Creating Splunk Knowledge Objects

Class Goals

- Provide a deep understanding of what Splunk knowledge objects are and how they are used
- Create and manage the following knowledge objects:
  - Lookups
  - Fields (aliases, calculated, and extractions)
  - Tags and event types
  - Workflow actions
  - Alerts
  - Scheduled reports
  - Macros
  - Data models

Course Outline

Module 1: Introduction

Module 2: Implementing Knowledge Objects

Module 3: Creating Lookups

Module 4: Creating Field Aliases and Calculated Fields

Module 5: Creating Field Extractions

Module 6: Creating Tags and Event Types

Module 7: Creating Workflow Actions

Module 8: Creating Alerts and Scheduled Reports

Module 9: Creating and Using Macros

Module 10: Creating Data Models

Module 1: Introduction

Module Objectives

- Review Buttercup Games
- Become familiar with the source types and event data used during the course
- Identify the categories of knowledge objects
- Define the role of a knowledge manager
- Describe the Common Information Model
- Understand the relationship between the CIM and knowledge objects
- Identify naming conventions
- Review permissions

Buttercup Games, Inc.

- Buttercup Games, Inc.
  - Is a multinational company with its HQ in San Francisco and offices in Boston and London
  - Sells product mainly through its worldwide chain of third party stores, but also sells through its online store
- For more information about Buttercup Games, please see Appendix B

Buttercup Games Environment

Data	host	sourcetype
AD/DNS data (non-Engineering)	adldapsv1	winauthentication_security
Badge reader data	badgesv1	history_access
Email data	cisco_router1	cisco_esa
Online transactions & Web server	www1	access_combined linux_secure
	www2	
	www3	
Retail sales data	vendorUS1	vendor_sales
Splunk indexer data	splunk1	ps
Web appliance data	cisco_router1	cisco_wsa_squid
Windows system logs	adldapsv1	win_audit

Your Role at Buttercup Games

- You are a Splunk user assigned to the power role
- You have a great understanding of all your company's data
- Your responsibilities are to create and manage Splunk knowledge objects for your stakeholders
- You implement best practices for naming conventions of all knowledge objects

What are Knowledge Objects?

- Knowledge objects are tools you use to discover and analyze various aspects of your data
  - **Fields and field extractions -** Data interpretation
  - **Event types** - Data classification
  - **Lookups and workflow actions** - Data enrichment
  - **Tags and aliases** – Normalization
  - **Data Models** – Representation of datasets which drives the pivot tool

Note

For more information go to:
http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge

What is a Knowledge Manager?

A knowledge manager:

- Oversees knowledge object creation and usage for a group or deployment
- Normalizes event data
- Creates data models for Pivot users

Note

For more information go to:
http://docs.splunk.com/Documentation/Splunk/6.3.0/Knowledge/Monitorandorganizeknowledgeobjects

What is the Common Information Model (CIM)?

- The Splunk Common Information Model provides a methodology to normalize data
- Leverage the CIM when creating field extractions, event types, and tags to ensure:
  - Multiple apps can co-exist on a single Splunk deployment
  - Object permissions can be set to global for the use of multiple apps
  - Easier and more efficient correlation of data from different sources and source types

CIM Add-On

- Splunk CIM is an add-on available on splunkbase:
  - https://splunkbase.splunk.com/app/1621/
  - Includes pre-configured data models
  - Data models consist of a set of standard fields and event category tags relevant to most IT data
- Examples of data models for IT specific domains:
  - Email
  - Malware
  - Network Traffic
  - Performance
  - Ticket Management
  - Web

Note

The installation of the CIM add-on is discussed in the Building Apps class.

Note

Data used by apps like Enterprise Security must adhere to the CIM. If the CIM is not followed, objects such as dashboards, reports, and alerts might not function properly.

Normalized Field Names - Email Data

Field name	Data type	Description	Possible values
action	string	Action taken by the reporting device.	delivered, blocked, quarantined, deleted, unknown
duration	number	The amount of time for the completion of the messaging event, in seconds.	Email
src	string	The system that sent the message. May be **aliased** from more specific fields, such as src_host, src_ip, or src_name.	

Normalized Field Names - Network Traffic

Field name	Data type	Description	Possible values
action	string	The action taken by the network device.	allowed, blocked, dropped, unknown
bytes	number	Total count of bytes handled by this device/ interface (bytes_in + bytes_out).	
bytes_in	number	How many bytes this device/interface received.	
bytes_out	number	How many bytes this device/interface transmitted.	
src	string	The source of the network traffic (the client requesting the connection). May be **aliased** from more specific fields, such as src_host, src_ip, or src_name.	

Normalized Field Names – Web Data

Field name	Data type	Description	Possible values
action	string	The action taken by the server or proxy.	
duration	number	The time taken by the proxy event, in milliseconds.	
http_method	string	The HTTP method used in the request.	GET, PUT, POST, DELETE, etc.
src	string	The source of the network traffic (the client requesting the connection).	
status	string	The HTTP response code indicating the status of the proxy request.	404, 302, 500, and so on.

Additional CIM Resources

Documentation:

http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/UnderstandandusetheCommonInformationModel

http://docs.splunk.com/Documentation/CIM/latest/User/Overview

http://docs.splunk.com/Documentation/CIM/latest/User/UsetheCIMtonormalizedataatsearchtime

Defining Naming Conventions

- To avoid confusion later, develop naming conventions for your Splunk implementation early for knowledge objects like reports, alerts, and dashboards
- This course uses simple names, but using a naming convention is more efficient
  - For example:
    - **Group:** Corresponds to the working group(s) of the user saving the search (examples: SEG. NEG. OPS. NOC)
    - **Search type:** Indicates the type of search (alert, report, summary-index-populating) (examples: Alert, Report, Summary)
    - **Platform:** Corresponds to the platform subjected to the search (examples: Windows, iSeries, Network)

Defining Naming Conventions (cont.)

- **Category**: Corresponds to the concern areas for the prevailing platforms (examples: DiskExchange, SQL, Event log, CPU, Jobs, Subsystems, Services, Security)
- **Time interval:** The time interval used by the search or on which the search runs, if it is a scheduled search (examples: 24h, 7d, 3m, etc.)
- **Description:** A meaningful description of the context and intent of the search, limited to one or two words if possible. Ensures the search name is unique. (examples: Failed_Passwords, Failed_Batch, Top_src_ip)

Examples:

- SEG_Alert_Windows_Eventlog_15m_Failures
- SEG_Report_iSeries_Jobs_12hr_Failed_Batch
- NOC_Summary_Network_Security_24hr_Top_src_ip

Note

For more information go to: http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjecttitles

Reviewing Permissions

	Description	Create	Read	Edit (write)
Private	Only the person who created the object can use it and edit it	User Power Admin	Person who created it Admin	Person who created it Admin
Shared in App	Object persists in the context of a specific app	Power Admin	User* Power* Admin	User* Power* Admin
Global	Object persists globally across all apps	Admin	User* Power* Admin	User* Power* Admin

* Permission to read and/or write if creator gives permission to that role

By default, **Shared in App** and **Global** gives everyone read permission – write permission is reserved for admin and object creator unless creator edits permissions

Module 2:
Creating Lookups

Module Objectives

- Describe lookups
- Examine a lookup file example
- Create a lookup file and definition
- Configure an automatic lookup
- Use the lookup in searches

Describing Lookups

- There are use cases where static or relatively unchanging data is required for searches, but is not available in the index
- For example, from an RFID in a badge reader event, you can look up employee information

Scenario

Display badge-ins during the last 4 hours with user name and department.

```
sourcetype=history_access
| table Address_Description, rfid,
  Username, Department
```

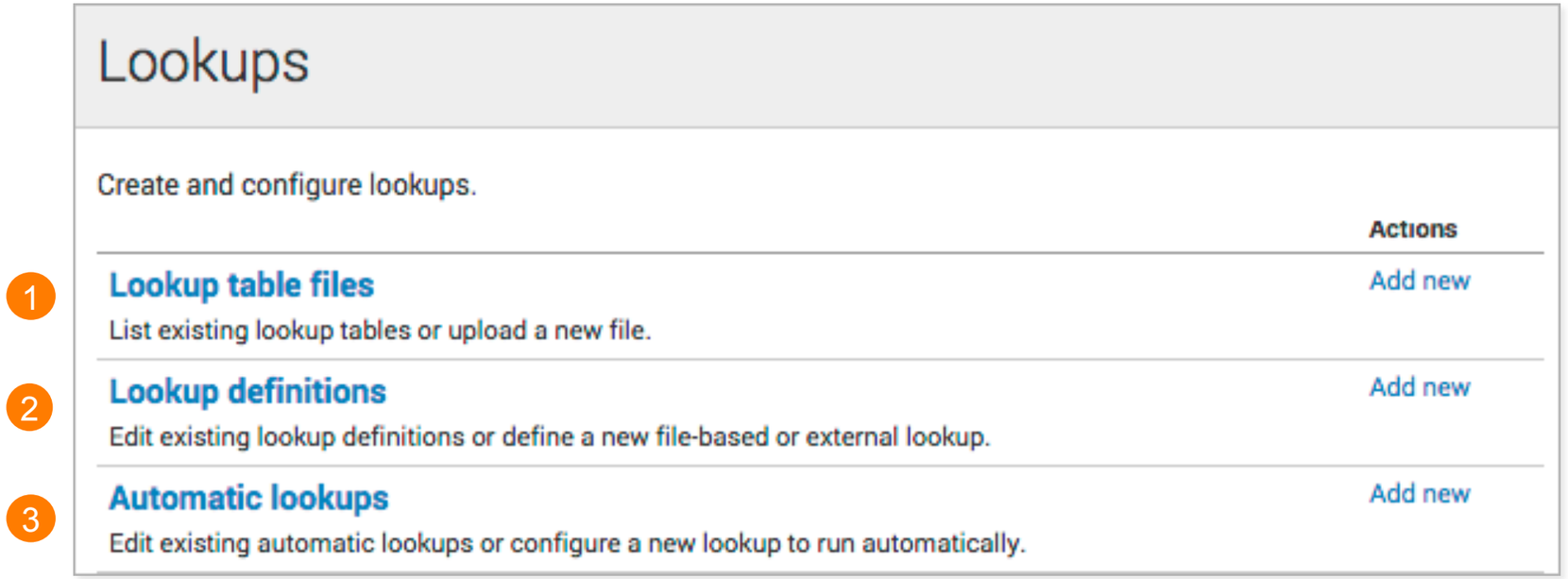
Address_Description	rfid	Username	Department
London	632071692298	yowen	Sales
London	963871339460	rjayaraman	Engineering
London	145297537706	npearce	SecOps
London	145297537706	npearce	SecOps
London	145297537706	npearce	SecOps
San Francisco	569361105570	kpercy	Compliance Officer
Boston	374765319282	emaxwell	ITOps
Boston	108423575302	apucci	Sales
Boston	108423575302	apucci	Sales

Describing Lookups (cont.)

- Lookups allow you to add more fields to your events:
  - Provide descriptions for http status codes (“file not found”, “service unavailable”)
  - Define sale prices for products
  - Associate RFIDs with user names, IP addresses, and workstation IDs
- Lookups can be defined in a static .csv file or it can be the output of a Python script
- After a field lookup is configured, you can use the lookup fields in searches
- The lookup fields also appear in the Fields sidebar
- Lookup field values are case-sensitive by default
  - Admins can change the `case_sensitive_match` option to `false` in transforms.conf
- Manage lookups from **Settings > Lookups**

Defining a File-based Lookup

1. Upload the file required for the lookup
2. Define the lookup type
3. Optionally, configure the lookup to run automatically



Lookup File – Example

- This example displays a lookup `.csv` file used to associate product information with productId
- First row represents field names (header)

```
productId, product_name, categoryId, price, sale_price, Code
```

- The `productId` field exists in the `access_combined` events
  - This is the **input** field
- All of the fields listed above are available to search after the lookup is defined
  - These are the **output** fields

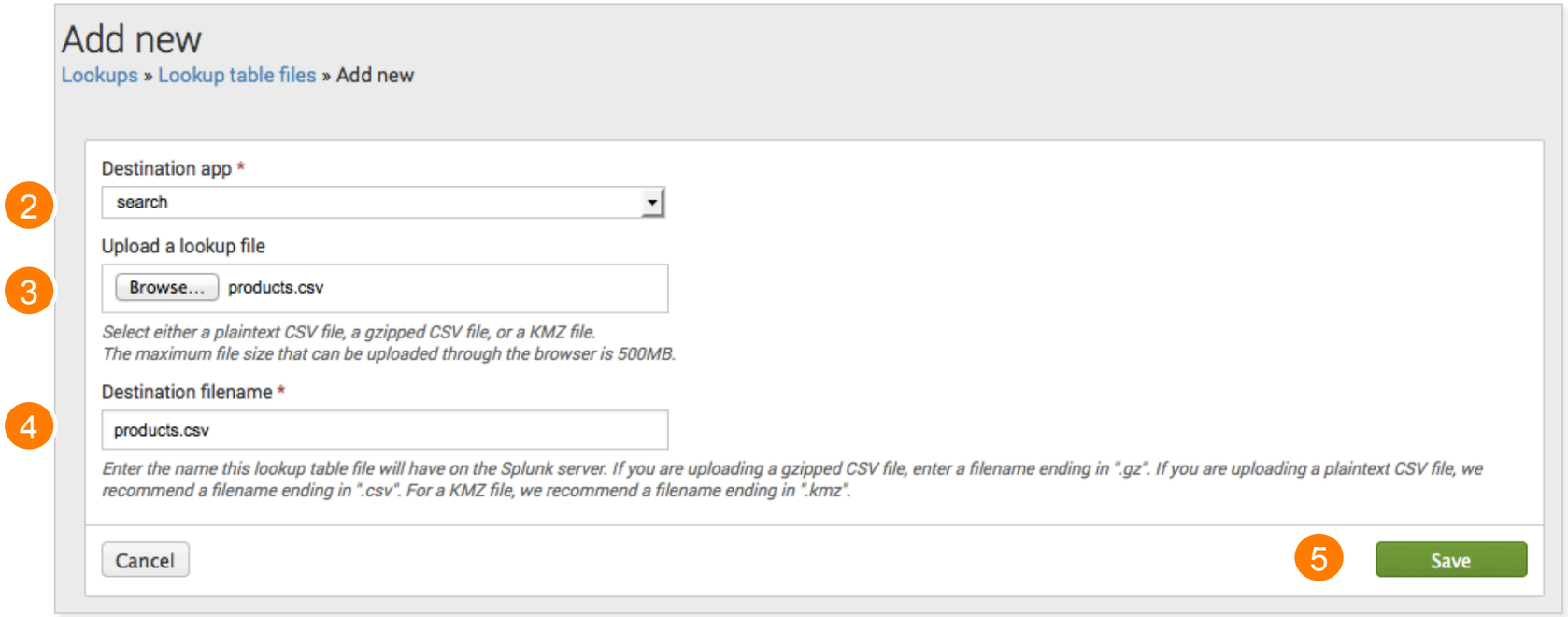
```
 GNU nano 2.3.1                File: products.csv

productId,product_name,categoryId,price,sale_price,Code
DB-SG-G01,Mediocre Kingdoms,STRATEGY,24.99,19.99,A
DC-SG-G02,Dream Crusher,STRATEGY,39.99,24.99,B
FS-SG-G03,Final Sequel,STRATEGY,24.99,16.99,C
WC-SH-G04,World of Cheese,SHOOTER,24.99,19.99,D
WC-SH-T02,World of Cheese Tee,TEE,9.99,6.99,E
PZ-SG-G05,Puppies vs. Zombies,STRATEGY,4.99,1.99,F
CU-PG-G06,Curling 2014,SPORTS,19.99,16.99,G
MB-AG-G07,Manganiello Bros.,ARCADE,39.99,24.99,H
MB-AG-T01,Manganiello Bros. Tee,TEE,9.99,6.99,I
FI-AG-G08,Orvil the Wolverine,ARCADE,39.99,24.99,J
BS-AG-G09,Benign Space Debris,ARCADE,24.99,19.99,K
SC-MG-G10,SIM Cubicle,SIMULATION,19.99,16.99,L
WC-SH-A01,Holy Blade of Gouda,ACCESSORIES,5.99,2.99,M
WC-SH-A02,Fire Resistance Suit of Provolone,ACCESSORIES,3.99,1.99,N
```

Creating a Lookup Table

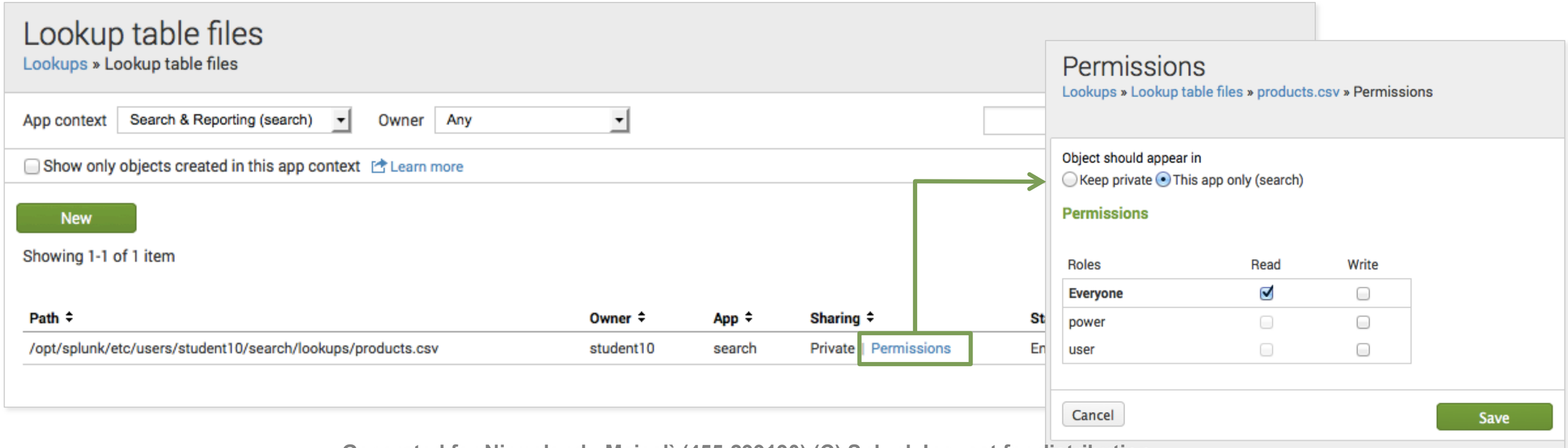
Settings > Lookups > Lookup table files

1. Click **New**
2. Select a destination app
3. Browse and select the `.csv` file to use for the lookup table
4. Enter a name for the lookup file
5. Save



Changing Permissions – Lookup File

- By default, lookup tables are created as Private
- To allow others to use the lookup table, the permissions must be changed



inputlookup Command

- Use the `inputlookup` command to load the results from a specified static lookup
- Useful to:
  - Review the data in the .csv file
  - Validate the lookup

Note

When using the inputlookup command, you can specify the filename ending with .csv or the lookup definition name

```
|inputlookup products.csv
```

All time

✓ 0 events (before 8/19/15 4:52:00.000 PM)

Job | Smart Mode

Events | Patterns | Statistics (14) | Visualization

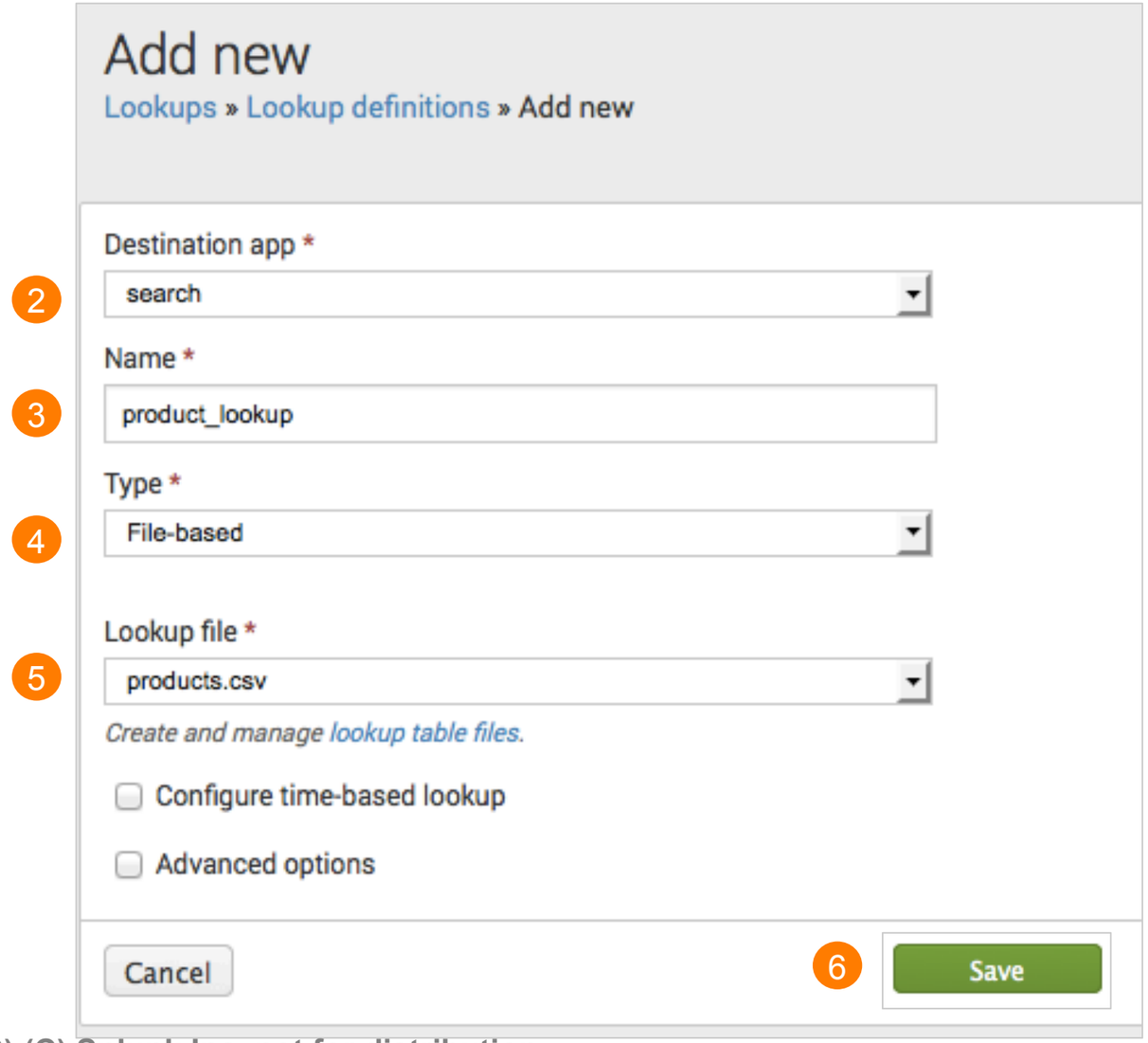
20 Per Page | Format | Preview

Code	categoryId	price	productId	product_name	sale_price
A	STRATEGY	24.99	DB-SG-G01	Mediocre Kingdoms	19.99
B	STRATEGY	39.99	DC-SG-G02	Dream Crusher	24.99
C	STRATEGY	24.99	FS-SG-G03	Final Sequel	16.99
D	SHOOTER	24.99	WC-SH-G04	World of Cheese	19.99
E	TEE	9.99	WC-SH-T02	World of Cheese Tee	6.99
F	STRATEGY	4.99	PZ-SG-G05	Puppies vs. Zombies	1.99
G	SPORTS	19.99	CU-PG-G06	Curling 2014	16.99
H	ARCADE	39.99	MB-AG-G07	Manganiello Bros.	24.99
I	TEE	9.99	MB-AG-T01	Manganiello Bros. Tee	6.99
J	ARCADE	39.99	FI-AG-G08	Orvil the Wolverine	24.99
K	ARCADE	24.99	BS-AG-G09	Benign Space Debris	19.99
L	SIMULATION	19.99	SC-MG-G10	SIM Cubicle	16.99
M	ACCESSORIES	5.99	WC-SH-A01	Holy Blade of Gouda	2.99
N	ACCESSORIES	3.99	WC-SH-A02	Fire Resistance Suit of Provolone	1.99

Creating a Lookup Definition

Settings > Lookups > Lookup definitions

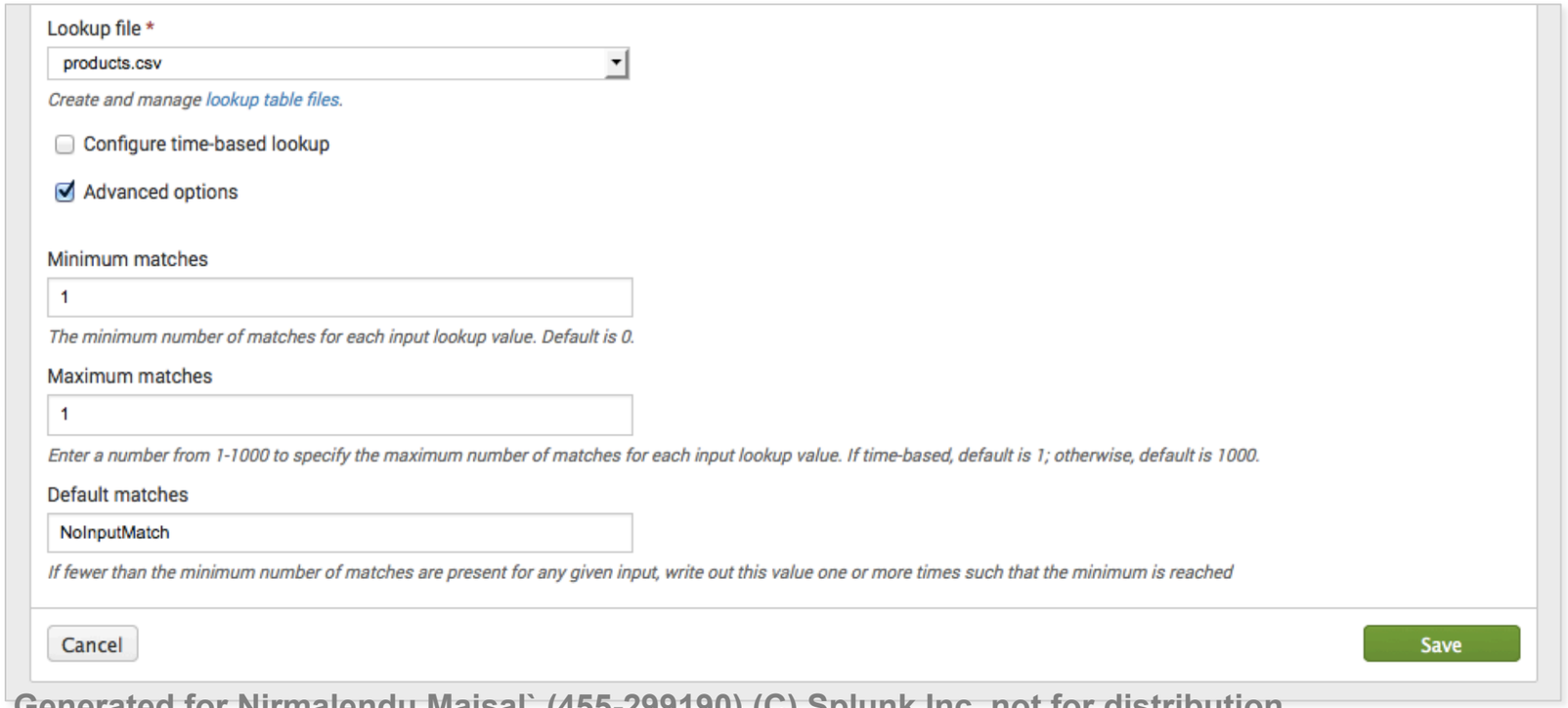
1. Click **New**
2. Select a destination app
3. Name the lookup definition
4. Select the lookup type, either File-based or External
5. From the drop-down, select a lookup file
6. Save



Advanced Options

Under Advanced options, you can specify:

1. Minimum number of matches for each input lookup value
2. Maximum number of matches for each input lookup value
3. Default value to output, if fewer than the minimum number of matches are present for a given input



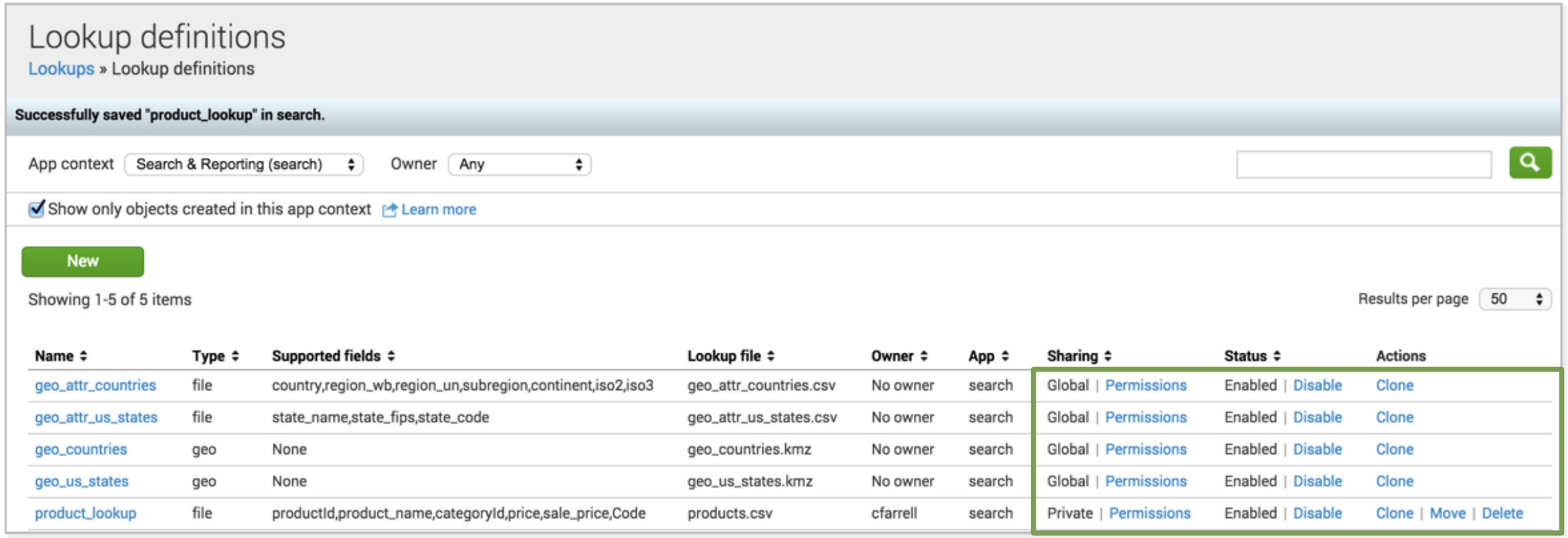
Managing Lookup Definitions

Based on your permissions, you can:

- Edit permissions
- Enable/disable
- Clone
- Delete
- Move

Note

Remember to set the permissions for the lookup definition appropriately.



lookup Command

- If a lookup is not configured to run automatically, use the lookup command in your search to use the lookup fields
- OUTPUT - If an OUTPUT clause is not specified, all fields in the lookup table that are not the match field are used as output fields

lookup Help More »
Explicitly invokes field value lookups.

Examples

There is a lookup table specified in a stanza name 'usertogroup' in transform.conf. This lookup table contains (at least) two fields, 'user' and 'group'. For each event, we look up the value of the field 'local_user' in the table and for any entries that matches, the value of the 'group' field in the lookup table will be written to the field 'user_group' in the event.

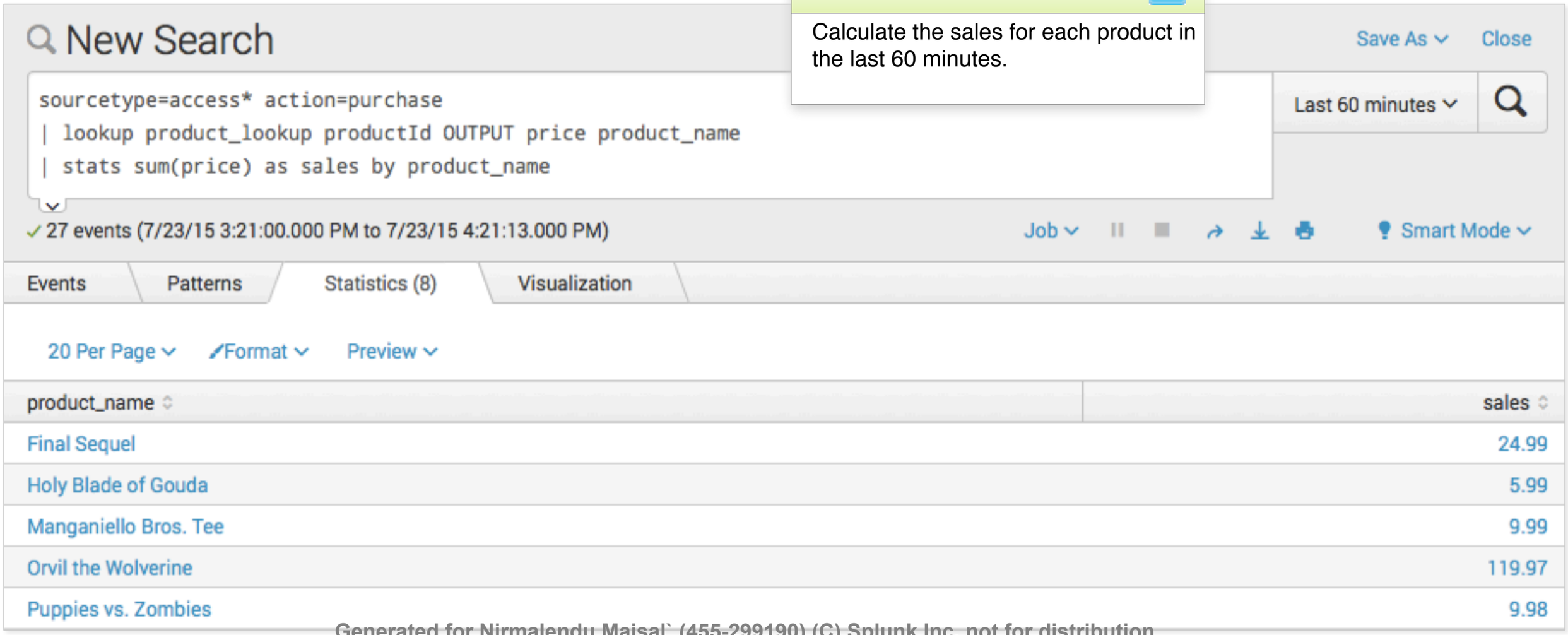
... | lookup usertogroup user as local_user OUTPUT group as user_group

- If OUTPUT is specified, the output lookup fields overwrite existing fields
- The output lookup fields exist only for the current search
- Use OUTPUTNEW when you do not want to overwrite existing fields

Using the lookup Command

Scenario

Calculate the sales for each product in the last 60 minutes.

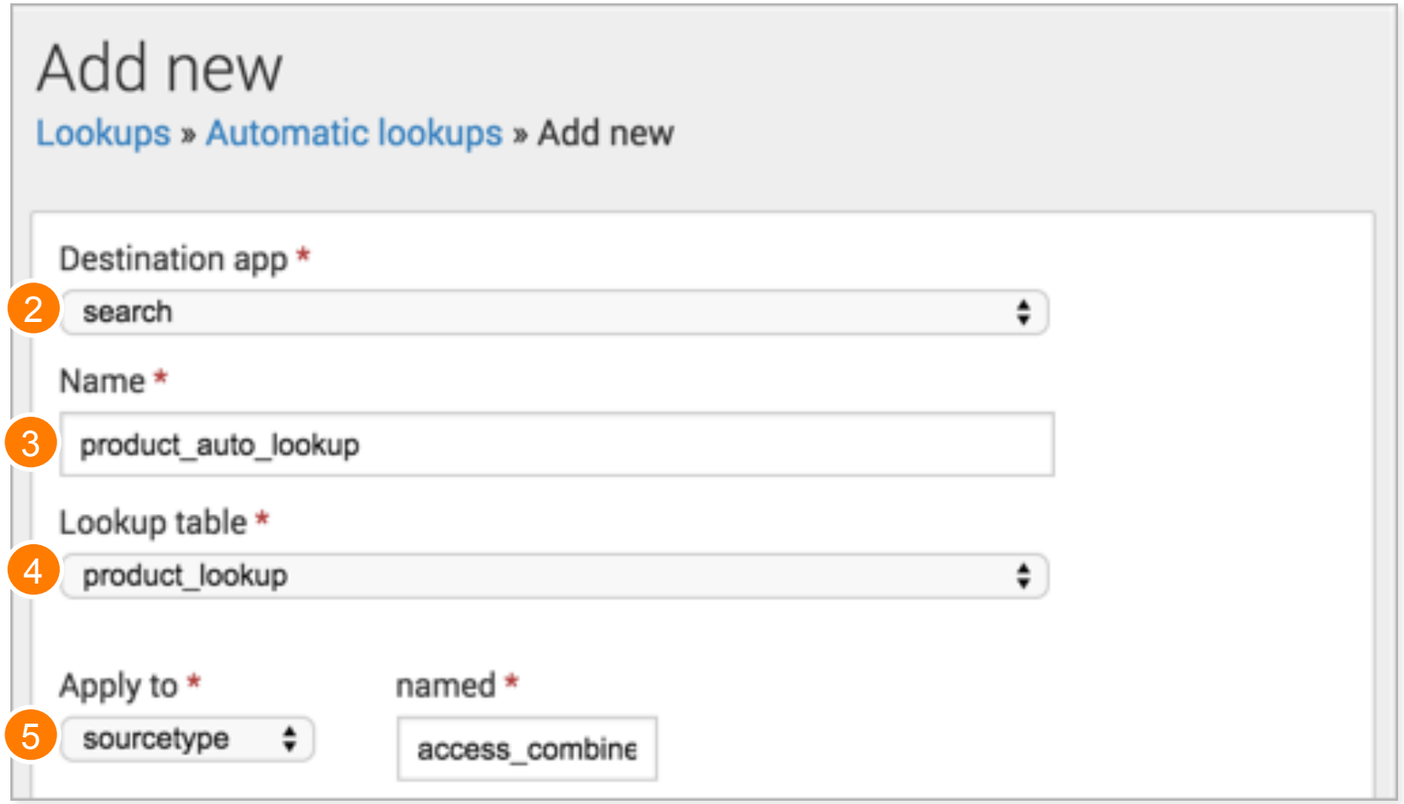


 | 18 April 2016

Creating an Automatic Lookup

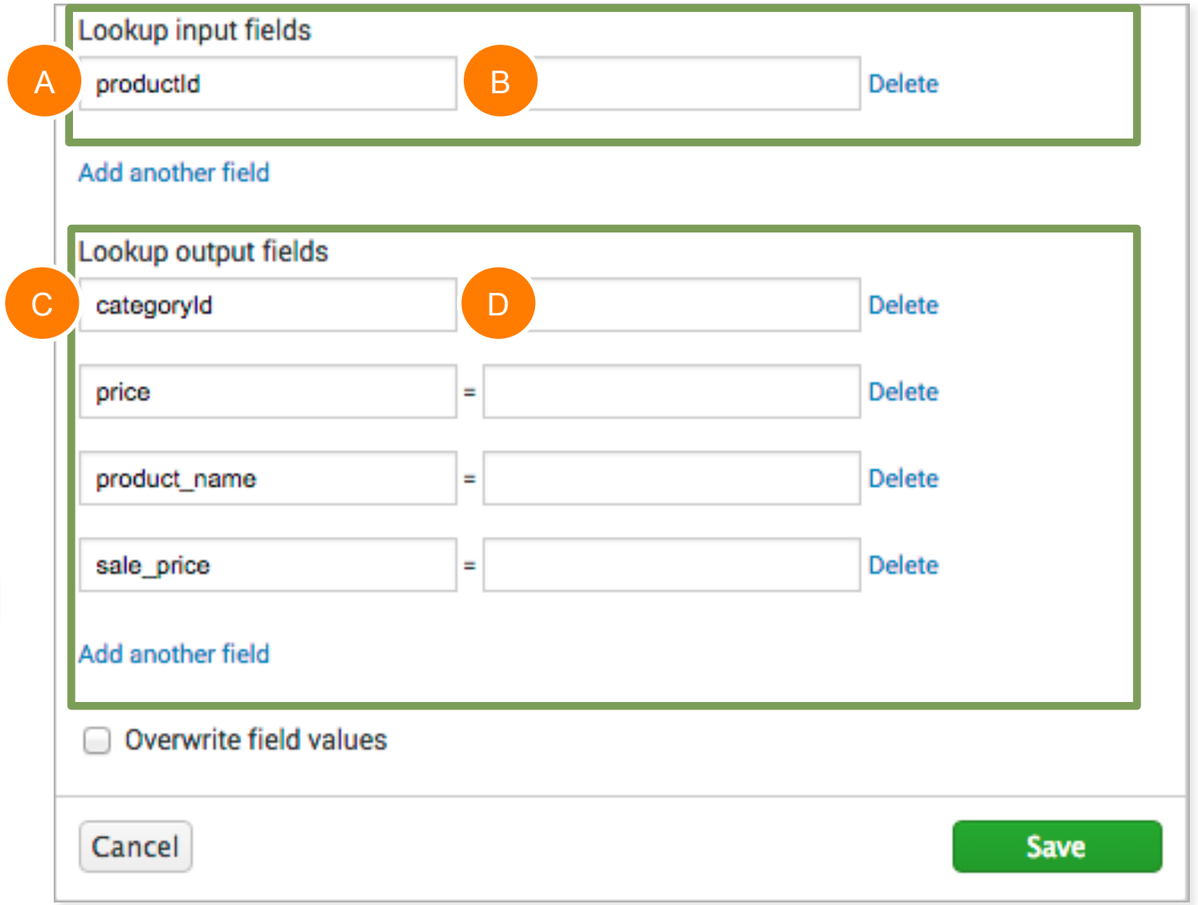
Settings > Lookups > Automatic lookups

1. Click **New**
2. Select the Destination app
3. Enter a Name for the lookup
4. Select the Lookup table definition
5. Select host, source, or sourcetype to apply the lookup and specify the name.



Creating an Automatic Lookup (cont.)

6. Define the Lookup input fields
   - Field(s) that exist in your events that you are relating to the lookup table
     A. Column name in CSV
     B. Field name in Splunk, if different from column name
7. Define the Lookup output fields
   - Field(s) from your lookup table that are added to the events
     C. Field name in lookup table
     D. Name you want displayed in Splunk, otherwise it inherits the column name
8. Save



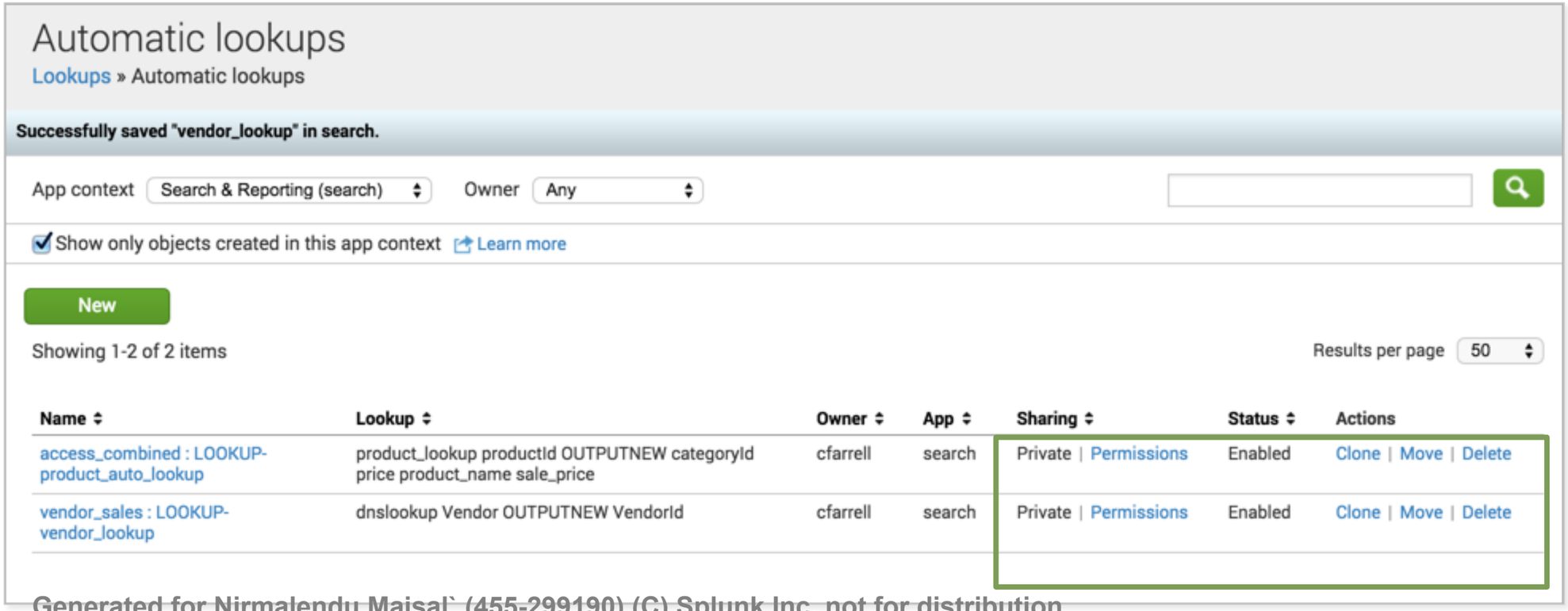
Managing Automatic Lookups

Based on your permissions, you can:

- Edit permissions
- Clone
- Delete
- Move

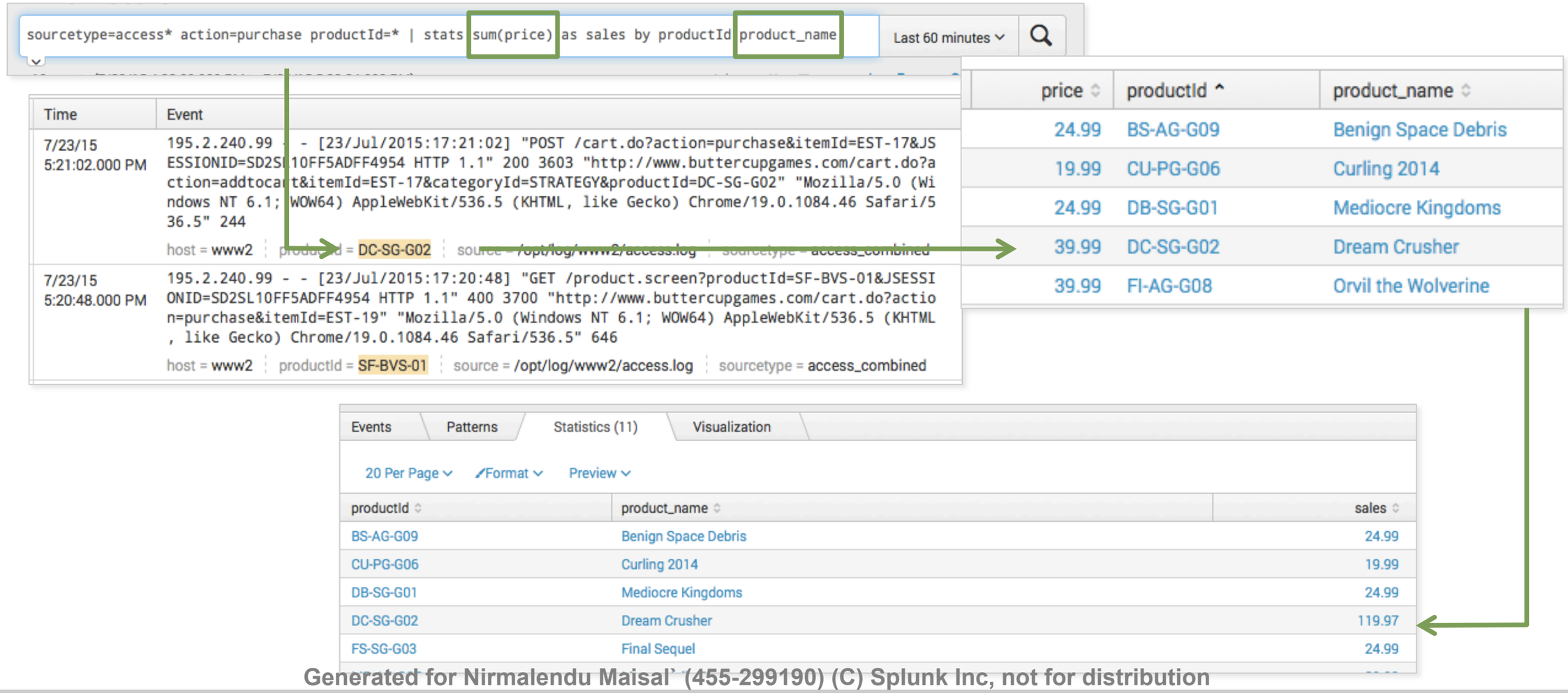
Note

Remember to set the permissions for the automatic lookup appropriately.



Using the Automatic Lookup

To use an automatic lookup, specify the output fields in your search



Describing Time-based Lookups

- If a field in the lookup table represents a timestamp, you can create a time-based lookup
- Example: use DHCP logs to identify users on your network based on their IP address and the timestamp
  - A script might copy DHCP log events to a .csv file when an ACK event occurs

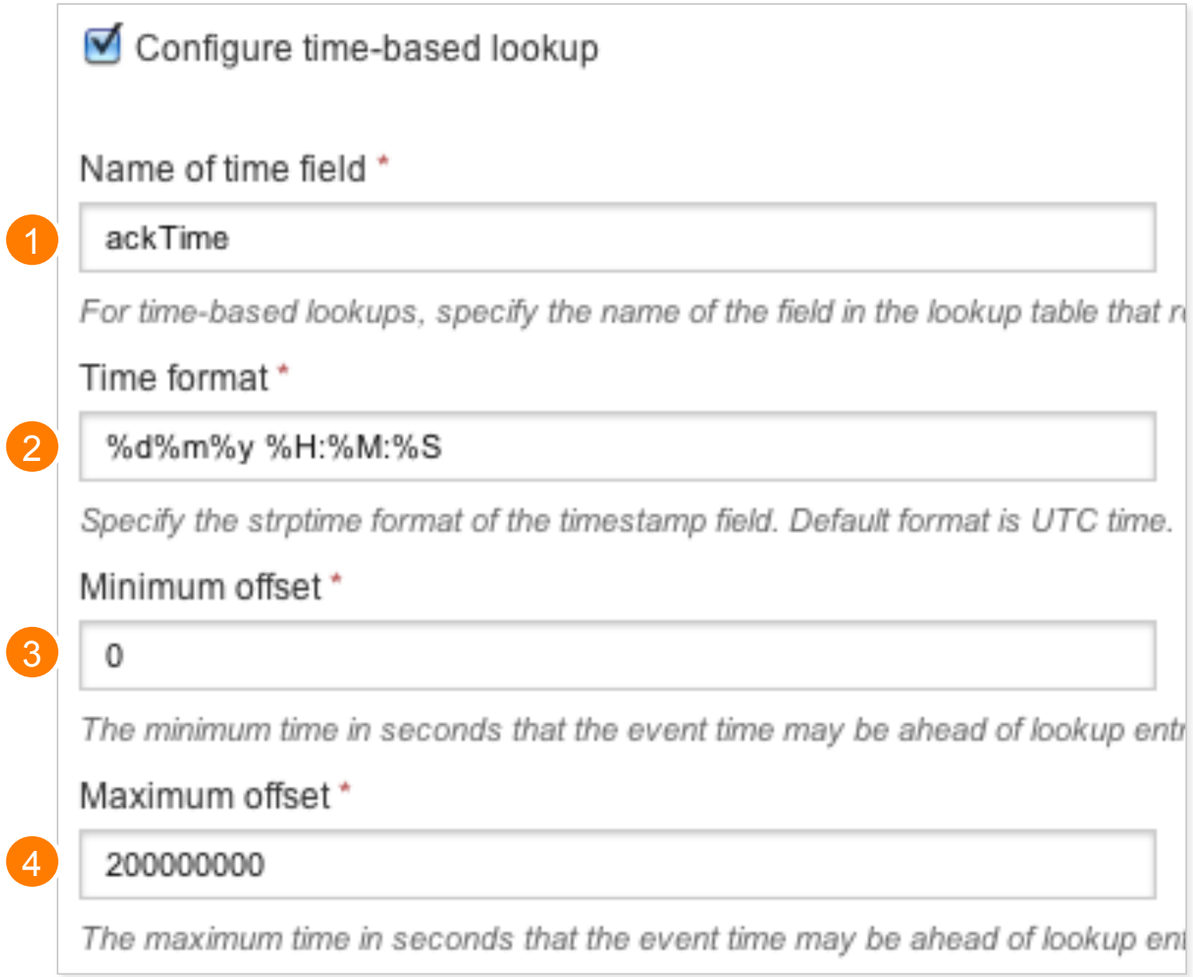
```
ACK:  1 110  08/06/14 11:40:06 171.64.20.120 00:0d:93:b1:9e:d6
```

  - .csv file contains the timestamp, IP address, username, and MAC address

```
ackTime,ip,user,macaddress
06AUG2014 11:40:06,171.64.20.120,bwilson,00:0d:93:b1:9e:d6
```

Configuring Time-based Lookups

1. Specify the name of the time field in the lookup
2. Enter the strptime format of the time field
3. Define the minimum offset in seconds
   - Default is 0
4. Define the maximum offset in seconds
   - There is no maximum offset by default



Note

The offset is the minimum and maximum amounts of time that an event may be later than a lookup entry.

Additional Lookup Options

In addition to creating and using a file-based lookup, you can also:

- Populate a lookup table with search results
  - `outputlookup` is discussed in the *Advanced Searching & Reporting* class
- Define a field lookup based on an external command; Python- and binary-based scripts
  - For more information, see the *Knowledge Manager Manual*
    docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addfieldsfromexternaldatasources
- Use the Splunk DB Connect app to create lookups with data from external SQL databases
- Populate events with fields from an App Key Value Store (KV Store) collection
  - KV Store lookups can only be invoked through REST endpoints or by using search commands such as lookup, inputlookup, and outputlookup, therefore cannot be set up as automatic
  - For more information, see the Knowledge Manager Manual
    docs.splunk.com/Documentation/Splunk/latest/Knowledge/ConfigureKVstorelookups

Module 3:
Creating Field Aliases and Calculated Fields

Module Objectives

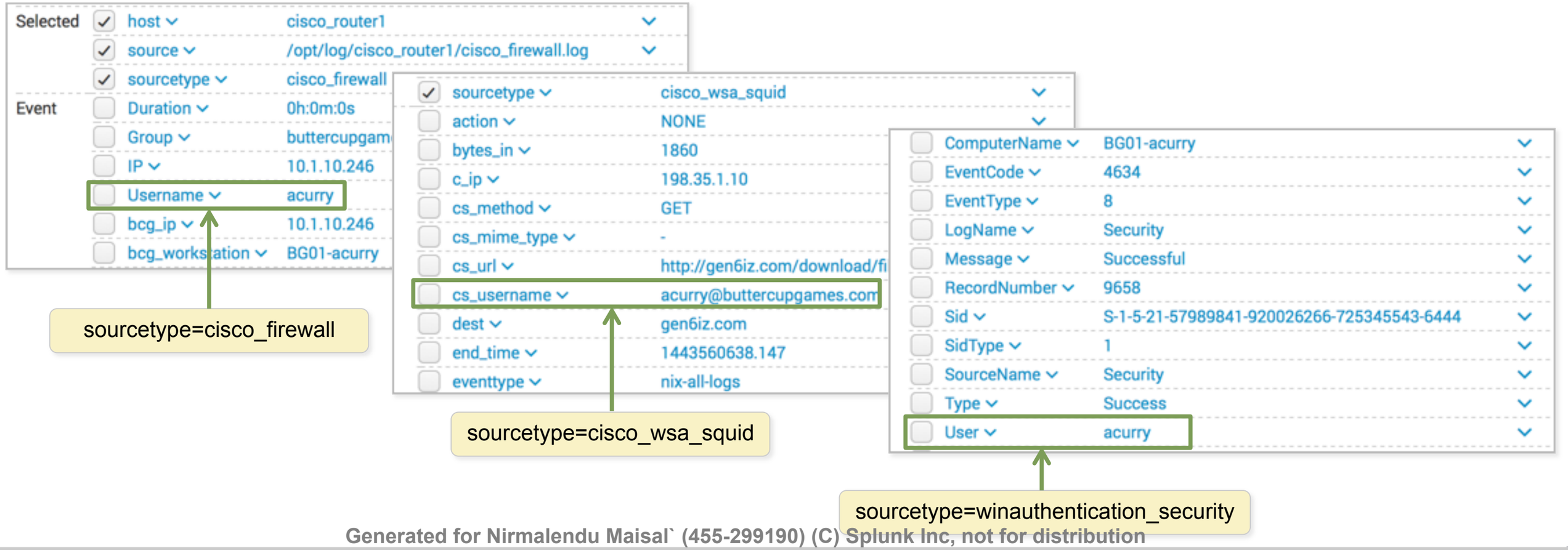
- Create and use field aliases
- Create calculated fields

Field Aliases

- A way to normalize data over several sources
- Multiple aliases can be applied to one field
- Applied after field extractions, before lookups
- Can apply field aliases to lookups

Field Alias Example

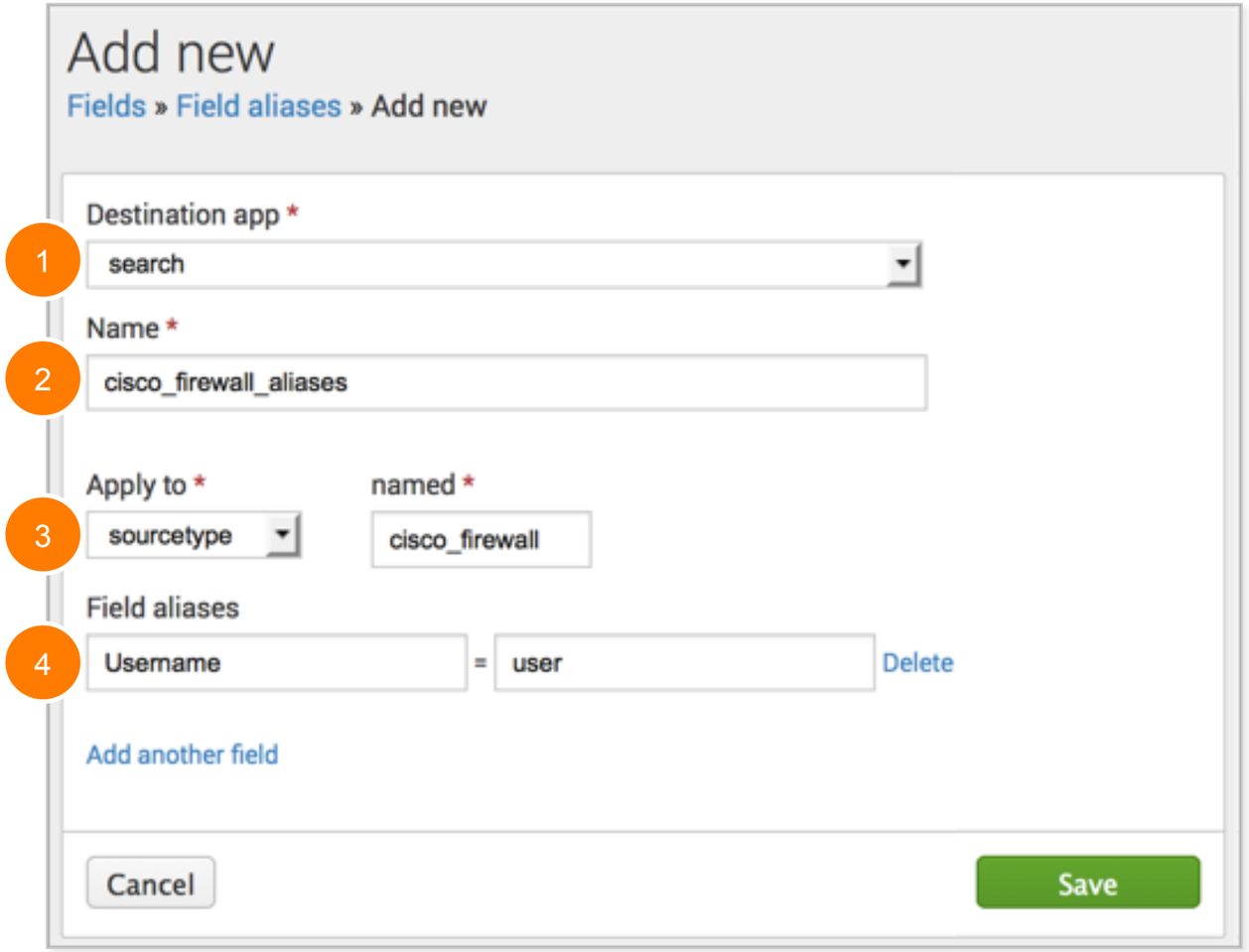
- Several source types contain some type of a username field
- To make data correlation and searching easier, normalize the username field



Creating a Field Alias

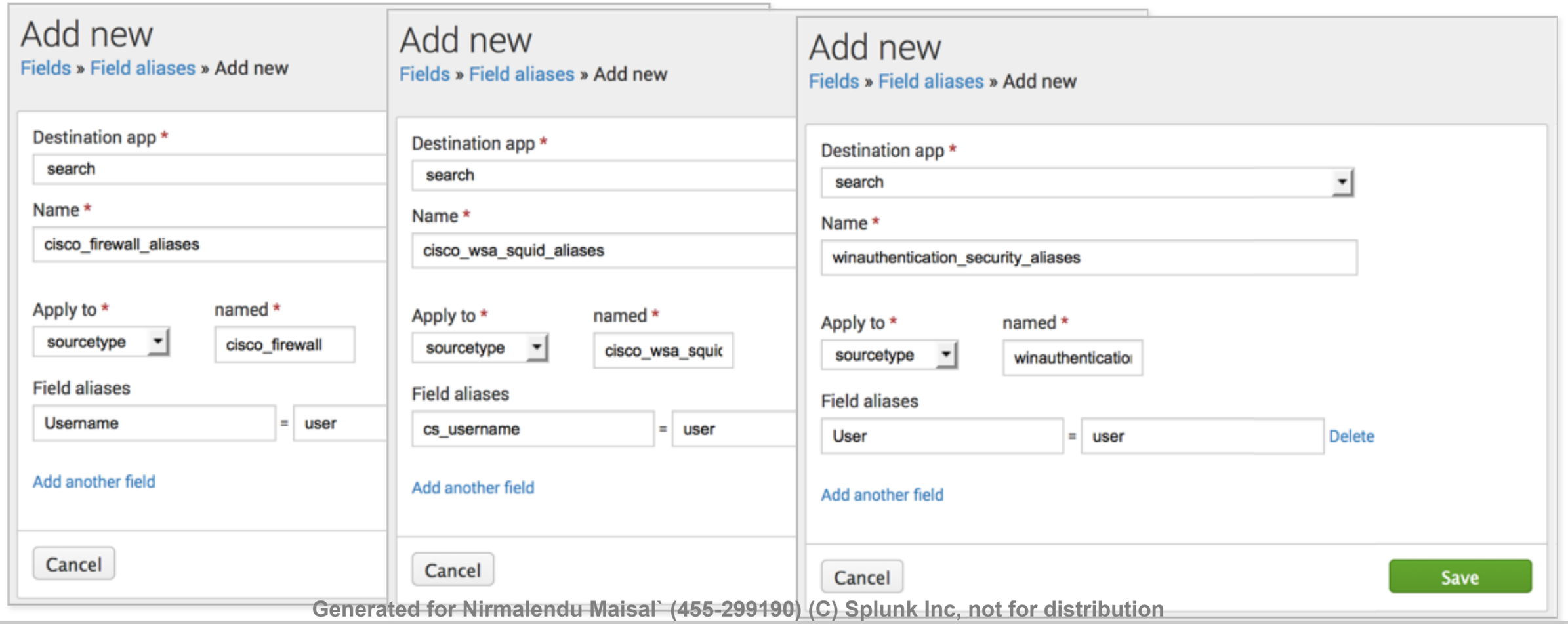
Settings > Fields > Field Aliases > New

1. Select the app associated with the field alias
2. Enter a Name for the field alias
3. Apply the field alias to a default field:
   - Host
   - Source
   - Sourcetype
4. Enter the name for the existing field and the new alias



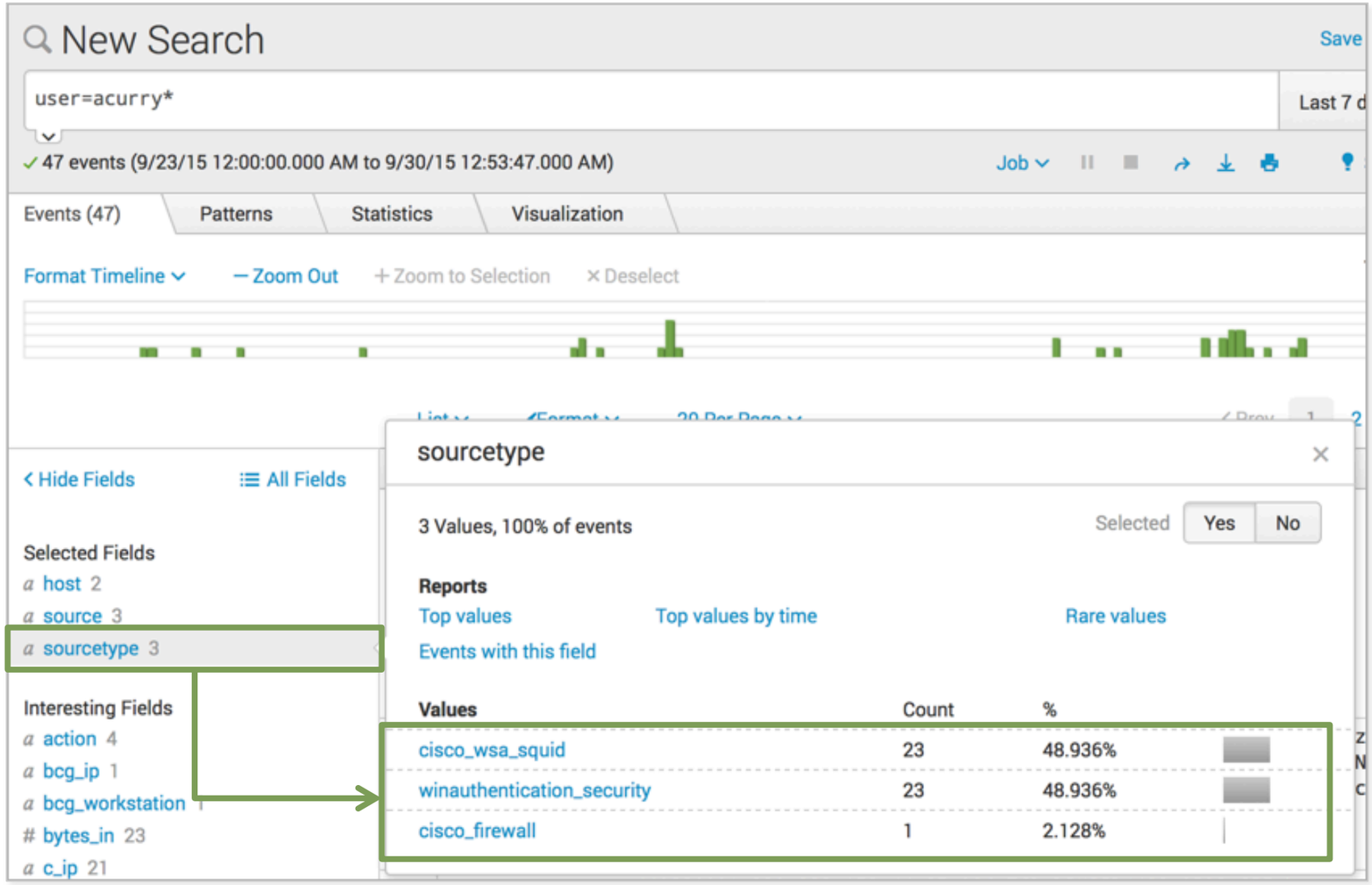
Creating a Field Alias (cont.)

In this example, one field alias will be used for the new ‘user’ field in multiple source types. A new field alias is required for each sourcetype:



Testing the Field Alias

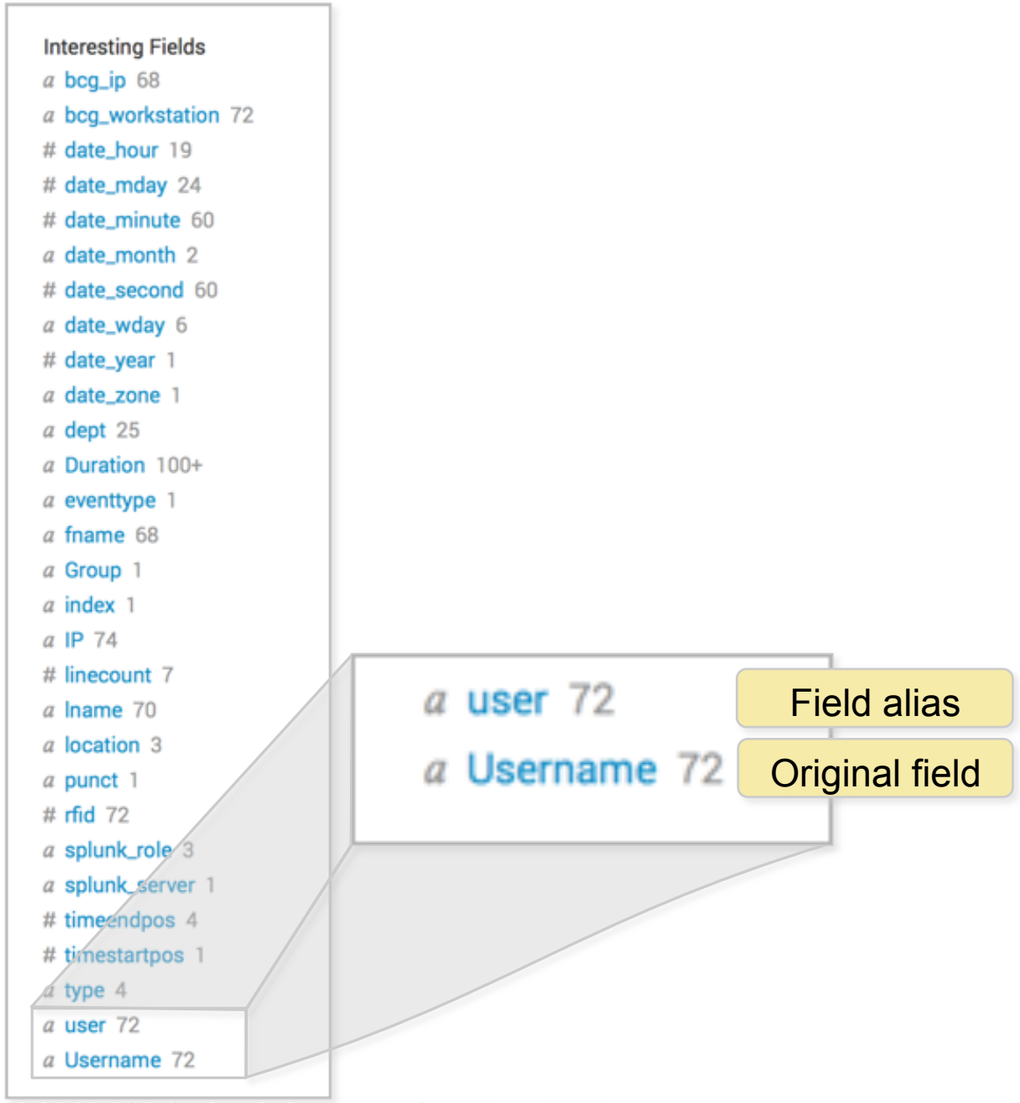
After the field alias has been created, perform a new search using the new field alias



Field Alias and Original Fields

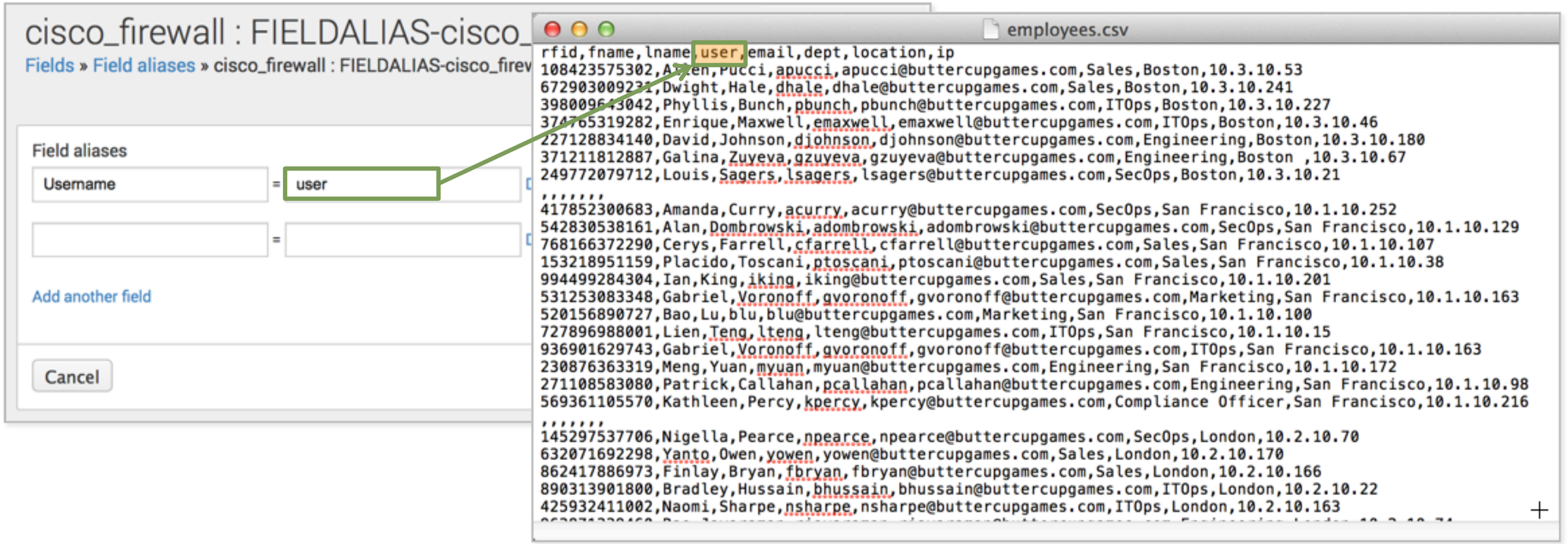
When you create a field alias, the original field is not affected.

Both fields will appear in the All Fields list and the Interesting Fields list, if it appears in at least 20% of events.



Field Aliases and Lookups

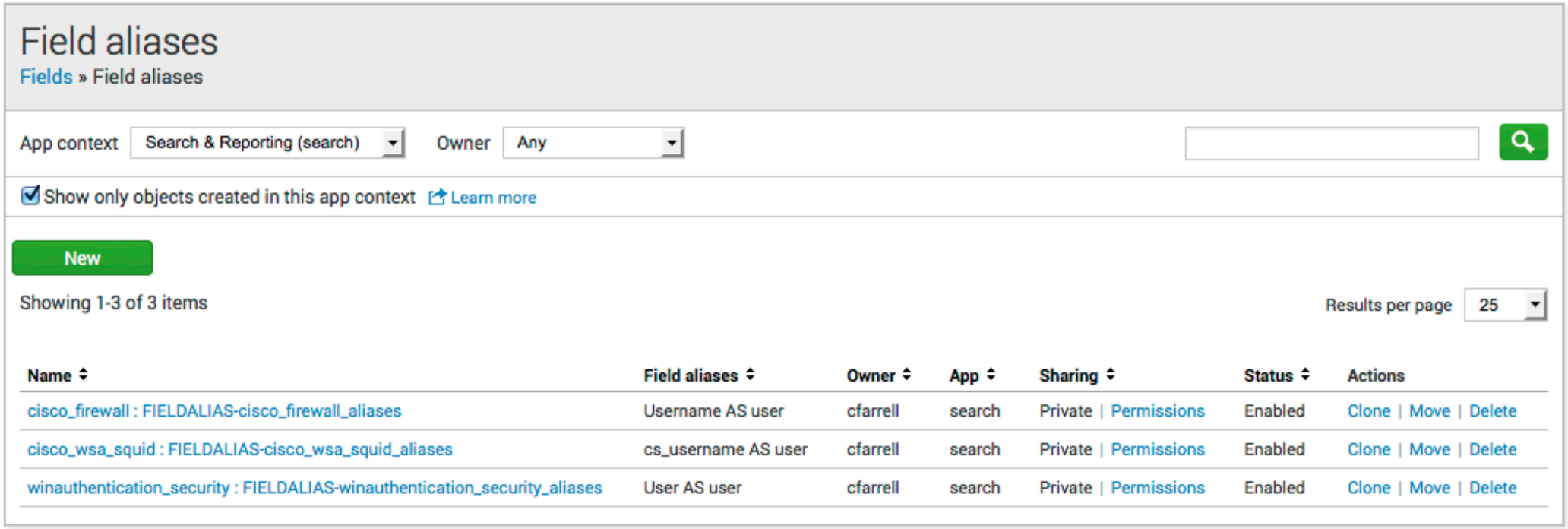
After you have defined your field aliases, you can create a lookup table to reference them



Managing Field Aliases

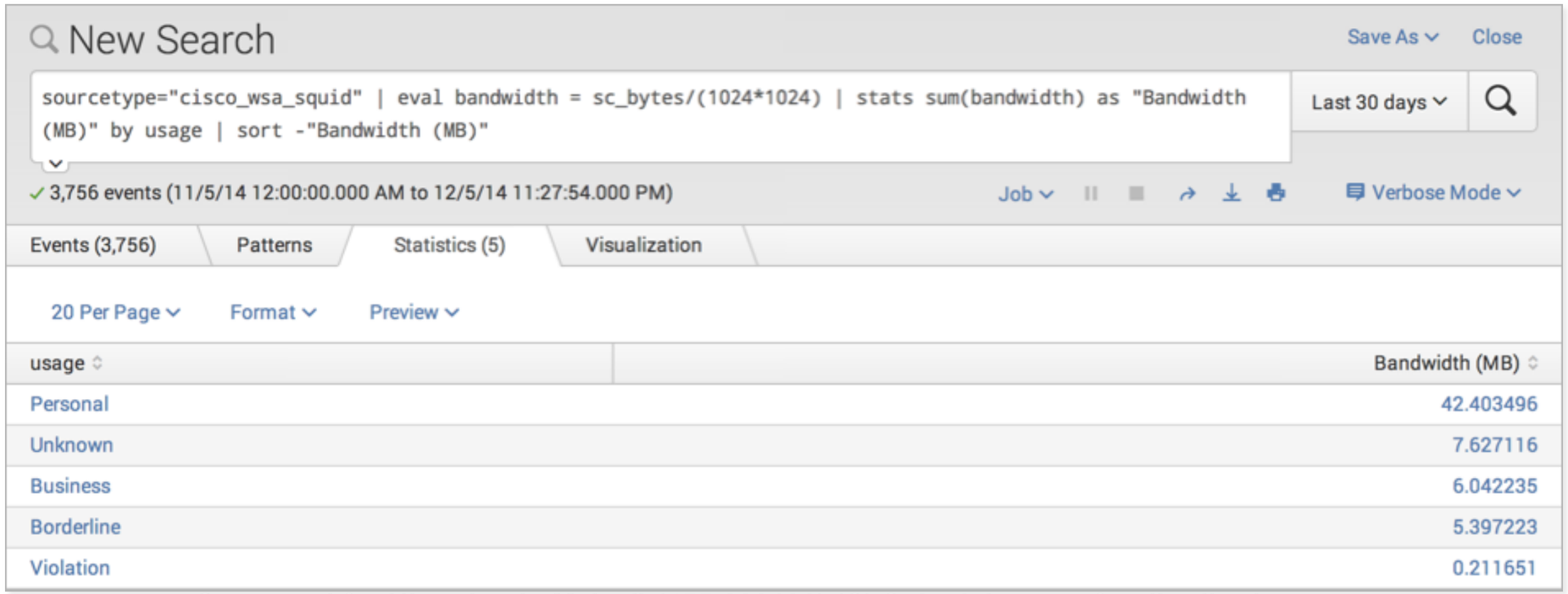
Settings > Fields > Field Aliases

- Edit permissions
- Clone
- Move
- Delete



What is a Calculated Field?

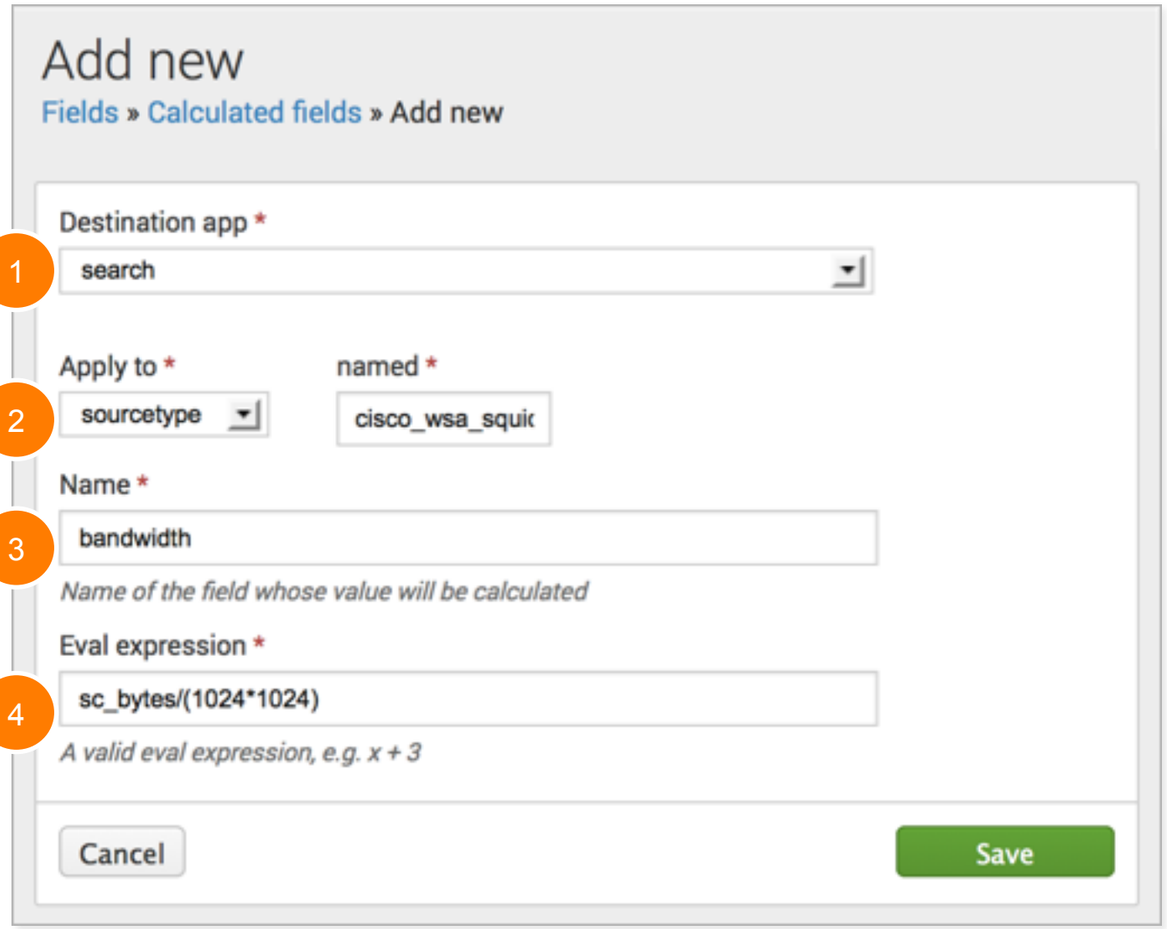
- Shortcut for performing repetitive, long, or complex transformations using the `eval` command
- Must be based on an extracted field
  - Output fields from a lookup table or fields/columns generated from within a search string are not supported



Creating a Calculated Field

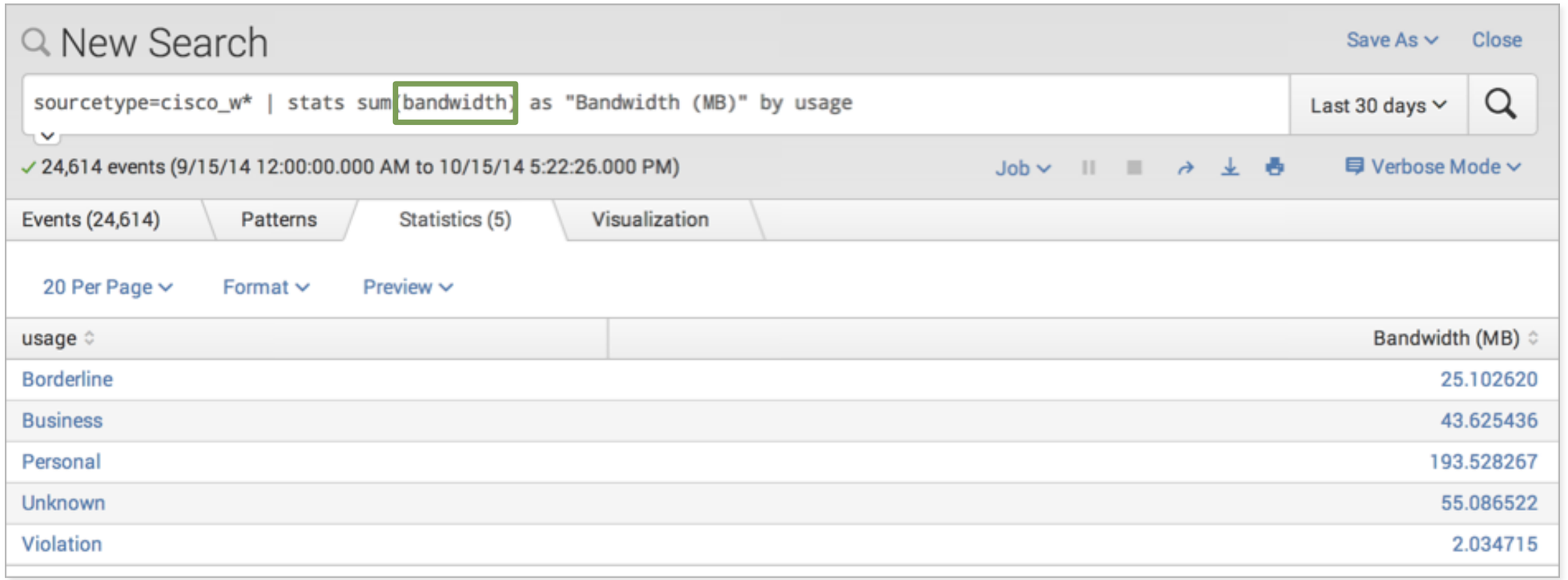
Settings > Fields > Calculated Fields > New

1. Select the app that will use the calculated field
2. Select host, source, or sourcetype to apply to the calculated field and specify the related name
3. Name the calculated field
4. Define the eval expression



Using a Calculated Field

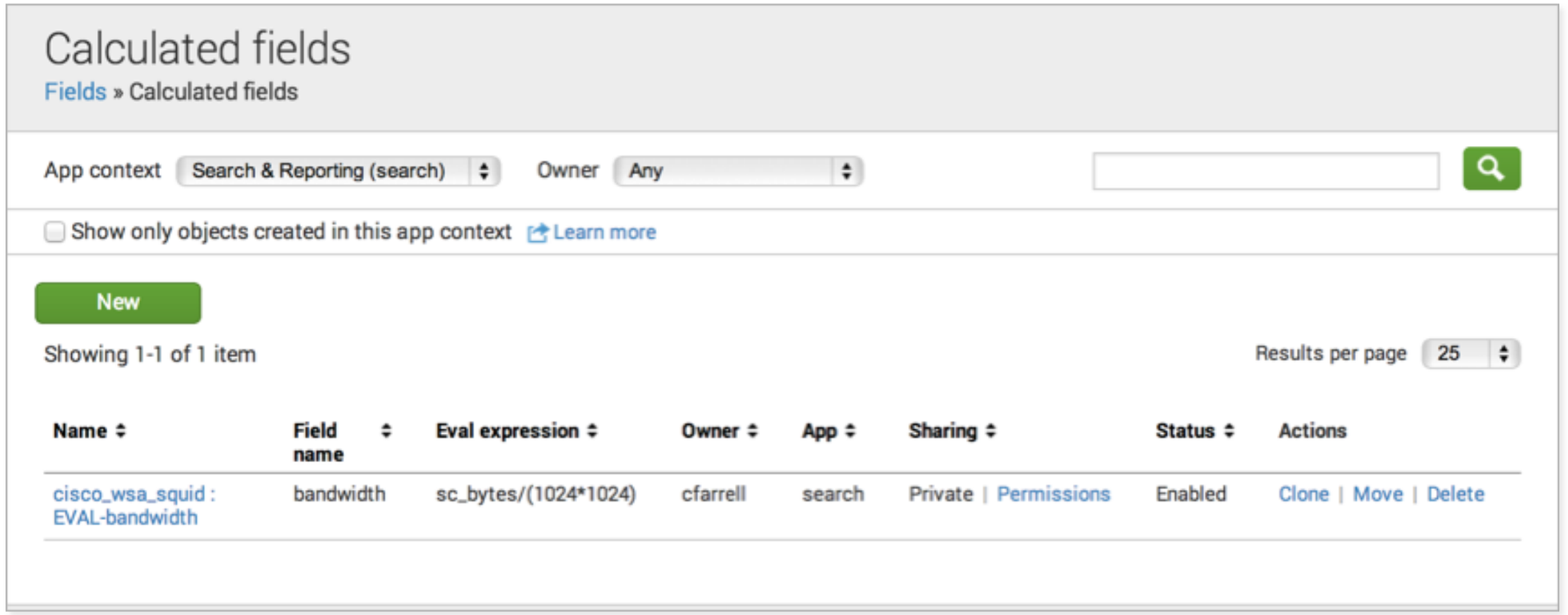
After you have created a calculated field, you can use it in a search like any other extracted field:



Managing Calculated Fields

Settings > Fields > Calculated Fields

- Edit permissions
- Clone
- Move
- Delete



Module 4:
Creating Field Extractions

Module Objectives

- Review the Field Extractor (FX) methods
  - Regex
  - Delimiter
- Identify the different options to extract fields using regex or delimiters (FX)
  - Settings
  - Fields sidebar
  - Event actions
- Review the process of extracting fields manually using regular expressions
- Use the Field Extraction Manager to modify extracted fields

Performing Field Extractions

- To extract fields that are static and often needed in searches, use FX
  - Graphical UI
  - Extract fields from events using regex or delimiter
  - Extracted fields persist as a knowledge object
  - Can be shared and re-used in multiple searches
- Access Field Extractor via Settings, Fields Sidebar, or Event Actions menu

Note

For more details, see:
http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/ExtractfieldsinteractivelywithIFX

Field Extraction Methods

You can use FX to perform the following field extractions:

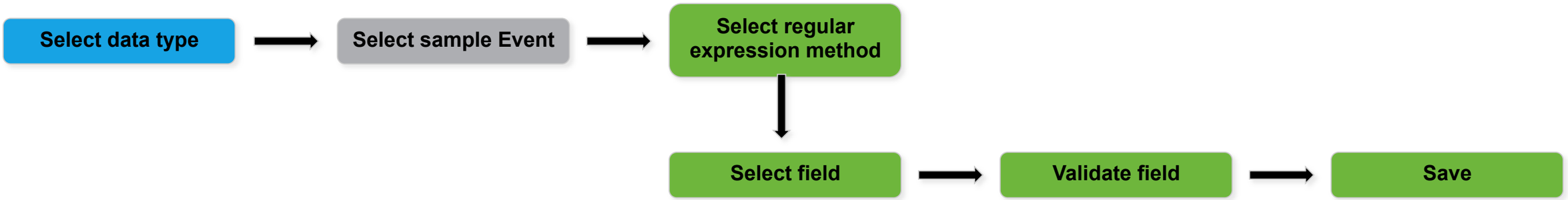
- **RegEx**
  - Use this option when your event contains unstructured data like a system log file. FX will attempt to extract the fields using a regular expression that matches similar events.
- **Delimiter**
  - Use this option when your event contains structured data like a .csv file. The data does not have headers and the fields may be separated by:
    - Space
    - Comma
    - Pipe
    - Tabs
    - Other characters

Note

For more details, see:
http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/ExtractfieldsinteractivelywithIFX

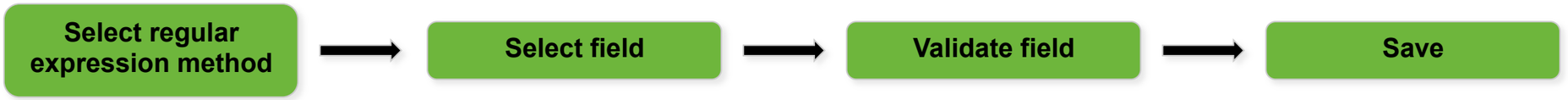
Field Extraction Workflow – Regular Expression

Settings



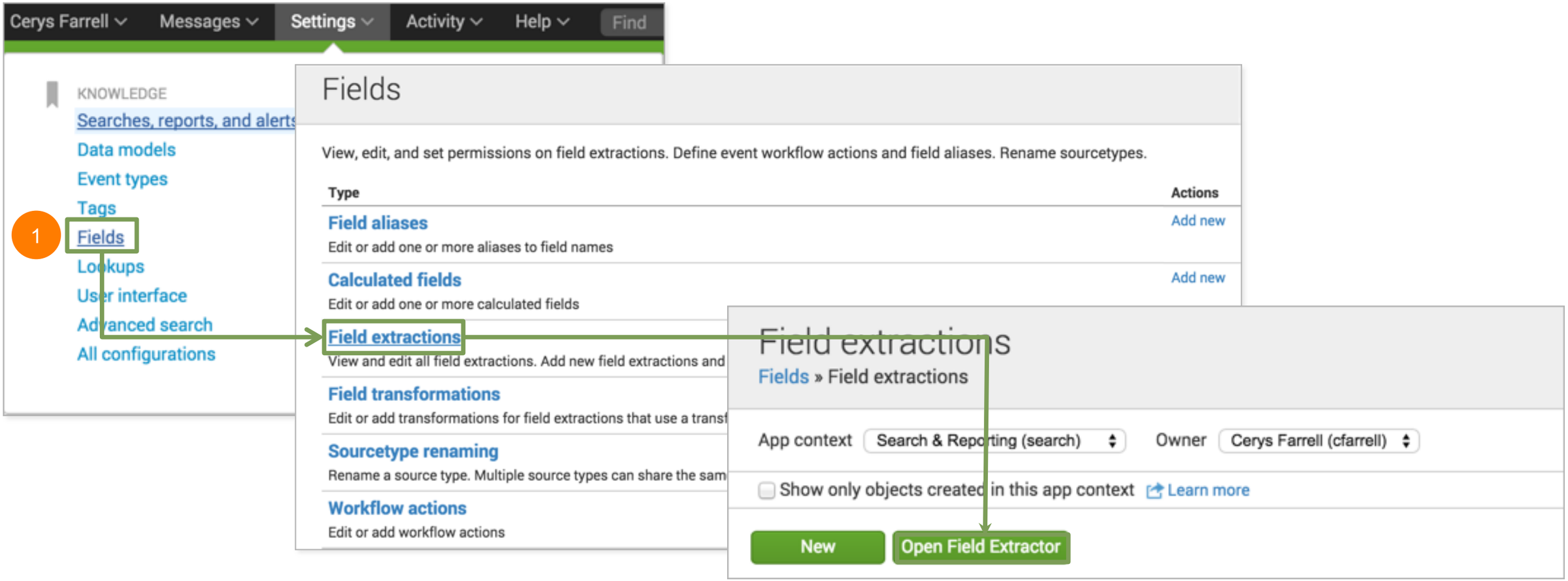
Fields Sidebar

Event Actions



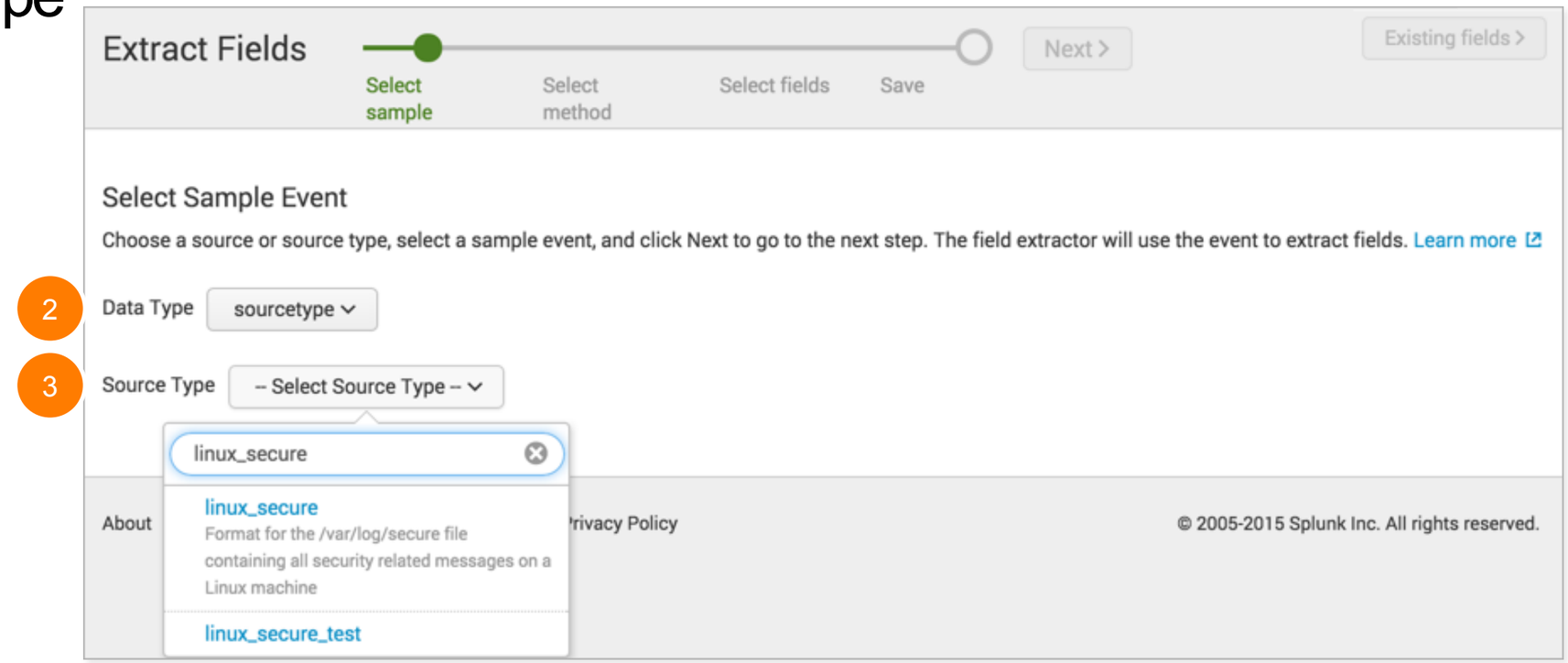
Regex Field Extractions from Settings

1. Settings > Fields > Field extractions > Open Field Extractor



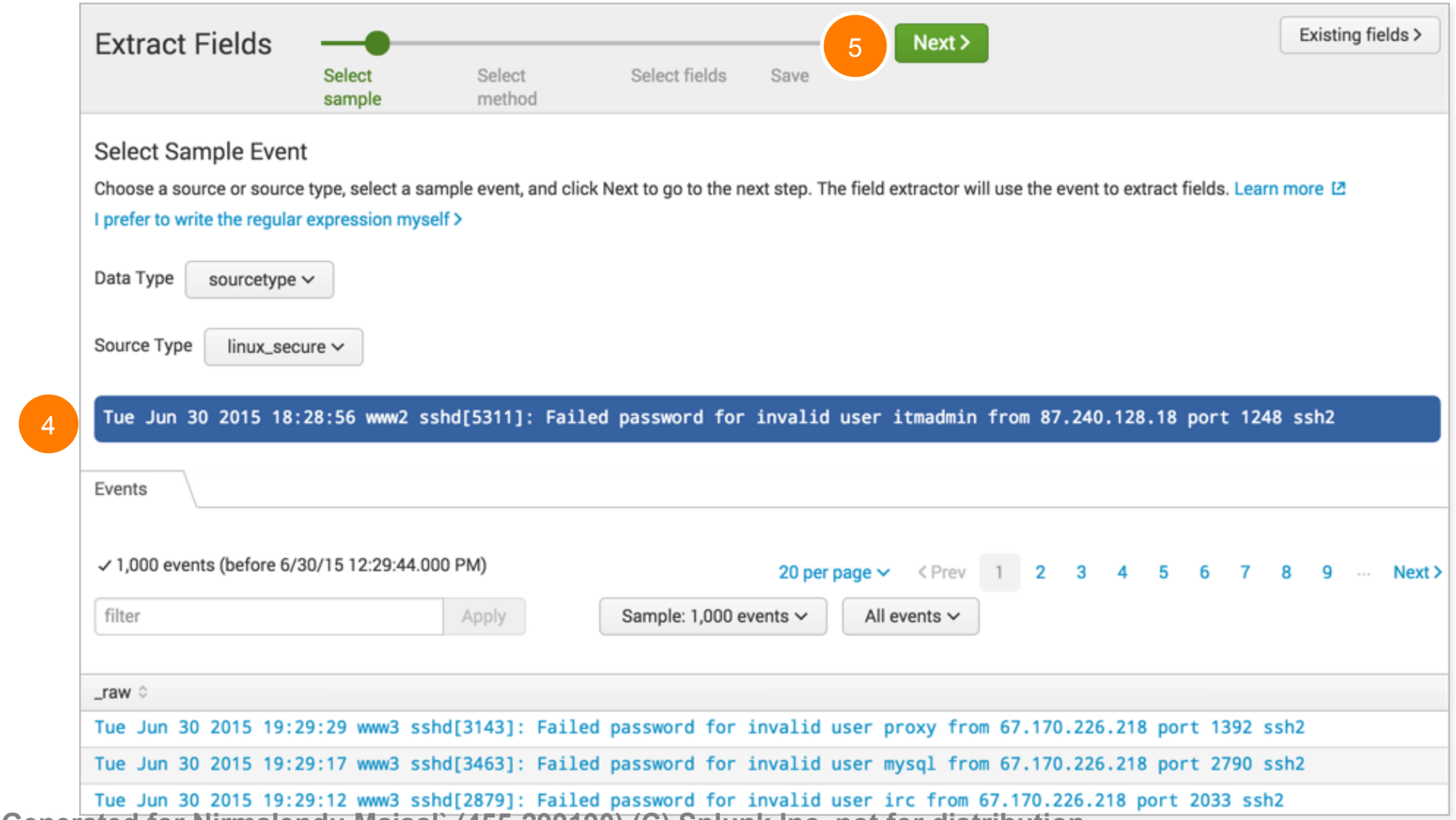
Regex Field Extractions from Settings (cont.)

2. Select the Data Type
   - sourcetype
   - source
3. Select the Source Type



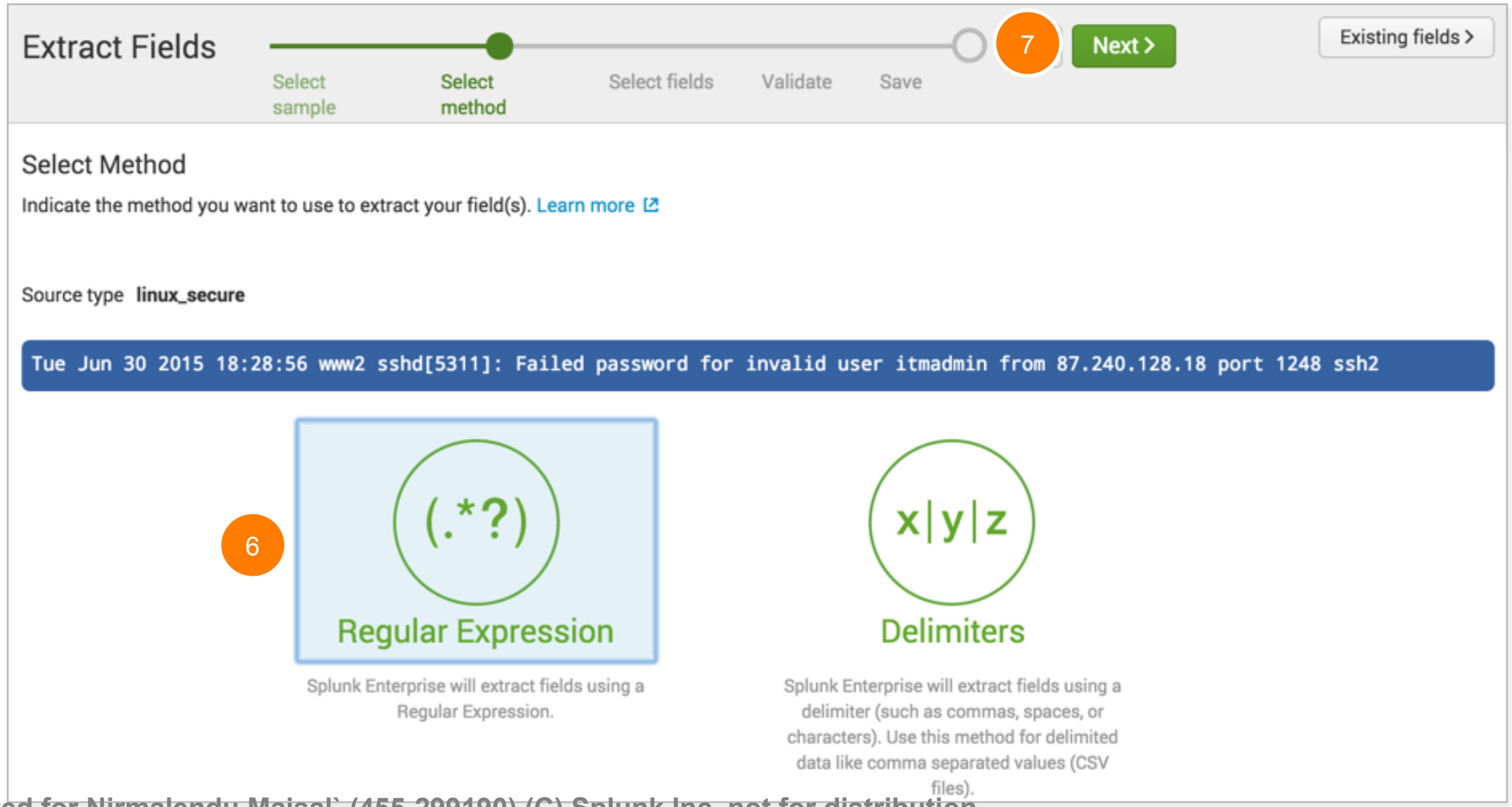
Regex Field Extractions from Settings –Select Sample

4. Select a sample event
5. Click **Next >**



Regex Field Extractions from Settings –Select Method

6. Select **Regular Expression**
7. Click **Next >**

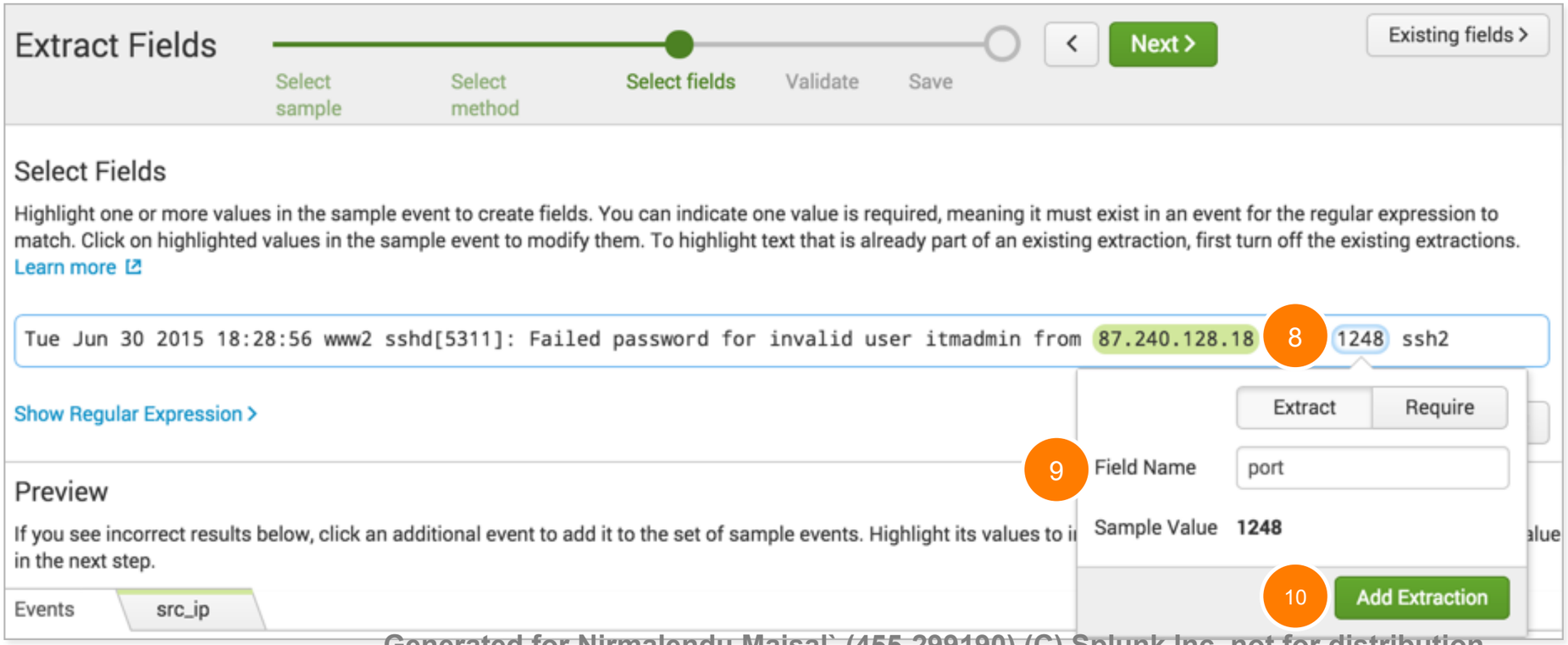


Regex Field Extractions from Settings –Select Values

8. Select the value(s) you want to extract. In this example, two fields are being extracted.
9. Provide a field name
10. Click **Add Extraction**

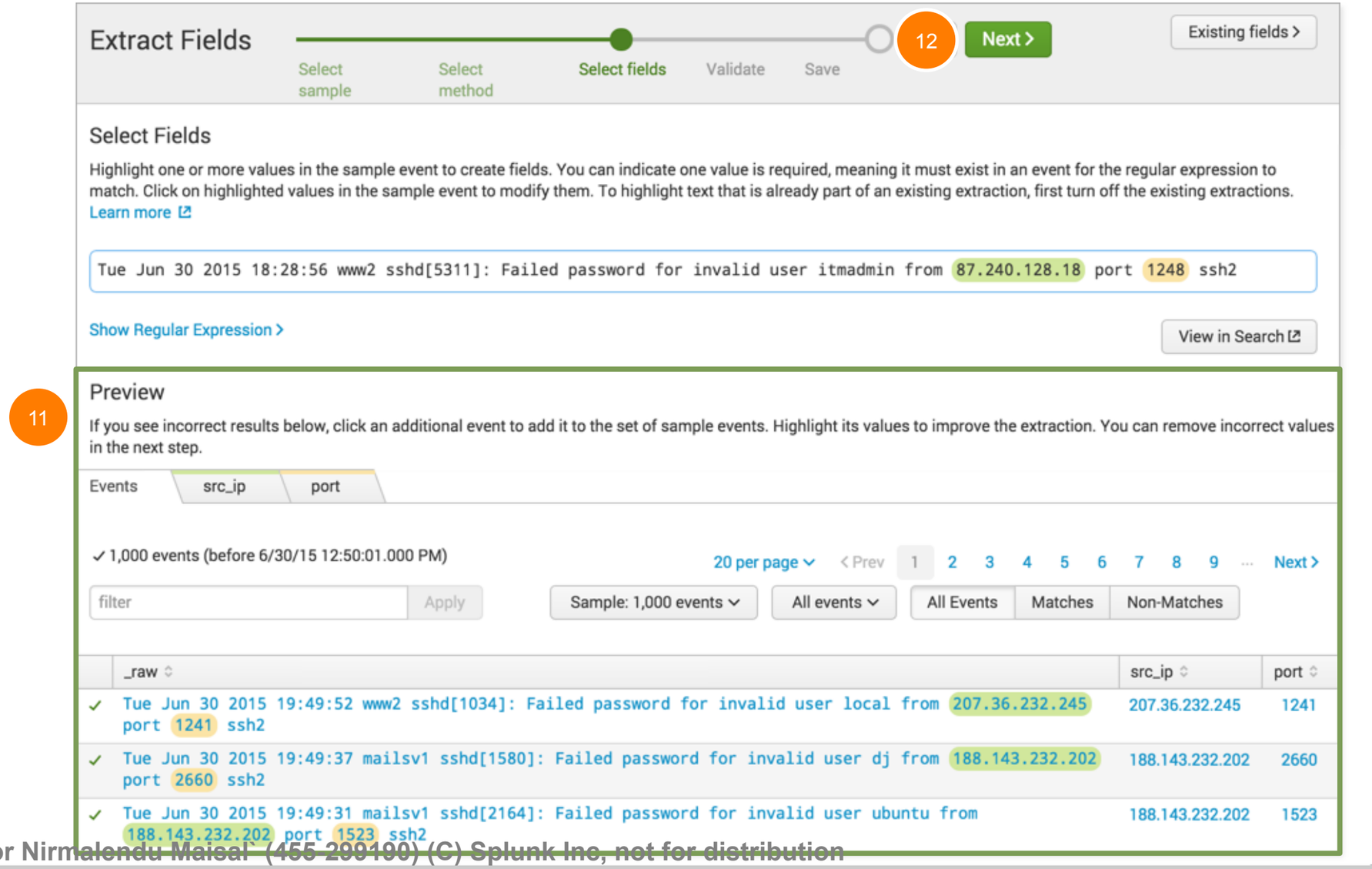
Note

Require option - only the events with that field name will appear in your search results.



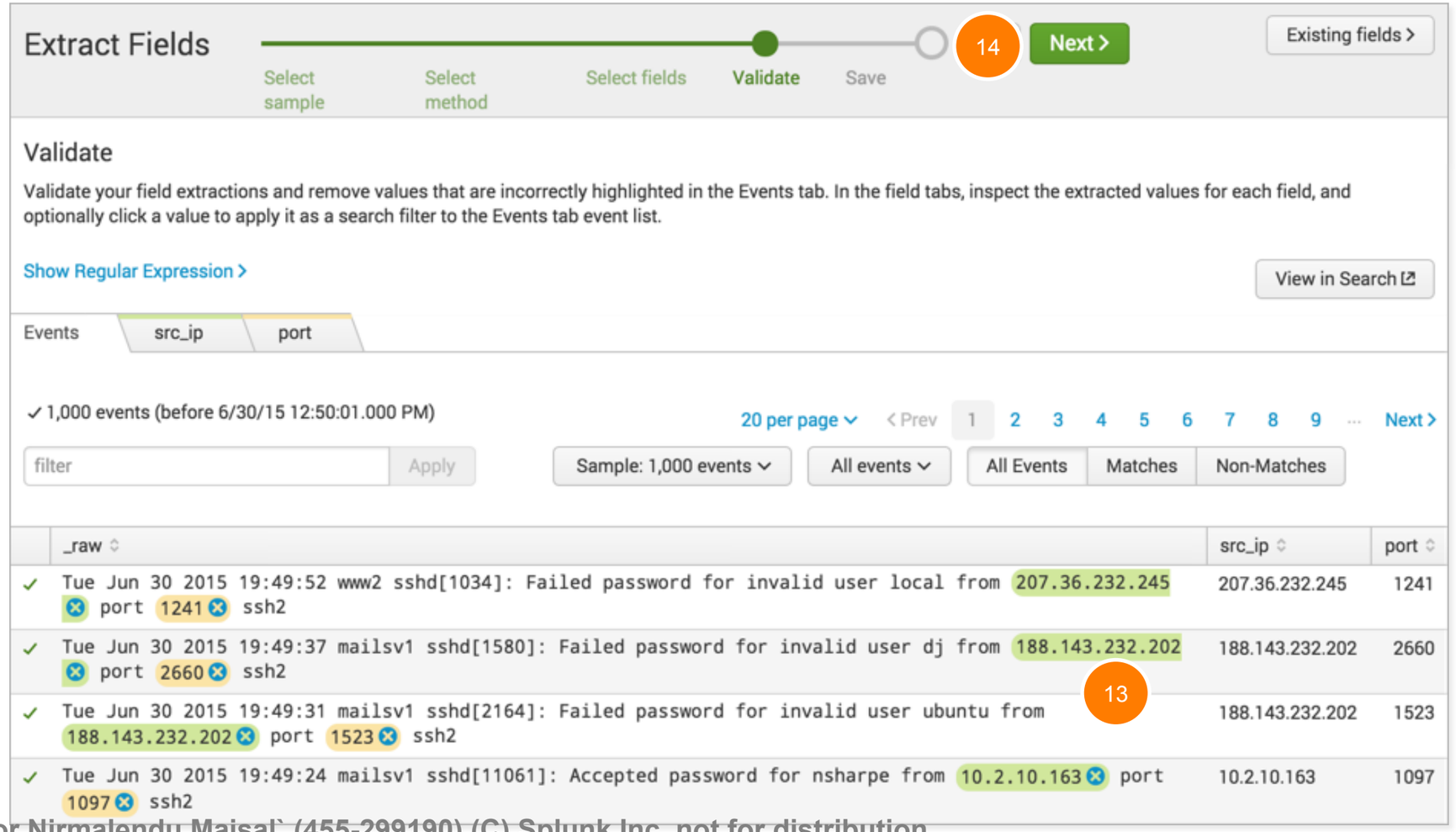
Regex Field Extractions from Settings – Preview

11. Preview the sample events
12. Click **Next**



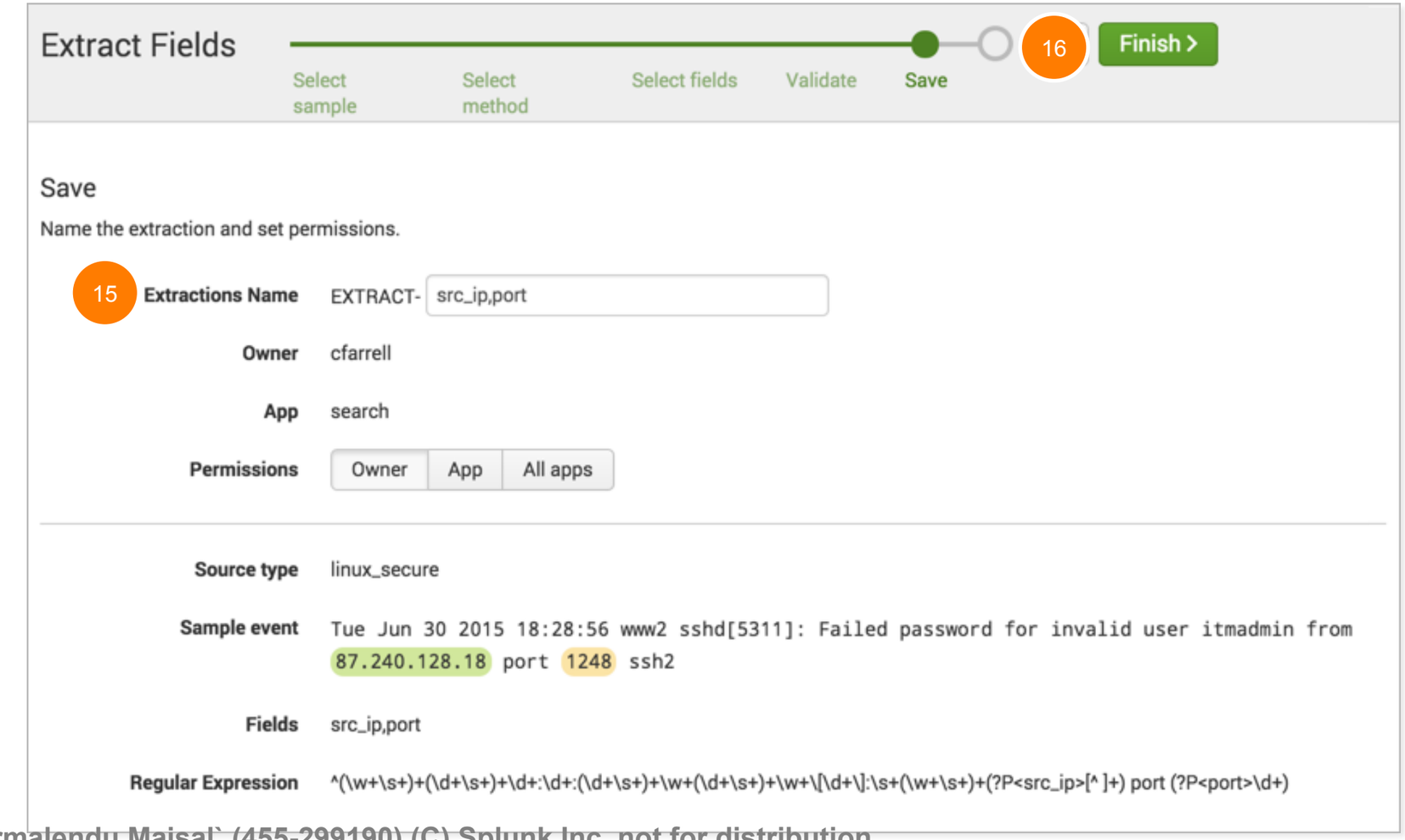
Regex Field Extractions from Settings – Validate

13. Validate the proper field values are extracted
14. Click **Next**

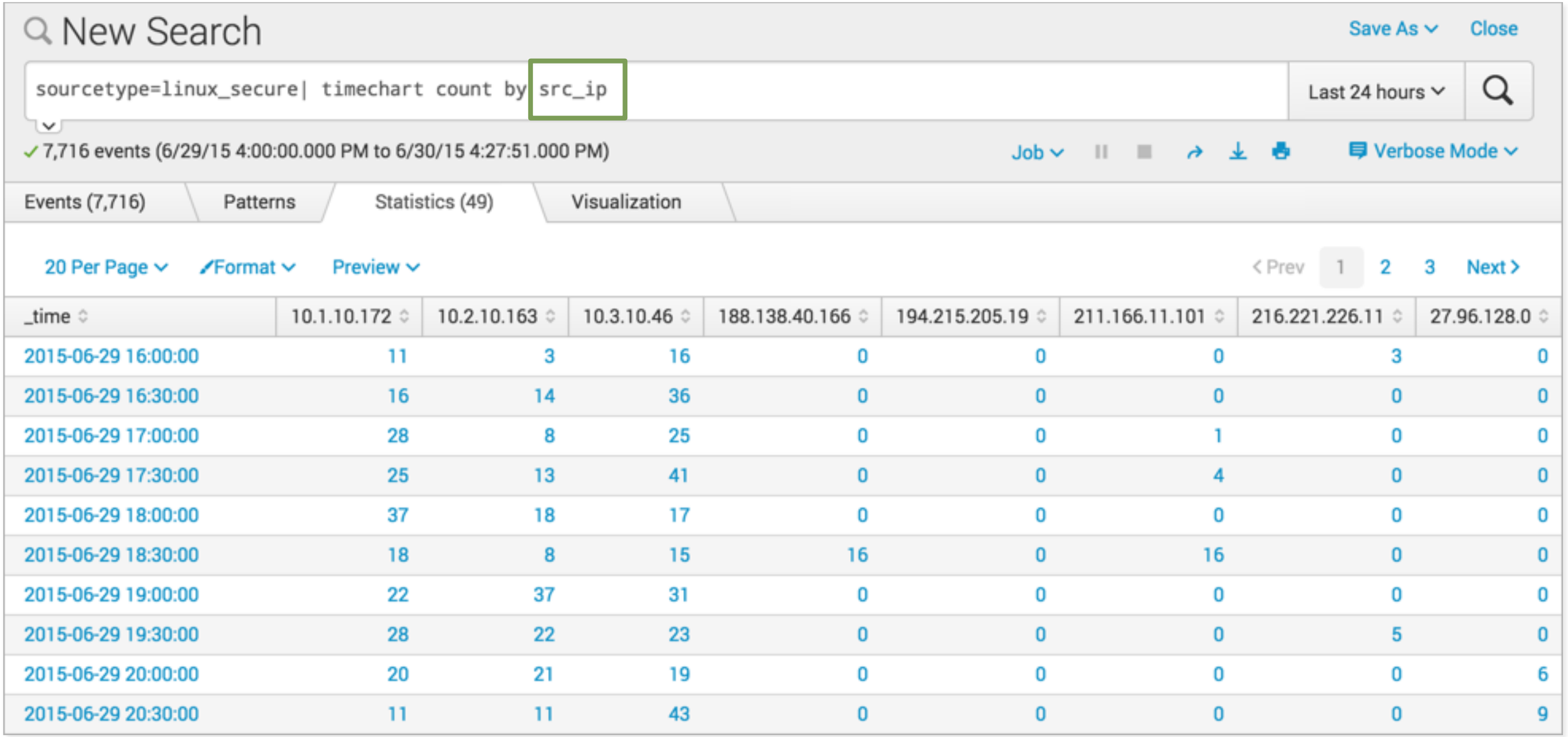


Regex Field Extractions from Settings – Save

15. Review the name for the newly extracted field and set permissions
16. Click **Finish**



Using the Extracted Field

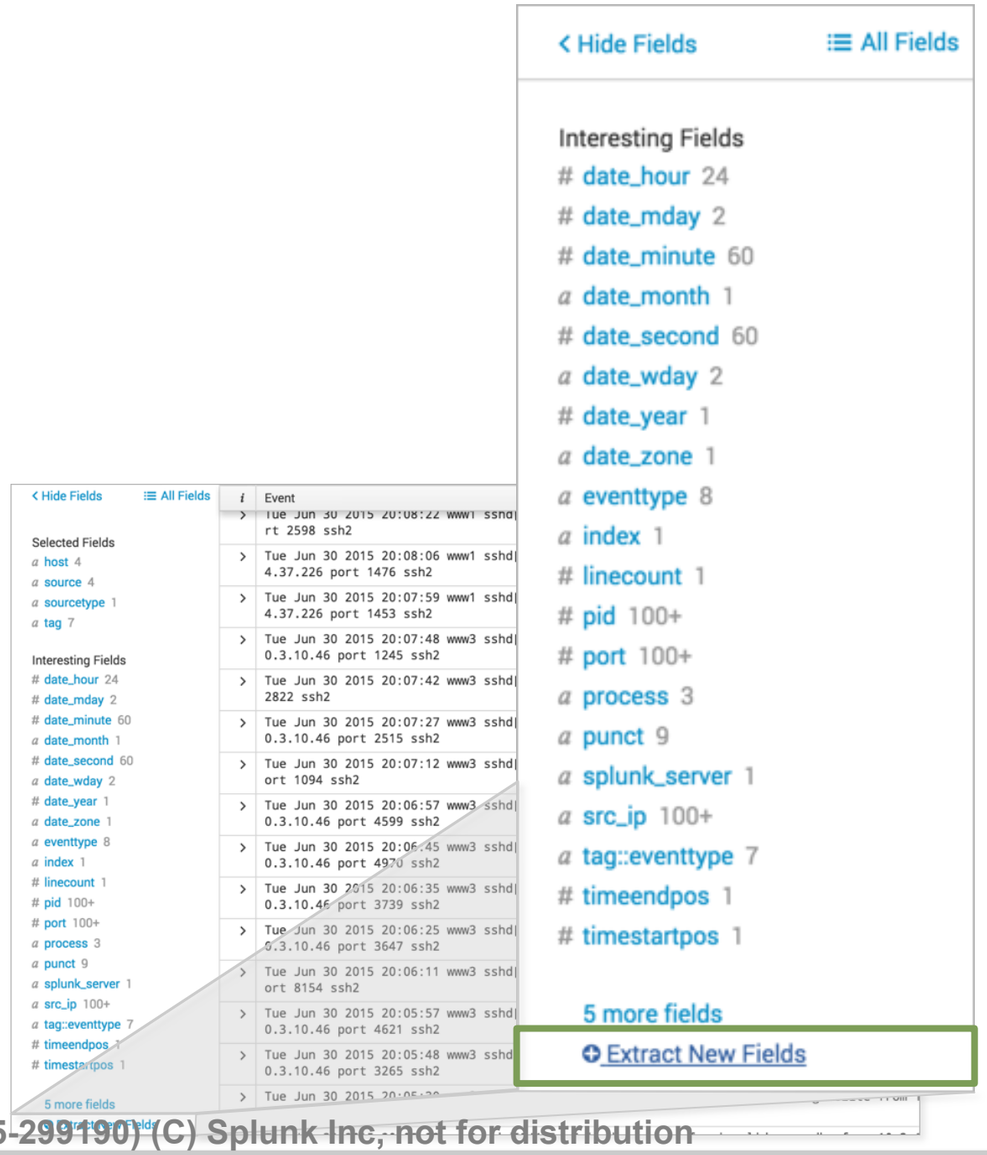


_time	10.1.10.172	10.2.10.163	10.3.10.46	188.138.40.166	194.215.205.19	211.166.11.101	216.221.226.11	27.96.128.0
2015-06-29 16:00:00	11	3	16	0	0	0	3	0
2015-06-29 16:30:00	16	14	36	0	0	0	0	0
2015-06-29 17:00:00	28	8	25	0	0	1	0	0
2015-06-29 17:30:00	25	13	41	0	0	4	0	0
2015-06-29 18:00:00	37	18	17	0	0	0	0	0
2015-06-29 18:30:00	18	8	15	16	0	16	0	0
2015-06-29 19:00:00	22	37	31	0	0	0	0	0
2015-06-29 19:30:00	28	22	23	0	0	0	5	0
2015-06-29 20:00:00	20	21	19	0	0	0	0	6
2015-06-29 20:30:00	11	11	43	0	0	0	0	9

Regex Field Extractions from the Fields Sidebar

Steps to extract fields:

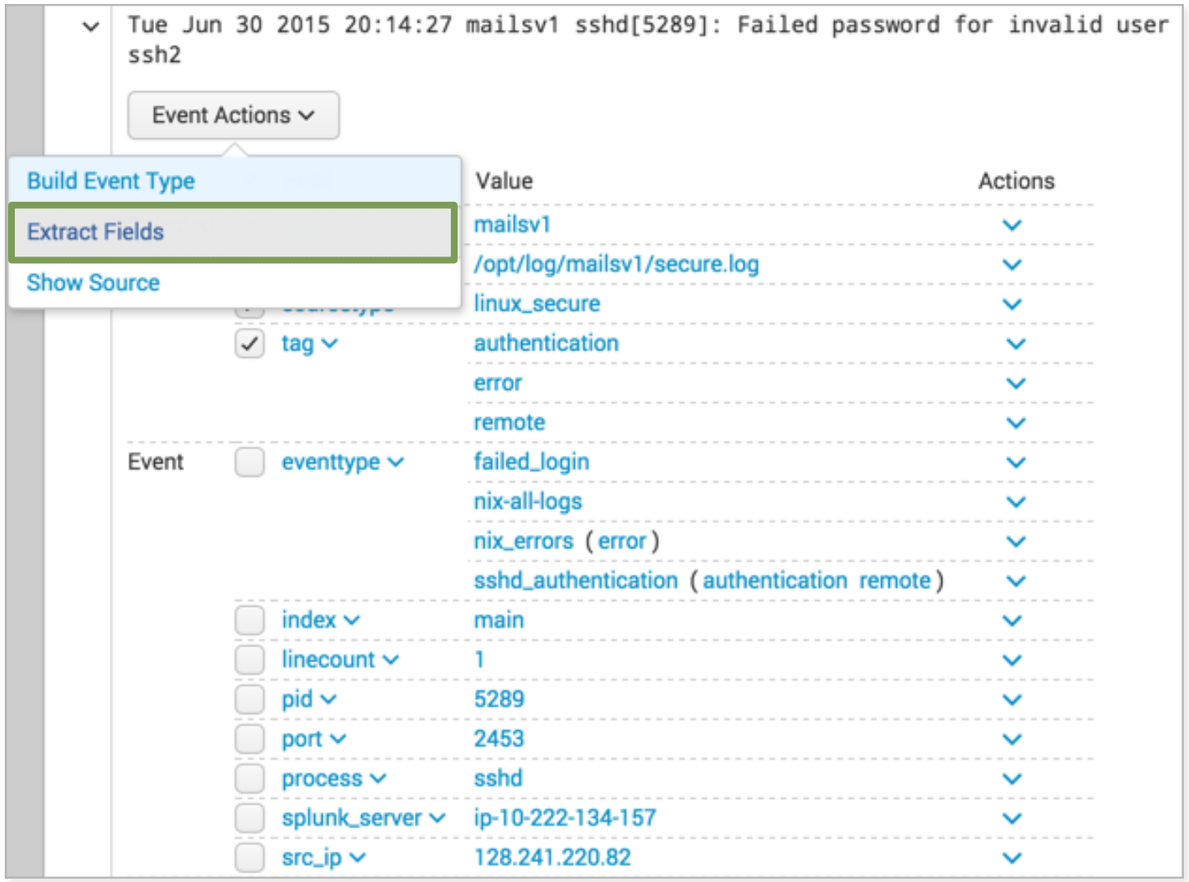
1. Click **Extract New Fields**
2. Select a sample event
3. Select the **Regex** extraction method
4. Select fields you want to extract and validate
5. Save your field extraction



Regex Field Extractions from Event Actions

Steps to extract fields:

1. Select **Extract Fields**
2. Select the **Regex** extraction method
3. Select fields you want to extract and validate
4. Save your field extraction



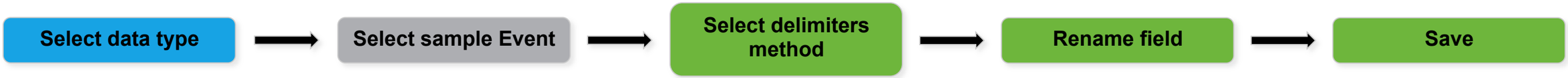
Delimiter Field Extractions

Use delimited field extractions when the event log does not have a header and fields are separated by spaces, commas, or characters

In this example, the fields are separated by commas

Field Extraction Workflow (Delimiters)

Settings

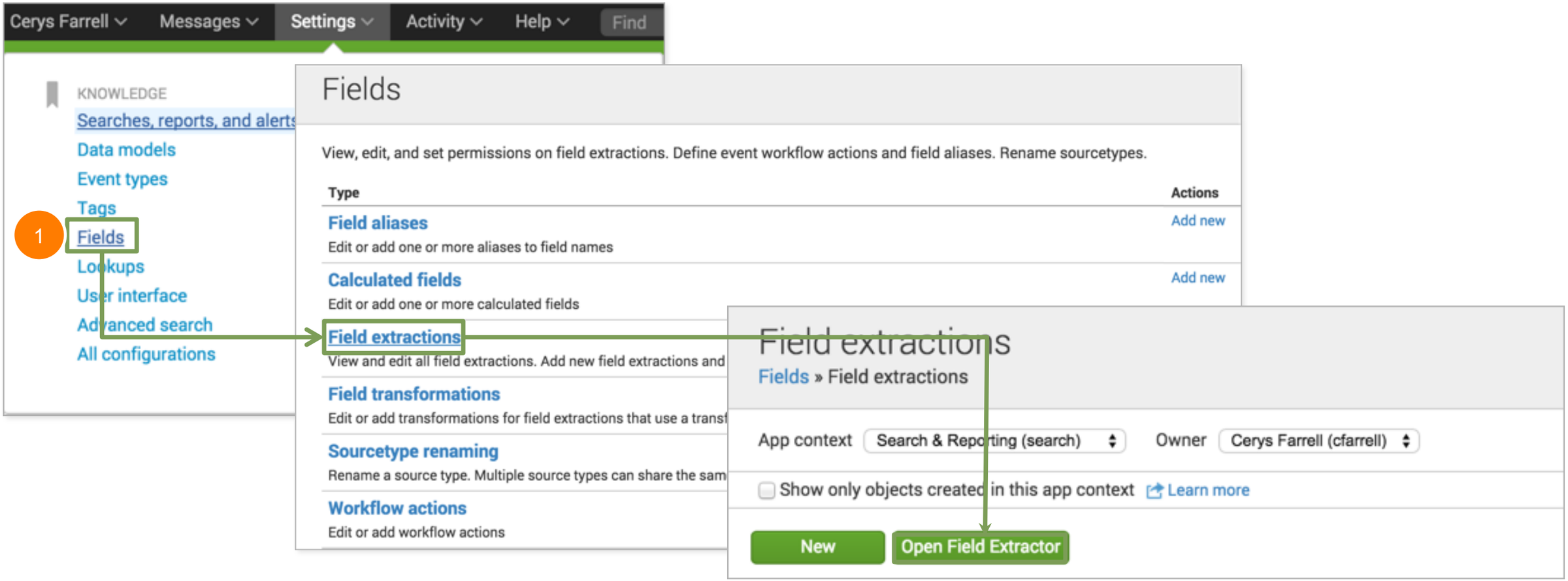


Fields Sidebar

Event Actions

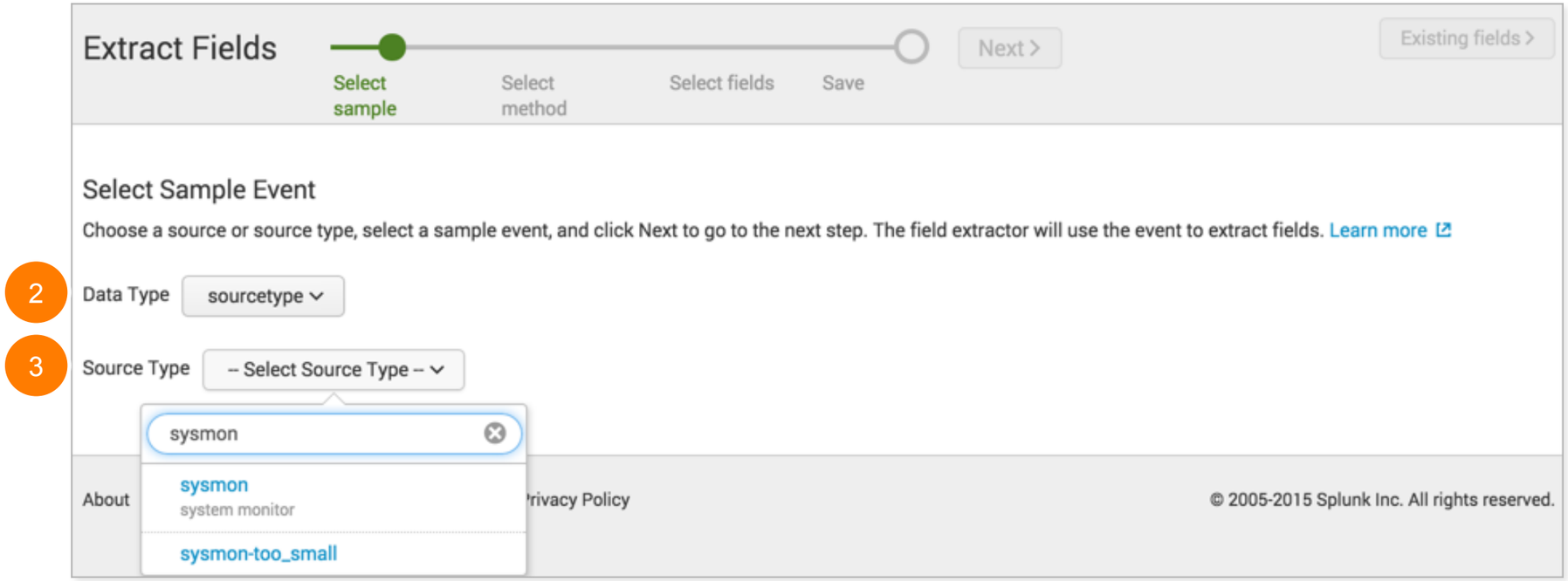
Delimiter Field Extractions from Settings

1. Settings > Fields > Field extractions > Open Field Extractor



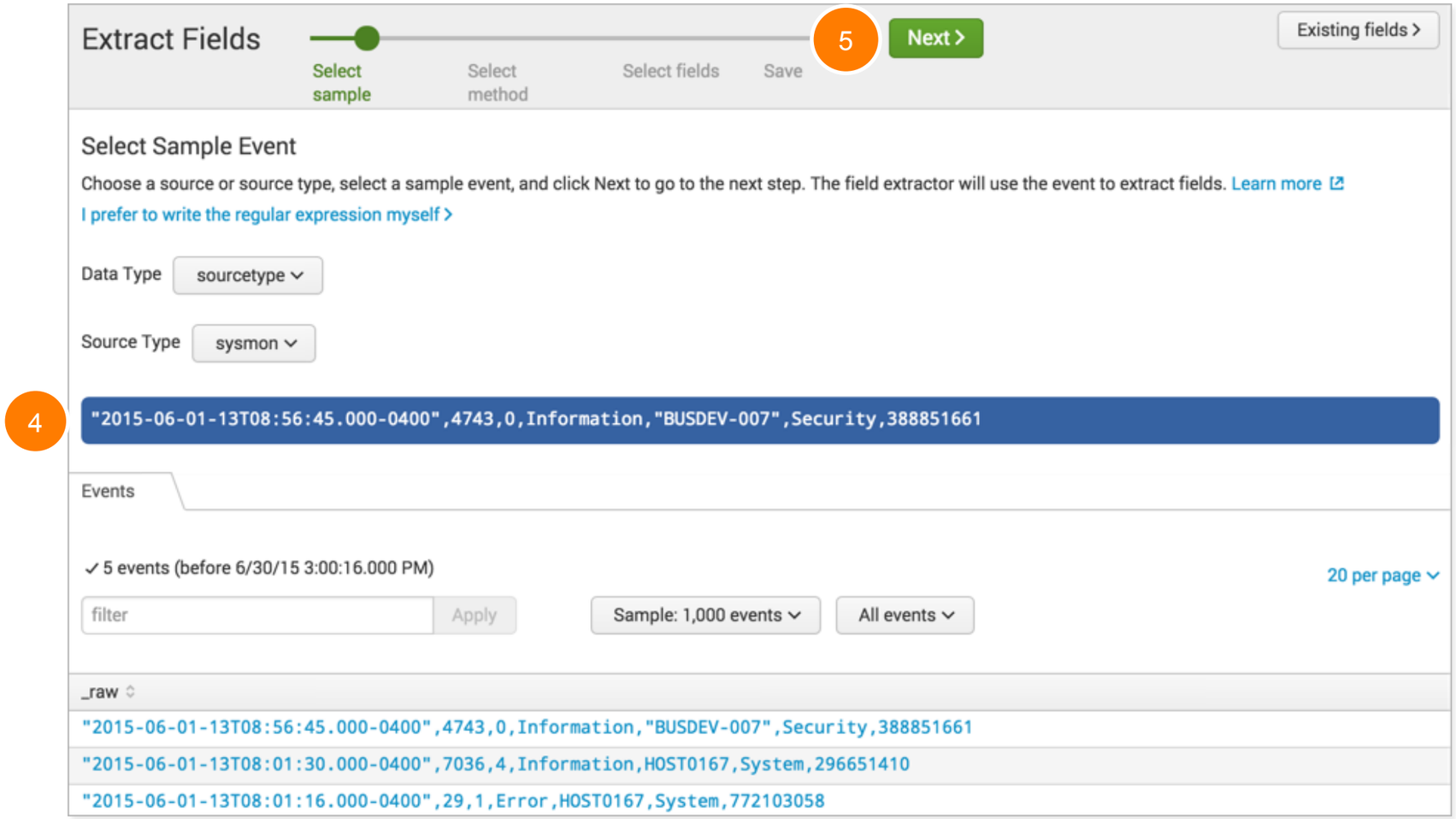
Delimiter Field Extractions from Settings – Select Sample

2. Select the Data Type
   - sourcetype
   - source
3. Select the Source Type



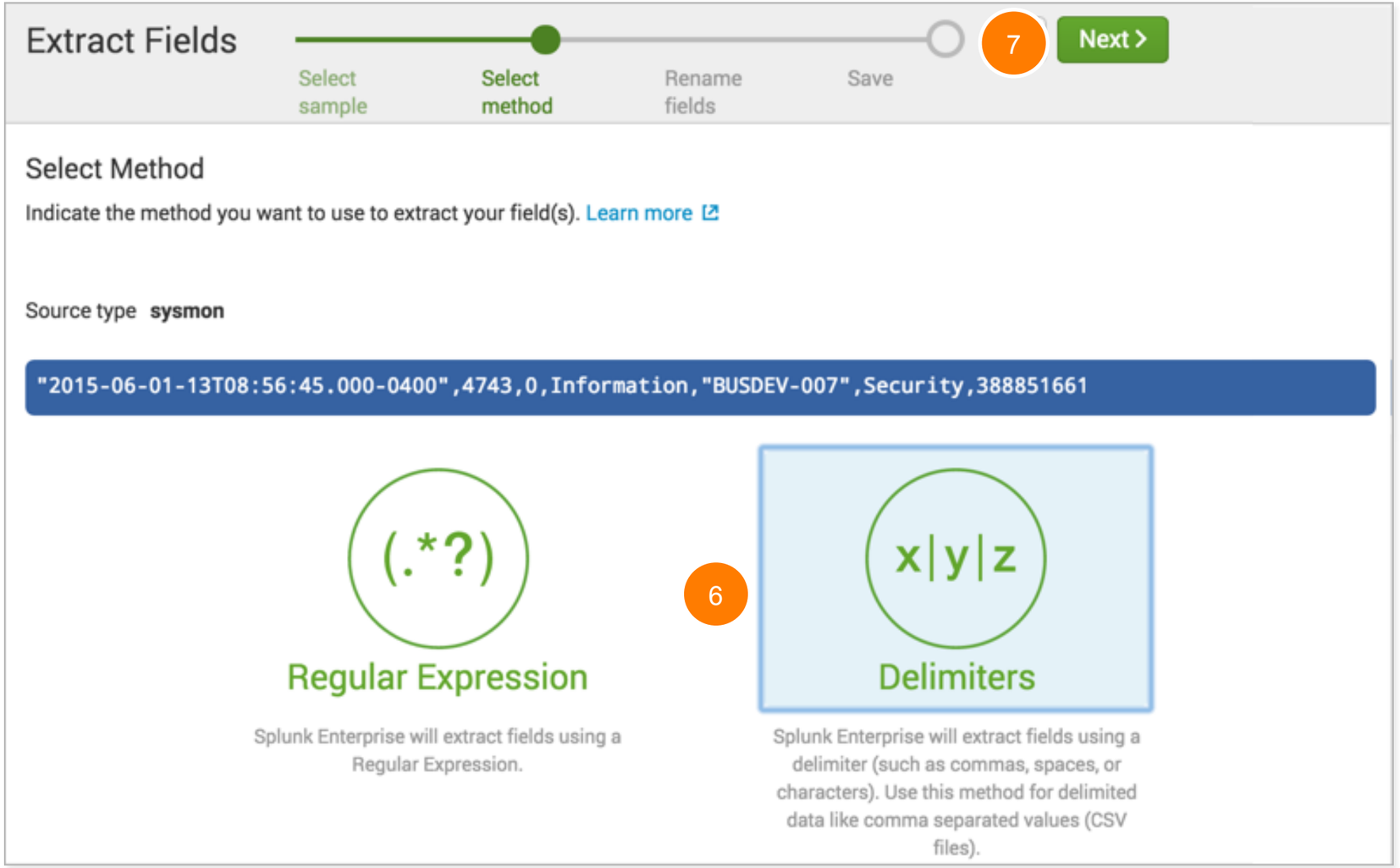
Delimiter Field Extractions from Settings – Select Event

4. Select a sample event
5. Click **Next >**



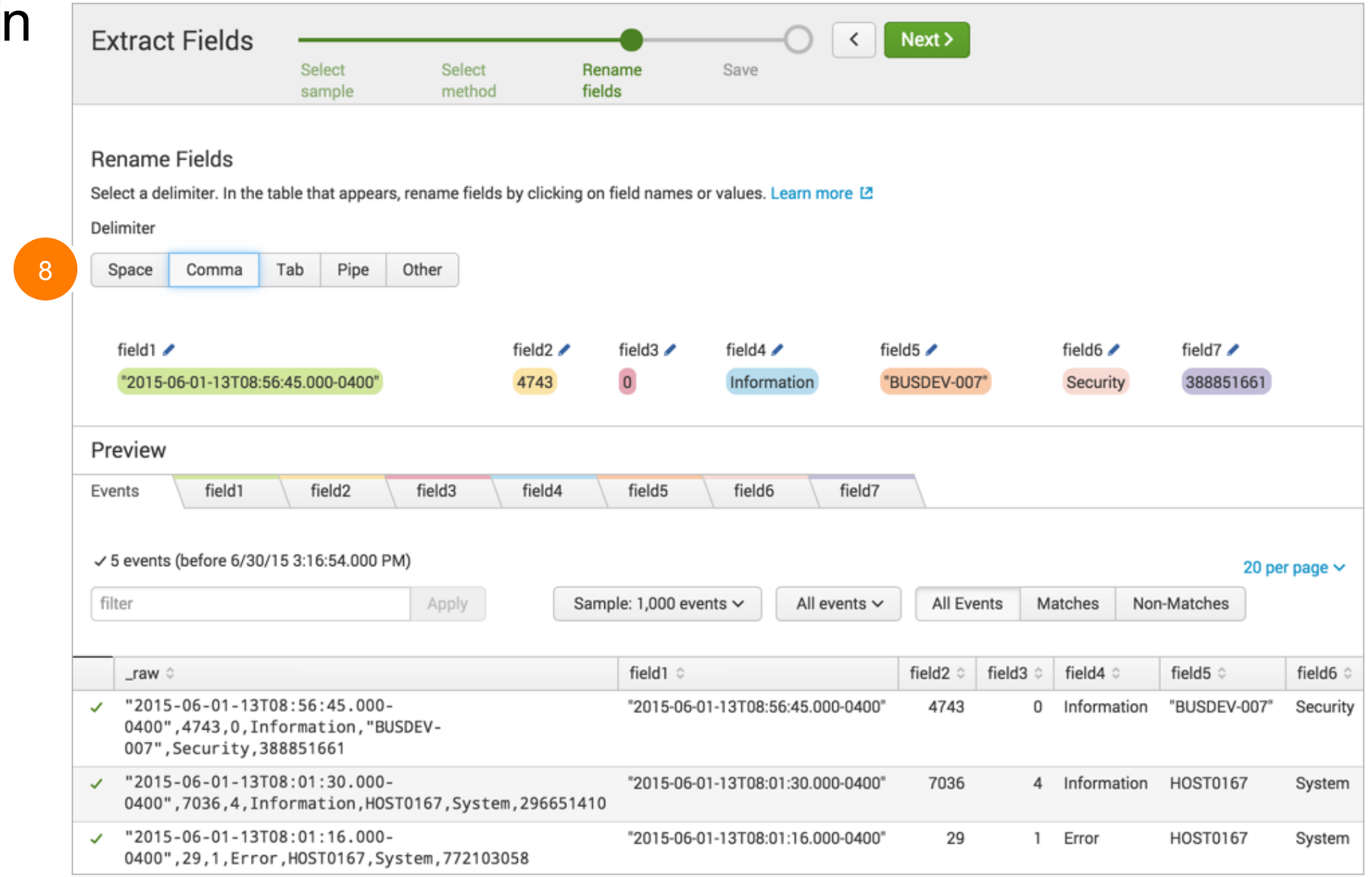
Delimiter Field Extractions from Settings – Select Method

6. Select **Delimiters**
7. Click **Next >**



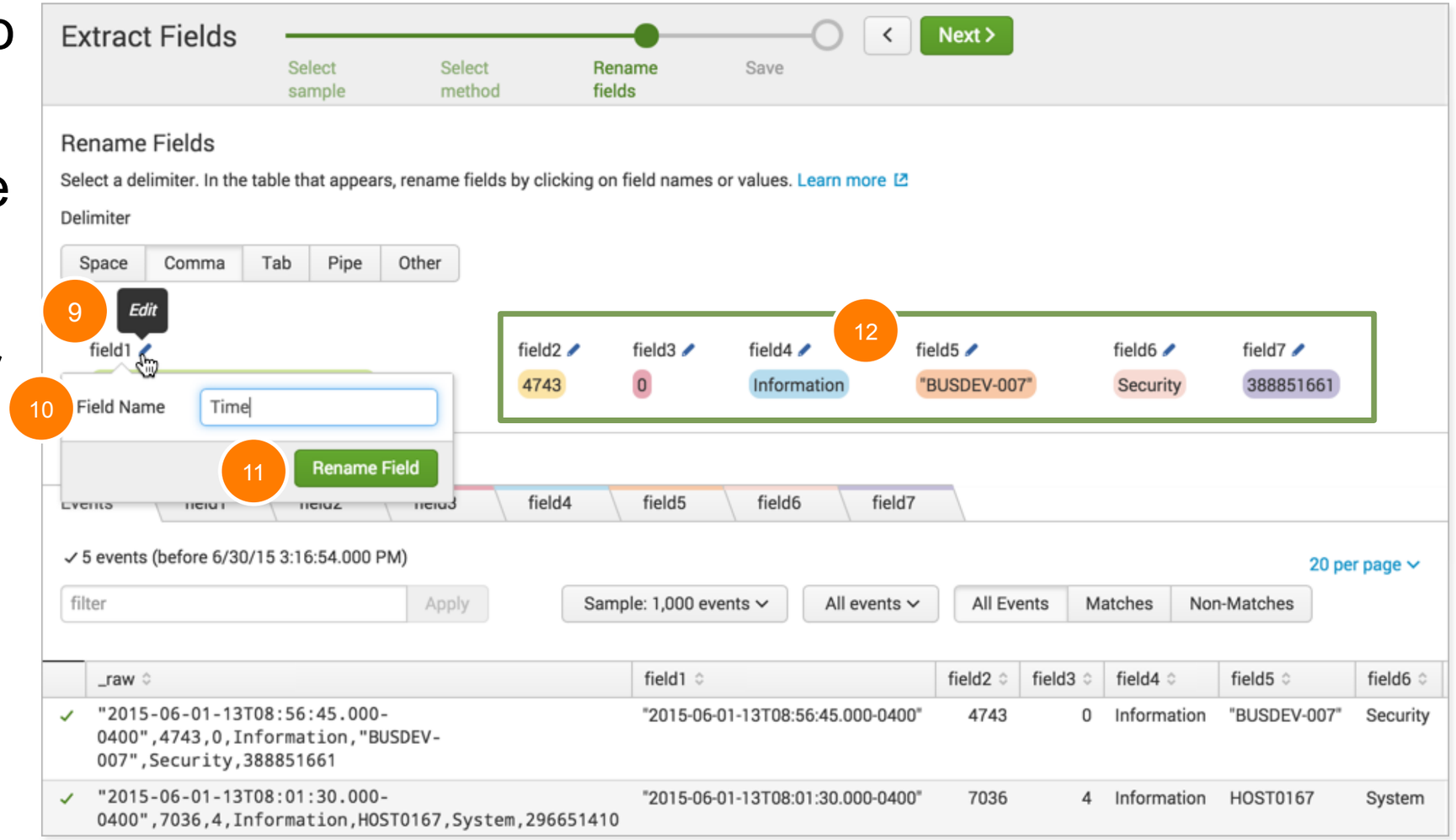
Delimiter Field Extractions from Settings - Select Delimiter

8. Select the Delimiter used in your event



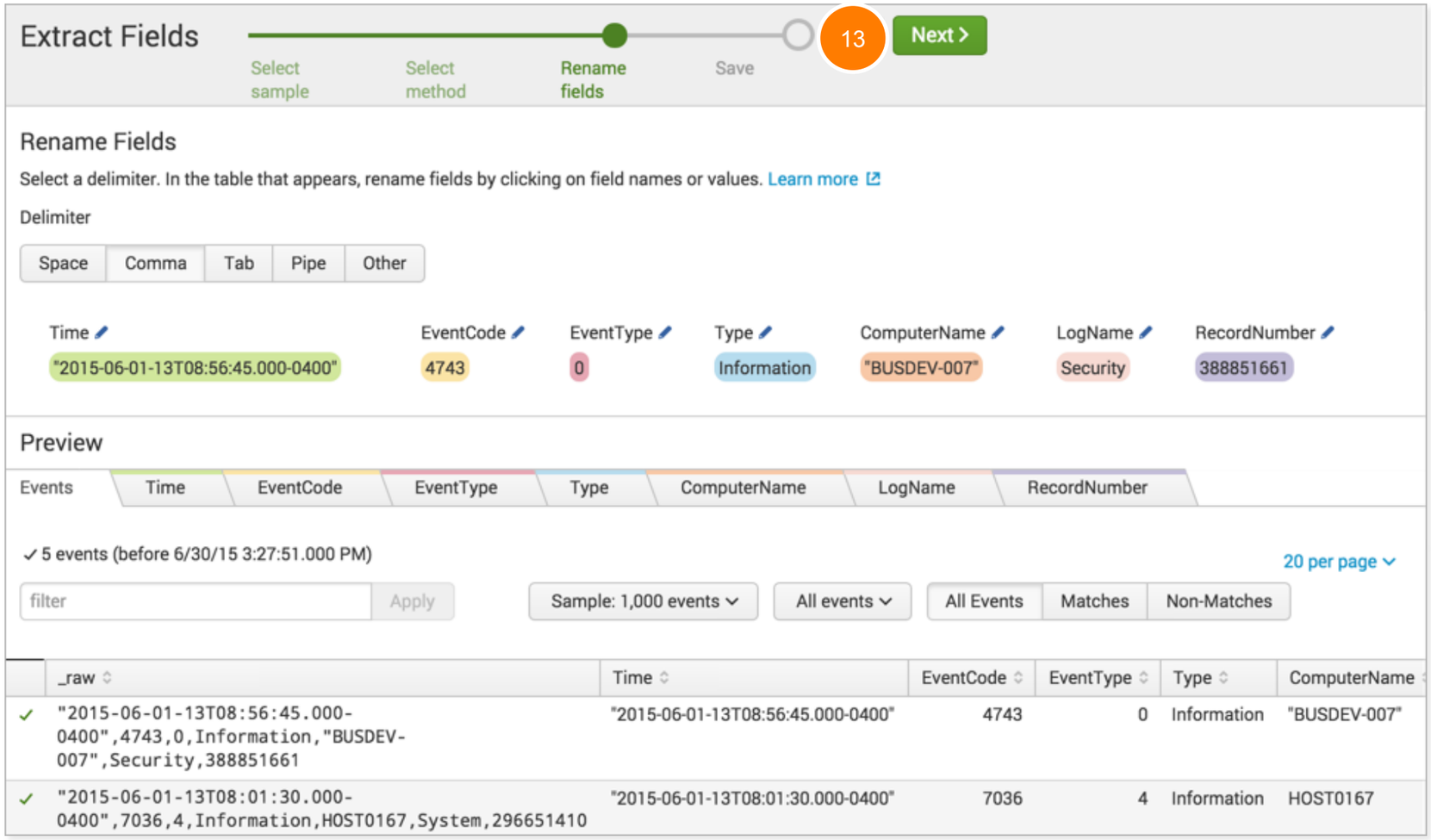
Delimiter Field Extractions from Settings – Rename field

9. Click the ✎ icon next to the default field name
10. Enter a new field name
11. Click **Rename Field**
12. Repeat these steps for all fields



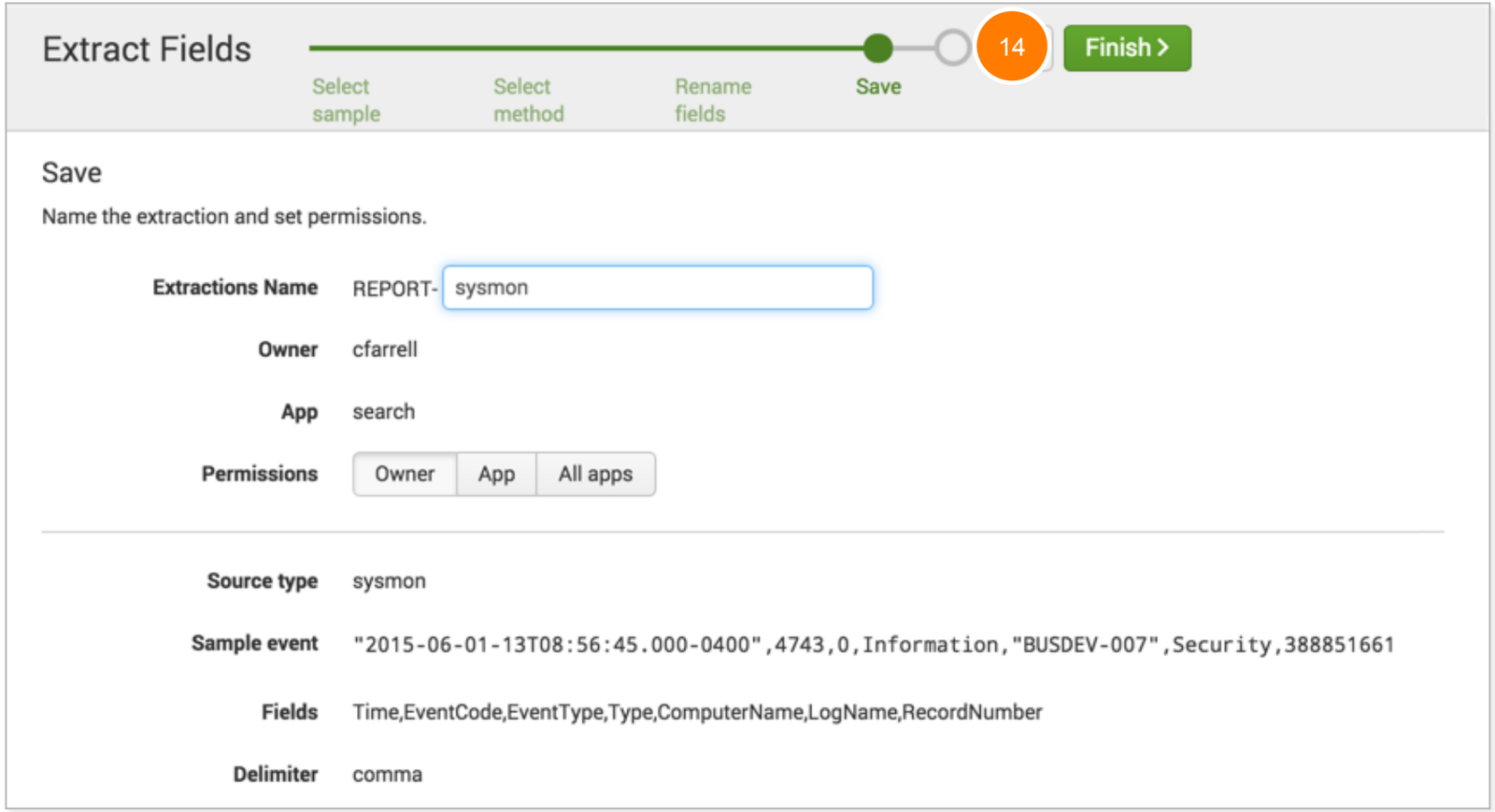
Delimiter Field Extractions from Settings – Rename field (cont.)

13. After all the fields are renamed, click **Next >**



Delimiter Field Extractions from Settings – Save

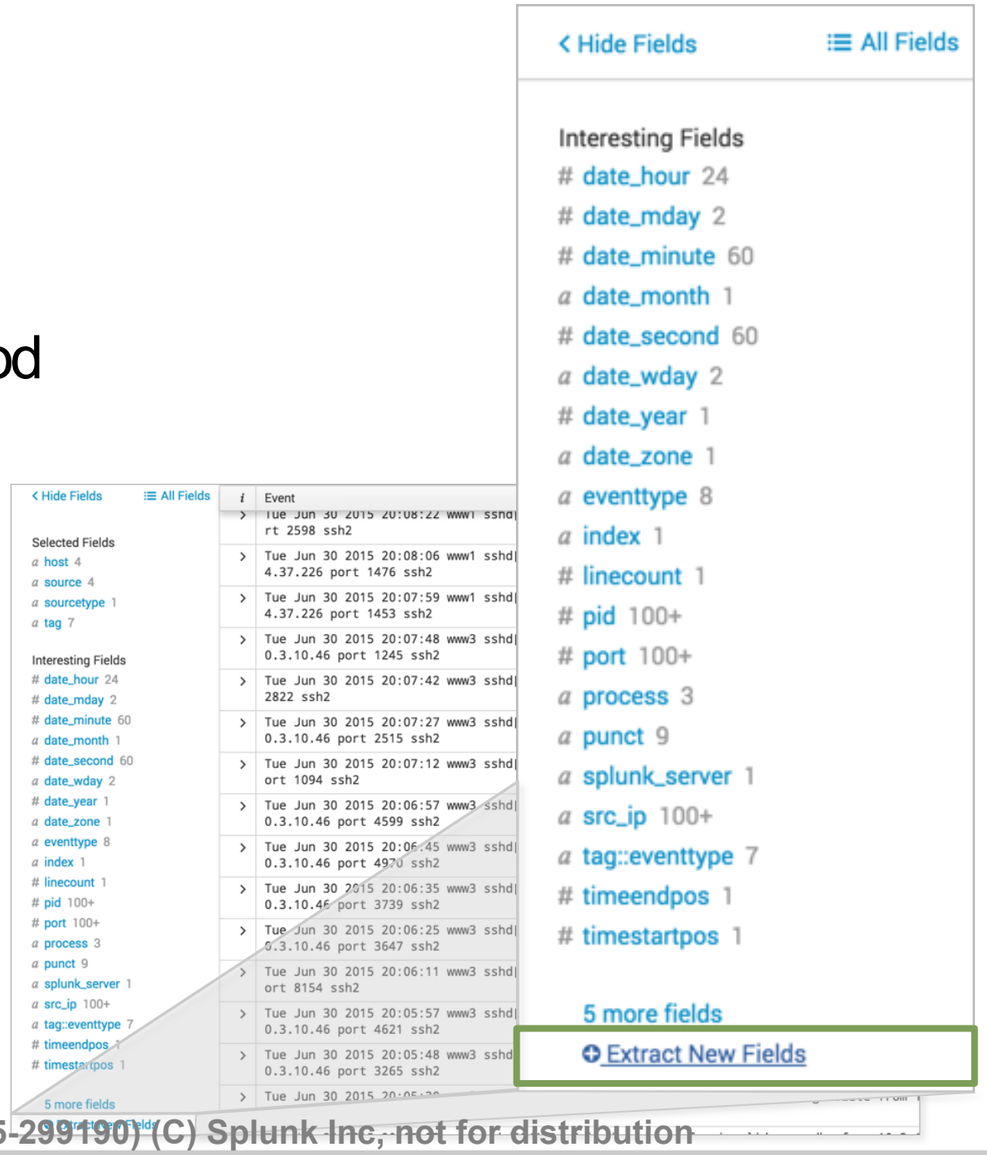
14. Review the name for your extraction and click **Finish >**



Delimiter Field Extractions from the Fields Sidebar

Steps to extract fields:

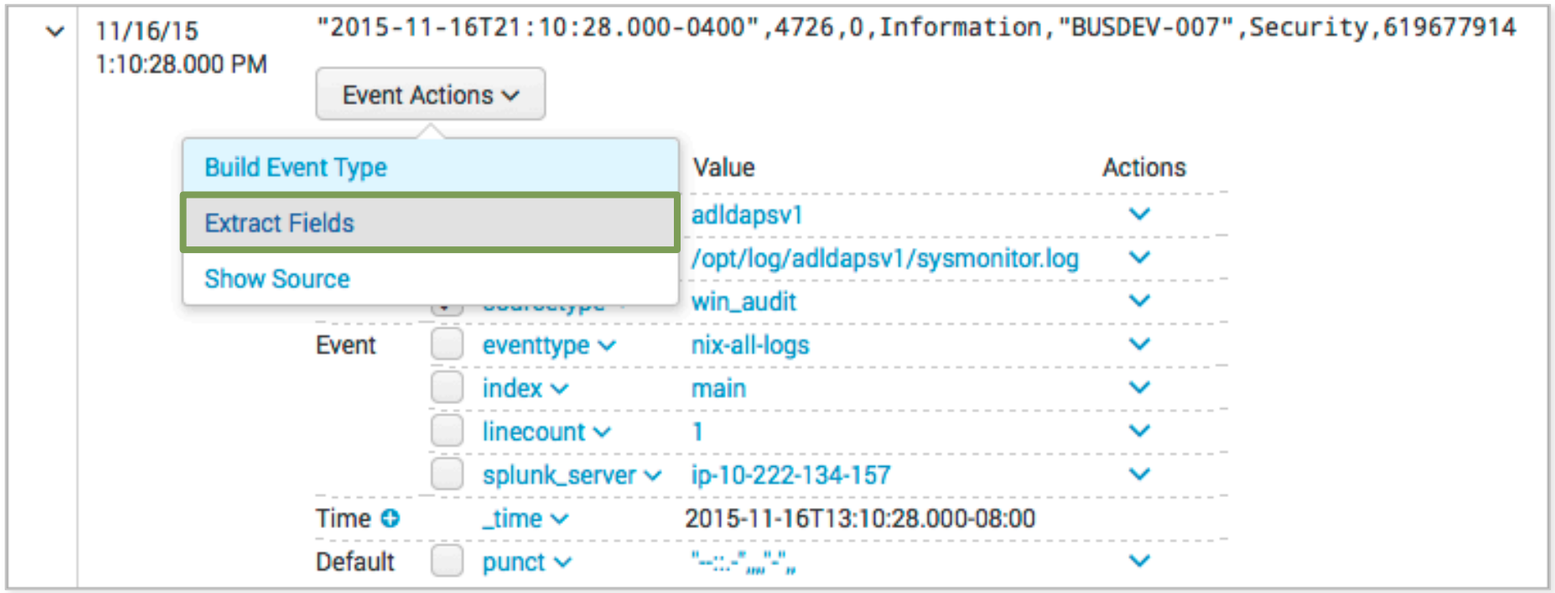
1. Click **Extract New Fields**
2. Select a sample event
3. Select the **Delimiters** extraction method
4. Rename fields
5. Save your field extraction



Delimiter Field Extractions from Event Actions

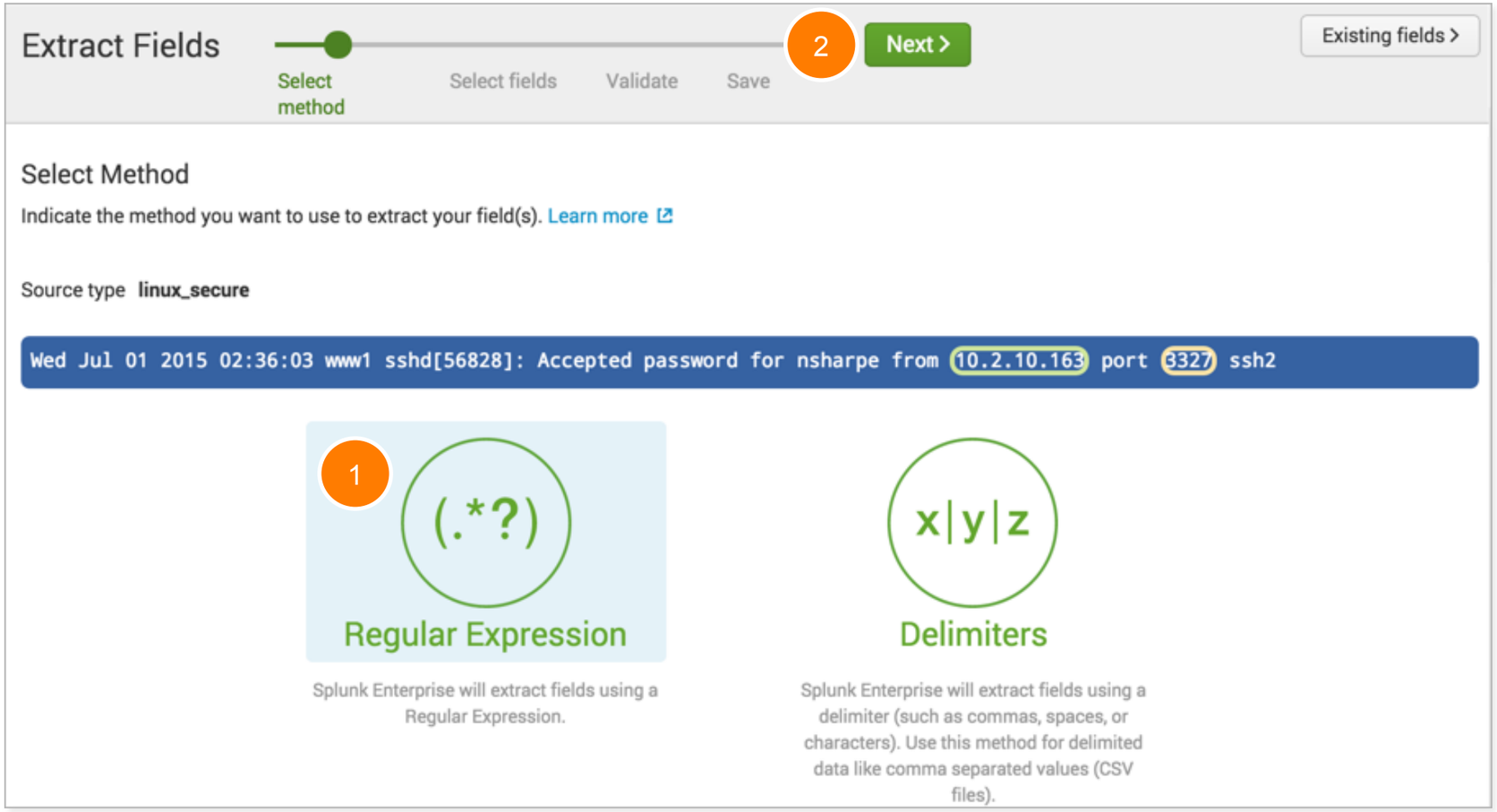
Steps to extract fields:

1. Click **Extract Fields**
2. Select the **Delimiters** extraction method
3. Select fields you want to extract and validate
4. Save your field extraction



Editing Regex for Field Extractions

1. From **Select Method**, click **Regular Expression**
2. Click **Next >**

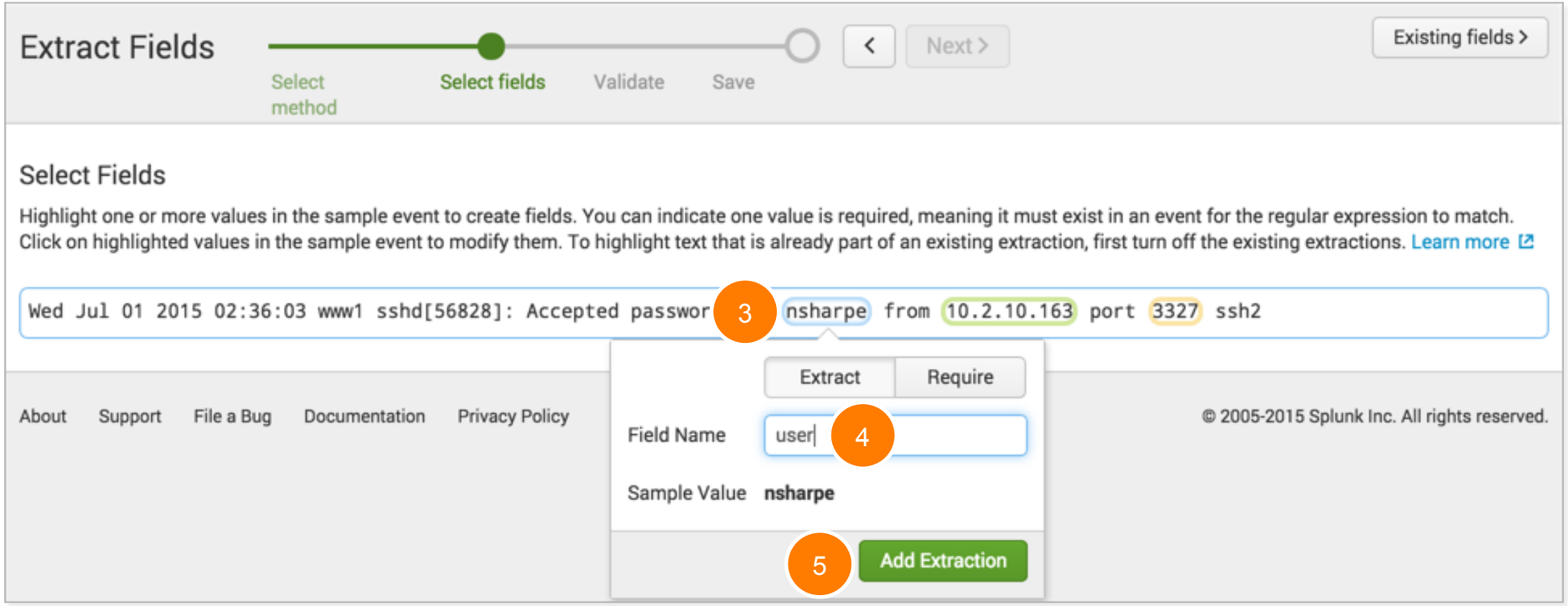


Editing Regex for Field Extractions – Select Field

3. Select the field to extract.
4. Provide a **Field Name**
5. Click **Add Extraction**

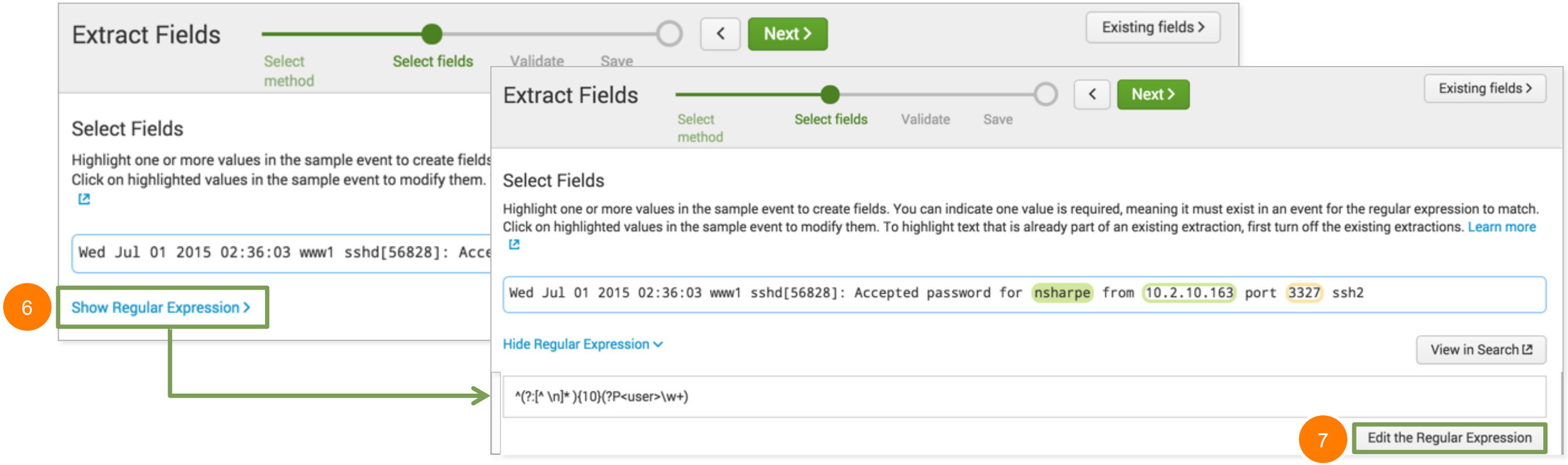
Note

For more information about Splunk Regular Expressions, see http://docs.splunk.com/Documentation/Splunk/6.2/Knowledge/AboutSplunkregularexpressions



Editing Regex for Field Extractions – Show Regex

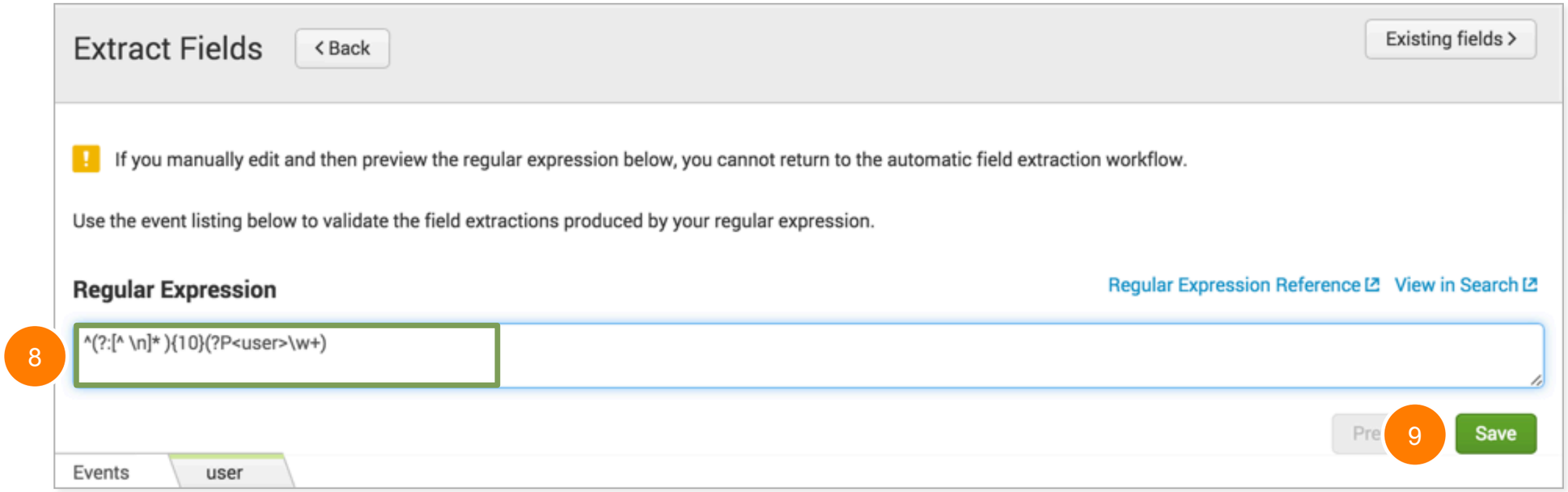
6. Click **Show Regular Expression >**
7. Click **Edit the Regular Expression**



Editing Regex for Field Extractions – Modify RegEx

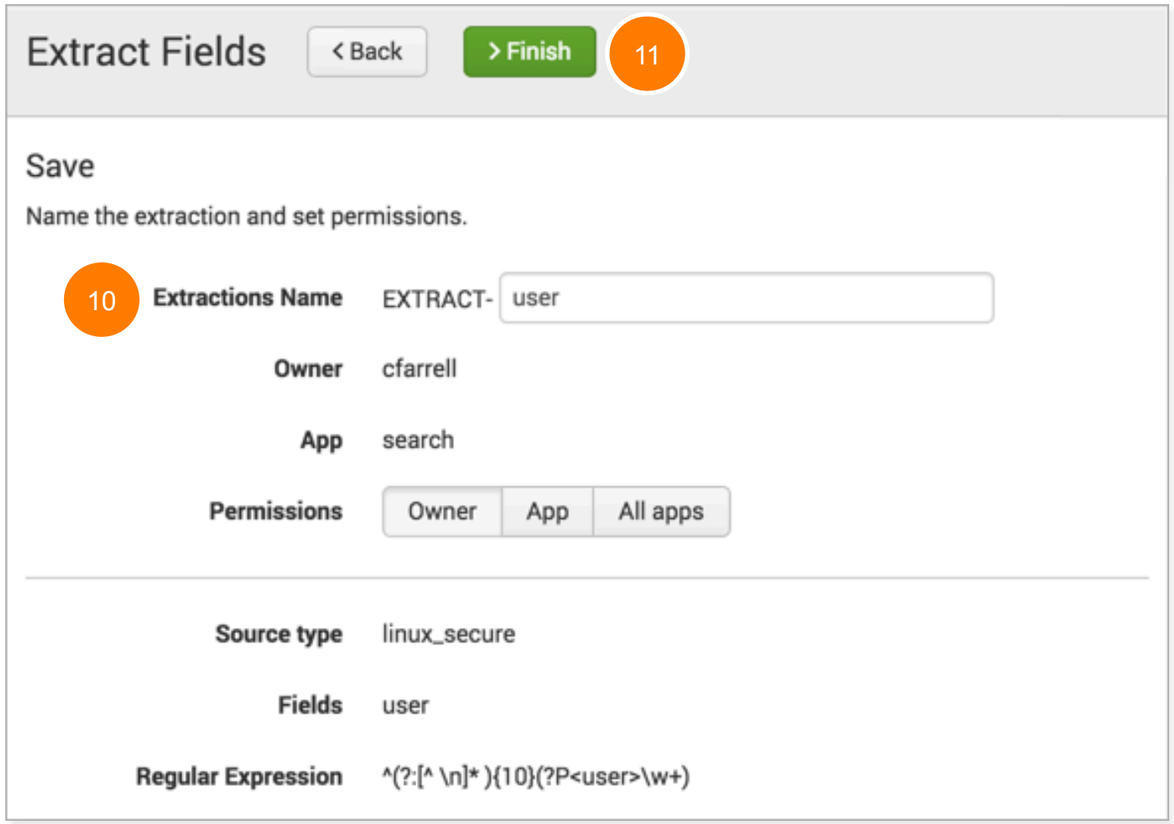
8. Update the regular expression
9. Click **Save**

***Once you edit the regular expression, you cannot go back to the Field Extractor UI**



Editing Regex for Field Extractions - Save

10. Review the **Extractions Name** and set permissions
11. Click **Finish**



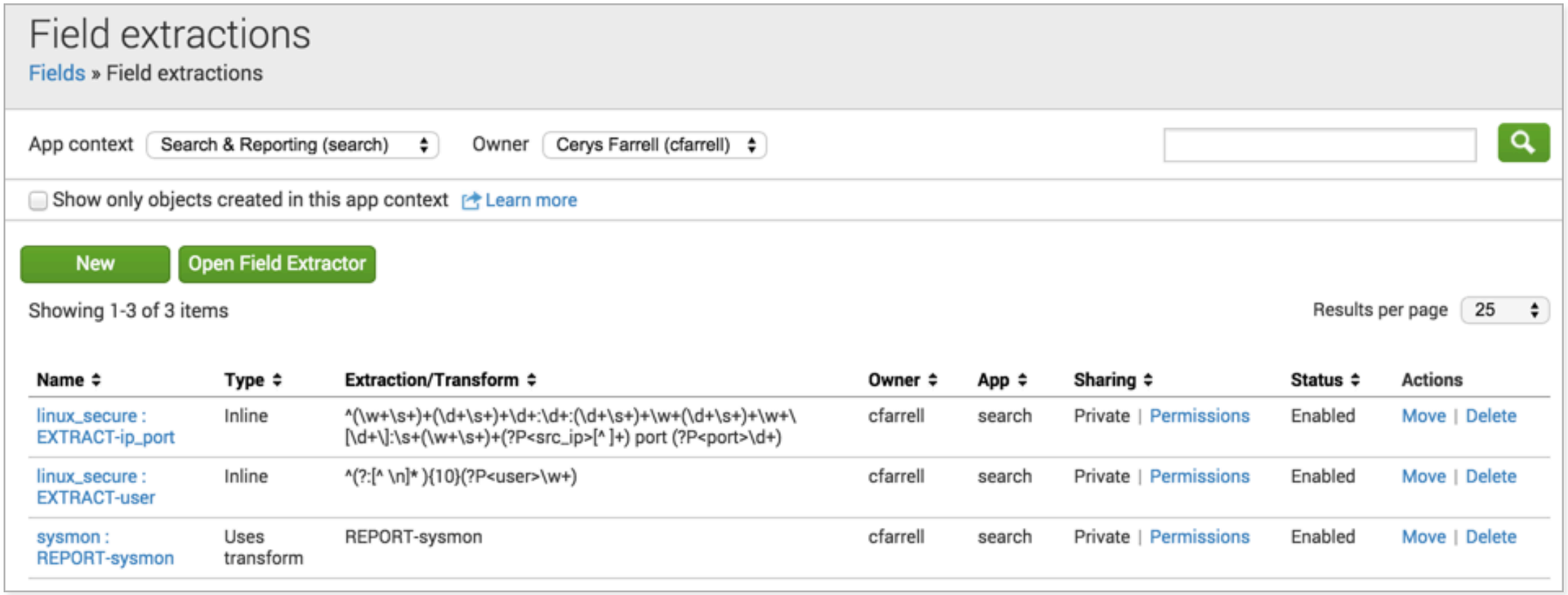
Managing Field Extractions

Settings > Fields > Field Extractions

- Edit permissions
- Move
- Delete

Note

For more information about directly editing these objects go to:
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Transformsconf



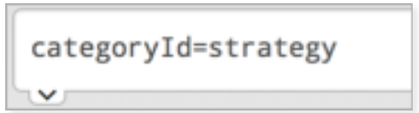
Module 5:
Creating Tags and Event Types

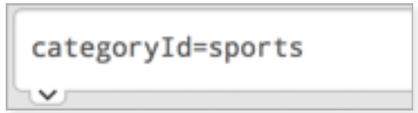
Module Objectives

- Create and use tags
- Describe event types and their uses
- Create an event type

Describing Tags

- Tags are like nicknames that you create for related field/value pairs
- Tags make your data more understandable and less ambiguous
  - Example: The following rating system needs to be applied to product categories
    - General – content is approved for all audiences
    - Teen – content is approved for audiences 13+
    - Mature – content is approved for audiences 18+



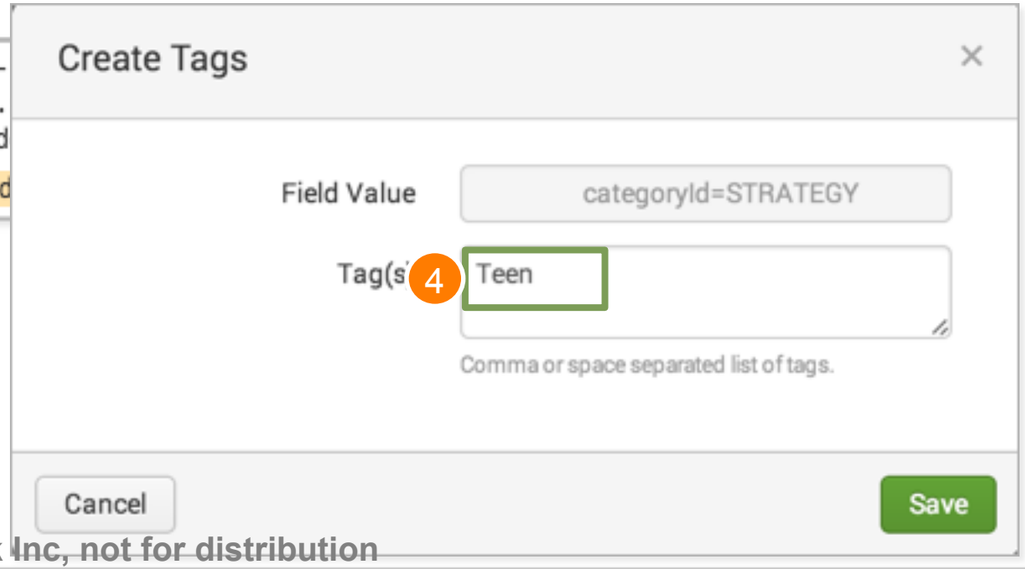


- You can create one or more tags for any field/value combination
- Tags are case sensitive

Creating Tags

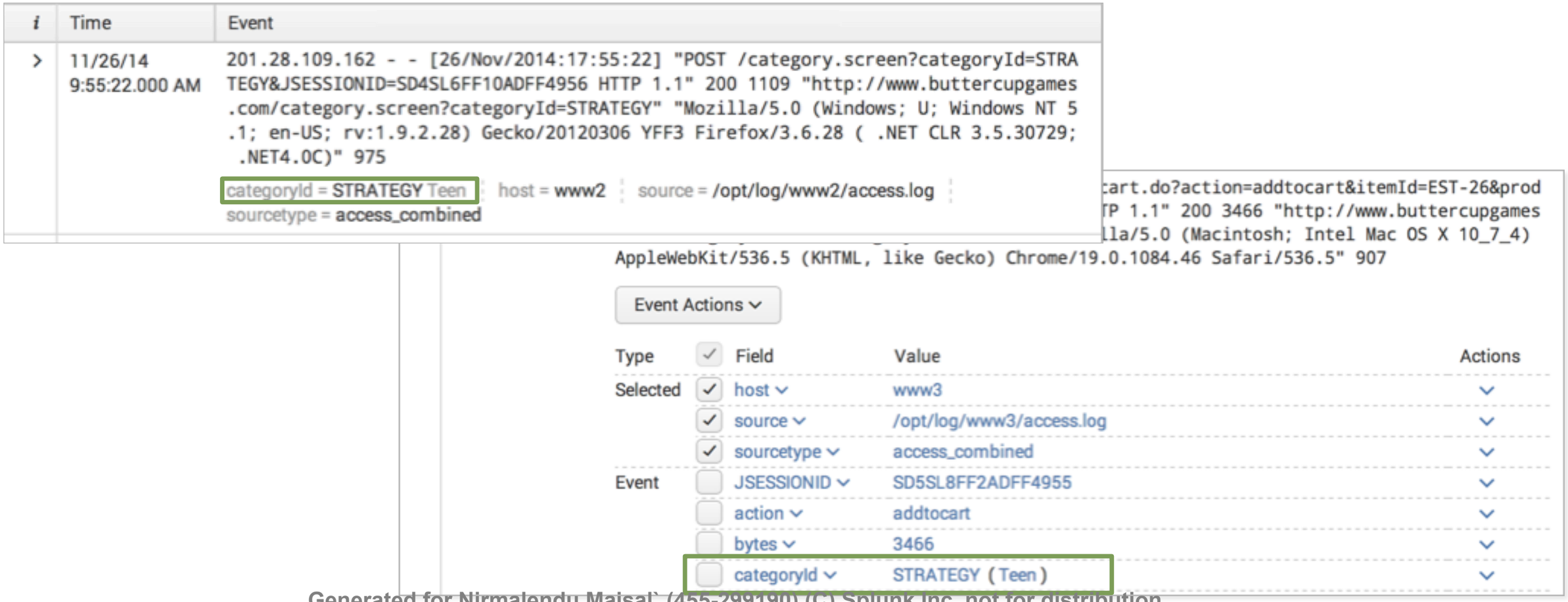
To create a tag:

1. Click on the arrow for event details
2. Under **Actions**, click the down arrow
3. Select **Edit Tags**
4. Name the tag(s) (comma-separated if using multiple tags)



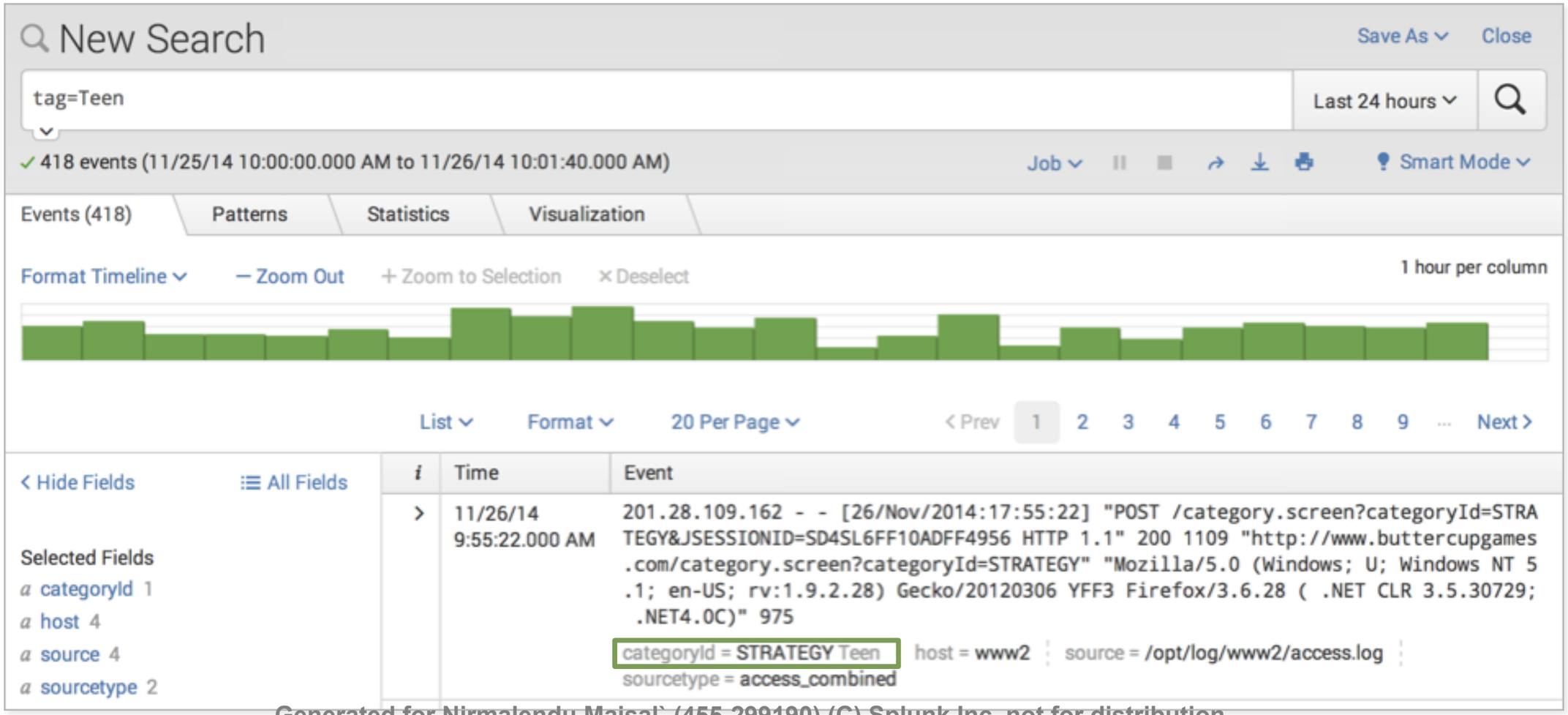
Viewing Tags

If a selected field value is tagged, the value of the tag appears in the results



Using Tags

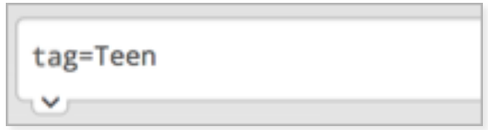
To use tags in a search, use the syntax: **tag=<*tag name*>**



Searching for Tags

To search for a tag associated with a value:

- tag=<tagname>

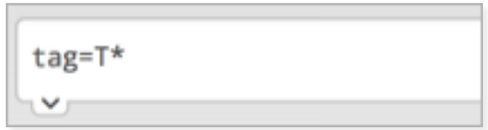


To search for a tag associated with a value on a specific field:

- tag::<field>=<tagname>

To search for a tag using a partial field value:

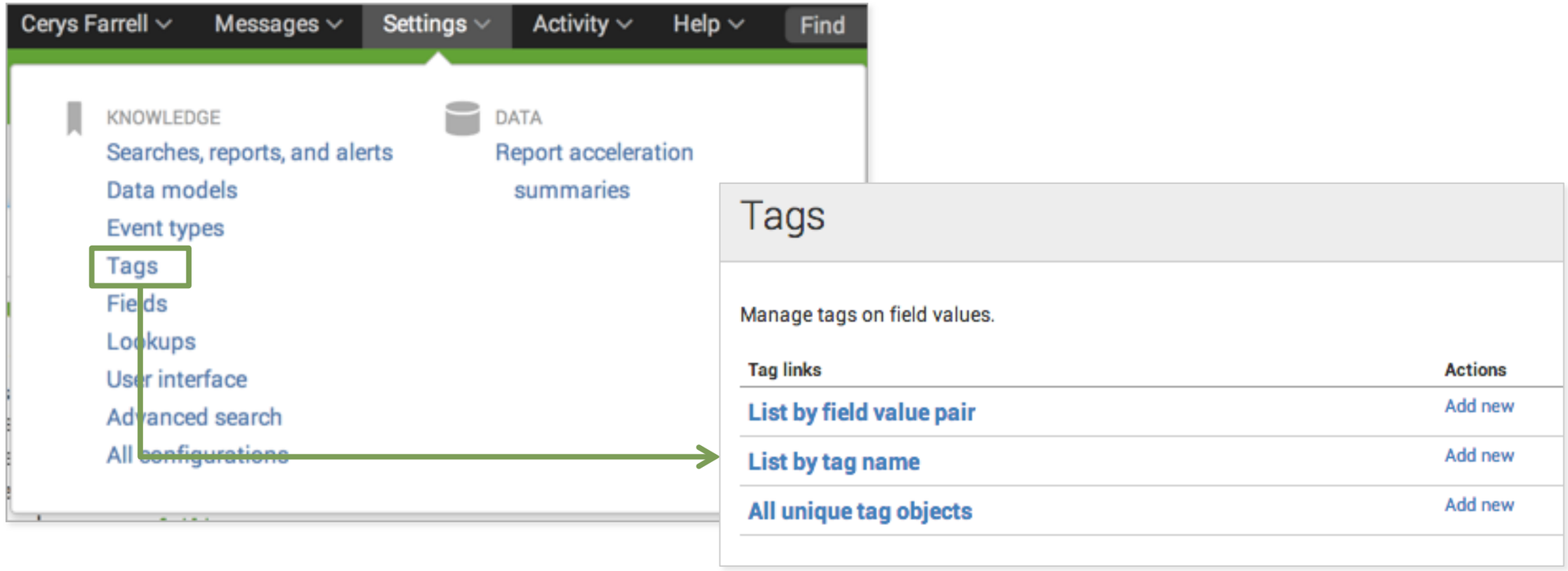
- use (*) wildcard



Managing Tags

Settings > Tags

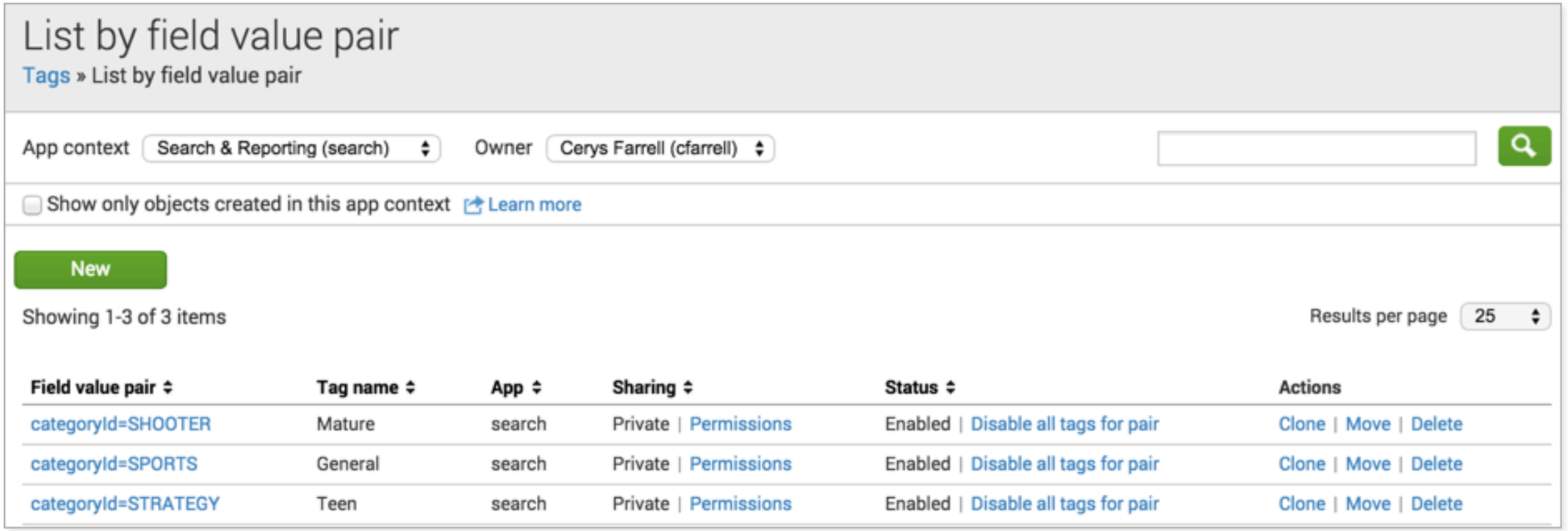
You can display tags by field value pair, tag name, or all unique tag objects



Managing Tags (cont.)

Settings > Tags > List by field value pair

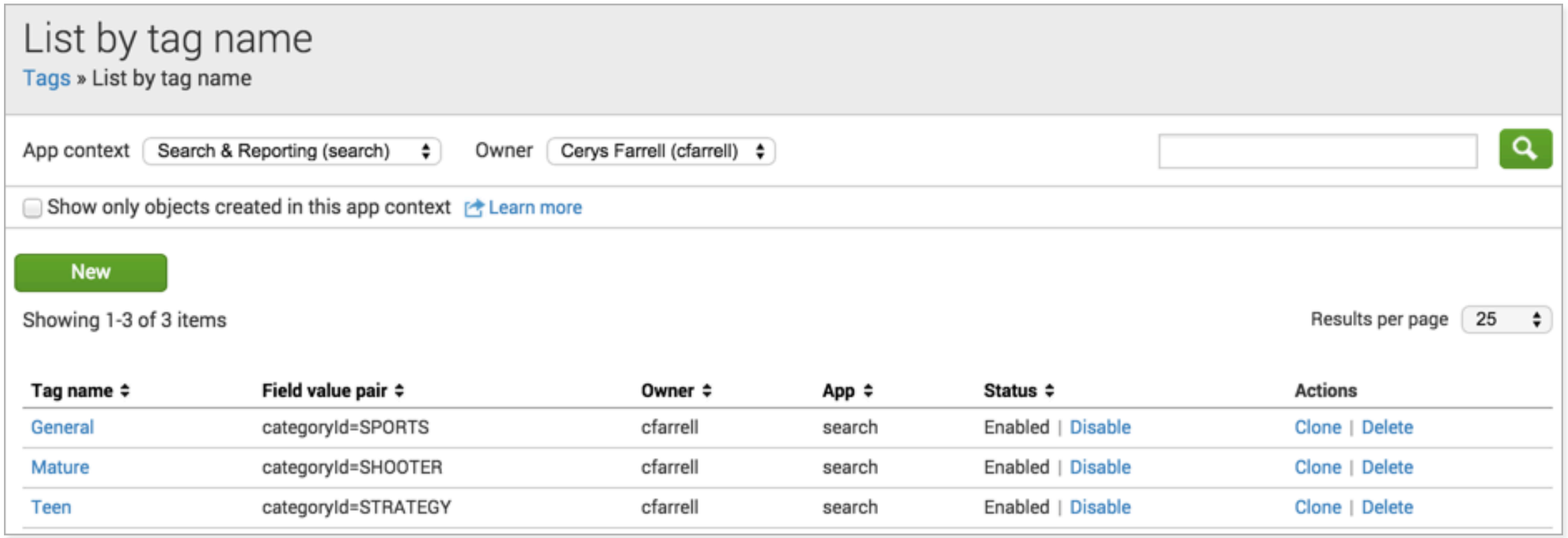
- Edit permissions
- Disable all tags for pair – disables the tag in searches and prevents it from being listed under **List by Tag Name** and **All unique tag objects**
- Clone
- Move
- Delete



Managing Tags (cont.)

Settings > Tags > List by tag name

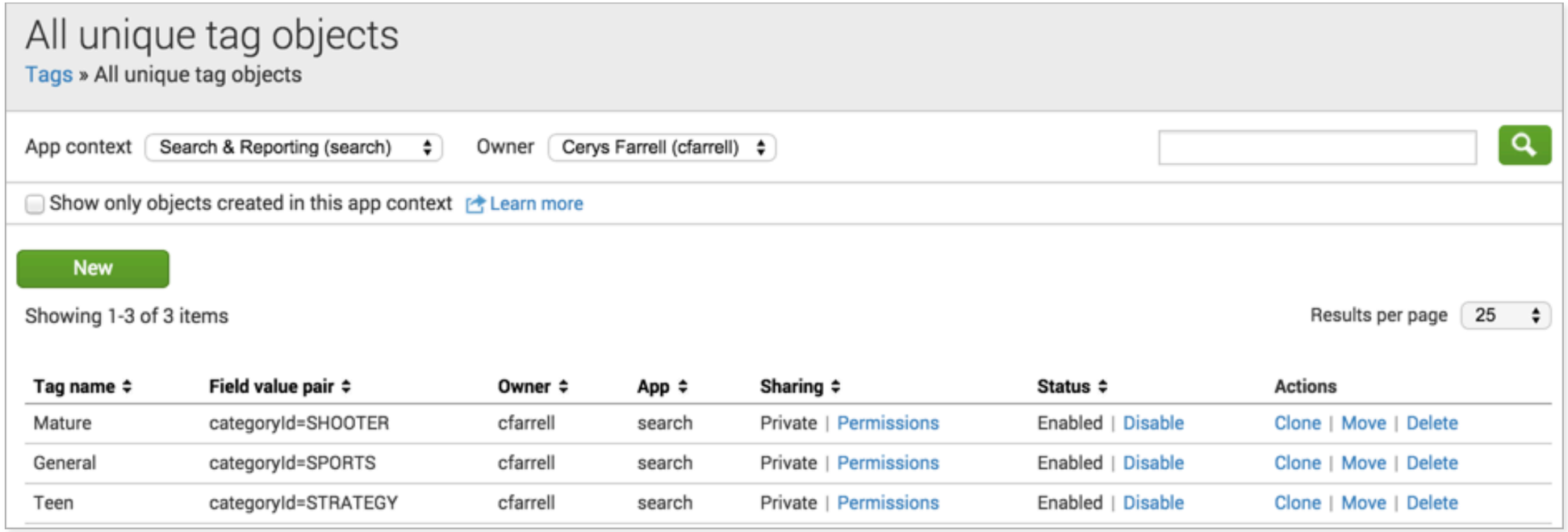
- Enable/Disable
- Clone
- Delete



Managing Tags (cont.)

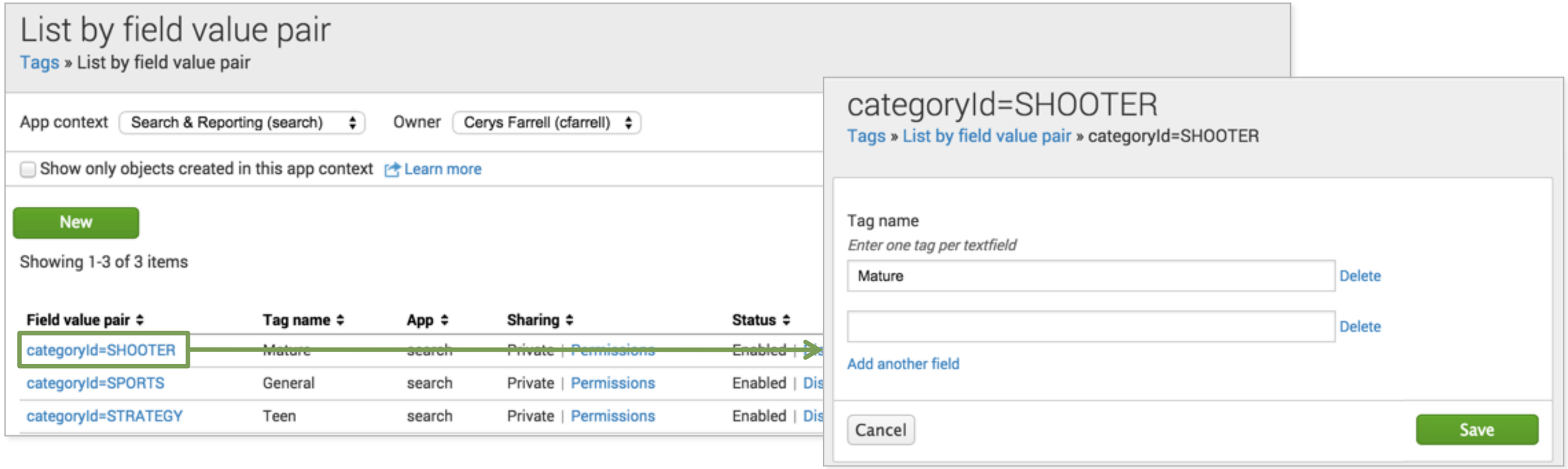
Settings > Tags > All unique tag objects

- Edit Permissions
- Enable/Disable
- Clone
- Move
- Delete



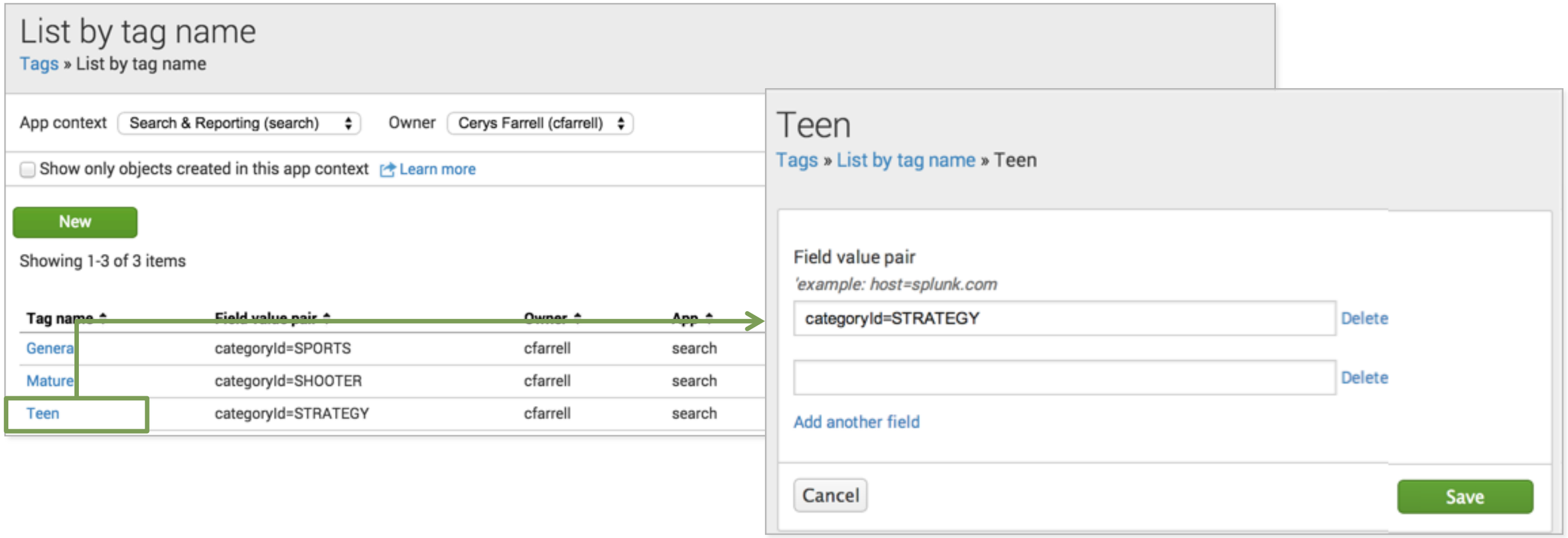
Adding/Changing the Tag Name

Click **List by field value pair** to add another tag or change the name of the tag



Adding/Changing the Field Value Pair

Click **List by tag name** to add or edit the field value pair for the tag



What is an Event Type?

- A method of categorizing events based on a search
- A useful method for institutional knowledge capturing and sharing
- Can be tagged to group similar types of events

Event Type Scenario

The sales team would like to track all online purchases by product type. An event type for each product category needs to be created:

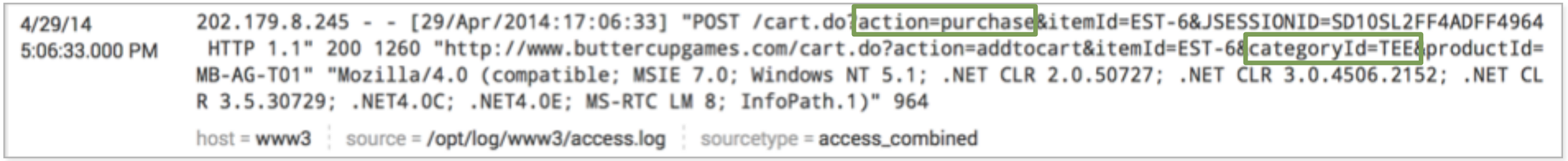
- Accessories
- Tees
- Arcade games
- Sports games
- Strategy games
- Shooter games

Event Type Example

To differentiate these events, create individual event types

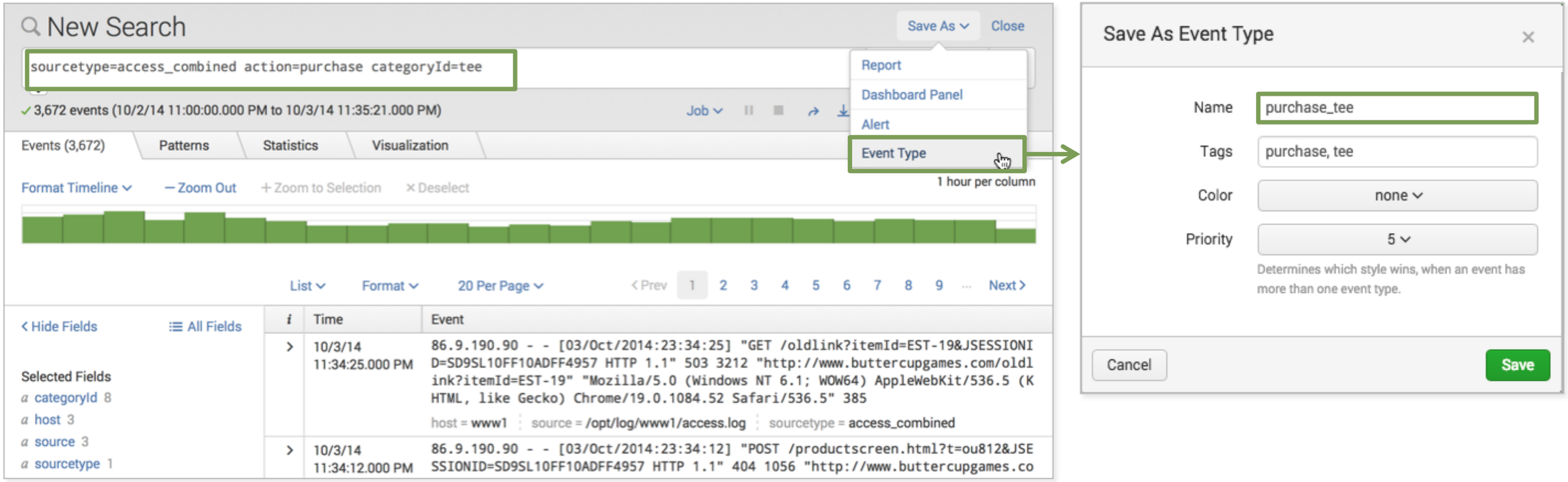
- purchase_accessories

- purchase_tee



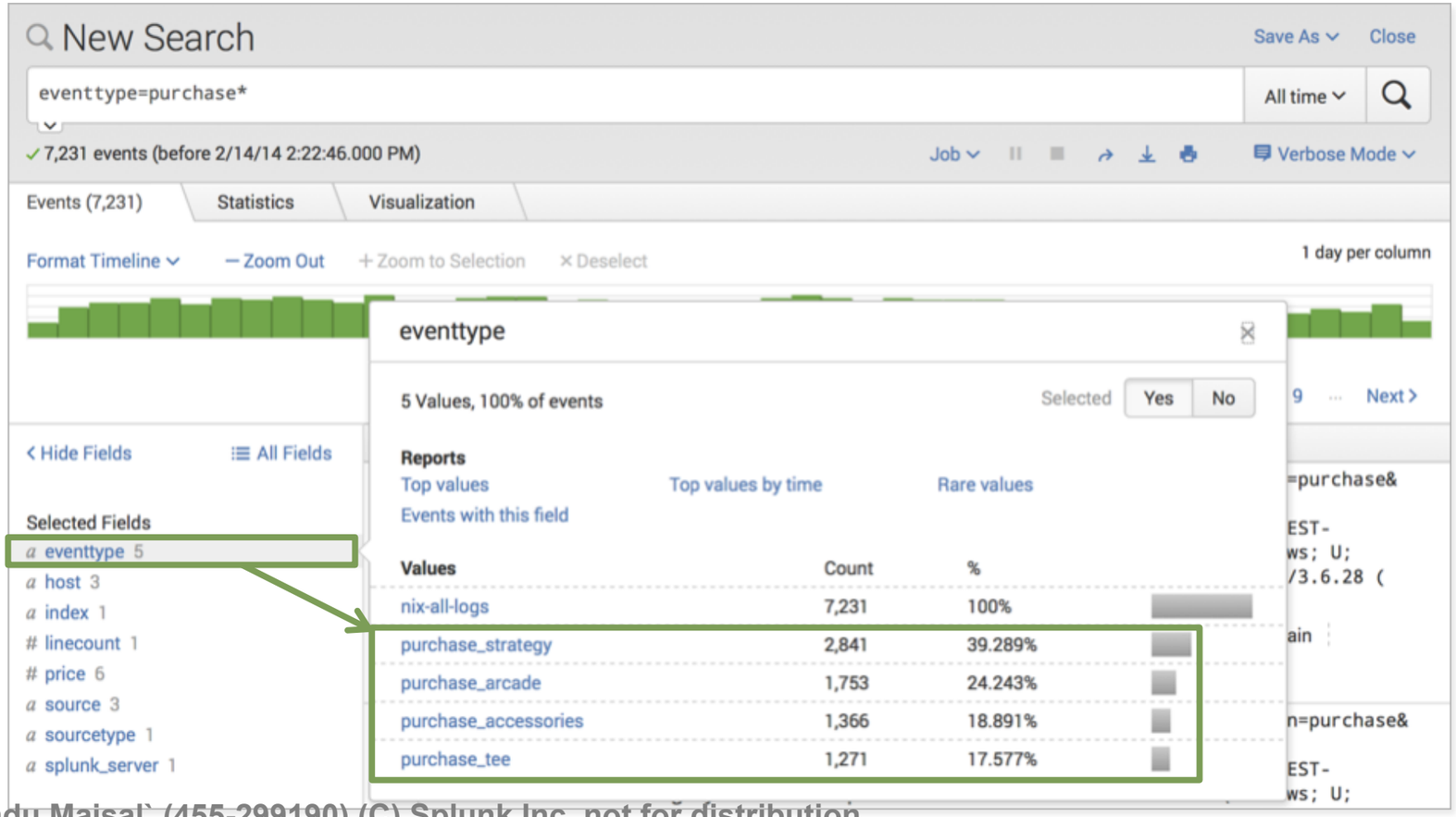
Creating an Event Type

1. Run a search and verify that all results meet your event type criteria
2. From the **Save As menu**, select **Event Type**
3. Provide a name for your event type (name should not contain spaces)



Using Event Types

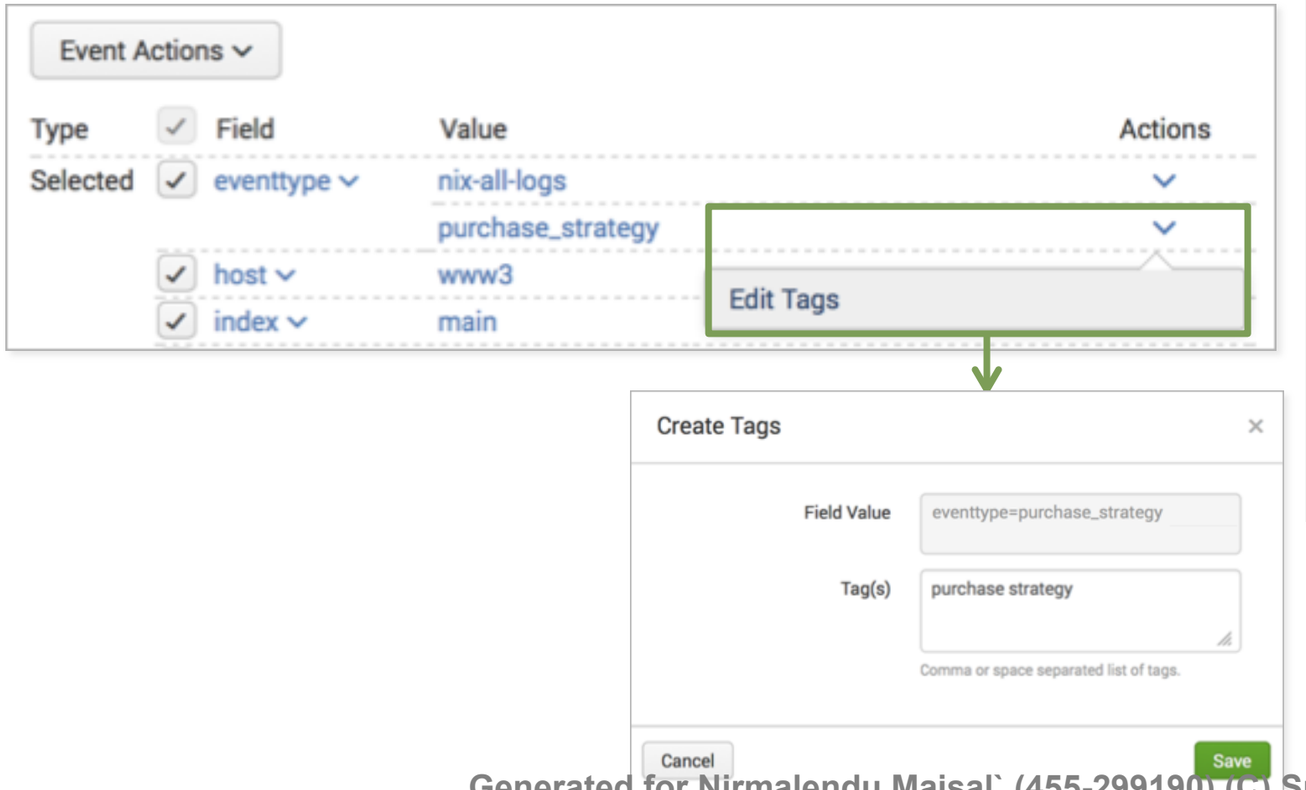
- To verify the event type, search for `eventtype=purchase*`
- 'eventtype' displays in the Fields sidebar and can be added as a selected field
- Splunk evaluates the events and applies the appropriate event types at search time
- Using the Fields sidebar, you can easily view the individual event types, the number of events, and percentage

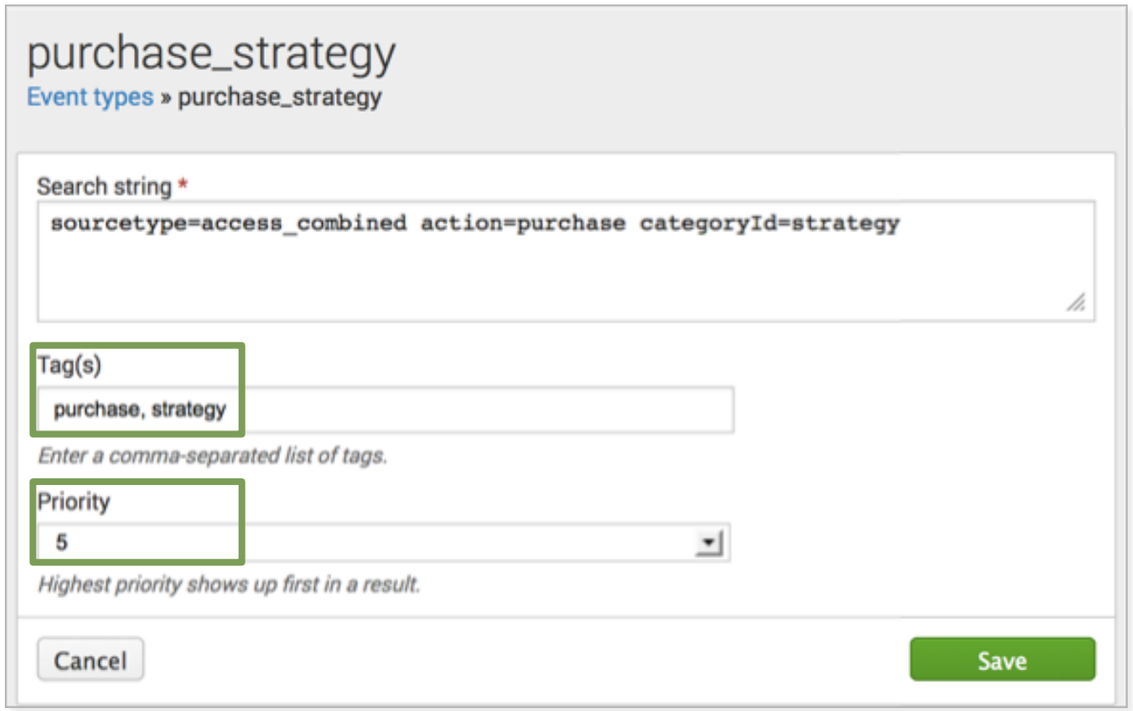


Tagging Event Types

You can tag event types two ways:

1. **Settings > Event Types**
2. **Event details > Actions**



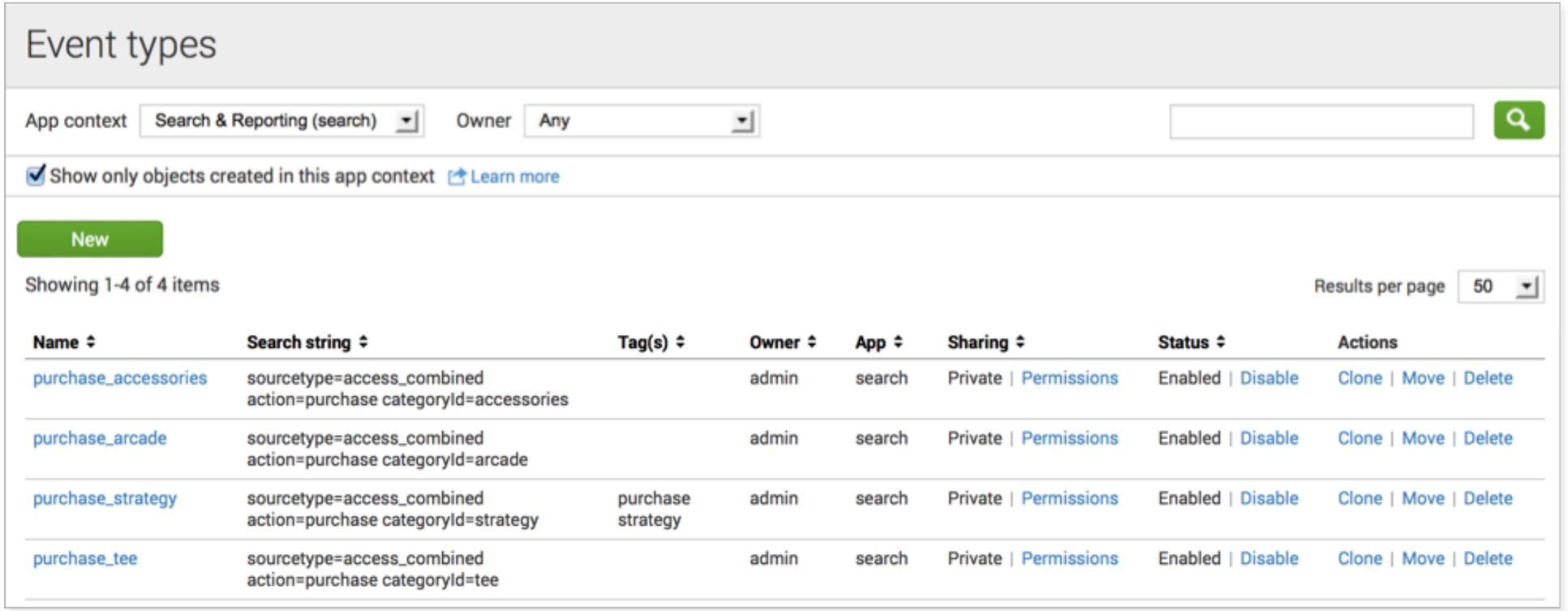


– The range for the priority is 1 (highest) to 10 (lowest)

Managing Event Types

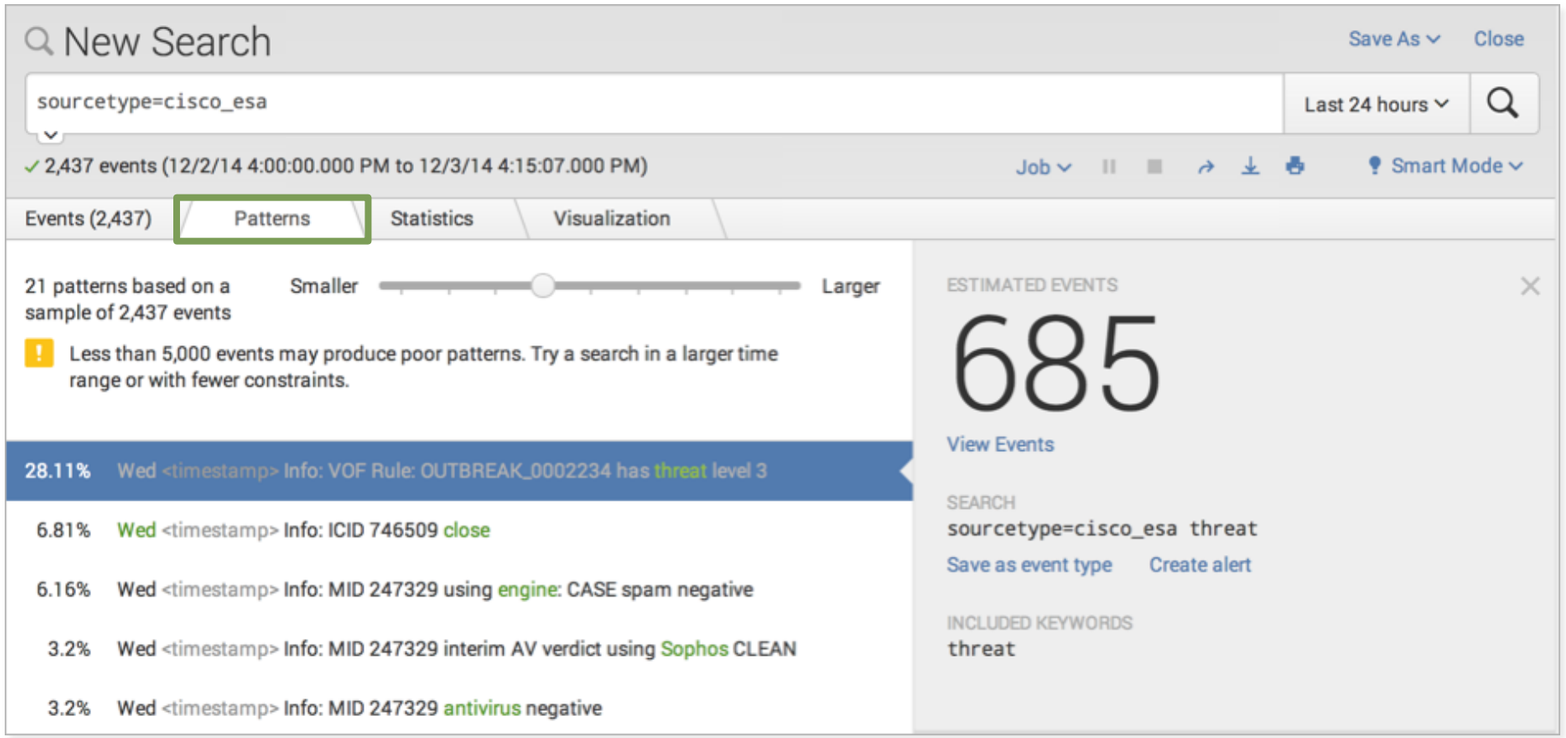
Settings > Event Types

- Edit permissions
- Enable/disable
- Clone
- Move
- Delete



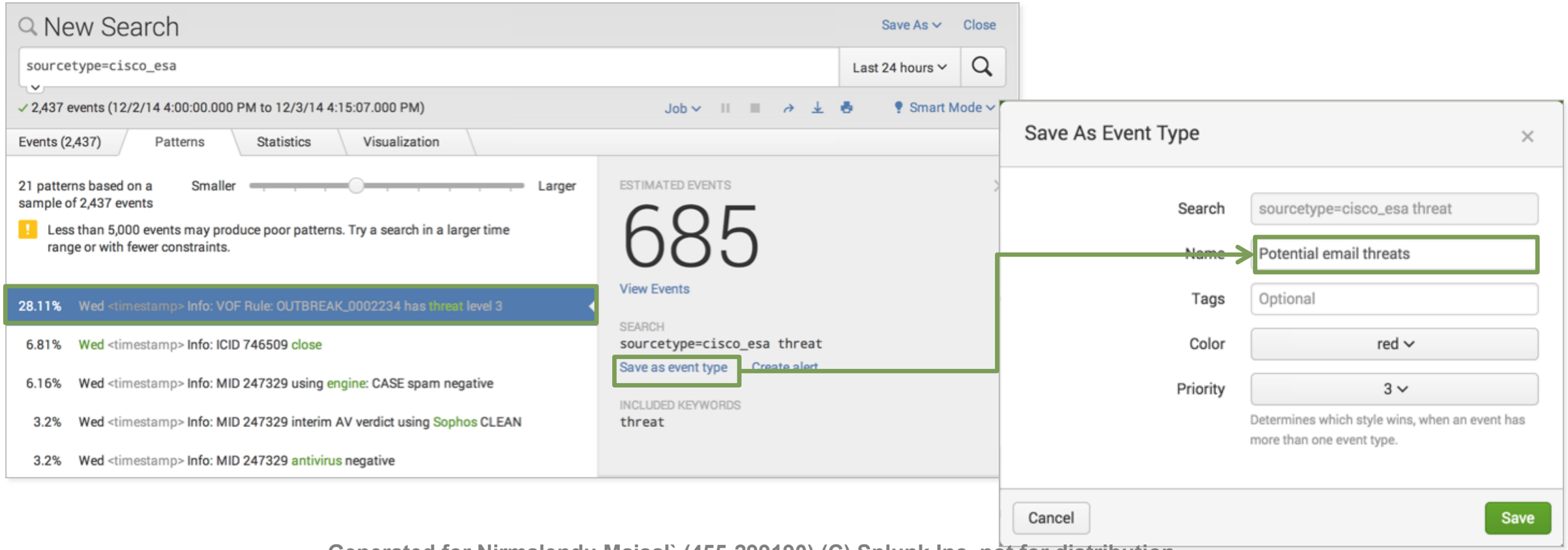
Creating an Event Type via Patterns

1. Run a search
2. Select the **Patterns** tab



Creating an Event Type via Patterns (cont.)

3. Select a pattern where the results meet your event type criteria
4. Click **Save as event type**



Event Types vs. Saved Reports

- Should I create an event type or a saved report?
  - Event Types
    - Categorize events based on a search string
    - Tag event types to organize data into categories
    - The `eventtype` field can be included in a search string
    - Does not include a time range
  - Saved Reports
    - Search criteria will not change
    - Includes a time range and formatting of the results
    - Share reports with Splunk users and may be added to dashboards

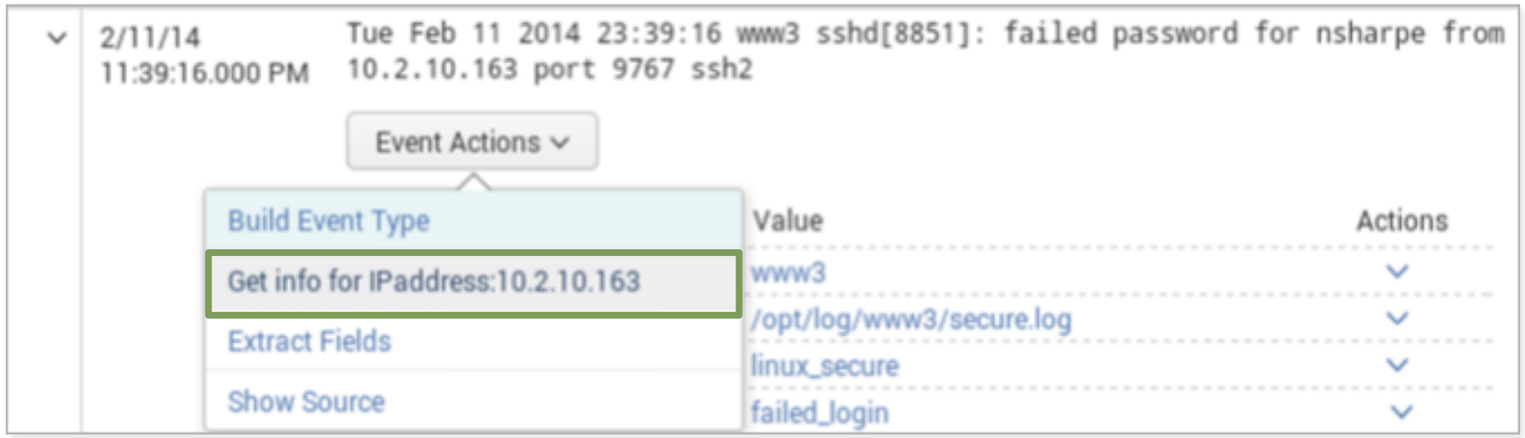
Module 6:
Creating Workflow Actions

Module Objectives

- Create a GET workflow action
- Create a POST workflow action
- Create a Search workflow action

What are Workflow Actions?

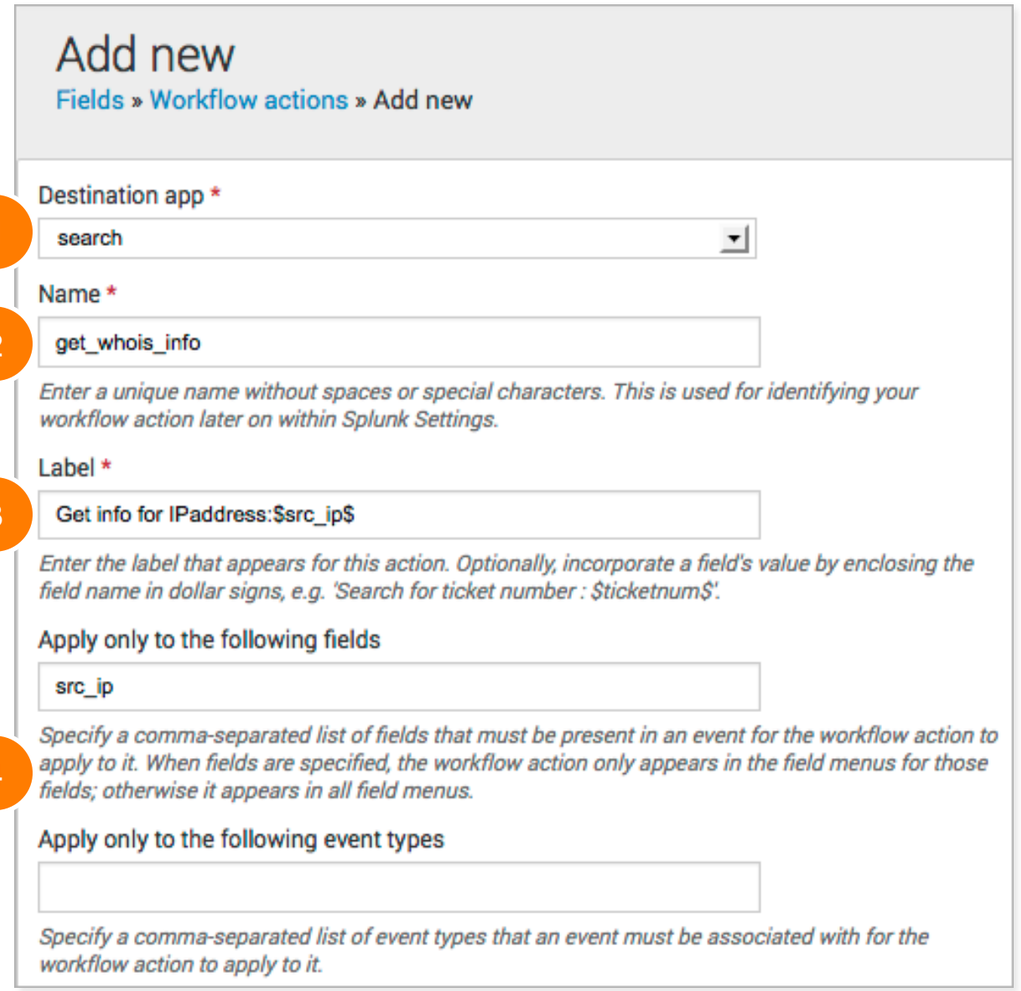
- Execute workflow actions from an event in your search results to interact with external resources or run another search
  - **GET** - pass information to an external web resource
  - **POST** - send field values to an external resource
  - **Search** - use field values to perform a secondary search



Creating a GET Workflow Action

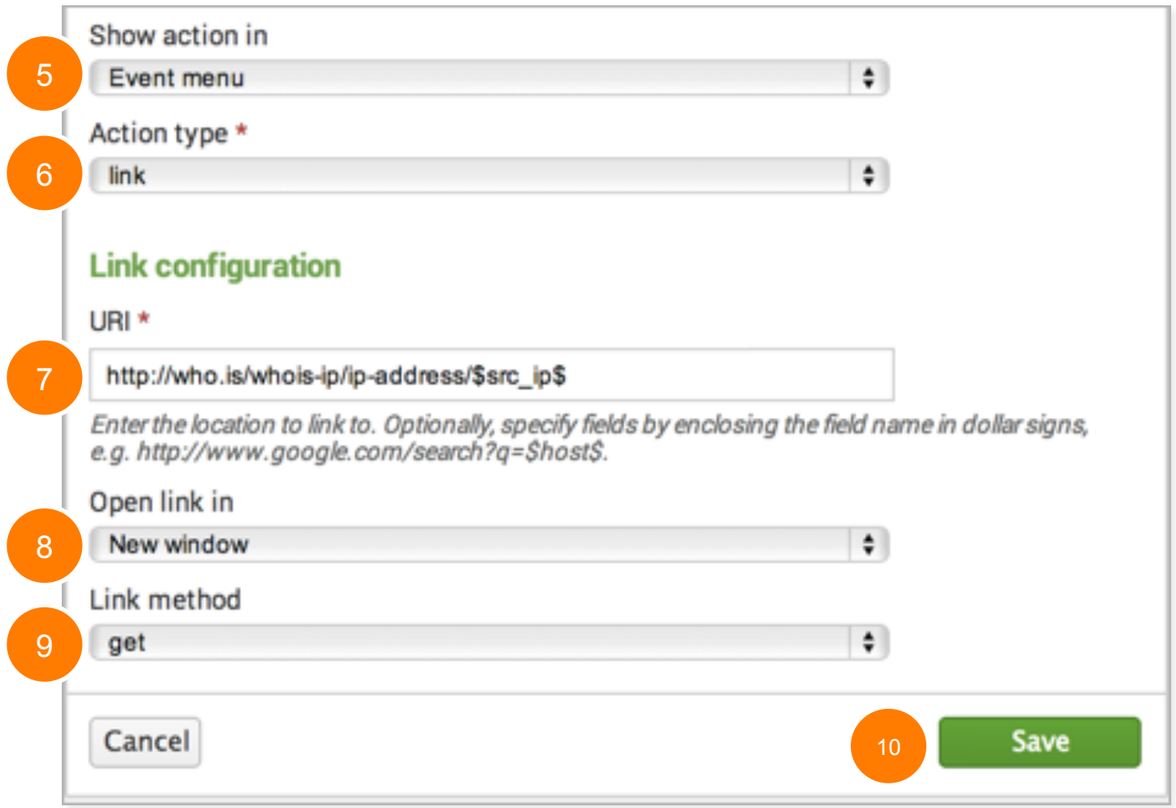
Settings > Fields > Workflow actions > New

1. Select the app
2. Name the workflow action with no spaces or special characters
3. Define the label, which will appear in the Event Action menu
4. Determine if your workflow action applies to a field or event type



Creating a GET Workflow Action (cont.)

5. From the **Show action in** drop down list, select **Event menu**
6. Select **link** as the **Action type**
7. Enter the URI of where the user will be directed
8. Specify if the link should open in a New window or Current window
9. Select the Link method of **get**
10. Save

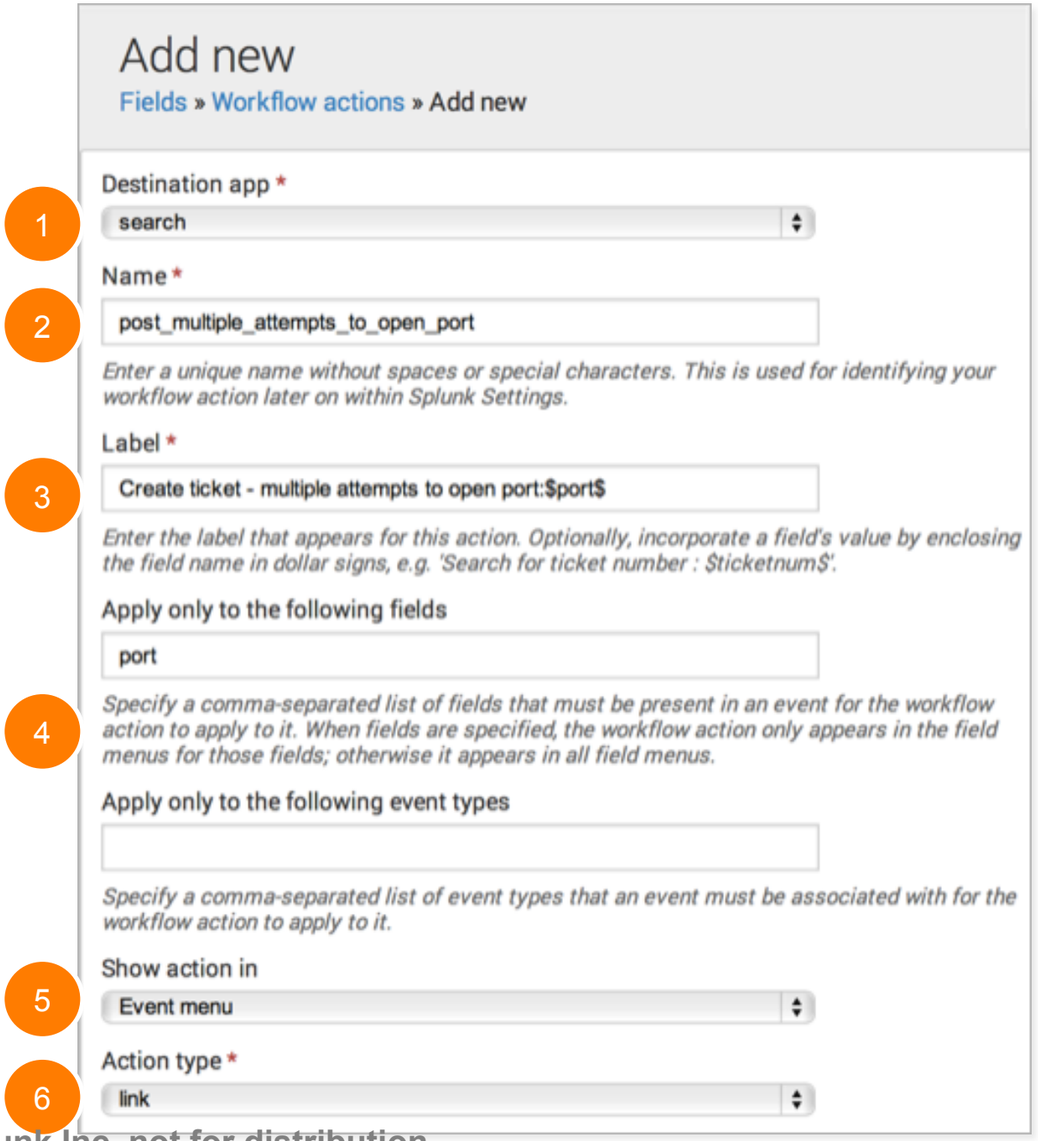


Testing the GET Workflow Action

Creating a Post Workflow Action

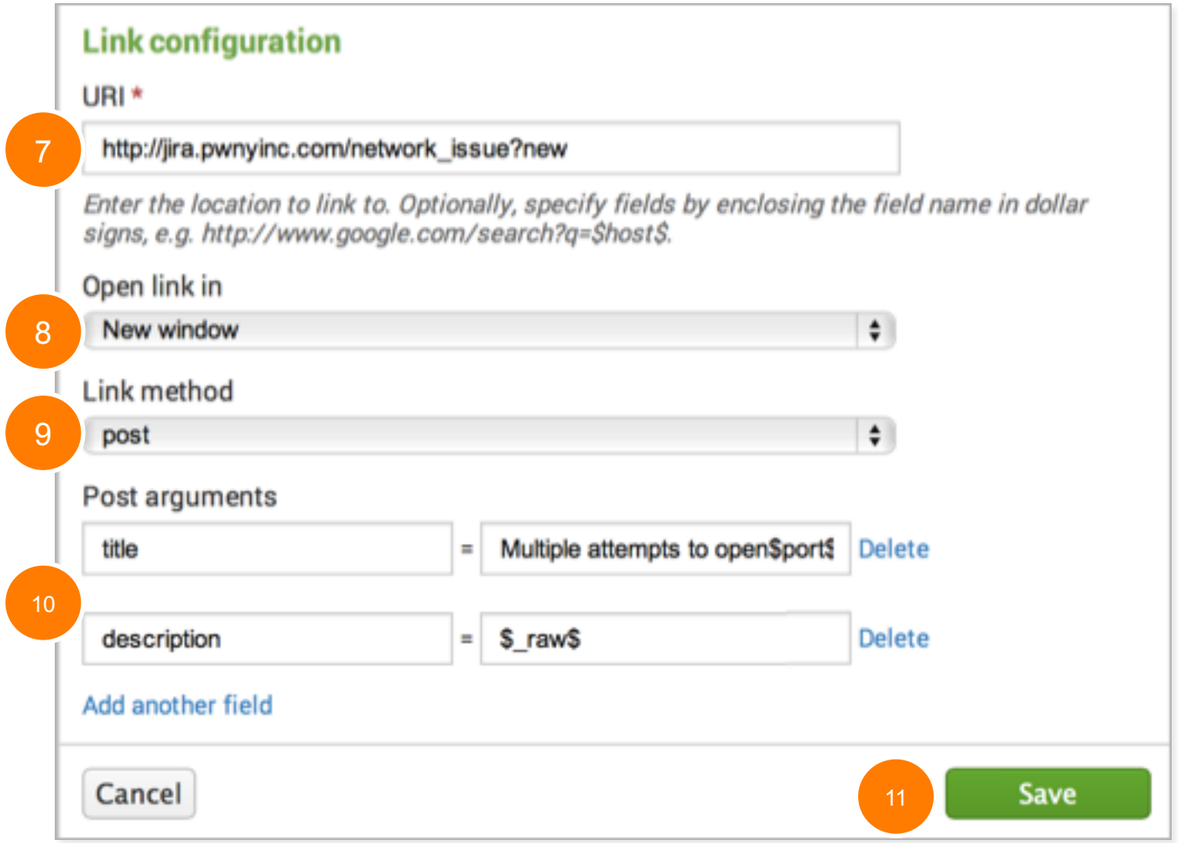
Settings > Fields > Workflow actions > New

Complete steps 1 – 6 as described in the previous example, Creating a GET Workflow Action



Creating a Post Workflow Action (cont.)

7. Enter the URI of where the user will be directed
8. Open the link in a **New window** or Current window
9. Select the Link method of **post**
10. Provide post argument parameters
11. Save

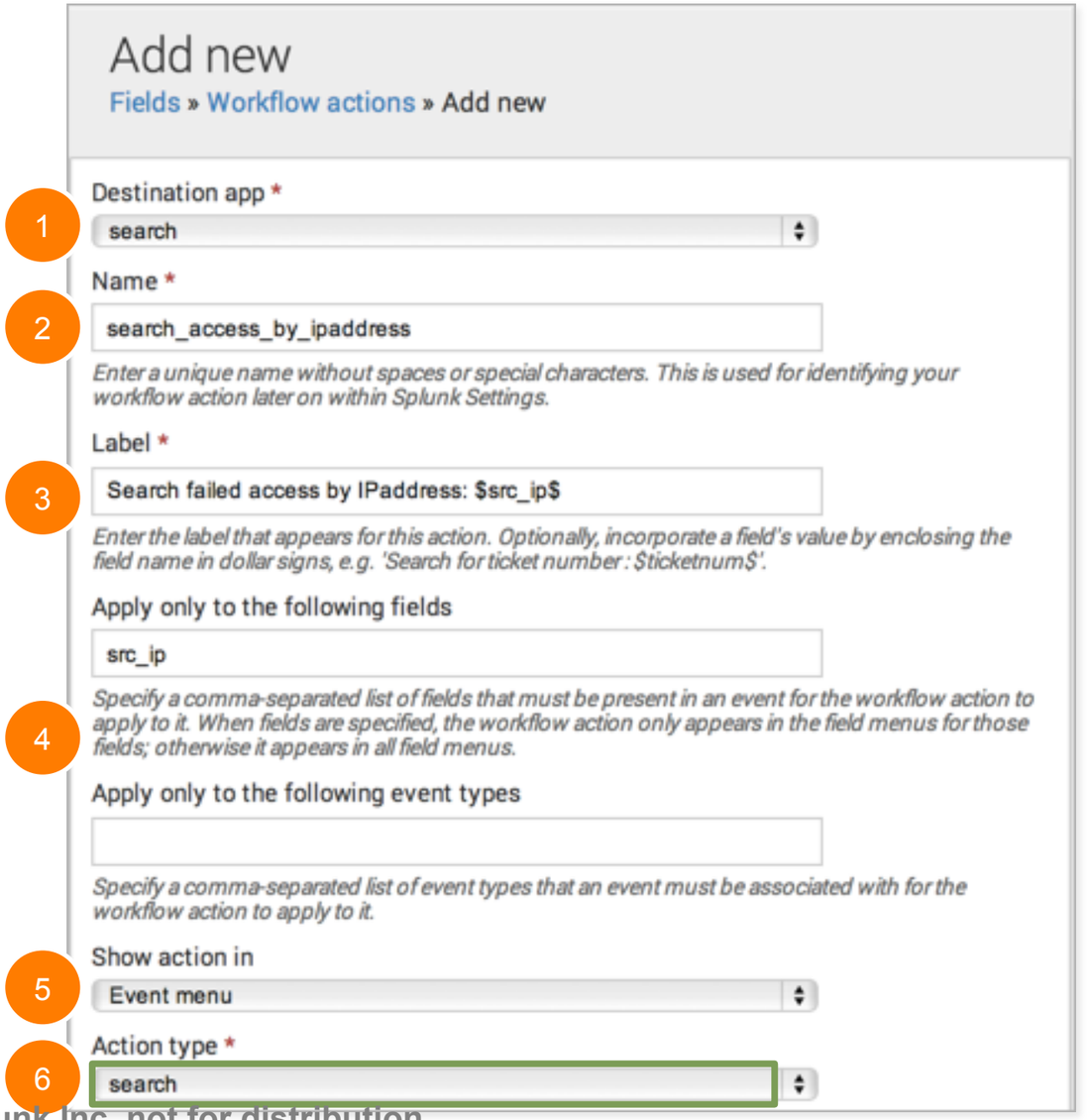


Creating a Search Workflow Action

Settings > Fields > Workflow actions> New

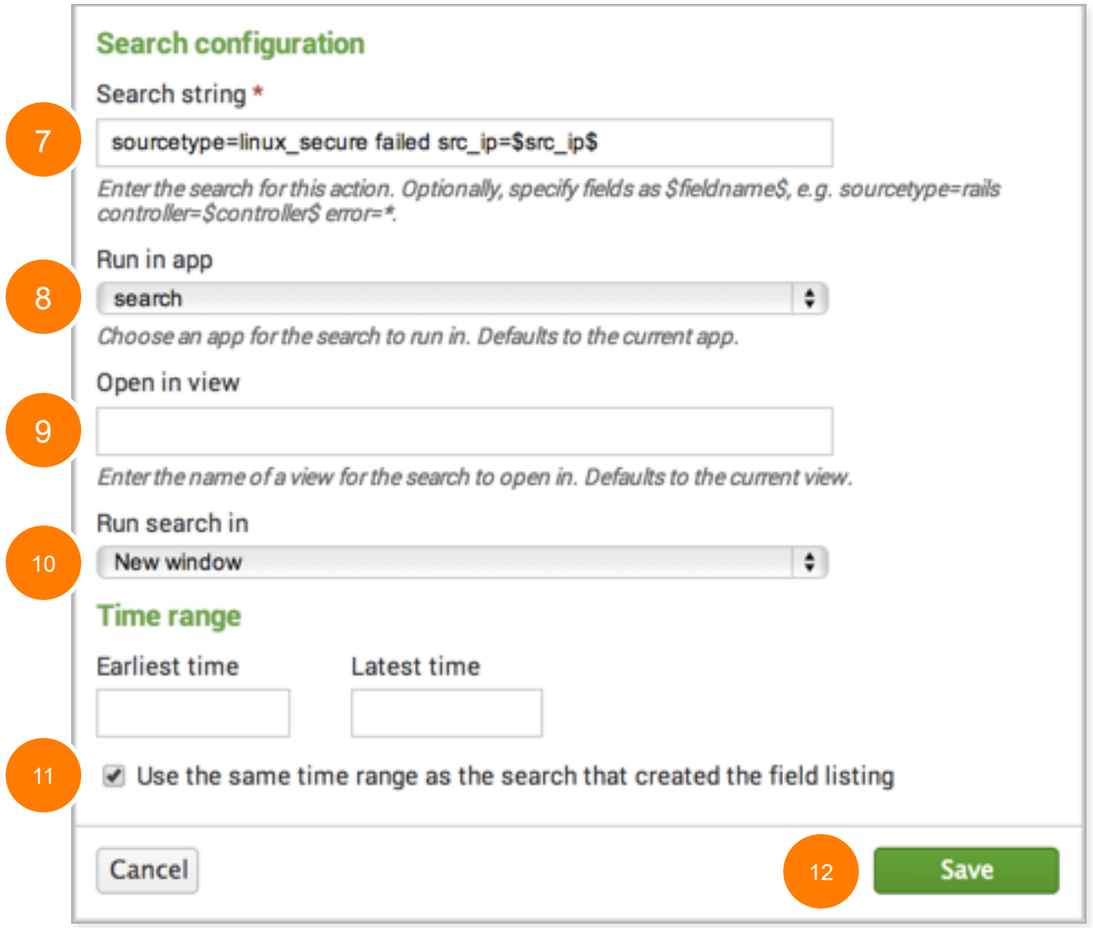
Complete steps 1 – 5 as described in the previous example, Creating a GET Workflow Action

6. Select **search** as the Action type

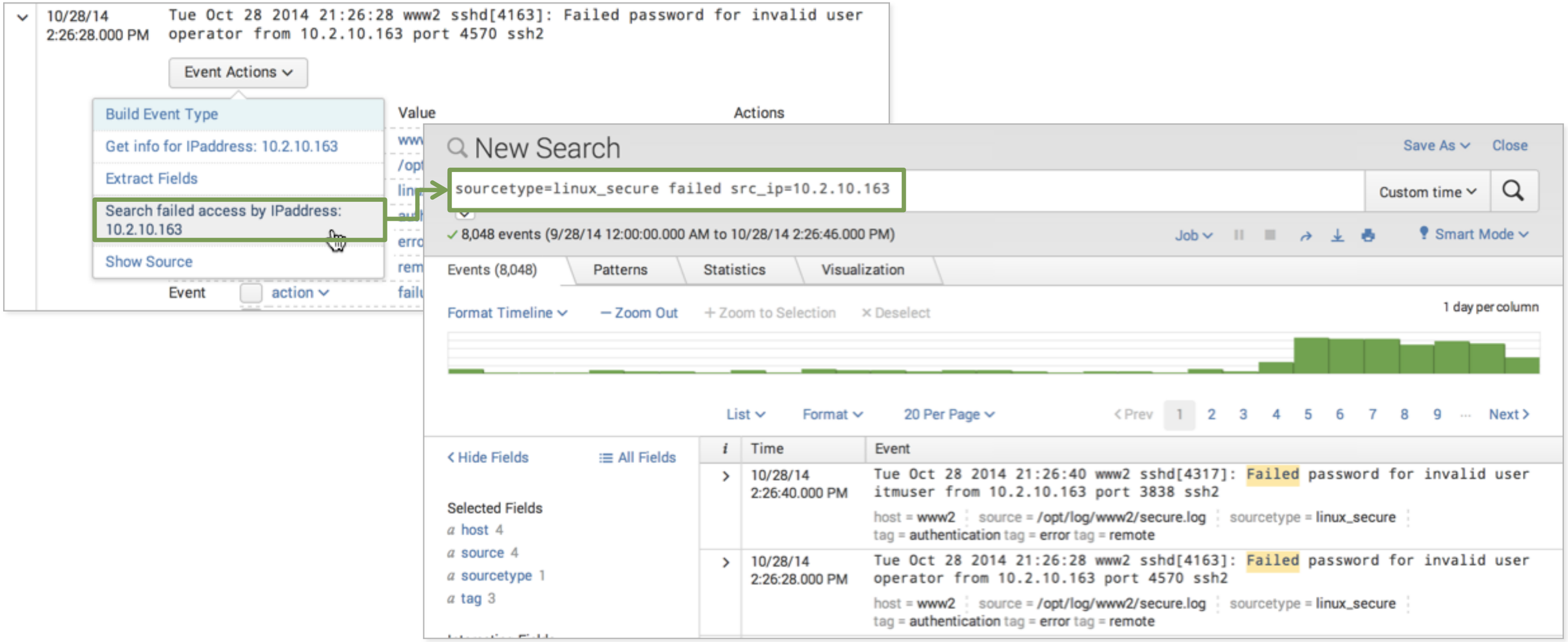


Creating a Search Workflow Action (cont.)

7. Enter the Search string
8. Select the app if it is different from the current app
9. Enter the view name where the search will execute
10. Indicate if the search should run in a New window or the Current window
11. Enter the time range for the search or choose to use the same time range as the search
12. Save



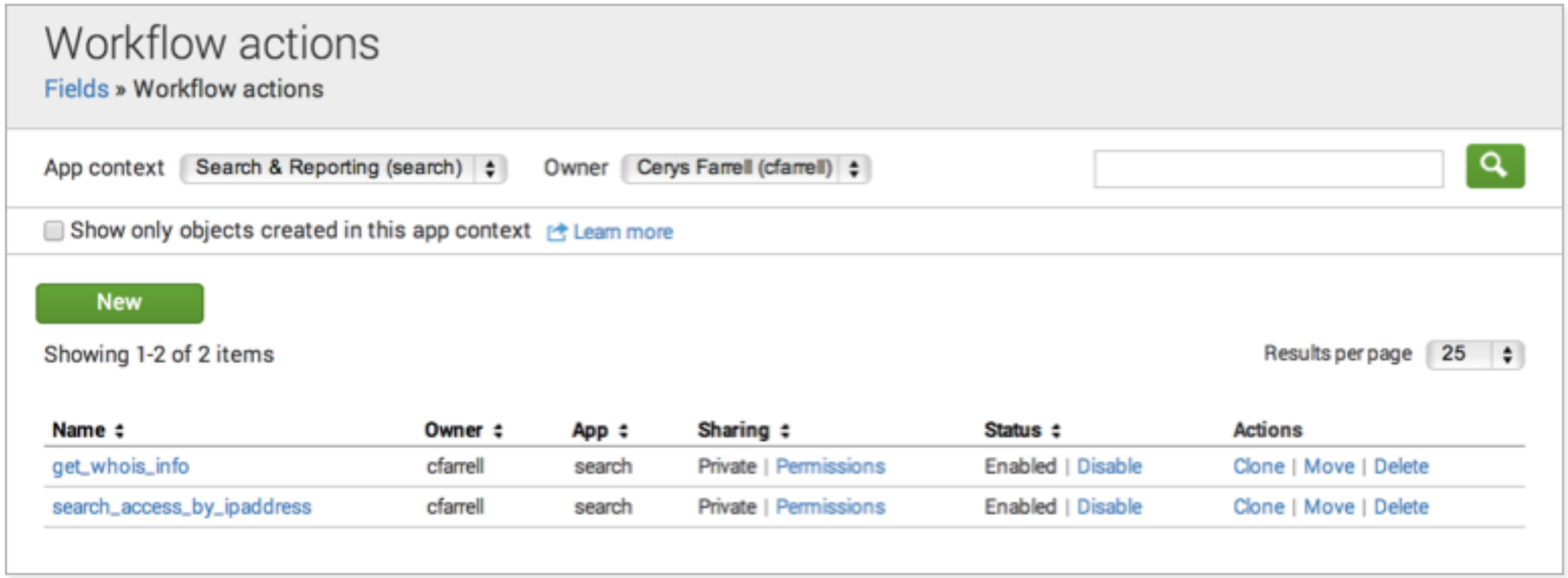
Testing the Search Workflow Action



Managing Workflow Actions

Settings > Fields > Workflow actions

- Edit permissions
- Enable / disable
- Clone
- Move
- Delete



Module 7: Creating Alerts and Scheduled Reports

Module Objectives

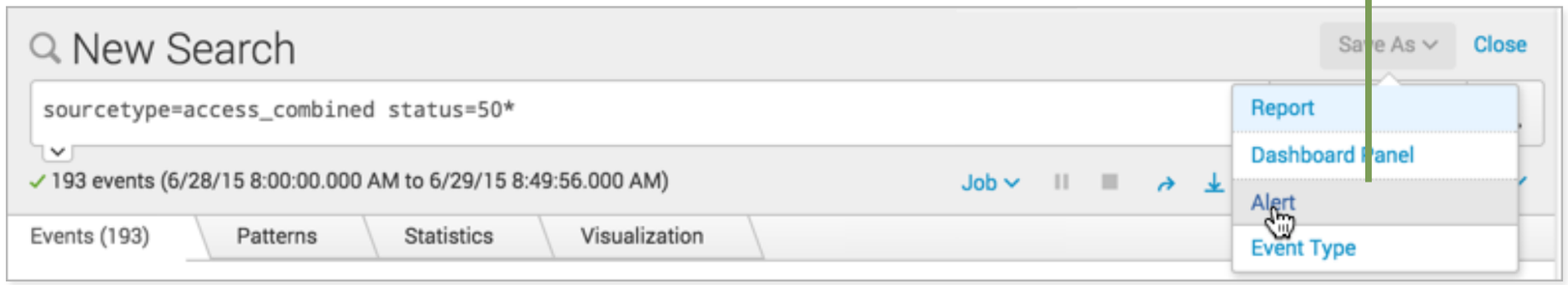
- Describe alerts and scheduled reports
- Create alerts and scheduled reports
  - Run the underlying search
  - Set the schedule, conditions, and actions
- View fired alerts and scheduled reports

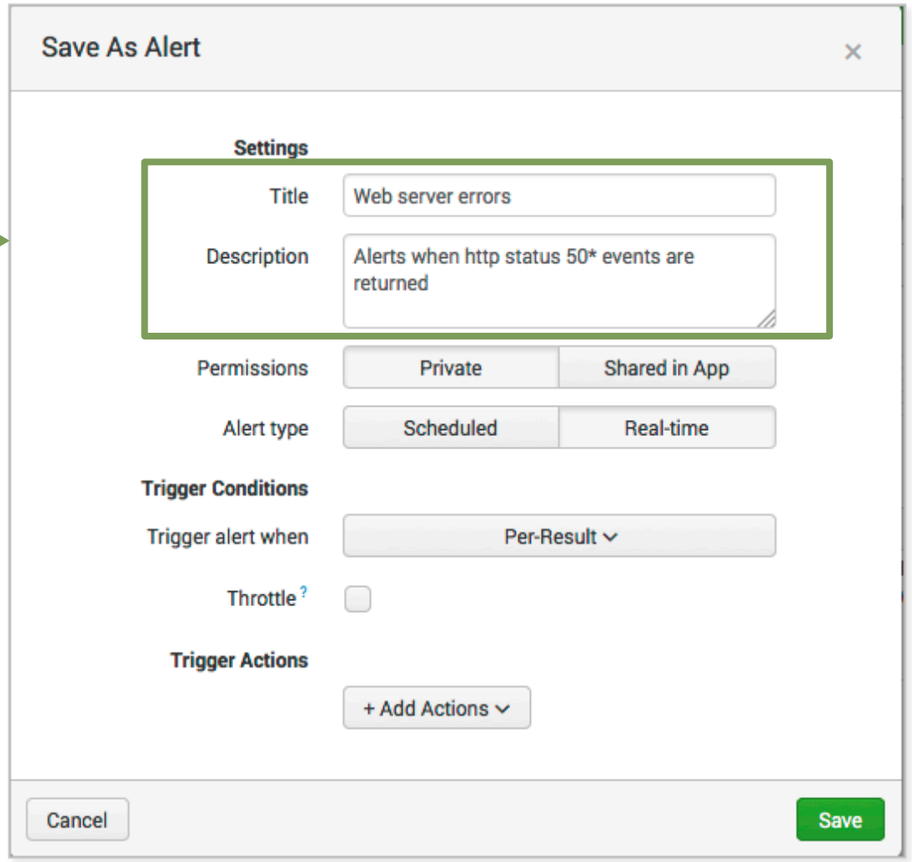
Alerting Overview

- Splunk alerts are based on searches that can run either:
  - On a regular **scheduled interval**
  - In **real-time**
- Alerts are triggered when the results of the search meet a specific condition that you define
- Based on your needs, alerts can:
  - List in triggered alerts
  - Send emails
  - Trigger scripts
  - Use a webhook
  - Run a custom alert

Creating an Alert

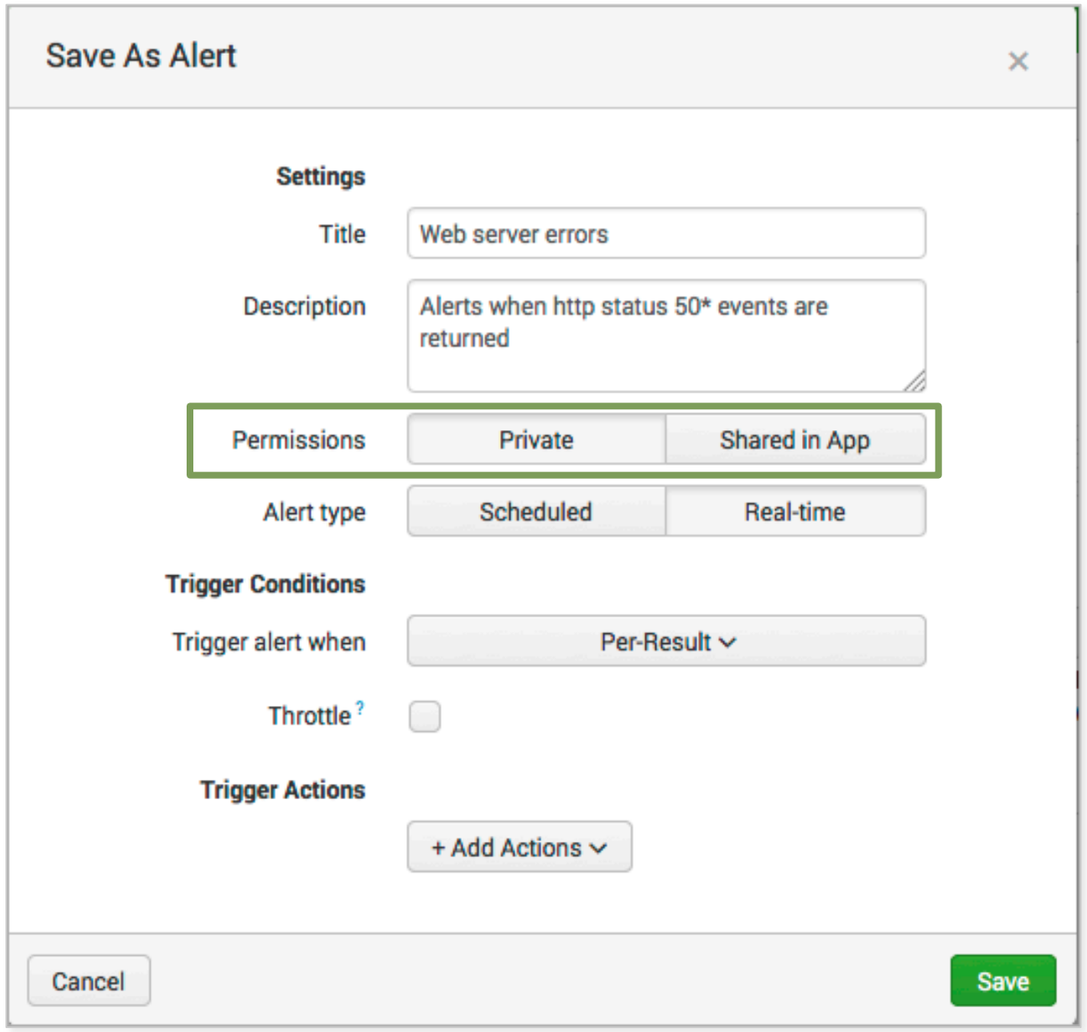
- Run a search
  - In this example, you're searching for server errors: any http request status that begins with 50 over the last 5 minutes
- Select **Save As** > **Alert**
- Give the alert a Title and Description





Setting Alert Permissions

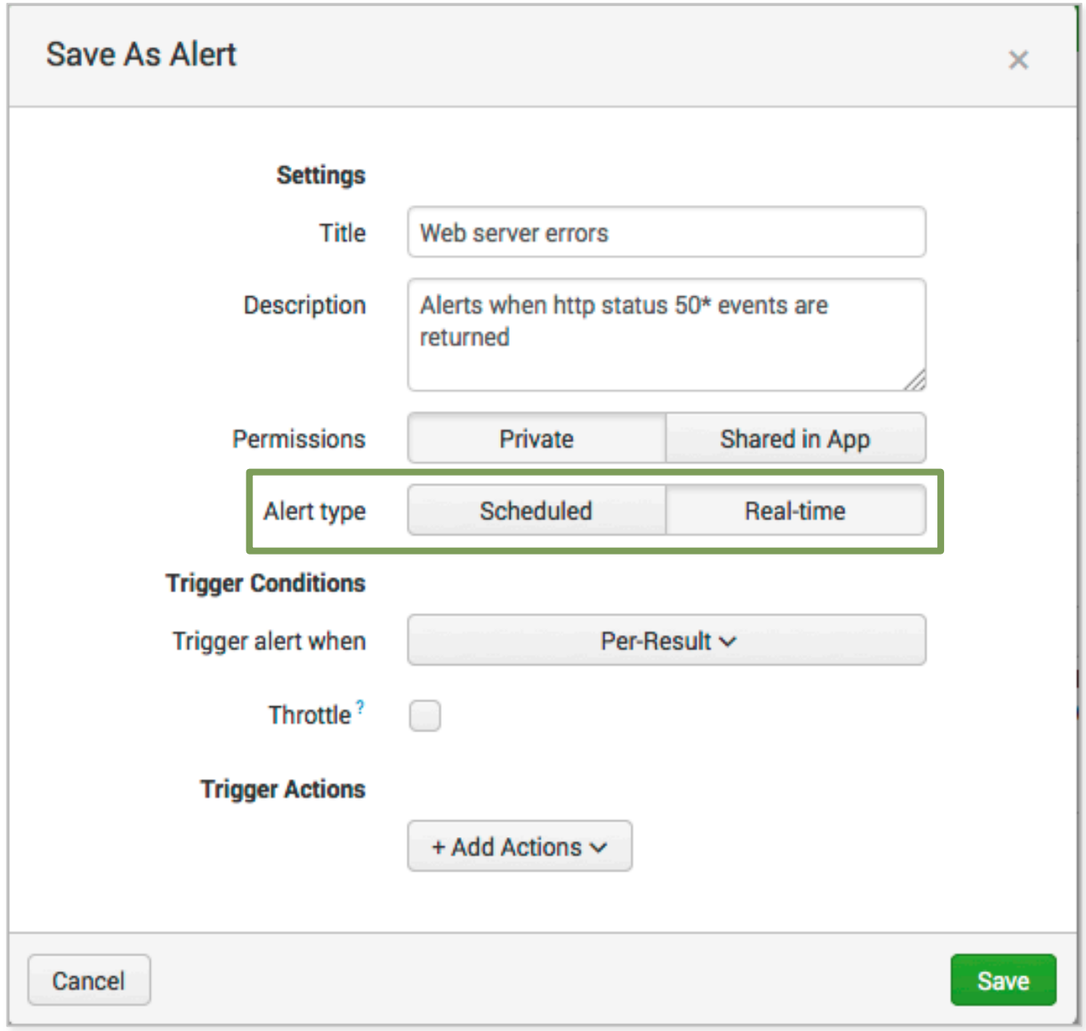
- Set the alert permissions
  - **Private** – only you can access, edit, and view triggered alerts
  - **Shared in app**
    - All users of the app can view triggered alerts
    - By default, everyone has read access and power has write access to the alert



Choosing Real Time or Scheduled Alert Type

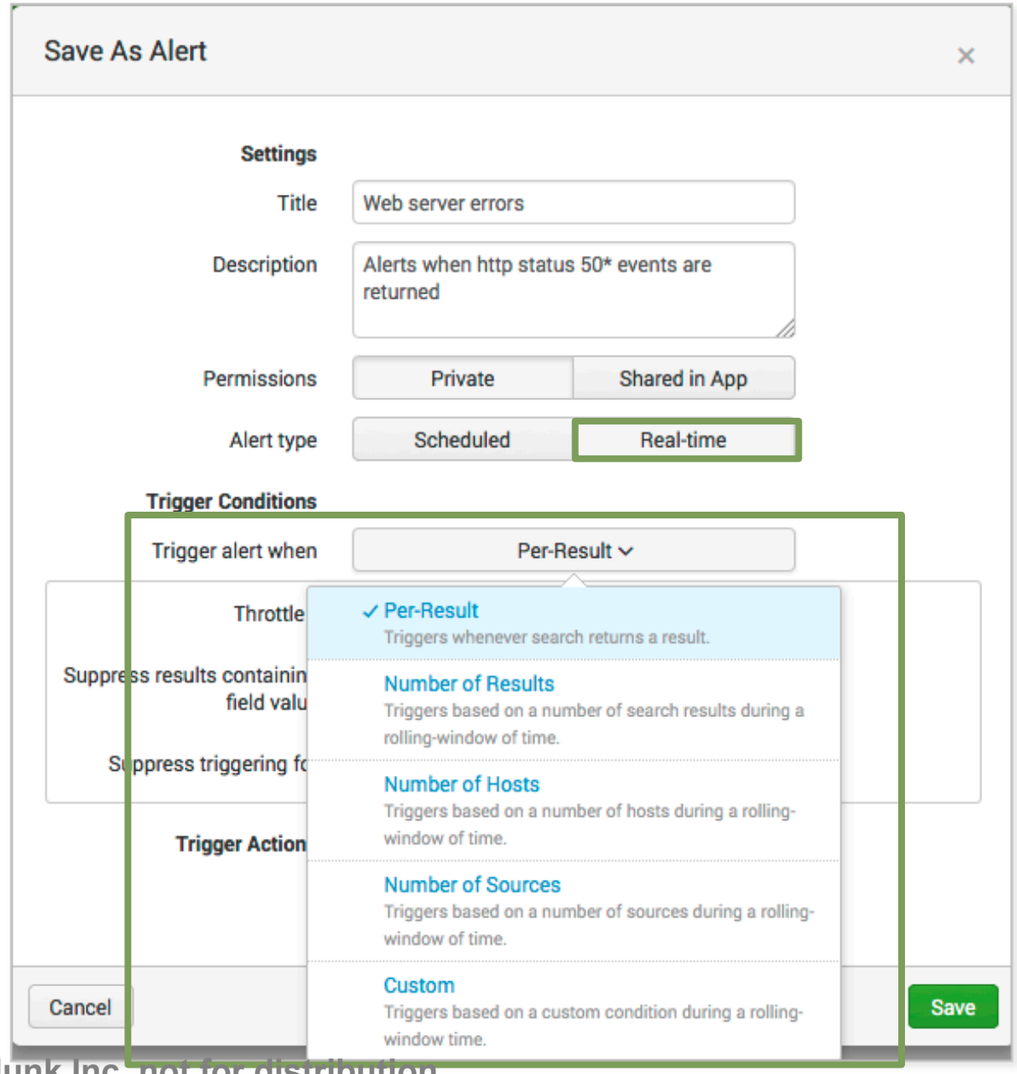
Choose an **Alert type** to determine how Splunk searches for events that may match your alert

- **Real-time** alerts
  - Search runs constantly in the background
  - Evaluates trigger conditions within a window of time based on the conditions you define
- **Scheduled** alerts
  - Search runs at a defined interval
  - Evaluates trigger condition when the search completes



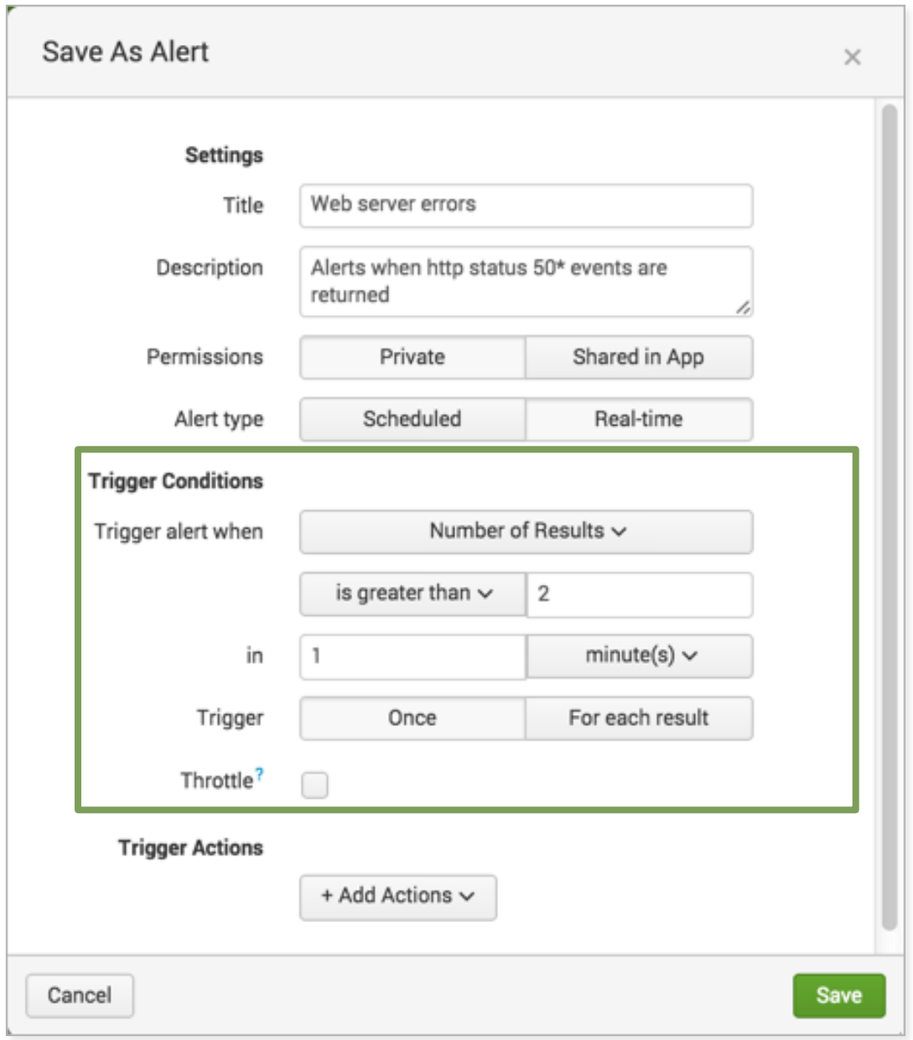
Setting Trigger Conditions – Real-time

- Trigger conditions allow you to capture a larger data set, then apply more stringent criteria to results before executing the alert
- You can set alerts to trigger:
  - **Per Result –** triggers when a result is returned
  - **Number of Results** – define how many results are returned before the alert triggers
  - **Number of Hosts** – define how many unique hosts are returned before the alert triggers
  - **Number of Sources** – define how many unique sources are returned before the alert triggers
  - **Custom** – define custom conditions using the search language



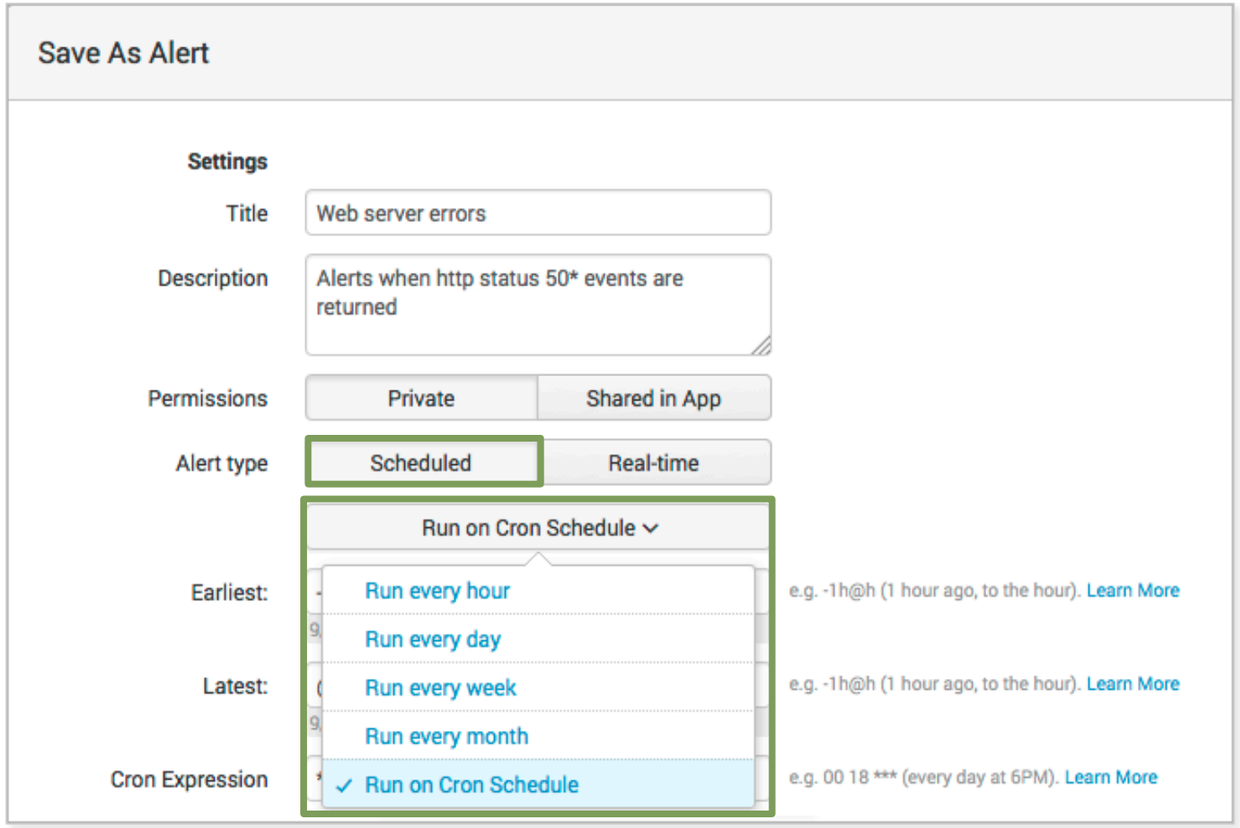
Setting Trigger Conditions – Real-time (cont.)

- In this example, the trigger condition is set to **Number of Results**
- In this **Real Time** alert example, if the number of results is greater than **2** within **1** minute, the alert triggers



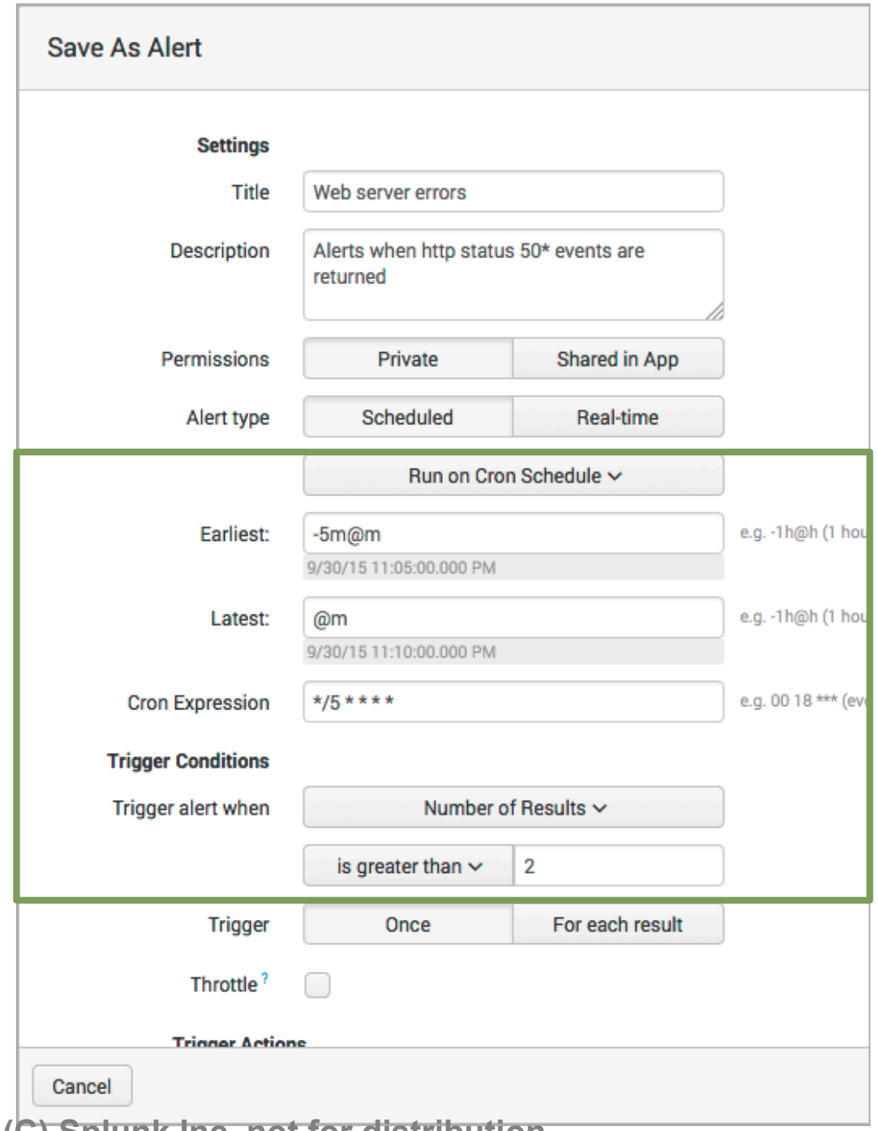
Setting the Alert Type – Scheduled

- From the frequency menu, choose to run the search every hour, day, week, month, or on a cron schedule
  - For the scheduled interval options, select the time the search will run
  - For cron schedule, define the cron expression



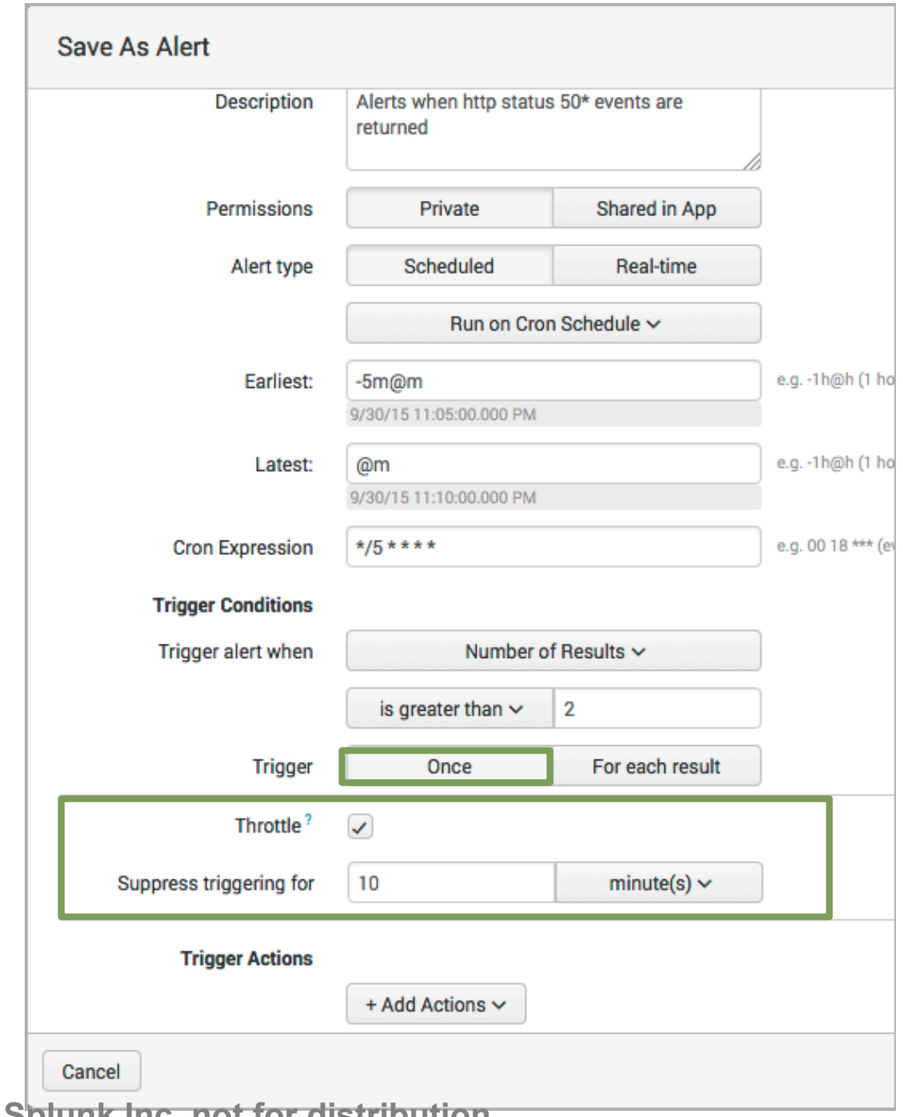
Setting Trigger Conditions – Scheduled

- For the cron schedule, enter the **earliest** and **latest** values to define the time range of the results
- Set trigger conditions for scheduled alerts (same steps outlined for real-time alerts)
  - The alert examines the complete results set after the search is run



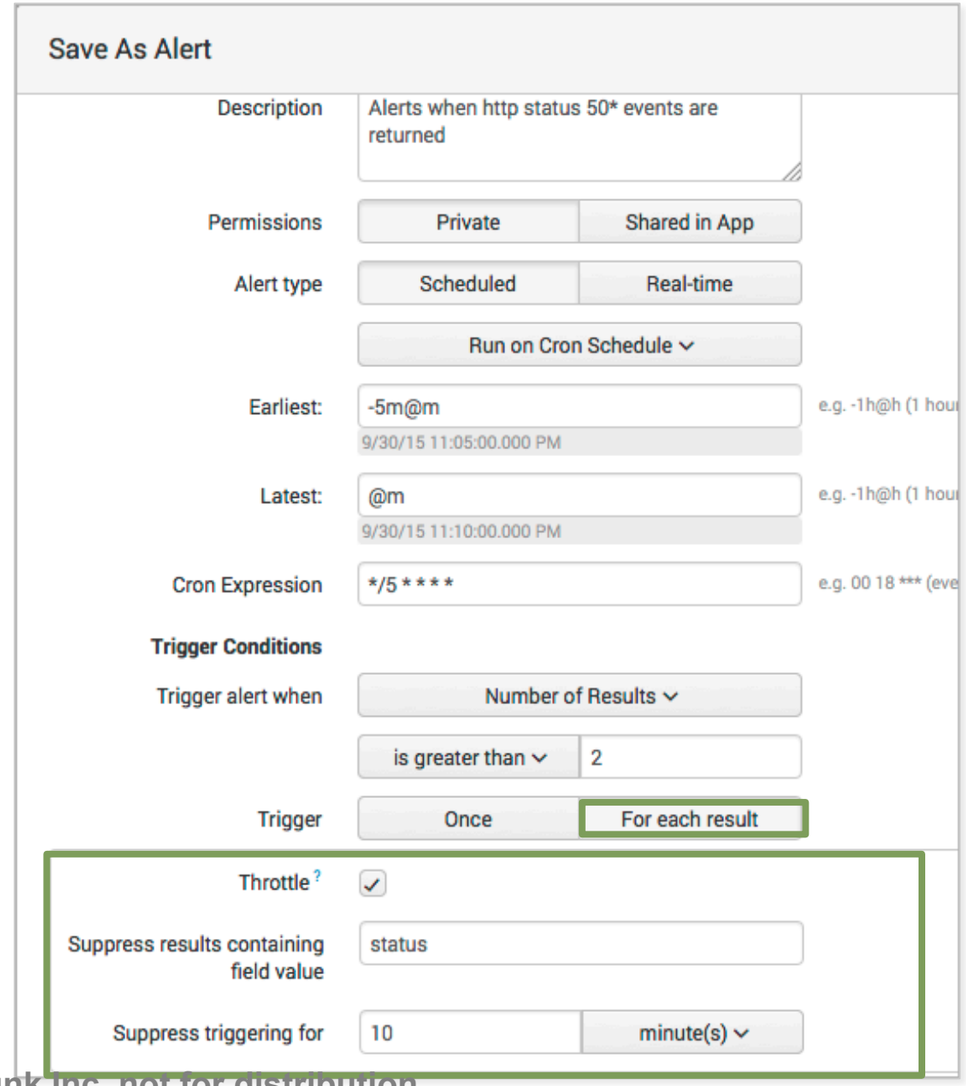
Alert Actions – Trigger Conditions: Once

- **Once** executes actions *one time* for all matching events within the scheduled time and conditions
  - Example: If your alert is scheduled to run every 30 seconds, and 40 results are returned, the alert only triggers and executes actions one time
- Select the **Throttling** option to suppress the actions for results within a specified time range



Alert Actions – Trigger Conditions: For Each Result

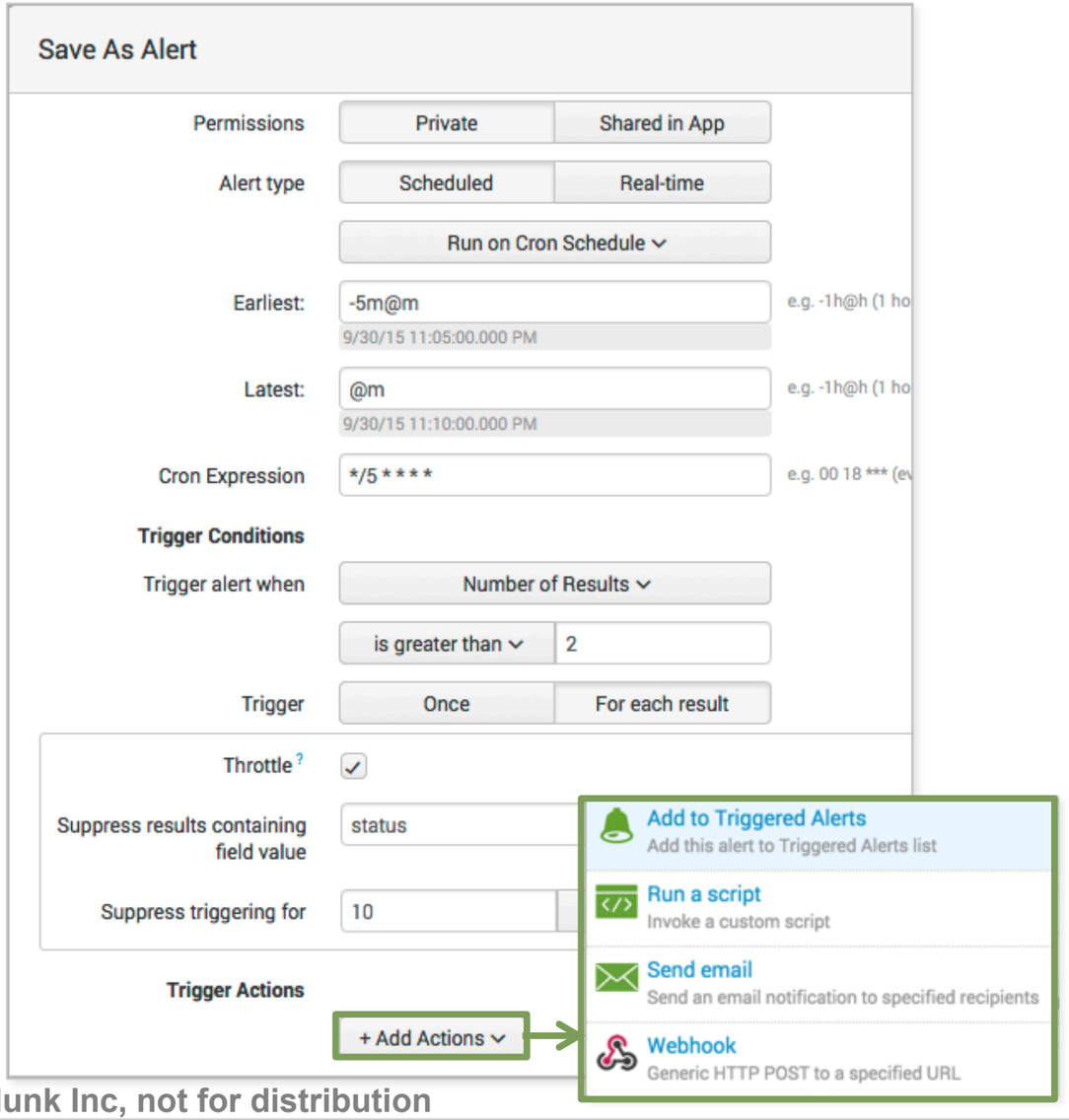
- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the **Throttling** option to suppress the actions for results that have the same field value, within a specified time range
  - Certain situations can cause a flood of alerts, when really you only want one
- Example: In a real time alert, only execute the actions once per status value for the next 30 seconds
  - 70 results are returned in a 1 minute window
  - 50 results include status=**500** and 20 include status=**503**
  - Actions would execute 4 times – once for each of the 2 status values, every 30 seconds



Add Trigger Actions

Add Actions

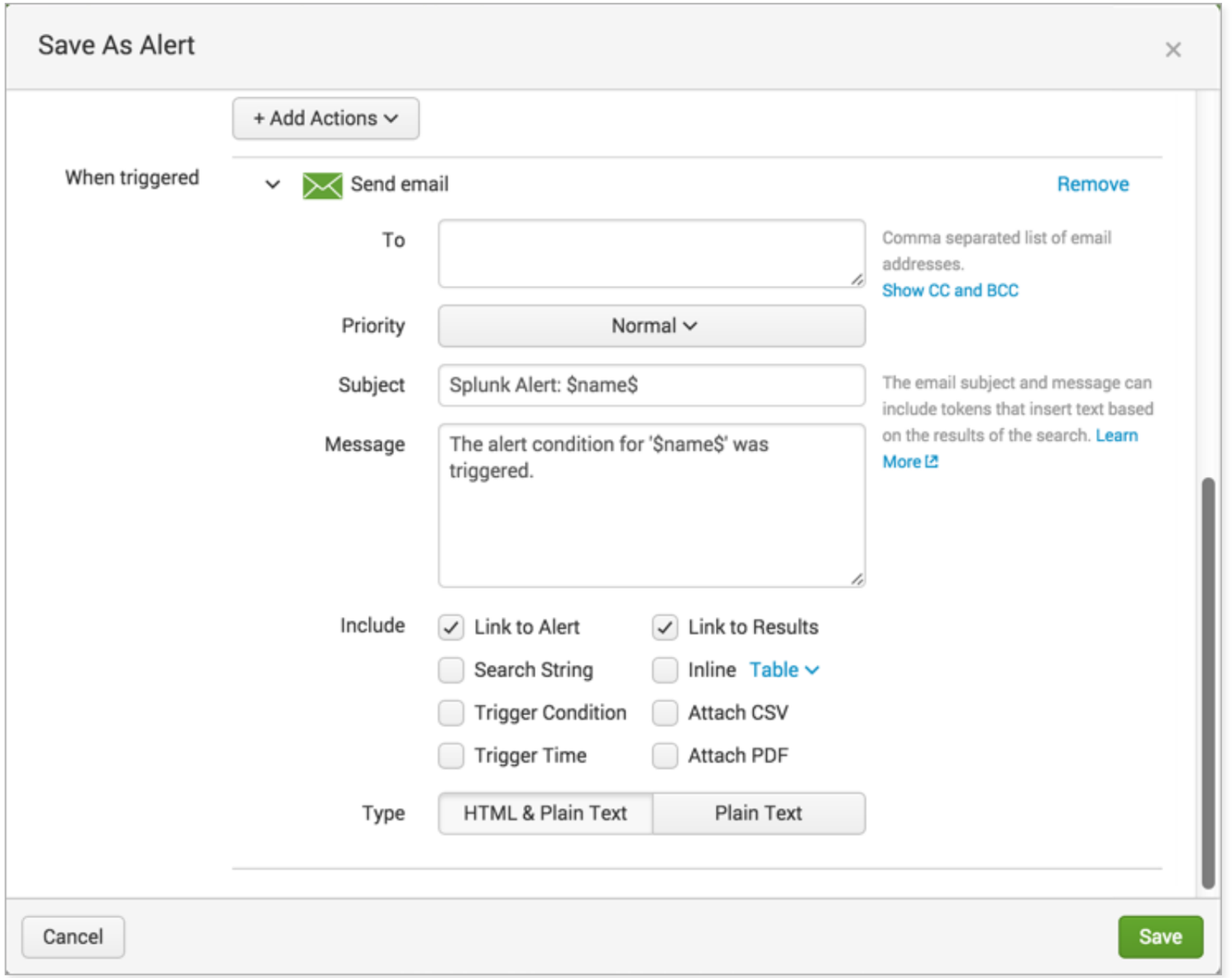
- **Add to Triggered Alerts** – adds the alert to the Activity > Triggered alerts view that shows severity and links to results
  - Choose an appropriate severity for the alert
- **Run a script** – runs a script that can perform some other action
- **Send Email** – sends an email with results to recipients that you define
- **Webhook** – calls a rest endpoint using http post request



Alert Actions – Send Email

Customize the content of email alerts

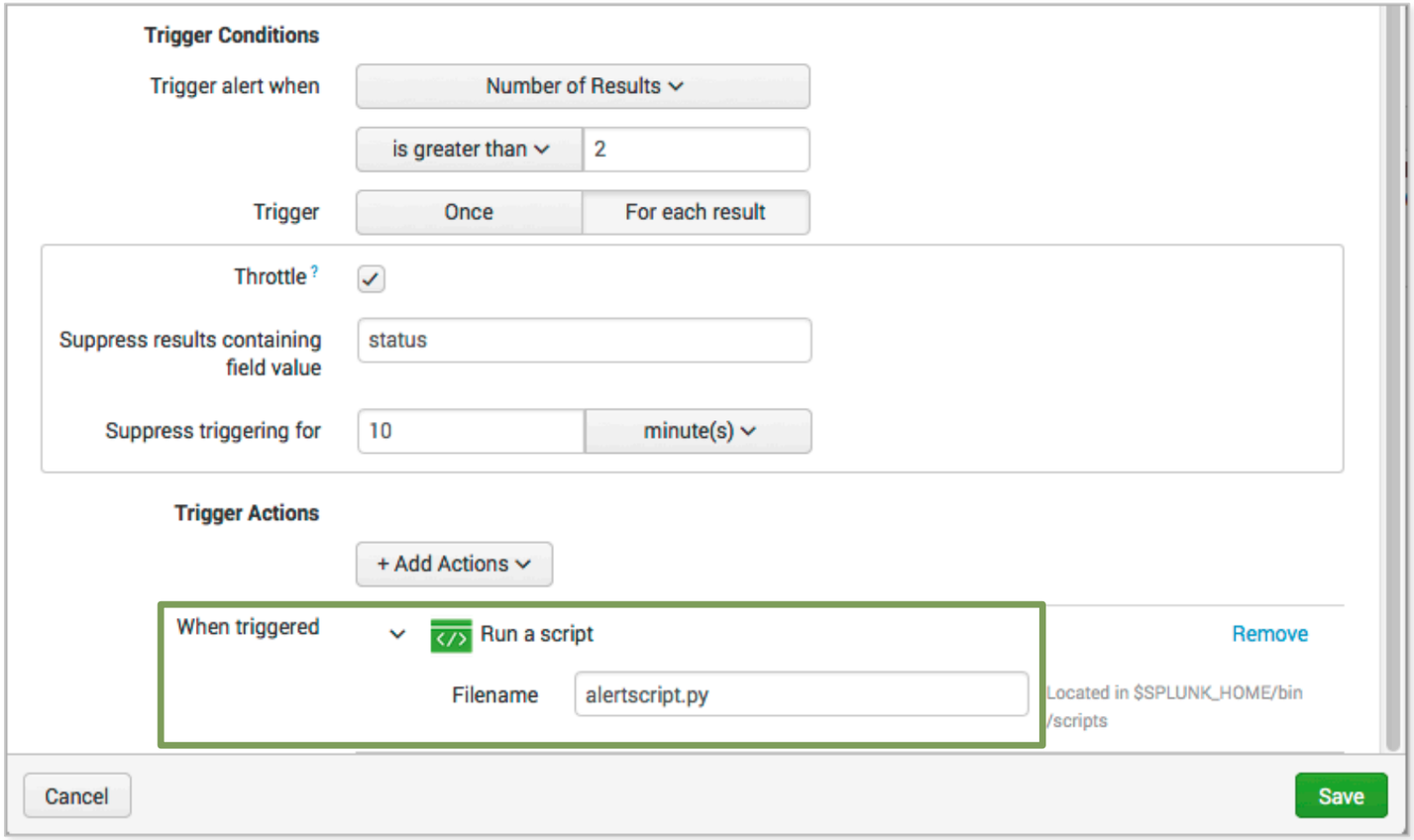
- **To** - enter the email address(es) of the alert recipients
- **Priority** – select the priority
- **Subject** – edit the subject of the email (the $name$ token is the title of the alert)
- **Message** – provide the message body of the email
- **Include** - select the format of the alert
- **Type** – select the format of the text message



Alert Actions – Run a Script

When an alert is triggered, you can launch a script

- Enter the name of the script
- All alert scripts need to reside in either of the following locations:
  - $SPLUNK_HOME/bin/scripts
  - $SPLUNK_HOME/etc/apps/<Appname>/bin/scripts

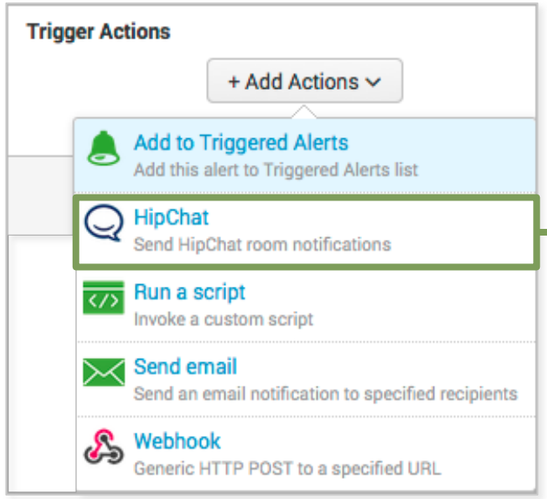


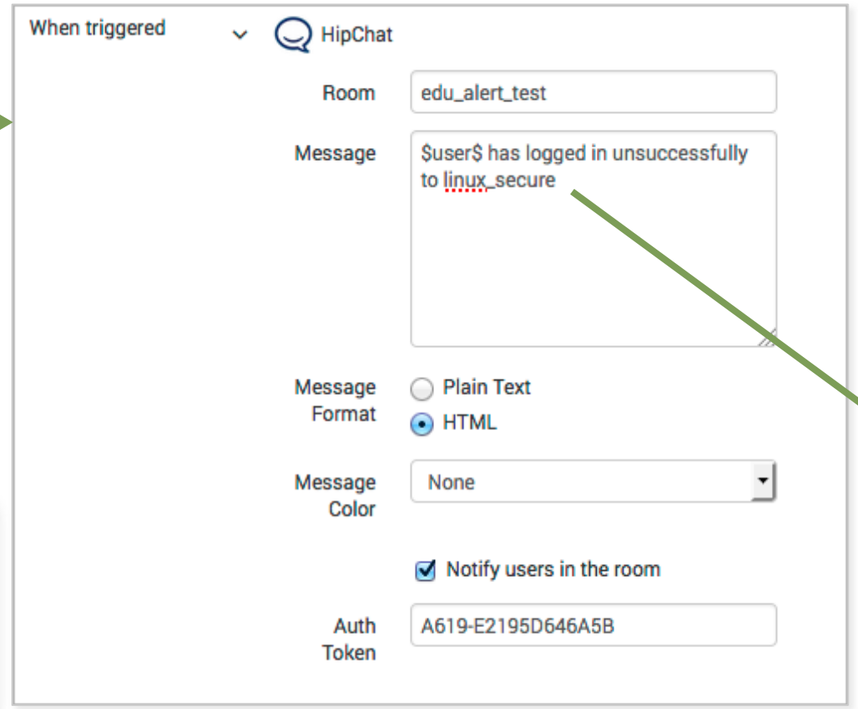
Note

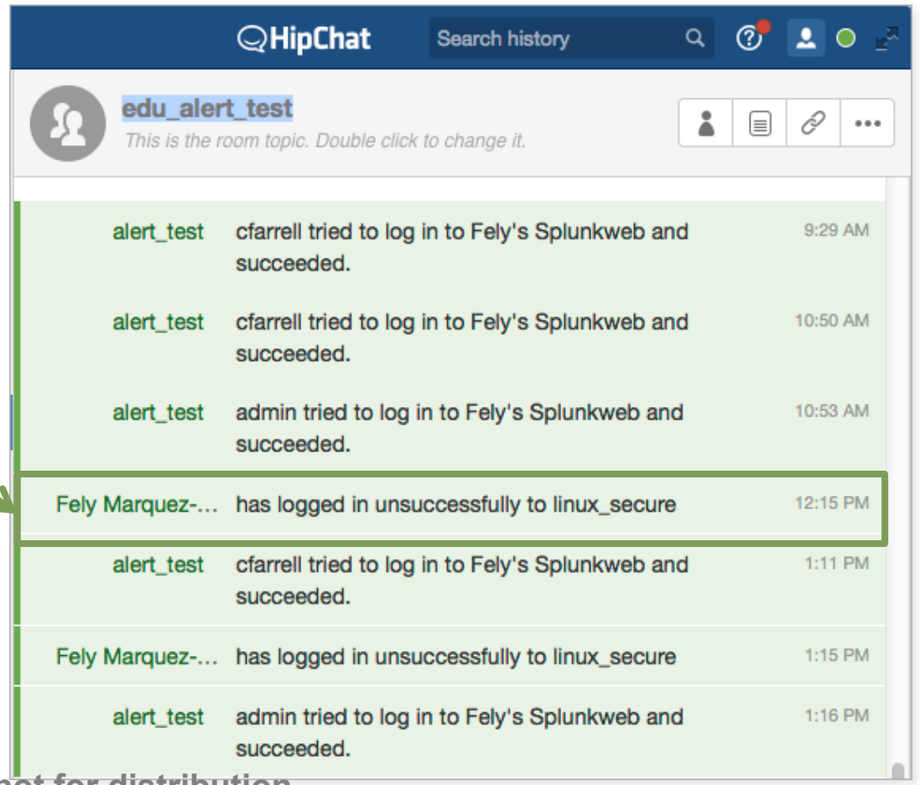
The proper permissions to your Splunk server are required to upload your script to these Splunk directories.

Custom Alert Action

- You can create a custom alert actions or download an app from Splunkbase
- In this example, the HipChat Room Notification Alert app is used





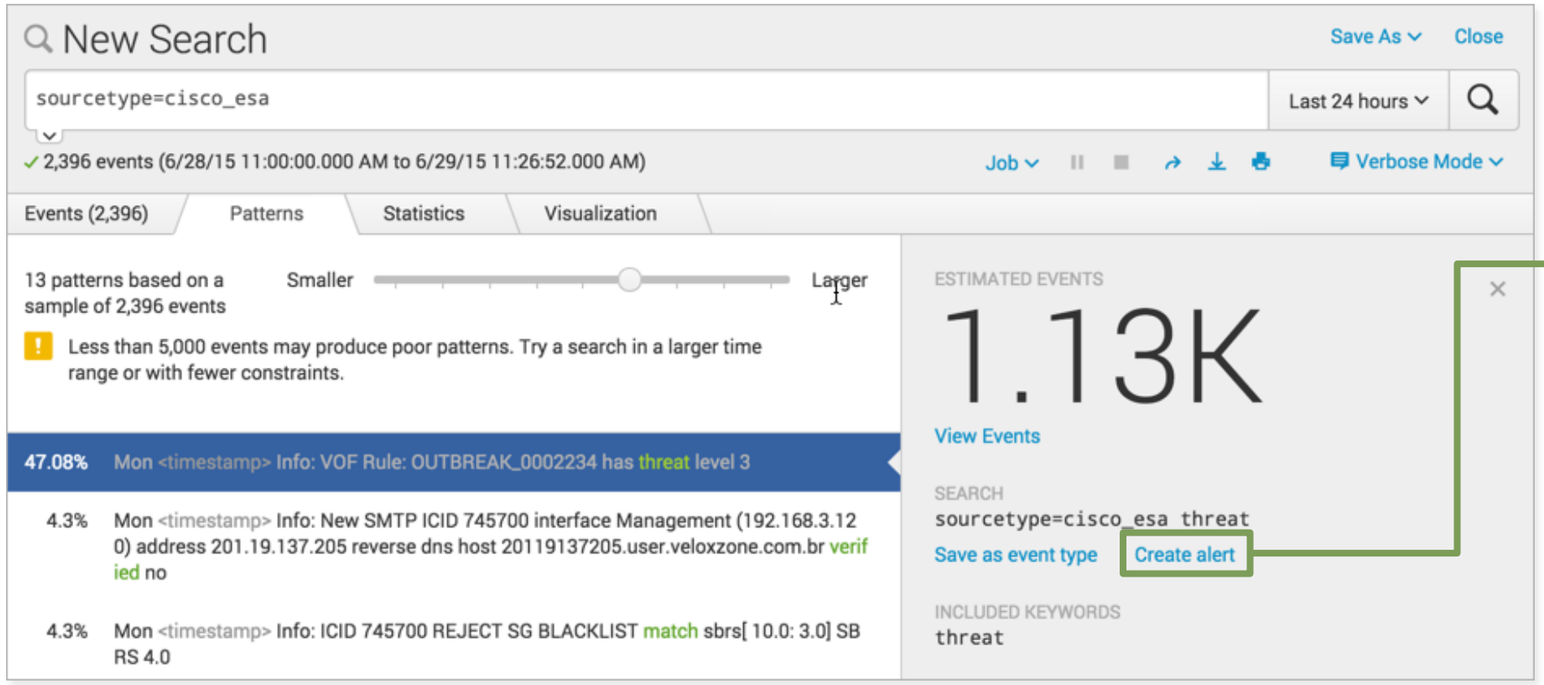


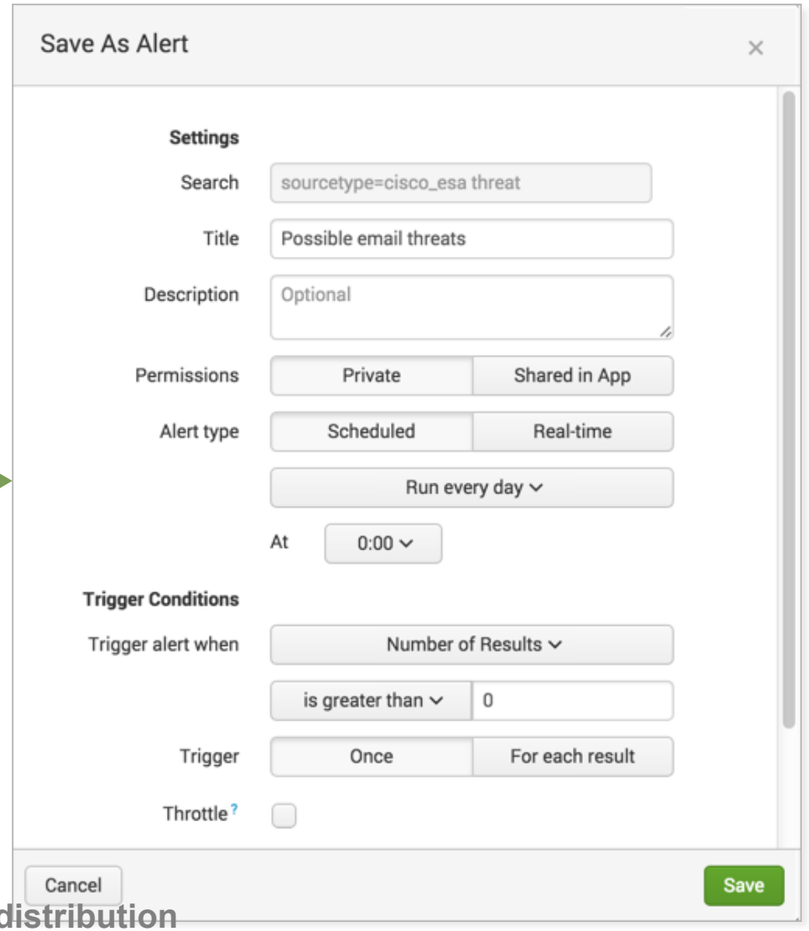
Note

For more information about Custom Alerts, see http://docs.splunk.com/Documentation/Splunk/latest/Alert/CreateCustomAlerts

Creating an Alert via Patterns

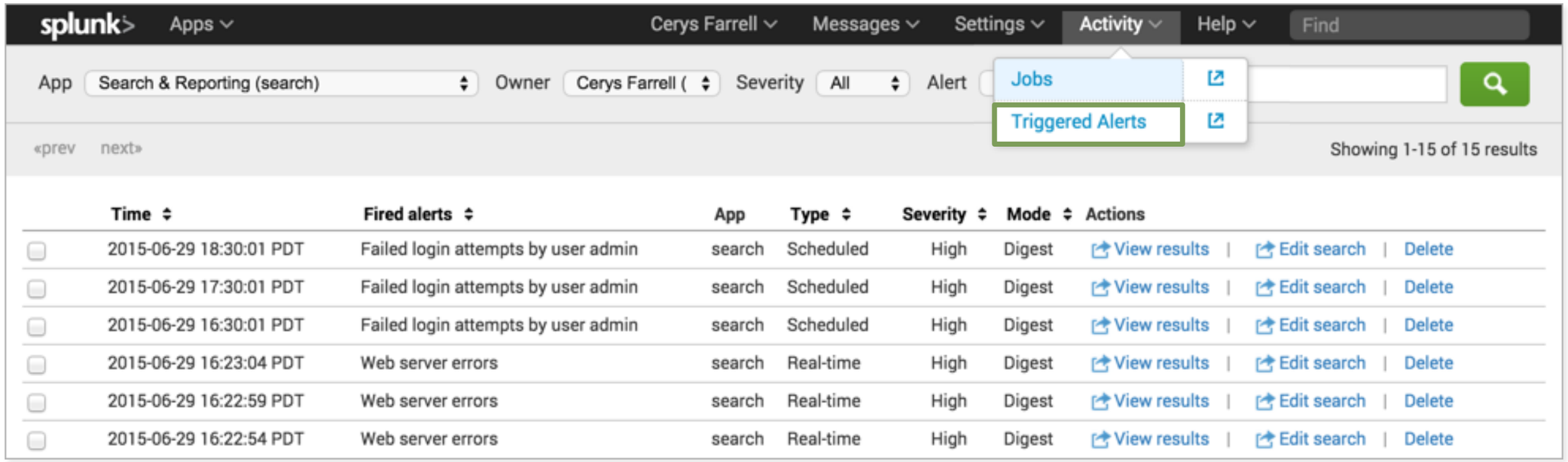
1. Run a search
   - In this example, you're searching for any patterns on the email server that need to be tracked
2. Select the **Patterns** tab and click **Create alert**
3. Configure your alert settings and **Save**





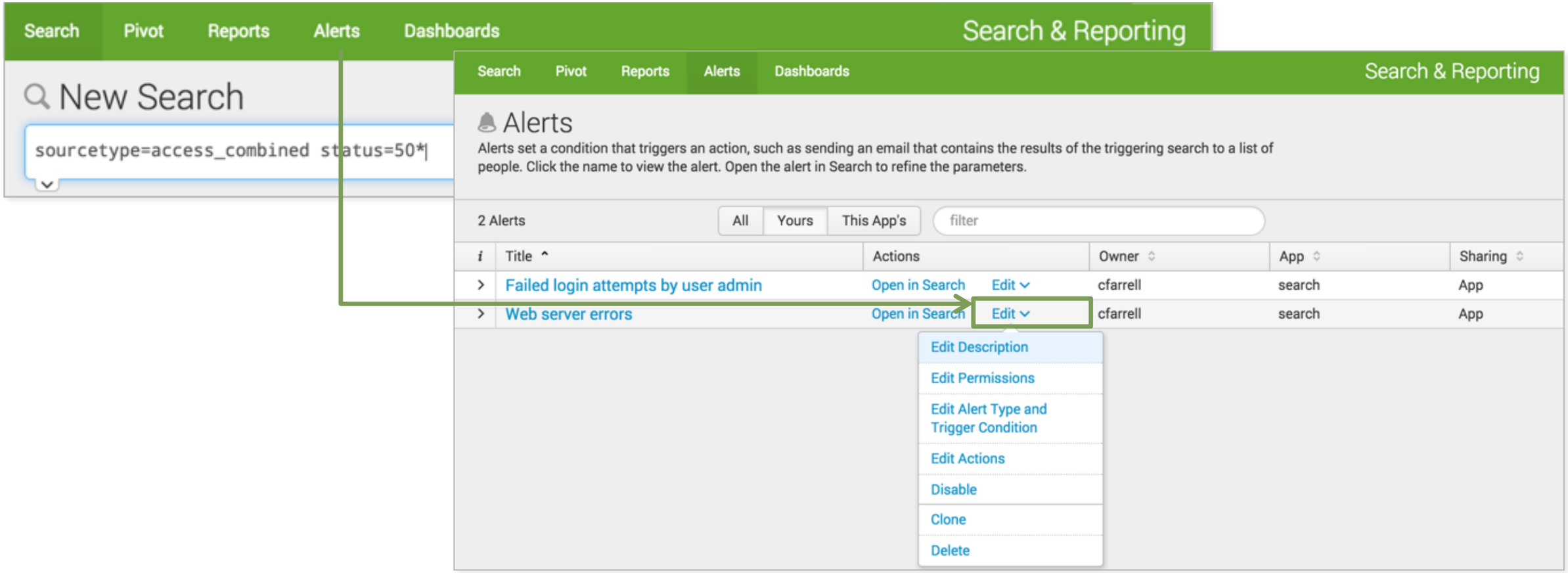
Viewing Triggered Alerts

- If you elected to list in triggered alerts, you can view the results by accessing **Activity > Triggered Alerts**
- Click **View results** to see the matching events that triggered the alert
- Click **Edit search** to modify the alert definition



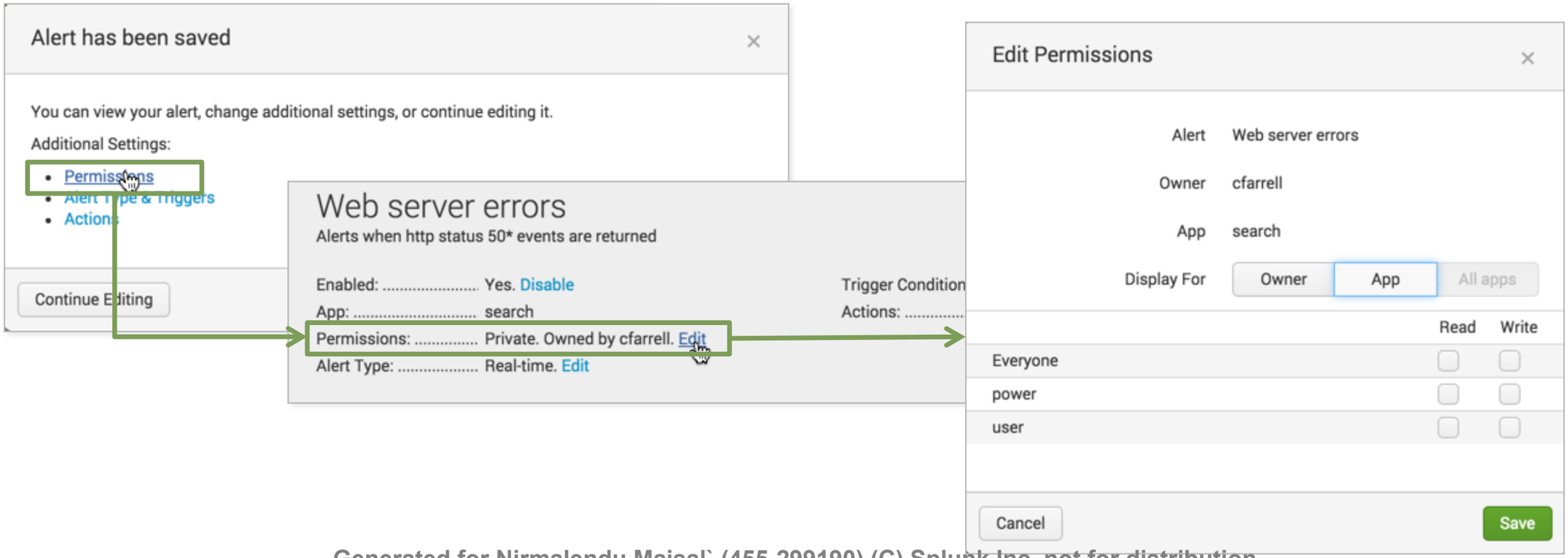
Editing Alerts

- From the search bar, click **Alerts**
- Select the alert and click **Edit**



Editing Alert Permissions

- Edit alert permissions
  - **Private** – only you can access, edit, and view triggered alerts
  - **Shared in app** – all users of the app can access, edit, and view triggered alerts

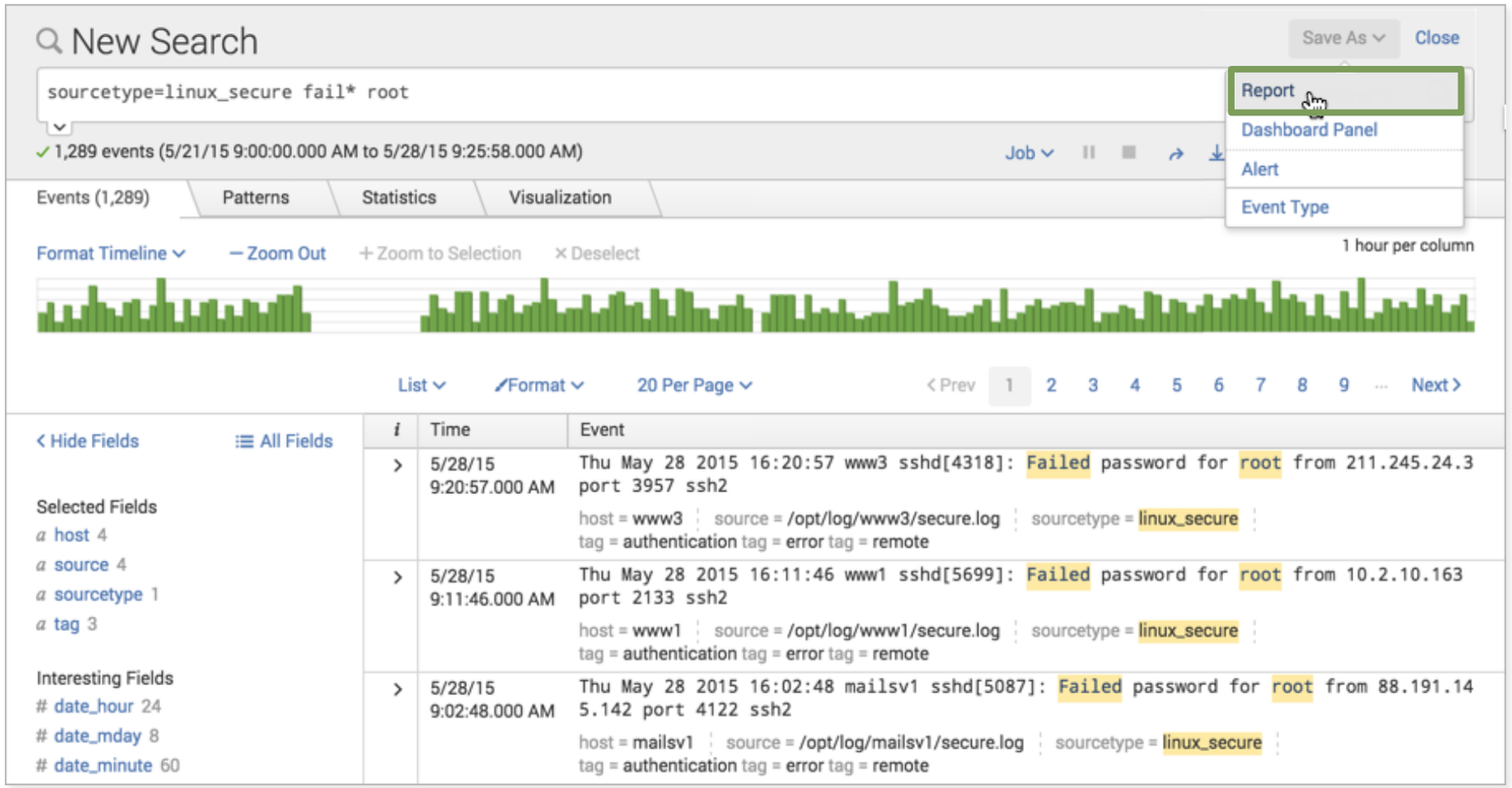


Using Scheduled Reports

- Scheduled Reports are useful for:
  - Monthly, weekly, daily executive/managerial roll up reports
  - Dashboard performance
  - Automatically sending reports via email

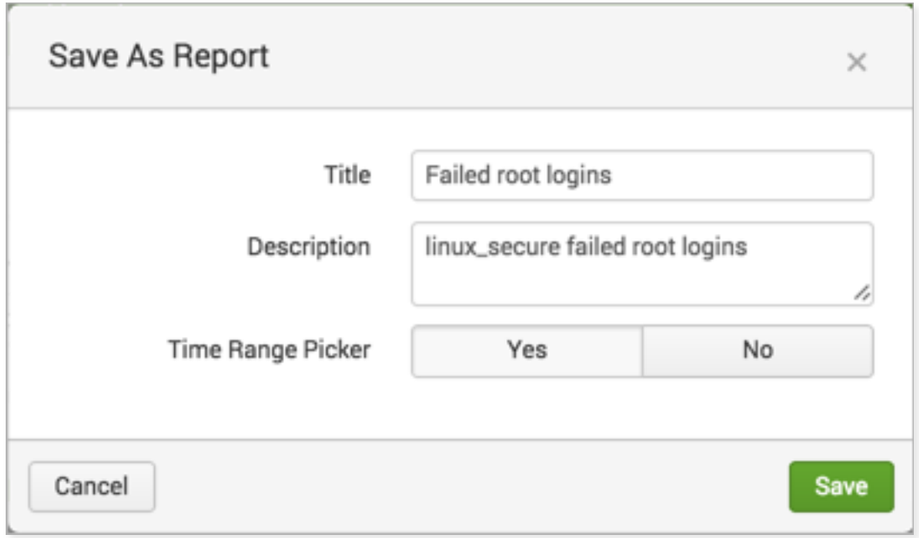
Creating a Scheduled Report

- Create your search
- From the **Save As** menu, select **Report**



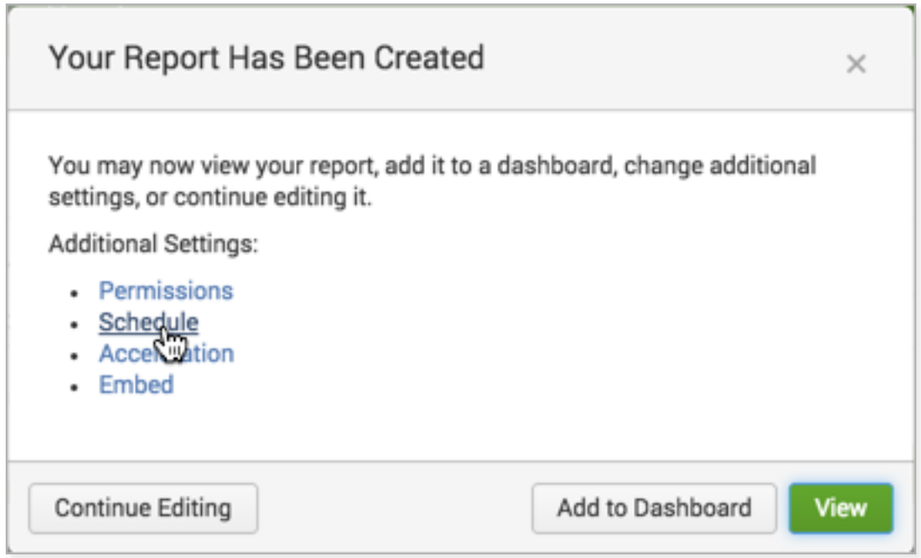
Creating a Scheduled Report (cont.)

- **Title** – enter a title for your report
- **Description** – provide a description
- **Time Range Picker** – you can add a time range picker to the report
- Click **Save**



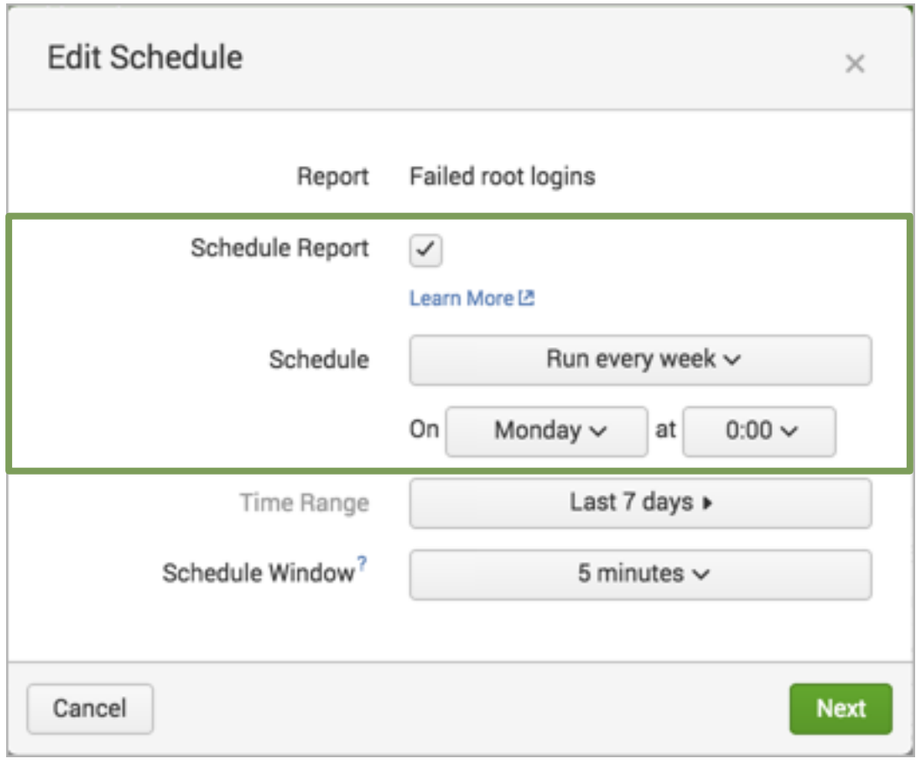
Creating a Scheduled Report (cont.)

After the report is created, click **Schedule**



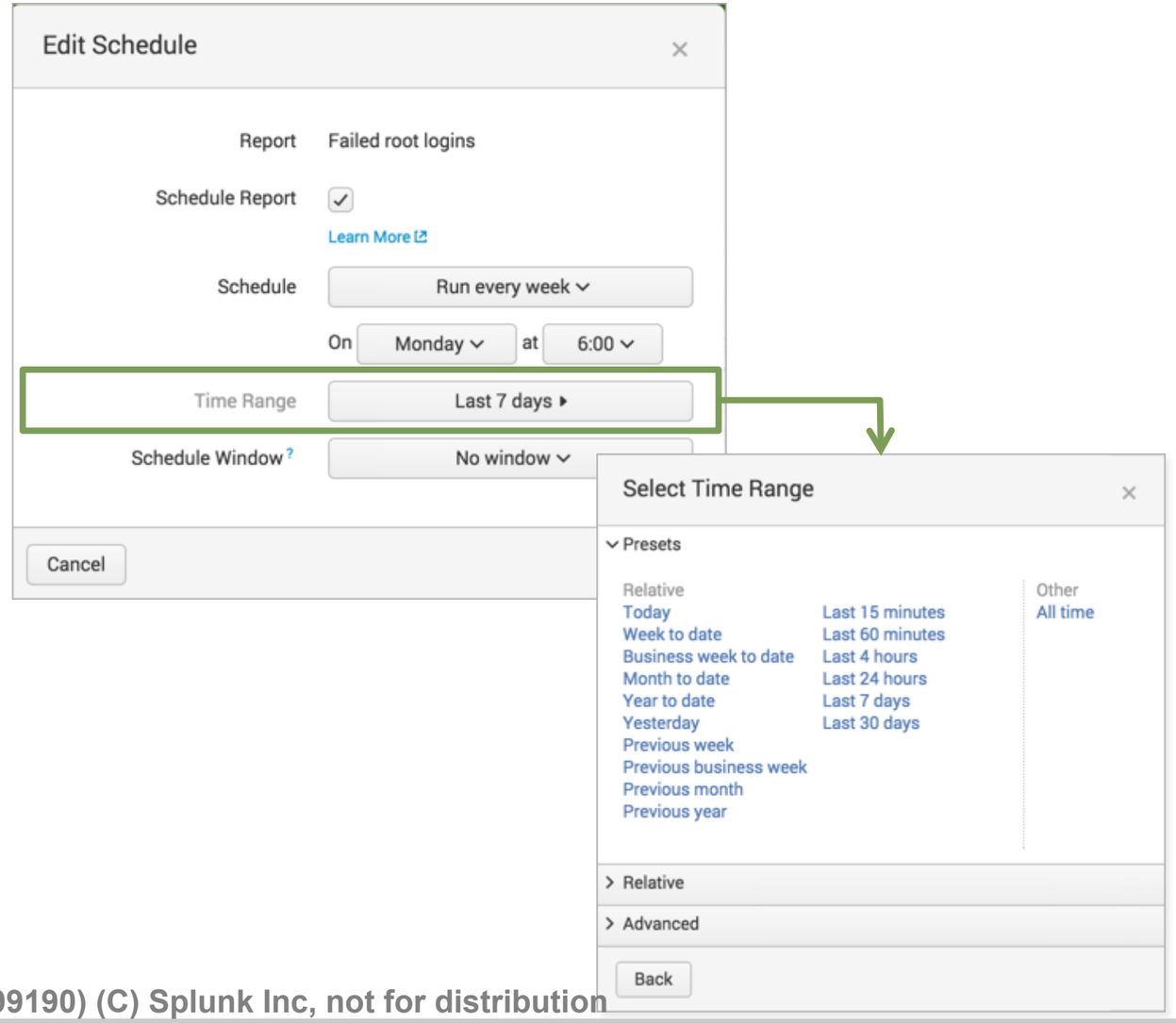
Creating a Scheduled Report – Define Schedule

- **Schedule Report** – click this checkbox
- **Schedule** – select the frequency to run the report
  - Run every hour
  - Run every day
  - Run every week
  - Run every month
  - Run on Cron Schedule



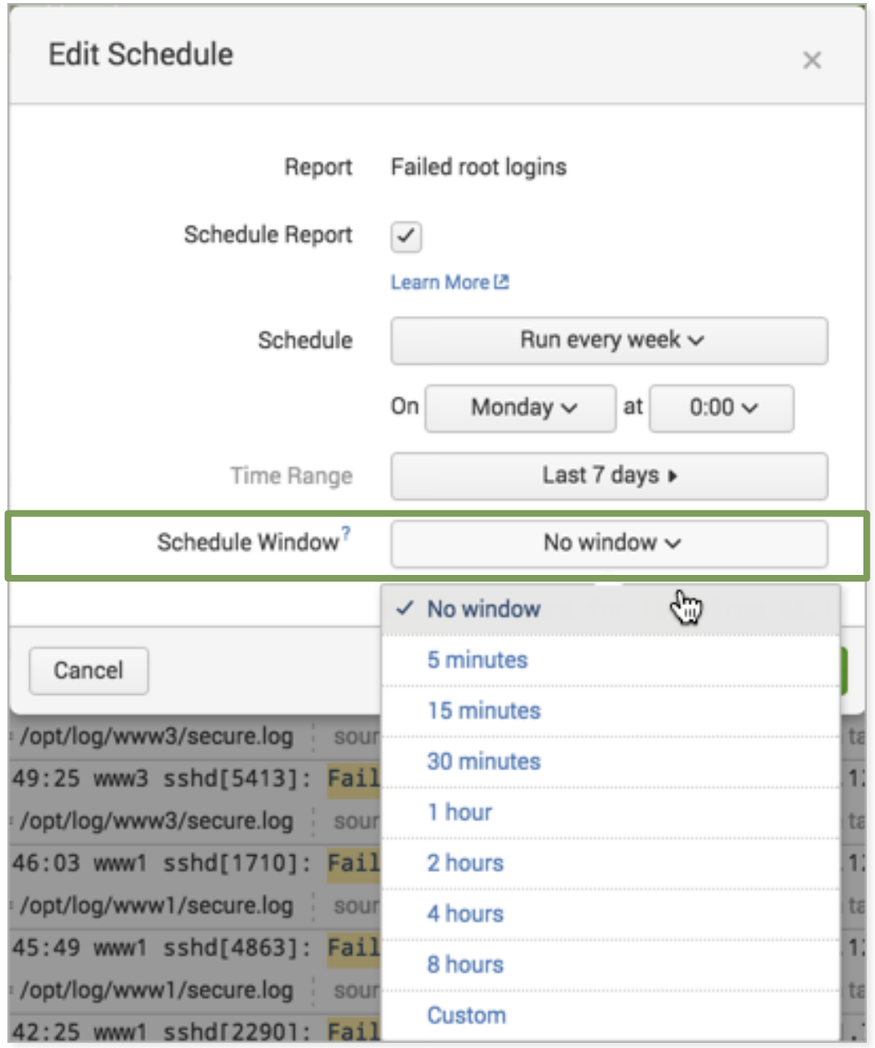
Creating a Scheduled Report – Select Time Range

- **Time Range** – By default, the search time range is used
  - Click the time range button to change the time range
  - You can select a time range from Presets, Relative, or Advanced
  - Typically, the time range is relative to the Schedule



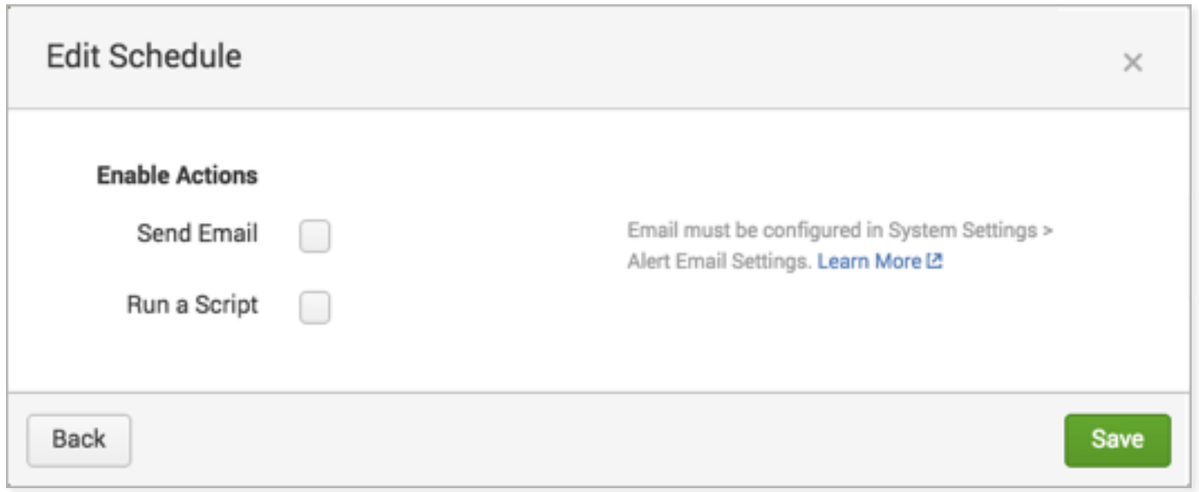
Creating a Scheduled Report – Schedule Window

- **Schedule Window** – This setting determines a time frame to run the report.
  - If there are other reports scheduled to run at the same time, you can provide a window in which to run the report
  - This setting provides efficiency when scheduling several reports to run
- After you configure the schedule report, click **Next**



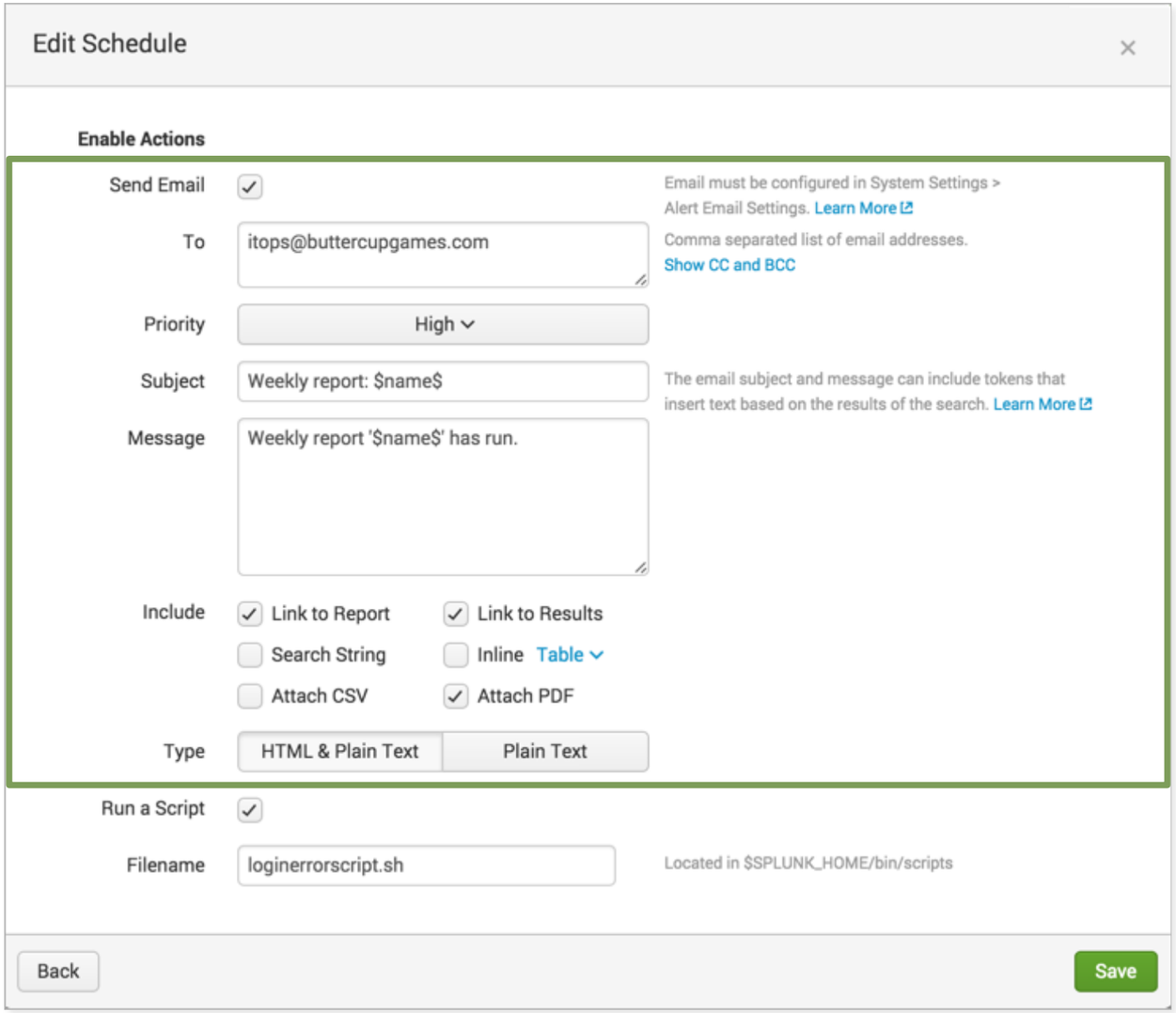
Creating a Scheduled Report – Enable Actions

- **Enable Actions**
  - **Send Email**: When an alert is triggered, an email is sent to the specified recipient
  - **Run a script**: A script is launched when an alert is triggered



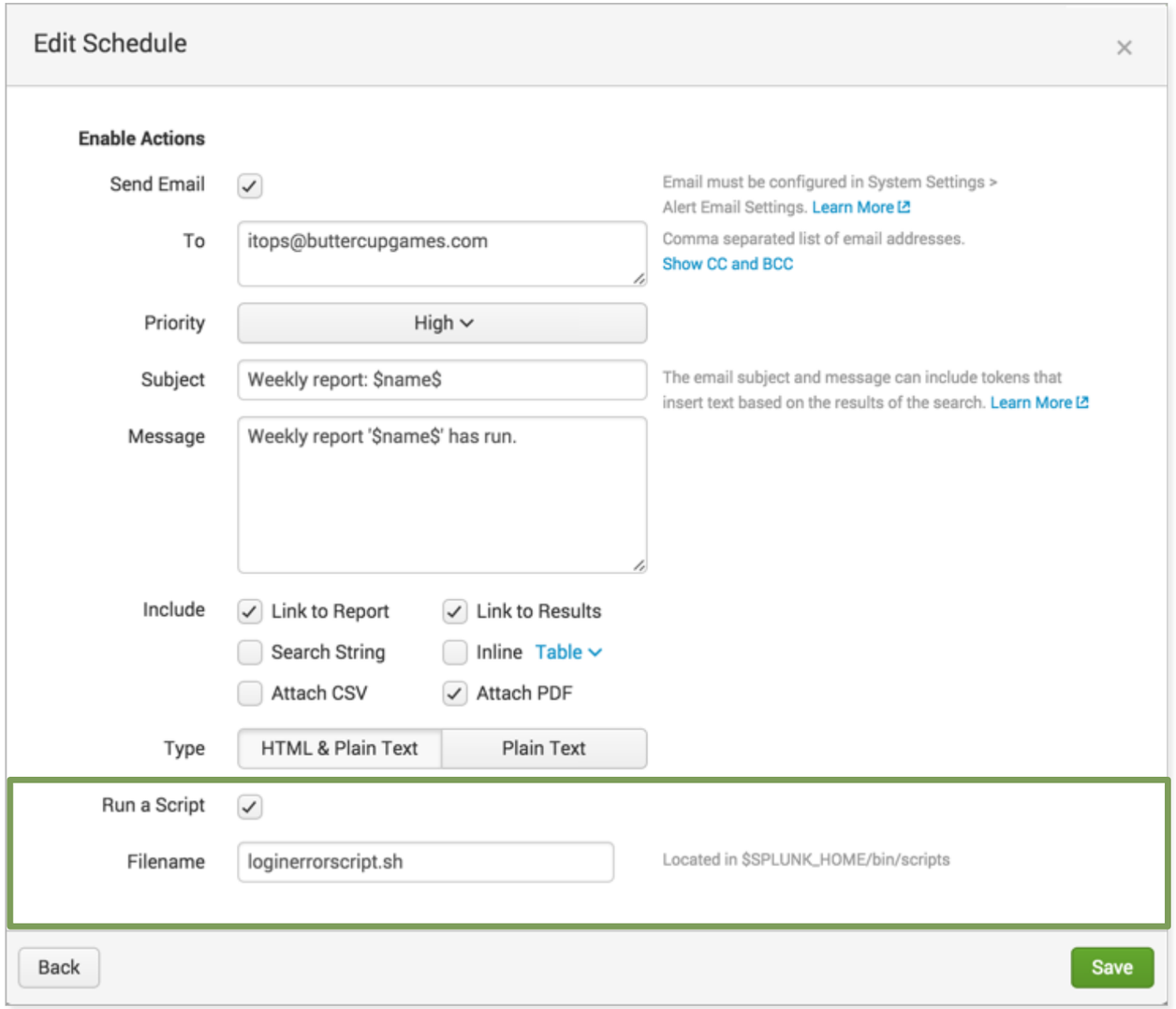
Creating a Scheduled Report – Send Email

1. Enter addresses in the **To** field, separated by a comma
2. Set the priority
3. Edit or keep the default subject
   - the $name$ variable includes the name of the report
   - In addition to a message, you can include other options like an inline table of the results, etc.
4. Define the email text type
5. After you have configured the actions, click **Save**



Creating a Scheduled Report – Run a Script

1. Enter the file name of the script
   - The script must reside in the $SPLUNK_HOME/bin/scripts directory
2. Click **Save**



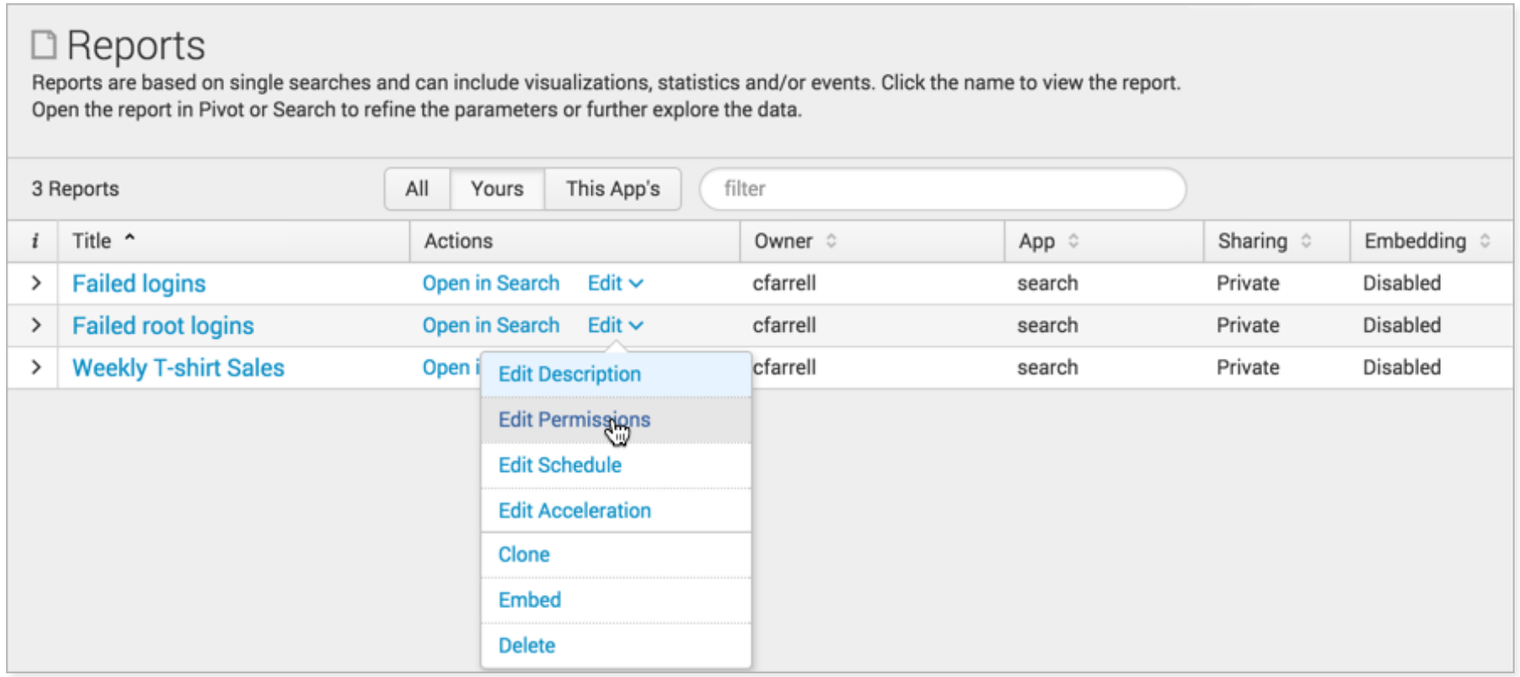
Note

The proper permissions to your Splunk server are required to upload your script to this Splunk directory.

Managing Scheduled Reports

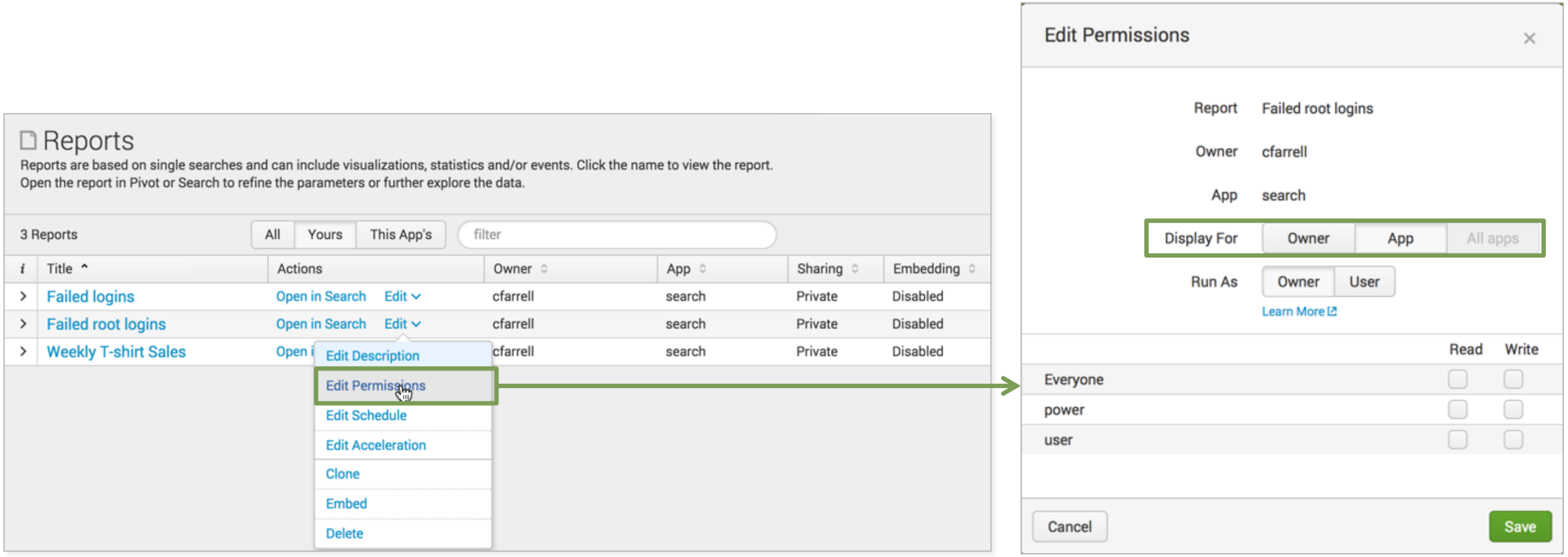
You can manage reports two ways:

- **Settings > Searches, reports and alerts**
- **Reports Menu**
  - Edit description
  - Edit permissions
  - Edit schedule
  - Edit acceleration
  - Clone
  - Embed
  - Delete



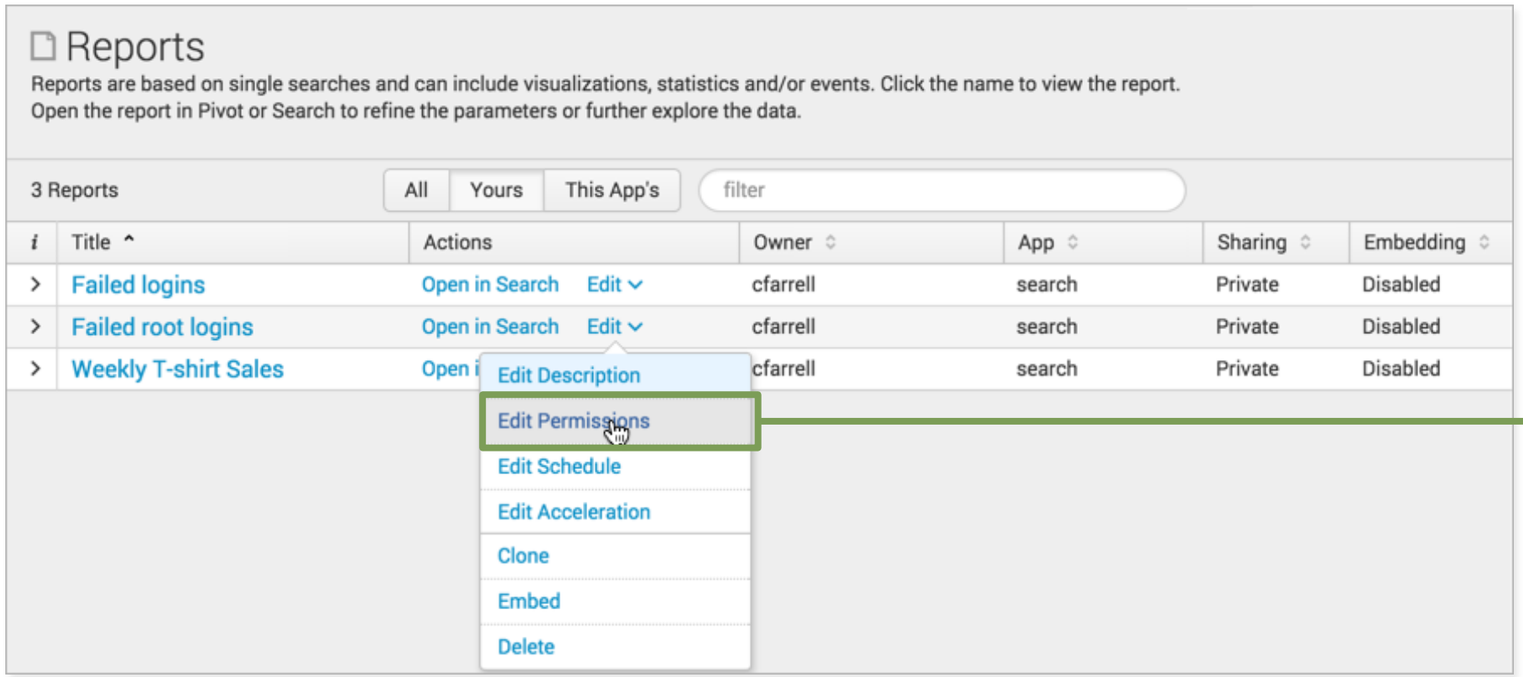
Managing Reports – Edit Permissions

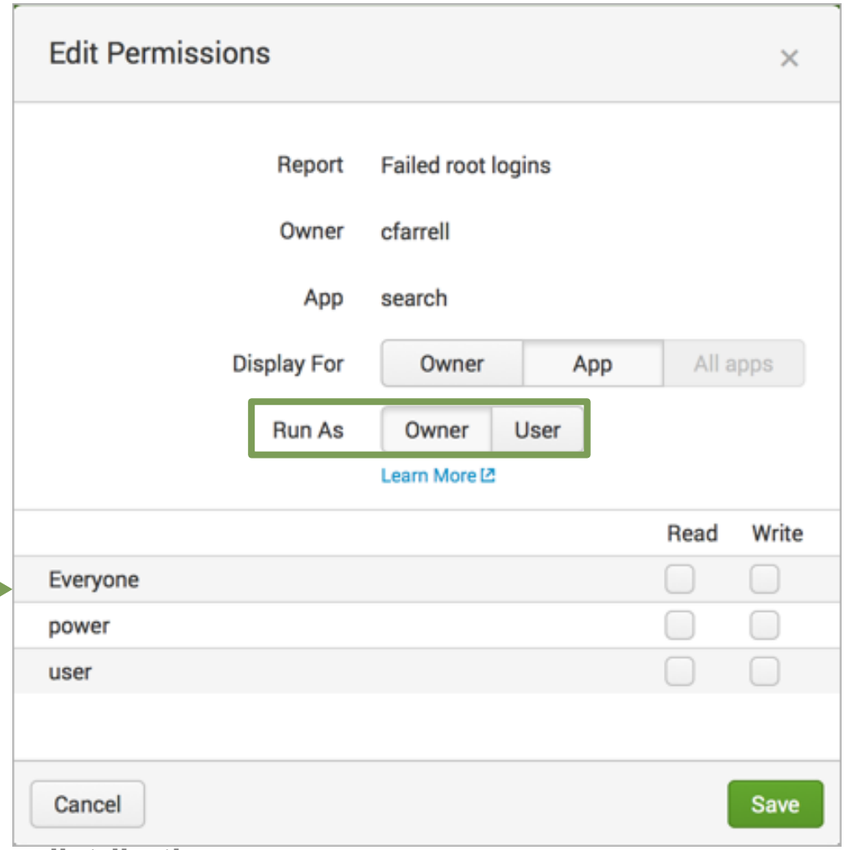
Display For determines who sees the scheduled report



Managing Reports – Edit Permissions (cont.)

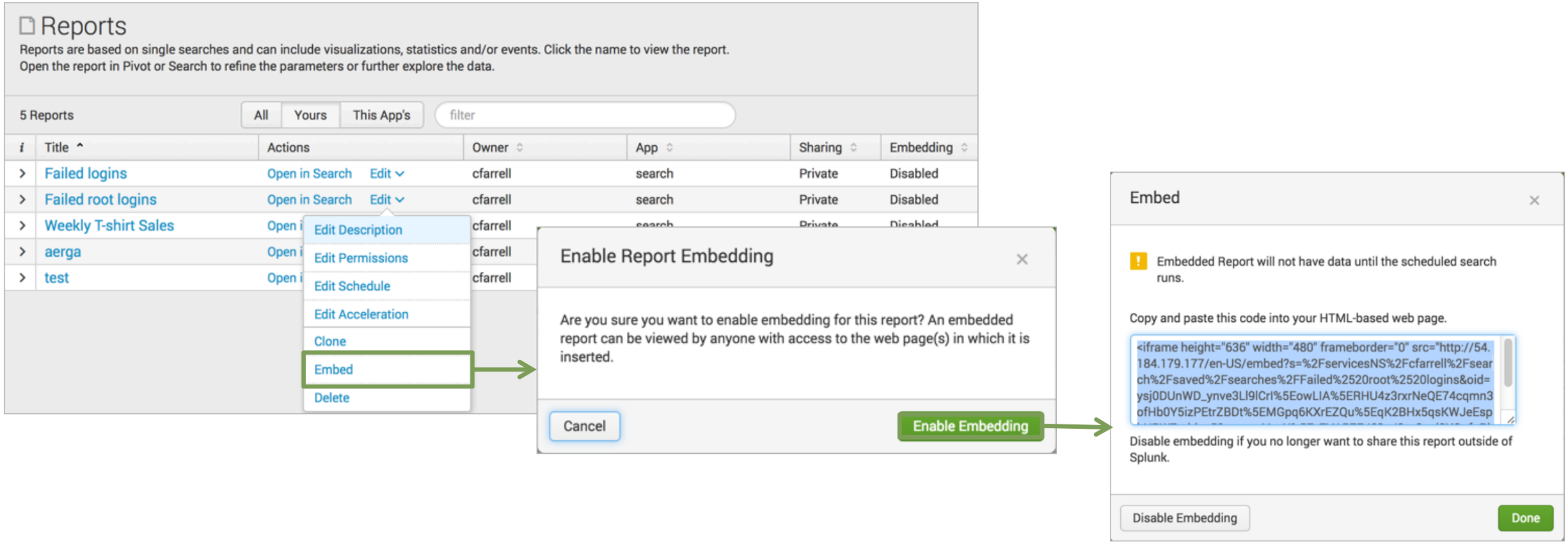
- **Run As** – determines which user profile is used at run time
  - Owner – all data accessible by the owner appears in the report
  - User – only data allowed to be accessed by the user role appears





Managing Reports – Embed

- To access the report results from a webpage, click **Edit** > **Embed**
  - Before a report can be embedded, it must be scheduled



Module 8: Creating and Using Macros

Module Objectives

- Describe macros
- Manage macros
- Create a basic macro
- Use a basic macro
- Define arguments / variables for a macro
- Add and use arguments with a macro

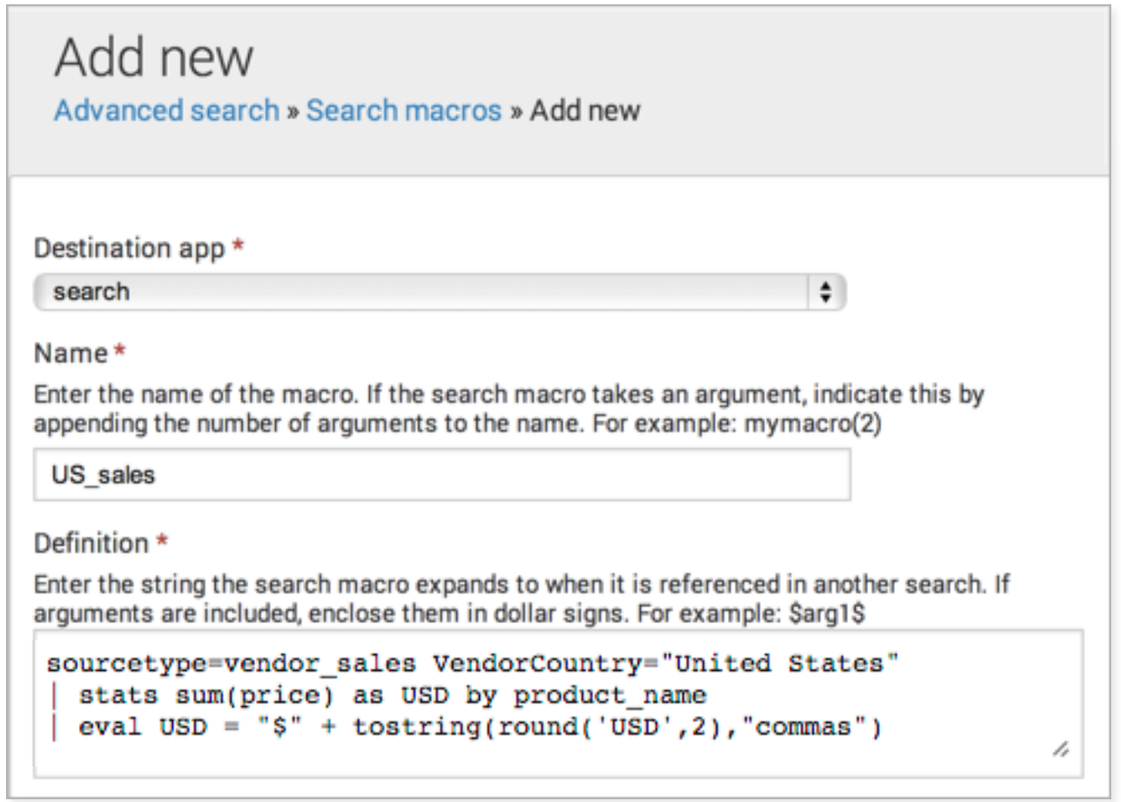
Macros Overview

- Useful when you frequently run searches or reports with similar search syntax
- The time range is selected at search time
- Macros can be a full search string or a portion of a search that can be reused in multiple places
- Allows you to define one or more arguments within the search segment
  - Pass values to the search string when using the macro

Creating a Basic Macro

Settings > Advanced search > Search Macros

1. Click **New**
2. Select the destination app
3. Enter a Name
4. Type the search string
5. Save



Note

Test your search string before saving your macro.

Using a Basic Macro

- Type the macro name into the search bar
- Surround the macro name with the **backtick** (or grave accent) character
  - **`macroname`** != 'macroname'
  - Do not confuse with single-quote character (')
- Pipe to more commands, or precede with search string

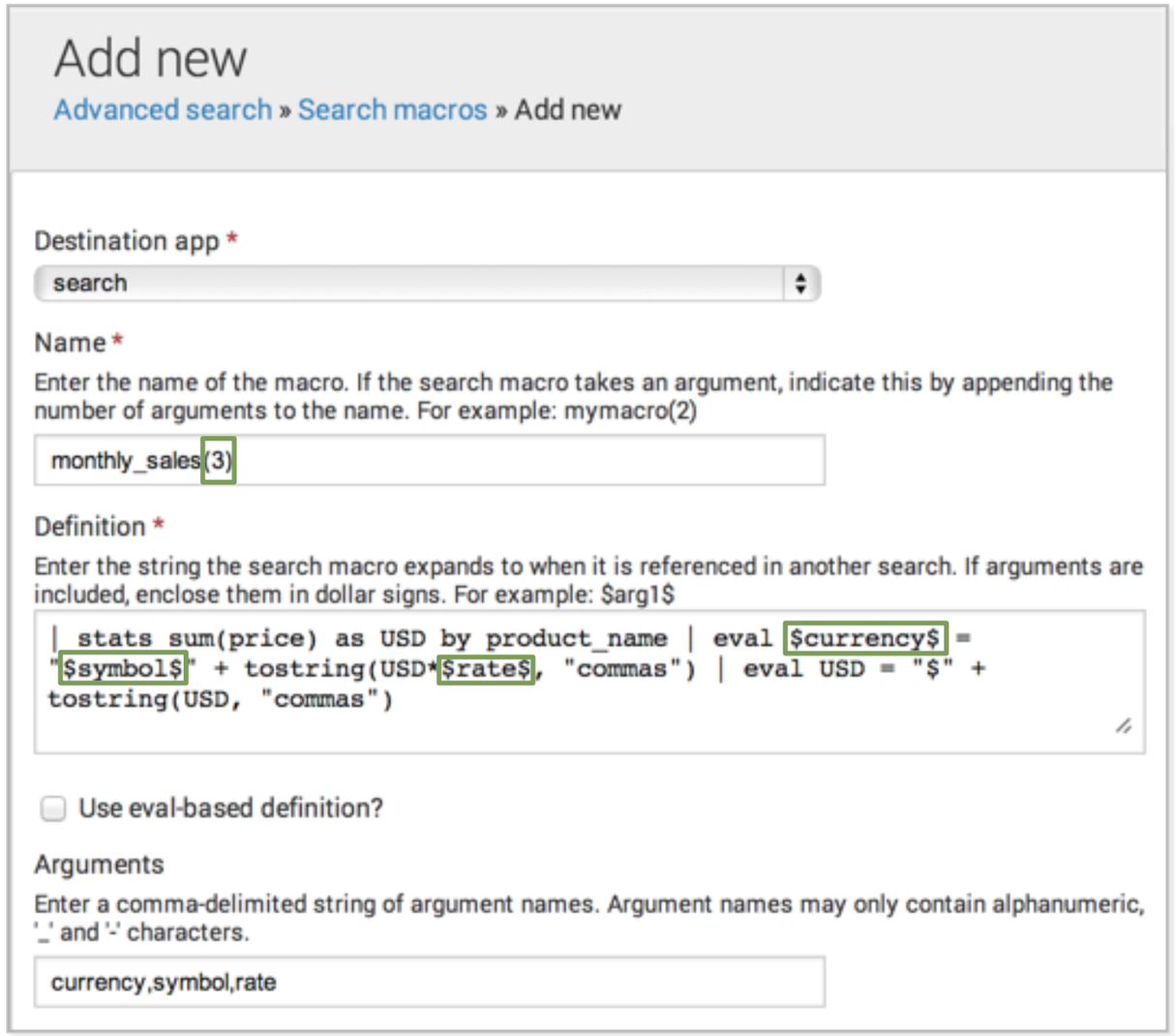
`US_sales`

```
sourcetype=vendor_sales
VendorCountry="United States"  | stats
sum(price) as USD by product_name | eval USD
= "$" + tostring(round('USD',2),"commas")
```

product_name	USD
Benign Space Debris	$2,848.86
Curling 2014	$3,518.24
Dream Crusher	$21,514.62
Final Sequel	$8,596.56
Fire Resistance Suit of Provolone	$1,695.75
Holy Blade of Gouda	$1,743.09
Manganiello Bros.	$11,717.07
Manganiello Bros. Tee	$3,066.93
Mediocre Kingdoms	$5,322.87

Adding Arguments

- Include the number of arguments in parentheses after the macro name
  - `monthly_sales(3)`
- Within the search definition, use `$arg$`
  - `currency=$currency$`
  - `symbol=$symbol$`
  - `rate=$rate$`
- In the **Arguments** field, enter the name of the argument(s)
- Provide one or more variables of the macro at search time



Using Arguments

When using a macro with arguments, include the argument(s) in parentheses following the macro name

```
sourcetype=vendor_sales VendorCountry=Germany
OR VendorCountry=France OR VendorCountry=Italy
`monthly_sales(euro,€,.79)`
```

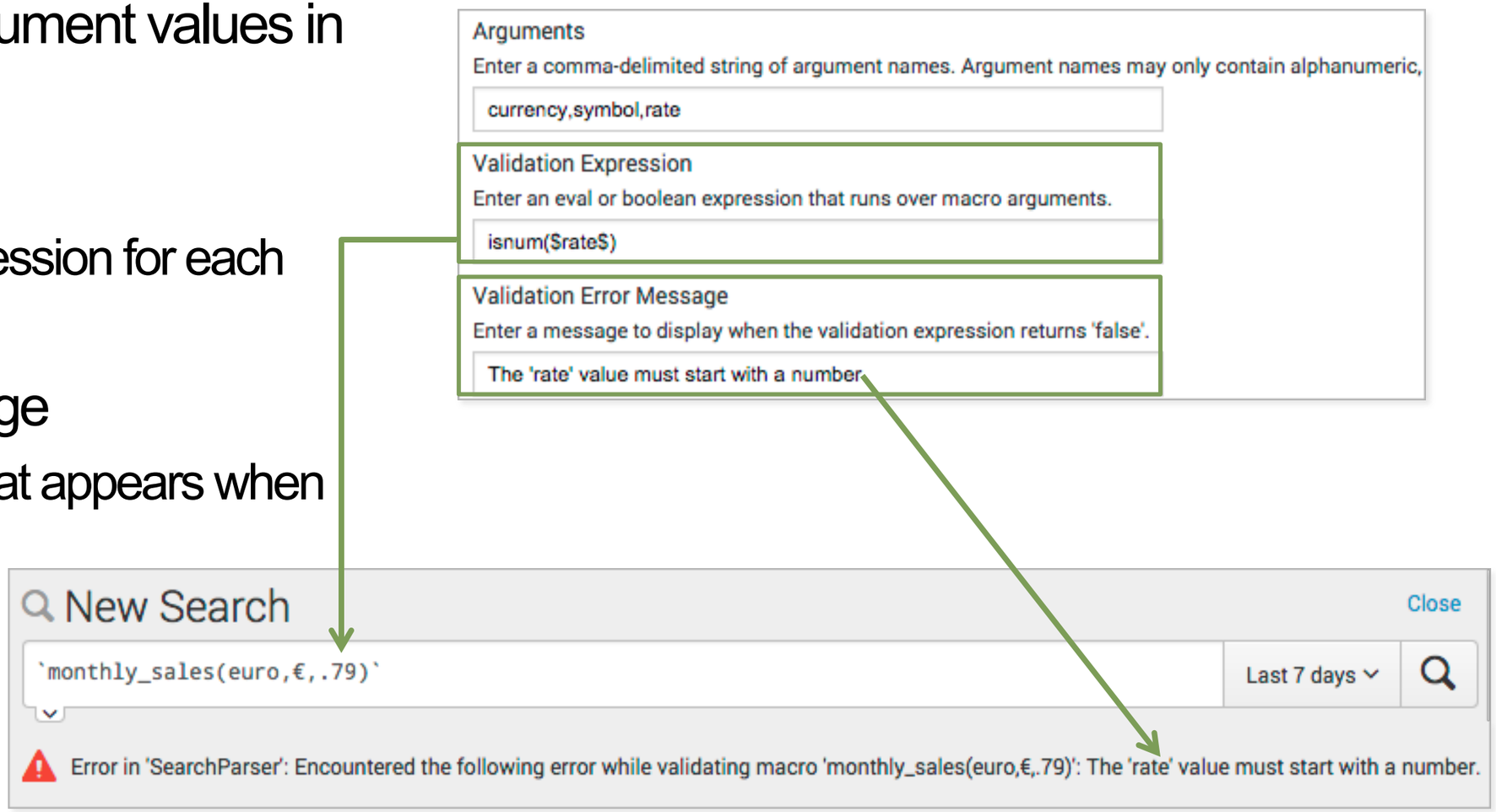
```
sourcetype=vendor_sales VendorCountry=Germany OR
VendorCountry=France OR VendorCountry=Italy
| stats sum(price) as USD by product_name |
eval euro = "€" + tostring(USD*.79, "commas")
| eval USD = "$" + tostring(USD, "commas")
```

product_name	USD	euro
Benign Space Debris	$974.61	€770
Curling 2014	$799.60	€632
Dream Crusher	$1,479.63	€1,169
Final Sequel	$324.87	€257
Fire Resistance Suit of Provolone	$195.51	€154
Holy Blade of Gouda	$203.66	€161
Manganiello Bros.	$3,079.23	€2,433
Manganiello Bros. Tee	$619.38	€489
Mediocre Kingdoms	$1,274.49	€1,007
Orvil the Wolverine	$1,719.57	€1,358
Puppies vs. Zombies	$44.91	€35
SIM Cubicle	$1,139.43	€900
World of Cheese	$1,299.48	€1,027
World of Cheese Tee	$619.38	€489

Validating Macros

You can validate the argument values in your macro

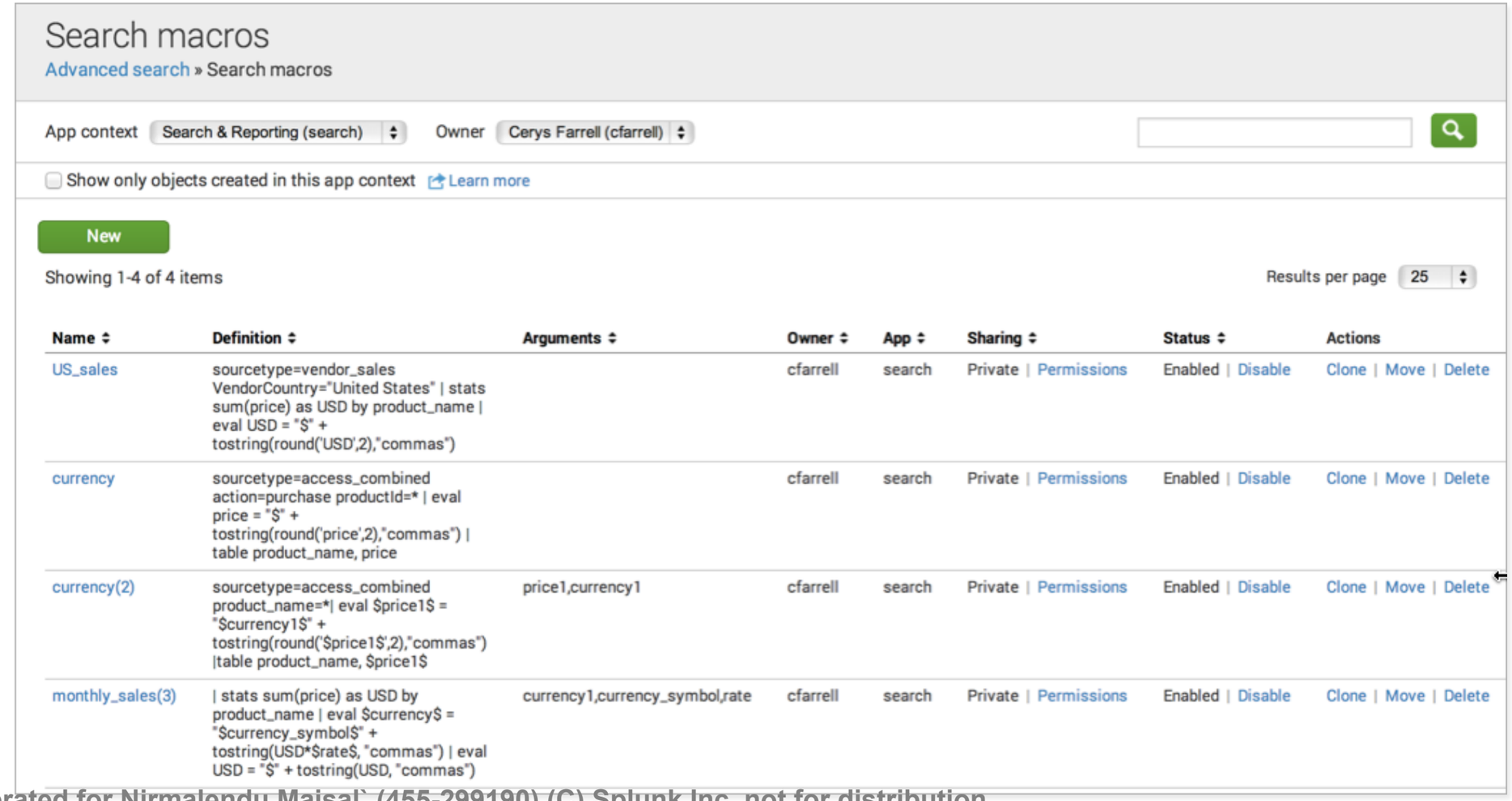
- Validation Expression
  - You can enter an expression for each argument
- Validation Error Message
  - This is the message that appears when you run the macro



Managing Macros

Settings > Advanced search > Search macros

- Edit permissions
- Enable / disable
- Clone
- Move
- Delete



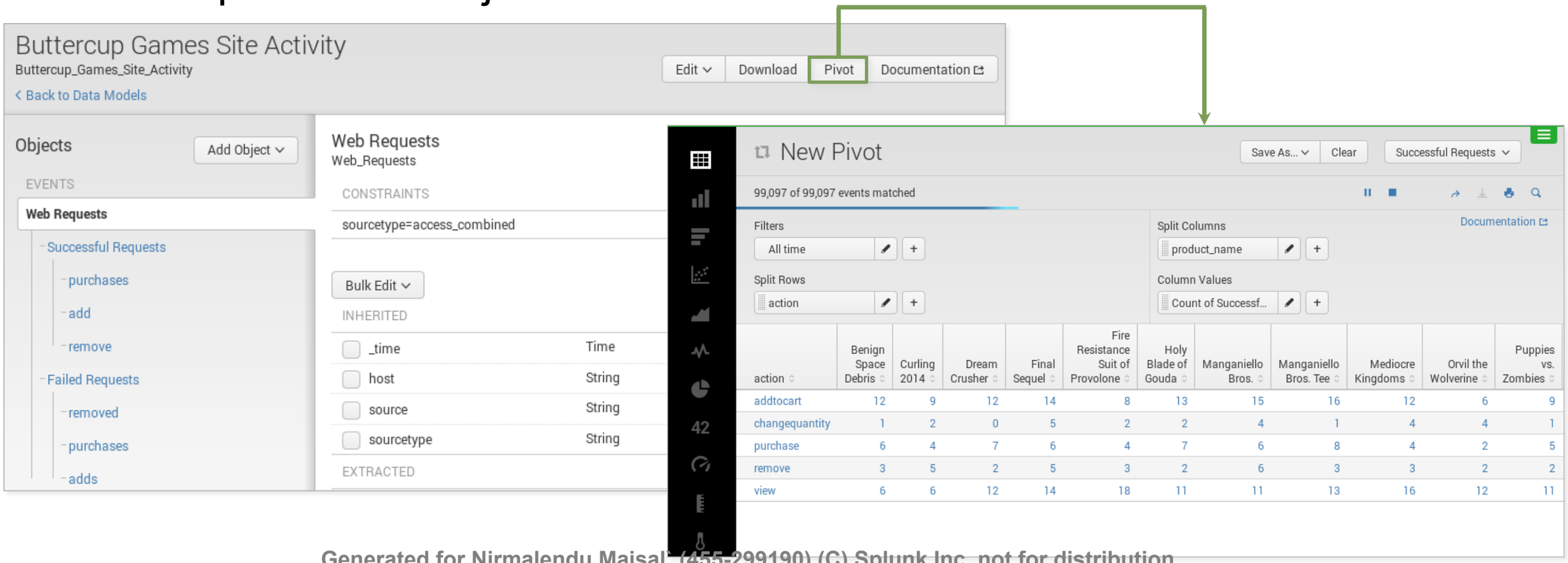
Module 9:
Creating Data Models

Objectives

- Describe the relationship between data models and Pivot
- Identify data model objects
- Identify object attributes
- Create a data model
- Use a data model in Pivot

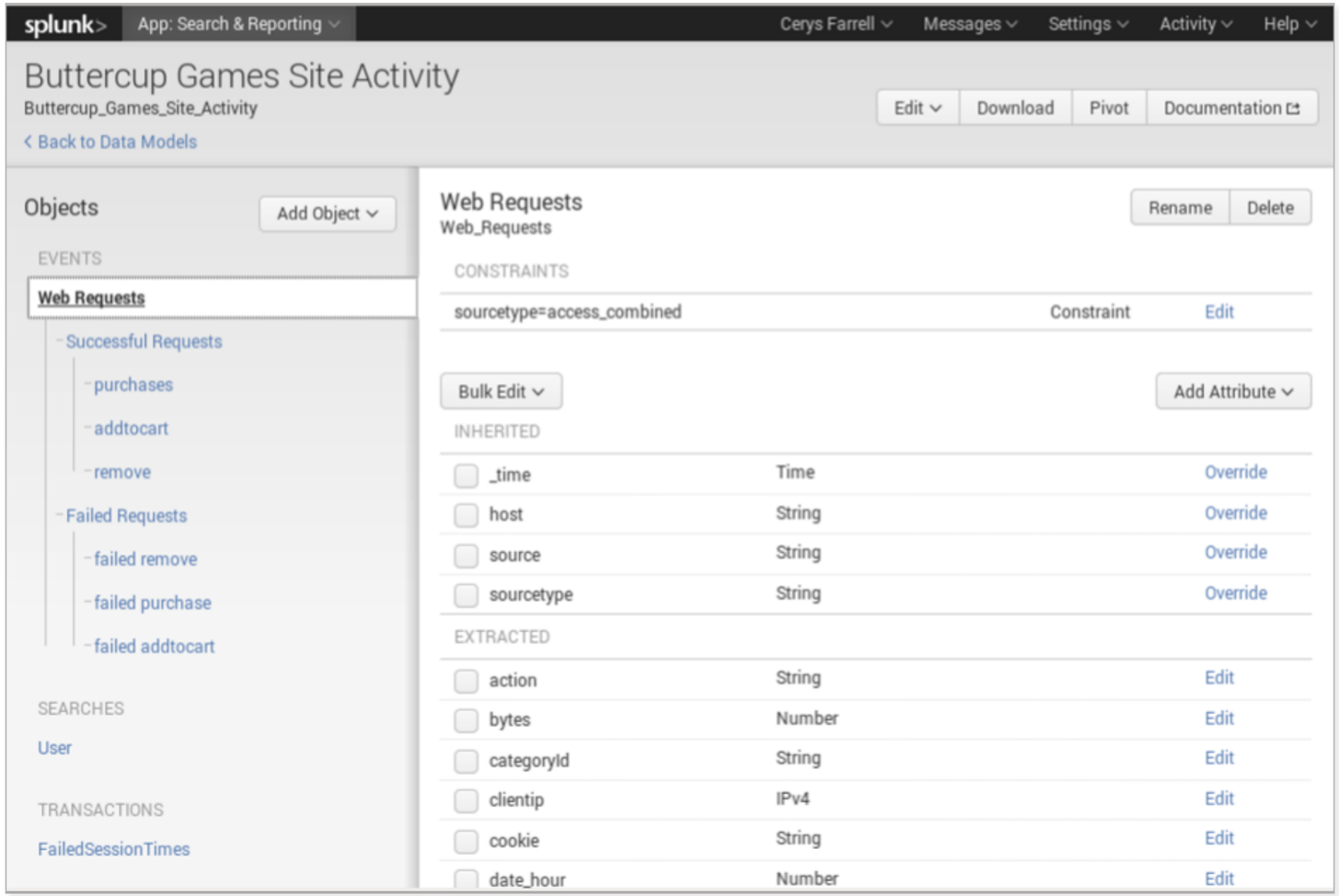
Reviewing Pivot

In the Using Splunk course, you learned how to use the Pivot interface to create reports and dashboards. As a knowledge manager, you are responsible for building the data model that provides the objects for Pivot.



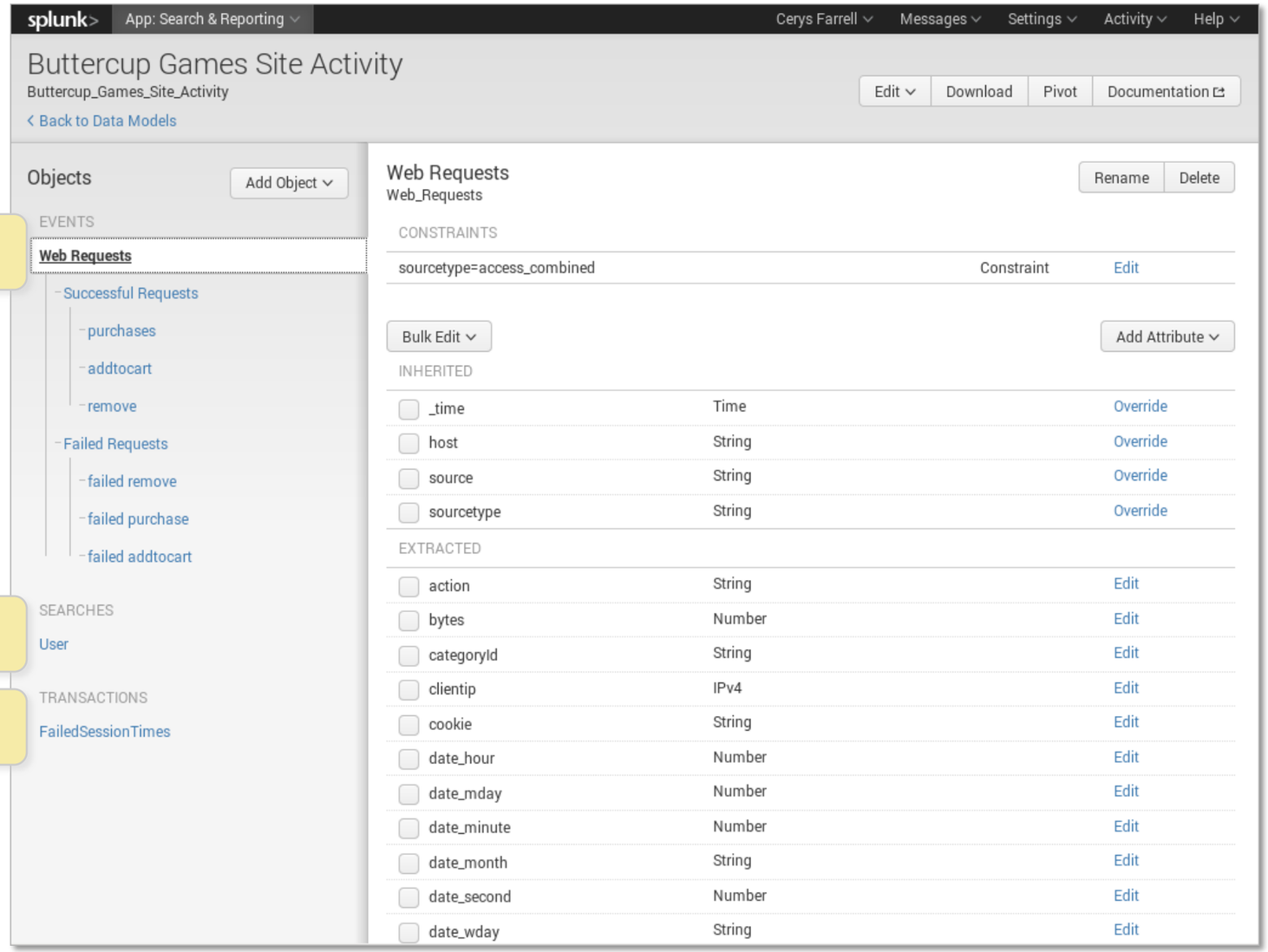
Overview of Data Models

- Hierarchically structured data set that generates searches and drives Pivot
  - Pivot reports are created based on data models



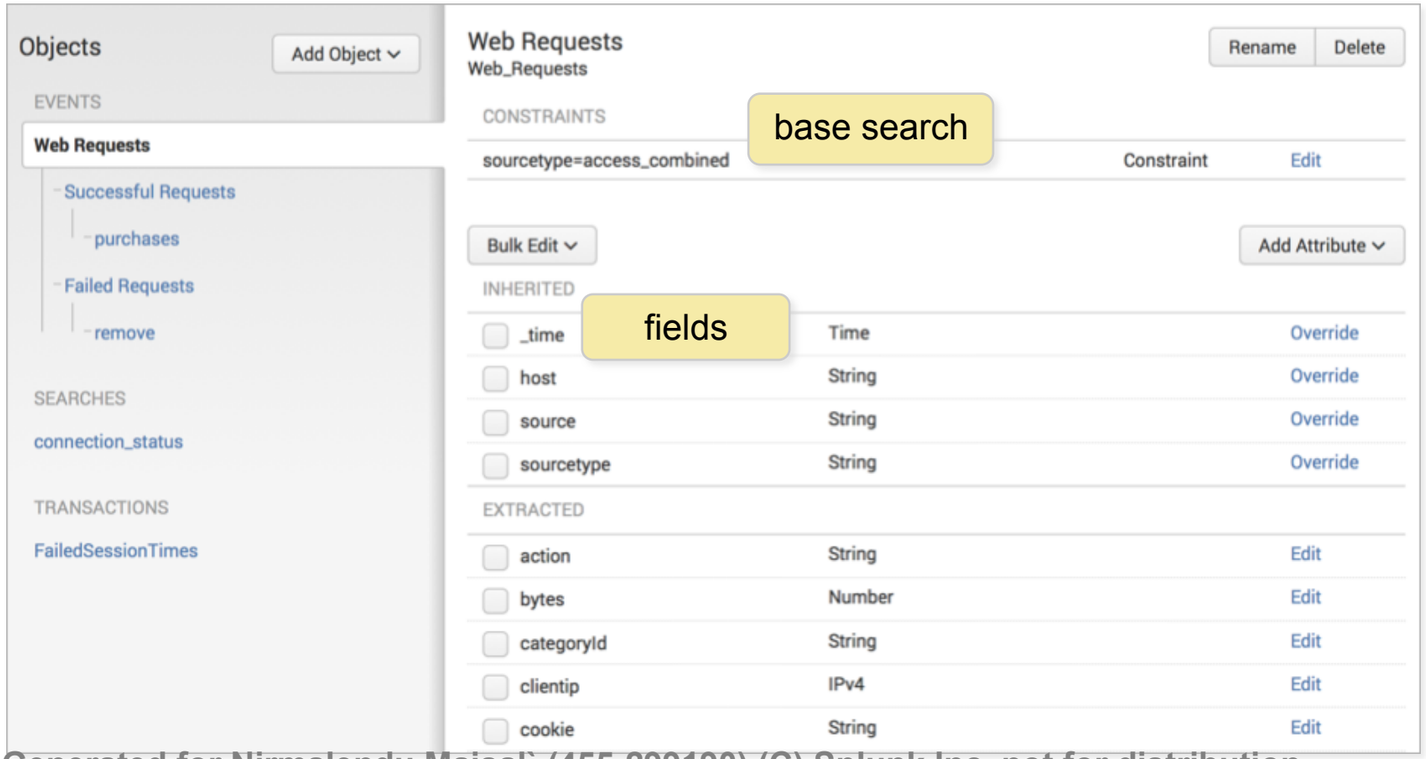
Data Model Objects

- Data models consist of 3 types of objects
  1. Events
  2. Searches
  3. Transactions

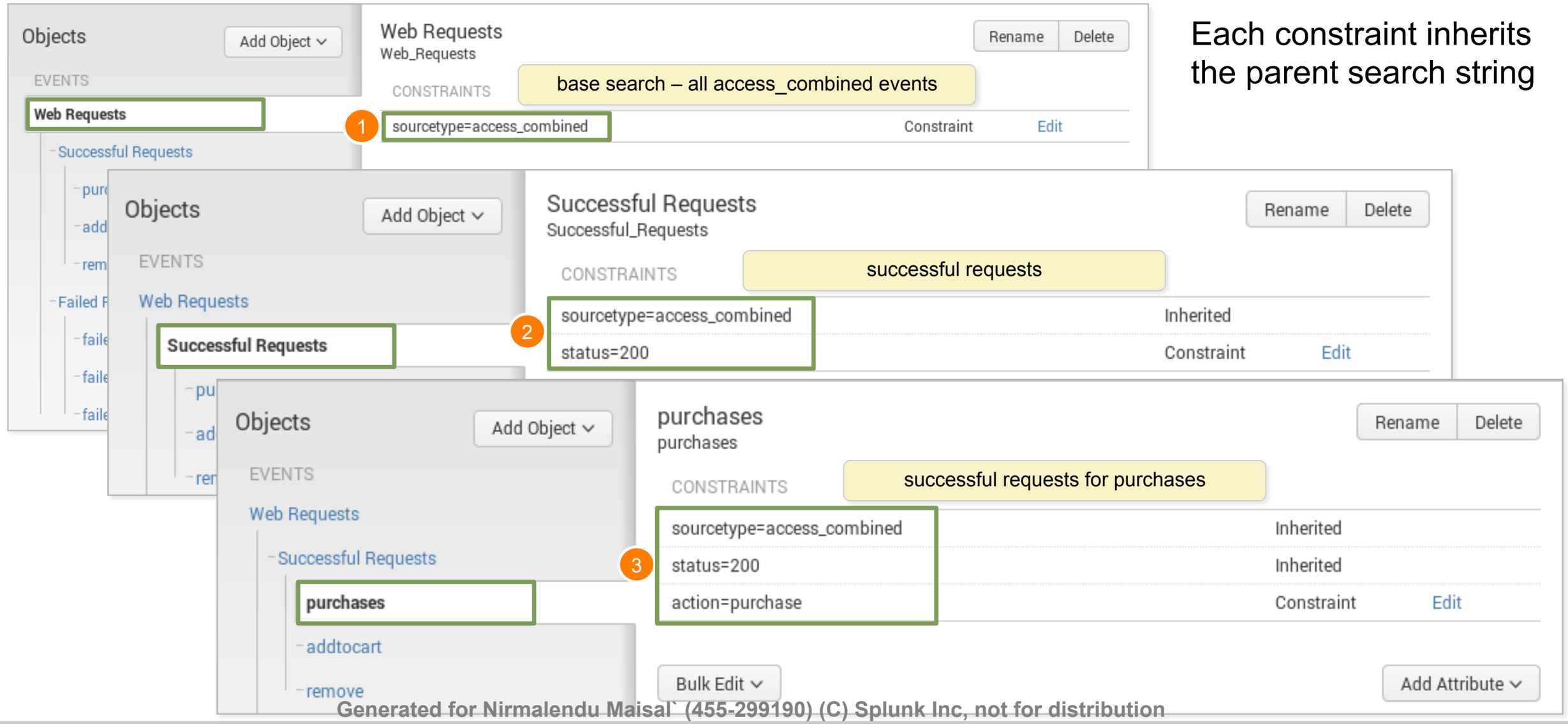


Data Model Events

- **Event objects** contain constraints and attributes
- **Constraints** are essentially the search broken down into a hierarchy
- **Attributes** are the fields and properties associated with the events



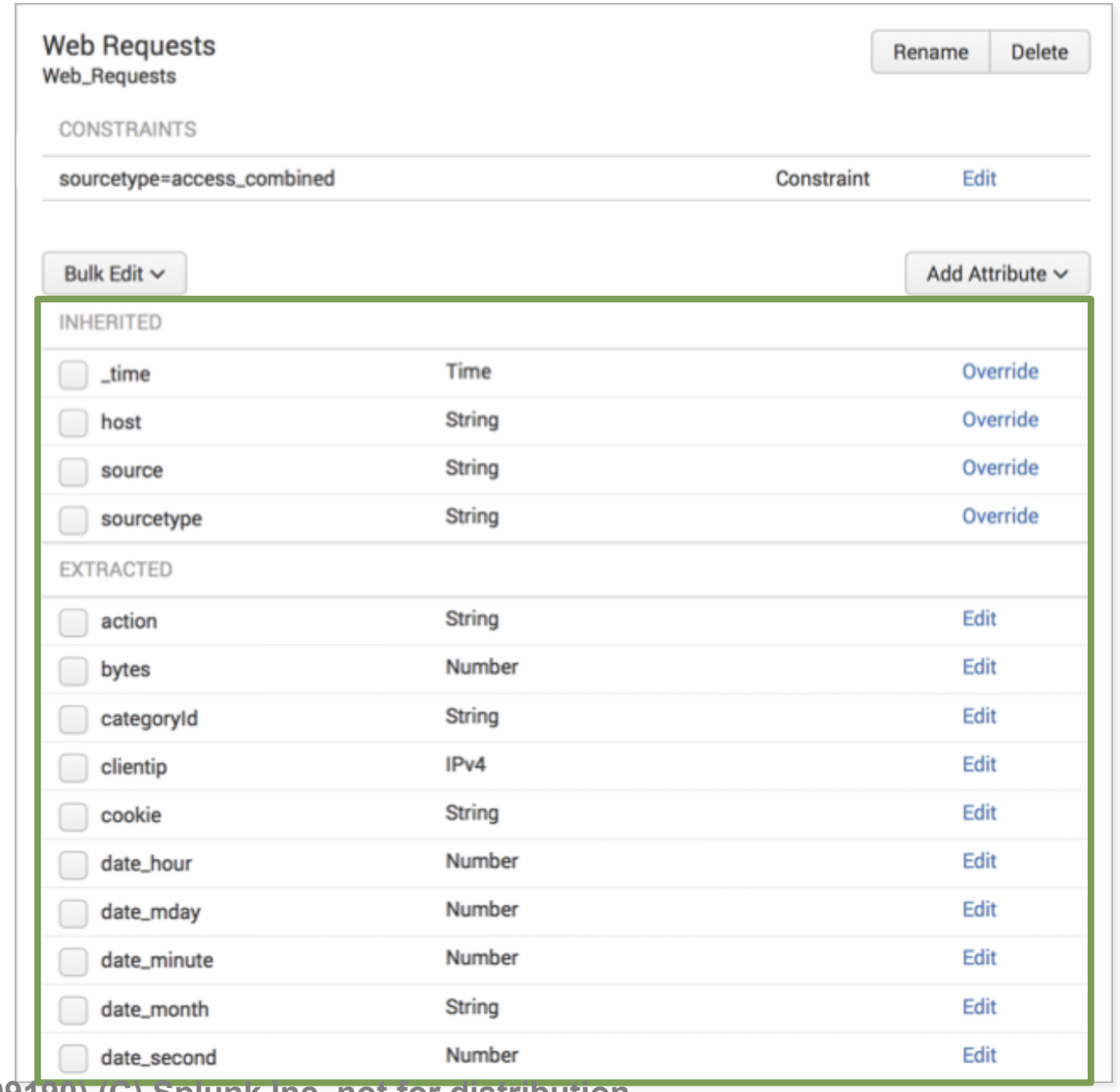
Event Object Hierarchy and Constraints



Each constraint inherits the parent search string

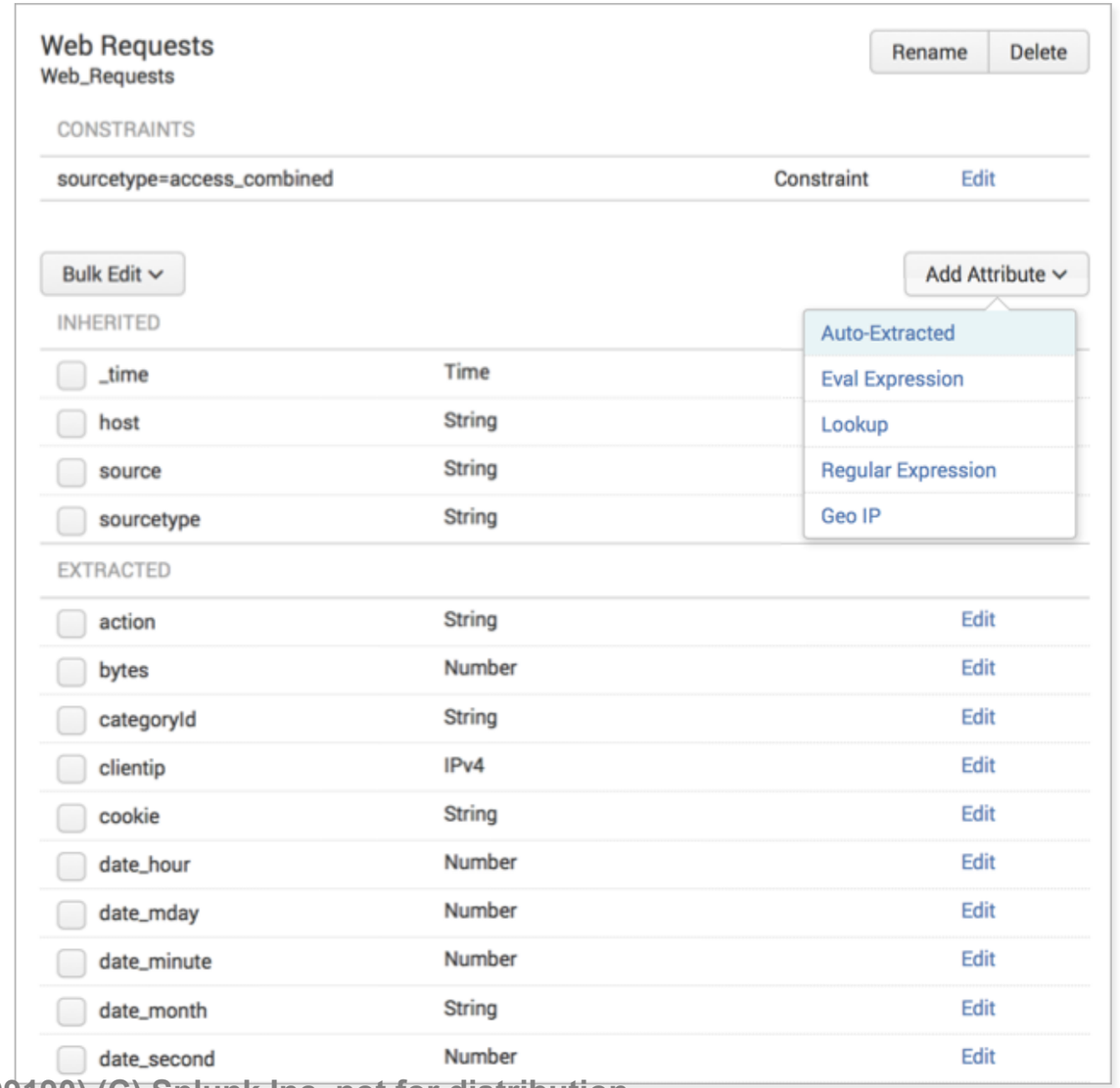
Object Attributes

- Attributes are the fields you want to include in the objects
- Like constraints, attributes are inherited from parent objects



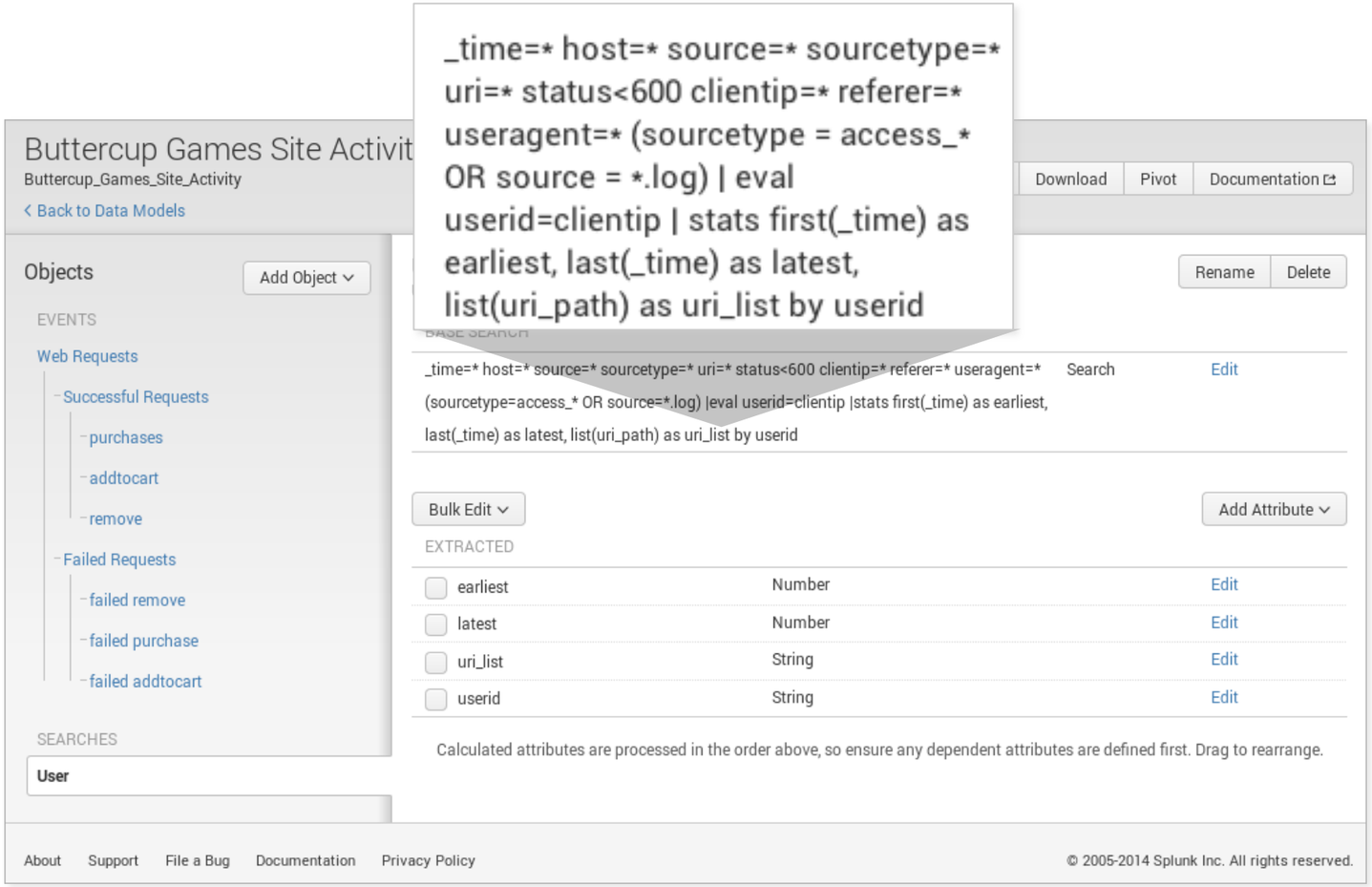
Object Attributes (cont.)

- **Auto-Extracted** – can be default fields or manually extracted fields
- **Eval Expression** – a new field based on an expression that you define
- **Lookup** – leverage an existing lookup table
- **Regular Expression** – extract a new field based on regex
- **Geo IP** – add geographical fields such as latitude/longitude, country, etc.



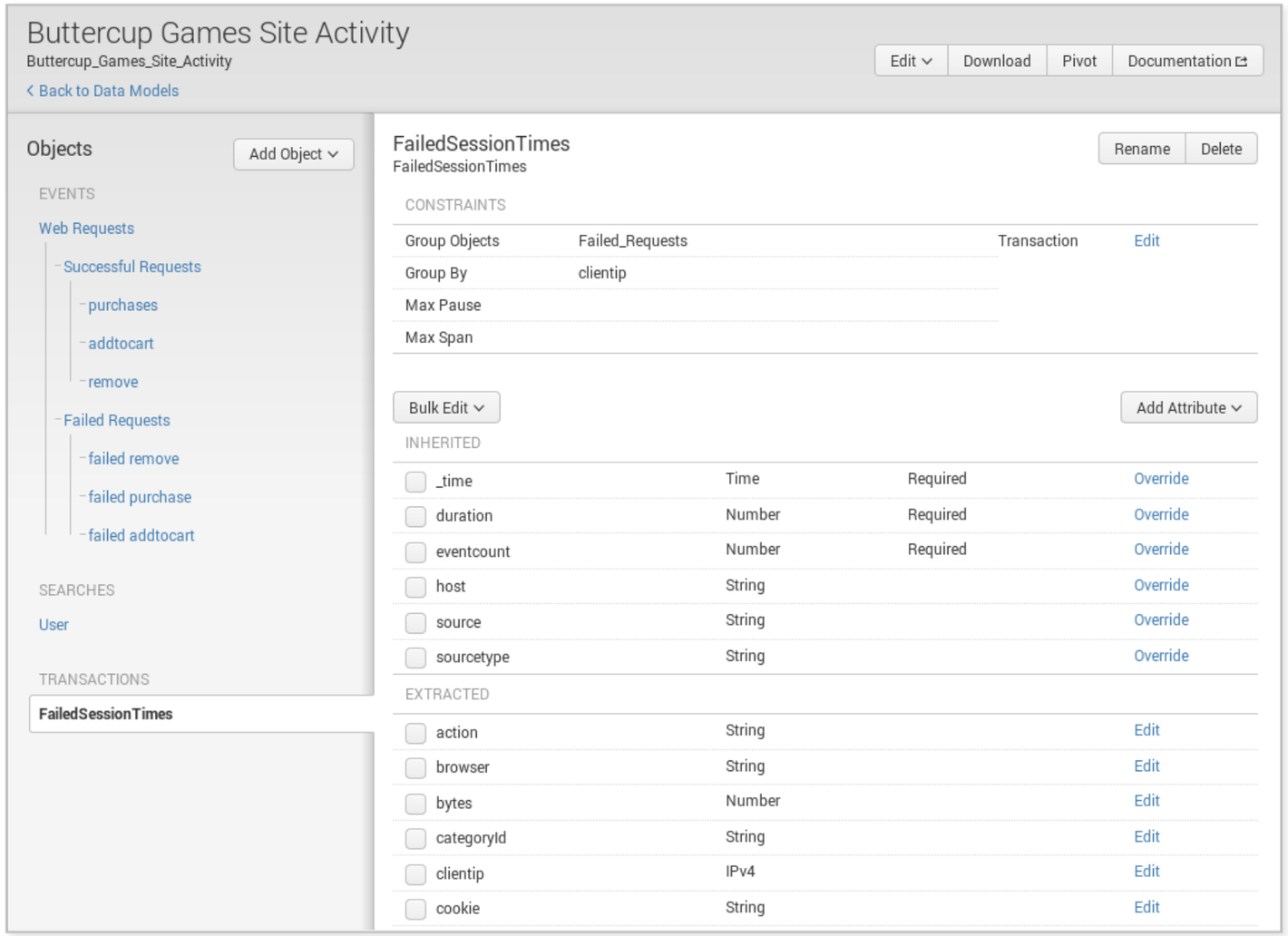
Data Model Search Objects

- Arbitrary searches that include transforming commands to define the dataset that they represent
- Search objects can also have attributes, which are added via the **Add Attribute** button



Data Model Transaction Objects

- Enable the creation of objects that represent transactions
- Use fields that have already been added to the model using event or search objects

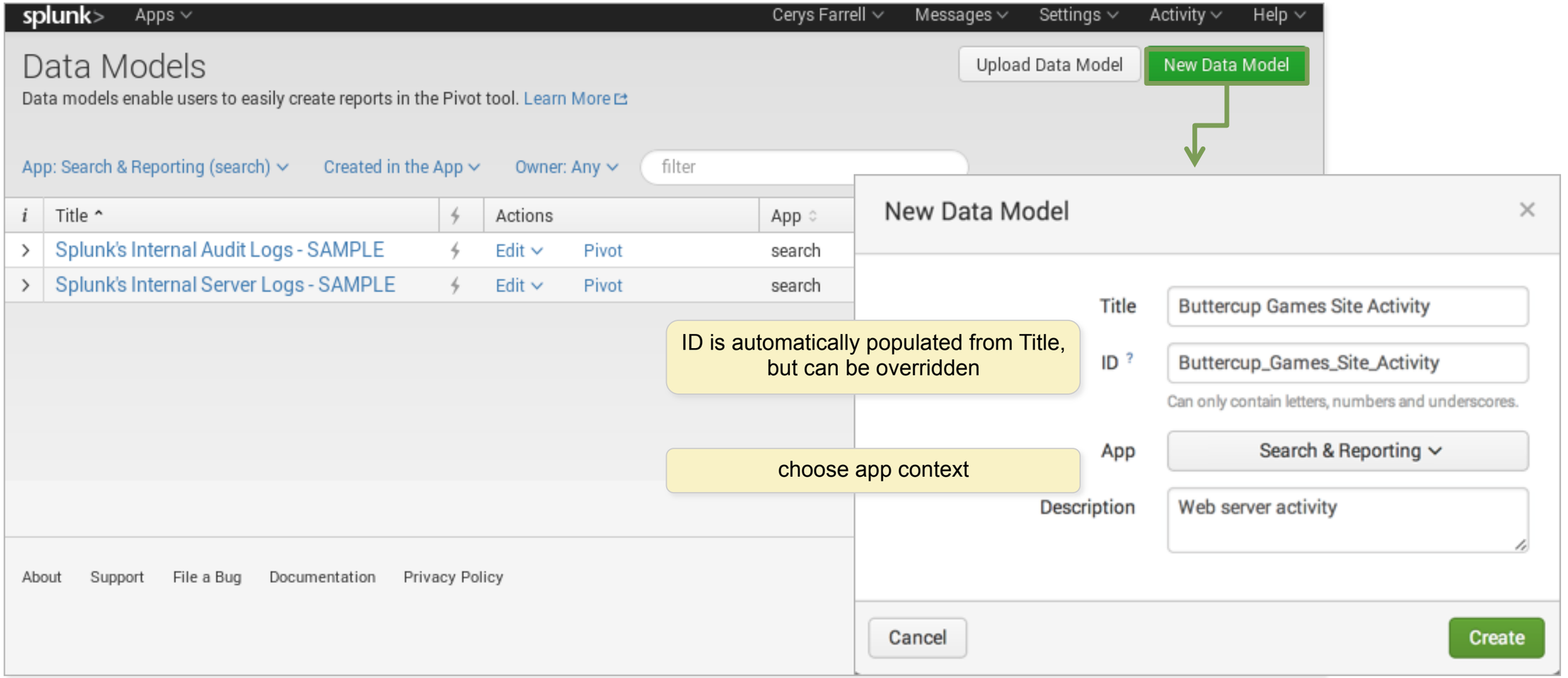


Search and Transaction Object Considerations

- There must be at least one event or search object before adding a transaction object
- Search and Transaction objects cannot benefit from persistent data model acceleration
  - Acceleration is discussed later in the module
- Think carefully about the reports your users will run
  - Can the same report be achieved with event objects?
- As you learn to create data models, consider the types of reports your users will run
  - Will they need raw events or transactional data?

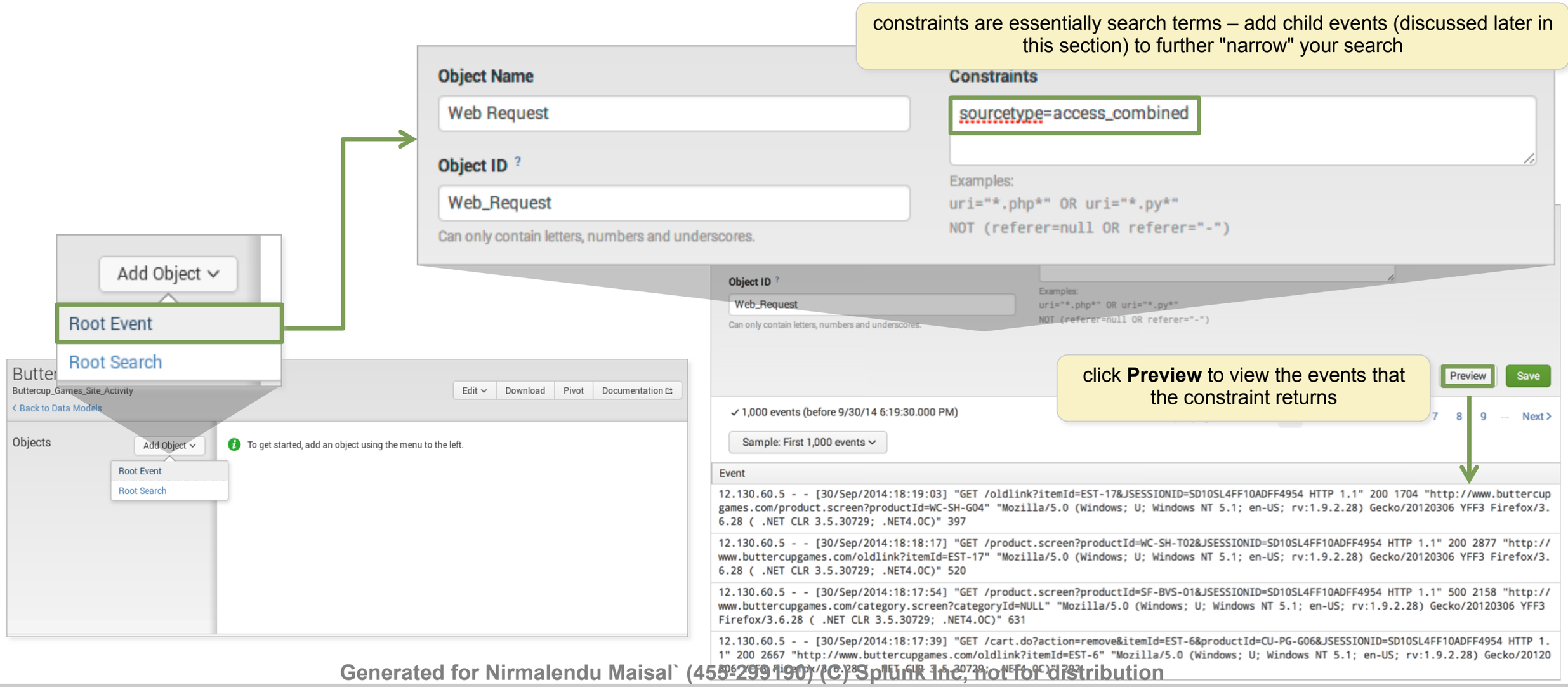
Creating a Data Model

Settings > Data Models



Adding a Root Event

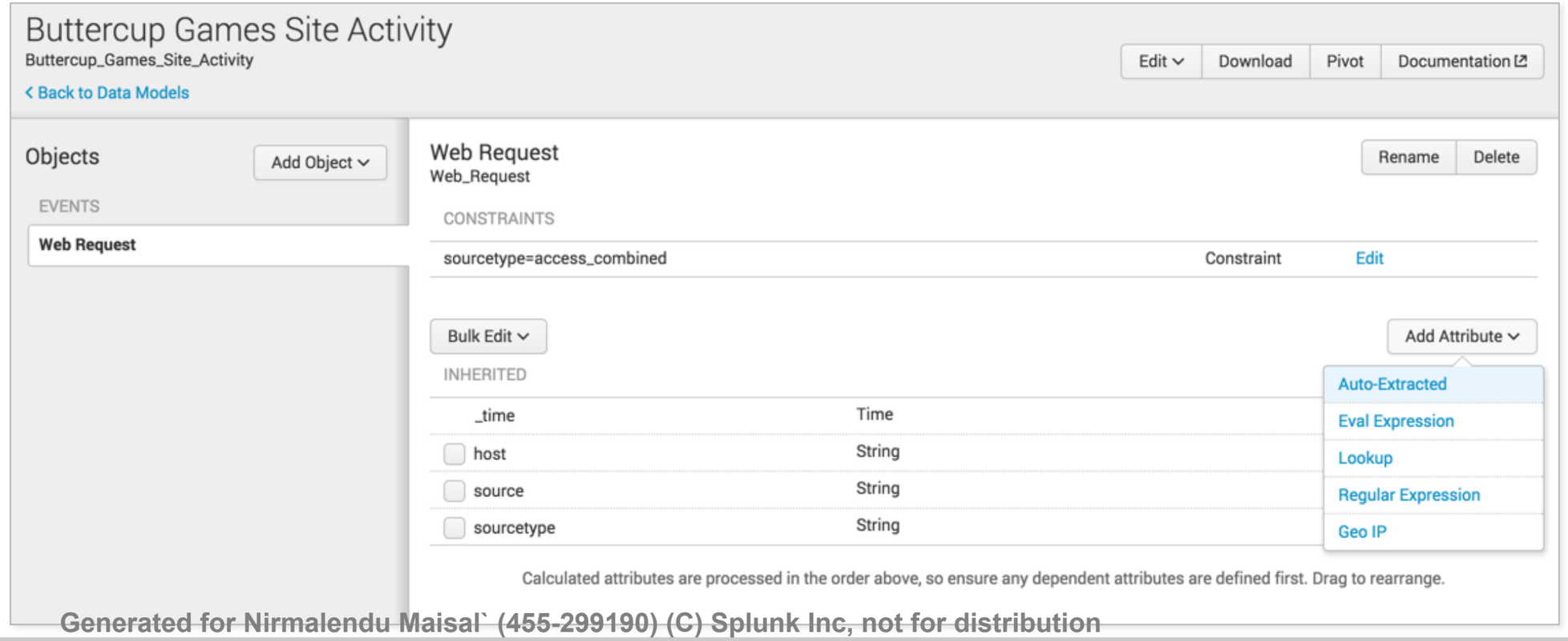
constraints are essentially search terms – add child events (discussed later in this section) to further "narrow" your search



click **Preview** to view the events that the constraint returns

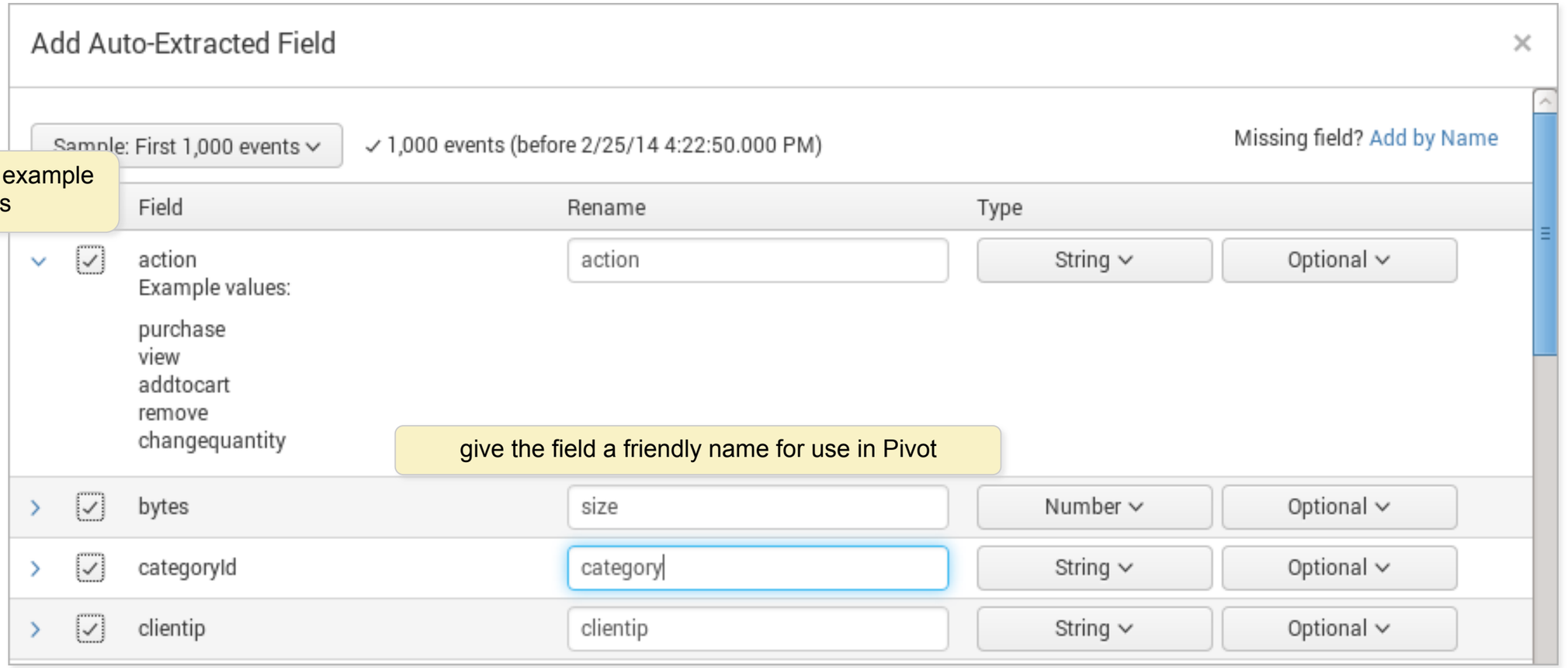
Adding a Root Event (cont.)

- In this example, the root event of this data model represents all web requests
- The Inherited attributes are default fields.
- Use **Add Attributes > Auto-Extracted** to add more fields



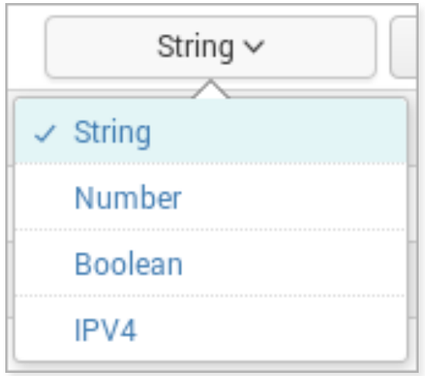
Adding Attributes – Auto-Extracted (Fields)

Fields that already exist for the constraint can be added as attributes to the data model



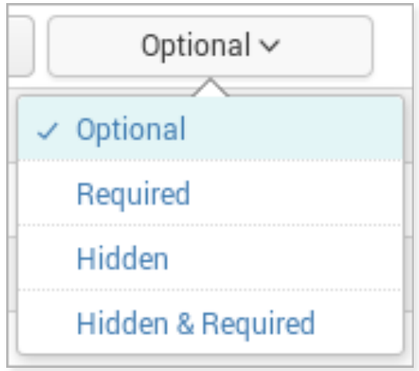
Attribute Types

- **String:** Field values are recognized as alpha-numeric
- **Number:** Field values are recognized as numeric
- **Boolean:** Field values are recognized as true/false or 1/0
- **IPV4:** Field values are recognized as IP addresses
  - This is an important field type, as at least one IPV4 attribute type must be present in the data model in order to add a Geo IP attribute



Attribute Flags

- **Required:** Only events that contain this field are returned in Pivot
- **Optional:** This field doesn't have to appear in every event

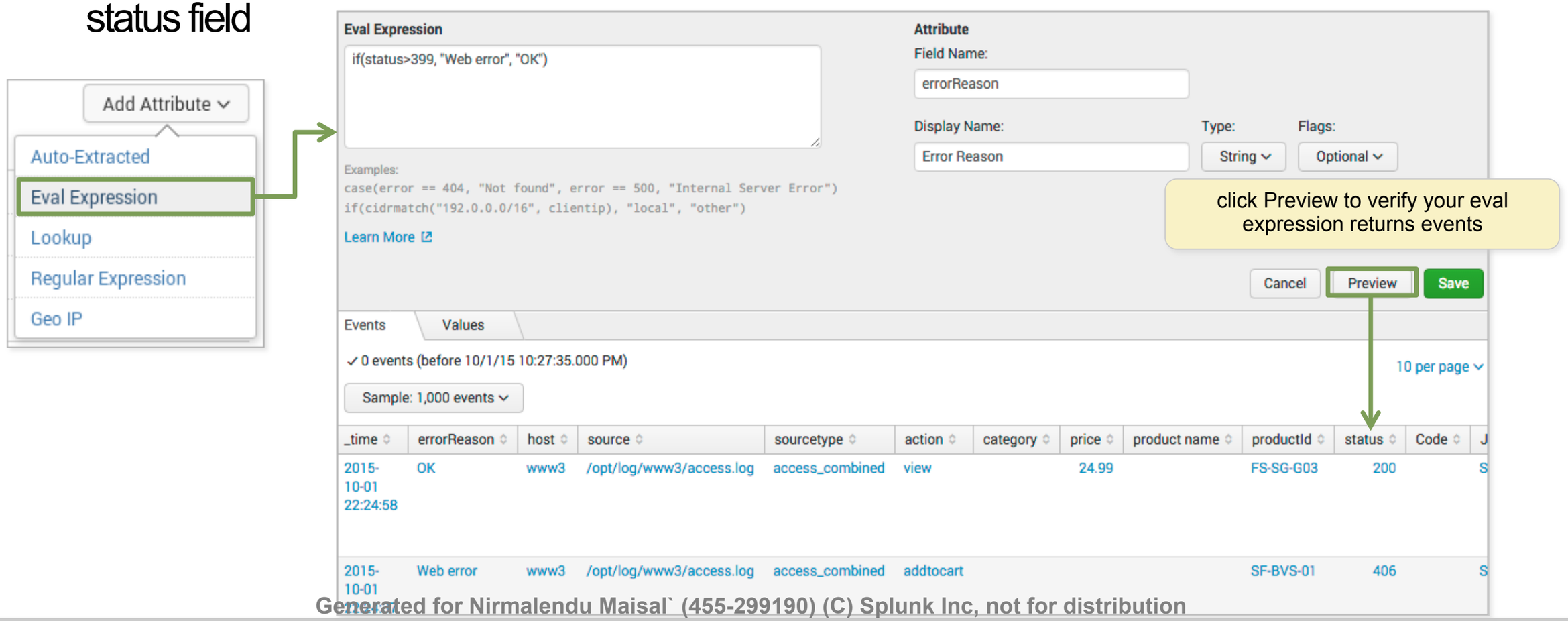


- **Hidden:** This field is not displayed to Pivot users when they select the object in Pivot
  - Use for fields that are only being used to define another attribute, such as an eval expression
- **Hidden & Required:** Only events that contain this field are returned, and the fields are hidden from use in Pivot

Adding Attributes – Eval Expressions

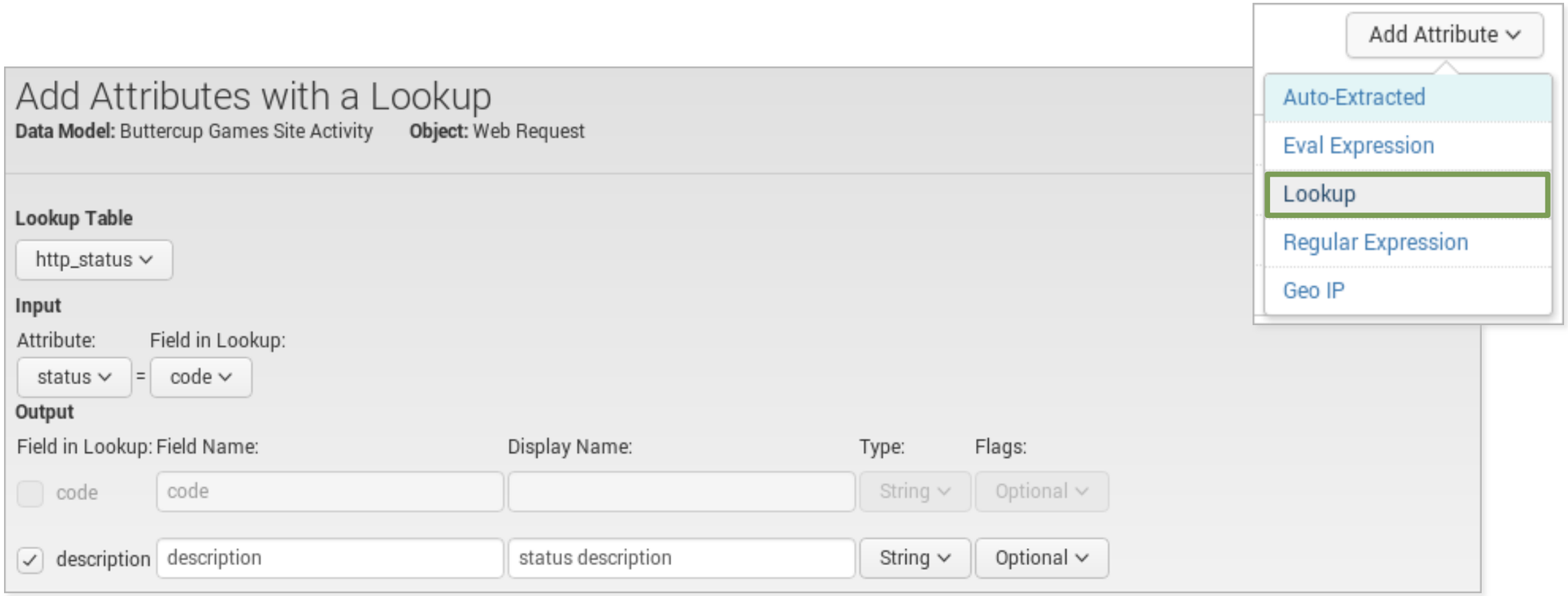
You can define a new field using an eval expression

- In this example, we create a field named Error Reason that evaluates the value of the status field



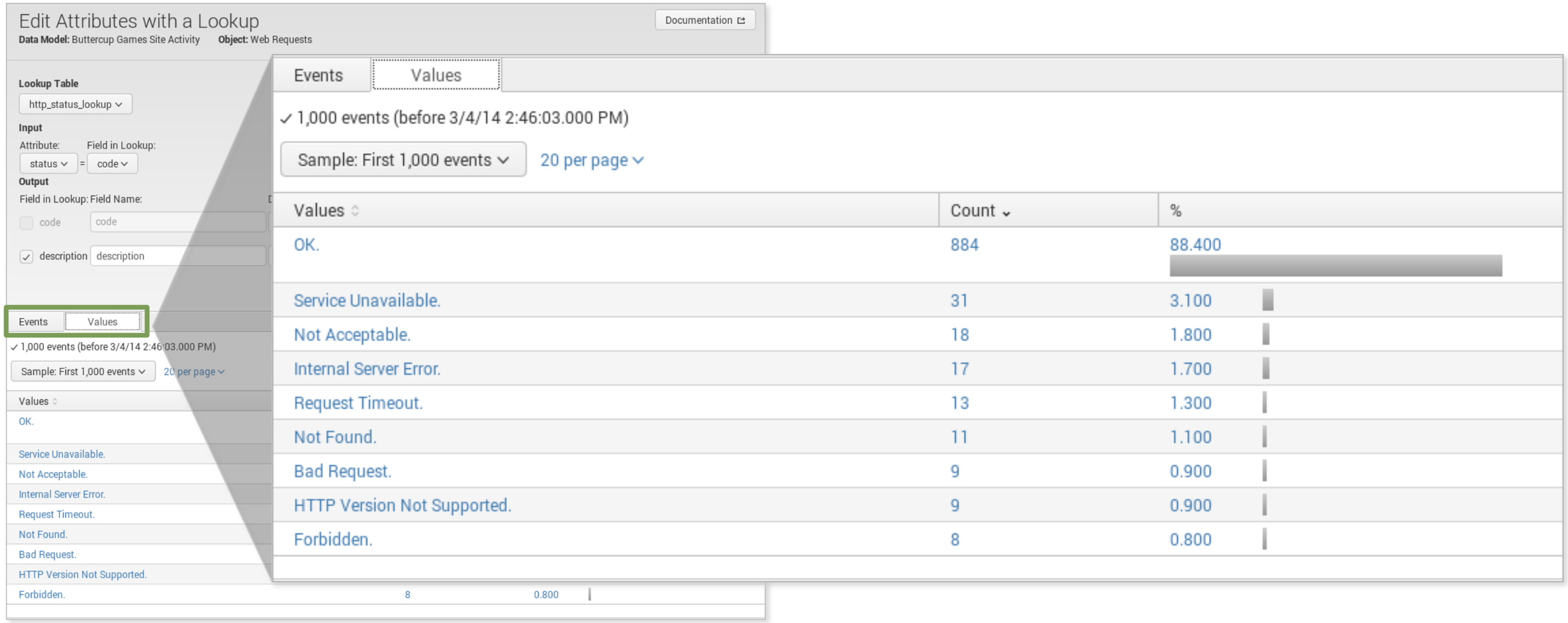
Adding Attributes – Lookups

- Leverage an existing lookup definition to add fields to your event object
- Configure the lookup attribute in the same way as an automatic lookup

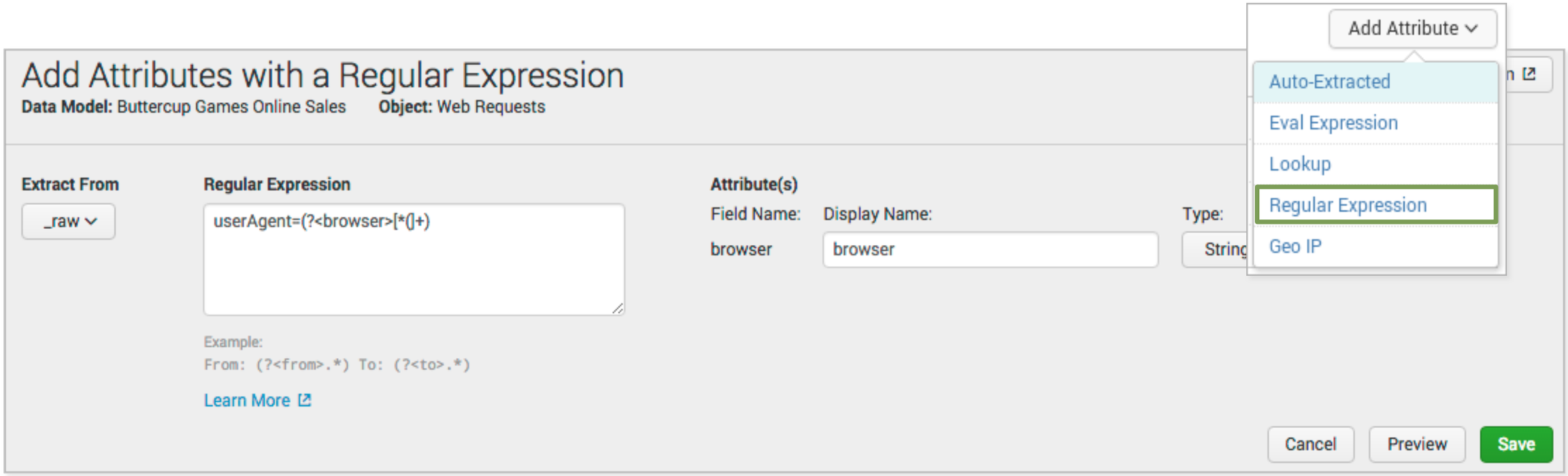


Adding Attributes – Lookups (cont.)

- Use Preview to test your lookup settings
- Use the Events and Values tab to verify your results

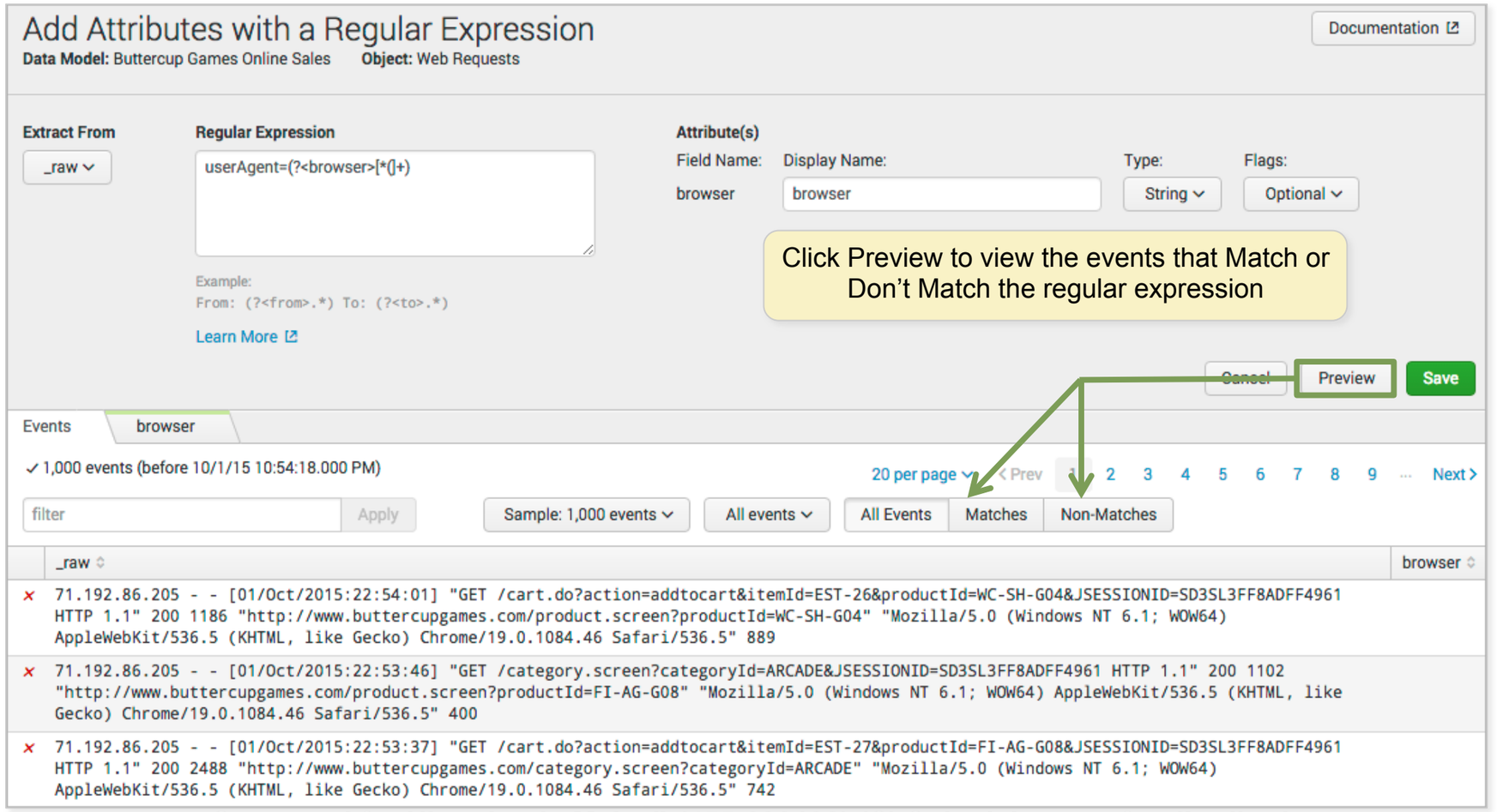


Adding Attributes – Regular Expression



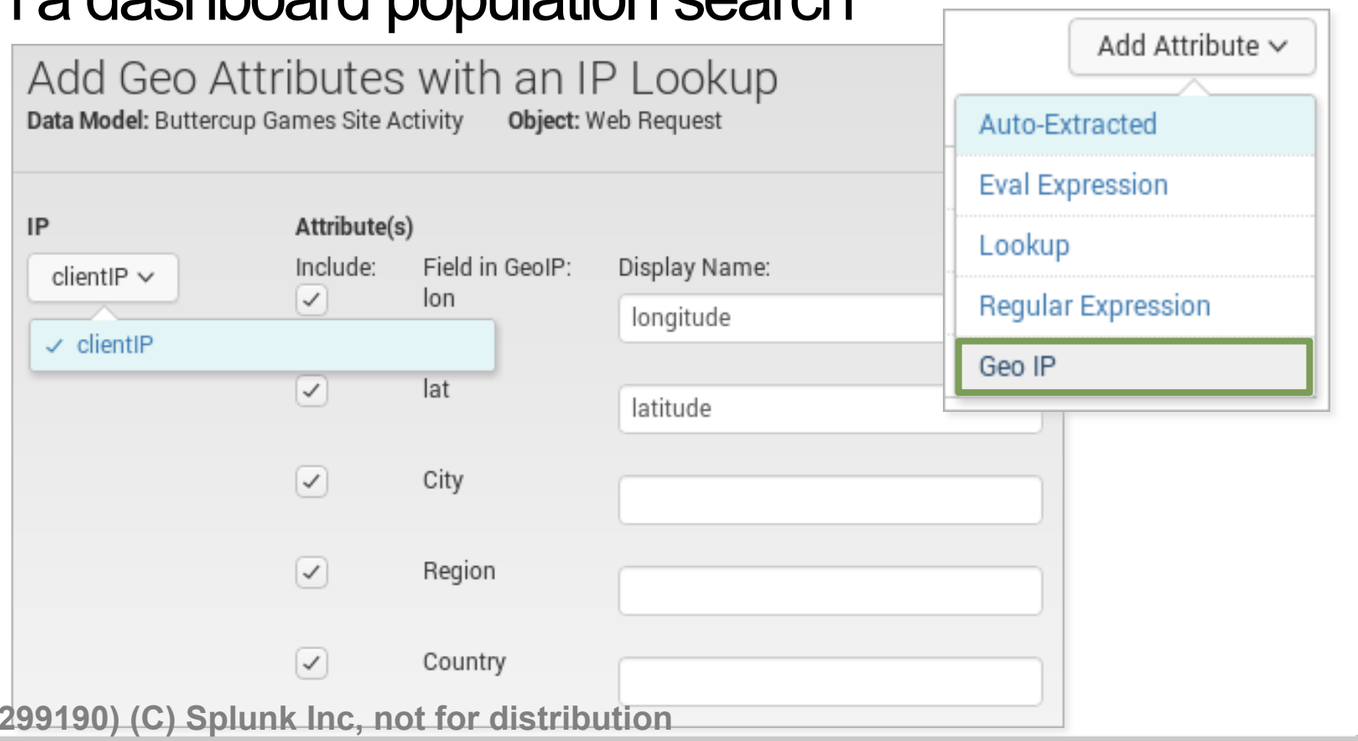
Adding Attributes – Regular Expression (cont.)

You can define a new field using a regular expression



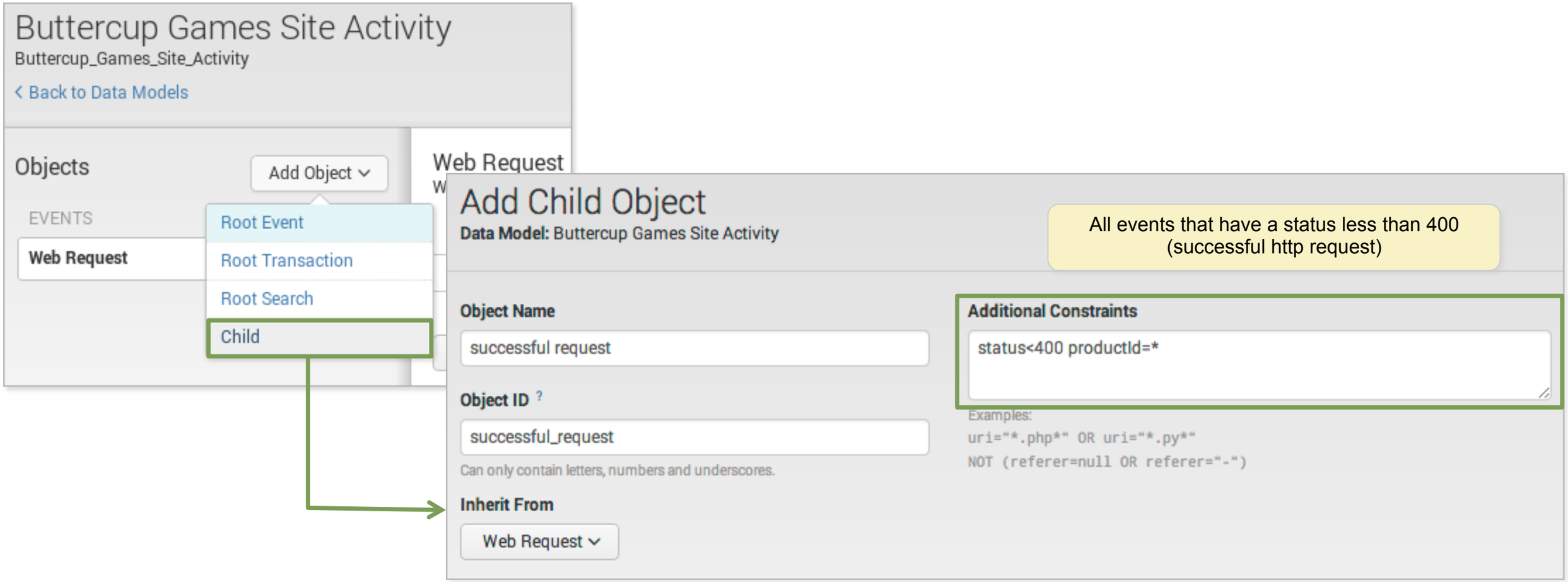
Adding Attributes - GeoIP

- Map visualizations require latitude/longitude fields
- To use Geo IP Lookup, at least one IP field must be configured as an IPv4 type
- While the map function isn't available in Pivot, the data model can be called using the **| pivot** command and <map> element in a dashboard population search
  - Select the field that contains the mapping to lat/lon
  - Identify the lat/lon and geo fields in the data



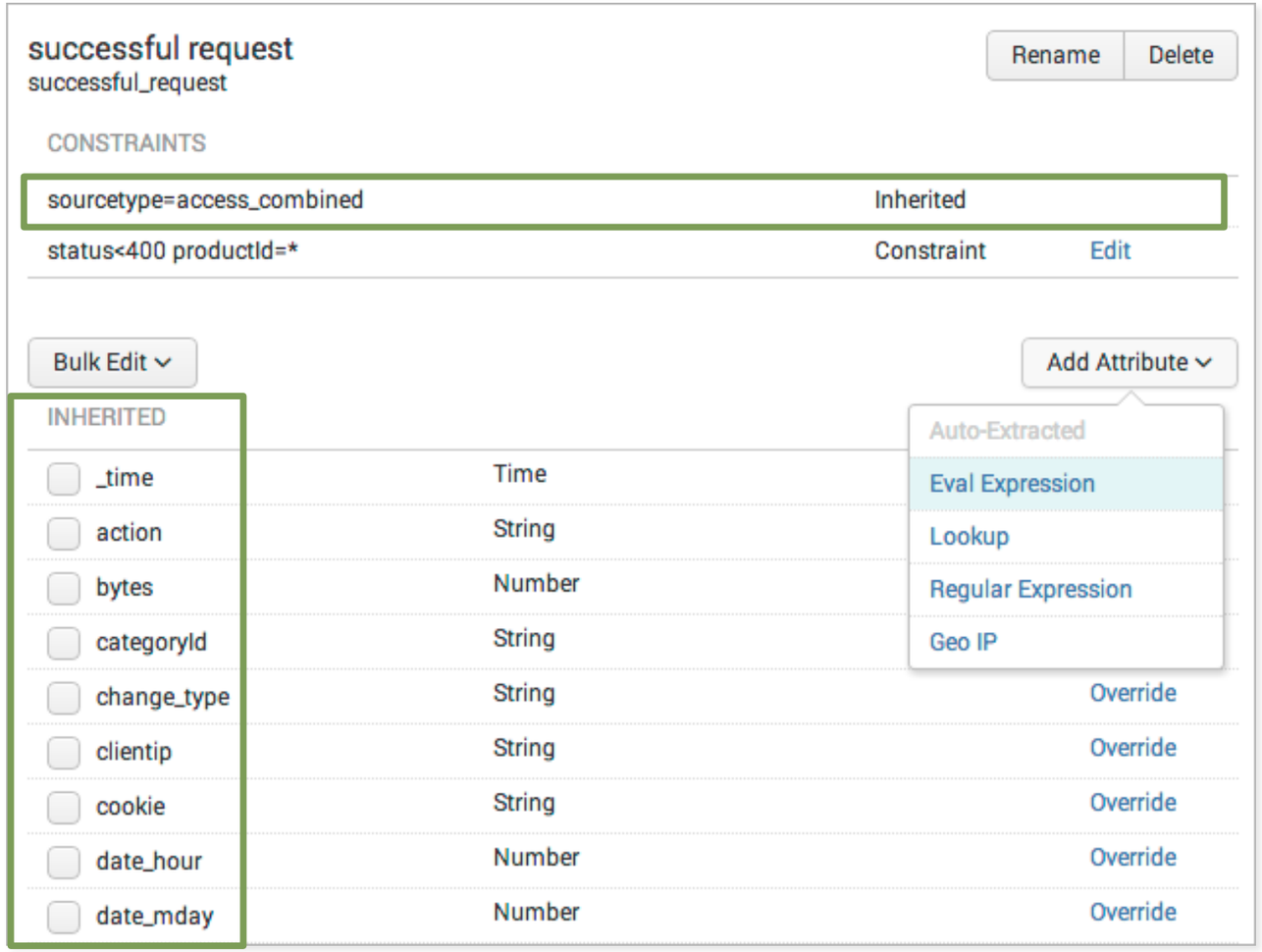
Adding Child Events

When you define a new child object, you give it one or more additional constraints



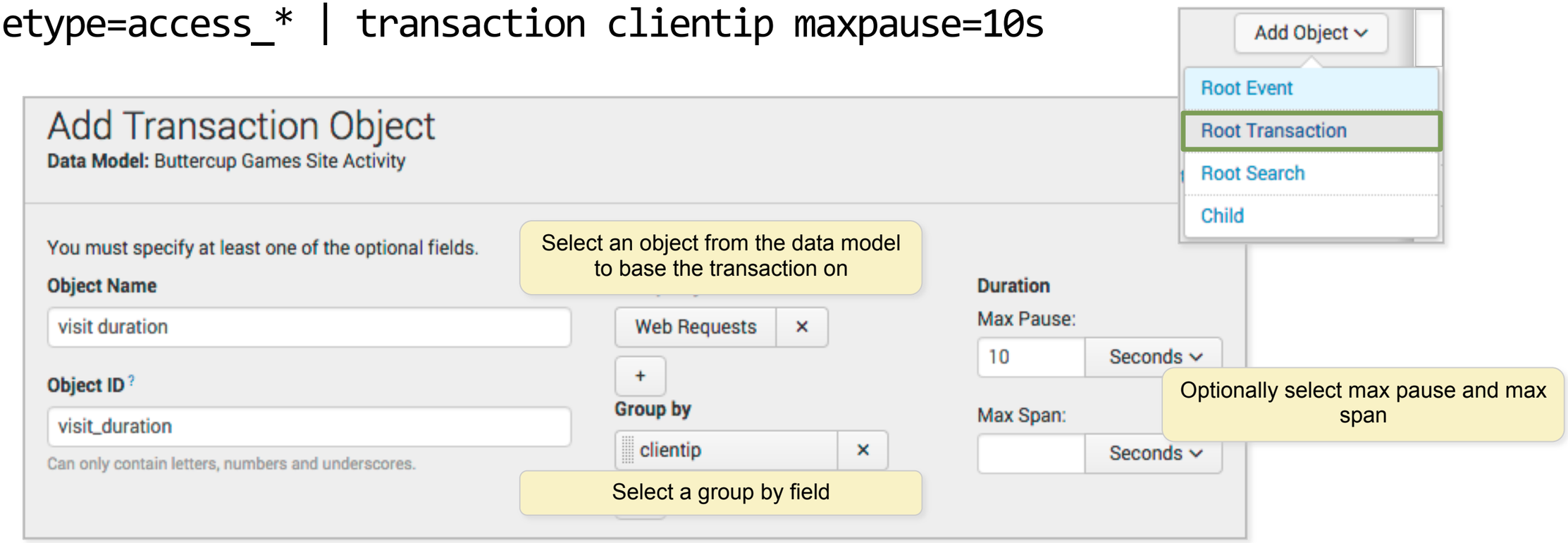
Adding Child Events (cont.)

- Child events inherit all attributes from the parent events
  - You can add more attributes to child events



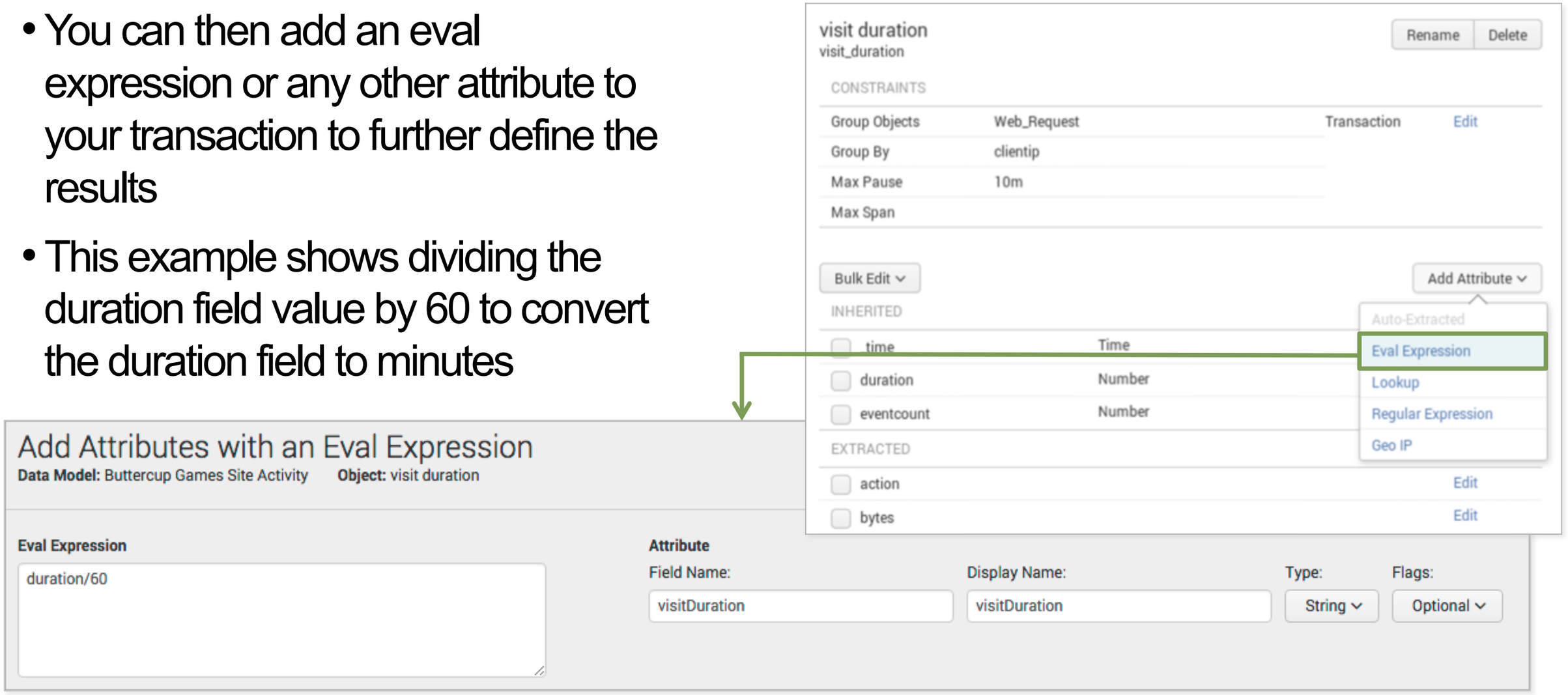
Adding a Transaction

- You can add a transaction to the data model
- The transaction object below would equate to the search:
  `sourcetype=access_* | transaction clientip maxpause=10s`



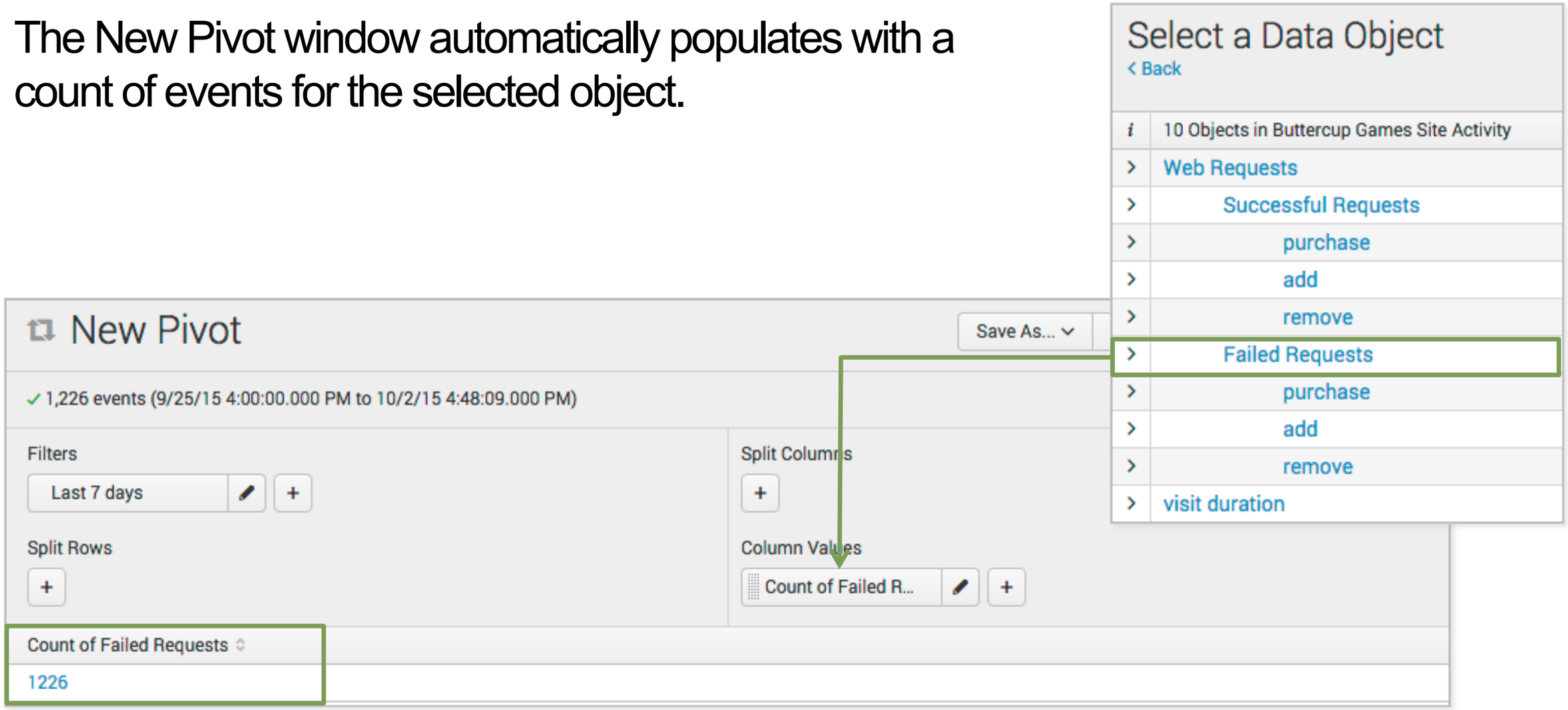
Adding a Transaction (cont.)

- You can then add an eval expression or any other attribute to your transaction to further define the results
- This example shows dividing the duration field value by 60 to convert the duration field to minutes



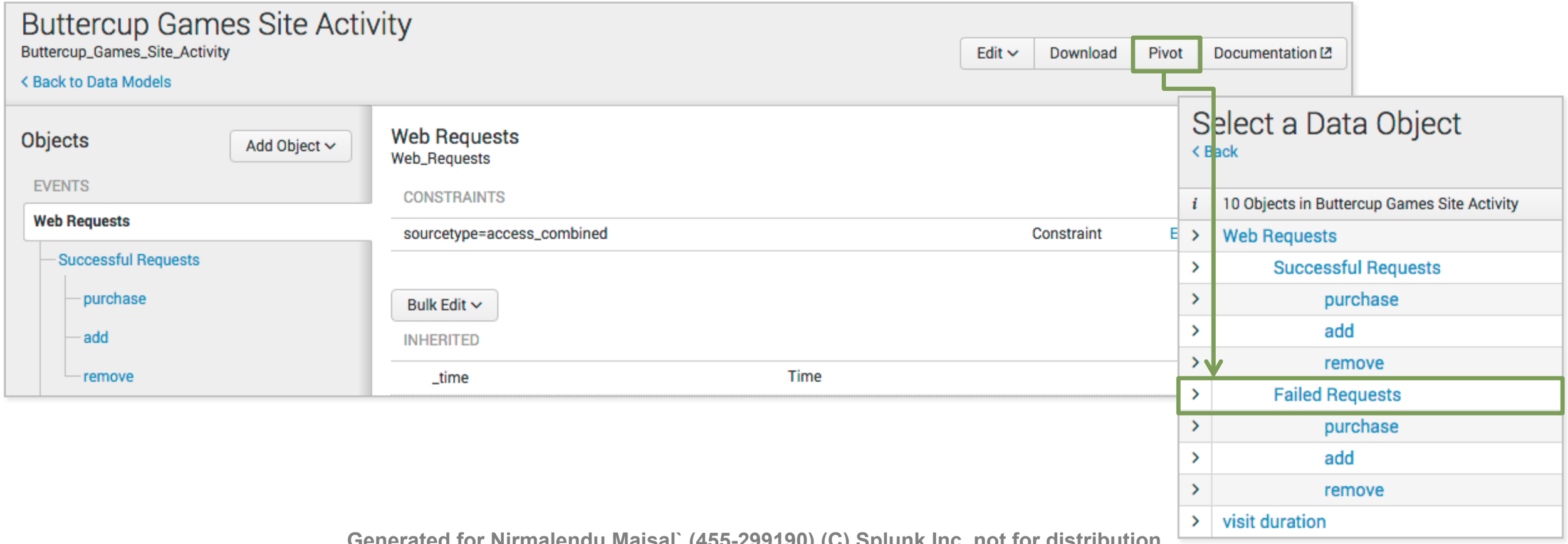
Using the Data Model in Pivot (cont.)

The New Pivot window automatically populates with a count of events for the selected object.



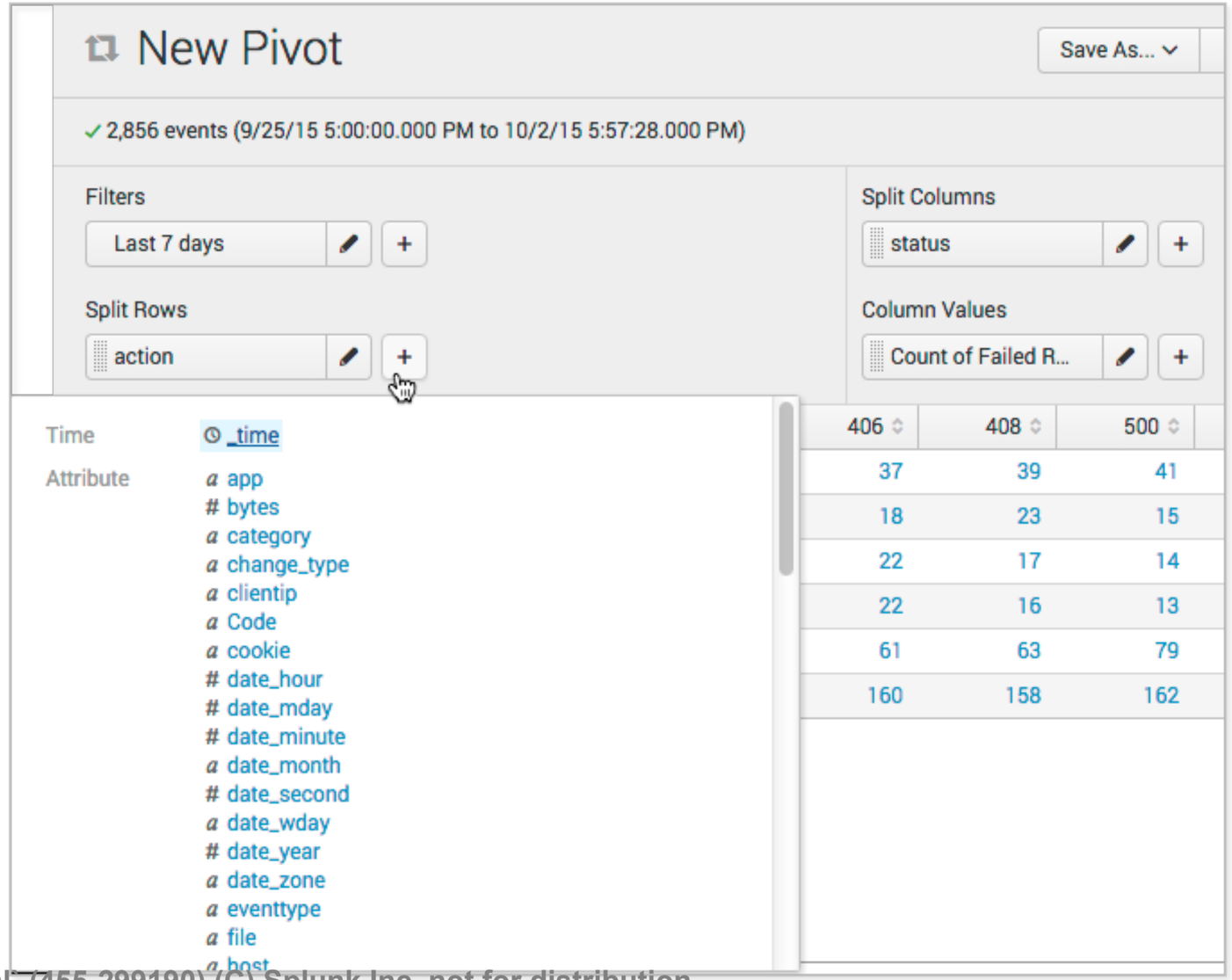
Using the Data Model in Pivot

- Click Pivot to access the Select an Object window
- Choose an object from the selected data model to begin building the report



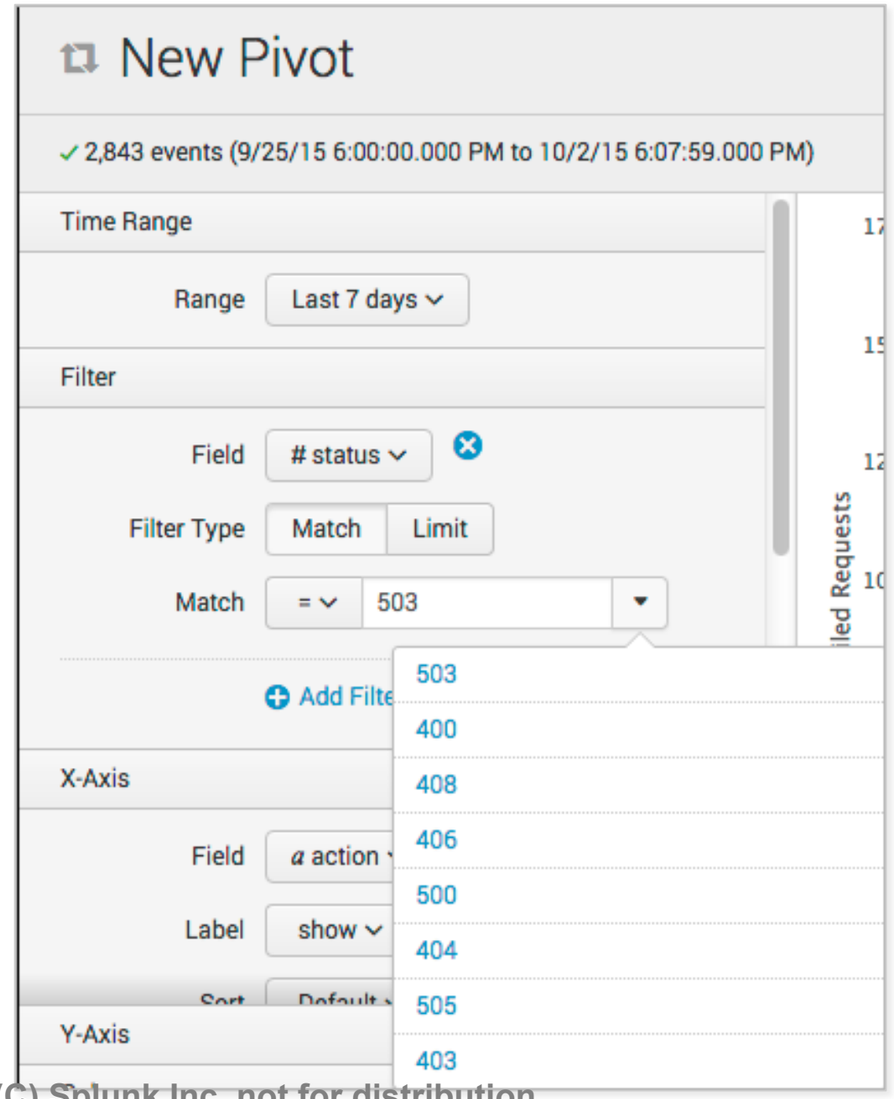
Pivot – Using Attributes

- The attributes associated with each object are available as splits for rows or columns
- In this example, the Pivot report will show a count of failed request actions by status

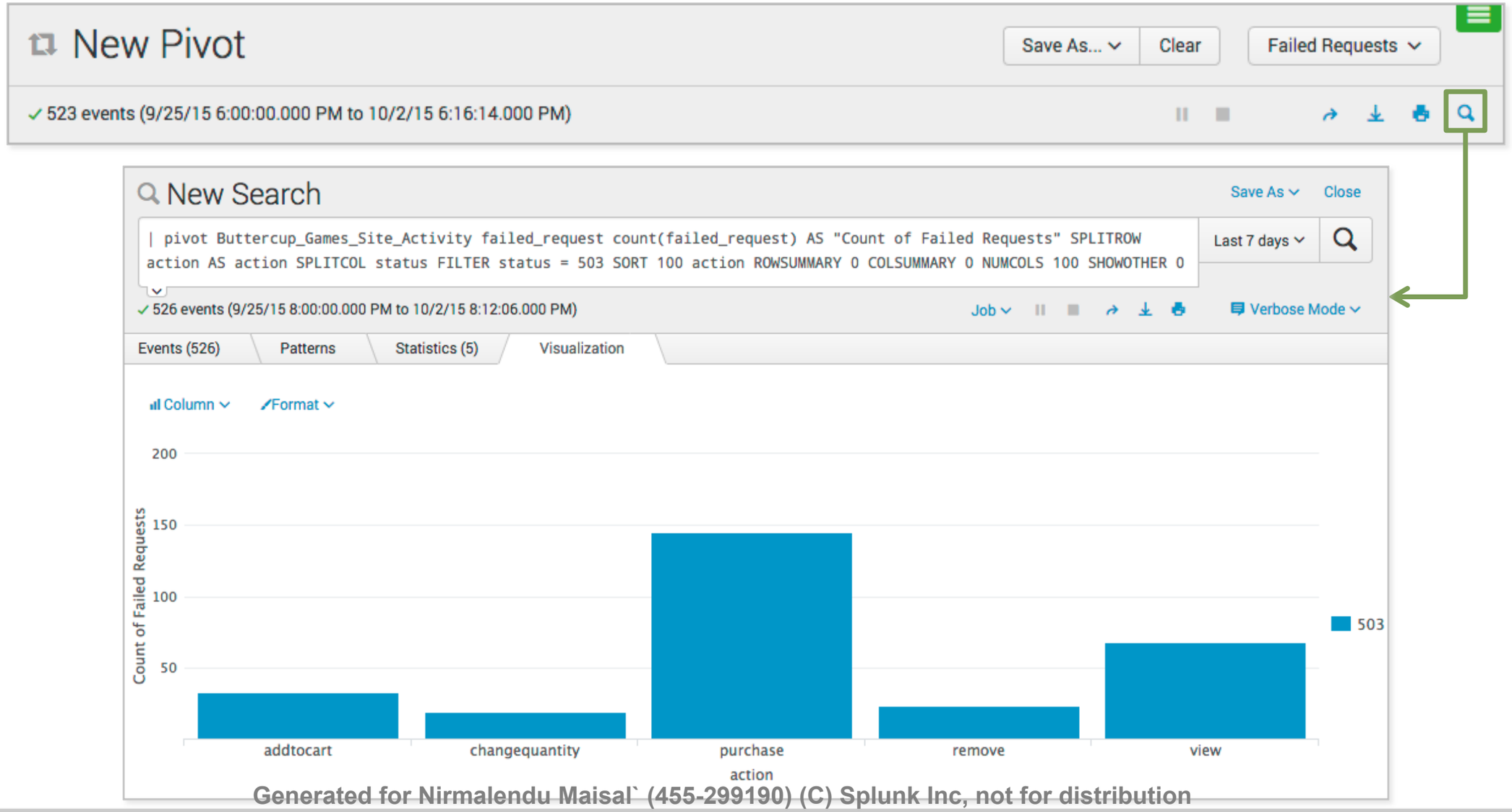


Pivot – Using Attributes (cont.)

- Attributes are also available for use as filters
- In this example, the Pivot report is filtered to only return results where status=503



Underlying Search



Underlying Search (cont.)

Data model name

Object name

```
| pivot Buttercup_Games_Site_Activity failed_request
count(failed_request) AS "Count of Failed requests"
```

Split row field (or attribute)

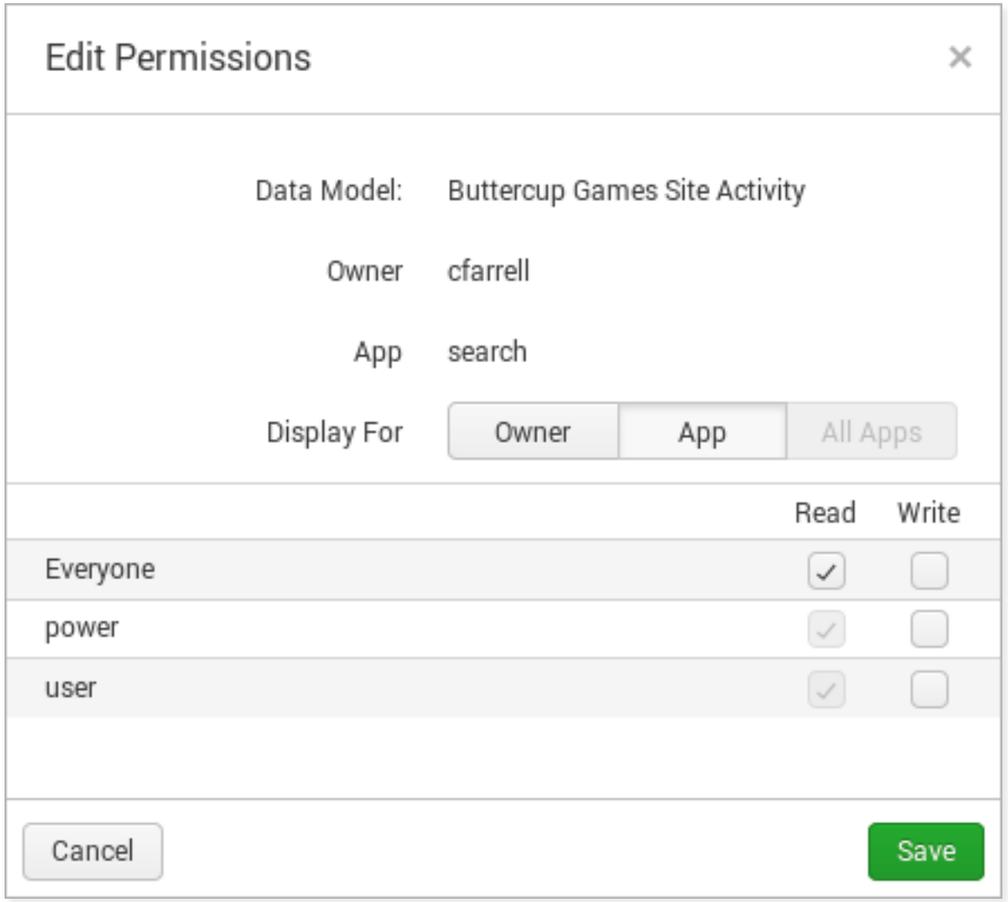
```
SPLITROW action AS action TOP 100
count(failed_request)
```

Split column field (or attribute) and filter field/value pair

```
SPLITCOL status
FILTER status = 503
```


Set Permissions

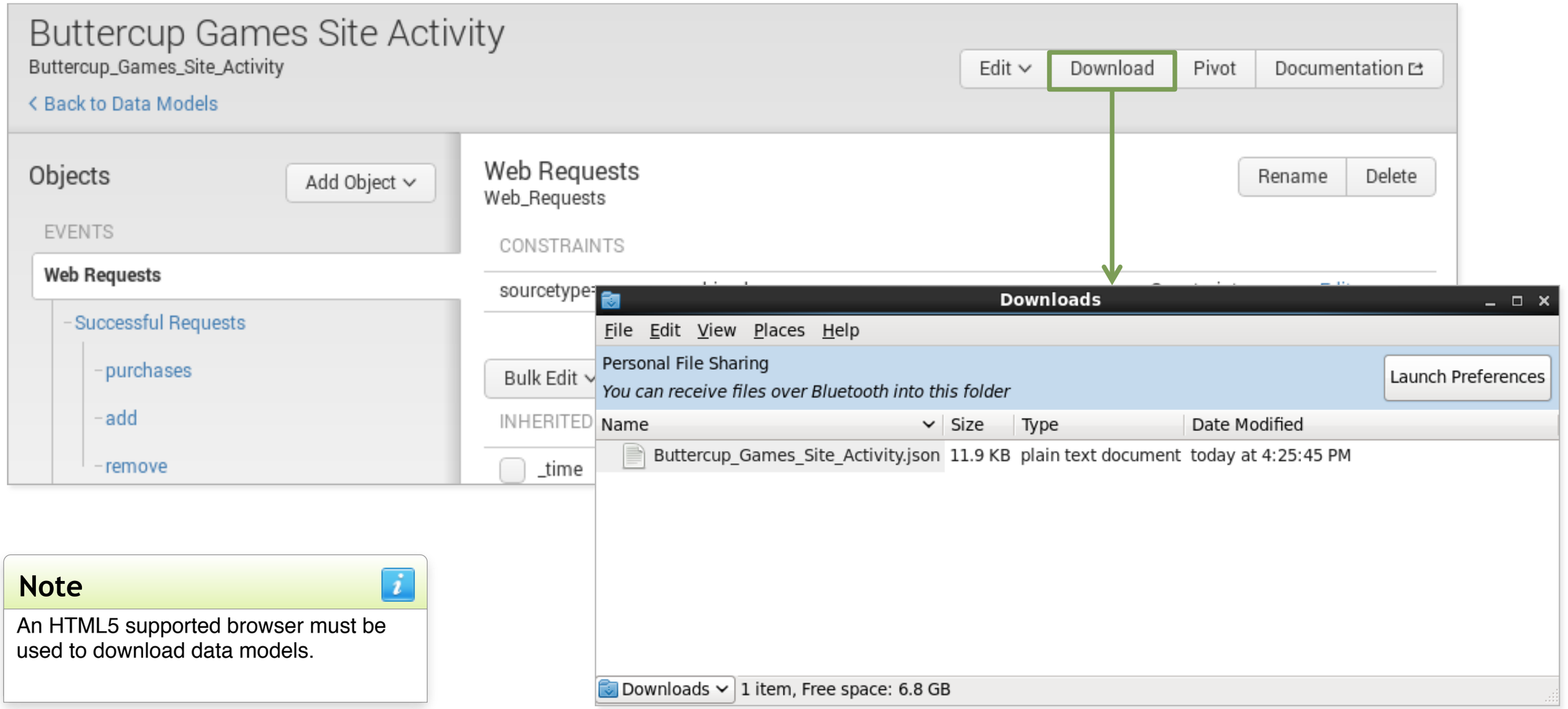
- When a data model is created, the owner can determine access based on the following permissions:
  - Who can see the data models
    - Owner, App, or All Apps
  - Which users can perform which actions (Read/Write)
    - Everyone
    - Power
    - User
    - Admin-defined roles, if applicable



Download and Upload Data Models

- Use the Splunk Web interface to download or upload data models:
  - Back up important data models
  - Collaborate with other Splunk users to create/modify/test data models
  - Move data models from a test environment to production instance

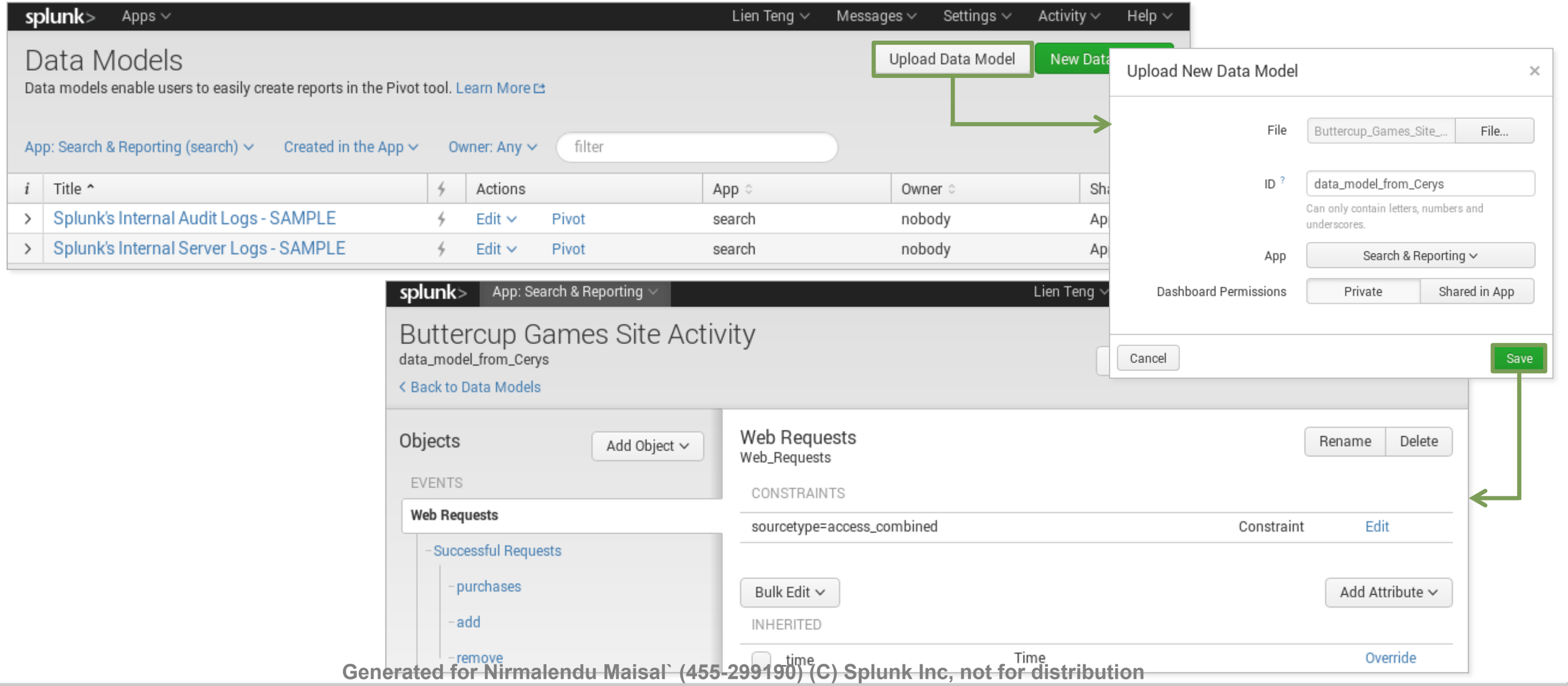
Downloading a Data Model



Note

An HTML5 supported browser must be used to download data models.

Uploading a Data Model

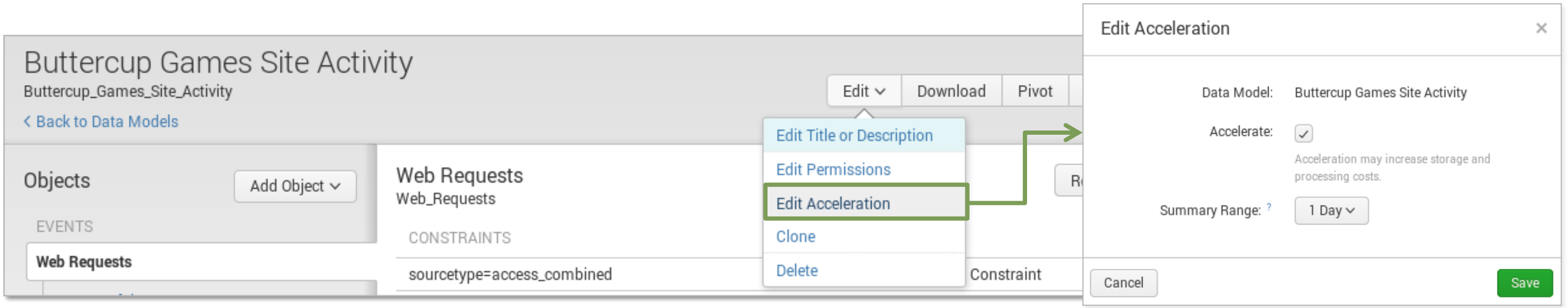


Accelerating a Data Model

- With persistent data model acceleration, all fields in the model become "indexed" fields in the table
- You must have administrative permissions or the accelerate_datamodel capability to accelerate a data model
- Private data models cannot be accelerated
- Accelerated data models cannot be edited

Note

Only root events can be accelerated. If there are multiple root events, only the first root event is accelerated.



Support Programs

- **Community**
  - **Splunk Answers:** answers.splunk.com
    Post specific questions and get them answered by Splunk community experts.
  - **Splunk Docs:** docs.splunk.com
    These are constantly updated. Be sure to select the version of Splunk you are using.
  - **Wiki:** wiki.splunk.com
    A community space where you can share what you know with other Splunk users.
  - **IRC Channel:** #splunk on the EFNet IRC server Many well-informed Splunk users “hang out” here.
- **Global Support**
  Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365.
  - **Email**: support@splunk.com
  - **Web:** http://www.splunk.com/index.php/submit_issue
- **Enterprise Support**
  Access your customer support team by phone and manage your cases online 24 x 7 (depending on support contract).

Thank You

