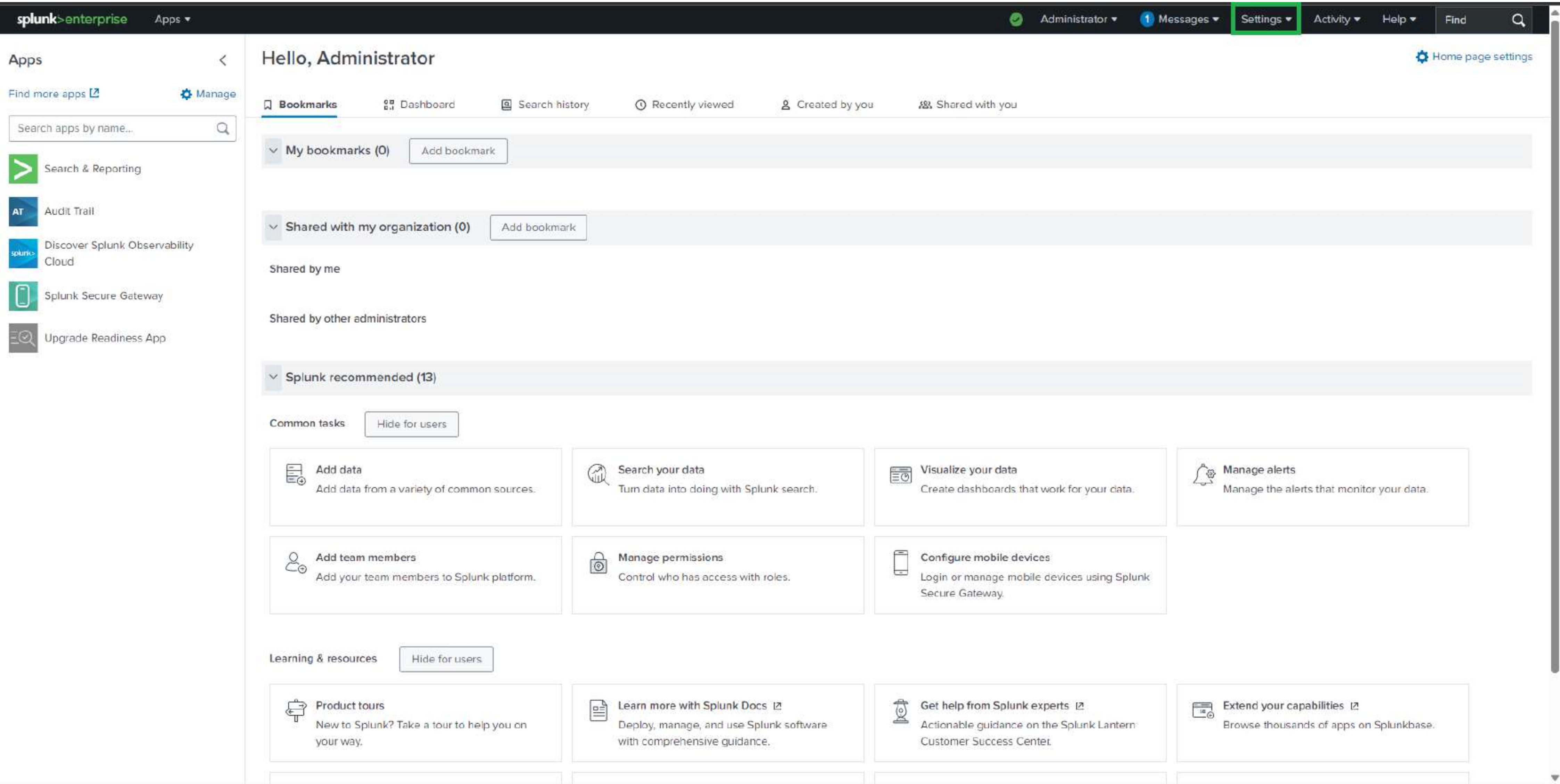


Apps

Find more apps

Manage

Search apps by name...

- Search & Reporting
- Audit Trail
- Discover Splunk Observability Cloud
- Splunk Secure Gateway
- Upgrade Readiness App

Hello, Administrator

Home page settings

Bookmarks | Dashboard | Search history | Recently viewed | Created by you | Shared with you

My bookmarks (0) Add bookmark

Shared with my organization (0) Add bookmark

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks Hide for users

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

Manage alerts
Manage the alerts that monitor your data.

Add team members
Add your team members to Splunk platform.

Manage permissions
Control who has access with roles.

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

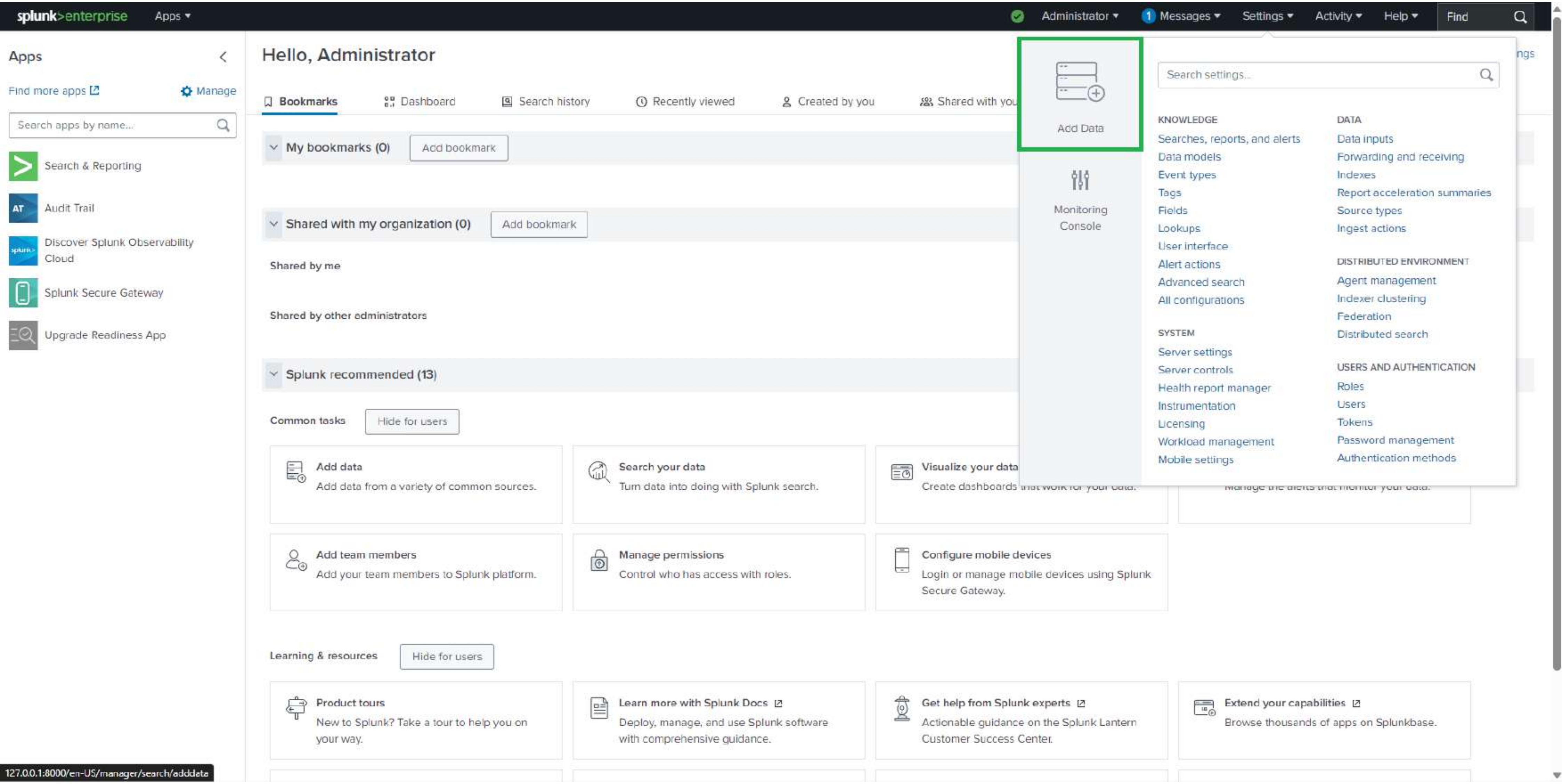
Learning & resources Hide for users

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

Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.

Extend your capabilities
Browse thousands of apps on Splunkbase.



splunk>enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Apps

Find more apps ↗ Manage

Search apps by name...

- Search & Reporting
- Audit Trail
- Discover Splunk Observability Cloud
- Splunk Secure Gateway
- Upgrade Readiness App

Hello, Administrator

Bookmarks | Dashboard | Search history | Recently viewed | Created by you | Shared with you

My bookmarks (0) Add bookmark

Shared with my organization (0) Add bookmark

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks Hide for users

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

Manage the alerts that monitor your data.

Add team members
Add your team members to Splunk platform.

Manage permissions
Control who has access with roles.

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learning & resources Hide for users

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

Learn more with Splunk Docs ↗
Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts ↗
Actionable guidance on the Splunk Lantern Customer Success Center.

Extend your capabilities ↗
Browse thousands of apps on Splunkbase.

Add Data

Monitoring Console

Search settings...

KNOWLEDGE
- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

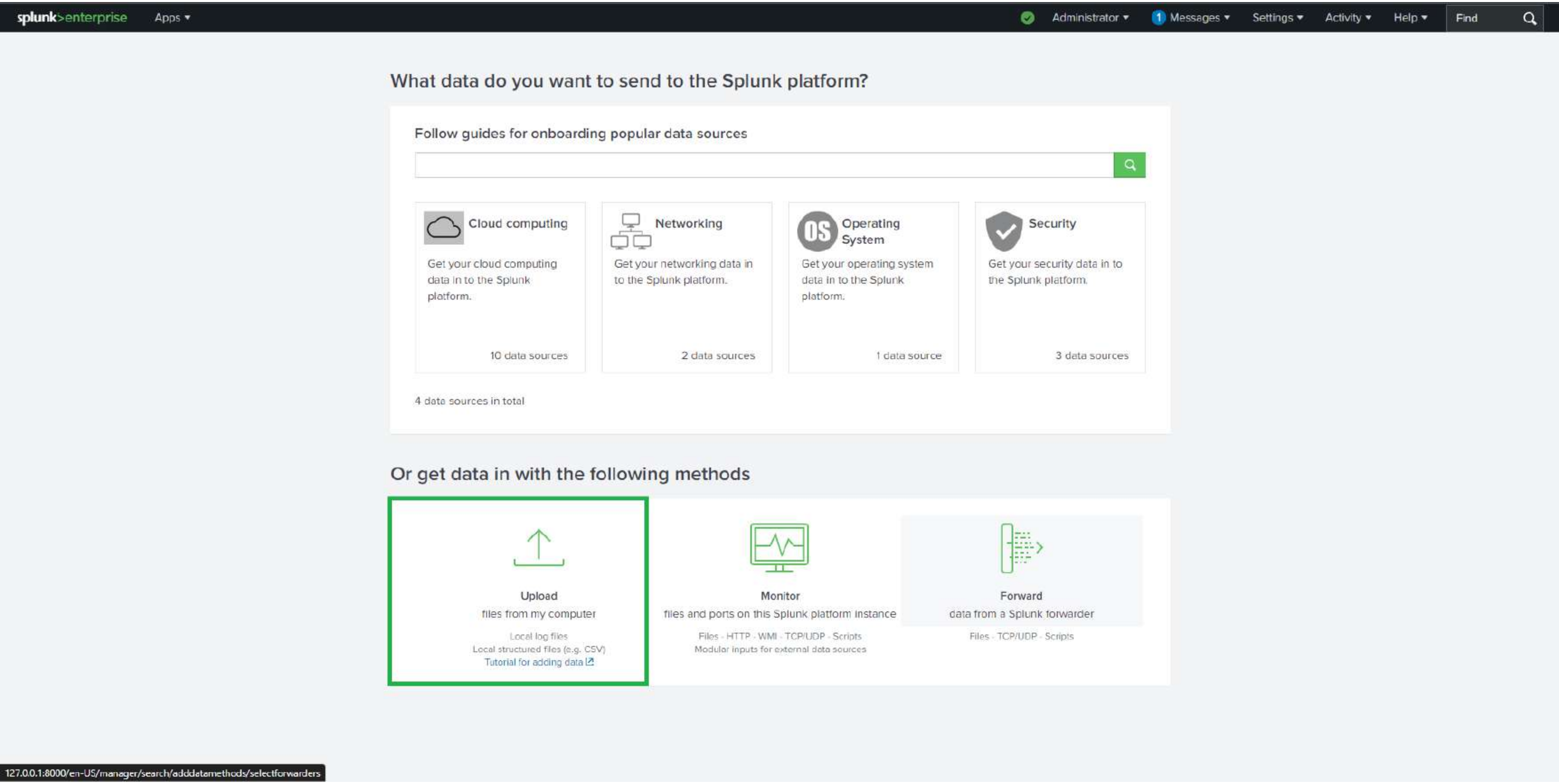
SYSTEM
- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management
- Mobile settings

DATA
- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT
- Agent management
- Indexer clustering
- Federation
- Distributed search

USERS AND AUTHENTICATION
- Roles
- Users
- Tokens
- Password management
- Authentication methods

127.0.0.1:8000/en-US/manager/search/adddata



What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing
Get your cloud computing data in to the Splunk platform.
10 data sources

Networking
Get your networking data in to the Splunk platform.
2 data sources

Operating System
Get your operating system data in to the Splunk platform.
1 data source

Security
Get your security data in to the Splunk platform.
3 data sources

4 data sources in total

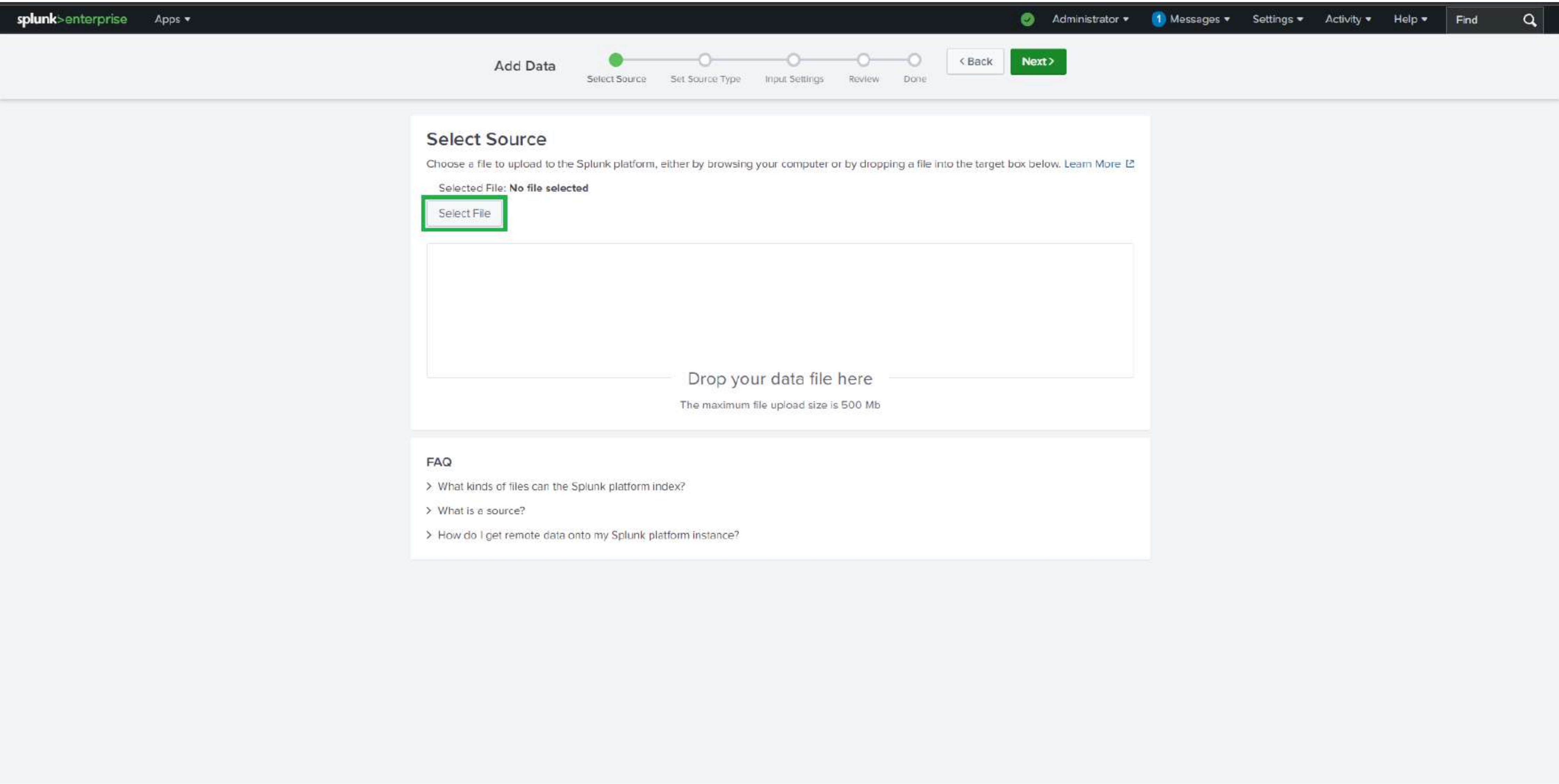
Or get data in with the following methods

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

127.0.0.1:8000/en-US/manager/search/adddatamethods/selectforwarders



Add Data

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **No file selected**

Drop your data file here

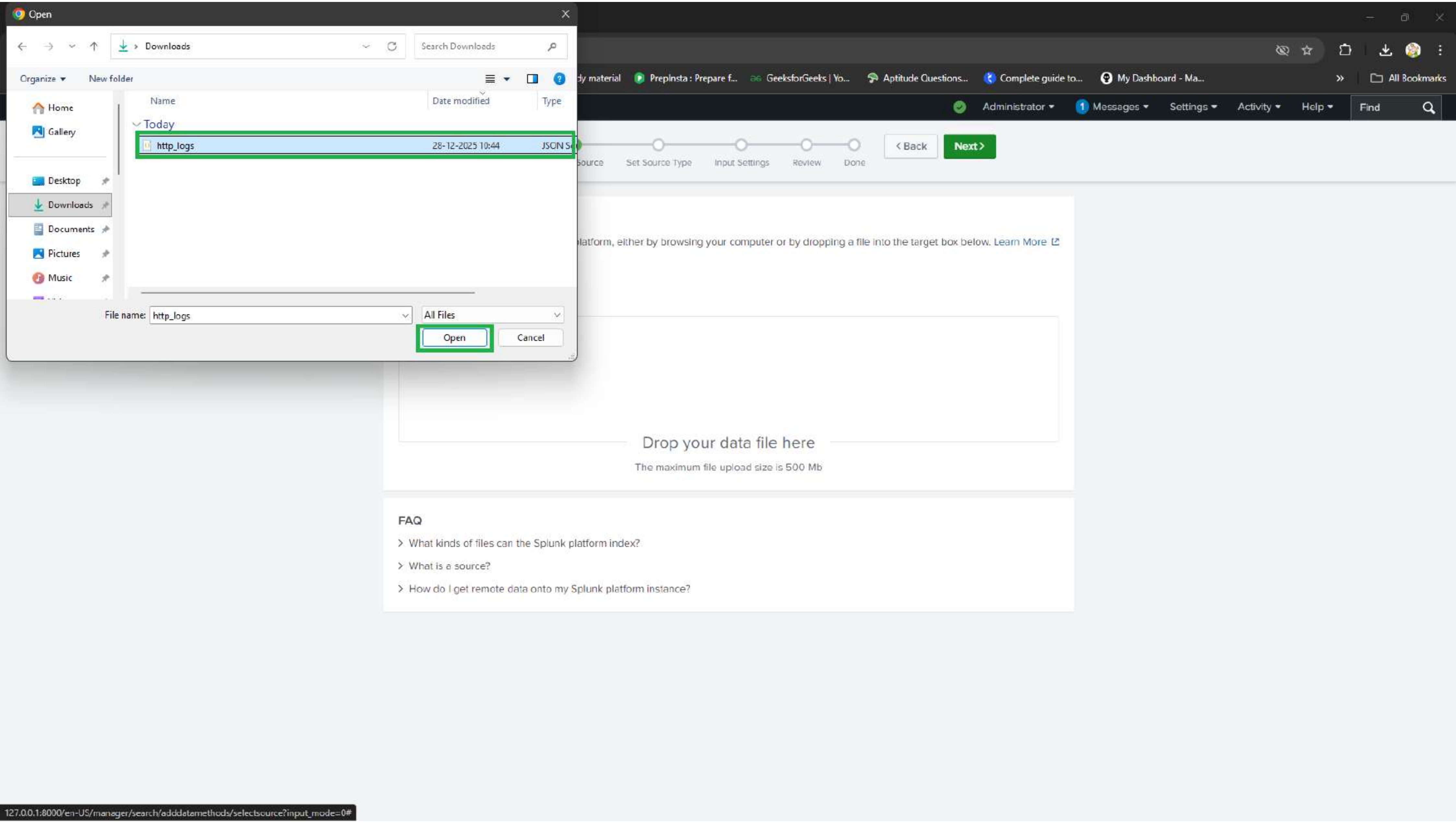
The maximum file upload size is 500 Mb

FAQ

> What kinds of files can the Splunk platform index?

> What is a source?

> How do I get remote data onto my Splunk platform instance?



Name	Date modified	Type
http_logs	28-12-2025 10:44	JSON S

File name: http_logs

All Files

latform, either by browsing your computer or by dropping a file into the target box below. Learn More

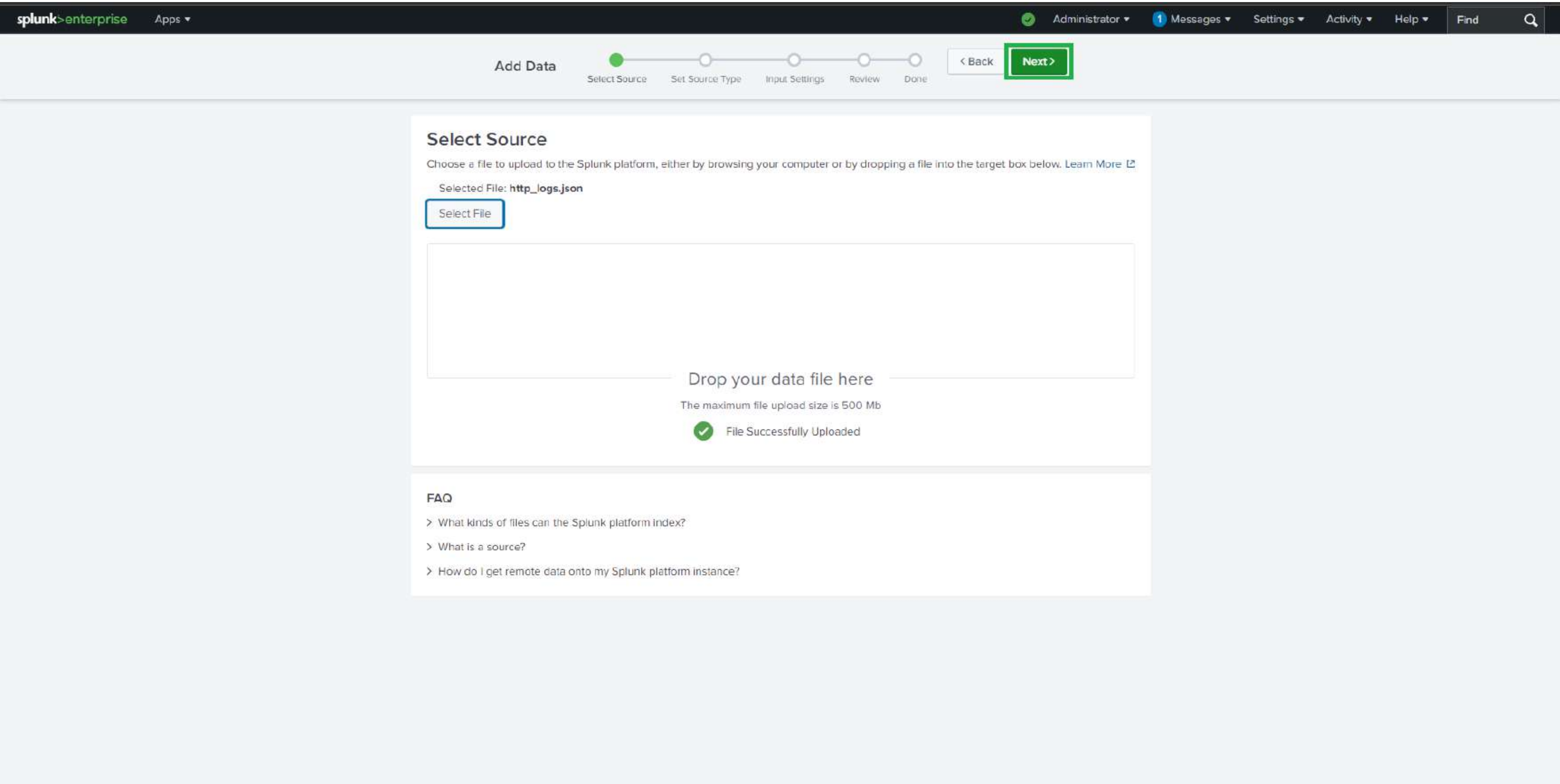
Drop your data file here

The maximum file upload size is 500 Mb

FAQ

- What kinds of files can the Splunk platform index?
- What is a source?
- How do I get remote data onto my Splunk platform instance?

127.0.0.1:8000/en-US/manager/search/adddatamethods/selectsource?input_mode=0#



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **http_logs.json**

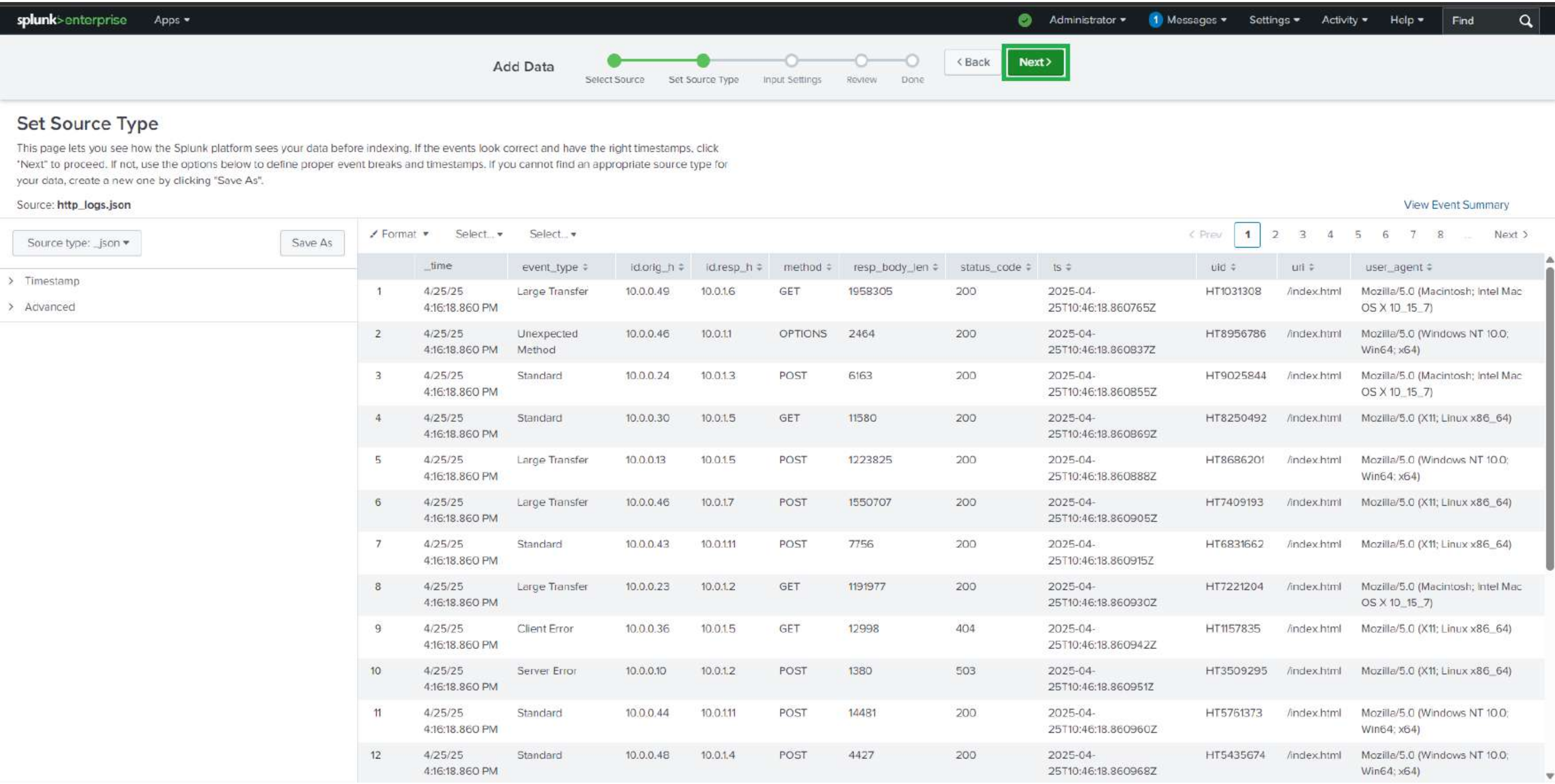
Drop your data file here

The maximum file upload size is 500 Mb

✓ File Successfully Uploaded

FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?
- > How do I get remote data onto my Splunk platform instance?

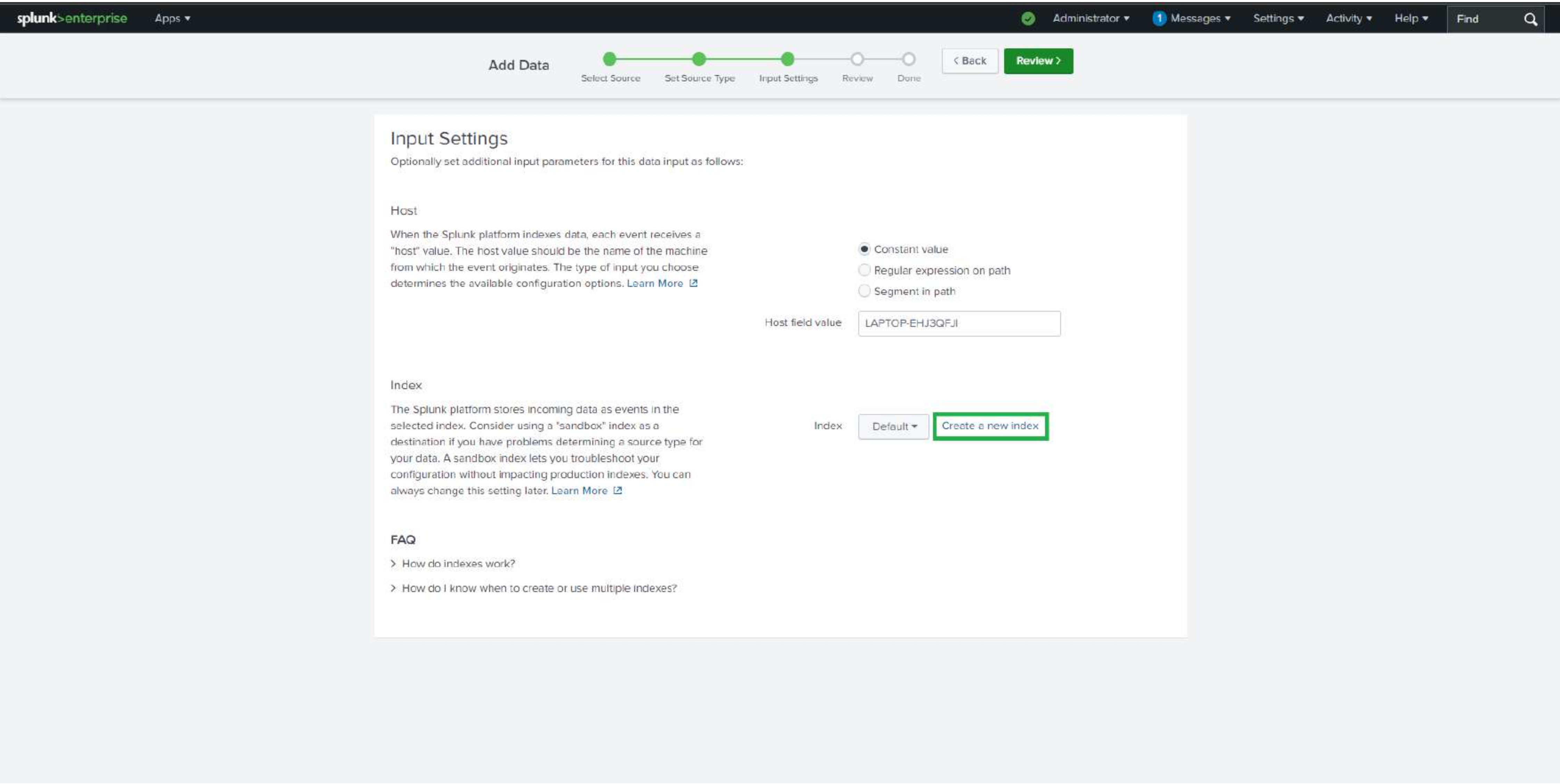


Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **http_logs.json**

	_time	event_type	id.orig_h	id.resp_h	method	resp_body_len	status_code	ts	uid	uri	user_agent
1	4/25/25 4:16:18.860 PM	Large Transfer	10.0.0.49	10.0.1.6	GET	1958305	200	2025-04-25T10:46:18.860765Z	HT1031308	/index.html	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
2	4/25/25 4:16:18.860 PM	Unexpected Method	10.0.0.46	10.0.1.1	OPTIONS	2464	200	2025-04-25T10:46:18.860837Z	HT8956786	/index.html	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
3	4/25/25 4:16:18.860 PM	Standard	10.0.0.24	10.0.1.3	POST	6163	200	2025-04-25T10:46:18.860855Z	HT9025844	/index.html	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
4	4/25/25 4:16:18.860 PM	Standard	10.0.0.30	10.0.1.5	GET	11580	200	2025-04-25T10:46:18.860869Z	HT8250492	/index.html	Mozilla/5.0 (X11; Linux x86_64)
5	4/25/25 4:16:18.860 PM	Large Transfer	10.0.0.13	10.0.1.5	POST	1223825	200	2025-04-25T10:46:18.860888Z	HT8686201	/index.html	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
6	4/25/25 4:16:18.860 PM	Large Transfer	10.0.0.46	10.0.1.7	POST	1550707	200	2025-04-25T10:46:18.860905Z	HT7409193	/index.html	Mozilla/5.0 (X11; Linux x86_64)
7	4/25/25 4:16:18.860 PM	Standard	10.0.0.43	10.0.1.11	POST	7756	200	2025-04-25T10:46:18.860915Z	HT6831662	/index.html	Mozilla/5.0 (X11; Linux x86_64)
8	4/25/25 4:16:18.860 PM	Large Transfer	10.0.0.23	10.0.1.2	GET	1191977	200	2025-04-25T10:46:18.860930Z	HT7221204	/index.html	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
9	4/25/25 4:16:18.860 PM	Client Error	10.0.0.36	10.0.1.5	GET	12998	404	2025-04-25T10:46:18.860942Z	HT1157835	/index.html	Mozilla/5.0 (X11; Linux x86_64)
10	4/25/25 4:16:18.860 PM	Server Error	10.0.0.10	10.0.1.2	POST	1380	503	2025-04-25T10:46:18.860951Z	HT3509295	/index.html	Mozilla/5.0 (X11; Linux x86_64)
11	4/25/25 4:16:18.860 PM	Standard	10.0.0.44	10.0.1.11	POST	14481	200	2025-04-25T10:46:18.860960Z	HT5761373	/index.html	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
12	4/25/25 4:16:18.860 PM	Standard	10.0.0.48	10.0.1.4	POST	4427	200	2025-04-25T10:46:18.860968Z	HT5435674	/index.html	Mozilla/5.0 (Windows NT 10.0; Win64; x64)



Input Settings

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

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value: LAPTOP-EHJ3QFJI

Index

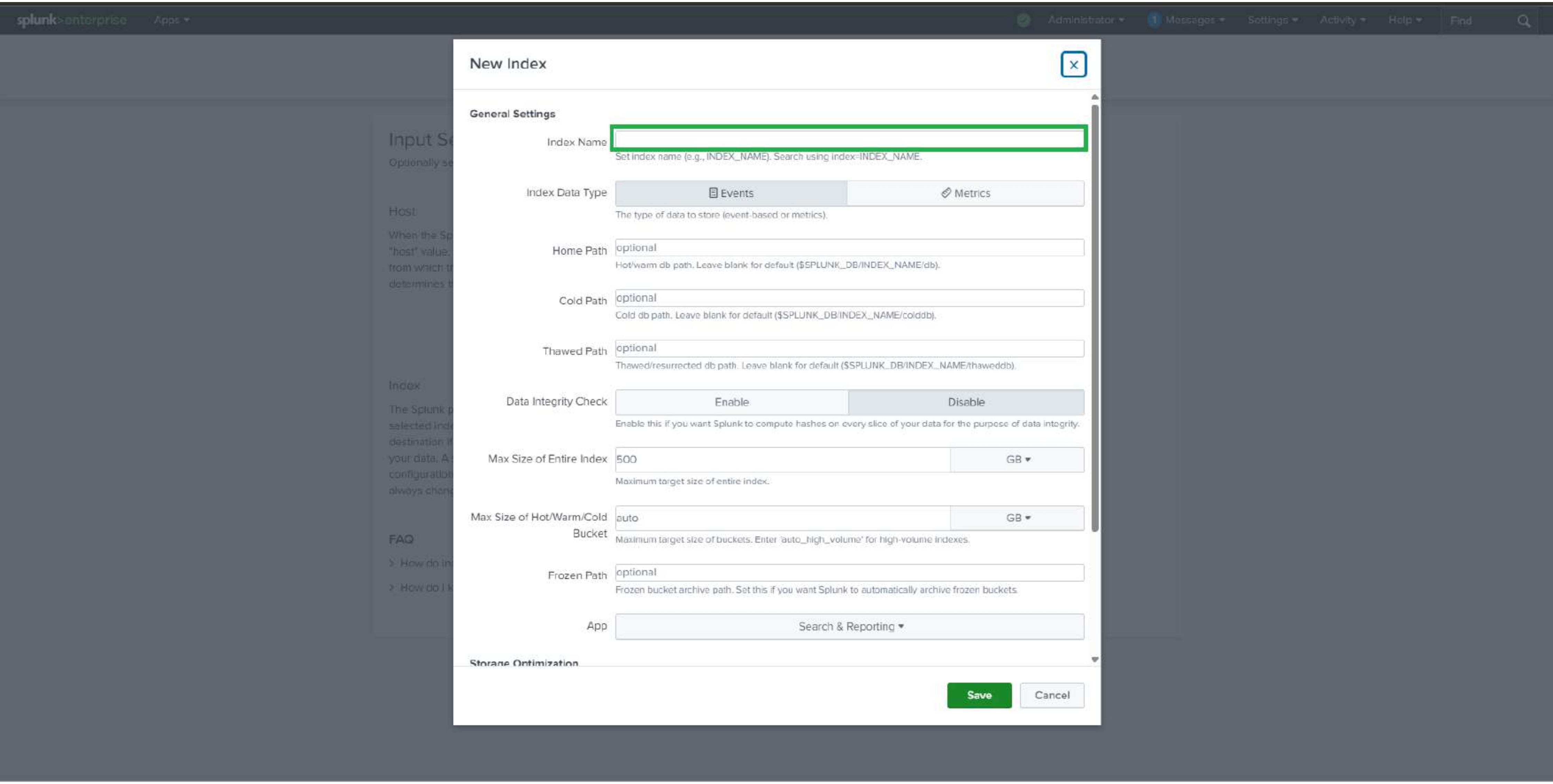
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default ▾ Create a new index

FAQ

› How do indexes work?

› How do I know when to create or use multiple indexes?



New Index

General Settings

Index Name

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Home Path: optional

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional

Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB ▾

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB ▾

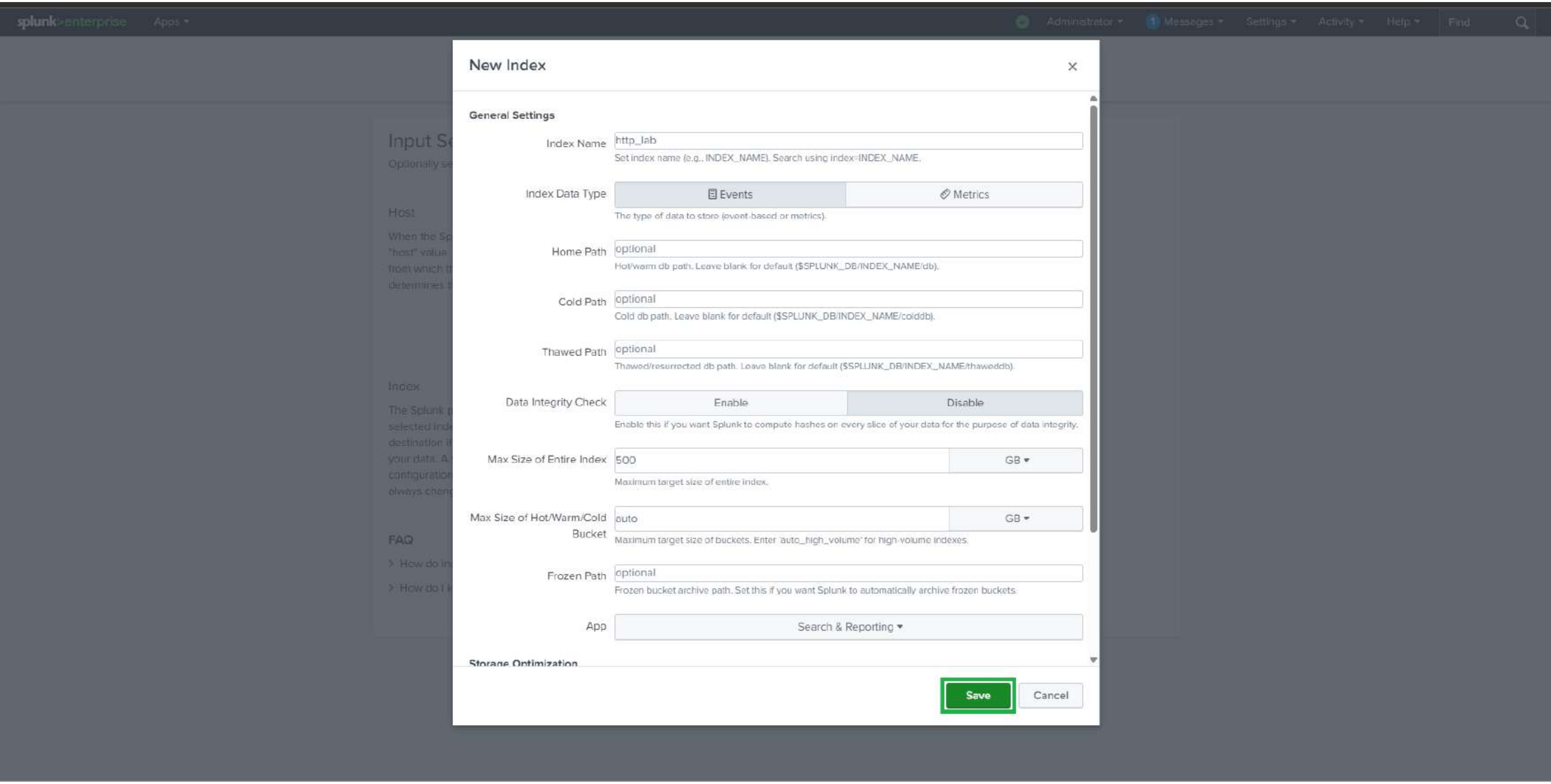
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting ▾

Storage Optimization



New Index ×

General Settings

Index Name: http_lab
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

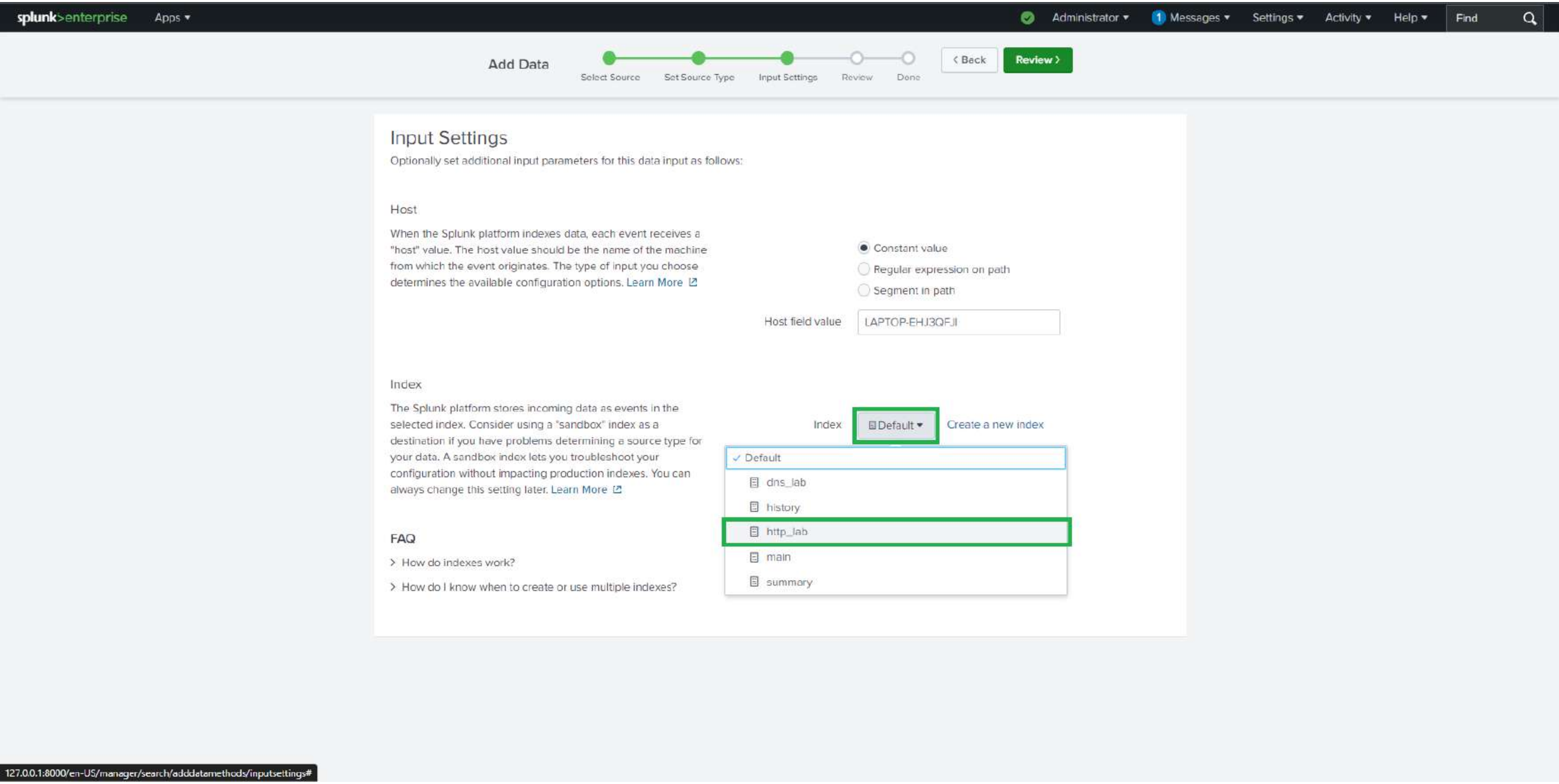
Max Size of Entire Index: 500 GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting ▾

Storage Optimization



Input Settings

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

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value LAPTOP-EHJ3QFJI

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

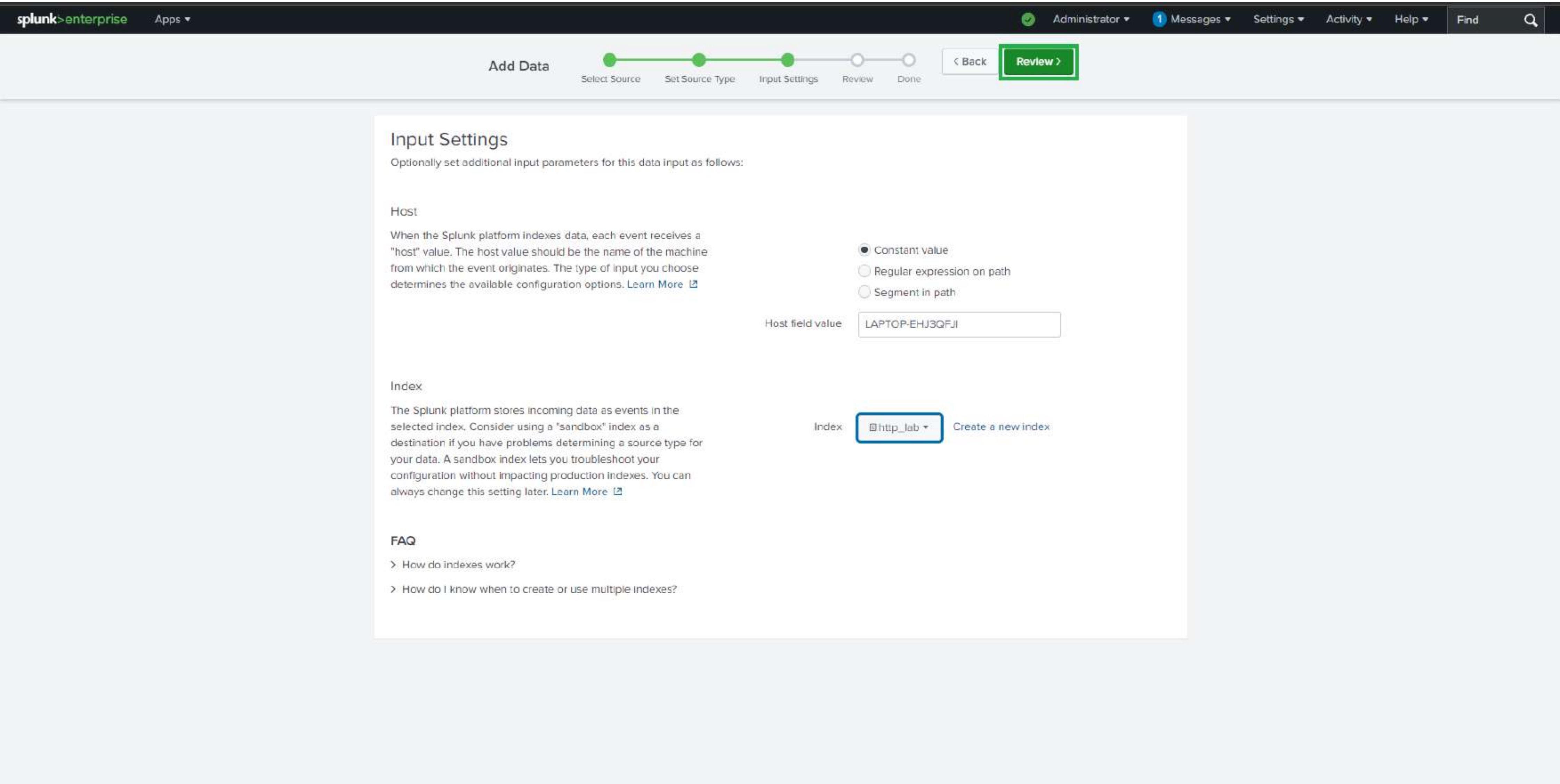
Index Default ▾ Create a new index

FAQ

› How do indexes work?

› How do I know when to create or use multiple indexes?

127.0.0.1:8000/en-US/manager/search/adddatamethods/inputsettings#



Input Settings

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

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value: LAPTOP-EHJ3QFJI

Index

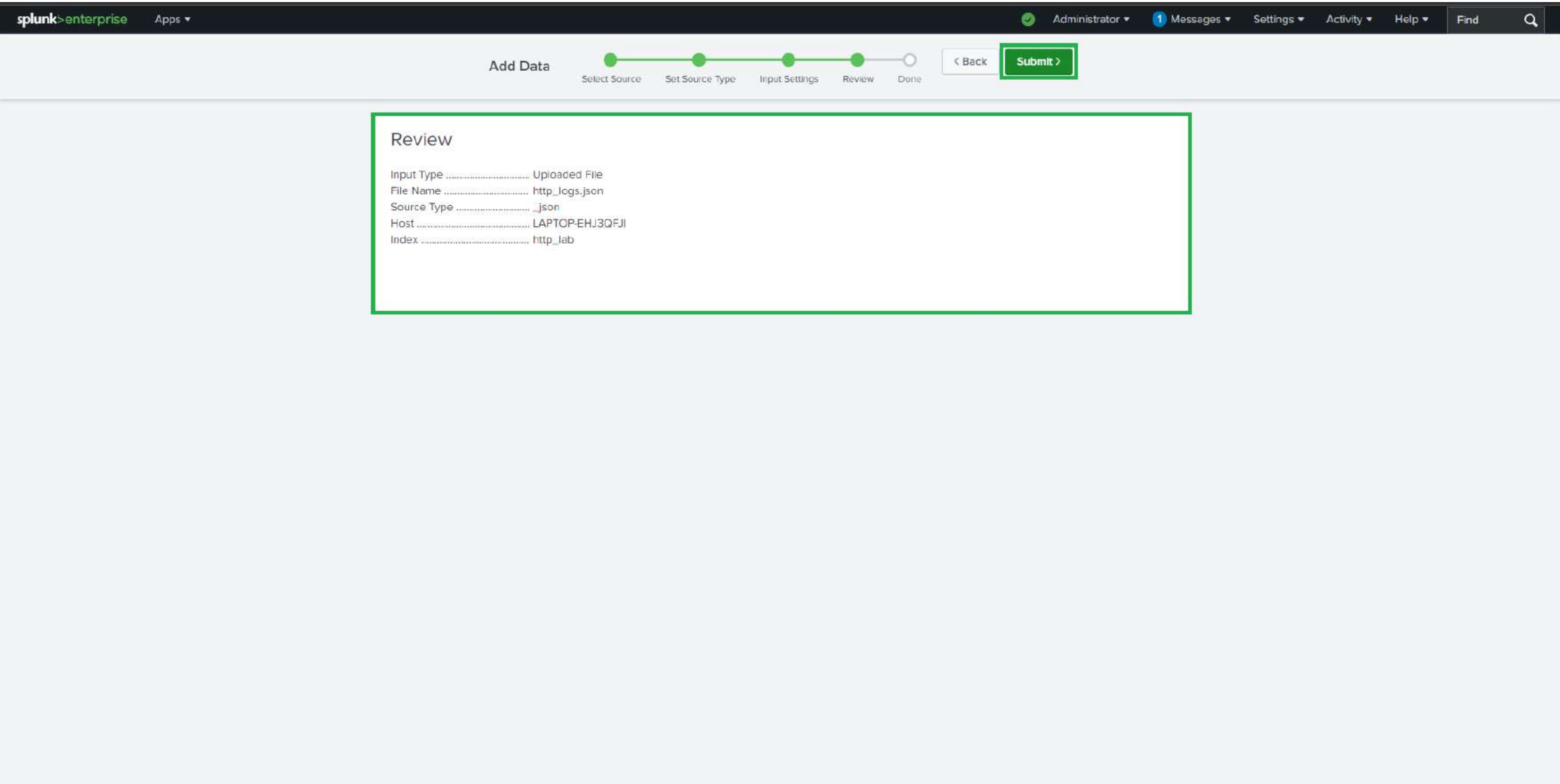
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: http_lab ▾ Create a new index

FAQ

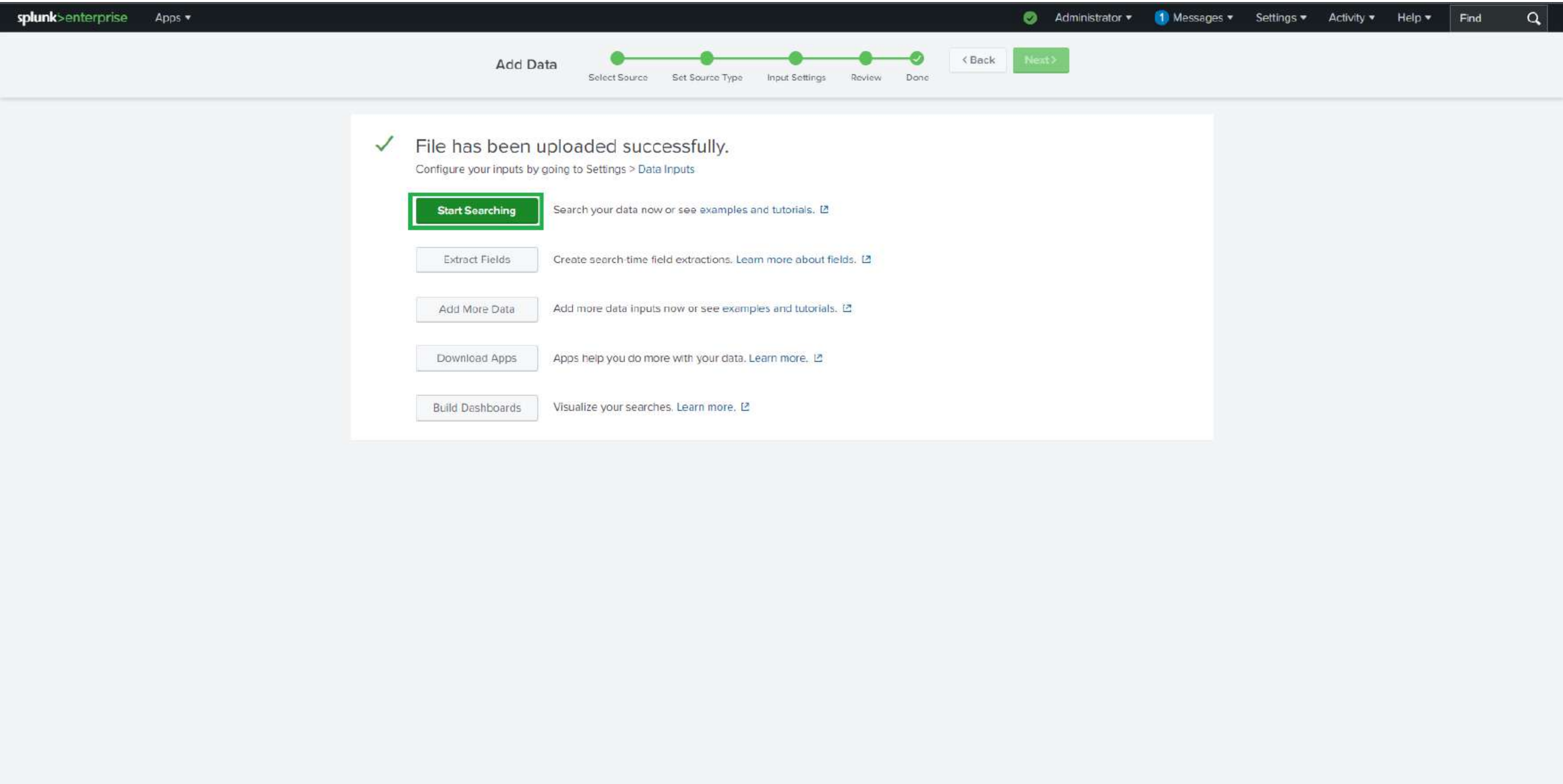
› How do indexes work?

› How do I know when to create or use multiple indexes?



Review

Input Type .... Uploaded File
File Name .... http_logs.json
Source Type .... _json
Host LAPTOP-EHJ3QFJI
Index .... http_lab



✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

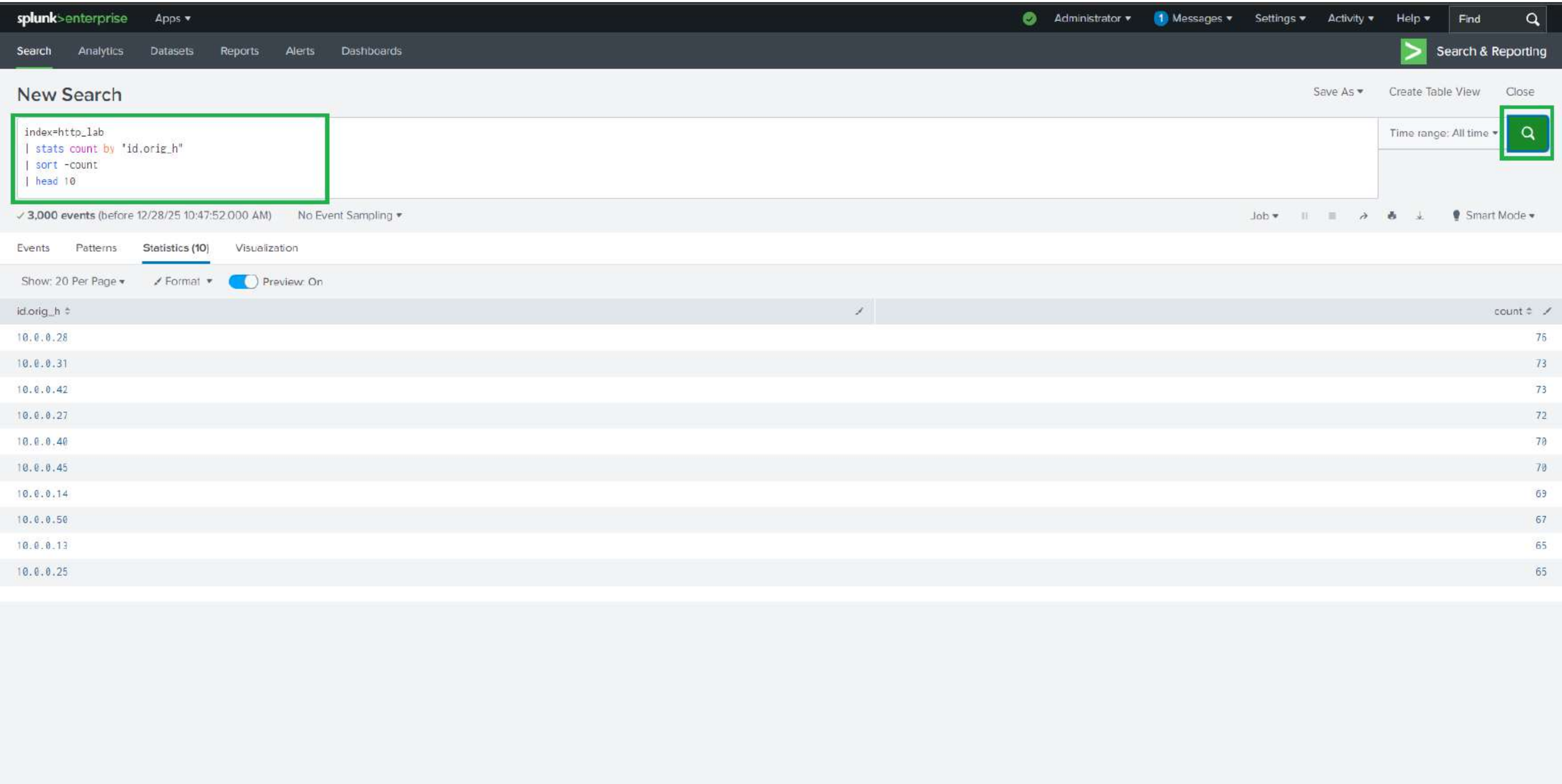
Start Searching — Search your data now or see examples and tutorials.

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

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

Download Apps — Apps help you do more with your data. Learn more.

Build Dashboards — Visualize your searches. Learn more.

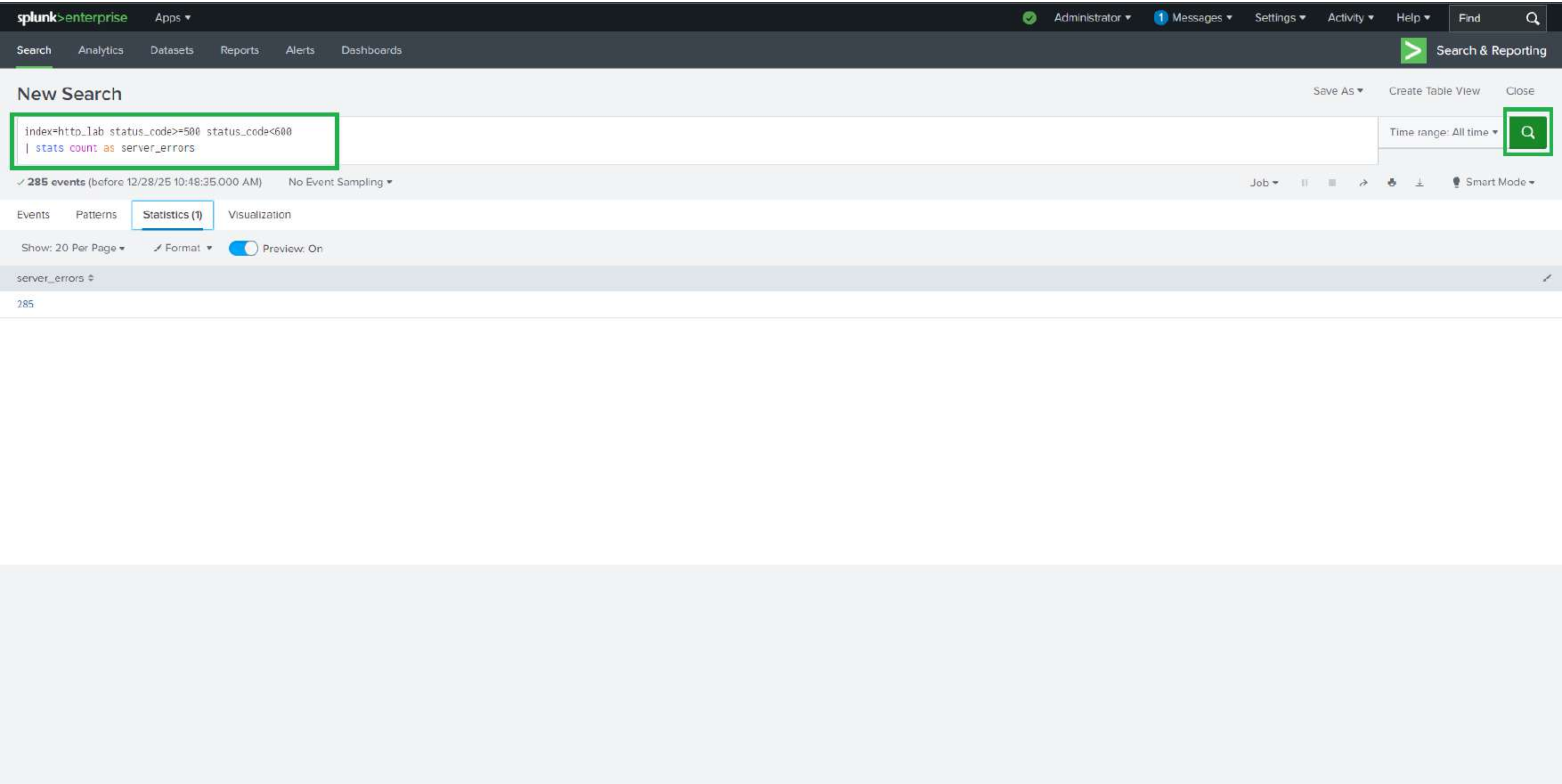


New Search

```
index=http_lab
| stats count by "id.orig_h"
| sort -count
| head 10
```

✓ 3,000 events (before 12/28/25 10:47:52.000 AM)

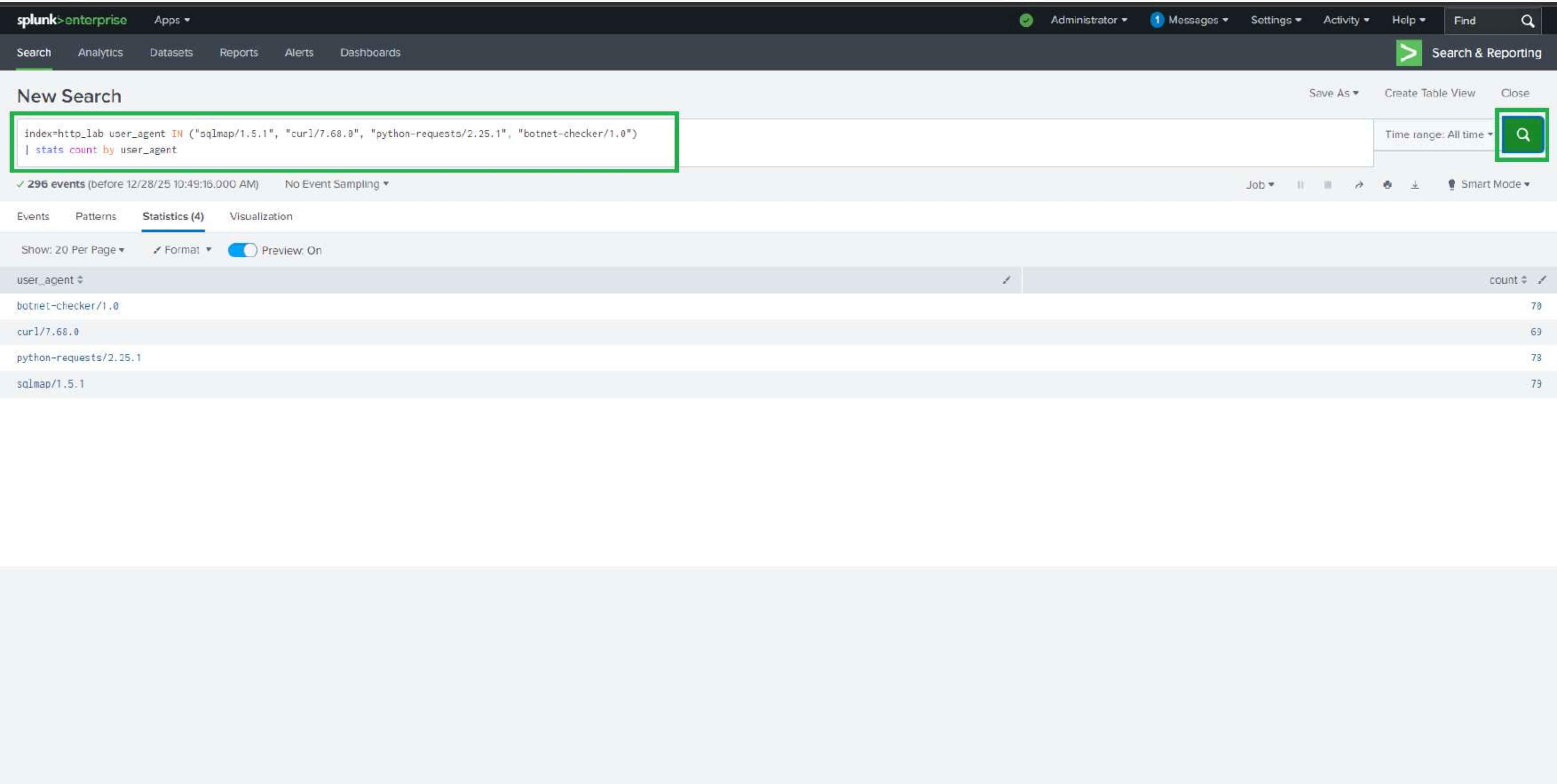
id.orig_h	count
10.0.0.28	76
10.0.0.31	73
10.0.0.42	73
10.0.0.27	72
10.0.0.40	70
10.0.0.45	70
10.0.0.14	69
10.0.0.50	67
10.0.0.13	65
10.0.0.25	65



```
index=http_lab status_code>=500 status_code<600
| stats count as server_errors
```

✓ 285 events (before 12/28/25 10:48:35.000 AM) No Event Sampling ▾

server_errors
285

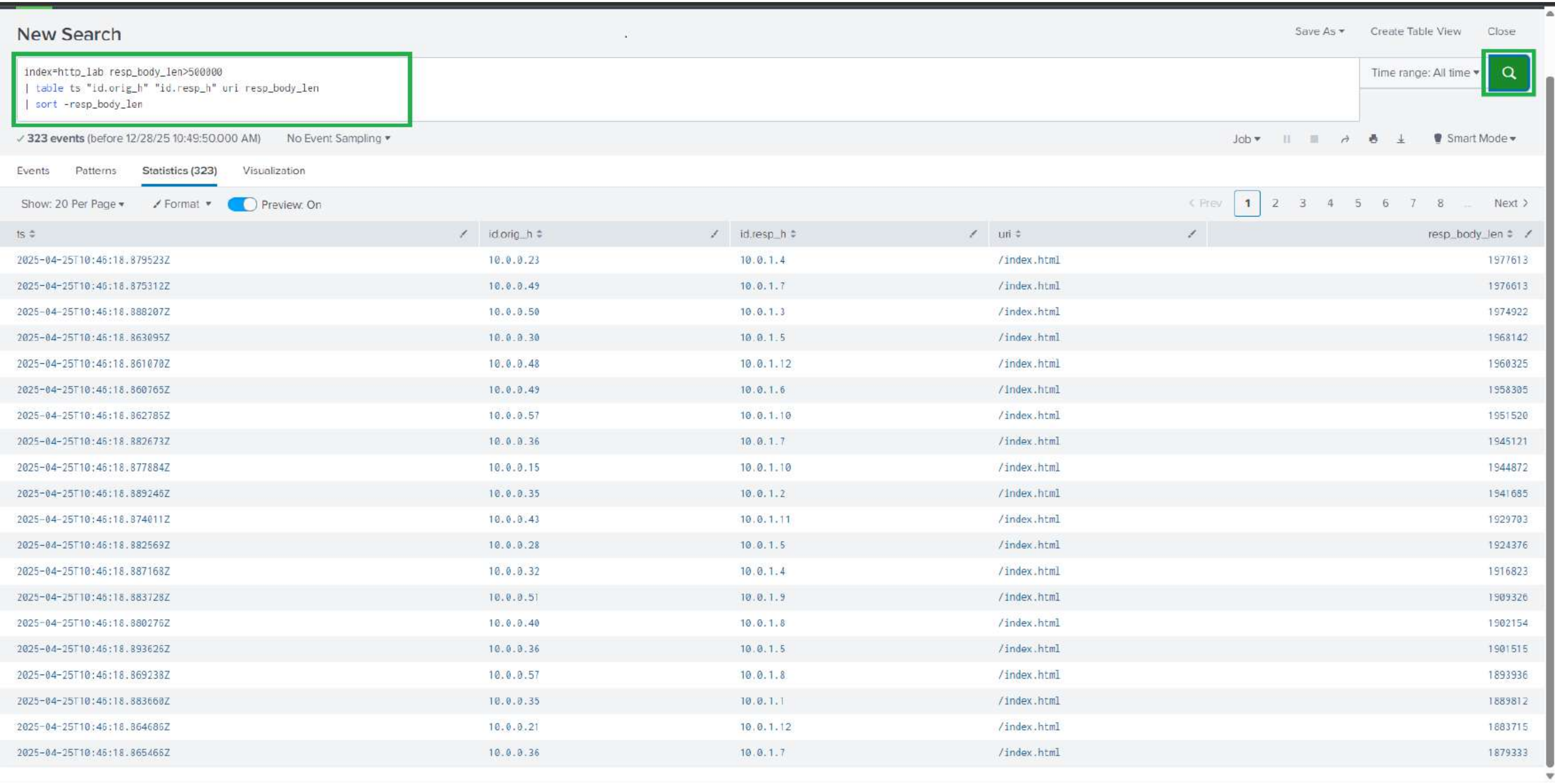


New Search

```
index=http_lab user_agent IN ("sqlmap/1.5.1", "curl/7.68.0", "python-requests/2.25.1", "botnet-checker/1.0")
| stats count by user_agent
```

✓ 296 events (before 12/28/25 10:49:16.000 AM)   No Event Sampling ▾

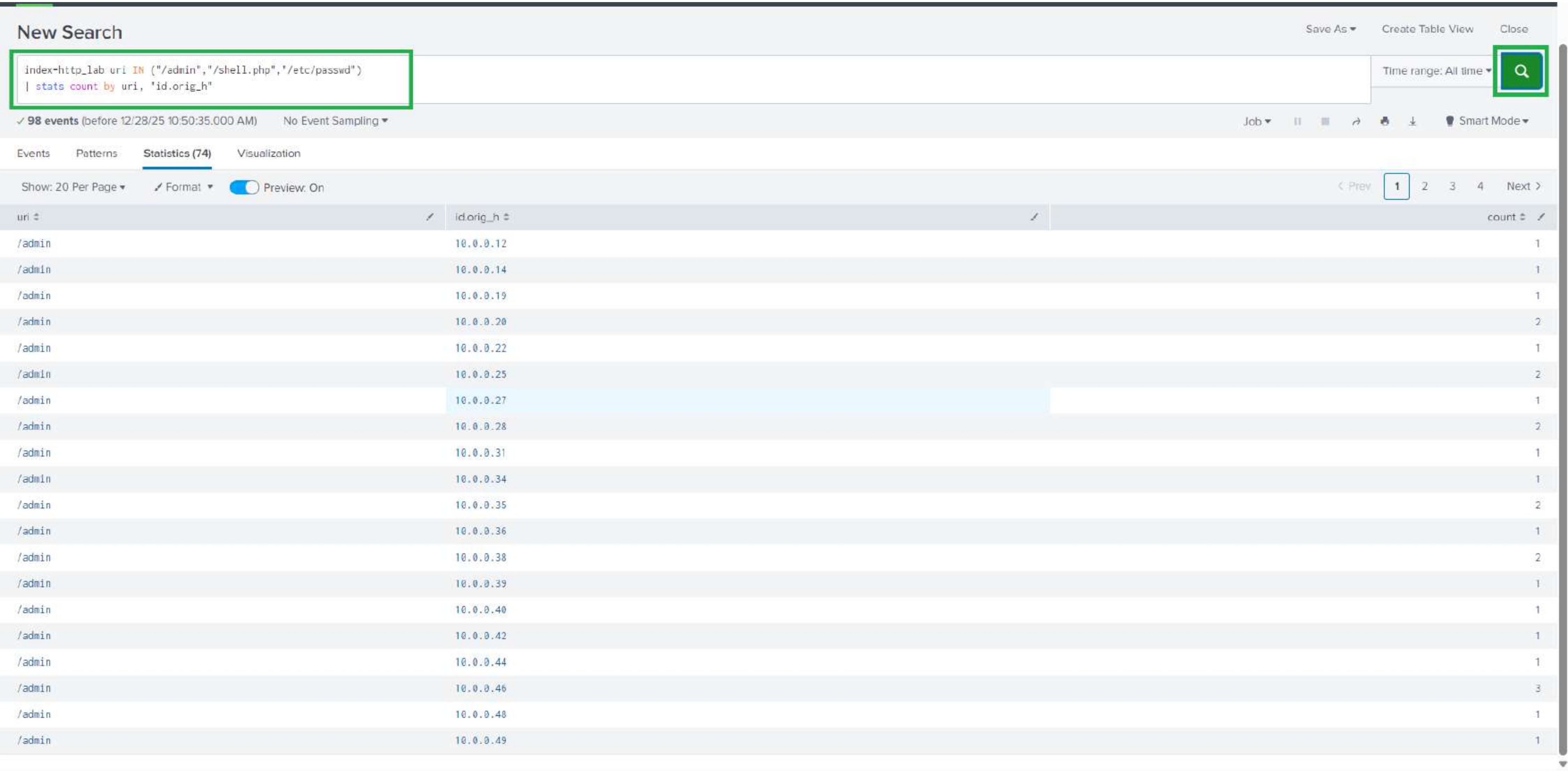
user_agent	count
botnet-checker/1.0	70
curl/7.68.0	69
python-requests/2.25.1	78
sqlmap/1.5.1	79



```
index=http_lab resp_body_len>500000
| table ts "id.orig_h" "id.resp_h" uri resp_body_len
| sort -resp_body_len
```

✓ **323 events** (before 12/28/25 10:49:50.000 AM) No Event Sampling ▾

ts	id.orig_h	id.resp_h	uri	resp_body_len
2025-04-25T10:46:18.879523Z	10.0.0.23	10.0.1.4	/index.html	1977613
2025-04-25T10:46:18.875312Z	10.0.0.49	10.0.1.7	/index.html	1976613
2025-04-25T10:46:18.888207Z	10.0.0.50	10.0.1.3	/index.html	1974922
2025-04-25T10:46:18.863095Z	10.0.0.30	10.0.1.5	/index.html	1968142
2025-04-25T10:46:18.861070Z	10.0.0.48	10.0.1.12	/index.html	1960325
2025-04-25T10:46:18.860765Z	10.0.0.49	10.0.1.6	/index.html	1958305
2025-04-25T10:46:18.862785Z	10.0.0.57	10.0.1.10	/index.html	1951520
2025-04-25T10:46:18.882673Z	10.0.0.36	10.0.1.7	/index.html	1945121
2025-04-25T10:46:18.877884Z	10.0.0.15	10.0.1.10	/index.html	1944872
2025-04-25T10:46:18.889246Z	10.0.0.35	10.0.1.2	/index.html	1941685
2025-04-25T10:46:18.874011Z	10.0.0.43	10.0.1.11	/index.html	1929703
2025-04-25T10:46:18.882569Z	10.0.0.28	10.0.1.5	/index.html	1924376
2025-04-25T10:46:18.887168Z	10.0.0.32	10.0.1.4	/index.html	1916823
2025-04-25T10:46:18.883728Z	10.0.0.51	10.0.1.9	/index.html	1909326
2025-04-25T10:46:18.880276Z	10.0.0.40	10.0.1.8	/index.html	1902154
2025-04-25T10:46:18.893626Z	10.0.0.36	10.0.1.5	/index.html	1901515
2025-04-25T10:46:18.869238Z	10.0.0.57	10.0.1.8	/index.html	1893936
2025-04-25T10:46:18.883660Z	10.0.0.35	10.0.1.1	/index.html	1889812
2025-04-25T10:46:18.864686Z	10.0.0.21	10.0.1.12	/index.html	1883715
2025-04-25T10:46:18.865466Z	10.0.0.36	10.0.1.7	/index.html	1879333



New Search

```
index=http_lab uri IN ("/admin","/shell.php","/etc/passwd")
| stats count by uri, 'id.orig_h"
```

✓ **98 events** (before 12/28/25 10:50:35.000 AM) No Event Sampling ▾

uri	id.orig_h	count
/admin	10.0.0.12	1
/admin	10.0.0.14	1
/admin	10.0.0.19	1
/admin	10.0.0.20	2
/admin	10.0.0.22	1
/admin	10.0.0.25	2
/admin	10.0.0.27	1
/admin	10.0.0.28	2
/admin	10.0.0.31	1
/admin	10.0.0.34	1
/admin	10.0.0.35	2
/admin	10.0.0.36	1
/admin	10.0.0.38	2
/admin	10.0.0.39	1
/admin	10.0.0.40	1
/admin	10.0.0.42	1
/admin	10.0.0.44	1
/admin	10.0.0.46	3
/admin	10.0.0.48	1
/admin	10.0.0.49	1