GLAB 200.2.2 - Splunk Fundamentals

Version 1.0, May 2023

Before you Begin - How to Complete This Activity

Having a Google account is strongly recommended.

Once logged in to your Google account, you can use this document's File menu to make a copy of the file. The copy will reside in your personal Google Drive. Once you have a copy of the lab file, you can type answers to questions and paste screenshots directly into the lab file.

NOTE: Do not request edit access to the file.

If you do not have a Google account, use this document's File menu to download the lab file in a format compatible with your document editor. Open the file for editing using your editor of choice (Microsoft Word, LibreOffice, PDF editor, or other), type answers to questions, and paste screenshots directly into the file.

When you have completed the lab, save the file in .pdf format.

Upload the completed .pdf document to Canvas using the Submit button.

Still confused? Refer to The Lab Process guide.

Introduction

Splunk Enterprise is a powerful platform for collecting, indexing, and analyzing machine-generated data. In this lab, you will connect to the Splunk training environment, log into a Splunk instance and explore the interface. Our main focus will be the Splunk Search & Reporting app. In this lab, you will connect to a Splunk server and explore the basics of the Splunk environment.

Note: As Splunk constantly evolves, images, functions, and tool locations may differ slightly from what is displayed here.

Objectives

- Launch the Splunk environment.
- Explore the Splunk Web interface.

Equipment

- A laptop or PC with Internet connectivity or A Windows Virtual Machine with Internet connectivity.
- A splunk.com/perscholas account - previously created on ACT 200.1.1: Access Splunk learning resources.

Instructions

Part 1: Launch the Splunk lab environment.

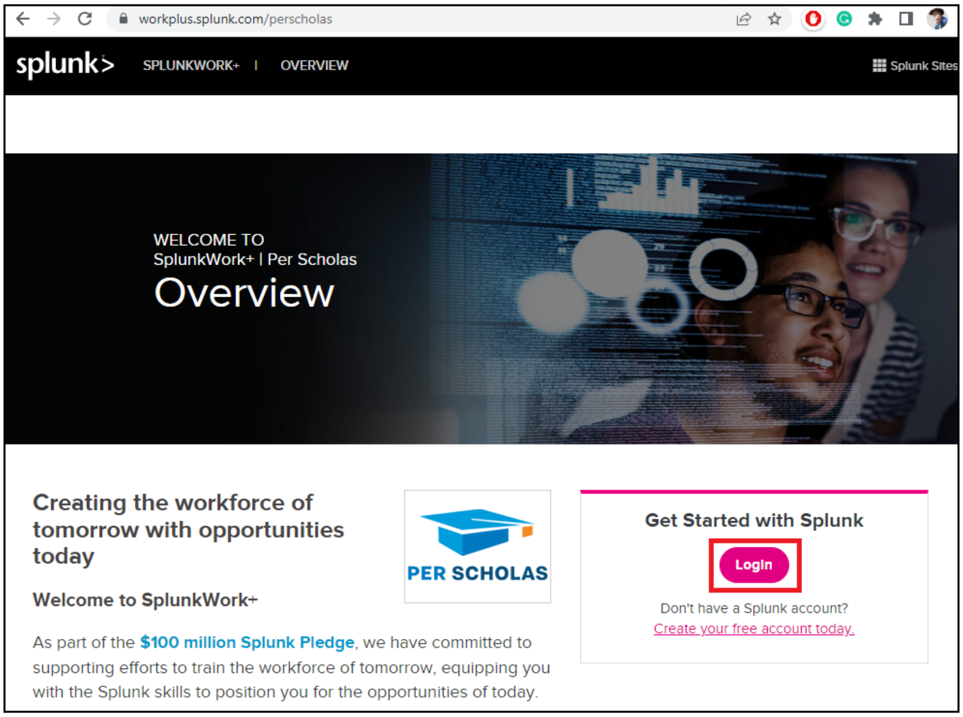
As a learner at Per Scholas, you can access 22 official Splunk courses, 16 of which include labs. In this Part, you will enroll in the Data Models (eLearning with labs) course and use the course's live lab environment to practice and complete this lab.

Note that each Splunk course that contains labs allows you to launch the lab environment three times. Each time, the lab environment will run for four hours.

In this part, we assume that you have a splunk.com/perscholas account. If you do not have one, please complete the ACT 200.1.1: Access Splunk learning resources activity first.

Step 1: Enroll in the Data Models course by Splunk.

a. *Using your Web browser, navigate to https://workplus.splunk.com/perscholas. On the* ***Get Started with Splunk*** *section, and click on the* ***Login*** *button.*

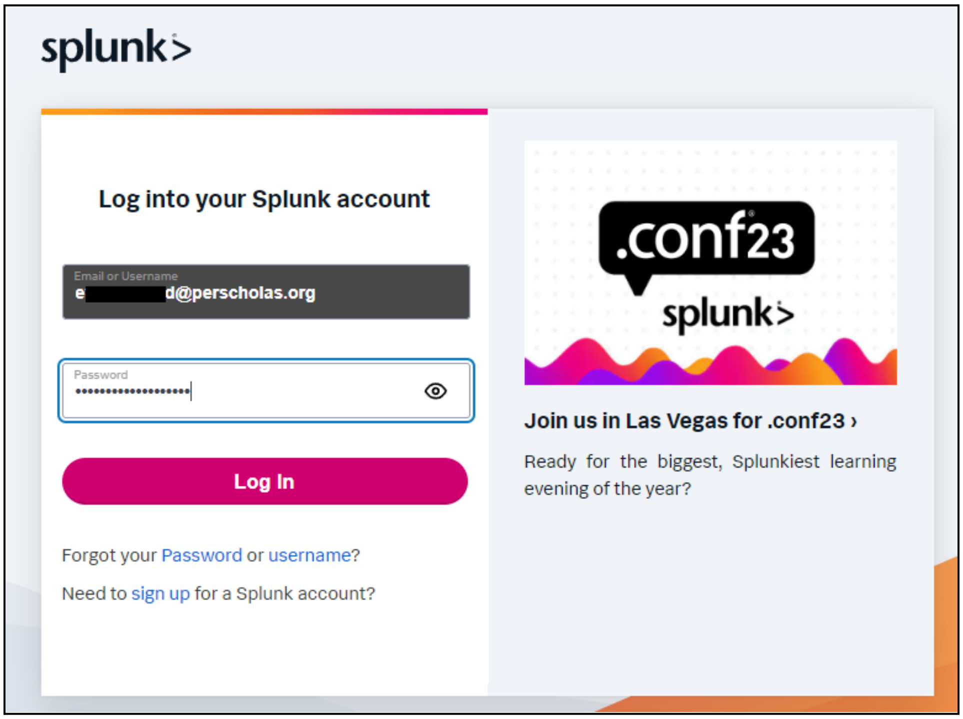

workplus.splunk.com/perscholas
splunk>
SPLUNKWORK+ | OVERVIEW
Splunk Sites
WELCOME TO
SplunkWork+ | Per Scholas
Overview
PER SCHOLAS
Get Started with Splunk
Login
Don't have a Splunk account?
Create your free account today.

Creating the workforce of tomorrow with opportunities today

Welcome to SplunkWork+

As part of the $100 million Splunk Pledge, we have committed to supporting efforts to train the workforce of tomorrow, equipping you with the Splunk skills to position you for the opportunities of today.

b. *On the **Splunk Account Login** section, enter the **Email or Username** you used to sign up for splunk.com, and click on the **Log In** button.*



Log into your Splunk account

Email or Username: e[redacted]d@perscholas.org

Password: ••••••••••••••••••

Forgot your Password or username?

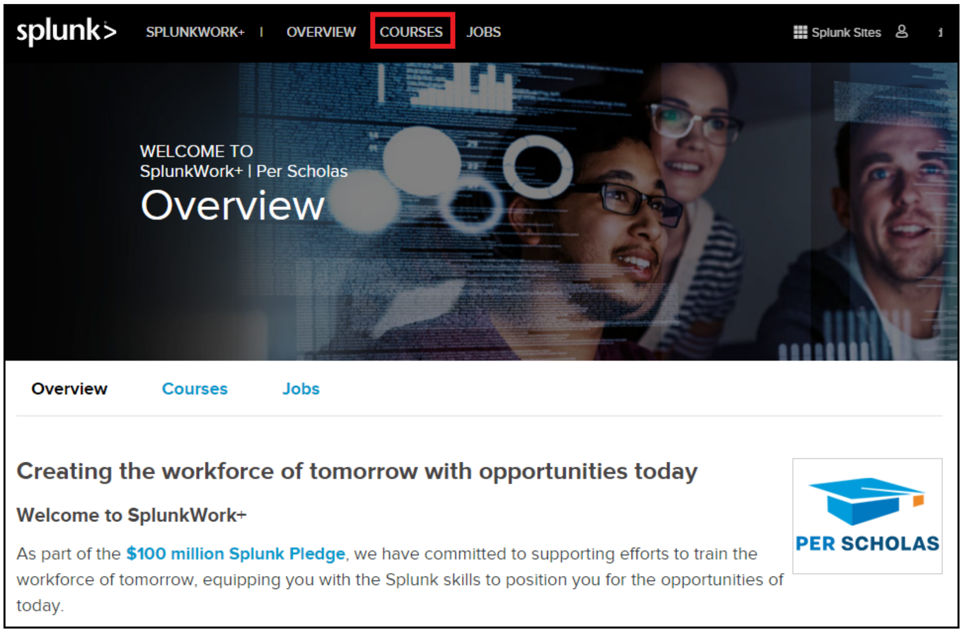
Need to sign up for a Splunk account?

Join us in Las Vegas for .conf23 ›

Ready for the biggest, Splunkiest learning evening of the year?

c. *Next, enter your **password** and click on the **Splunk Account Login** button.*

d. *Once you are signed in, click on the **Courses** tab on the **WELCOME TO SplunkWork+ | Per Scholas** page.*



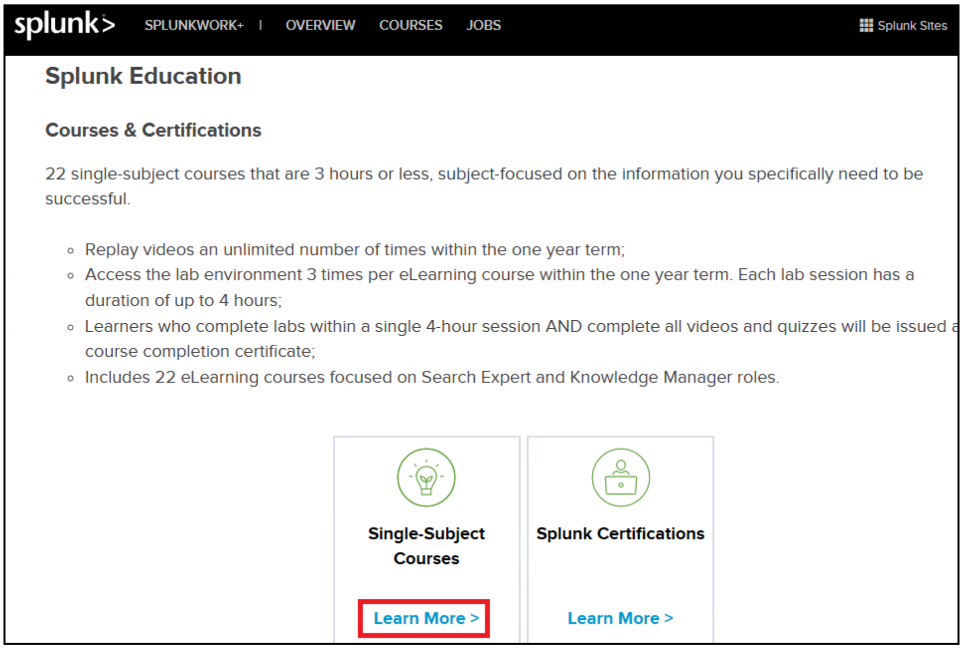
WELCOME TO
SplunkWork+ | Per Scholas
Overview

Creating the workforce of tomorrow with opportunities today

Welcome to SplunkWork+

As part of the $100 million Splunk Pledge, we have committed to supporting efforts to train the workforce of tomorrow, equipping you with the Splunk skills to position you for the opportunities of today.

e. *Scroll to the **Splunk Education** section and click the **Learn More >** link under **Single-Subject Courses**.*



Splunk Education

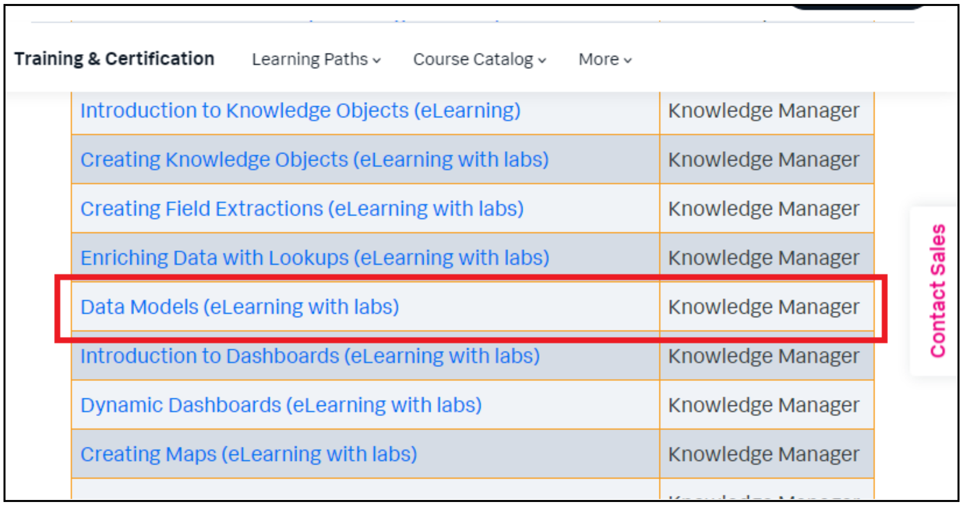
Courses & Certifications

22 single-subject courses that are 3 hours or less, subject-focused on the information you specifically need to be successful.

- Replay videos an unlimited number of times within the one year term;
- Access the lab environment 3 times per eLearning course within the one year term. Each lab session has a duration of up to 4 hours;
- Learners who complete labs within a single 4-hour session AND complete all videos and quizzes will be issued a course completion certificate;
- Includes 22 eLearning courses focused on Search Expert and Knowledge Manager roles.

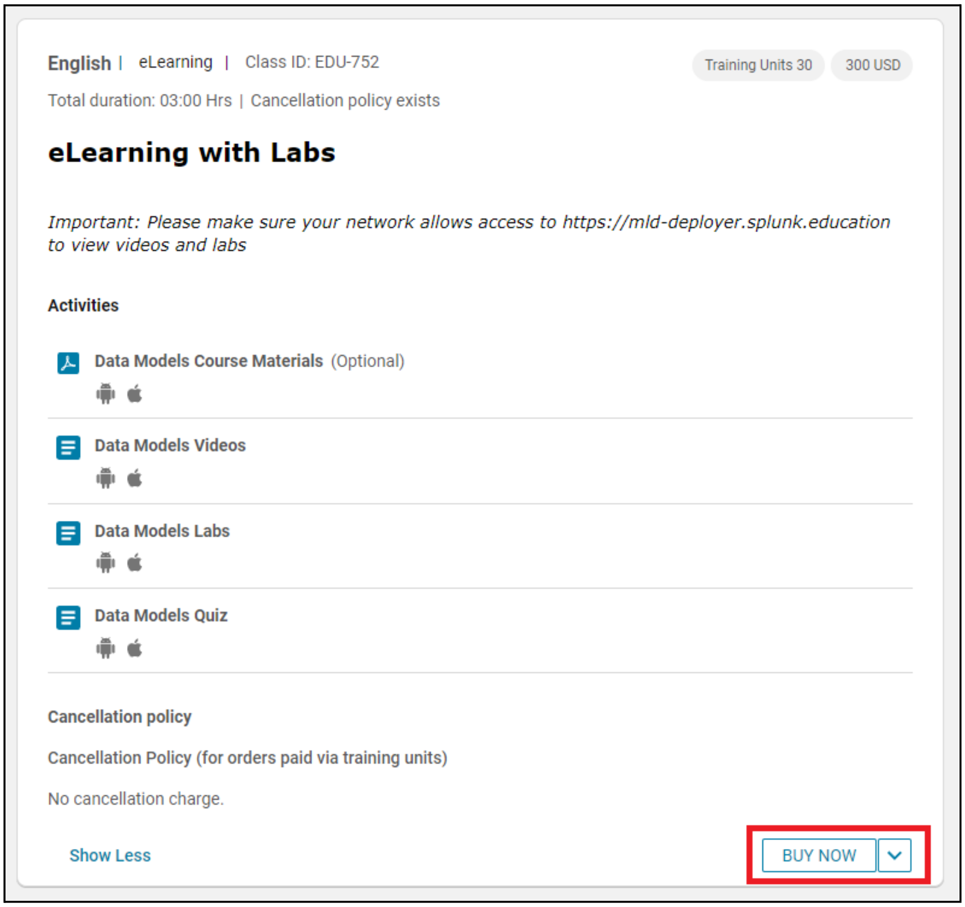
f. *Scroll down on the **Splunk Pledge Education Benefits (SplunkWork+)** page and review the courses available under the **Included Courses** section.*

g. *Locate and click the **Data Models (eLearning with labs)** course.*



Introduction to Knowledge Objects (eLearning)	Knowledge Manager
Creating Knowledge Objects (eLearning with labs)	Knowledge Manager
Creating Field Extractions (eLearning with labs)	Knowledge Manager
Enriching Data with Lookups (eLearning with labs)	Knowledge Manager
Data Models (eLearning with labs)	Knowledge Manager
Introduction to Dashboards (eLearning with labs)	Knowledge Manager
Dynamic Dashboards (eLearning with labs)	Knowledge Manager
Creating Maps (eLearning with labs)	Knowledge Manager

h. *Scroll down on the **Data Models** page, and click the **BUY NOW** button (Don't worry, you will **not** have to pay for this course).*



English | eLearning | Class ID: EDU-752

Training Units 30 | 300 USD

Total duration: 03:00 Hrs | Cancellation policy exists

eLearning with Labs

Important: Please make sure your network allows access to https://mld-deployer.splunk.education to view videos and labs

Activities

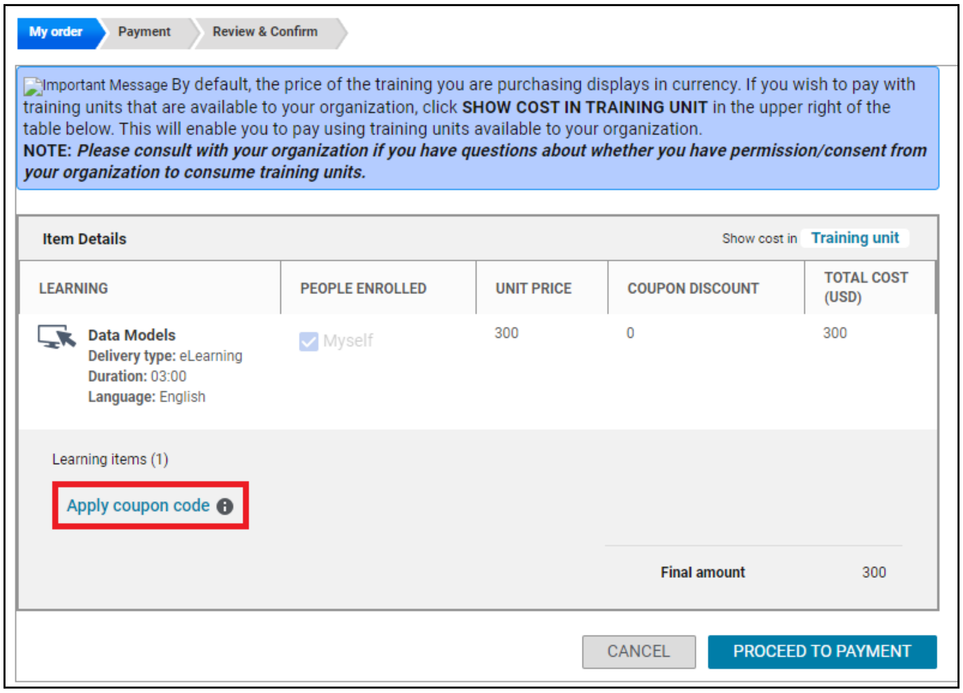
- Data Models Course Materials (Optional)
- Data Models Videos
- Data Models Labs
- Data Models Quiz

Cancellation policy

Cancellation Policy (for orders paid via training units)

No cancellation charge.

i. *On the **My order** step, click on the **Apply coupon code** link.*



Important Message By default, the price of the training you are purchasing displays in currency. If you wish to pay with training units that are available to your organization, click **SHOW COST IN TRAINING UNIT** in the upper right of the table below. This will enable you to pay using training units available to your organization.
NOTE: ***Please consult with your organization if you have questions about whether you have permission/consent from your organization to consume training units.***

Item Details — Show cost in Training unit

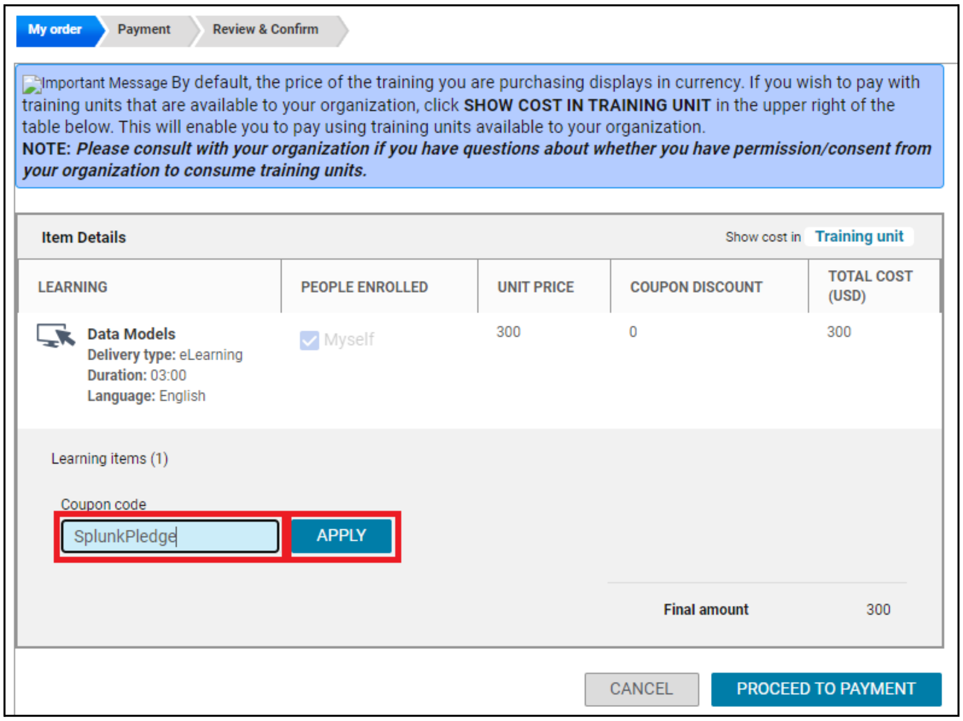
LEARNING	PEOPLE ENROLLED	UNIT PRICE	COUPON DISCOUNT	TOTAL COST (USD)
Data Models **Delivery type:** eLearning **Duration:** 03:00 **Language:** English	☑ Myself	300	0	300

Learning items (1)

Apply coupon code

Final amount 300

j. *Enter the coupon **SplunkPledge** into the **Coupon code** box and click on the **APPLY** button.*



Important Message By default, the price of the training you are purchasing displays in currency. If you wish to pay with training units that are available to your organization, click **SHOW COST IN TRAINING UNIT** in the upper right of the table below. This will enable you to pay using training units available to your organization.
NOTE: ***Please consult with your organization if you have questions about whether you have permission/consent from your organization to consume training units.***

Item Details Show cost in Training unit

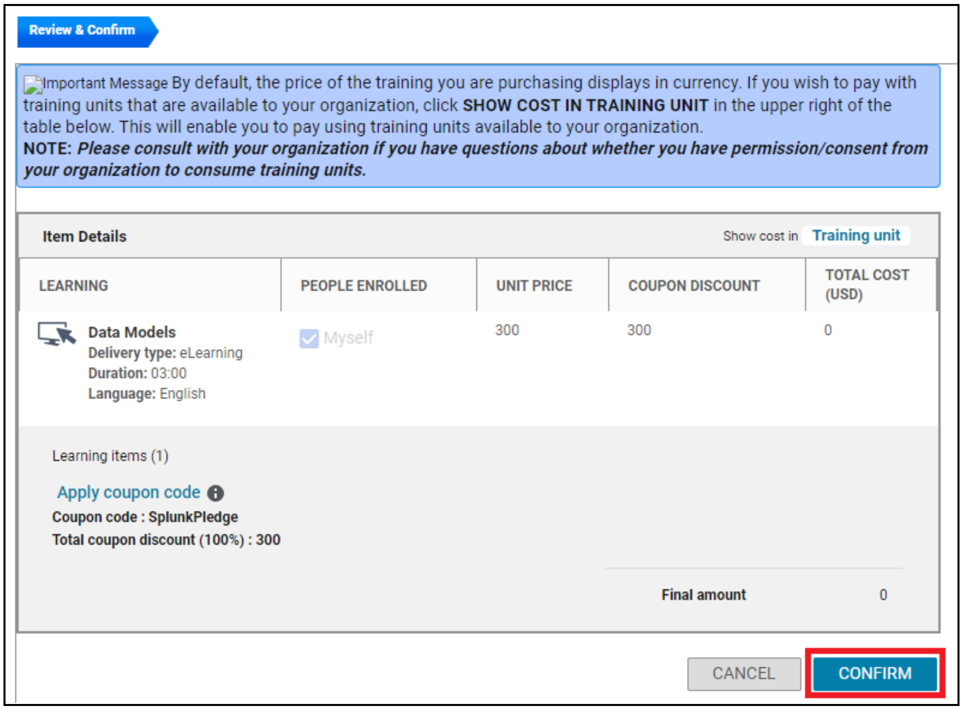
LEARNING	PEOPLE ENROLLED	UNIT PRICE	COUPON DISCOUNT	TOTAL COST (USD)
Data Models **Delivery type:** eLearning **Duration:** 03:00 **Language:** English	☑ Myself	300	0	300

Learning items (1)

Coupon code: SplunkPledge

Final amount 300

k. *Note that the **Total coupon discount is (100%): 300** and that the **Final amount is 0**. Next, click on the **CONFIRM** button.*



Important Message By default, the price of the training you are purchasing displays in currency. If you wish to pay with training units that are available to your organization, click **SHOW COST IN TRAINING UNIT** in the upper right of the table below. This will enable you to pay using training units available to your organization.
NOTE: ***Please consult with your organization if you have questions about whether you have permission/consent from your organization to consume training units.***

Item Details Show cost in Training unit

LEARNING	PEOPLE ENROLLED	UNIT PRICE	COUPON DISCOUNT	TOTAL COST (USD)
Data Models **Delivery type:** eLearning **Duration:** 03:00 **Language:** English	☑ Myself	300	300	0

Learning items (1)

Apply coupon code

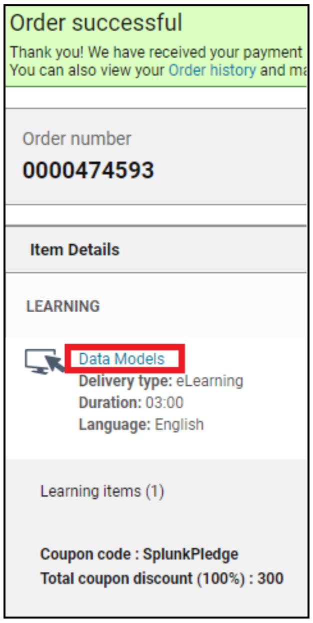
Coupon code : SplunkPledge
Total coupon discount (100%) : 300

Final amount 0

l. *Take a screenshot of the **Order successful notification** and paste the image into the box below. (Note: You will also get an email confirming your registration).*

[Paste image here]

m. *Launch the course by clicking the **Data Models** link on the **Order Successful** page under the **Item Details** section.*



Order successful

Thank you! We have received your payment

You can also view your Order history and ma

Order number

0000474593

Item Details

LEARNING

Data Models

Delivery type: eLearning

Duration: 03:00

Language: English

Learning items (1)

Coupon code : SplunkPledge

Total coupon discount (100%) : 300

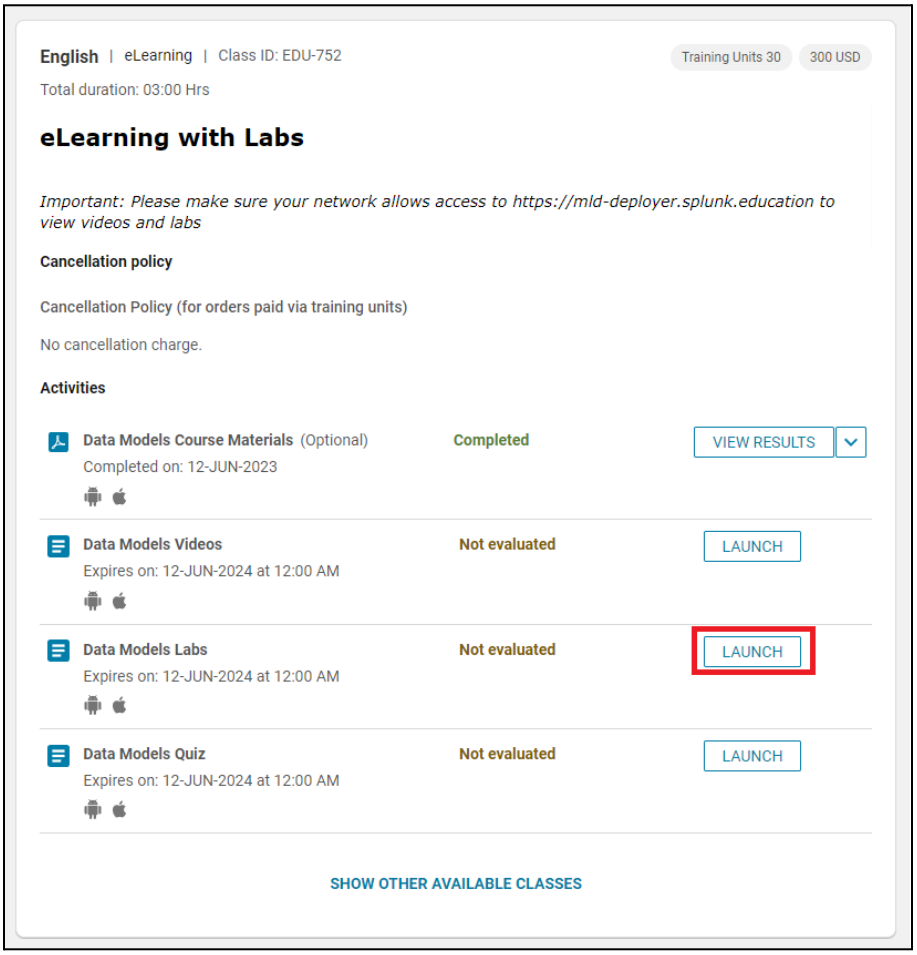
Step 2: Launch the Splunk lab environment.

In this step, you will launch the Splunk lab environment from the Data Models course. Once the server is up, it will run for four hours.

Note: In this lab, you use the Splunk environment provided for the Data Models course for practice. You do not have to complete the Data Models course or the course's lab (if you want to take the course, please do so in your free time).

a. *If you still need to do so, go to your **Data Models** course (Note: You can also access the course via the registration confirmation email sent to the account used to register for the course)*

b. *On the **Data Models In Progress page**, scroll down to the **Data Models Labs** section and click the **LAUNCH** button.*



English | eLearning | Class ID: EDU-752

Total duration: 03:00 Hrs

eLearning with Labs

Important: Please make sure your network allows access to https://mld-deployer.splunk.education to view videos and labs

Cancellation policy

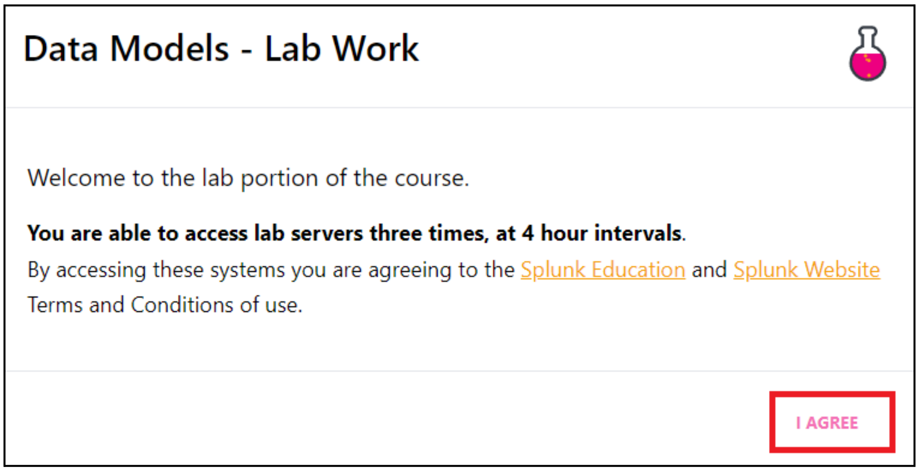
Cancellation Policy (for orders paid via training units)

No cancellation charge.

Activities

Data Models Course Materials (Optional) Completed on: 12-JUN-2023	Completed	VIEW RESULTS
Data Models Videos Expires on: 12-JUN-2024 at 12:00 AM	Not evaluated	LAUNCH
Data Models Labs Expires on: 12-JUN-2024 at 12:00 AM	Not evaluated	LAUNCH
Data Models Quiz Expires on: 12-JUN-2024 at 12:00 AM	Not evaluated	LAUNCH

c. *Review the welcome notification on the **Data Models - Lab Work** page and click on the **I AGREE** link.*



Data Models - Lab Work

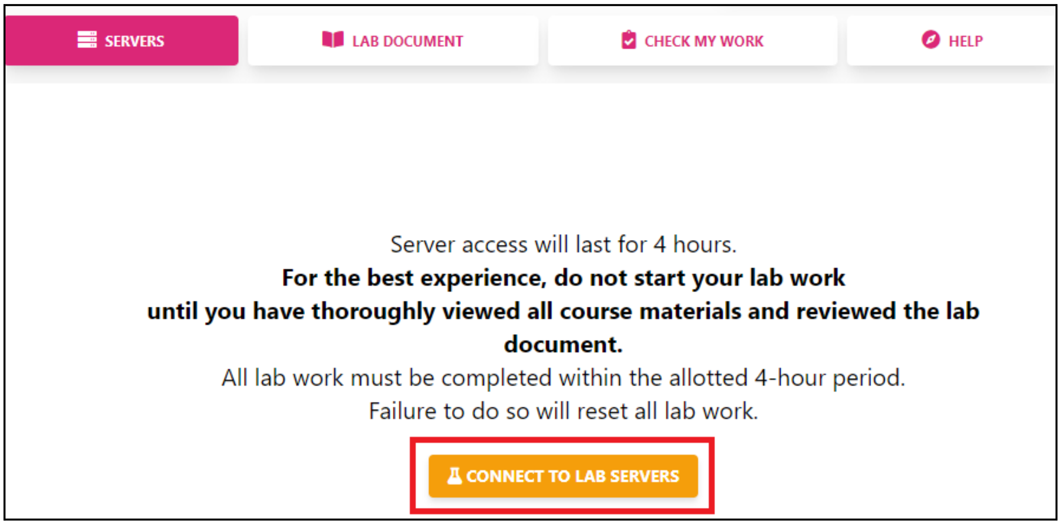
Welcome to the lab portion of the course.

You are able to access lab servers three times, at 4 hour intervals.

By accessing these systems you are agreeing to the Splunk Education and Splunk Website Terms and Conditions of use.

d. *On the **Data Models Labs** page, the **GUIDE** section contains instructions on using the lab resources **when taking the Data Models course**. For **THIS** lab, **ignore the GUIDE**. You do not need to look at the LAB DOCUMENT as **you are not working on the Data Models course**.*

e. *Under the **SERVERS** tab, click on the **CONNECT TO LAB SERVERS** button. Note it may take several minutes for the servers to be available.*



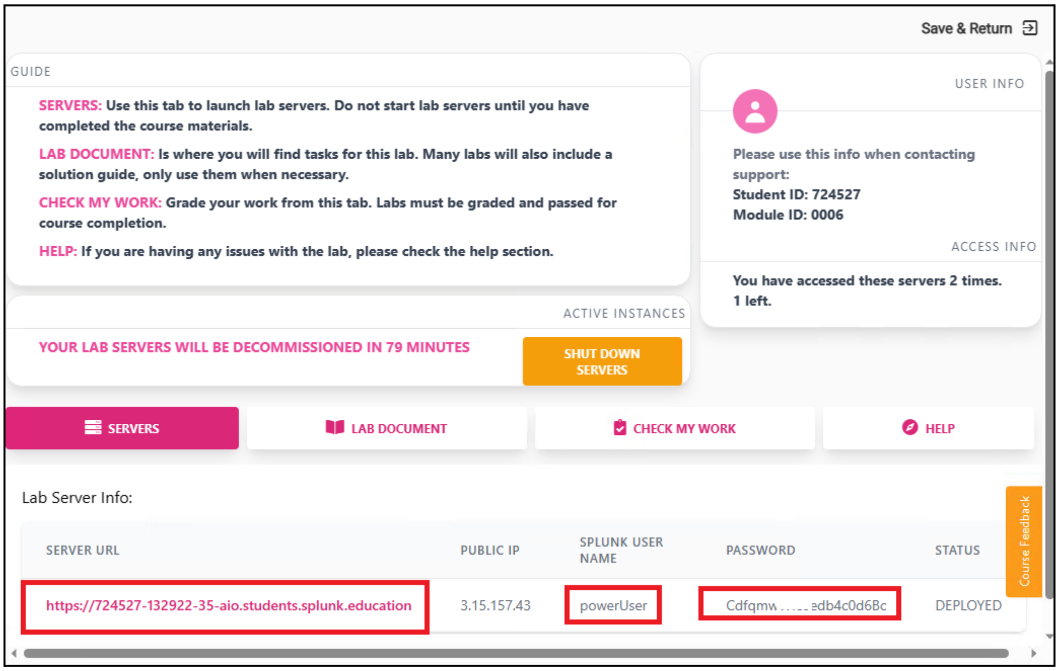
Server access will last for 4 hours.

For the best experience, do not start your lab work until you have thoroughly viewed all course materials and reviewed the lab document.

All lab work must be completed within the allotted 4-hour period.

Failure to do so will reset all lab work.

f. *Once the lab server is ready, the **Data Models Labs** page will display the **SERVER URL**, a **SPLUNK USER NAME**, and **PASSWORD**. Click on the **SERVER URL** link.*



GUIDE

SERVERS: Use this tab to launch lab servers. Do not start lab servers until you have completed the course materials.

LAB DOCUMENT: Is where you will find tasks for this lab. Many labs will also include a solution guide, only use them when necessary.

CHECK MY WORK: Grade your work from this tab. Labs must be graded and passed for course completion.

HELP: If you are having any issues with the lab, please check the help section.

USER INFO

Please use this info when contacting support:
Student ID: 724527
Module ID: 0006

ACCESS INFO

You have accessed these servers 2 times. 1 left.

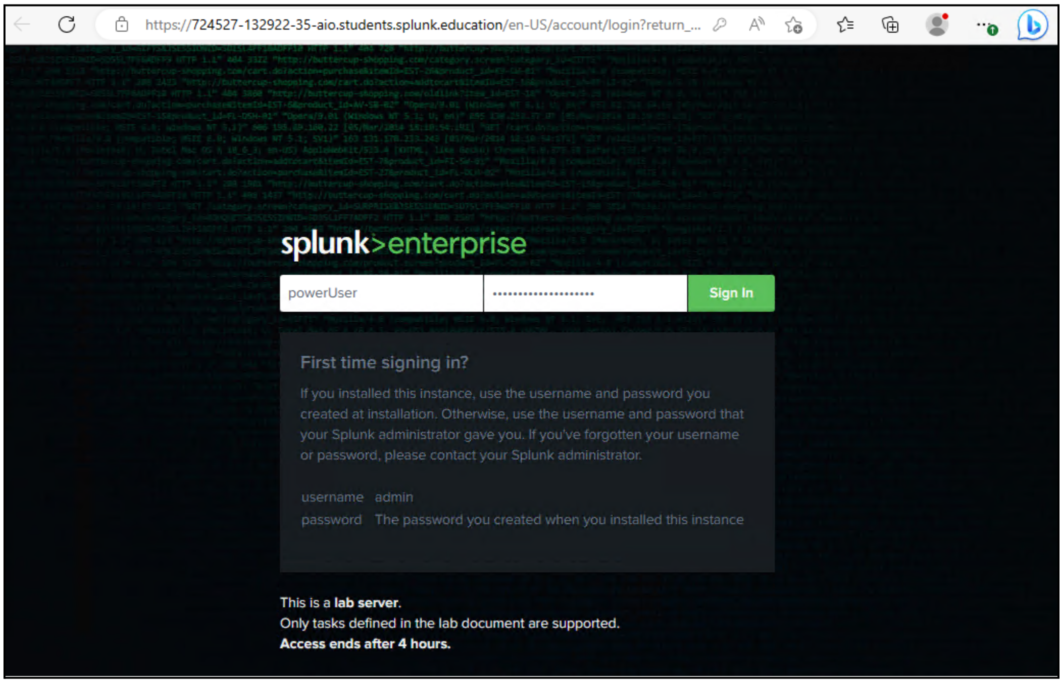
ACTIVE INSTANCES

YOUR LAB SERVERS WILL BE DECOMMISSIONED IN 79 MINUTES

Lab Server Info:

SERVER URL	PUBLIC IP	SPLUNK USER NAME	PASSWORD	STATUS
https://724527-132922-35-aio.students.splunk.education	3.15.157.43	powerUser	Cdfqmw......edb4c0d6Bc	DEPLOYED

g. *The **splunk>enterprise sign-in** page will open on a **new** browser tab. Enter the **username** and **password** provided to you in the previous step, and click the **Sign in** button.*


https://724527-132922-35-aio.students.splunk.education/en-US/account/login?return_...
splunk>enterprise
powerUser
••••••••••••••••••••
Sign In

First time signing in?

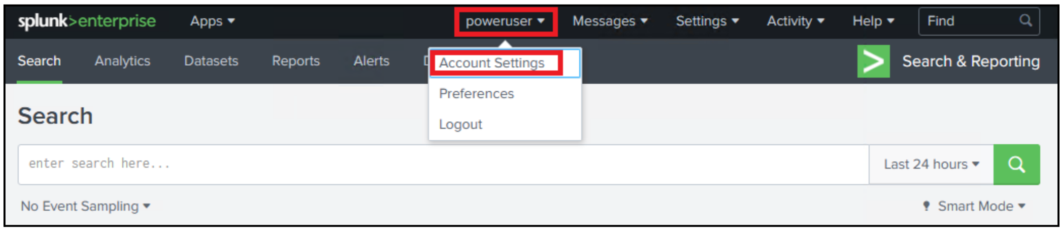
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

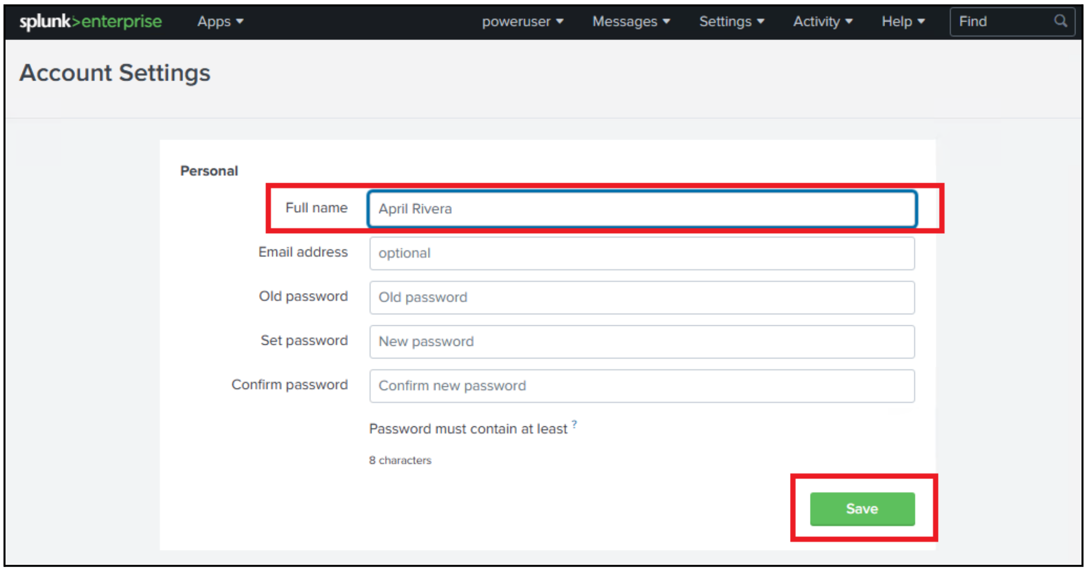
This is a **lab server**.
Only tasks defined in the lab document are supported.
Access ends after 4 hours.

h. *You may see a pop-up window welcoming you to the lab environment. You can click **Continue to Tour,** but this is not required. Click **Skip** to dismiss the window.*

i. *Click on the **username** you logged in with (at the top of the screen), and then choose **Account Settings** from the drop-down menu.*



j. *On the **Account Settings** page, in the **Full name** box, enter your **first** and **last** name. Next, click on the **Save** button.*



Account Settings

Personal

Full name: April Rivera

Email address: optional

Old password: Old password

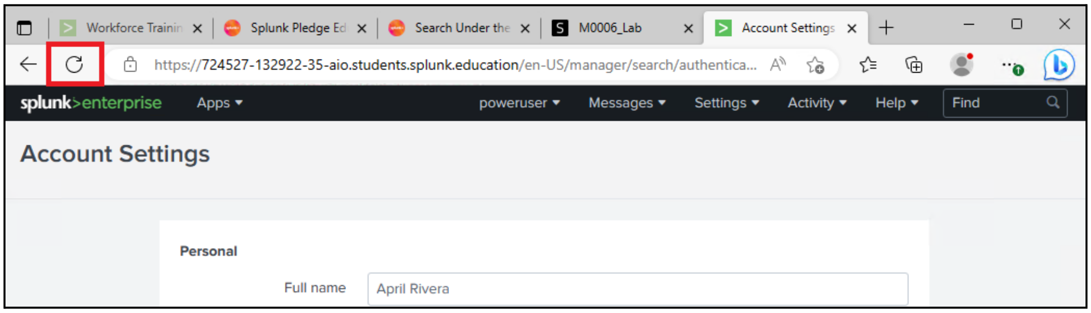
Set password: New password

Confirm password: Confirm new password

Password must contain at least ?

8 characters

k. *Refresh/reload your browser window to reflect the recent changes to the interface.*



https://724527-132922-35-aio.students.splunk.education/en-US/manager/search/authentica...

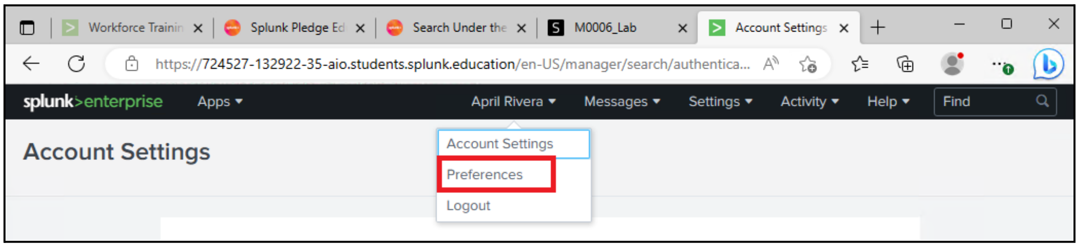
Account Settings

Personal

Full name: April Rivera

NOTE: Sometimes, there can be delays in executing an action, such as saving in the UI or returning search results. If you are experiencing a delay, please allow the UI a few minutes to execute your action.

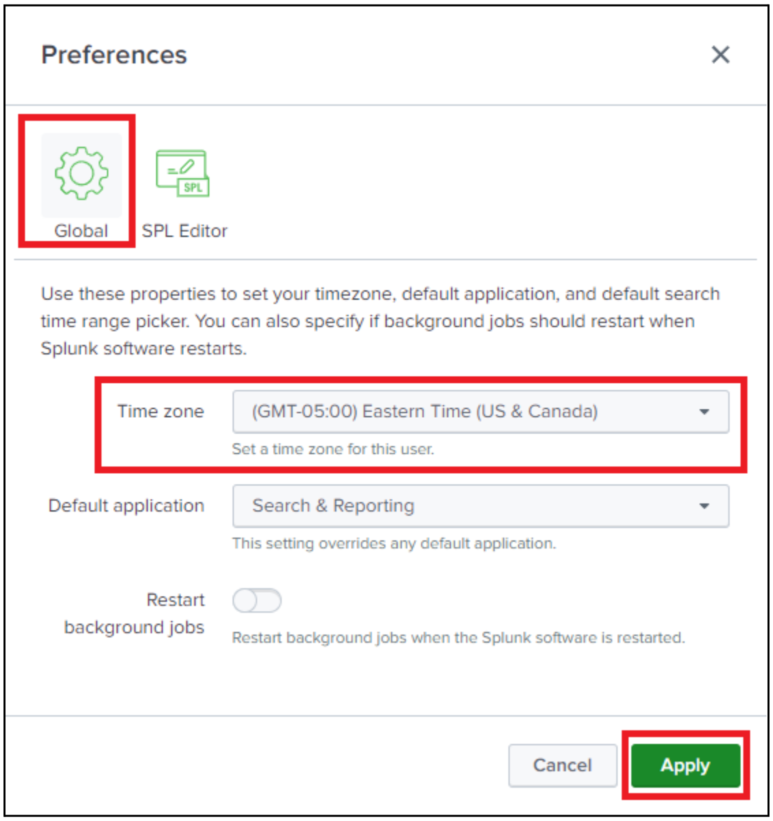
l. *Navigate to **user name > Preferences**.*



https://724527-132922-35-aio.students.splunk.education/en-US/manager/search/authentica...

Account Settings

m. *Under the **Global** tab, choose **your local time zone** from the **Time zone** drop-down menu, and click on the **Apply** button.*



Preferences

Use these properties to set your timezone, default application, and default search time range picker. You can also specify if background jobs should restart when Splunk software restarts.

Time zone: (GMT-05:00) Eastern Time (US & Canada)

Set a time zone for this user.

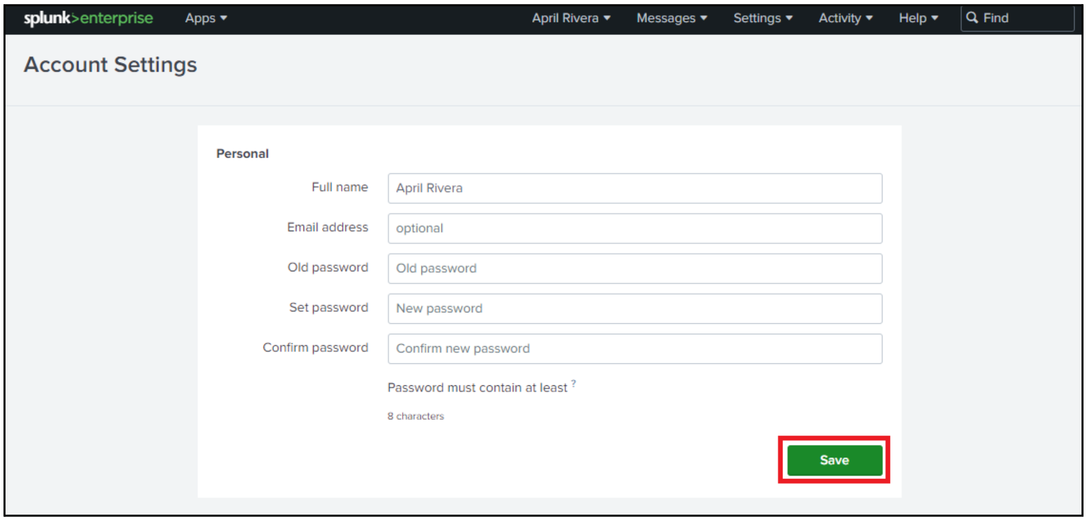
Default application: Search & Reporting

This setting overrides any default application.

Restart background jobs: ○

Restart background jobs when the Splunk software is restarted.

n. *Back on the **Account Settings** page, click on the **Save** button.*



Account Settings

Personal

Full name: April Rivera

Email address: optional

Old password: Old password

Set password: New password

Confirm password: Confirm new password

Password must contain at least ?

8 characters

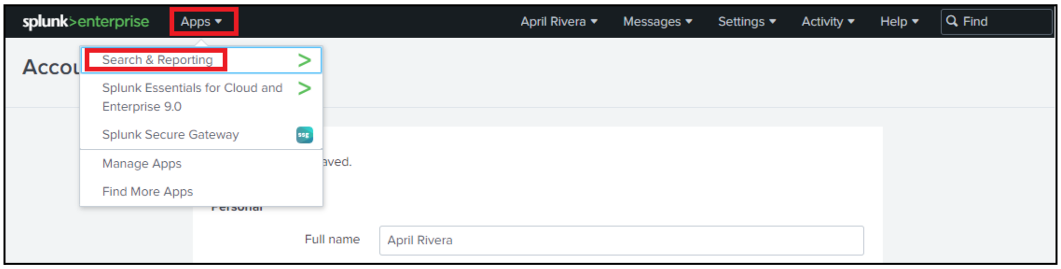
o. *Take a **screenshot** of the **Splunk interface page** displaying **your name** instead of the username you used to sign in. Paste the image into the box below.*

[Paste image here]

Part 2: Explore the Splunk Web interface.

Step 1: Explore the Search & Reporting App and available data.

a. *From the **splunk>enterprise** Web interface page, click on the **Apps** drop-down menu. Note the Manage Apps and Find More Apps menu items. Click on the **Search & Reporting** menu item.*



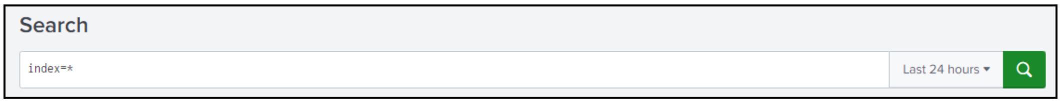
b. *You may see a Welcome pop-up window. You can click **Continue to Tour,** but this is not required. Click **Skip** to dismiss the window.*

c. *Take some time to **click around** and get familiar with the interface.*

d. *What are some of the **available sections** and **items** under the **Search** tab on the **Search & Reporting** App page? Enter your answer into the box below*

[enter answer here]

e. *Back on the* ***Search & Reporting*** *App page, type* ***index=**** *into the search bar. Set the time range to* ***Last 24 hours****, and click the* ***green magnifying glass*** *button.*



Search

index=*

Last 24 hours

f. *Use the results (displayed under the Search bar, as events, and in the fields sidebar) to* ***answer*** *the following questions.*

g. *How many index(es) are present in the current environment?*

[enter answer here]

h. *What is the index(es) name(s)?*

[enter answer here]

i. *What is the number of returned events?*

[enter answer here]

j. *How many sourcetype(s) are present in the current environment?*

[enter answer here]

k. *What is the sourcetype(s) name(s)?*

[enter answer here]

l. *Using the* ***Job inspector,*** *enter the time it took for the search to complete.*

[enter answer here]

m. *Using the* ***Timeline chart****, determine at what time during the 24 hours did Splunk record the largest number of events?*

[enter answer here]

n. *What was the number of events during that time?*

[enter answer here]

o. *Use the* ***Timeline*** *to* ***filter*** *the events in the results list to the* ***selected time****. Use the* ***+ Zoom to selection*** *button above the Timeline to rerun the search. Take a screenshot of the Search bar and the results list and paste it into the box below.*

[Paste image here]

p. *Using the* ***Fields sidebar****, determine how many* ***clientip*** *values were found in the events list. Enter the number into the box below.*

[enter number here]

q. *Using the* ***Fields sidebar****, determine the* ***top value*** *(present in the majority of events) of an IP address. Into the box below, enter the* ***IP address,*** *the* ***number of events*** *that* ***occurred*** *with* ***this IP address****, and the* ***percentage*** *of this value in the total number of events.*

IP address: *Count:* *%:*

r. *Add the* ***clientip*** *field to the* ***SELECTED FIELDS*** *section. How many fields now reside under the* ***SELECTED FIELDS*** *section?*

[enter answer here]

s. *Using the* ***clientip*** *field from the* ***SELECTED FIELDS*** *sidebar, click on the top* ***IP address*** *value to add it to the search string. Take a screenshot of the result and paste it into the box below.*

[Paste image here]

Step 2: Explore the Search & Reporting freely.

At this point, you can submit the lab. Still, the server you launched is up for four hours. Use this time to continue exploring the Splunk environment. Click around, experiment, and try things out. Attempt to search for something that makes sense to you. Consider scenarios you would like to run and try to collect relevant data.

Once the server times out, you can access it two more times. Use this opportunity to spend more time in the Splunk world.

Splunk is complex, and the more you play with it, the better you will understand it.