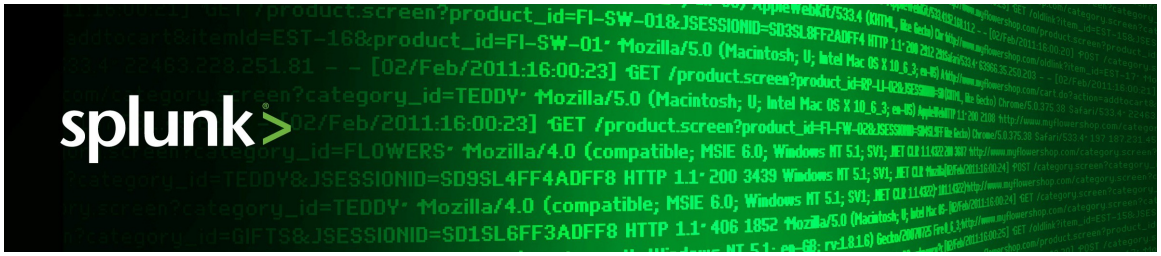


Splunk® Enterprise Data Model and Pivot Tutorial 7.0.0

Generated: 11/17/2017 4:06 pm

Table of Contents

Introduction

About the Data Model and Pivot Tutorial

This tutorial guides you through adding data to your Splunk deployment, building simple data models from this tutorial data, and creating new pivots from the data models.

Prerequisites for this tutorial

This tutorial assumes that you have access to a Splunk deployment.

If you do not have access to a Splunk deployment, you can use a trial version of the Splunk software. For instructions on downloading a trial version, installing, and starting the software, see the following topics in the *Search Tutorial*.

- What you need for this tutorial
- Install Splunk Enterprise on Linux, Windows, or Mac OS X
- Start Splunk Enterprise and launch Splunk Web

What's covered in this tutorial?

A breakdown of what you will find in each of the sections of this tutorial follows.

- **Introduction** describes the pre-requisites and system requirements for completing this tutorial. It also describes **Splunk Web**, which is the interface for using Splunk Enterprise and Pivot.
- **Part 1: Getting data into Splunk Enterprise** walks you through adding the tutorial data into Splunk Enterprise. The tutorial data, which is a sample data set composed of web server and MySQL logs for a fictional online game store, is included for download in this chapter.
- **Part 2: Building a data model** walks you through creating a new data model, defining the root dataset, editing dataset fields, defining child fields.
- **Part 3: Designing a Pivot report** walks you through creating and saving Pivot tables and charts.
- **Part 4: Creating dashboards** walks you through creating new dashboards and adding Pivots to new and existing dashboards.

Using a PDF of the tutorial

Do not copy and paste searches or regular expressions directly from the PDF into Splunk Web. In some cases, doing so causes errors because of hidden characters that are included in the PDF formatting.

What you need for this tutorial

To start this tutorial, you need access to a Splunk deployment version 6.0 or higher, either Splunk Cloud or Splunk Enterprise.

> **Note:** If you already have access to a Splunk deployment, skip this chapter and start with Part 1: Load the tutorial data.

If you intend to download, install, and start Splunk Enterprise, this topic contains system requirements and tells you what you need to know about Splunk licenses.

System requirements

You can use Splunk Enterprise on Linux, Windows, and Mac OS. For this tutorial, your computer must meet the specifications listed in the following table.

Requirement	Minimum supported hardware capacity
Non-Windows platforms	1x1.4GHz CPU, 1GB RAM
Windows platforms	Pentium 4 or equivalent at 2GHz, 2GB RAM
Web browser	The latest versions of Chrome, Firefox, and Safari browsers are supported with Splunk Enterprise 6.0 and later

This is a snapshot of the Splunk Enterprise system requirements. See the System Requirements topic in the *Installation* manual.

Create a Splunk.com account

You need a Splunk.com account to download the free trial Splunk software. If you do not already have a Splunk.com account, you need to create an account. If

you already have an account, you need to log in to that account.

1. Go to http://www.splunk.com/.
2. Create an account, or log in to an existing account.

    ◊ To create an account, click **My Account > Sign Up**. Enter the registration information.
    ◊ To log in to an existing account, click **My Account > Login**.

Download the latest version of Splunk Enterprise

If it has been a while since you downloaded the Splunk Trial software, download the trial software again. It is possible that the Trial license converted to a Free license. The Free license has some limitations that will not allow you to complete all parts of this tutorial. See Splunk trial licenses for more information.

1. Identify the installer that you want use with the tutorial.

Operating system	For this tutorial	Available installers
Linux	**Use any of the installers.**	3 installers. An RPM download for RedHat, a DEB package for Debian Linux, and a TAR file installer.
Mac OSX	**Use the DMG packaged graphical installer.**	2 installers. A DMG package and a TAR file installer.
Windows	**Use the MSI file graphical installer.**	2 installers. An MSI file and a compressed ZIP file.

2. Download the free trial version of the installer for Splunk Enterprise.
3. Accept the license agreement and click **Start Your Download Now**.

Splunk trial licenses

When you download Splunk Enterprise for the first time, you get an Enterprise Trial license for 60 days. This Enterprise Trial license includes all of the features, but limits the amount of data that you can index each day. The daily limit is 500MB.

After 60 days, the Enterprise Trial license converts to a Free license and some of the features, such as authentication and alerting, are disabled. The Free license also includes the 500MB each day of indexing volume, but has no expiration date.

Installing and starting Splunk Enterprise

For instructions on installing, and starting the software, see the following topics in the *Search Tutorial*.

- Install Splunk Enterprise on Linux, Windows, or Mac OS X
- Start Splunk Enterprise and launch Splunk Web

Next steps

The next topic describes how to navigate the views in Splunk Web.

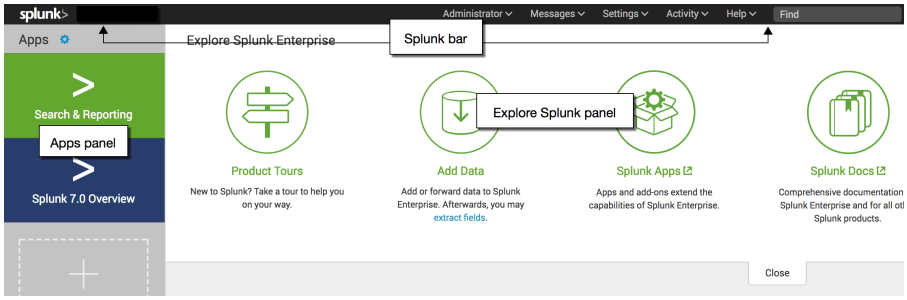
Navigating Splunk Web

Splunk Web is the primary user interface for searching, problem investigation, reporting on results, and administrating Splunk deployments. This topic discusses how to find the pages in Splunk Web that you need to complete this tutorial.

About Splunk Home

Splunk Home is the initial page in Splunk Web. Splunk Home is an interactive portal to the data and applications that you can access from this Splunk Enterprise instance. The main parts of the Splunk Home page are the Apps panel, the Explore Splunk panel, and the Splunk bar.

The following screen image shows the Splunk Home page for Splunk Enterprise. Splunk Cloud has a similar Home Page.



Apps panel

The **Apps** panel lists the applications that are installed on your Splunk instance. The list shows only the apps that you have permission to view.

When you first open Splunk Web, you see **Search & Reporting** and **7.0 Overview** in the Apps panel. The **Search & Reporting** app is sometimes referred to as simply the **Search app**. The **7.0 Overview" is an app that contains information about the new and updated features in the 7.0 version. There might be other apps listed on the Apps panel if other applications are installed on your computer.**

The **Data Model** and **Pivot** editors are part of the **Search & Reporting app**.

Explore Splunk panel

The Explore Splunk panel contains links to pages where you can get help.

Splunk Cloud
: You can take a product tour or access the documentation that is used the most.

Splunk Enterprise
: You can take a product tour, add data, browse for new apps, or access the documentation.

Splunk bar

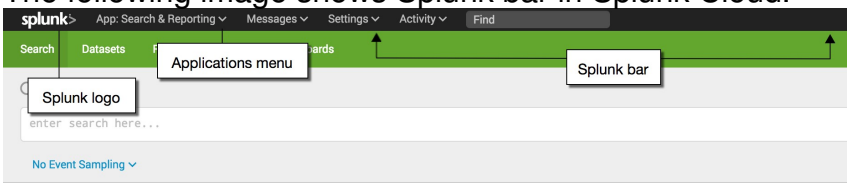
The Splunk bar appears on every page in Splunk Web. You use this bar to switch between apps, configure your Splunk deployment, view system-level messages, and monitor the progress of search jobs.

1. Click **Search & Reporting**.

   When you are in an app, the Applications menu displays in the Splunk bar. Use this menu to switch between apps.

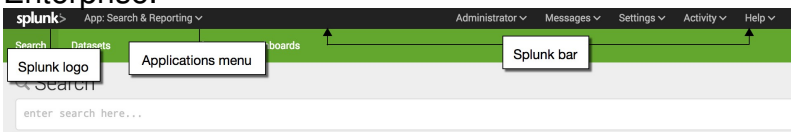
   Splunk Cloud

   The following image shows Splunk bar in Splunk Cloud.

   Splunk Enterprise

   The following image shows the Splunk bar in Splunk Enterprise.

   We will explore the Search app in detail. For now, let's return to Splunk Home.

2. Click the **Splunk** logo on the Splunk bar.

   Regardless of where you are in an app, you can always click the Splunk logo to return to Splunk Home.

Next steps

Continue to the next topic to add the tutorial data to your Splunk deployment.

Part 1: Getting data into your Splunk deployment

Load the tutorial data

This topic walks you through downloading the tutorial data set and adding it to Splunk Enterprise. You can complete this tutorial in several hours, but if you want to spread it out over a few days, download a new sample data file and add it.

Download the sample data file

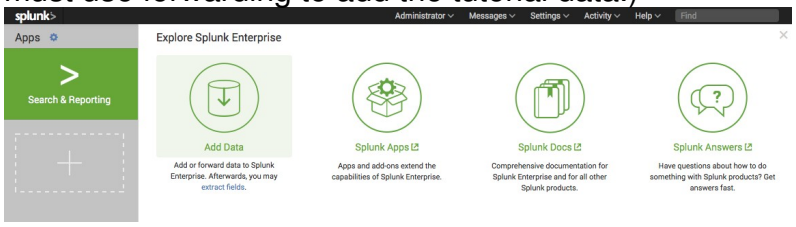
This tutorial uses a fictitious game store, called Buttercup Games, that sells games and related items in an online store.

You must download the compressed data file to use with this tutorial. The compressed data file contains web access log files, secure formatted log files, and sales log files for the Buttercup Games store. The `tutorialdata.zip` file is updated daily and contains events that are timestamped for the previous 7 days.

Do not uncompress the file.

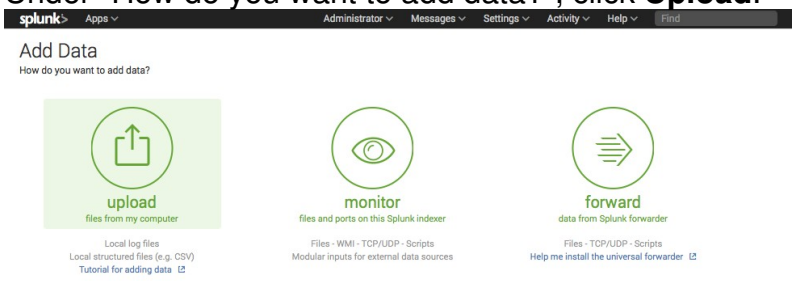
Add the sample data

1. Log into your Splunk deployment. If you are not in Splunk Home, click the Splunk logo on the Splunk bar to go to Splunk Home.
2. Under **Explore Splunk Enterprise**, click **Add data**. (**Note:** If your Splunk deployment is a self-service Splunk Cloud deployment, choose **Settings** and click **Add Data**. The **Add Data** option does not appear if your deployment is a managed Splunk Cloud deployment. In this case you must use forwarding to add the tutorial data.)

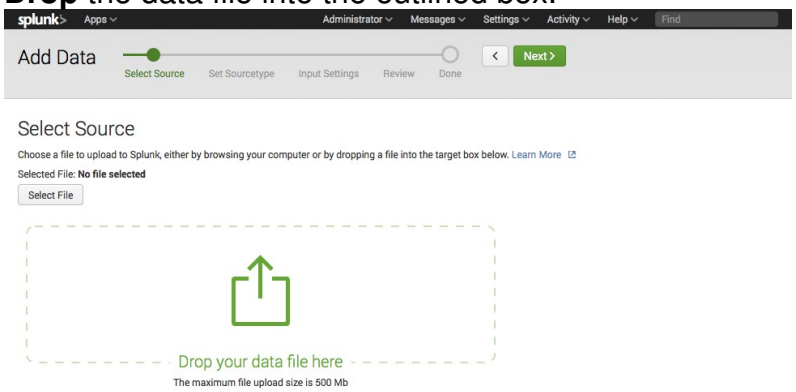


The **Add Data** view displays three options for adding data, lists of common data types, and add-ons you can use to extend Splunk Enterprise's capabilities to add data.

3. Under "How do you want to add data?", click **Upload**.



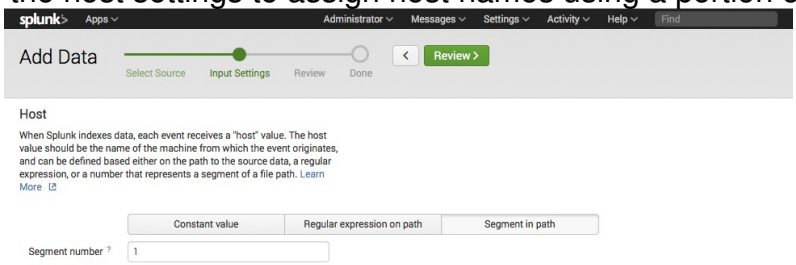
4. Under **Select Source**, click **Select File** to browse for the tutorial data or **Drop** the data file into the outlined box.



Because the tutorial data file is an archived data file, the next step in the Add Data workflow changes from **Set Sourcetype** to **Input Settings**.

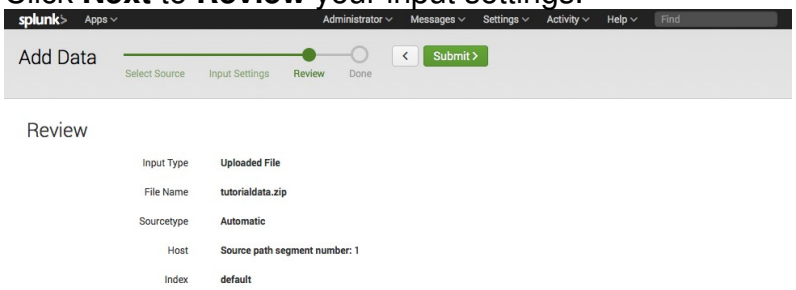
5. Click **Next** to continue to **Input Settings**. Under **Input Settings**, you can override the default settings for Host, Source type, and Index.

6. Modify the host settings to assign host names using a portion of the path name:

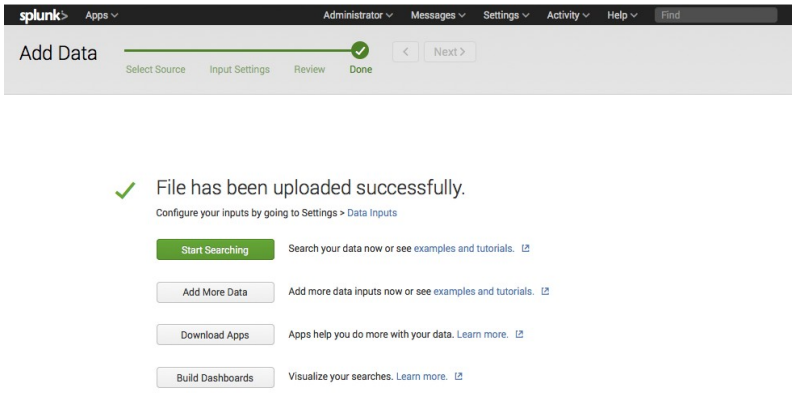


7. Select **Segment in path** from the menu.
8. Type in **1** for the segment number.

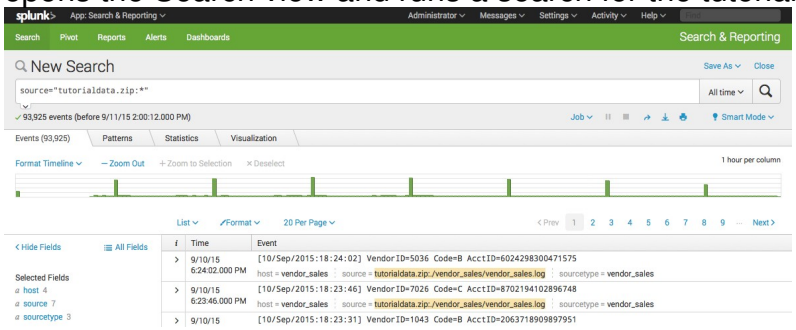
9. Click **Next** to **Review** your input settings.



10. Click **Submit**.



11. To confirm that the data added successfully, click **Start Searching**. This opens the Search view and runs a search for the tutorial data source.



Next steps

Some of the examples in this tutorial require data from external lookup tables. Now that you have added data to Splunk Enterprise, the next topic walks you through adding the lookup tables.

Add lookup files

The data models and pivots that you create in this tutorial require some fields from an external **lookup file**. This topic guides you through the steps to add the lookup to your Splunk deployment and create a new lookup definition.

With CSV lookups, you can reference fields in an external CSV file that match fields in your event data. Using this match, you can enrich your event data by adding more meaningful information and searchable fields to each event. For this tutorial the lookup file maps the `productId` in the tutorial data to a product name and price in the lookup file.

The remaining Parts in this tutorial dependent on you completing the steps in this section. If you do not configure the lookup, the data models and pivots will not produce the correct results.

If you completed the Search Tutorial, you can skip this step and go to Part 2: Building a data model.

Download and uncompress the lookup file

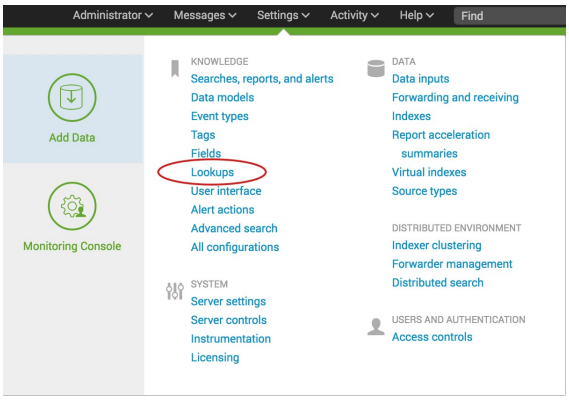
1. Download the Prices.csv.zip file.
2. Uncompress the file.

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

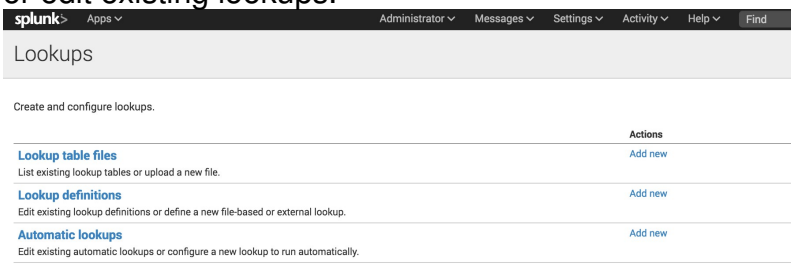
productId	product_name	price	sale_price	Code
DB-SG-G01	Mediocre Kingdoms	24.99	19.99	A
DC-SG-G02	Dream Crusher	39.99	24.99	B
FS-SG-G03	Final Sequel	24.99	16.99	C
WC-SH-G04	World of Cheese	24.99	19.99	D

Find the Lookups manager

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



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

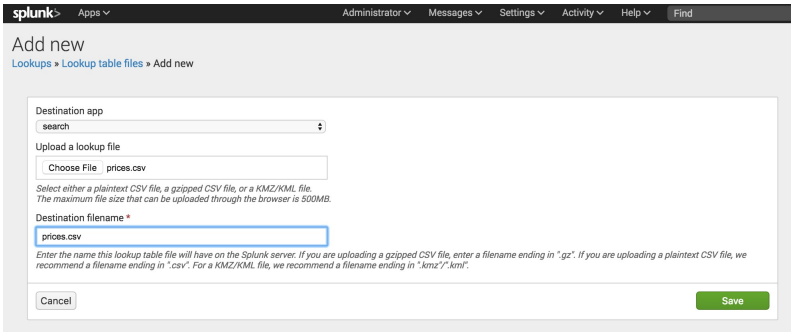


Upload the lookup table file

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** view to upload the CSV file that you want to use.



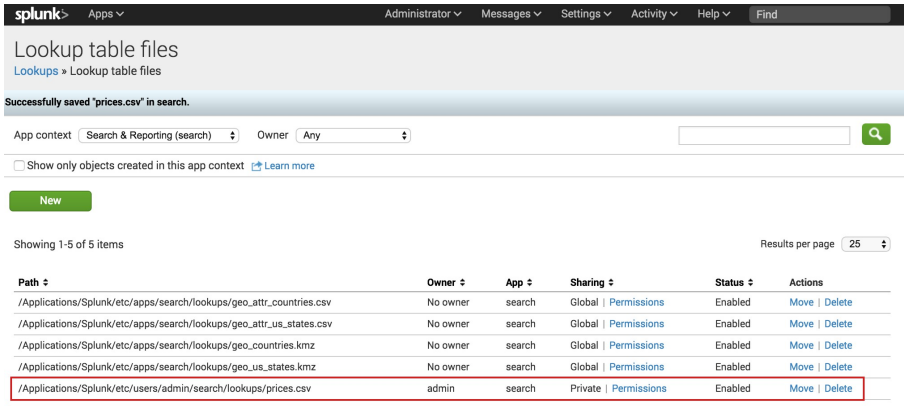
3. The **Destination app** field specifies which app you want to upload the lookup table file to. To upload the file in the Search app, you do not need to change anything. The default value is **search**.
4. Under **Upload a lookup file**, click **Choose File** and browse for the **prices.csv** file.
5. 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.

6. 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.

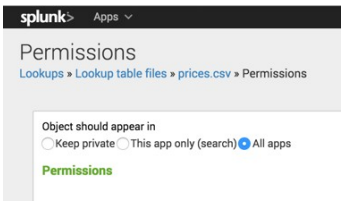


The other lookup table files in the list are included with the Splunk software.

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**.



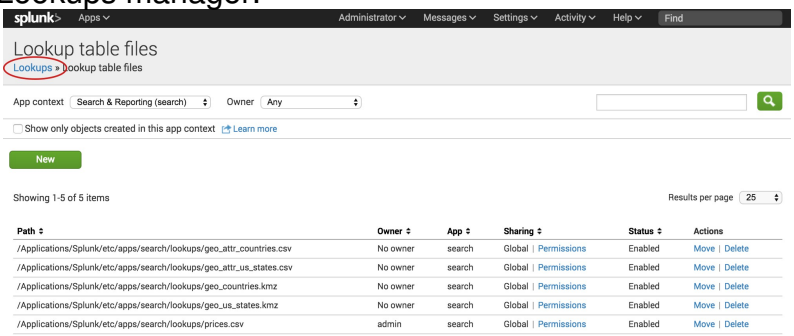
5. Click **Save**.
   The Sharing setting for the prices.csv lookup table is set to **Global**.

Path	Owner	App	Sharing
/Applications/Splunk/etc/apps/search/lookups/geo_attr_countries.csv	No owner	search	Global | Permissions
/Applications/Splunk/etc/apps/search/lookups/geo_attr_us_states.csv	No owner	search	Global | Permissions
/Applications/Splunk/etc/apps/search/lookups/geo_countries.kmz	No owner	search	Global | Permissions
/Applications/Splunk/etc/apps/search/lookups/geo_us_states.kmz	No owner	search	Global | Permissions
/Applications/Splunk/etc/apps/search/lookups/prices.csv	admin	search	Global | Permissions

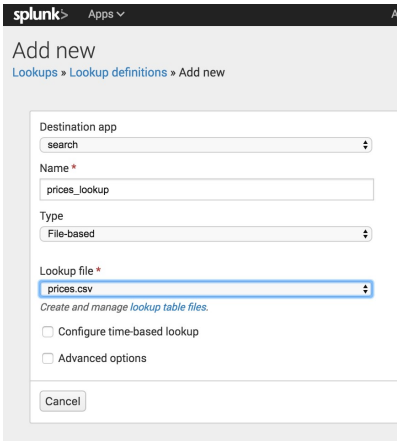
Add the field lookup definition

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 view, select **Lookups** in the breadcrumbs to return to the Lookups manager.

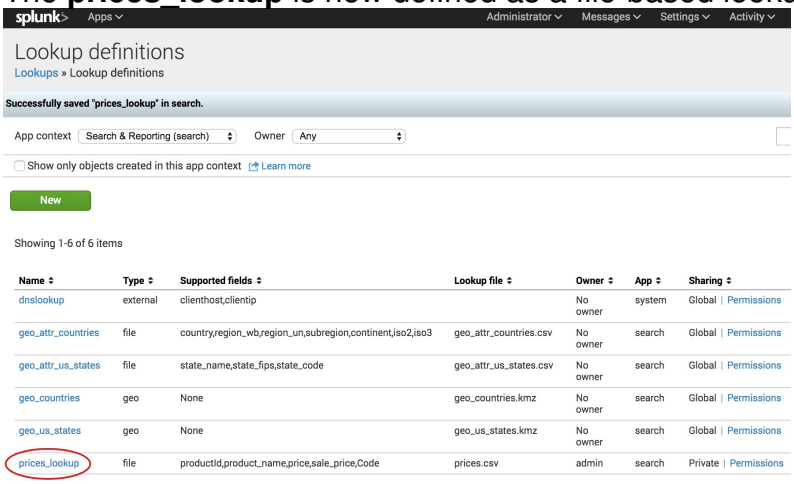


2. For **Lookup definitions**, click **Add New**.
   The Add new lookups definitions page opens, where you define the field lookup.
3. There is no need to change the **Destination app** setting. It is already set to **search**, referring to the Search app.
4. For **Name**, type `prices_lookup`.
5. For **Type**, select **File-based**.
   A file-based lookup is typically a static table, such as a CSV file.
6. For **Lookup file**, select **prices.csv**, which is the name of the lookup table file that you created.



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

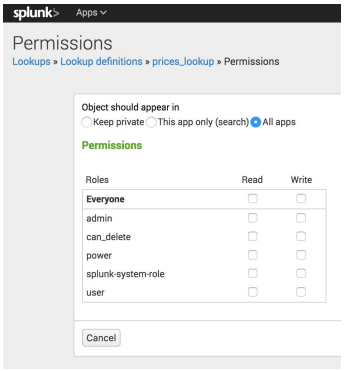
   The **prices_lookup** is now defined as a file-based lookup.



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**.



3. 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.

Next steps

Continue to the next section to learn about data models and how to create them.

Part 2: Building a data model

About data models and data model datasets

The topics in this chapter show you how to use the Data Model Builder to design and build data models for the tutorial data.

What is a data model?

A data model is a type of knowledge object that applies an information structure to raw data, making it easier to use. Each data model represents a category of event data. Data models are composed of **data model datasets**. More specifically, a data model is a hierarchical search-time mapping of knowledge about one or more datasets. A data model encodes the domain knowledge necessary to build a variety of specialized searches of those datasets. Briefly put, data models generate searches. These specialized searches are in turn used to generate reports for Pivot users.

To create an effective data model, you must understand your data sources. You need to understand whether your data sources are derived from a log file, TCP/UDP network input, received from a scripted input for an API, and so on. You also need to understand your data semantics - how the various fields in your data are extracted, related, and organized. This information can affect your data model architecture.

Data models can get their fields from **extractions** that are defined on the Splunk Web **Settings > Fields > Field extractions** page or, for Splunk Enterprise, by editing the `props.conf` and `transforms.conf` files. But when you define your data model, you can also arrange to have it get additional fields at search time by using regex-based field extractions, **lookups**, or `eval` expressions.

In this tutorial, your data sources are web access and secure log files. Most of the fields are automatically extracted. Other fields are added using lookup files and calculated with eval expressions.

About data model datasets

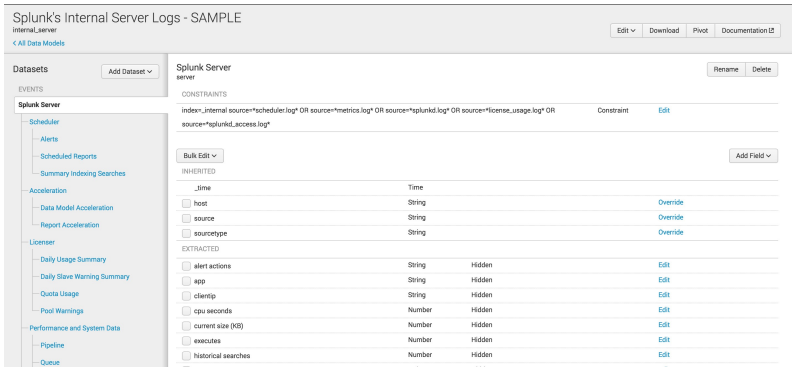
Data models are composed of one or more datasets. Each dataset corresponds in some manner to a set of data in your index. Datasets break down into four types:

- Events datasets
- Search datasets
- Transaction datasets
- Child datasets

Datasets in data models can be arranged in parent/child relationships. Each top-level or root dataset can have child datasets which inherit the constraints and fields of the parent and have additional constraints and fields of their own.

Note: Data model datasets are a category of **knowledge object**. However, data model datasets often use other knowledge objects such as **extracted fields**, **calculated fields**, and **lookups** to define the specific sets of data that the data model dataset represents.

Here is an example of a data model as viewed through the Data Model Builder.



In this example, the dataset hierarchy is in the left-hand sidebar. The Splunk Server root event dataset is selected. The Splunk Server dataset contains all of the data in the data model. The child datasets that branch off of the Splunk Server object, such as Scheduler, Acceleration, and Licenser, and each child dataset contains different subsets of that data.

On the right side of the Data Model Builder are the dataset constraints that define the dataset and the list of fields associated with the dataset. The other topics in this chapter show you how to create a data model. You will learn how to use the Data Model Builder to define the dataset hierarchies and dataset fields for the data model.

Dataset constraints

All data model datasets are defined by sets of constraints that filter out events that are not relevant to the dataset. These constraints help to define the data that

the dataset represents. A typical constraint looks like the first part of a search, before pipes and additional search commands are added.

Constraints are inherited by child datasets to ensure that each child dataset represents a subset of the data from the parent datasets. Pivot users can then use these child datasets to design reports with datasets that already have extraneous data prefiltered out.

Dataset fields

Dataset fields come in five flavors: Auto-extracted, Eval expression, Lookup, Regular Expression, and Geo IP.

Dataset fields are inherited. A child dataset will automatically have all of the fields that belong to its parent. You can design a relatively simple data model where all of the necessary fields for a specific dataset tree are defined in its root dataset, and the child datasets would be differentiated from the root dataset and from each other only by their constraints.

Fields serve several purposes. They are the set of fields that Pivot users work with to define and generate a pivot report. The set of fields you have access to is determined by the dataset you choose when you enter Pivot. You might add fields to a child dataset to provide fields to Pivot users that are specific to the dataset covered by that dataset.

Learn more about data models

The information discussed in this topic is limited to what you need to know to build the data models for the tutorial data. For more information, see About data models and Design data models in the *Knowledge Manager Manual*.

Next steps

Proceed to the next topic, where you will create a new data model.

Create a new data model

This topic shows you how to create new data models based on the tutorial data. Data models are created within Pivot and you need to have the admin or power role to create a data model.

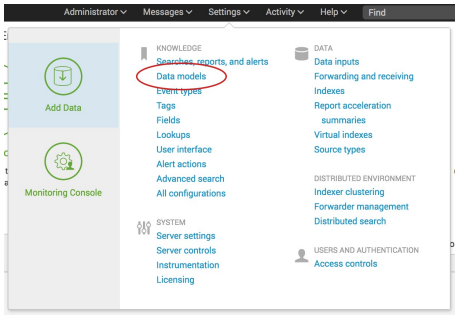
Enable roles to create a data model

By default only users with the admin or power role can create data models. For other users, the ability to create a data model is tied to whether their roles have "write" access to an app. Since this tutorial uses a trial installation, you have admin privileges by default and should be able to continue.

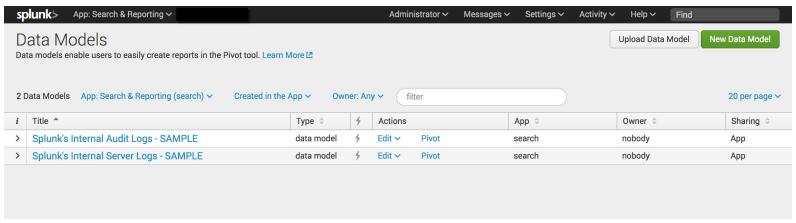
If you are not able to create or edit a data model, you may need to check your permissions. For more information, read About data model permissions in the Knowledge Manager Manual.

Navigate to the Data Models management page

1. If you are not in the Search app, click the App menu and select **Search & Reporting app**.
2. In the Splunk bar, click **Settings**.



3. Under **Knowledge**, click **Data Models**.

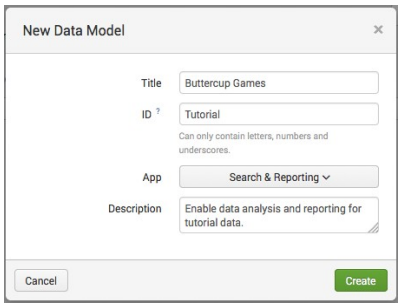


This takes you to the **Data Models** management page. The Data Models management page lists the built-in data models and any data models that you have defined. For the Search app, there are two built-in data models.

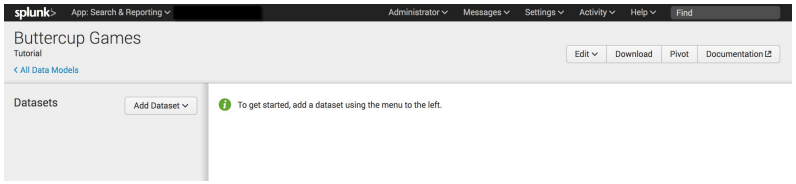
Use this page to manage the permissions, acceleration, cloning, and removal of existing data models. You also use this page to upload a data model or create a new data model.

Create a new data model

1. In the **Data Models** page, click **New Data Model**.



2. In the **New Data Model** dialog box, for **Title** type `Buttercup Games`.
   The Title field accepts any character, as well as spaces.
3. Optional. For **ID**, type `Tutorial`.
   If you don't change the ID, it automatically uses the same name as the title, without spaces. In this example it uses `Buttercup_Games`.
   The ID must be a unique identifier for the data model. It cannot contain spaces or any characters that aren't alphanumeric, underscores, or hyphens (a-z, A-Z, 0-9, _, or -). Spaces between characters are also not allowed. Once you define the data model ID, you can't change it.
4. For **App**, select **Search & Reporting**.
5. Optional. For **Description**, type `Enables data analysis and reporting for tutorial data.`
6. Click **Create**. The editor page for the new Buttercup Games data model appears. You will edit add a root dataset to this data model in the next step.



7. Click the link **All Data Models**.
   The Data Models page shows the new **Buttercup Games** data model that you created.

Note: There was a terminology change in version 6.5.0 from "objects" to "datasets". For more information about data model datasets, see About data models datasets.

Next steps

Continue to the next topic to add a root dataset to the Buttercup Games data model.

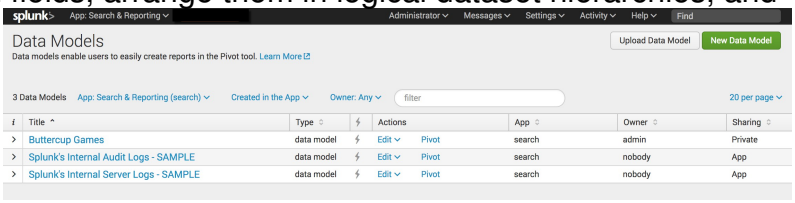
Define a root dataset for the data model

In the last topic, you created the data model called `Buttercup Games`.

This topic walks you through adding a root dataset for Buttercup Games purchases.

Add a root dataset

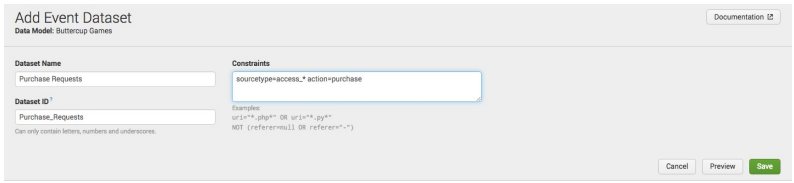
1. From the **Data Models** list, click **Buttercup Games**.
   This opens the Buttercup Games dataset in the editor page. You use the editor page to design a new data model or redesign an existing data model. You can create datasets for your data model, define their constraints and fields, arrange them in logical dataset hierarchies, and maintain them.



   Data models are typically composed of dataset hierarchies built on root event datasets. Each root event dataset represents a set of data that is defined by a constraint, which is a simple search that filters out events that are not relevant to the dataset. For more information about root event datasets and root search datasets see Design data models.

   Let's create a dataset to track purchase requests on the Buttercup Games website.
2. To define the first event base dataset for the data model, click **Add Dataset**.

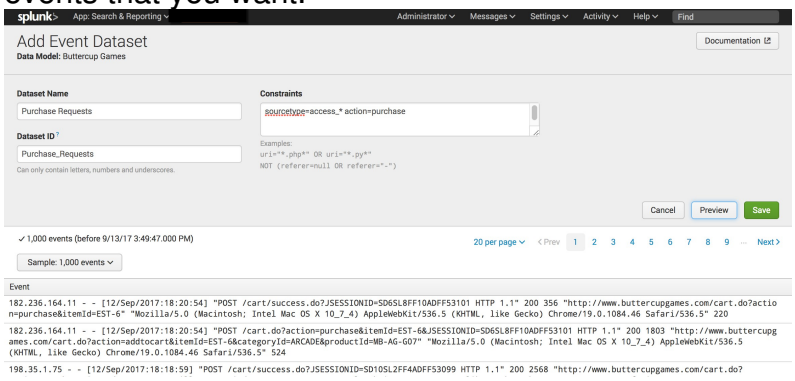
   Your first root dataset can be either a **Root event**, **Root search**.
3. Select **Root event**. The **Add Event Dataset** editor opens.



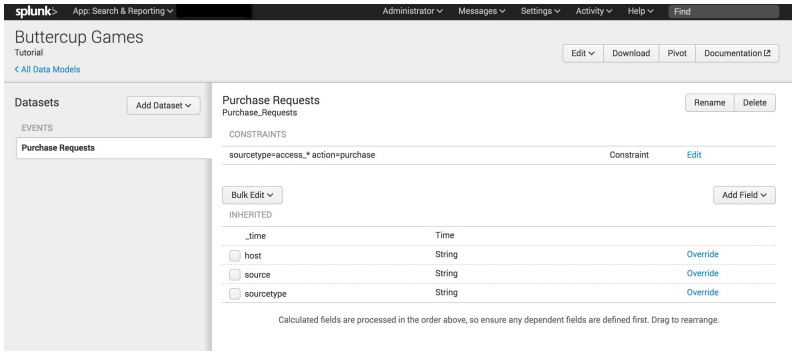
4. For **Dataset Name** type `Purchase Requests`. The **Dataset Name** field can accept any character, including spaces.
5. Optional. The **Dataset ID** field is automatically populated when you type in the **Dataset Name**. The value **Purchase_Requests** should appear in the field.

   The **Dataset ID** must be a unique identifier for the dataset. The ID can be comprised of alphanumeric, underscore, or hyphen (a-z, A-Z, 0-9, _, or -) characters. Spaces are not allowed.

   After you add the dataset, you cannot change the **Dataset ID**.
6. In the **Contraints** field, type this search constraint: `sourcetype=access_* action=purchase`.
   This constraint limits the dataset to events that are web access page requests that are purchase events.
7. Click **Preview** to test whether the constraints you have specified return the events that you want.



8. Click **Save**. The fields are added to the dataset under the INHERITED field category.



The list of fields for the root dataset includes: _time, host, source, and

sourcetype. If you want to add child datasets to client and server errors, you need to edit the fields list to include additional fields.

Next steps

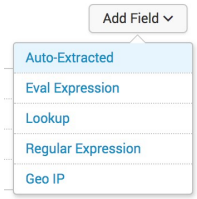
Continue to the next topic to add more fields to the **Purchase Requests** dataset.

Edit fields list

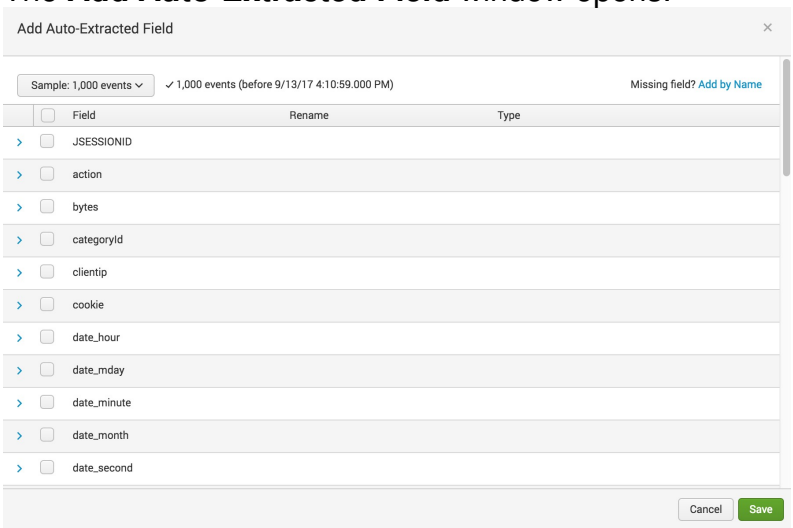
Add automatically extracted fields

The **Auto-extract** field type is an extracted field that is recognized automatically (such as a default or indexed field) or a **search-time** field extraction that you have defined in Splunk Web on the **Field Extractions** page or, if you are using Splunk Enterprise, by editing the `props.conf` and `transforms.conf` files.

1. In the Buttercup Games dataset editor, click **Add Field**.
2. Select **Auto-Extracted**.

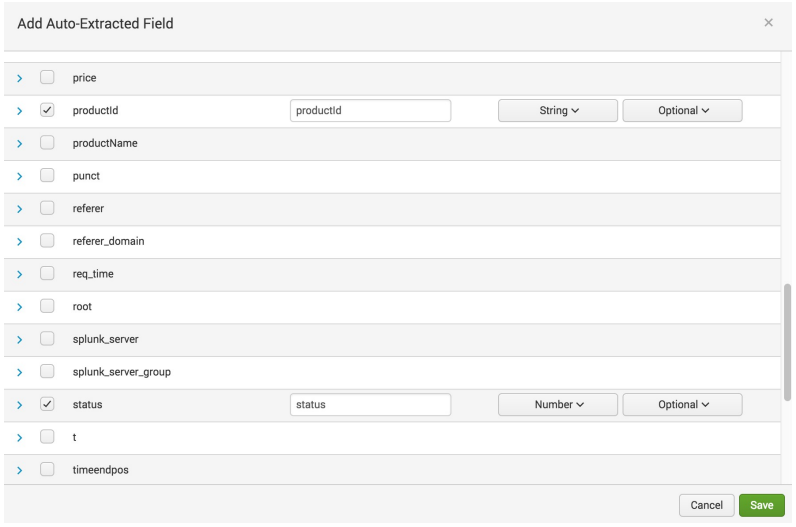


The **Add Auto-Extracted Field** window opens.



3. Scroll through the list of automatically extracted fields and check the following fields:

- action
- categoryId
- productId
- status



For each field you check, the data type of the field in displayed. For example, the `status` field should show **Number** for the data type.

You can designate that dataset fields be Required, Optional, Hidden, or Hidden & Required. **Optional** means that the field does not need to appear in every event represented by the dataset. The field might appear in some of the dataset events and not others. The default is **Optional**, which is the setting you want for these fields.

4. Click **Save**. The fields are added to the dataset under the EXTRACTED field category.

Add lookup fields to the dataset

Creating a lookup field requires at least one **lookup definition** defined in the Lookups manager. The lookup definition tells Splunk software where the lookup table is and how to connect to it. When the lookup definition is in place, Splunk software can match the values of a field in your events to the values of a field in the lookup table. The corresponding field/value combinations are applied to your dataset as lookup fields.

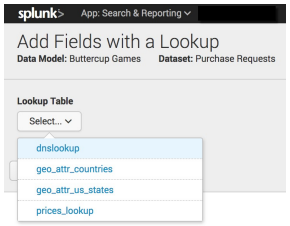
Prerequisite

The field lookup must be uploaded and defined before you edit the data model dataset. Verify that you added the `prices.csv` lookup table and defined the `price_lookup` in Part 1 of this tutorial. See Add lookup files.

If you define an automatic lookup, then the fields are already added to the events. You must then add the lookup fields as automatically extracted fields.

If you do not define an automatic lookup, use the following steps to add the lookup fields to the dataset.

1. You should still be in the **Buttercup Games** dataset editor with the **Purchase Requests** dataset displayed.
2. Click **Add Field** and select **Lookup**.
3. For **Lookup Table**, select **prices_lookup**.



The prices_lookup file has descriptive product names and prices for each of the items sold on the Buttercup Games website. The lookup table has headers and values like the following sample:

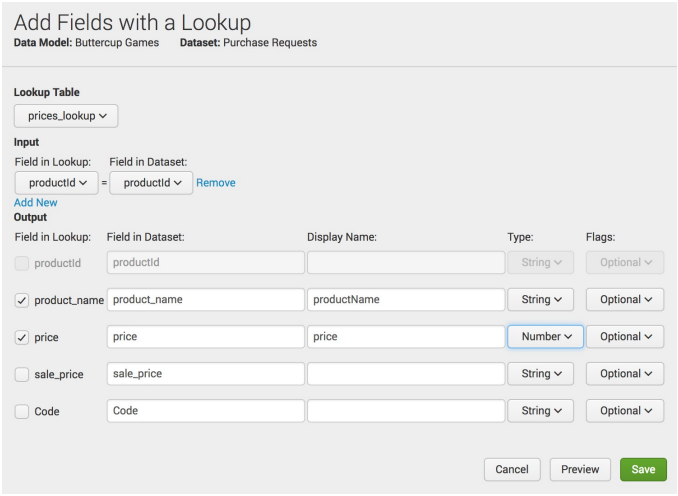
productId,product_name,price,sale_price,Code

DB-SG-G01,Mediocre Kingdoms,24.99,19.99,A

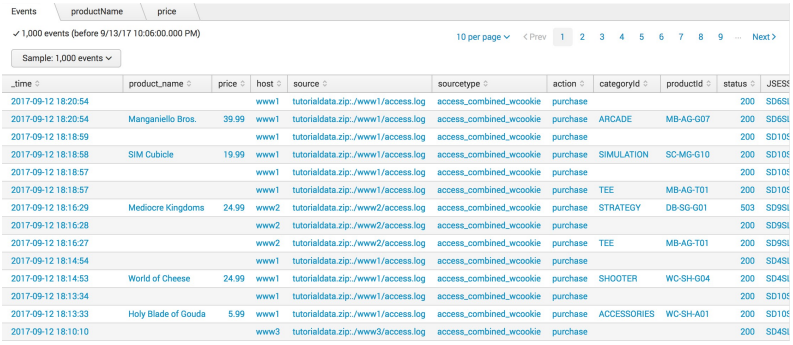
You can specify the input and output fields.

4. Under **Input**, for the **Field in Lookup** the `productId` should already be selected.
   The **Field in Lookup** is the name of the field used in the CSV lookup table.
5. For the **Field in Dataset** select `productId`.
   The **Field in Dataset** is the name of the field used in the event data.
6. Under **Output**, check the **product_name** and **price** fields.
   The output fields listed are from the header row of the lookup table are listed under **Field Names**. You can specify a **Display Name** for each fields. This display name is the name used for the field in your events. Because productId is the field used to match between the events and lookup table, you cannot change its display name.
7. For product_name, in the **Display Name** field type `productName`.

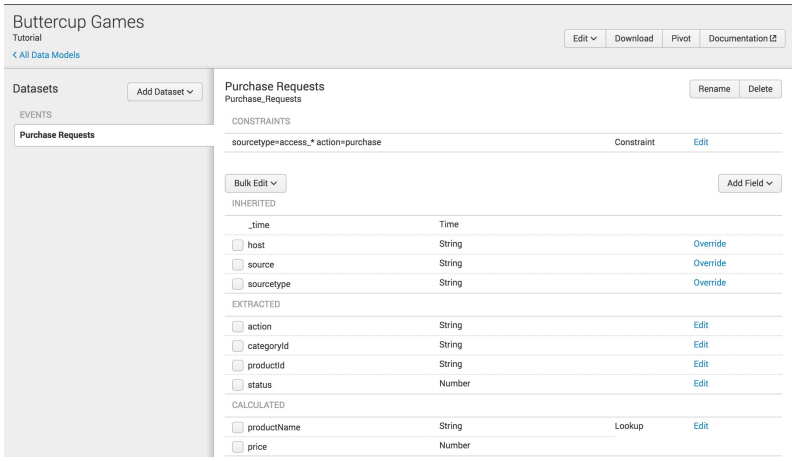
8. For price, in the **Display Name** field type `price`. Ensure that the **Type** is set to **Number**.



9. Click **Preview** to review the fields that you want to add.
   Scroll down to see the preview. Use the **Events** tabs to view the events in a table. There are also tabs for each of the fields you specified as output fields. In this tutorial you specified **productName** and **prices** as the output fields.



10. Click **Save**. The lookup fields are added to the dataset under the CALCULATED field category.



Next steps

Add child datasets.

Define child datasets

A child dataset inherits all of the constraints and fields that belong to its parent dataset. When you define a new child dataset, you give it one or more additional constraints, to further focus the dataset.

In the previous topic, you added a root dataset called **Purchase Requests** to track purchases on the Buttercup Games website. Now you want to add child datasets for tracking successful and failed purchases.

Add a child dataset

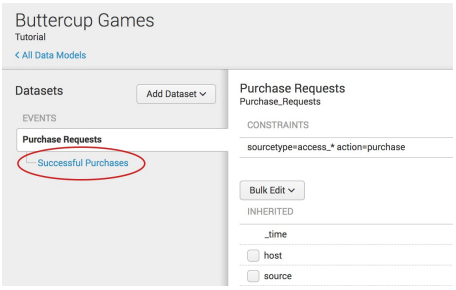
1. In the **Buttercup Games** dataset editor page, click **Add Dataset** and select **Child**.
   This opens an editor window, **Add Child Dataset**.
2. On the **Add Child Dataset** page, for **Dataset Name** type `Successful Purchases`.
3. The **Dataset ID** field should show `Successful_Purchases`. For this tutorial, you are not going to change the **Dataset ID**. Similar the **Dataset ID** for the root dataset, the ID cannot be changed after you save the dataset.
4. For **Inherit From** select **Purchase Requests** from the list.
   This setting tells the child dataset which parent dataset to inherit the fields and constraints from.
5. In the **Additional Constraints** field, type `status=200`.

This status code is for successful purchases. The search for the events in this dataset will look something like this:

```
sourcetype=access_* action=purchase status=200
```

6. Optional. You can click **Preview** to see the events that are returned.
7. Click **Save**.

   The Buttercup Games dataset editor page shows that the **Successful Purchases** child dataset is added to the **Purchase Requests** root dataset.

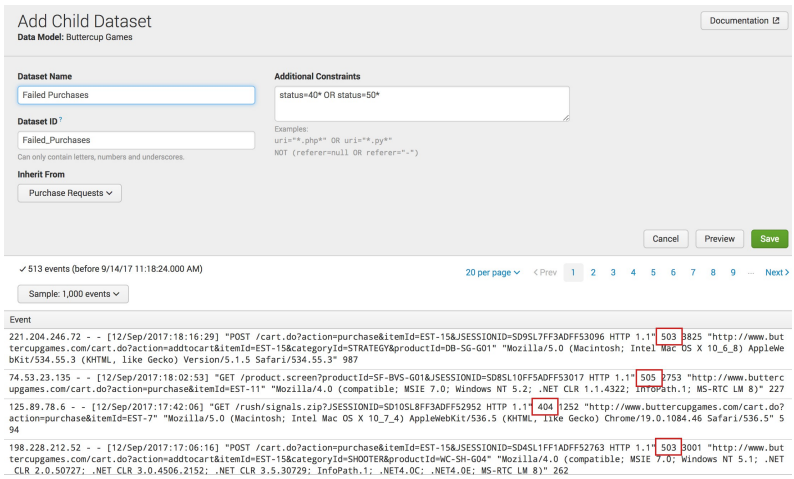


Add a second child dataset

1. In the **Buttercup Games** dataset editor page, click **Add Dataset** and select **Child**.
2. On the **Add Child Dataset** page, for **Dataset Name** type `Failed Purchases`.
3. The **Dataset ID** field should show `Failed_Purchases`. For this tutorial, you are not going to change the **Dataset ID**.
4. For **Inherit From**, make sure that **Purchase Requests** is selected.
5. In the **Additional Constraints** field, type `status=40* OR status=50*`. This status code is for server or system errors, which result in failed purchases. The search for the events in this dataset will look something like this:

   ```
   sourcetype=access_* action=purchase status=40* OR status=50*
   ```

6. Optional. You can click **Preview** to see the events that are returned.



7. Click **Save**.

Next steps

Now that you've created data models, you can generate pivot reports. Continue to the next chapter to learn about Pivot and how to create pivot reports.

Part 3: Designing a Pivot report

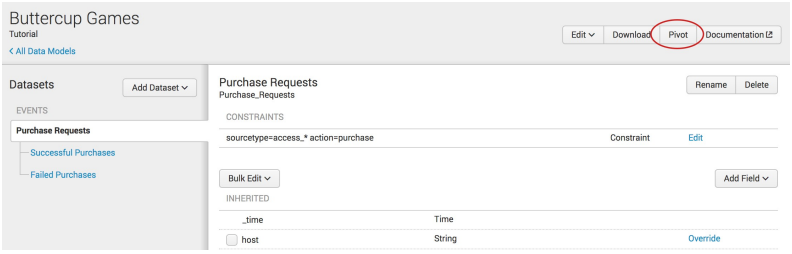
About Pivot

The Splunk Pivot tool lets you quickly design reports with tables and data visualizations that present different aspects of a selected Data Model. Pivot lets you generate these reports with a UI interface instead of having to use the search processing language.

Accessing Pivot from the Datasets page

In Part 2, you built a data model and created a root dataset called **Purchase Requests** and added two child datasets, one for successful purchases and one for failed purchases.

1. From the Buttercup Games dataset editor page, click **Pivot**.



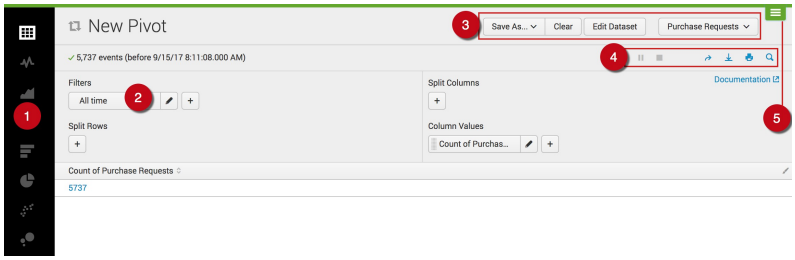
2. Select the Purchase Requests dataset. This is the dataset that you want use to create the pivot.

   The **New Pivot** page appears and shows information using the Purchase Requests dataset.

   If your browser window is not full screen, the Apps bar is hidden. You can access the Apps bar by click the menu icon in the upper right corner of the window. The Apps bar slides down. Click the menu icon again to hide the Apps bar.

The New Pivot editor

The following image shows the New Pivot editor page. The key components of the editor page are highlighted.



The components of the New Pivot editor page that are identified in the image are described in the following table.

Number	Element	Description
1	**Visualization types**	A list of icons that represent different visualization types.
2	**Filters**	You can specify time range and field filters for your pivot.
3	**Pivot actions**	Use the Pivot actions to: • Save the pivot as a report or dashboard panel. • Clear, or remove, the changes that you made in the Pivot editor. This enables you to experiment with the different visualizations before you save the pivot. • Edit the current dataset. • Other data model dataaset actions, such as view the data model for the current dataset, select a different dataset, and acceleration actions.
4	**Job actions**	Pivot job actions are similar to search job actions. You can pause or stop the progress of the pivot job, share or export the pivot job, and open the pivot in the Search app.
5	**Apps bar**	Navigate between the different views in the application you are in. For the Search & Reporting app the views are: Search, Datasets, Reports, Alerts, and Dashboards.

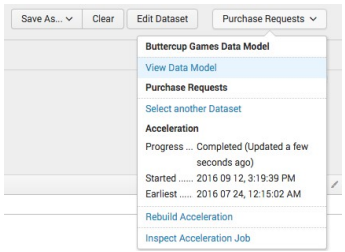
Visualization types

The left-hand vertical bar contains icons that represent different visualization types. Selecting a different icon controls which Pivot builder and report interfaces display. Visualization types are: Statistics Table (default), Column Chart, Bar Chart, Scatter Chart, Bubble Chart, Area Chart, Line Chart, Pie Chart, Single Value Display, Radial Gauge, Marker Gauge, and Filler Gauge.

Pivot actions

The upper horizontal bar displays document-related actions. These actions include:

- **Save as...:** Save the current report as a new one (**Report**) or as a dashboard panel (**Dashboard Panel**).
- **Clear:** Reset the interface to its initial state, which will dismiss the saved report (if applicable), change the visualization type to Statistics Table, and populate the report with a single Column Value for the count of the dataset and a time filter for all time (if _time is an applicable field).
- **Data model dataset:** This is the right-most button. It takes its label from the data model dataset that was selected. For example, in the screenshot it is "Purchase Requests". Use this menu to navigate back to the list of data models (**Select another Data Model**), navigate back to the list of data model datasets (**Select another Dataset**), or edit the selected data model dataset (**Edit Dataset**). Additionally, you can rebuild acceleration and inspect the acceleration job.



Job actions

The Pause and Stop buttons control the progress of the Pivot job. Other actions include: **Share**, **Export**, **Print**, and **Open in Search**. Clicking **Open in Search** opens the Search view and runs the current search string.

Learn more

The topic briefly described what you need to know to access the pivot interface and build Pivots in the rest of this chapter. Read the Pivot Manual for more information.

Next steps

Continue to the next topic, where you will use Pivot to build a report from the **Buttercup Games** data models you created in a previous chapter.

Create and save a pivot report

This topic shows you how to use Pivot to create and save a simple report. This example uses the data model datasets that you created in Part 2 of this tutorial Create a new data model.

This is a very simple example. You will create more complex pivots later in this tutorial.

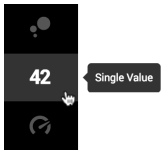
Create a new pivot

By default, the Pivot Editor interface displays elements to define a pivot table. There are four basic pivot element categories: Filters, Split Rows, Split Columns, and Column Values. When you first open the Pivot Editor for a specific dataset, only two elements are defined:

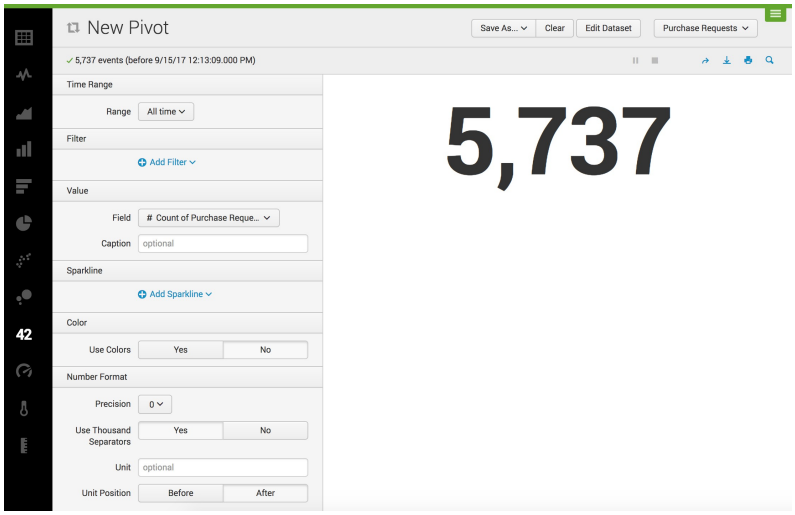
- A time range Filter element, which is set to **All time** by default.
- A Column Values element, which set to **Count of <dataset_name>**.

This gives you the single value, which is the total count of events returned by the dataset over all time. In this tutorial, this count is the "Count of Purchase Requests".

1. Select the Single Value visualization type in the Visualization bar.



The display changes to show you the options for the Single Value visualization.



This visualization type includes options to specify:

- **Time Range**. By default, the time range is set to All time.
- **Filter**. You can specify fields to filter on.
- **Value**. Single value visualizations, which includes the three gauge visualization types, use the first column value element for their single value. In this dataset, the field is "Count of Purchase Requests".
- **Sparkline**. Displays a sparkline chart under the single value.
- **Color**. You can specify whether to use color and set the colors for specific ranges.
- **Number Format**. You can format the precision for the number and select whether or not to use a comma.

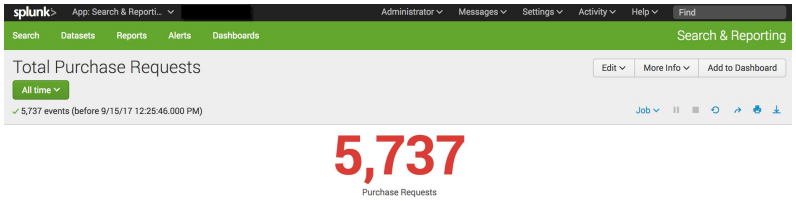
2. Under the **Value** section, for **Caption**, type **Purchase Requests**.
3. Under the **Color** section for **Use Colors**, click **Yes**.

Save the Pivot as a report

After you define a pivot, you can save it as either a report or a dashboard panel. In this tutorial, you save the single value display as a report. Dashboards and dashboard panels are discussed later in the tutorial.

1. Click **Save As** and select **Report**.
2. For **Title**, type `Total Purchase Requests`.
3. Optional. For **Description** you can type a description for the report.
4. For **Time Range Picker**, the **Yes** setting should already be selected.

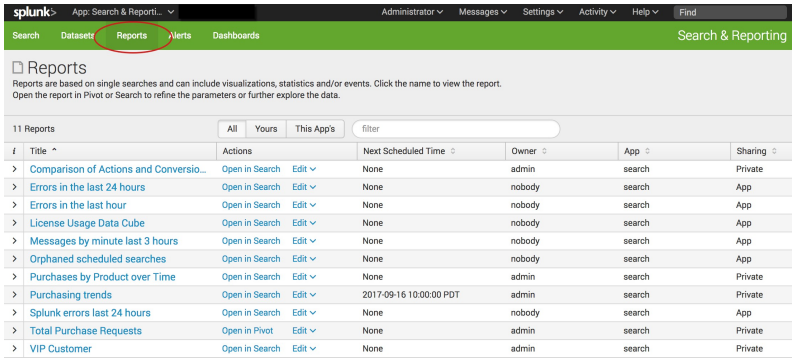
5. Click **Save**.
   After the report saves, a window indicating that your report has been created. You can change additional settings for the saved report, continue editing the current pivot, add the pivot to a dashboard, or view the report.
6. Click **View** to view the report.



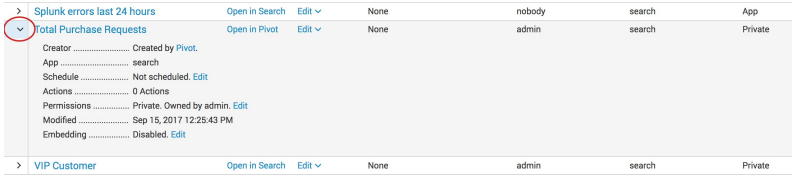
View saved reports

A report that is created from Pivot will always be saved under the current app and owner namespace.

1. Click **Reports** in the Apps bar to view the list of all saved reports.



2. In the information column, click the greater than (>) symbol to view information about the **Total Purchase Requests** report.



3. Click the name of the report, **Total Purchase Requests**, to view the report.

Next steps

In this topic, you created and saved a report using Pivot. Continue to the next topic to create more pivot visualizations.

Create a pivot table

In the previous topic you used Pivot to find the total number of purchase requests and saved the single value display as a report. In this topic, you will use the Pivot visualization editor to create a pivot table of the Buttercup Games Successful Purchases dataset.

The Successful Purchases dataset has fields for the products purchased from the Buttercup Games website. This includes the automatically extracted fields, such as categoryId and productId, as well as the lookup fields, price and product_name, that you added when you built the dataset.

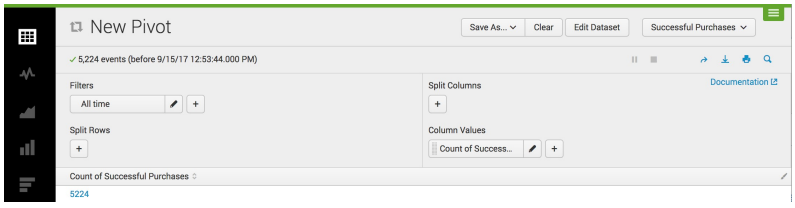
The Buttercup Games online store sells hundreds products, in of a variety of categories. You want to know more about the items that were purchased over the past week. You can create a pivot report that breaks down the total number of purchase events by product name. Using the report, you can quickly see which of the products were the top sellers for that period.

Define a new pivot

1. From the Splunk bar, select **Settings > Data models**.
2. Select the **Buttercup Games** data model.
3. In the Datasets editor page, click **Pivot**.

   In the Select a Dataset page, select the **Successful Purchases** child dataset.

   The **New Pivot** editor for **Successful Purchases** opens.



Add pivot elements

You can add multiple elements from each pivot element category to define your pivot table. It's easy to add, define, and remove pivot elements in the process of determining what information your table should provide.

- **To add a pivot element:** Click the + icon. This opens up the element dialog, where you choose a field and then define how the element uses that field.
- **To inspect or edit an element:** Click the "pencil" icon on the element. This opens the element dialog.
- **To reorder and transfer pivot elements:** Drag and drop an element within its pivot element category to reorder it. Drag and drop elements between element categories to transfer them.
- **To remove pivot elements from the Pivot Editor:** Open its element dialog and click the **Remove** button, or drag the element up or down until it turns red and drop it.

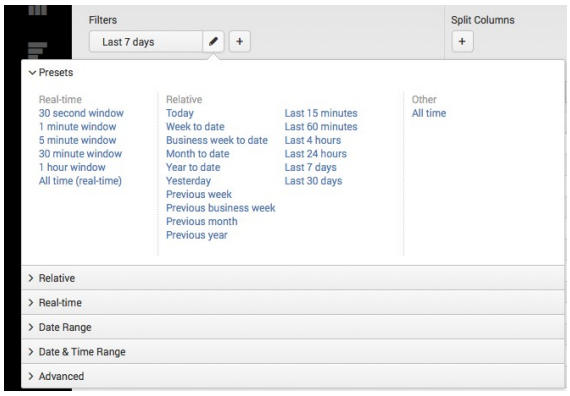
Under **Filters**, the time filter is always present when you build a pivot; you cannot remove it. It defines the time range for which the pivot returns results. It operates exactly like the time range menu that is in use throughout Splunk Web. For more information, see Select time ranges to apply to your search in the *Search Manual*.

Change the time range filter

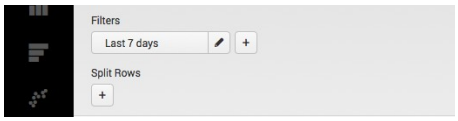
Currently your Pivot table shows a single value, the total count of Successful Purchases over **All time**.

Change the time range to view the Successful Purchases over a different time range:

1. Under **Filters**, click the pencil icon to open the time range picker.



2. In the **Presets** list under the **Relative** column, click **Last 7 days**.

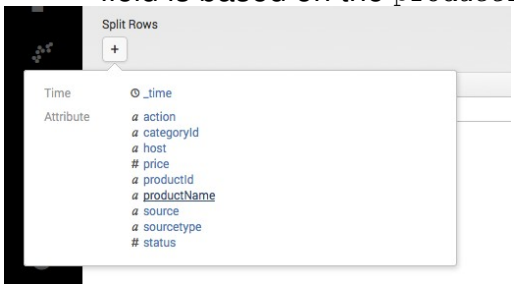


If no events are returned, it simply means that you downloaded the `tutorialdata.zip` file more than a week ago. Select a longer time range, such as **Previous month** or you can keep the default time range, **All time**.

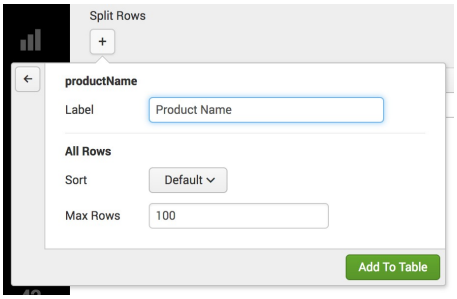
Add a Split Row element

You can add pivot elements to see the Count of Successful Purchases for each product by name:

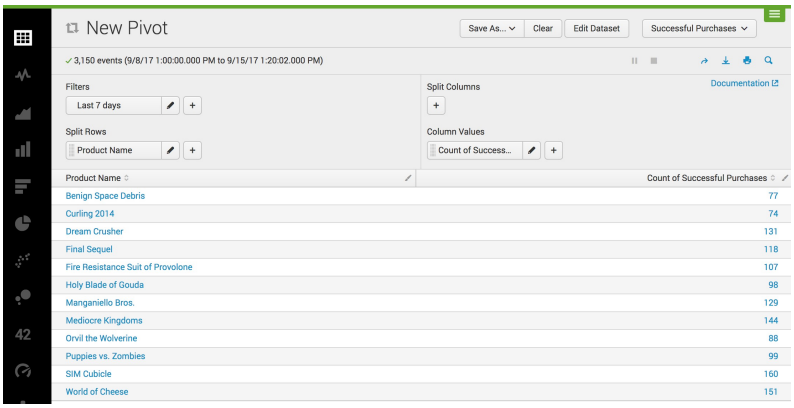
1. Under **Split Rows**, click **+** and select **productName**.
   This is the lookup field that contains the name of each product. This field is based on the `productId` field in the events.



   A dialog box opens where you can format the field.
2. For **Label**, type **Product Name**.



3. Click **Add To Table**.

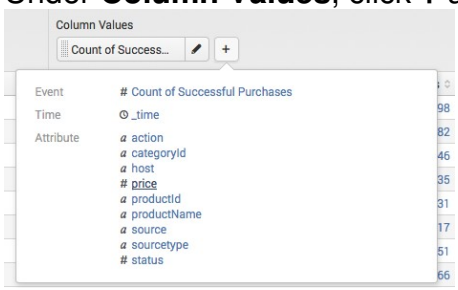


The table shows the count of successful purchases for the past 7 days for each product.

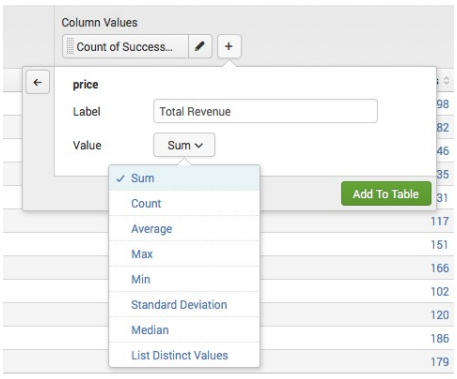
Add a Column Value element

Now you want the table to show the total revenue earned for each product that was successfully purchased.

1. Under **Column Values**, click **+** and select `price`.

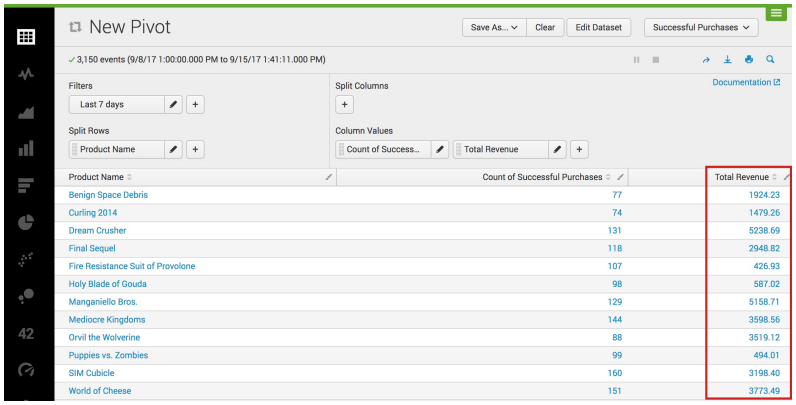


2. In the dialog box, specify how you want the information to appear in the table.
3. For **Label**, type **Total Revenue**.
4. For **Value**, select **Sum**.



This creates a field called **Total Revenue**, which is the summation of the price for each successful purchase of the product.
You can add the `price` values as another Split Row, if you want to see the cost of each individual product in this table.

5. Click **Add To Table**.

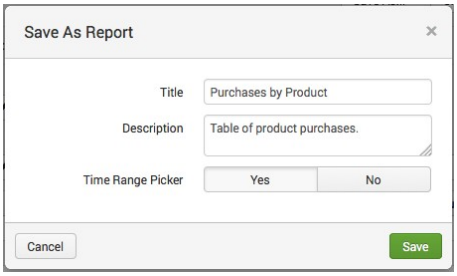


The table shows the new Total Revenue column with the total amount earned from the purchases of each product.

Save the pivot table

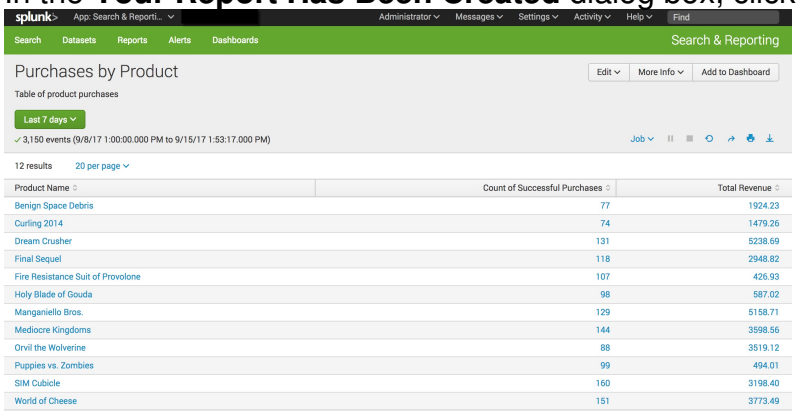
Now it is time to save the pivot table as a report.

1. Click **Save As** and select **Report**.



2. For **Title**, type `Purchases by Product`.

3. Optional. For **Description** type **Table of Product Purchases**.
4. For **Time Range Picker**, the **Yes** setting should already be selected.
5. Click **Save**.
6. In the **Your Report Has Been Created** dialog box, click **View**.



Next steps

Continue to the next topic to create some simple pivot visualizations.

Create a pivot chart

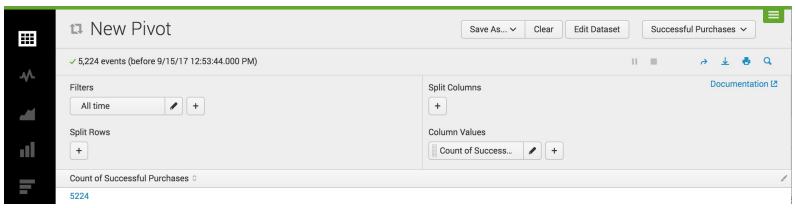
In the previous topic you used Pivot visualization editor to build a table. In this topic, you will use the same dataset to create chart visualizations.

Define a new Pivot

1. From the Splunk bar, select **Settings > Data models**.
2. Select the **Buttercup Games** data model.
3. In the Datasets editor page, click **Pivot**.

   In the Select a Dataset page, select the **Successful Purchases** child dataset.

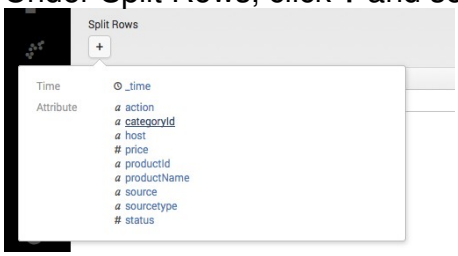
   The **New Pivot** editor for **Successful Purchases** opens.



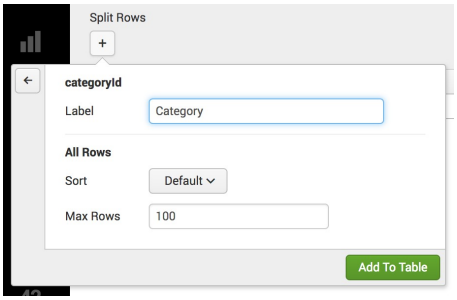
Add Pivot elements

For the pivot chart, let's report on the count of successful purchases by category. To do this, you will add a Split Row using the `categoryId` field.

1. Under Split Rows, click **+** and select `categoryId` from the list.

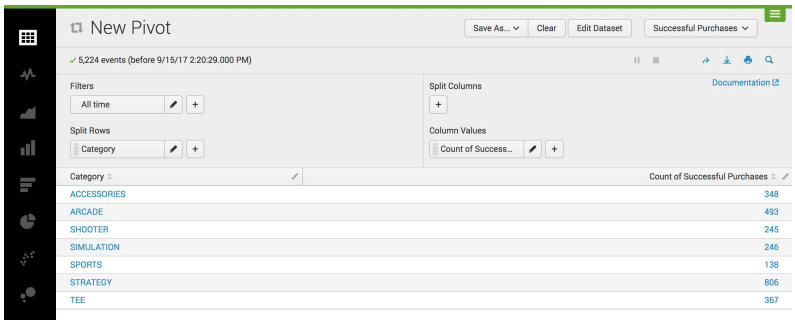


2. For **Label** type `Category`.



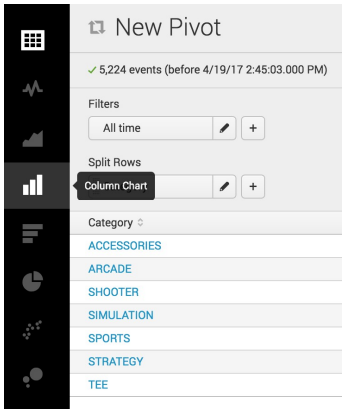
3. Click **Add to table**.

   The Pivot table displays a list of the product categories and a count of the successful purchases.
   The next step is to change the table into a chart.



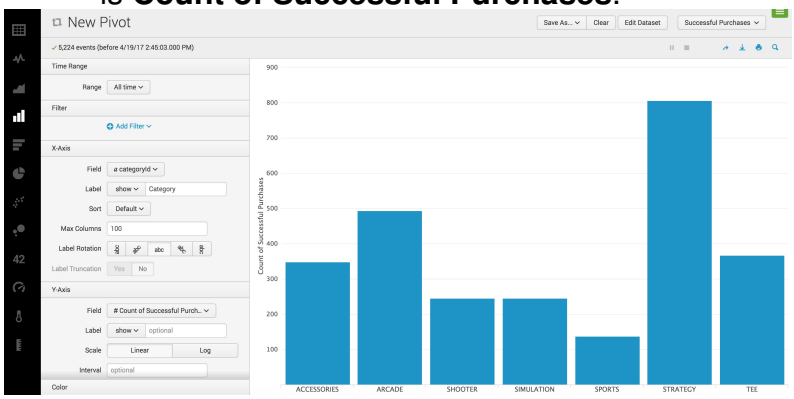
Change the visualization type

1. Click the **Column Chart** icon from the visualization bar.



The display changes to show you the options for the Column chart visualization.

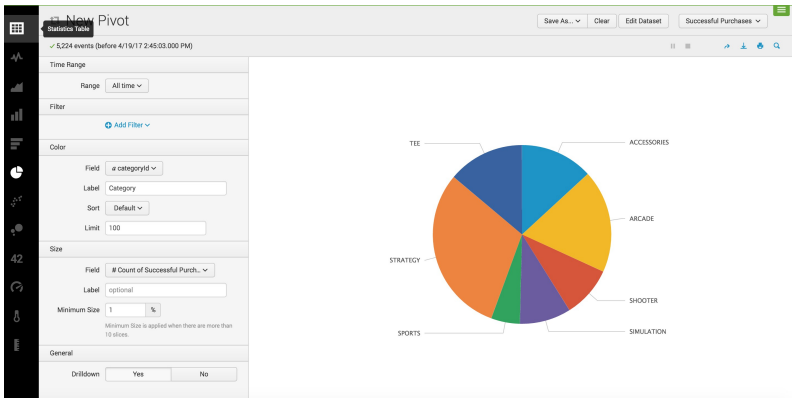
- Column charts use the first split row element in pivot table definitions to provide their **X-axis** values. In this case, that **Split Row** is **Category**.
- Column charts use the first column value element in pivot table definitions to provide their **Y-axis** values. Here, that **Column Value** is **Count of Successful Purchases**.



This data can also be visualized as a pie chart.

2. Click the **Pie Chart** icon from the visualization bar.
   The display changes to show you the options for the Pie chart visualization.
   - Pie charts use the values from the first **Split Row** element (Category) to determine the number and colors of their slices.

- Pie charts use the first **Column Value** element (Count of Successful Purchases) to determine the relative sizes of their slices.



Hover over a slice of the pie chart to view the metrics. You will see Category, Count of Successful Purchases, and the percentage that the slice of pie is of the total Count of Successful Purchases.

Next steps

In this chapter you created three pivots and saved two of them as reports. This last pivot chart, you will save as a dashboard panel. Continue to the next chapter to read about dashboards.

Part 4: Creating a dashboard

About dashboards

Pivots make it easy to interactively build and edit **dashboards** without writing a single line of XML code.

- **Add a pivot you have just created to a new or existing dashboard:** You can jump right into dashboard creation after creating a pivot visualization by using the Create Dashboard Panel. It guides you through the process of creating a dashboard panel based on the search and adding it to a new or preexisting dashboard. When you finish, you are still in the Pivot view.

- **Use the Dashboard Editor to create dashboards and populate them with dashboard panels:** You can also use the Dashboard Editor to edit existing dashboards. This method of dashboard creation is useful if you have a set of pivot reports that you want to quickly base a set of dashboard panels upon.

Change dashboard permissions

You can specify access to a dashboard from the Dashboard Editor. However, your user role and capabilities defined for that role might limit the type of access you can define.

If your user role is *admin* with the default set of capabilities, then you can create dashboards that are private, visible in a specific app, or visible in all apps. You can also provide access to other user roles, such as *user*, *admin*, and other roles with specific capabilities.

For additional information on setting up permissions for dashboards and other knowledge objects refer to Manage knowledge object permissions in the Admin Manual.

Change dashboard panel visualizations

After you create a panel with the Dashboard Editor, use the Visualization Editor to change the visualization type displayed in the panel, and to determine how that visualization displays and behaves. The Visualization Editor only allows you to choose from visualization types that have their data structure requirements

matched by the search that has been specified for the panel.

- For an overview of the various visualization types and their formatting/display options, see the Visualization reference topic in the Dashboards and Visualizations manual.
- For more information about the data structures required by the visualization types see Data structure requirements for visualizations in the Dashboards and Visualizations manual.

Edit the XML configuration of a dashboard

Although you are not required to use XML to build dashboards, you can edit a dashboard's panels by editing the XML configuration for the dashboard. Using XML provides access to features that are not available from the Dashboard Editor. For example, you can edit the XML configuration to change the name of dashboard or specify a custom number of rows in a table.

For more information about editing XML for dashboards created with the Dashboard Editor, see Dashboard examples in the Dashboards and Visualizations manual.

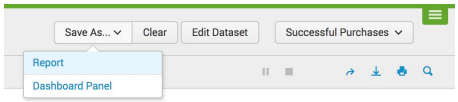
Add pivots to a dashboard

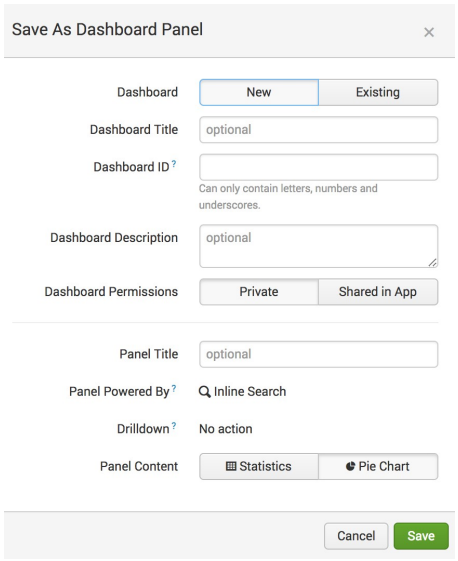
This topic continues where you left off in Part 3: Designing a Pivot Report. The last pivot you created was a pie chart. If you haven't created that chart, you can return to the previous topic and do so. Now, you will save that visualization to a new dashboard panel and then add all previous pivot reports to the same dashboard.

Save a Pivot as a dashboard panel

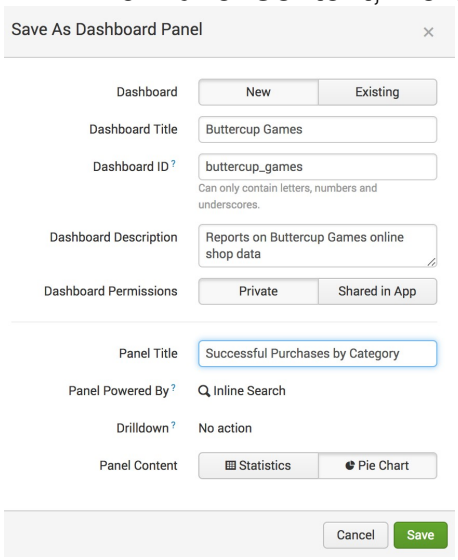
You just created a pie chart, now let's save it to a dashboard panel.

1. Click **Save as** and select **Dashboard Panel**.

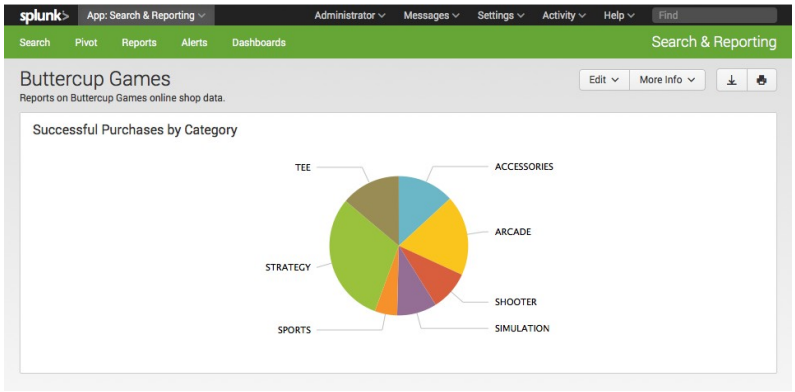




2. In the Save As Dashboard Panel dialog box, specify the following values:
    1. For **Dashboard**, **New** is already selected. You are creating a new dashboard to hold the new dashboard panel. There is no need to change this.
    2. For **Dashboard Title** type `Buttercup Games`.
    3. The **Dashboard ID** automatically updates to show `buttercup_games`. There is no need to change this value.
    4. Optional. For **Dashboard Description** type `Reports on Buttercup Games online shop data`.
    5. The **Dashboard Permissions** is already set to **Private**. There is no need to change this setting. If you want to share a dashboard with others, you can change the setting later.
    6. For **Panel Title** type `Successful Purchases by Category`.
    7. For **Panel Content**, **Pie** is already selected.



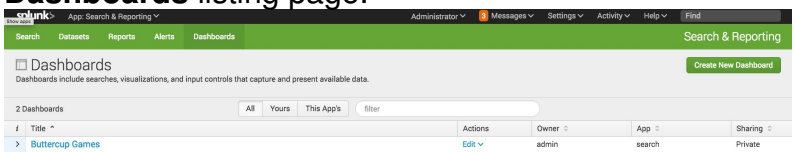
3. Click **Save**.
4. Click **View Dashboard**.



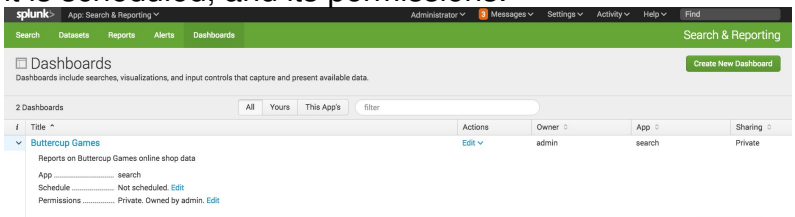
View and edit dashboard panels

After you save a dashboard, you can access it by clicking **Dashboards** in the app navigation bar.

1. Click **Dashboards** in the app navigation bar. This takes you to the **Dashboards** listing page.



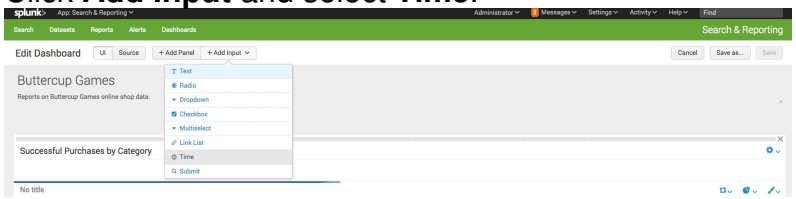
   You can **Create a new dashboard** and edit existing dashboards. You see the **Buttercup Games** dashboard you just created.
2. Under the **i** column, click the arrow next to **Buttercup Games** to see more information about the dashboard: What app context it is in, whether or not it is scheduled, and its permissions.



   There are also quick links to edit the dashboard's Schedule and Permissions inline with the information. To view the dashboard, click the dashboard's **Title** or select the **Edit** option under **Actions**. **Note:** If you click to view a dashboard and you cannot view it (or it displays blank), check that you have read access to the data model. To do this, go to the **Manage Data Models** view and edit the Permissions for the **Buttercup Games** data model to share in the App.

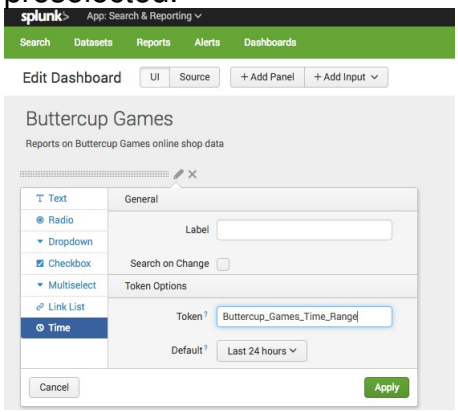
Add an input to the dashboard

1. In the **Dashboards** list, click **Buttercup Games** to return to that dashboard.
2. Click **Edit**. The **Edit: Buttercup Games** view opens.
   In this view, you have edit buttons: **Add Input**, **Add Panel**, and **Source**.
3. Click **Add Input** and select **Time**.



This adds a shared time range picker input to the dashboard editor.

4. Click the **Edit Input** icon for the time range picker. It looks like a pencil. This opens a set of input controls. The **Time** input type should be preselected.



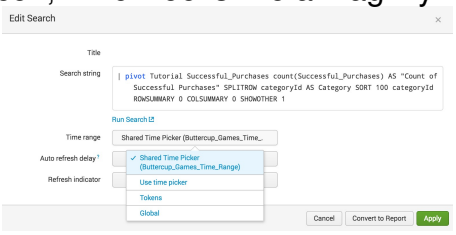
5. Change the **Token** value to **Buttercup_Games_Time_Range** and click **Apply.**

   This step redefines the name of the input token for the time range picker. Because the default names of input tokens are not very descriptive (field1, field2, field3, and so on), you may want to do this when you give your dashboard multiple inputs. It makes it easier to understand which input you are working with.

You can also optionally change the default time range for the picker by changing the value of **Default**. Right now it defaults to **Last 24 hours**.

In the next two steps you connect your dashboard panel to this time range picker.

6. In the **Successful Purchases by Category** dashboard panel, click the **Edit Search** icon, which looks like a magnifying glass. The **Edit Search** dialog opens.



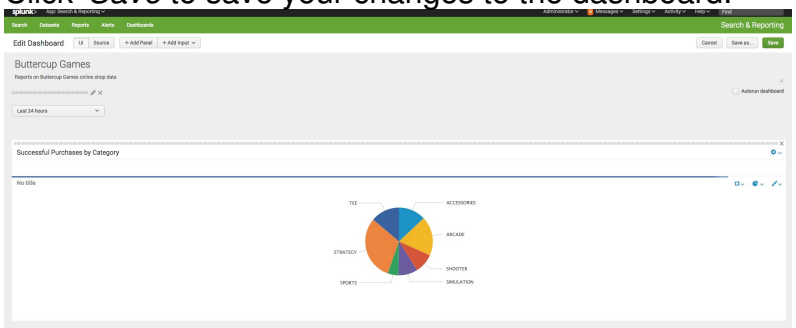
7. Click **Time Range** and select **Shared Time Picker (Buttercup_Games_Time_Range)**.
8. Click **Apply**.

   The panel is now hooked up to the shared time range picker input. The inline search that powers the panel now uses the time range selected for the shared time range picker.

   If your chart does not appear, try changing the time range picker to **Last 7 days**. The reason that this might occur is that you uploaded the `tutorialdata.zip` file more than 24 hours ago and there are no events in the tutorial data for the last 24 hours.

   You can have dashboards that offer a mix of panels that work with the shared time range picker and panels that show data for fixed time ranges.

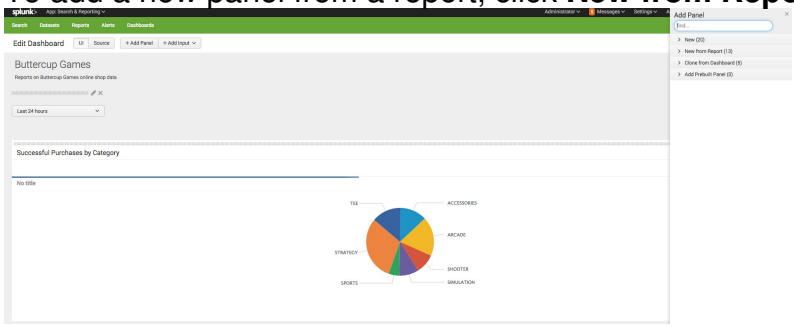
   If your dashboard does not appear, try refreshing the page.
9. Click '*Save* to save your changes to the dashboard.



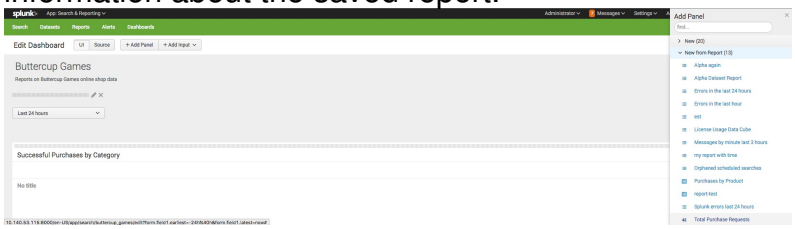
Add saved reports to the dashboard

Add another panel using one of the saved reports you created earlier.

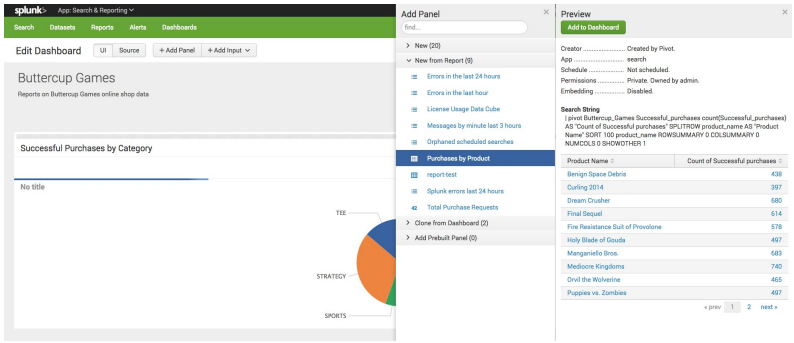
1. In the **Buttercup Games** dashboard, click **Edit**.
2. In the **Edit: Buttercup Games** view, click **Add Panel**. The **Add Panel** sidebar menu slides open.
3. To add a new panel from a report, click **New from Report**.



4. Click **Total Purchase Requests**. This slides open a preview panel with information about the saved report.



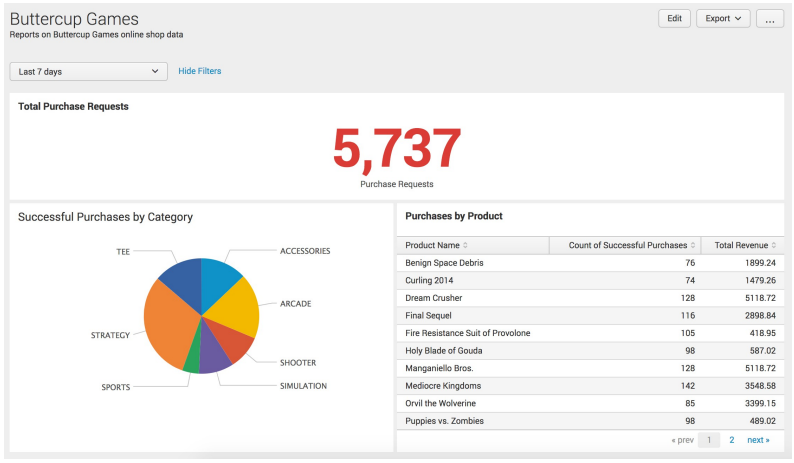
5. Click **Add to Dashboard**. The new panel is placed in the dashboard editor. You can click anywhere to close the **Add Panel** sidebar menu or choose another report to add to the dashboard. Before you close the **Add Panel** sidebar menu, add a second report.
6. Click **Purchases by Product**.



7. Click **Add to Dashboard**.
8. Close the sidebar menu. While in the dashboard editor view, drag and drop the panels to rearrange them on the dashboard.

   The type of panel that you add to a dashboard determines whether you can connect the panel to the shared Time Range Picker. If the panel is a report, you cannot connect it to the shared Time Range Picker. However, reports can be scheduled to run at a set time interval.

9. Click **Save**. Your dashboard should look like this:



Next steps

This completes the Data Model and Pivot Tutorial. Continue to the next chapter to read about what you can do next.

Next steps

More Data model and Pivot resources

This tutorial is a brief introduction to building data models and then using them to create pivot visualizations and reports. For more details, refer to the following manuals.

- **Knowledge Manager Manual:** Contains a section that shows you how to design and build data models using the Data Model Editor.
- **Pivot Manual:** Explains how to use the Pivot Editor to generate tables, charts, and other visualizations of your event data.
- **Dashboards and Visualizations:** Contains information on how to build and enhance dashboards and visualizations. This manual also contains a link to the Dashboards Quick Reference Guide, which provides an overview of the most common operations, definitions, and commands that you will use when you create dashboards and visualizations.

We encourage you to investigate the tutorial data, run more searches, and create more dashboards!

To learn more about the Splunk Search Processing Language, see the Search Tutorial.

To learn more about Splunk features and how to use them, see the selection of Education videos and classes.