

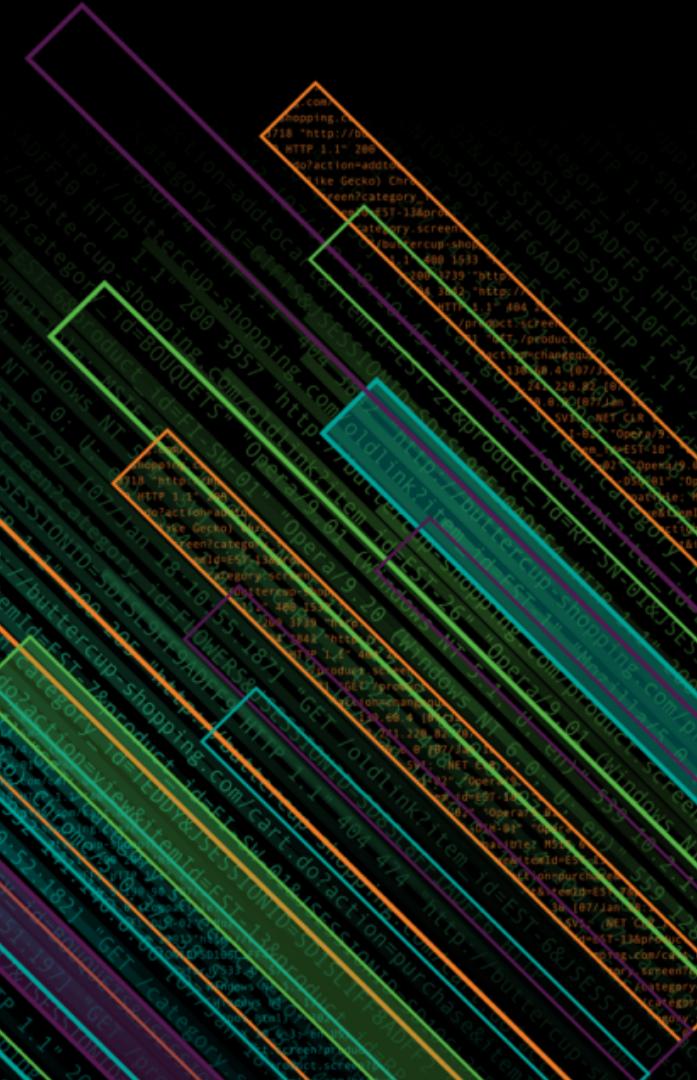


splunk>

Become a Splunk Token Master

Mike Deane | Cyber Security Automation, Red Alpha, LLC

October 4, 2018



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.



A vertical column of log entries from a Splunk search results page. The entries show various HTTP requests and responses, including file uploads, product purchases, and session IDs. The text is extremely small and dense.



My son is a plant manager,
he builds Freightliner trucks
in North Carolina.

Cyber Security Automation

mike.deane@red-alpha.com

Red Alpha, LLC

I have a 80lb seven month old puppy at home, his name is Gunther. He is part Rottweiler and part Standard Poodle.



Me, on the Thames
in London, visiting
my daughter who
works in the “Walkie
Talkie” building. She
is a financial
accountant for CNA-
Hardy.

Mike Deane

splunk> .conf18



114 National Business Parkway, Suite 200
Annapolis Junction, MD 20701

<https://www.red-alpha.com/>

This breakout session for **ABSOLUTE BEGINNERS***

- ▶ **Get the data for the code examples:**
 - <http://splk.it/f1data>
 - http://docs.splunk.com/Documentation/Splunk/7.0.1/SearchTutorial/Systemrequirements#Download_the_tutorial_data_files
- ▶ **Get the code examples:**
 - <https://github.com/endurall/splunk-token-master>

*can serve as a refresher for Splunkers with some experience or even grizzled veterans

*maybe trainers will want to attend, to see what remediation may be required for the poor noobs that are here

Token Mastery Roadmap for Absolute Beginners

- ▶ Step 1: Use OOTB (out-of-the-box) Splunk Web **event search** and **report drilldowns**
- ▶ Step 2: Use Simple XML, use the **dashboard drilldown editor** and **predefined tokens**
- ▶ Step 3: Use Simple XML, leverage **custom (including auto generated) tokens** in **forms**
- ▶ Step 4: Use Simple XML, manipulate interactions with **JavaScript extensions**
- ▶ Step 5: Insert **INLINE HTML** into Simple XML and do amazing things with JavaScript extensions
- ▶ Step 6: Leave Simple XML and, possibly, leave Splunk Web entirely!!!
 - Simple XML converted to HTML code and Splunk Web Framework (JavaScript) extensions
 - Access Splunk data from your own external web site, using the SplunkJS Stack
 - Splunk Add-on to Splunk Web
 - Splunk App for Splunk Web
 - Splunk App (runs a completely custom GUI, does not run in Splunk Web)
 - Splunk REST API
 - Splunk SDKs (JavaScript, Java, Python, C#)

Skills Needed To Become A Token Master

- ▶ **Splunk**
 - **SPL**
 - Understand the **file/directory structure** of **Splunk applications**
 - **Simple XML**
- ▶ **JavaScript**
 - Understand the use of **RequireJS** (modular script loader)
 - Understand the use of **backbone.js** (model-view-presenter framework)
 - Understand the use of **jQuery** (client-side DOM manipulation)
 - Understand the **Splunk Web Framework** and the **SplunkJS Stack**
- ▶ **Web application development**
 - **HTML**
 - **CSS**
 - Understand the basics of **web application servers**

Step 1: OOTB Event Search and Report Drilldowns

Drilldowns are the Model for All Splunk Interactivity



Searching

Search > *

Select Time Range

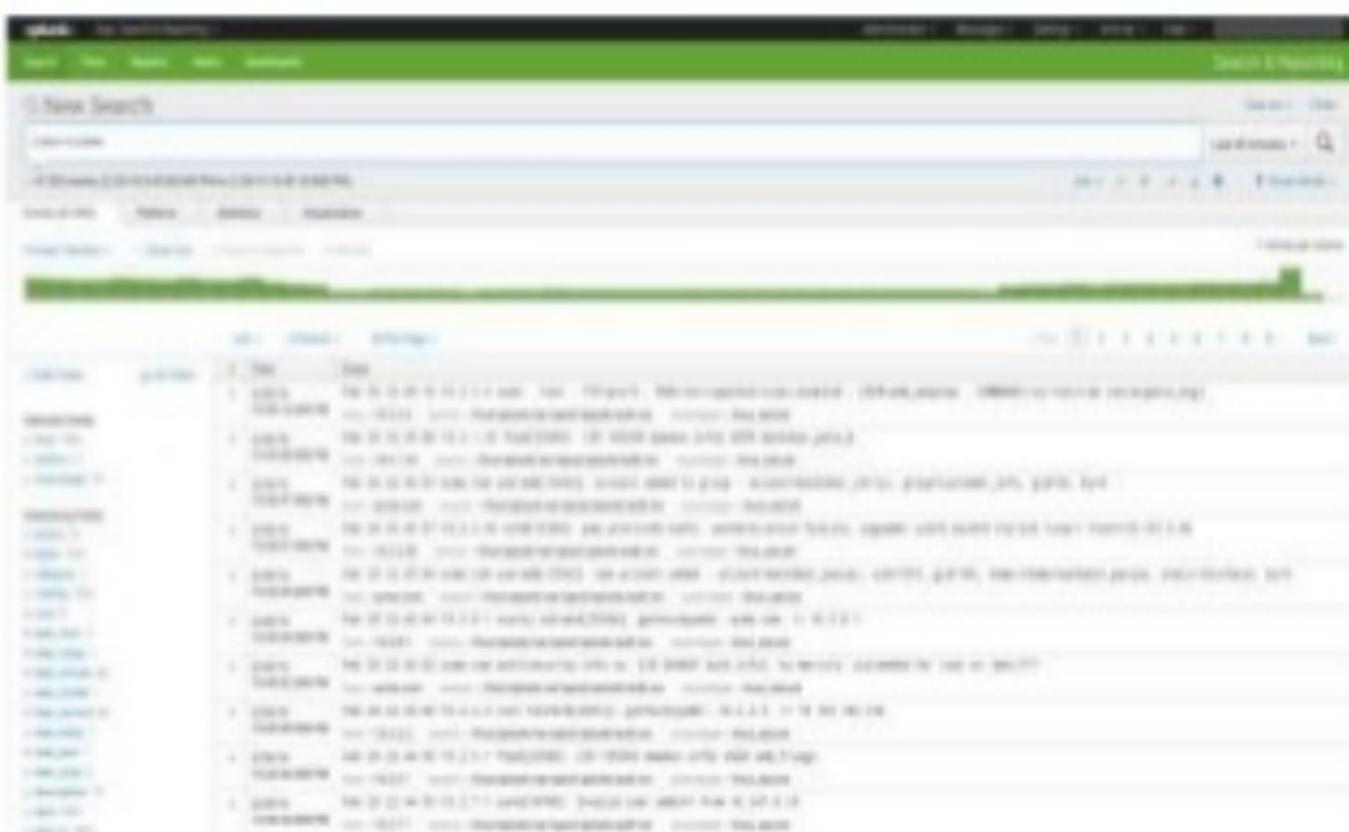
- Historical, custom, or real-time

Select Mode

- Smart, Fast, Verbose

Using the timeline

- Click events and zoom in and out
 - Click and drag over events for a specific range



Select Search Events, Then Drill Down

Rerun the Search Based on 1-of-3 Options

Type	Field	Value
Selected	host	DESKTOP-84HSNVJ
Selected	source	WinEventLog:Application
Event	ComputerName	deanemachine
Event	EventCode	16384
Event	EventType	4
Event	SourceName	Microsoft-Windows-Security-SPD
Event	TaskCategory	The operation completed successfully
Type	Type	
Time	_time	
Default	index	
Default	linecount	
Default	punct	
Default	sourcetype	

Select a search event

1. You can add the selected value as a filter to the existing search
2. You can exclude that value in the existing search
3. You can run a whole new search looking only for that event

Select Search Events, Then Drill Down

Rerun the Search by Narrower Time Range

The screenshot shows the Splunk search interface. At the top, there's a navigation bar with tabs for 'Time' and 'Event'. Below the navigation bar, the 'Event Actions' dropdown is open, showing two sections: 'Selected' and 'Event'. Under 'Selected', 'host' and 'source' are checked, with values 'DESKTOP-84HSNVJ' and 'WinEventLog:Application' respectively. Under 'Event', 'ComputerName' is set to 'deanemachine' and 'EventCode' is set to '16384'. Below this, a modal window titled '_time' is displayed. It contains a section for 'Events Before or After' with three options: 'Before this time', 'After this time', and 'At this time', with 'At this time' being selected. There's also a 'Nearby Events' section with a dropdown for 'second(s)' set to '5' and an 'Apply' button. A red arrow points from the text 'Narrow the search based on time' to the 'At this time' button in the modal window.

Narrow the search
based on time

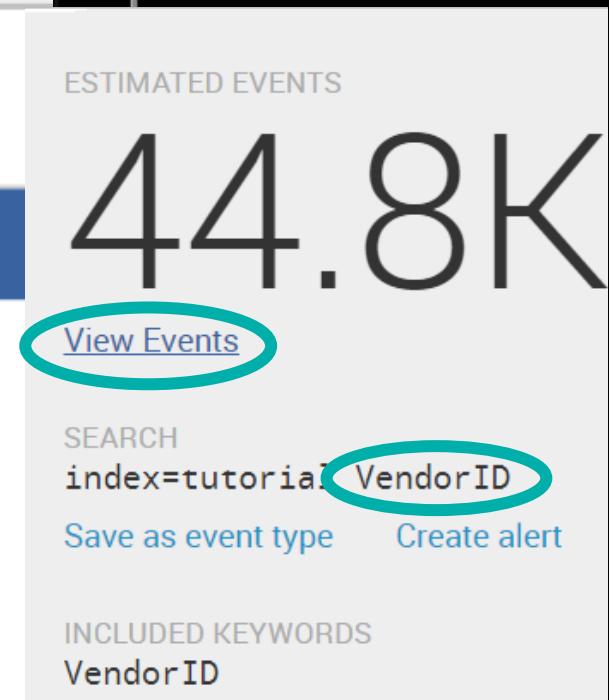
Select Search Patterns, Then Drill Down

Filter Down the Search to a Single Pattern

The screenshot shows the Splunk Patterns interface. At the top, it displays "109,880 events (before 7/30/18 11:15:50.000 PM)" and "No Event Sampling". Below this, there are tabs for "Events (109,880)", "Patterns", "Statistics (4)", and "Visualization". A message indicates "4 patterns based on a sample of 50,000 events" with a slider for "Smaller" to "Larger". The main list shows the following patterns:

- 40.73% <timestamp>| VendorID=5036 Code=50242983004
- 11.64% 195.2.240.99 -- [<timestamp>] "GET /mId=EST-21&JS8S1.1" 200
1842 "http://www.buttercupgames.co.t.scren?prodG02" Windows
NT 5.1; en-US; rv:1.9.2.28) Gecko/201F3 Firefox/3.6R 3.5
- 5.41% Thu <timestamp>mailsv1 sshd[5276]:ssword for invserve51 ssh2
- 4.34% 65.19.167.94 -- [<timestamp>] "GET /creen?categoryR&J9FF53028

Select a pattern value (highlighted), a summary statistics panel appears with a [View Events](#) link to run that search



Select Search Statistics, Then Drill Down

Rerun the Search Based on 1-of-4 Options

The screenshot shows the Splunk search interface with the following details:

- Search bar: * | stats count by sourcetype
- Event count: 193,129 events (before 7/30/18 11:39:49.000 PM)
- Sampling: No Event Sampling
- Tab navigation: Events (193,129) (selected), Patterns, Statistics (107), Visualization
- Page settings: 20 Per Page, Format, Preview
- Filter dropdown: sourcetype
- Selected filter value: WinEventLog:Application (highlighted with a red arrow)
- Result pane: sourcetype = WinEventLog:Application
- Actions menu (dropdown): View events, Other events, Exclude from results, New search (with four blue icons)

Select a statistic

1. You can add the selected value as a filter to the existing search
2. You can run a whole new search where NOT EQUAL to that value
3. You can exclude that value in the existing search
4. You can run a whole new search looking only for that value

New Search

Save As ▾

Close

sourcetype=linux_secure "Failed password"

Last 60 minutes ▾



✓ 74 events (10/5/14 9:01:00.000 PM to 10/5/14 10:01:52.000 PM)

Job ▾ II ■ ↗ ↓ ↕ Smart Mode ▾

Events (74)

Statistics

Visualization

Format Timeline ▾

Zoom Out

Zoom to Selection

Deselect

1 minute per column



List ▾

Format ▾

20 Per Page ▾

◀ Prev 1 2 3 4 Next ▶

< Hide Fields

>All Fields

	i	Time	Event
	>	10/5/14 10:00:47.000 PM	Sun Oct 05 2014 22:00:47 www1 sshd[1812]: Failed password for daemon from 10.2.10.163 port 3868 ssh2 host = www1 source = /opt/log/www1/secu... sourcetype = linux_secure
	>	10/5/14 10:00:16.000 PM	Sun Oct 05 2014 22:00:16 www1 sshd[1755]: Failed password for nsharpe from 10.2.10.163 port 4007 ssh2 host = www1 source = /opt/log/www1/secu... sourcetype = linux_secure
	>	10/5/14 9:59:37.000 PM	Sun Oct 05 2014 21:59:37 www1 sshd[5453]: Failed password for ftp from 91.208.184.24 port 3187 ssh2 host = www1 source = /opt/log/www1/secu... sourcetype = linux_secure
	>	10/5/14 9:59:28.000 PM	Sun Oct 05 2014 21:59:28 www1 sshd[4472]: Failed password for ftp from 91.208.184.24 port 1815 ssh2 host = www1 source = /opt/log/www1/secu... sourcetype = linux_secure
	>	10/5/14 9:58:39.000 PM	Sun Oct 05 2014 21:58:39 www1 sshd[3610]: Failed password for squid from 91.208.184.24 port 4066 ssh2 host = www1 source = /opt/log/www1/secu... sourcetype = linux_secure
	>	10/5/14	Sun Oct 05 2014 21:58:28 www1 sshd[2586]: Failed password for apache from 91.208.184.24 port 2103 ssh2

Selected Fields

a host 4

a source 4

a sourcetype 1

Interesting Fields

date_hour 2

date_mday 1

date_minute 47

a date_month 1

date_second 37

SEARCH EVENTS DRILLDOWN DEMO

splunk> .conf18

What drilldown options do you have available for a report?

Answer: Only 1.

When you click on a report the Splunk Search and Reporting application will open, a new search will be executed, and the new search result will be the original search filtered by whatever selection you made on the report.

Select A Report, Then Drill Down

Filter Down the Search to Include Only the Selections You Make on the Report

- When you make a selection on the visualization, a new search will run

The screenshot illustrates the process of selecting a report and then drilling down into its search results. On the left, a report titled "example_report" is displayed. It includes a green button for "Last 7 days" and a summary that 90,358 events were found between July 24, 2018, and July 31, 2018. Below this, a chart shows the count of events over time, with a specific bar for "access_combined_wcookie" highlighted by a green oval. The text "sourcetype: access_combined_wcookie" and "count: 32,528" is overlaid on this bar. On the right, the search results for this selection are shown. The search bar at the top contains the query "index = tutorial sourcetype=access_combined_wcookie". The results table shows 32,528 events, with the first two entries listed:

Time	Event
7/29/18 6:22:16.000 PM	91.205.189.15 - - [29/Jul/2018:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP/1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 JSESSIONID = SD6SL7FF7ADFF53113 ; host = DESKTOP-84HSNVJ ; source = tutorialdata.zip:\www2\access.log
7/29/18 6:22:15.000 PM	91.205.189.15 - - [29/Jul/2018:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP/1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779 JSESSIONID = SD6SL7FF7ADFF53113 ; host = DESKTOP-84HSNVJ ; source = tutorialdata.zip:\www2\access.log

Differences Between Reports, Dashboards, and Forms

Report

A report is a table or a visualization displaying data returned from a search. You can save a table or a visualization as a report. A report is built using the Splunk Web user interface. It is not editable or customizable, other than the configuration options available in the Splunk Web UI.

Dashboard

You can also save a table or visualization as a dashboard panel (an object on a dashboard). A dashboard is editable and customizable using Simple XML, HTML, and SDKs.

Form

A special kind of dashboard is a form. The dashboard is transformed into a form when data entry and selection mechanisms are added (i.e., text boxes, dropdown lists, multiselect lists, checkboxes, radio buttons, submit button, etc.).

Step 2: Dashboards Drilldown Editor, Predefined Tokens, & Simple XML

Dashboard Interactivity Based on Predefined Tokens



Save As Dashboard Panel

Dashboard New Existing

Dashboard Title

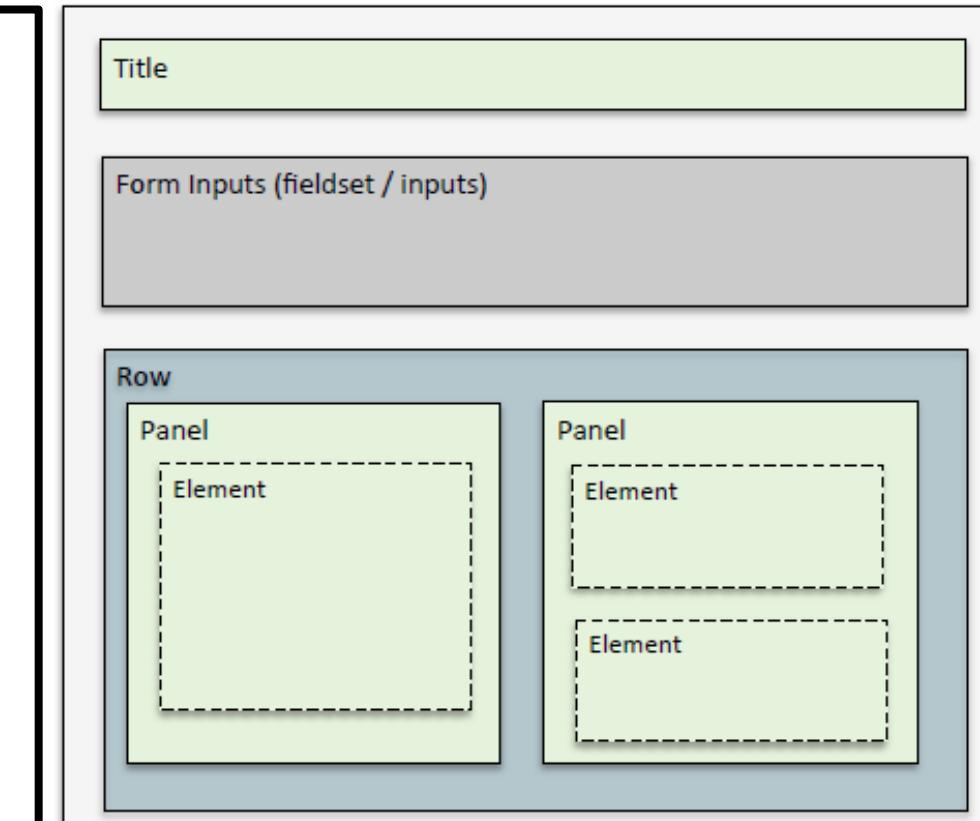
Dashboard ID ?
Can only contain letters, numbers and underscores.

Dashboard Description

Dashboard Permissions Private Shared in App

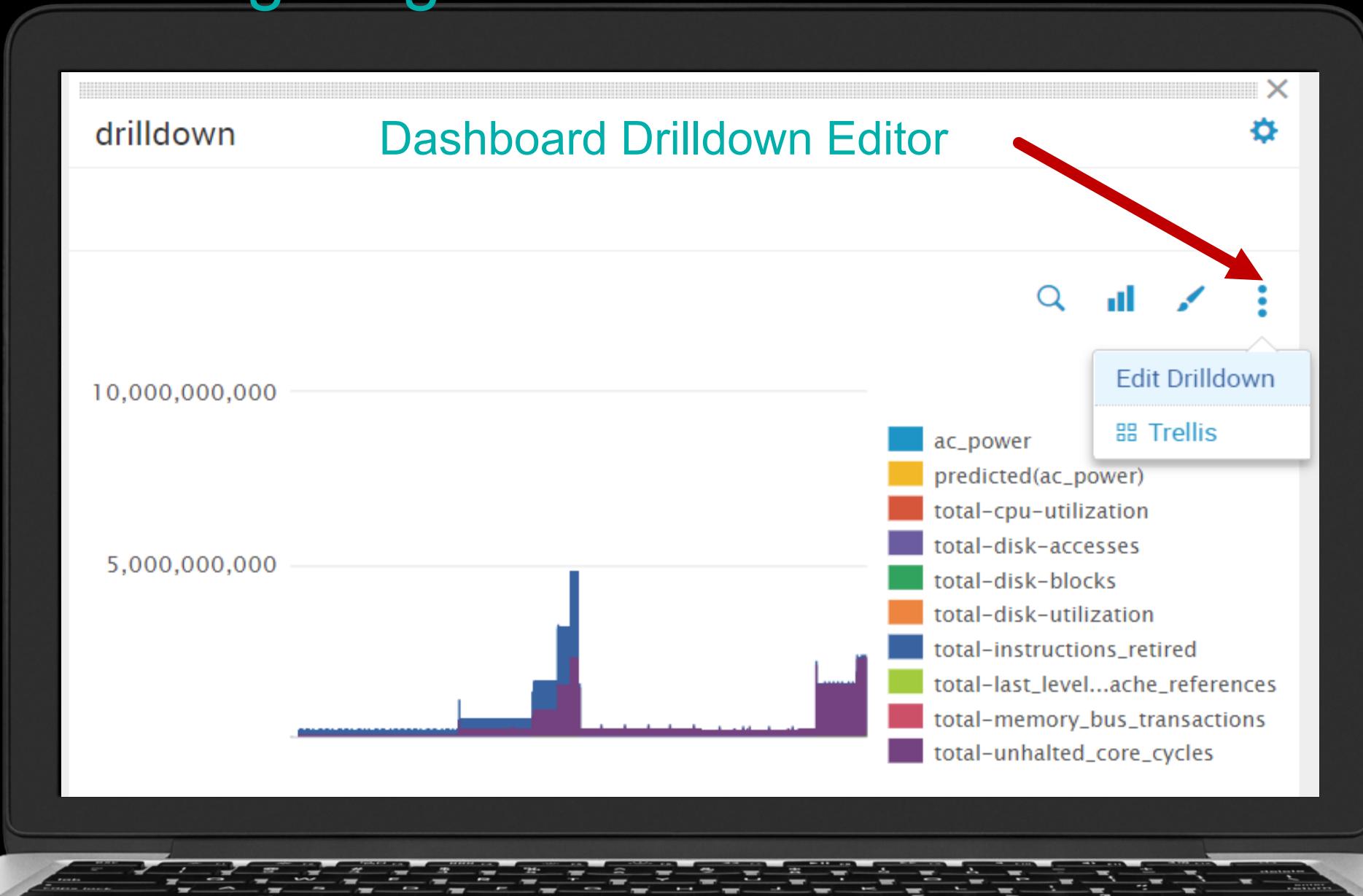
Drilldown is disabled when you save a visualization to a dashboard. After saving, open the dashboard editor to access configuration options for the visualization. Click "Edit Drilldown" to enable and configure drilldown.

Drilldown No action



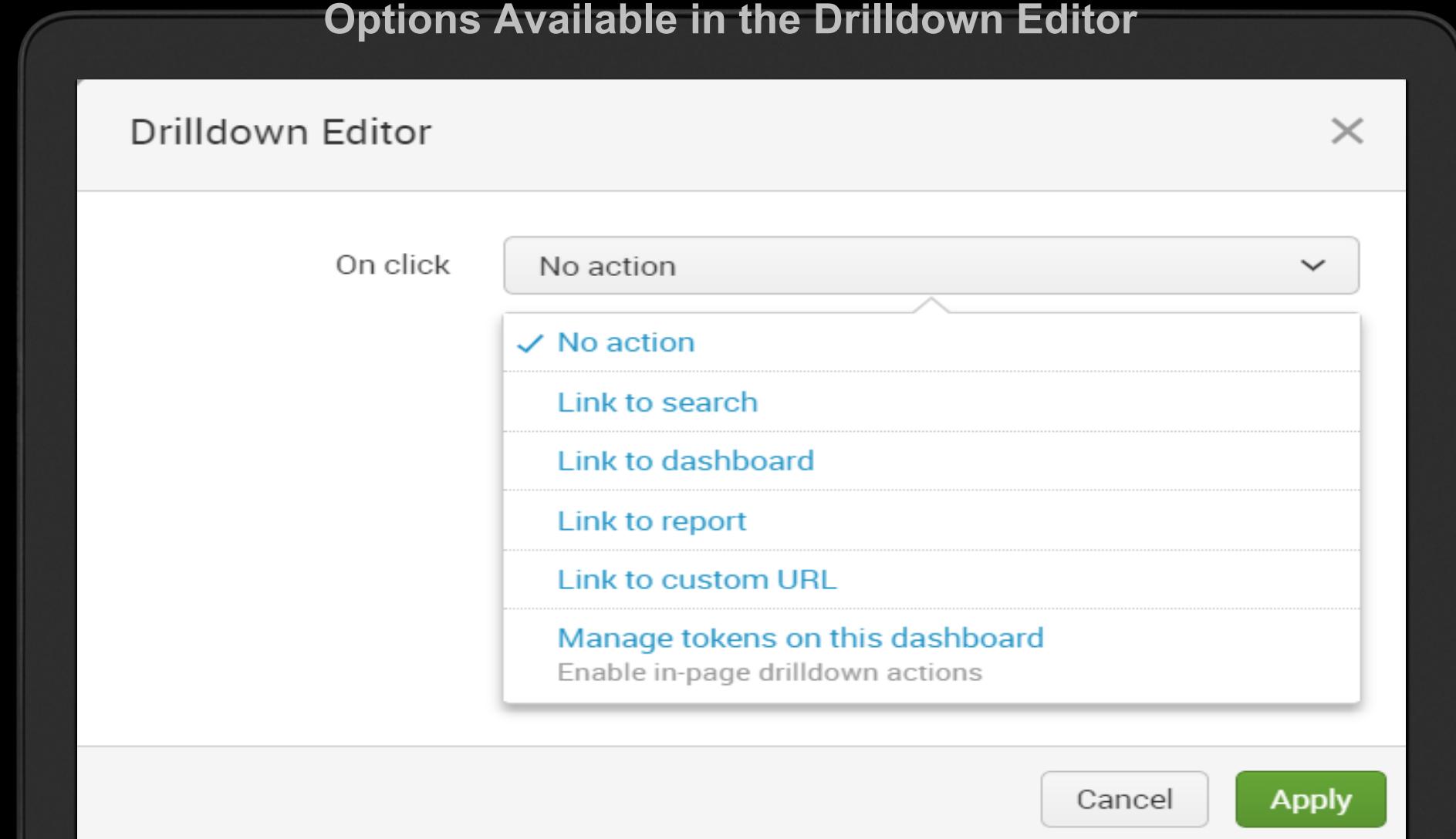
Once you have saved a table or visualization as a dashboard panel, you can edit it using the Dashboard Drilldown Editor (see the next slide).

Configuring Drilldown on a Dashboard



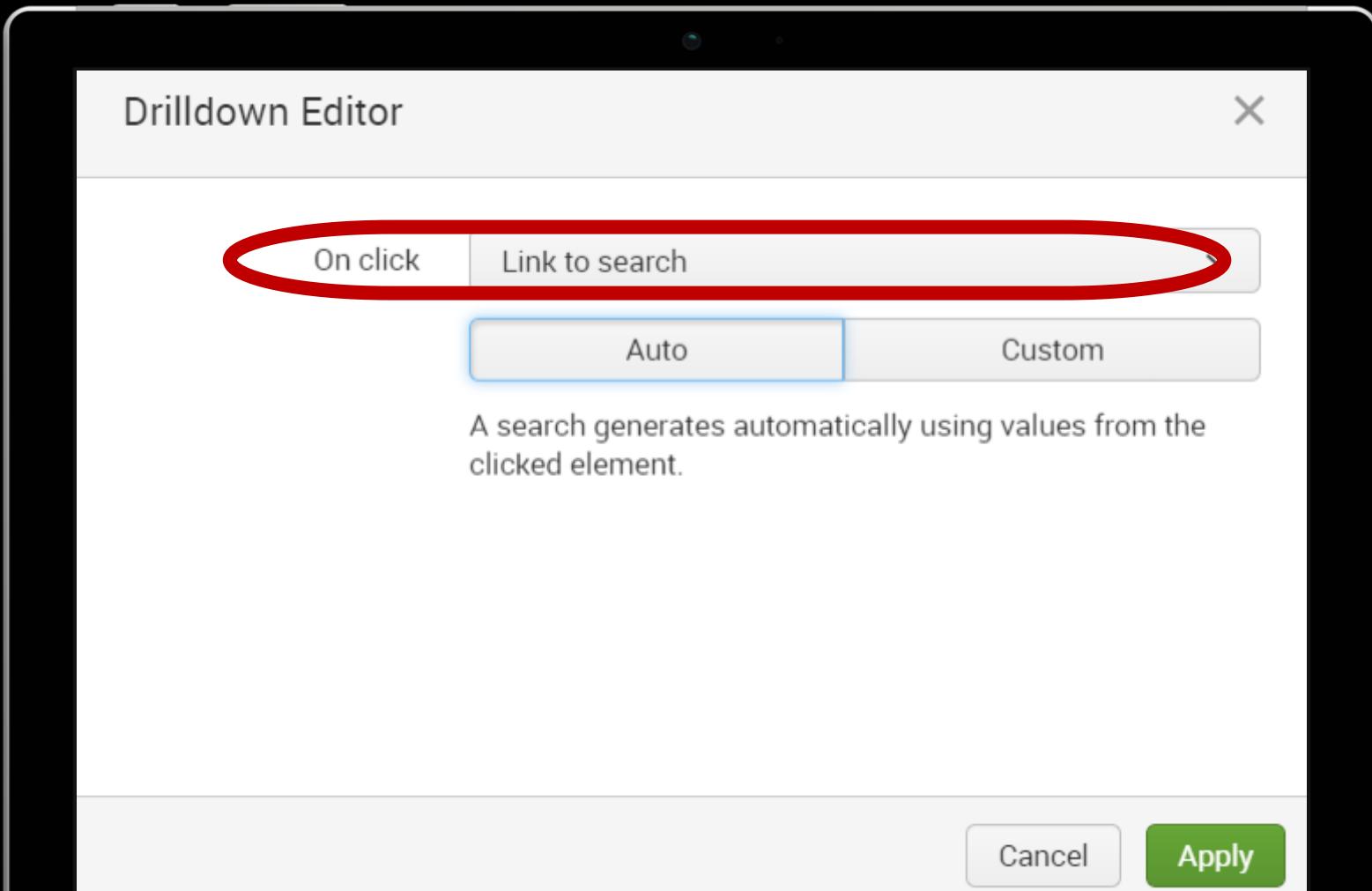
Dashboard Drilldown Editor

Options Available in the Drilldown Editor



Dashboard Link to Search Drilldown

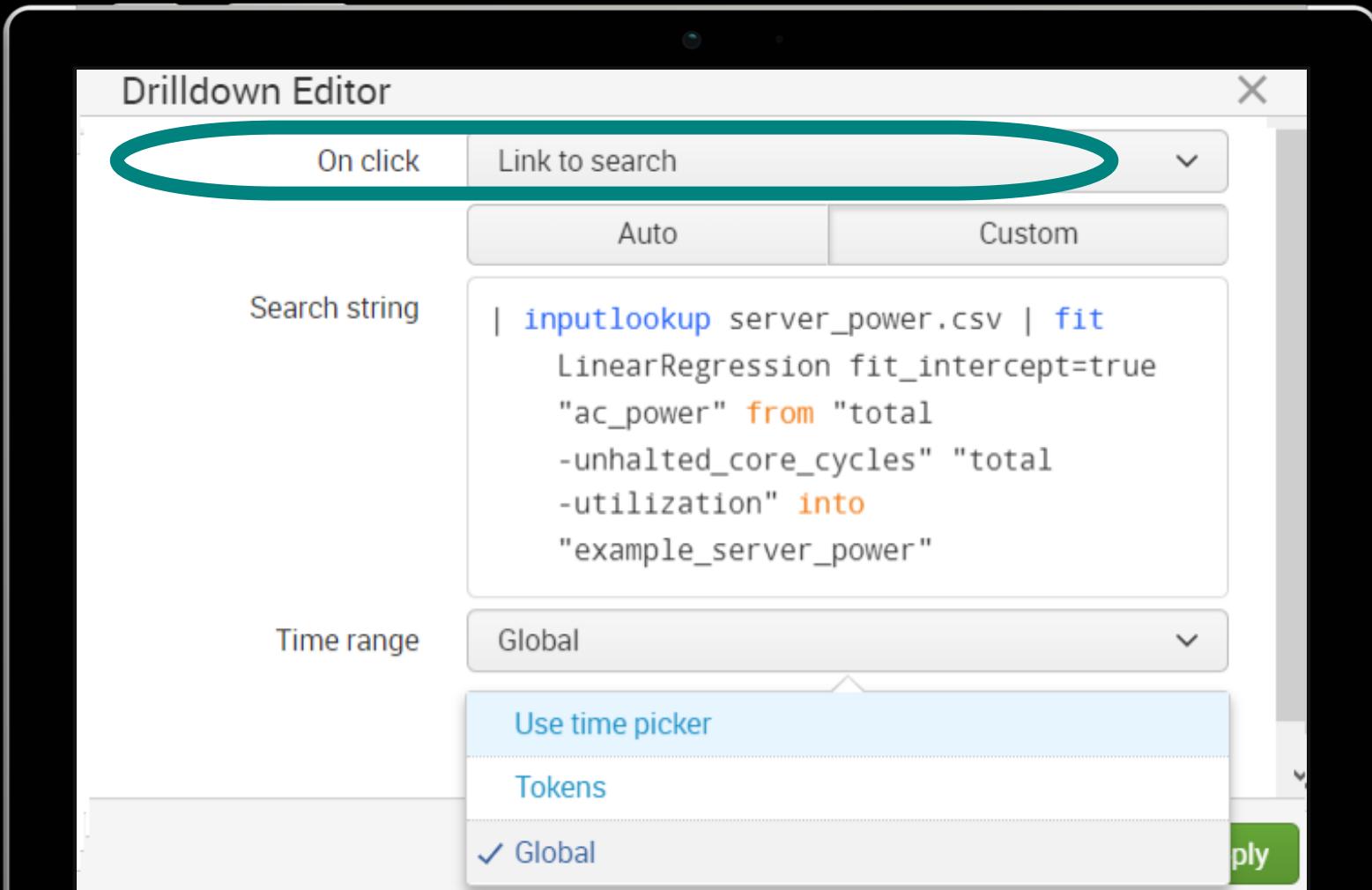
Auto Settings



- ▶ When you make a selection on the visualization, the selected value will be added as a filter to the existing search

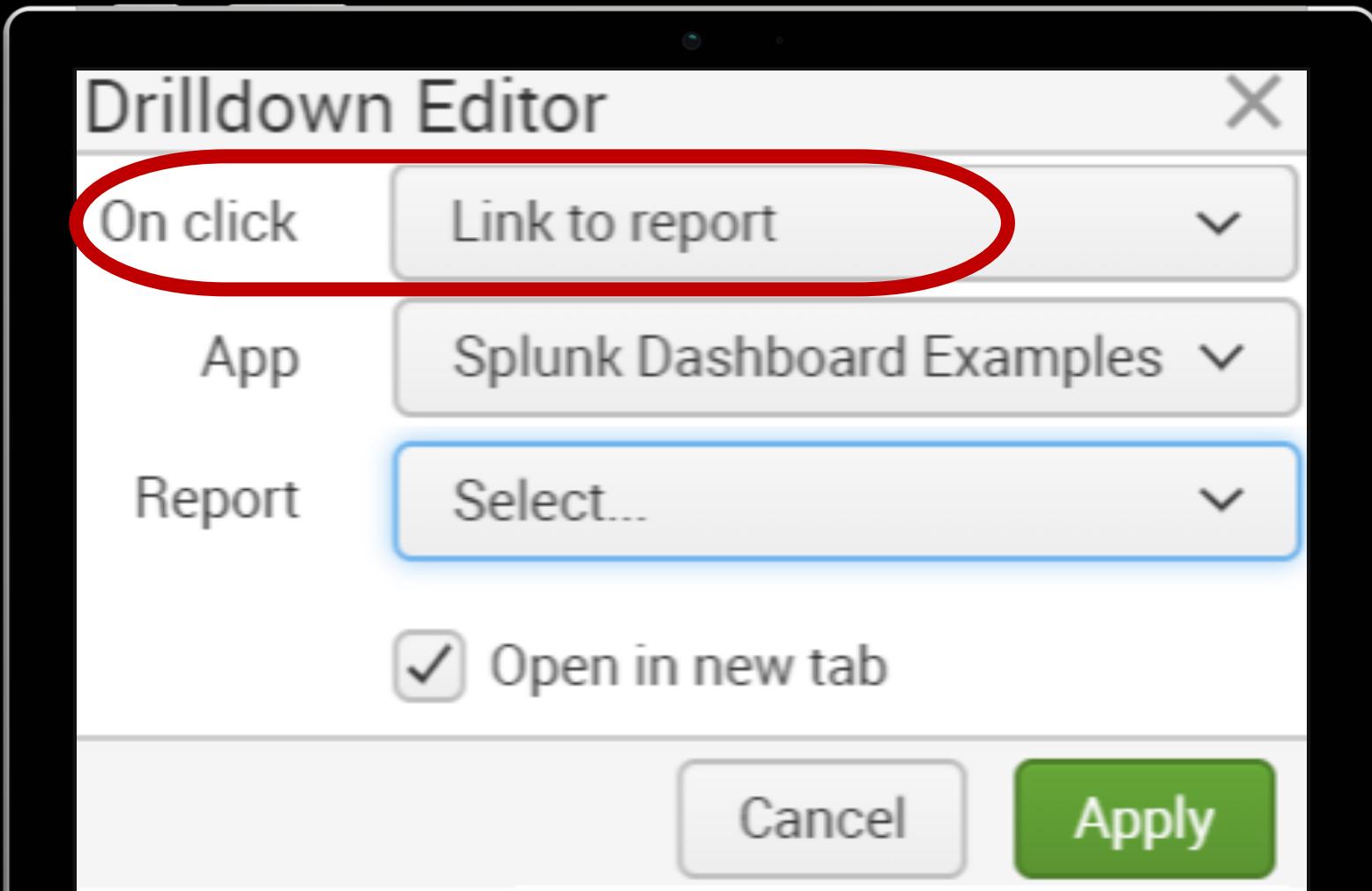
Dashboard Link to Search Drilldown

Custom Settings: Run a Completely Different Search



- ▶ When you make a selection on the visualization, a new search will run
 - Customize the search string to run
 - Configure the time range for the search
 - **NOTICE: Tokens are an option, this is the first sign of tokens!!!**

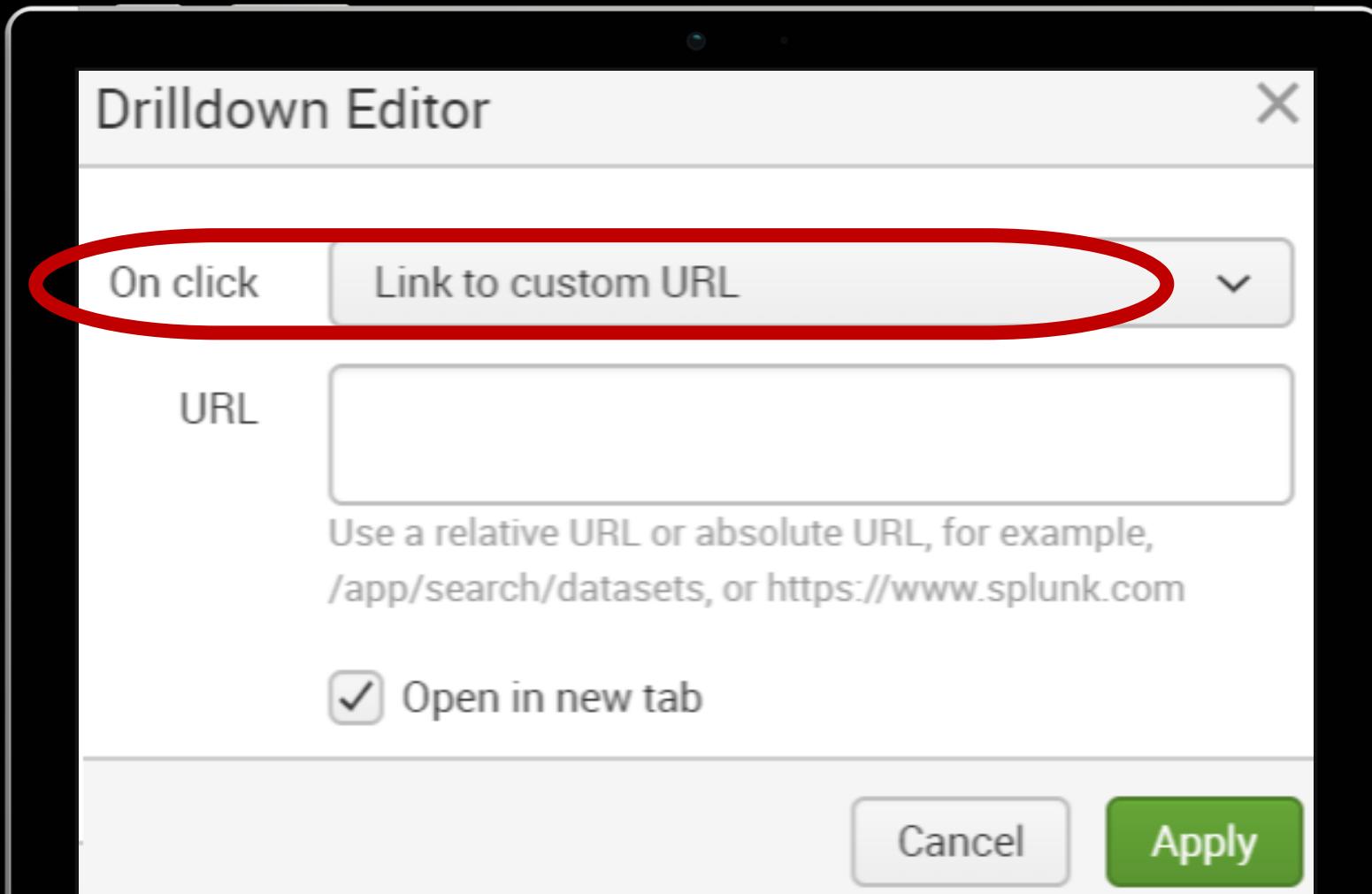
Dashboard Link to Report Drilldown



- ▶ When you make a selection on the visualization, a pre-existing report will open

Dashboard Link to Custom URL Drilldown

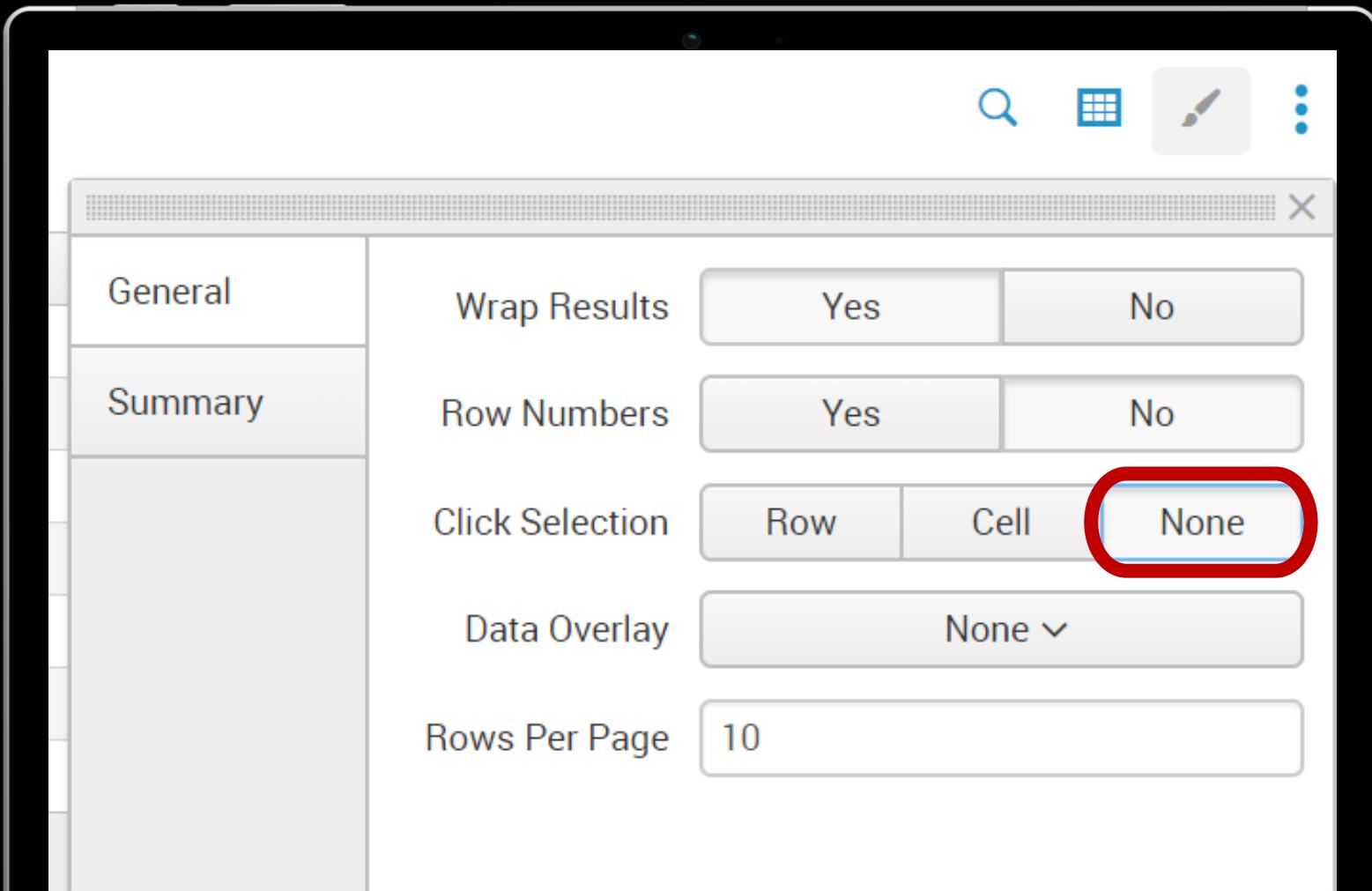
May be external to Splunk



- ▶ When you make a selection on the visualization, a URL will open

Dashboard Disable Drilldown

No Drilldown on this Dashboard



- Select paint brush
 - General tab
 - Click Selection
 - None

Drilldown Elements

sourcetype	source
scheduler	schedule
splunk_python	python
splunk_web_access	access
splunk_web_service	service
splunkd	d
splunkd_access	access
splunkd_ui_access	access

Disable Drilldown Action

Disable drilldown action through UI Editor or editing XML.

[NEW EXAMPLE](#)

6.2 6.3 6.4 6.5 6.6



Drilldown to Search

Enable drilldown to search action through UI editor or editing XML.

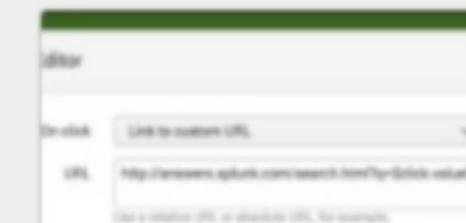
[NEW EXAMPLE](#)

6.2 6.3 6.4 6.5 6.6



Drilldown Link to Report

Enable link to report action through UI Editor or editing XML.



Drilldown Link to Custom URL

Enable link to custom url action through UI Editor or editing XML.

DASHBOARD DRILLDOWN EDITOR DRILLDOWN TO SEARCH, LINK TO REPORT, LINK TO URL, & DISABLE DRILLDOWN

https://answers.splunk.com/questions/1023357/drilldown-elements-on-a-dashboards.html

Poll Question

How many Splunk Web predefined tokens can you name?

How Many Splunk Web Predefined Tokens Can You Name?

Answer: There are many.

Event (all): click.name, click.value, click.name2, click.value2, row.<fieldname>, earliest, latest

Trellis: trellis.name, trellis.value

Chart: row.<x-axis-name>

Map: click.lat.name, click.lat.value, click.lon.name, click.lon.value

Cluster Map: click.bounds.<orientation>

Environment: see on a following slide

Job Properties: see on a following slide

Predefined Tokens for Splunk Environment Information

Name	Description
\$env:user\$	Current user's user name
\$env:user_realname\$	Current user full name.
\$env:user_email\$	Current user email address.
\$env:app\$	Current app context
\$env:locale\$	Current locale
\$env:page\$	Currently open page
\$env:product\$	Current instance product type
\$env:instance_type\$	Indicates whether the current instance is Splunk Cloud or an on-premises deployment
\$env:is_cloud\$	Indicates if the current instance is Splunk Cloud. This token is only set when "true".
\$env:is_enterprise\$	Indicates if the current instance is a Splunk Enterprise deployment. This token is only set when "true".
\$env:is_hunk\$	Indicates if the current instance is a Hunk deployment. This token is only set when "true".
\$env:is_lite\$	Indicates if the current instance is a Splunk Light deployment. This token is only set when "true".
\$env:is_lite_free\$	Indicates if the current instance is using a Splunk Light free license. This token is only set when "true".
\$env:is_free\$	Indicates if the current instance is using a Splunk Enterprise free license. This token is only set when "true".
\$env:version\$	Current instance product version

Predefined Tokens for Search Job Properties

`$job.earliestTime$`: Initial job start time.

`$job.latestTime$`: Latest time recorded for the search job.

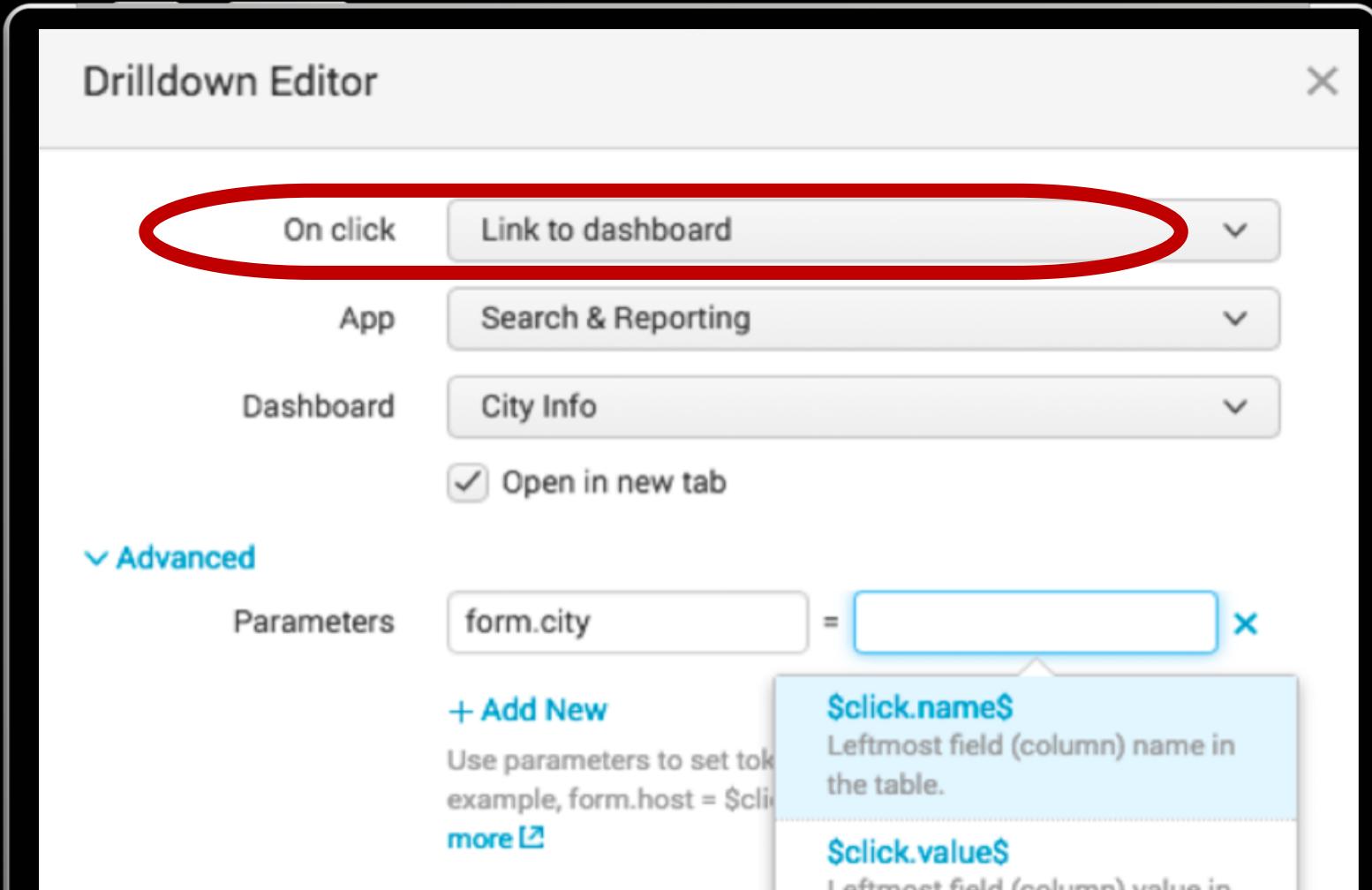
`$job.resultCount$`: Number of results a search job returned.

`$job.runDuration$`: Time, in seconds, for the search to complete.

`$job.messages$`: List of error and/or debug messages generated by the search job.

Dashboard Link to Dashboard Drilldown

Select a Different Dashboard & Pass Parameters to the Search in the Other Dashboard



- When you make a selection on the visualization, a pre-existing dashboard will open
 - Parameters can be passed to the other dashboard
 - NOTICE:** The parameters are passed using tokens!!!
 - parameter = predefined or custom token**

Dashboard In-page Drilldown

Configure In-page Drilldown Actions

Drilldown Editor

On Click Manage tokens on this dashboard ▾

- No action
- Link to search
- Link to dashboard
- Link to report
- Link to custom URL
- Manage tokens on this dashboard

Dashboard In-page Drilldown

<set>, <unset> and <eval> are the Configurable Options

The screenshot shows the Splunk Drilldown Editor interface. At the top left, it says "Drilldown Editor". Below that is a toolbar with two buttons: "On Click" (highlighted with a teal oval) and "Manage tokens on this dashboard". A dropdown menu is open next to the "Manage tokens" button. Below the toolbar, there is a text area with instructions: "Use <set>, <eval>, and <unset> to update token values. This can help you create responsive content or display changes in dashboards and forms. Learn more" with a link icon. Underneath this text is a "Set" dropdown menu, followed by input fields for "Token name" and "Token value", and a delete "X" button. At the bottom of this section is a "+ Add New" button. At the very bottom, there is a note: "Example: form.host = \$click.value2\$ or host = \$row.host\$".

<set> option
<unset> option
<eval> option

In-page Drilldown with Perma-Linking

Enable in-page interaction through UI Editor or editing XML.

Drilldown Link Dashboard

Enable link to dashboard action thro UI Editor or editing XML.

DASHBOARD DRILLDOWN EDITOR IN-PAGE DRILLDOWN & LINK TO ANOTHER DASHBOARD

130 69.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10ADF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_6&product_name=GIFTS_1&size=S&w_qty=1" "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST_26&product_id=EST_26&product_name=Buttercup_Smoothie_Cream_4_6" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 30 128 241.229.82 - [07/Jan 18:10:57:123] "GET /category.screen?category_id=EST_16&product_id=RP-LI-02" "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST_26&JSESSIONID=SD5SL9F1ADFF3 HTTP 1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=changequantity?itemId=EST_16&product_id=EST_16&product_name=RP-LI-02" "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST_6&JSESSIONID=SD15L4FF10 HTTP 1.1" 404 317 27.160.8.0 - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST_26&JSESSIONID=SD5SL9F1ADFF3 HTTP 1.1" 200 4318 "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST_6&JSESSIONID=SD15L4FF10 HTTP 1.1" 404 128 241.229.82 - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST_26&product_id=EST_26&product_name=Buttercup_Smoothie_Cream_4_6" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 30 128 69.4 - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L4FF10 HTTP 1.1" 404 72@ "http://buttercup-shopping.com/cart.do?action=view&itemId=EST_6&product_id=EST_6&product_name=GIFTS_1&size=S&w_qty=1" "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST_26&product_id=EST_26&product_name=Buttercup_Smoothie_Cream_4_6" "Opera/9.80 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 30

```
<dashboard>
```

```
  <label>predefined-token-drilldown</label>
```

```
  <row>
```

```
    <panel>
```

```
      <table><title>Drilldown to http://answers.splunk.com</title>
```

```
      <search>
```

```
        <query>
```

```
          index=_internal | stats count by sourcetype | sort -count
```

```
        </query>
```

```
        <earliest>-60m</earliest>
```

```
        <latest>now</latest>
```

```
        </search>
```

```
      <drilldown target="blank">
```

```
        <link>
```

```
          http://answers.splunk.com/search.html?q=$click.value$
```

```
        </link>
```

```
      </drilldown>
```

```
    </table>
```

\$click.value\$

PREDEFINED TOKENS DEMO

Step 3: Forms Custom Tokens & Simple XML

Interactivity Based on
Custom Tokens (*including Auto Generated*)



Custom Token

```
<form>
  <label>JavaScript How To Video</label>
  <fieldset submitButton="false">
    <input type="dropdown" token="product_name">
      <label>Select Product</label>
      <search>
        <query>sourcetype=access_combined product_name=* | dedup product_name
        </query>
        <earliest>-7d@h</earliest>
        <latest>now</latest>
      </search>
      <fieldForLabel>Product Name</fieldForLabel>
      <fieldForValue>product_name</fieldForValue>
    </input>
  </fieldset>
  <row>
    <panel>
      <table>
        <search>
          <query>sourcetype=access_combined product_name=$product_name | stats count(action) as "Action Count" by action | rename act
          </query>
          <earliest>-24h</earliest>
          <latest>now</latest>
        </search>
      </table>
    </panel>
  </row>
</form>
```

```
<dashboard>
  <label>custom-token-show-panel</label>
  <row>
    <panel>
      <table> <title>Event counts by sourcetype</title>
      <search>
        <query>index=_internal | stats count by sourcetype | sort -count</query>
      </search>
      <drilldown>
        <set token="show_panel">true</set>
        <set token="selected_value">$click.value$</set>
      </drilldown>
    </table>
  </panel>
  <panel depends="$show_panel$">
    <event><title>Recent events for $selected_value$</title>
    <search>
      <query>index=_internal sourcetype=$selected_value$</query>
    </search>
  </panel>
```

Show table based
on existence of one
or more tokens

```
<table depends="$showTable$, $selected_sourcetype$">
  <option name="foo">bar</option>
</table>
```

CUSTOM TOKENS DEMO - DASHBOARD

When are tokens automatically generated for you?

Answer: Form Inputs

**When you add a form input to a dashboard,
the dashboard is transformed into a form, and
a token is generated automatically**

Auto Generated Tokens

Placing a Form Input onto a Dashboard Automatically Generates a Token

- ▶ When you add an input to a form, a token is generated automatically
 - You can customize the token name
- ▶ You have to put the plumbing in, the auto generated token will not do anything without some configuration or editing of the Simple XML by you
 - The token must be populated with some value that you can then use to perform an action
- ▶ Although the token is auto generated for you, it is really just a convenience and is exactly like a custom token
 - An auto generated token does not automatically do anything

Form Editor

General

Label field2

Search on Change

Token Options

Token? field2

Default?

Initial Value?

Token Prefix?

Token Suffix?

Token Value Prefix?

Token Value Suffix?

Static Options

Dynamic Options

Cancel

Apply

Form inputs (forms only)

<fieldset>
<input>

- ▶ <text>
- ▶ <checkbox>
- ▶ <dropdown>
- ▶ <multiselect>
- ▶ <radio>

<search> (to populate input choices)

Form Input - Cascading Dropdowns

```
<input type="dropdown" token="Country" searchWhenChanged="true">  
<search><query>... | stats count by Country
```

```
<input type="dropdown" token="Region" searchWhenChanged="true">  
<search><query>... | stats count by Region
```

```
<input type="dropdown" token="City" searchWhenChanged="true">  
<search><query>... | stats count by City
```

```
<table>  
<search><query>... | stats list(count), values(categoryId) by Country Region City  
<option name="drilldown">cell</option>
```

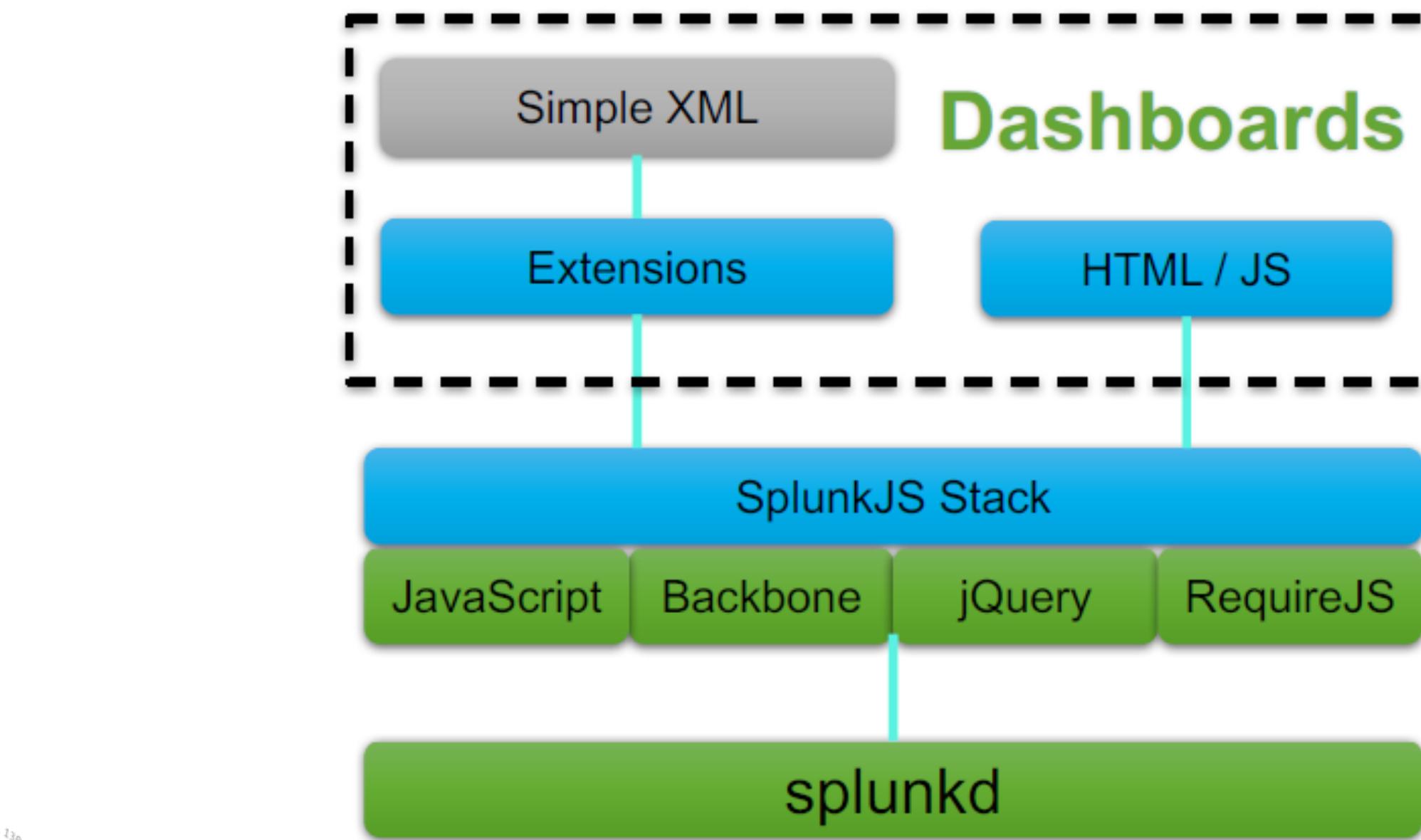
```
<map>  
<search><query>... Country=$Country|$|s$ Region=$Region|$|s$ City=$City|$|s$ | geostats count by categoryId  
<option name="drilldown">none</option>
```

CUSTOM TOKENS DEMO - FORMS

Step 4: Simple XML & JavaScript Extensions

Interactivity Based on JavaScript Extensions





JavaScript Extensions

Directory location: Where to place the JavaScript file.

Splunk/etc/apps/\$app\$/appserver/static/

**ALWAYS. ALWAYS. ALWAYS,
start the RequireJS block with “splunk/mvc” and
end the RequireJS block with “splunk/mvc/simplexml/ready!”**

```
require([
    "splunkjs/mvc",
    "splunkjs/mvc/textinputview",
    "splunkjs/mvc/simplexml/ready!",
],
```

form-multiselect.xml

```
<input id="multi1" type="multiselect" token="release_year" searchWhenChanged="false">
<valuePrefix>release_year=</valuePrefix>
<valueSuffix>"</valueSuffix>
<delimiter> OR </delimiter>

<input type="dropdown" token="genre_id" searchWhenChanged="false">

<input type="dropdown" token="orig_ln" searchWhenChanged="false">
```

multiselect.js

```
require([
  'jquery',
  'underscore',
  'splunkjs/mvc',
  'splunkjs/mvc/simplexml/ready!'
],  
function($,_mvc){  
  
  var multi1 = mvc.Components.get("multi1")  
  
  multi1.on("change",function(){  
    current_val = multi1.val()  
  
    console.log("Current Vals: " + current_val)  
  
    var first_choice_value = multi1.options.choices[0].value;  
  
    if (current_val.length > 1 && current_val.indexOf(first_choice_value) == 0) {  
      multi1.val(_.without(current_val, first_choice_value));  
    }  
  
    if (current_val.length > 1 && current_val.indexOf(first_choice_value) > 0) {  
      multi1.val([first_choice_value]);  
    }  
  });  
});
```

JAVASCRIPT EXTENSION DEMO

Poll Question

Can you name any problems you might solve with Simple XML, custom tokens, & JavaScript extensions?

Step 5: Simple XML, INLINE HTML & JavaScript Extensions

Interactivity based on manipulation of **INLINE HTML** with **JavaScript Extensions**



INLINE HTML

Typically, you will insert INLINE HTML inside a Simple XML <row>.

```
<row>
  <html>
    <div id="htmltable">
      <table>
        <tr>
          <td><img src = " /static/app/is_app_one/graph.png" /></td>
          <td>
            <p>Lorem ipsum ...</p>
            <p>Nulla ut congue ...</p>
            <p>Etiam pharetra ...</p>
          </td>
        </tr>
      </table>
    </div>
  </html>
</row>
```

HTML Custom Button (Reset)

```
<html>  
  <center>  
    <button type="button" id="buttonId" class="btn">Reset</button>  
  </center>  
</html>
```

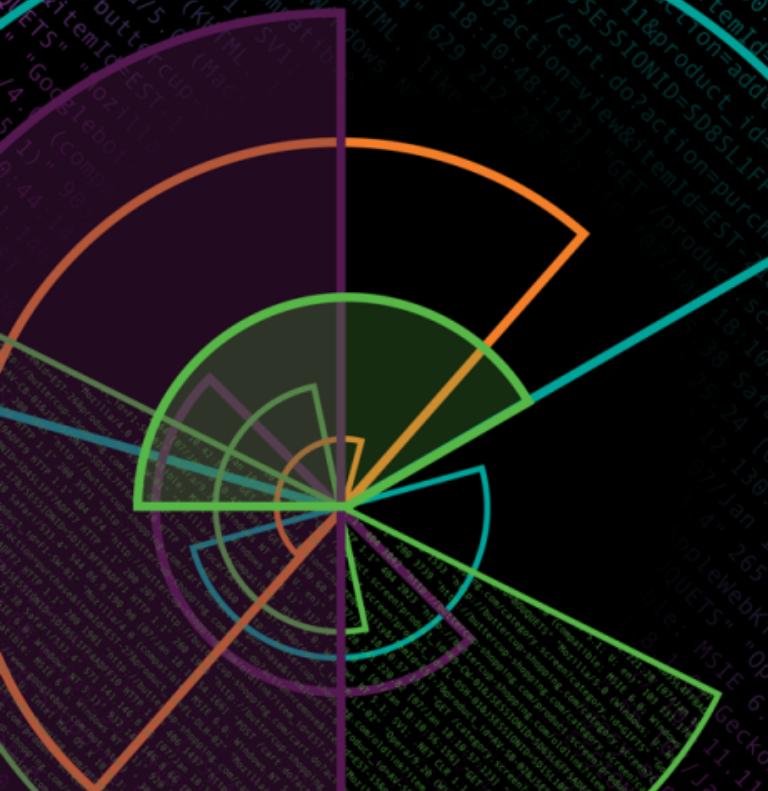
```
require([  
  'jquery',  
  'splunkjs/mvc',  
  'splunkjs/mvc/simplexml/ready!'  
], function ($, mvc) {  
  var tokens = mvc.Components.get("default");  
  tokens.on("change:app", function() {  
    $('#buttonId').on("click", resetAppToken);  
  });  

```

INLINE HTML & JAVASCRIPT EXTENSION DEMO

Step 6: Splunk Application Development without Simple XML

Many, many different Splunk Development Options



Next Steps: Roadmap For New Token Masters

- ▶ Convert Simple XML to HTML code and leverage JavaScript extensions
- ▶ Splunk Add-ons to Splunk Web
- ▶ Splunk Certified Applications for Splunk Web
- ▶ Splunk Applications (entirely custom GUI, does not run in Splunk Web)

- ▶ Splunk Rest APIs
- ▶ Splunk SDKs (JavaScript, Java, Python, C#)
 - Manage Splunk configurations and objects.
 - Integrate search results into your applications.
 - Log directly to Splunk.
 - Present a custom UI

Dynamic Columns

```
<div class="input input-radio" id="input1">
```

```
var input1 = new RadioGroupInput({
  "id": "input1",
  "choices": [
    {"value": "pickme", "label": "Pick Me"},
    {"value": "instantmillions", "label": "Instant Millions"}
  ],
  "default": "pickme",
  "searchWhenChanged": true,
  "selectFirstChoice": false,
  "value": "$form.field1$",
  "el": $('#input1')
}, {tokens: true}).render();
```

100% CONVERTED TO HTML DEMO

Boundaries

- ▶ **Boundary 1: No need for dashboards.**
 - Event searches and reports suffice
- ▶ **Boundary 2: No need for forms.**
 - Default behaviors of dashboards suffice
- ▶ **Boundary 3: No need for custom user interfaces.**
 - Default behaviors of forms suffice
- ▶ **Boundary 4: No need to insert some HTML capabilities not available in Splunk Web.**
 - JavaScript extensions with Simple XML provides adequate user interface customization
- ▶ **Boundary 5: No need for traditional web development with HTML, CSS, & JavaScript**
 - JavaScript extensions with INLINE HTML does what Simple XML cannot do

Q&A

Mike Deane | Speaker

Mike Deane

Cyber Security Automation

<https://www.cybersoar.io>

mike.deane@red-alpha.com
321-652-8356



Join the Pony Poll



[ponypoll.com/***](http://ponypoll.com/)

Thank You

Don't forget to rate this session
in the .conf18 mobile app



BONUS

INLINE HTML enables easily formatting blocks of text.

```
<dashboard>
  <row>
    <panel>
      <html>
        <div style="text-align: left;">
          This is Splunk dashboard text that spans
          across
        </div>
      </html>
    </panel>
  </row>
  <row>
    <panel>
      <html>
        <div style="text-align: center;">
          <h1>
            </h1>
          </div>
        </html>
      </panel>
    </row>
    <row>
      <panel>
        <single>
          <search>
            <query>.....</query>
            <earliest>0</earliest>
            <latest></latest>
          </search>
        </single>
      </panel>
    </row>
  </dashboard>
```

This is Splunk dashboard text that spans

multiple lines.</br>

This is text centered above a chart.