

Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[sourcetype=db_audit] OR [cs_mime_type] indicates either a source type or the name of a field.

NOTE: Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment.

Lab Module 3 – Install Splunk Enterprise

Description

This lab exercise will get Splunk Enterprise installed in your lab environment and create a user with a Power role.

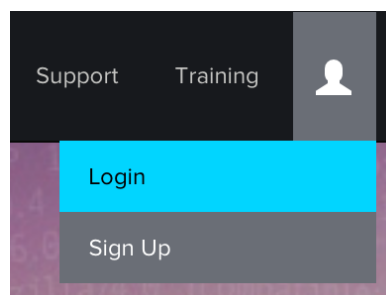
NOTE: Every system and network can be different. If you have any trouble installing please check the documentation for your operating system.

Steps

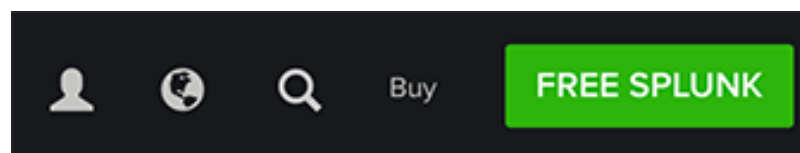
Scenario: You have recently joined the team at Buttercup Games as a Splunk Administrator. You have been asked to install Splunk Enterprise and create accounts for users.

Task 1: Download Splunk Enterprise for your operating system.

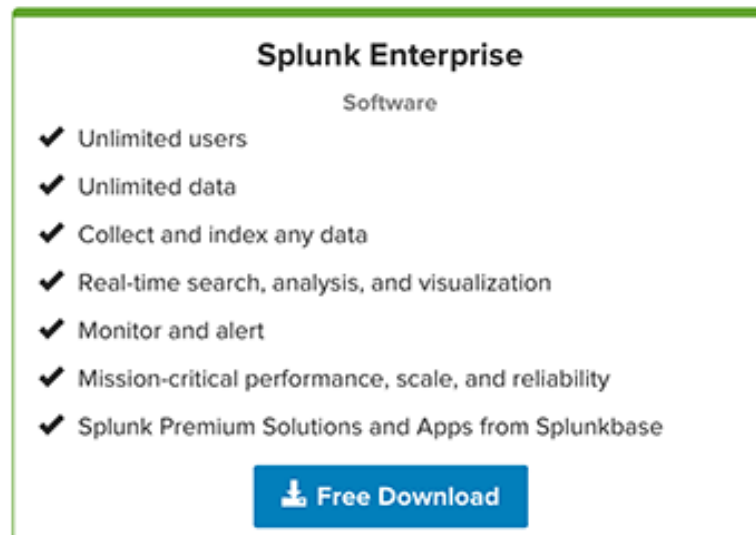
1. Direct your web browser to <http://splunk.com>.
2. Log in to your splunk.com account or create a new account using the **Login** link in the splunk.com user menu.



3. Once logged in, Click the green **Free Splunk** button in the top right of the interface.



- Under the **Core Products** header, click the **Free Download** button for Splunk Enterprise.



- Use the tabs to select your operating system, and click the **Download Now** button for your architecture.



NOTE: To install Splunk Enterprise, please proceed to the task matching your environment.



Windows OS – Task 2



Linux OS – Task 3

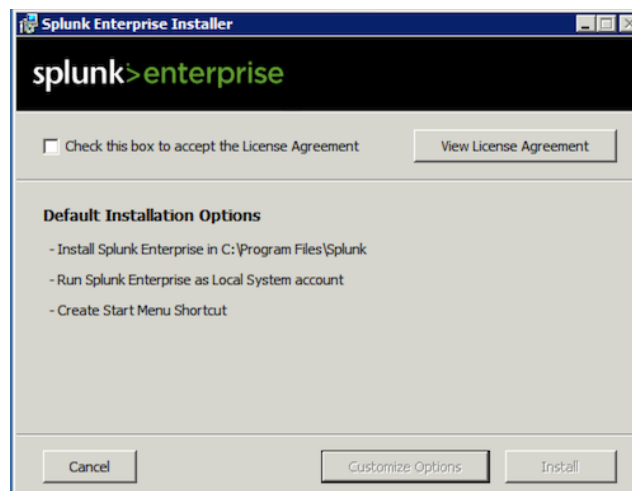


Mac OS – Task 4

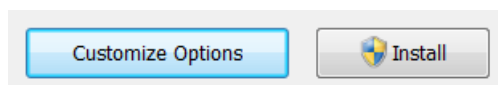


Task 2: Install Splunk Enterprise in a Windows environment.

- Locate the **splunk.msi** file that you downloaded earlier, and double click it.
- The installer will run and display the **Splunk Enterprise Installer** panel.



8. View the license agreement by clicking the **View License Agreement** button, and accept the license agreement using the **Check this box to accept the License Agreement** checkbox.
9. There is button to customize the installation, but for this lab we will use the default install options by clicking the **Install** button.



10. The installer will install the software and display the **Installation Complete** panel.



11. The **Launch browser with Splunk Enterprise** check box will be selected by default. Clicking the **Finish** button will open Splunk Web in your default browser.
12. Go to Task 5 to continue with the lab.



Task 3: Install Splunk Enterprise in a Linux environment.

NOTE: For this task we will be using the .tgz archive of Splunk Enterprise.

13. From a terminal window, on the server you are installing to, move to the directory containing the **splunk.tgz** file you downloaded earlier.

14. Untar the archive to the **opt** folder in the root directory of the server.

```
sudo tar xvf splunk.tgz -C /opt
```

15. Move to the **bin** directory inside the **splunk** folder.

```
cd /opt/splunk/bin
```

16. Start **Splunk** by using the **start** command with the **accept-license** argument. Optionally, leave off the **accept-license** argument to read the license agreement.

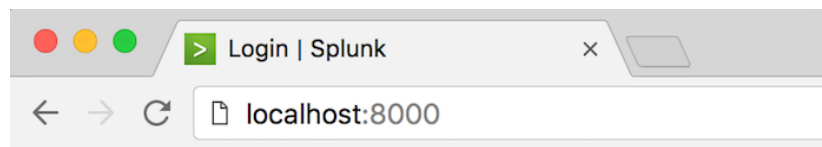
```
sudo ./splunk start --accept-license
```

17. **Splunk Enterprise** will check prerequisites and configurations. When finished, it will display a message letting you know that **Splunk Web** is ready:

```
The Splunk web interface is at http://*****:8000
```

18. Open a browser window and direct it to the IP address or domain name of your server with a port of 8000.

19. You will see **Splunk Web** in your browser.



20. Go to Task 5 to continue with the lab.



Task 4: Install Splunk Enterprise in a Mac environment.

21. Locate the **splunk.dmg** file that you downloaded earlier, and double click it.

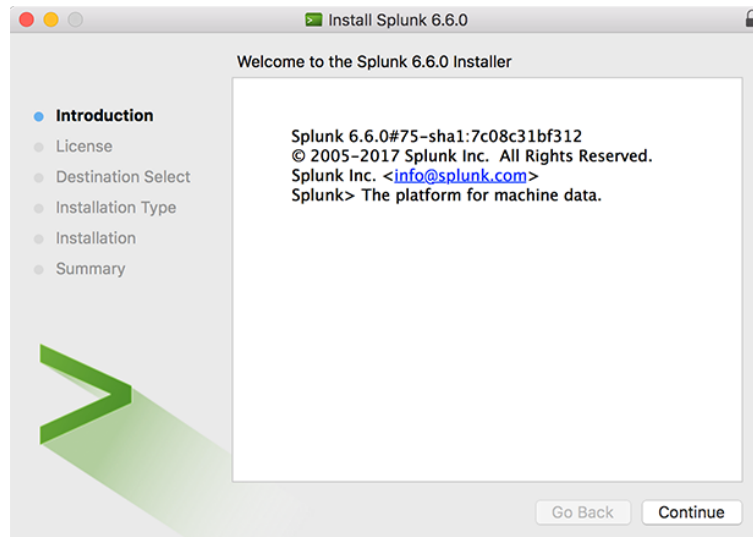
22. The Splunk Installer disk image will open.

23. Double click the **Install Splunk** icon.

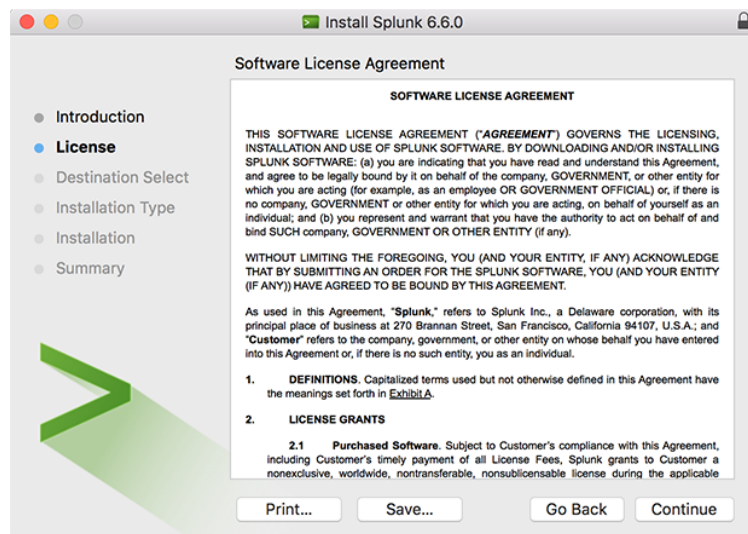


Install Splunk

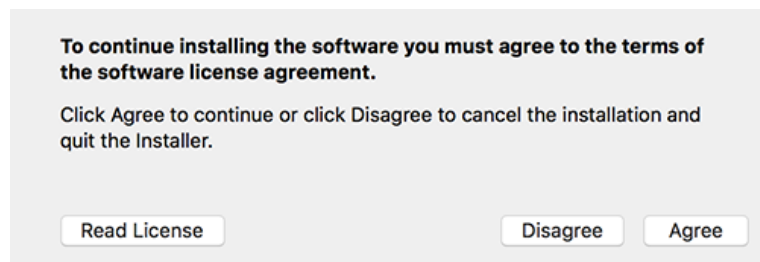
24. The installer will run and display the **Splunk Enterprise Installer** panel.



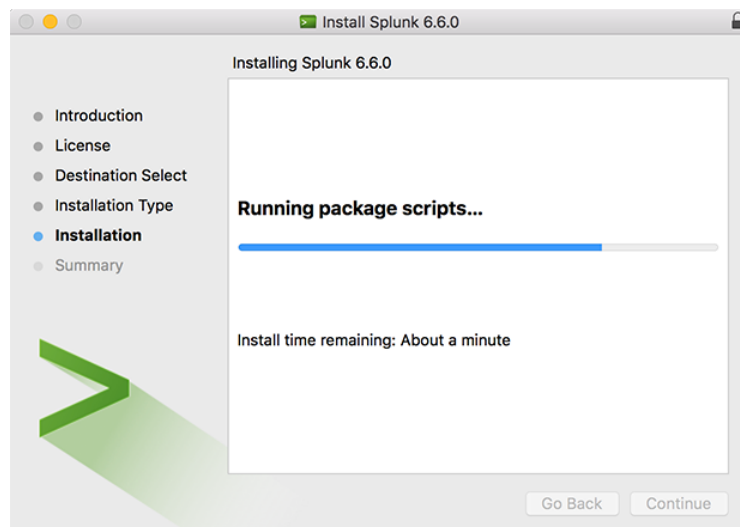
25. Clicking **Continue** will display the **Software License Agreement**.



26. Click the **Continue** and the **Agree** button to accept the license.



27. Clicking the **Install** button will start the installation process.



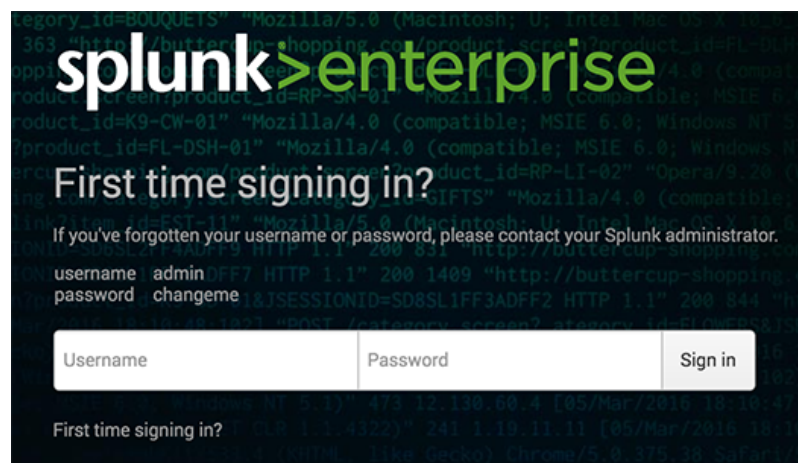
28. Once installed, Splunk will open **Splunk's Little Helper**. Clicking the **OK** button will allow Splunk to initialize on your system.



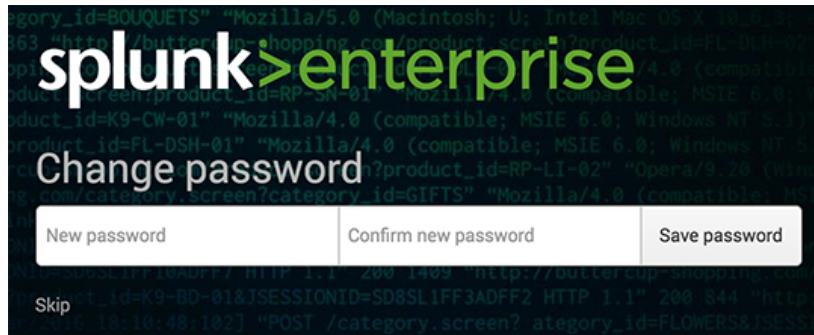
29. Click the **Start and Show Splunk** button. Splunk will open a terminal window, start Splunk and display Splunk Web in your default browser.

Task 5: Log into Splunk Web.

30. If you do not see Splunk Web in your browser, please navigate to **http://<host name or ip address>:8000**
31. The first time you log into Splunk Web you will use the default Username of **admin** and password of **changeme**.

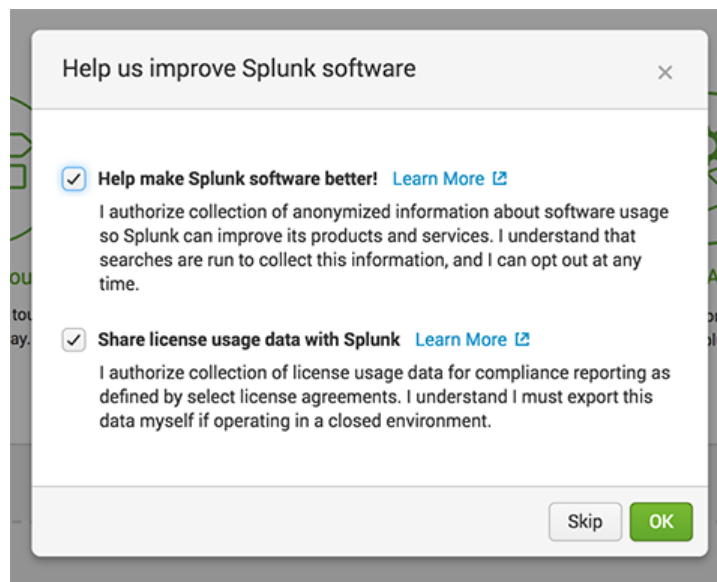


32. You will be asked to change and save a new password. It is a best policy to do so.



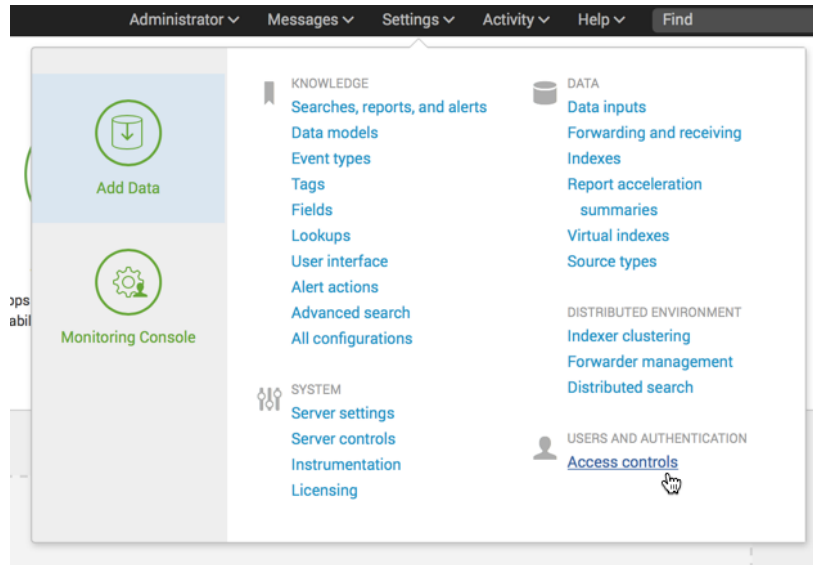
NOTE: If you lose your password Splunk support will not be able to help you retrieve it.

33. You may choose to authorize Splunk to send software and license usage data.



Task 6: Create a user with the power role.

34. From the Splunk bar, select **Access controls** from the **Settings** menu.



35. On the **Access controls** page, click **Add new** for a **User**.

Access controls

Specify authentication method, manage user settings, and manage roles.

	Actions
Authentication method	
Users	Add new
Roles	Add new

NOTE: We will be creating a Power User account to use with this course. Please use suggested username and password if you do not want to create your own. If you create a different username, Splunk Support will not be able to help you with log in issues.

36. Enter `uname` into the **Username** field.

Username *

Full name

Email address

37. Select your time zone from the **Time zone** drop down menu.

Email address

Time zone

- ✓ -- Default System Timezone --
- (GMT) Greenwich Mean Time
- (GMT-11:00) Midway Island, Samoa
- (GMT-10:00) Hawaii-Aleutian
- (GMT-10:00) Hawaii
- (GMT-09:30) Marquesas Islands
- (GMT-09:00) Gambier Islands
- (GMT-09:00) Alaska
- (GMT-08:00) Tijuana, Baja California
- (GMT-08:00) Pitcairn Islands
- (GMT-08:00) Pacific Time (US & Canada)**
- (GMT-07:00) Mountain Time (US & Canada)
- (GMT-07:00) Chihuahua, La Paz, Mazatlan

38. In the **Assign to roles** section, click on the **user** icon under **Selected roles** to remove it from the list.

Assign to roles

Assign this user to one or more roles. The user will inherit all the settings and capabilities from these roles.

Available roles [add all »](#) Selected roles [« clear all](#)

- admin
- can_delete
- power
- splunk-system-role
- user

- user

39. Click on the **power** icon under **Available roles** to add it to the **Selected roles** list.

Assign to roles

Assign this user to one or more roles. The user will inherit all the settings and capabilities from these roles.

Available roles [add all »](#) Selected roles [« clear all](#)

- admin
- can_delete
- power
- splunk-system-role
- user

- power

40. Enter a password of `5p1unkbcup` for the **Password** and **Confirm password** fields then click **Save**

Set password

Password *


Confirm password

41. After the user has been saved, you will be returned to the User management page.

Users

[Access controls](#) » Users

Successfully saved "uname". This user will be disabled after the Enterprise Trial License expires.



New

Showing 1-2 of 2 items

Results per page 25

Username	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	roles	Actions
admin	Splunk	Administrator	changeme@example.com	None	launcher	system	admin	Clone
uname	Splunk	None	None	America/Los_Angeles	launcher	system	power	Clone Delete