Splunk Module – 4 & 5

Creating Lookups

Creating Field Aliases and Calculated Fields

Creating Field Extractions

Creating Tags and Event Types

Creating Workflow Actions

Creating Alerts and Scheduled Reports

Creating and Using Macros

: Creating Data Models

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
```

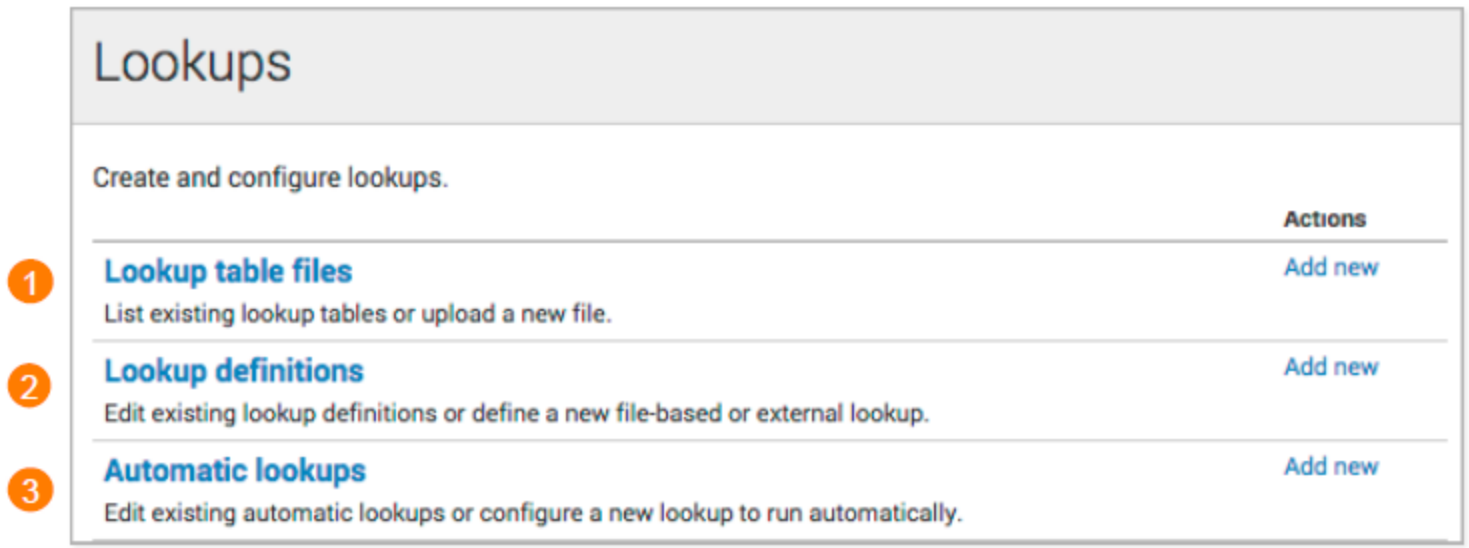
Address_Description	rfid	Username	Department
London	632071692298	yowen	Sales
London	963871339460	rjayaraman	Engineering
London	145297537706	npearce	SecOps
London	145297537706	npearce	SecOps
London	145297537706	npearce	SecOps
San Francisco	569361105570	kpercy	Compliance Officer
Boston	374765319282	emaxwell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

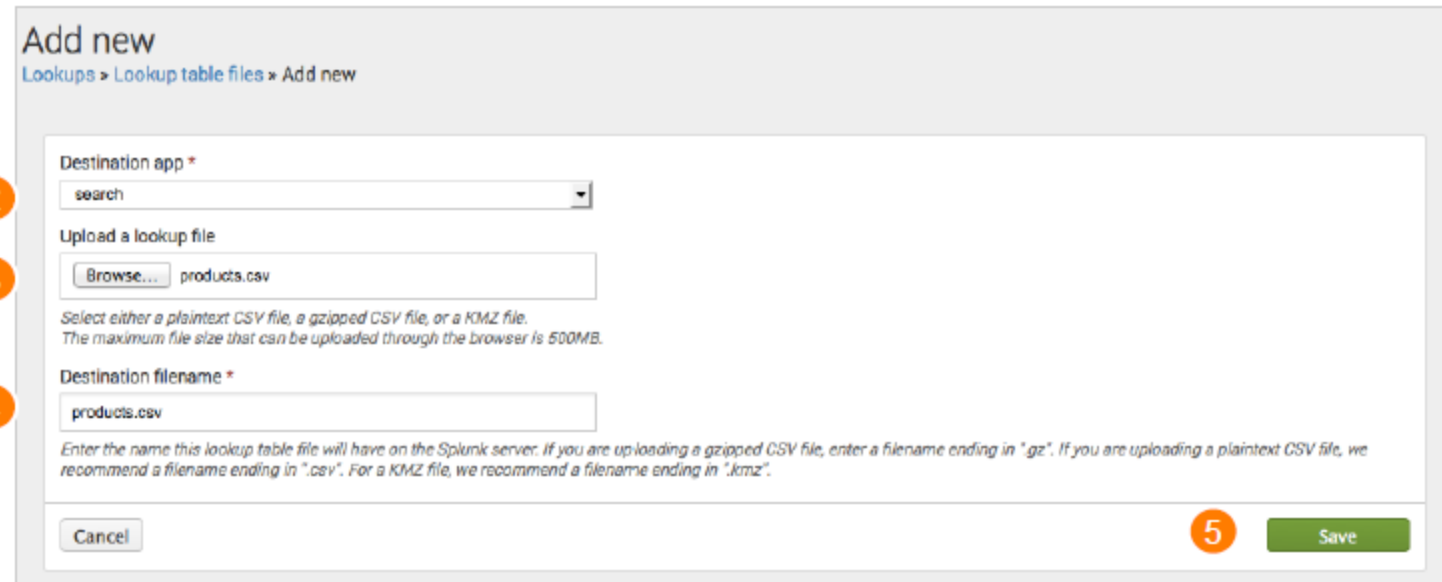
1. Upload the file required for the lookup
2. Define the lookup type
3. Optionally, configure the lookup to run automatically



Creating a Lookup Table

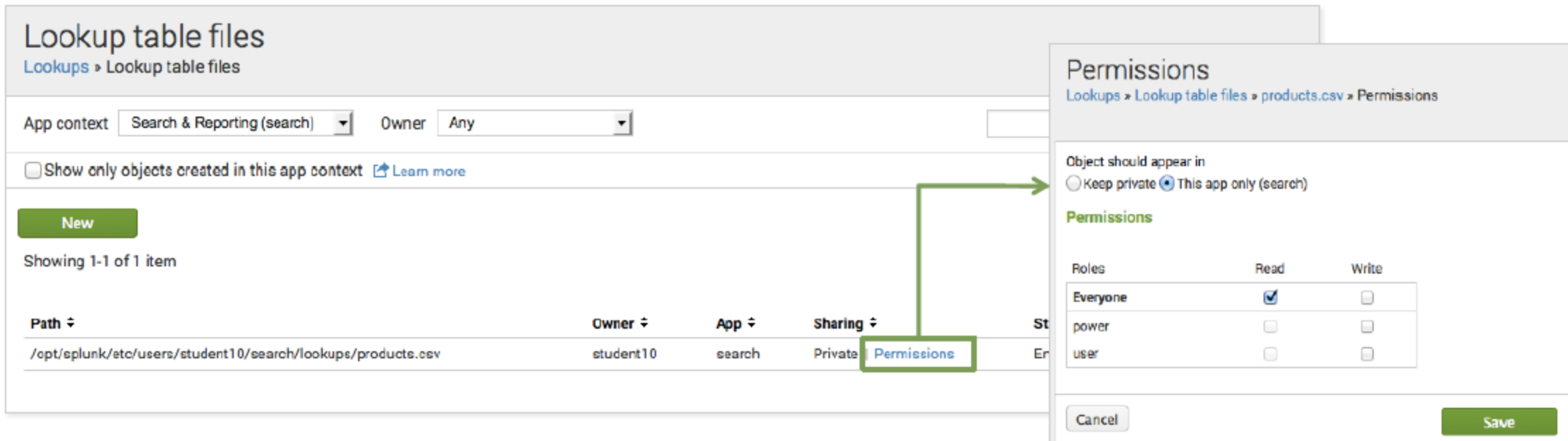
Settings > Lookups > Lookup table files

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

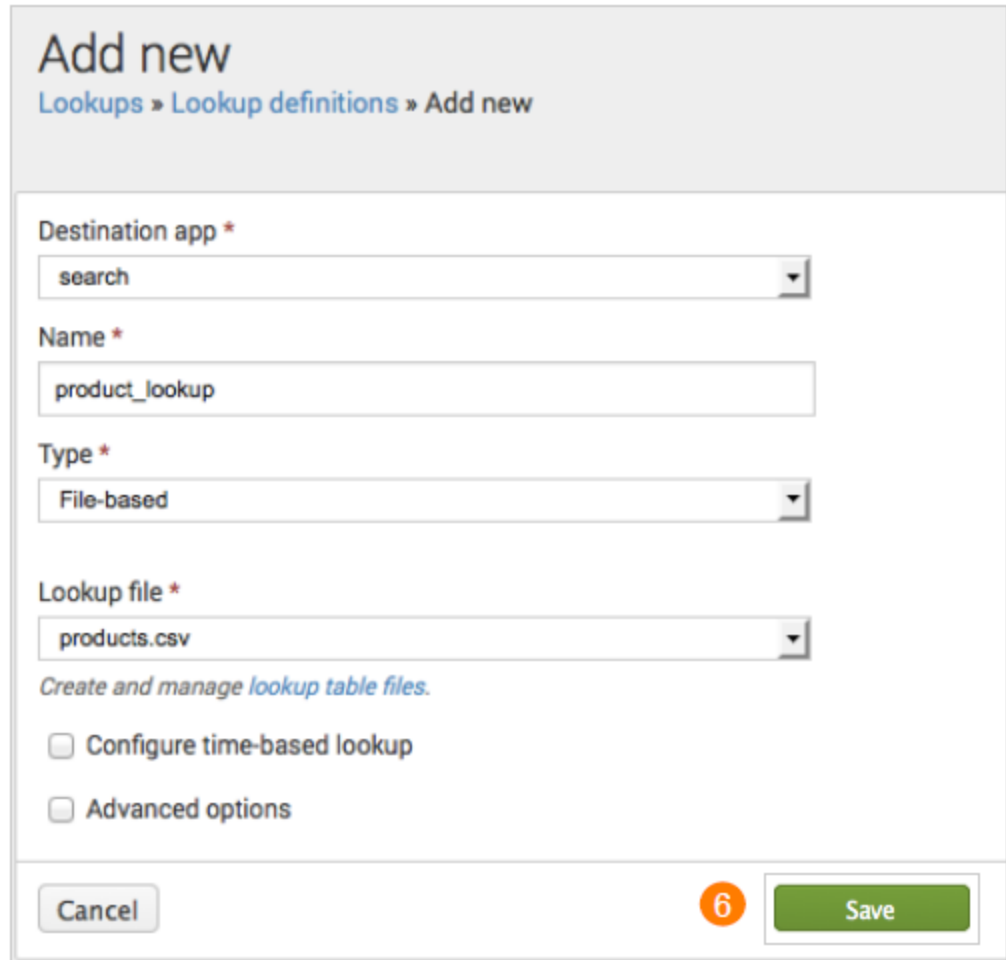
20 Per Page | Format | Preview

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

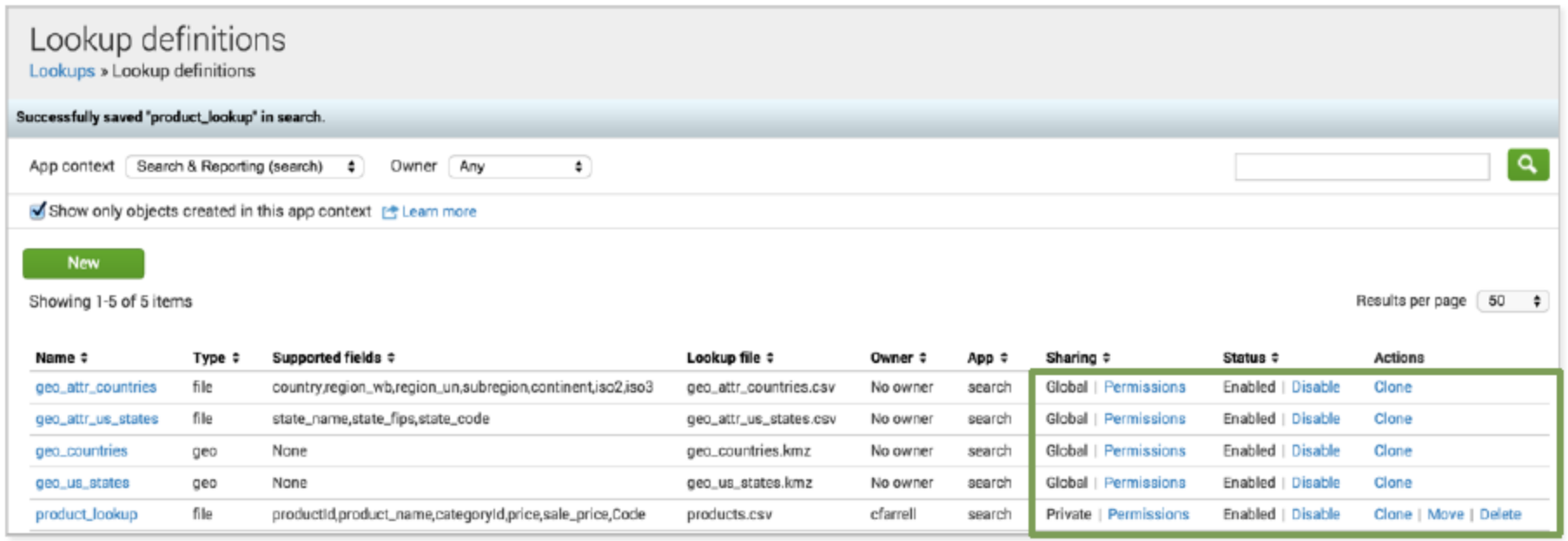
Managing Lookup Definitions

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

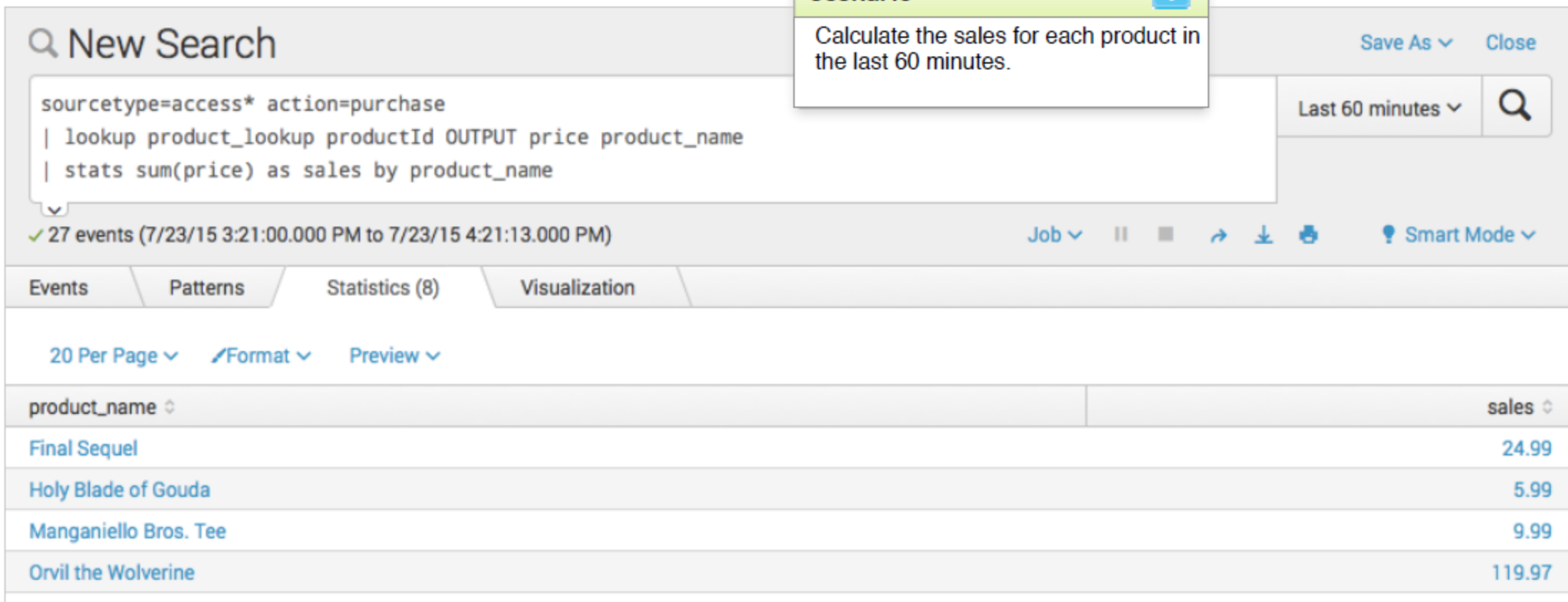
There is a lookup table specified in a stanza name 'usertogroup' in transform.conf. This lookup table contains (at least) two fields, 'user' and 'group'. For each event, we look up the value of the field 'local_user' in the table and for any entries that matches, the value of the 'group' field in the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

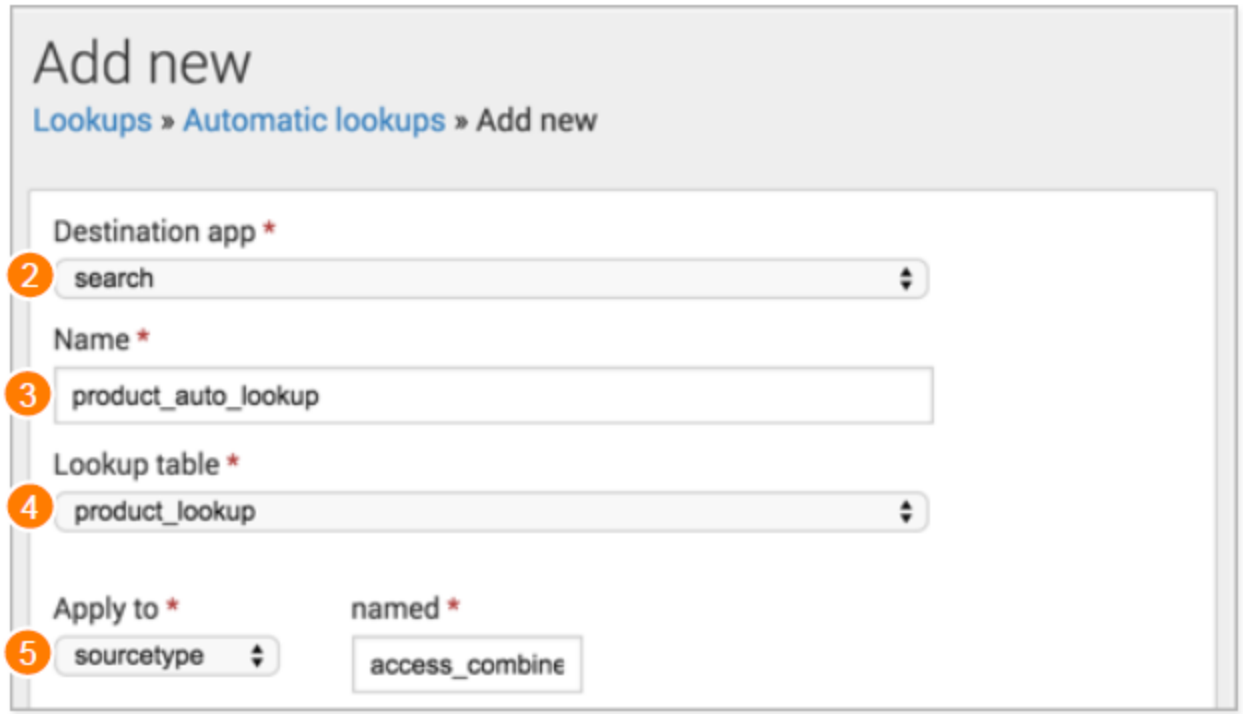
Calculate the sales for each product in the last 60 minutes.



Creating an Automatic Lookup

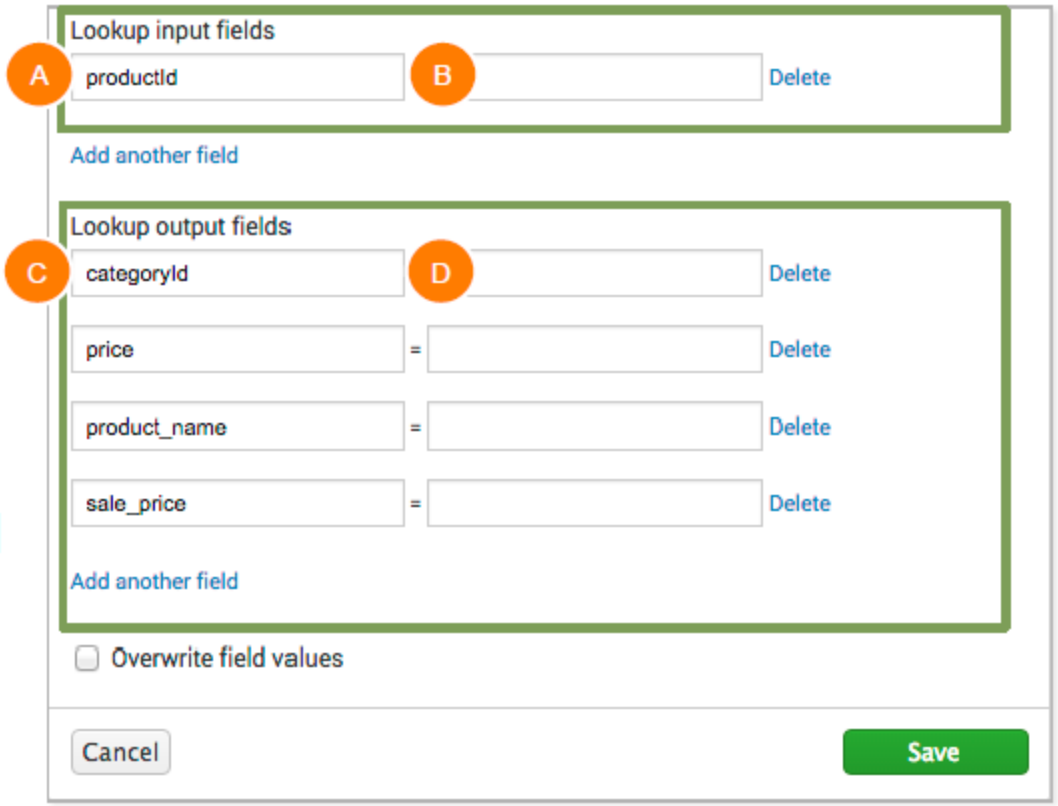
Settings > Lookups > Automatic lookups

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



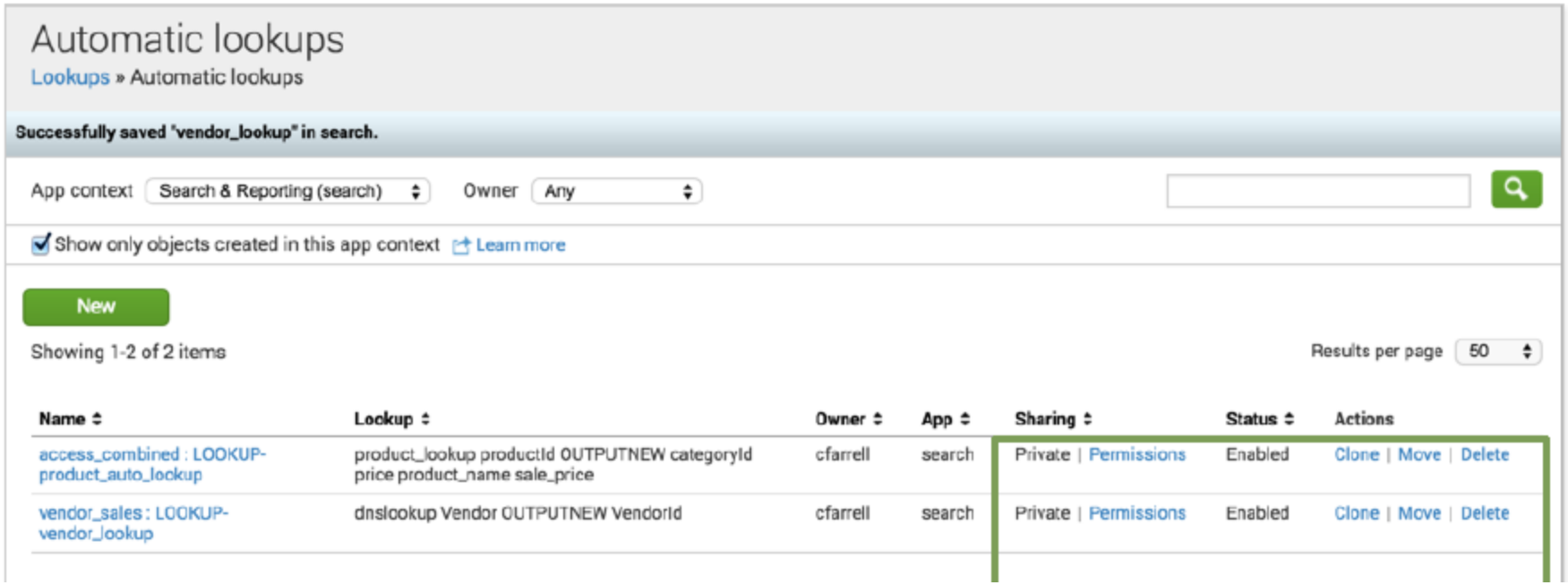
Managing Automatic Lookups

Based on your permissions, you can:

- Edit permissions
- Clone
- Delete
- Move

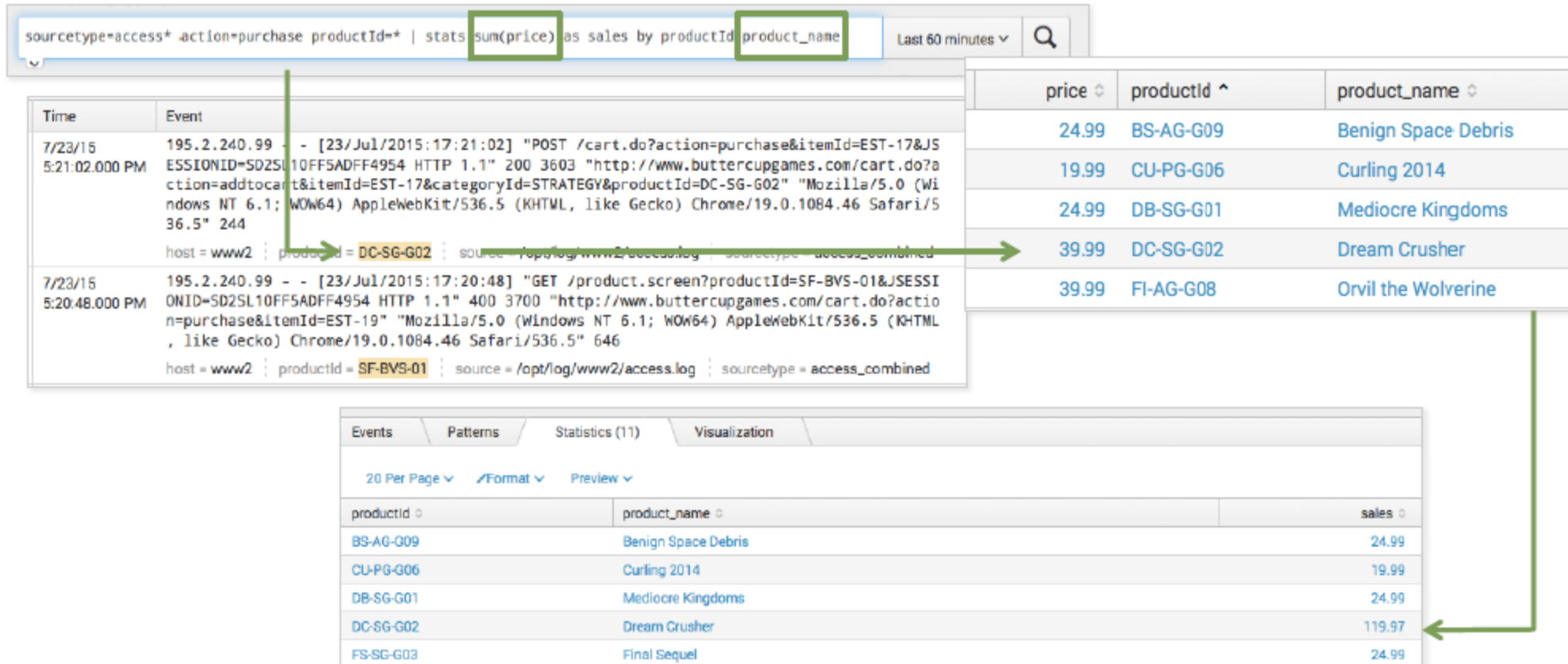
Note

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



Module Objectives

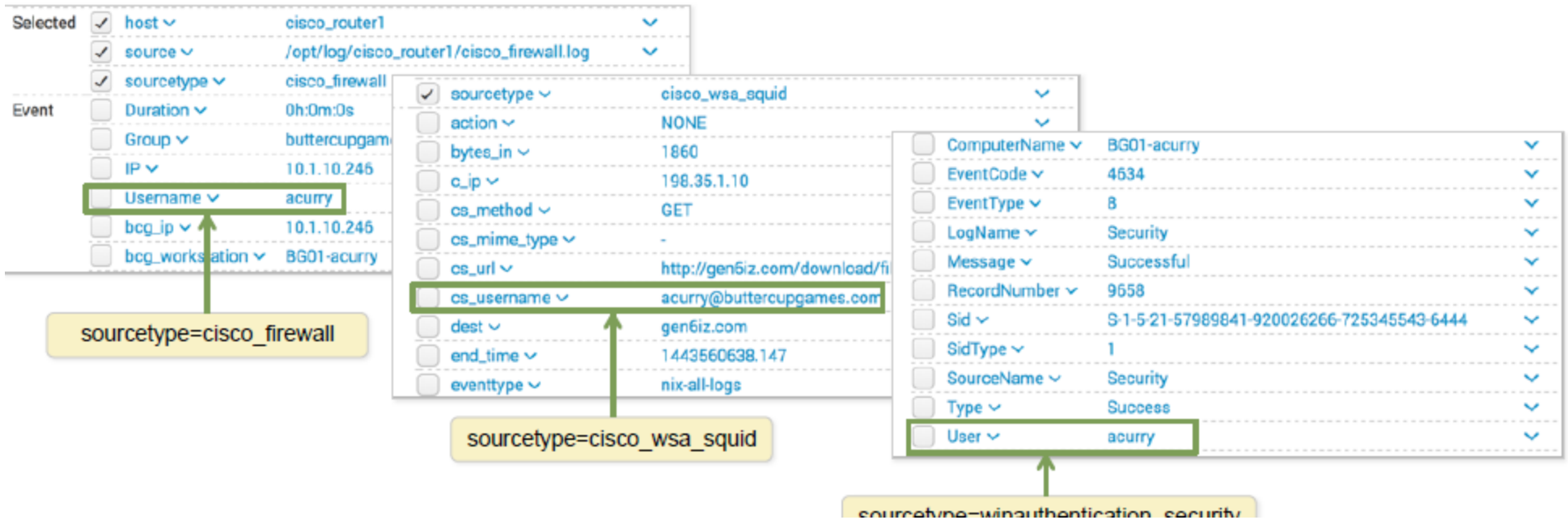
- Create and use field aliases
- Create calculated fields

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

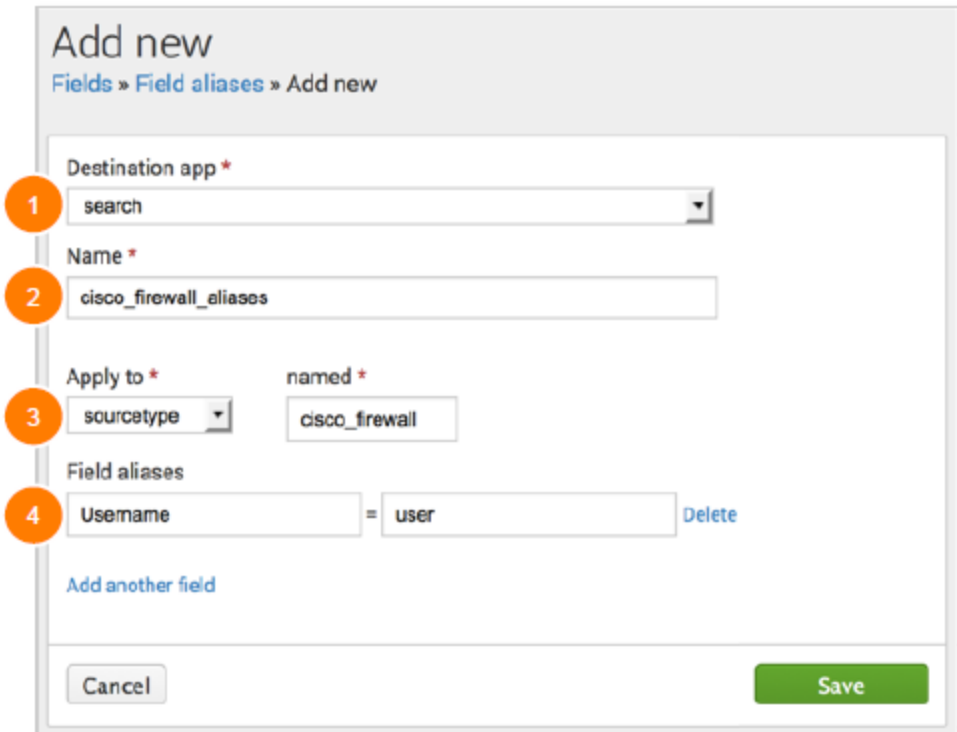
- Several source types contain some type of a username field
- To make data correlation and searching easier, normalize the username field



Creating a Field Alias

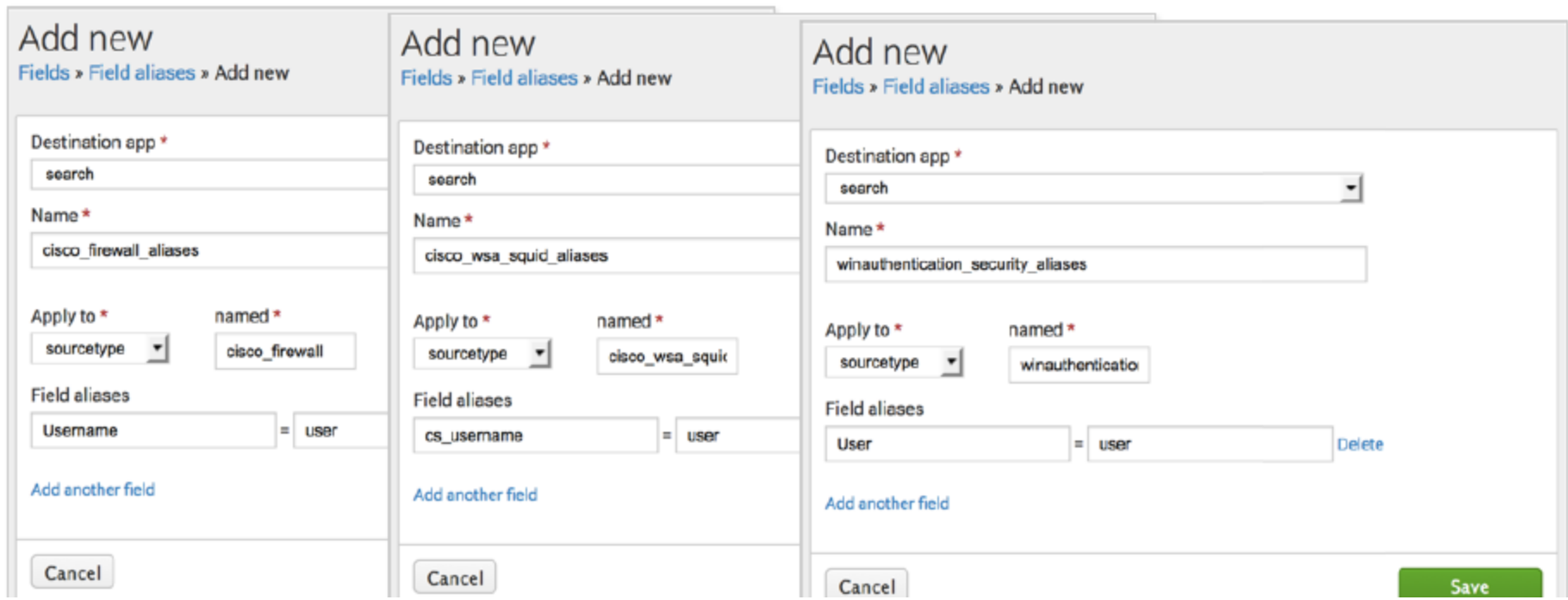
Settings > Fields > Field Aliases > New

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



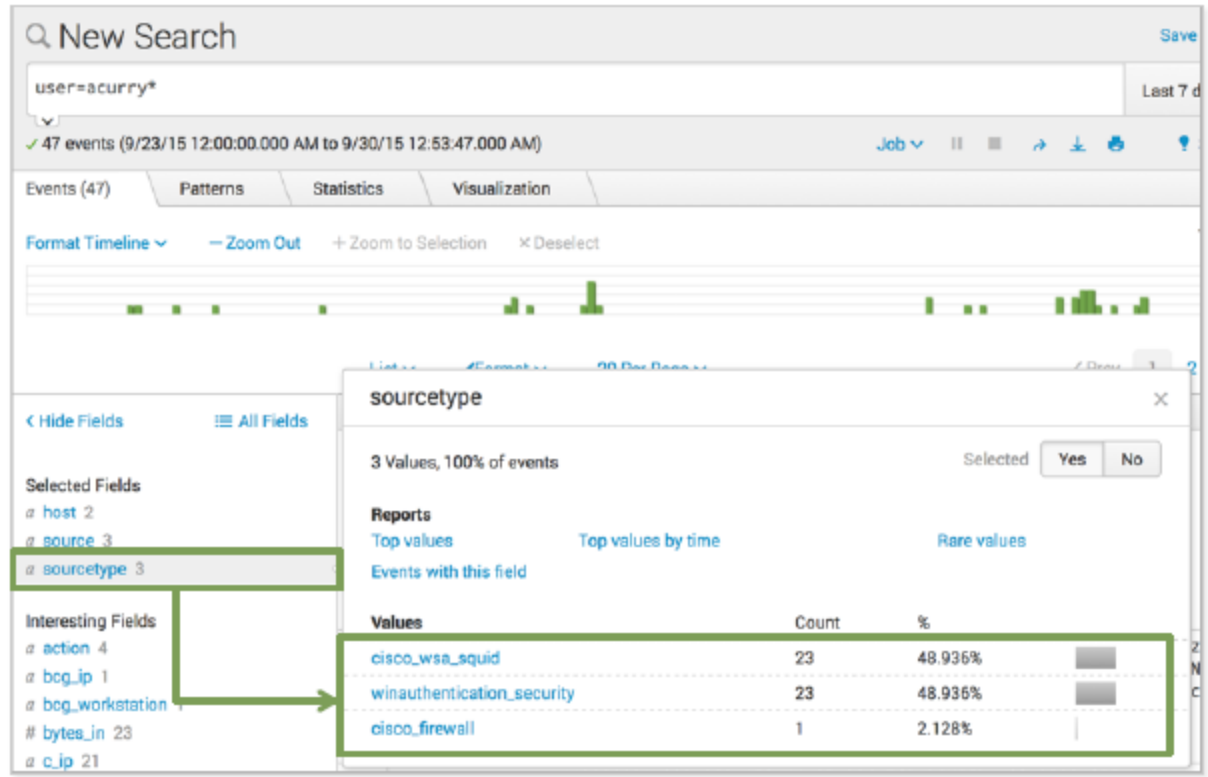
Creating a Field Alias (cont.)

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

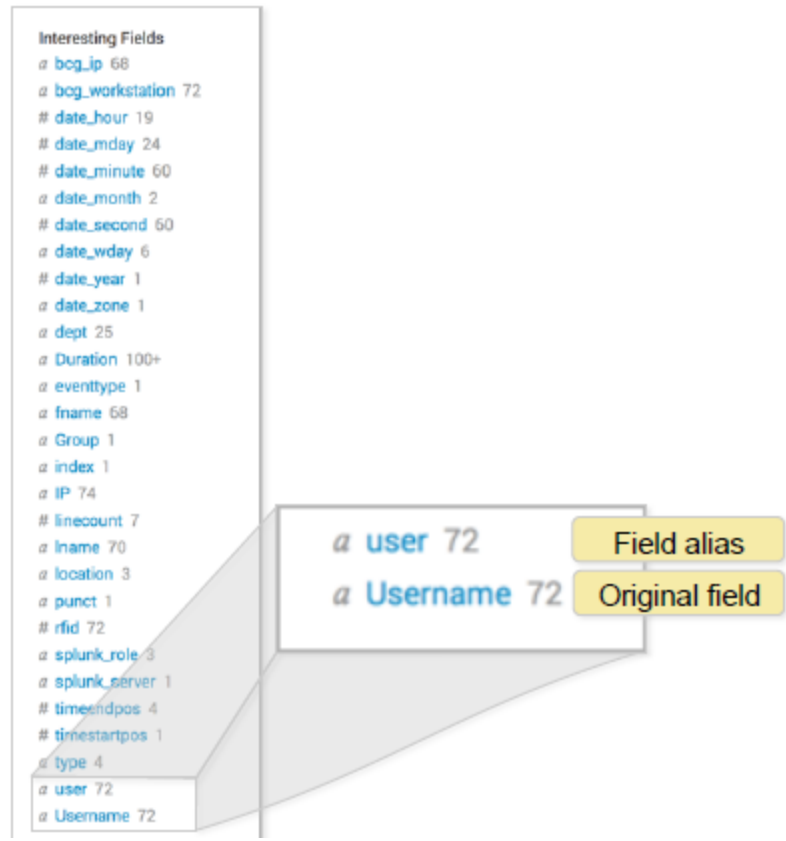
After the field alias has been created, perform a new search using the new field alias



Field Alias and Original Fields

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

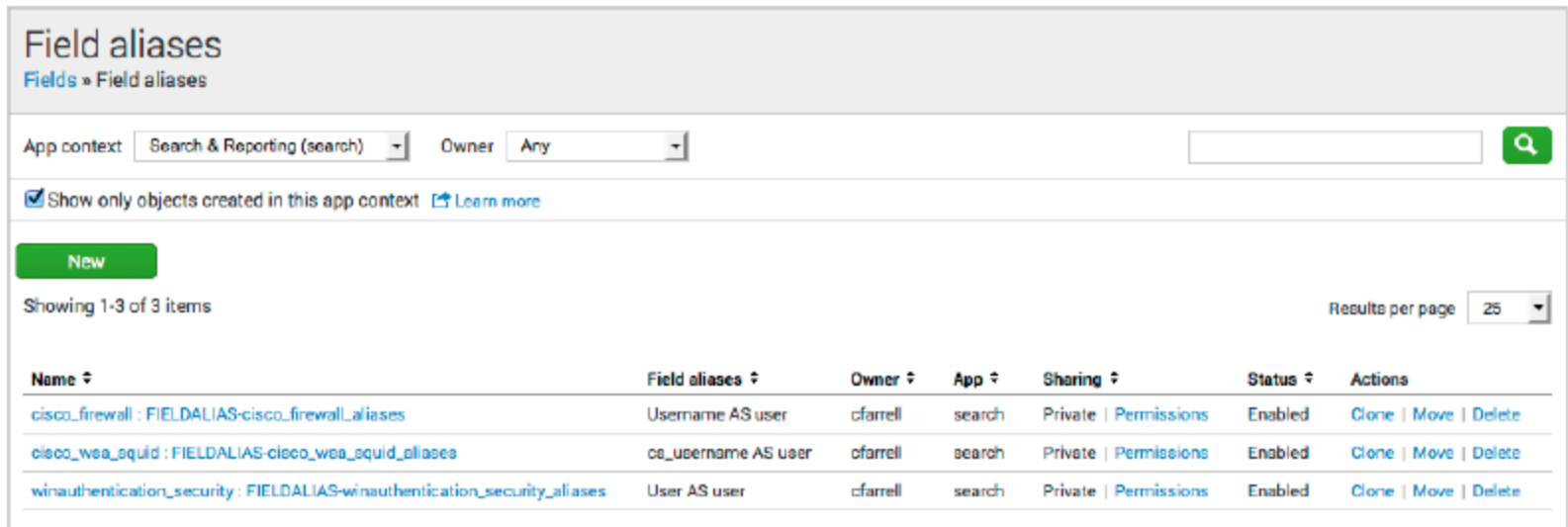
Both fields will appear in the All Fields list and the Interesting Fields list, if it appears in at least 20% of events.



Managing Field Aliases

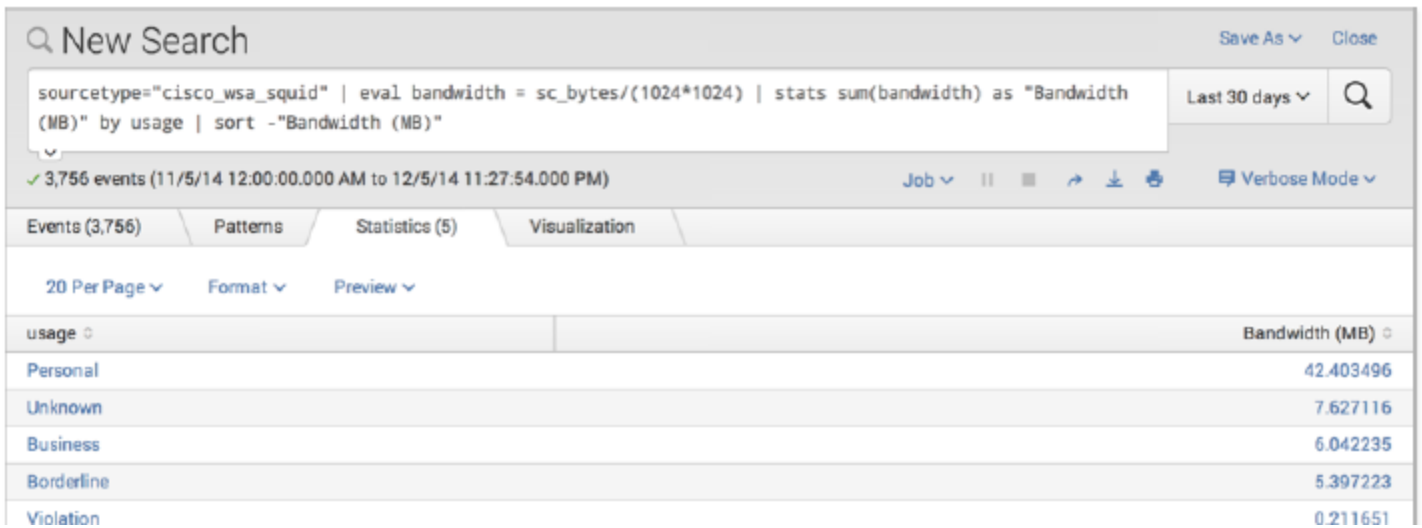
Settings > Fields > Field Aliases

- Edit permissions
- Clone
- Move
- Delete



What is a Calculated Field?

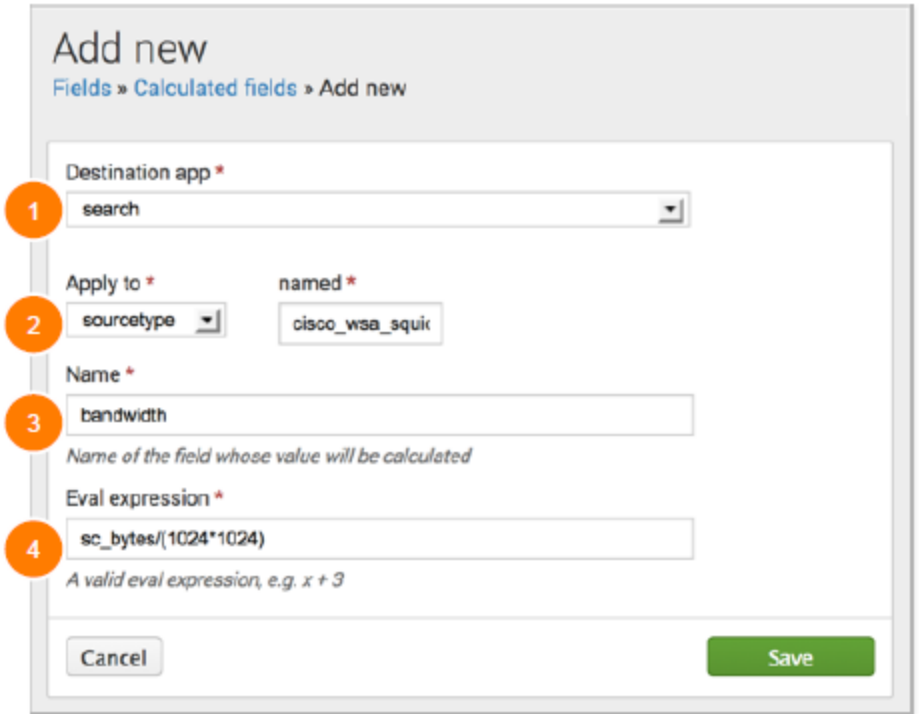
- Shortcut for performing repetitive, long, or complex transformations using the `eval` command
- Must be based on an extracted field
  - Output fields from a lookup table or fields/columns generated from within a search string are not supported



Creating a Calculated Field

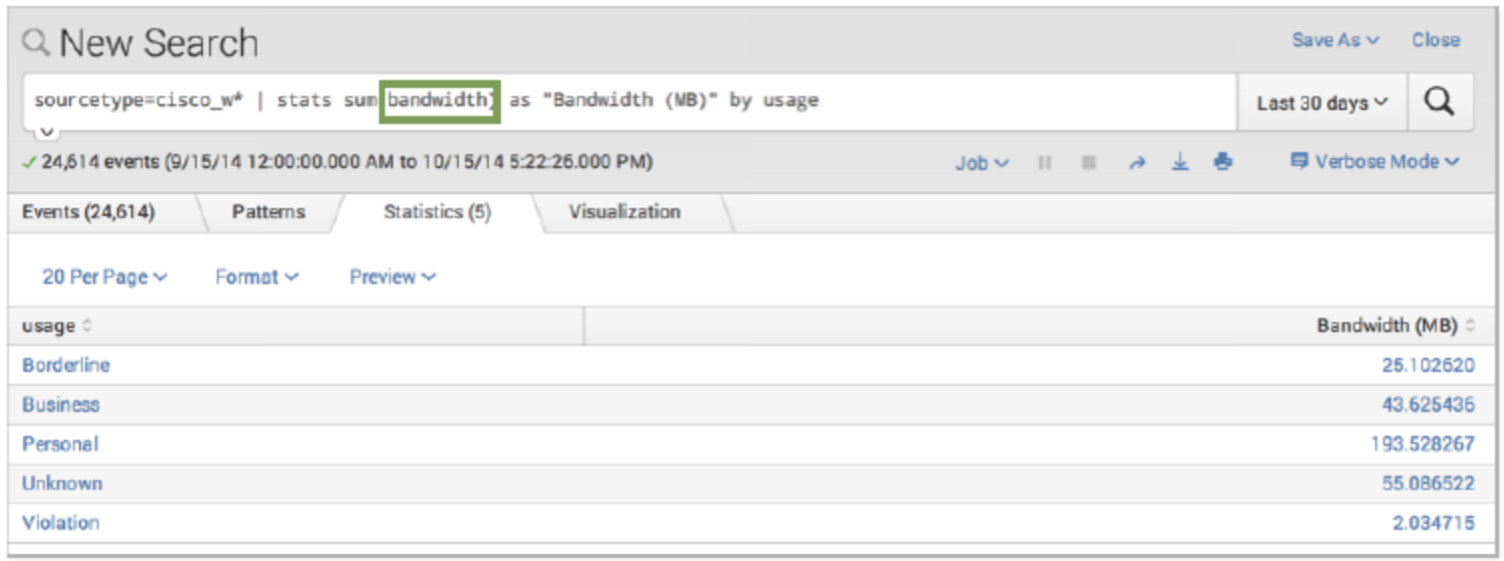
Settings > Fields > Calculated Fields > New

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

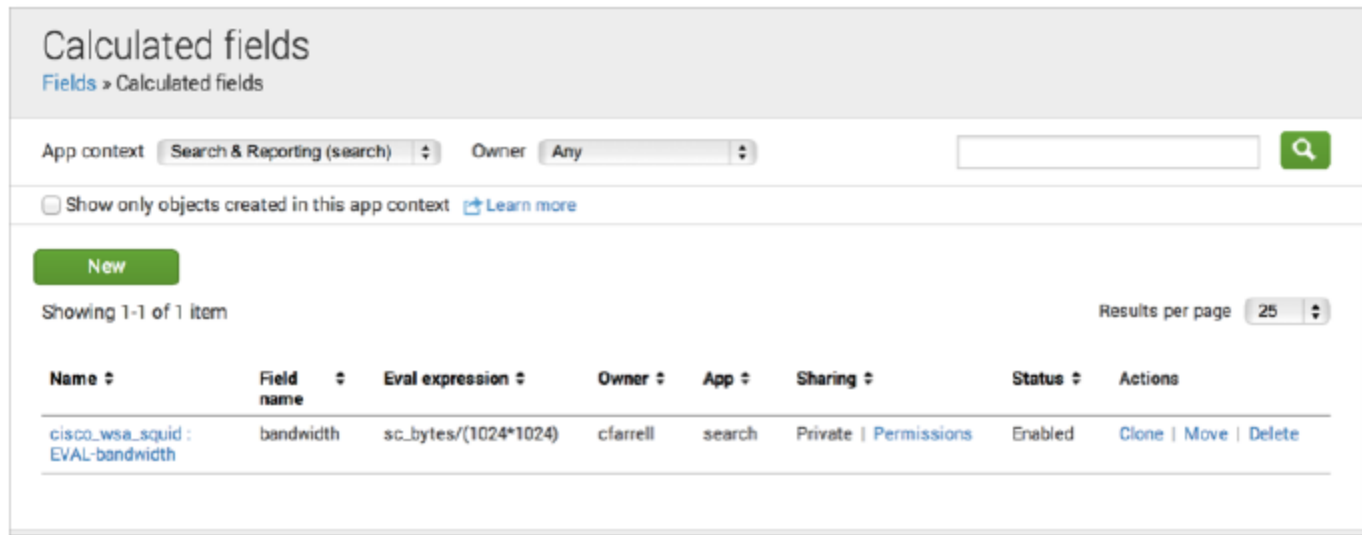
After you have created a calculated field, you can use it in a search like any other extracted field:



Managing Calculated Fields

Settings > Fields > Calculated Fields

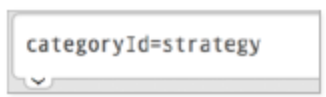
- Edit permissions
- Clone
- Move
- Delete

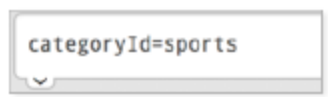


- Create and use tags
- Describe event types and their uses
- Create an event type

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+



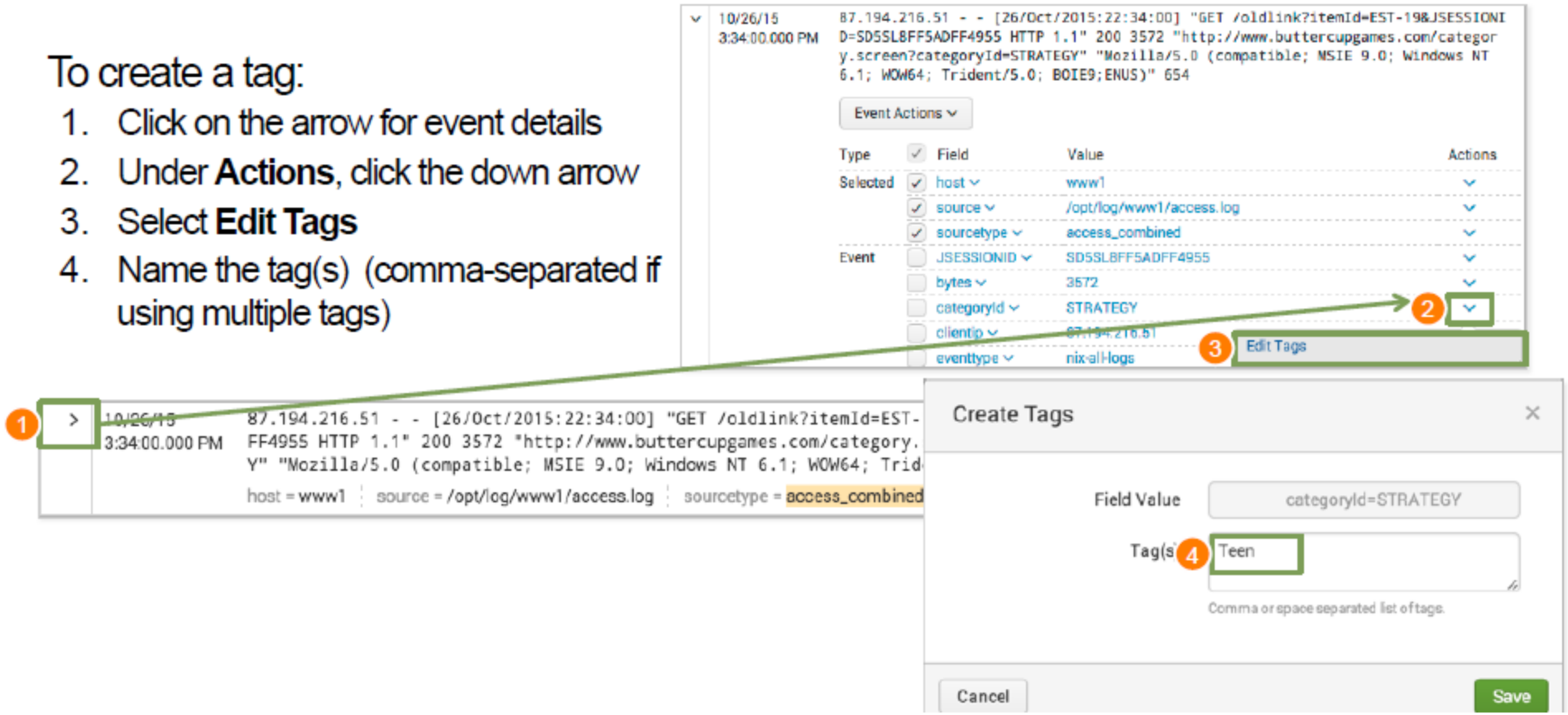


- You can create one or more tags for any field/value combination
- Tags are case sensitive

Creating Tags

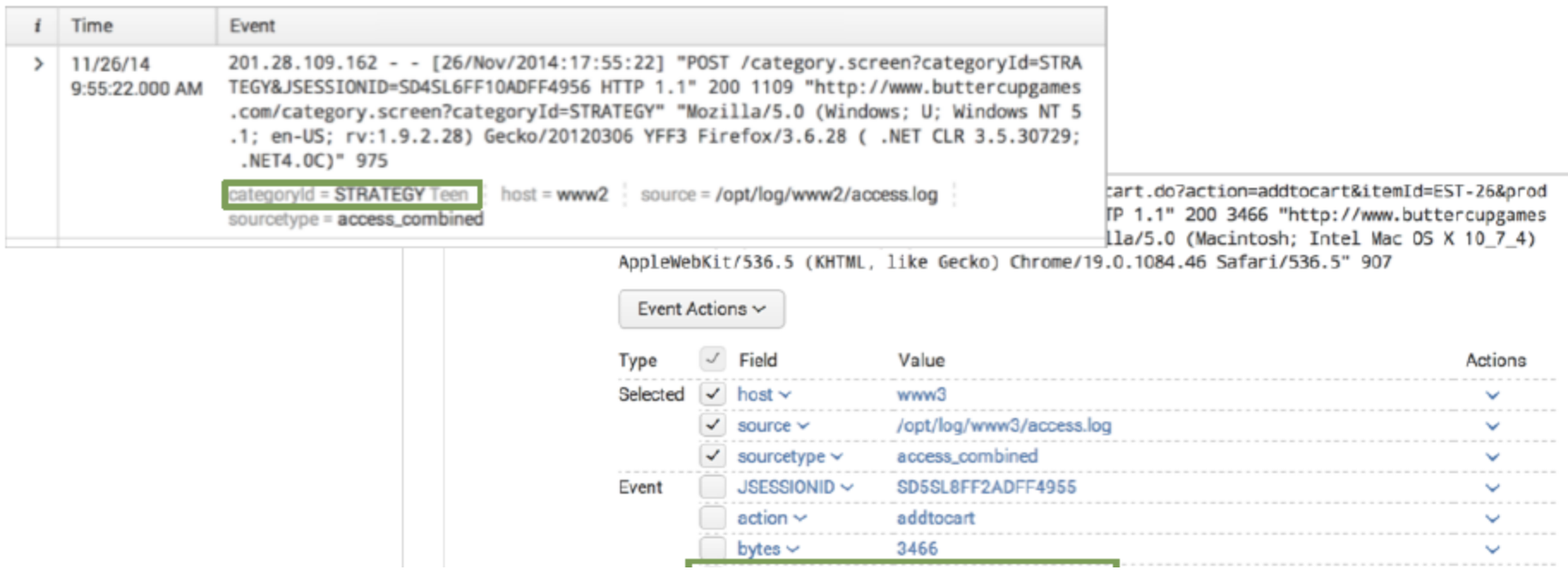
To create a tag:

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)



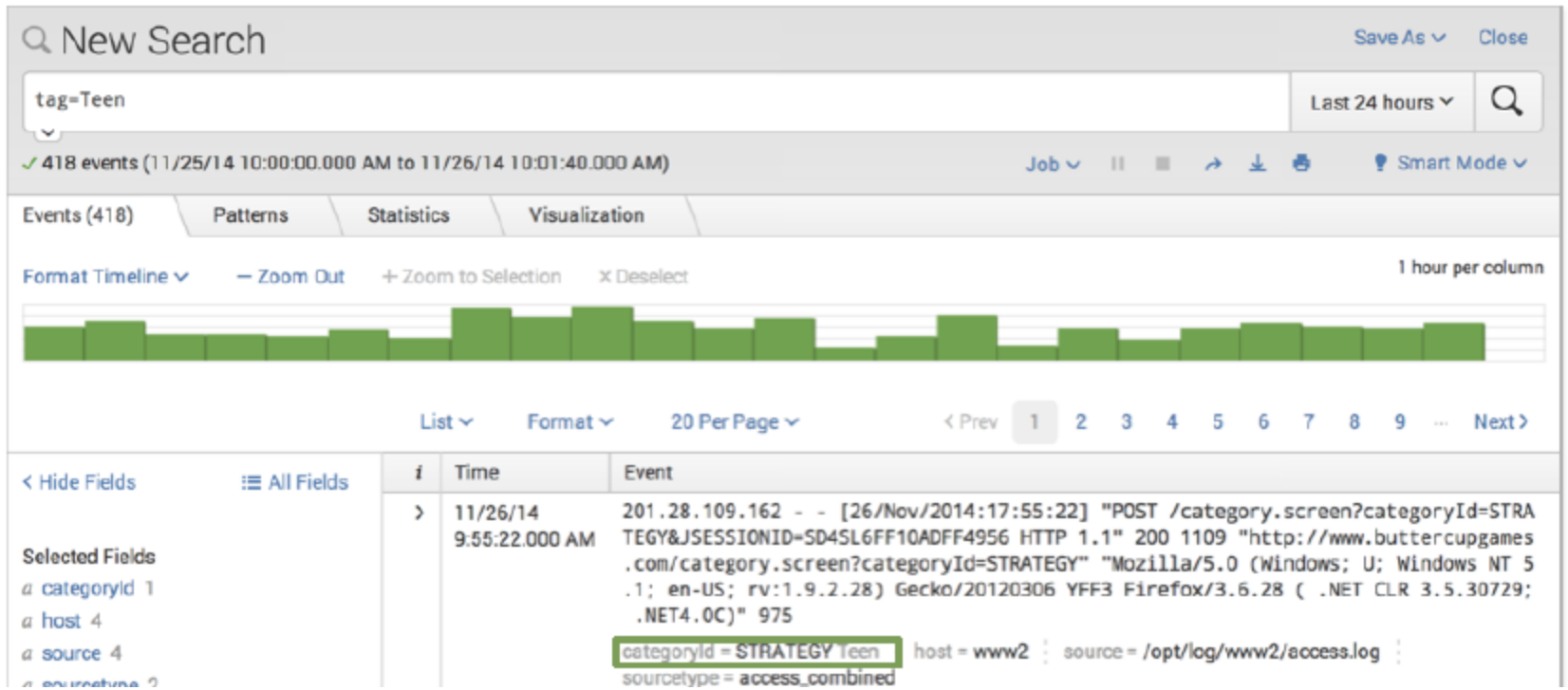
Viewing Tags

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>

```
tag=Teen
```

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

- tag::<field>=<tagname>

```
tag::categoryId=Teen
```

To search for a tag using a partial field value:

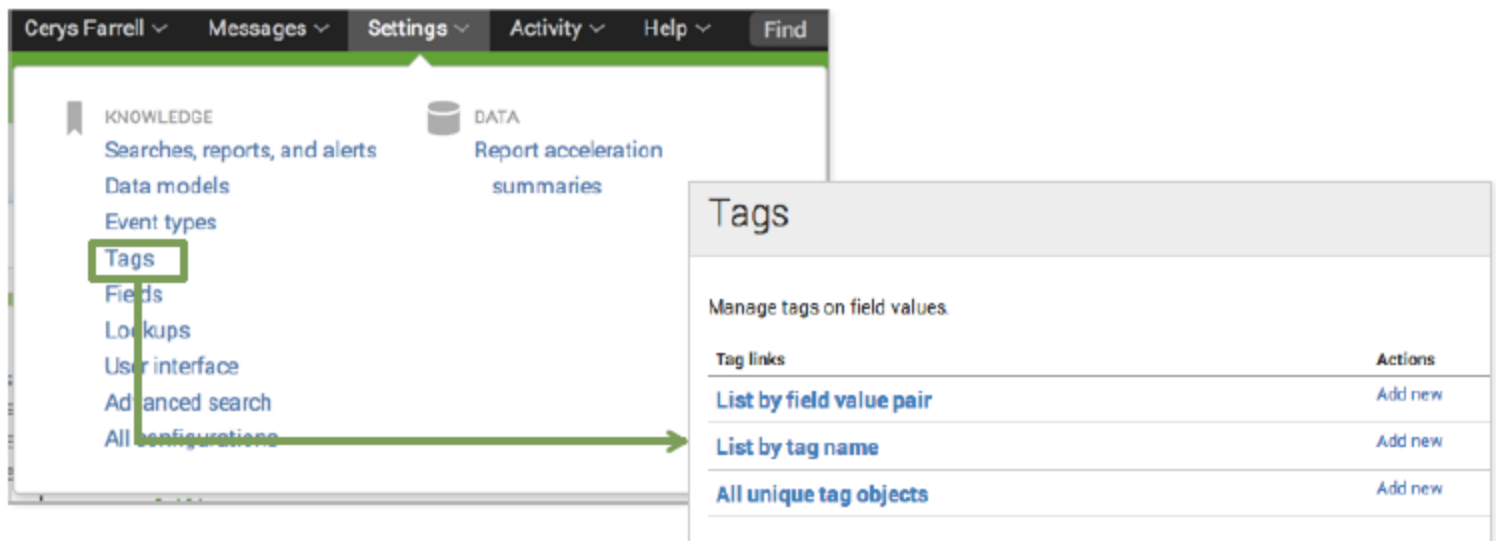
- use (*) wildcard

```
tag=T*
```

Managing Tags

Settings > Tags

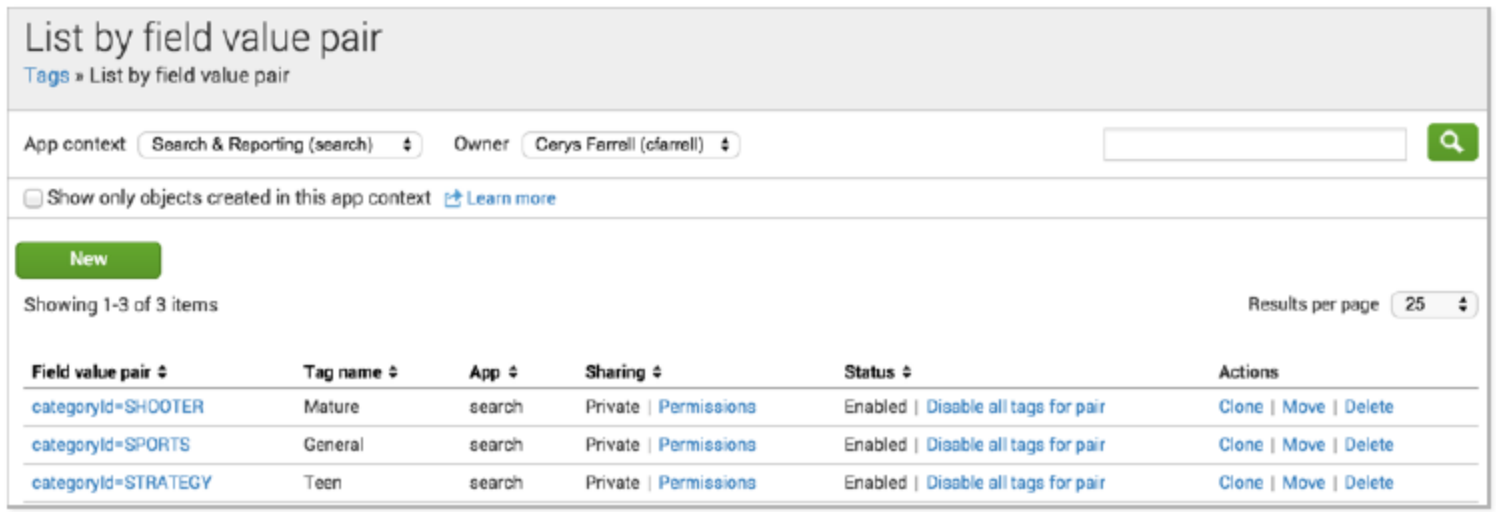
You can display tags by field value pair, tag name, or all unique tag objects



Managing Tags (cont.)

Settings > Tags > List by field value pair

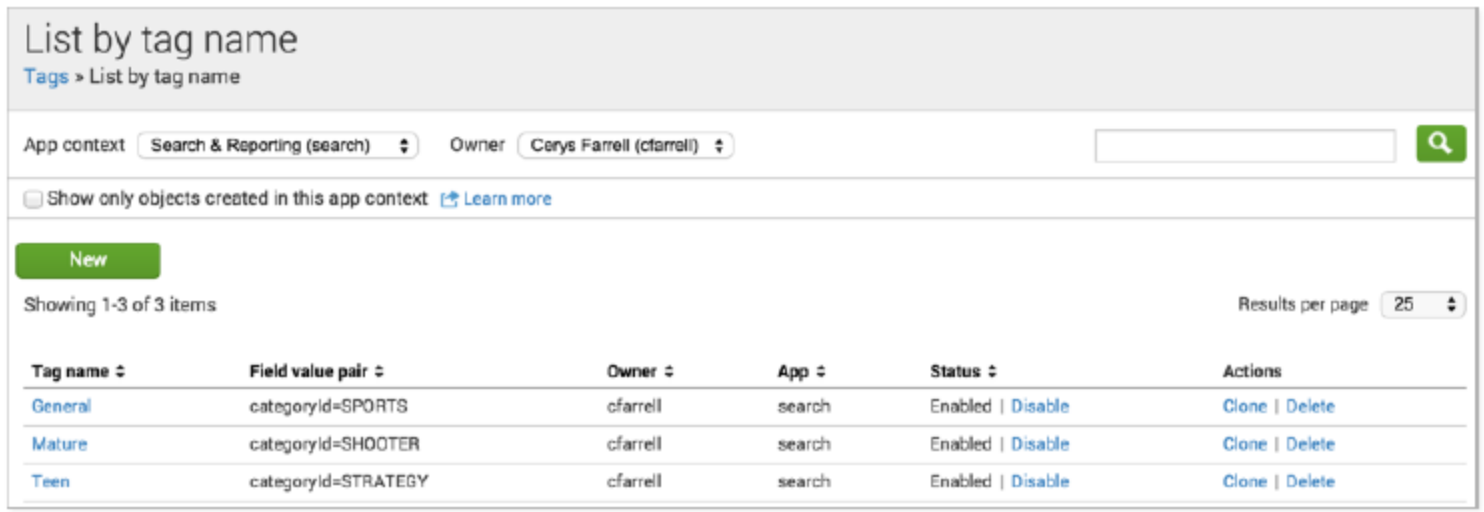
- Edit permissions
- Disable all tags for pair – disables the tag in searches and prevents it from being listed under **List by Tag Name** and **All unique tag objects**
- Clone
- Move
- Delete



Managing Tags (cont.)

Settings > Tags > List by tag name

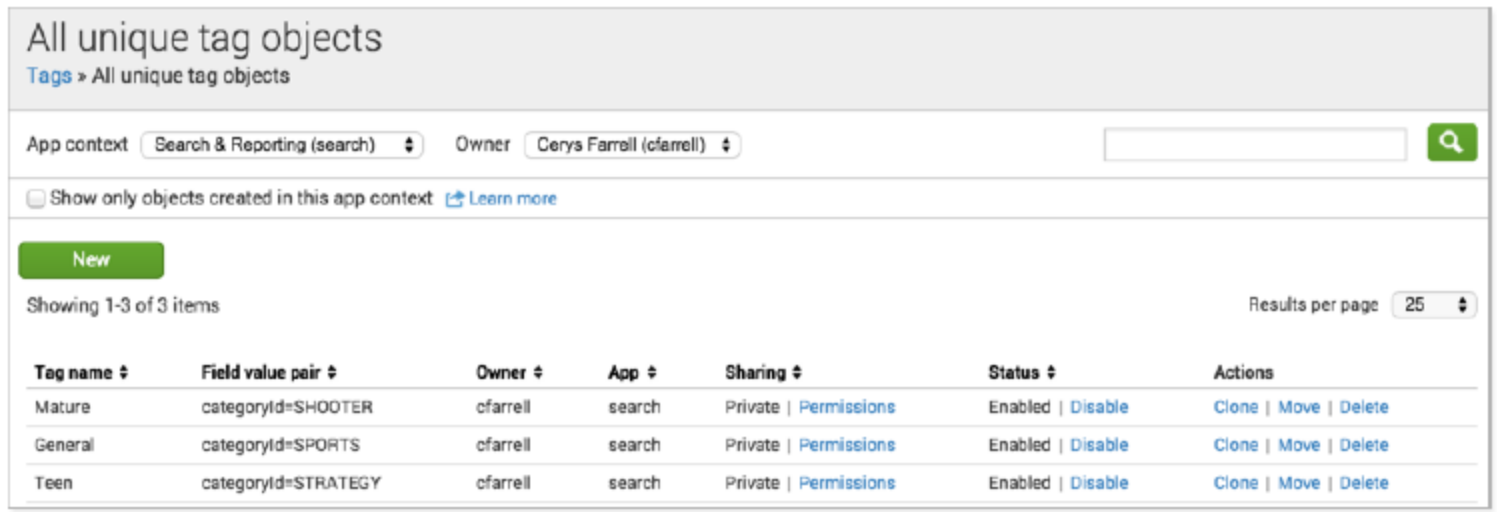
- Enable/Disable
- Clone
- Delete



Managing Tags (cont.)

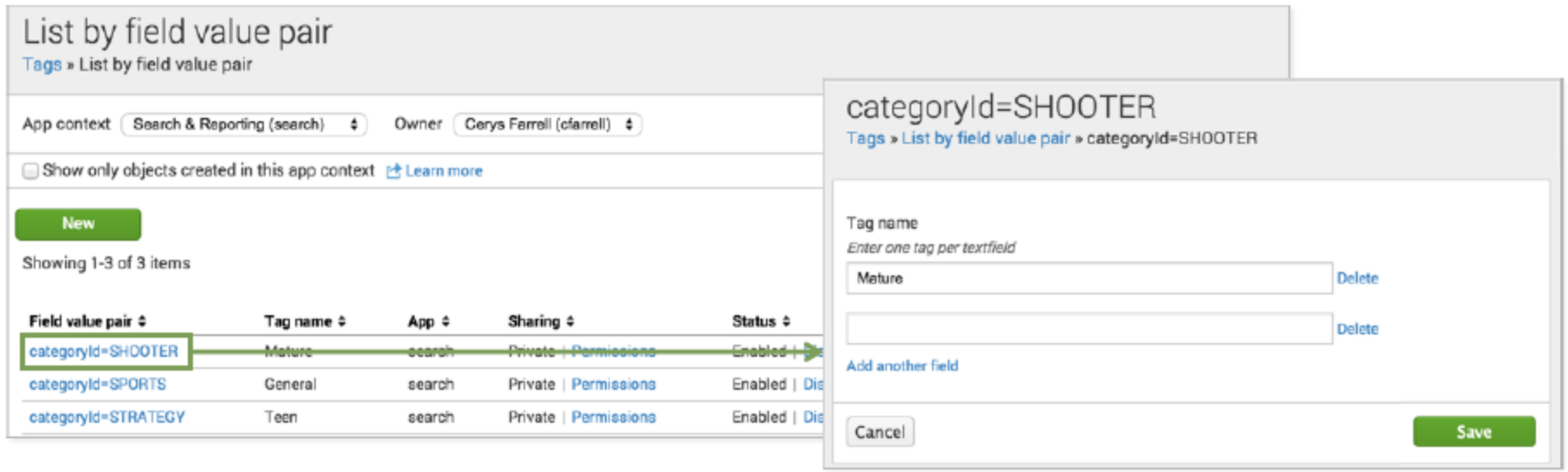
Settings > Tags > All unique tag objects

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



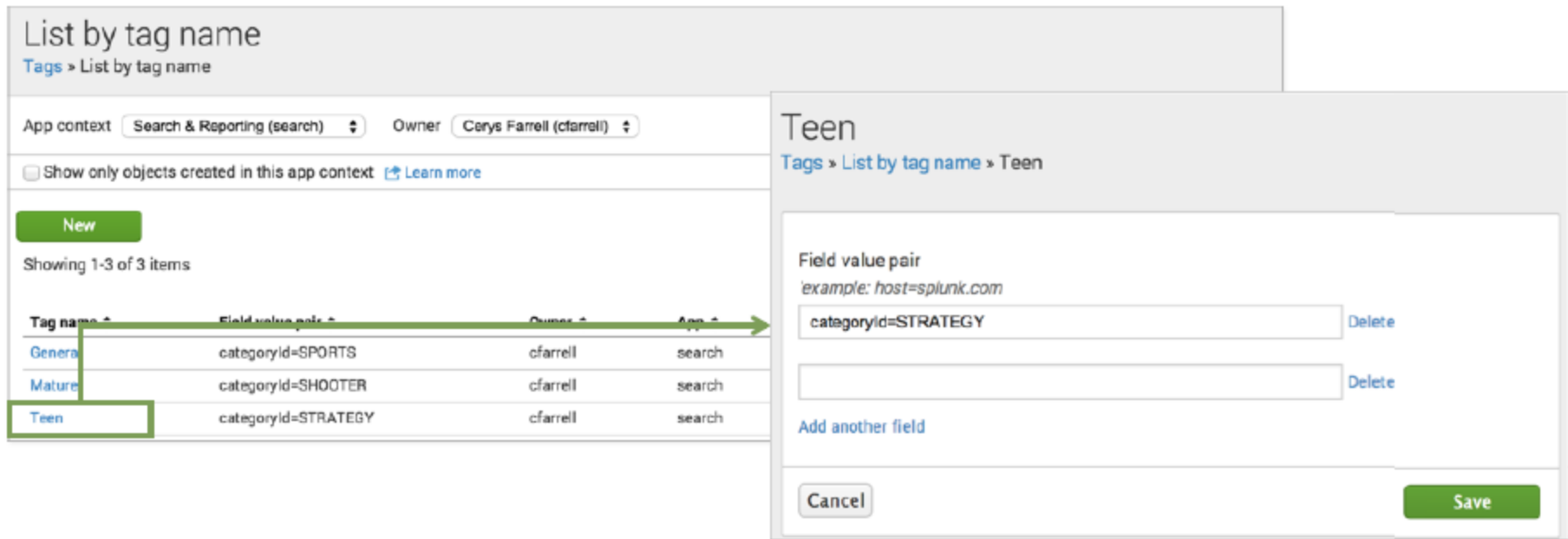
Adding/Changing the Tag Name

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

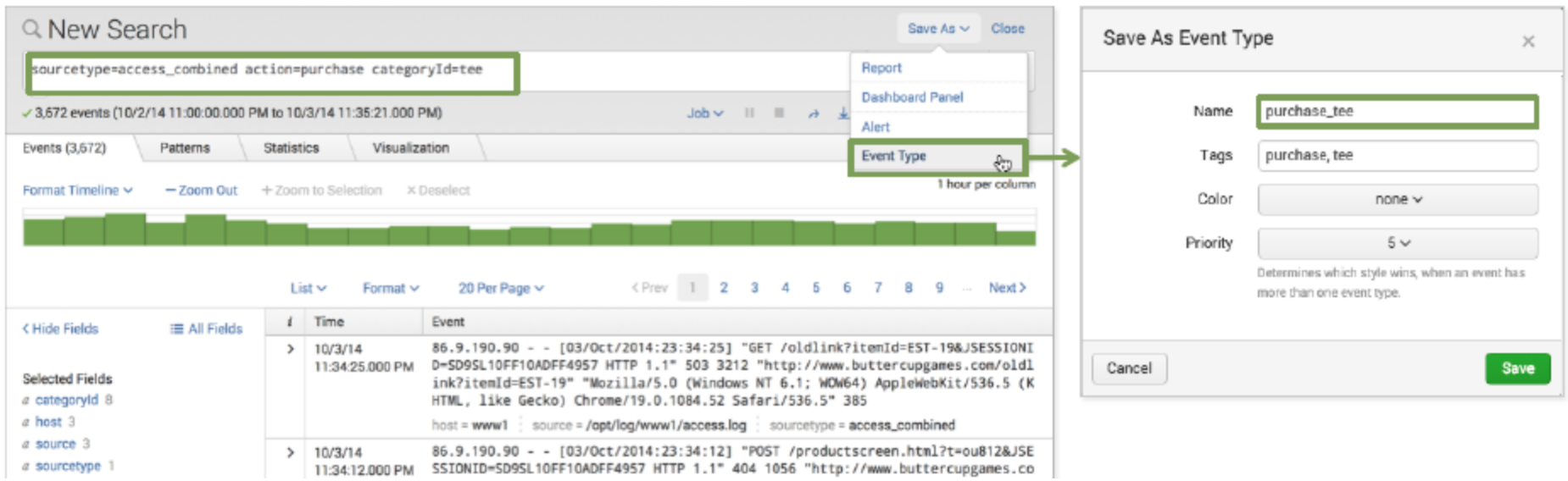
To differentiate these events, create individual event types

- purchase_accessories

- purchase_tee

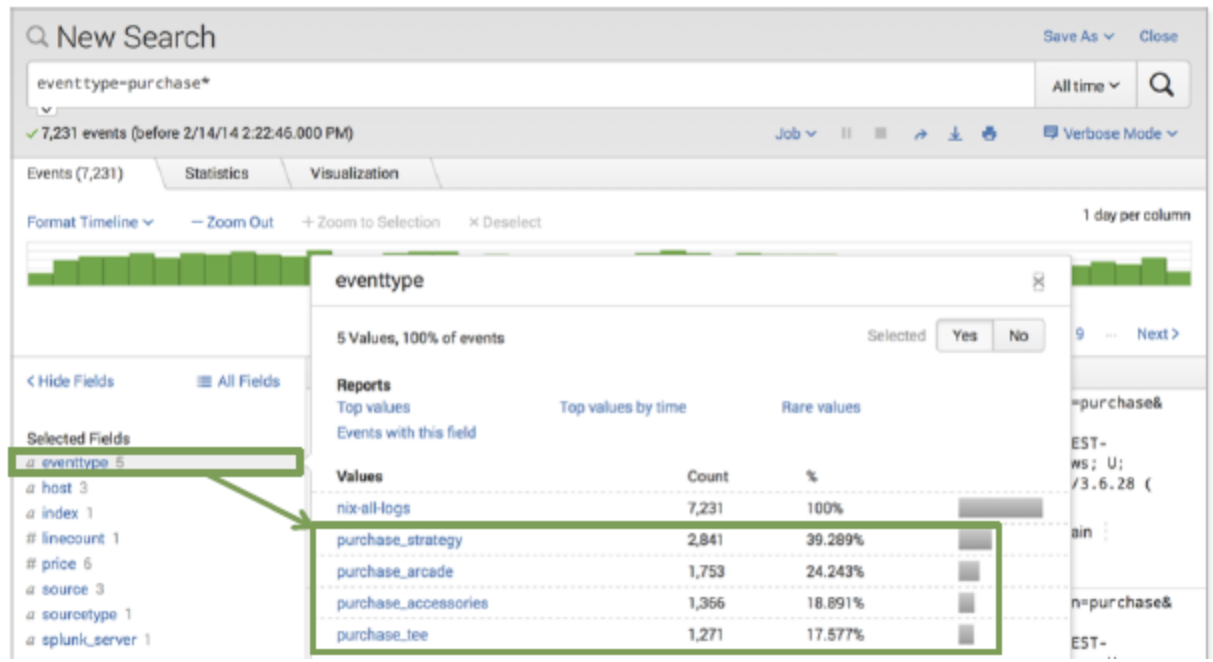
Creating an Event Type

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

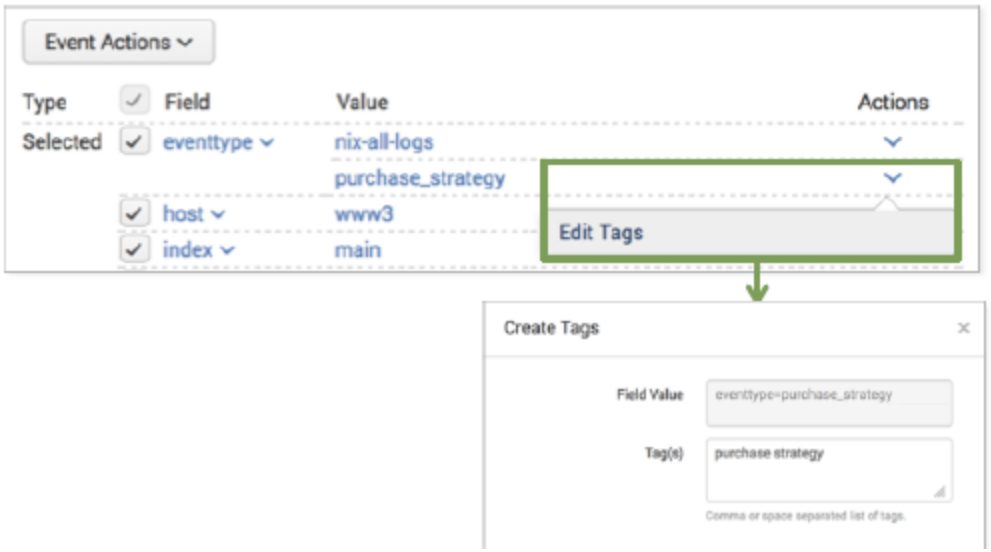
- To verify the event type, search for `eventtype=purchase*`
- 'eventtype' displays in the Fields sidebar and can be added as a selected field
- Splunk evaluates the events and applies the appropriate event types at search time
- Using the Fields sidebar, you can easily view the individual event types,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

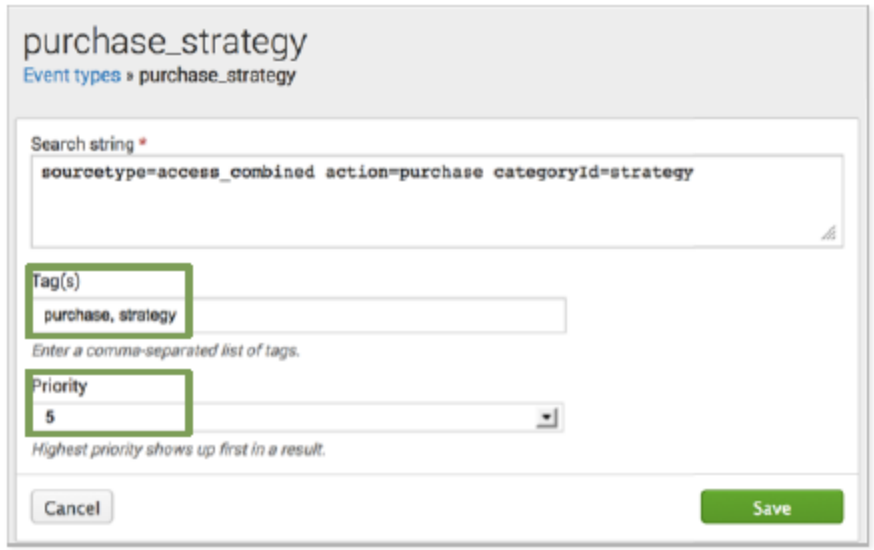


Tagging Event Types

You can tag event types two ways:

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



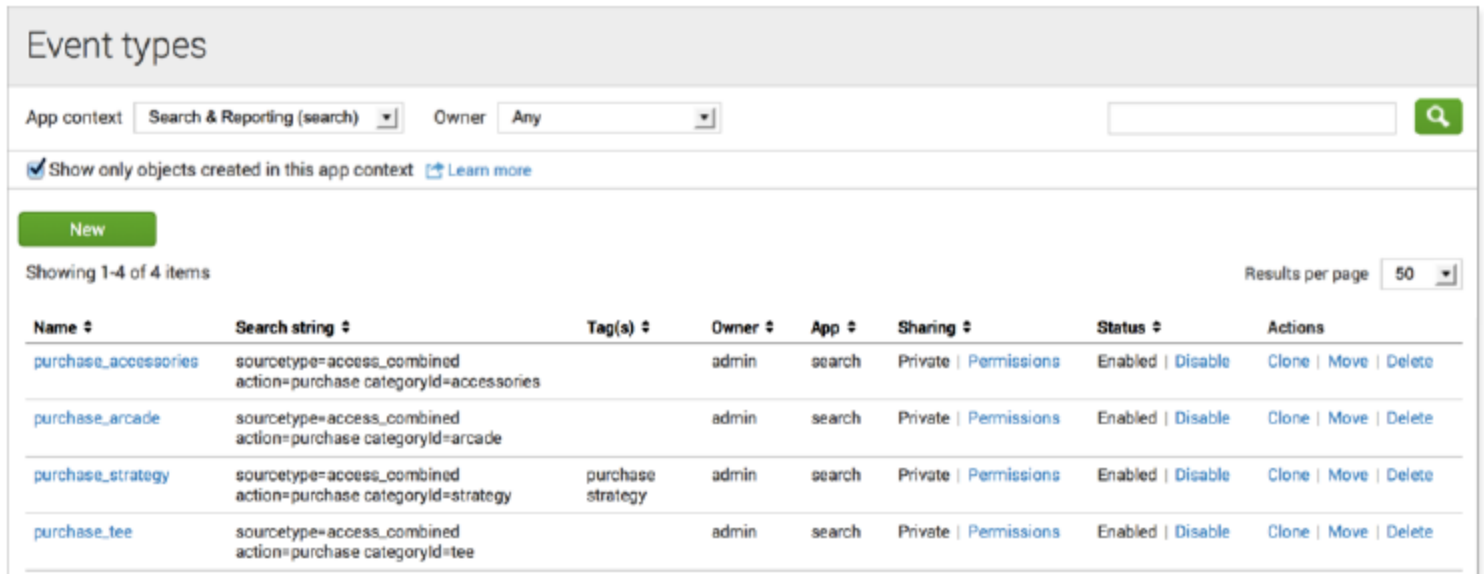


- The range for the priority is 1 (highest) to 10 (lowest)

Managing Event Types

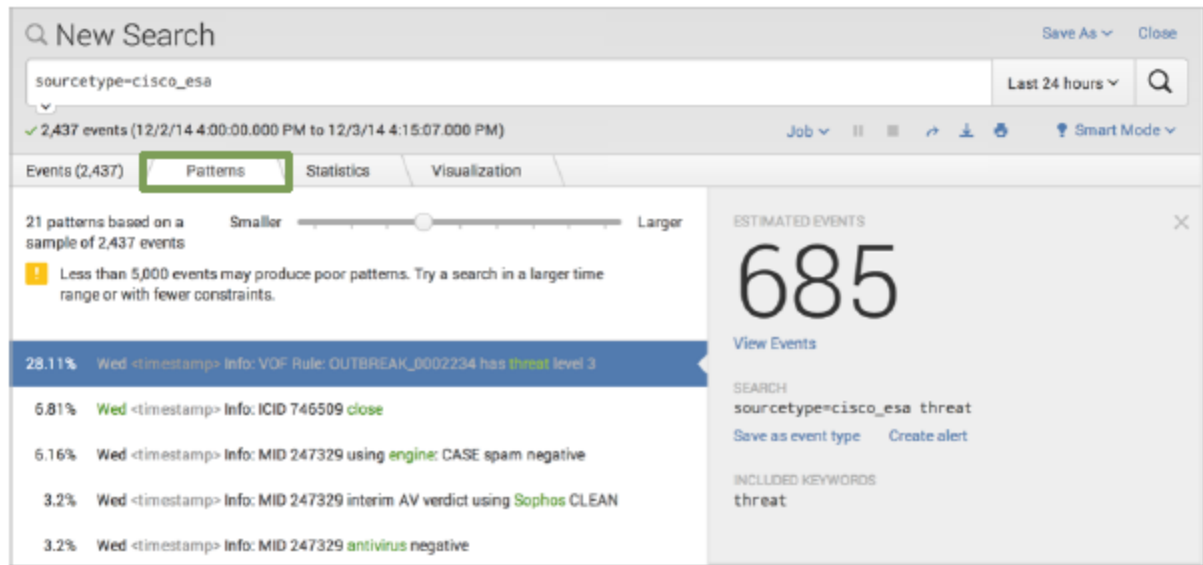
Settings > Event Types

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



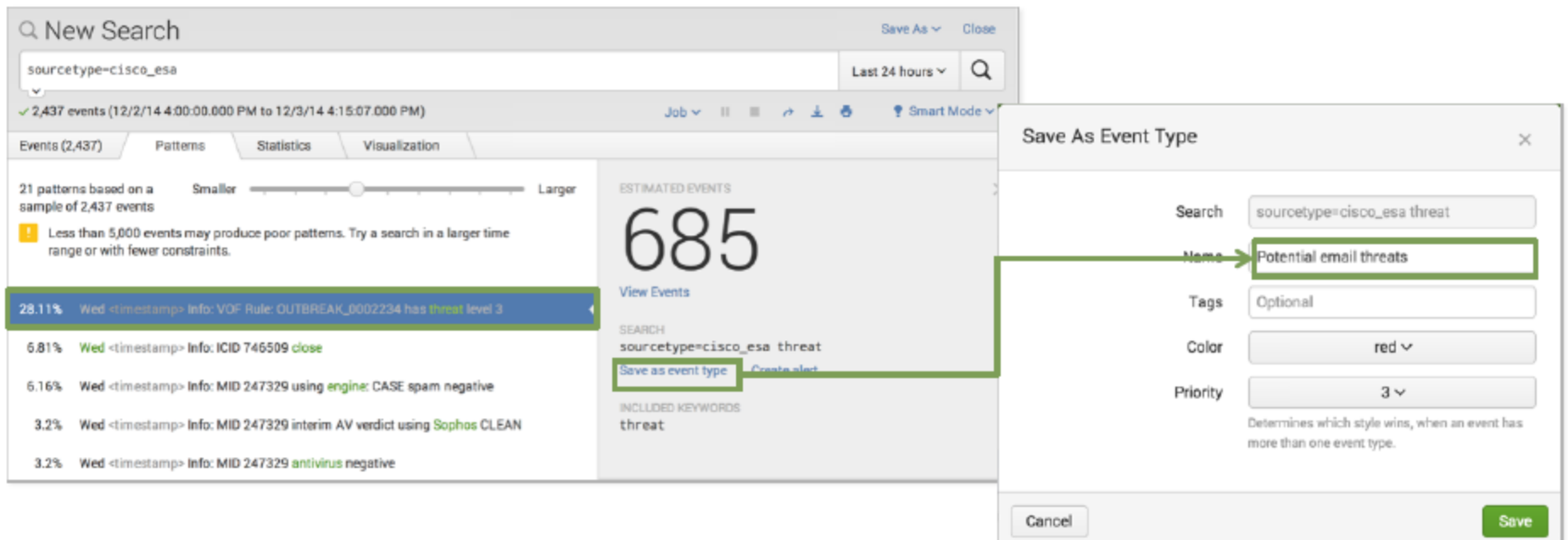
Creating an Event Type via Patterns

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

- 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

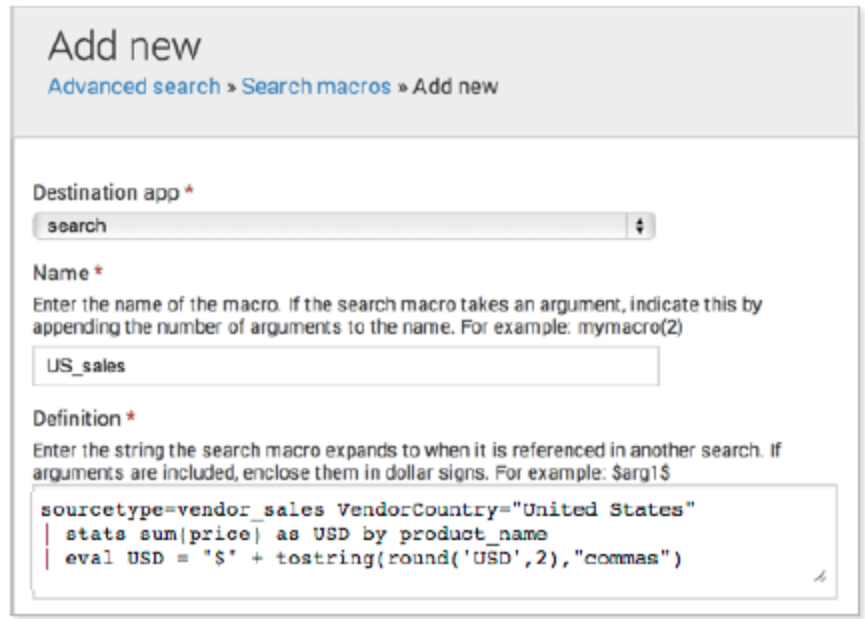
Macros Overview

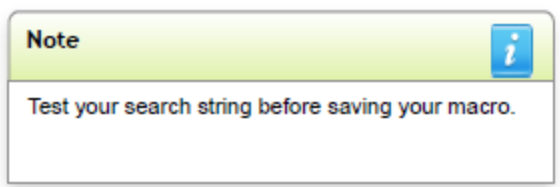
- Useful when you frequently run searches or reports with similar search syntax
- The time range is selected at search time
- Macros can be a full search string or a portion of a search that can be reused in multiple places
- Allows you to define one or more arguments within the search segment
  - Pass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

Creating a Basic Macro

Settings > Advanced search > Search Macros

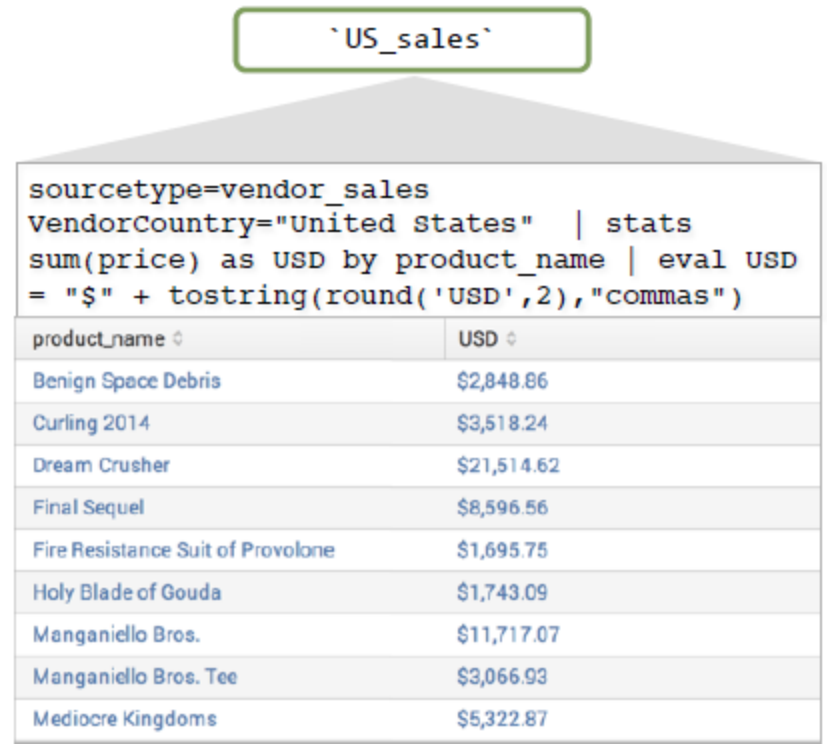
1. Click **New**
2. Select the destination app
3. Enter a Name
4. Type the search string
5. Save





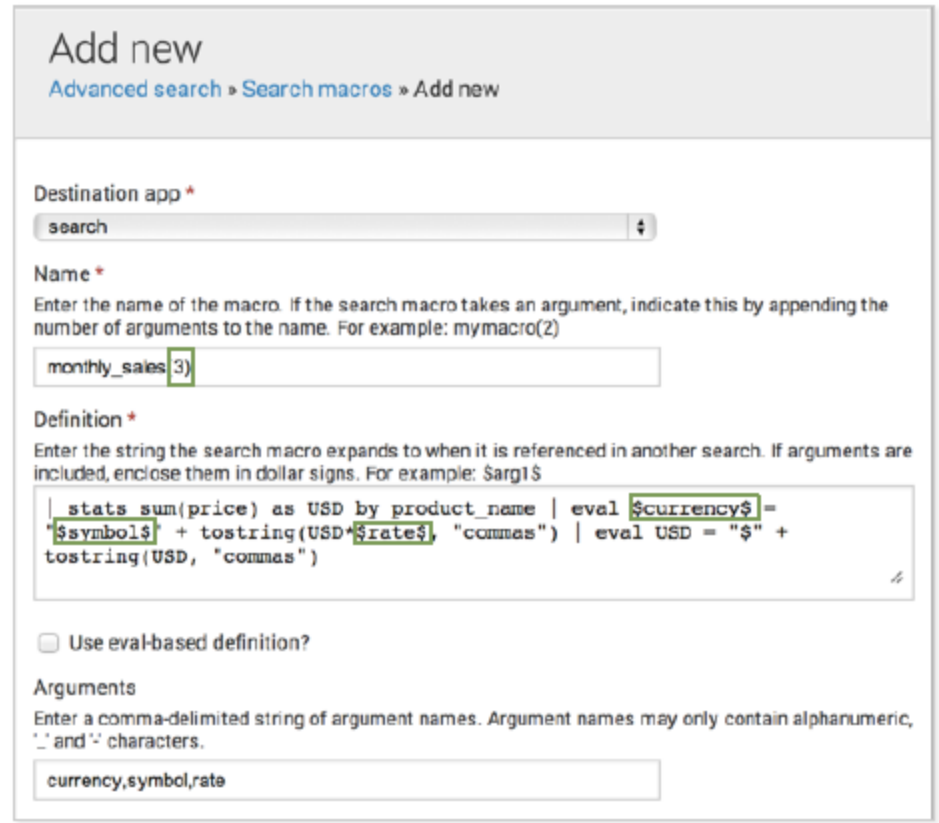
Using a Basic Macro

- 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



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)`
```

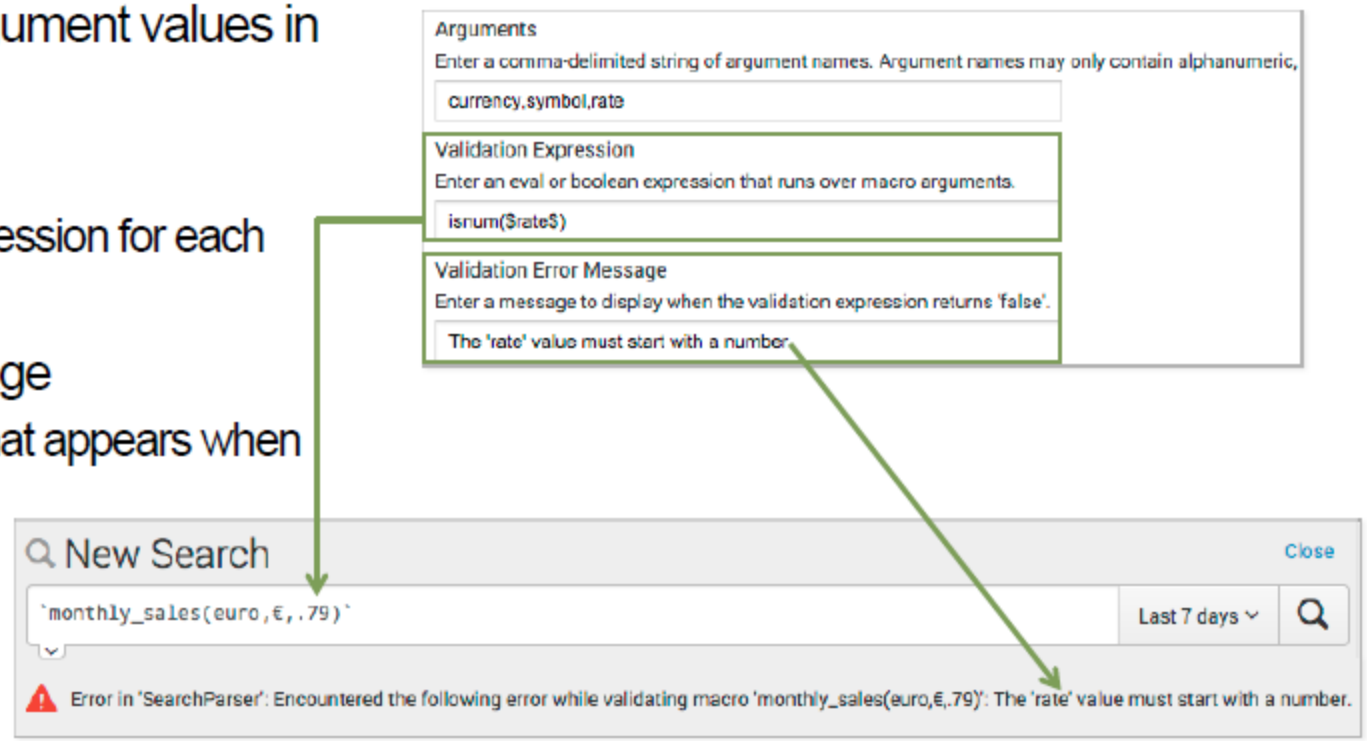
```
sourcetype=vendor_sales VendorCountry=Germany OR
VendorCountry=France OR VendorCountry=Italy
| stats sum(price) as USD by product_name |
eval euro = "€" + tostring(USD*.79, "commas")
| eval USD = "$" + tostring(USD, "commas")
```

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

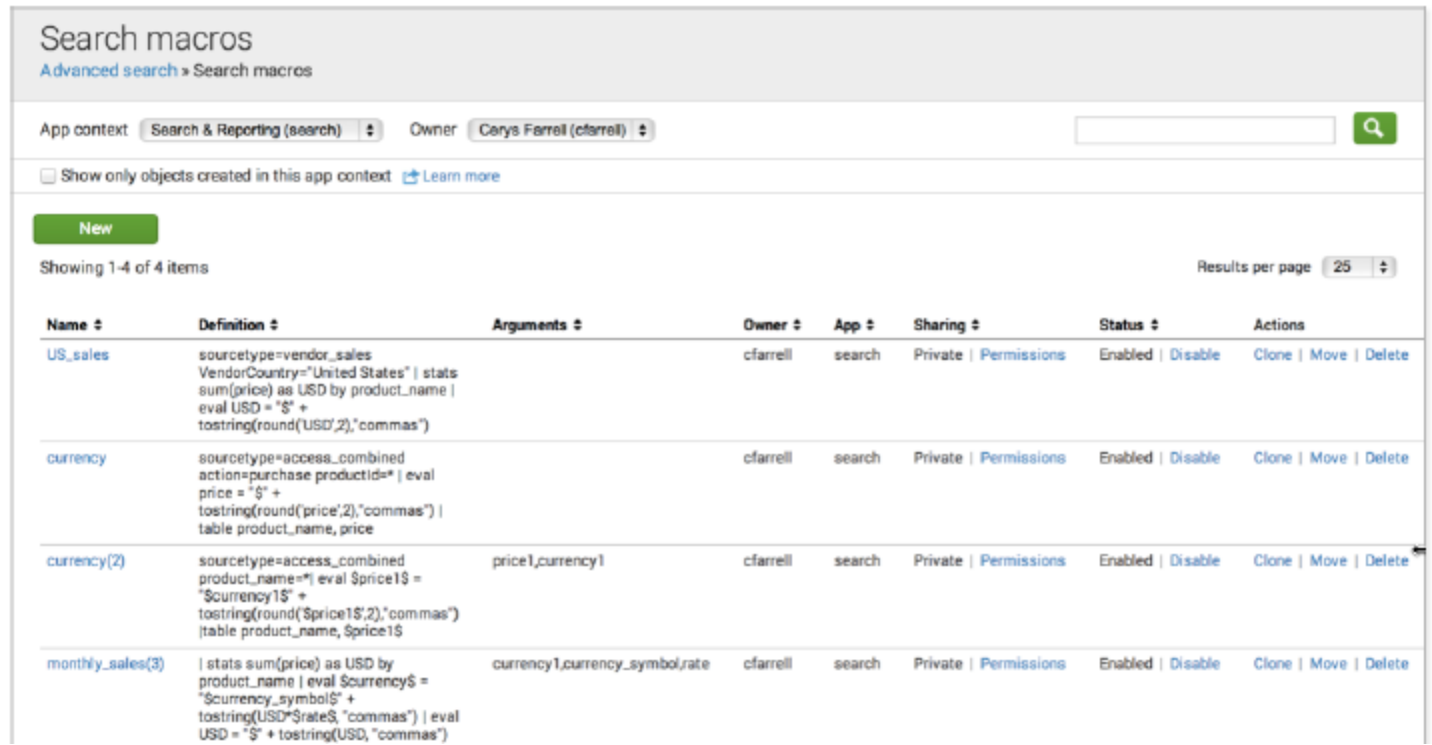
- Validation Expression
  - You can enter an expression for each argument
- Validation Error Message
  - This is the message that appears when you run the macro



Managing Macros

Settings > Advanced search > Search macros

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

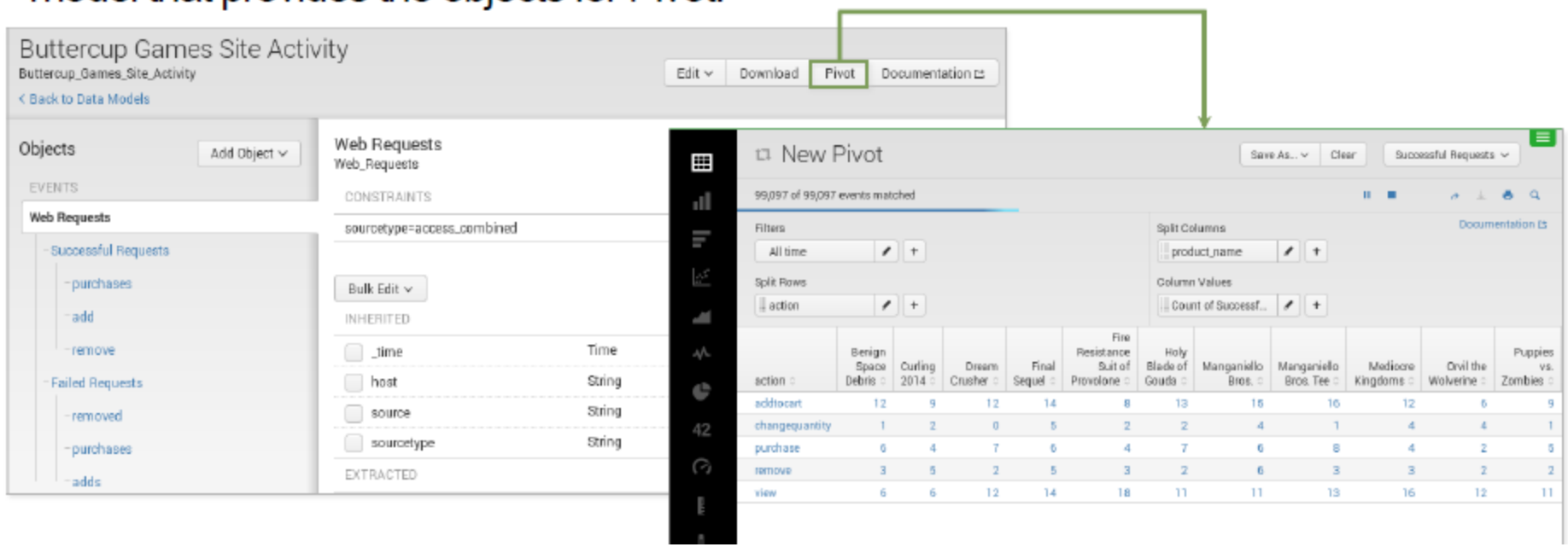


Objectives

- 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

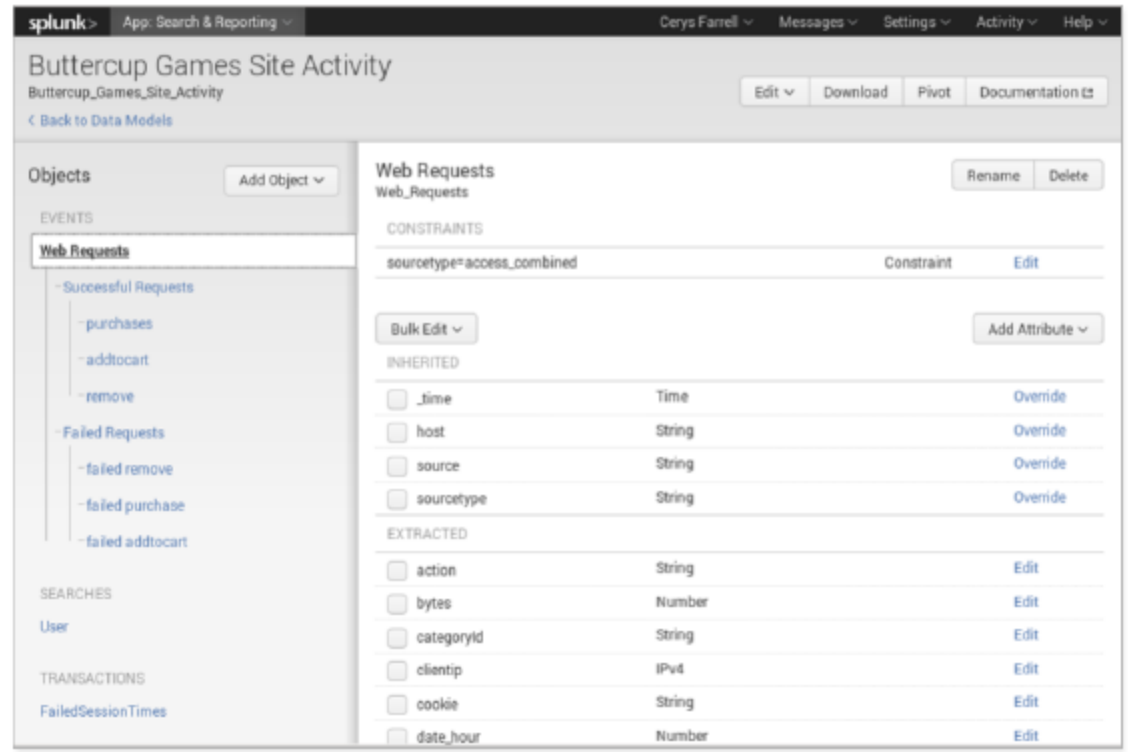
Reviewing Pivot

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.



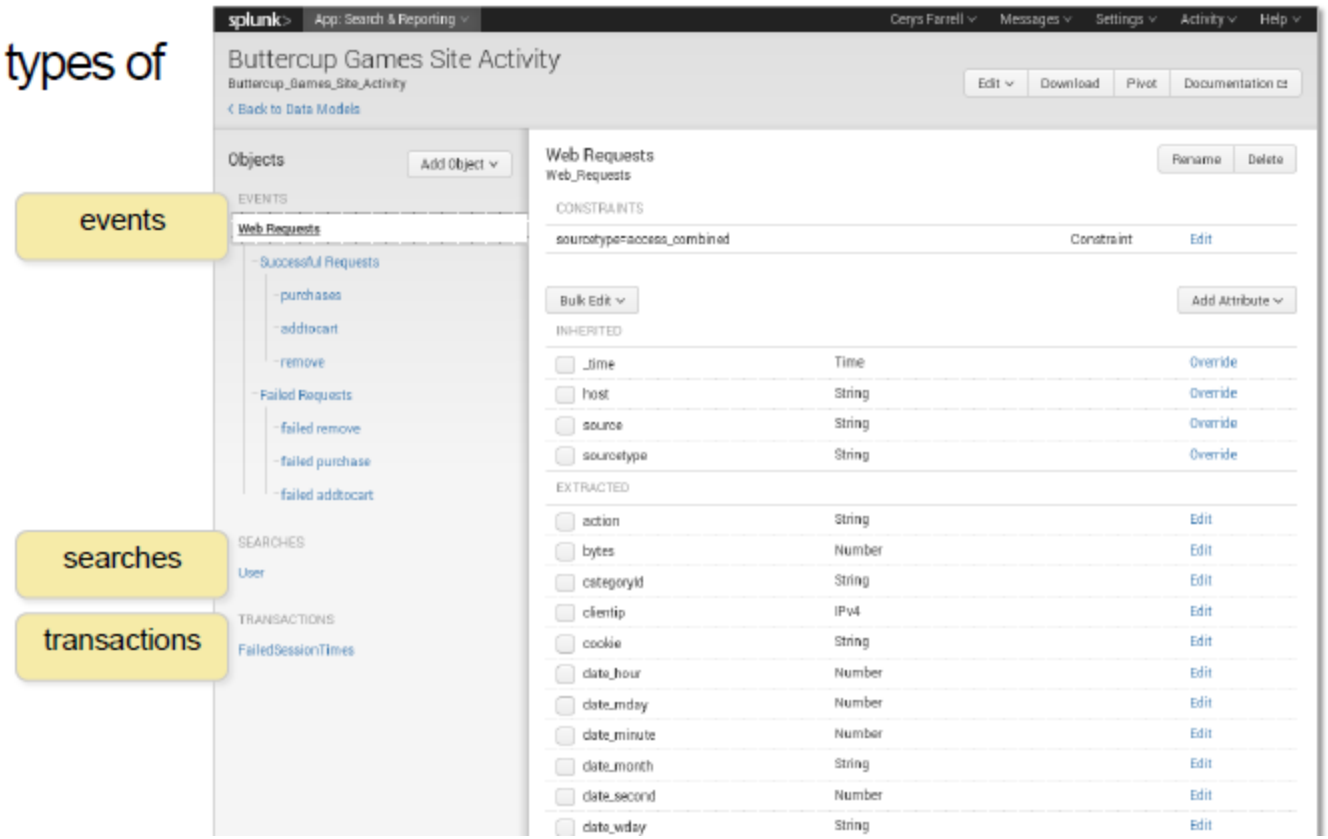
Overview of Data Models

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

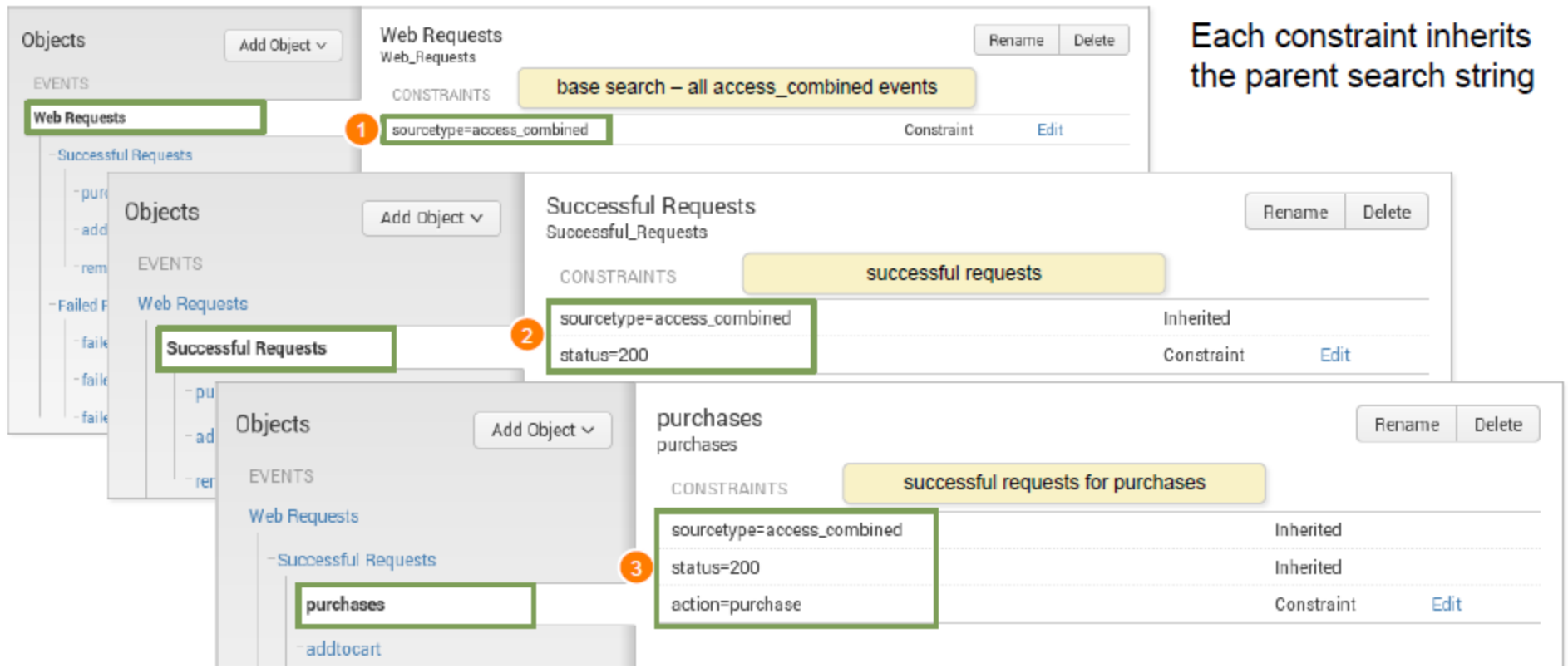


Data Model Objects

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



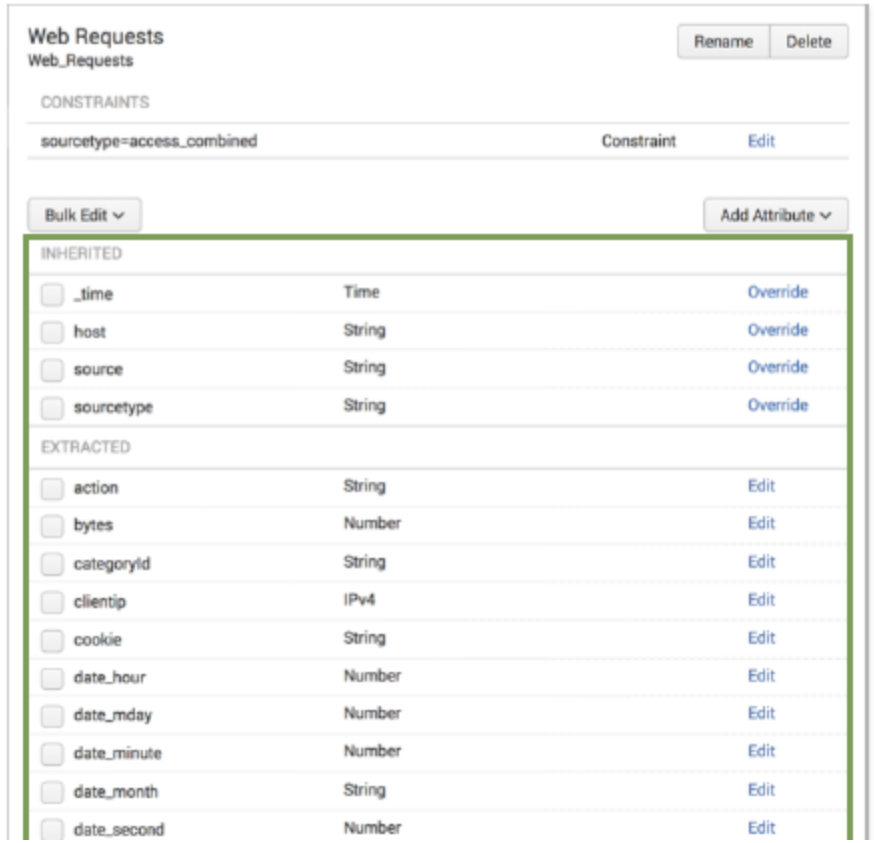
Event Object Hierarchy and Constraints



Each constraint inherits the parent search string

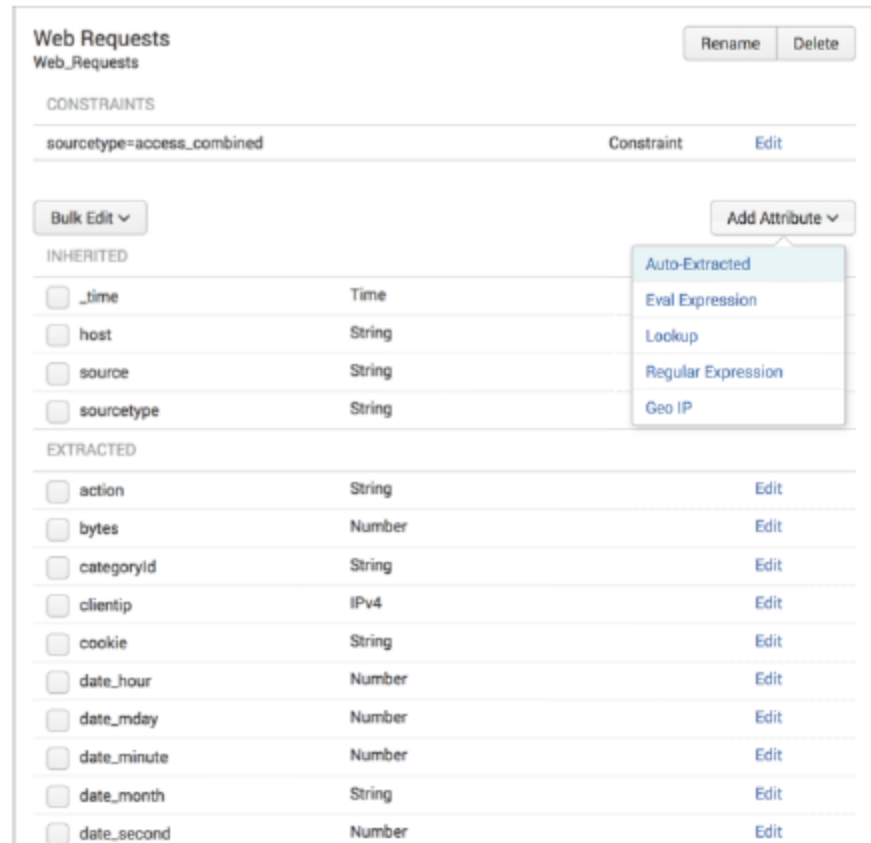
Object Attributes

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



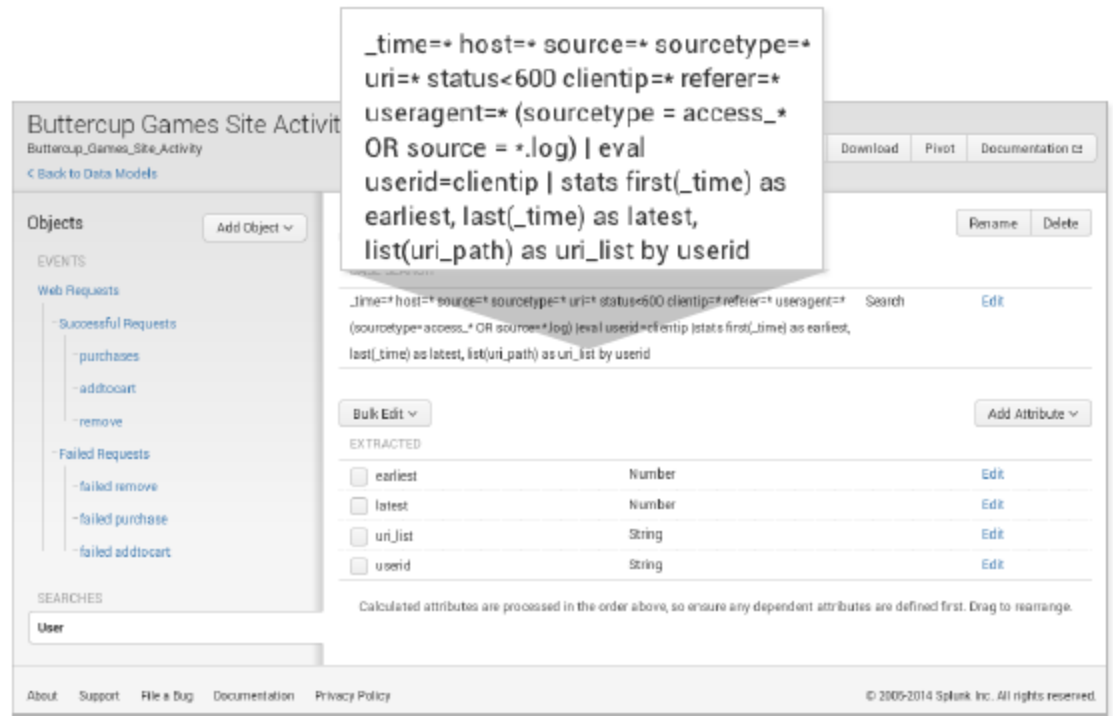
Object Attributes (cont.)

- **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.



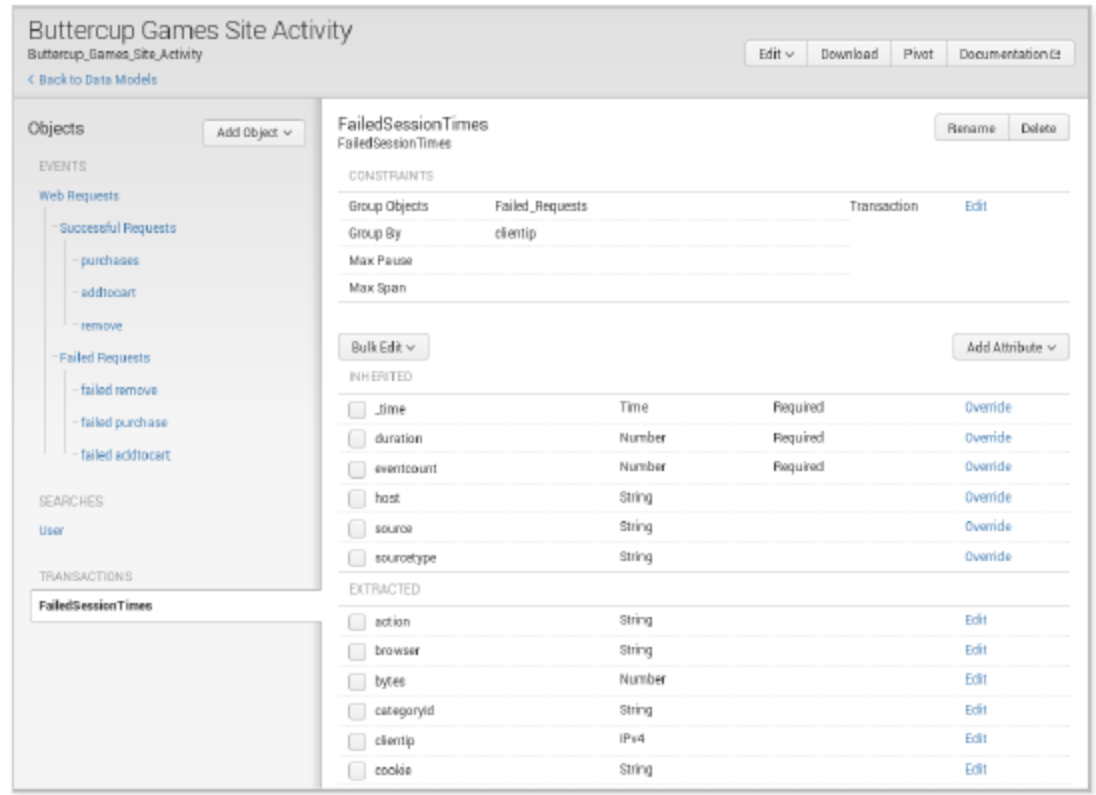
Data Model Search Objects

- 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



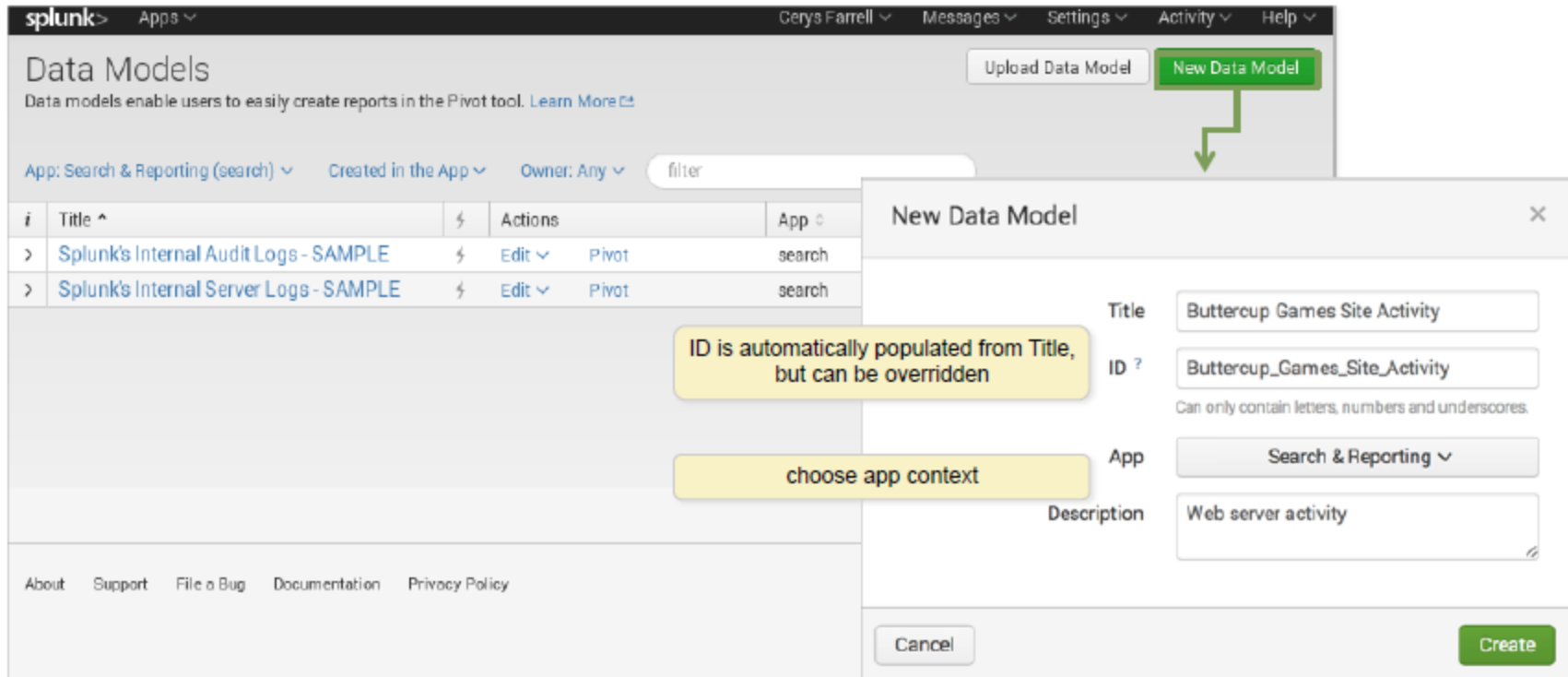
Data Model Transaction Objects

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

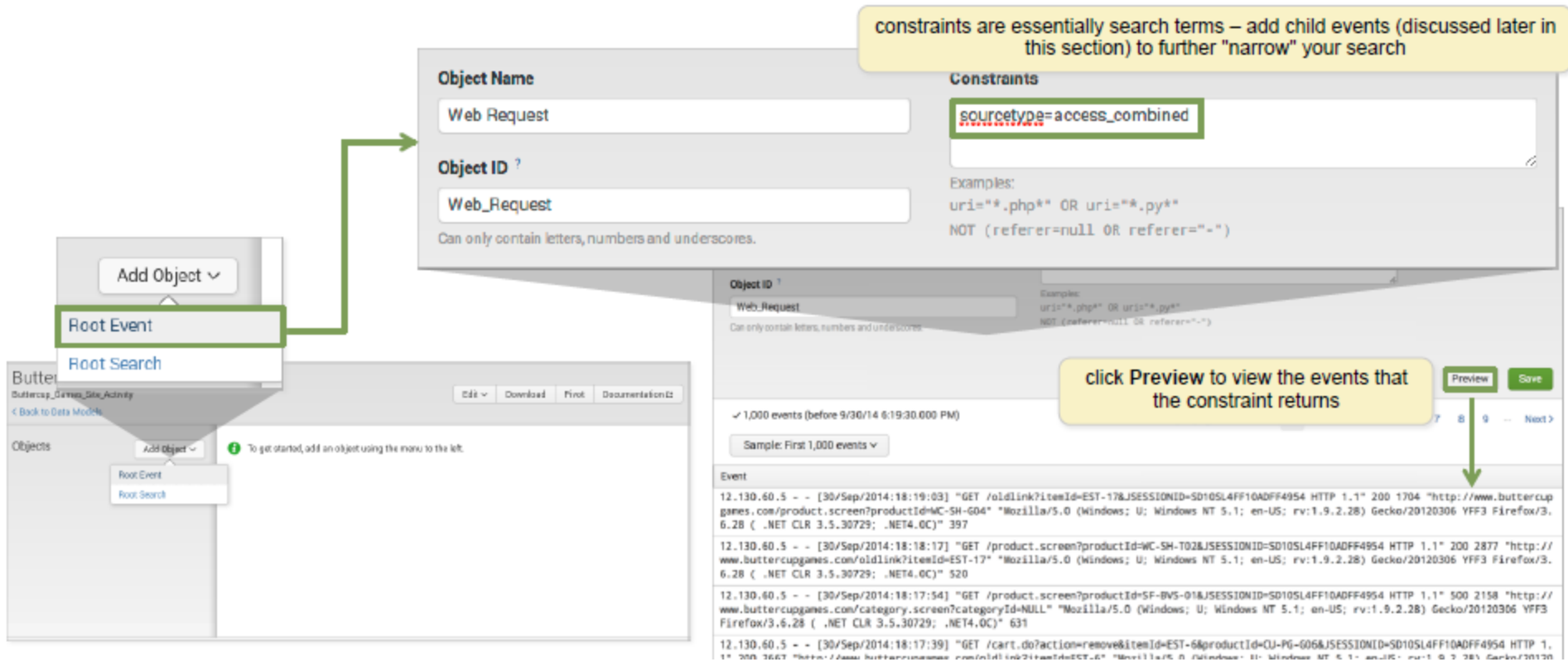


Creating a Data Model

Settings > Data Models

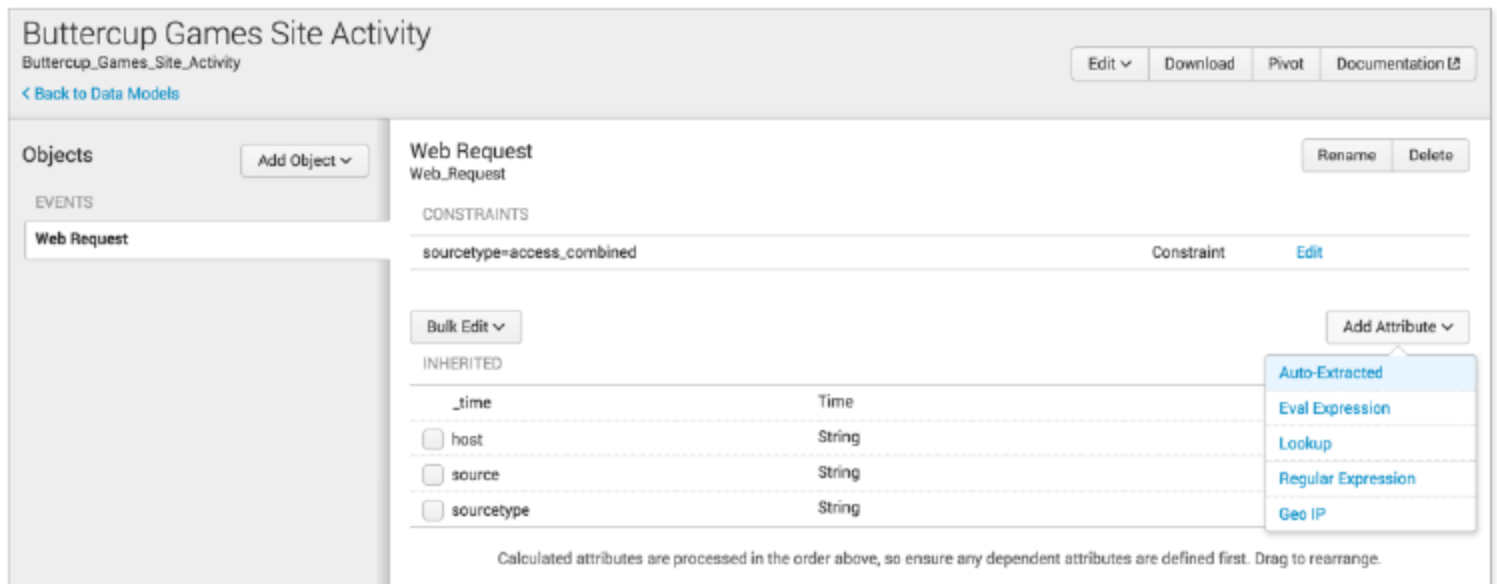


Adding a Root Event



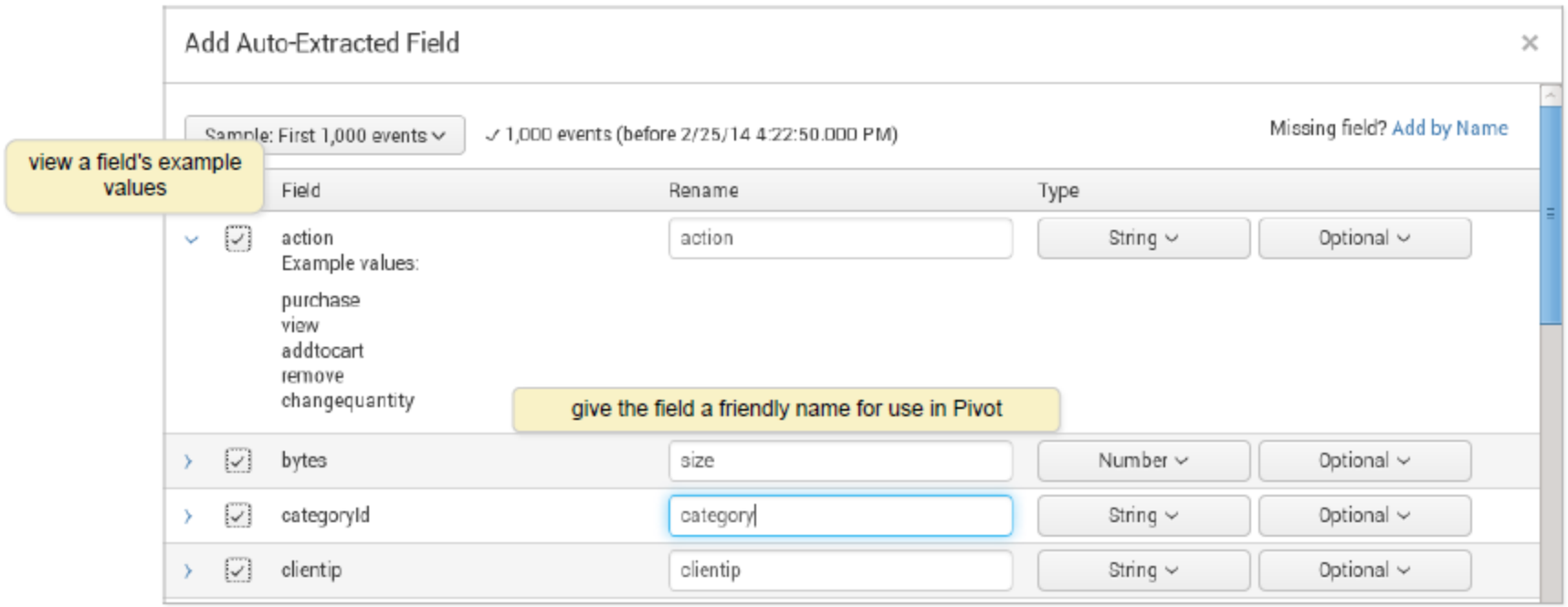
Adding a Root Event (cont.)

- 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



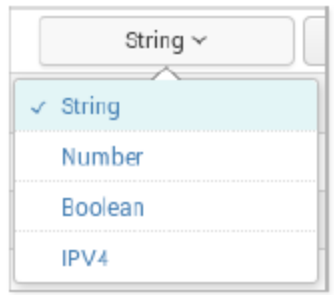
Adding Attributes – Auto-Extracted (Fields)

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



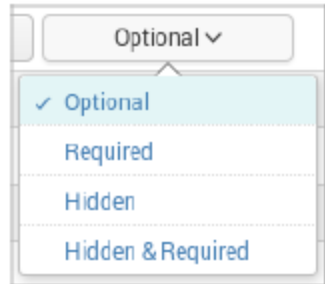
Attribute Types

- **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

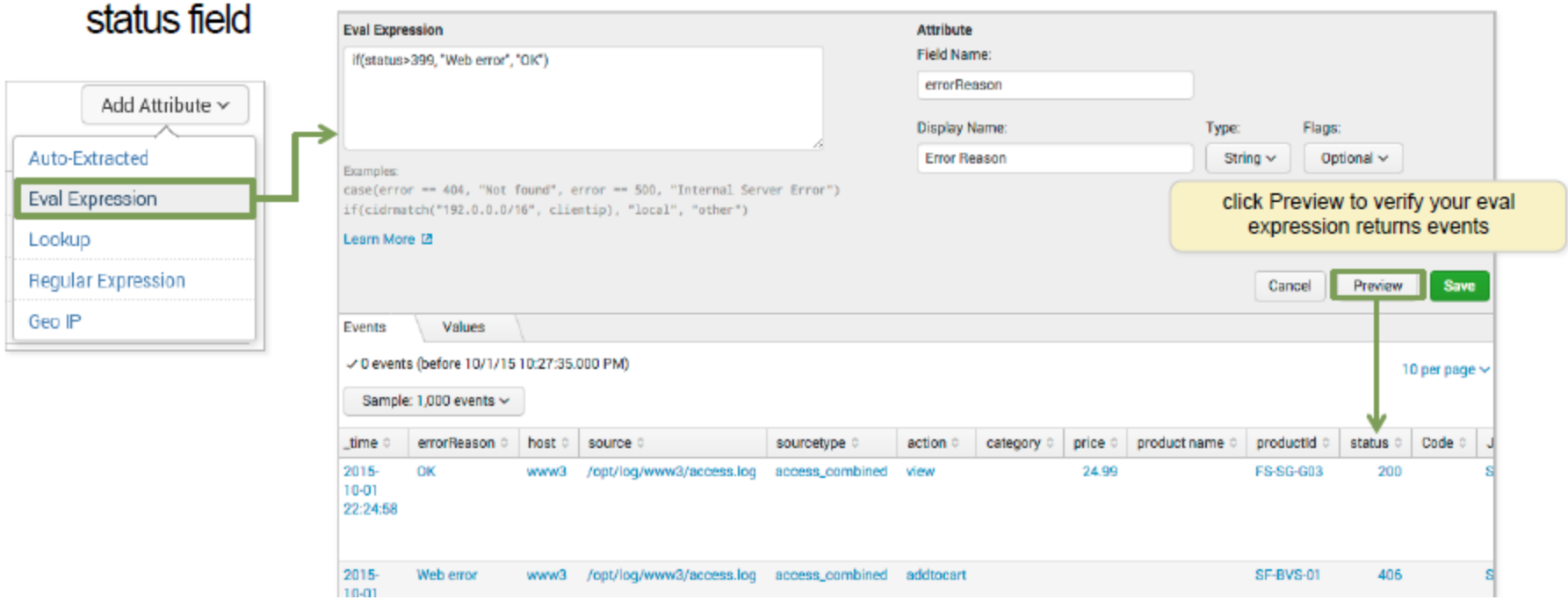


- **Hidden:** This field is not displayed to Pivot users when they select the object in Pivot
  - Use for fields that are only being used to define another attribute, such as an eval expression
- **Hidden & Required:** Only events that contain this field are returned, and the fields are hidden from use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

Adding Attributes – Eval Expressions

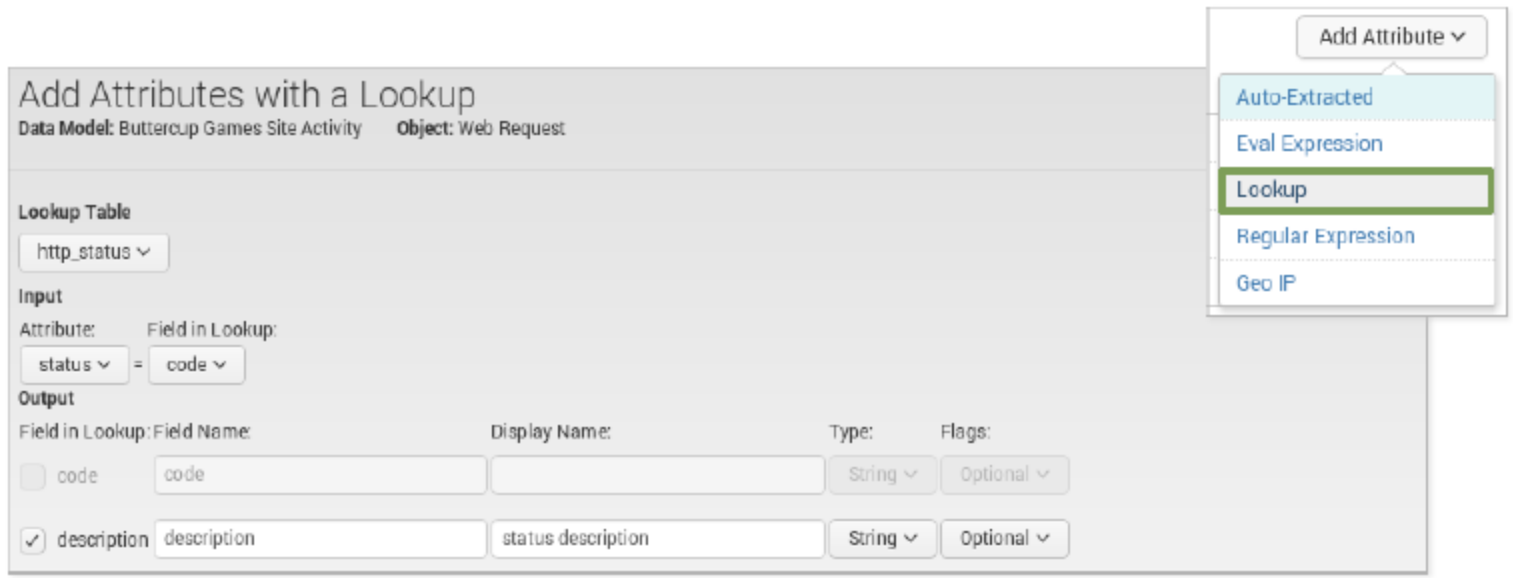
You can define a new field using an eval expression

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



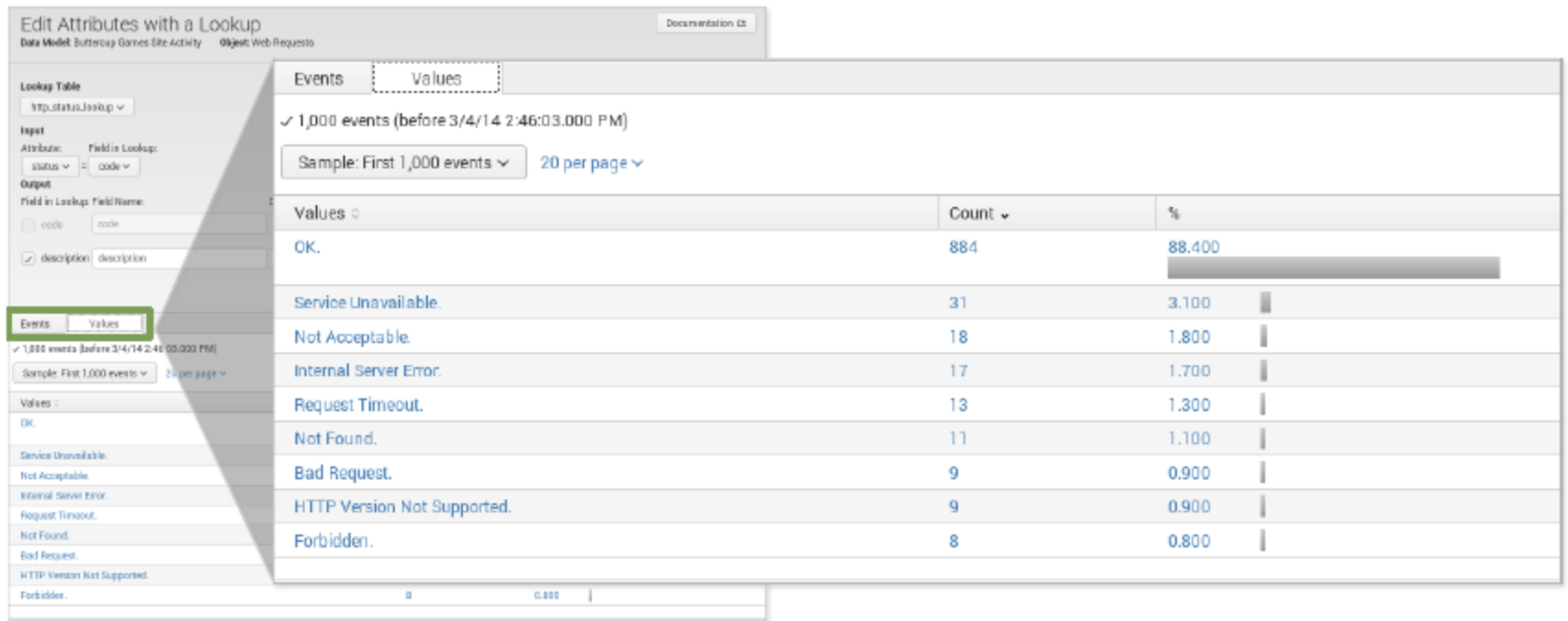
Adding Attributes – Lookups

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



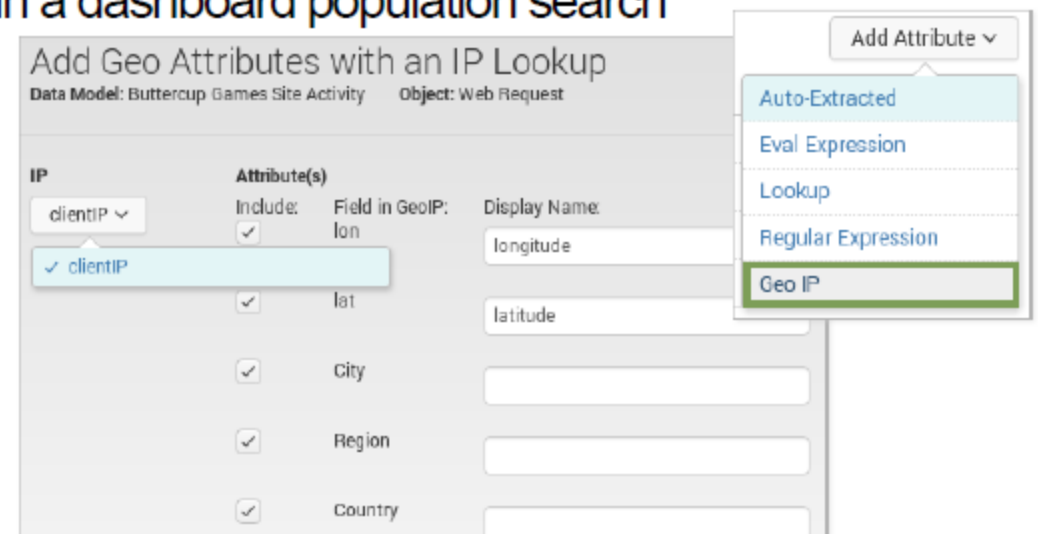
Adding Attributes – Lookups (cont.)

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



Adding Attributes - 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

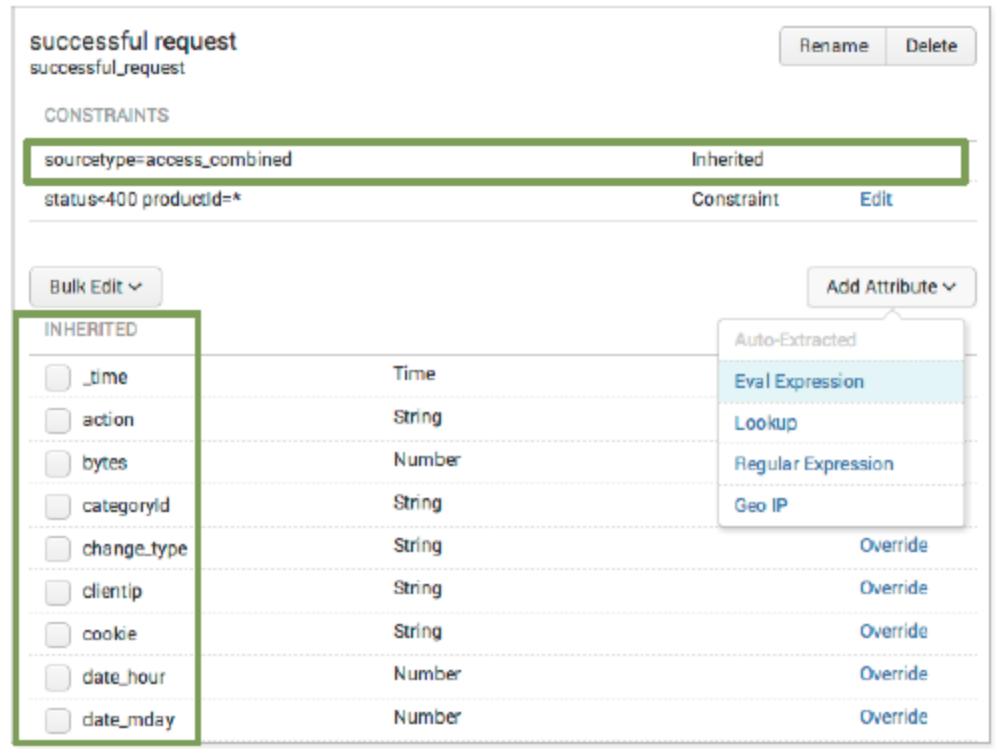


Adding Child Events

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

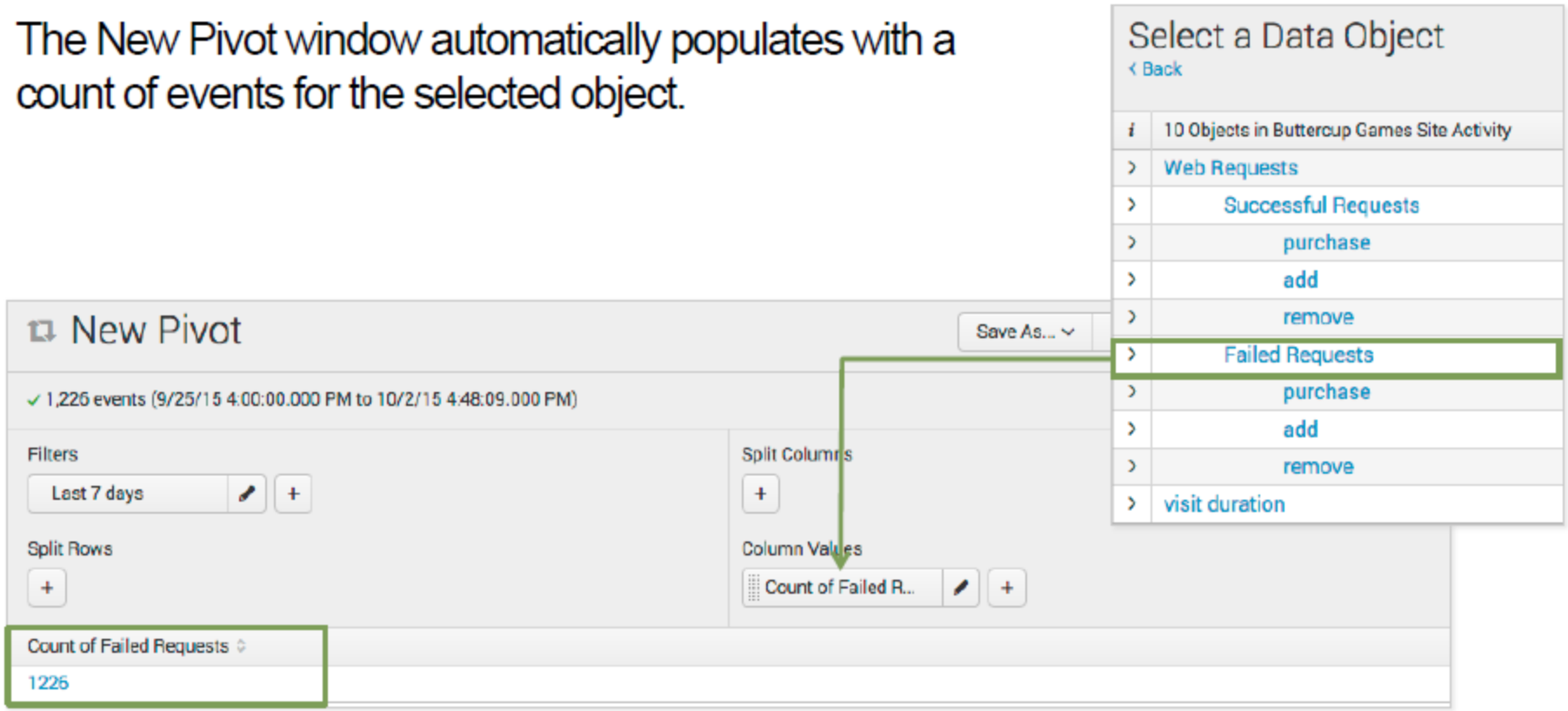
Adding Child Events (cont.)

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



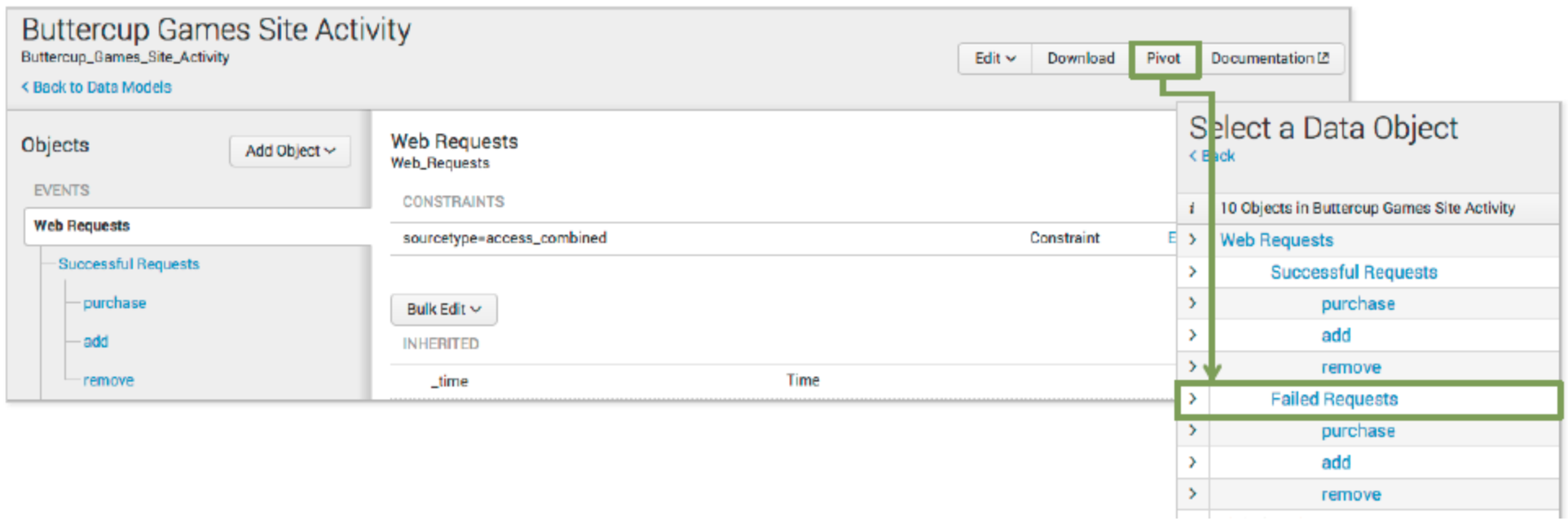
Using the Data Model in Pivot (cont.)

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



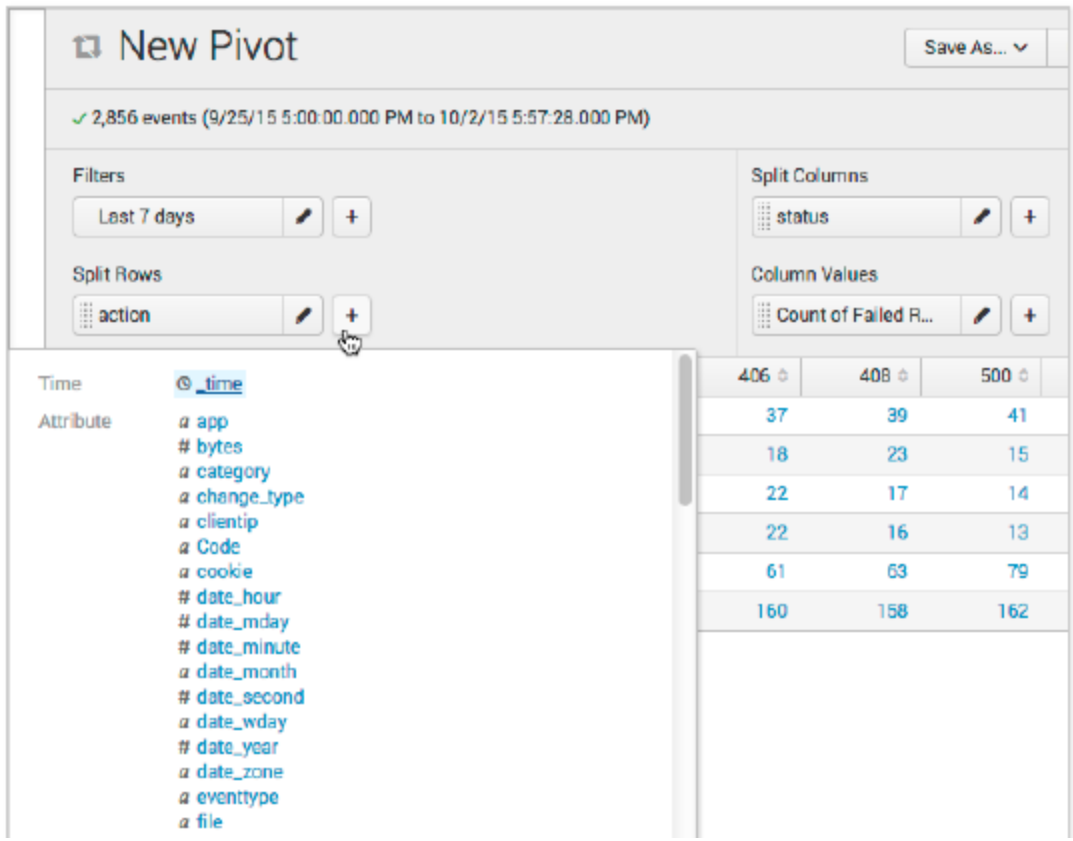
Using the Data Model in Pivot

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



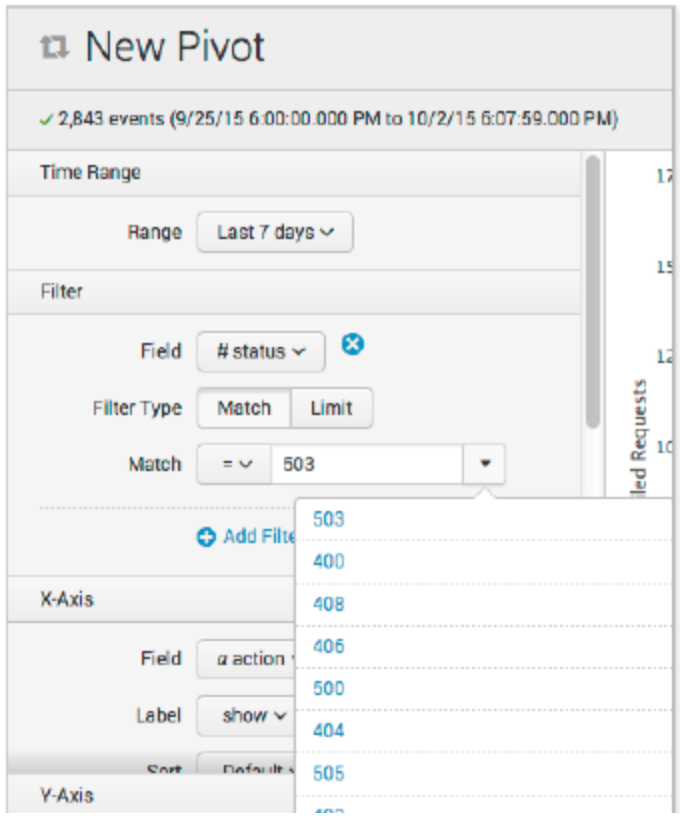
Pivot – Using Attributes

- 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

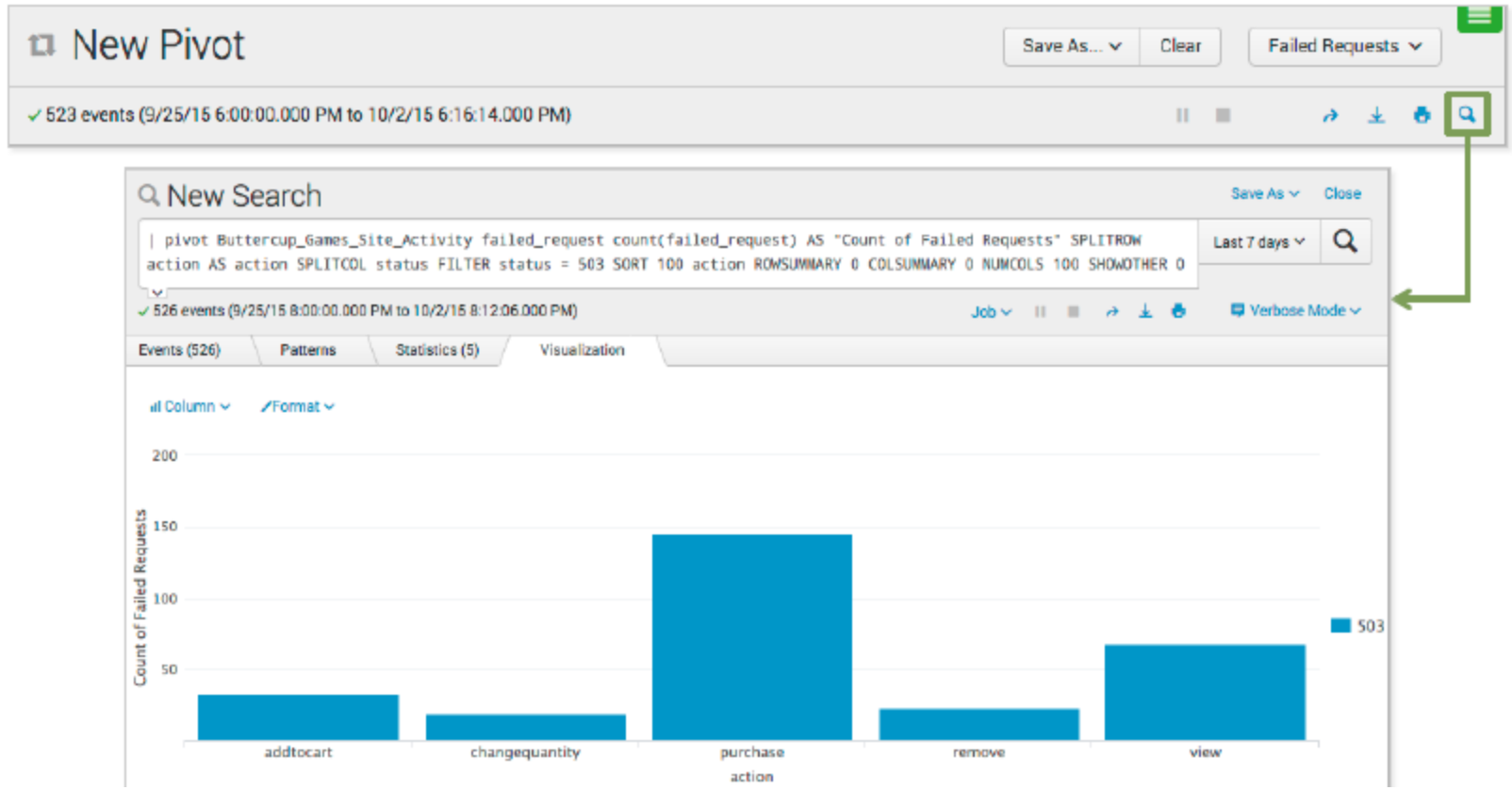


Pivot – Using Attributes (cont.)

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

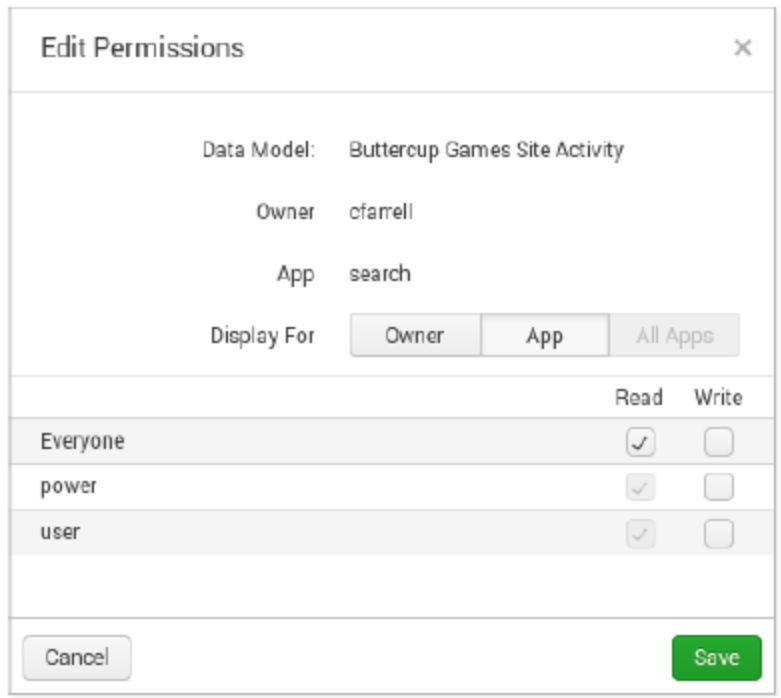


Underlying Search



Set Permissions

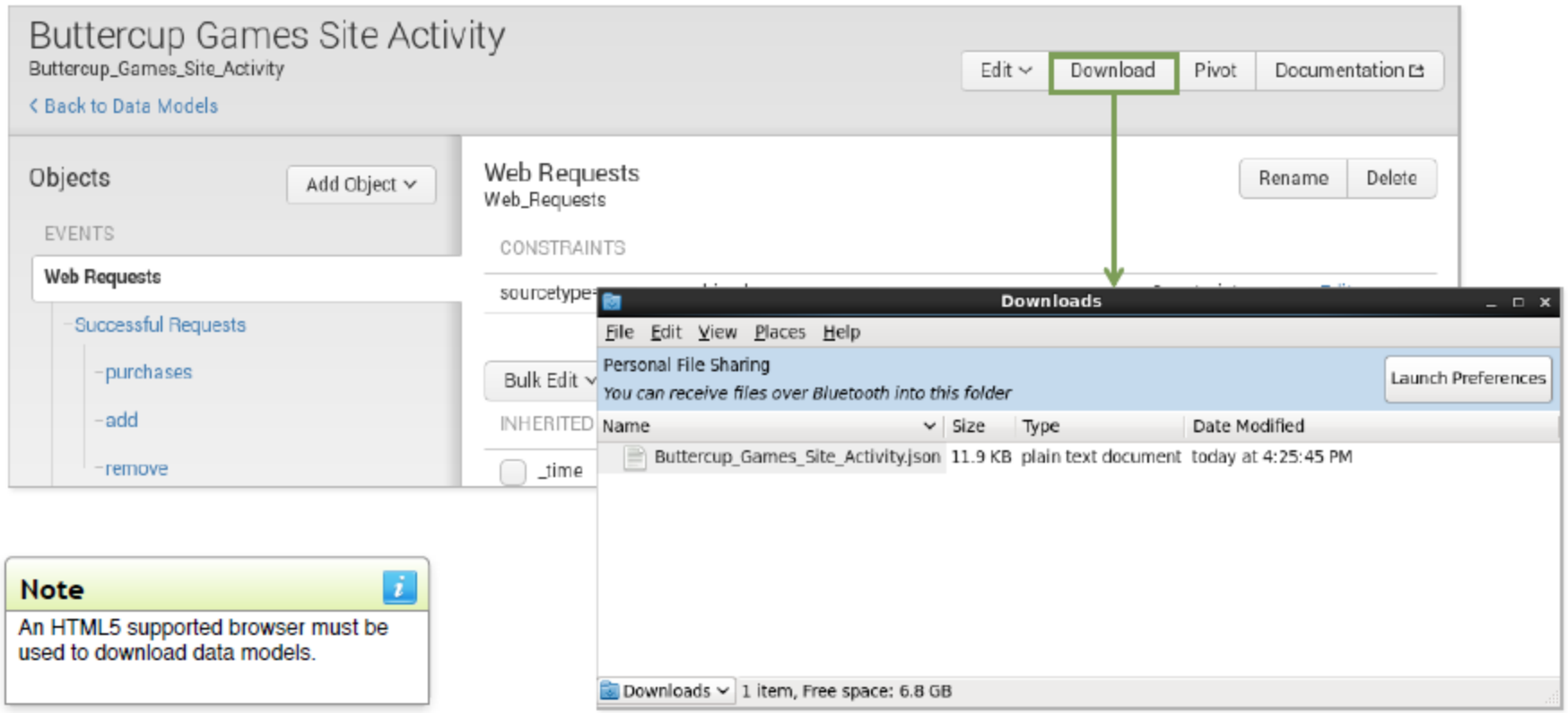
- When a data model is created, the owner can determine access based on the following permissions:
  - Who can see the data models
    - Owner, App, or All Apps
  - Which users can perform which actions (Read/ Write)
    - Everyone
    - Power
    - User
    - Admin-defined roles, if applicable



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

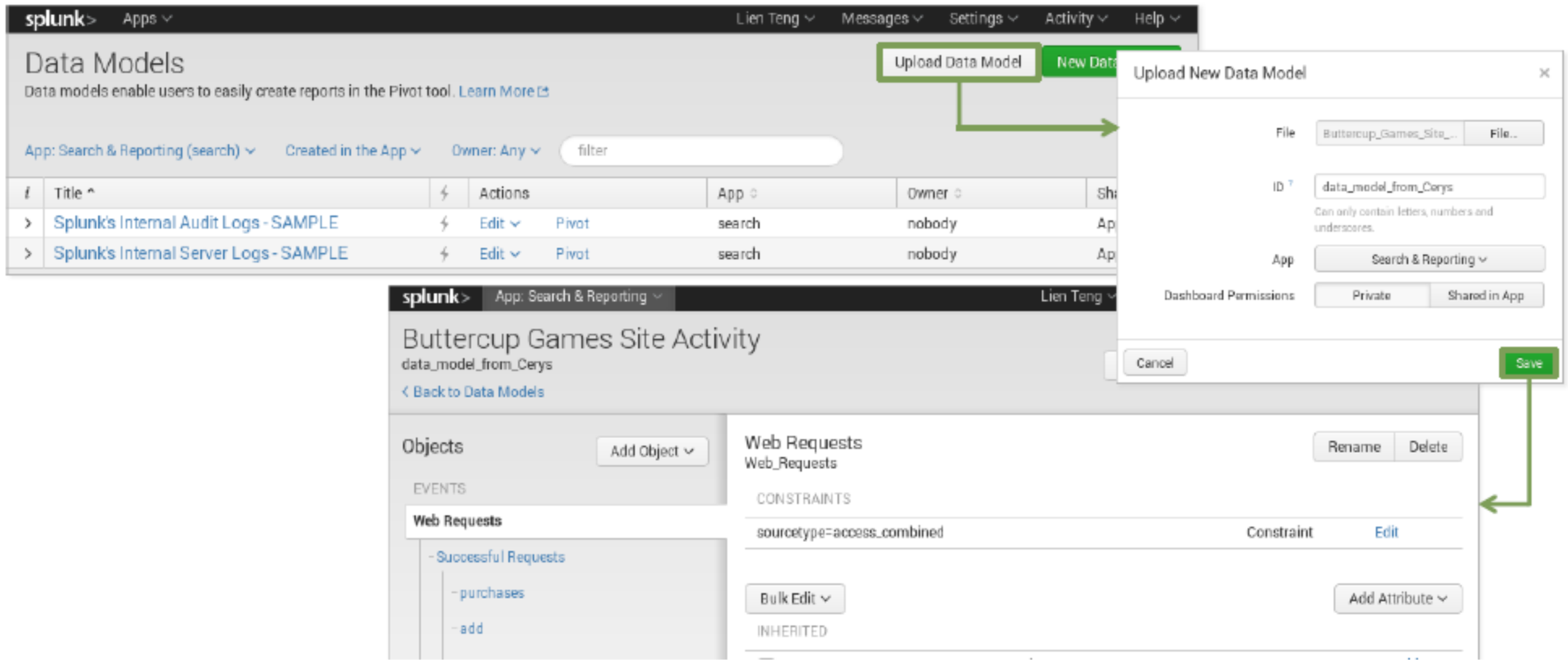
Downloading a Data Model



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.