Creating Knowledge Objects

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Lab Exercise slides reference the hands-on lab exercise guide
- Do not distribute

Course Goals

- Create search macros
- Create event types
- Understand event types and use the event type builder
- Compare event types and reports
- Create workflow actions
- Create tags and aliases
- Create calculated fields

Course Outline

- Knowledge Objects and Search-time Operations
- Create Event Types
- Create Workflow Actions
- Create Tags and Aliases
- Create Search Macros
- Create Calculated Fields

Knowledge Objects & Search-time Operations

Topic Objectives

- Understand role of knowledge objects for enriching data
- Define search-time operation sequence

Knowledge Objects

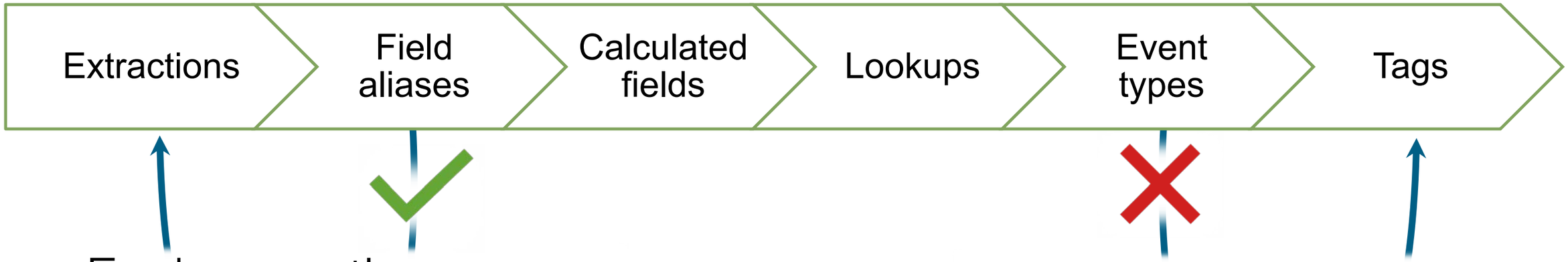
- Knowledge objects are user-defined entities that can be used to enrich data and retrieve specific information about data
- Can be shared or used privately
- The following knowledge objects are discussed in this course:
  - Event types
  - Workflow actions
  - Tags
  - Field aliases
  - Search macros
  - Calculated fields

Search-time Operation Sequence

After running a search, Splunk performs a specific sequence of operations to pull knowledge objects and apply them to the events returned by the search

Search-time Operation Sequence

Search-time operations are always applied in the same order when generating the knowledge objects



Each operation can reference fields derived from operations that **precede** them

No operation can reference fields that are derived by operations that **follow** them

Create Event Types

Topic Objectives

- Define event types
- Create event types using:
  - New Event Type
  - Search page
  - Event Type Builder
- Use Event Types
- Find Event Types
- Tag event types
- Compare event types and reports

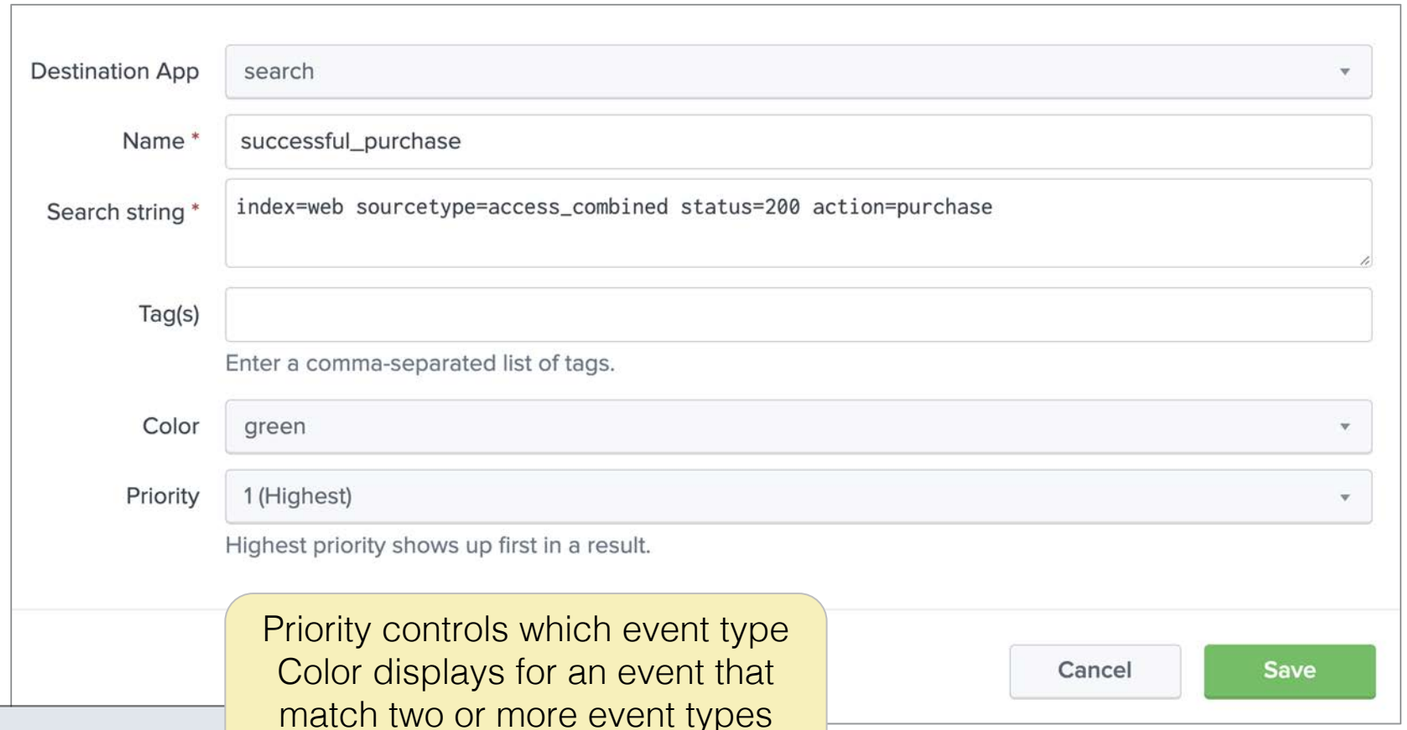
Define Event Types

- Categorizes events based on a search string
- A useful method for institutional knowledge capturing and sharing
- Can be tagged to group similar types of events
- Processed after extractions, field aliases, calculated fields, and lookup in the Search Time Operation Sequence

Create an Event Type: New Event Type

Settings > Event types > **New Event Type**

- Choose a Destination App
- Name the event type
- The Search string is the basic search that meets your event type criteria



Priority controls which event type Color displays for an event that match two or more event types

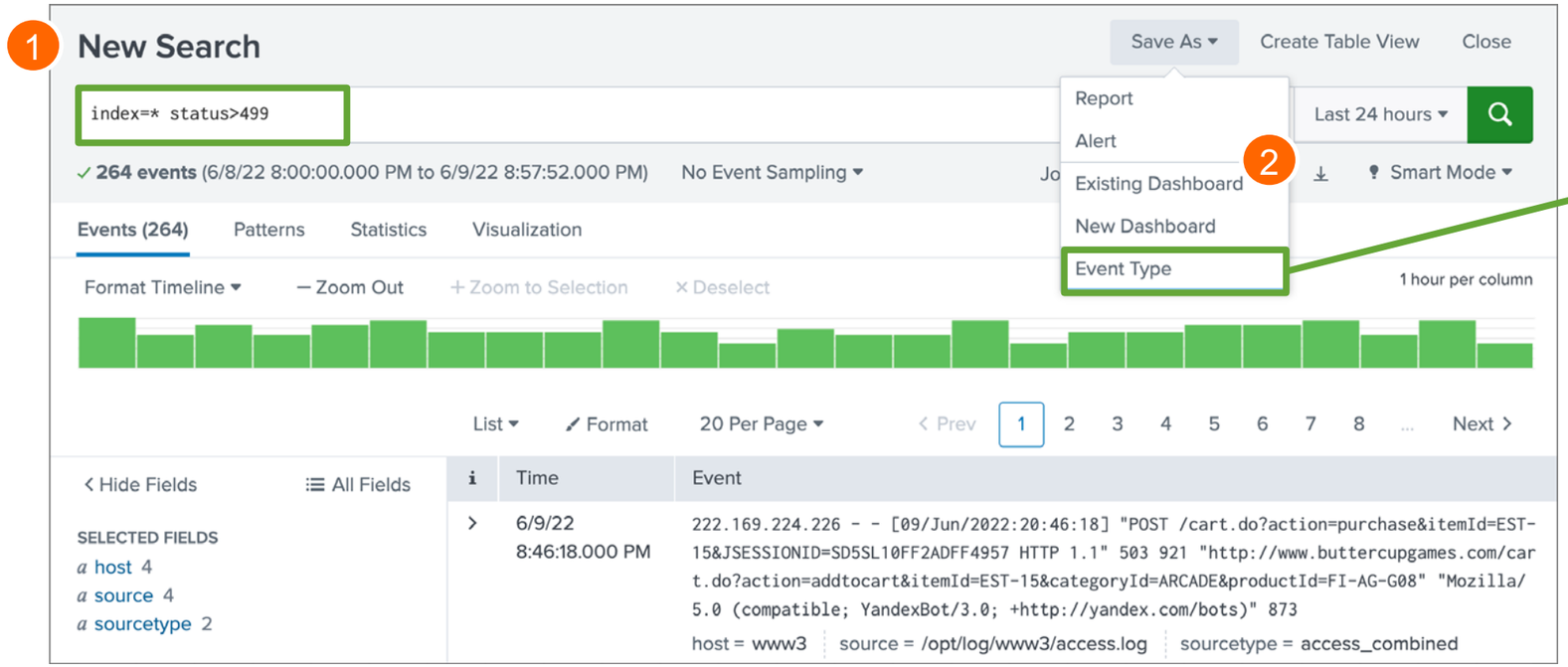
`index=web`

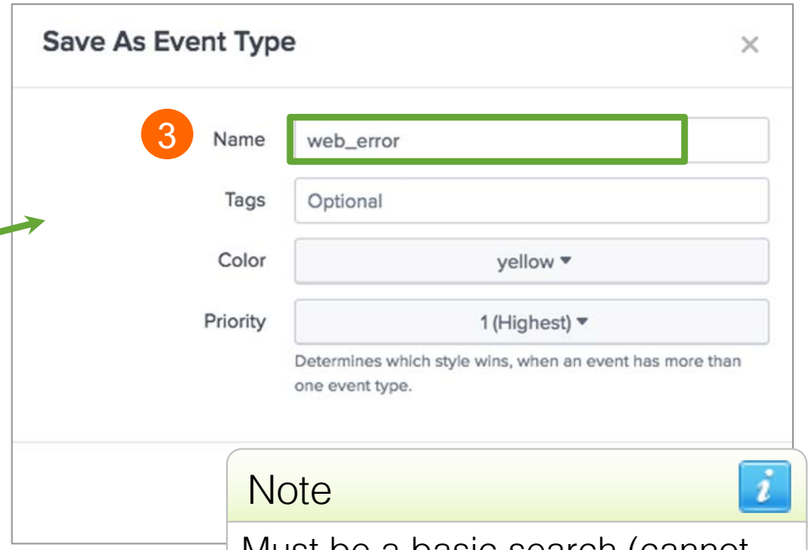
i	Time	Event
>	6/9/22 8:53:20.000 PM	188.173.152.100 - - [09/Jun/2022:20:53:20] "POST /cart/success.do?JSESSIONID=SD4SL5FF10ADFF4955 HTTP 1.1" 200 1426 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-21" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 780 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined

 | 11 August 2022

Create an Event Type: Search

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)



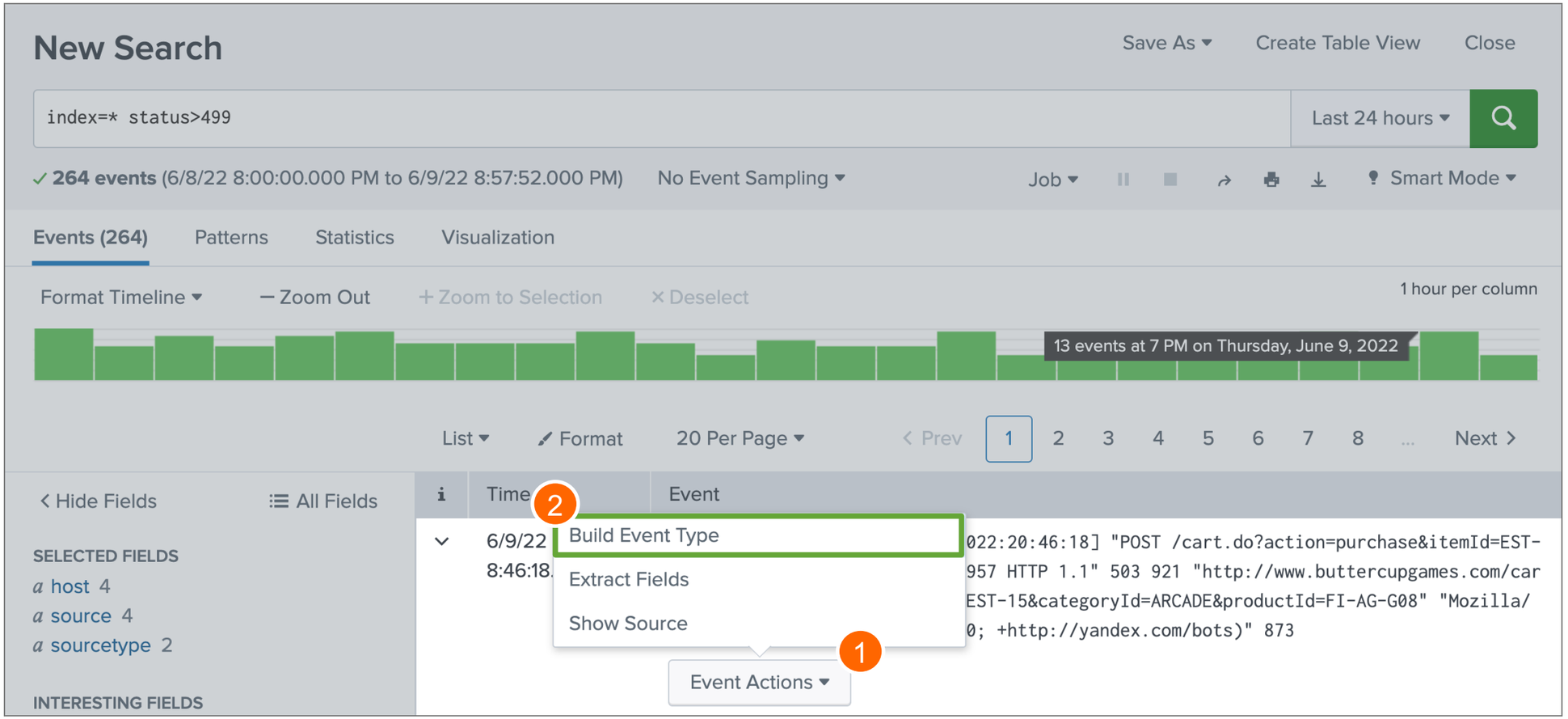


Note

Must be a basic search (cannot contain pipes or subsearches).

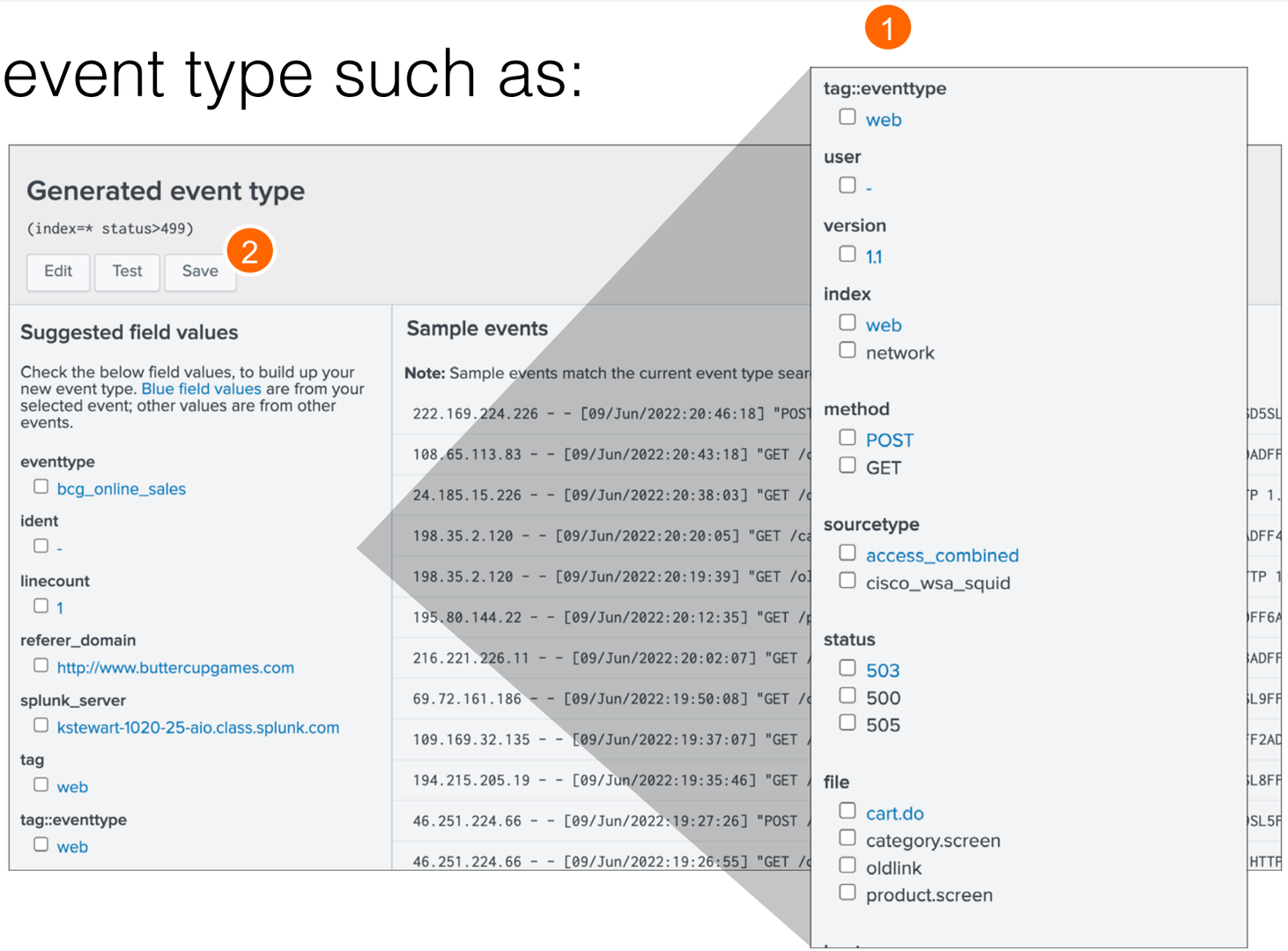
Create an Event Type: Event Type Builder

From the event details, select **Event Actions > Build Event Type**



Create an Event Type: Event Type Builder (cont.)

1. Refine the criteria for your event type such as:
   - Search string
   - Field values
   - Tags
2. Verify your selections and click Save



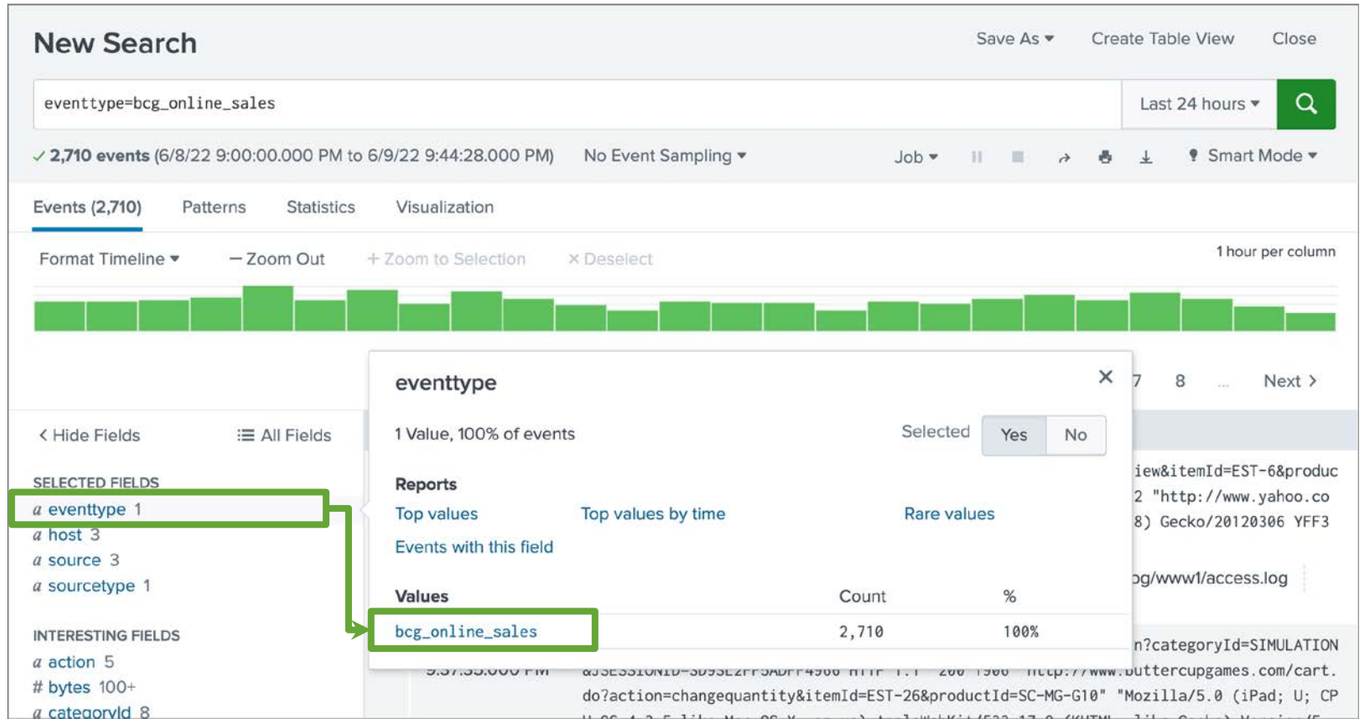
Note

The preferred—and easier—method for creating an event type is from the Search page, as previously shown. While the Event Type Builder can be used, it provides somewhat more limited functionality.

 | 11 August 2022

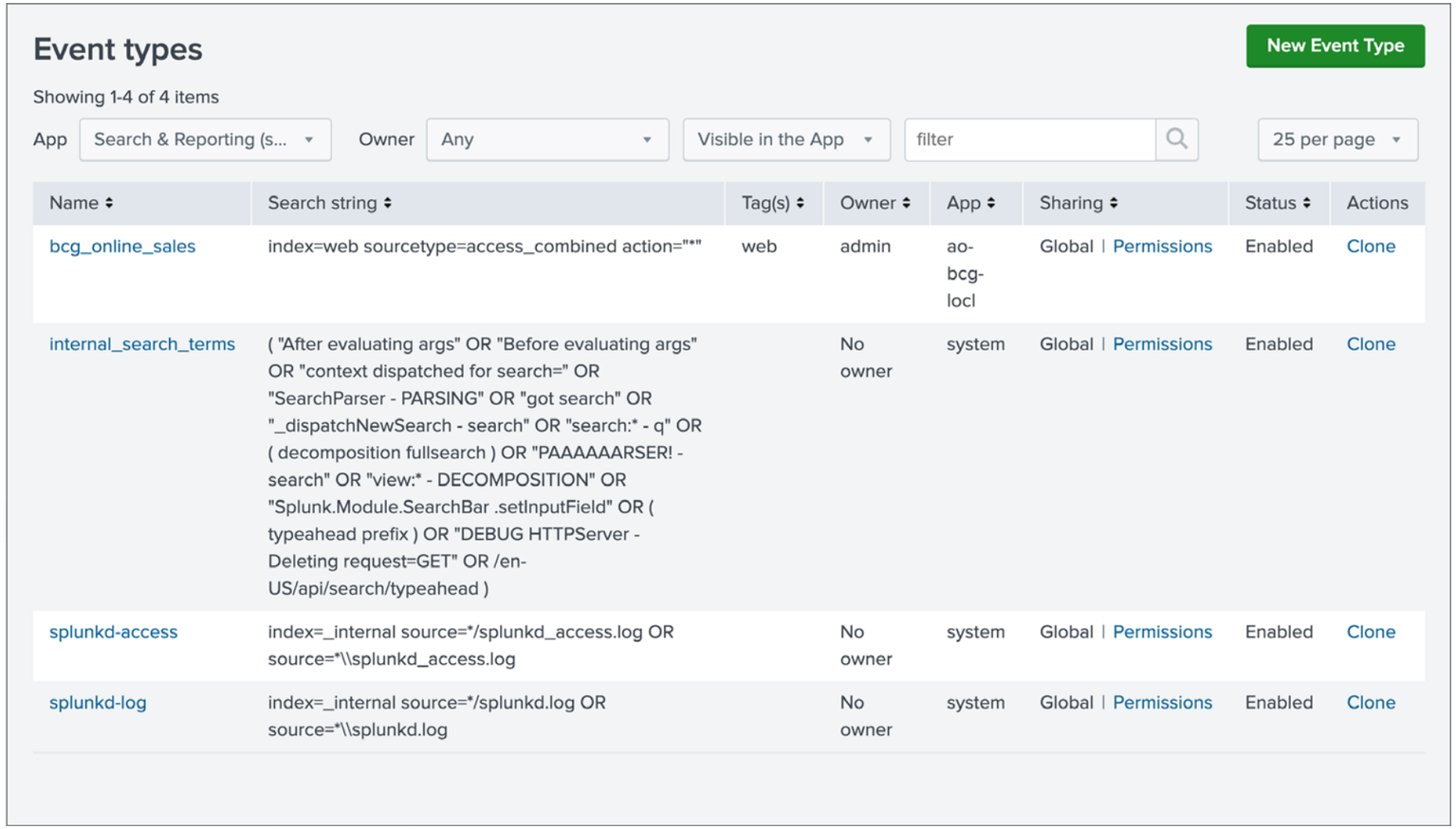
Use Event Types

- To verify the event type, search for **`eventtype=<event type>`**
- Fields sidebar displays **`eventtype`**, which can be added as a selected field
- Events are evaluated and the appropriate event types are applied at search time
- Using the Fields sidebar, view event types and their statistics



Find Created Event Types

- Settings > Event types
  - Displays event types you have permission to view or edit
  - Create new, clone, or maintain existing event types



Event types

New Event Type

Showing 1-4 of 4 items

App: Search & Reporting (s... | Owner: Any | Visible in the App | filter | 25 per page

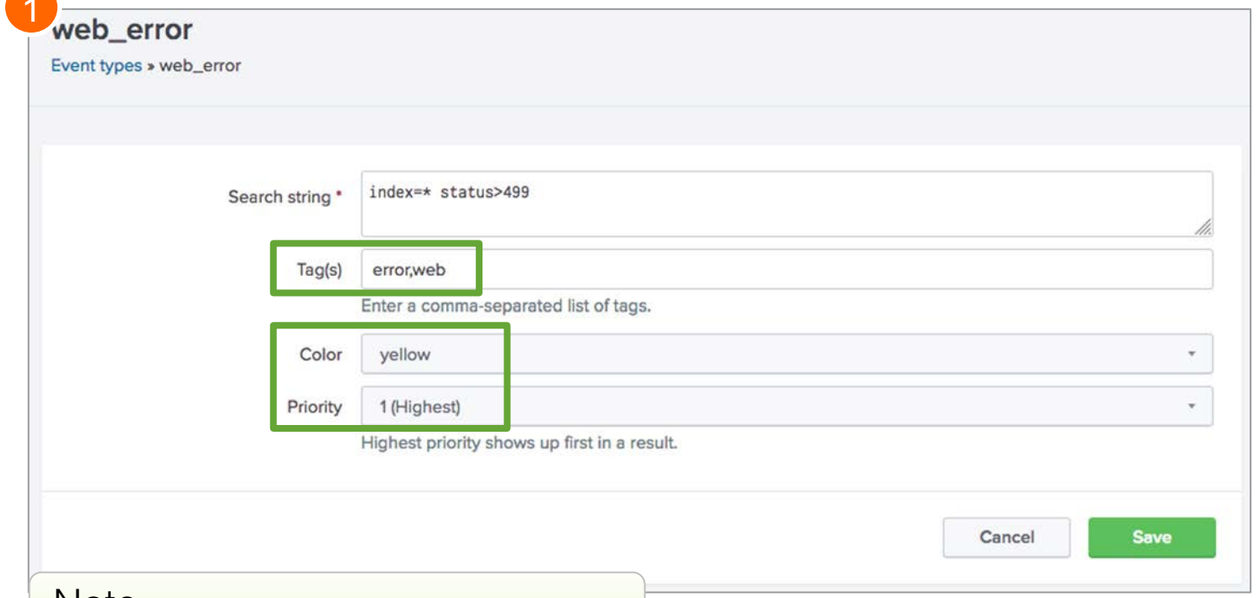
Name	Search string	Tag(s)	Owner	App	Sharing	Status	Actions
bcg_online_sales	index=web sourcetype=access_combined action="*"	web	admin	ao-bcg-locl	Global | Permissions	Enabled	Clone
internal_search_terms	("After evaluating args" OR "Before evaluating args" OR "context dispatched for search=" OR "SearchParser - PARSING" OR "got search" OR "_dispatchNewSearch - search" OR "search:* - q" OR (decomposition fullsearch) OR "PAAAAAARSER! - search" OR "view:* - DECOMPOSITION" OR "Splunk.Module.SearchBar .setInputField" OR (typeahead prefix) OR "DEBUG HTTPServer - Deleting request=GET" OR /en-US/api/search/typeahead)		No owner	system	Global | Permissions	Enabled	Clone
splunkd-access	index=_internal source=*/splunkd_access.log OR source=*\\splunkd_access.log		No owner	system	Global | Permissions	Enabled	Clone
splunkd-log	index=_internal source=*/splunkd.log OR source=*\\splunkd.log		No owner	system	Global | Permissions	Enabled	Clone

Tag Event Types

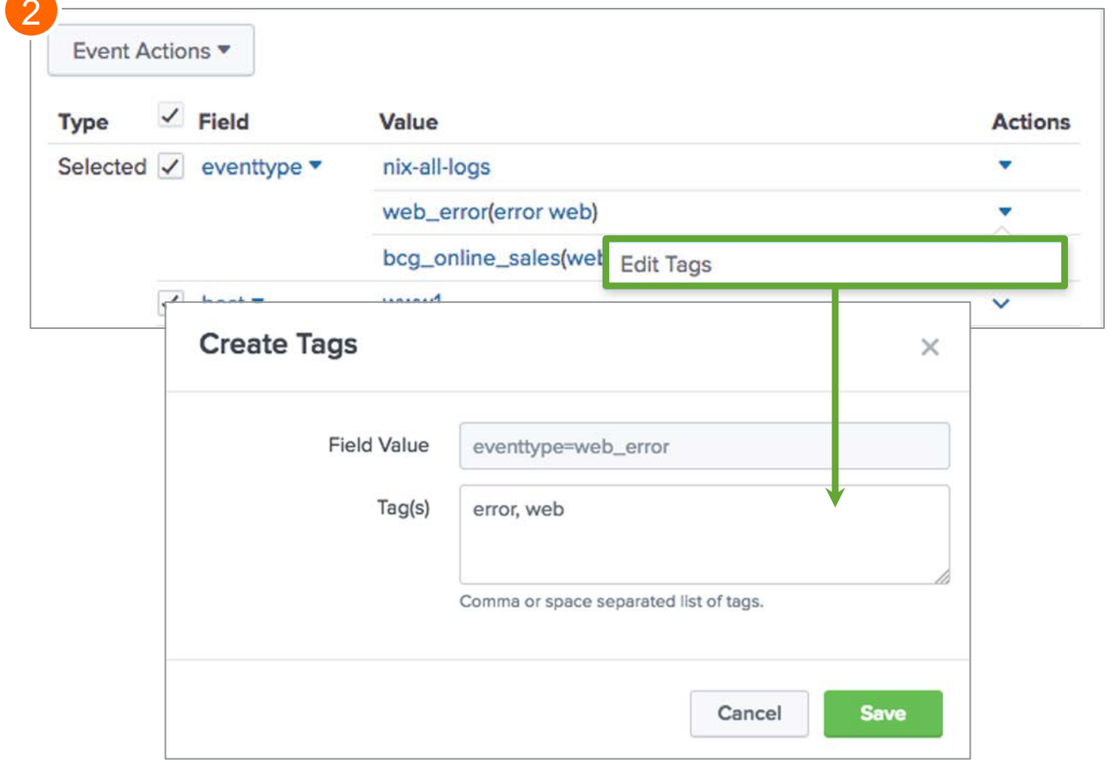
Event types can be tagged in two ways:

1. Settings > Event types
2. Event details > Actions

1



2



Note

Tags are discussed in more detail in a later topic.

Event Types vs. Saved Reports

Event Types

- Categorize events based on a search string
- Used to categorize events into groups
- Inspects incoming events to see if they match a set of criteria
- The eventtype field can be included in a search string
- Does not include a time range

Saved Reports

- Search criteria do not change
- Can be shared with Splunk users and added to dashboards
- Includes a time range and formatting of the results

Create Event Types Lab Exercise

Time: 10 minutes

Tasks:

- Log into Splunk and configure the instance
- Create an event type for status errors

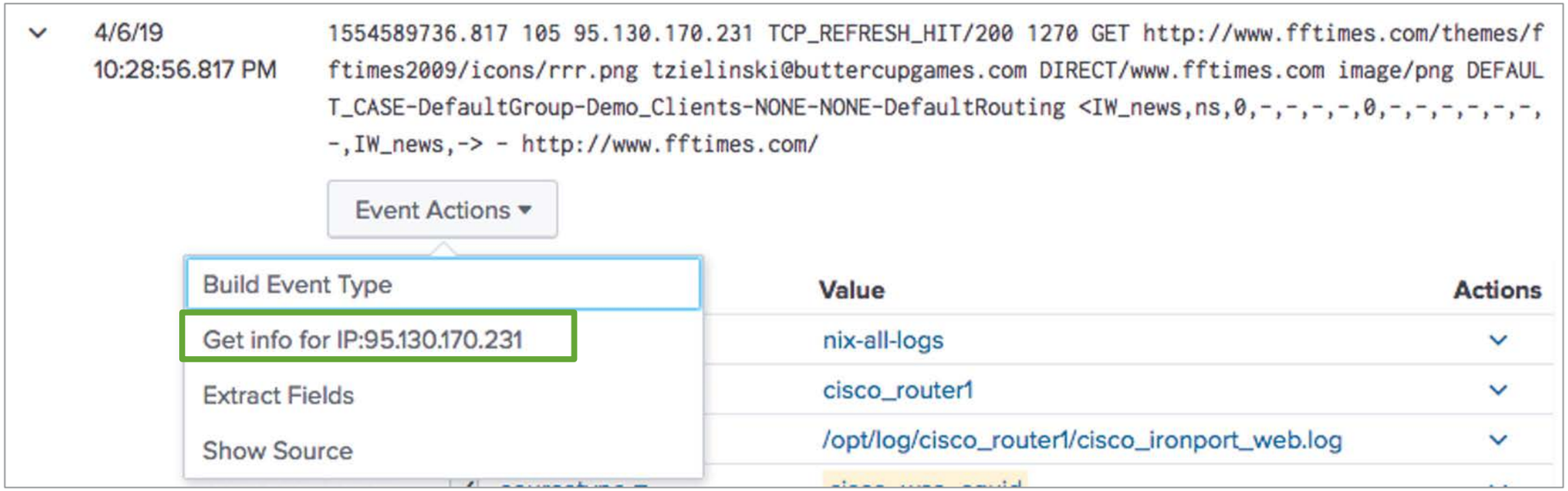
Create Workflow Actions

Topic Objectives

- Identify what are workflow actions
- Create a GET, POST, and search workflow action
- Test workflow actions

What are Workflow Actions?

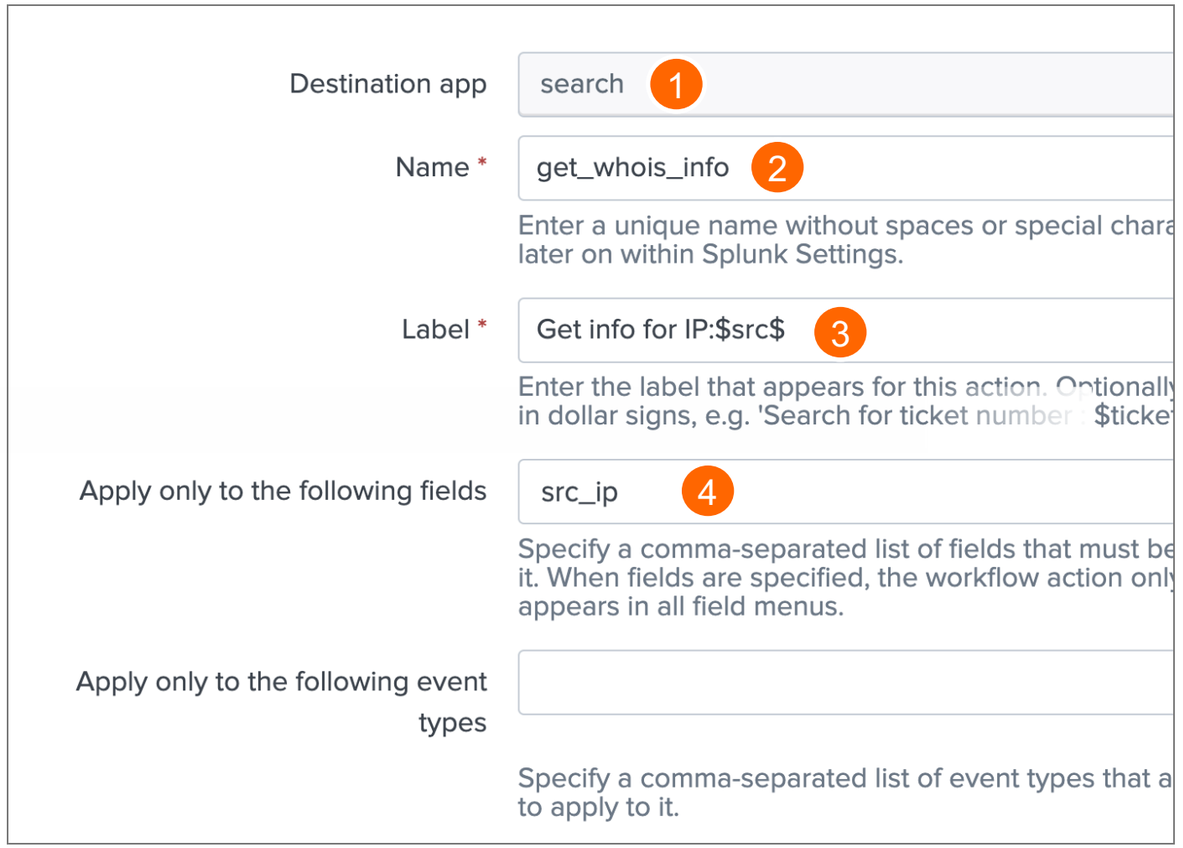
- Workflow actions allow the user to interact with web resources directly from events and fields present in the search results
  - **GET:** retrieve information from an external resource
  - **POST:** send field values to an external resource
  - **Search:** use field values to perform a secondary search



Create a GET Workflow Action

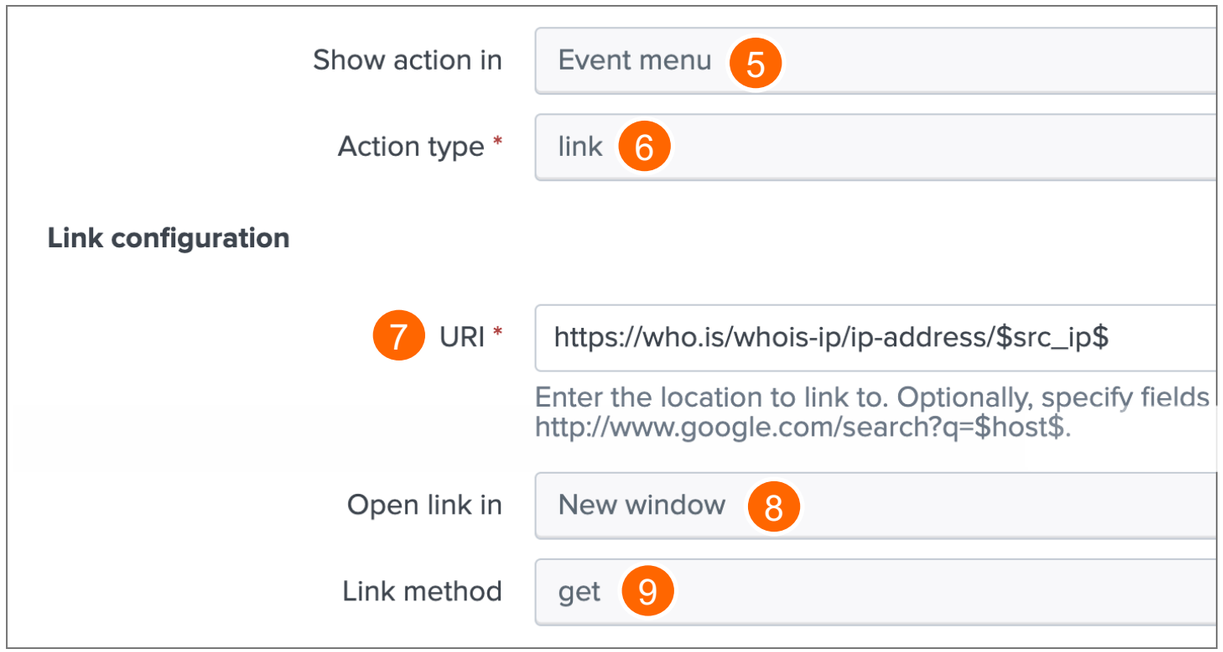
Settings > Fields > Workflow Actions > **New Workflow Action**

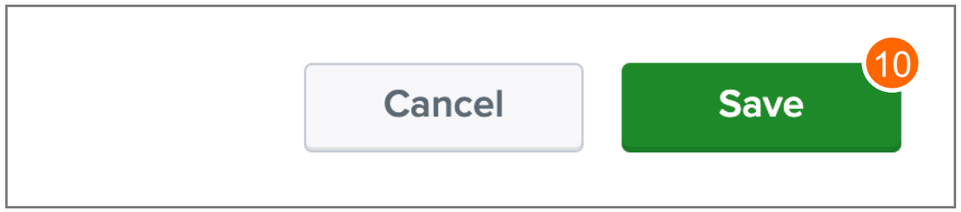
1. Select the **Destination app**
2. **Name** the workflow action (no spaces or special characters)
3. Define the **Label**
4. Determine if your workflow action applies to a field or event type



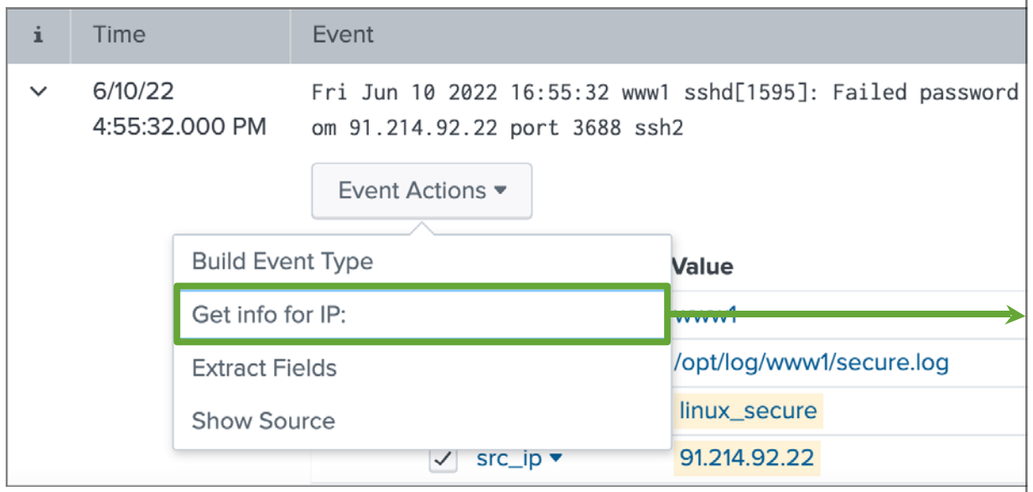
Create a GET Workflow Action (cont.)

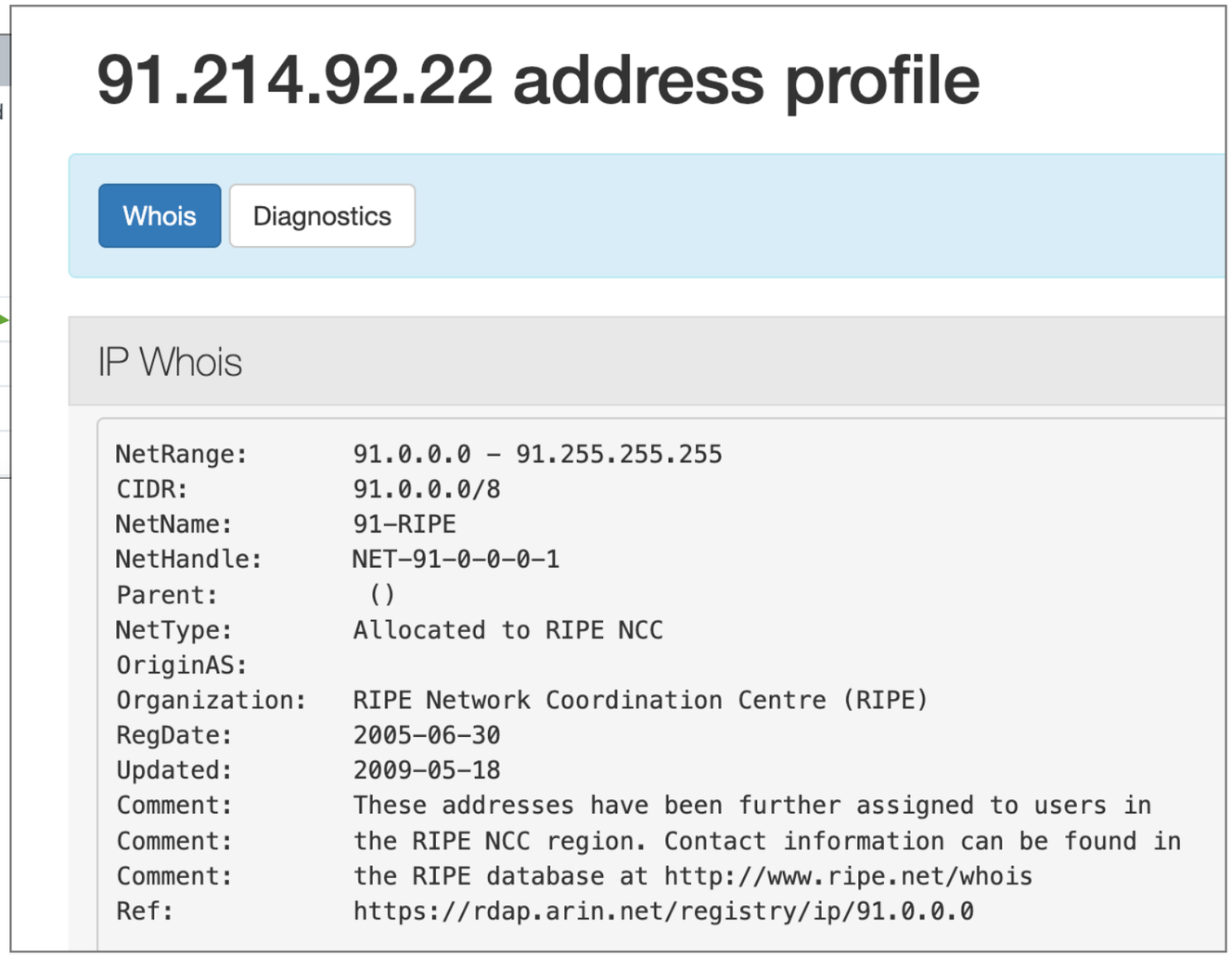
5. From the **Show action in** drop-down list, select **Event menu**, **Fields menu**, or **Both**
6. From **Action type** drop-down list, select **link**
7. Enter the **URI** of where the user will be directed
8. Specify if the link should open in a **New window** or **Current window**
9. Set **Link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





Test the GET Workflow Action

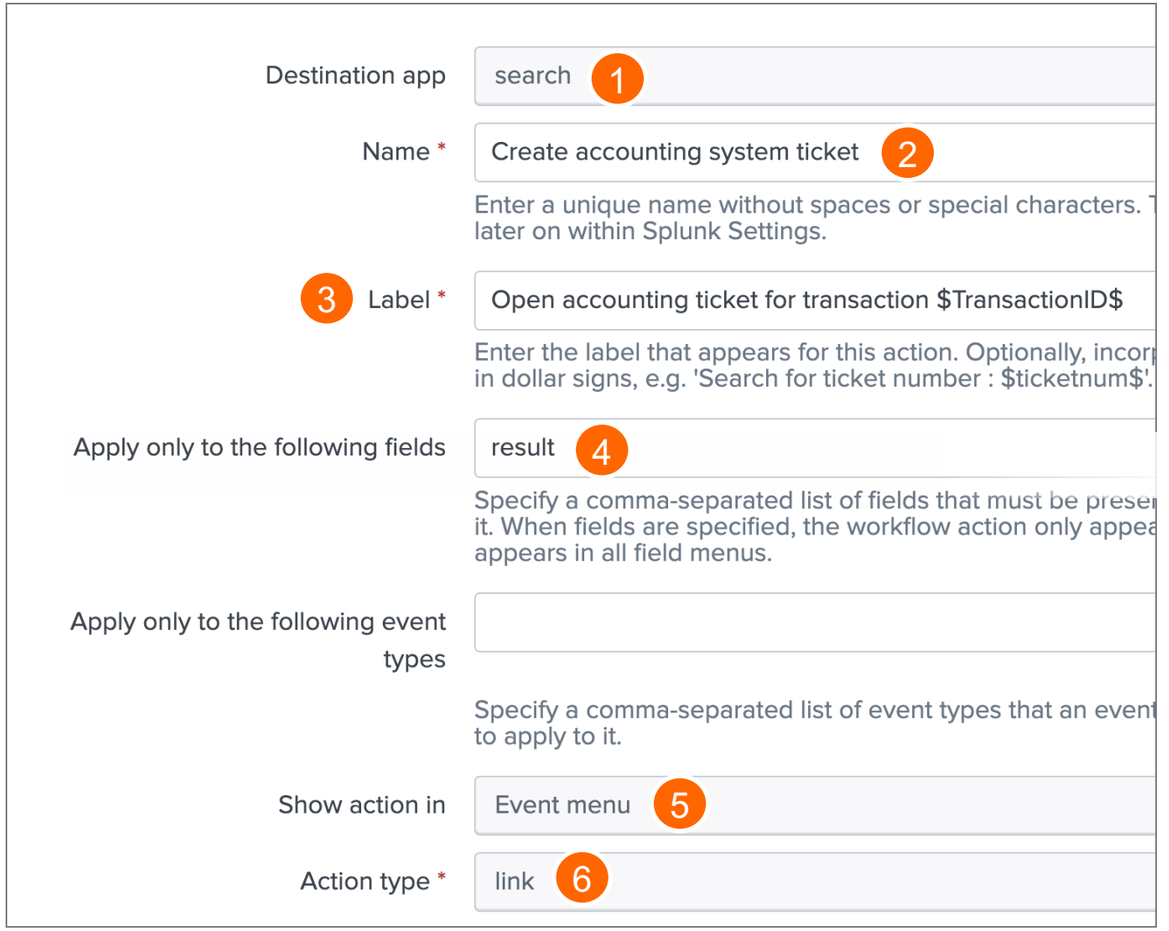




Create a POST Workflow Action

Settings > Fields > Workflow Actions > **New Workflow Action**

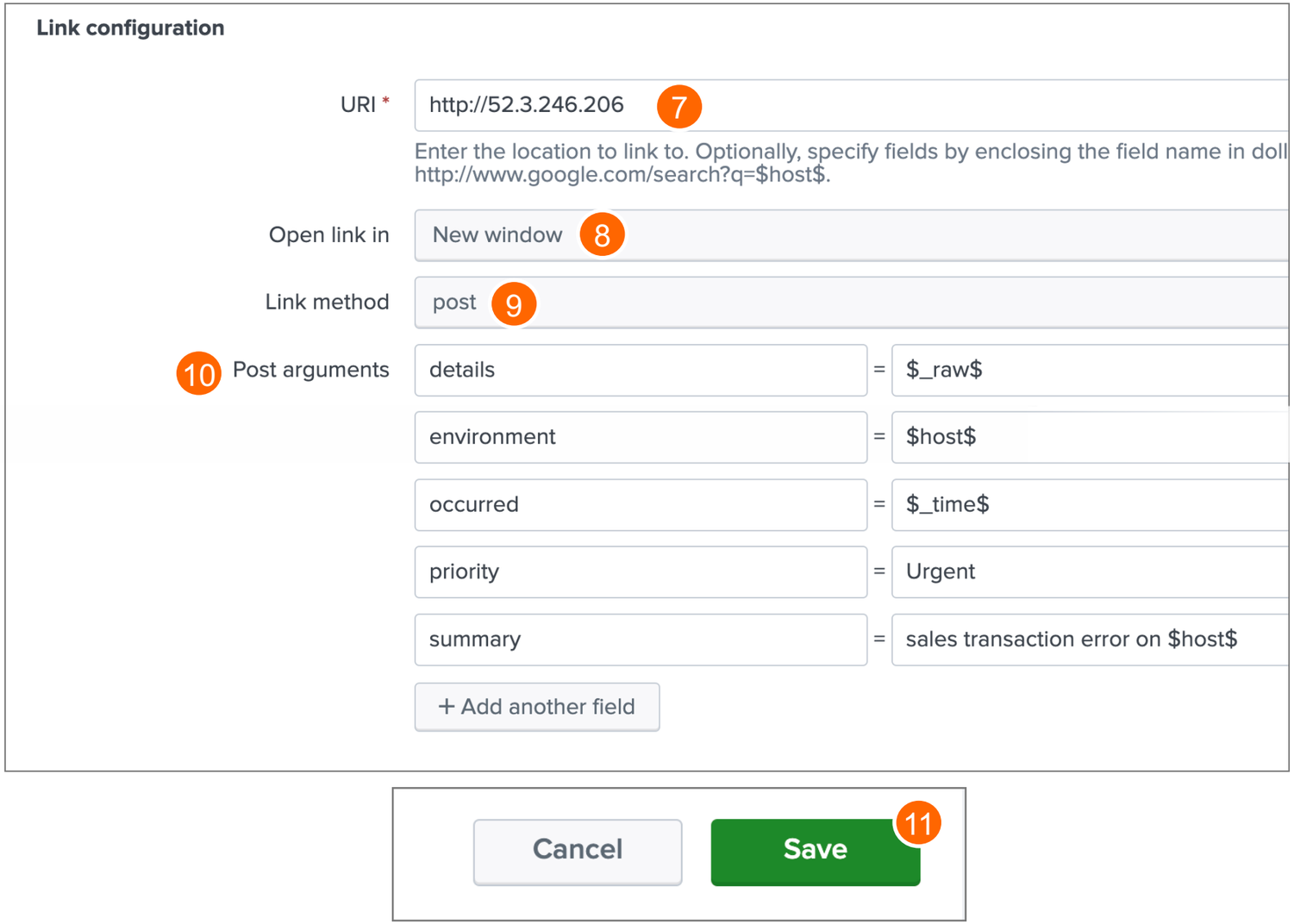
Complete steps 1 – 6 as described in the previous example for creating a GET workflow action



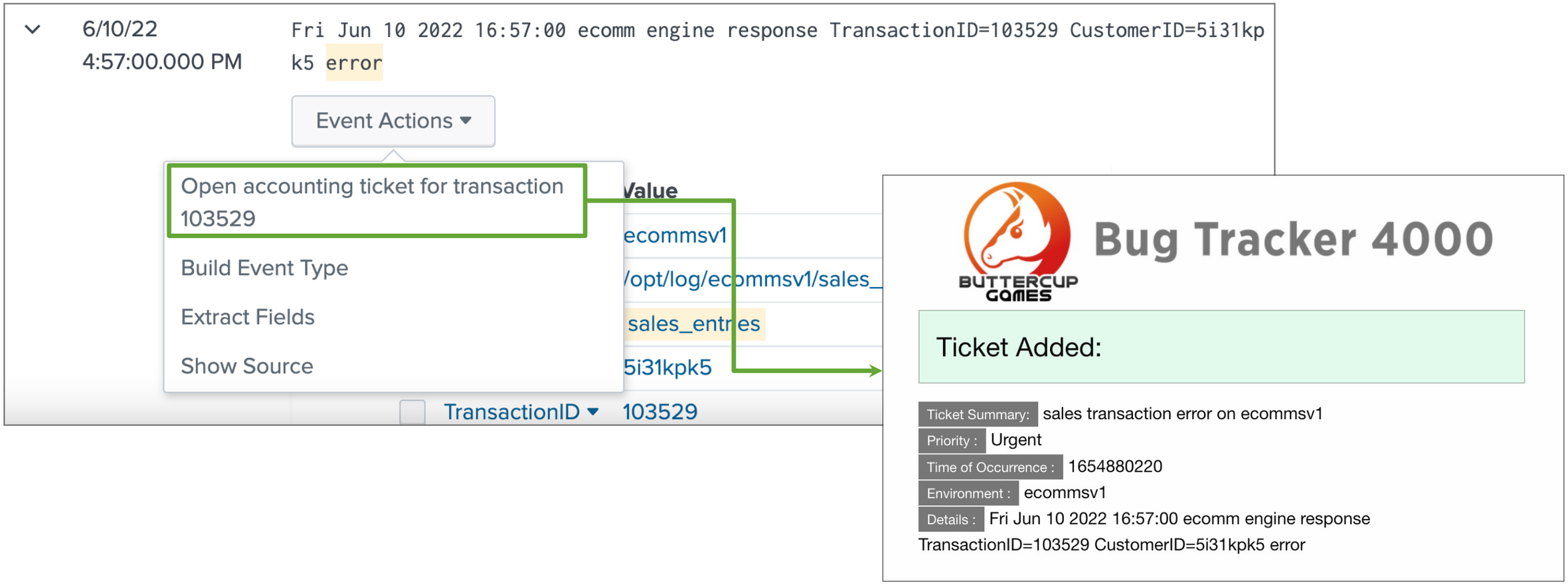
 | 11 August 2022

Create 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**



Test the POST Workflow Action

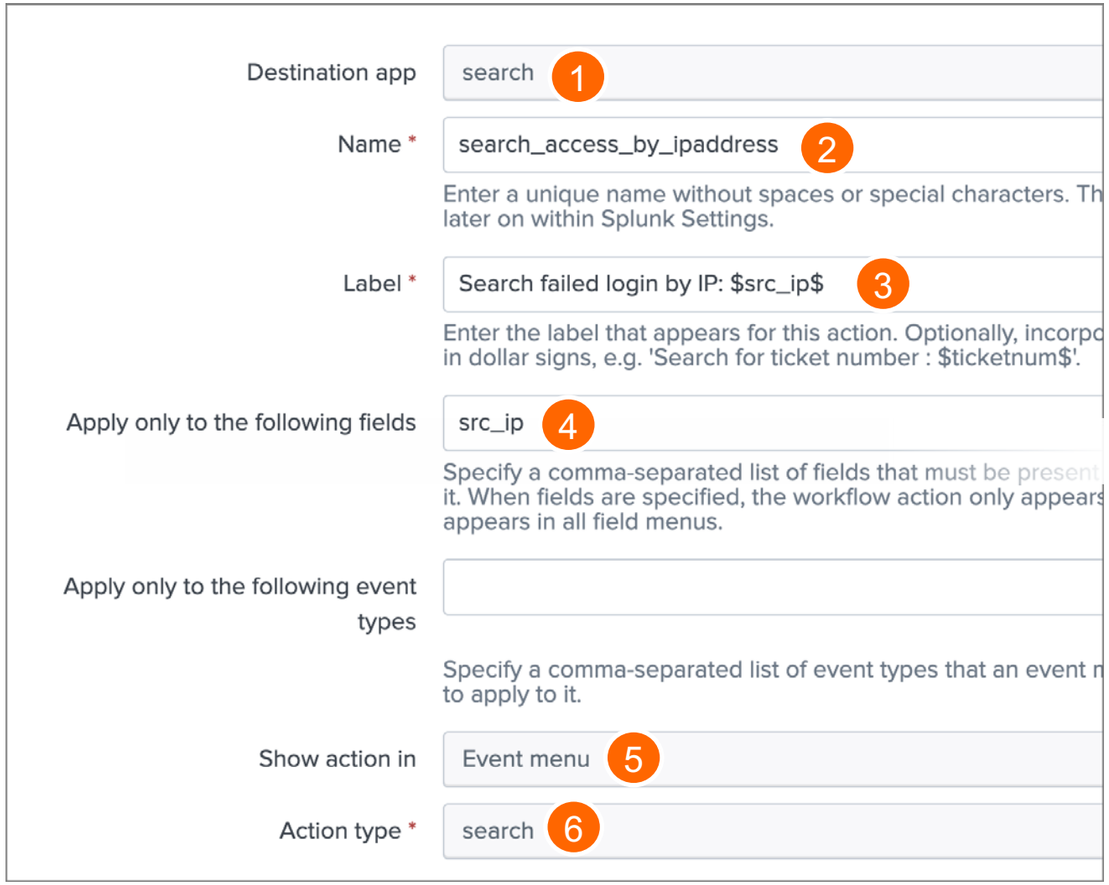


Create a Search Workflow Action

Settings > Fields > Workflow Actions > **New Workflow Action**

Complete steps 1 – 5 as described in the previous example for creating a GET workflow action

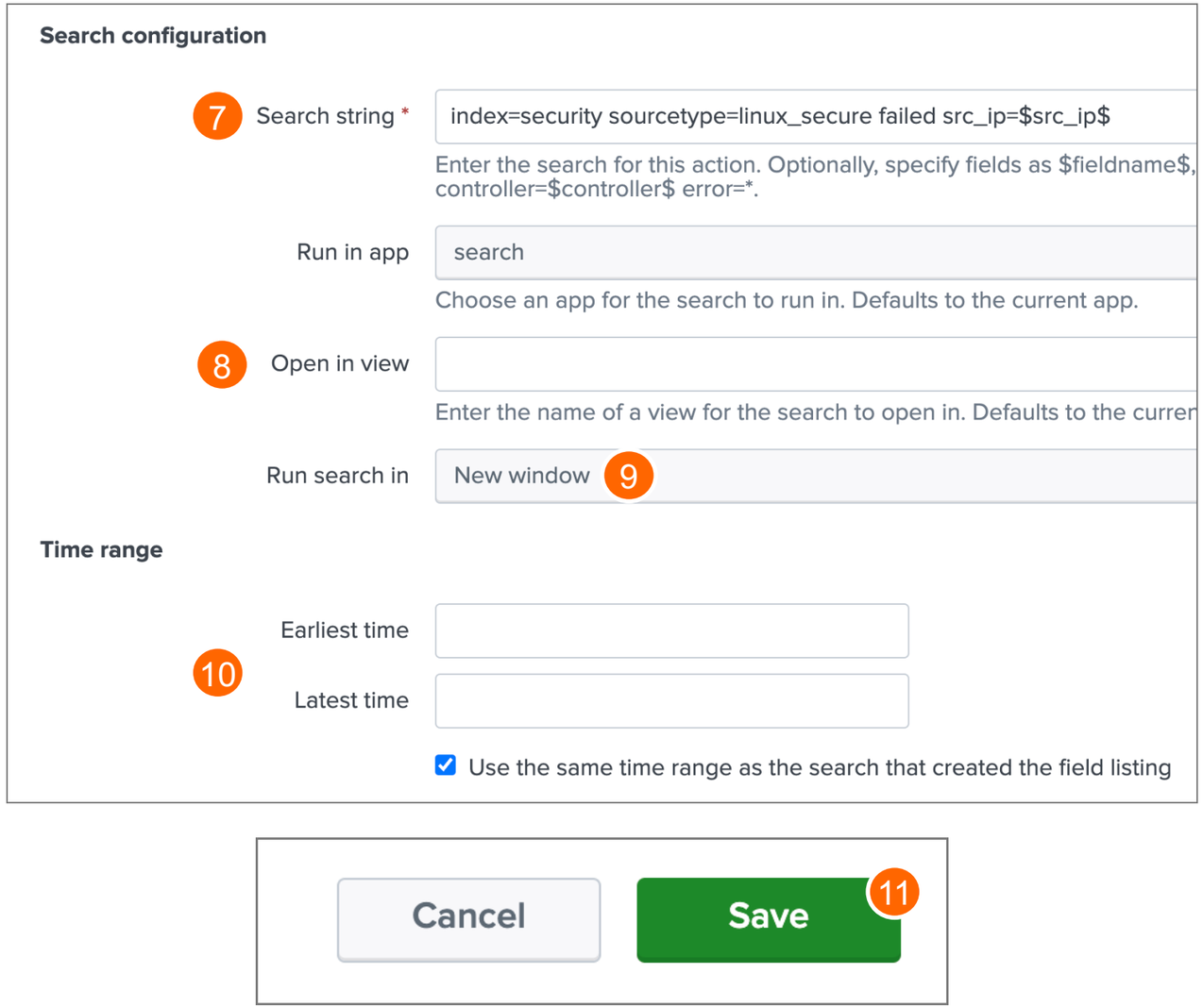
6. From the **Action type** drop-down list, choose **search**



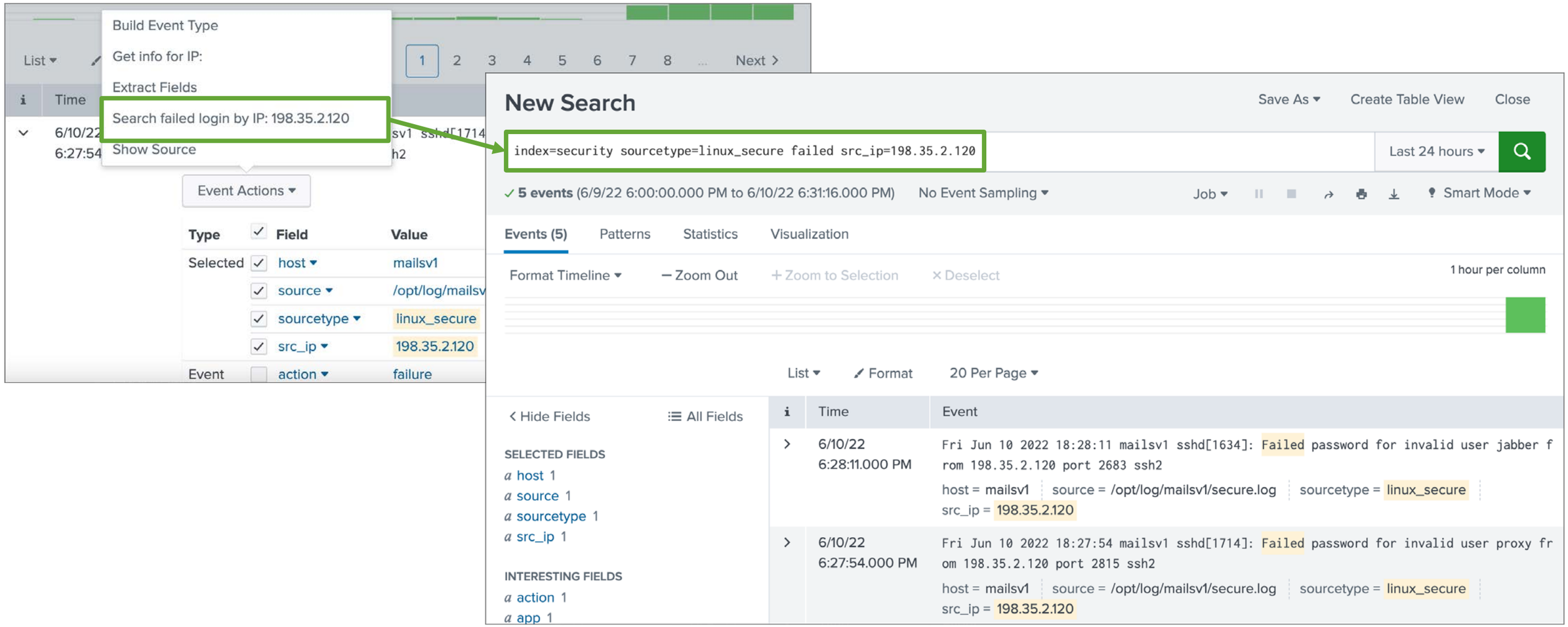
 | 11 August 2022

Create a Search Workflow Action (cont.)

7. Enter the **Search string**
8. Enter the view name where the search will execute
9. Indicate if the search should run in a **New window** or the **Current window**
10. Set time range options
11. Save



Test the Search Workflow Action



Create Workflow Actions Lab Exercise

Time: 15 minutes

Tasks:

- Create a GET workflow to track external login attempts
- Create a POST workflow action that creates an IT ticket in an external system
- Create a Search workflow that performs a search for all failed password events associated with a specific IP address

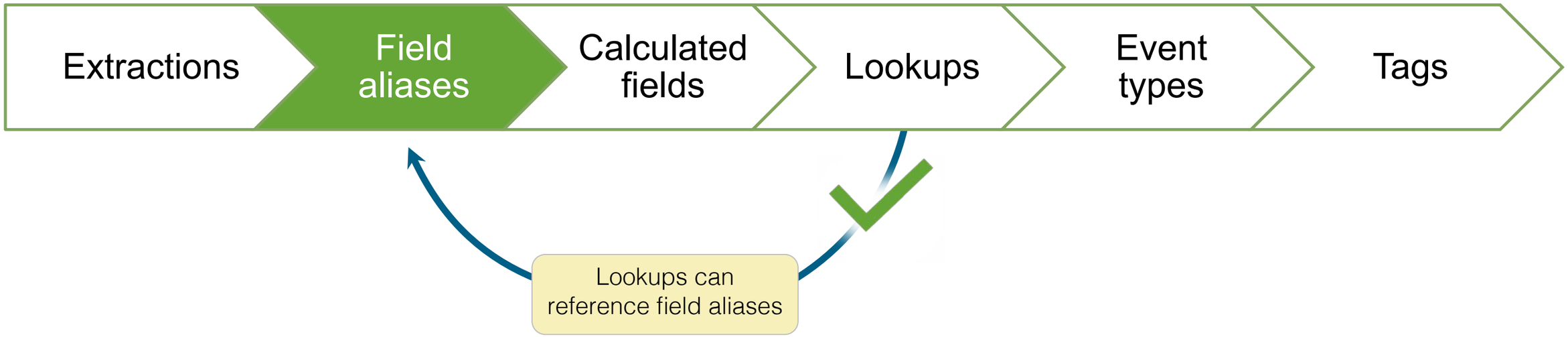
Create Tags and Aliases

Topic Objectives

- Define field aliases
- Create field aliases
- Search with field aliases
- Define tags
- Create and view tags
- Search with tags
- Manage tags

Define Field Aliases

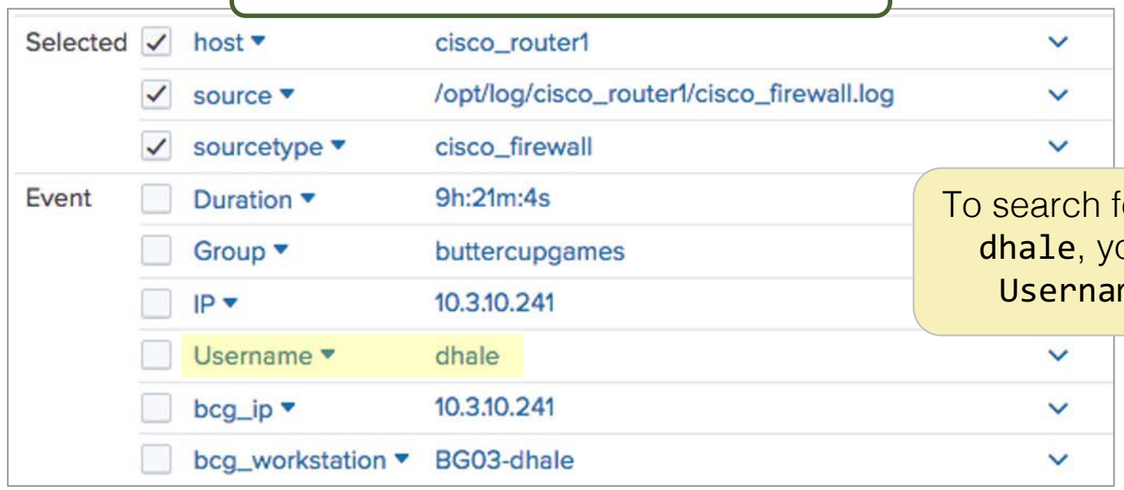
- A way to associate an additional (new) name with an existing field name, like a nickname
- Field aliases can be used to normalize field names
- Can be referenced by knowledge objects that succeed aliases in the search process pipeline



Field Alias Example

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

`sourcetype=cisco_firewall`



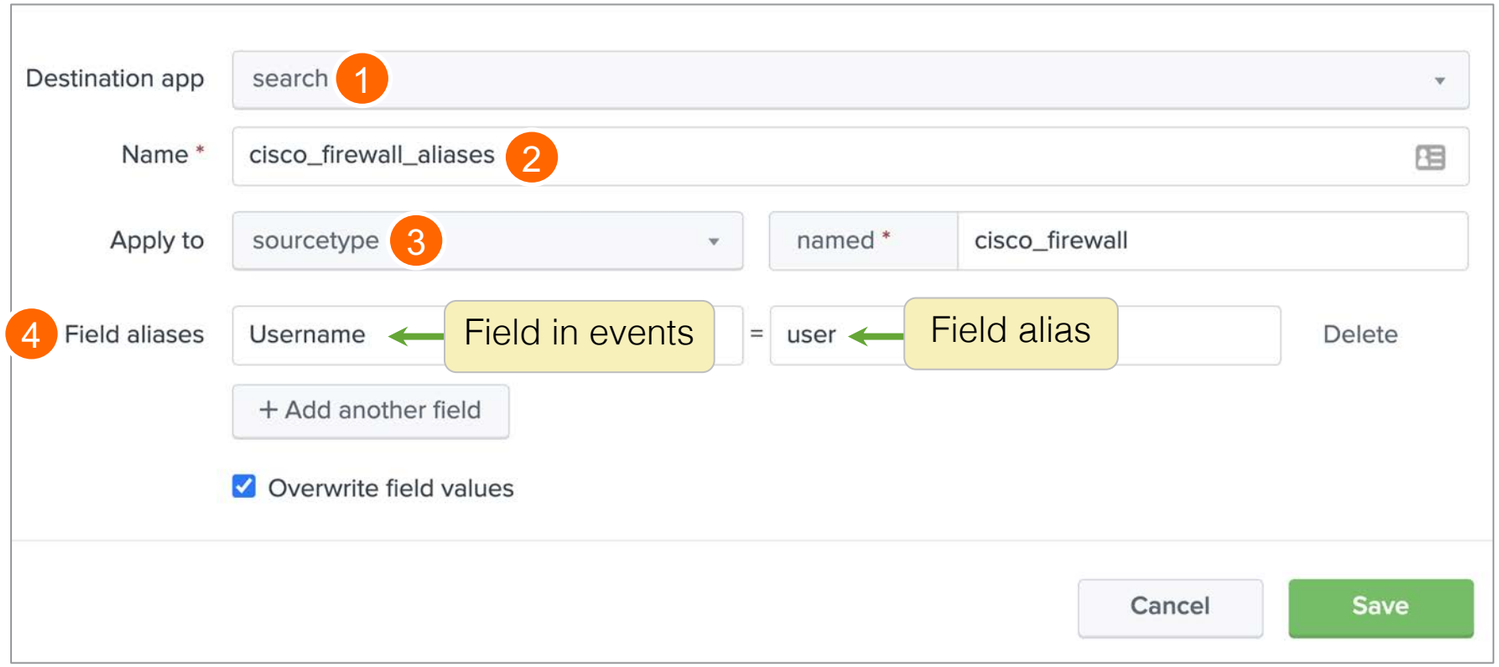
To search for all events involving the user `dhale`, you would have to search for:
`Username=dhale OR User=dhale`

`sourcetype=winauthentication_security`

Create a Field Alias

Settings > Fields > Field aliases > **New Field Alias**

1. Select **Destination app** for field alias
2. Enter a **Name** for the field alias (not for searching)
3. Choose which **host**, **source**, or **sourcetype** the field alias will be applied to
4. Enter existing field name and its new alias

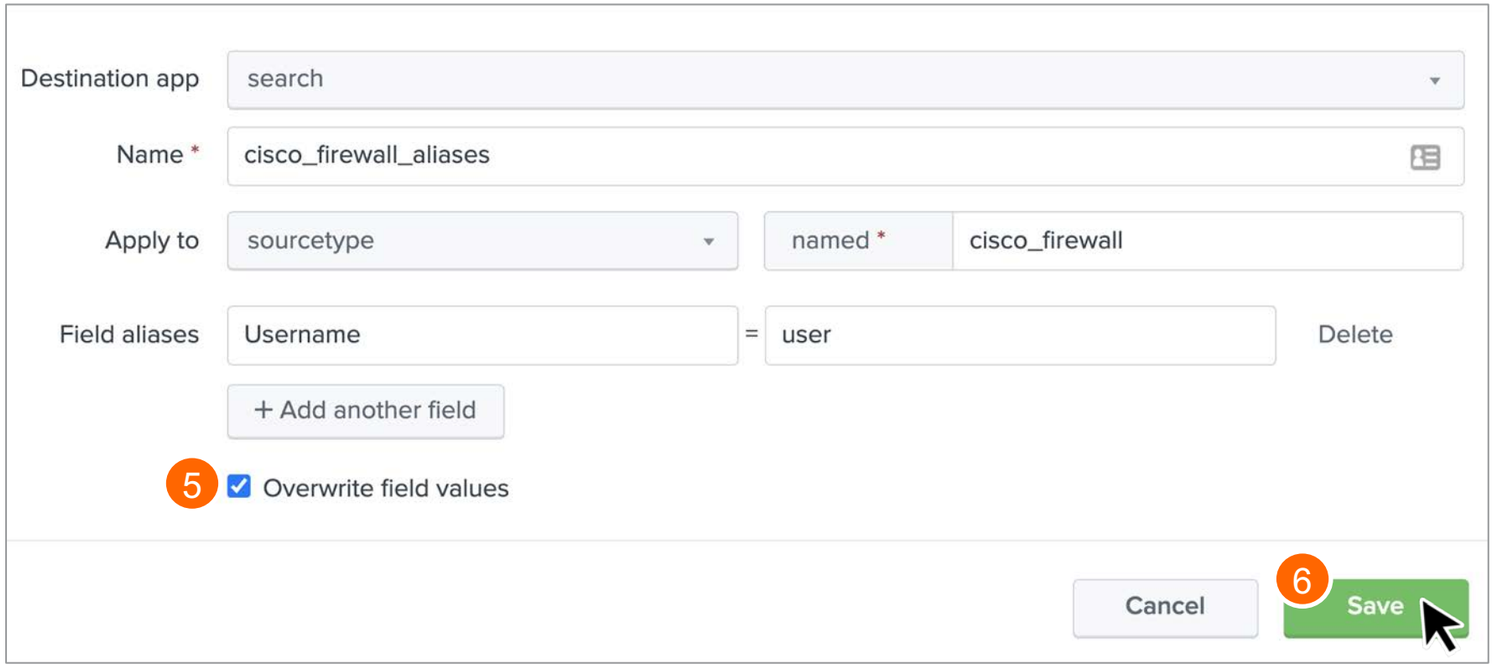


Create a Field Alias (cont.)

Settings > Fields > Field aliases > **New Field Alias**

5 **Overwrite field values** affects the behavior of a field alias

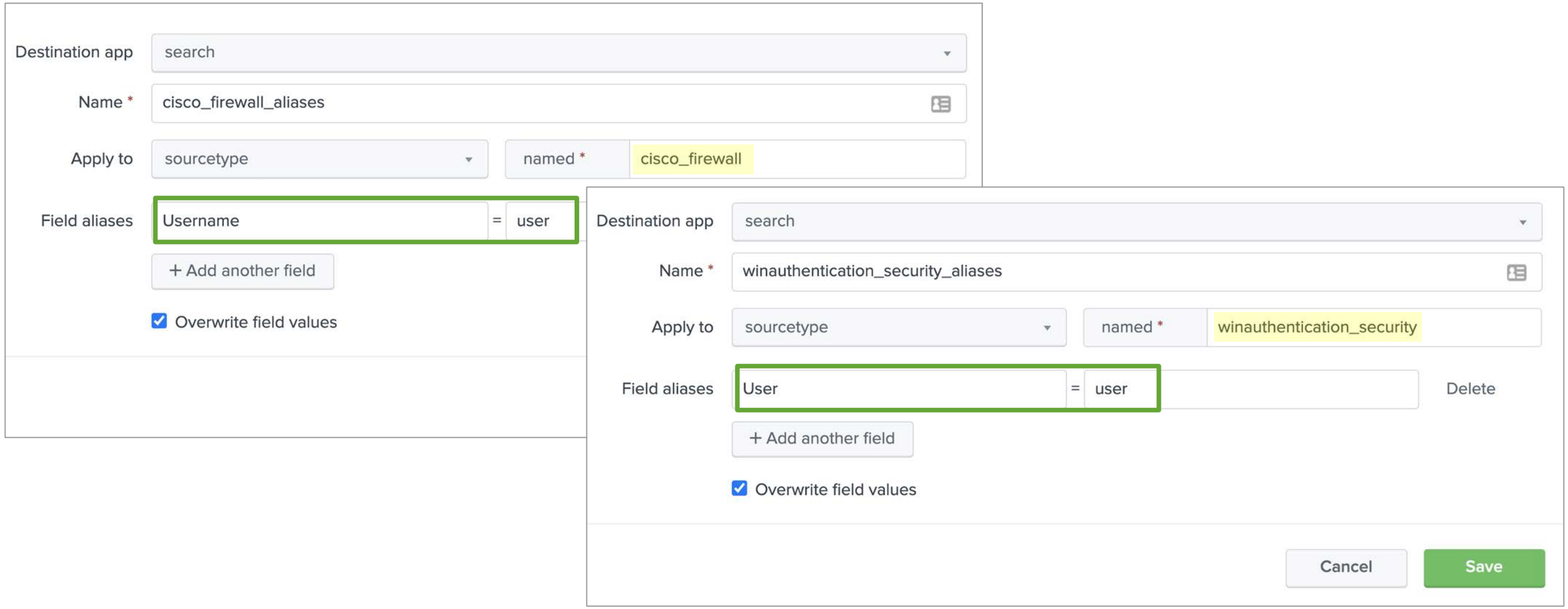
- If checked:
  - If user already exists, Splunk replaces user values with Username values
  - If Username doesn't exist or has no value, Splunk removes user from results
- If unchecked, no fields values are



6 Save

Create a Field Alias (cont.)

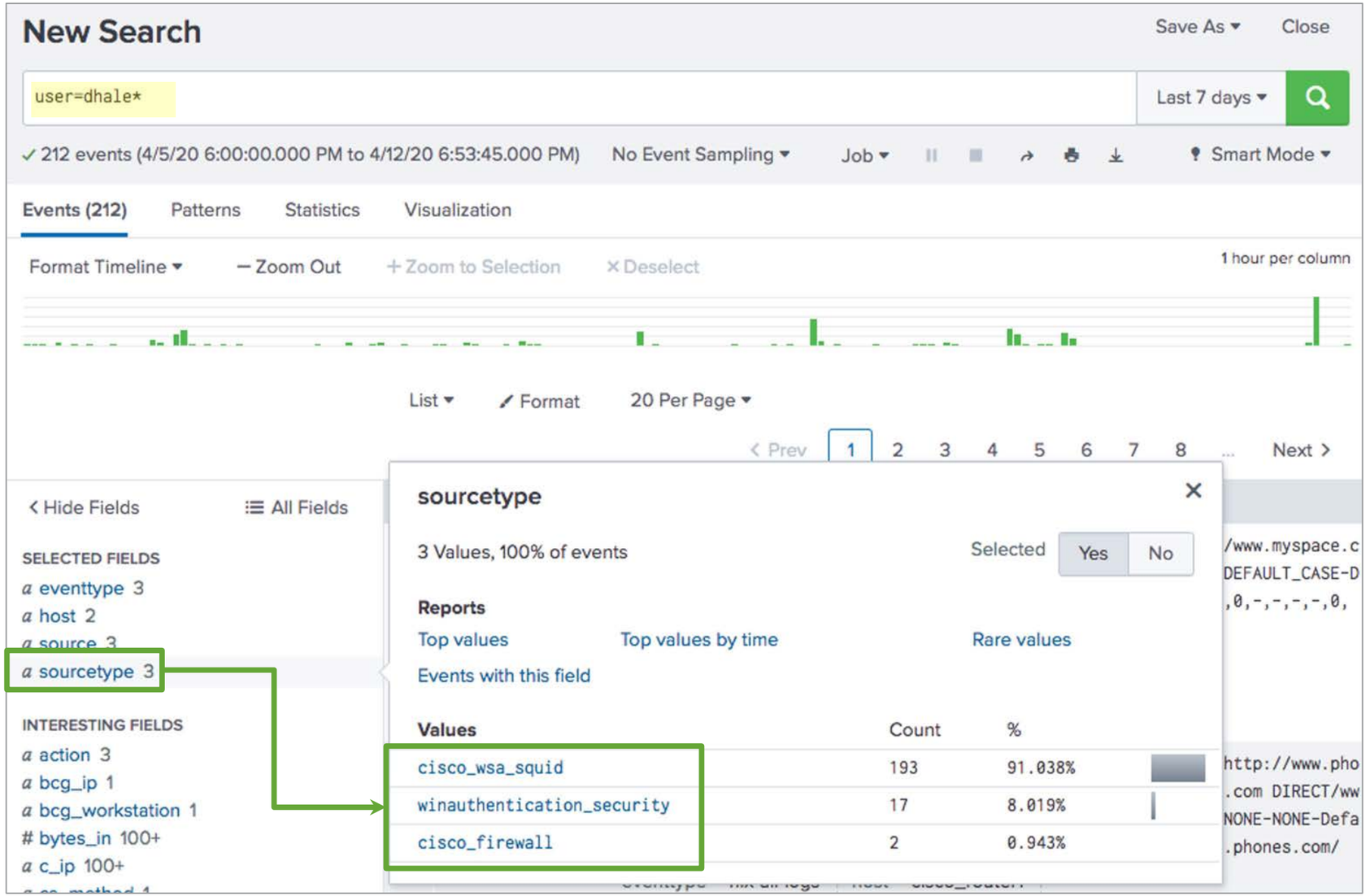
New field alias required for each sourcetype



 | 11 August 2022

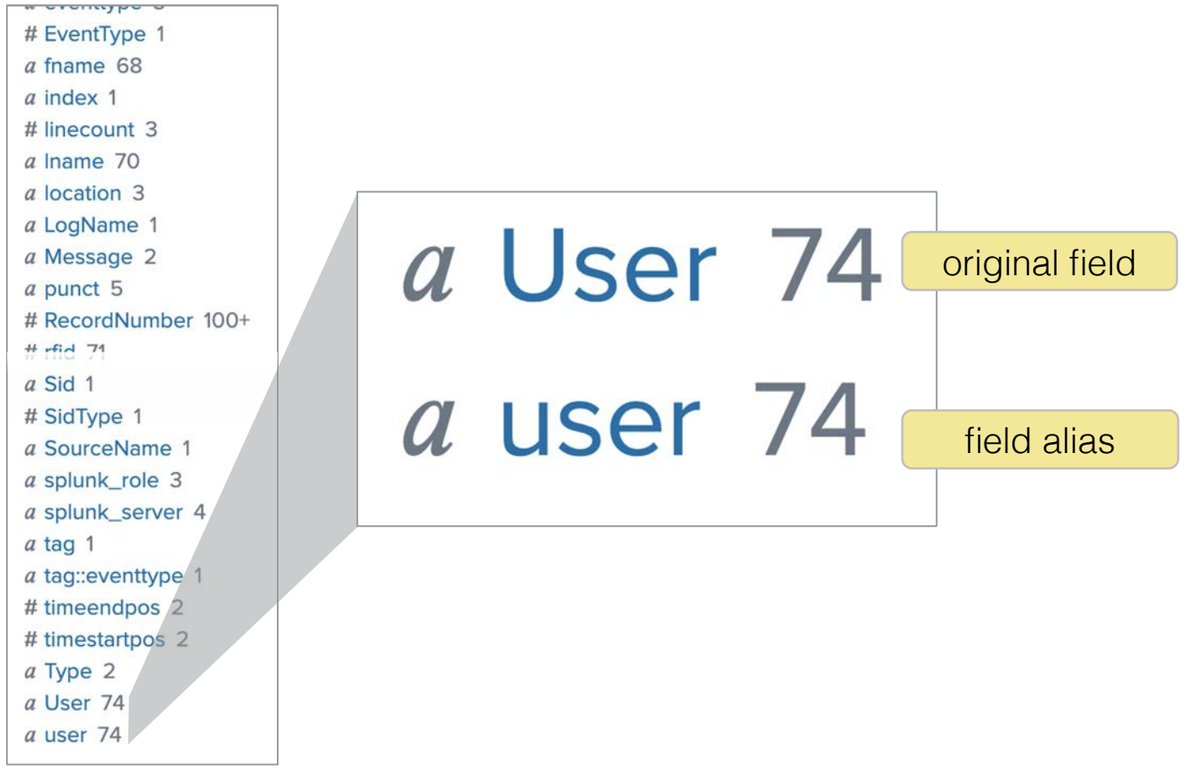
Search with Field Alias: Testing

After the field alias is created, perform a search using the new field alias



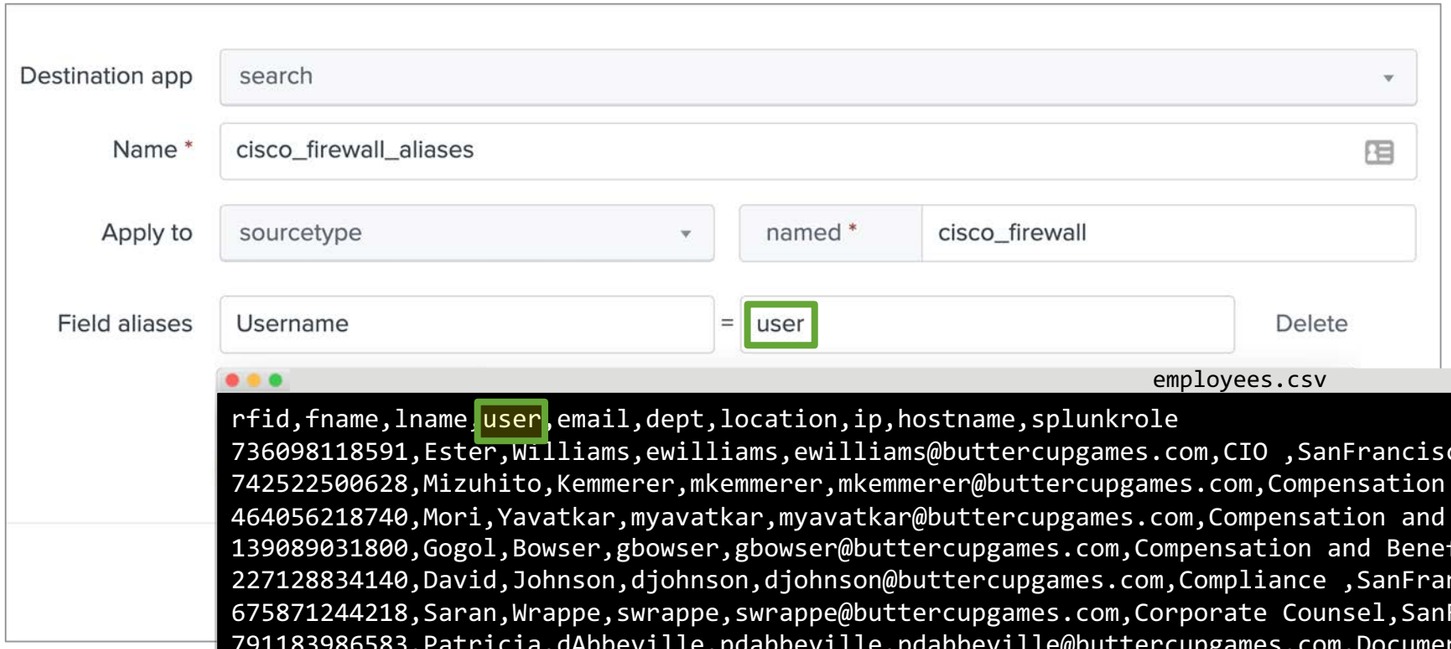
Search with Field Aliases: Original Fields

- When you create a field alias, the original field is not affected
- Both fields appear in the **All Fields** and **Interesting Fields** lists, if they appear in at least 20% of events



Search with Field Aliases: Lookups

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

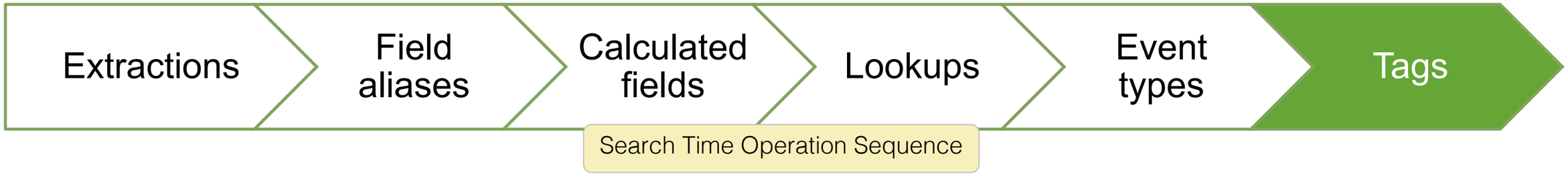


employees.csv

```
rfid,fname,lname,user,email,dept,location,ip,hostname,splunkrole
736098118591,Ester,Williams,ewilliams,ewilliams@buttercupgames.com,CIO ,SanFrancisco,10.1.10.133,BG01-ewilliams,power
742522500628,Mizuhito,Kemmerer,mkemmerer,mkemmerer@buttercupgames.com,Compensation and Benefits,Boston,10.2.10.3,BG02-mkemmerer,user
464056218740,Mori,Yavatkar,myavatkar,myavatkar@buttercupgames.com,Compensation and Benefits,SanFrancisco,10.1.10.140,BG01-myavatkar,user
139089031800,Gogol,Bowser,gbowser,gbowser@buttercupgames.com,Compensation and Benefits,London,10.3.10.22,BG03-gbowser,user
227128834140,David,Johnson,djohnson,djohnson@buttercupgames.com,Compliance ,SanFrancisco,10.3.10.180,BG02-djohnson,power
675871244218,Saran,Wrappe,swrappe,swrappe@buttercupgames.com,Corporate Counsel,SanFrancisco,10.1.10.188,BG01-swrappe,user
791183986583,Patricia,dAbbeville,pdabbeville,pdabbeville@buttercupgames.com,Documentation,SanFrancisco,10.1.10.52,BG01-pdabbeville,user
632071692298,Yanto,Owen,yowen,grao@buttercupgames.com,Documentation,London,10.2.10.170,BG03-yowen,user
559129672655,Enrique,Dutra,edutra,edutra@buttercupgames.com,Engineering,Boston,10.2.10.77,BG02-edutra,power
382839148784,Meng,Yuan,myuan,myuan@buttercupgames.com,Engineering,SanFrancisco,10.1.10.238,BG01-myuan,power
356025036673,Guoxiang,Nooteboom,gnooteboom,gnooteboom@buttercupgames.com,Engineering,SanFrancisco,10.1.10.12,BG01-gnooteboom,power
569361105570,Kathleen,Percy,kpercy,kpercy@buttercupgames.com,Engineering,SanFrancisco,10.1.10.216,BG01-kpercy,power
```

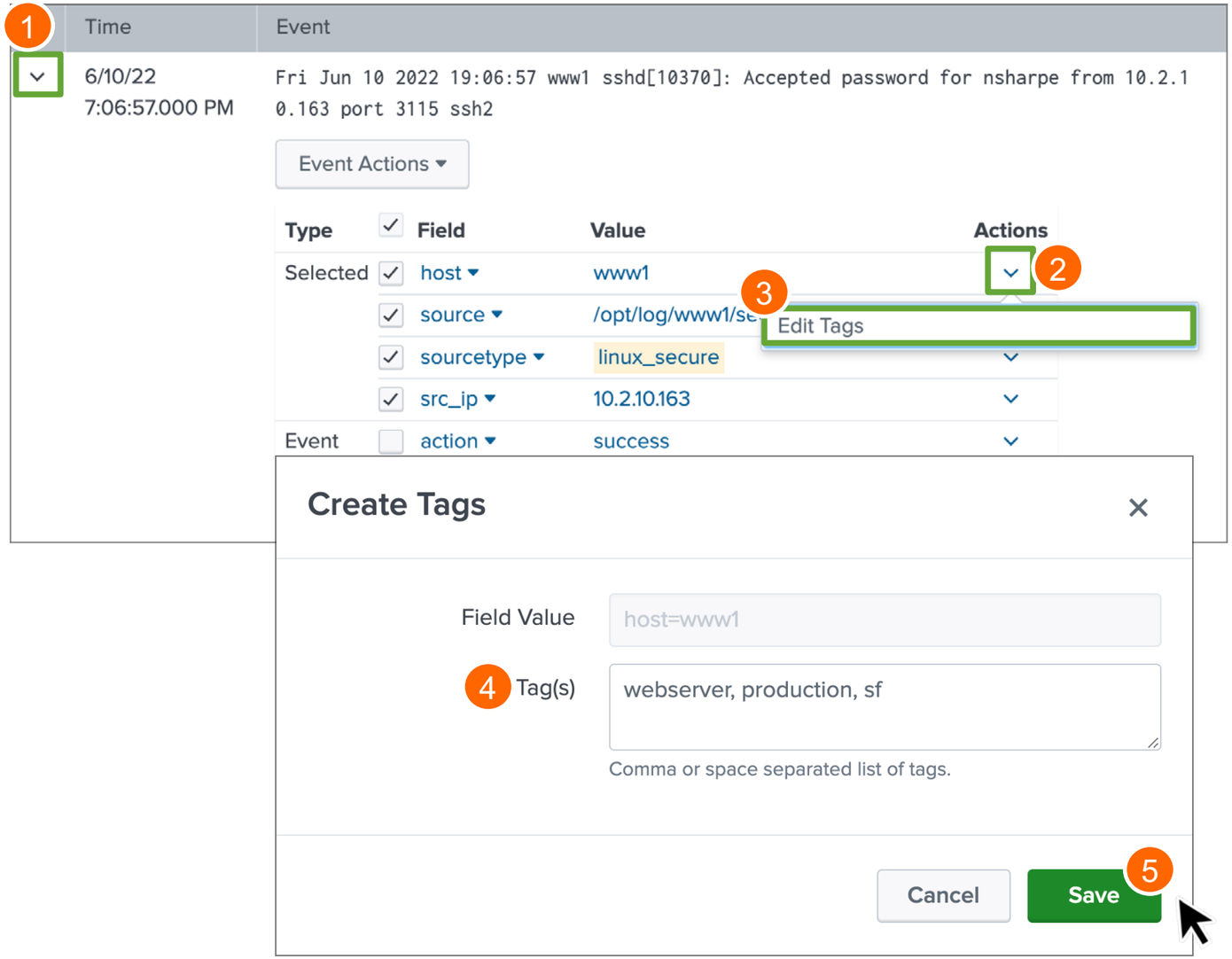

Define Tags

- A knowledge object that enables you to search for events that contain specific field/value combinations
- Tags are labels that you create for field/value pairs
- Tags make your data more understandable and less ambiguous
- Any field/value combination can be referenced by more than one tag and any tag can be applied to more than one field/value pair
- Tags are case sensitive



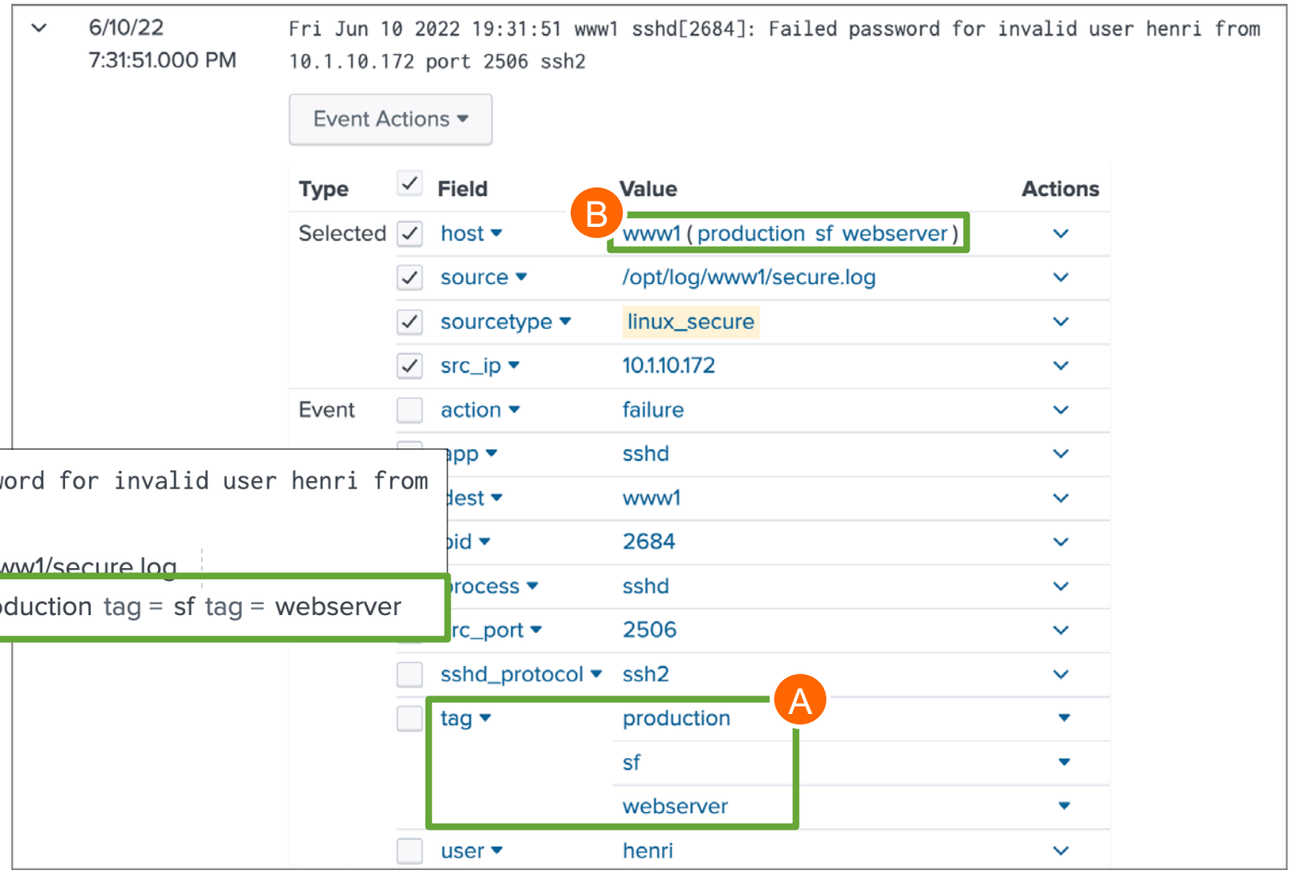
Create Tags

1. Click the info arrow for event details
2. Under **Actions**, click the down arrow (fields menu)
3. Select **Edit Tags**
4. Enter the **Tag** labels associated with this key/value pair separated by commas
5. Save



View Tags

- When tagged field/value pairs are selected, the tags appear
  - A In the results as tags
  - B In parentheses next to the associated field/value pair



Search for Tags

A tag associated with a value:

```
tag=<tagname>
```

```
tag=webserver
```

A tag using a partial field value:

```
tag=<partial-tagname>*
```

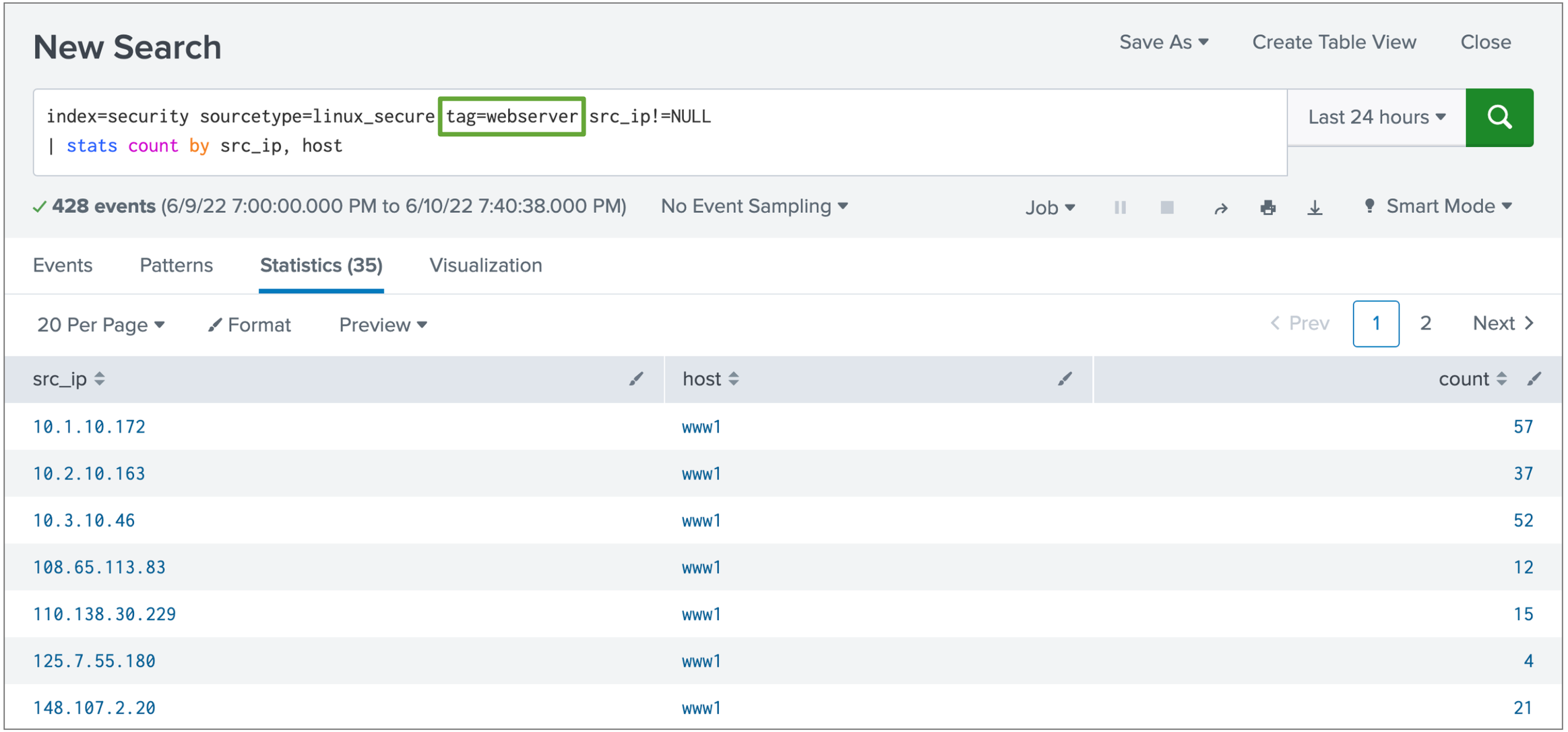
```
tag=w*
```

A tag associated with a value on a specific field:

```
tag::<field>=<tagname>
```

```
tag::host=webserver
```


Use Tags in a Search

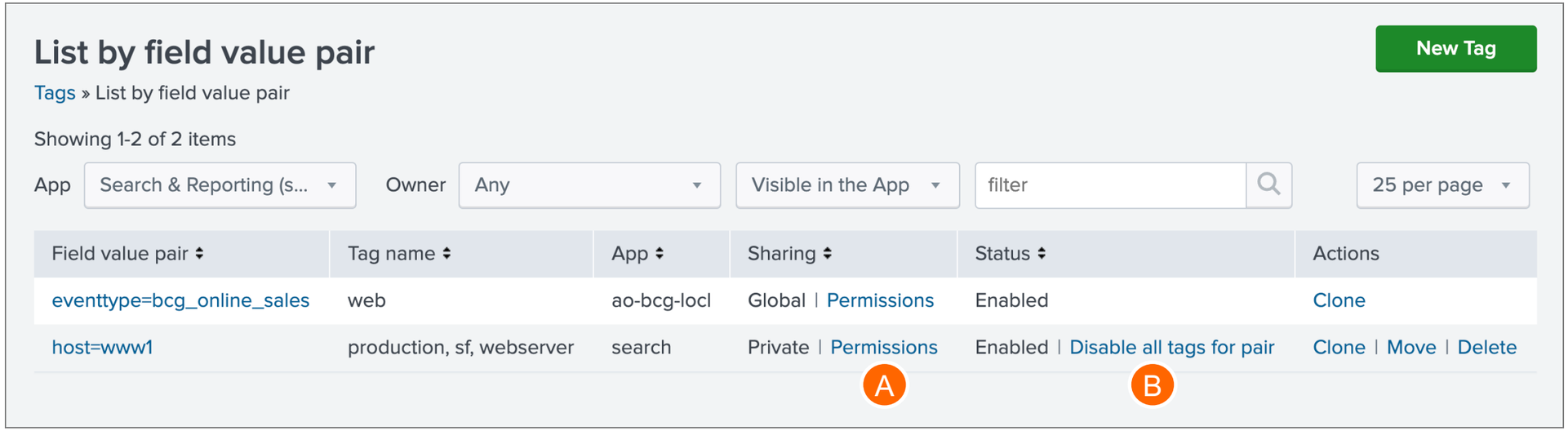


src_ip	host	count
10.1.10.172	www1	57
10.2.10.163	www1	37
10.3.10.46	www1	52
108.65.113.83	www1	12
110.138.30.229	www1	15
125.7.55.180	www1	4
148.107.2.20	www1	21

Manage Tags: Permissions / Status

Settings > Tags > List by field value pair

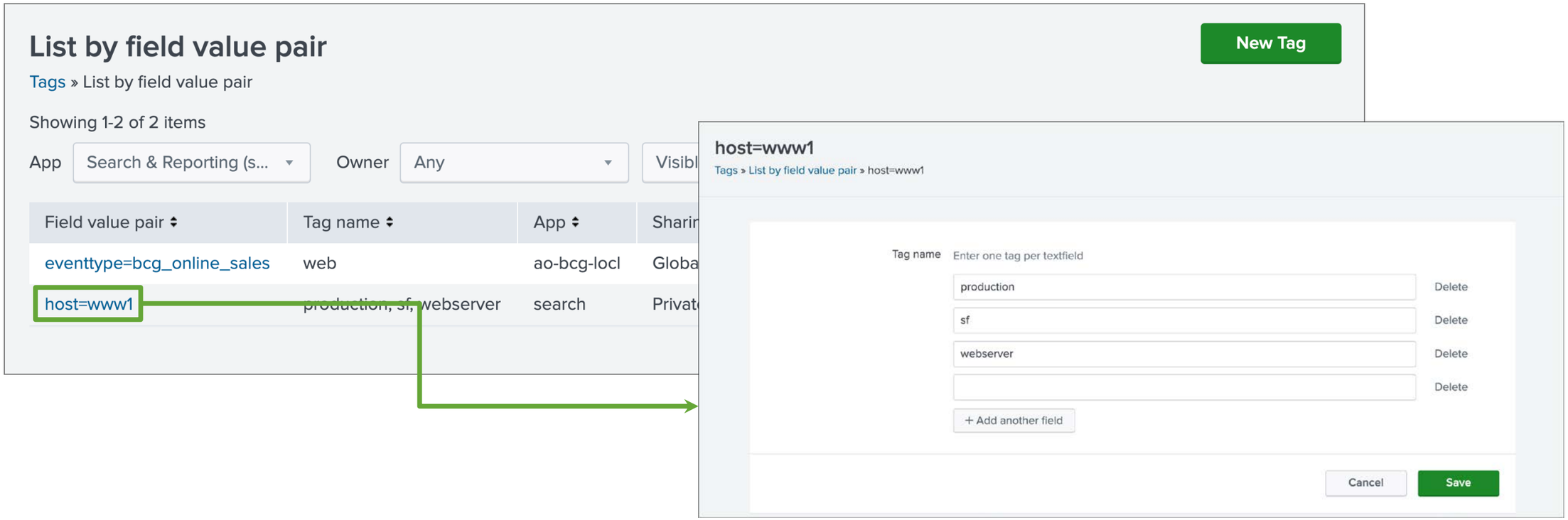
- A Edit permissions
- B Disable all tags for the pair: disables the tag in searches and prevents it from being listed under List by Tag Name and All unique tag objects



Manage Tags: Tag Name

Settings > Tags > List by field value pair

Click Field value pair to add additional tags or change the name of the tag



Create Tags and Aliases Lab Exercises

Time: 15 minutes

Tasks:

- Create a field alias for the `cs_username` and `users` fields
- Create a field alias for the `http_action` and `http_method` fields
- Create tags to identify all admin accounts

Create Search Macros

Topic Objectives

- Define macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Use nested macros
- Use macros with other knowledge objects
- Use tags/event types with macros
- Create macros considerations

Define Macros

- Useful for frequently run searches with similar syntax
- Time range selected at search time
- Can be a full search string or a portion of a search that can be reused in multiple places
- Allows you to define arguments within a search segment and pass parameters at execution time

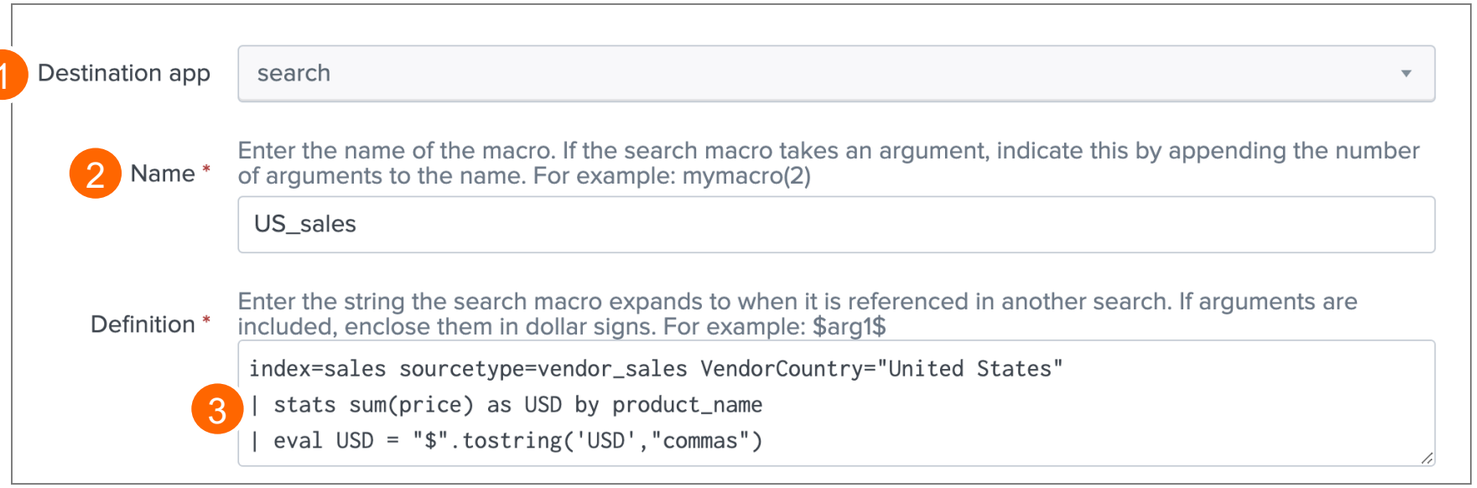

```
index=sales sourcetype=vendor_sales
VendorCountry="United States"
| stats sum(price) as USD by product_name
| eval USD = "$".tostring(USD, "commas")
```

product_name	USD
Benign Space Debris	$49.98
Curling 2014	$99.95
Dream Crusher	$479.88
Final Sequel	$49.98
Fire Resistance Suit of Provolone	$39.90
Holy Blade of Gouda	$71.88
Manganiello Bros.	$319.92
Manganiello Bros. Tee	$79.92
Mediocre Kingdoms	$149.94

Create a Macro: Without Arguments

Settings > Advanced Search > Search macros> Add new

1. Choose destination app
2. Create the macro name that will be used in search
3. Test the macro definition, i.e., search string, before creating macro
4. Save



Macros are called to the search line by wrapping the macro name in back ticks

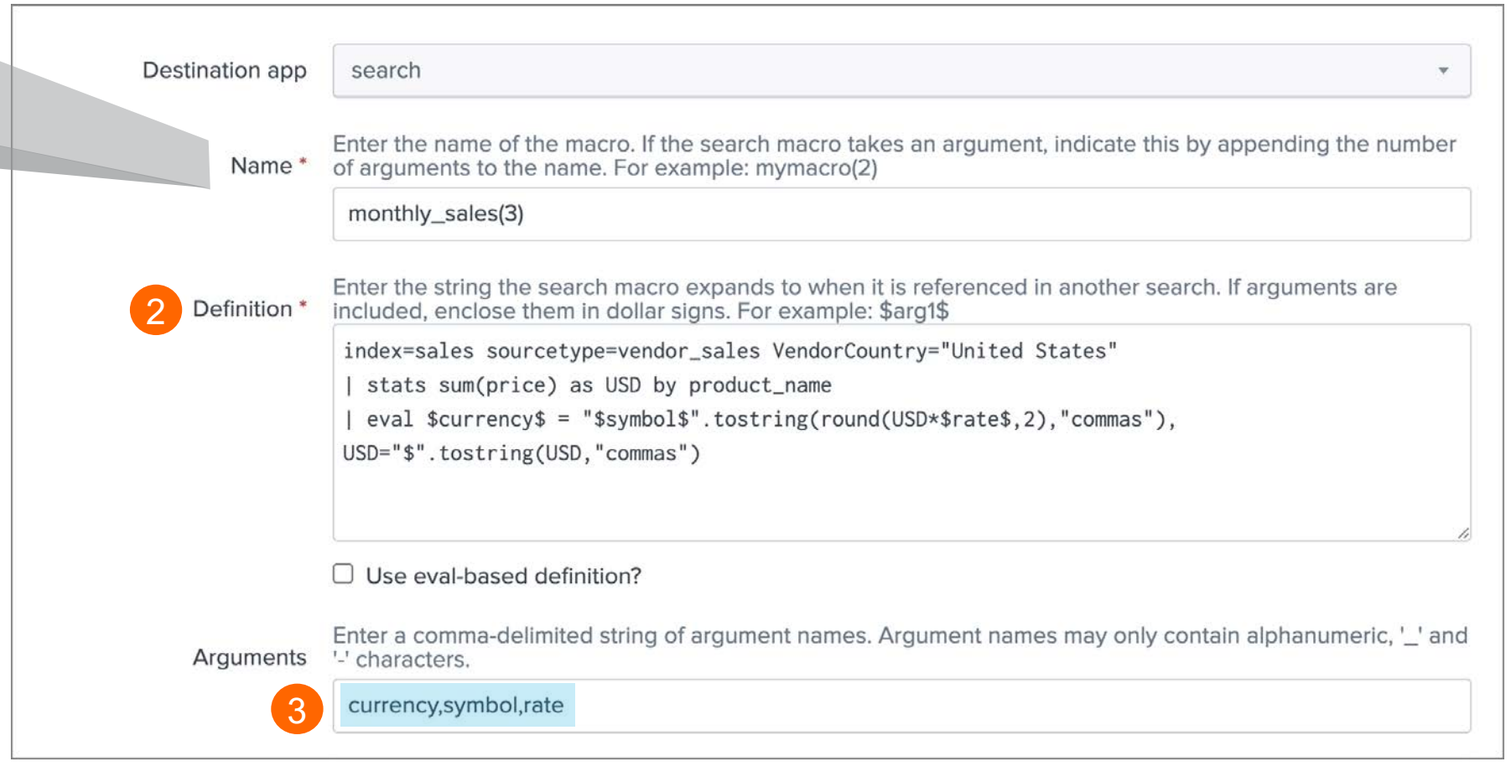
Mac Windows

Create a Macro: With Arguments

Settings > Advanced Search > Search macros> Add new

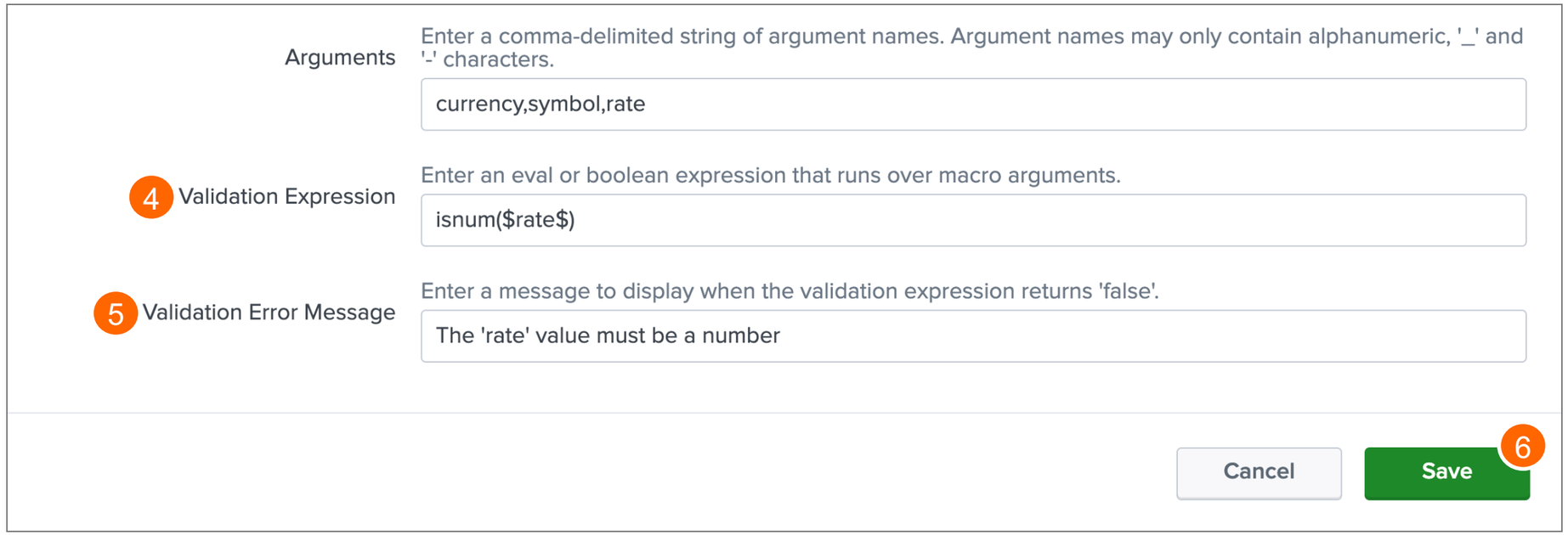
1. monthly_sales(3)

1. Add arguments by including the number of arguments, in parenthesis, after the macro name
2. Specify argument names and surround with $ in the macro Definition
3. List arguments in order, separated with commas

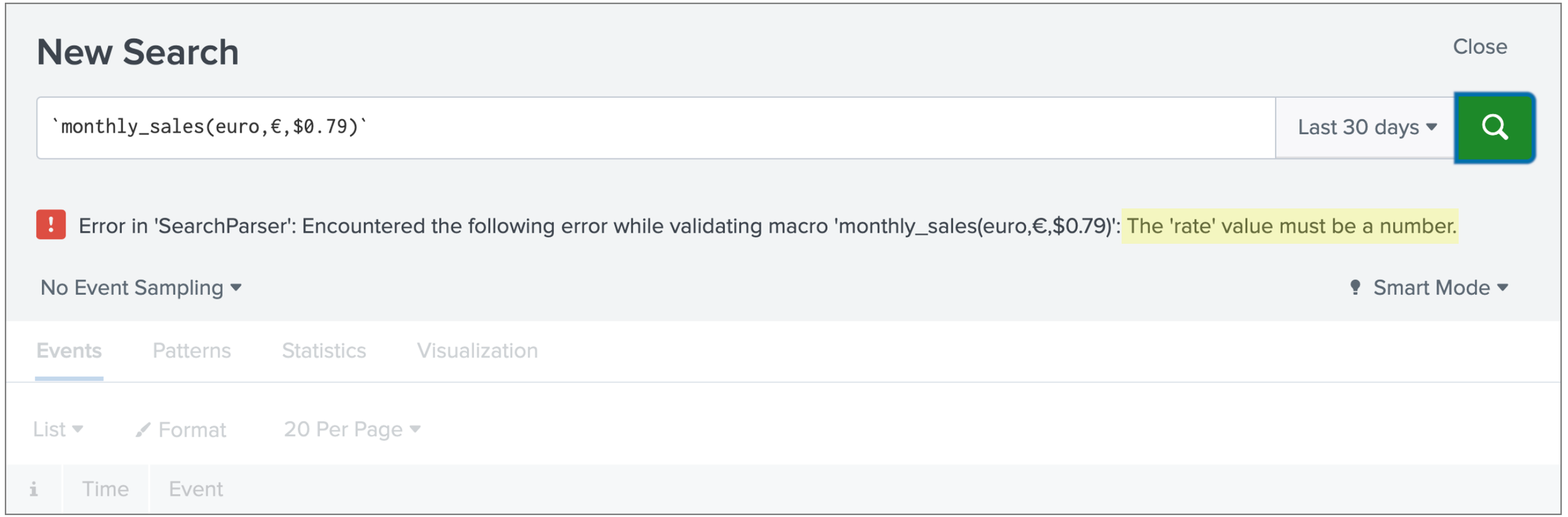


Validate Macro Arguments

4. Define a Validation Expression to verify arguments using eval or boolean expressions
5. Create a Validation Error Message to be displayed if arguments fail validation
6. Save



Validate Macro Arguments (cont.)



Use Macros with Arguments at Search Time

- Include arguments in parentheses, separated by commas, following the macro name
- Be sure to pass in the arguments **in the same order** as you listed them when creating macro

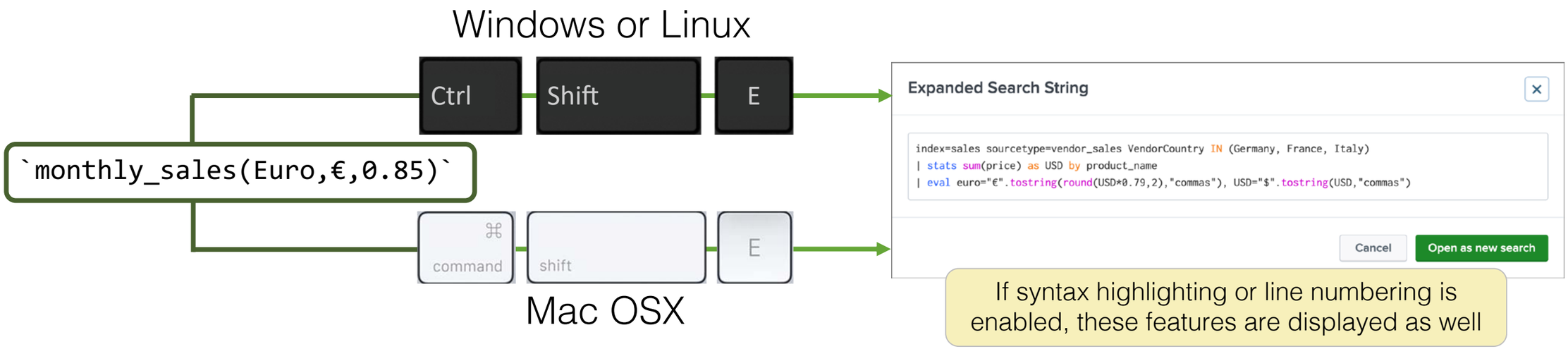
```
`monthly_sales(euro,€,0.79)`
```

```
index=sales sourcetype=vendor_sales
VendorCountry IN(Germany, France, Italy)
| stats sum(price) as USD by product_name
| eval euro="€".tostring(round(USD*0.79,2),
"commas"), USD="$".tostring(USD,"commas")
```

product_name	USD	euro
Benign Space Debris	$1,149.54	€908.14
Curling 2014	$839.58	€663.27
Dream Crusher	$919.77	€726.62
Final Sequel	$374.85	€296.13
Fire Resistance Suit of Provolone	$227.43	€179.67
Holy Blade of Gouda	$233.61	€184.55
Manganiello Bros.	$3,319.17	€2,622.14

Preview a Macro

To expand search macros, use the keyboard shortcut:



Splunk displays the expanded search string, resolving all nested search macros

Note

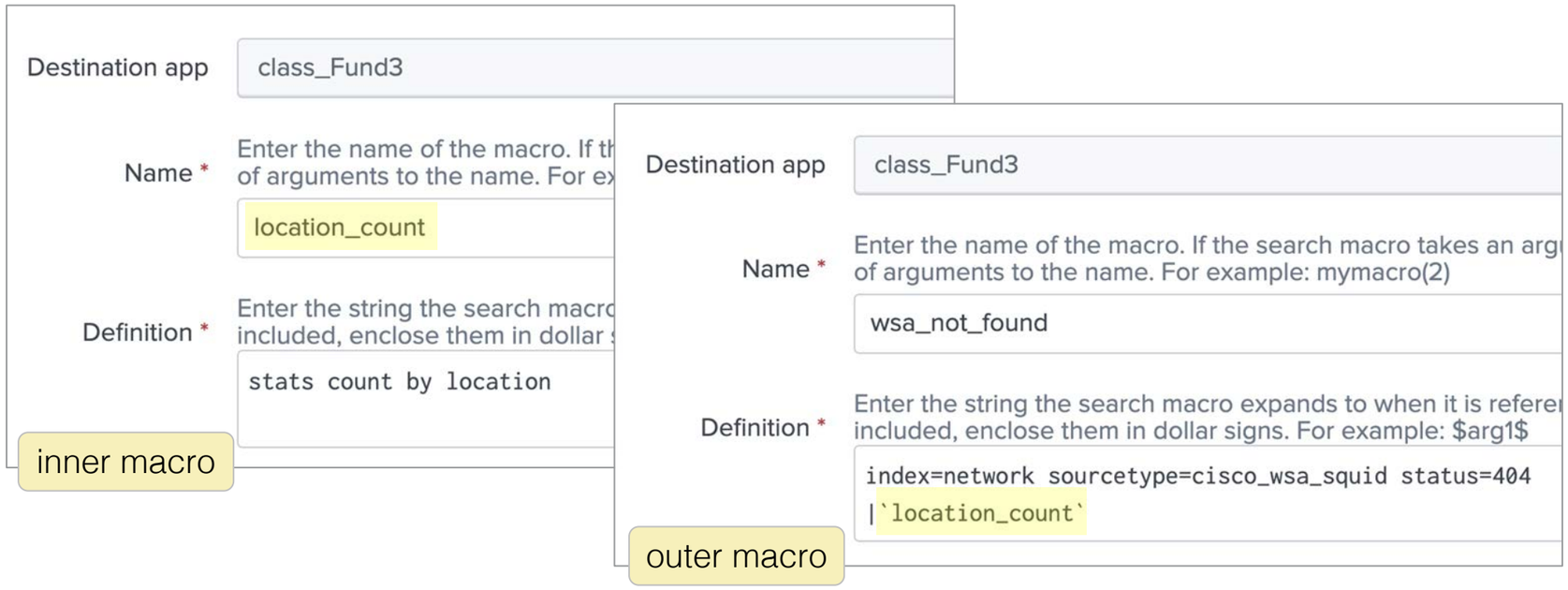
You cannot edit in preview.

 | 11 August 2022

Use Nested Search Macros

Macros can be nested within each other

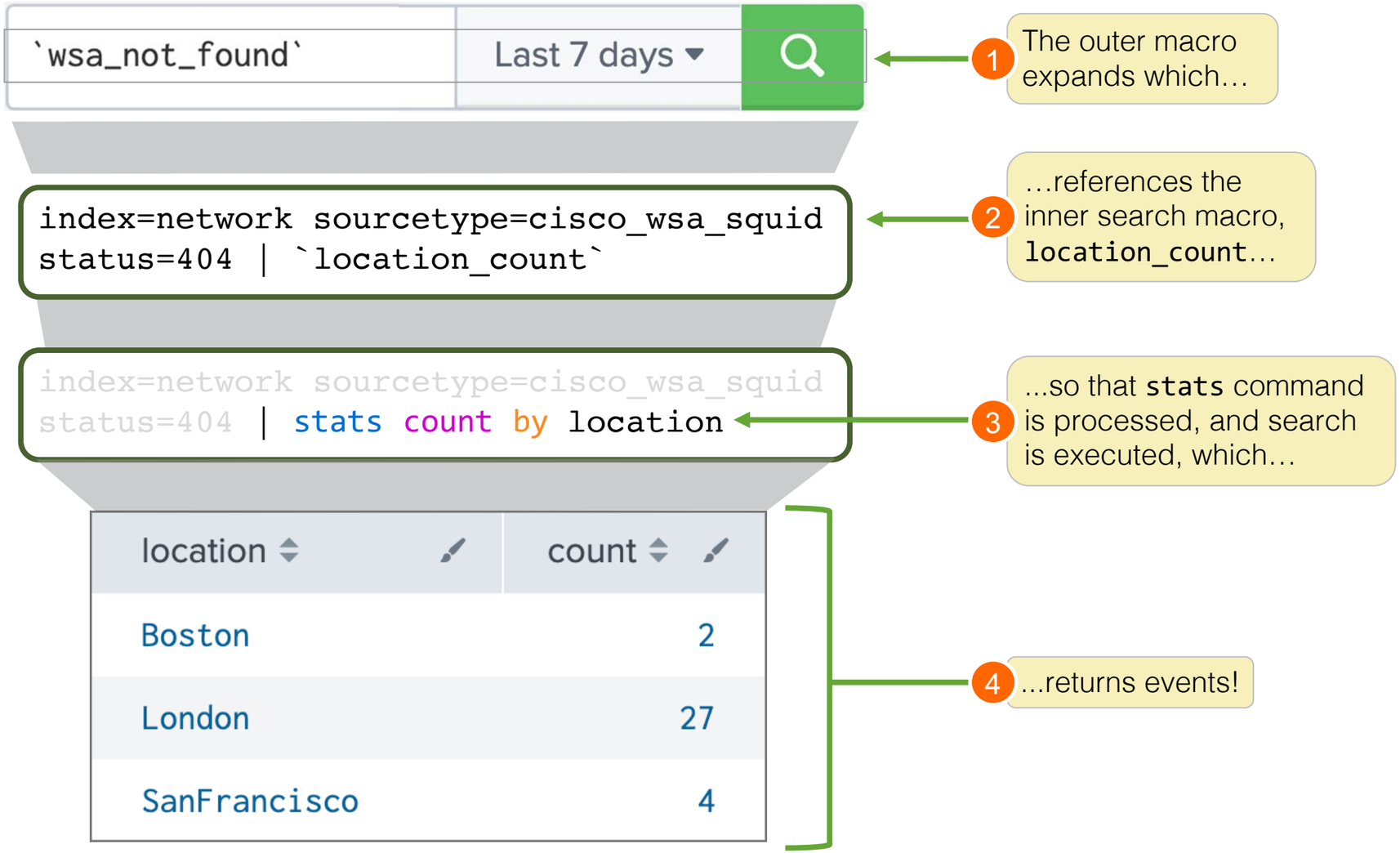
1. Create “inner” macro first
2. Put “inner” macro name surrounded by backticks in definition of “outer” macro



Use Nested Search Macros Example

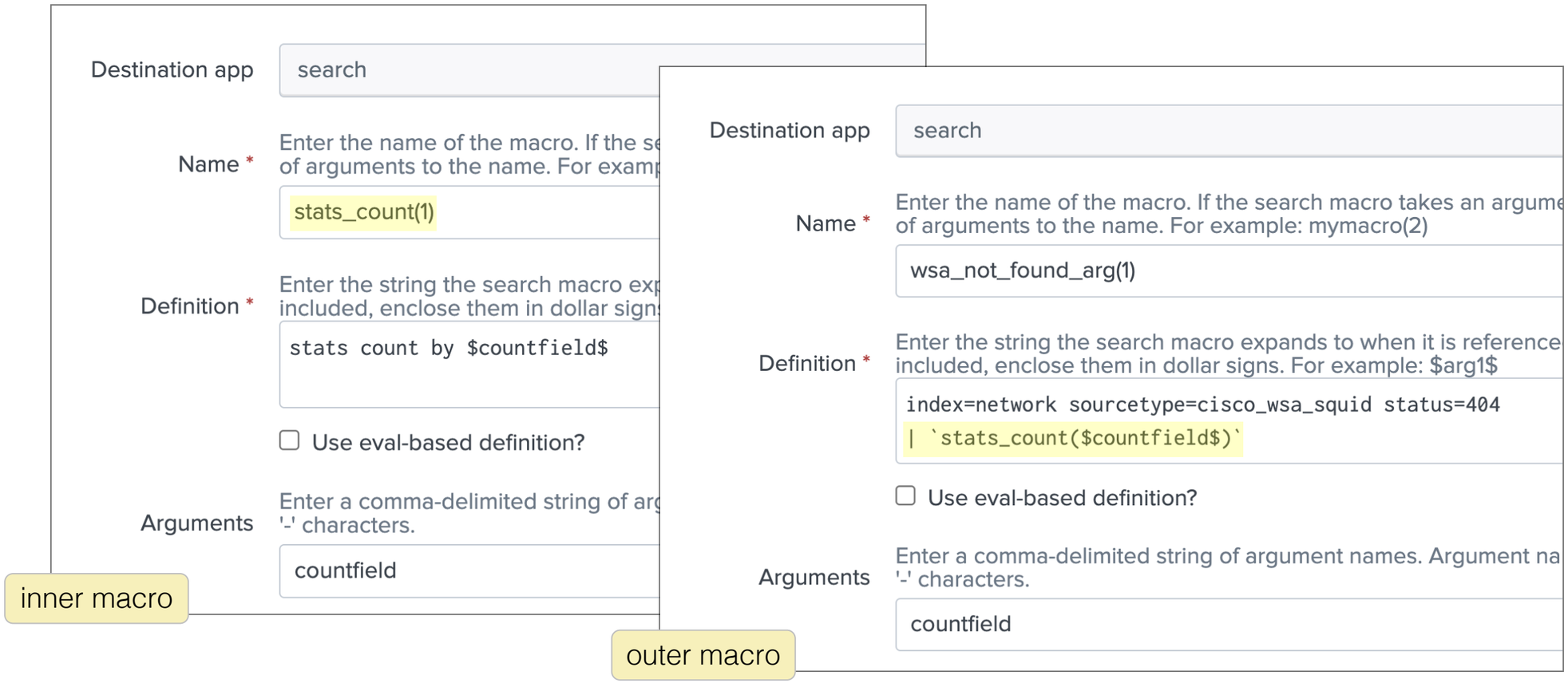
Scenario

Display the count of web security events with status 404 by location during the last 7 days.



Use Nested Search Macros with Arguments

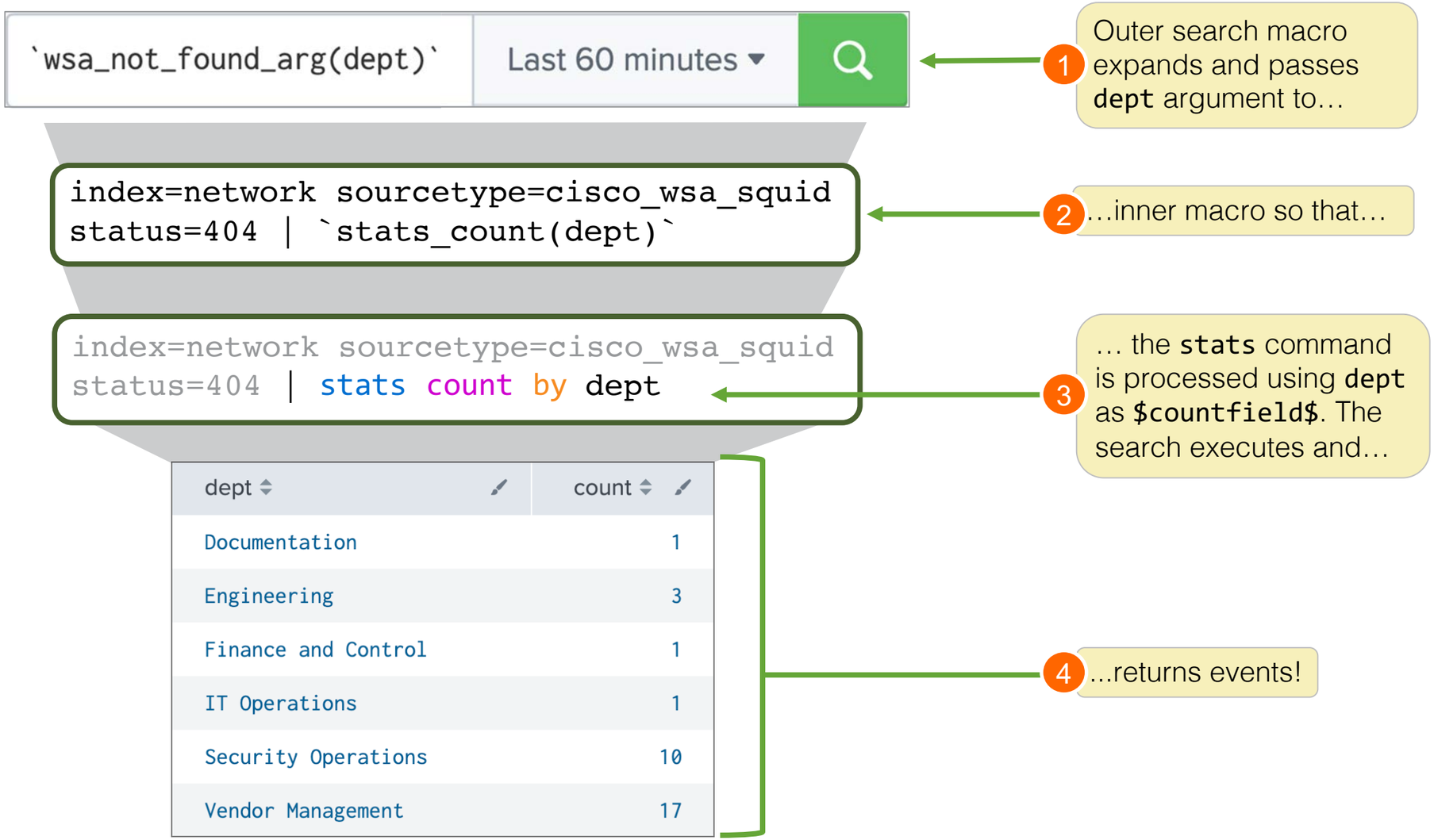
- Arguments can be passed from “outer” macro to “inner” macro
- Provide variable values at search time



Use Nested Search Macros with Arguments (cont.)

Scenario

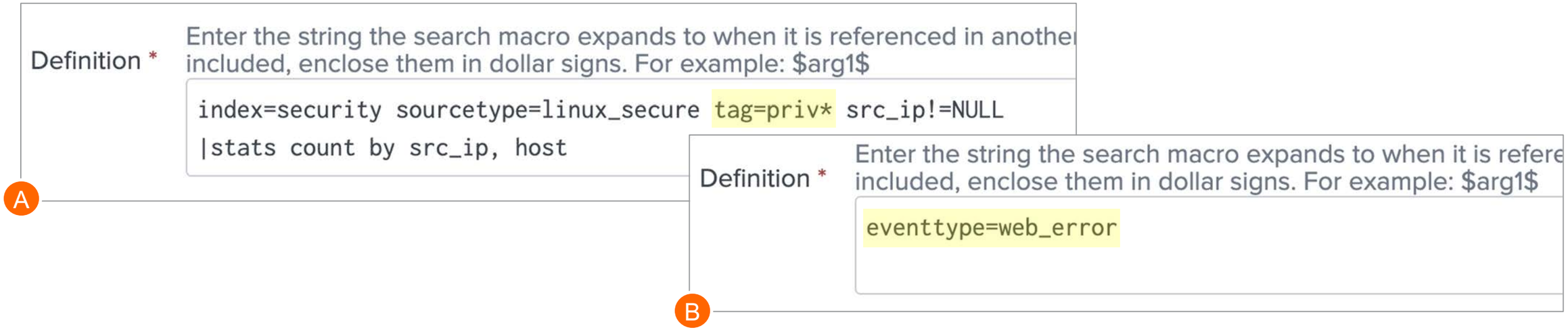
Display the count of web security events with status 404 by department during the last 60 minutes.



Use Macros with Other Knowledge Objects

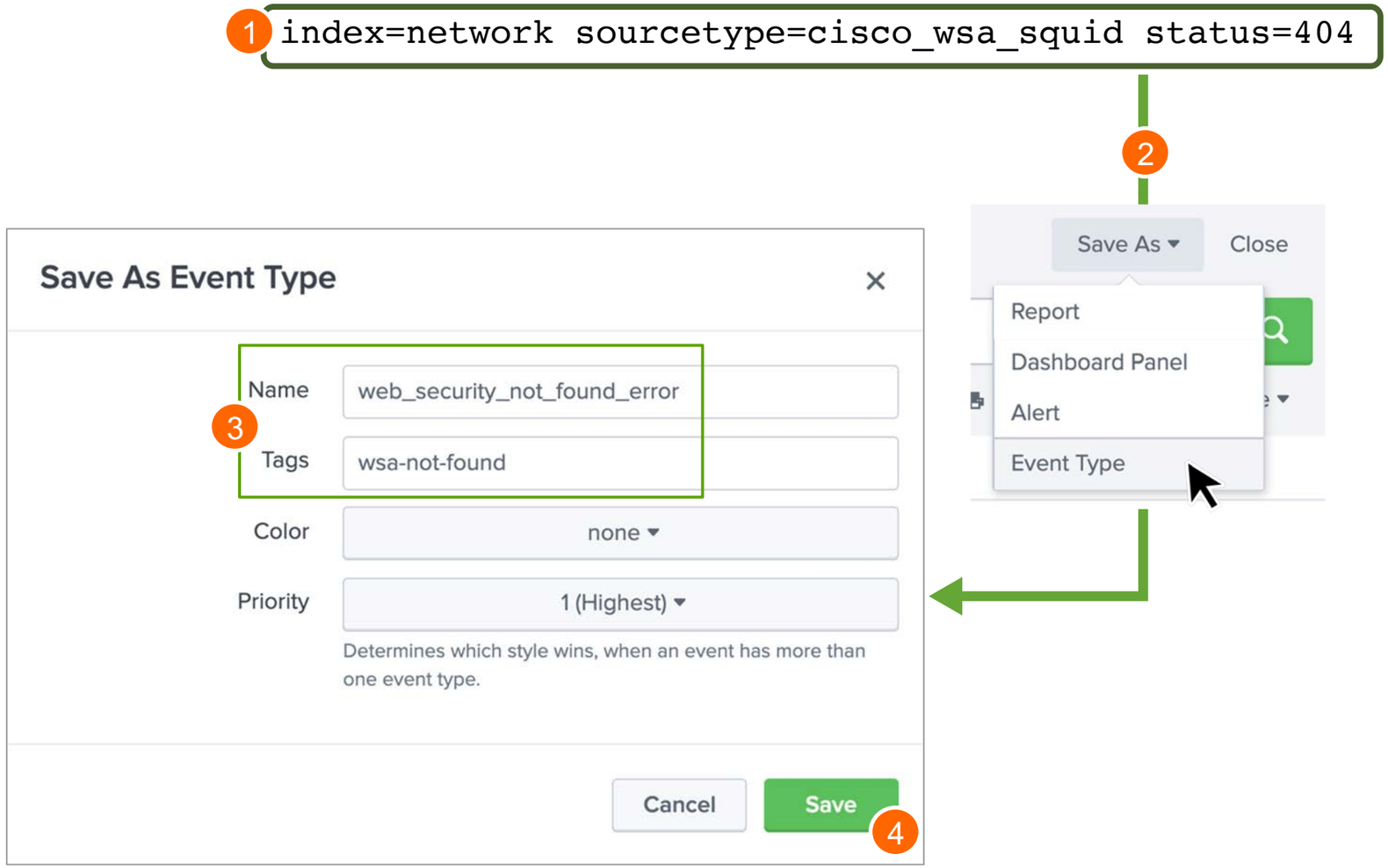
A. Reference knowledge objects in macros just as you would from the search bar—field aliases, calculated fields, tags, etc.

B. The following slides show how to use tags and event types with macros



Use Tags/Event Types with Macros

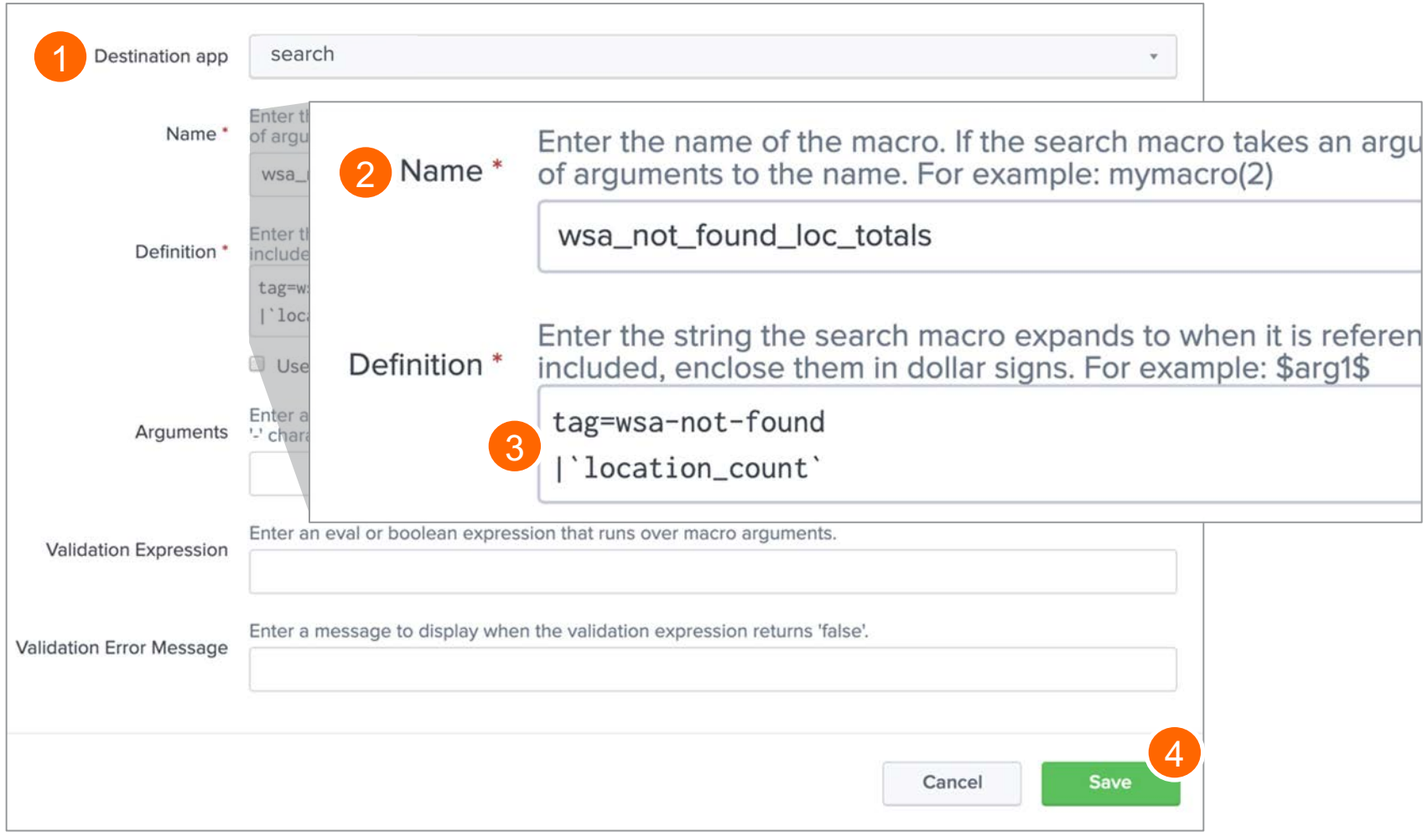
1. Run a search and verify that all results meet your event type criteria
2. **Save As** > **Event Type**
3. Provide a **Name** and optional **Tags** for your event type
4. **Save**



Use Tags/Event Types with Macros (cont.)

Settings > Advanced Search > Search macros> Add new

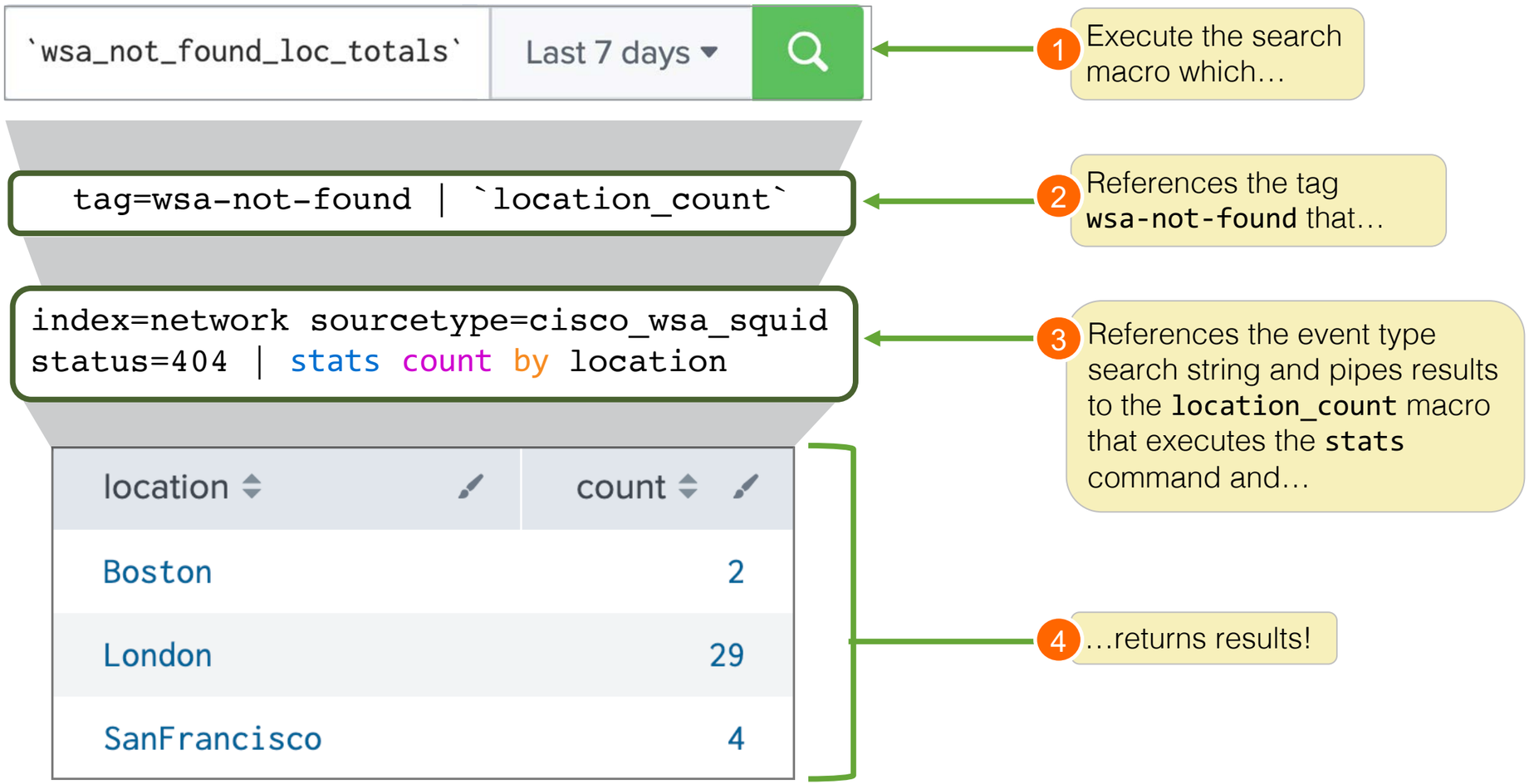
1. Choose Destination app
2. Enter a name for the macro
3. Include the event type OR tag in the macro Definition
4. Save



Use Tags/Event Types with Macros (cont.)

Scenario

Display the count of web security events with status 404 by location during the last 7 days.



Create Macros: Considerations

- When validating more than one argument
  - Use **AND** operator if you want all expressions to be validated
  - The validation error message should be inclusive of all validations
- When creating a macro that begins with a command, don't include a pipe
  - Allow the user to enter the pipe before the macro
    - Avoids having two consecutive pipes, which would give an error

Create Search Macros Lab Exercise

Time: 15 minutes

Tasks:

- Create a macro that will provide a table displaying the total of products in certain European countries
- Use a macro with arguments in a search
- Edit a macro and use the `isnum` function to validate the rate field

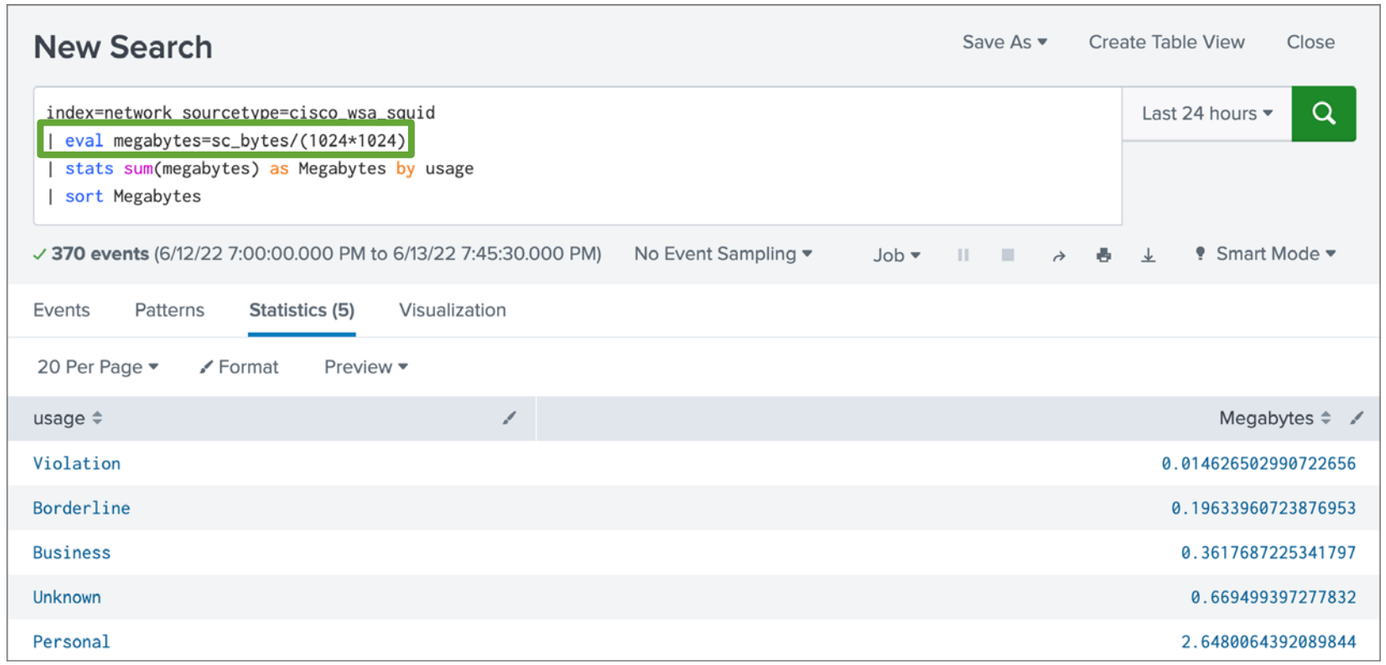
Create Calculated Fields

Topic Objectives

- What is a calculated field
- Create a calculated field
- Use a calculated field

What is a Calculated Field?

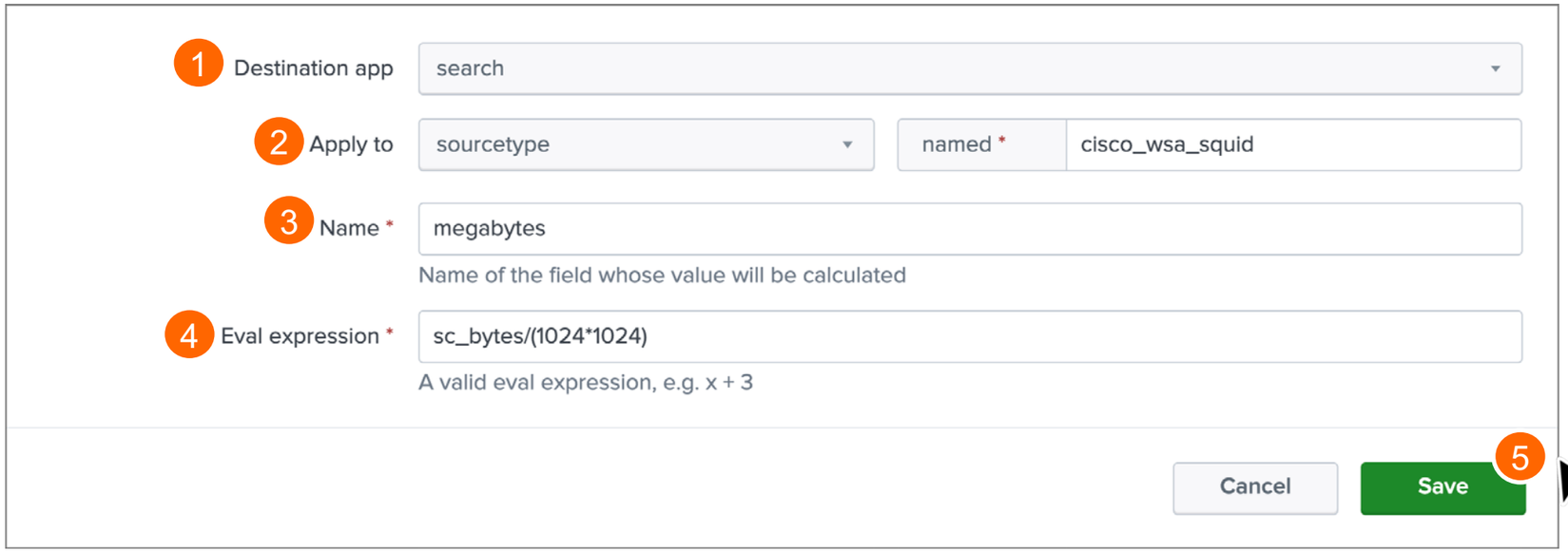
- Shortcut for performing repetitive, long, or complex calculations using the **`eval`** command
- Can only be based on extracted or aliased fields



Create a Calculated Field

Settings > Fields > Calculated fields > **New Calculated Field**

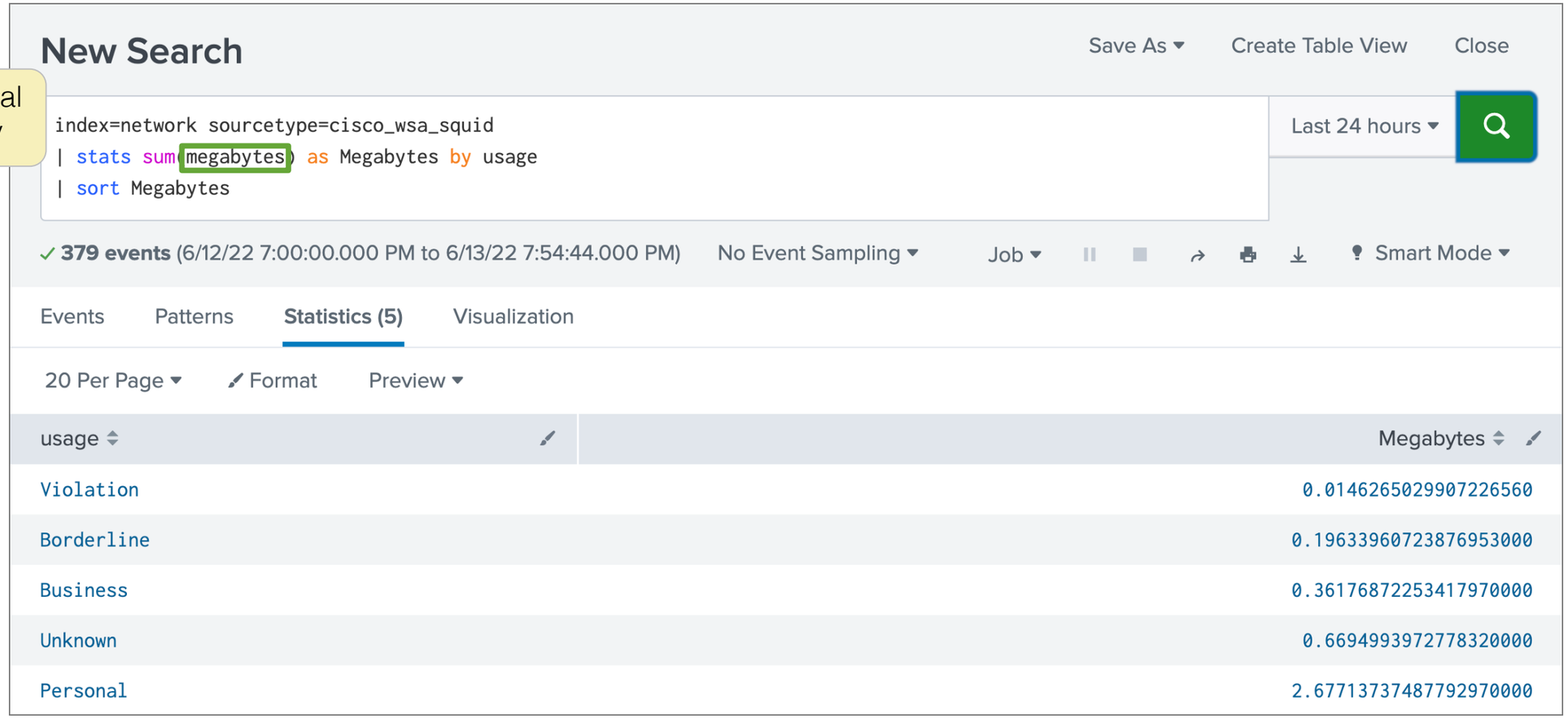
1. Select the app that will use the calculated field
2. Select and specify the **host**, **source**, or **sourcetype** to apply to the calculated field
3. **Name** the calculated field
4. Define the **Eval expression**
5. Save



Use a Calculated Field

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

No manual eval is necessary



Create Calculated Fields Lab Exercise

Time: 5 minutes

Tasks:

- Create a calculated field that converts bytes to MB

Wrap-up Slides

Community

- Splunk Community Portal
  community.splunk.com
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs
  splunk.com/blog/
- Splunk Apps
  splunkbase.com
- Splunk Dev Google Group
  groups.google.com/forum/#!forum/splunkdev
- Splunk Docs on Twitter
  twitter.com/splunkdocs
- Splunk Dev on Twitter
  twitter.com/splunkdev
- Splunk Live!
  splunklive.splunk.com
- .conf
  conf.splunk.com

Support Programs

- **Web**

  Documentation: dev.splunk.com and docs.splunk.com

  Wiki: wiki.splunk.com

- **Splunk Lantern**
  Guidance from Splunk experts

  lantern.splunk.com

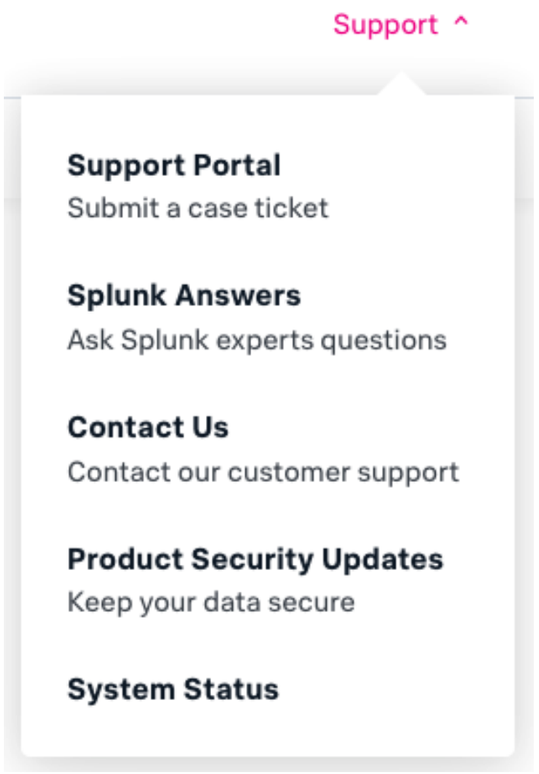
- **Global Support**
  Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365

  Web: splunk.com/index.php/submit_issue

- **Enterprise, Cloud, ITSI, Security Support**

  Web: splunk.com/en_us/about-splunk/contact-us.html#tabs/customersupport

  Phone: (855) SPLUNK-S or (855) 775-8657



Learning Paths (cont.)

Knowledge Manager - Recommended Courses

Free eLearning courses are in blue and courses with an * are present in both learning paths.

- What is Splunk *
- Introduction to Splunk *
- Using Fields *
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards
- Using Choropleth
- Search Optimization *

Learning Paths

Search Expert - Recommended Courses

Free eLearning courses are in blue and courses with an * are present in both learning paths.

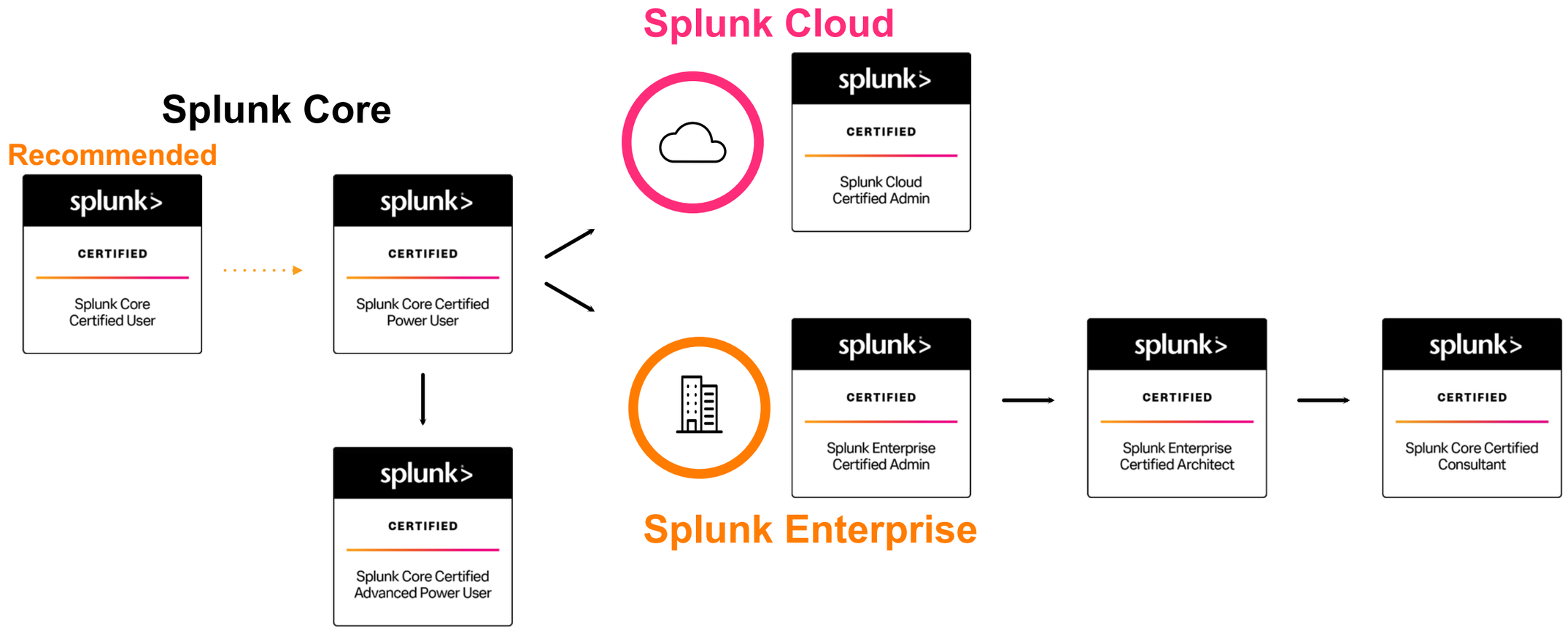
- What is Splunk *
- Introduction to Splunk *
- Using Fields *
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization *

Splunk Certification

Offerings & Requirements

Splunk Core and Beyond

Regardless of which Splunk product you use, it all starts with Splunk Core



Splunk Core Certified Power User

This entry-level certification demonstrates an individual's foundational competence of Splunk's core software

Prerequisite Certification(s):

- None

Prerequisite Course(s):

- None

Splunk Core Certified Power User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 2 **or** the following courses:

- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Correlation Analysis
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Data Models
- Using Choropleth

See here for registration assistance.

Congratulations! You are a...

Recommended Next Steps

- Splunk Core Certified Advanced Power User
- Splunk Enterprise Certified Admin
- Splunk Cloud Certified Admin

 | 11 August 2022

Thank You