Introduction

About Splunk Cloud

Splunk Inc. is an American public multinational corporation based in San Francisco, California. It produces software for searching, monitoring, and analyzing machine-generated big data through a Web-style interface. Splunk Cloud is one of Splunk's products that delivers the capabilities of Splunk as Software-as-a-Service.

Why should Splunk Cloud be Integrated with Thycotic Secret Server?

The integration of Splunk Cloud is done with Thycotic Secret Server to forward the Syslogs of Thycotic Secret Server to Splunk Cloud.

Integrating Splunk Cloud with Secret Server

Secret Server is a web-based password vault used throughout the world to help organizations properly manage privileged accounts. This guide will assist you with your Splunk Cloud and Secret Server integration project.

Configuration

Integrating Splunk Cloud with Secret Server

The following are the overall steps to integrate Splunk Cloud with Secret Server.

- Registering with Splunk
- Installing and configuring Universal Forwarder
- Configuration using TCP

  Note: Please be aware that the last steps are only for users that are interested in publishing the Splunk App. These steps are not required for configuring Splunk Cloud with Secret Server.

Publishing and Packaging Splunk App

The Splunk app is a quick way to get analysis, reports, health checks, and usage of your on-premises Secret Server instance. The App is created on the enterprise edition of Splunk so that it can be packaged and published on the Splunkbase.

Publishing and Packaging Splunk App to Splunkbase

To create a Splunk App, ensure that the prerequisites are met. This section provides the steps to create an app, dashboard, and package the app.

The following are the steps to be performed:

- Create an App
- Create Dashboard
- Package the App

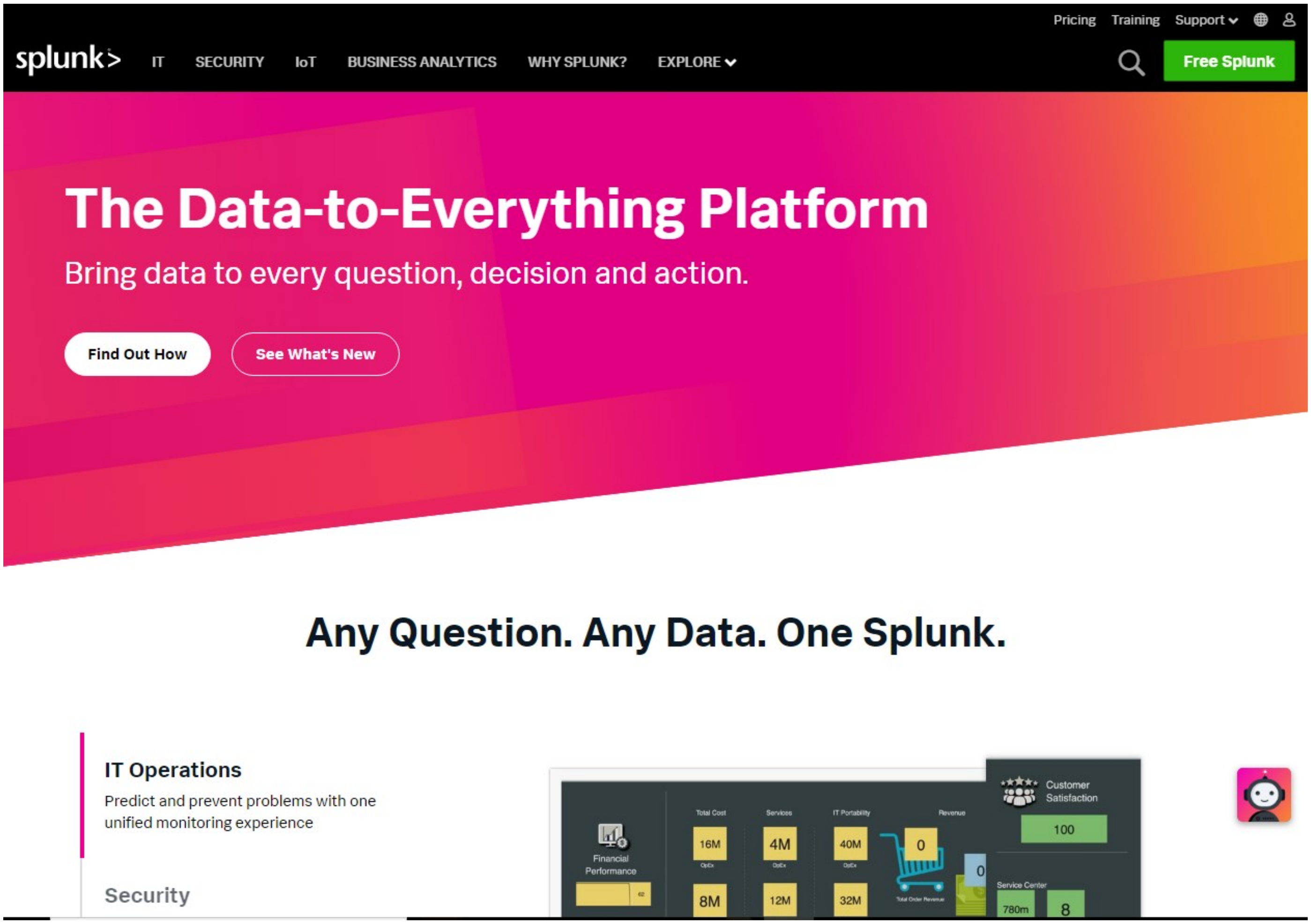
Registering with Splunk

Register with Splunk to obtain the URL, username, password, and access to the Splunk's instance.

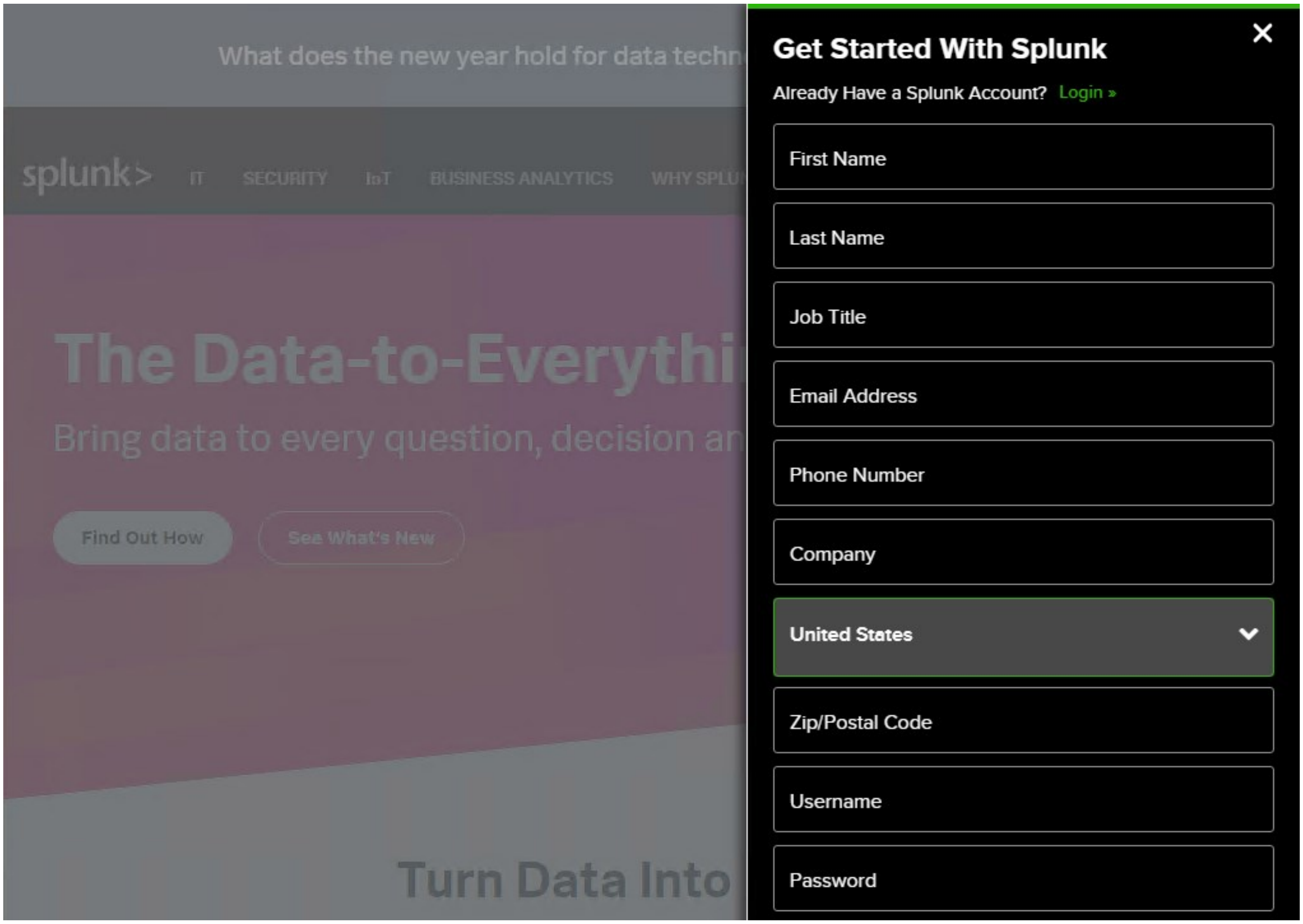
> **Note:** This step may be skipped, if you currently have a Splunk cloud instance.

To register with Splunk:

1. In the browser, type the following URL: https://www.splunk.com and press **Enter**. The Splunk website appears.



2. On the upper-right, click **Free Splunk**. The **Get Started With Splunk** webpage appears.



Get Started With Splunk

Already Have a Splunk Account? Login »

First Name

Last Name

Job Title

Email Address

Phone Number

Company

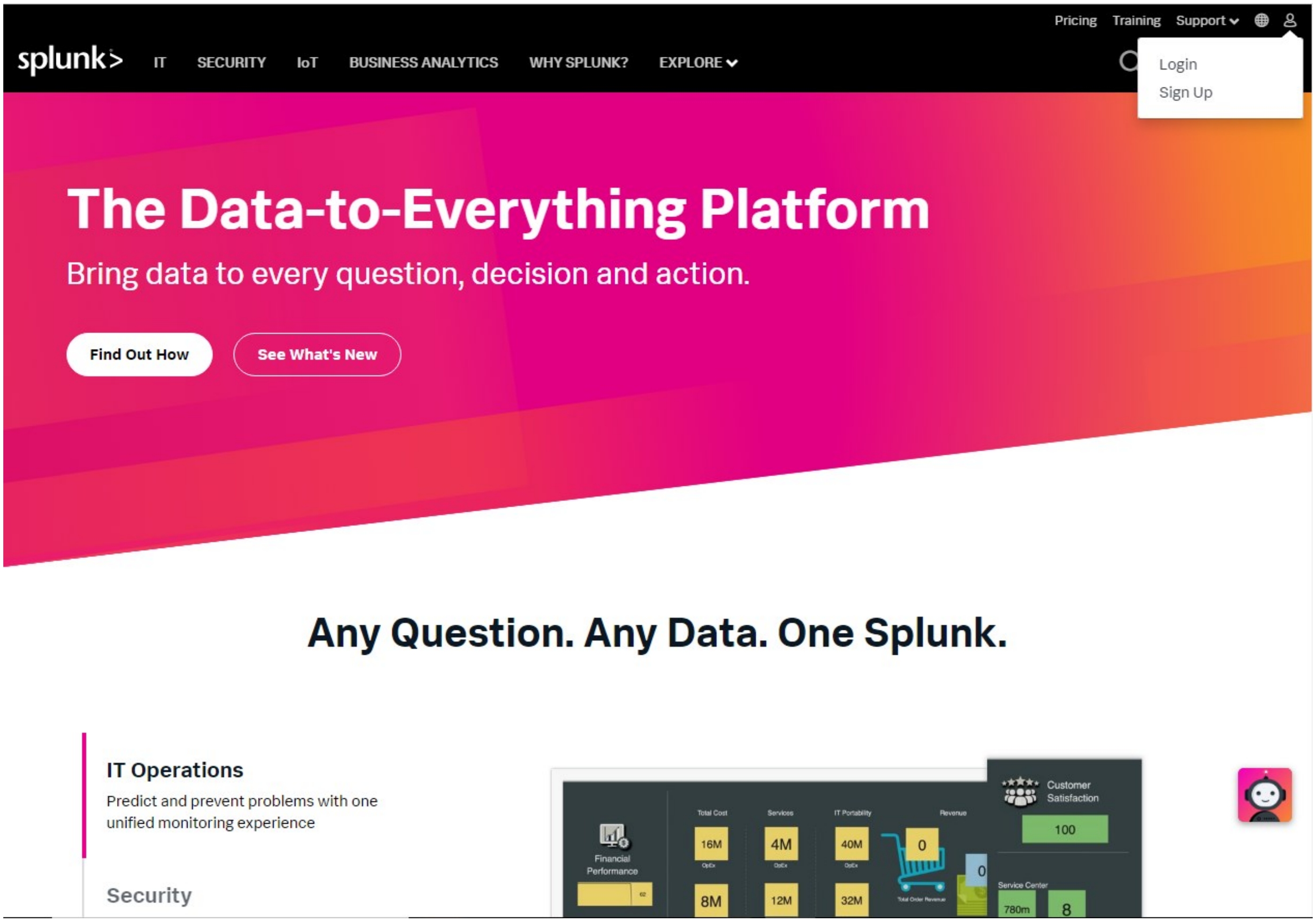
United States

Zip/Postal Code

Username

Password

3. Fill the form. An email is sent to the registered **Email Address**.
4. From the email, copy the **Your Splunk Cloud URL** and paste it in a browser. Press **Enter.** The Splunk website appears.



The Data-to-Everything Platform

Bring data to every question, decision and action.

Any Question. Any Data. One Splunk.

IT Operations

Predict and prevent problems with one unified monitoring experience

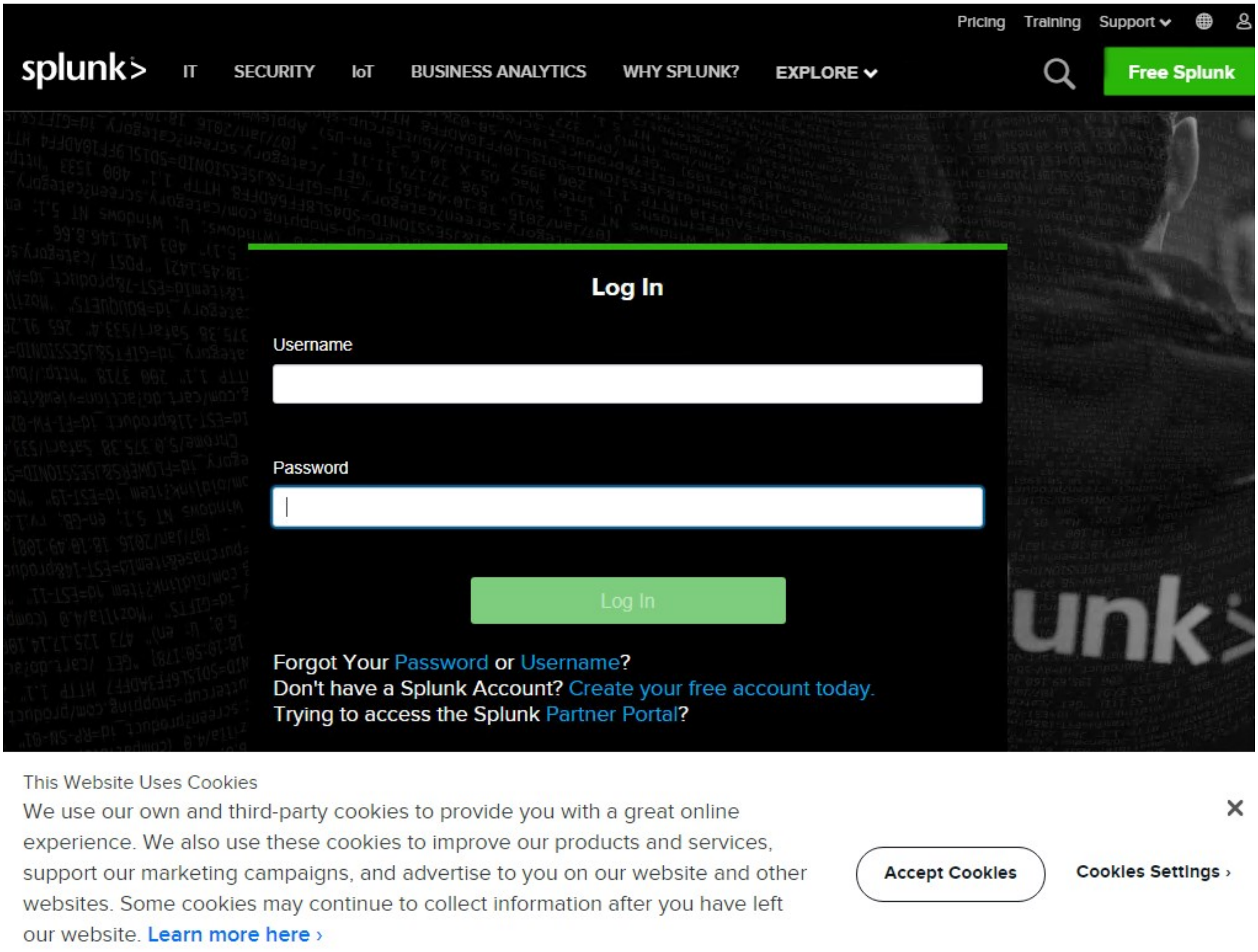
Security

Installing and Configuring Universal Forwarder

Install and configure the Universal Forwarder on the server where Secret Server is installed. The Universal Forwarder sends data to the Splunk platform.

To install and configure Universal Forwarder:

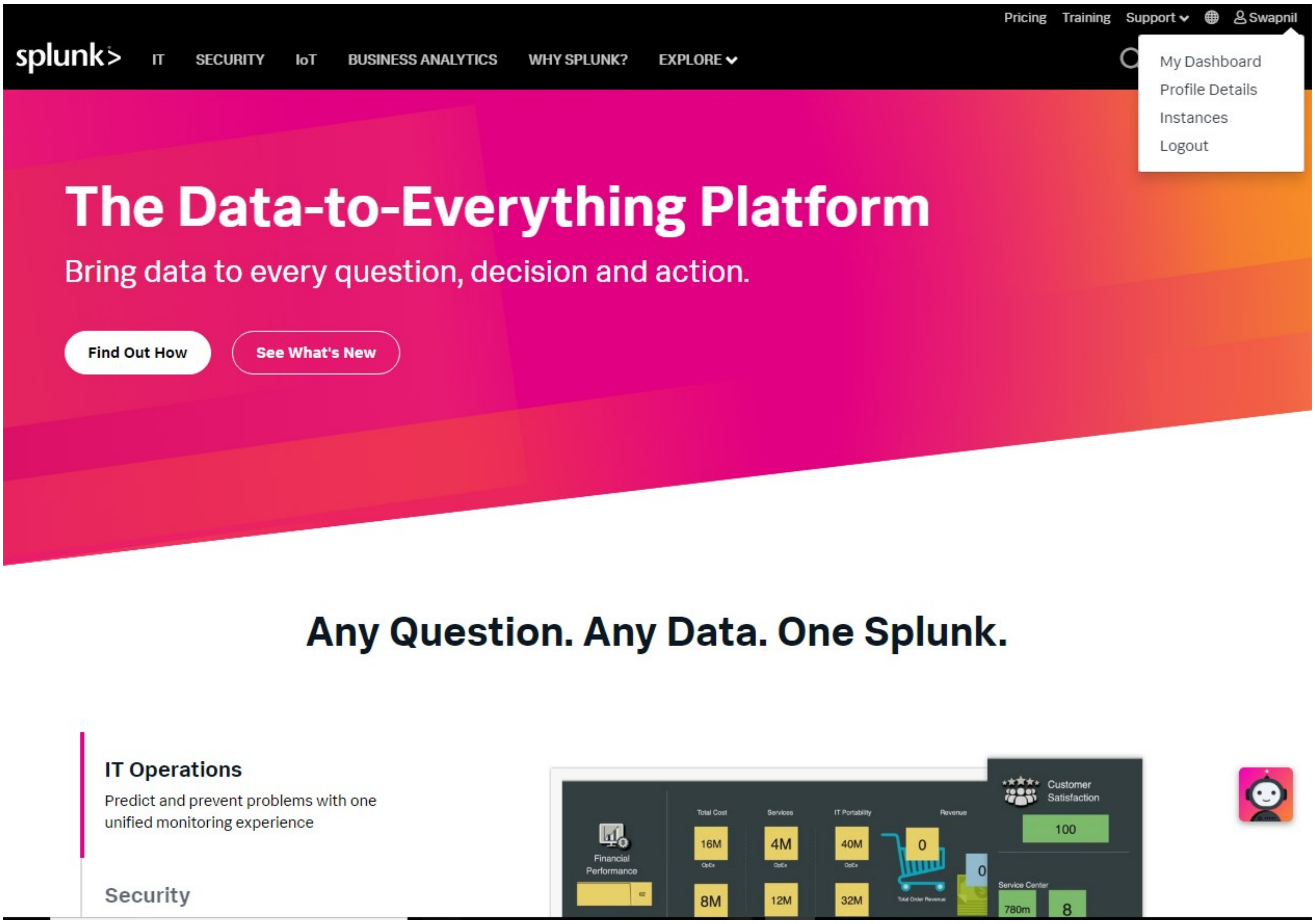
1. On the upper-right of the Splunk website, click **Username | Login**. The **Log In** window appears.



Forgot Your Password or Username?
Don't have a Splunk Account? Create your free account today.
Trying to access the Splunk Partner Portal?

This Website Uses Cookies
We use our own and third-party cookies to provide you with a great online experience. We also use these cookies to improve our products and services, support our marketing campaigns, and advertise to you on our website and other websites. Some cookies may continue to collect information after you have left our website. Learn more here ›

2. For the **Username**, enter the username.
3. For the **Password**, enter the password.
4. Click **Log In**.



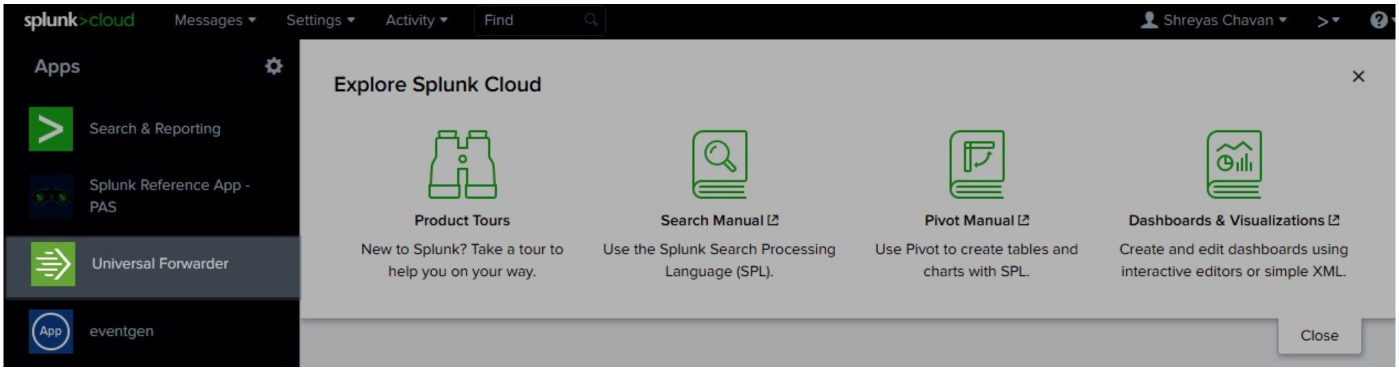
The Data-to-Everything Platform

Bring data to every question, decision and action.

Any Question. Any Data. One Splunk.

Predict and prevent problems with one unified monitoring experience

5. On the upper-right click **Username I Instances**. The **Explore Splunk Cloud** window appears.



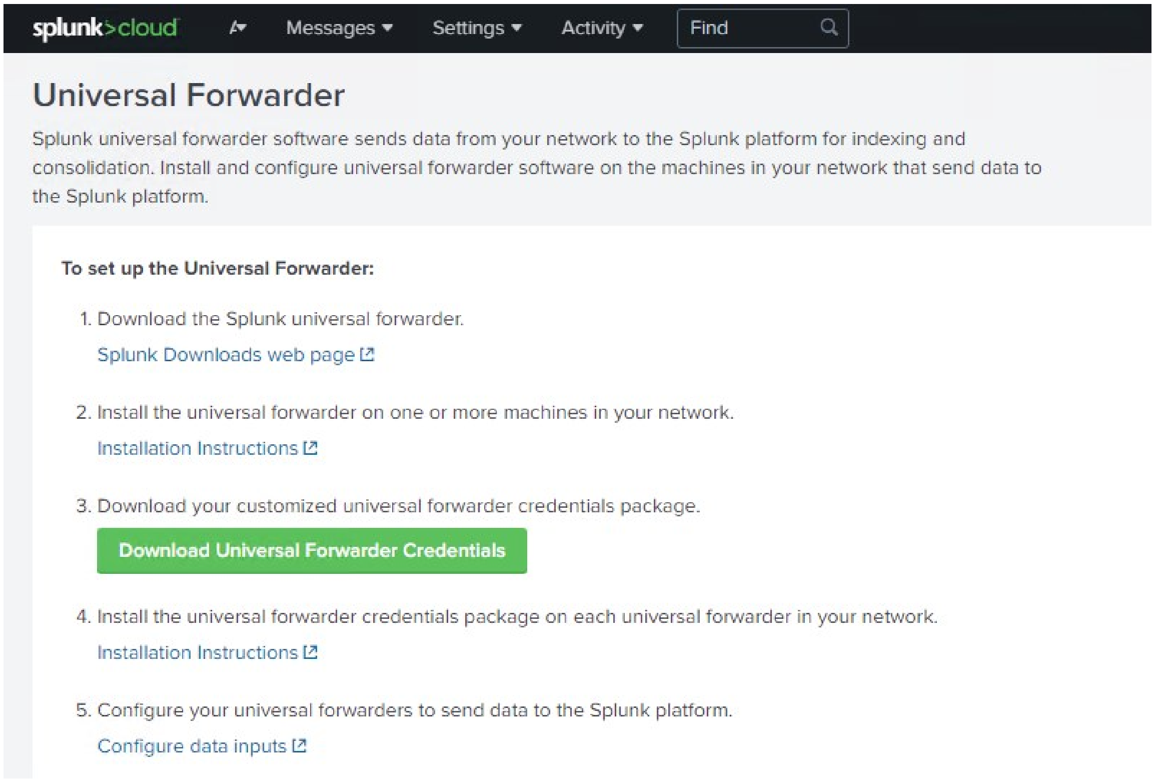
New to Splunk? Take a tour to help you on your way.

Use the Splunk Search Processing Language (SPL).

Use Pivot to create tables and charts with SPL.

Create and edit dashboards using interactive editors or simple XML.

6. On the left-hand side, click **Universal Forwarder**. The **Universal Forwarder** window appears.



Universal Forwarder

Splunk universal forwarder software sends data from your network to the Splunk platform for indexing and consolidation. Install and configure universal forwarder software on the machines in your network that send data to the Splunk platform.

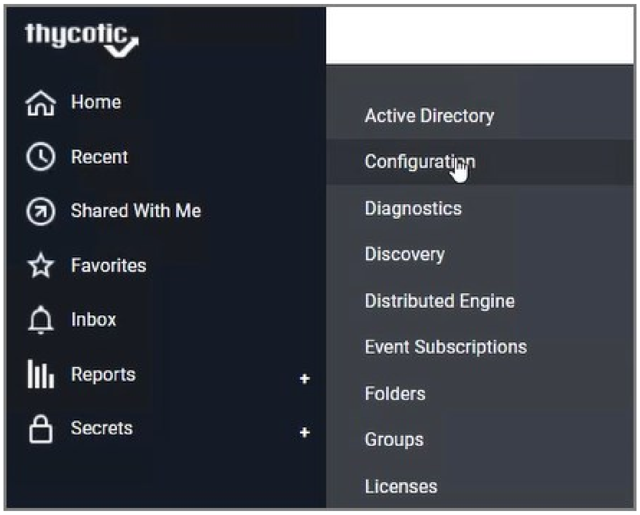
To set up the Universal Forwarder:

1. Download the Splunk universal forwarder.
   Splunk Downloads web page
2. Install the universal forwarder on one or more machines in your network.
   Installation Instructions
3. Download your customized universal forwarder credentials package.
   Download Universal Forwarder Credentials
4. Install the universal forwarder credentials package on each universal forwarder in your network.
   Installation Instructions
5. Configure your universal forwarders to send data to the Splunk platform.
   Configure data inputs

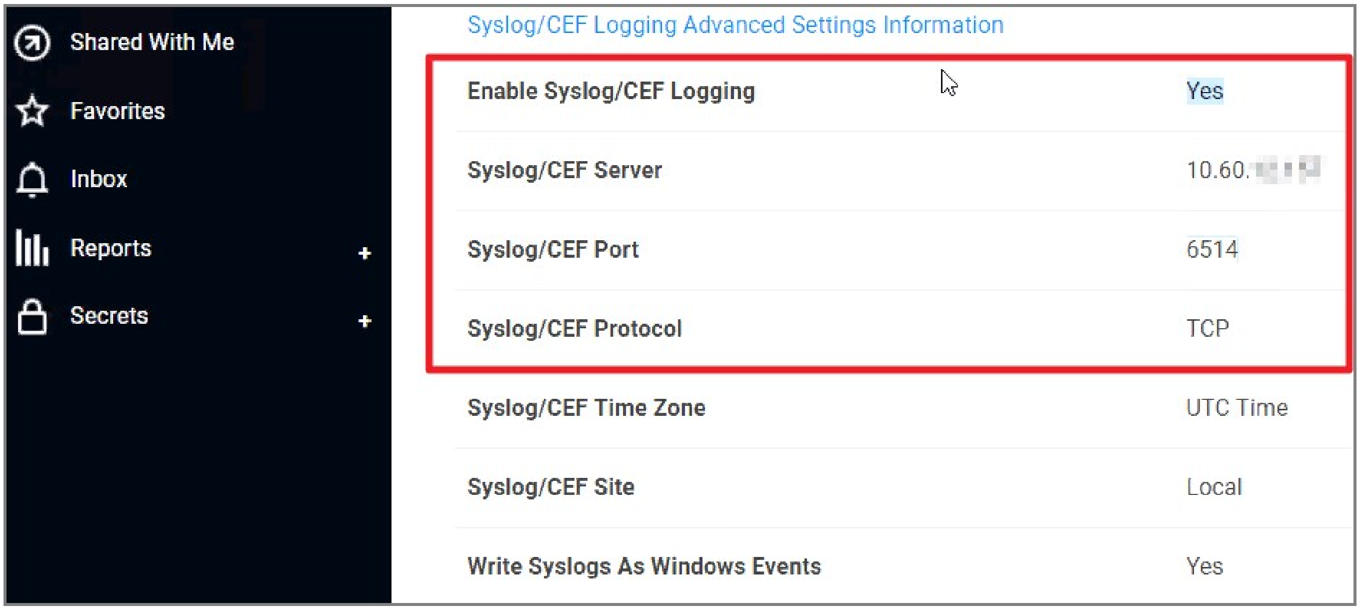
7. Follow Steps 1 to 5 as mentioned on the screen above.

Configuration for TCP

1. Navigate to **Secret Server**.
2. Go to **Admin I Configuration**.



3. Click on **Syslog/CEF logging Advanced Settings Information**.
4. Edit the following settings:
   - **Enable Syslog/CEF Logging**: Yes
   - **Syslog/CEF Server**: IP address for the server
   - **Syslog/CEF Port**: Port number
   - **Syslog/CEF Protocol**: TCP

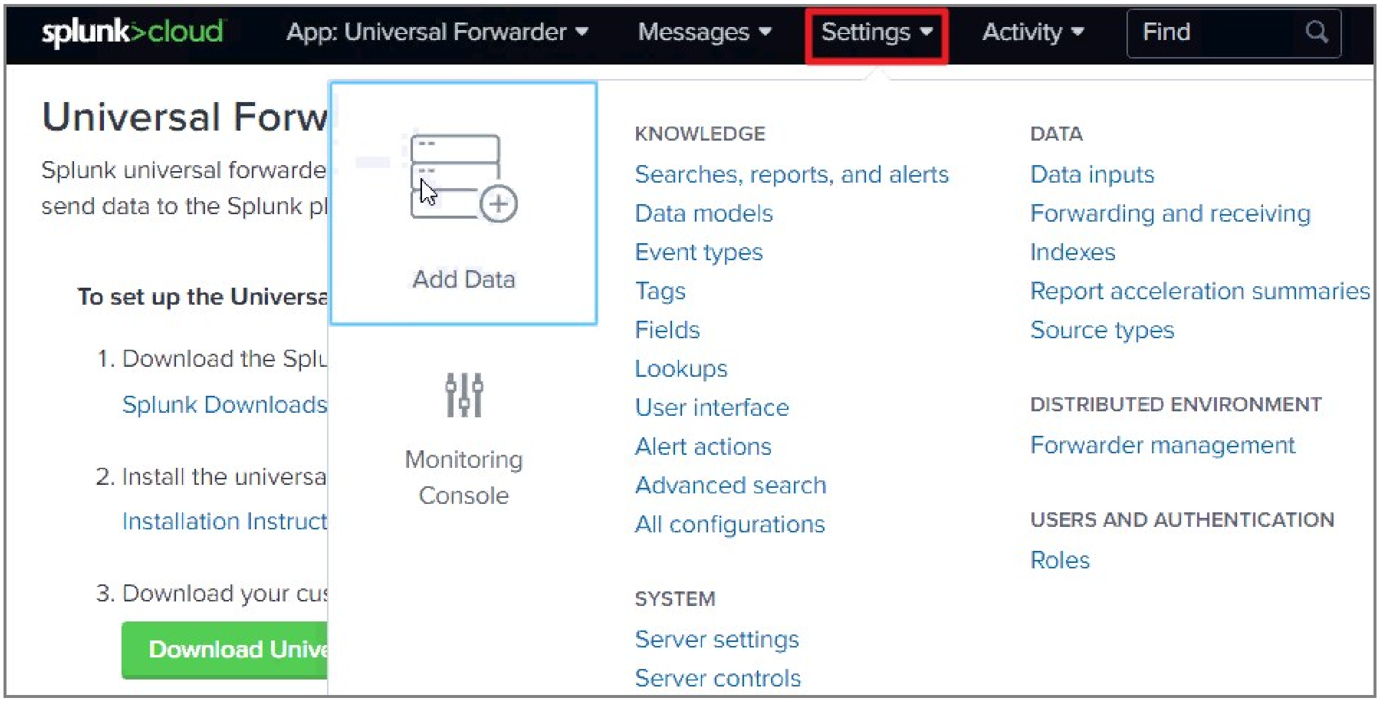


Syslog/CEF Logging Advanced Settings Information

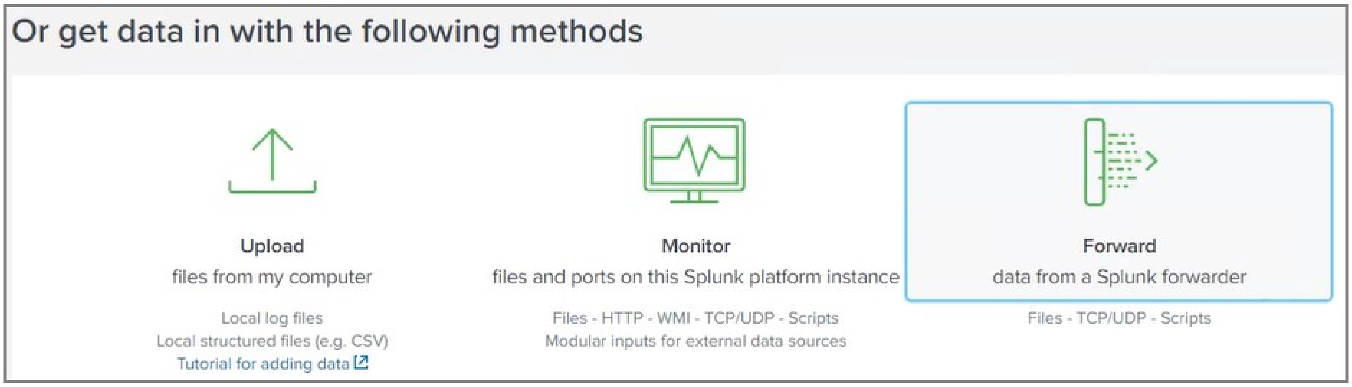
Enable Syslog/CEF Logging	Yes
Syslog/CEF Server	10.60.[redacted]
Syslog/CEF Port	6514
Syslog/CEF Protocol	TCP
Syslog/CEF Time Zone	UTC Time
Syslog/CEF Site	Local
Write Syslogs As Windows Events	Yes

5. Click **Save**.
6. Navigate to **Splunk Cloud**.

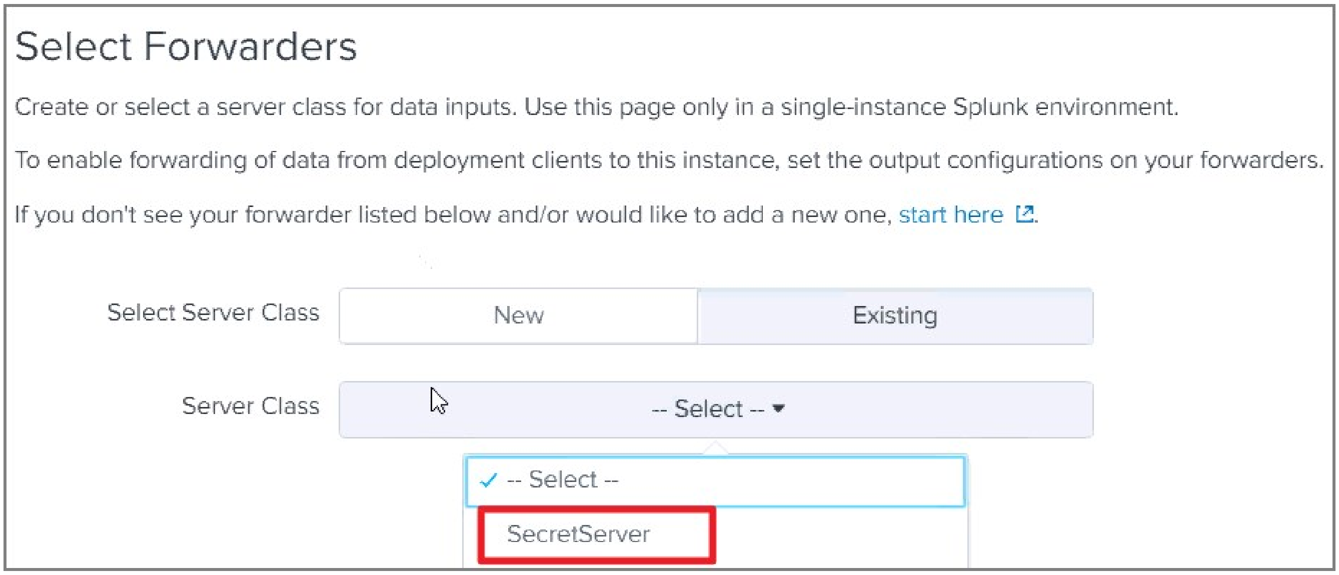
7. Click on **Settings**.
8. Click on **Add Data**.



9. Click on **Forward**.


Or get data in with the following methods
Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data
Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources
Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

10. You can create a **New Server Class** or select a previously created one.



Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

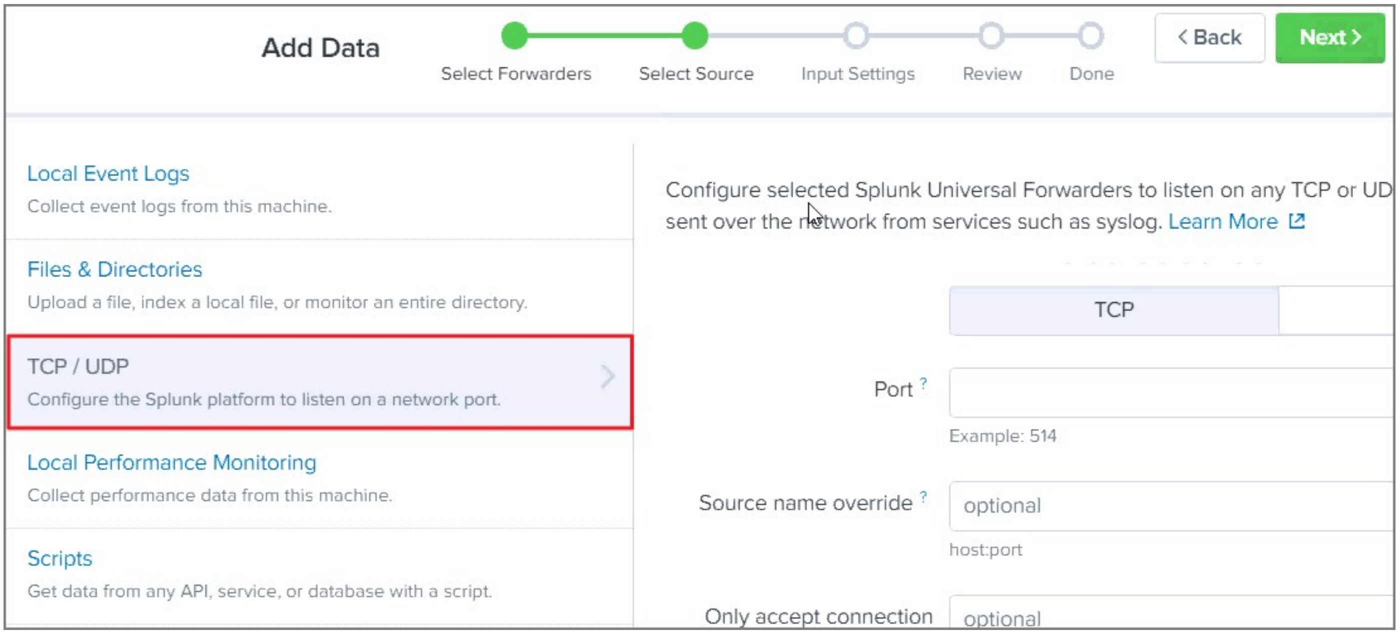
To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders.

If you don't see your forwarder listed below and/or would like to add a new one, start here.

Select Server Class: New | Existing

Server Class: -- Select --

11. Click on the option for **TCP/UDP**.



Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Configure selected Splunk Universal Forwarders to listen on any TCP or UD sent over the network from services such as syslog. Learn More

TCP

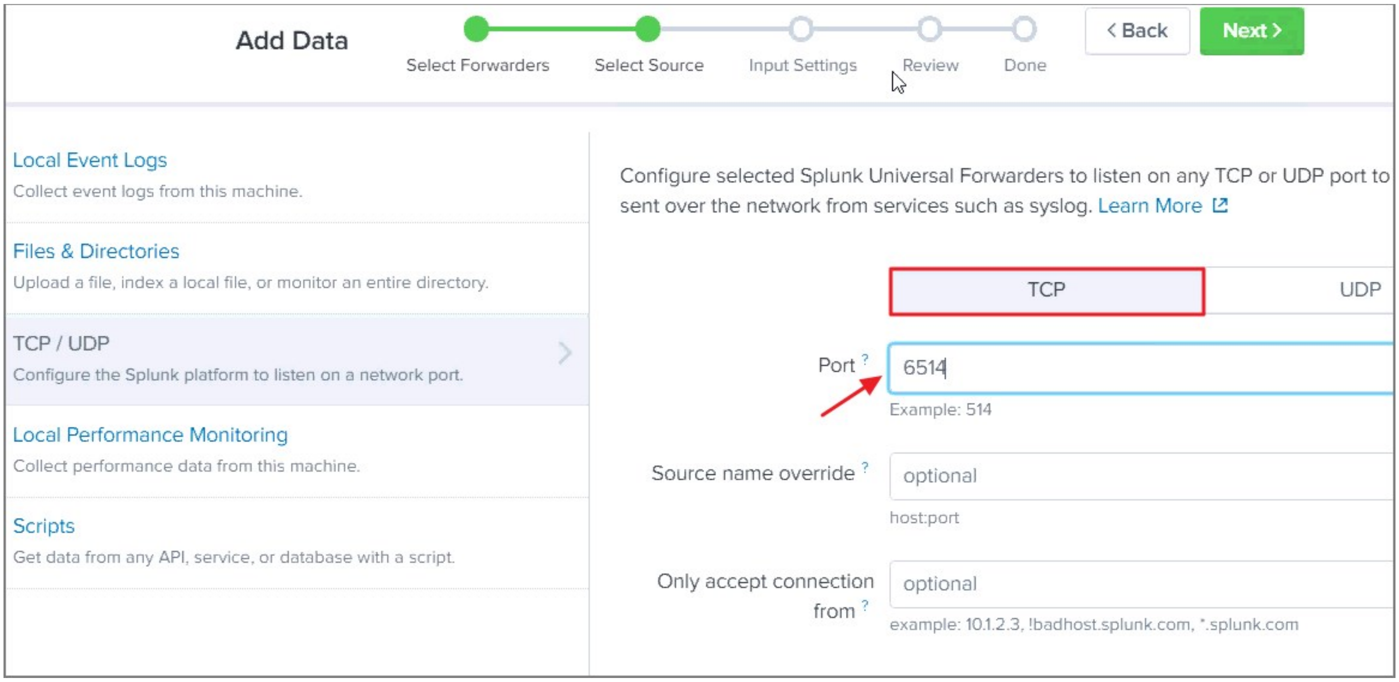
Port ?
Example: 514

Source name override ? optional
host:port

Only accept connection optional

12. Click on **TCP**.

13. Enter the **port number** for the server.



Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Configure selected Splunk Universal Forwarders to listen on any TCP or UDP port to sent over the network from services such as syslog. Learn More

TCP UDP

Port ? 6514
Example: 514

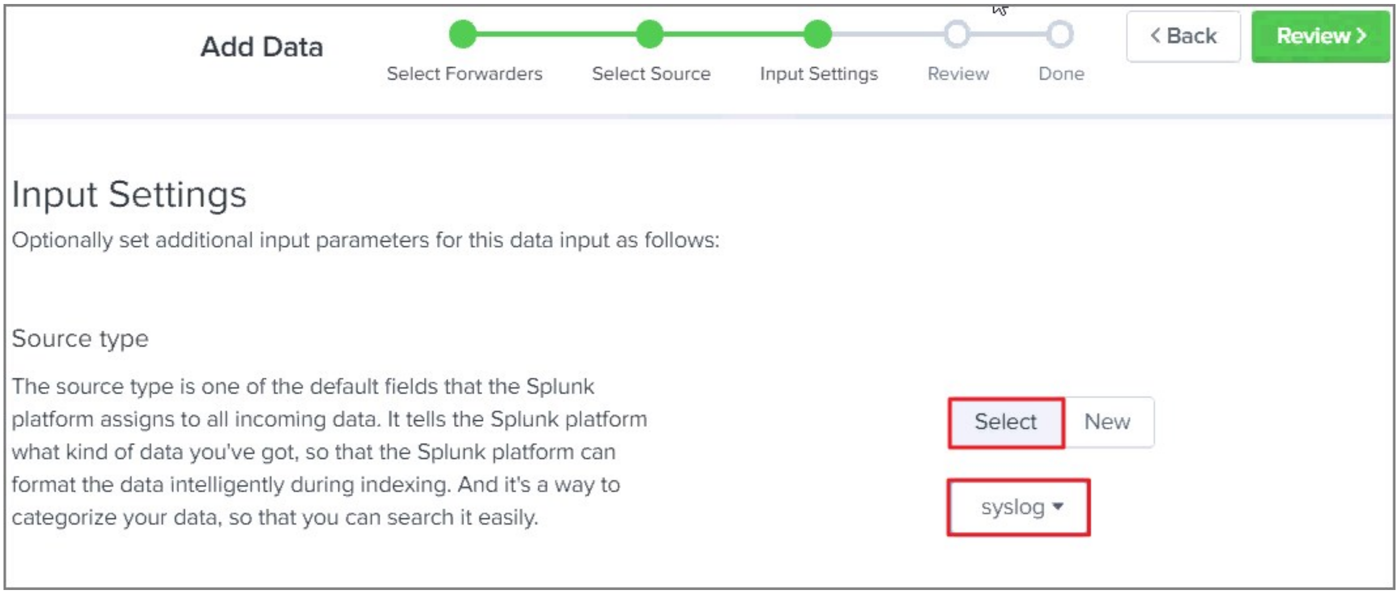
Source name override ? optional
host:port

Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

14. Click **Next**.

15. Click on **Source Type**.

16. Enter **syslog**.



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

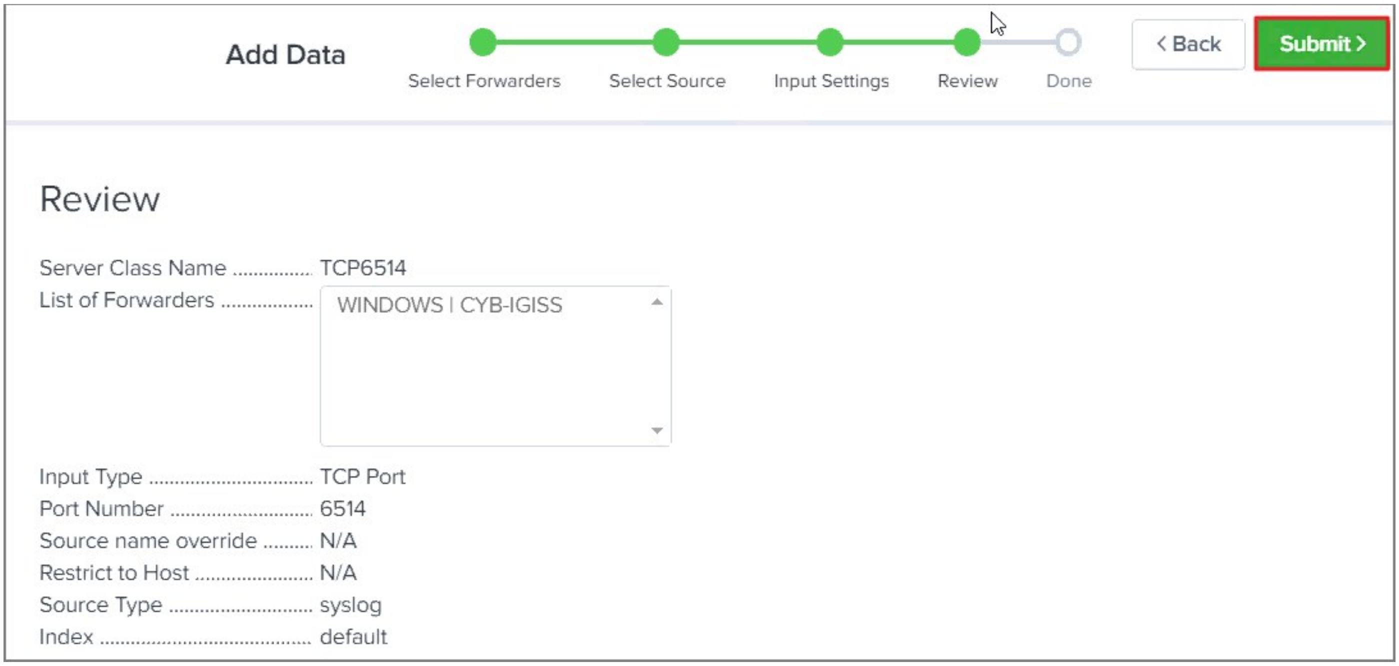
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select New

syslog ▾

17. Click on **Review**.

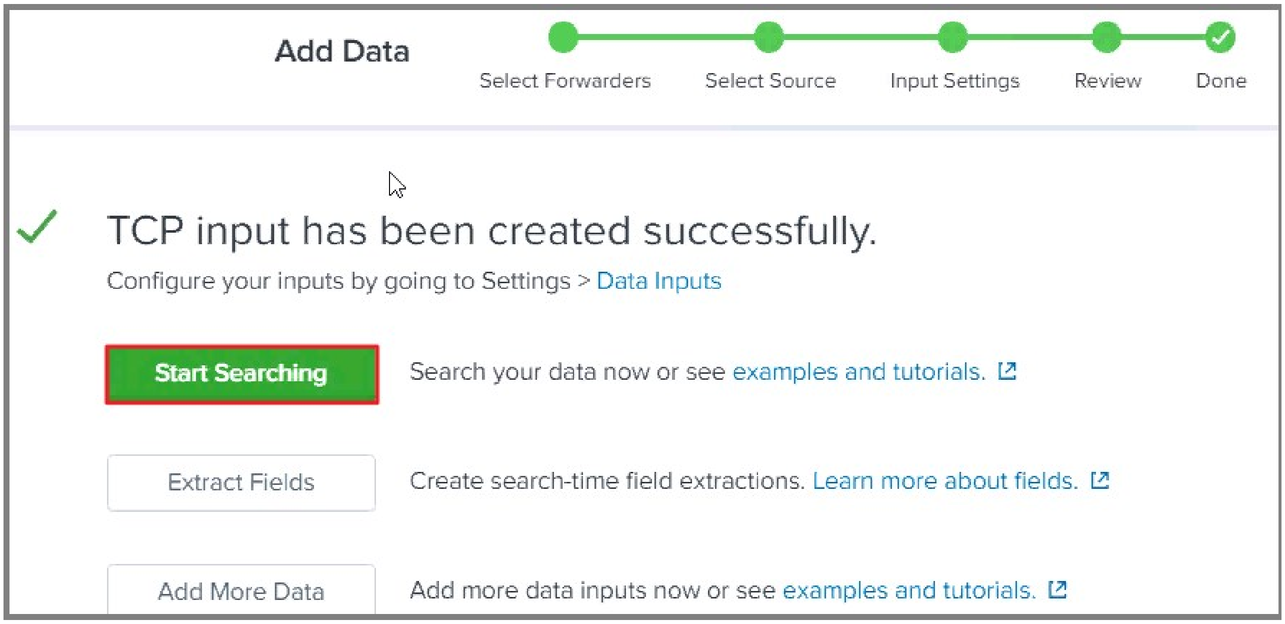
18. Review your settings and click **Submit**.



Review

Server Class Name TCP6514
List of Forwarders .... WINDOWS I CYB-IGISS
Input Type .... TCP Port
Port Number 6514
Source name override .... N/A
Restrict to Host .... N/A
Source Type .... syslog
Index .... default

19. You can then click **Start Searching** after the connection was successfully created.



TCP input has been created successfully.

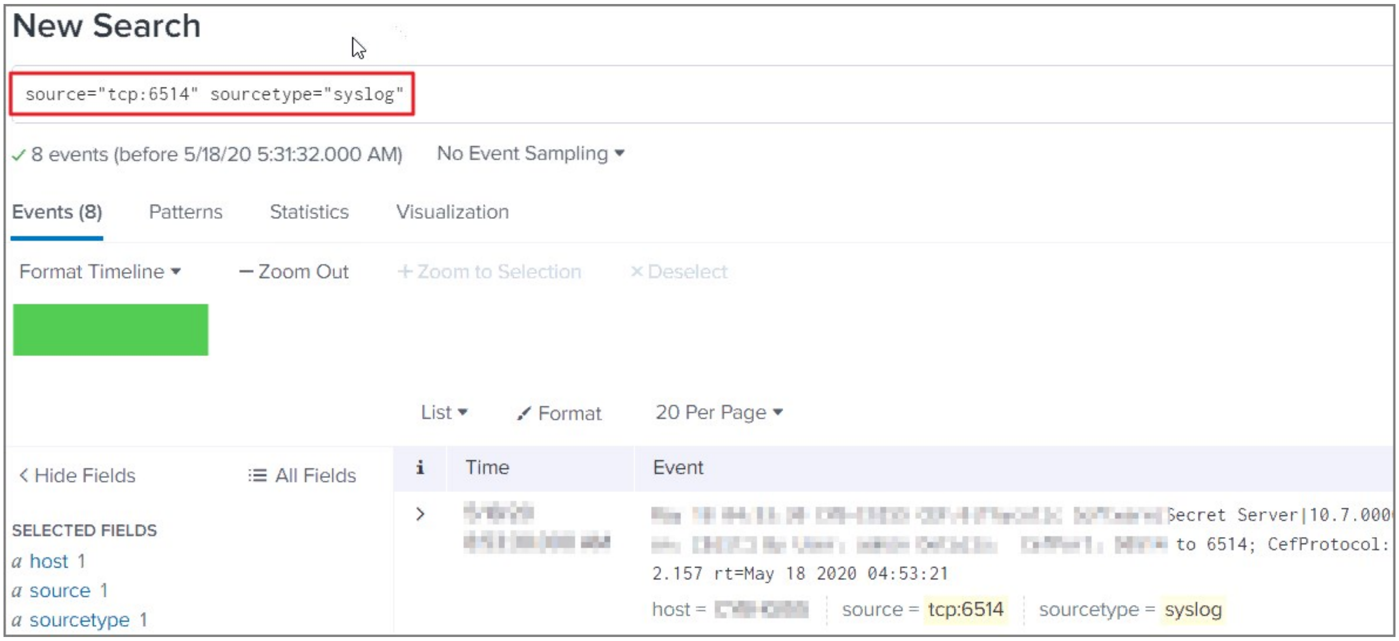
Configure your inputs by going to Settings > Data Inputs

Start Searching — Search your data now or see examples and tutorials.

Extract Fields — Create search-time field extractions. Learn more about fields.

Add More Data — Add more data inputs now or see examples and tutorials.

Example of syslog output:



New Search

```
source="tcp:6514" sourcetype="syslog"
```

✓ 8 events (before 5/18/20 5:31:32.000 AM)

SELECTED FIELDS
- *a* host 1
- *a* source 1
- *a* sourcetype 1

i	Time	Event
>	[redacted]	[redacted]Secret Server|10.7.000 [redacted] to 6514; CefProtocol: 2.157 rt=May 18 2020 04:53:21 host = [redacted] source = tcp:6514 sourcetype = syslog

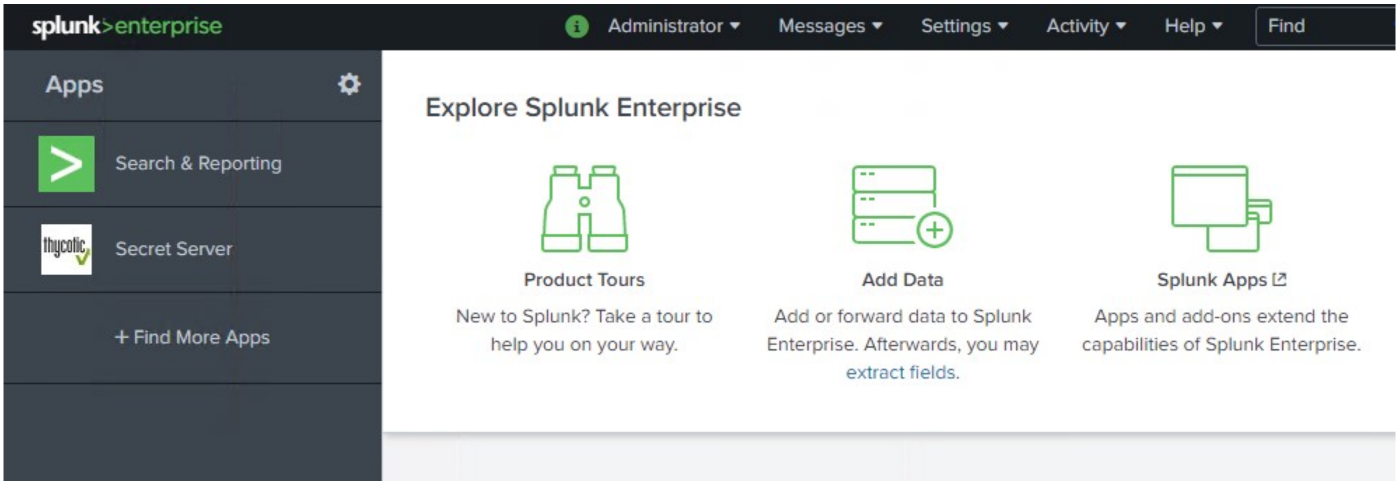
Create an App

The first step is to fill in the information for the **Add new page** to create an App.

To create an App

1. Go to **Splunk Enterprise**.

   Note: After installing Splunk enterprise edition, you can open an enterprise by entering the URL https://localhost:8000.



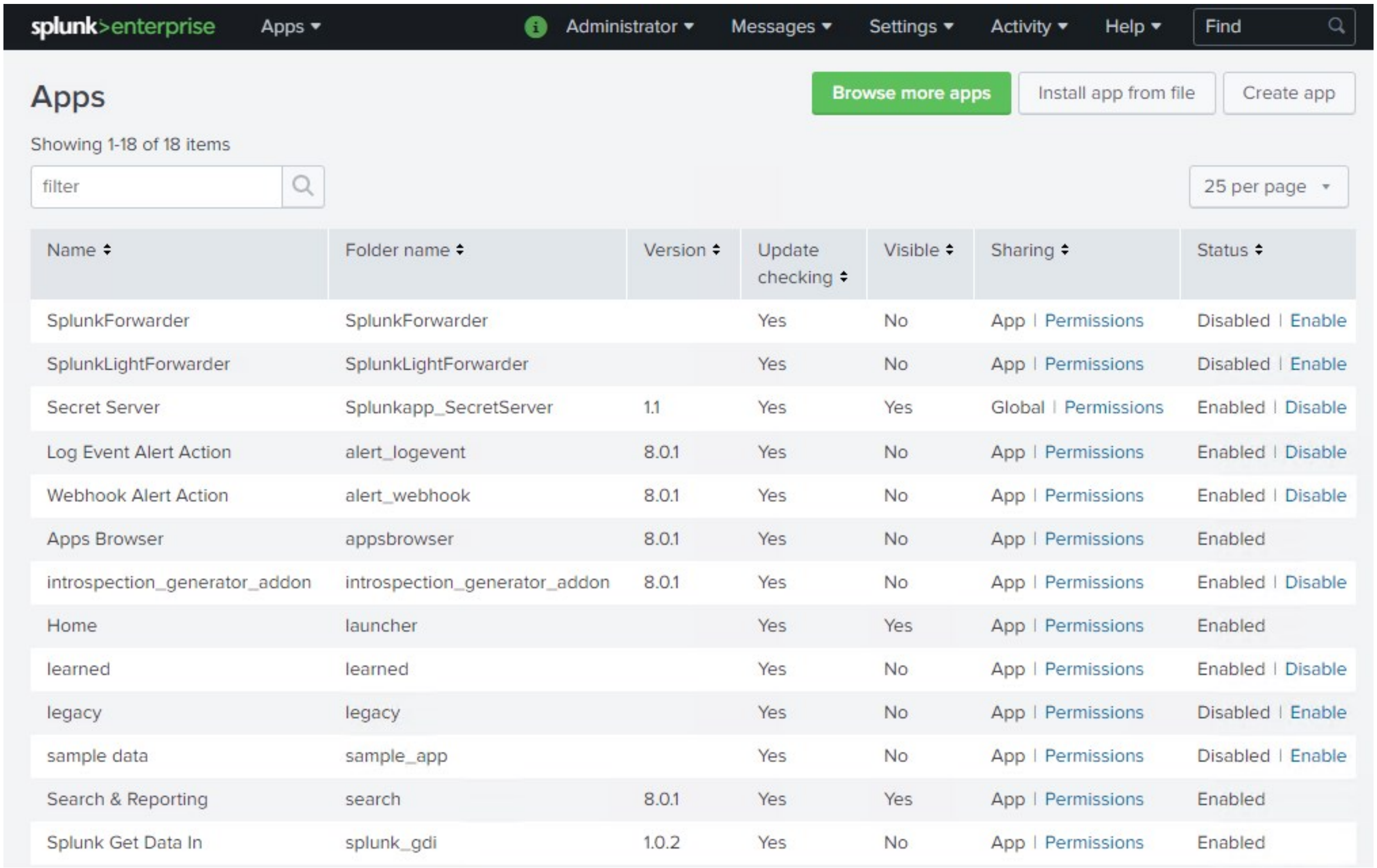
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

2. On the left-hand side, click the **Manage Apps** icon. The **Apps** page appears.

   ⚙

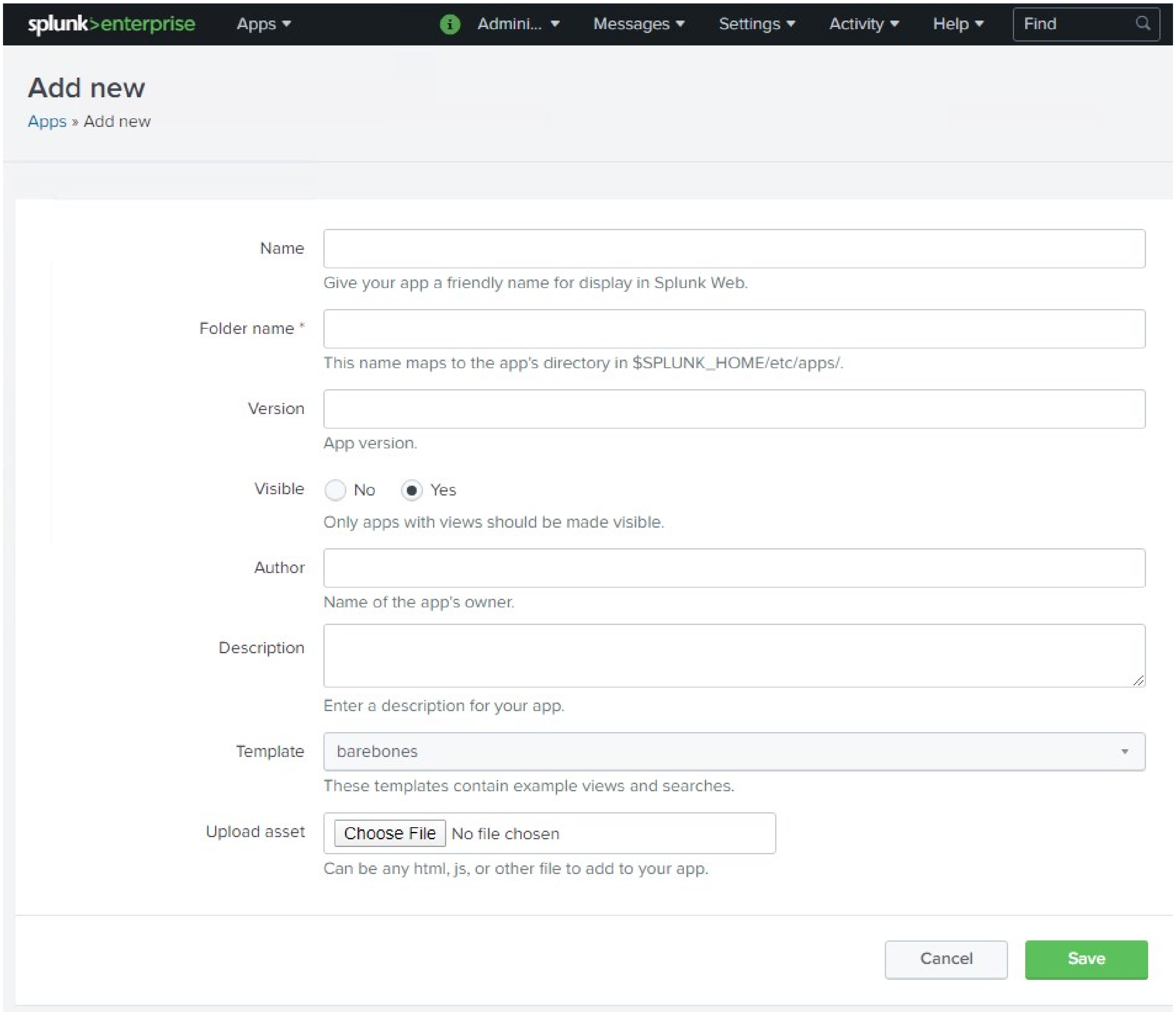


Apps

Showing 1-18 of 18 items

Name ⬍	Folder name ⬍	Version ⬍	Update checking ⬍	Visible ⬍	Sharing ⬍	Status ⬍
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable
Secret Server	Splunkapp_SecretServer	1.1	Yes	Yes	Global | Permissions	Enabled | Disable
Log Event Alert Action	alert_logevent	8.0.1	Yes	No	App | Permissions	Enabled | Disable
Webhook Alert Action	alert_webhook	8.0.1	Yes	No	App | Permissions	Enabled | Disable
Apps Browser	appsbrowser	8.0.1	Yes	No	App | Permissions	Enabled
introspection_generator_addon	introspection_generator_addon	8.0.1	Yes	No	App | Permissions	Enabled | Disable
Home	launcher		Yes	Yes	App | Permissions	Enabled
learned	learned		Yes	No	App | Permissions	Enabled | Disable
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable
sample data	sample_app		Yes	No	App | Permissions	Disabled | Enable
Search & Reporting	search	8.0.1	Yes	Yes	App | Permissions	Enabled
Splunk Get Data In	splunk_gdi	1.0.2	Yes	No	App | Permissions	Enabled

3. On the upper-right click **Create app**. The **Add new** page appears.



Add new

Apps » Add new

Name

Give your app a friendly name for display in Splunk Web.

Folder name *

This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.

Version

App version.

Visible ○ No ● Yes

Only apps with views should be made visible.

Author

Name of the app's owner.

Description

Enter a description for your app.

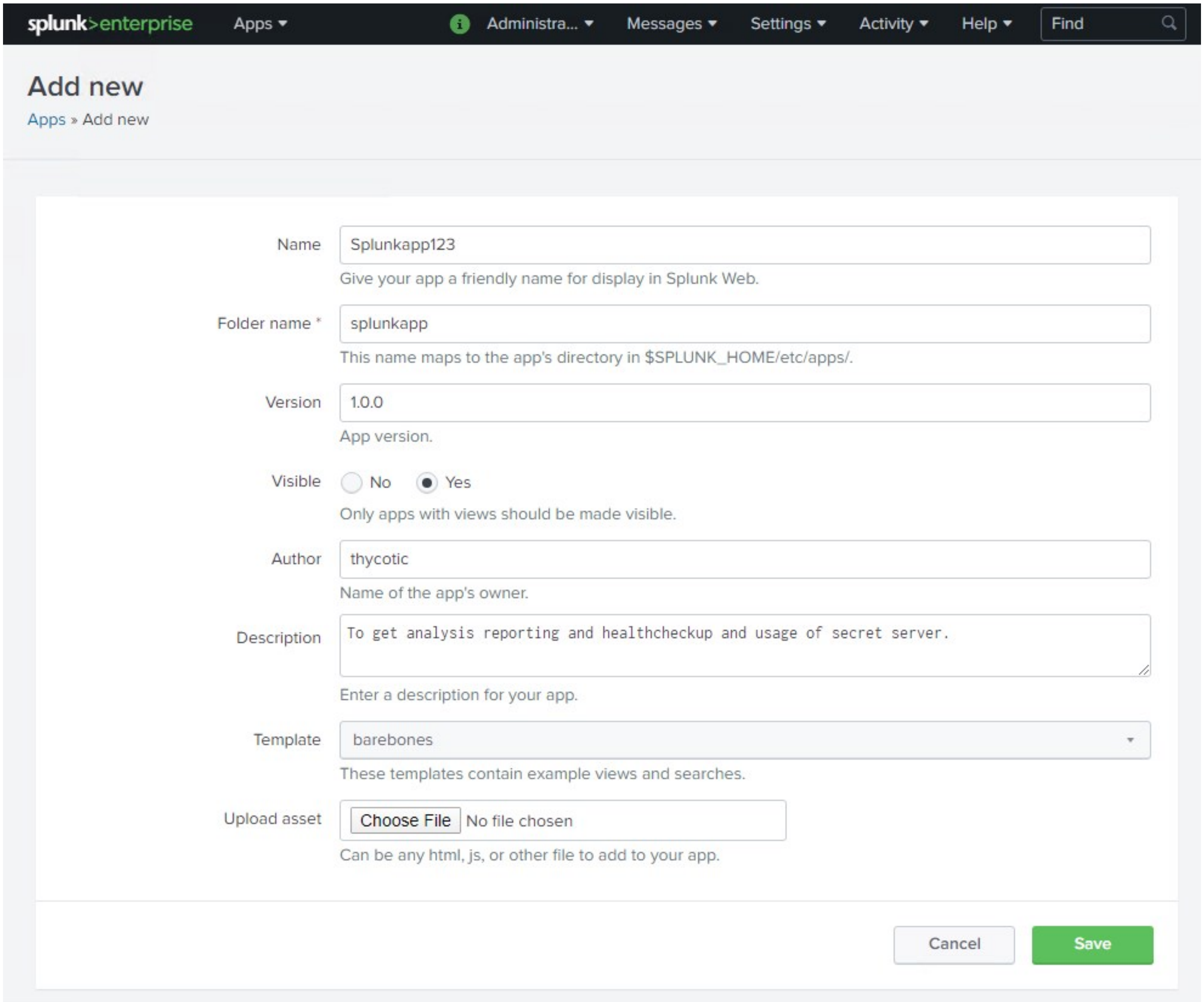
Template barebones

These templates contain example views and searches.

Upload asset Choose File No file chosen

Can be any html, js, or other file to add to your app.

4. In the **Add new** page, fill in the information:



Add new

Apps » Add new

Name: Splunkapp123
Give your app a friendly name for display in Splunk Web.

Folder name *: splunkapp
This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.

Version: 1.0.0
App version.

Visible: ○ No ● Yes
Only apps with views should be made visible.

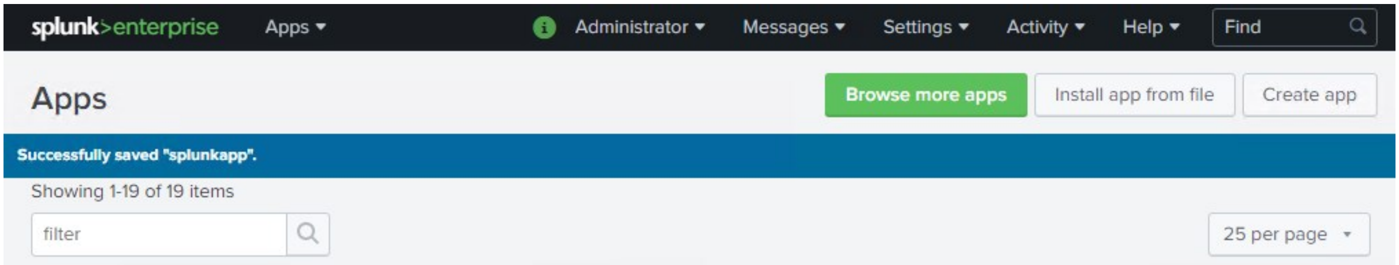
Author: thycotic
Name of the app's owner.

Description: To get analysis reporting and healthcheckup and usage of secret server.
Enter a description for your app.

Template: barebones
These templates contain example views and searches.

Upload asset: Choose File No file chosen
Can be any html, js, or other file to add to your app.

5. Select the default template.
6. Click **Save**. On the upper-left, a message, **Successfully saved "splunkapp".** appears.



Successfully saved "splunkapp".

Showing 1-19 of 19 items

7. The Splunk app is saved.

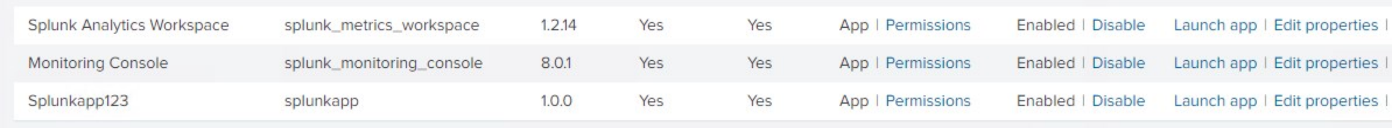
You can check the new app at the following location on your computer where enterprise edition is installed: C:\\Program Files\\Splunk\\etc\\apps.

Create Dashboard

The second step is to fill in the Create a New Dashboard dialog box and add source code to create a new dashboard.

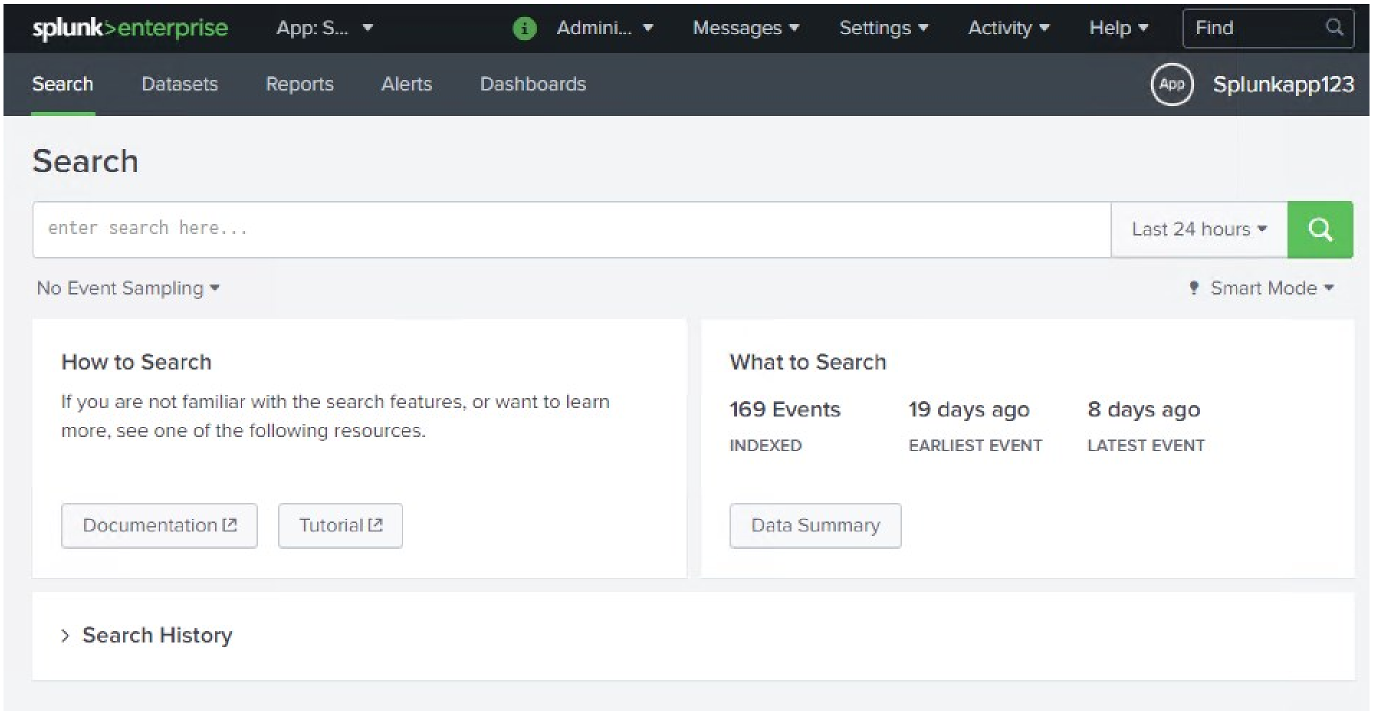
To create a dashboard

1. Go to the **Apps** page.
2. Click **Launch app** in the **Actions** column of the app you created.



Splunk Analytics Workspace	splunk_metrics_workspace	1.2.14	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties |
Monitoring Console	splunk_monitoring_console	8.0.1	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties |
Splunkapp123	splunkapp	1.0.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties |

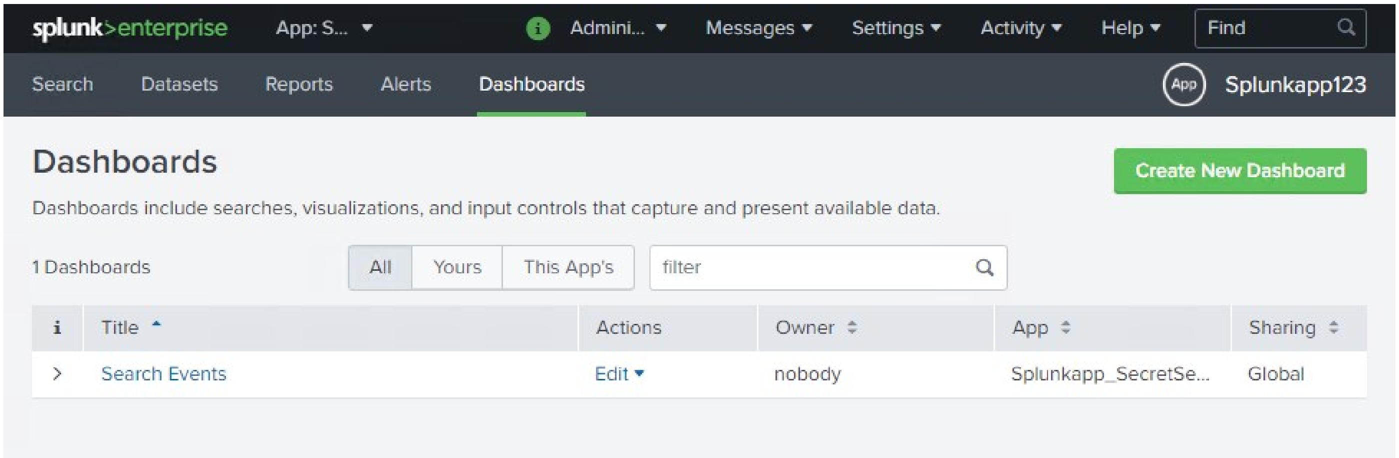
3. The **Search** page appears.



If you are not familiar with the search features, or want to learn more, see one of the following resources.

169 Events	19 days ago	8 days ago
INDEXED	EARLIEST EVENT	LATEST EVENT

4. Click the **Dashboard** menu. The **Dashboards** page appears.



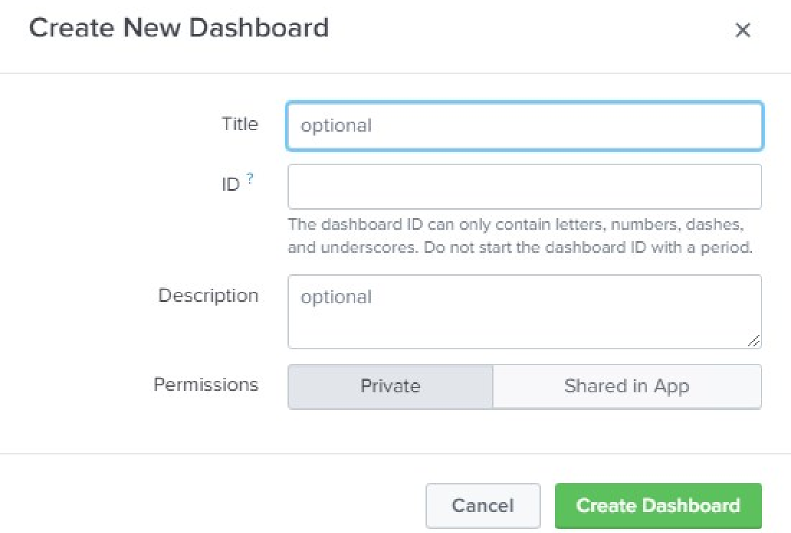
Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

1 Dashboards

i	Title	Actions	Owner	App	Sharing
>	Search Events	Edit	nobody	Splunkapp_SecretSe...	Global

5. Click **Create New Dashboard**. The **Create New Dashboard** dialog box appears.



Title: optional

ID ?

The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.

Description: optional

Permissions: Private | Shared in App

6. In the **Title** text box, type the title for the dashboard.
7. In the **Permissions** field, select **Shared in App**.
8. Click **Create Dashboard**. The