splunk>

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.

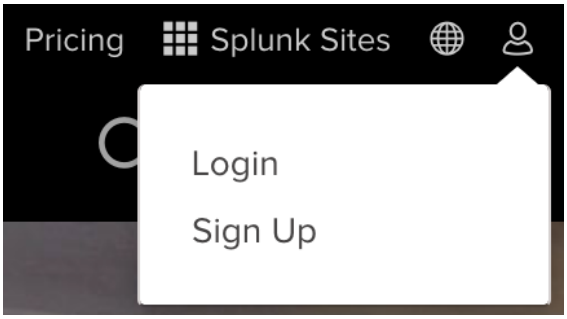
NOTE: Every system and network can be different. If you have any trouble installing please check the documentation for your operating system.

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.

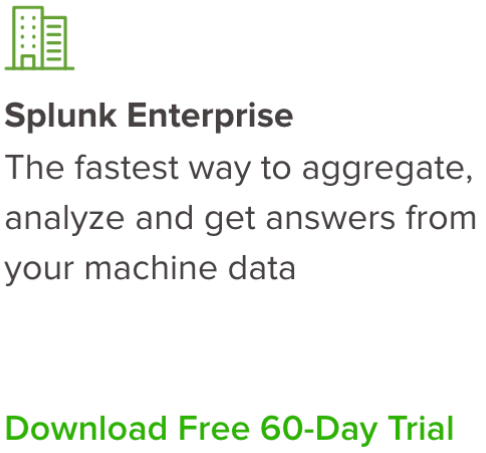
Task 1: Download Splunk Enterprise for your operating system.

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.

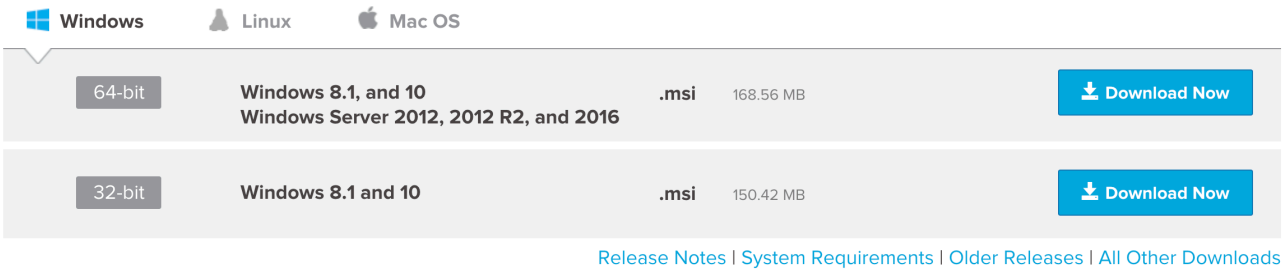


3. Once logged in, Click the green **Free Splunk** button in the top right of the interface.

4. Under **Splunk Enterprise**, click the **Free Download Free 60-day Trial** link.



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

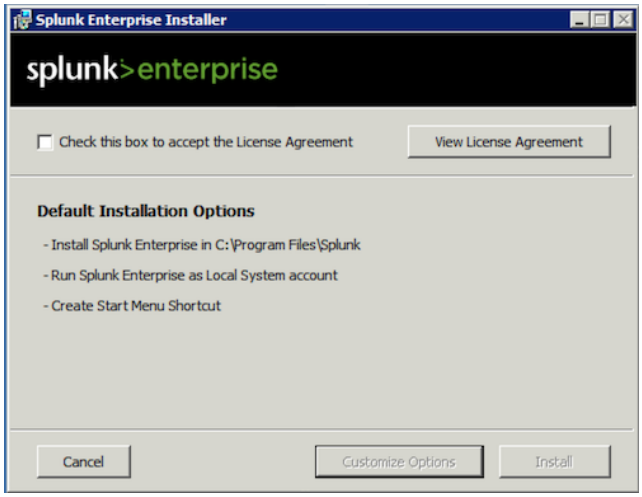


NOTE: To install Splunk Enterprise, please proceed to the task matching your environment.

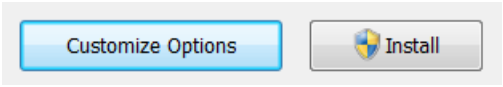
	Windows OS – Task 2
	Linux OS – Task 3
	Mac OS – Task 4

Task 2: Install Splunk Enterprise in a Windows environment.

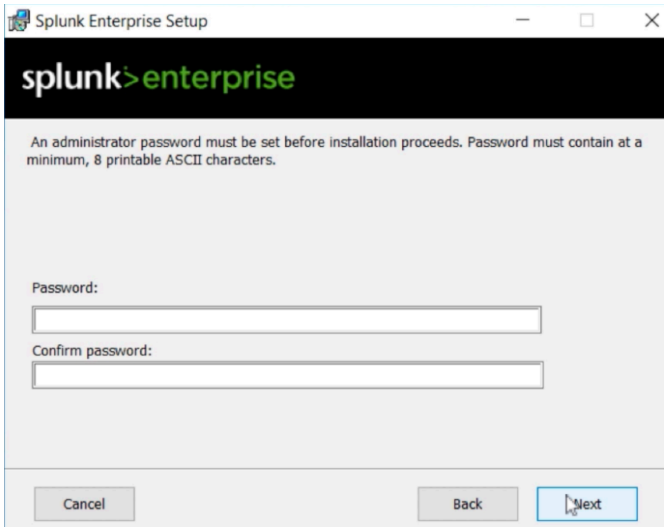
6. Locate the **splunk.msi** file that you downloaded earlier, and double click it.
7. The installer will run and display the **Splunk Enterprise Installer** panel.



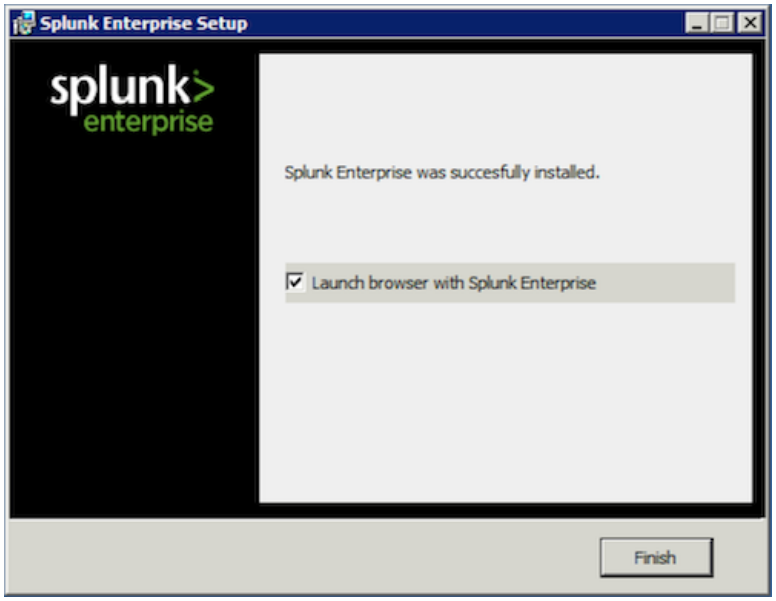
8. View the license agreement by clicking the **View License Agreement** button, and accept the license agreement using the **Check this box to accept the License Agreement** checkbox.
9. There is a button to customize the installation, but for this lab we will use the default install options by clicking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



10. The installer will ask you to create a password for your Administrator account.



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



12. 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.
13. 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.

14. From a terminal window, on the server you are installing to, move to the directory containing the **splunk.tgz** file you downloaded earlier.
15. Untar the archive to the **opt** folder in the root directory of the server.

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

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

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

17. 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
```

18. You will be asked to enter a password for your Administrator account.

```
Please enter a new password:
```

19. **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
```

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

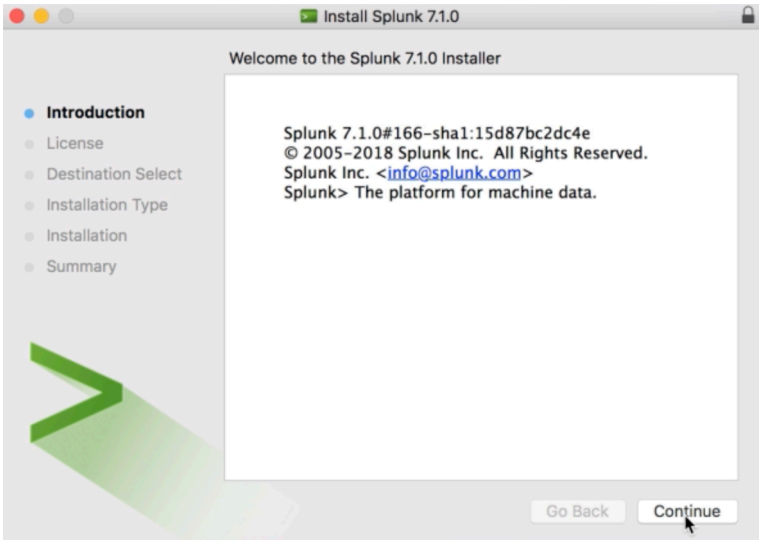
21. You will see **Splunk Web** in your browser.

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

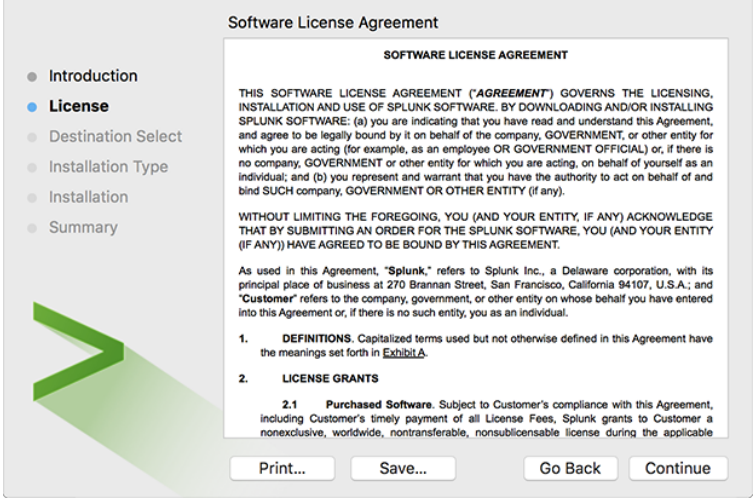
Task 4: Install Splunk Enterprise in a Mac environment.

23. Locate the **splunk.dmg** file that you downloaded earlier, and double click it.
24. The Splunk Installer disk image will open.
25. Double click the **Install Splunk** icon.

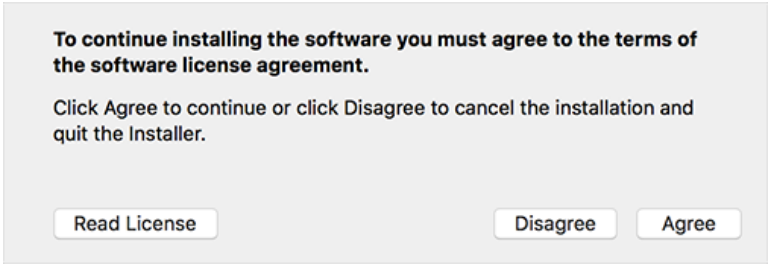
26. The installer will run and display the **Splunk Enterprise Installer** panel.



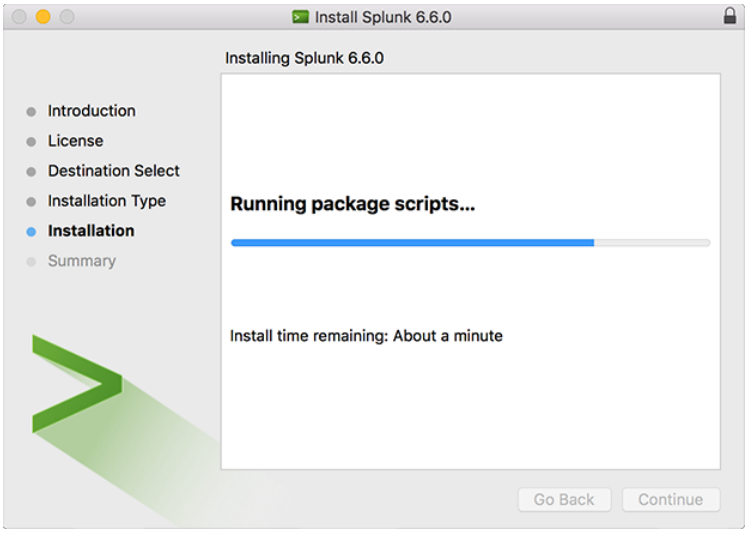
27. Clicking **Continue** will display the **Software License Agreement.**



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



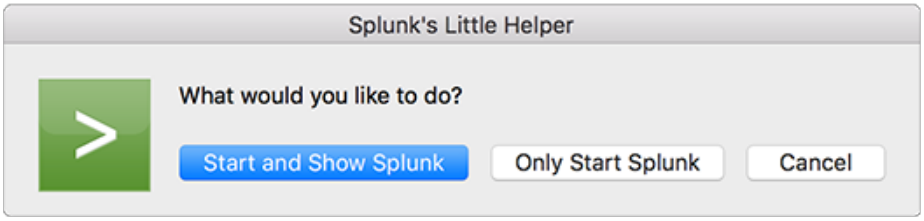
29. Clicking the **Install** button will start the installation process.



30. Once installed, Splunk will open **Splunk's Little Helper.** Clicking the **OK** button will allow Splunk to initialize on your system.
31. A terminal window will open and you will be asked to enter a password for your Administrator account.

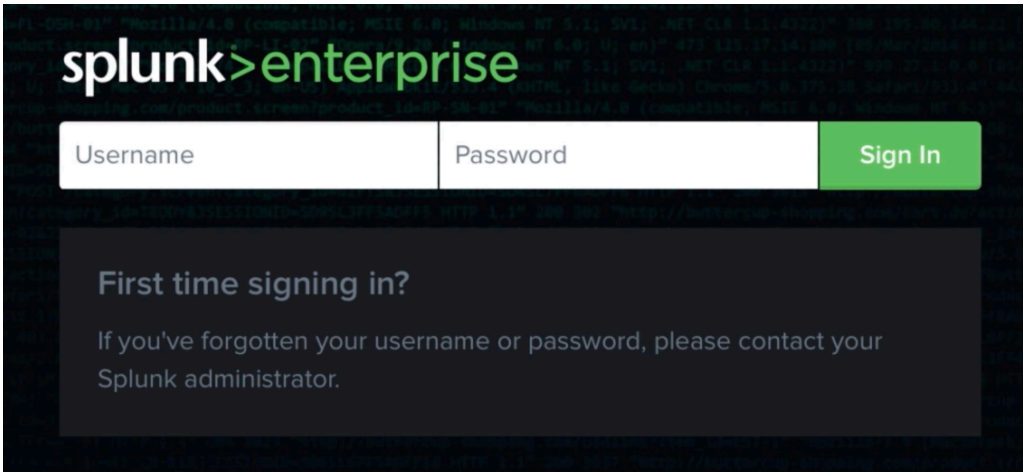
```
Please enter a new password:
```

32. The terminal window will close. Click the **Start and Show Splunk** button in Splunk's Little Helper. Splunk will open a terminal window, start Splunk and display Splunk Web in your default browser.



Task 5: Log into Splunk Web.

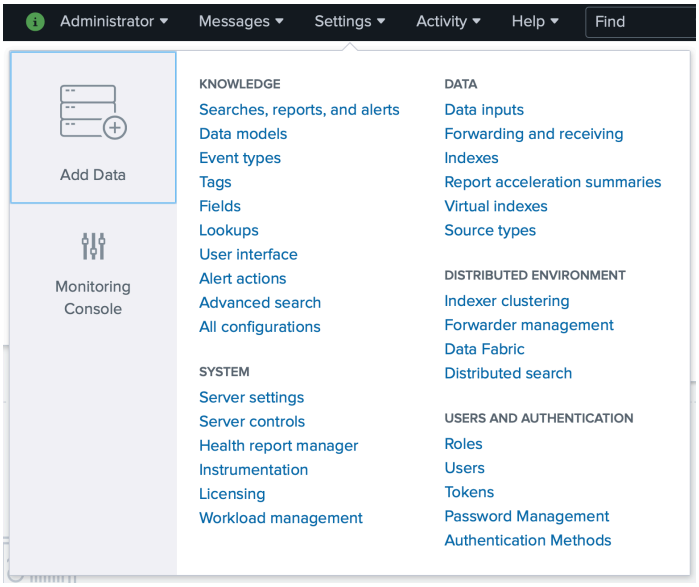
33. If you do not see Splunk Web in your browser, please navigate to **http://<host name or ip address>:8000**
34. Log into your administrator account using the Username of **admin** and the password you created during install.



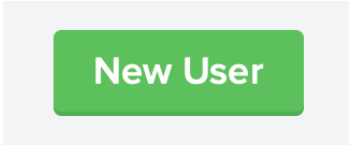
NOTE: If you lose your password Splunk support will not be able to help you retrieve it.

Task 6: Create a user with the power role.

35. From the Splunk bar, select **Users** from the **Settings** menu.

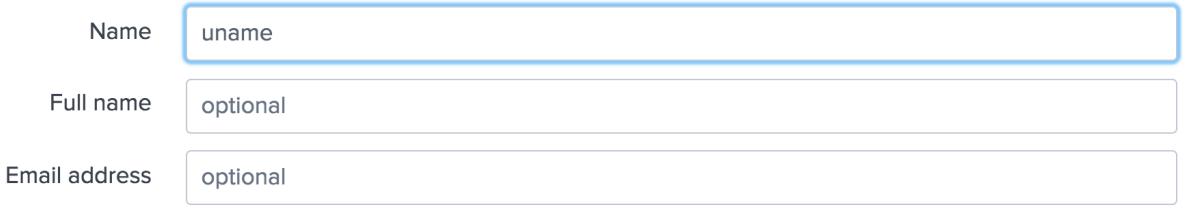


36. On the **Users** page, click the **New User** button.



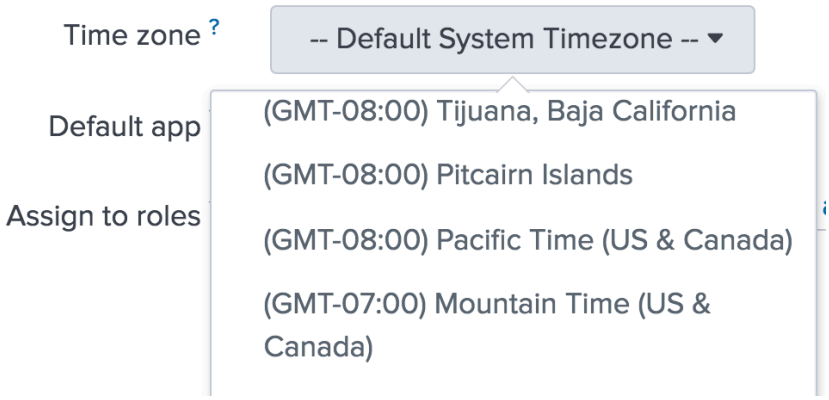
NOTE: We will be creating a Power User account to use with this course. Please use suggested username and password if you do not want to create your own. If you create a different username, Splunk Support will not be able to help you with log in issues.

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

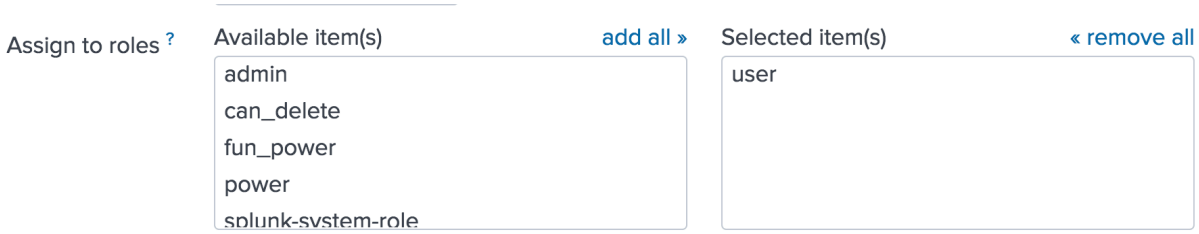


38. Enter a password of `5p1unkbcup` for the **Password** and **Confirm password** fields.

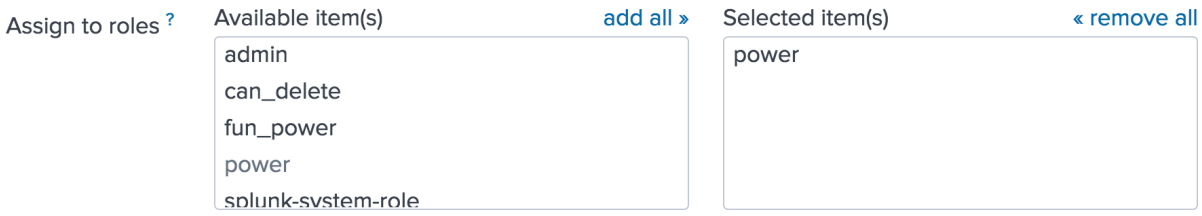
39. Select your time zone from the **Time zone** drop down menu.



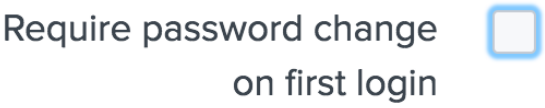
40. In the **Assign to roles** section, click on the **user** icon under **Selected item(s)** to remove it from the list.



41. Click on the **power** icon under **Available item(s)** to add it to the **Selected item(s)** list.



42. Remove the check mark from **Require password change on first login** and click **Save**



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