Data Normalization: Tags and Aliases

Tag Creation

1. Go to Settings 🡪 click Tags
2. Click List by tag name 🡪 Add New
3. Type tag name 🡪 Failures
4. Field value pair ->status=5\*
5. Click save
6. Go to Search bar 🡪 type tag=”failure”
7. Or type tag::status=”failure”
8. Or type tag::status=”fail\*”

Other ways to create a tag

=========================

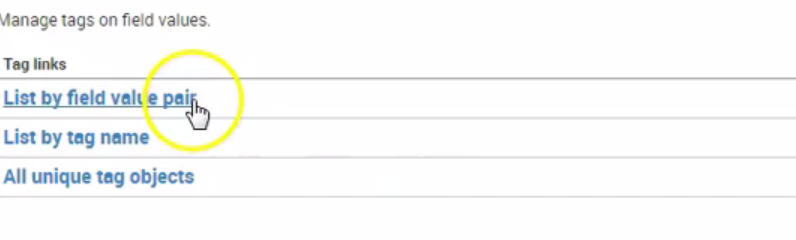
Go to Search and Reporting App 🡪 type sourcetype=access\_combined\_wcookie

Then expand the > choose any one field and edit tag as given below :

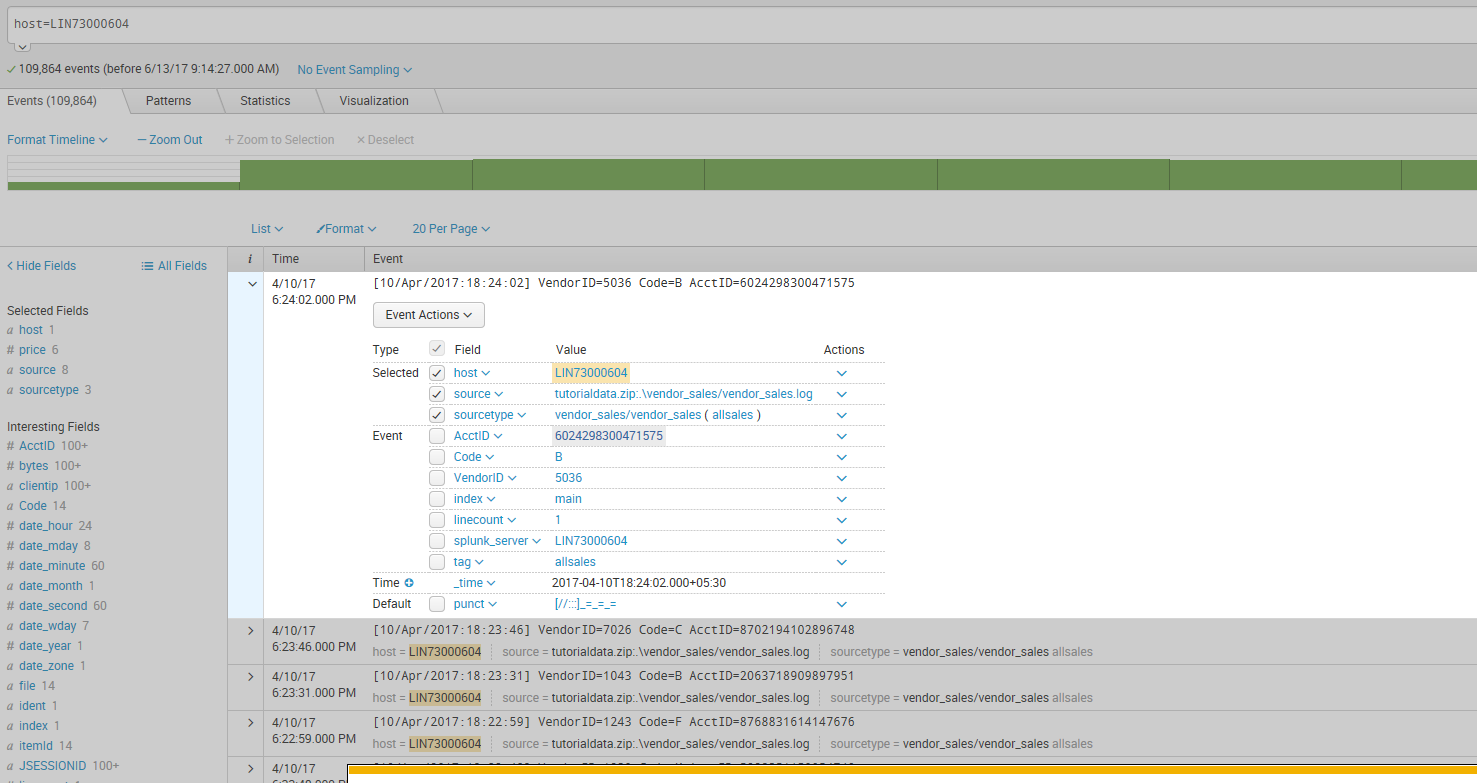


Another method :

Go to Settings 🡪 tags 🡪 list by value pair

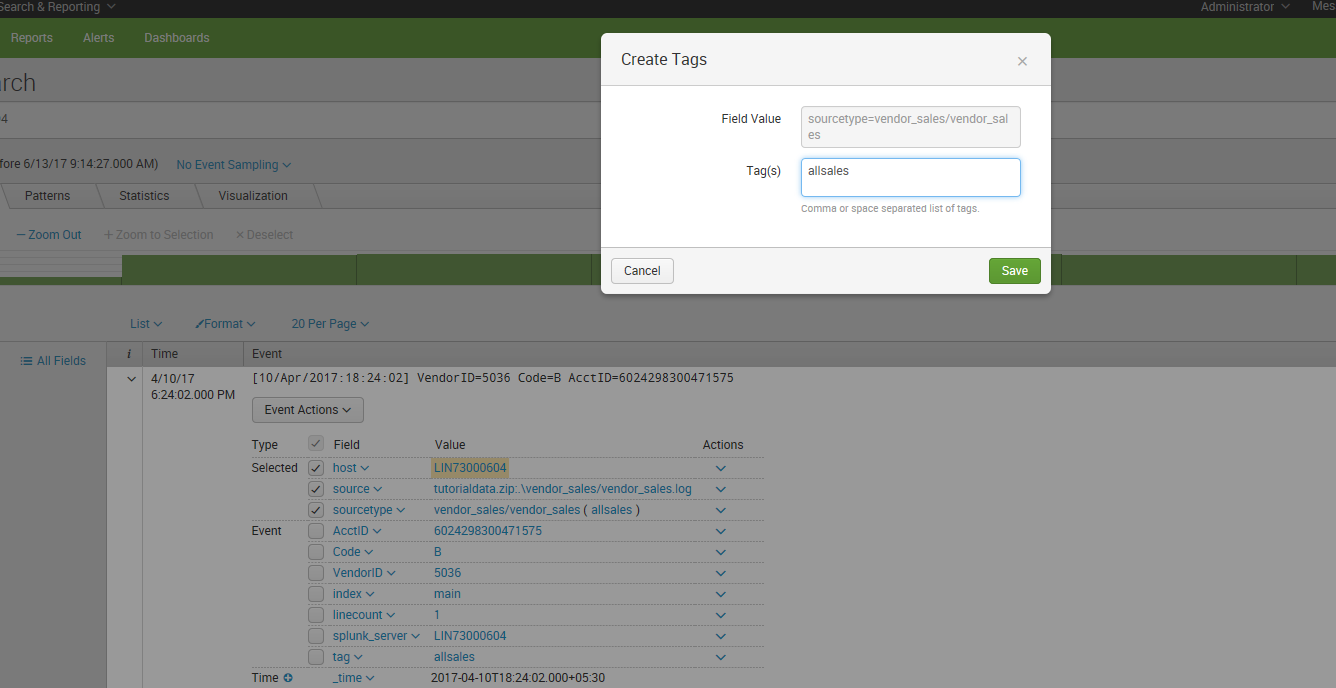


1. Tag field value pairs
2. Locate an event with a field-value pair that you want to tag.
3. Expand a row to see the full list of fields extracted from the event.
4. Click the **Actions** arrow for the field-value pair that you want to create a tag for and select **Edit Actions**.



4. In the Create Actions dialog box , define one or more tags for the field-value pair.

Values for the **Tag(s)** field must be separated by commas or spaces.



## Using the Tag page in Settings

The Tags page gives you three views of your tags. Each view is a different tag organization.

* Field-value pair
* Name
* Unique ID.

### Managing tag sets associated with specific field-value pairs

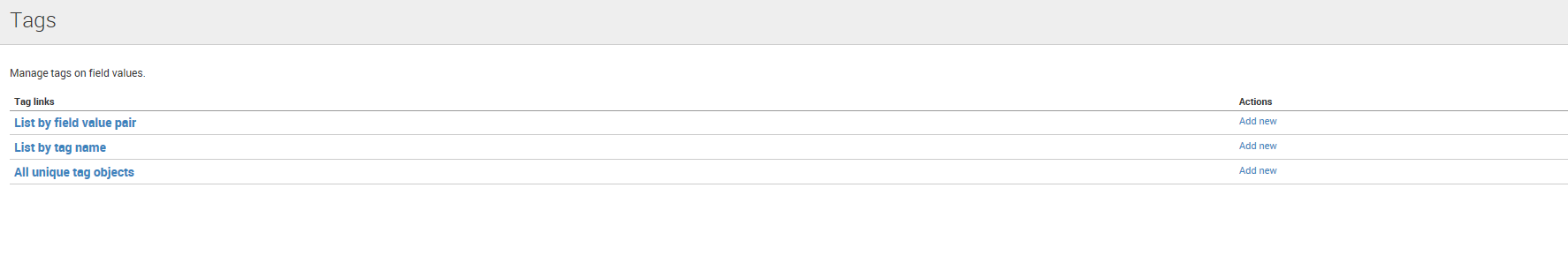
From the **List by field-value pair** page, you can review and edit the tag sets that have been associated with particular field-value pairs.

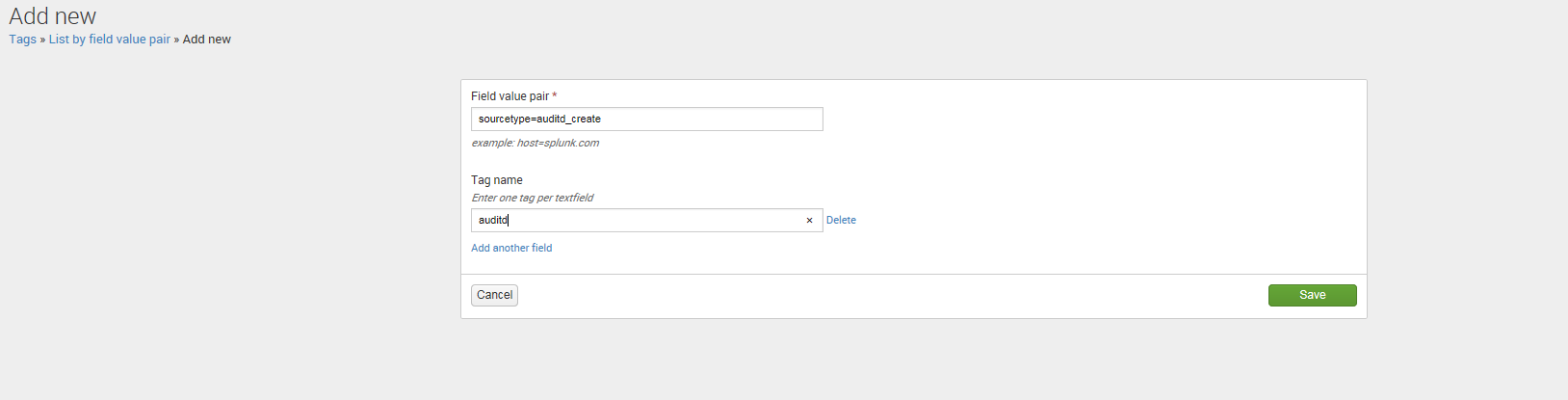
Use this page to manage the permissions for a field-value combination with tags.

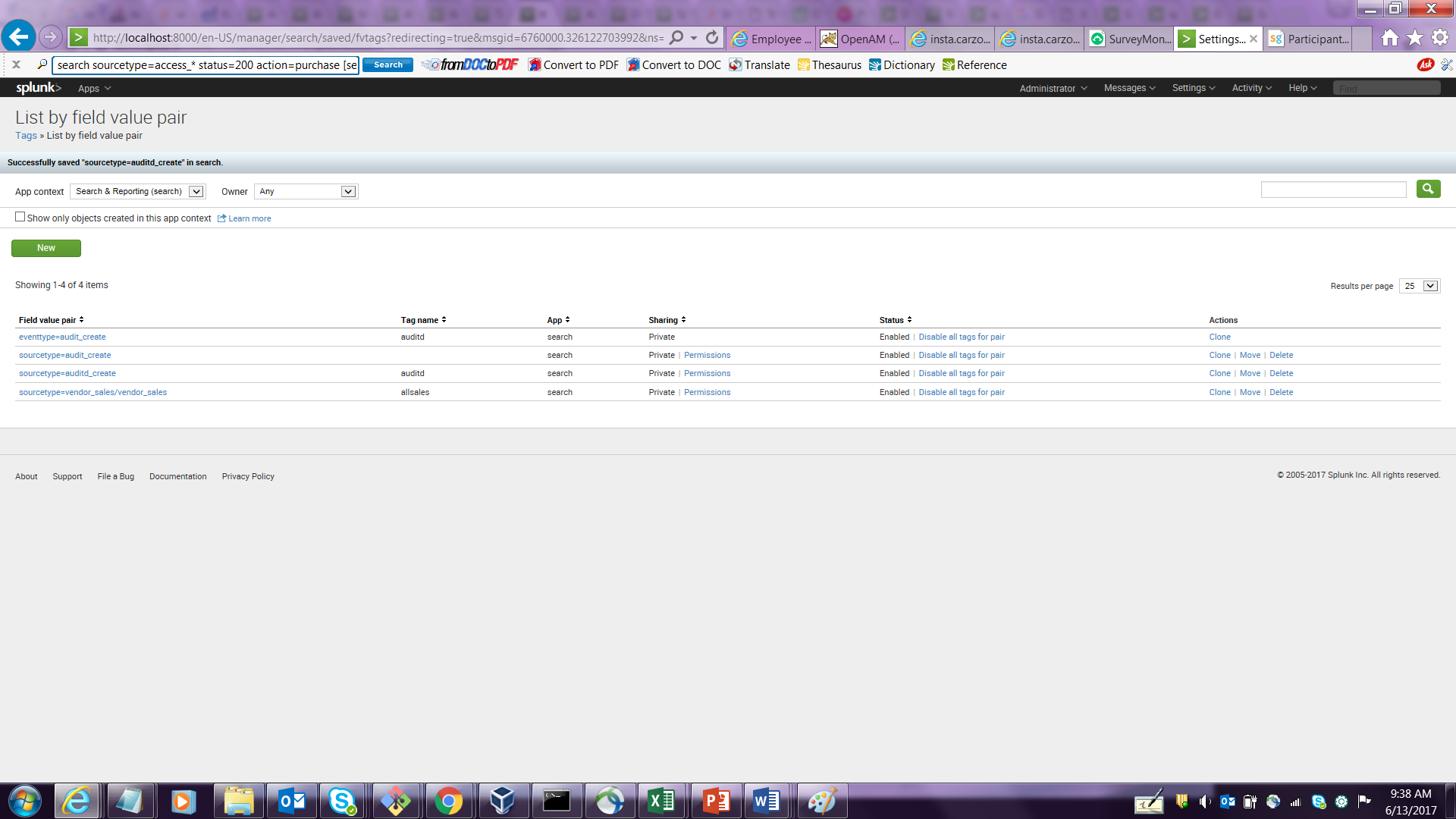
To see the list of tags for a field-value pair, locate the pairing and click on the field-value pair. This opens the associated detail page for that pair.

The following is an example of a set of tags that are defined for the eventtype=auditd\_create field-value pair.

Click **New** on the **List by field-value pair** page, to define a set of tags for a field-value pair.





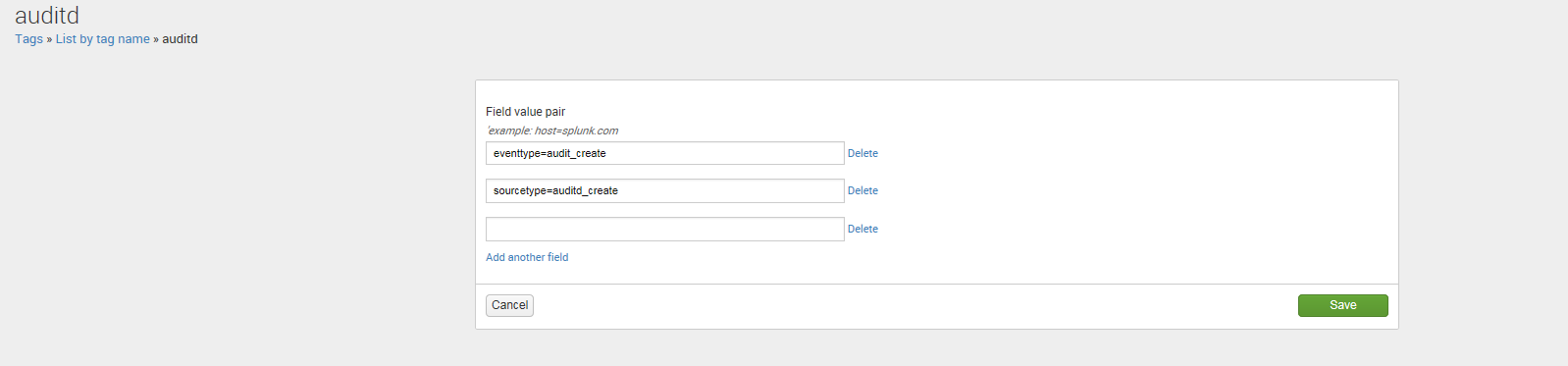


Reviewing and updating sets of field-value pairs associated with specific tags

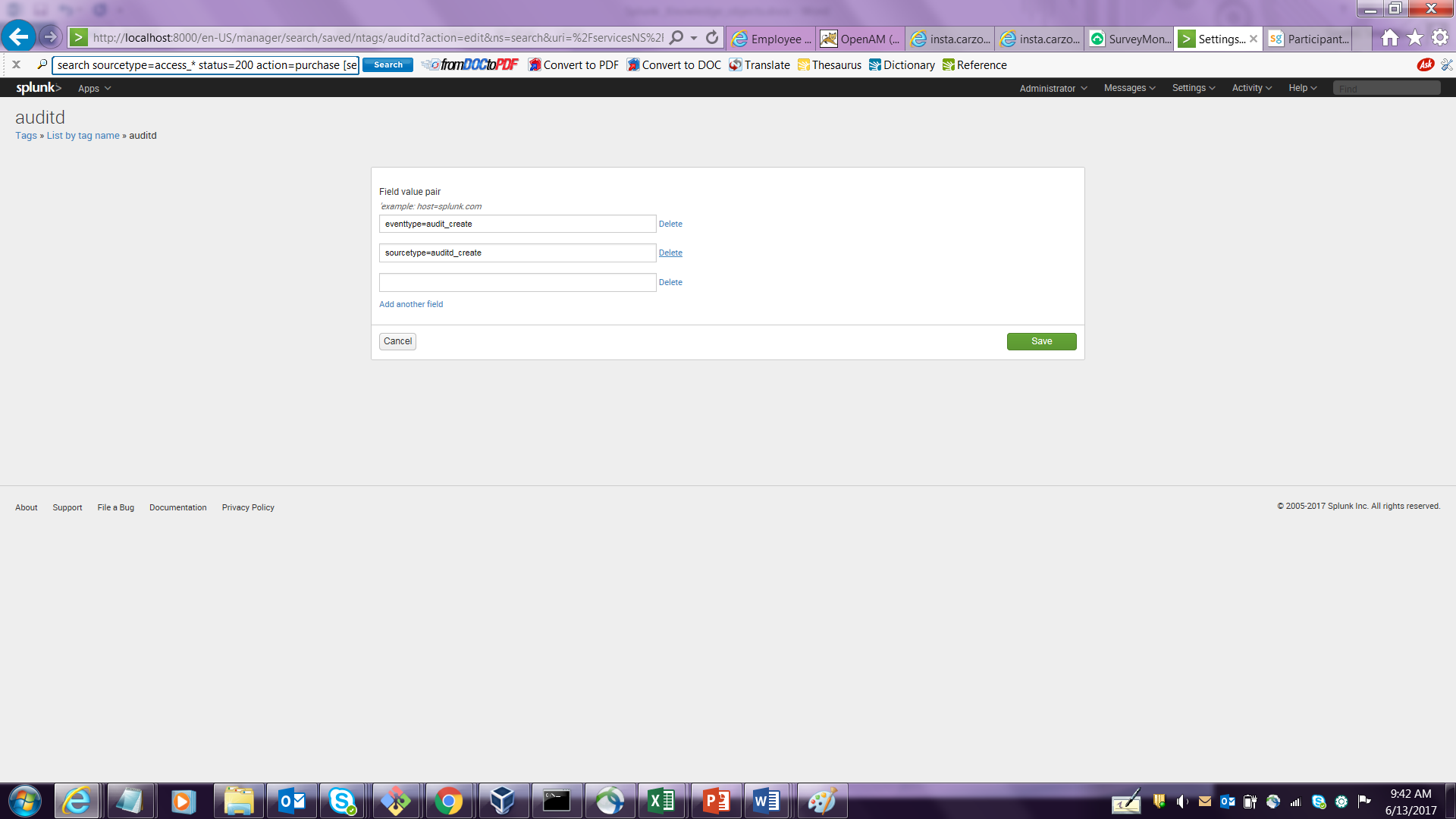
On the List by tag name page in Splunk Web, you can review and edit the sets of field-value pairs that have been associated with specific tags.

You cannot manage permissions for the set of field-value pairs associated with a tag on this page.

You can see the list of field-value pairings for a particular tag. Find the tag in the List by tag name page, and click on the tag name in the Tag name column. This opens the detail page for the tag.



Deleting the tag and modifying it



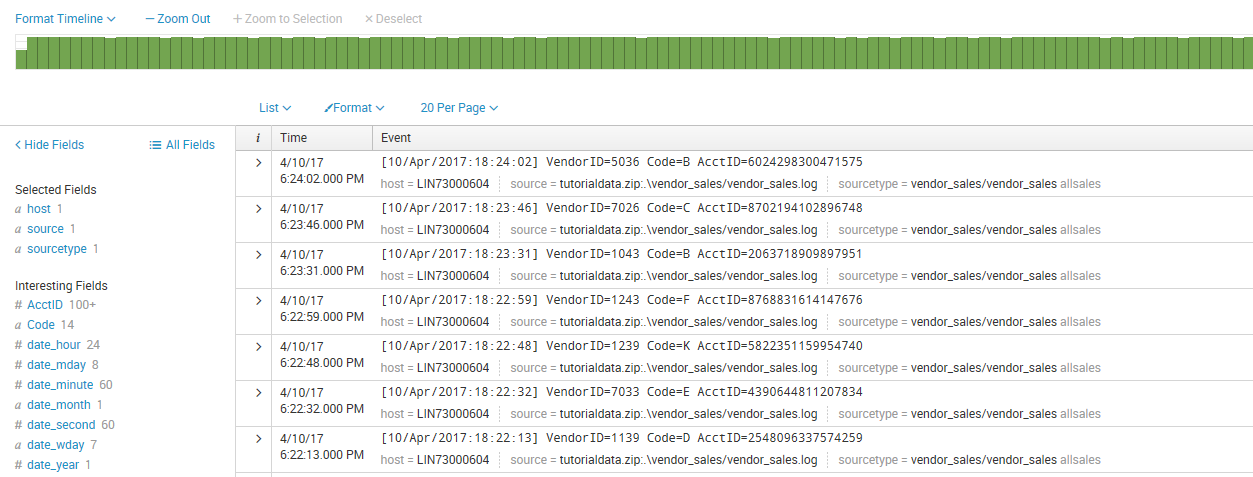
**Search for tagged field values**

You have two ways to search for tags. To search for a tag associated with a value in any field, use the following syntax:

tag=<tagname>

To search for a tag associated with a value in a specific field, use the following syntax:

tag::<field>=<tagname>



You can use the asterisk (\*) wildcard when you search keywords and field values, including for eventtypes and tags.

For example, if you have multiple eventtype tags for various types of IP addresses, such as IP-src and IP-dest, you can search for all of them with:

tag::eventtype=IP-\*

To find all hosts whose tags contain "local", search for the following tag:

tag::host=\*local\*

To search for the events with eventtypes that have no tags, you can search for the following Boolean expression:

NOT tag::eventtype=\*

**Disabling and deleting tags**

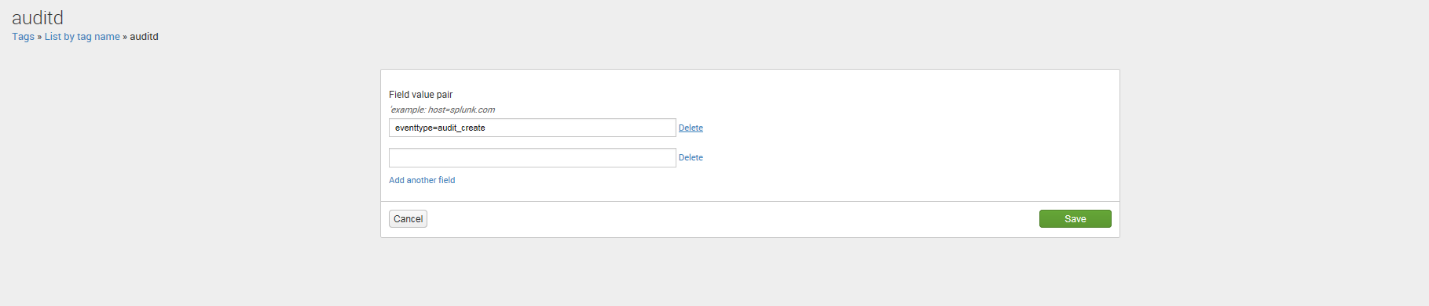
If you have a tag that you no longer want to use, or want to have associated with a particular field-value pairing, you can disable it or remove it.

* Remove a tag association for a specific field-value pair in the search results.
* Bulk disable or delete a tag, even if it is associated to multiple field values, with the List by tag name page.
* Bulk disable or delete the associations between a field-value pair and a set of tags by using the List by field-value pair page.

**Delete a tag with multiple field-value pair associations**

 Use Splunk Web to remove a tag from your system, even if it is associated with dozens of field-value pairs. This method lets you get rid of all of these associations in one step.

Select **Settings > Tags > List by tag name**. Delete the tag. If you don't see a delete link for the tag, you don't have permission to delete it. When you delete tags, be aware of downstream dependencies.



**Disable or delete the associations between a field-value pairing and a set of tags**

Use this method to bulk-remove the set of tags that is associated to a field-value pair. This method enables you to get rid of these associations in a single step. It *does not* remove the field-value pairing from your data, however.

Select **Settings > Tags > List by field-value pair**. Delete the field-value pair. If you do not see a delete link for the field-value pair, you do not have permission to delete it. When you delete these associations, be aware of downstream dependencies that may be adversely affected by their removal.

**Disable and delete tags**

You can remove a tag association for a specific field value through the Search app. You can also disable or delete tags, even if they are associated with multiple field values in Settings.

**Remove a tag association for a specific field value in search results**

You can remove a tag associated with a field value in your search results.

1. Click the arrow next to the event.
2. Under **Actions**, click open the arrow next to the field value.
3. Select Edit Tags to open the **Create Tags** window.
4. In the **Create Tags** window, delete the tags that you want to disable from the **Tags** field.
5. Click **Save**.

This action removes this tag and field value association from the system. If this is the only field value the tag is associated with, the tag is removed from the system.

**Rename source types at search time**

To rename the source type, add the rename attribute to your source type stanza:

rename = <string>

**Note:** A source type name can only contain the letters a though z, the numerals 0 through 9, and the \_ (underscore) character.

For example, say you're using the source type "cheese\_shop" for your application server. Then, accidentally, you index a pile of data as source type "whoops". You can rename "whoops" to "cheese\_shop" with this props.conf stanza:

[whoops]

rename=cheese\_shop

Now, a search on "cheese\_shop" will bring up all the "whoops" events as well as any events that had a "cheese\_shop" source type from the start:

sourcetype=cheese\_shop

If you ever need to single out the "whoops" events, you can use \_sourcetype in your search:

\_sourcetype=whoops

**Important:** Data from a renamed source type will only use the search-time configuration for the target source type ("cheese\_shop" in this example). Any field extractions for the original source type ("whoops" in the example) will be ignored.

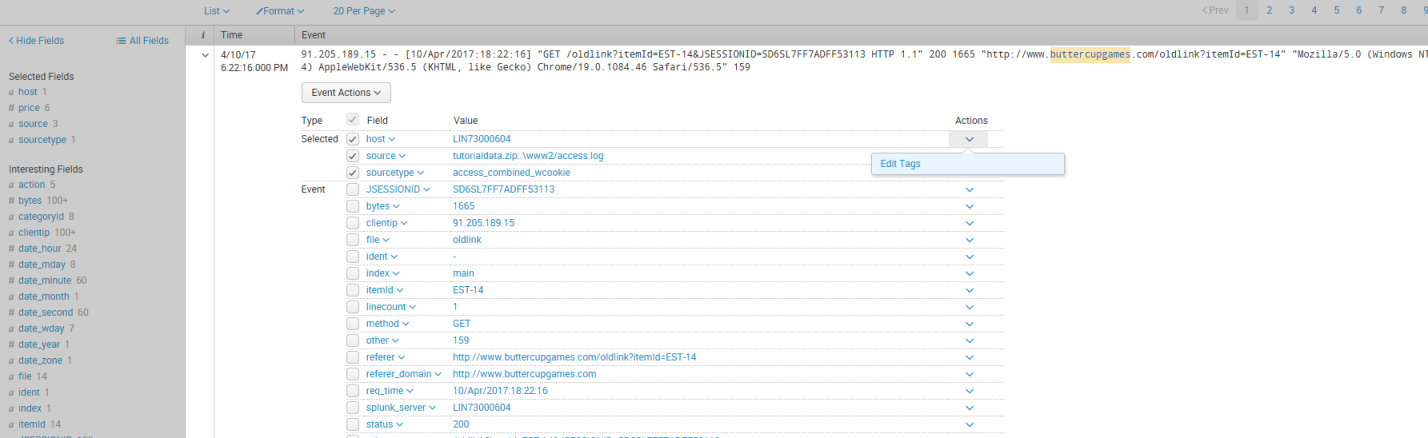
**Tag the host field**

Useful for

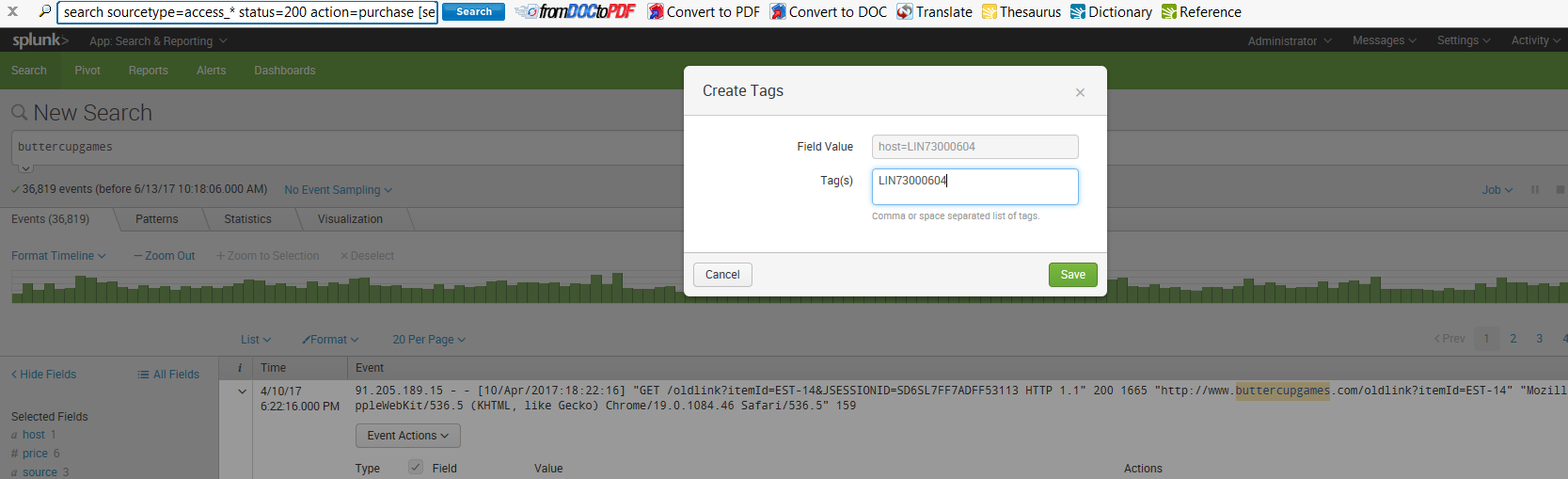
1. Knowledge capture and sharing
2. Crafting more precise searches

**Add a tag to the host field in search results**

1. Perform a search for data from the host you'd like to tag.
2. In the search results, click on the arrow associated with the event containing the field you want to tag. In the expanded list, click on the arrow under **Actions** associated the field, then select **Edit Tags**.



1. n the Create Tags dialog enter the host field value that you'd like to tag, for example in Field Value enter **Tag host= <current host value>**. Enter your tag or tags, separated by commas or spaces, and click **Save**.



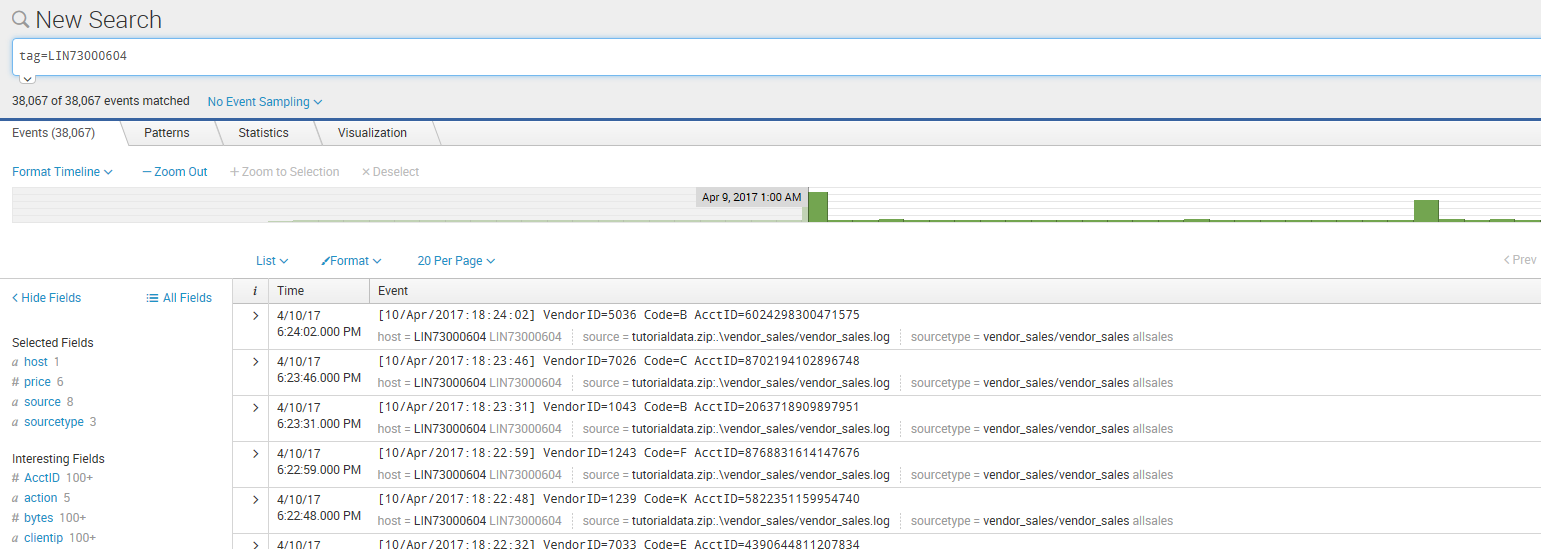
Tag Event types

============

Add tags to event types using Splunk web

Splunk Web enables you to view and edit lists of event types.

* Navigate to **Settings > Event types**.
* Locate the event type you want to tag and click on its name to go to its detail page.
  + **Note:** Keep in mind that event types are often associated with specific Splunk apps. They also have role-based permissions that can prevent you from seeing and/or editing them.
* On the detail page for the event type, add or edit tags in the **Tags** field.
* Click **Save** to confirm your changes.
* Once you have tagged an event type, you can search for it in the search bar with the syntax tag::<field>=<tagname> or tag=<tagname>:
* tag=foo
* tag::host=\*local\*



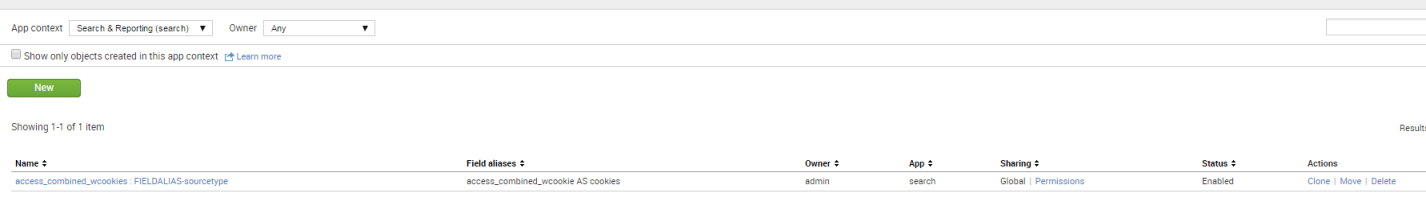
Create field aliases in Splunk Web

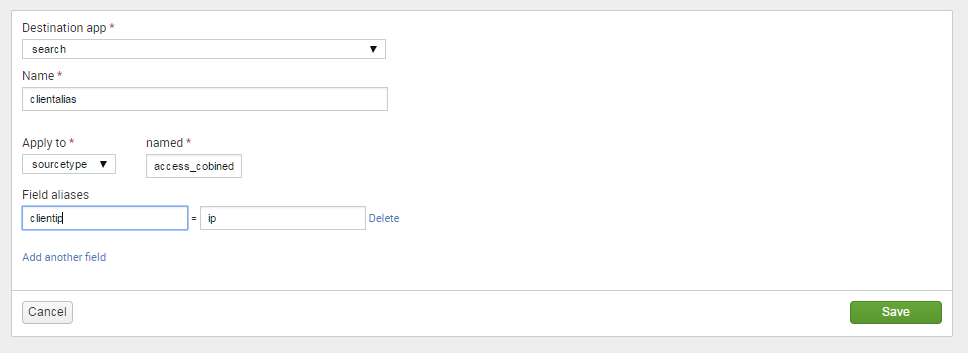
**Using field aliases to normalize your data**

1. Locate a field within your search that you would like to alias.
2. Select **Settings > Fields > Field aliases**.
3. Select an app to use the alias.
4. Enter a name for the alias.
5. Select the host, source, or sourcetype to apply to a default field.
6. Enter the name for the existing field and the new alias.
7. Click Save.



Select Field Aliases





Click save

Change permissions

Click on Search and Reporting app 🡪type sourcetype =access\_combined\_wcookie

Configure Filed aliases in props.conf

1. Add the following line to a stanza in props.conf:

FIELDALIAS-<class> = <orig\_field\_name> AS <new\_field\_name>

* + <orig\_field\_name> is the original name of the field.
  + <new\_field\_name> is the alias to assign to the field.
  + You can include multiple field alias renames in one stanza.

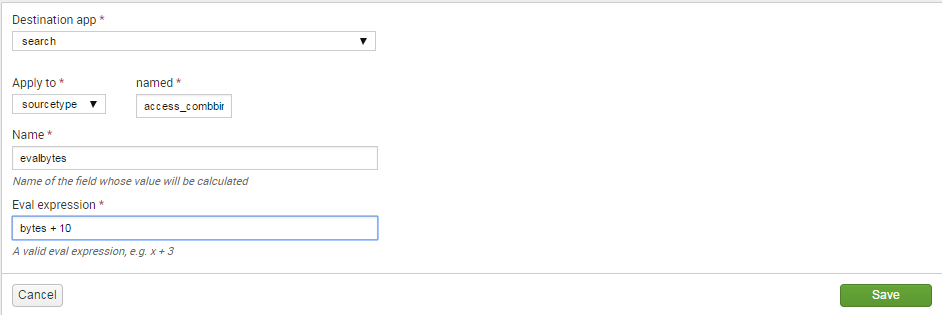
1. Restart Splunk Enterprise for your changes to take effect.

Calculated fields

=================



Select calculated fields 🡪New



Click on save

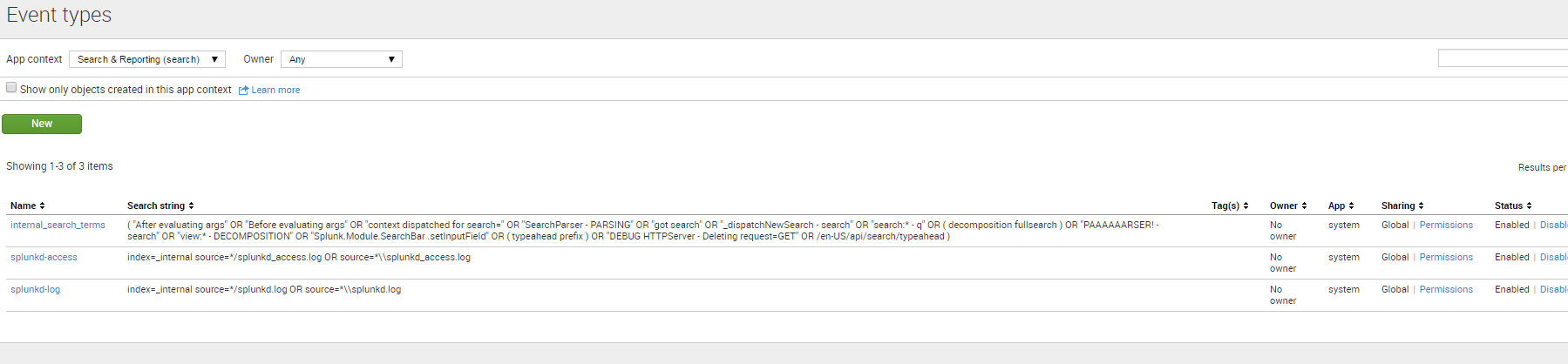
Change permission

Go to Search and Reporting App -> type sourcetype=access\_combined\_wcookie

Check for evalbytes under interesting fields

Eventtypes

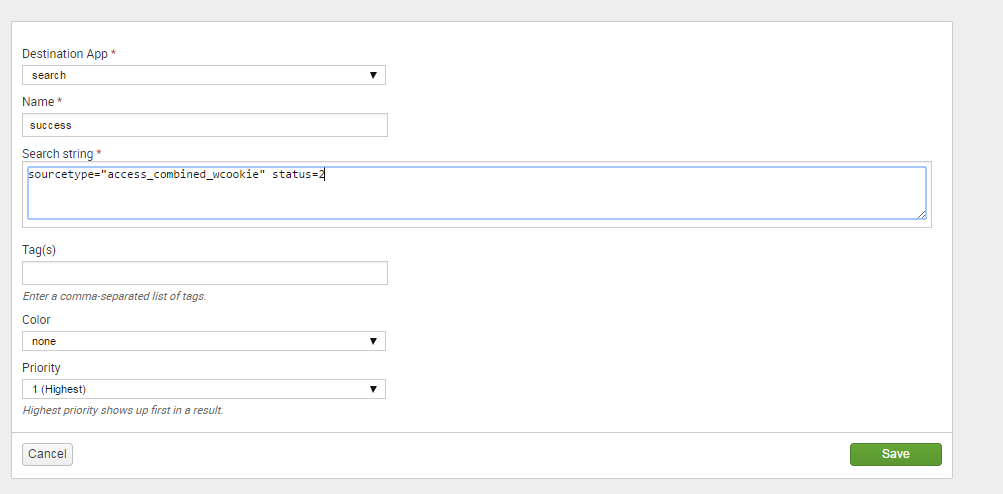
Click on Settings 🡪 Eventtypes



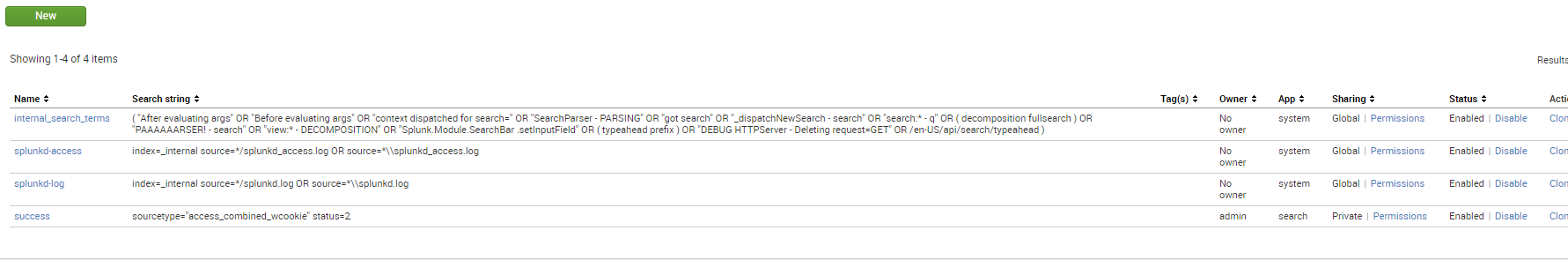
Click New

Type under search string

Sourcetype=”access\_combined\_wcookie” status=2\*



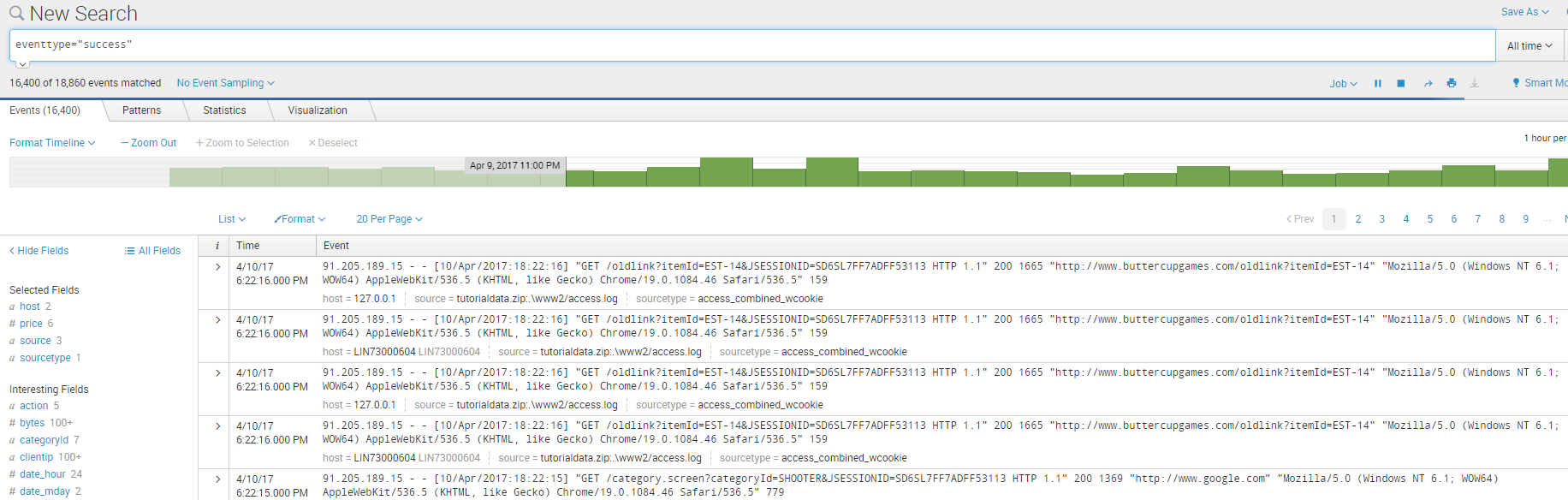
Click save



Change permissions 🡪this app

Go to Search&reporting app 🡪 type

eventtype=”success”



Another method :2

Go To Save As 🡪 Eventtype

Method 3:

Expand > 🡪 Go to Event Actions 🡪 Build Event type