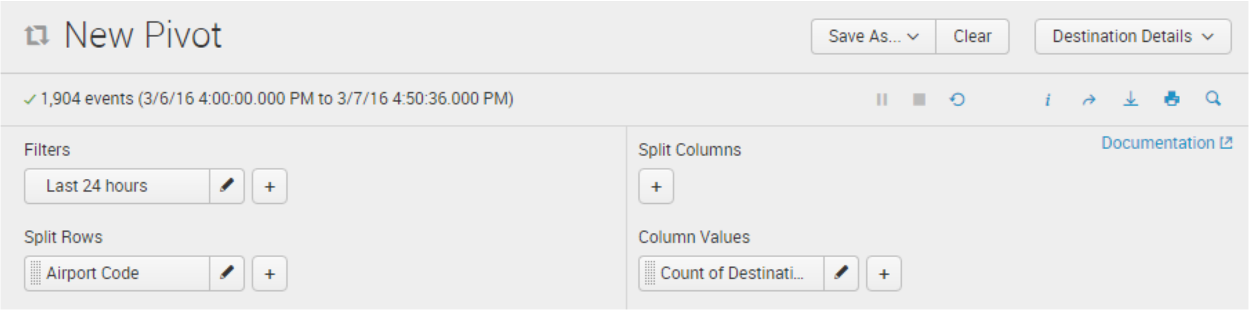
Subject: Splunk Report: $name$ — The email subject and message can include tokens that insert text based on the results of the search. Learn More

Message: The scheduled report '$name$' has run.

Include: ☑ Link to Report ☑ Link to Results
□ Search String □ Inline Table
□ Attach CSV ☑ Attach PDF

Type: HTML & Plain Text | Plain Text

Run a Script □



New Pivot

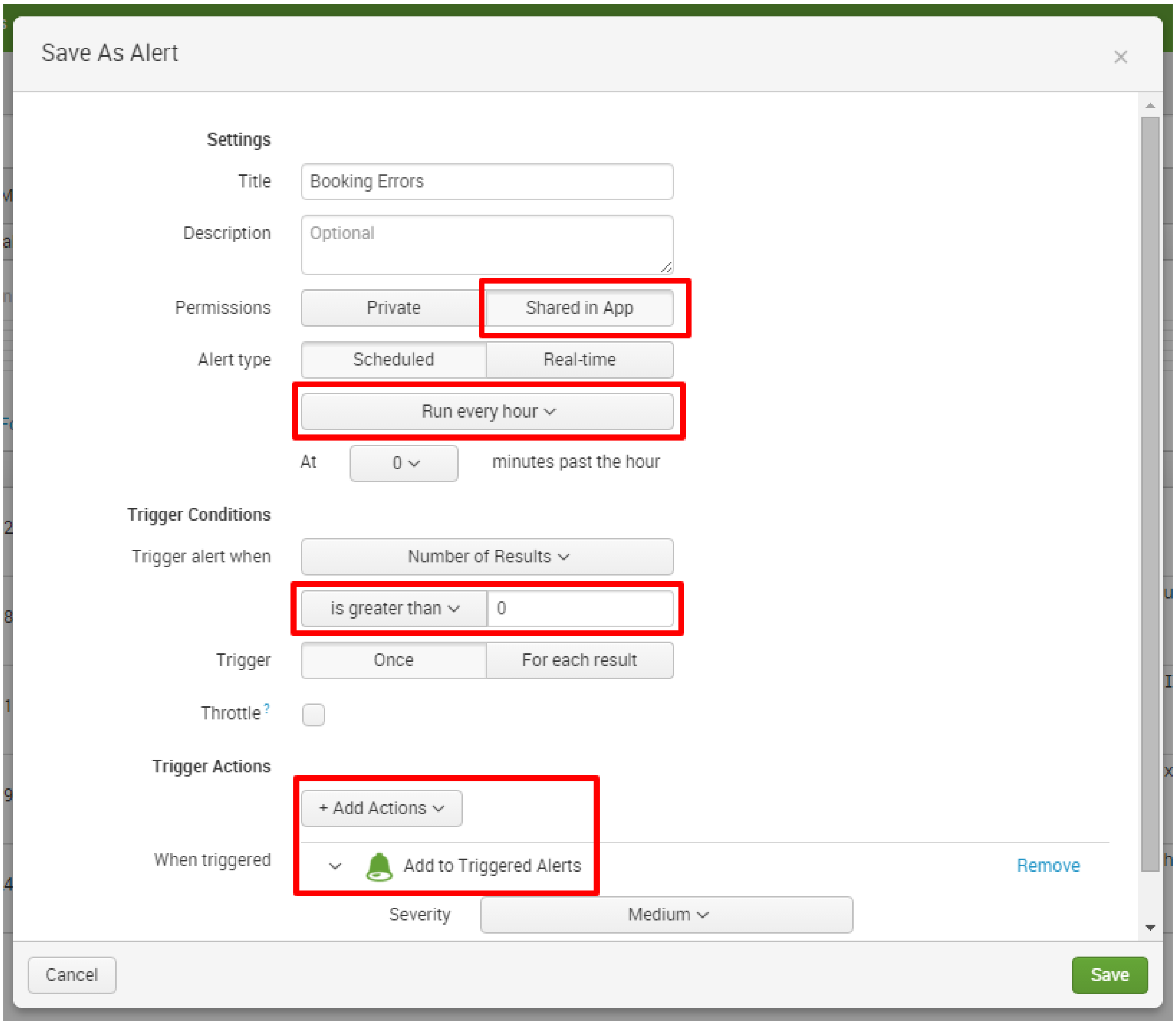
✓ 1,904 events (3/6/16 4:00:00.000 PM to 3/7/16 4:50:36.000 PM)

Filters: Last 24 hours

Split Rows: Airport Code

Split Columns

Column Values: Count of Destinati...



Save As Alert

Settings

Title: Booking Errors

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Trigger Conditions

Trigger alert when: Number of Results

is greater than 0

Trigger: Once | For each result

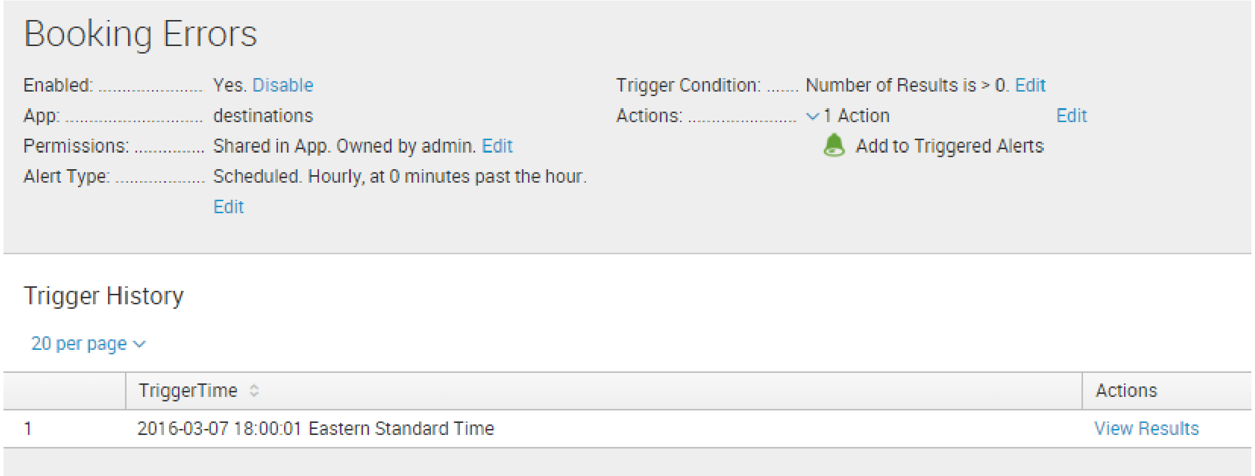
Throttle ? □

Trigger Actions

+ Add Actions

When triggered: Add to Triggered Alerts — Remove

Severity: Medium



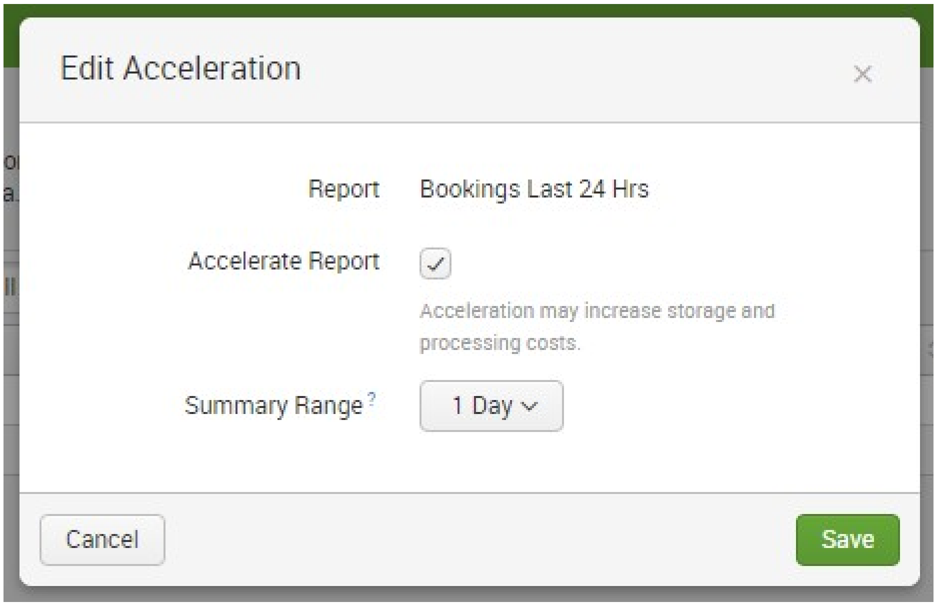
Booking Errors

Enabled:	Yes. Disable	Trigger Condition:	Number of Results is > 0. Edit
App:	destinations	Actions:	1 Action Edit
Permissions:	Shared in App. Owned by admin. Edit		Add to Triggered Alerts
Alert Type:	Scheduled. Hourly, at 0 minutes past the hour. Edit		

Trigger History

20 per page

	TriggerTime	Actions
1	2016-03-07 18:00:01 Eastern Standard Time	View Results



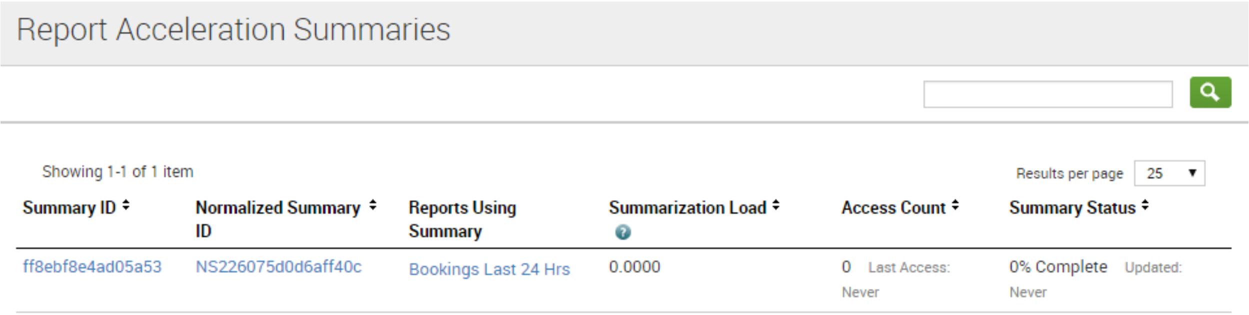
Edit Acceleration

Report: Bookings Last 24 Hrs

Accelerate Report ☑

Acceleration may increase storage and processing costs.

Summary Range ?: 1 Day

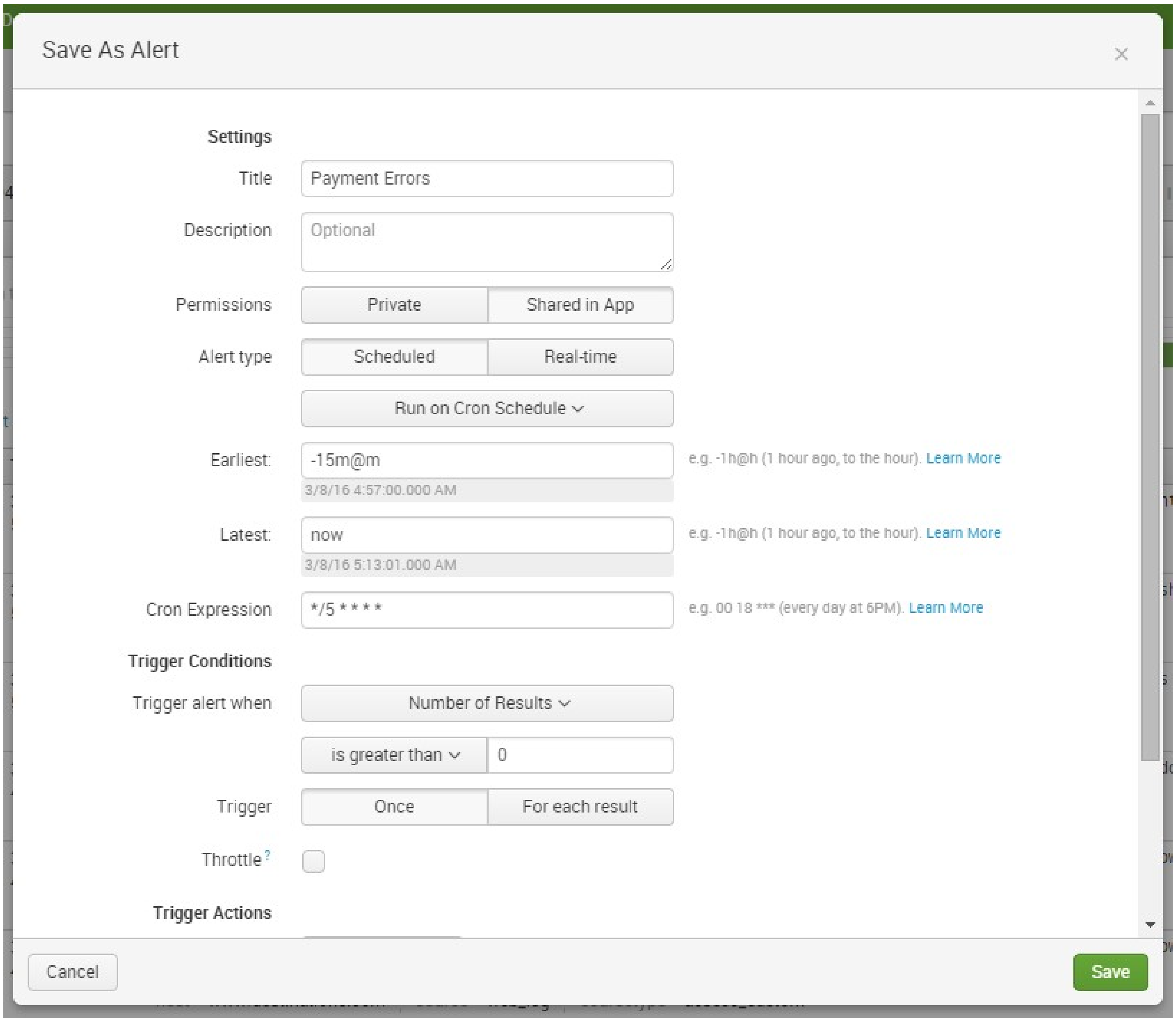


Report Acceleration Summaries

Showing 1-1 of 1 item

Results per page 25

Summary ID	Normalized Summary ID	Reports Using Summary	Summarization Load	Access Count	Summary Status
ff8ebf8e4ad05a53	NS226075d0d6aff40c	Bookings Last 24 Hrs	0.0000	0 Last Access: Never	0% Complete Updated: Never



Save As Alert

Settings

Title: Payment Errors

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run on Cron Schedule

Earliest: -15m@m
3/8/16 4:57:00.000 AM
e.g. -1h@h (1 hour ago, to the hour). Learn More

Latest: now
3/8/16 5:13:01.000 AM
e.g. -1h@h (1 hour ago, to the hour). Learn More

Cron Expression: */5 * * * *
e.g. 00 18 *** (every day at 6PM). Learn More

Trigger Conditions

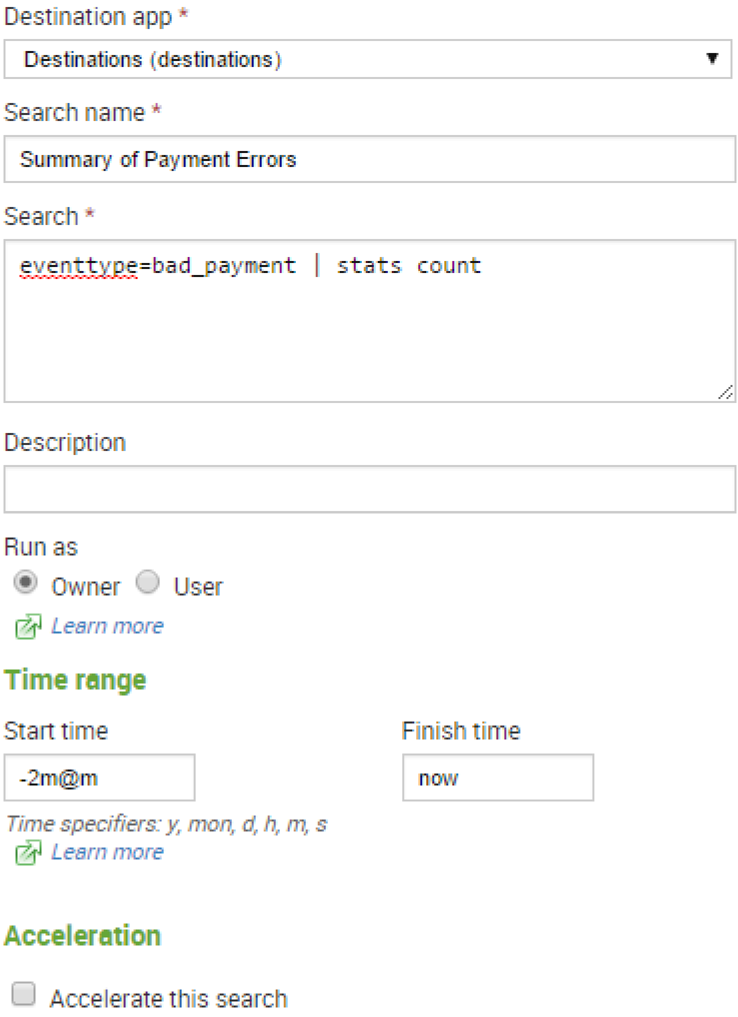
Trigger alert when: Number of Results

is greater than 0

Trigger: Once | For each result

Throttle? □

Trigger Actions



Destination app *

Destinations (destinations) ▼

Search name *

Summary of Payment Errors

Search *

```
eventtype=bad_payment | stats count
```

Description

Run as

● Owner ○ User

Time range

Start time

-2m@m

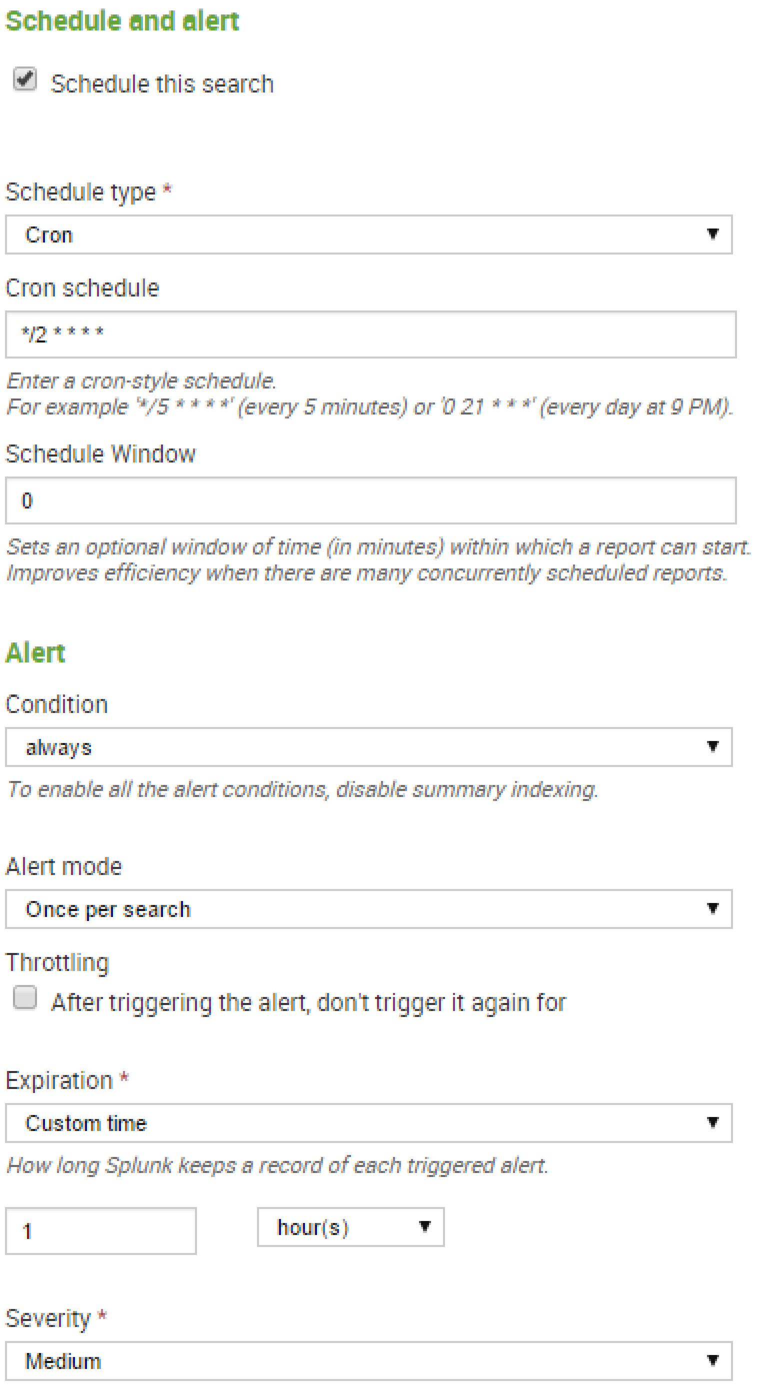
Finish time

now

Time specifiers: y, mon, d, h, m, s

Acceleration

□ Accelerate this search



Schedule and alert

☑ Schedule this search

Schedule type *

Cron ▾

Cron schedule

*/2 * * * *

Enter a cron-style schedule.
For example '/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).*

Schedule Window

0

Sets an optional window of time (in minutes) within which a report can start.
Improves efficiency when there are many concurrently scheduled reports.

Alert

Condition

always ▾

To enable all the alert conditions, disable summary indexing.

Alert mode

Once per search ▾

Throttling

□ After triggering the alert, don't trigger it again for

Expiration *

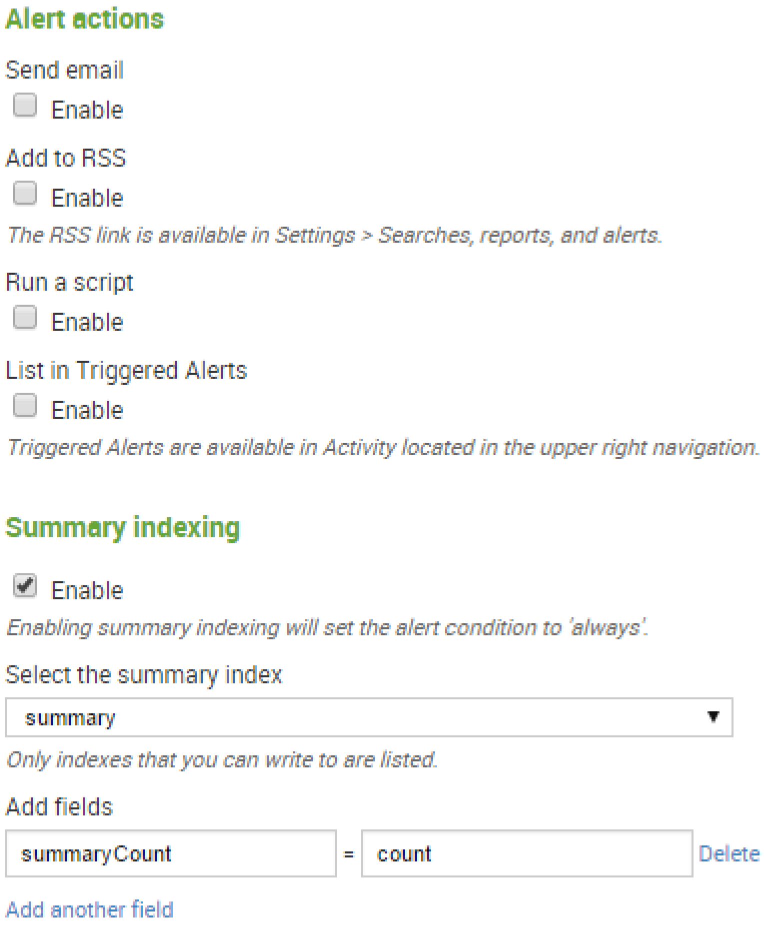
Custom time ▾

How long Splunk keeps a record of each triggered alert.

1 hour(s) ▾

Severity *

Medium ▾



Alert actions

Send email

☐ Enable

Add to RSS

☐ Enable

The RSS link is available in Settings > Searches, reports, and alerts.

Run a script

☐ Enable

List in Triggered Alerts

☐ Enable

Triggered Alerts are available in Activity located in the upper right navigation.

Summary indexing

☑ Enable

Enabling summary indexing will set the alert condition to 'always'.

Select the summary index

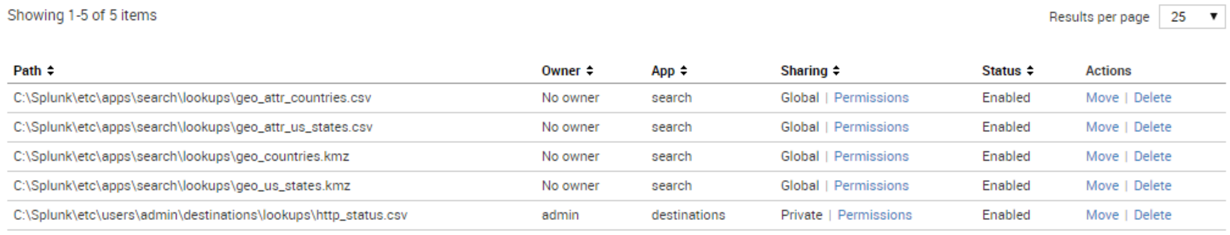
summary ▼

Only indexes that you can write to are listed.

Add fields

summaryCount = count Delete

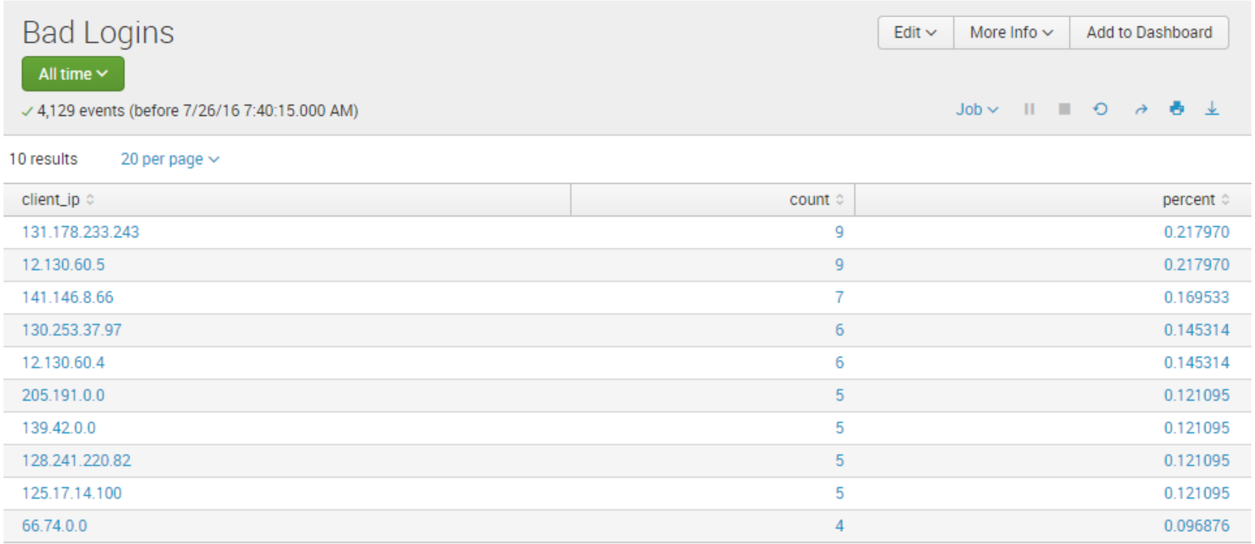
Add another field



Showing 1-5 of 5 items

Results per page 25 ▼

Path ⬍	Owner ⬍	App ⬍	Sharing ⬍	Status ⬍	Actions
C:\Splunk\etc\apps\search\lookups\geo_attr_countries.csv	No owner	search	Global | Permissions	Enabled	Move | Delete
C:\Splunk\etc\apps\search\lookups\geo_attr_us_states.csv	No owner	search	Global | Permissions	Enabled	Move | Delete
C:\Splunk\etc\apps\search\lookups\geo_countries.kmz	No owner	search	Global | Permissions	Enabled	Move | Delete
C:\Splunk\etc\apps\search\lookups\geo_us_states.kmz	No owner	search	Global | Permissions	Enabled	Move | Delete
C:\Splunk\etc\users\admin\destinations\lookups\http_status.csv	admin	destinations	Private | Permissions	Enabled	Move | Delete



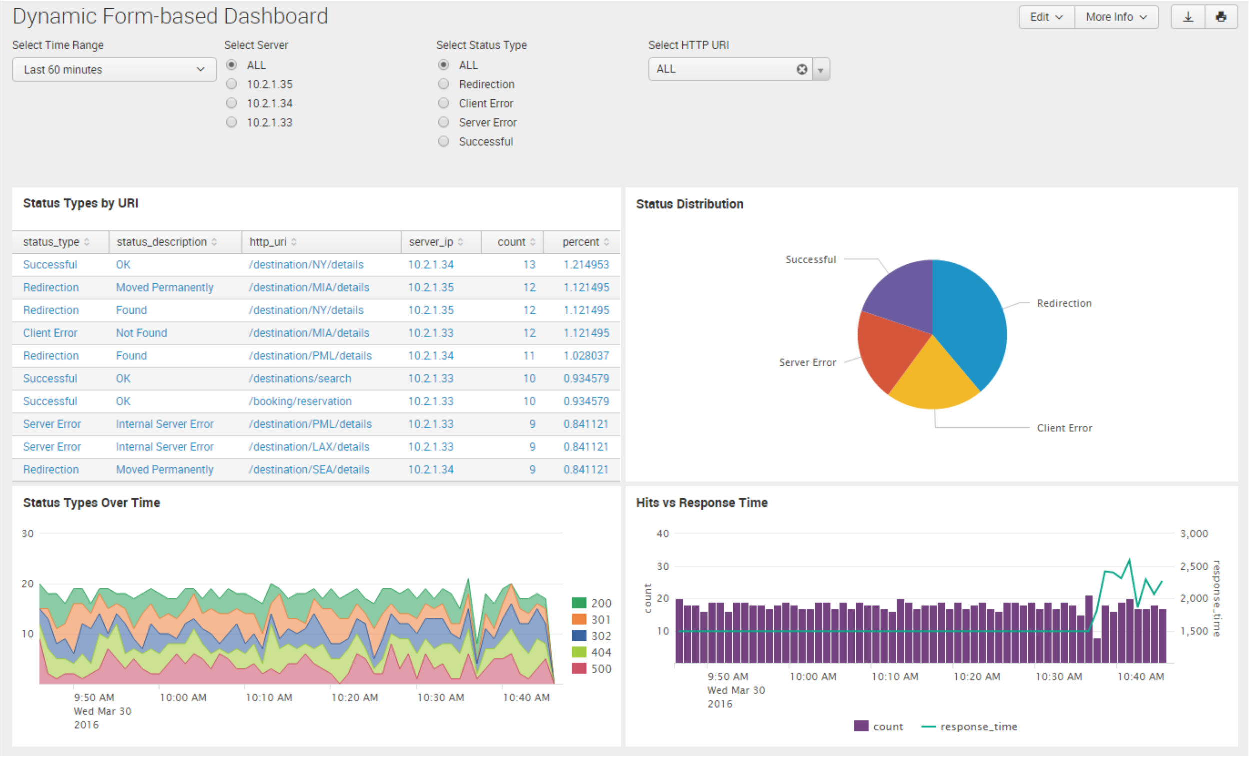
Bad Logins

✓ 4,129 events (before 7/26/16 7:40:15.000 AM)

10 results

client_ip	count	percent
131.178.233.243	9	0.217970
12.130.60.5	9	0.217970
141.146.8.66	7	0.169533
130.253.37.97	6	0.145314
12.130.60.4	6	0.145314
205.191.0.0	5	0.121095
139.42.0.0	5	0.121095
128.241.220.82	5	0.121095
125.17.14.100	5	0.121095
66.74.0.0	4	0.096876

Chapter 6: Panes of Glass



Dynamic Form-based Dashboard

Select Time Range: Last 60 minutes

Select Server
● ALL
○ 10.2.1.35
○ 10.2.1.34
○ 10.2.1.33

Select Status Type
● ALL
○ Redirection
○ Client Error
○ Server Error
○ Successful

Select HTTP URI: ALL

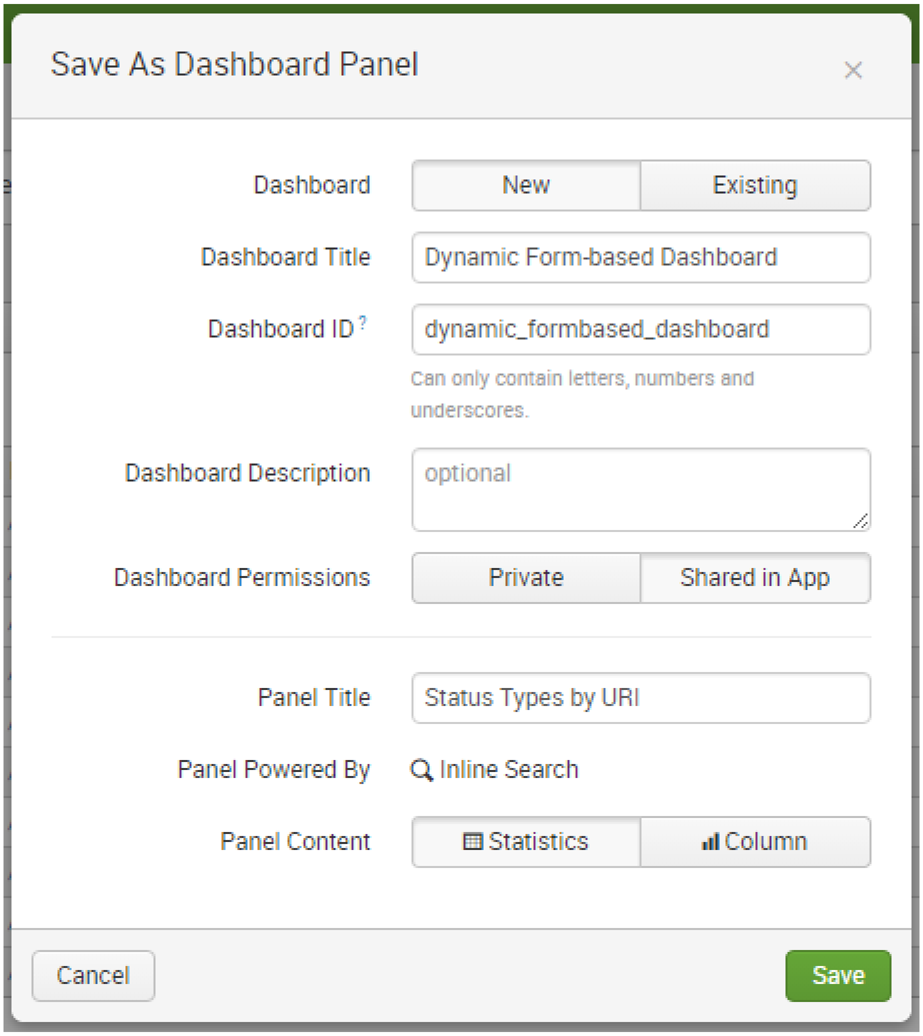
Status Types by URI

status_type	status_description	http_uri	server_ip	count	percent
Successful	OK	/destination/NY/details	10.2.1.34	13	1.214953
Redirection	Moved Permanently	/destination/MIA/details	10.2.1.35	12	1.121495
Redirection	Found	/destination/NY/details	10.2.1.35	12	1.121495
Client Error	Not Found	/destination/MIA/details	10.2.1.33	12	1.121495
Redirection	Found	/destination/PML/details	10.2.1.34	11	1.028037
Successful	OK	/destinations/search	10.2.1.33	10	0.934579
Successful	OK	/booking/reservation	10.2.1.33	10	0.934579
Server Error	Internal Server Error	/destination/PML/details	10.2.1.33	9	0.841121
Server Error	Internal Server Error	/destination/LAX/details	10.2.1.33	9	0.841121
Redirection	Moved Permanently	/destination/SEA/details	10.2.1.34	9	0.841121

Status Distribution

Status Types Over Time

Hits vs Response Time



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Dynamic Form-based Dashboard

Dashboard ID: dynamic_formbased_dashboard

Can only contain letters, numbers and underscores.

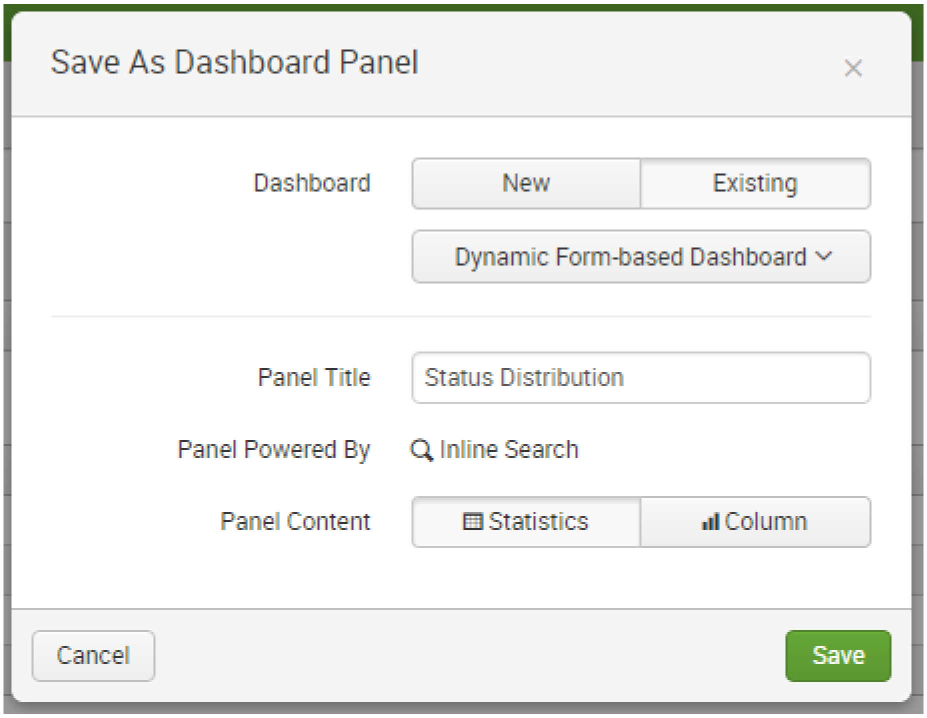
Dashboard Description: optional

Dashboard Permissions: Private | Shared in App

Panel Title: Status Types by URI

Panel Powered By: Inline Search

Panel Content: Statistics | Column



Save As Dashboard Panel

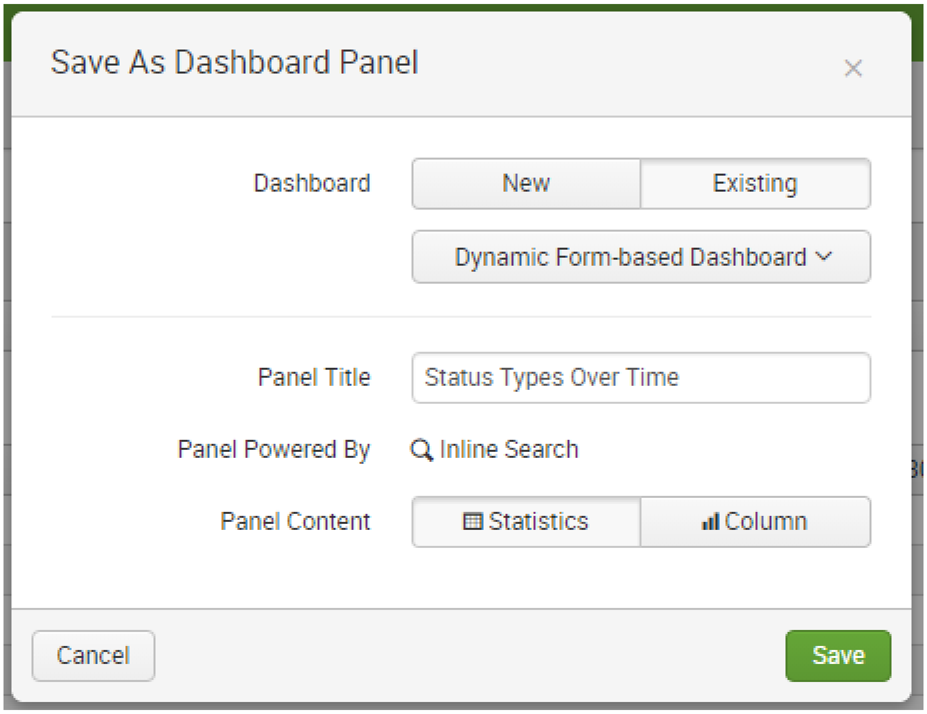
Dashboard: New | Existing

Dynamic Form-based Dashboard

Panel Title: Status Distribution

Panel Powered By: Inline Search

Panel Content: Statistics | Column



Save As Dashboard Panel

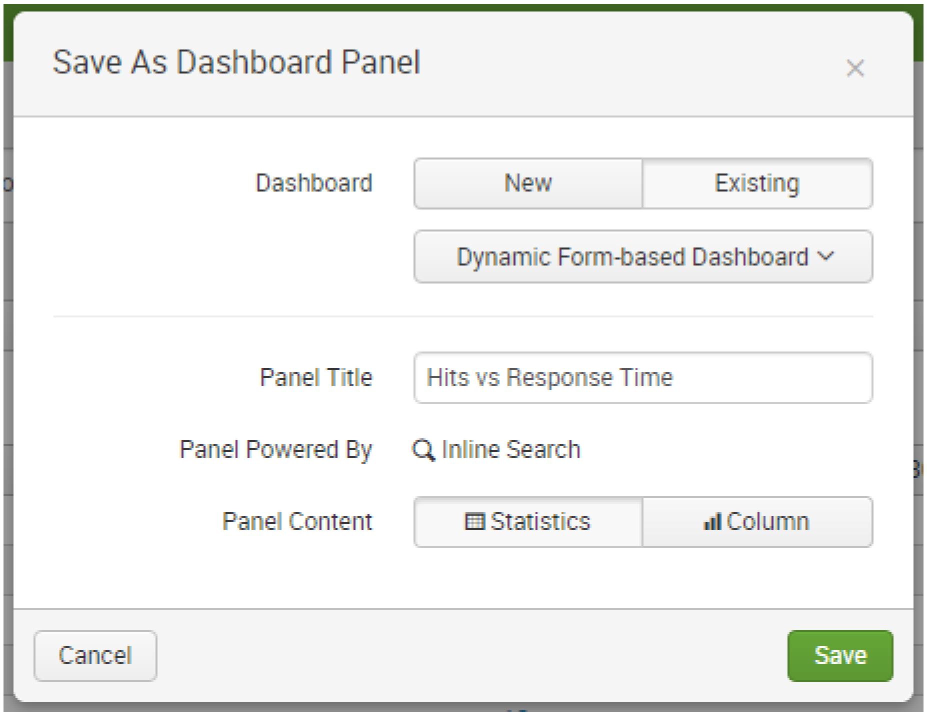
Dashboard: New | Existing

Dynamic Form-based Dashboard

Panel Title: Status Types Over Time

Panel Powered By: Inline Search

Panel Content: Statistics | Column



Save As Dashboard Panel

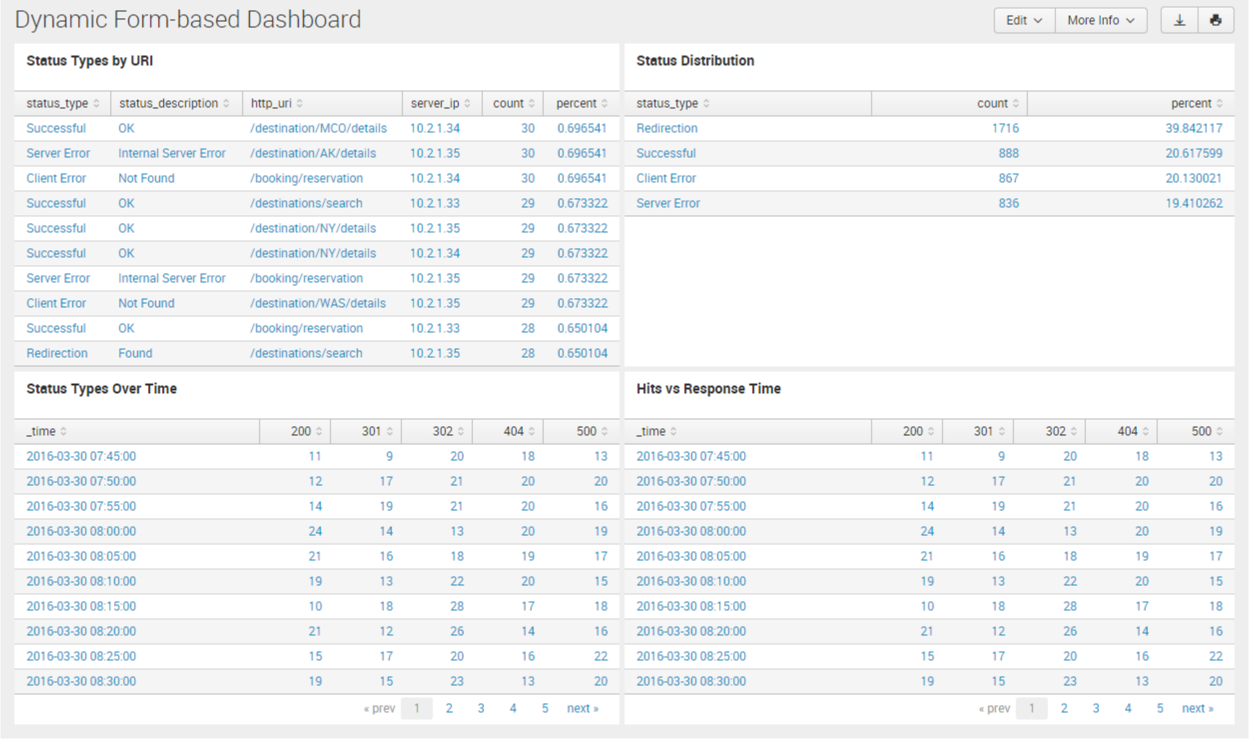
Dashboard: New | Existing

Dynamic Form-based Dashboard

Panel Title: Hits vs Response Time

Panel Powered By: Inline Search

Panel Content: Statistics | Column



Dynamic Form-based Dashboard

Status Types by URI

status_type	status_description	http_uri	server_ip	count	percent
Successful	OK	/destination/MCO/details	10.2.1.34	30	0.696541
Server Error	Internal Server Error	/destination/AK/details	10.2.1.35	30	0.696541
Client Error	Not Found	/booking/reservation	10.2.1.34	30	0.696541
Successful	OK	/destinations/search	10.2.1.33	29	0.673322
Successful	OK	/destination/NY/details	10.2.1.35	29	0.673322
Successful	OK	/destination/NY/details	10.2.1.34	29	0.673322
Server Error	Internal Server Error	/booking/reservation	10.2.1.35	29	0.673322
Client Error	Not Found	/destination/WAS/details	10.2.1.35	29	0.673322
Successful	OK	/booking/reservation	10.2.1.33	28	0.650104
Redirection	Found	/destinations/search	10.2.1.35	28	0.650104

Status Distribution

status_type	count	percent
Redirection	1716	39.842117
Successful	888	20.617599
Client Error	867	20.130021
Server Error	836	19.410262

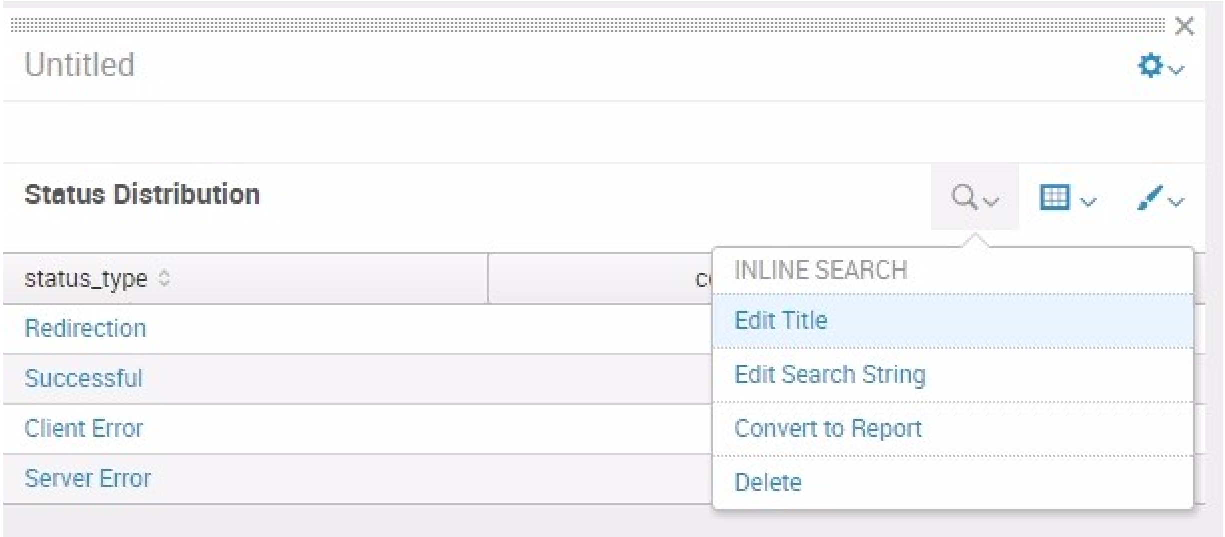
Status Types Over Time

_time	200	301	302	404	500
2016-03-30 07:45:00	11	9	20	18	13
2016-03-30 07:50:00	12	17	21	20	20
2016-03-30 07:55:00	14	19	21	20	16
2016-03-30 08:00:00	24	14	13	20	19
2016-03-30 08:05:00	21	16	18	19	17
2016-03-30 08:10:00	19	13	22	20	15
2016-03-30 08:15:00	10	18	28	17	18
2016-03-30 08:20:00	21	12	26	14	16
2016-03-30 08:25:00	15	17	20	16	22
2016-03-30 08:30:00	19	15	23	13	20

Hits vs Response Time

_time	200	301	302	404	500
2016-03-30 07:45:00	11	9	20	18	13
2016-03-30 07:50:00	12	17	21	20	20
2016-03-30 07:55:00	14	19	21	20	16
2016-03-30 08:00:00	24	14	13	20	19
2016-03-30 08:05:00	21	16	18	19	17
2016-03-30 08:10:00	19	13	22	20	15
2016-03-30 08:15:00	10	18	28	17	18
2016-03-30 08:20:00	21	12	26	14	16
2016-03-30 08:25:00	15	17	20	16	22
2016-03-30 08:30:00	19	15	23	13	20

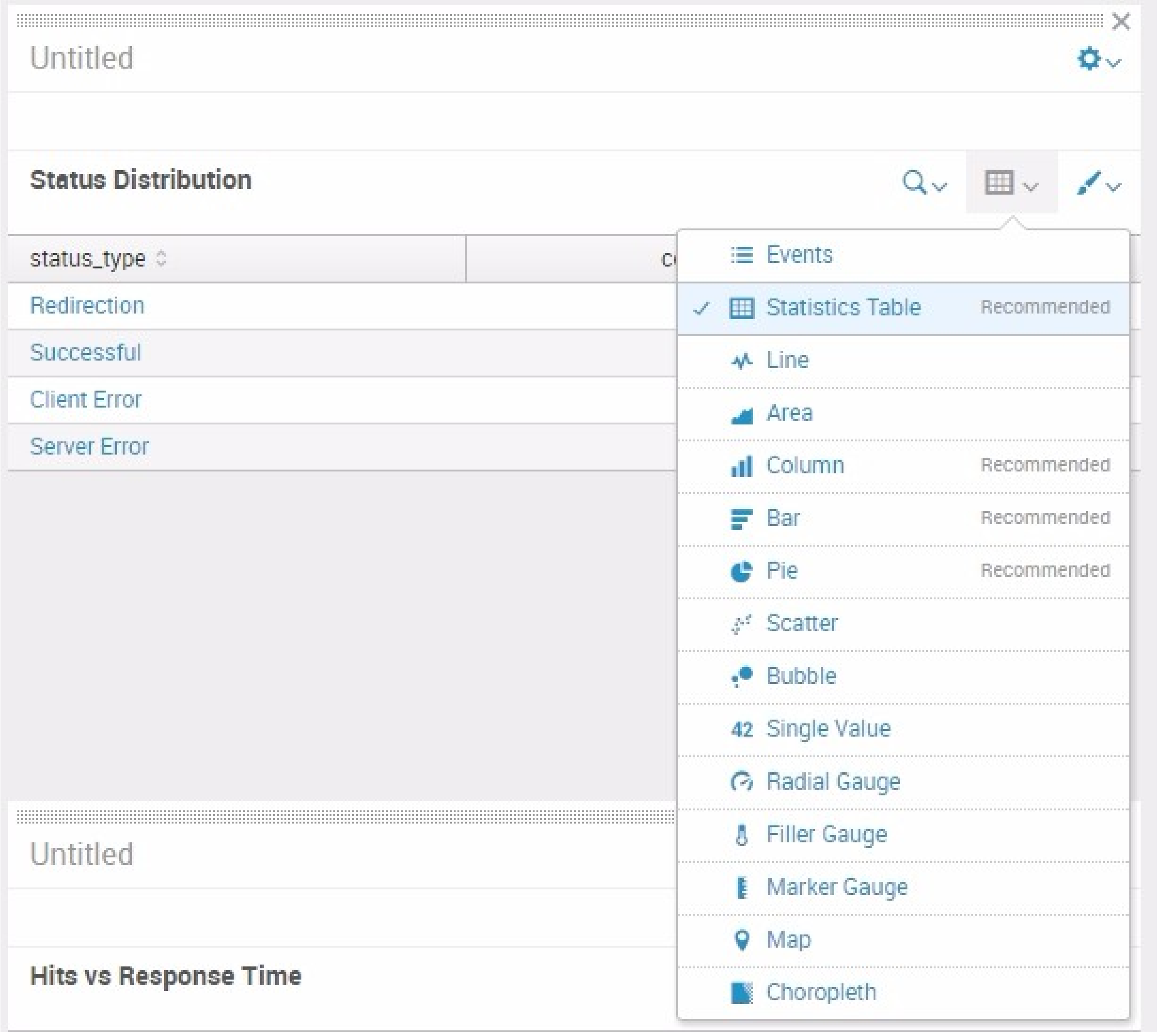
Status Distribution



Untitled

Status Distribution

status_type	c
Redirection	
Successful	
Client Error	
Server Error	



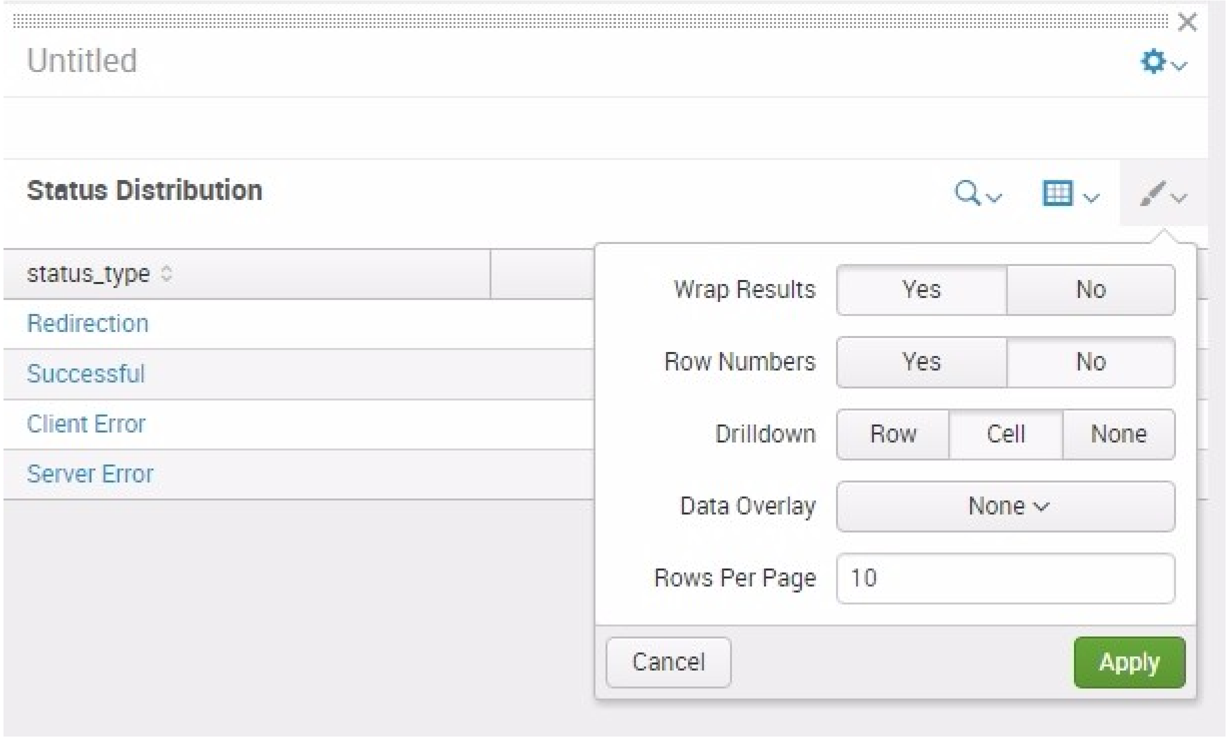
Untitled

Status Distribution

status_type	c
Redirection	
Successful	
Client Error	
Server Error	

Untitled

Hits vs Response Time



Untitled

Status Distribution

status_type
Redirection
Successful
Client Error
Server Error

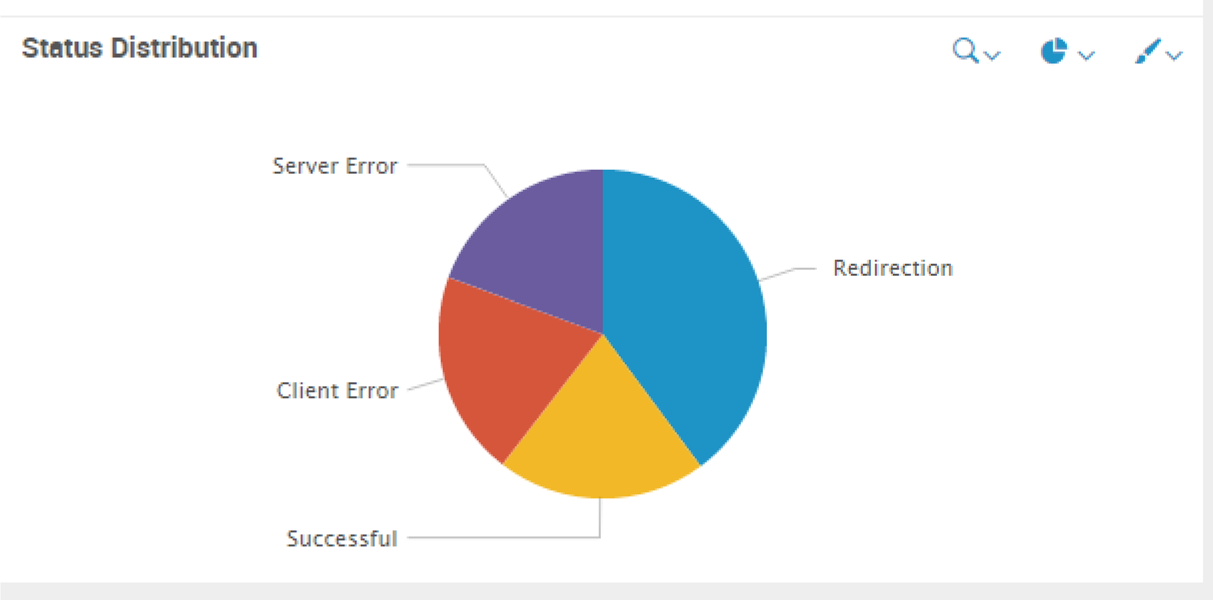
Wrap Results: Yes | No

Row Numbers: Yes | No

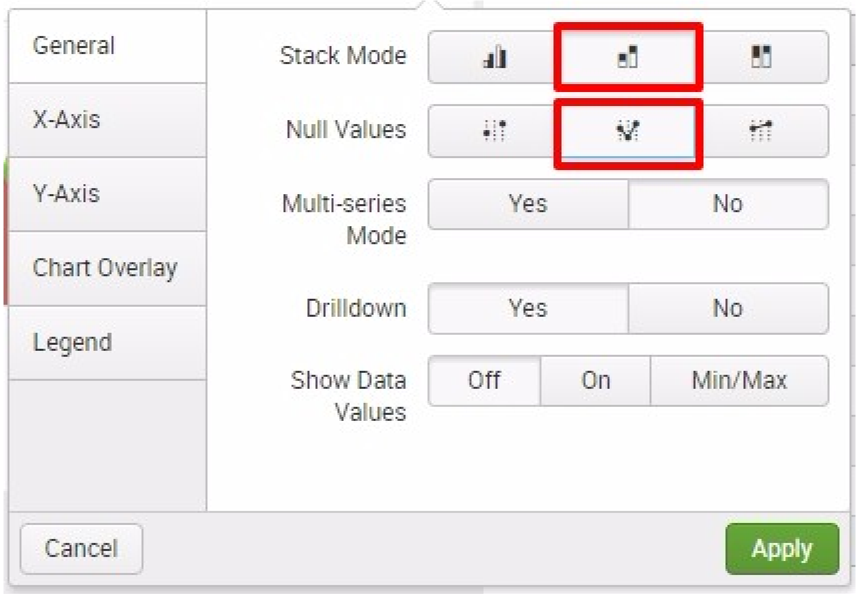
Drilldown: Row | Cell | None

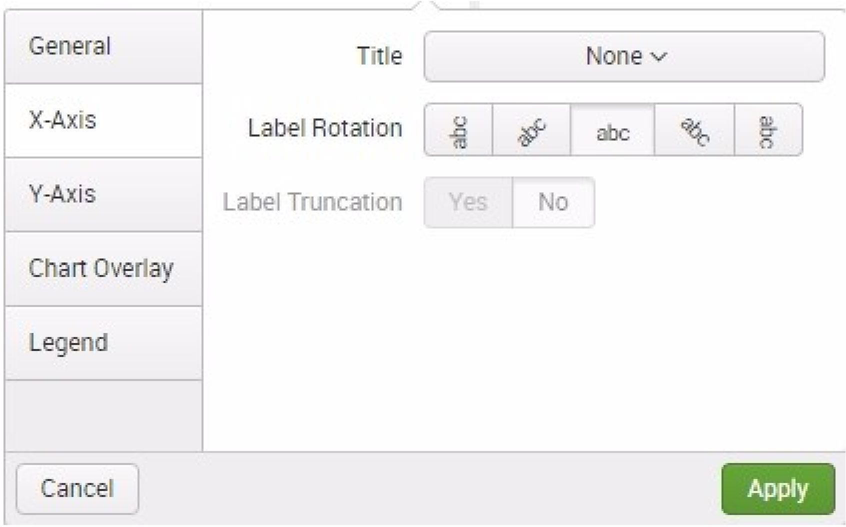
Data Overlay: None

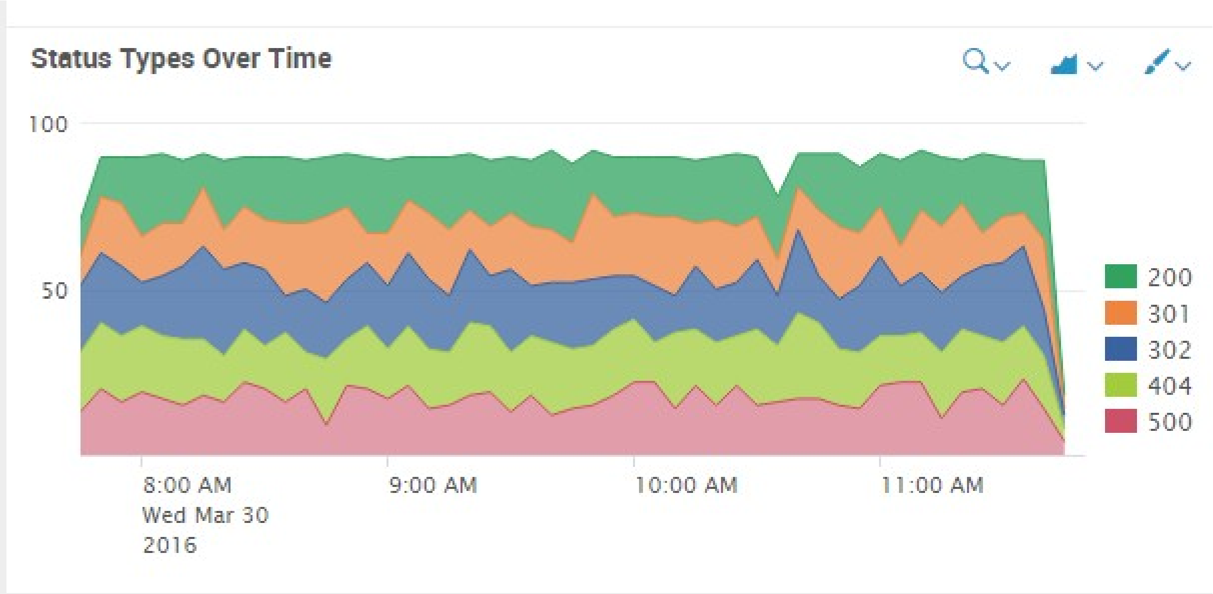
Rows Per Page: 10

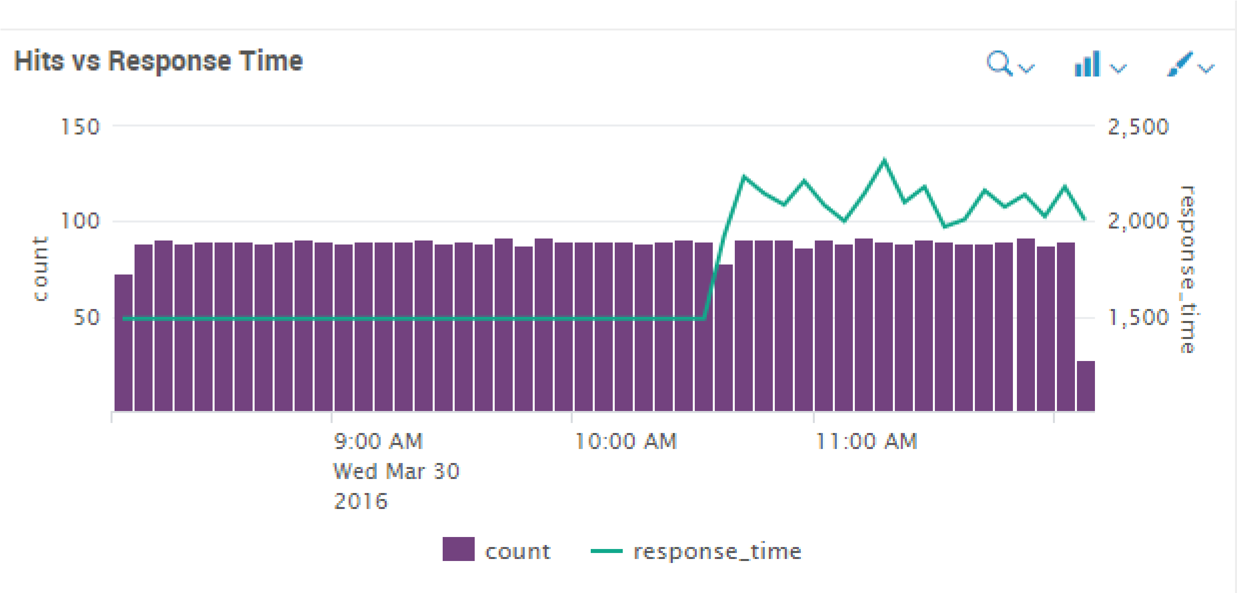


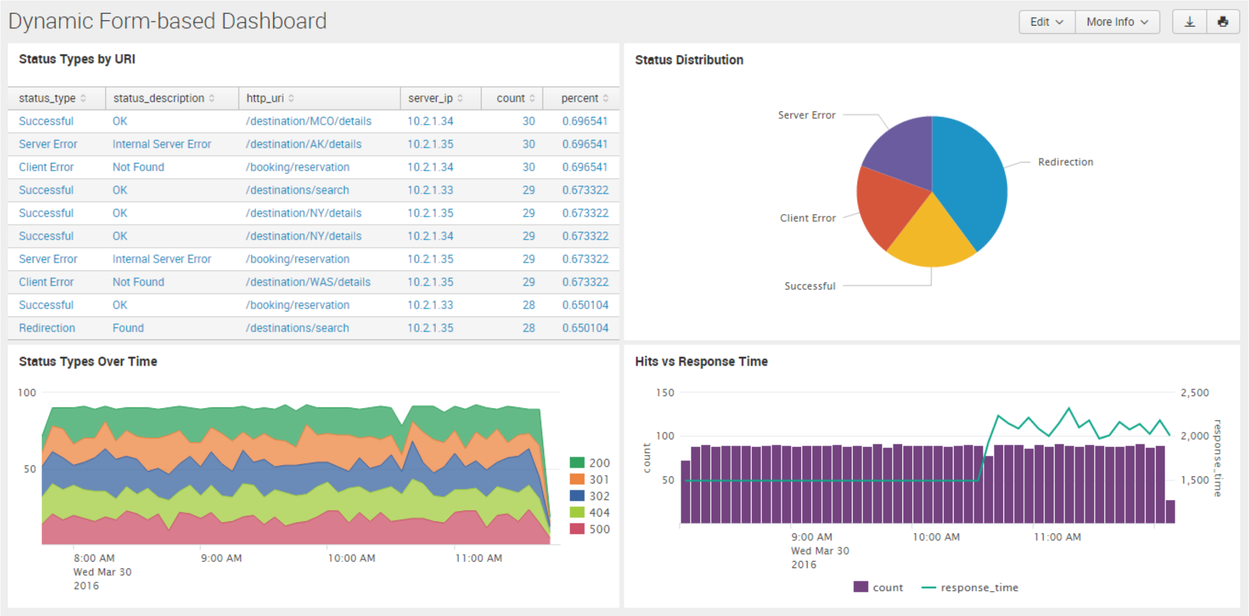
Status Distribution


General
X-Axis
Y-Axis
Chart Overlay
Legend
Stack Mode
Null Values
Multi-series Mode
Yes
No
Drilldown
Yes
No
Show Data Values
Off
On
Min/Max
Cancel
Apply


General
X-Axis
Y-Axis
Chart Overlay
Legend
Title
None
Label Rotation
abc
abc
abc
abc
abc
Label Truncation
Yes
No
Cancel
Apply

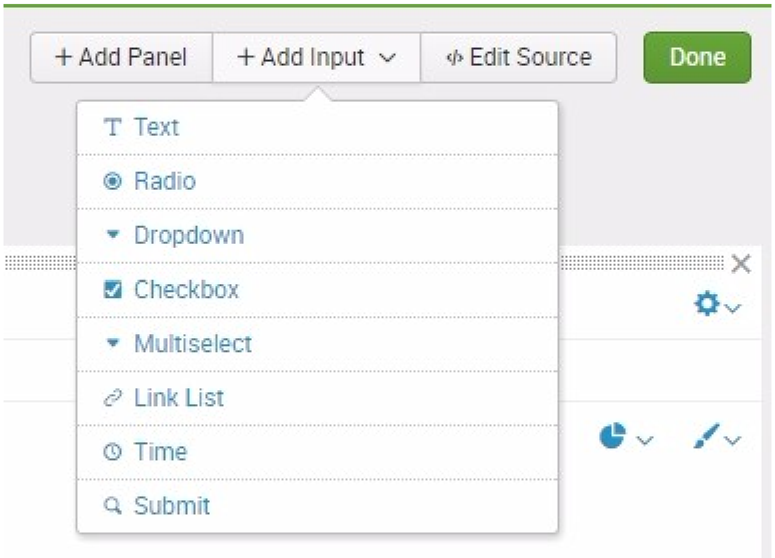

Status Types Over Time
100
50
8:00 AM
Wed Mar 30
2016
9:00 AM
10:00 AM
11:00 AM
200
301
302
404
500

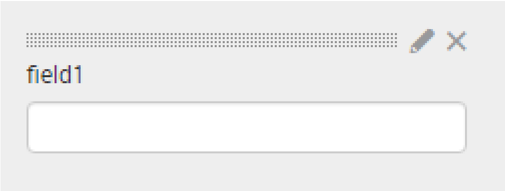

Hits vs Response Time
150
100
50
count
2,500
2,000
1,500
response_time
9:00 AM
Wed Mar 30
2016
10:00 AM
11:00 AM
count
response_time

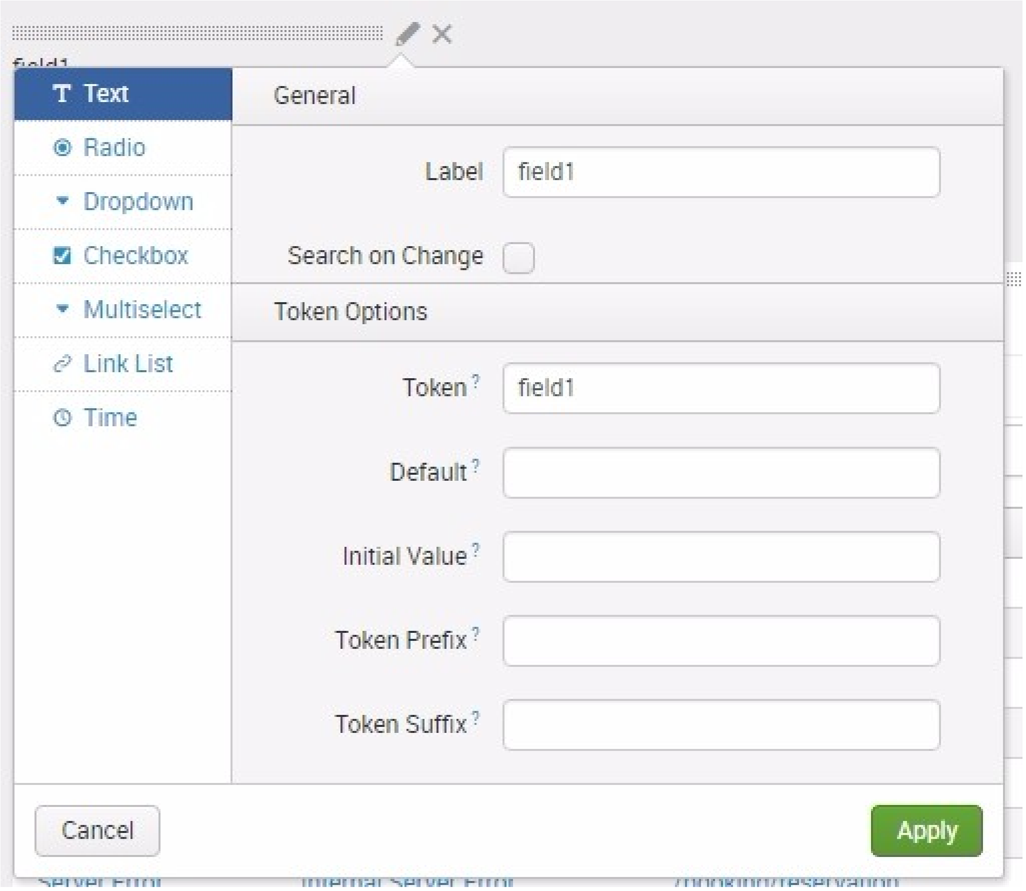


Status Types by URI

status_type	status_description	http_uri	server_ip	count	percent
Successful	OK	/destination/MCO/details	10.2.1.34	30	0.696541
Server Error	Internal Server Error	/destination/AK/details	10.2.1.35	30	0.696541
Client Error	Not Found	/booking/reservation	10.2.1.34	30	0.696541
Successful	OK	/destinations/search	10.2.1.33	29	0.673322
Successful	OK	/destination/NY/details	10.2.1.35	29	0.673322
Successful	OK	/destination/NY/details	10.2.1.34	29	0.673322
Server Error	Internal Server Error	/booking/reservation	10.2.1.35	29	0.673322
Client Error	Not Found	/destination/WAS/details	10.2.1.35	29	0.673322
Successful	OK	/booking/reservation	10.2.1.33	28	0.650104
Redirection	Found	/destinations/search	10.2.1.35	28	0.650104







General

Label: field1

Search on Change: □

Token Options

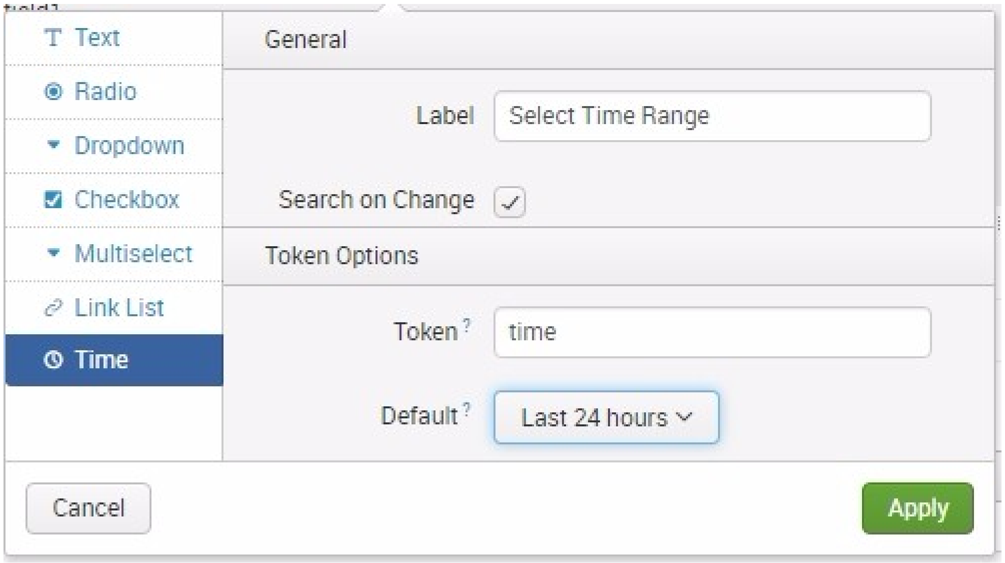
Token: field1

Default:

Initial Value:

Token Prefix:

Token Suffix:



General

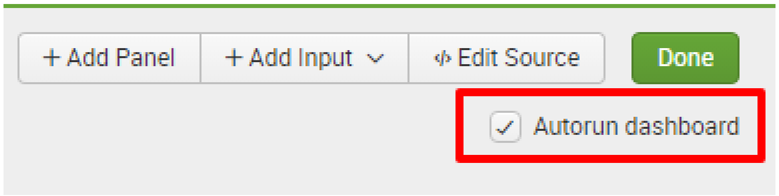
Label: Select Time Range

Search on Change: ☑

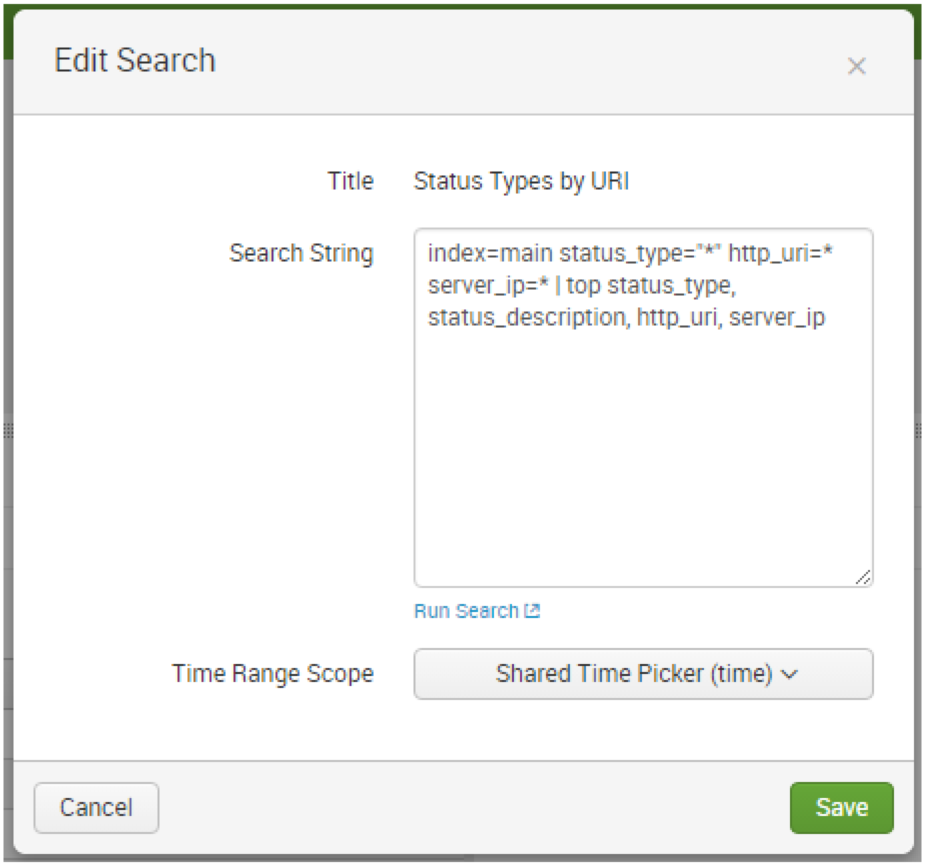
Token Options

Token: time

Default: Last 24 hours



☑ Autorun dashboard



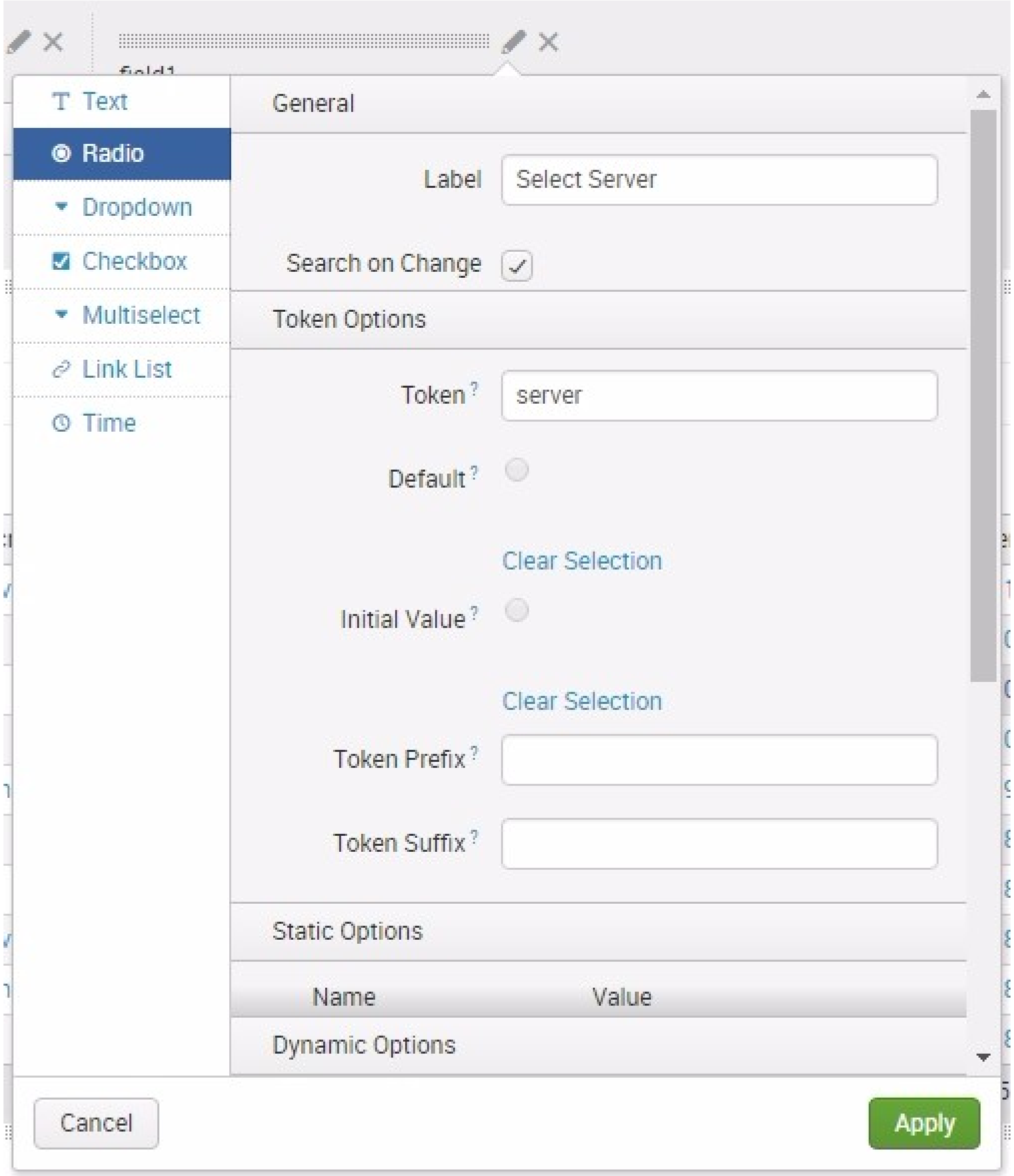
Edit Search

Title Status Types by URI

Search String

```
index=main status_type="*" http_uri=*
server_ip=* | top status_type,
status_description, http_uri, server_ip
```

Time Range Scope Shared Time Picker (time)



General

Label: Select Server

Search on Change ☑

Token Options

Token ?: server

Default ? ○

Initial Value ? ○

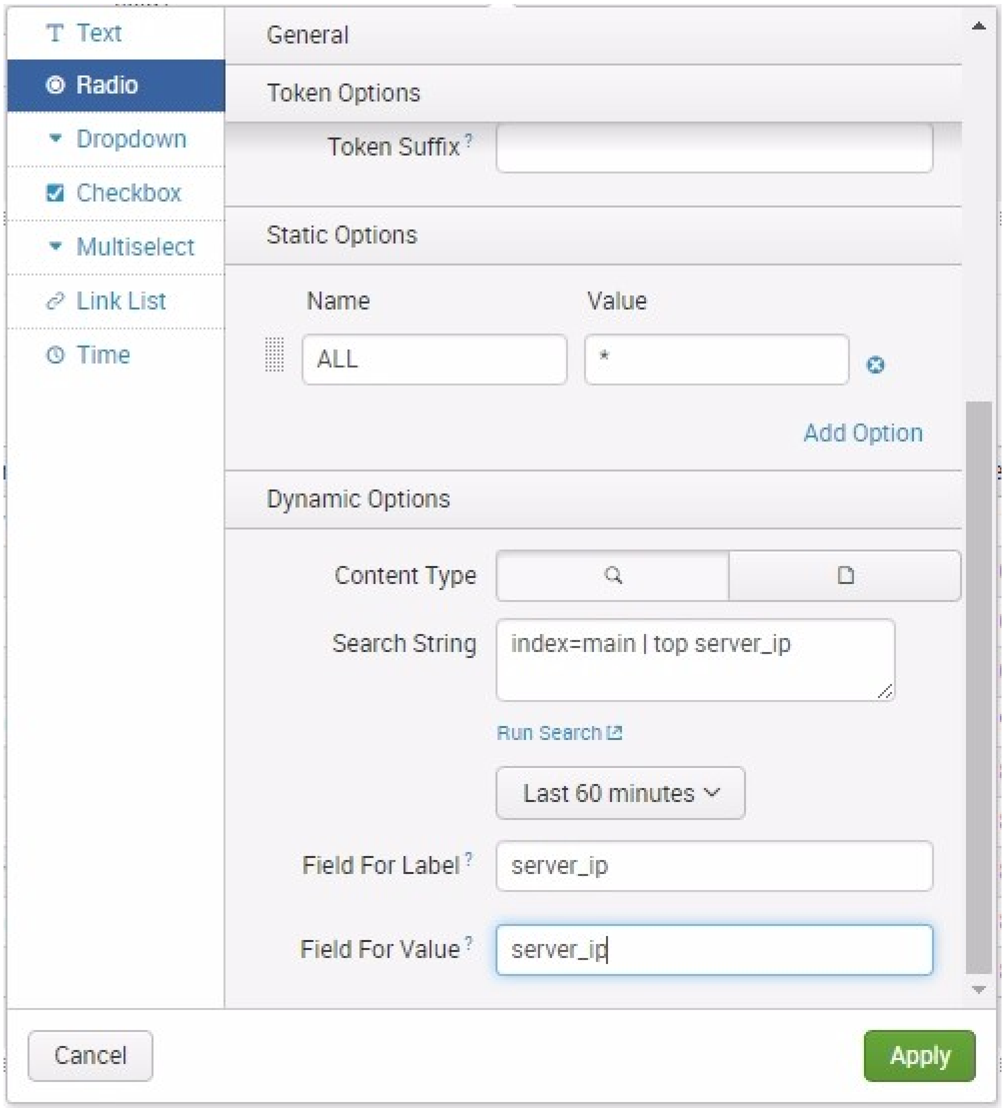
Token Prefix ?:

Token Suffix ?:

Static Options

Name	Value

Dynamic Options



Token Suffix ?

Static Options

Name	Value
ALL	*

Dynamic Options

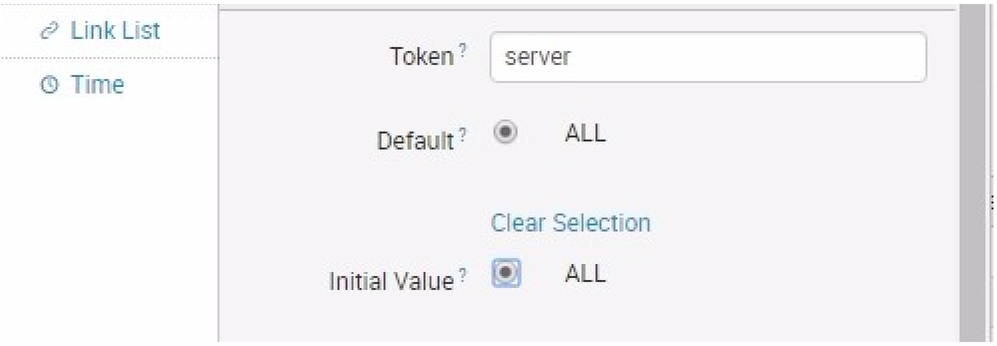
Content Type

Search String: index=main | top server_ip

Last 60 minutes

Field For Label ?: server_ip

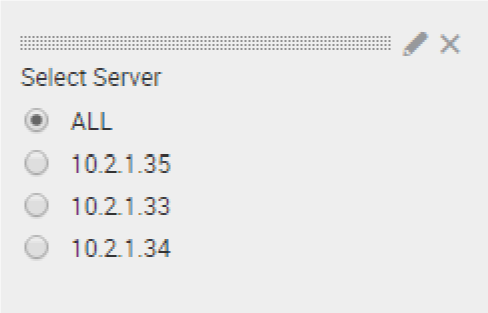
Field For Value ?: server_ip



Token ?: server

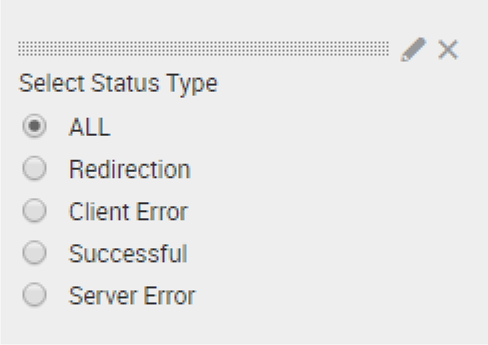
Default ?: ● ALL

Initial Value ?: ● ALL



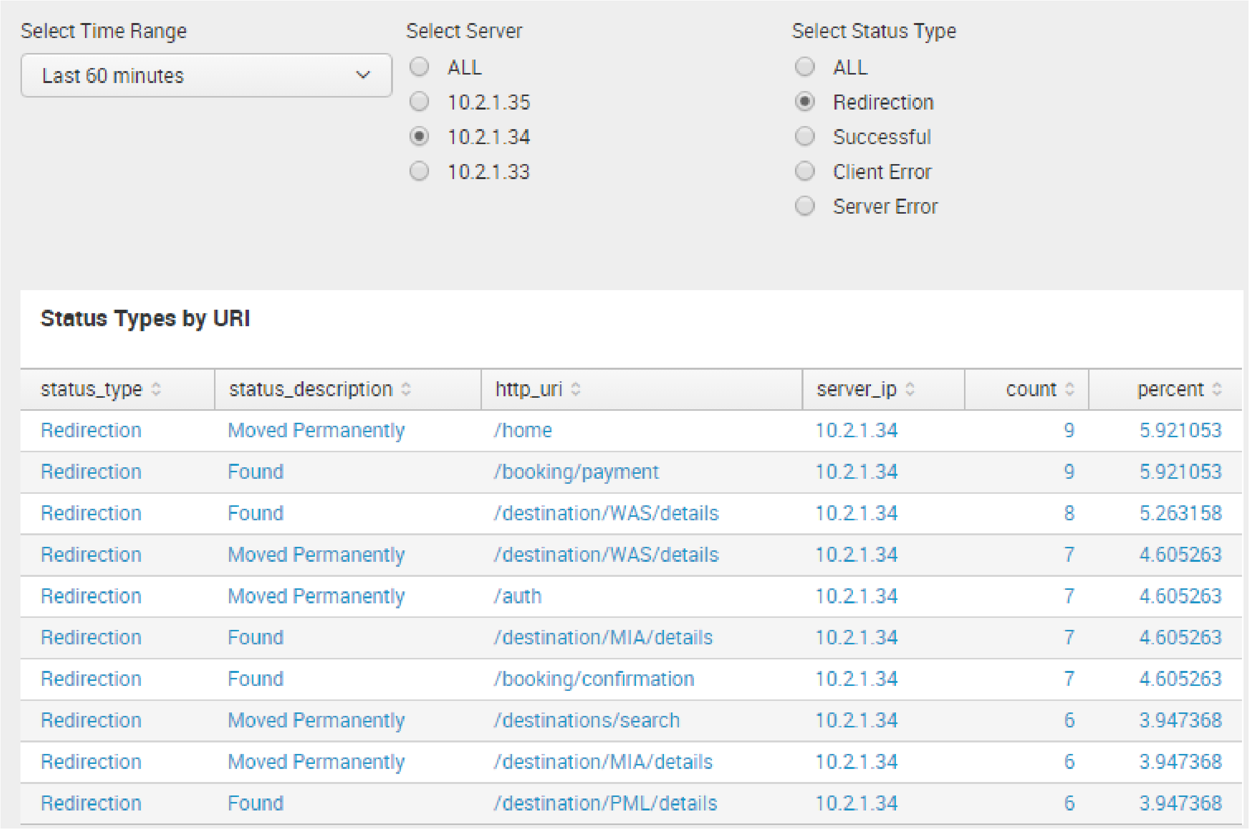
Select Server

- ● ALL
- ○ 10.2.1.35
- ○ 10.2.1.33
- ○ 10.2.1.34



Select Status Type

- ● ALL
- ○ Redirection
- ○ Client Error
- ○ Successful
- ○ Server Error



Select Time Range: Last 60 minutes

Select Server

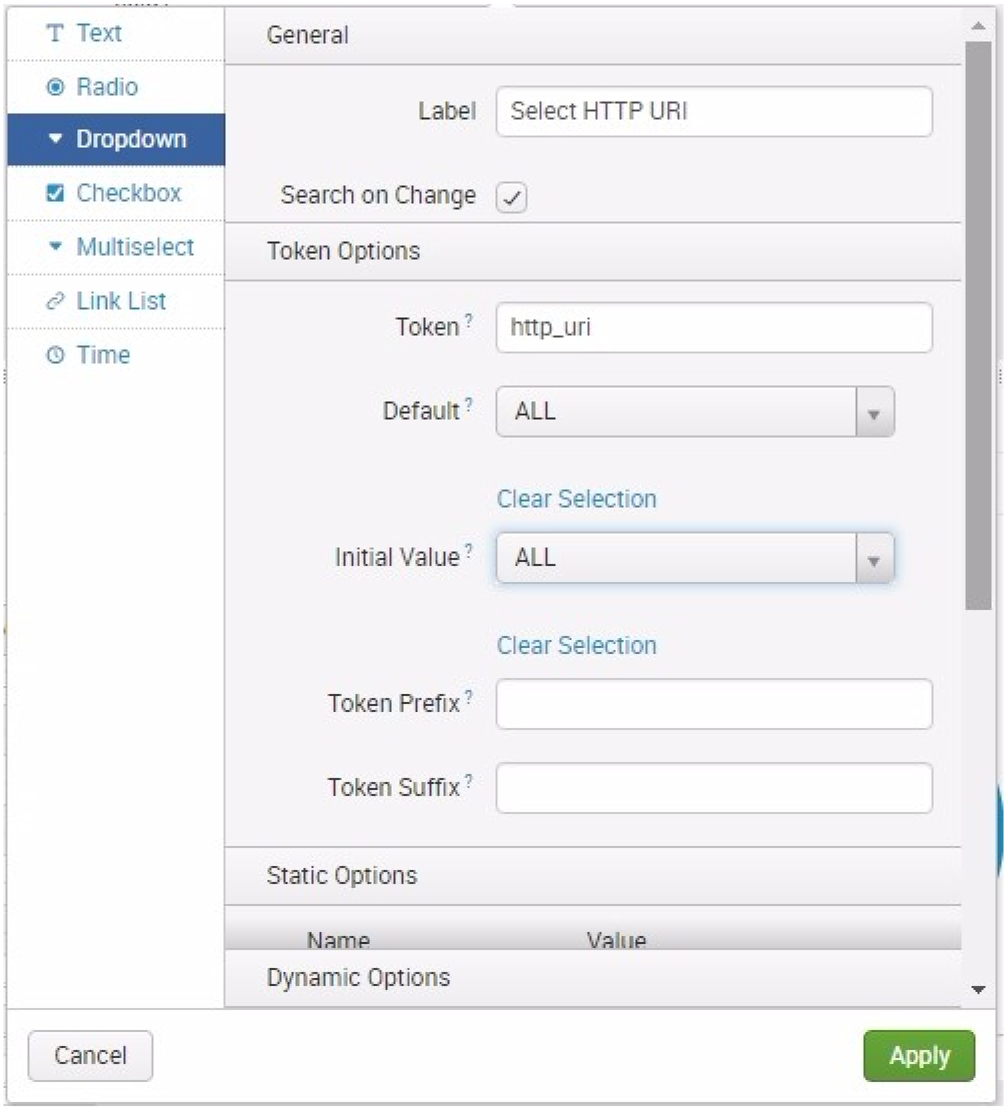
- ○ ALL
- ○ 10.2.1.35
- ● 10.2.1.34
- ○ 10.2.1.33

Select Status Type

- ○ ALL
- ● Redirection
- ○ Successful
- ○ Client Error
- ○ Server Error

Status Types by URI

status_type	status_description	http_uri	server_ip	count	percent
Redirection	Moved Permanently	/home	10.2.1.34	9	5.921053
Redirection	Found	/booking/payment	10.2.1.34	9	5.921053
Redirection	Found	/destination/WAS/details	10.2.1.34	8	5.263158
Redirection	Moved Permanently	/destination/WAS/details	10.2.1.34	7	4.605263
Redirection	Moved Permanently	/auth	10.2.1.34	7	4.605263
Redirection	Found	/destination/MIA/details	10.2.1.34	7	4.605263
Redirection	Found	/booking/confirmation	10.2.1.34	7	4.605263
Redirection	Moved Permanently	/destinations/search	10.2.1.34	6	3.947368
Redirection	Moved Permanently	/destination/MIA/details	10.2.1.34	6	3.947368
Redirection	Found	/destination/PML/details	10.2.1.34	6	3.947368



General

Label: Select HTTP URI

Search on Change ☑

Token Options

Token ?: http_uri

Default ?: ALL

Initial Value ?: ALL

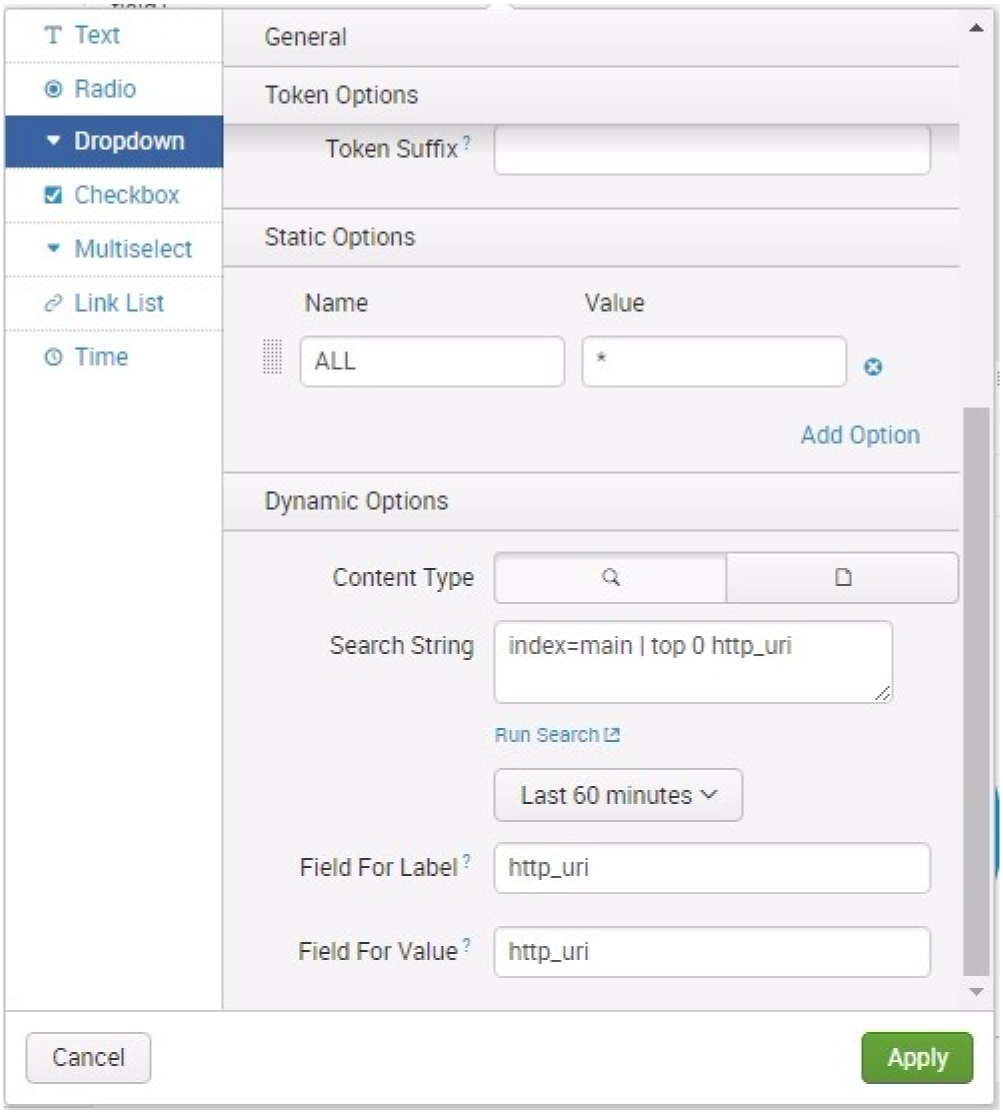
Token Prefix ?:

Token Suffix ?:

Static Options

Name	Value

Dynamic Options



Token Suffix

Name	Value
ALL	*

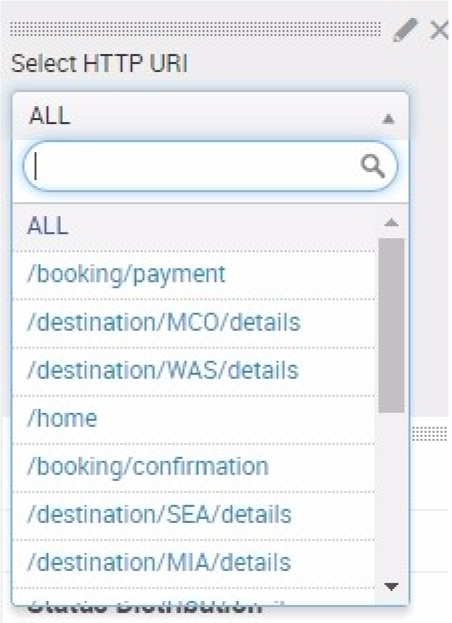
Content Type

Search String: index=main | top 0 http_uri

Last 60 minutes

Field For Label: http_uri

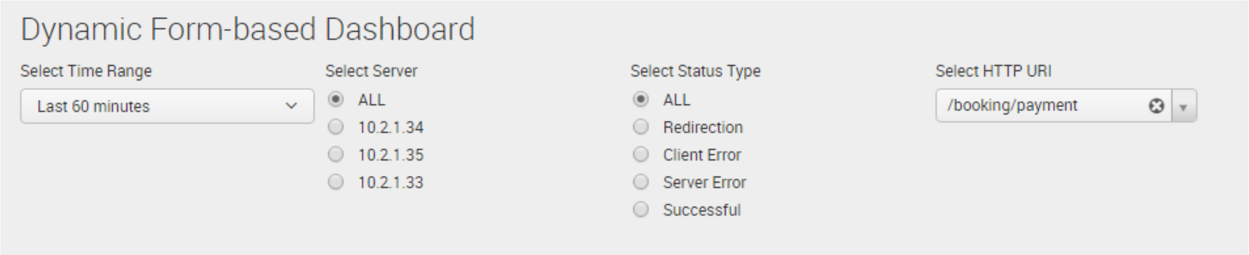
Field For Value: http_uri



Select HTTP URI

ALL

- ALL
- /booking/payment
- /destination/MCO/details
- /destination/WAS/details
- /home
- /booking/confirmation
- /destination/SEA/details
- /destination/MIA/details



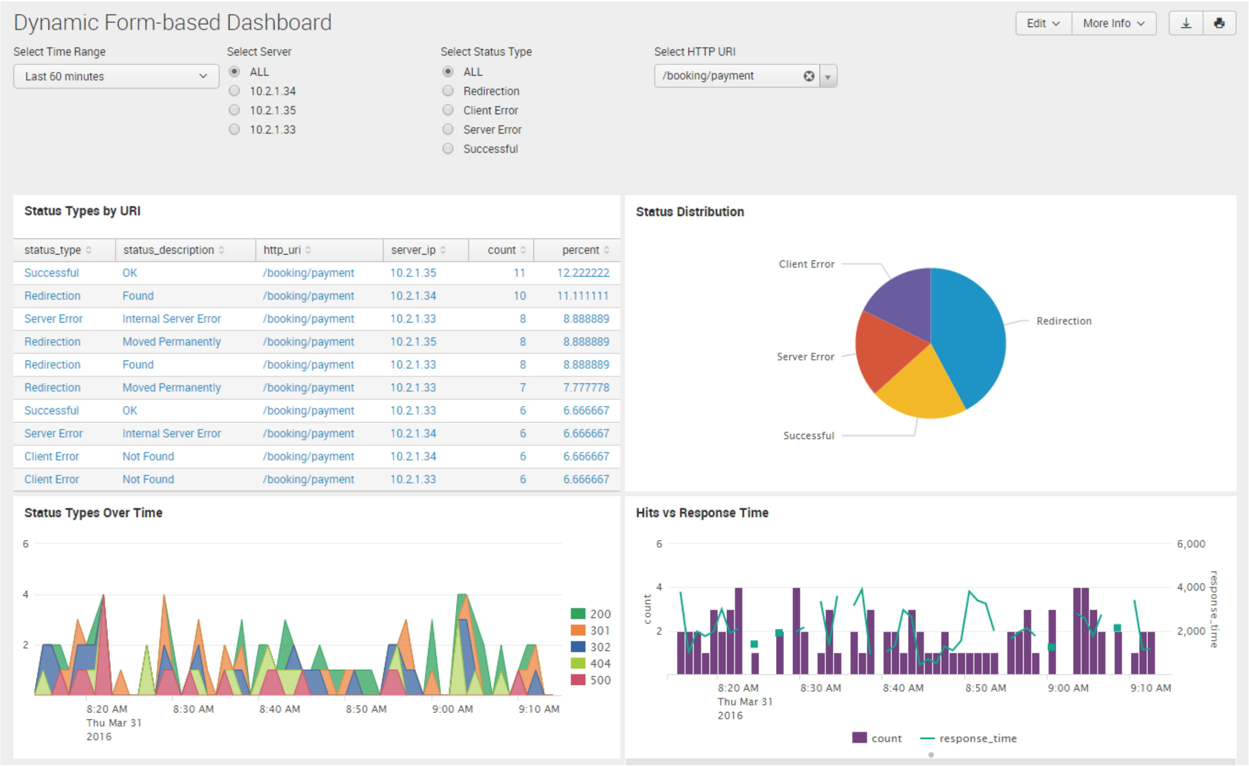
Dynamic Form-based Dashboard

Select Time Range: Last 60 minutes

Select Server: ● ALL ○ 10.2.1.34 ○ 10.2.1.35 ○ 10.2.1.33

Select Status Type: ● ALL ○ Redirection ○ Client Error ○ Server Error ○ Successful

Select HTTP URI: /booking/payment



Dynamic Form-based Dashboard

Select Time Range: Last 60 minutes

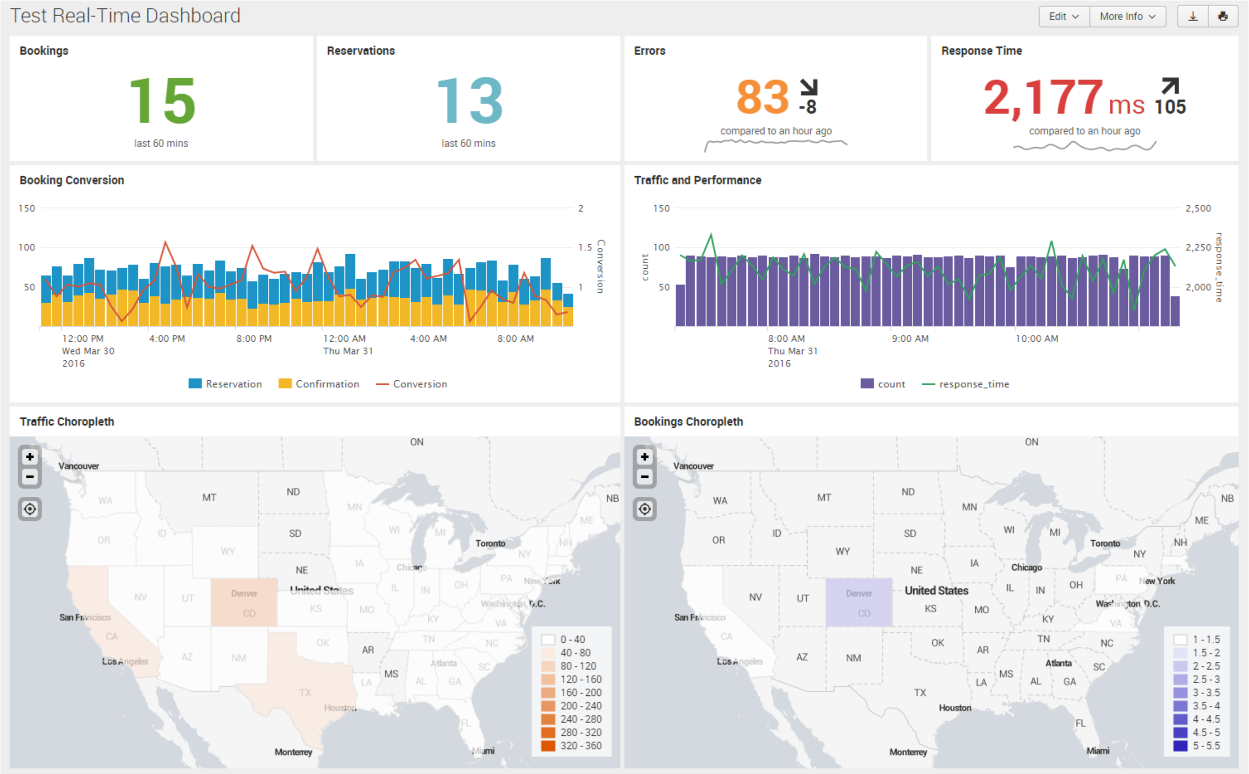
Select Server: ● ALL ○ 10.2.1.34 ○ 10.2.1.35 ○ 10.2.1.33

Select Status Type: ● ALL ○ Redirection ○ Client Error ○ Server Error ○ Successful

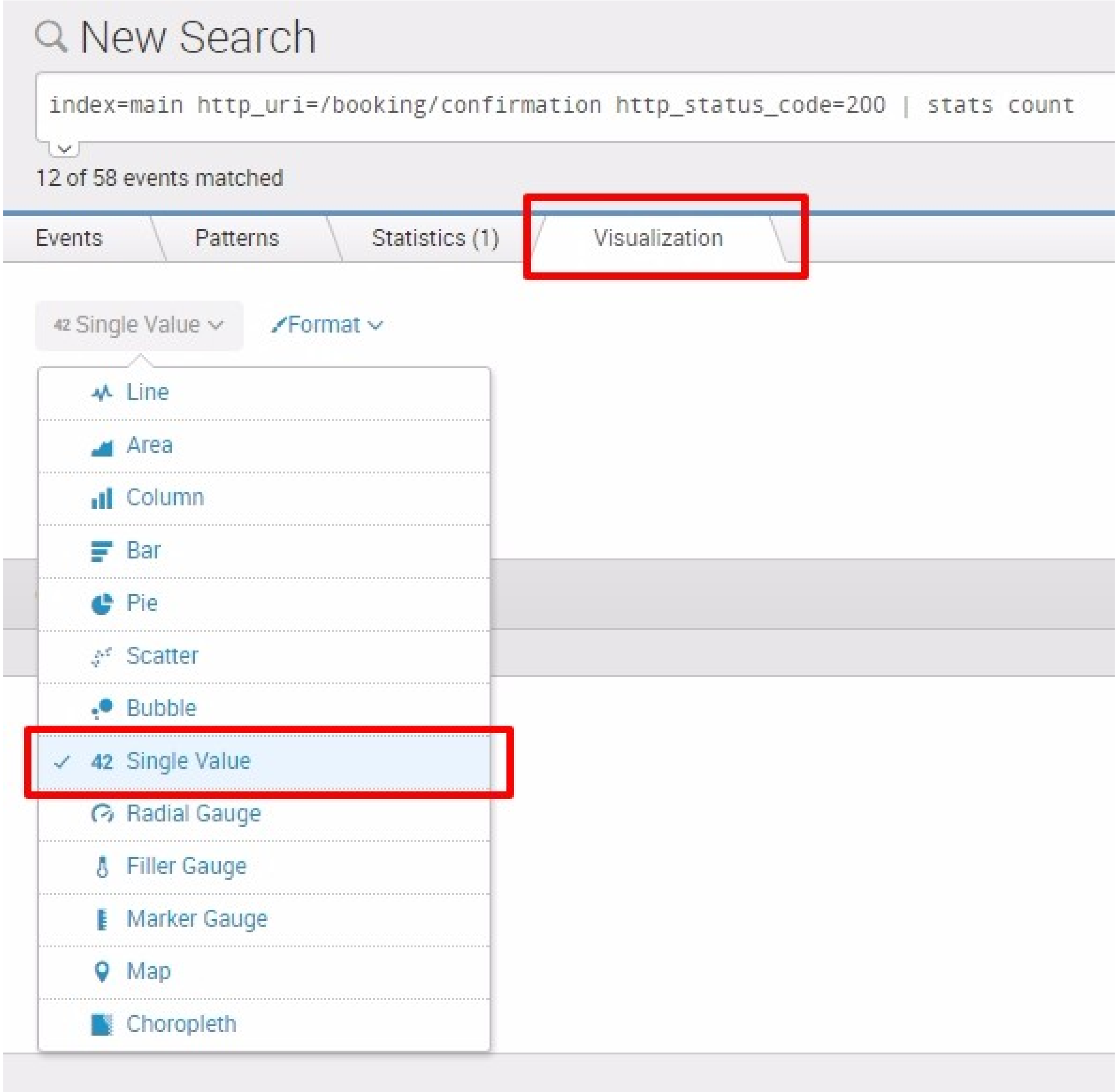
Select HTTP URI: /booking/payment

Status Types by URI

status_type	status_description	http_uri	server_ip	count	percent
Successful	OK	/booking/payment	10.2.1.35	11	12.222222
Redirection	Found	/booking/payment	10.2.1.34	10	11.111111
Server Error	Internal Server Error	/booking/payment	10.2.1.33	8	8.888889
Redirection	Moved Permanently	/booking/payment	10.2.1.35	8	8.888889
Redirection	Found	/booking/payment	10.2.1.33	8	8.888889
Redirection	Moved Permanently	/booking/payment	10.2.1.33	7	7.777778
Successful	OK	/booking/payment	10.2.1.33	6	6.666667
Server Error	Internal Server Error	/booking/payment	10.2.1.34	6	6.666667
Client Error	Not Found	/booking/payment	10.2.1.34	6	6.666667
Client Error	Not Found	/booking/payment	10.2.1.33	6	6.666667



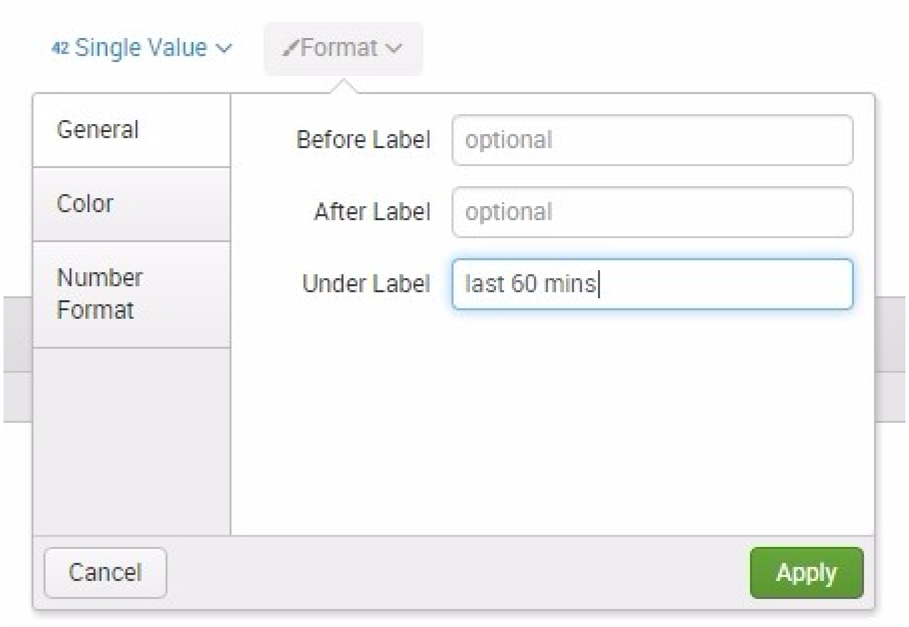
Test Real-Time Dashboard
Edit
More Info
Bookings
15
last 60 mins
Reservations
13
last 60 mins
Errors
83 ↘ -8
compared to an hour ago
Response Time
2,177 ms ↗ 105
compared to an hour ago
Booking Conversion
150
100
50
2
1.5
1
Conversion
12:00 PM
Wed Mar 30
2016
4:00 PM
8:00 PM
12:00 AM
Thu Mar 31
4:00 AM
8:00 AM
Reservation
Confirmation
Conversion
Traffic and Performance
150
100
50
count
2,500
2,250
2,000
response_time
8:00 AM
Thu Mar 31
2016
9:00 AM
10:00 AM
count
response_time
Traffic Choropleth
0 - 40
40 - 80
80 - 120
120 - 160
160 - 200
200 - 240
240 - 280
280 - 320
320 - 360
Bookings Choropleth
1 - 1.5
1.5 - 2
2 - 2.5
2.5 - 3
3 - 3.5
3.5 - 4
4 - 4.5
4.5 - 5
5 - 5.5
Vancouver
ON
WA
MT
ND
MN
NB
OR
ID
SD
WI
MI
ME
WY
Toronto
NY
NH
NE
IA
Chicago
PA
New York
NV
UT
Denver
CO
United States
IL
IN
OH
KS
MO
Washington D.C.
San Francisco
KY
VA
CA
OK
TN
NC
AZ
NM
AR
Los Angeles
MS
Atlanta
SC
AL
GA
LA
TX
Houston
FL
Monterrey
Miami



New Search

```
index=main http_uri=/booking/confirmation http_status_code=200 | stats count
```

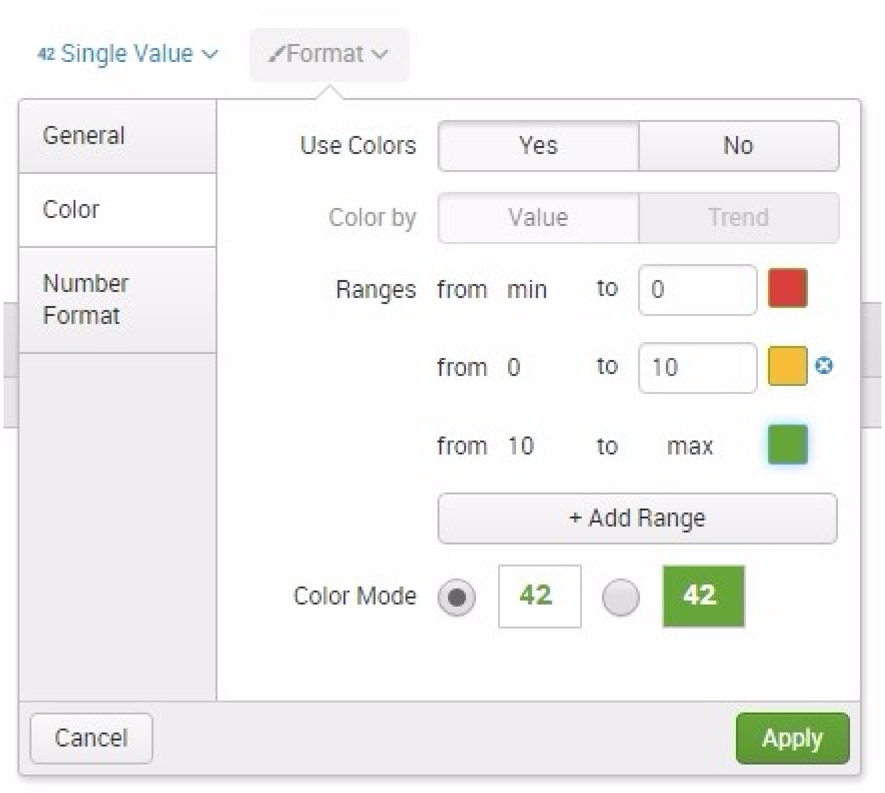
12 of 58 events matched



Before Label optional

After Label optional

Under Label last 60 mins



Use Colors [✓ Yes] No

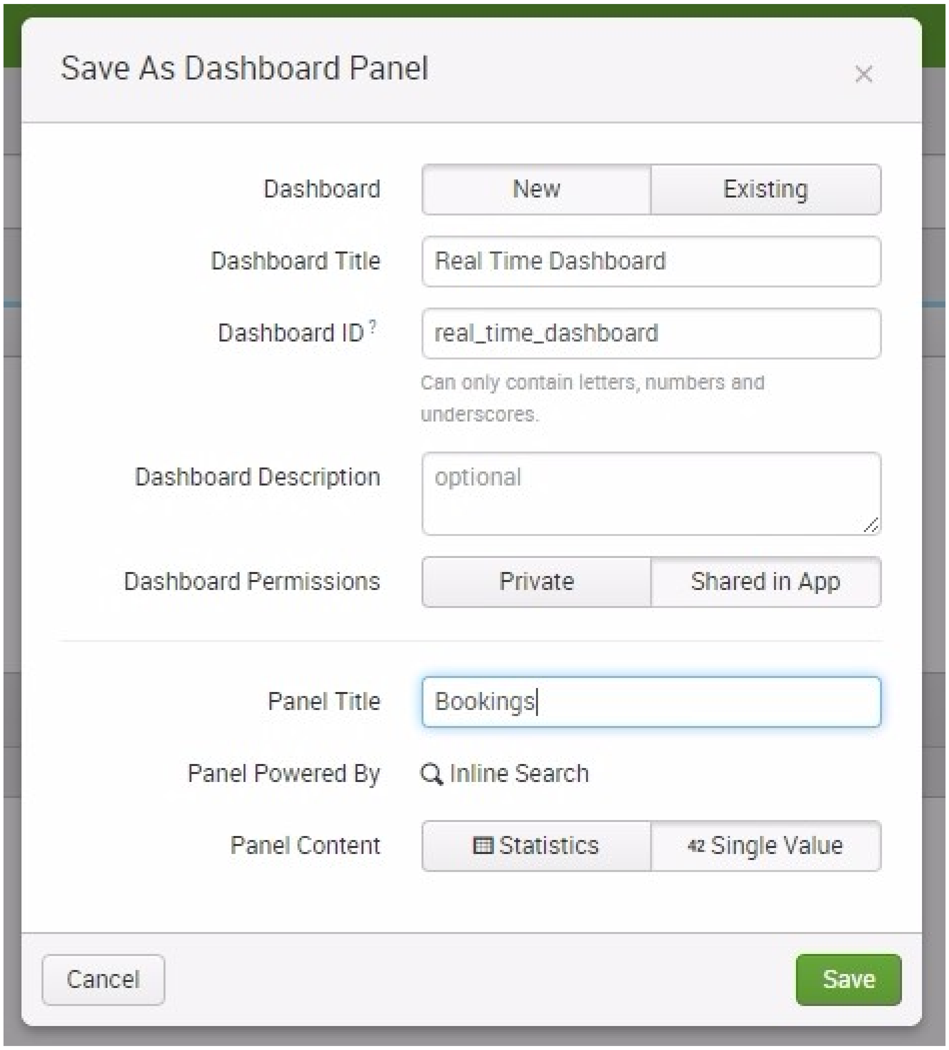
Color by [✓ Value] Trend

Ranges from min to 0 🟥

from 0 to 10 🟨

from 10 to max 🟩

Color Mode ● 42 ○ 42



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Real Time Dashboard

Dashboard ID ?: real_time_dashboard

Can only contain letters, numbers and underscores.

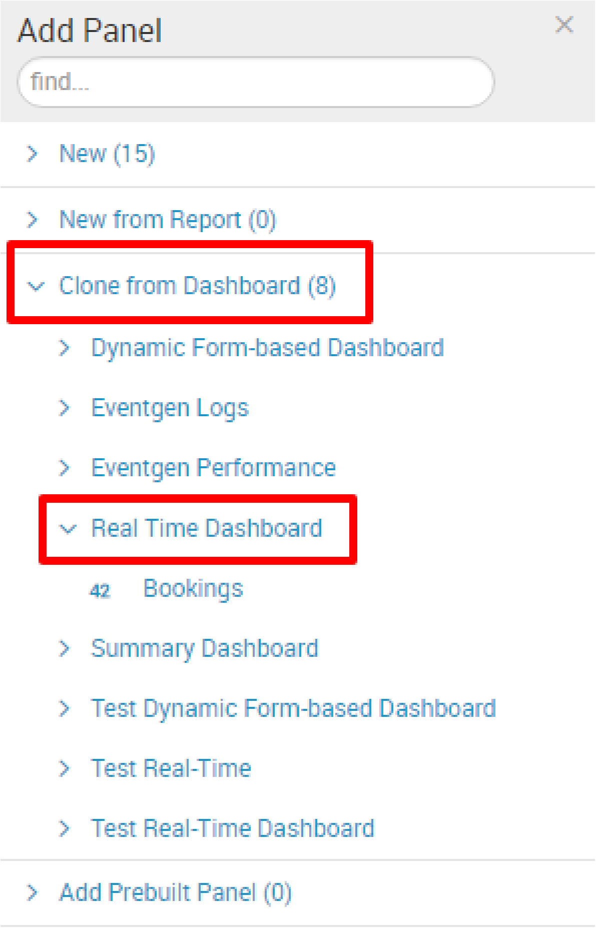
Dashboard Description: optional

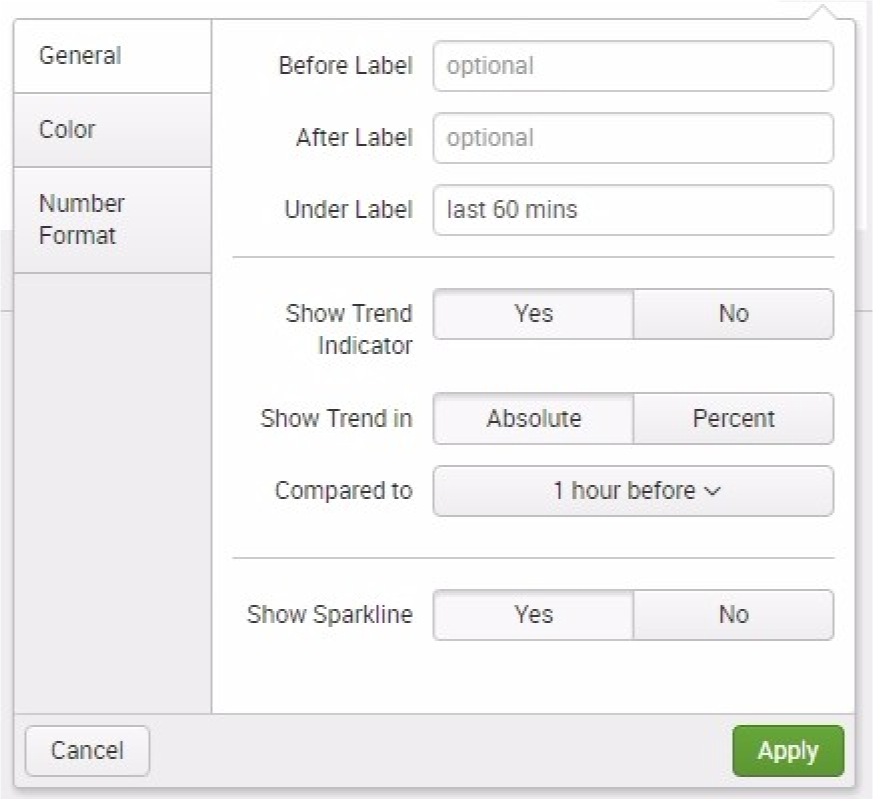
Dashboard Permissions: Private | Shared in App

Panel Title: Bookings

Panel Powered By: Inline Search

Panel Content: Statistics | 42 Single Value


Add Panel
find...
New (15)
New from Report (0)
Clone from Dashboard (8)
Dynamic Form-based Dashboard
Eventgen Logs
Eventgen Performance
Real Time Dashboard
42
Bookings
Summary Dashboard
Test Dynamic Form-based Dashboard
Test Real-Time
Test Real-Time Dashboard
Add Prebuilt Panel (0)



Before Label: optional

After Label: optional

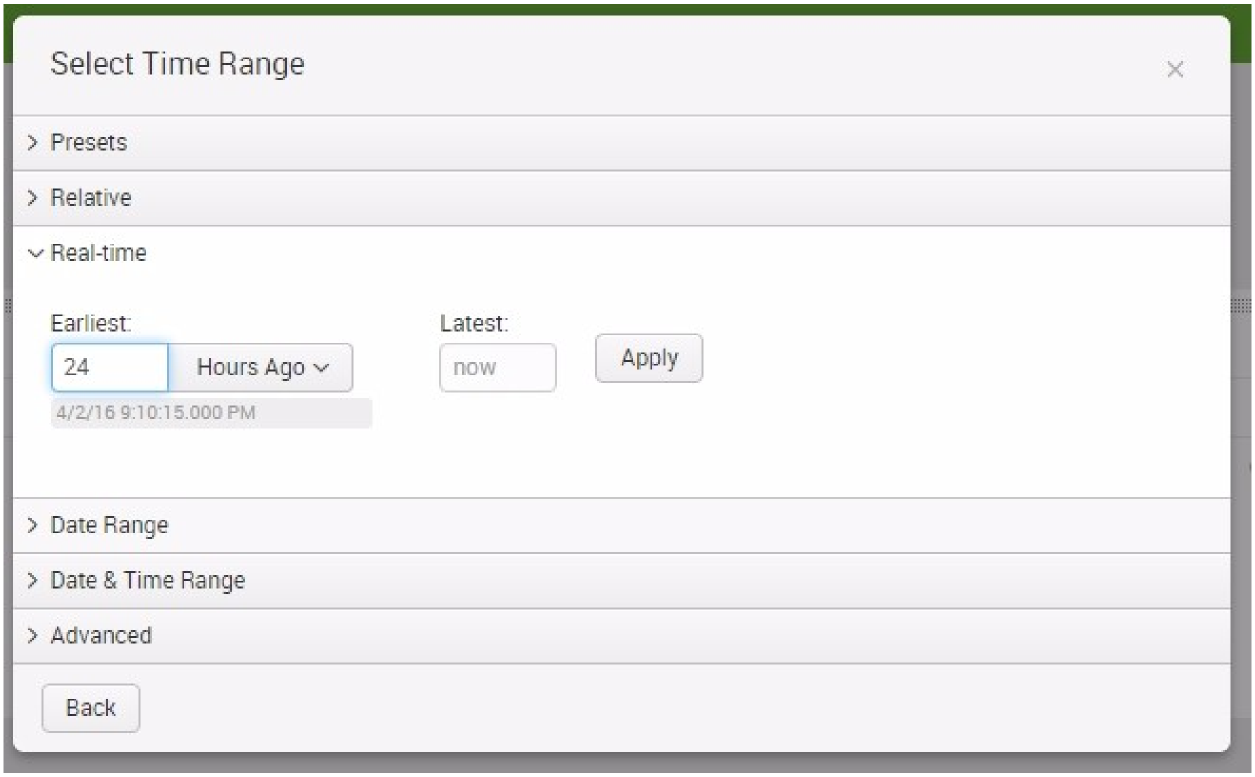
Under Label: last 60 mins

Show Trend Indicator: Yes | No

Show Trend in: Absolute | Percent

Compared to: 1 hour before

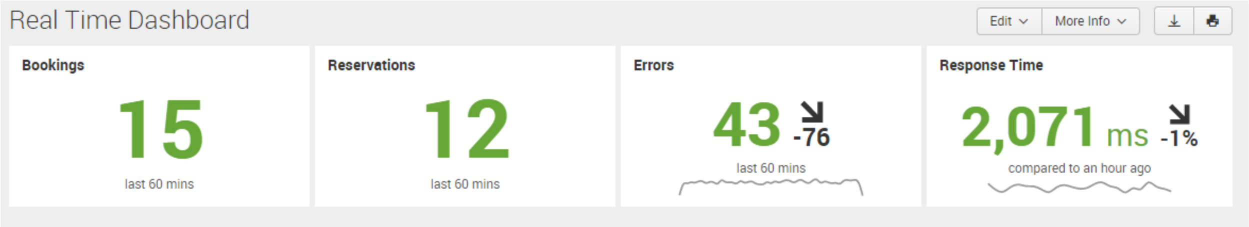
Show Sparkline: Yes | No

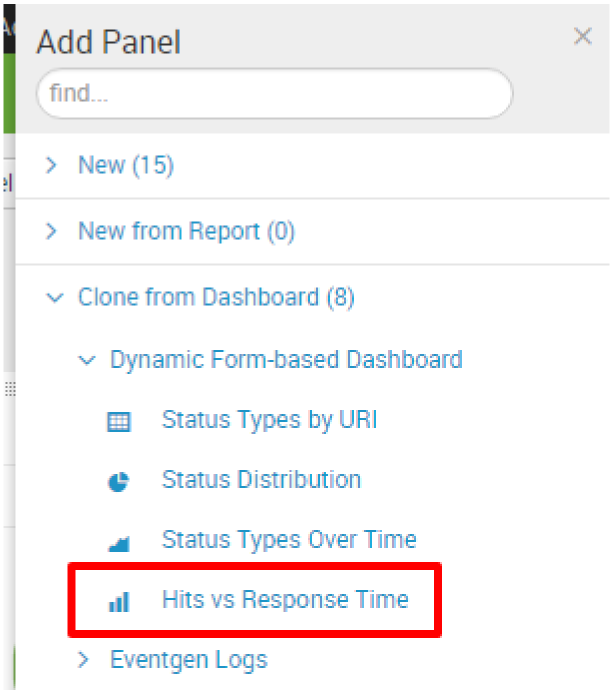


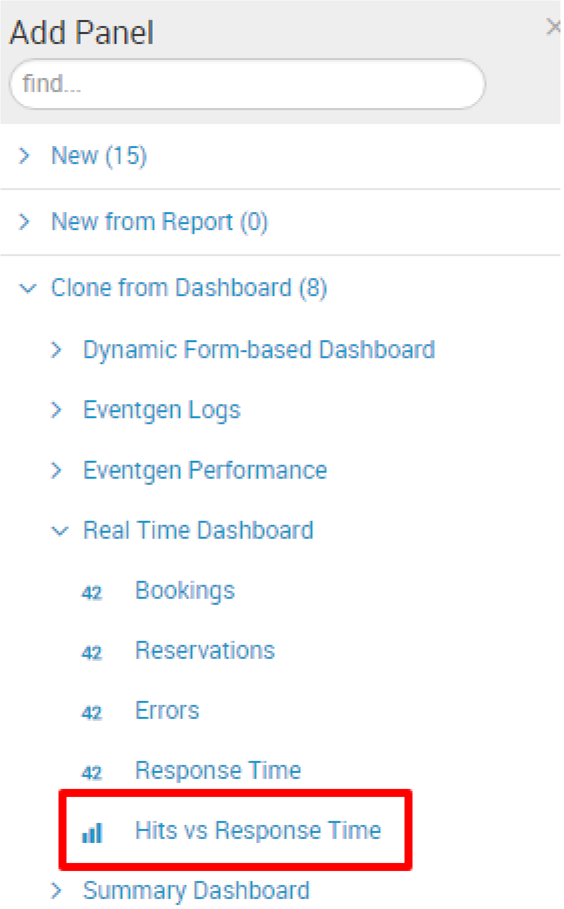
Earliest: 24 Hours Ago

4/2/16 9:10:15.000 PM

Latest: now


Real Time Dashboard
Edit
More Info
Bookings
15
last 60 mins
Reservations
12
last 60 mins
Errors
43
-76
last 60 mins
Response Time
2,071 ms
-1%
compared to an hour ago

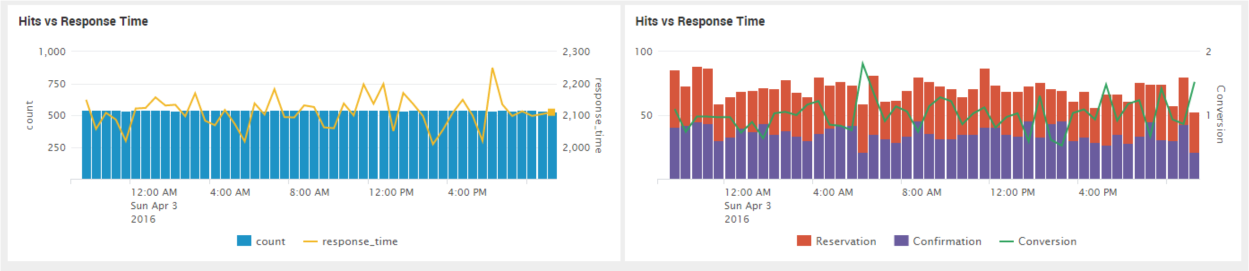

Add Panel
find...
New (15)
New from Report (0)
Clone from Dashboard (8)
Dynamic Form-based Dashboard
Status Types by URI
Status Distribution
Status Types Over Time
Hits vs Response Time
Eventgen Logs

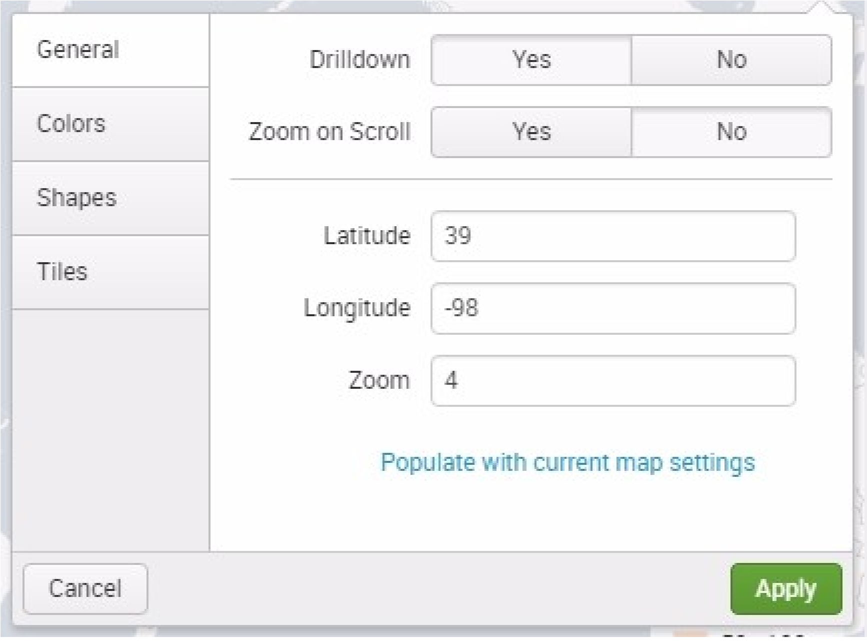


Add Panel ×

find...

- › New (15)
- › New from Report (0)
- ⌄ Clone from Dashboard (8)
  - › Dynamic Form-based Dashboard
  - › Eventgen Logs
  - › Eventgen Performance
  - ⌄ Real Time Dashboard
    - 42 Bookings
    - 42 Reservations
    - 42 Errors
    - 42 Response Time
    - 📊 Hits vs Response Time
  - › Summary Dashboard





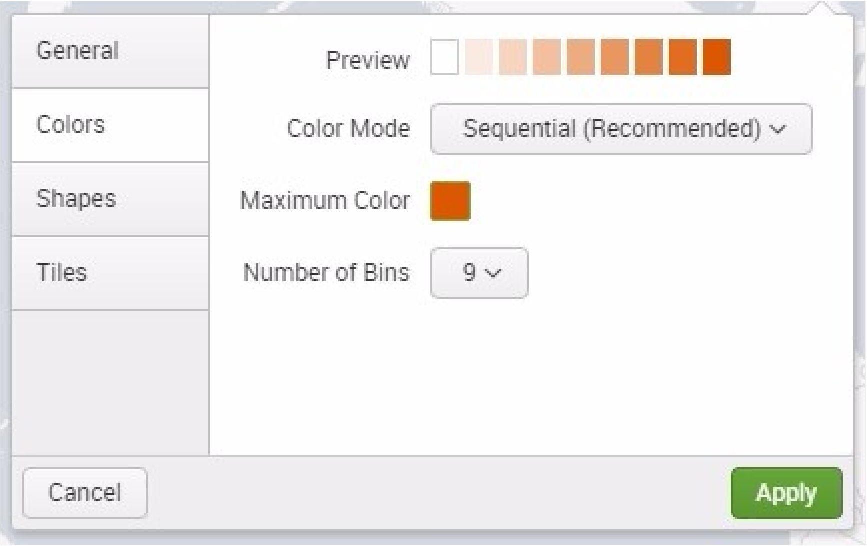
Drilldown Yes No

Zoom on Scroll Yes No

Latitude 39

Longitude -98

Zoom 4

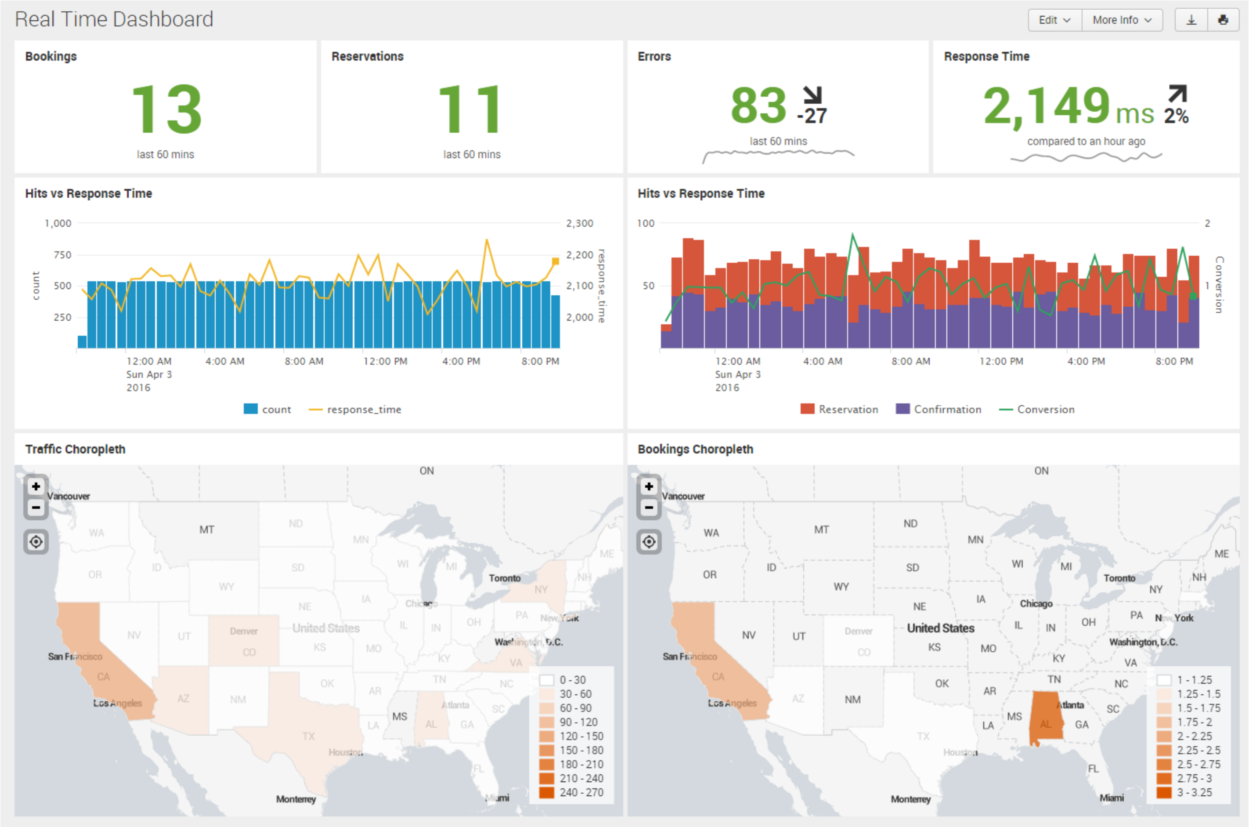


Preview □ 🟧 🟧 🟧 🟧 🟧 🟧 🟧 🟧

Color Mode Sequential (Recommended)

Maximum Color 🟧

Number of Bins 9



Real Time Dashboard

Bookings
13
last 60 mins

Reservations
11
last 60 mins

Errors
83 -27
last 60 mins

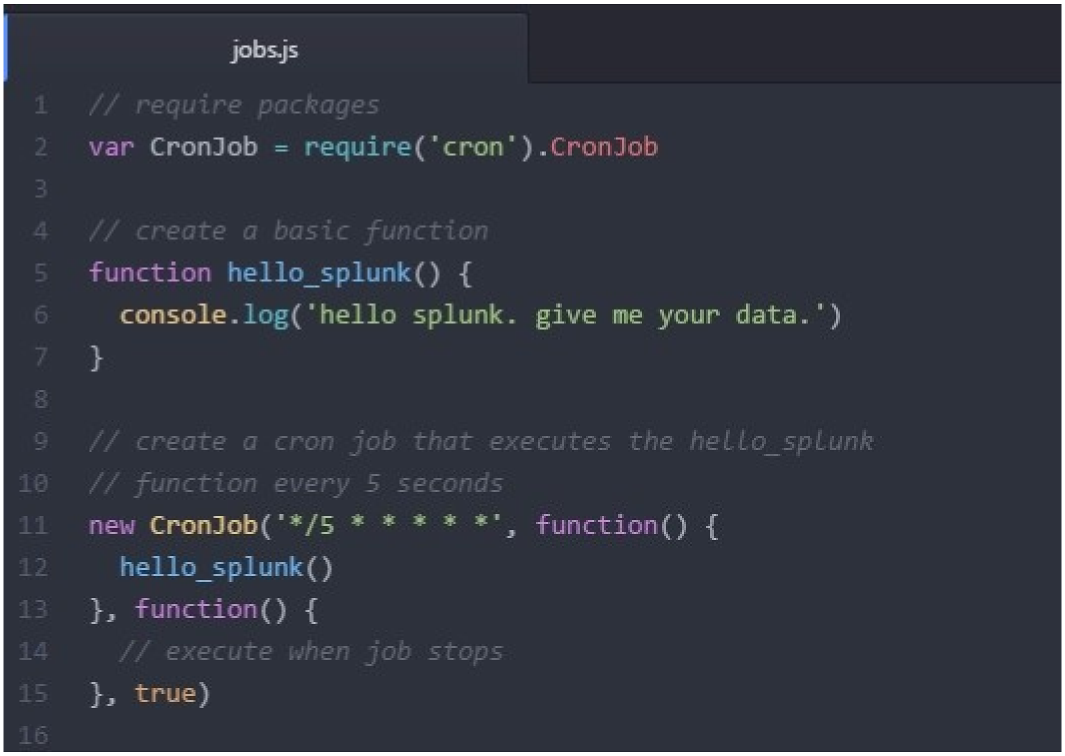
Response Time
2,149 ms 2%
compared to an hour ago

Hits vs Response Time

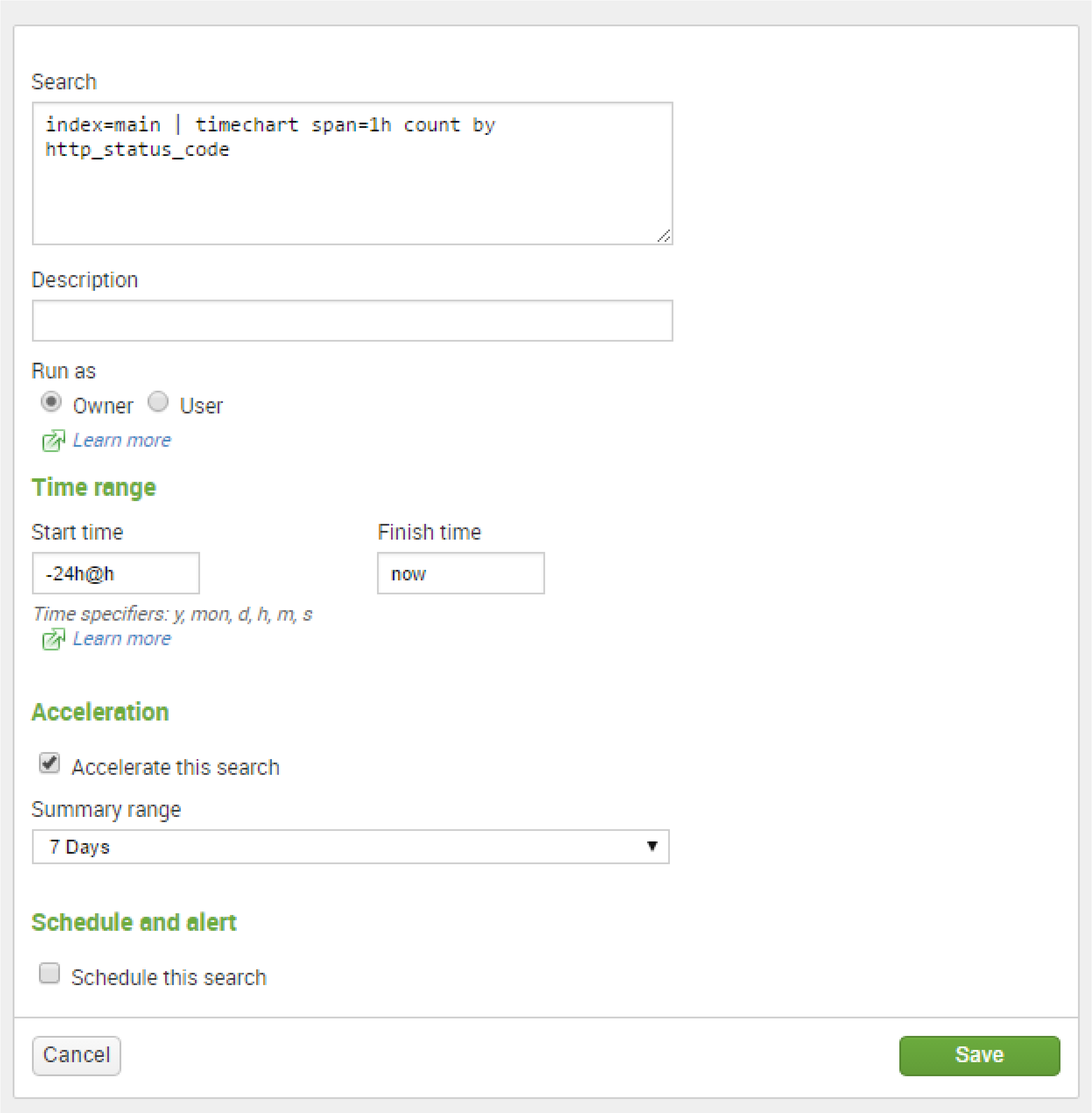
Hits vs Response Time

Traffic Choropleth

Bookings Choropleth



```
// require packages
var CronJob = require('cron').CronJob

// create a basic function
function hello_splunk() {
  console.log('hello splunk. give me your data.')
}

// create a cron job that executes the hello_splunk
// function every 5 seconds
new CronJob('*/5 * * * * *', function() {
  hello_splunk()
}, function() {
  // execute when job stops
}, true)

```



Search

```
index=main | timechart span=1h count by
http_status_code
```

Description

Run as

● Owner ○ User

Learn more

Time range

Start time: -24h@h

Finish time: now

Time specifiers: y, mon, d, h, m, s

Learn more

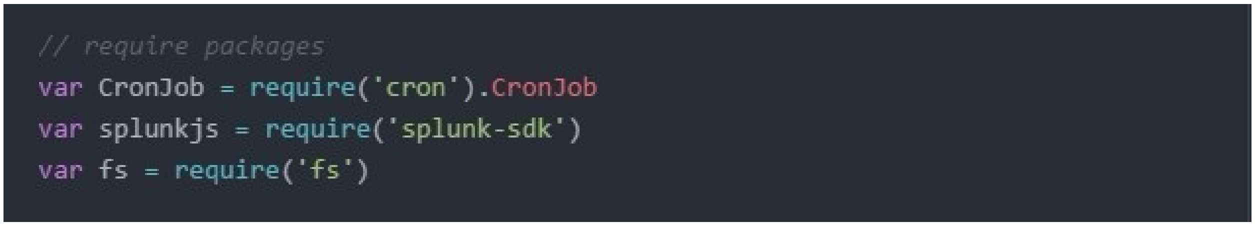
Acceleration

☑ Accelerate this search

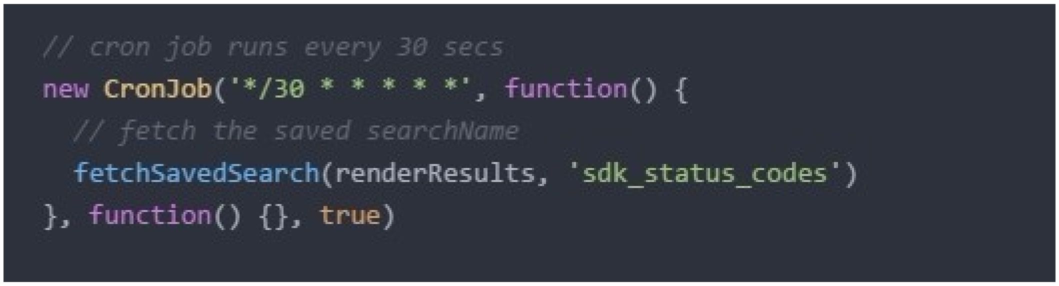
Summary range: 7 Days

Schedule and alert

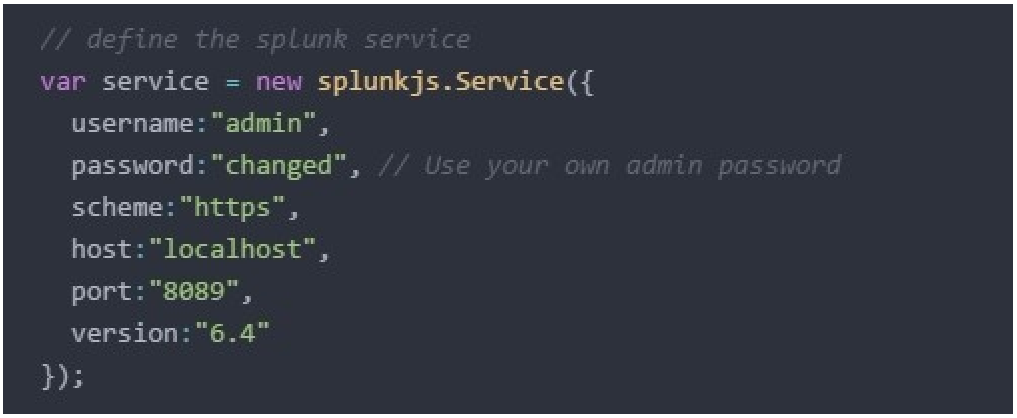
□ Schedule this search



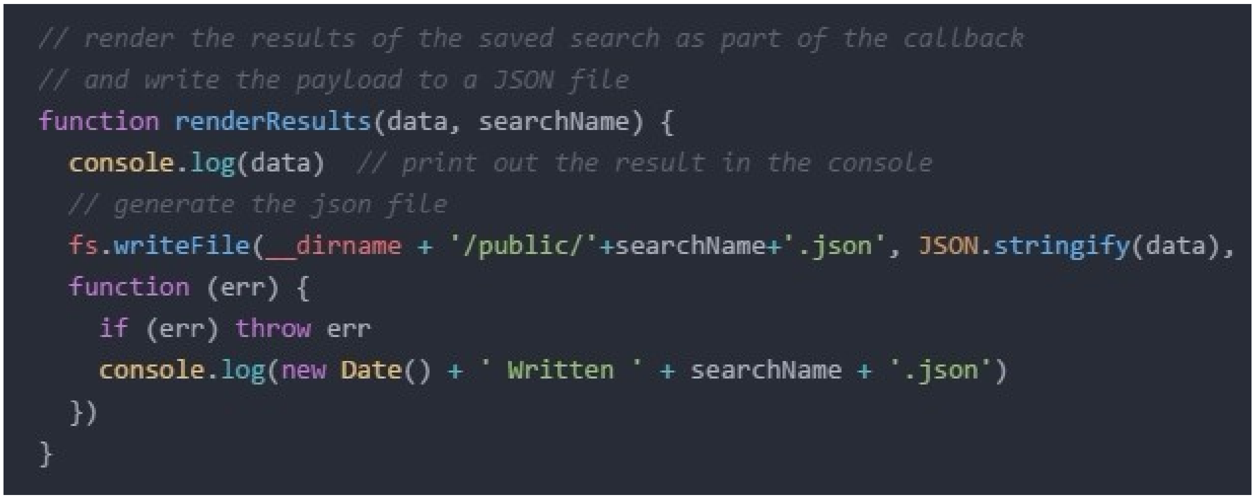
```
// require packages
var CronJob = require('cron').CronJob
var splunkjs = require('splunk-sdk')
var fs = require('fs')
```



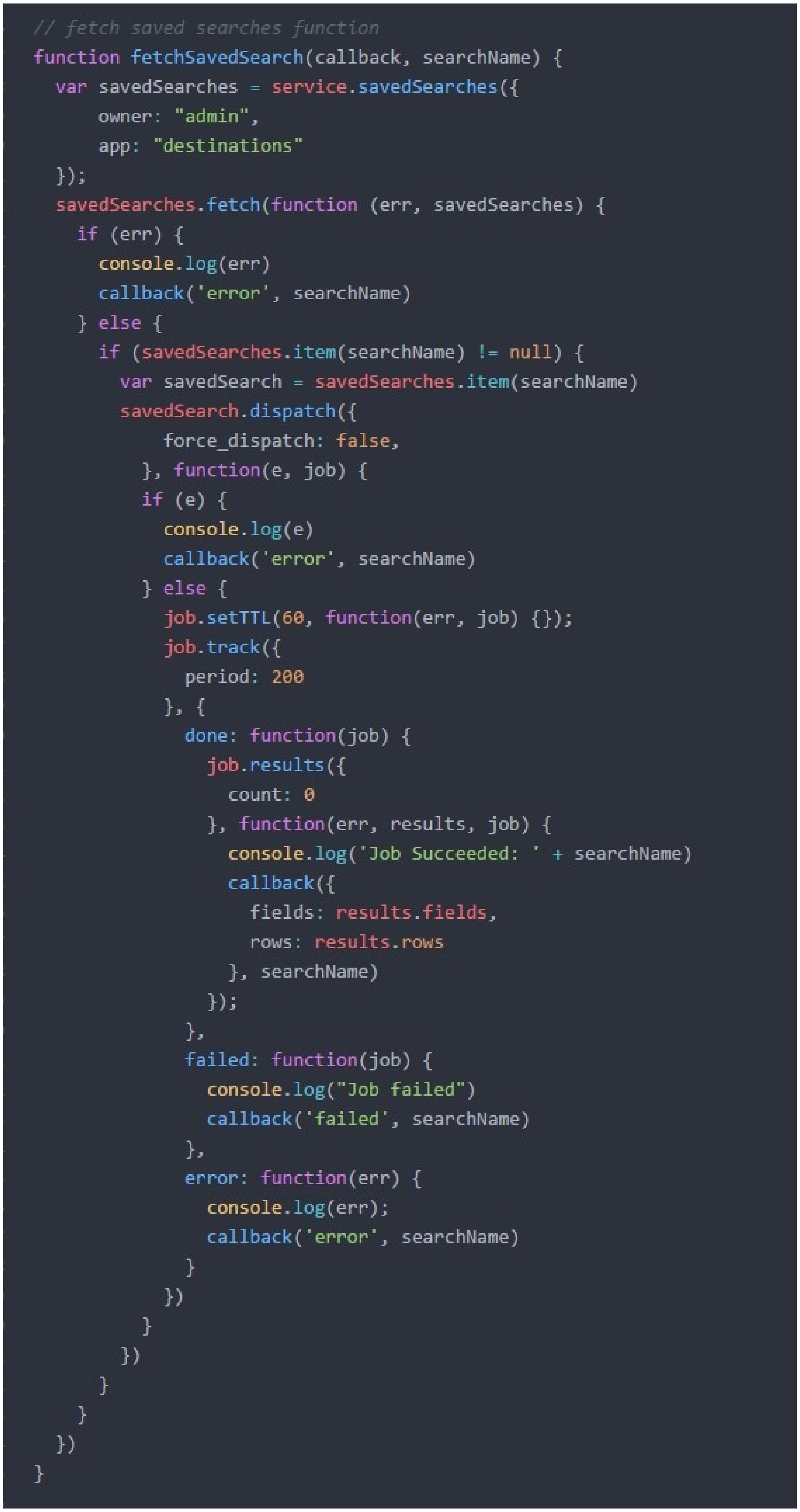
```
// cron job runs every 30 secs
new CronJob('*/30 * * * * *', function() {
  // fetch the saved searchName
  fetchSavedSearch(renderResults, 'sdk_status_codes')
}, function() {}, true)
```



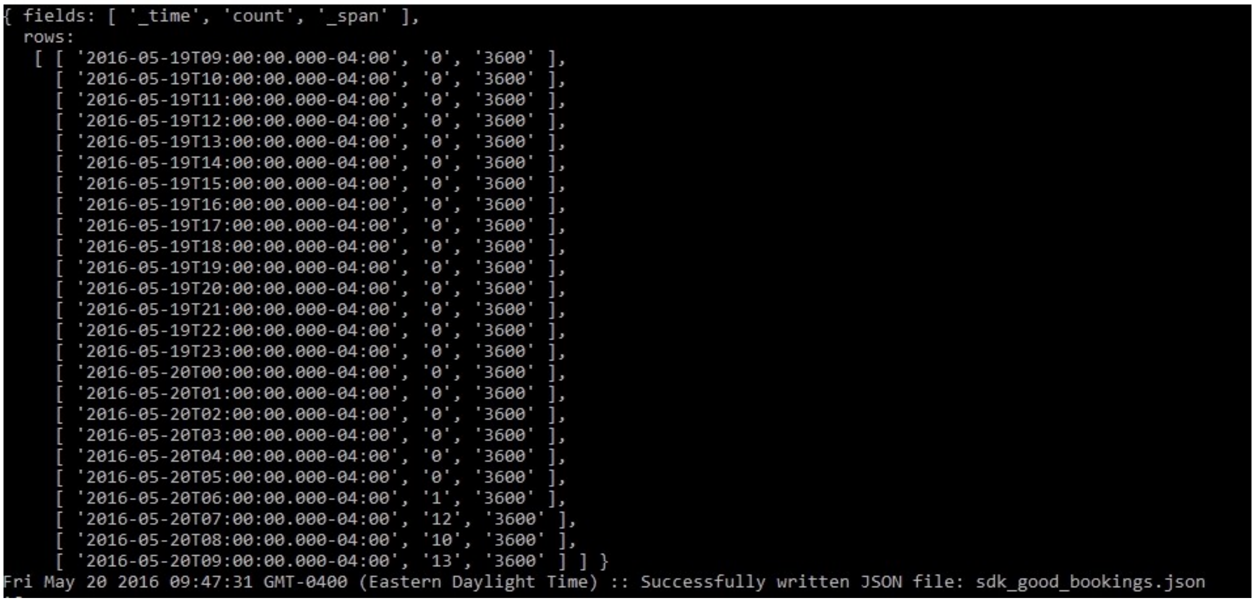
```
// define the splunk service
var service = new splunkjs.Service({
  username:"admin",
  password:"changed", // Use your own admin password
  scheme:"https",
  host:"localhost",
  port:"8089",
  version:"6.4"
});
```



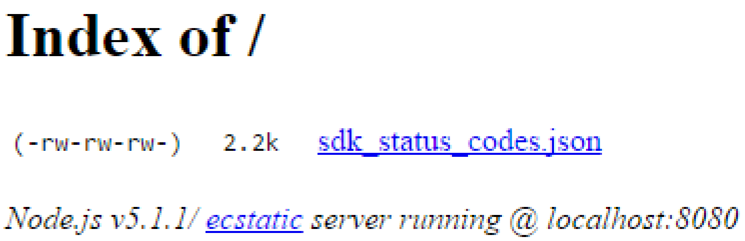
```
// render the results of the saved search as part of the callback
// and write the payload to a JSON file
function renderResults(data, searchName) {
  console.log(data)  // print out the result in the console
  // generate the json file
  fs.writeFile(__dirname + '/public/'+searchName+'.json', JSON.stringify(data),
  function (err) {
    if (err) throw err
    console.log(new Date() + ' Written ' + searchName + '.json')
  })
}
```



```
// fetch saved searches function
function fetchSavedSearch(callback, searchName) {
  var savedSearches = service.savedSearches({
      owner: "admin",
      app: "destinations"
  });
  savedSearches.fetch(function (err, savedSearches) {
    if (err) {
      console.log(err)
      callback('error', searchName)
    } else {
      if (savedSearches.item(searchName) != null) {
        var savedSearch = savedSearches.item(searchName)
        savedSearch.dispatch({
            force_dispatch: false,
          }, function(e, job) {
          if (e) {
            console.log(e)
            callback('error', searchName)
          } else {
            job.setTTL(60, function(err, job) {});
            job.track({
              period: 200
            }, {
              done: function(job) {
                job.results({
                  count: 0
                }, function(err, results, job) {
                  console.log('Job Succeeded: ' + searchName)
                  callback({
                    fields: results.fields,
                    rows: results.rows
                  }, searchName)
                });
              },
              failed: function(job) {
                console.log("Job failed")
                callback('failed', searchName)
              },
              error: function(err) {
                console.log(err);
                callback('error', searchName)
              }
            })
          }
        })
      }
    }
  })
}
```



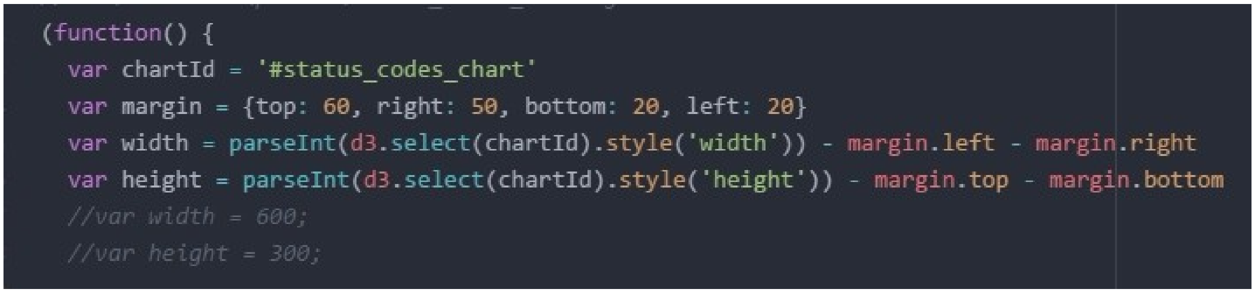
```
{ fields: [ '_time', 'count', '_span' ],
  rows:
   [ [ '2016-05-19T09:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T10:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T11:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T12:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T13:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T14:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T15:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T16:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T17:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T18:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T19:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T20:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T21:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T22:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-19T23:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T00:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T01:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T02:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T03:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T04:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T05:00:00.000-04:00', '0', '3600' ],
     [ '2016-05-20T06:00:00.000-04:00', '1', '3600' ],
     [ '2016-05-20T07:00:00.000-04:00', '12', '3600' ],
     [ '2016-05-20T08:00:00.000-04:00', '10', '3600' ],
     [ '2016-05-20T09:00:00.000-04:00', '13', '3600' ] ] }
Fri May 20 2016 09:47:31 GMT-0400 (Eastern Daylight Time) :: Successfully written JSON file: sdk_good_bookings.json
```



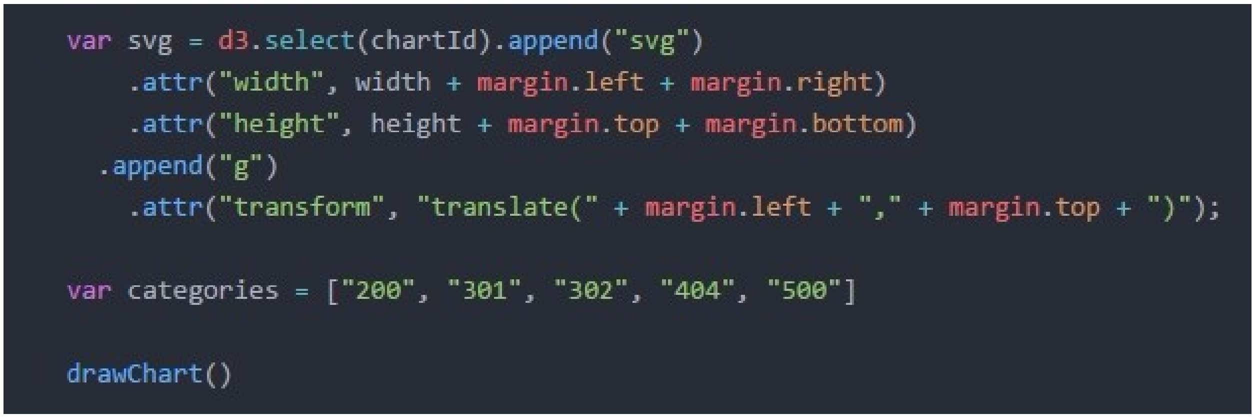
Index of /

(-rw-rw-rw-)   2.2k   sdk_status_codes.json

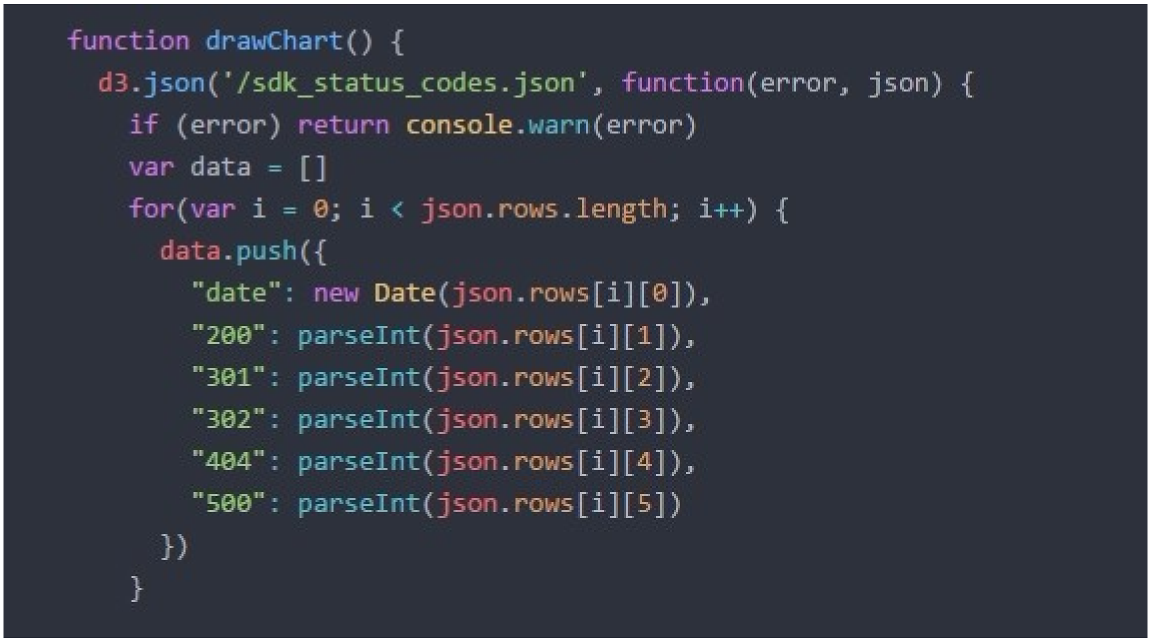
Node.js v5.1.1/ ecstatic server running @ localhost:8080



```
(function() {
  var chartId = '#status_codes_chart'
  var margin = {top: 60, right: 50, bottom: 20, left: 20}
  var width = parseInt(d3.select(chartId).style('width')) - margin.left - margin.right
  var height = parseInt(d3.select(chartId).style('height')) - margin.top - margin.bottom
  //var width = 600;
  //var height = 300;
```

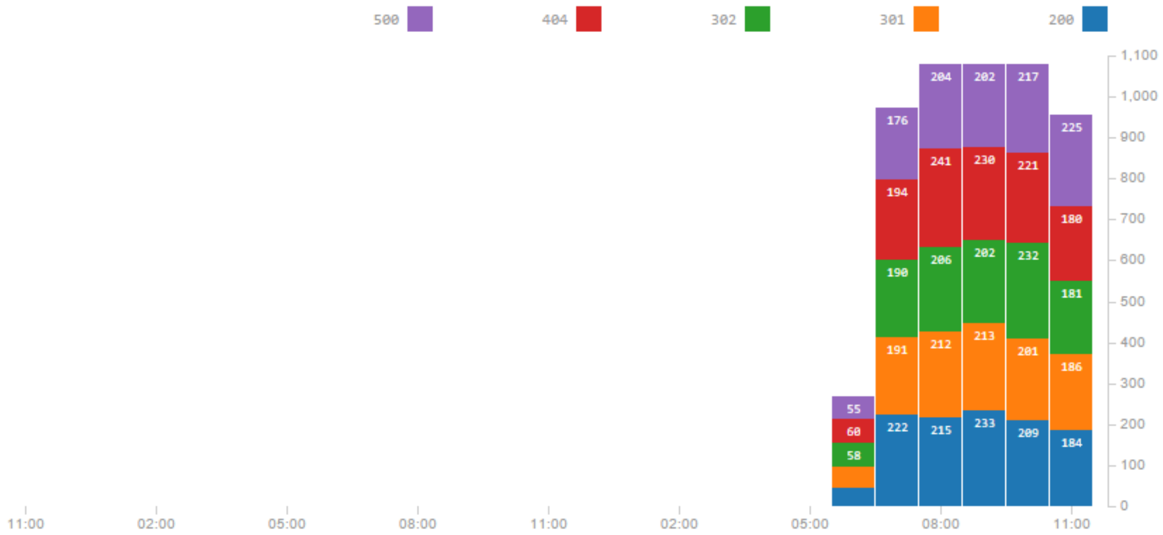


```
var svg = d3.select(chartId).append("svg")
    .attr("width", width + margin.left + margin.right)
    .attr("height", height + margin.top + margin.bottom)
  .append("g")
    .attr("transform", "translate(" + margin.left + "," + margin.top + ")");

var categories = ["200", "301", "302", "404", "500"]

drawChart()
```

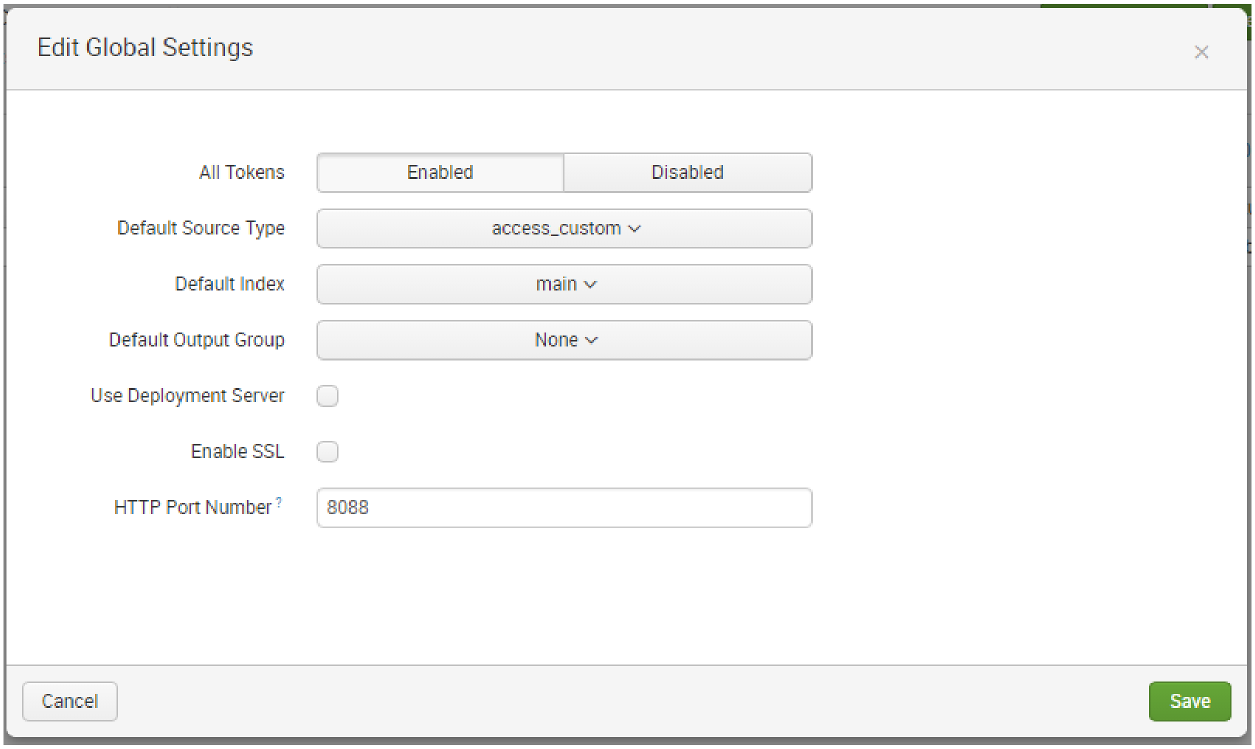


```
function drawChart() {
  d3.json('/sdk_status_codes.json', function(error, json) {
    if (error) return console.warn(error)
    var data = []
    for(var i = 0; i < json.rows.length; i++) {
      data.push({
        "date": new Date(json.rows[i][0]),
        "200": parseInt(json.rows[i][1]),
        "301": parseInt(json.rows[i][2]),
        "302": parseInt(json.rows[i][3]),
        "404": parseInt(json.rows[i][4]),
        "500": parseInt(json.rows[i][5])
      })
    }
```

Real Time Dashboard



Chapter 8: HTTP Event Collector



Edit Global Settings

All Tokens: Enabled | Disabled

Default Source Type: access_custom

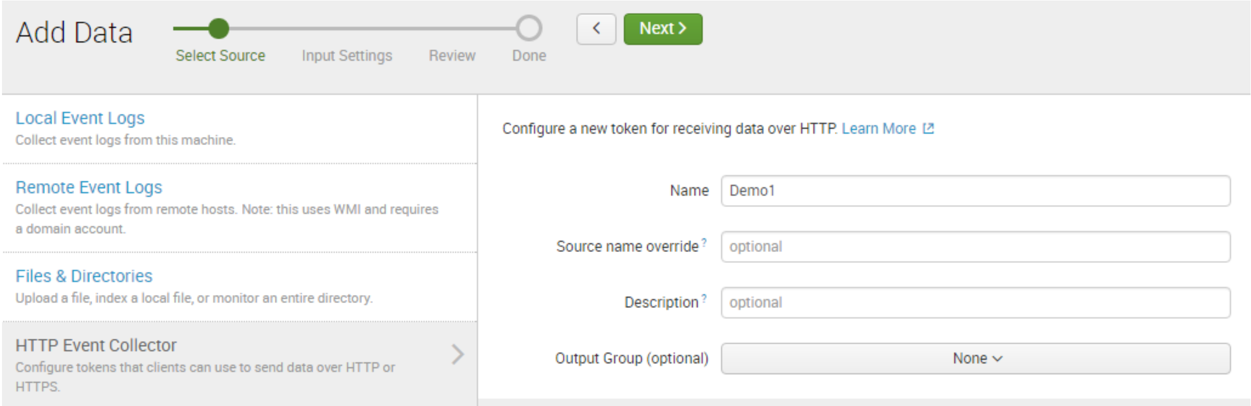
Default Index: main

Default Output Group: None

Use Deployment Server ☐

Enable SSL ☐

HTTP Port Number ?: 8088



Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

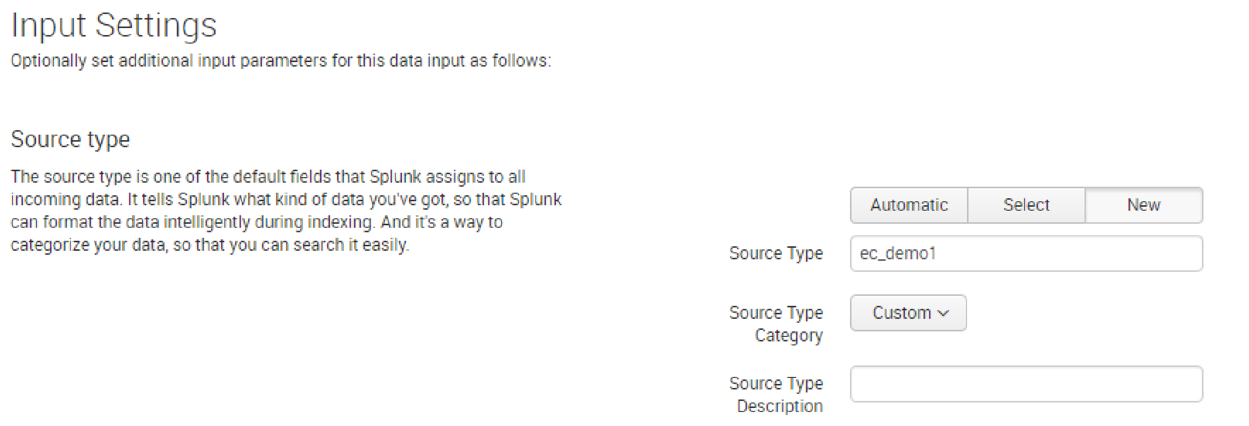
Configure a new token for receiving data over HTTP. Learn More

Name: Demo1

Source name override ?: optional

Description ?: optional

Output Group (optional): None



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

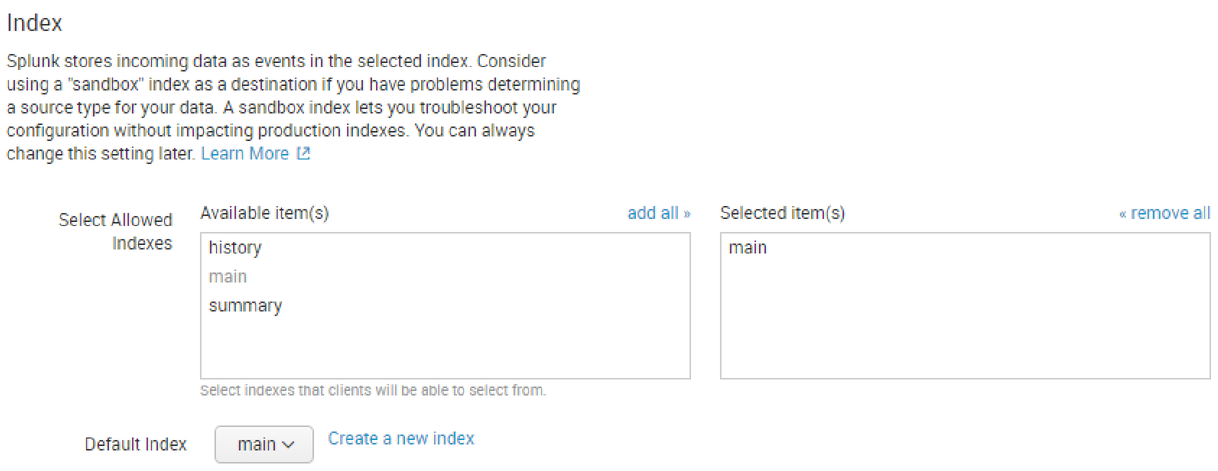
The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic | Select | New

Source Type: ec_demo1

Source Type Category: Custom

Source Type Description:



Index

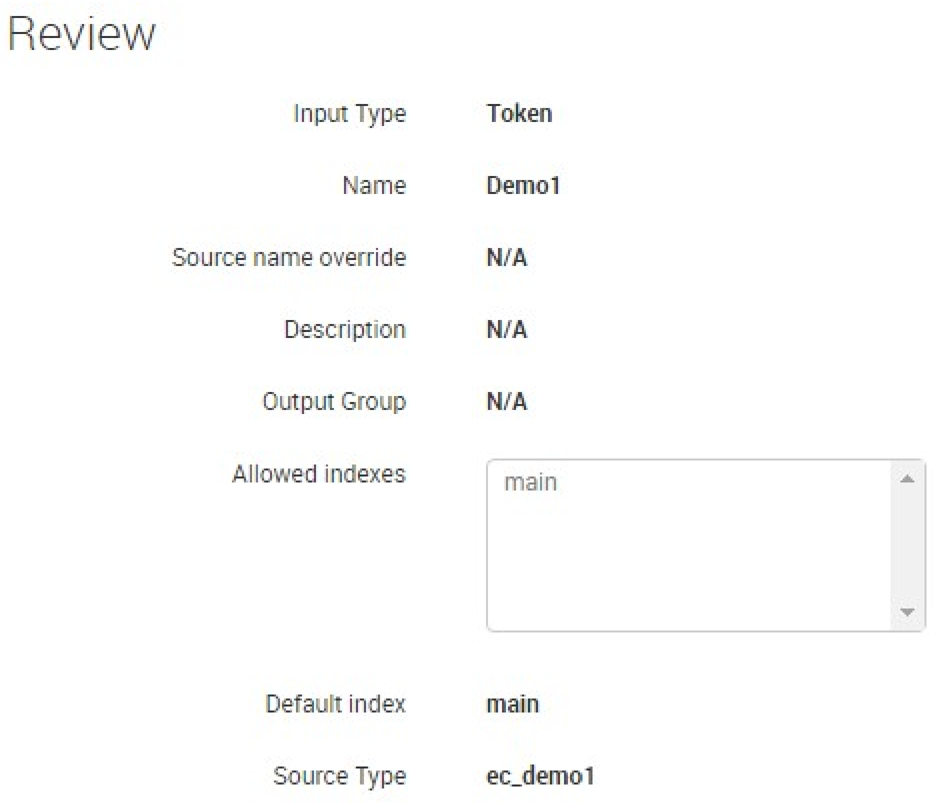
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Select Allowed Indexes

Available item(s) add all »	Selected item(s) « remove all
history main summary	main

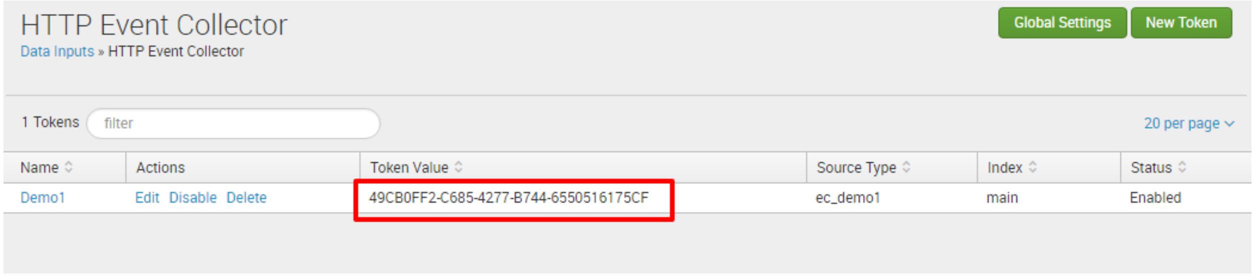
Select indexes that clients will be able to select from.

Default Index: main



Review

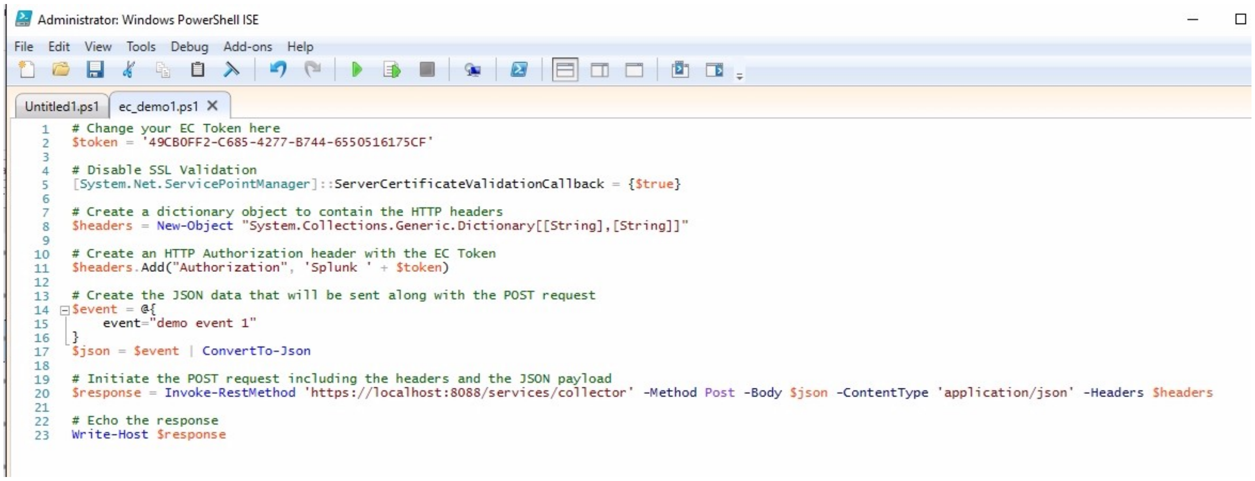
Input Type	Token
Name	Demo1
Source name override	N/A
Description	N/A
Output Group	N/A
Allowed indexes	main
Default index	main
Source Type	ec_demo1



HTTP Event Collector

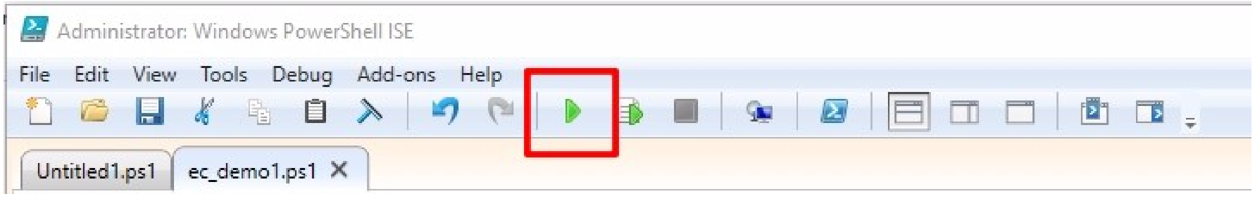
Data Inputs » HTTP Event Collector

Name	Actions	Token Value	Source Type	Index	Status
Demo1	Edit Disable Delete	49CB0FF2-C685-4277-B744-6550516175CF	ec_demo1	main	Enabled

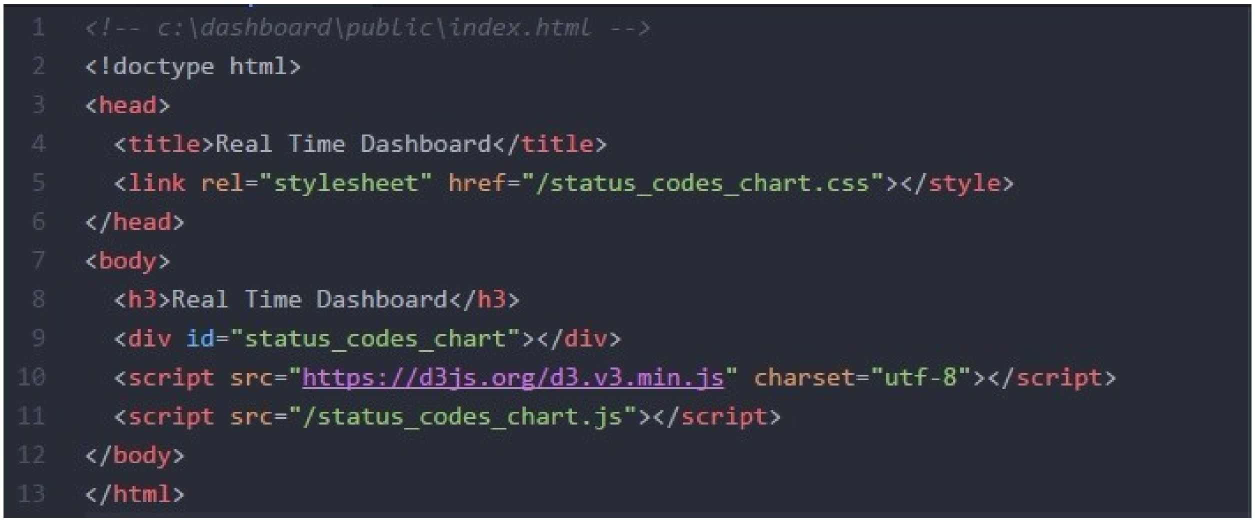


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1
ec_demo1.ps1

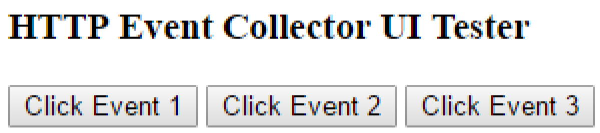
```powershell
# Change your EC Token here
$token = '49CB0FF2-C685-4277-B744-6550516175CF'

# Disable SSL Validation
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}

# Create a dictionary object to contain the HTTP headers
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"

# Create an HTTP Authorization header with the EC Token
$headers.Add("Authorization", 'Splunk ' + $token)

# Create the JSON data that will be sent along with the POST request
$event = @{
    event="demo event 1"
}
$json = $event | ConvertTo-Json

# Initiate the POST request including the headers and the JSON payload
$response = Invoke-RestMethod 'https://localhost:8088/services/collector' -Method Post -Body $json -ContentType 'application/json' -Headers $headers

# Echo the response
Write-Host $response
```



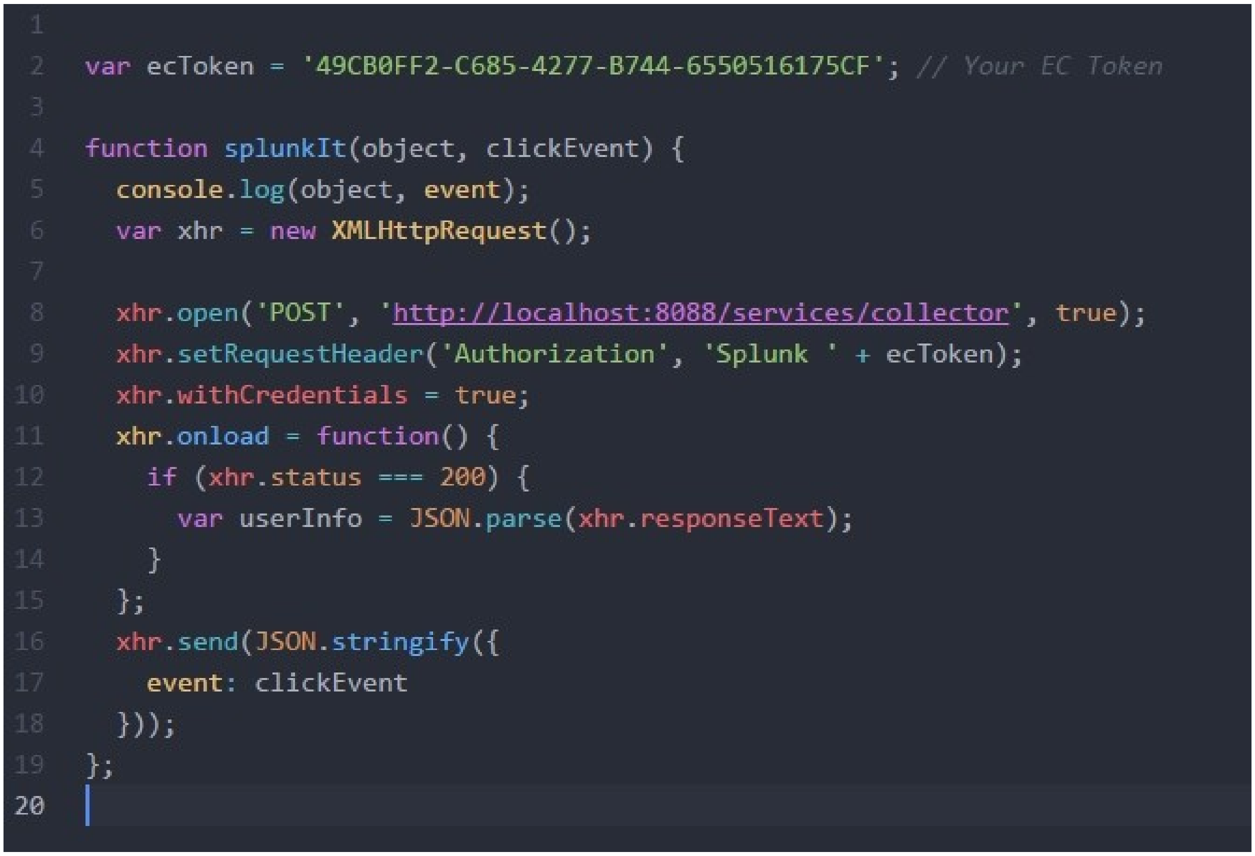
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1
ec_demo1.ps1



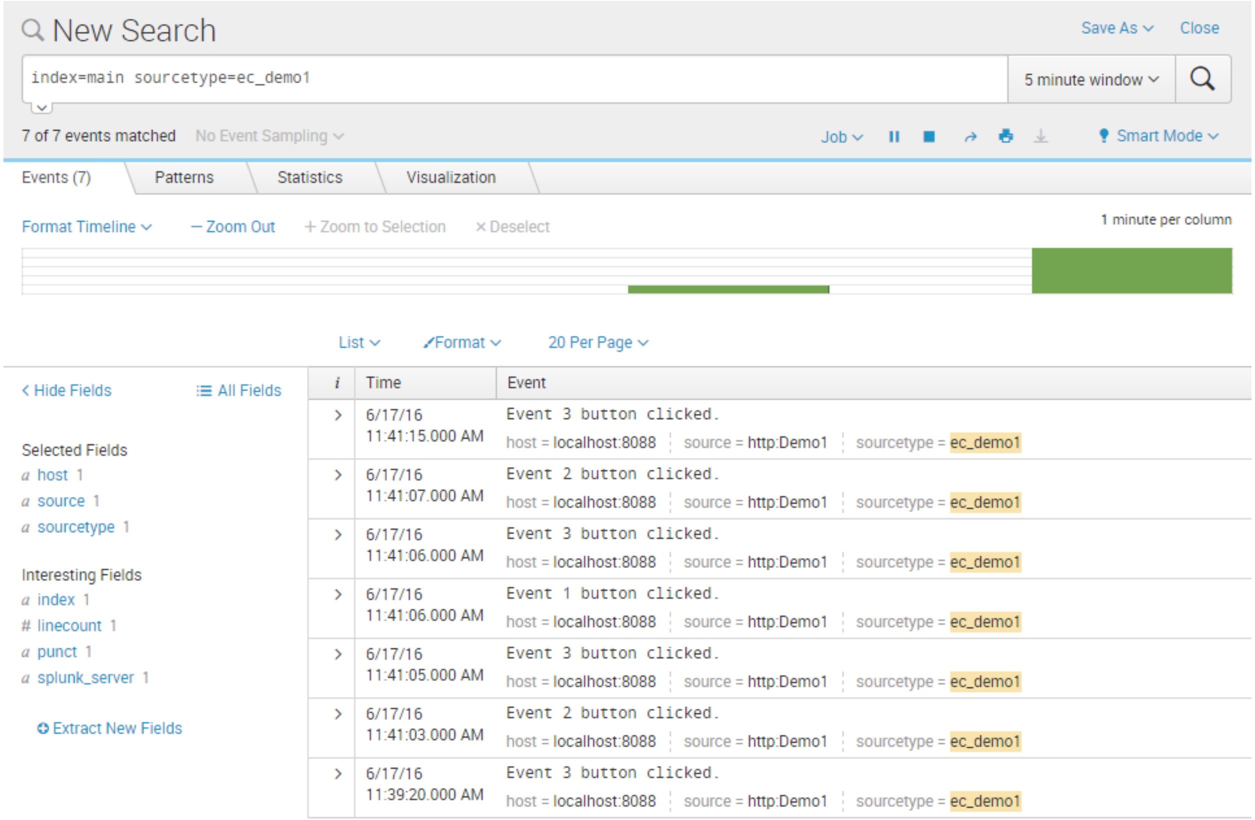
```html
<!-- c:\dashboard\public\index.html -->
<!doctype html>
<head>
  <title>Real Time Dashboard</title>
  <link rel="stylesheet" href="/status_codes_chart.css"></style>
</head>
<body>
  <h3>Real Time Dashboard</h3>
  <div id="status_codes_chart"></div>
  <script src="https://d3js.org/d3.v3.min.js" charset="utf-8"></script>
  <script src="/status_codes_chart.js"></script>
</body>
</html>
```



HTTP Event Collector UI Tester



```
var ecToken = '49CB0FF2-C685-4277-B744-6550516175CF'; // Your EC Token

function splunkIt(object, clickEvent) {
  console.log(object, event);
  var xhr = new XMLHttpRequest();

  xhr.open('POST', 'http://localhost:8088/services/collector', true);
  xhr.setRequestHeader('Authorization', 'Splunk ' + ecToken);
  xhr.withCredentials = true;
  xhr.onload = function() {
    if (xhr.status === 200) {
      var userInfo = JSON.parse(xhr.responseText);
    }
  };
  xhr.send(JSON.stringify({
    event: clickEvent
  }));
};

```



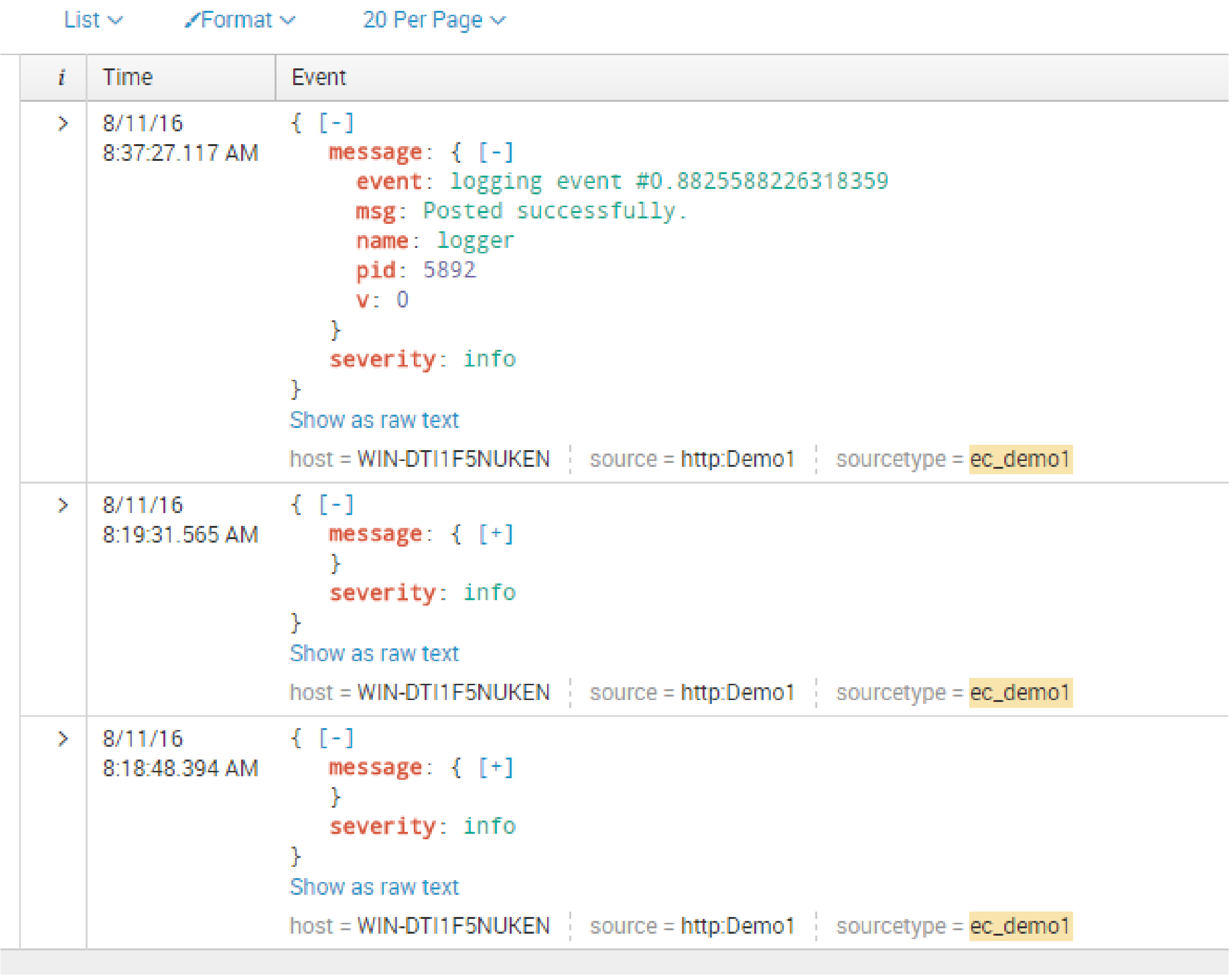
```
index=main sourcetype=ec_demo1
```

7 of 7 events matched No Event Sampling

Selected Fields
a host 1
a source 1
a sourcetype 1

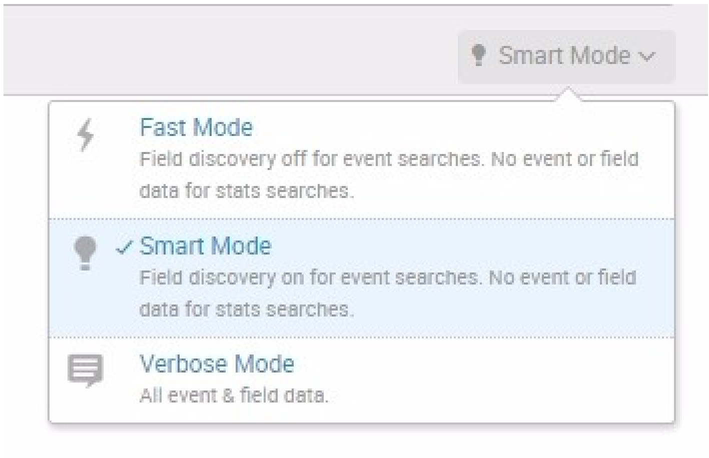
Interesting Fields
a index 1
# linecount 1
a punct 1
a splunk_server 1

i	Time	Event
>	6/17/16 11:41:15.000 AM	Event 3 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1
>	6/17/16 11:41:07.000 AM	Event 2 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1
>	6/17/16 11:41:06.000 AM	Event 3 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1
>	6/17/16 11:41:06.000 AM	Event 1 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1
>	6/17/16 11:41:05.000 AM	Event 3 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1
>	6/17/16 11:41:03.000 AM	Event 2 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1
>	6/17/16 11:39:20.000 AM	Event 3 button clicked. host = localhost:8088 source = http:Demo1 sourcetype = ec_demo1



```
 i   Time                Event
 >   8/11/16             { [-]
     8:37:27.117 AM         message: { [-]
                              event: logging event #0.8825588226318359
                              msg: Posted successfully.
                              name: logger
                              pid: 5892
                              v: 0
                            }
                            severity: info
                         }
                         Show as raw text
                         host = WIN-DTI1F5NUKEN   source = http:Demo1   sourcetype = ec_demo1
 >   8/11/16             { [-]
     8:19:31.565 AM         message: { [+]
                            }
                            severity: info
                         }
                         Show as raw text
                         host = WIN-DTI1F5NUKEN   source = http:Demo1   sourcetype = ec_demo1
 >   8/11/16             { [-]
     8:18:48.394 AM         message: { [+]
                            }
                            severity: info
                         }
                         Show as raw text
                         host = WIN-DTI1F5NUKEN   source = http:Demo1   sourcetype = ec_demo1
```

Chapter 9: Best Practices and Advanced Queries

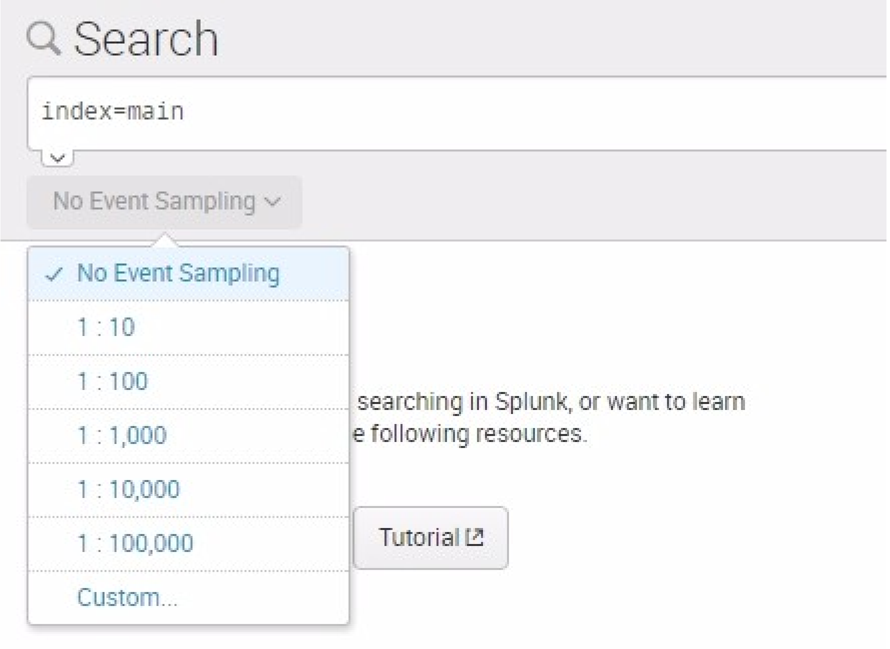


Smart Mode

Fast Mode
Field discovery off for event searches. No event or field data for stats searches.

✓ Smart Mode
Field discovery on for event searches. No event or field data for stats searches.

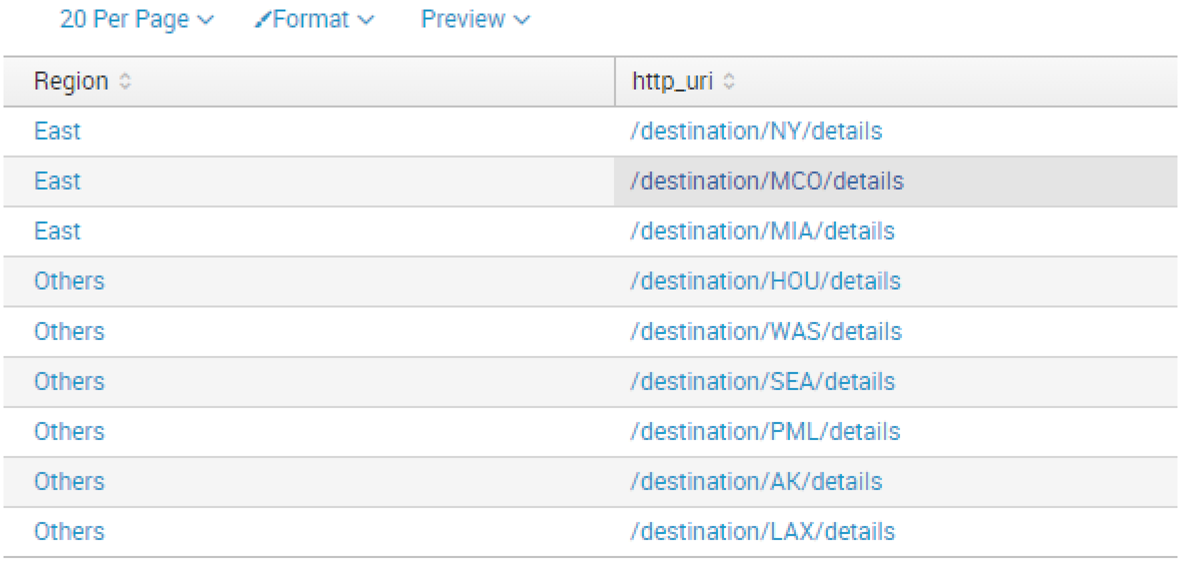
Verbose Mode
All event & field data.



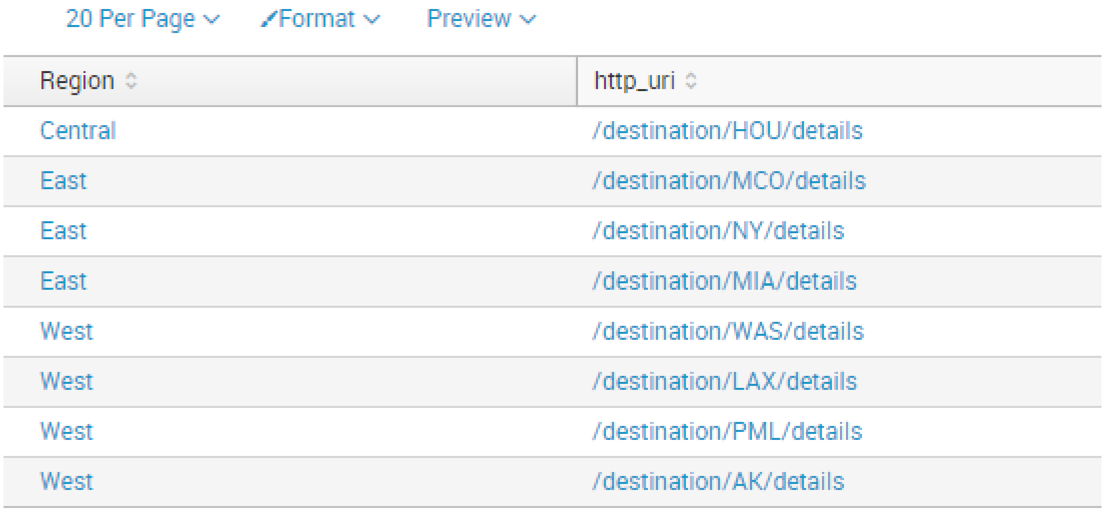
Search

```
index=main
```

No Event Sampling



Region	http_uri
East	/destination/NY/details
East	/destination/MCO/details
East	/destination/MIA/details
Others	/destination/HOU/details
Others	/destination/WAS/details
Others	/destination/SEA/details
Others	/destination/PML/details
Others	/destination/AK/details
Others	/destination/LAX/details



Region	http_uri
Central	/destination/HOU/details
East	/destination/MCO/details
East	/destination/NY/details
East	/destination/MIA/details
West	/destination/WAS/details
West	/destination/LAX/details
West	/destination/PML/details
West	/destination/AK/details