# Alert Types:

Splunk has multiple alert types, including scheduled and real-time, and you can create custom alert actions to extend the platform's functionality:

* Scheduled: Creates a CRON job to run an alert at a specified time
* Real-time: Triggers an alert based on a search and a specified time interval
* Custom alert actions: User-defined actions that can be implemented in a script and packaged in a Splunk app

# To create an alert in Splunk, you can:

1. Go to Splunk and enter a search string
2. Select a mode and click the magnifying icon to search
3. Select Save As and then Alert
4. Enter a title, description, and permissions
5. Select an alert type
6. Set the alert type to Scheduled to create a CRON job
7. Select Run on CRON Schedule and a time range

You can also create custom alert actions to extend the Splunk platform with specialized alerting functionality. For example, you can create a custom alert action to send a customized notification to users via your company's instant messaging system.

<https://docs.splunk.com/Documentation/SplunkCloud/latest/Alert/AlertTypesOverview#:~:text=Alert%20type%20comparison,scheduled%20and%20real%2Dtime%20alerts.&text=Searches%20according%20to%20a%20schedule,result%20or%20result%20field%20counts>.

# Splunk Lookups

Splunk has some enormously powerful features for analyzing data. One of the most popular is the ability to take highly analytical information and render it in ways that are understandable by everyone. This feature is referred to as data enrichment. Splunk **lookups** command enables data enrichment is built into Splunk processing language.

## What are Splunk Lookups?

Lookups provide the ability to substitute cryptic information with more readable information without altering the meaning. For example, A successful rendering of a website in a browser can be identified by the HTTP code of 200 or (OK) and an unsuccessful rendering might be a HTTP code of 400 or (Page not found). If you had to create a report on the successful and unsuccessful Web page hits you would not want your audience to ponder; what is the meaning of 200? Or what is the meaning of 400? …while they are reading your report. You can use a Lookup to take the cryptic value of 200 and render the human readable equivalent of (OK).

### **The Benefits of Splunk Lookups**

We examined one of the benefits of lookups, but there are other benefits as well.

#### **Benefit #1**

You can use a lookup to provide additional information to a search from a separate file. This is a way to add more valuable information to the search that might appeal to the view of search results.

#### **Benefit #2**

Lookups can be used as a way of dynamically filtering events in a search. This provides the ability to filter events based on a list of preset values.

#### **Benefit #3**

Lookups can be used to detect events that are not supposed to show up in the data. It is a form of anomaly detection.

## Types of Splunk lookups

There are three basic lookup commands in the Splunk Processing Language.

**Lookup Command**

The lookup command provides match field-value combinations in event data with field-value combination inside an external lookup table file or KV-STORE database table.

**Inputlookup Command**

The inputlookup command searches the content of a lookup table. The lookup table can be in a CSV file or KV-STORE database table.

**Outputlookup Command**

The outputlookup command can write information into a CSV file or KV-STORE database table.

## How do you use lookups?

**Example #1**

You can use lookups to provide information to a search that is not currently available in the raw data. Let us say that you have a lookup table that is name “product\_info” and it contains the following information:



Suppose you want you to provide the product and price in your output results using the Code field values from your raw data in Splunk and you want all the fields to show up in a report. You can add the lookup table to your search like this:

**sourcetype vendor | stats count by product\_code | lookup product\_code OUTPUTNEW product, price**.

You can then use a table command to render all the fields in an appropriate format.

**Example #2**

You can use a lookup to filter events in a more dynamic way. What if you only want to display events that contain certain field values and not others? Then you might use a search like this:

**| makeresults | eval code=”b” | search [ inputlookup product\_code.csv | fields code]**.

**Example #3**

You can use a lookup to find events that are not supposed be in the data. They are called anomalies. To use a look as an anomaly detector the search might look like this:

**sourcetype=my\_source\_events | stats count by events\_to\_inspect as suspected\_anomalies | search NOT [| inputlookup known\_match.csv] | table component.**

## Conclusion

Splunk lookups power offers capability for data enrichment making your search results more human-readable and relevant. Using Splunk lookups for filtering, adding, and tracking information is an excellent feature for making your search more effective and valuable to audiences.

### **If you found this helpful…**

You don’t have to master Splunk by yourself in order to get the most value out of it. Small, day-to-day optimizations of your environment can make all the difference in how you understand and use the data in your Splunk environment to manage all the work on your plate.

Cue Atlas Assessment: Instantly see where your Splunk environment is excelling and opportunities for improvement. From download to results, the whole process takes less than 30 minutes using the button below:

# Splunk - Lookups

In the result of a search query, we sometimes get values which may not clearly convey the meaning of the field. For example, we may get a field which lists the value of product id as a numeric result. These numbers will not give us any idea of what kind of product it is. But if we list the product name along with the product id, that gives us a good report where we understand the meaning of the search result.

Such linking of values of one field to a field with same name in another dataset using equal values from both the data sets is called a lookup process. The advantage is, we retrieve the related values from two different data sets.

## Steps to Create and Use Lookup File

In order to successfully create a lookup field in a dataset, we need to follow the below steps −

### **Create Lookup File**

We consider the dataset with host as web\_application, and look at the productid field. This field is just a number, but we want product names to be reflected in our query result set. We create a lookup file with the following details. Here, we have kept the name of the first field as **productid** which is same as the field we are going to use from the dataset.

productId,productdescription

WC-SH-G04,Tablets

DB-SG-G01,PCs

DC-SG-G02,MobilePhones

SC-MG-G10,Wearables

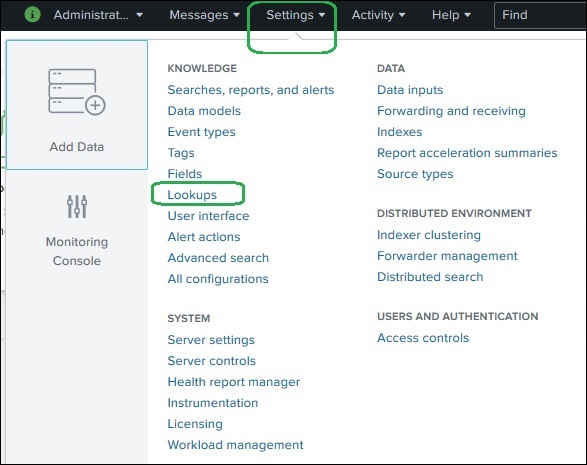
WSC-MG-G10,Usb Light

GT-SC-G01,Battery

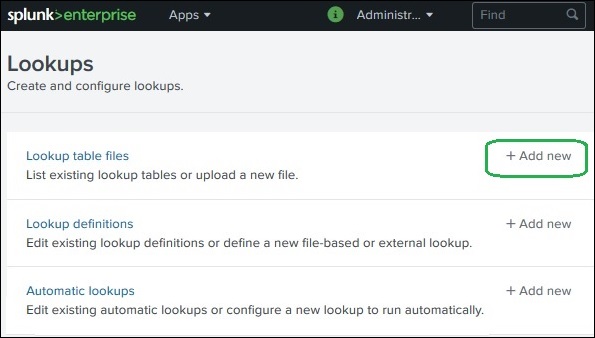
SF-BVS-G01,Hard Drive

### **Add the Lookup File**

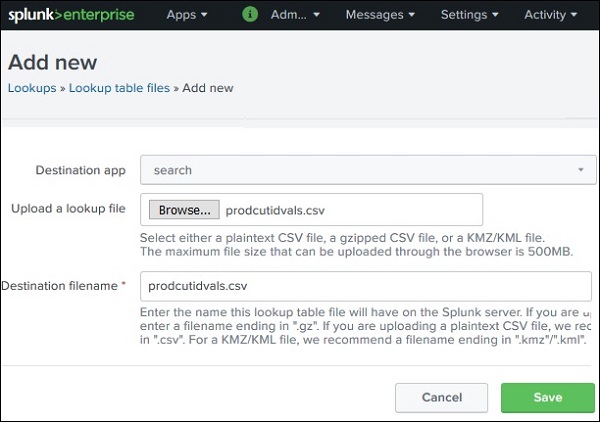
Next, we add the lookup file to Splunk environment by using the Settings screens as shown below −



After selecting the Lookups, we are presented with a screen to create and configure lookup. We select lookup table files as shown below.



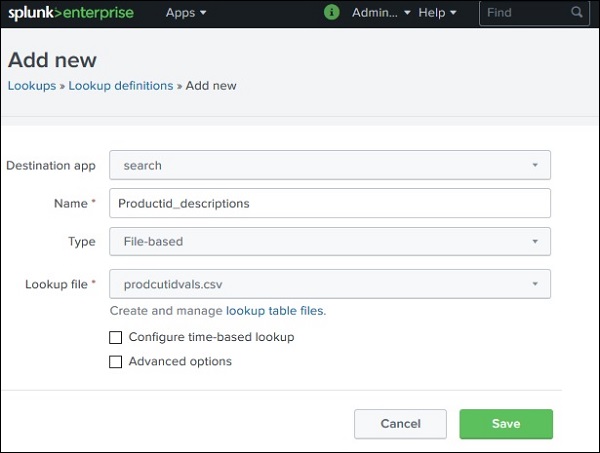
We browse to select the file **productidvals.csv** as our lookup file to be uploaded and select search as our destination app. We also keep the same destination file name.



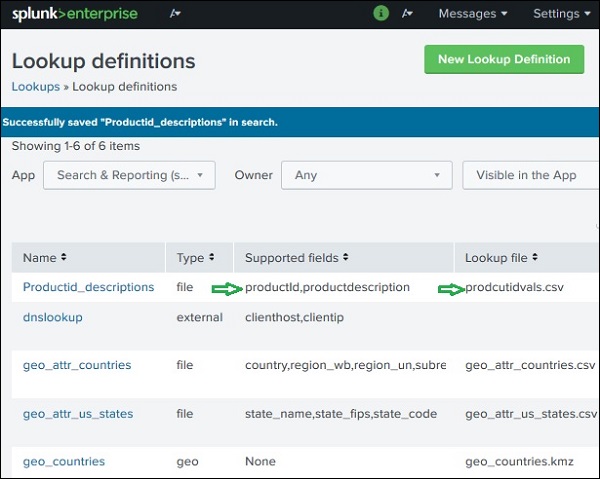
On clicking the save button, the file gets saved to the Splunk repository as a lookup file.

### **Create Lookup Definitions**

For a search query to be able to lookup values from the Lookup file we just uploaded above, we need to create a lookup definition. We do this by again going to **Settings → Lookups → Lookup Definition → Add New**.

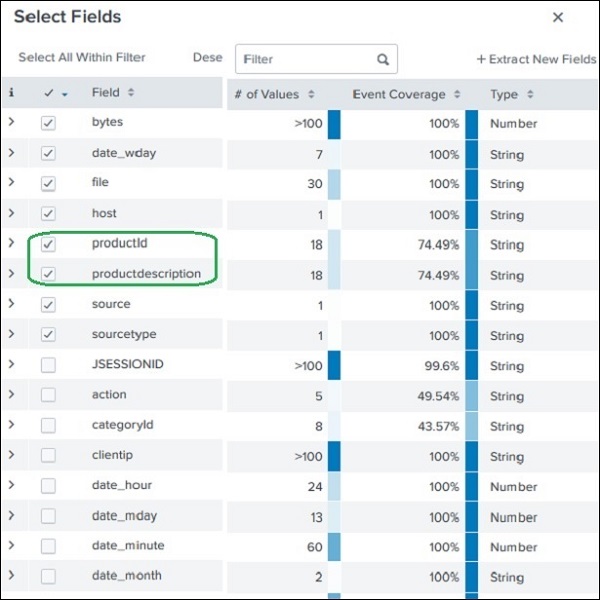


Next, we check the availability of the lookup definition we added by going to **Settings → Lookups → Lookup Definition**.



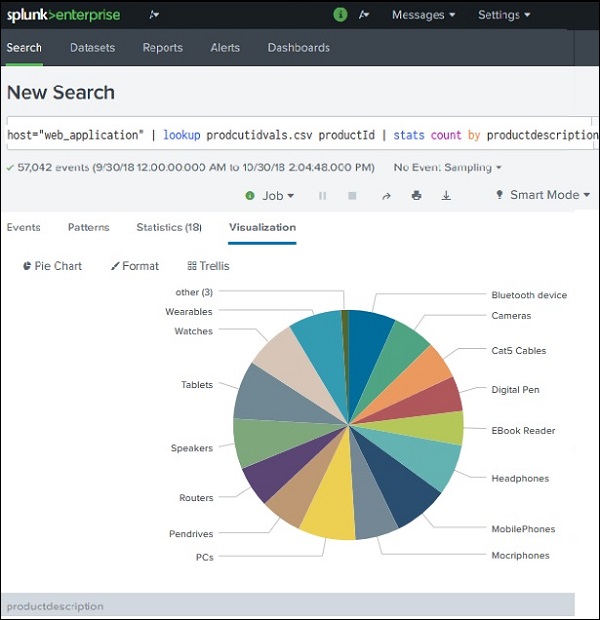
### **Selecting Lookup Field**

Next, we need to select the lookup field for our search query. This is done my going to **New search → All Fields**. Then check the box for **productid** which will automatically add the **productdescription** field from the lookup file also.



### **Using the Lookup Field**

Now we use the Lookup field in the search query as shown below. The visualization shows the result with productdescription field instead of productid.



Print Page

[Previous](https://www.tutorialspoint.com/splunk/splunk_pivot_and_datasets.htm)

<https://www.tutorialspoint.com/splunk/splunk_lookups.htm>

[Next](https://www.tutorialspoint.com/splunk/splunk_schedules_and_alerts.htm)

Advertisements