

# The Beginning: Splunk in Action

Splunk, whose name was inspired by the process of exploring caves, or *spelunking*, helps analysts, operators, programmers, and many others explore many types of data, including raw machine data from their organizations, by collecting, analyzing, and acting on them. This multinational company, cofounded by Michael Baum, Rob Das, and Erik Swan, has a core product called Splunk Enterprise. This product manages searches, inserts, deletes, filters, and analyzes big data that is generated by machines, as well as many other types of data.

## NOTE

Throughout this lab, we will be covering the fundamental, barebones concepts of Splunk so you can learn quickly and efficiently. We reserve any deep discussion of concepts to Splunk's online documentation. Where necessary, we provide links to help provide you with the practical skills, and examples, so you can get started quickly. All images and exercise materials used in this book are available at <http://github.com/ericksond/splunk-essentials>. Instructions for Mac OS X can also be found in the GitHub repository mentioned in the preceding link.

With very little time, you can achieve direct results using Splunk, which you can access through a free enterprise trial license. While this license limits you to 500 MB of data ingested per day, it will allow you to quickly get up to speed with Splunk and learn the essentials of this powerful software.

The exercises in this chapter may look challenging at first, but if you follow what we've written closely, we believe you will quickly learn the fundamentals you need to use Splunk effectively. Together, we will make the most of the Trial License and give you a visible result that you can use to create valuable insights for your company (and, if you like, proudly show to your friends and coworkers).

# Your Splunk.com account

First you will need to register for a Splunk.com account. This is the account that you will use if you decide to purchase a license later. Go ahead and do this now. From here on, the password you use for your Splunk.com account will be referred to as your Splunk.com password.

## Obtaining a Splunk.com account

To obtain your Splunk.com account, perform the following steps:

1. Go to the Splunk signup page at <http://www.splunk.com>.
2. In the upper right hand corner, click on **My Account | Sign Up**.
3. Enter the information requested.
4. Create a username and password.

You will then need to download the Splunk Enterprise software. Go to <http://download.splunk.com> and select the Splunk Enterprise free download. Choose your operating system, being careful to select 32- or 64-bit (whichever is appropriate in your case; most should select 64-bit, which most computers today use). For Windows, download the \*.msi file. For Mac OS X, download the \*.dmg file. In this book, we will work with Version 6.4.1 or later.

The installation is very straightforward. Follow the steps for your particular operating system, whether it be Windows or Mac OS X.

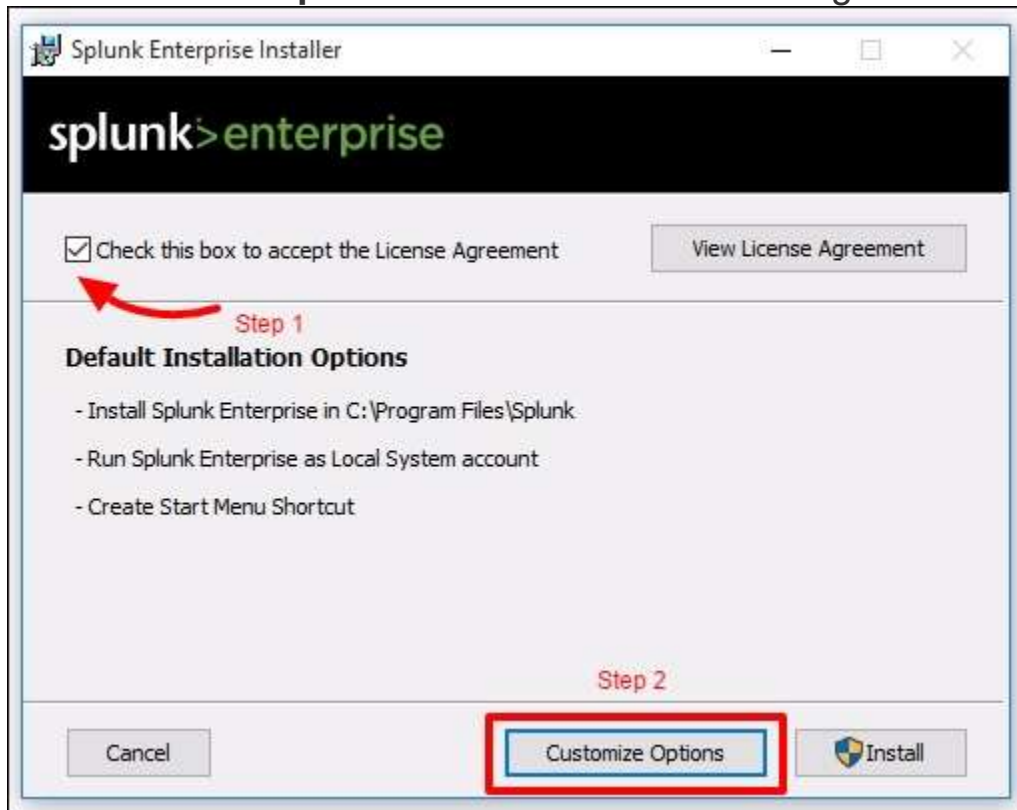
## NOTE

Make sure that there is no previous installation of Splunk in your system. If there is, uninstall the old version before proceeding with the next steps.

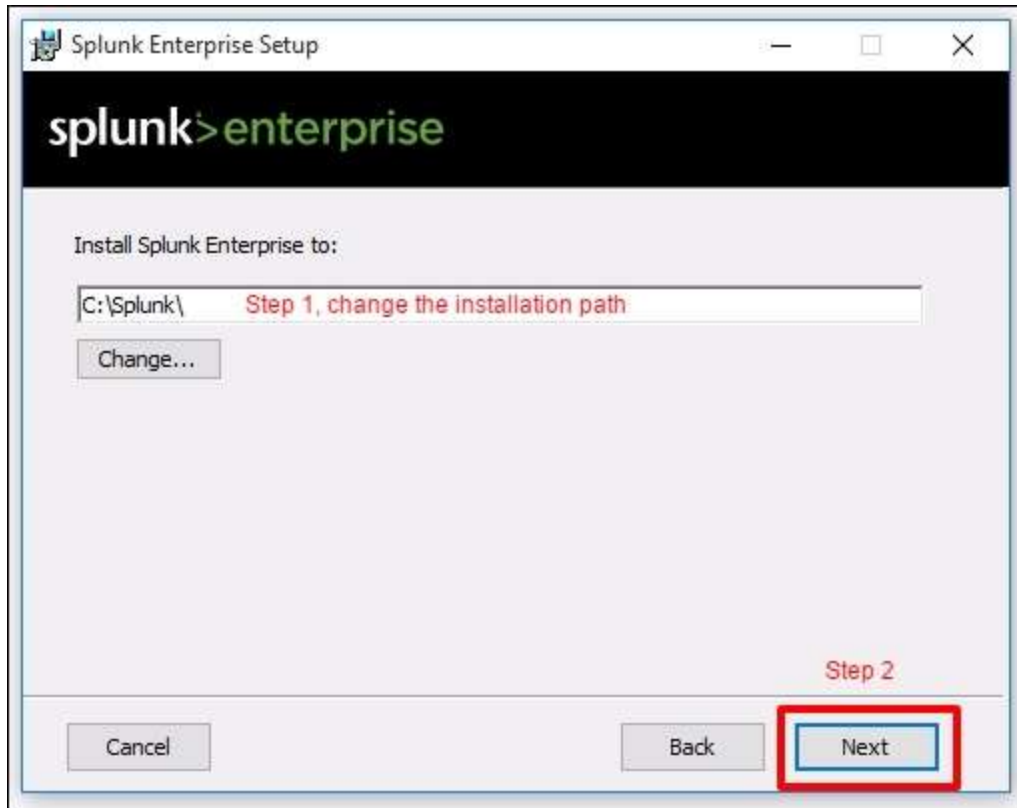
# Installing Splunk on Windows

These are the instructions you need to follow to install Splunk on your Windows desktop. Take your time and do not rush the installation. Many chapters in this book will rely on these steps:

1. Run the installer that you downloaded.
2. Check the box to accept the License Agreement and then click on **Customize Options** as shown in the following screenshot:



3. Change the **installation path** to `c:\Splunk`. You will thank us later as it simplifies issuing **Splunk CLI (command-line interface)** commands. This is also a best practice used by modern Windows administrators. Remember to eliminate white spaces in directory names as well, as it causes complications with scripting. Click on **Next** to continue as seen in the following screenshot:



4. Install Splunk Enterprise as the **Local System** and then click on **Next**.
5. Leave the checkbox selected to **Create Start Menu Shortcut**.
6. Click on **Install**.
7. Wait for the installation to complete.
8. Click on **Finish** to complete the installation. It will attempt to launch Splunk for the first time in your default browser.

## NOTE

Throughout the book, you will see references to `$SPLUNK_HOME`. This will be the installation directory of Splunk. In Windows, as a convention used in this book, `$SPLUNK_HOME` will be at `C:\Splunk`.

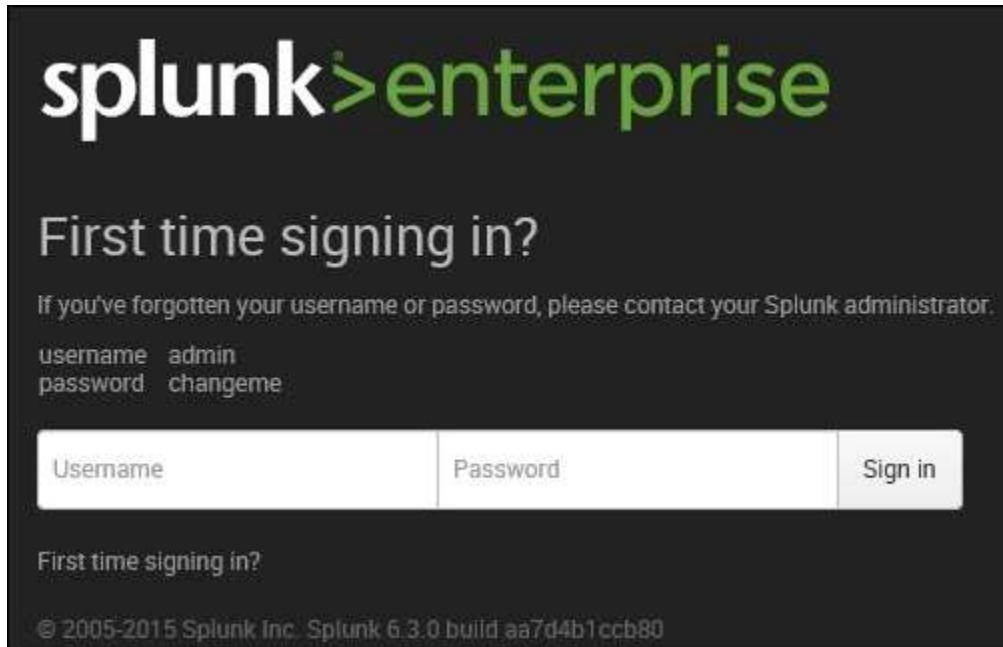
## Logging in the first time

Launch the application the first time in your default browser. You can also manually access the Splunk web page via the `http://localhost:8000` URL.

## NOTE

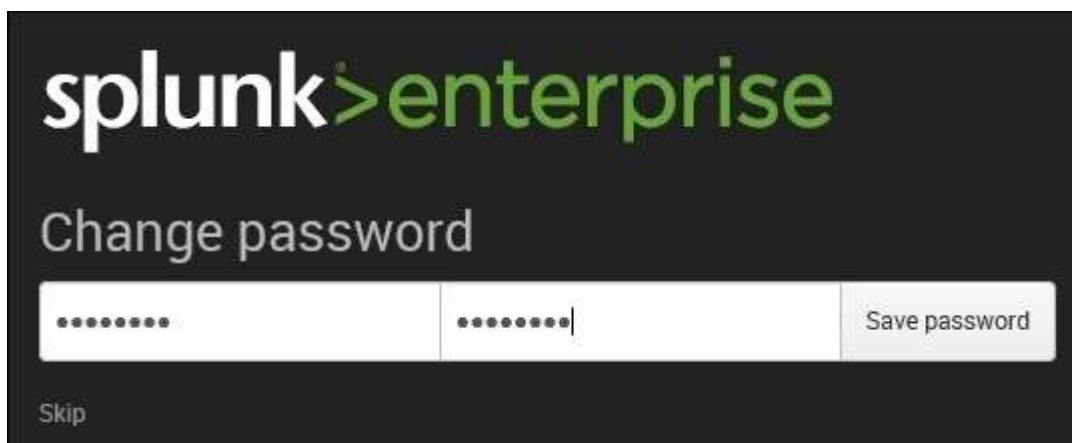
Splunk requires you to use a modern browser. It supports most versions of Google Chrome, Firefox, and newer versions of Internet Explorer. It may not support older versions of Internet Explorer.

Log in with the default username and password (**admin : changeme**) as indicated in the following screenshot:



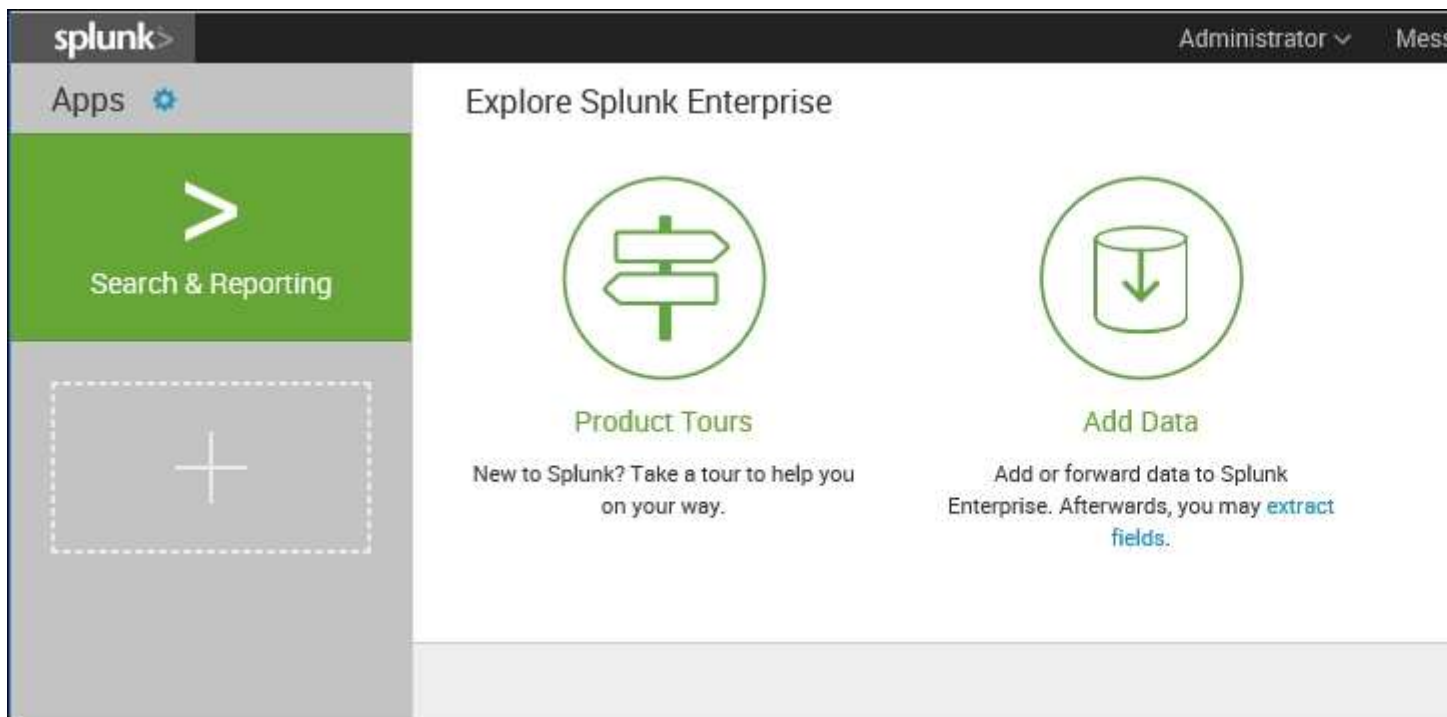
The screenshot shows the Splunk Enterprise login interface. At the top is the 'splunk>enterprise' logo. Below it, the text 'First time signing in?' is displayed. A message states: 'If you've forgotten your username or password, please contact your Splunk administrator.' Below this message, the default credentials are listed: 'username admin' and 'password changeme'. There are three input fields: 'Username', 'Password', and a 'Sign in' button. At the bottom, there is a link for 'First time signing in?' and a copyright notice: '© 2005-2015 Splunk Inc. Splunk 6.3.0 build aa7d4b1ccb80'.

The next step is to change the default administrator password, while keeping the default username. Do not skip this step. Make security an integral part of your day-to-day routine. Choose a password that will be secure:



The screenshot shows the 'Change password' page in Splunk Enterprise. It features the 'splunk>enterprise' logo at the top. Below the logo, the text 'Change password' is displayed. There are two input fields for the new password, each containing a series of dots. To the right of the second input field is a 'Save password' button. At the bottom left, there is a 'Skip' link.

Assuming all goes well, you will now see the default Splunk **Search & Reporting** dashboard:



## Run a simple search

You are finally ready to run your very first Splunk search query:

1. Go ahead and create your first Splunk search query. Click on the **Search & Reporting** app. You will be introduced to Splunk's very own internal index: this is Splunk's way of *splunking* itself (or collecting detailed information on all its underlying processes).
2. In the **New Search** input, type in the following search query (more about the **Search Processing Language (SPL)** in, [Chapter 3, Search Processing Language](#)):

3. `SPL> index=_internal sourcetype=splunkd`

### NOTE

The `SPL>` prefix will be used as a convention in this book to indicate a `Search` command as opposed to the `c:\>` prefix which indicates a Windows command.

The underscore before the index name `_internal` means that it is a system index internally used by Splunk. Omitting the underscore will not yield any result, as `internal` is not a default index.

- This search query will have as an output the raw events from the `metrics.log` file that is stored in the `_internal` index. A log file keeps track of every event that takes place in the system. The `_internal` index keeps track of every event that occurs and makes it easily accessible.
- Take a look at these raw events, as shown in the following screenshot. You will see fields listed on the left side of the screen. The important **Selected Fields** are **host**, **source**, and **sourcetype**. We will go into more detail about these later, but suffice it to say that you will frequently search on one of these, as we have done here. As you can see from the highlighted fields, we indicated that we were looking for events where `sourcetype=splunkd`. Underneath **Selected Fields**, you will see **Interesting Fields**. As you can tell, the purposes of many of these fields are easy to guess:

2,138 events (10/31/15 5:48:48.000 AM to 10/31/15 6:03:48.000 AM)

Events (2,138) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 9 ... Next

	Time	Event
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=thruput, instantaneous_kbps=1.048615, instantaneous_eps=4.129061, average_kbps=0.943057, total_k_processed=31135.000000, kb=32.506836, ev=128.000000 host=WIN-DT11F5NUKEN source=C:\Splunk\var\log\splunk\metrics.log sourcetype=splunkd
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=syslog_outp ut, instantaneous_kbps=0.000000, instantaneous_eps=0.000000, average_kbps=0.000000, total_k_processed=0.000000, kb=0.000000, ev=0.000000 host=WIN-DT11F5NUKEN source=C:\Splunk\var\log\splunk\metrics.log sourcetype=splunkd
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=index_thrup ut, instantaneous_kbps=1.048615, instantaneous_eps=3.516154, average_kbps=0.942937, total_k_processed=31131.000000, kb=32.506836, ev=109.000000 host=WIN-DT11F5NUKEN source=C:\Splunk\var\log\splunk\metrics.log sourcetype=splunkd
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=queue, name=winparsing, m ax_size_kb=500, current_size_kb=0, largest_size=0, smallest_size=0 host=WIN-DT11F5NUKEN source=C:\Splunk\var\log\splunk\metrics.log sourcetype=splunkd

Selected Fields  
 a host 1  
 a source 1  
 a sourcetype 1

Interesting Fields  
 a component 1  
 # cpu\_seconds 1  
 # cumulative\_hits 100+  
 # current\_size 2  
 # current\_size\_kb 1  
 # date\_hour 2  
 # date\_mday 1  
 # date\_minute 15