Enabling Lookup Fields

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

There are five key steps to enabling fields lookups:

1. Upload the lookup file
2. Share the uploaded file with the applications
3. Create a lookup definition and specify permissions
4. Share the lookup definition
5. Optional. Make the lookup definition automatic

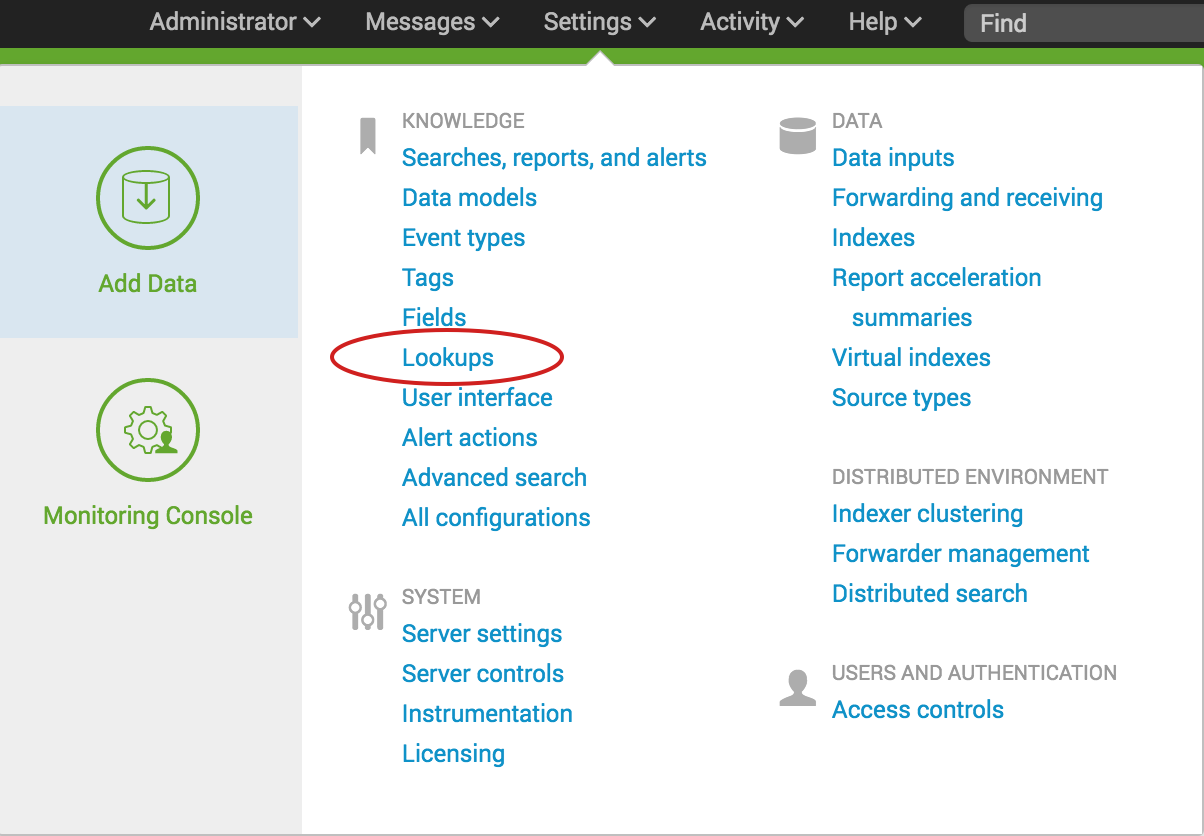
Uncompressed the Prices.csv.zip file.

The prices.csv files contains the product names, price, and code. For example:

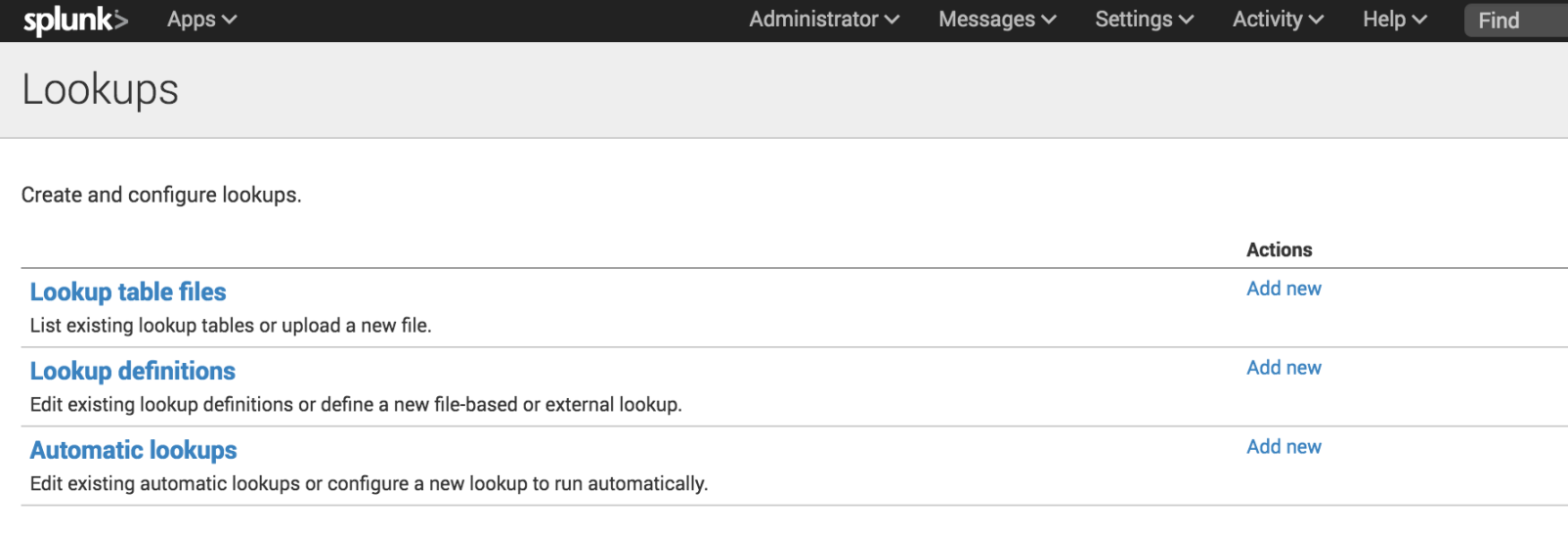
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **productId** | **product\_name** | **price** | **sale\_price** | **Code** |
| DB-SG-G01 | Mediocre Kingdoms | 24.99 | 19.99 | A |
| DC-SG-G02 | Dream Crusher | 39.99 | 24.99 | B |
| FS-SG-G03 | Final Sequel | 24.99 | 16.99 | C |
| WC-SH-G04 | World of Cheese | 24.99 | 19.99 | D |

Find the Lookups manager

1. In the Splunk bar, click **Settings**.
2. In the **Knowledge** section, click **Lookups**.

[](http://docs.splunk.com/File:6.5.0_tutorial_settings_lookups.png)

The Lookups manager opens, where you can create new lookups or edit existing lookups.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupsmanager.png)

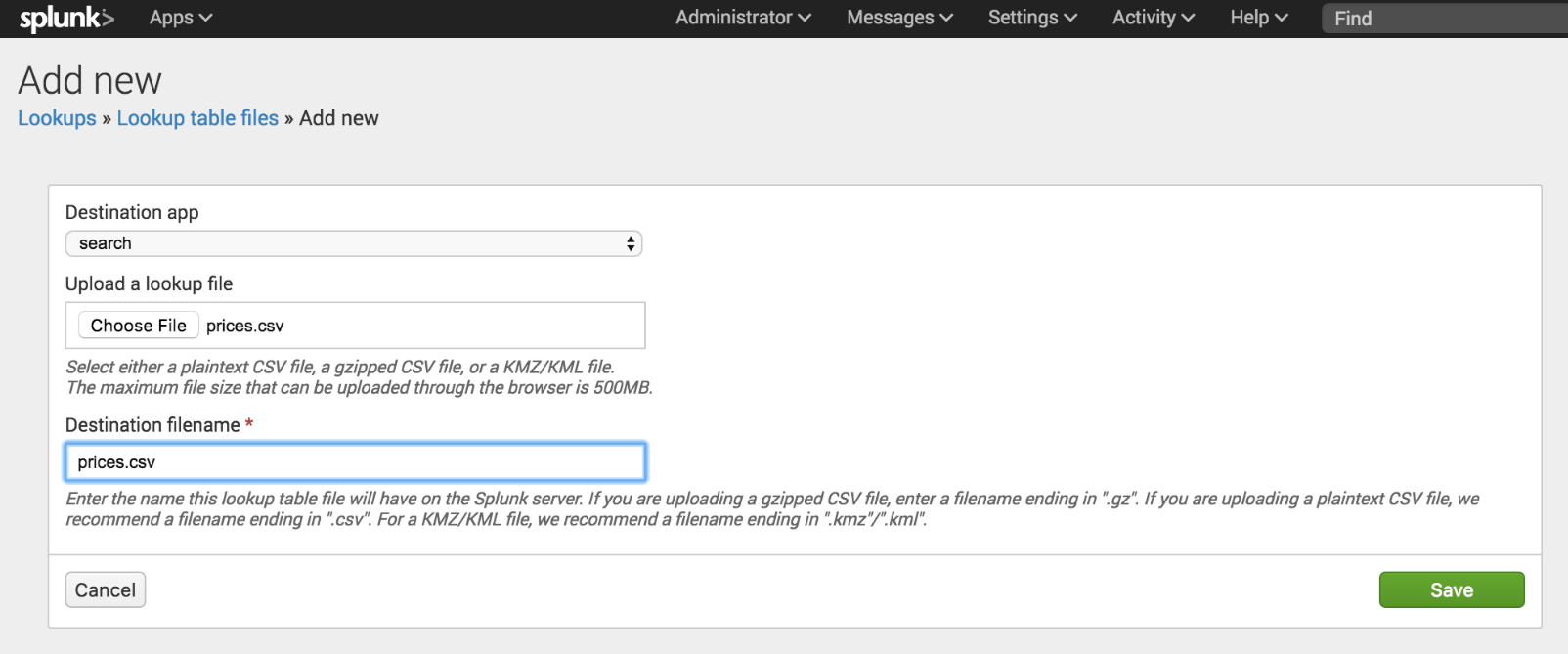
You can view and edit existing lookups by clicking on the links in the Lookups manager. In the next few sections of this tutorial, you will upload lookup table files, create lookup definitions, and create automatic lookups.

Upload the lookup table file

To use a lookup table file, you must upload the file to your Splunk platform.

1. In the Lookups manager, locate **Lookup table files**.
2. In the Actions column click **Add new**.

You use the **Add new** lookup table files view to upload CSV files that you want to use.

[](http://docs.splunk.com/File:6.5.0_tutorial_addnewlookuptable.png)

1. The **Destination app** field specifies which app you want to upload the lookup table file to. To upload the file in the Search app, you do not need to change anything. The default value is **search**.
2. Under **Upload a lookup file**, click **Choose File** and browse for the **prices.csv** file.
3. Under **Destination filename**, type **prices.csv**.

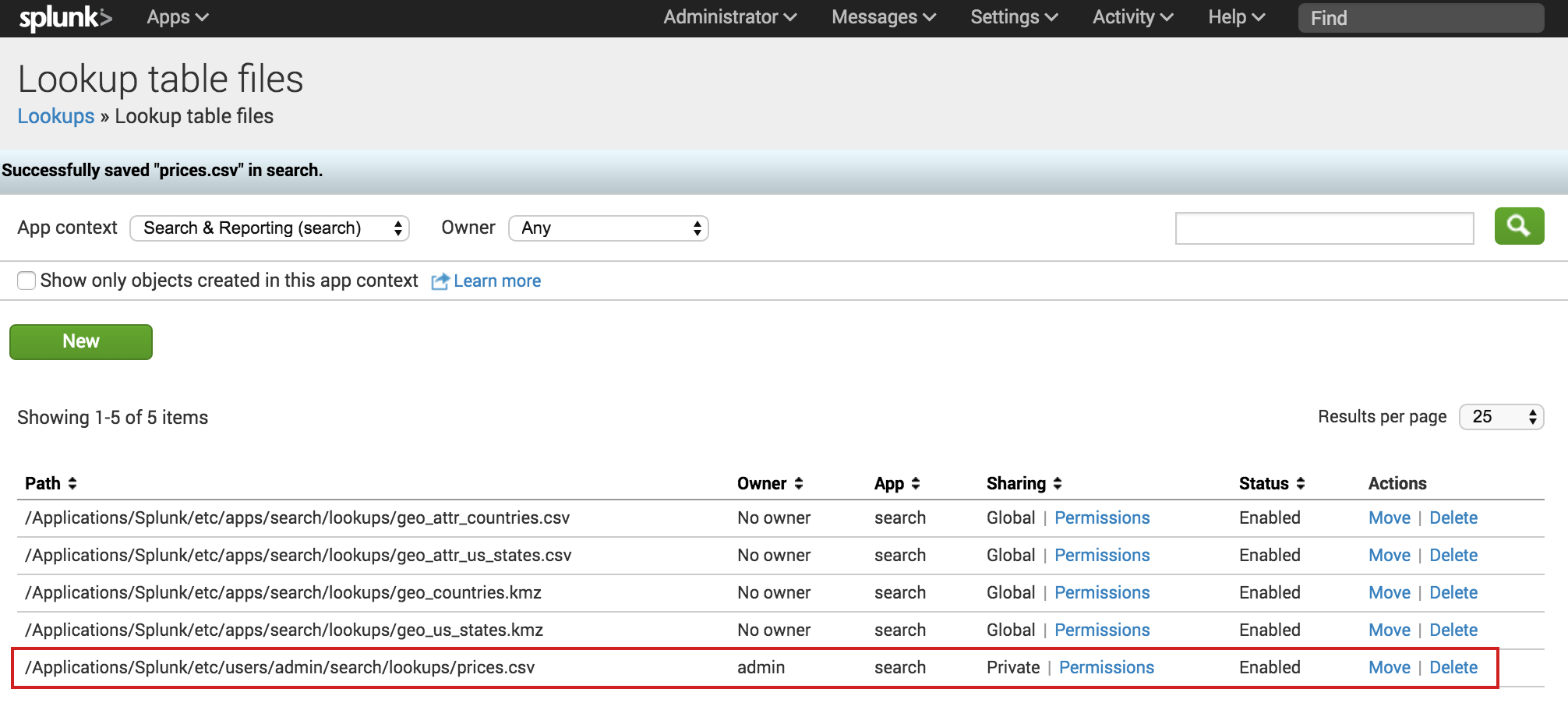
This is the name that you will use to refer to the file when you create a lookup definition.

1. Click **Save**.

This uploads your lookup file to the Search app and displays the lookup table files list.

If the Splunk software does not recognize or cannot upload the file, you can take the following actions.

* Check that the file is uncompressed.
* If an error message indicates that the file does not have line breaks, the file has become corrupted. This can happen if the file is opened in Microsoft Excel before it is uploaded. You should delete the Prices.csv.zip and prices.csv files. Then download the ZIP file again, and uncompress the file.

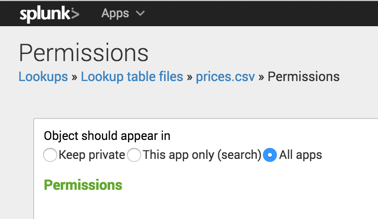
[](http://docs.splunk.com/File:6.5.0_tutorial_lookuptablefiles.png)

The other lookup table files in the list are included with the Splunk software.

Share the lookup table file

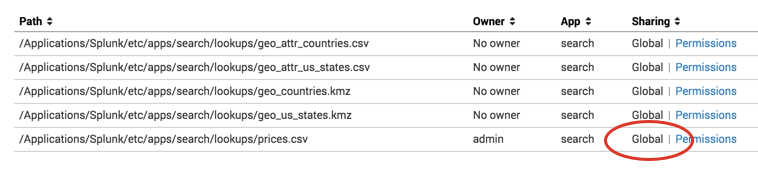
Now that the lookup table file is uploaded, you need tell the Splunk software which applications can use this file. You can share the lookup table file with the Search app or with all of the apps.

1. In the **Lookup table files** list, locate the prices.csv file at the bottom of the **Path** list.
2. In the **Sharing** column, notice that prices.csv is listed as **Private**.
3. To share the lookup table file, click **Permissions**.
4. In the Permissions dialog box, under **Object should appear in**, select **All apps**.

[](http://docs.splunk.com/File:6.4_tutorial_lookuptablepermissions.png)

1. Click **Save**.

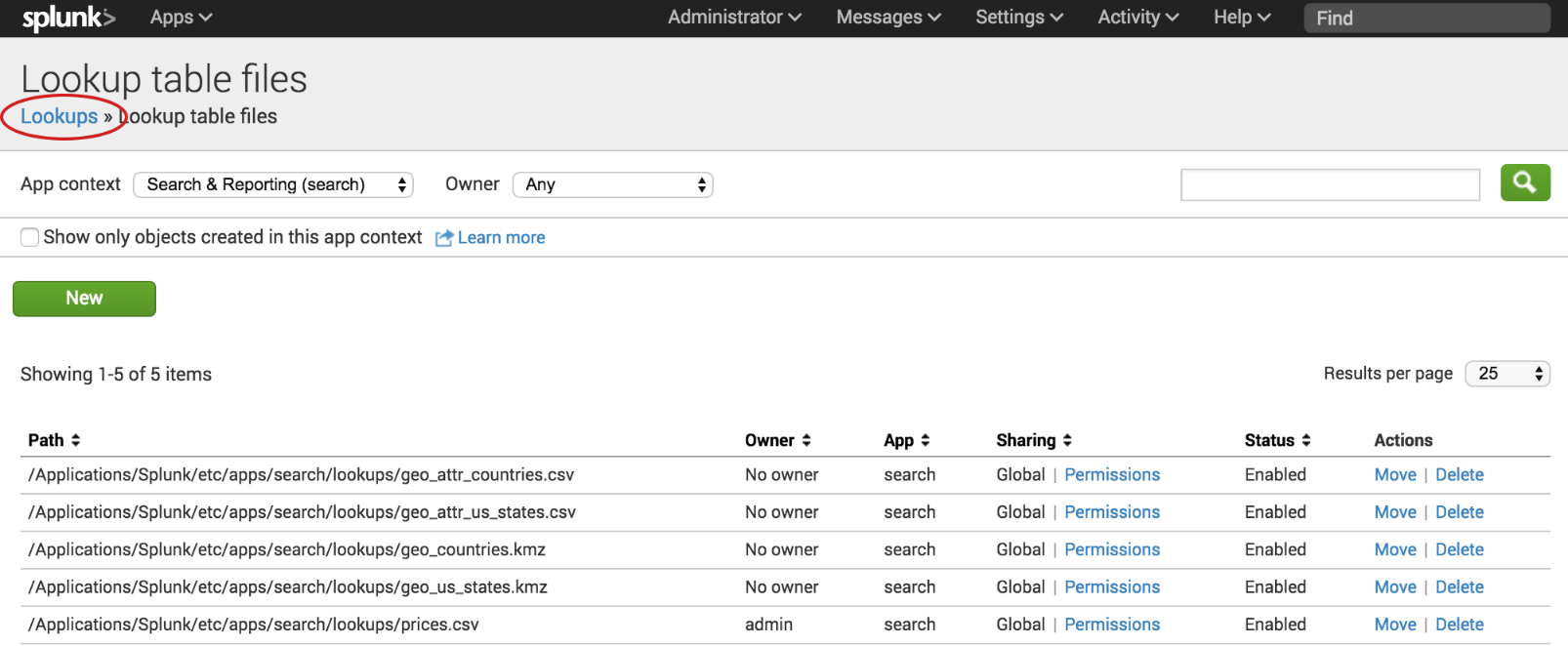
The Sharing setting for the prices.csv lookup table is set to **Global**.

[](http://docs.splunk.com/File:6.4_tutorial_lookuptableglobal.png)

Add the field lookup definition

It is not sufficient to share the lookup table file with an application. You must create a lookup definition from the lookup table file.

1. In the Lookup table file dialog box, select **Lookups** in the breadcrumbs to return to the Lookups manager.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupfilebreadcrumbs.png)

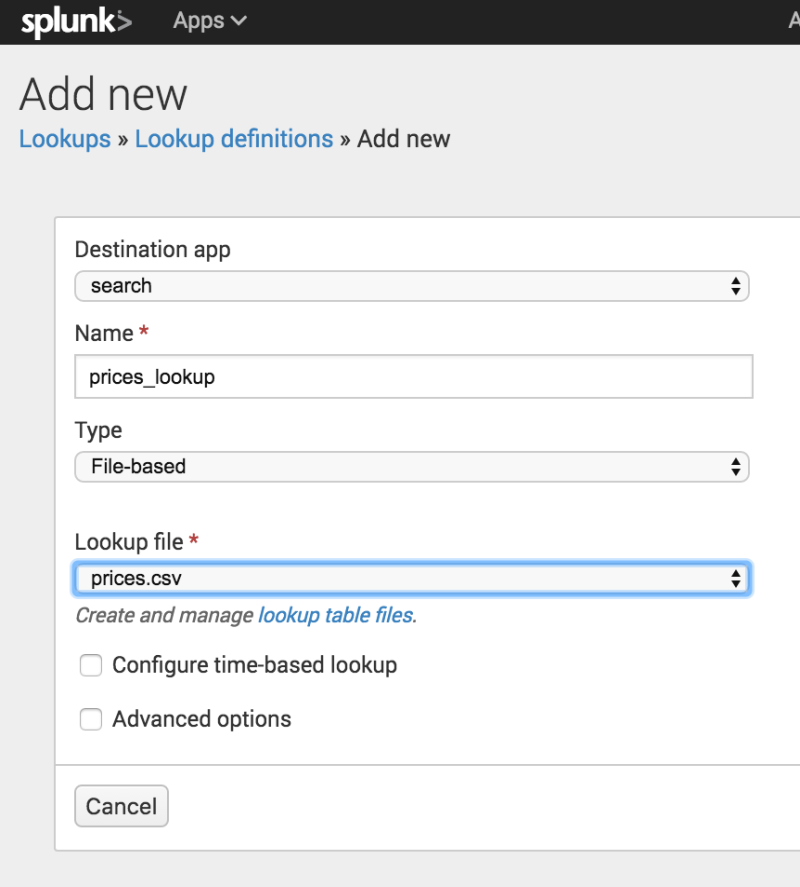
1. For **Lookup definitions**, click **Add New**.

The Add new lookups definitions page opens, where you define the field lookup.

1. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
2. For **Name**, type **prices\_lookup**.
3. For **Type**, select **File-based**.

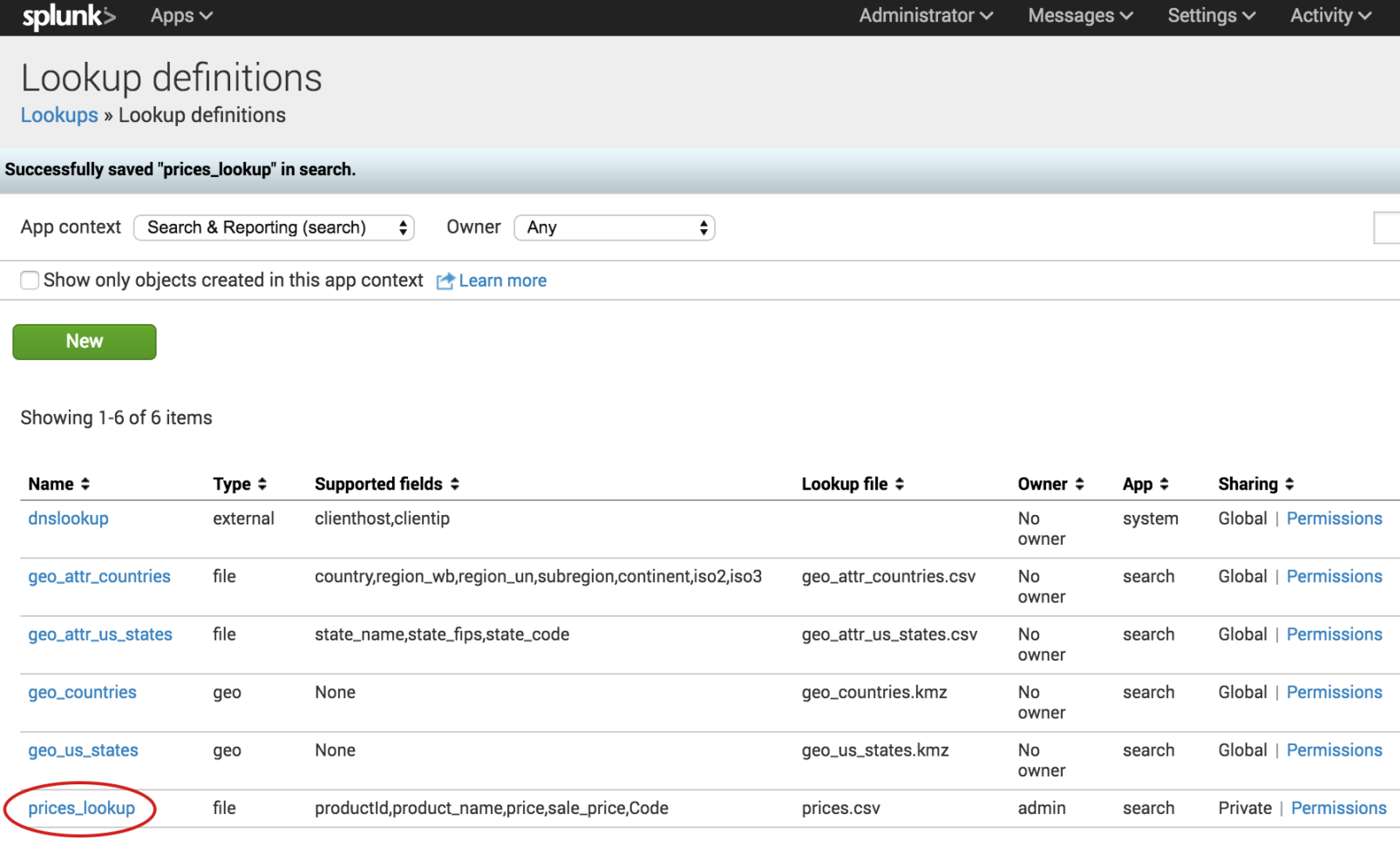
A file-based lookup is typically a static table, such as a CSV file.

1. For **Lookup file**, select **prices.csv**, which is the name of the lookup table file that you created.

[](http://docs.splunk.com/File:6.5.0_tutorial_newlookupdefinition.png)

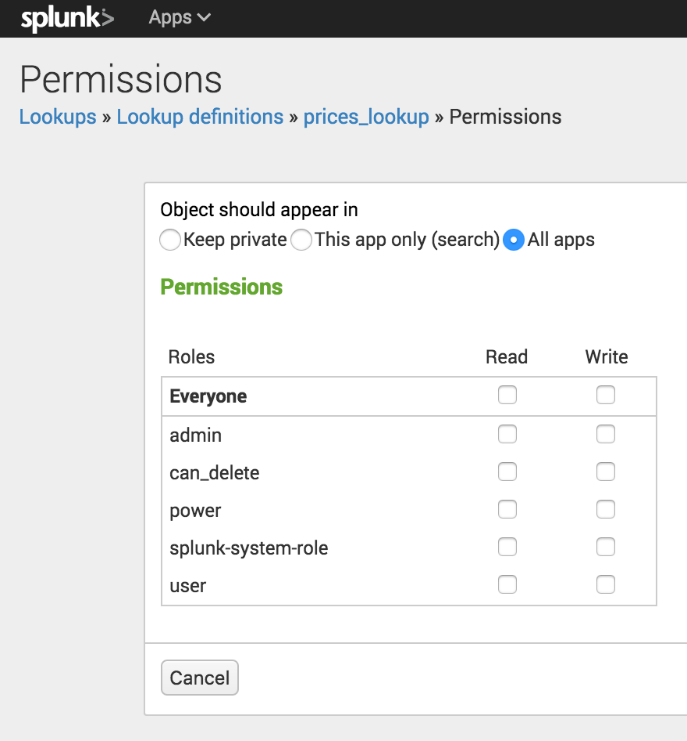
1. For **Configure time-based lookup** and **Advanced options**, leave the check boxes unselected.
2. Click **Save**.

The **prices\_lookup** is now defined as a file-based lookup.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupdefinitionsaved.png)

Share the lookup definition with all apps

1. Now that you have created the lookup definition, you need to specify in which apps you want to use the definition.
2. In the Lookup definitions list, for the prices\_lookup, click **Permissions**.
3. In the Permissions dialog box, under **Object should appear in**, select **All apps**.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupdefinitionspermissions.png)

1. Click **Save**.

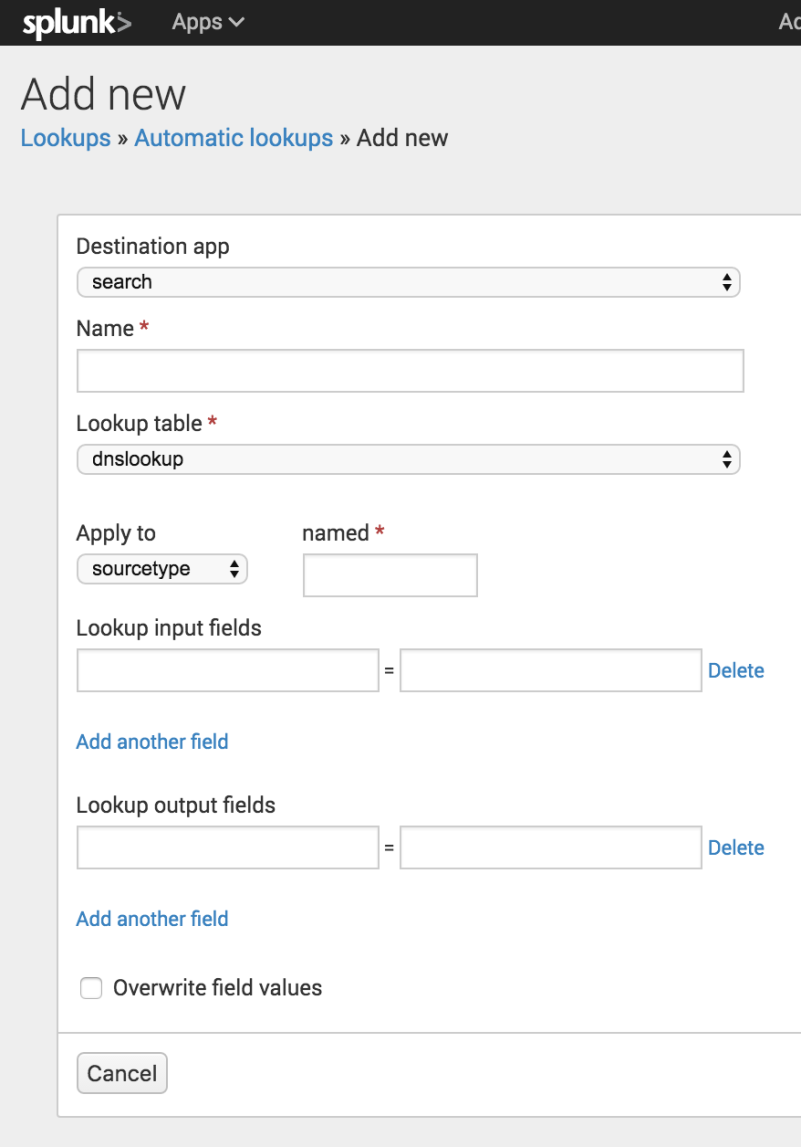
In the Lookup definitions page, prices\_lookup now has **Global** permissions.

You can use this field lookup to add information from the lookup table file to your events. You use the field lookup by specifying the lookup command in a search string. Or, you can set the field lookup to run automatically.

Make the lookup automatic

Instead of using the lookup command in your search when you want to apply a field lookup to your events, you can set the lookup to run automatically.

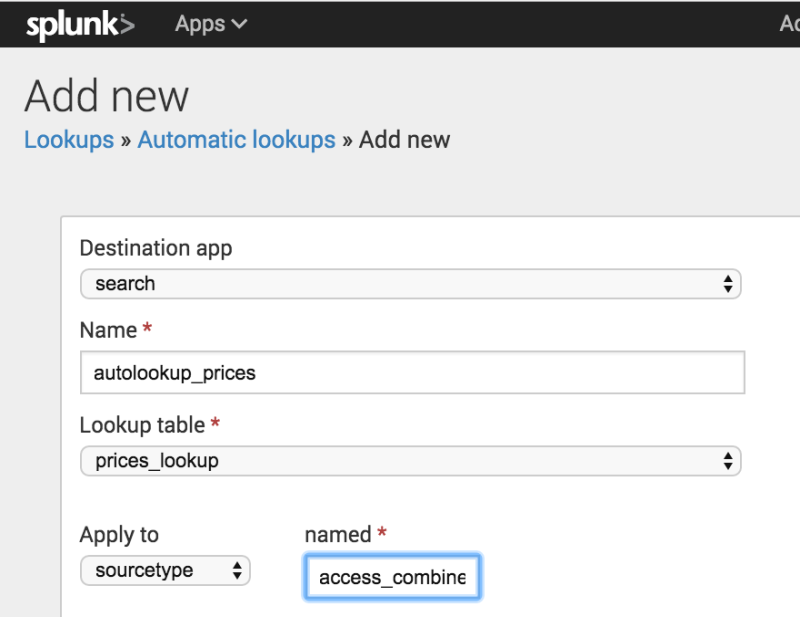
1. In the Lookups manager, for Automatic lookups, click Add New.
2. This takes you to the Add new automatic lookups view, where you configure the lookup to run automatically.

[](http://docs.splunk.com/File:6.5.0_tutorial_newautomaticlookups.png)

1. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
2. For **Name**, type **autolookup\_prices**.
3. For **Lookup table**, select **prices\_lookup**.

The other options are lookups that are based on the lookup table files that come with the product.

1. For **Apply to**, the value **sourcetype** is already selected. For **named**, type **access\_combined\_wcookie**.

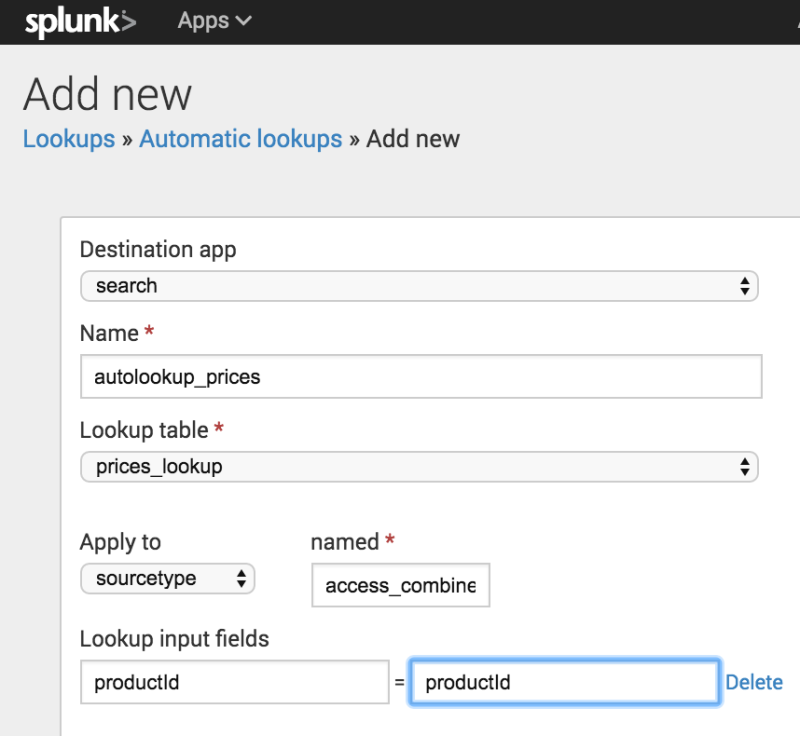
[](http://docs.splunk.com/File:6.5.0_tutorial_autolookup_sourcetype.png)

1. For **Lookup input fields**, type **productId** in both text boxes.

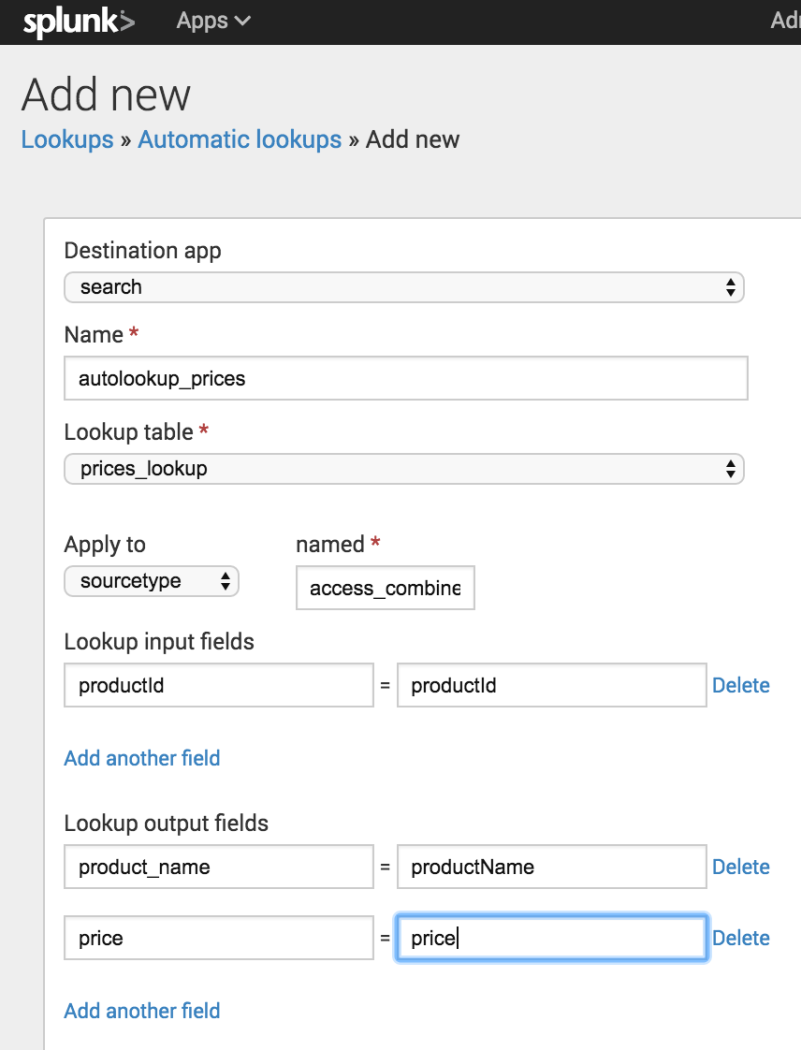
The lookup input fields are where you associate values from the lookup table file with values in your events.

* + The first text box specifies the value in the lookup table file.
  + The second text box specifies the value in your events.

The lookup table file has a **productId** column that contains values that match the values in the **productId** field in the events.

[](http://docs.splunk.com/File:6.5.0_tutorial_autolookupinputfields.png)

1. For **Lookup output fields**, specify the names of the fields from the lookup table file that you want to add to your event data. You can specify different names. The lookup table file has several fields. You will specify two of the fields to appear in your events.
   * In the first text box, type **product\_name**. This is the field in the prices.csv file that contains the descriptive name for each productId.
   * In the second text box, after the equal sign, type **productName**. This is the name of the field that will appear in your events for the descriptive name of the product.
   * Click **Add another field** to add another field after the first one.
   * Type **price** in the first text box. This is the field in the prices.csv file that contains the price for each productId. Let's use the same name for the field that will appear in your events. Type **price** in the second text box.

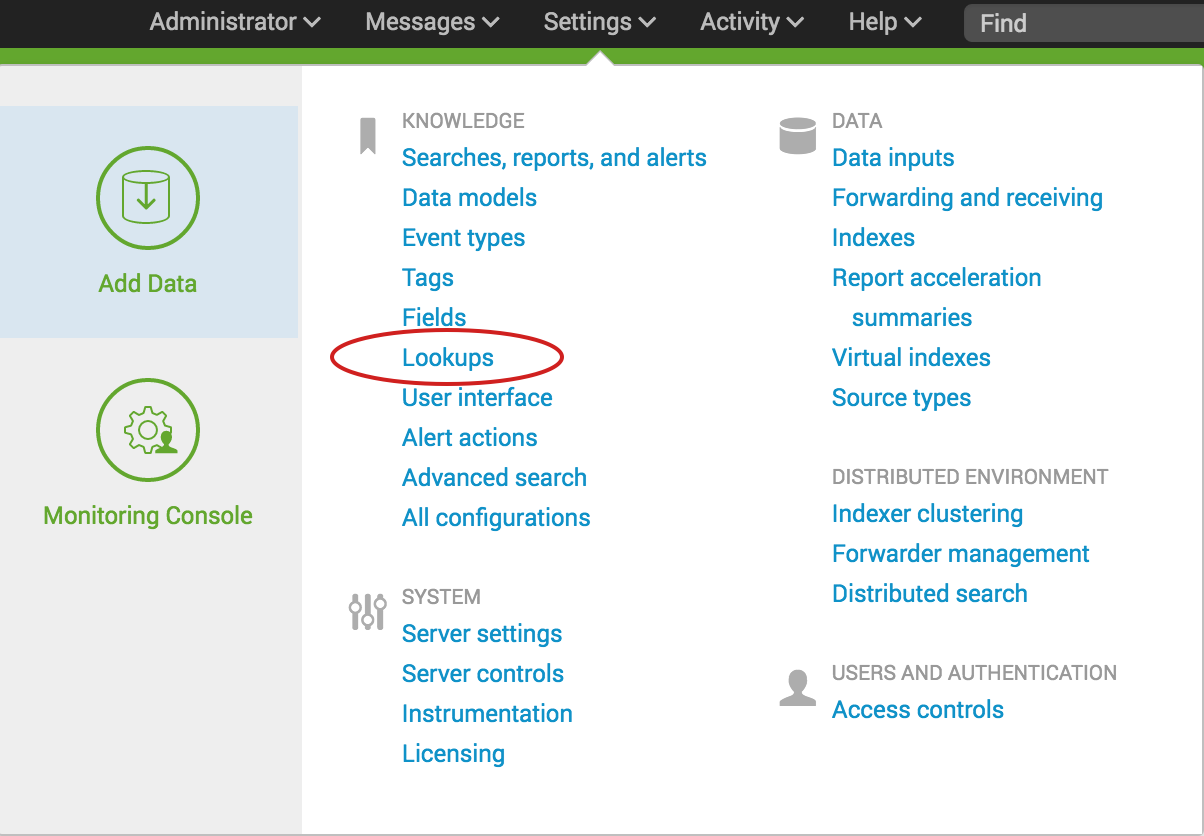
[](http://docs.splunk.com/File:6.5.0_tutorial_autolookupoutputfields.png)

1. Keep **Overwrite field values** unchecked.
2. Click **Save**.

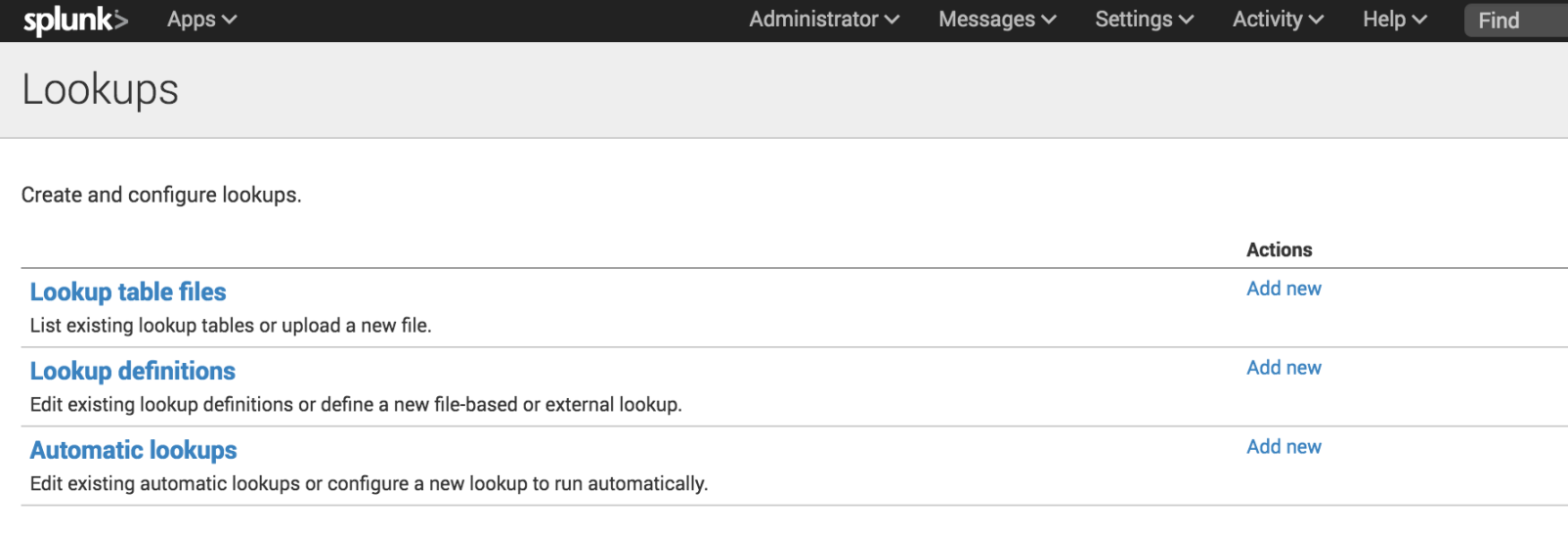
The Automatic lookup view appears and the lookup that you configured, autolookup\_prices, is in the list. The full name is **access\_combined\_wcookie : LOOKUP-autolookup\_prices**.

Find the Lookups manager

1. In the Splunk bar, click **Settings**.
2. In the **Knowledge** section, click **Lookups**.

[](http://docs.splunk.com/File:6.5.0_tutorial_settings_lookups.png)

The Lookups manager opens, where you can create new lookups or edit existing lookups.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupsmanager.png)

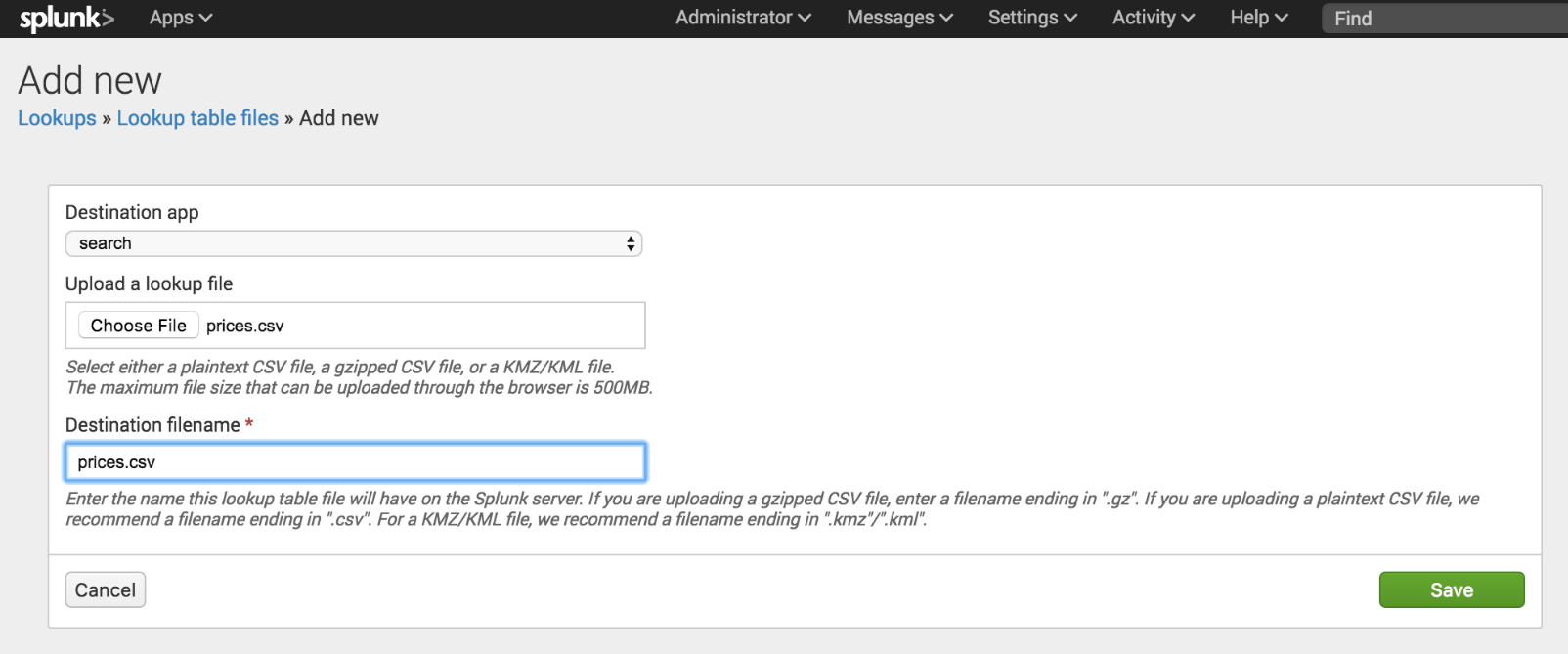
You can view and edit existing lookups by clicking on the links in the Lookups manager. In the next few sections of this tutorial, you will upload lookup table files, create lookup definitions, and create automatic lookups.

Upload the lookup table file

To use a lookup table file, you must upload the file to your Splunk platform.

1. In the Lookups manager, locate **Lookup table files**.
2. In the Actions column click **Add new**.

You use the **Add new** lookup table files view to upload CSV files that you want to use.

[](http://docs.splunk.com/File:6.5.0_tutorial_addnewlookuptable.png)

1. The **Destination app** field specifies which app you want to upload the lookup table file to. To upload the file in the Search app, you do not need to change anything. The default value is **search**.
2. Under **Upload a lookup file**, click **Choose File** and browse for the **prices.csv** file.
3. Under **Destination filename**, type **prices.csv**.

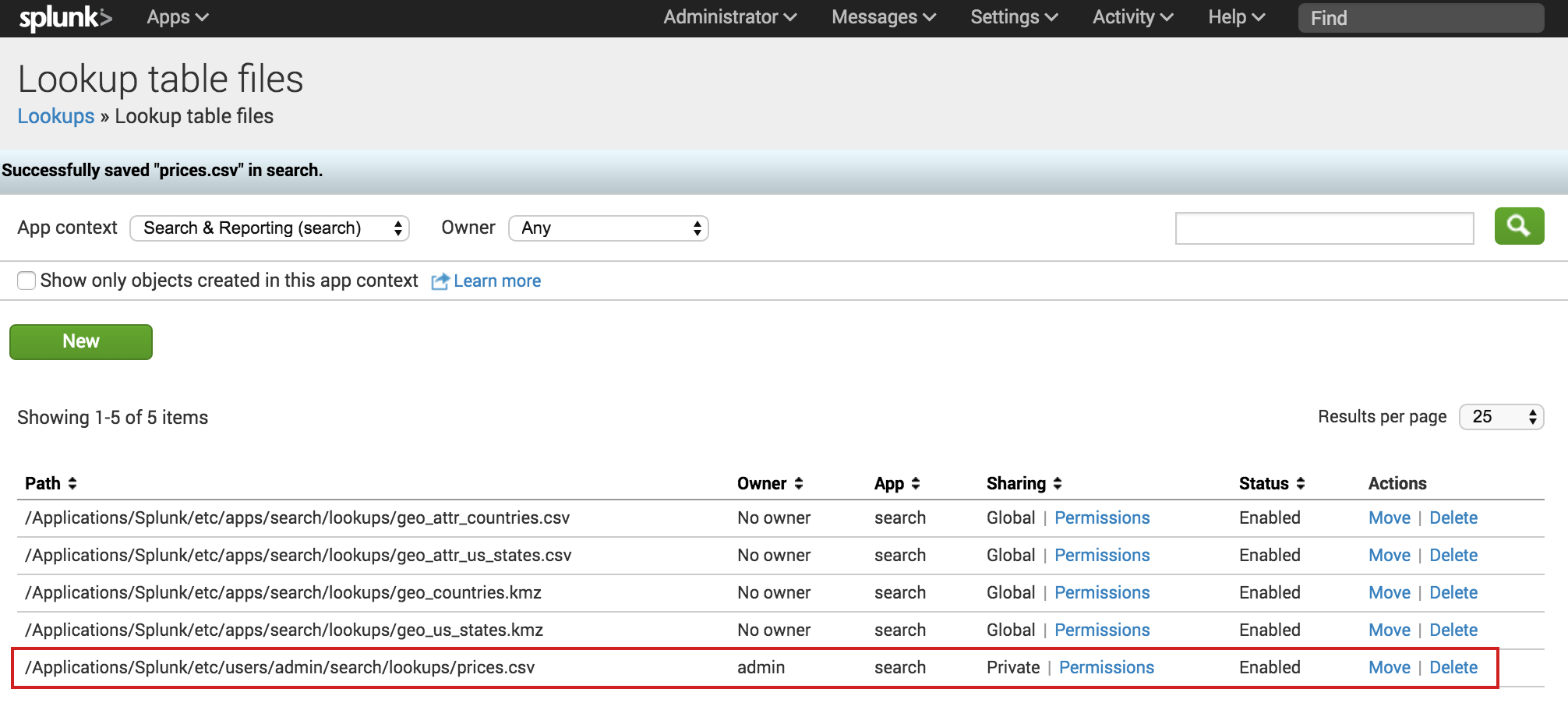
This is the name that you will use to refer to the file when you create a lookup definition.

1. Click **Save**.

This uploads your lookup file to the Search app and displays the lookup table files list.

If the Splunk software does not recognize or cannot upload the file, you can take the following actions.

* Check that the file is uncompressed.
* If an error message indicates that the file does not have line breaks, the file has become corrupted. This can happen if the file is opened in Microsoft Excel before it is uploaded. You should delete the Prices.csv.zip and prices.csv files. Then download the ZIP file again, and uncompress the file.

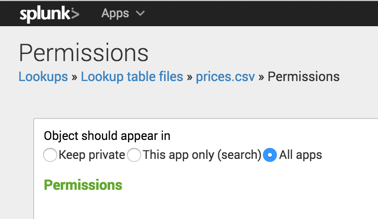
[](http://docs.splunk.com/File:6.5.0_tutorial_lookuptablefiles.png)

The other lookup table files in the list are included with the Splunk software.

Share the lookup table file

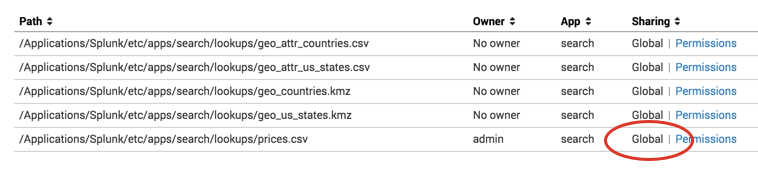
Now that the lookup table file is uploaded, you need tell the Splunk software which applications can use this file. You can share the lookup table file with the Search app or with all of the apps.

1. In the **Lookup table files** list, locate the prices.csv file at the bottom of the **Path** list.
2. In the **Sharing** column, notice that prices.csv is listed as **Private**.
3. To share the lookup table file, click **Permissions**.
4. In the Permissions dialog box, under **Object should appear in**, select **All apps**.

[](http://docs.splunk.com/File:6.4_tutorial_lookuptablepermissions.png)

1. Click **Save**.

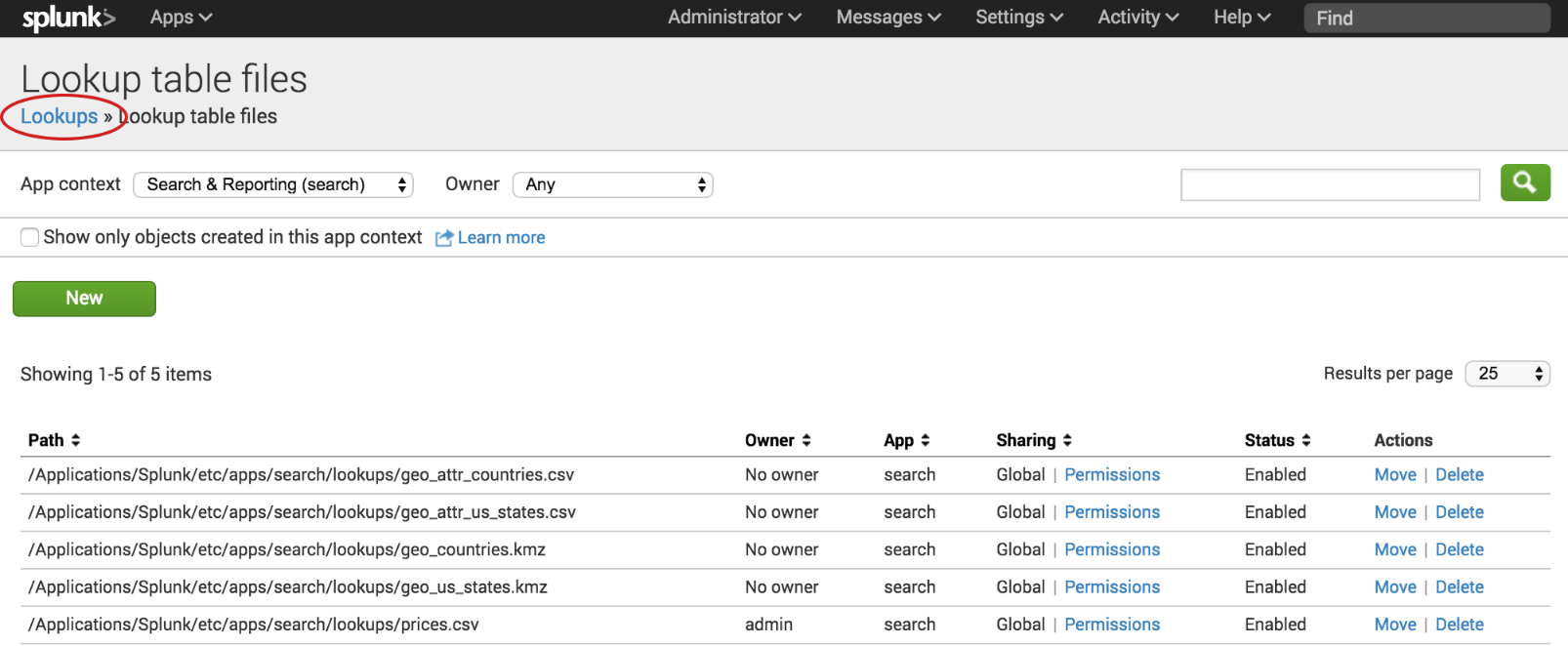
The Sharing setting for the prices.csv lookup table is set to **Global**.

[](http://docs.splunk.com/File:6.4_tutorial_lookuptableglobal.png)

Add the field lookup definition

It is not sufficient to share the lookup table file with an application. You must create a lookup definition from the lookup table file.

1. In the Lookup table file dialog box, select **Lookups** in the breadcrumbs to return to the Lookups manager.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupfilebreadcrumbs.png)

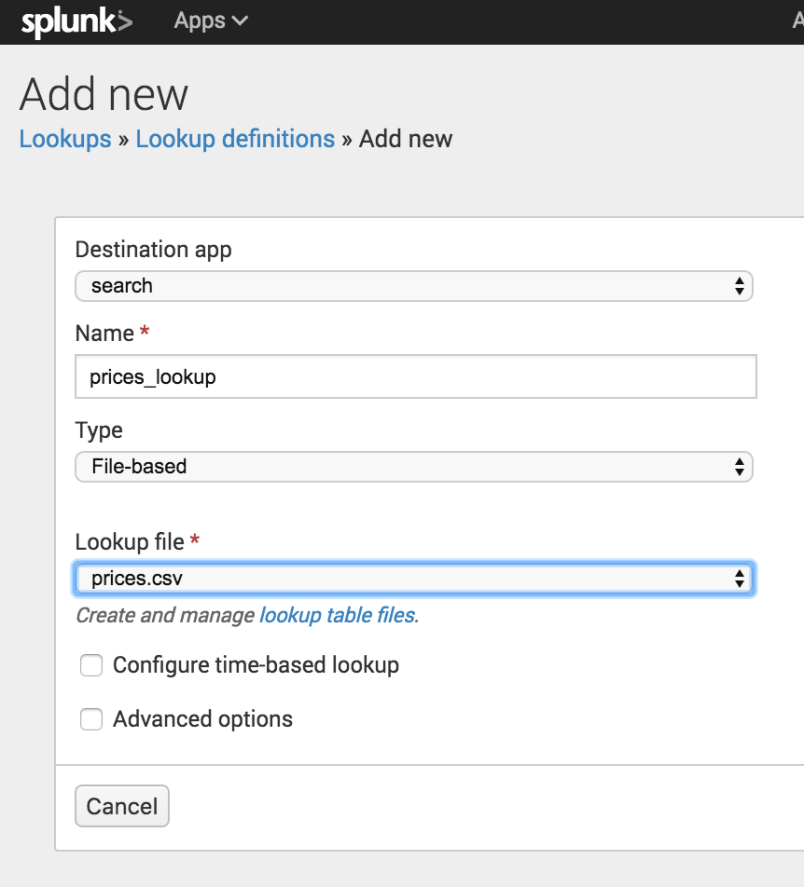
1. For **Lookup definitions**, click **Add New**.

The Add new lookups definitions page opens, where you define the field lookup.

1. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
2. For **Name**, type **prices\_lookup**.
3. For **Type**, select **File-based**.

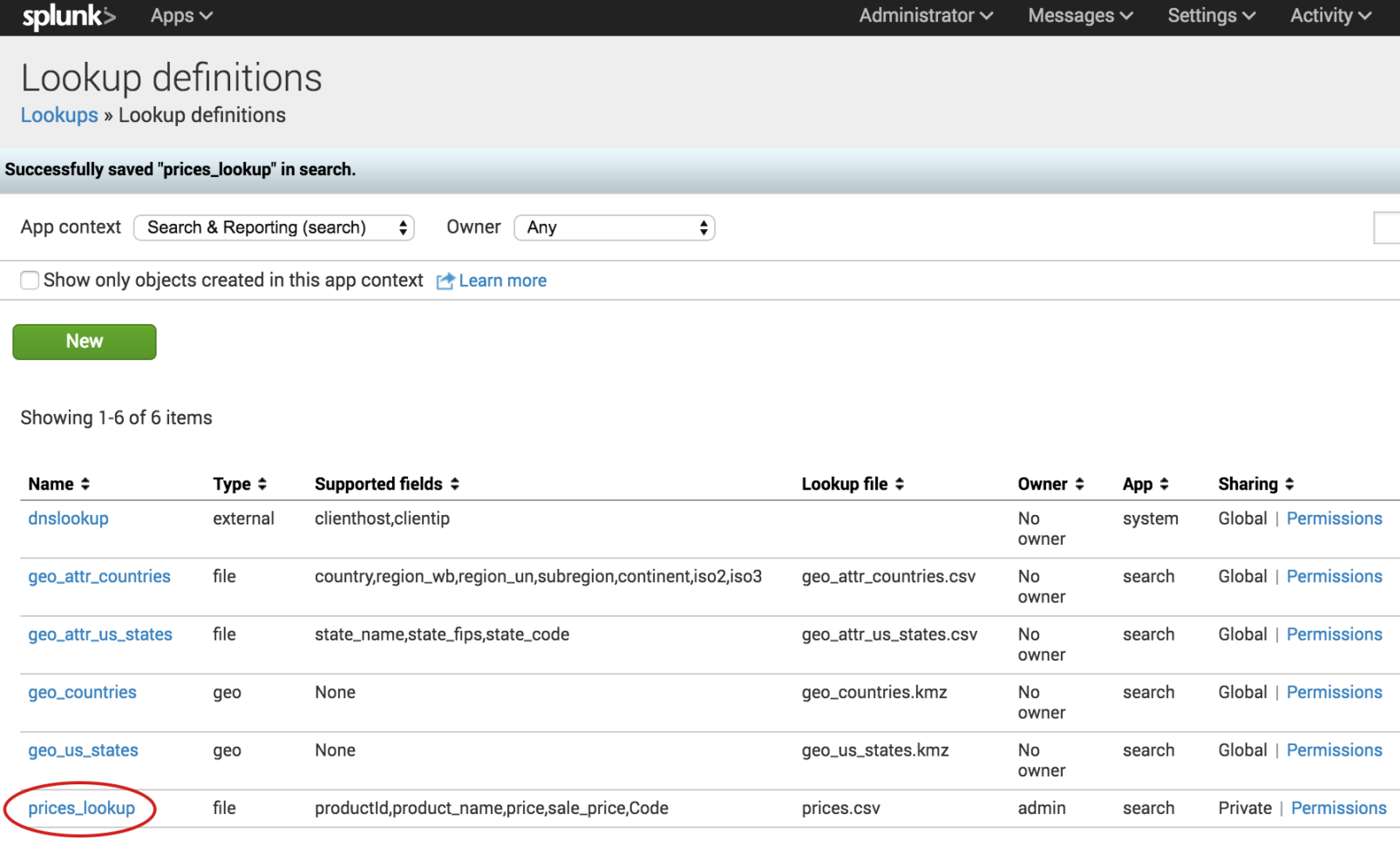
A file-based lookup is typically a static table, such as a CSV file.

1. For **Lookup file**, select **prices.csv**, which is the name of the lookup table file that you created.

[](http://docs.splunk.com/File:6.5.0_tutorial_newlookupdefinition.png)

1. For **Configure time-based lookup** and **Advanced options**, leave the check boxes unselected.
2. Click **Save**.

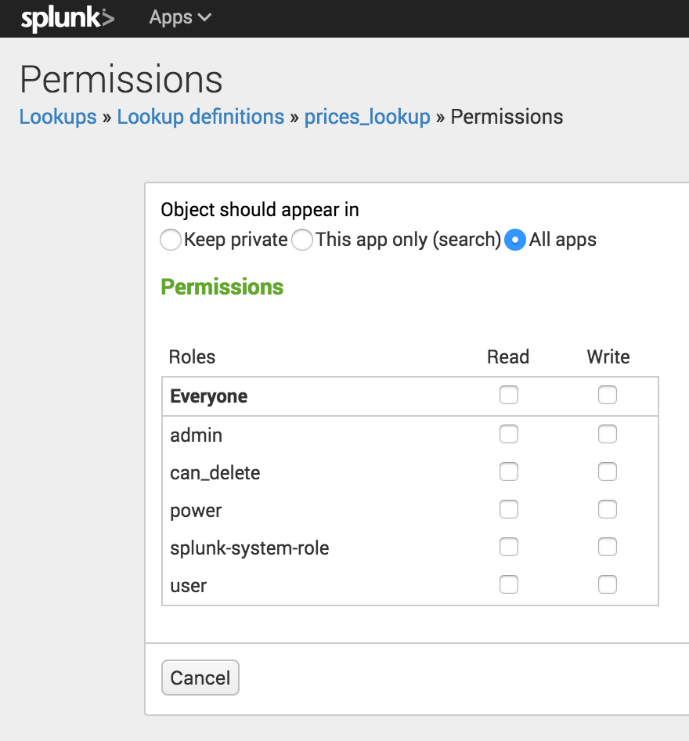
The **prices\_lookup** is now defined as a file-based lookup.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupdefinitionsaved.png)

Share the lookup definition with all apps

Now that you have created the lookup definition, you need to specify in which apps you want to use the definition.

1. In the Lookup definitions list, for the prices\_lookup, click **Permissions**.
2. In the Permissions dialog box, under **Object should appear in**, select **All apps**.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookupdefinitionspermissions.png)

1. Click **Save**.

In the Lookup definitions page, prices\_lookup now has **Global** permissions.

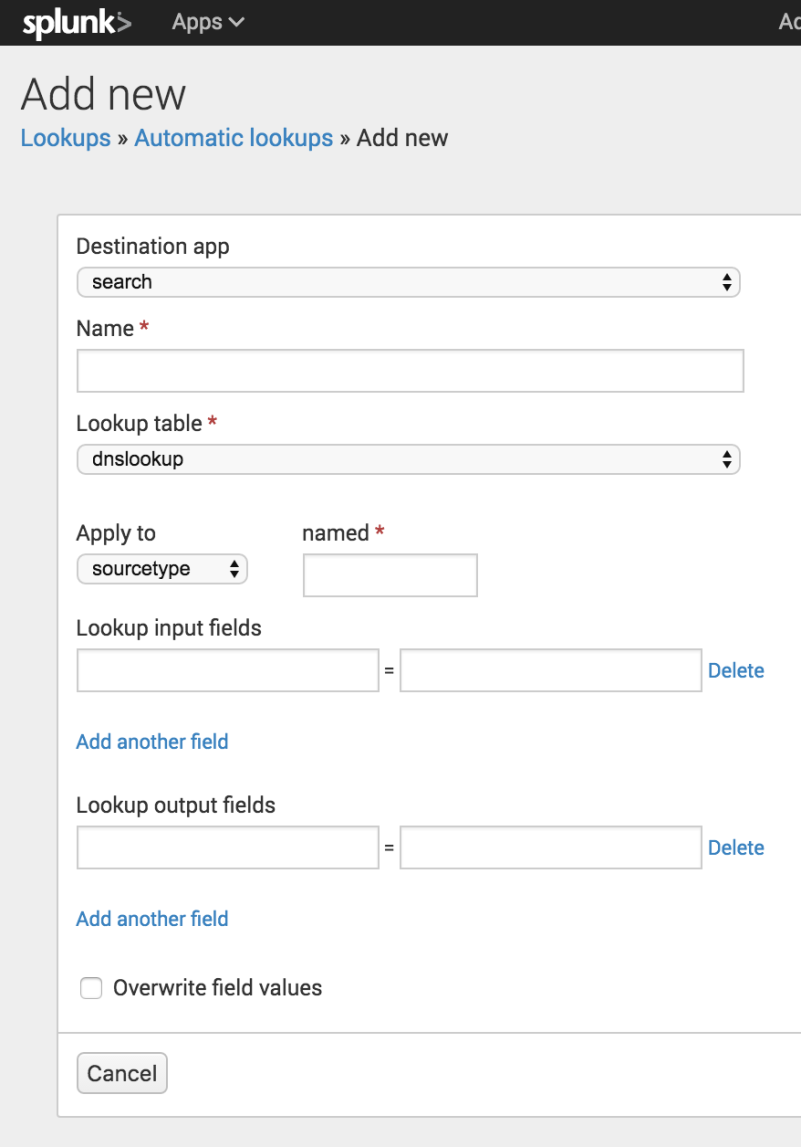
You can use this field lookup to add information from the lookup table file to your events. You use the field lookup by specifying the lookup command in a search string. Or, you can set the field lookup to run automatically.

Make the lookup automatic

Instead of using the lookup command in your search when you want to apply a field lookup to your events, you can set the lookup to run automatically.

1. In the Lookups manager, for **Automatic lookups**, click **Add New**.

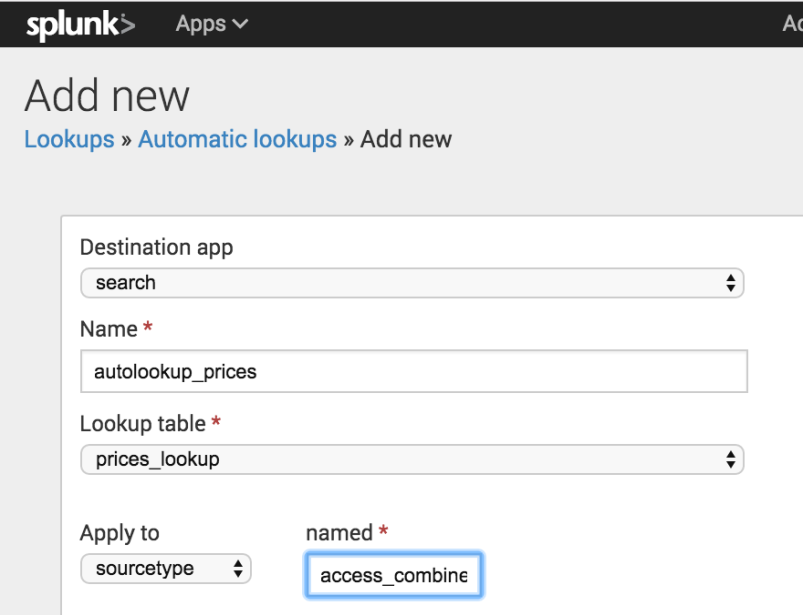
This takes you to the Add new automatic lookups view, where you configure the lookup to run automatically.

[](http://docs.splunk.com/File:6.5.0_tutorial_newautomaticlookups.png)

1. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
2. For **Name**, type **autolookup\_prices**.
3. For **Lookup table**, select **prices\_lookup**.

The other options are lookups that are based on the lookup table files that come with the product.

1. For **Apply to**, the value **sourcetype** is already selected. For **named**, type **access\_combined\_wcookie**.

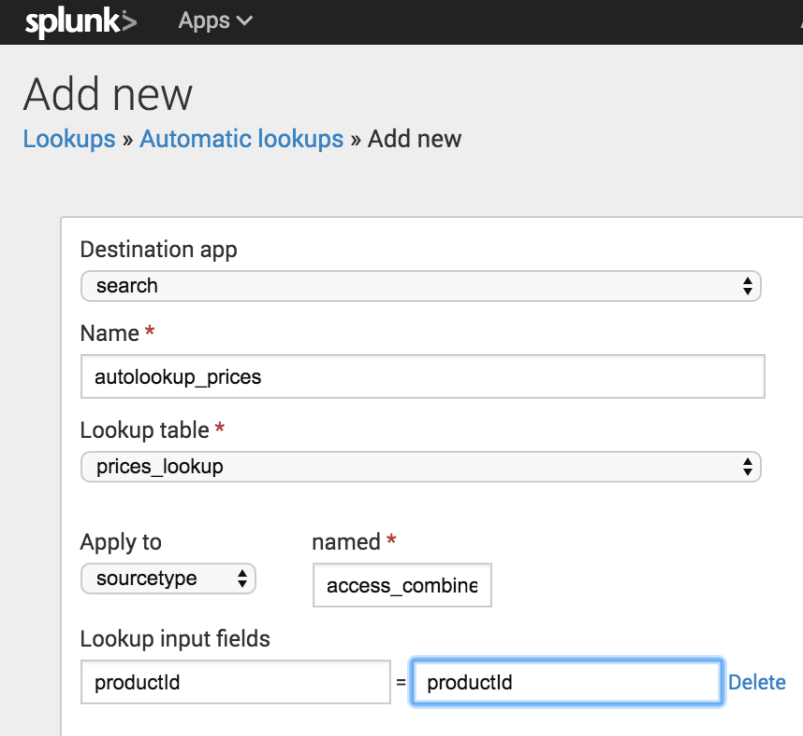
[](http://docs.splunk.com/File:6.5.0_tutorial_autolookup_sourcetype.png)

1. For **Lookup input fields**, type **productId** in both text boxes.

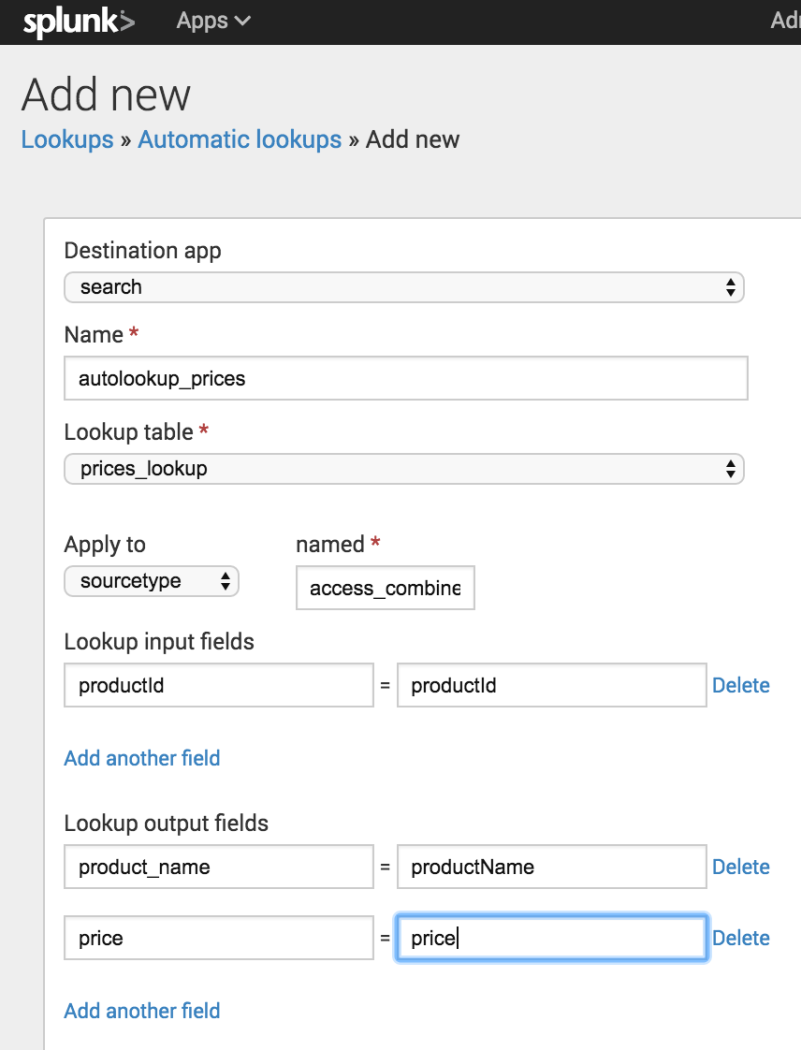
The lookup input fields are where you associate values from the lookup table file with values in your events.

* + The first text box specifies the value in the lookup table file.
  + The second text box specifies the value in your events.

The lookup table file has a **productId** column that contains values that match the values in the **productId** field in the events.

[](http://docs.splunk.com/File:6.5.0_tutorial_autolookupinputfields.png)

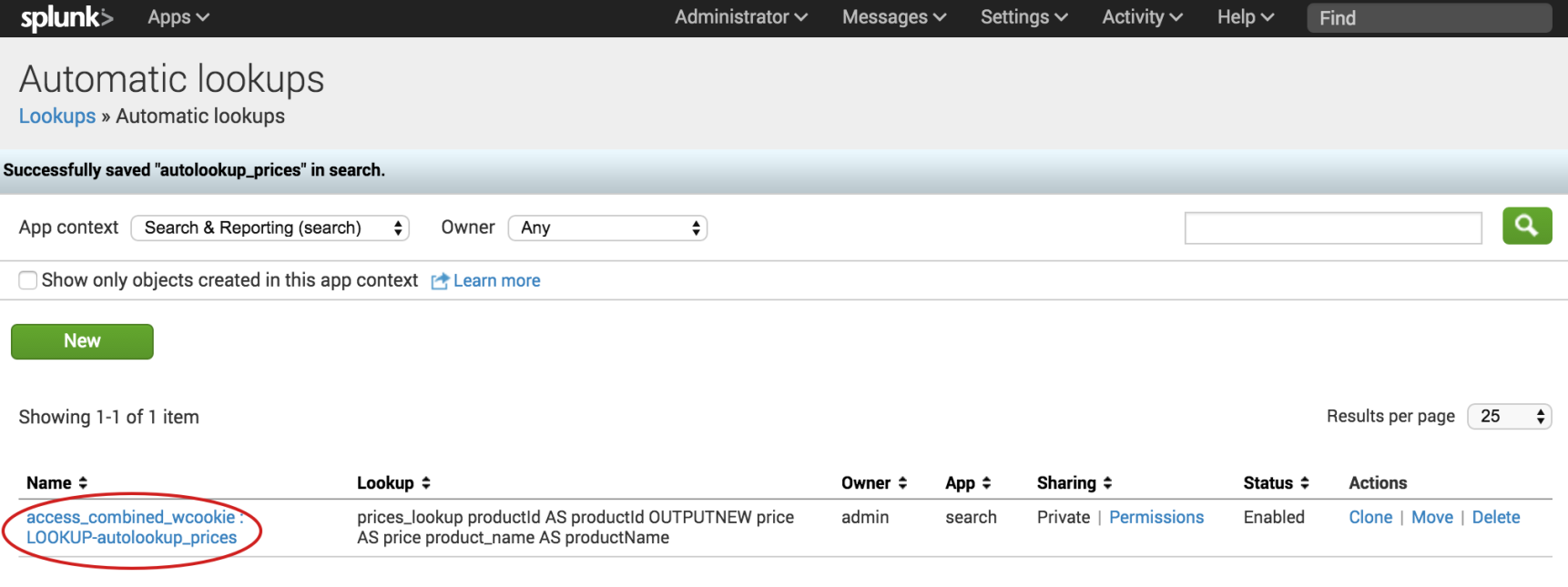
1. For **Lookup output fields**, specify the names of the fields from the lookup table file that you want to add to your event data. You can specify different names. The lookup table file has several fields. You will specify two of the fields to appear in your events.
   * In the first text box, type **product\_name**. This is the field in the prices.csv file that contains the descriptive name for each productId.
   * In the second text box, after the equal sign, type **productName**. This is the name of the field that will appear in your events for the descriptive name of the product.
   * Click **Add another field** to add another field after the first one.
   * Type **price** in the first text box. This is the field in the prices.csv file that contains the price for each productId. Let's use the same name for the field that will appear in your events. Type **price** in the second text box.

[](http://docs.splunk.com/File:6.5.0_tutorial_autolookupoutputfields.png)

1. Keep **Overwrite field values** unchecked.

Click **Save**.

The Automatic lookup view appears and the lookup that you configured, autolookup\_prices, is in the list. The full name is **access\_combined\_wcookie : LOOKUP-autolookup\_prices**.

[](http://docs.splunk.com/File:6.5.0_tutorial_autolookupssaved.png)

Search with field lookups

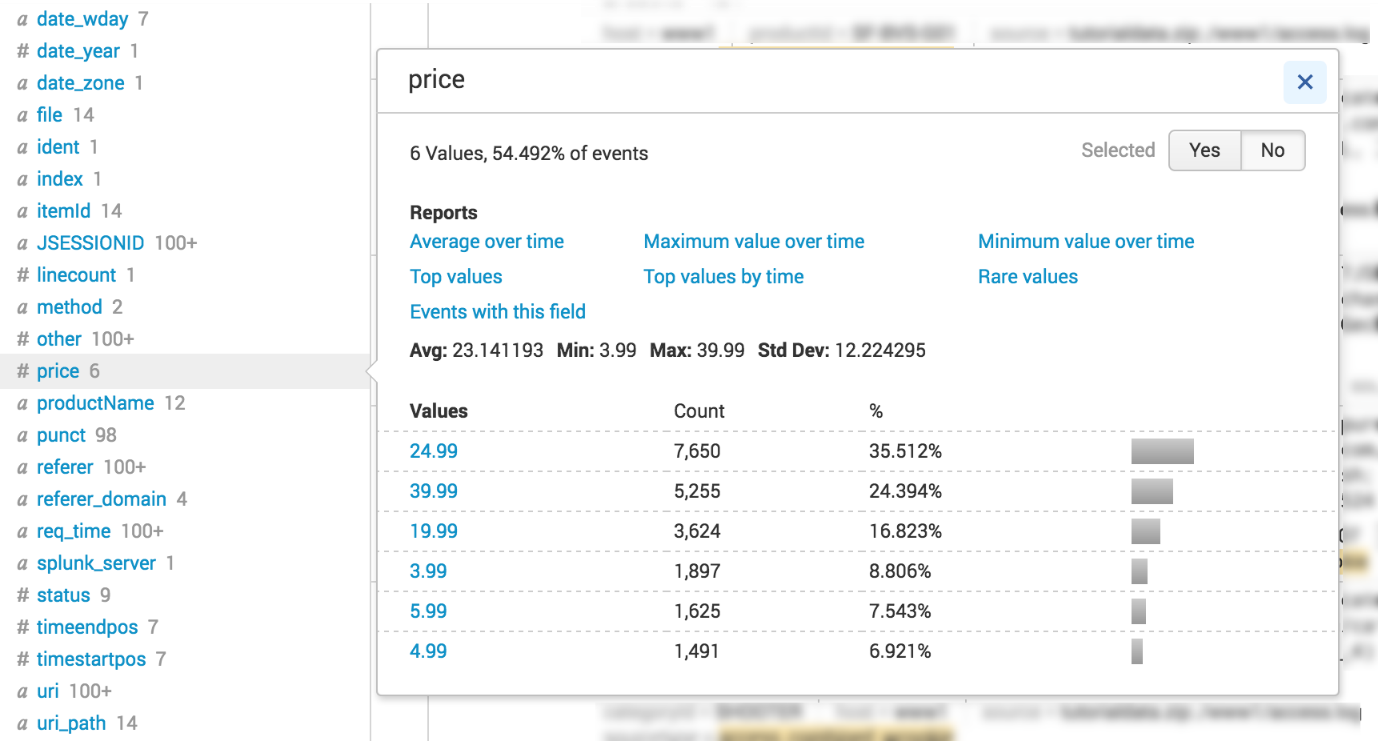
Show the lookup fields in the search results

Because the prices\_lookup is an automatic lookup the fields from the look will automatically appear in your search results.

1. From the Automatic Lookups window. In the **Apps** menu, click **Search & Reporting** to return to the Search summary view.
2. Change the time range to **All time**.
3. Run the following search to locate all of the web access activity.

sourcetype=access\_\*

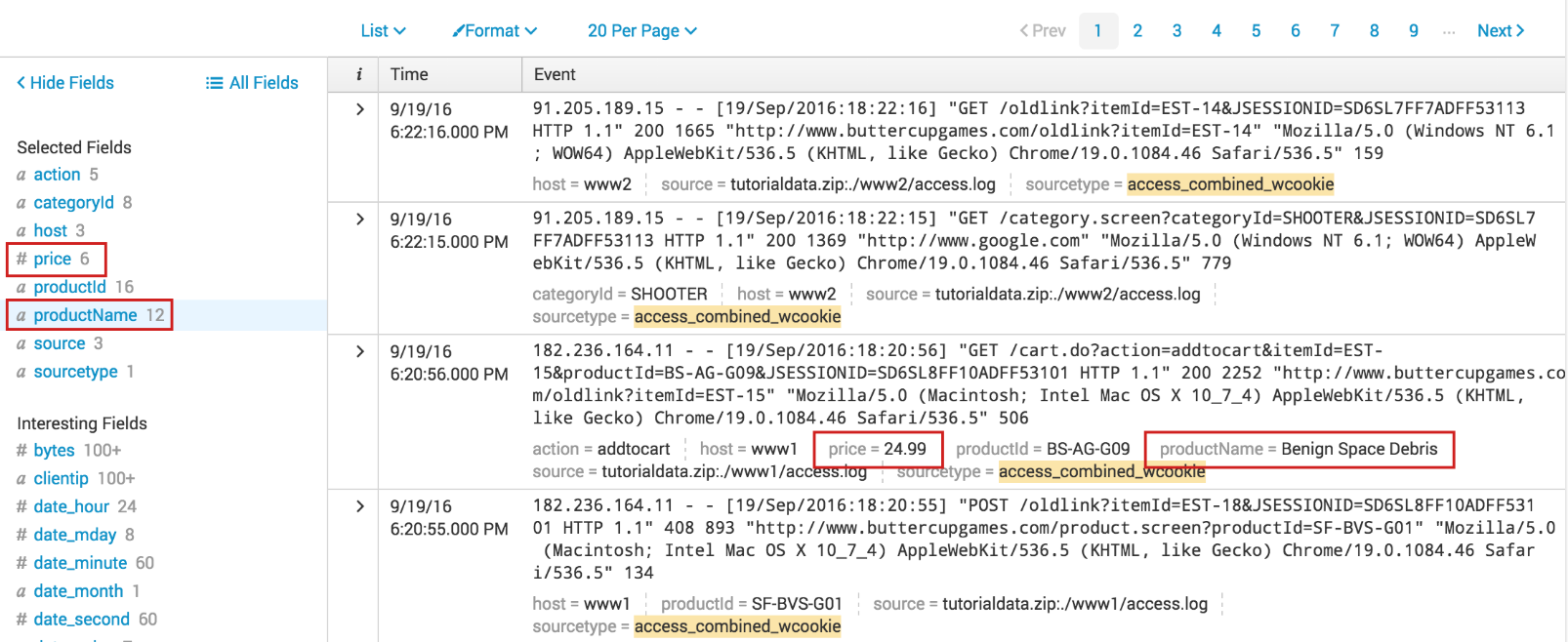
1. Scroll through the list of **Interesting Fields** in the Fields sidebar, and find the price field.
2. Click **price** to open the summary dialog box for that field.

[](http://docs.splunk.com/File:6.5.0_tutorial_price_fieldsummary.png)

1. Next to **Selected**, click **Yes**. This moves the **prices** field from the list of **Interesting Fields** to the list of **Selected Fields** in the Fields sidebar.
2. Close the dialog box.
3. Scroll through the list of **Interesting Fields** in the Fields sidebar, and find the productName field.
4. Click **productName** to open the summary dialog box for the field.
5. Next to **Selected**, click **Yes**.
6. Close the dialog box.

Both the price field and the productName field appear in the Selected Fields list and in the search results.

Notice that not every event shows the price and the productName fields.

[](http://docs.splunk.com/File:6.5.0_tutorial_selected_lookupfields.png)

Search with the new lookup fields

When you setup the automatic lookup, you specified that the productId field in your indexed events corresponds to the productId field in the prices.csv file.

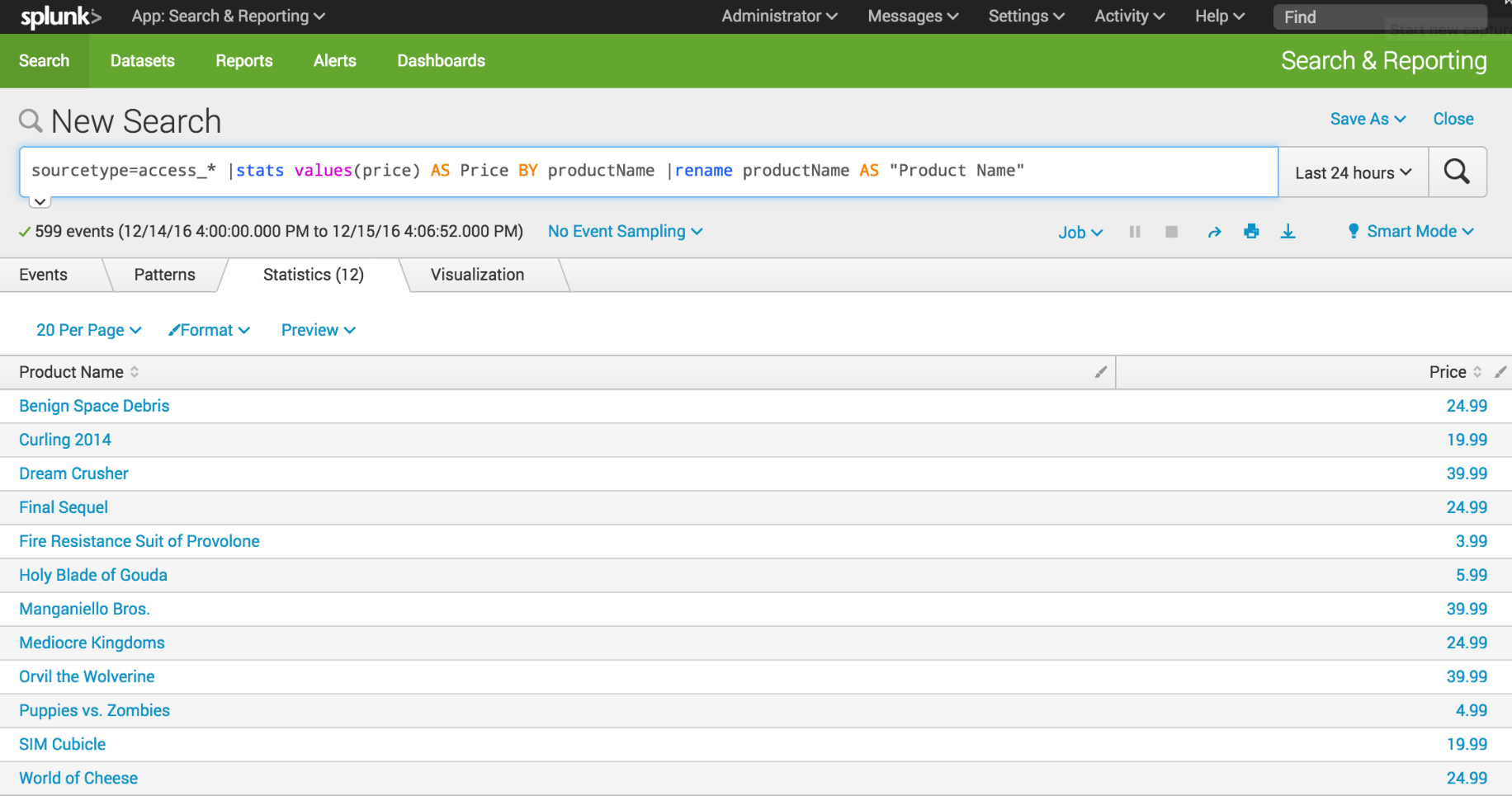
When you run a search, the Splunk software uses that relationship to retrieve, or lookup, data from the prices.csv file.

This enables you to specify the productName and price fields directly in your search. The product name and price information does not exist in our indexed fields. This information exists in the lookup file, prices.csv.

Example: Display the product names and prices

1. To show a list of the Buttercup Games product names and the corresponding prices, run the following search.

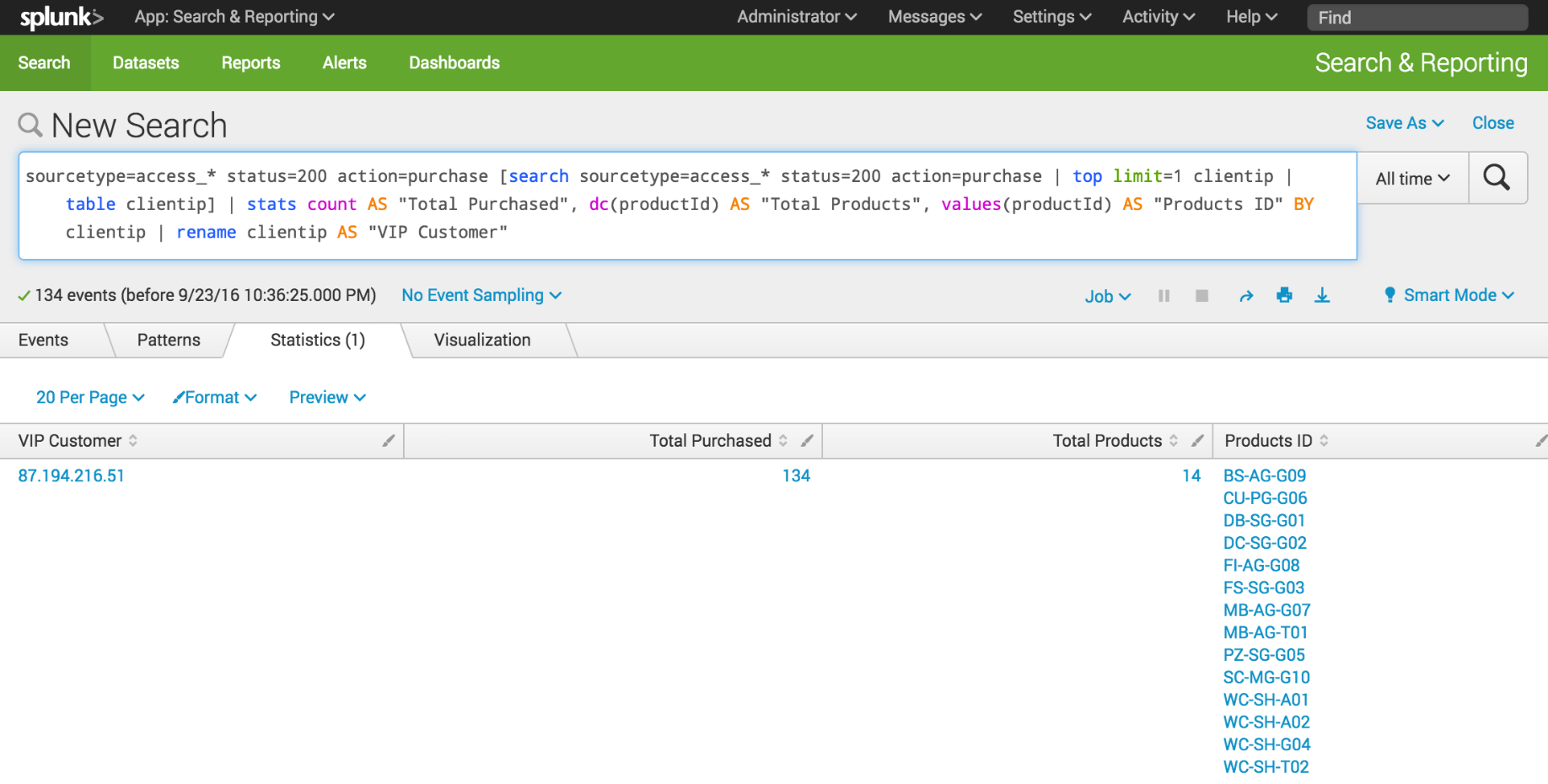
sourcetype=access\_\* |stats values(price) AS Price BY productName |rename productName AS "Product Name"

[](http://docs.splunk.com/File:6.5.1216_tutorial_lookup_prices.png)

Example: Display the VIP client purchases

In the previous section about subsearches, you created a search that returned the product IDs of the products that a VIP client purchased.

sourcetype=access\_\* status=200 action=purchase [search sourcetype=access\_\* status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products", values(productId) AS "Products ID" BY clientip | rename clientip AS "VIP Customer"

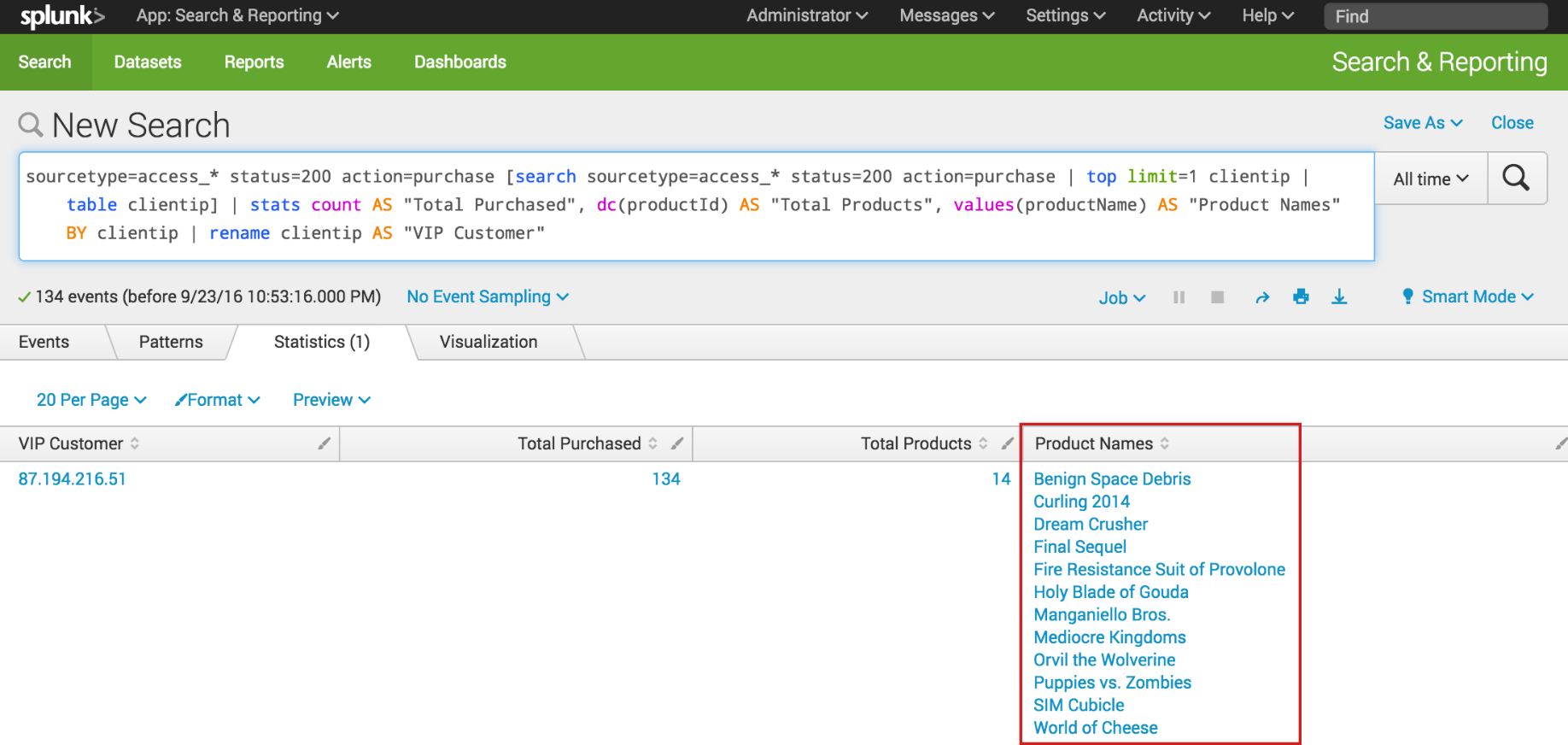
[](http://docs.splunk.com/File:6.5.0_tutorial_lookupsearch1.png)

The events return the product IDs because that is the only data in your events about the product. However, now that you have defined the automatic lookup, you can return the actual product names.

1. Make sure that the time range is set to **All time**.
2. Using the same search, for the **values** parameter, replace the productId field with the productName field.

sourcetype=access\_\* status=200 action=purchase [search sourcetype=access\_\* status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products", values(productName) AS "Product Names" BY clientip | rename clientip AS "VIP Customer"

The results are the same as in the previous search, showing the purchases by the VIP customer. However, the results are more meaningful because the product names, which are coming from the lookup table, appear instead of the more cryptic product IDs.

[](http://docs.splunk.com/File:6.5.0_tutorial_lookup_subsearch.png)