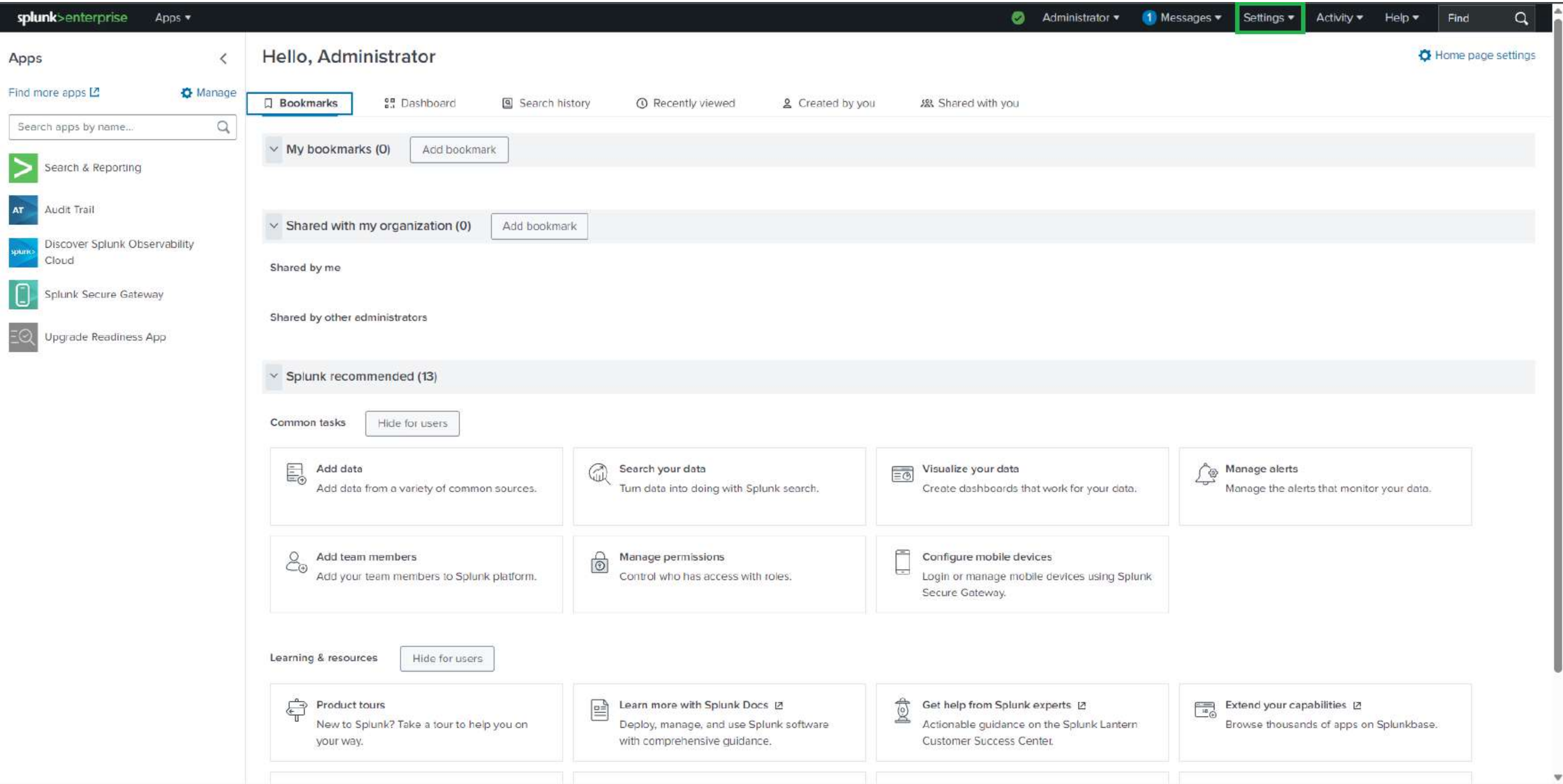


Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks

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.

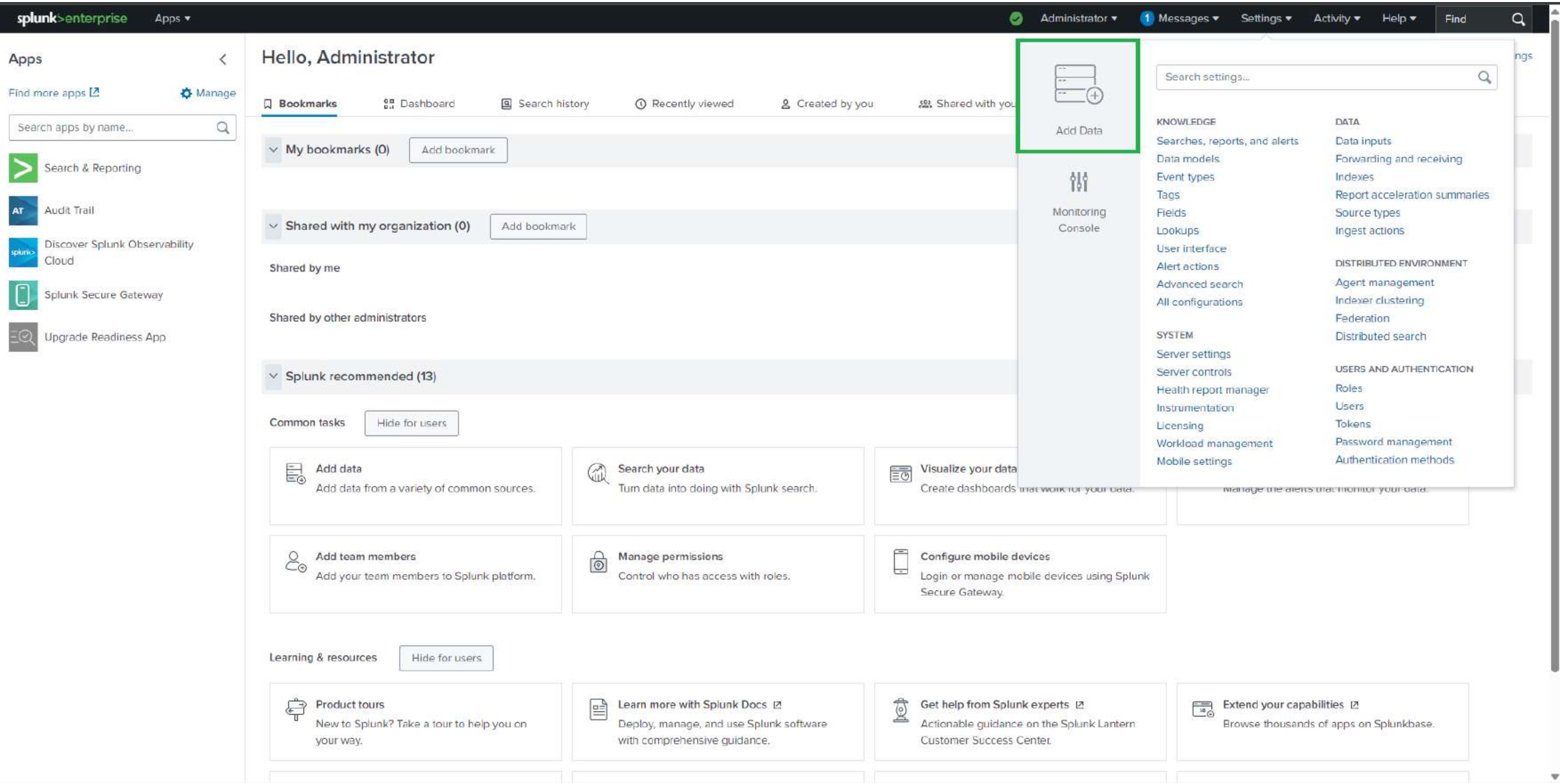
Learning & resources

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.



Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks

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.

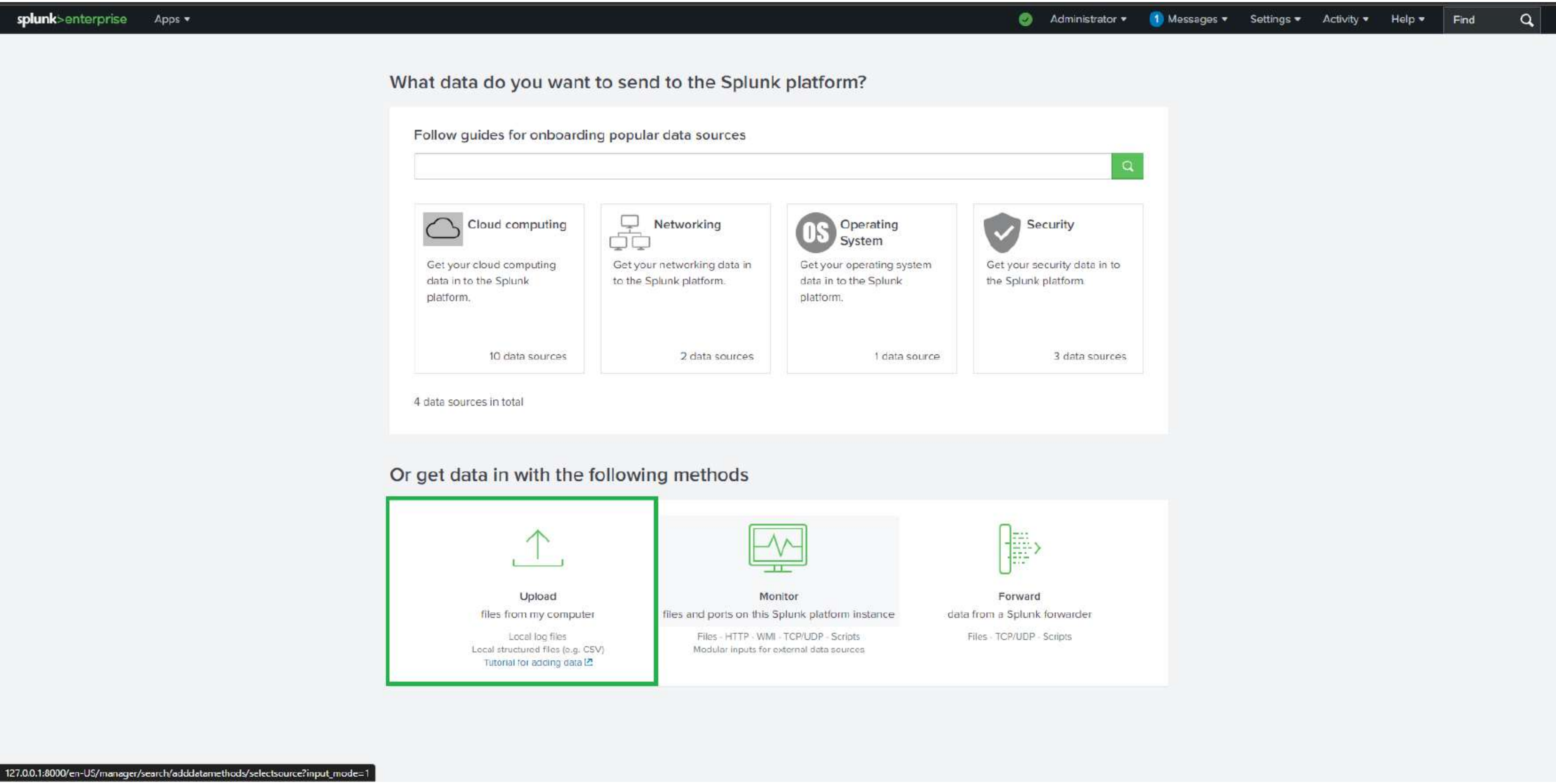
Learning & resources

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.



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

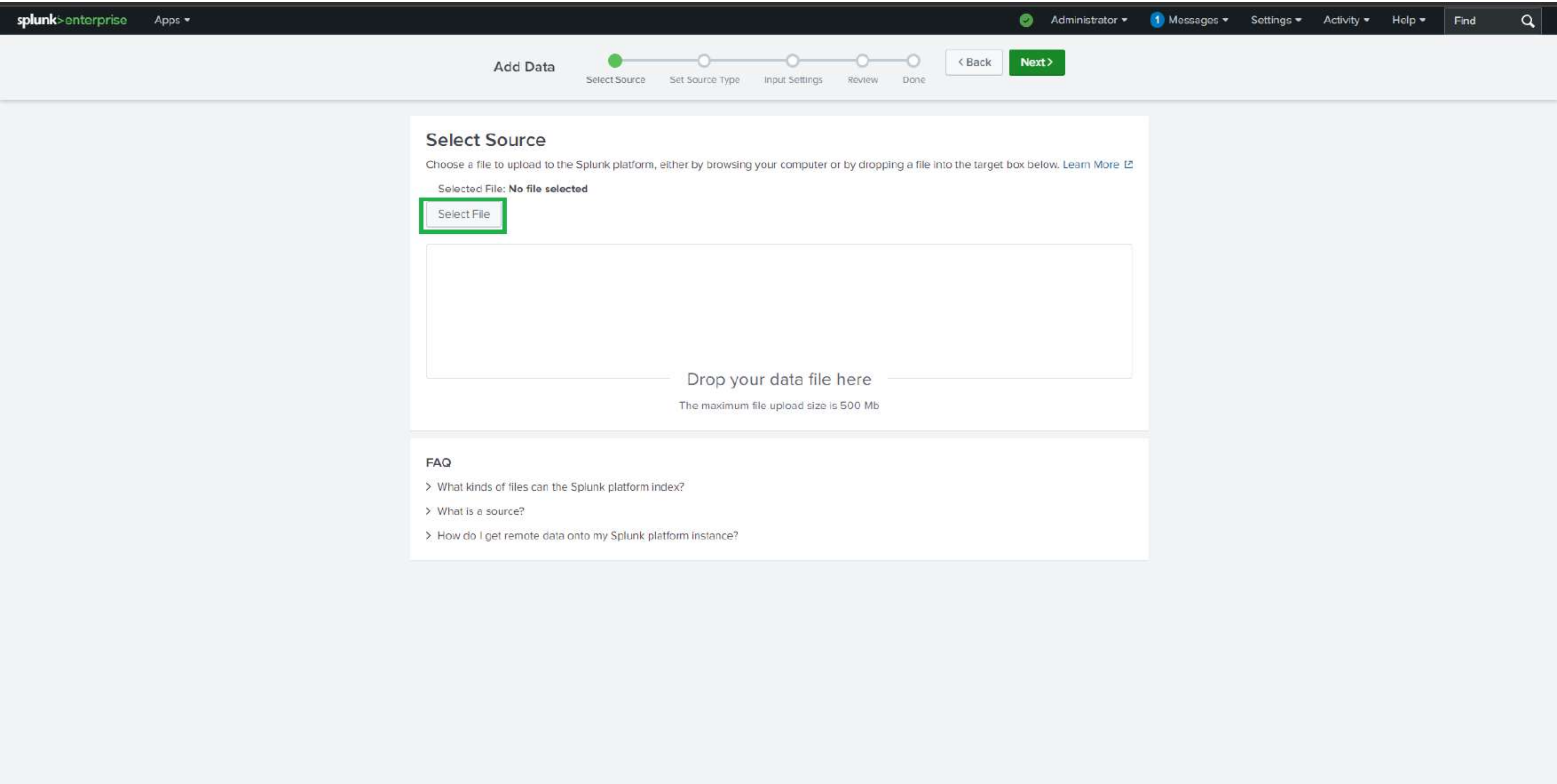
Or get data in with the following methods

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/selectsource?input_mode=1



Select Source

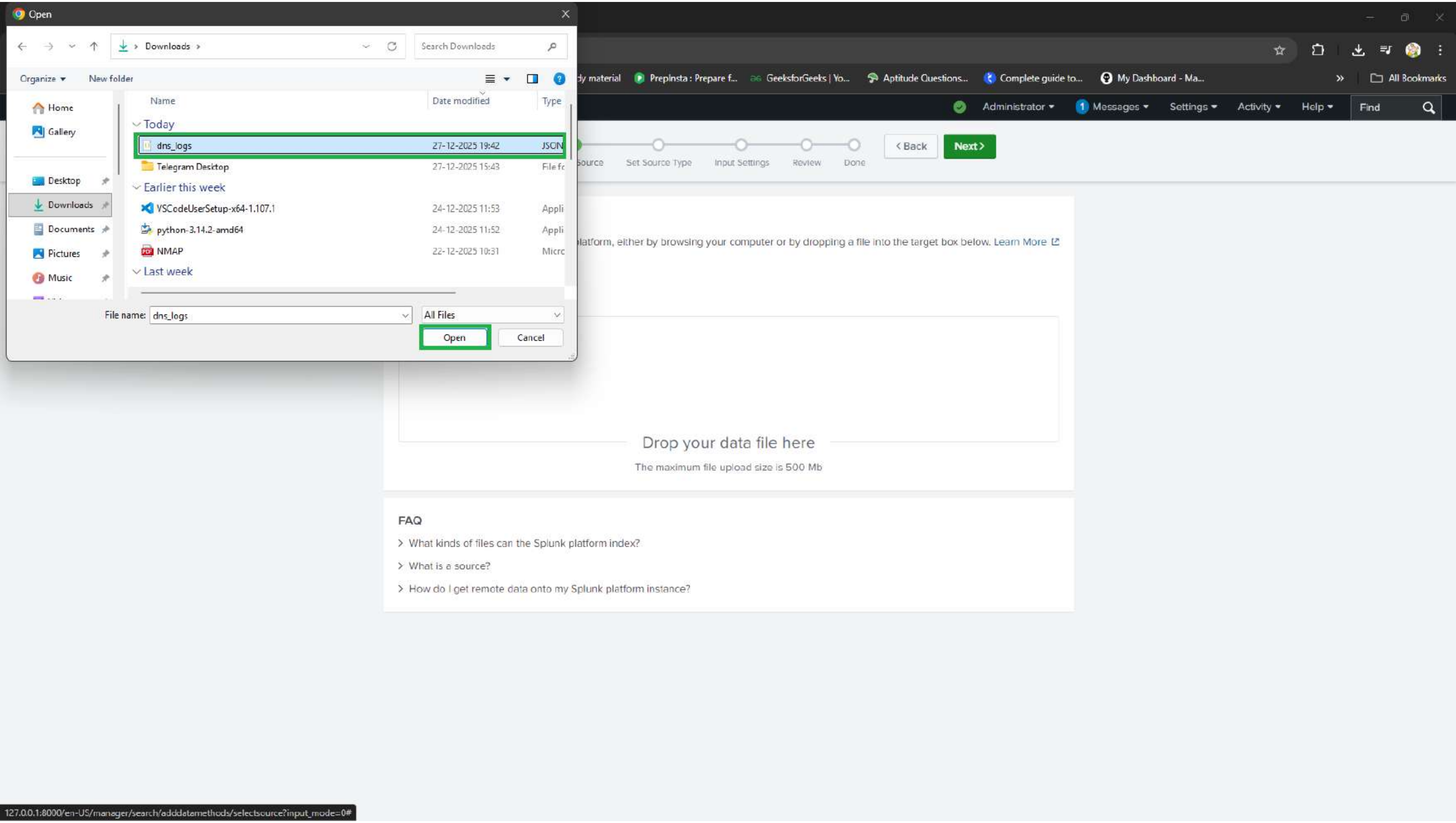
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **No file selected**

Drop your data file here

The maximum file upload size is 500 Mb

- 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
Today		
dns_logs	27-12-2025 19:42	JSON
Telegram Desktop	27-12-2025 15:43	File fc
Earlier this week		
VSCodeUserSetup-x64-1.107.1	24-12-2025 11:53	Appli
python-3.14.2-amd64	24-12-2025 11:52	Appli
NMAP	22-12-2025 10:31	Micrc
Last week		

File name: dns_logs

All Files

Open   Cancel

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

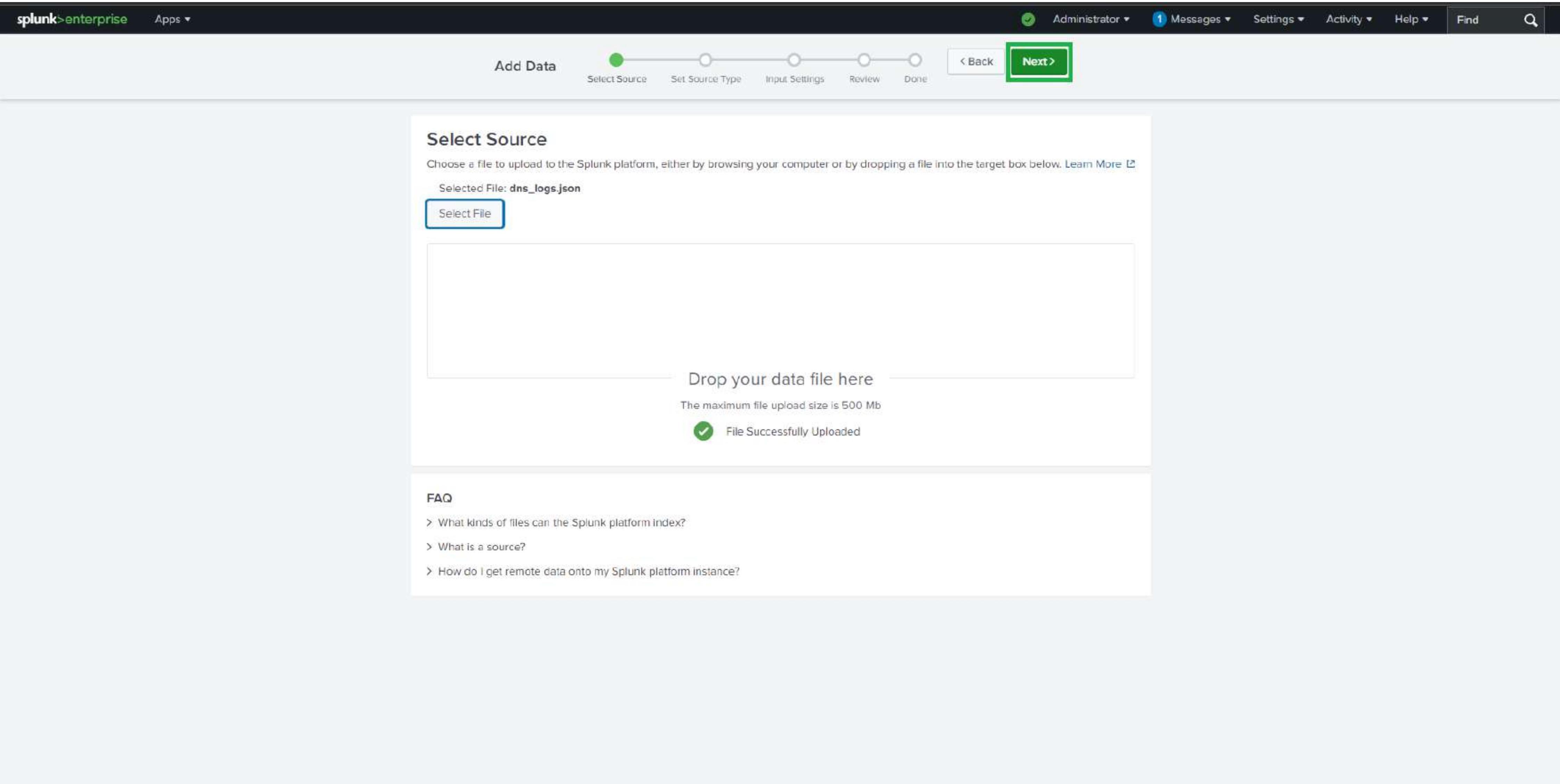
FAQ

> 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: **dns_logs.json**

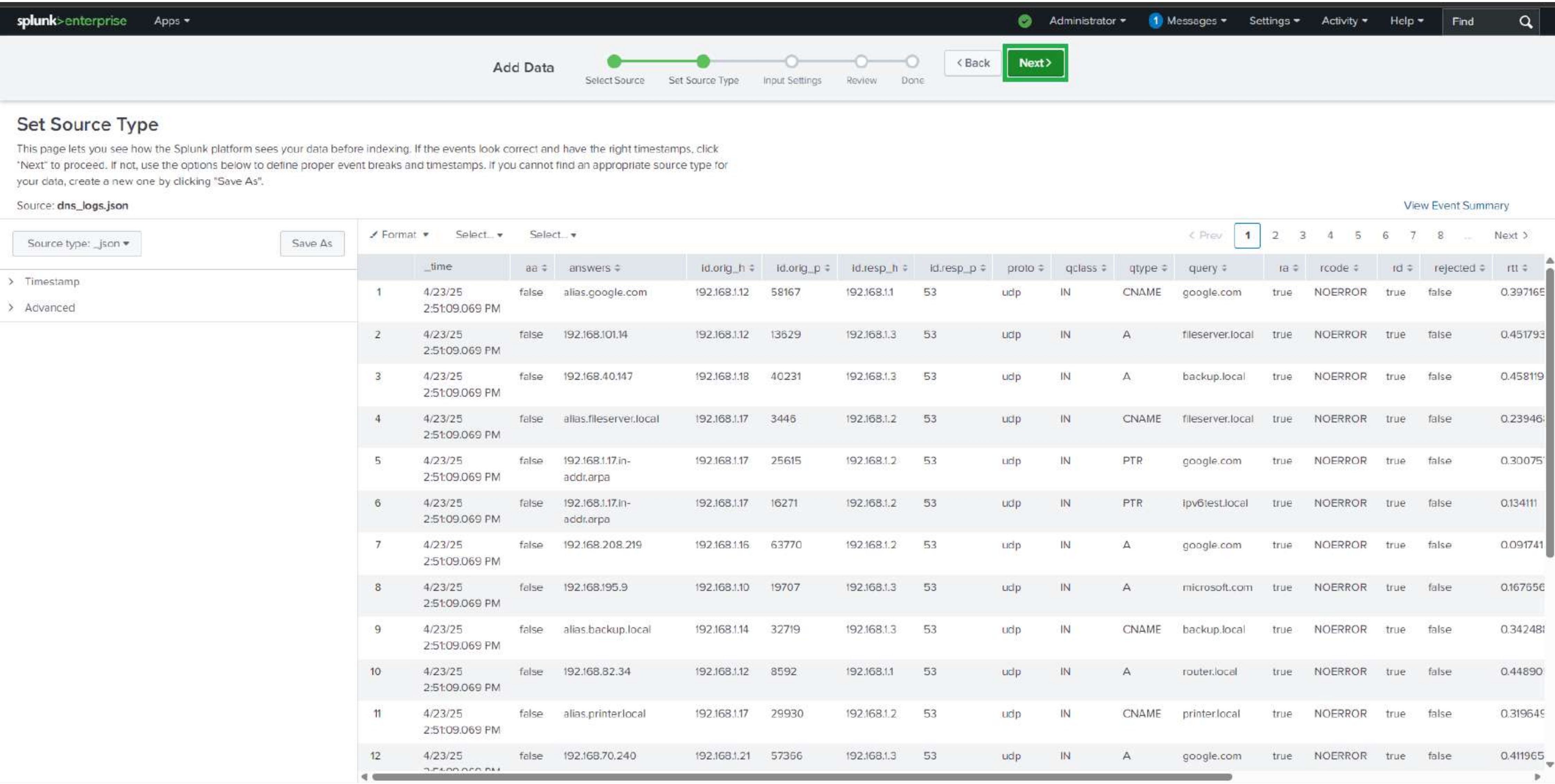
Drop your data file here

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?

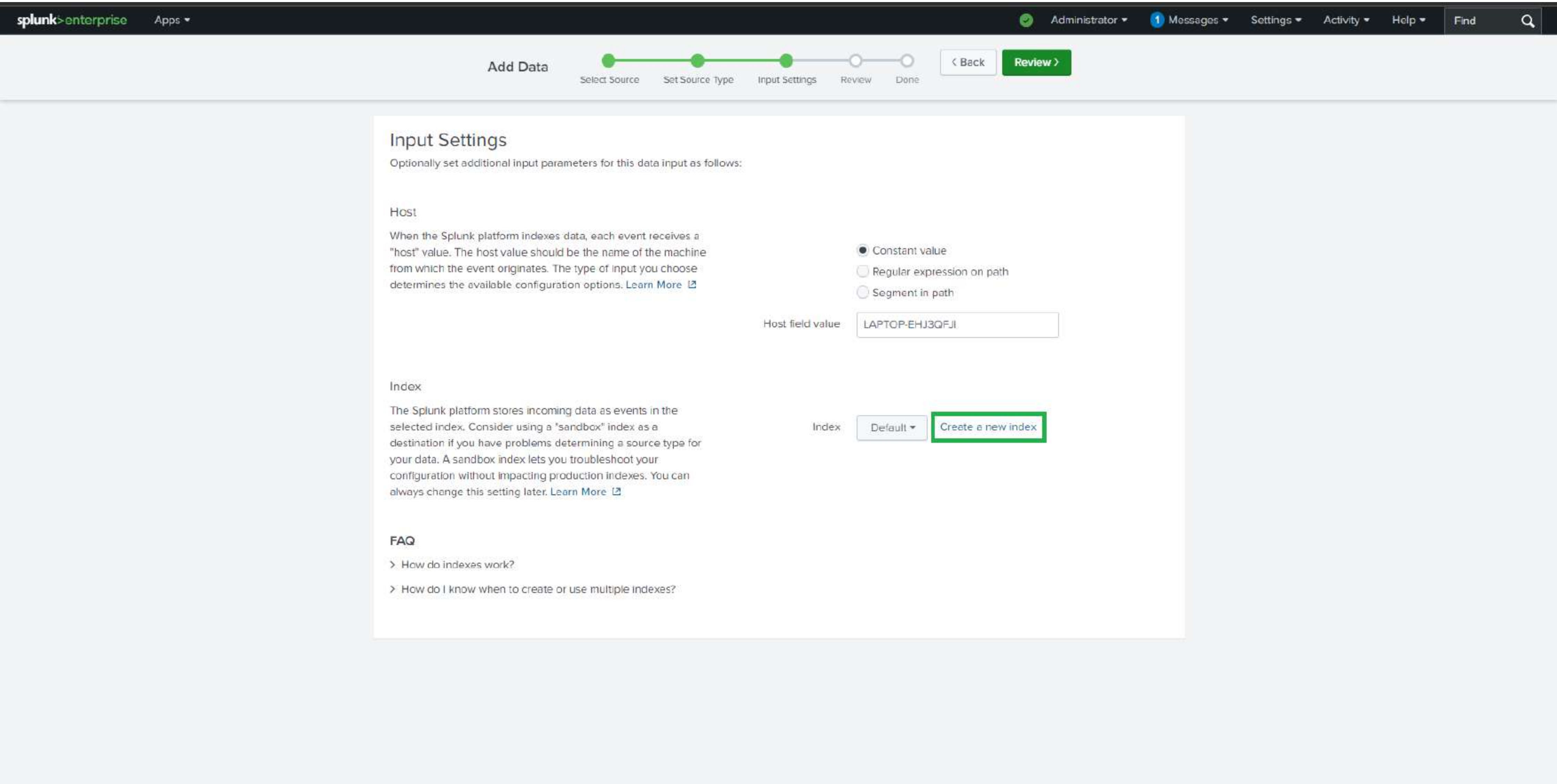


Set Source Type

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: **dns_logs.json**

	_time	aa	answers	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	qclass	qtype	query	ra	rcode	rd	rejected	rtt
1	4/23/25 2:51:09.069 PM	false	alias.google.com	192.168.1.12	58167	192.168.1.1	53	udp	IN	CNAME	google.com	true	NOERROR	true	false	0.397165
2	4/23/25 2:51:09.069 PM	false	192.168.101.14	192.168.1.12	13629	192.168.1.3	53	udp	IN	A	fileserver.local	true	NOERROR	true	false	0.451793
3	4/23/25 2:51:09.069 PM	false	192.168.40.147	192.168.1.18	40231	192.168.1.3	53	udp	IN	A	backup.local	true	NOERROR	true	false	0.458119
4	4/23/25 2:51:09.069 PM	false	alias.fileserver.local	192.168.1.17	3446	192.168.1.2	53	udp	IN	CNAME	fileserver.local	true	NOERROR	true	false	0.23946
5	4/23/25 2:51:09.069 PM	false	192.168.1.17.in-addr.arpa	192.168.1.17	25615	192.168.1.2	53	udp	IN	PTR	google.com	true	NOERROR	true	false	0.30075
6	4/23/25 2:51:09.069 PM	false	192.168.1.17.in-addr.arpa	192.168.1.17	16271	192.168.1.2	53	udp	IN	PTR	ipv6test.local	true	NOERROR	true	false	0.134111
7	4/23/25 2:51:09.069 PM	false	192.168.208.219	192.168.1.16	63770	192.168.1.2	53	udp	IN	A	google.com	true	NOERROR	true	false	0.091741
8	4/23/25 2:51:09.069 PM	false	192.168.195.9	192.168.1.10	19707	192.168.1.3	53	udp	IN	A	microsoft.com	true	NOERROR	true	false	0.167656
9	4/23/25 2:51:09.069 PM	false	alias.backup.local	192.168.1.14	32719	192.168.1.3	53	udp	IN	CNAME	backup.local	true	NOERROR	true	false	0.34248
10	4/23/25 2:51:09.069 PM	false	192.168.82.34	192.168.1.12	8592	192.168.1.1	53	udp	IN	A	router.local	true	NOERROR	true	false	0.44890
11	4/23/25 2:51:09.069 PM	false	alias.printer.local	192.168.1.17	29930	192.168.1.2	53	udp	IN	CNAME	printer.local	true	NOERROR	true	false	0.31964
12	4/23/25	false	192.168.70.240	192.168.1.21	57366	192.168.1.3	53	udp	IN	A	google.com	true	NOERROR	true	false	0.411965



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

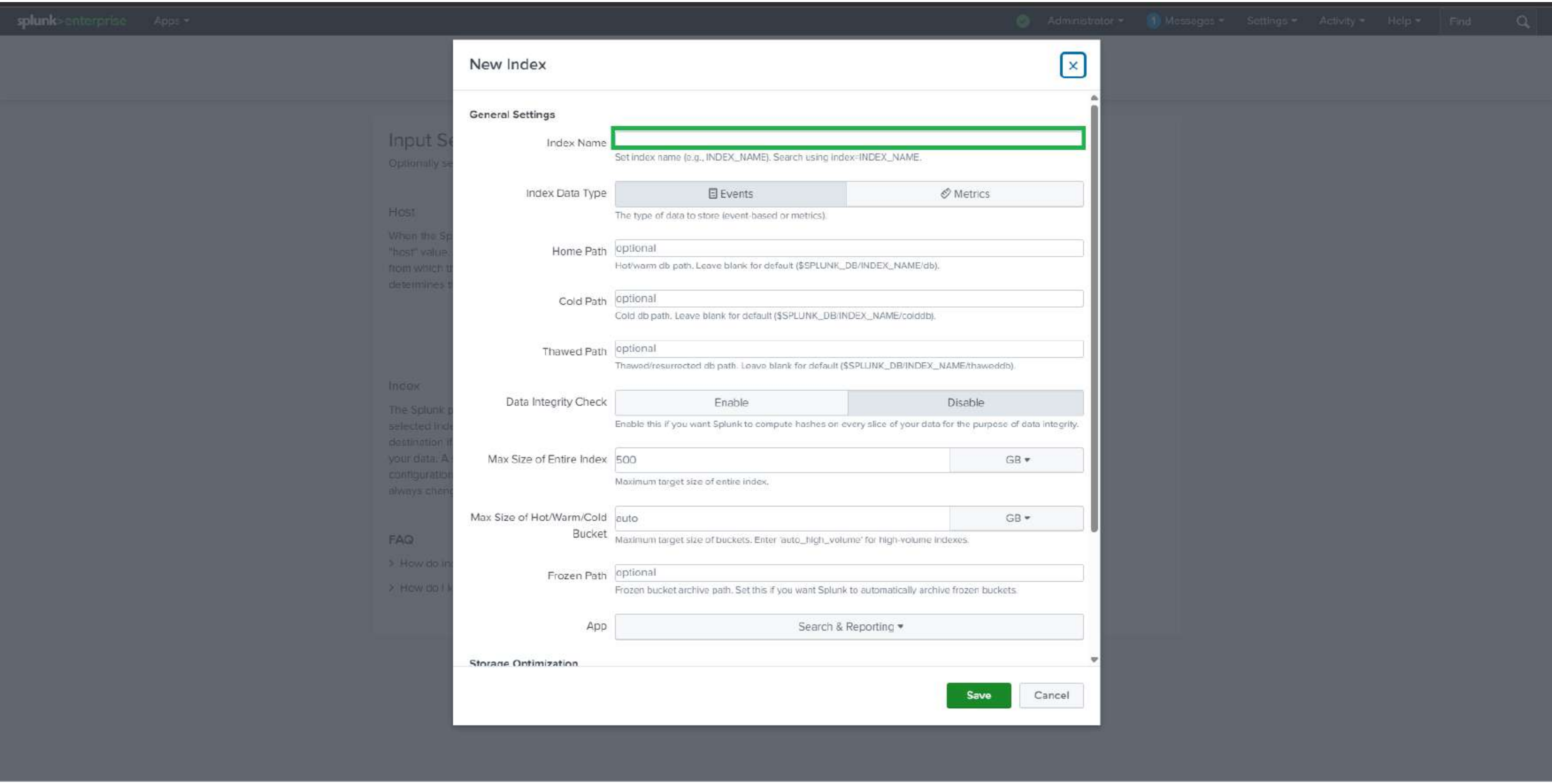
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change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

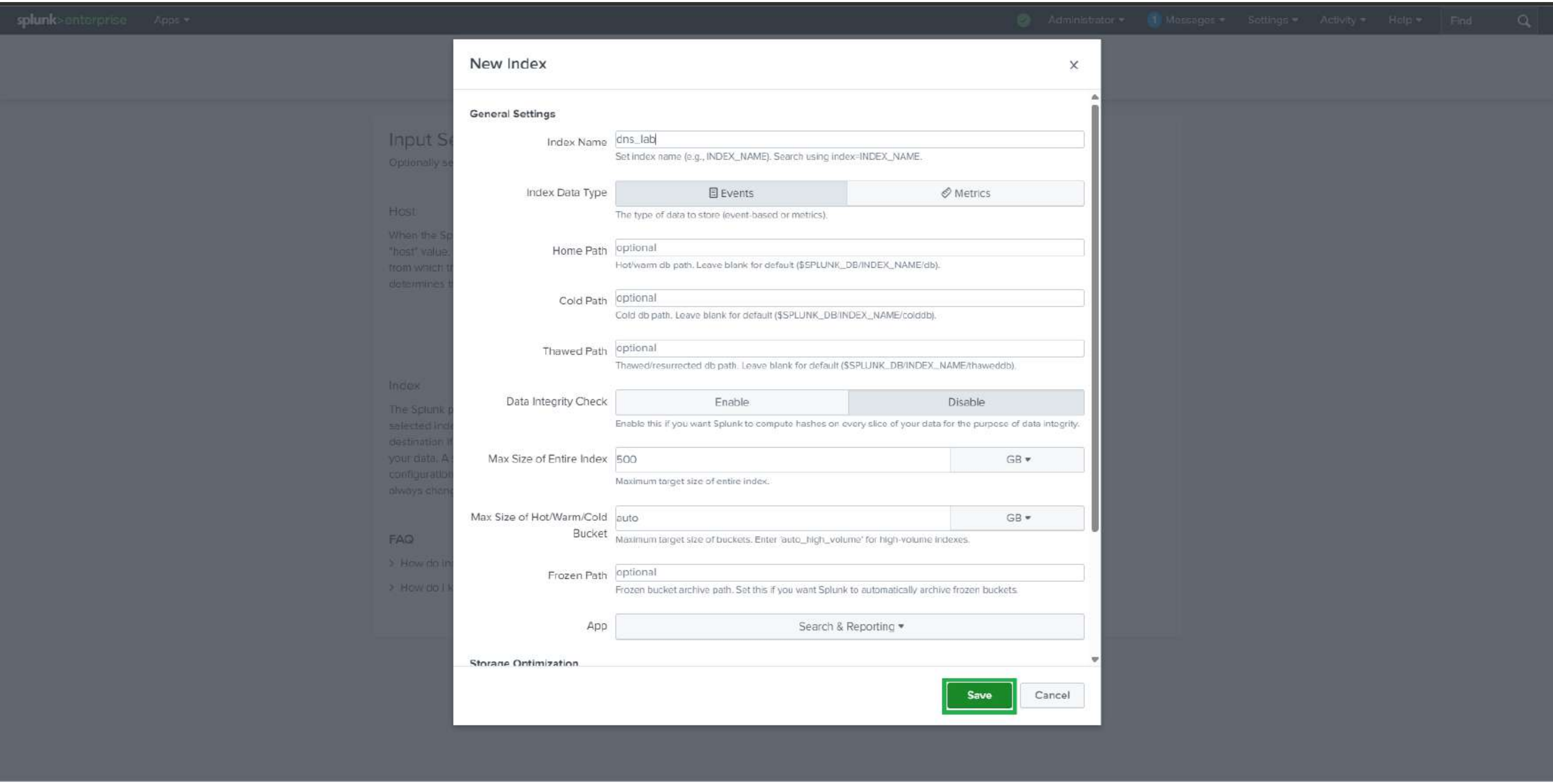
Max Size of Entire Index: 500 GB ▾
Maximum target size of entire index.

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: dns_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.

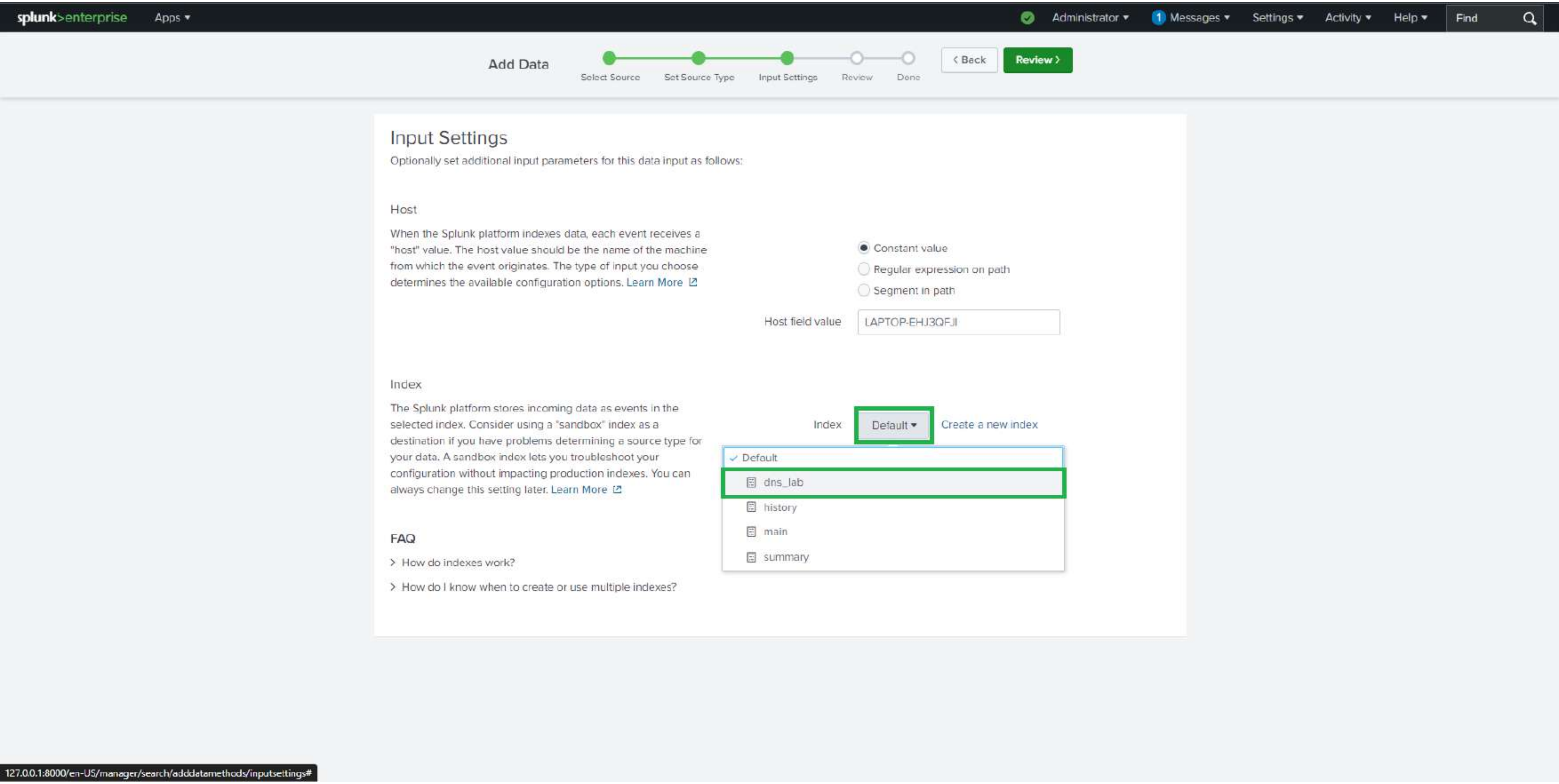
Max Size of Entire Index: 500 GB ▾
Maximum target size of entire index.

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

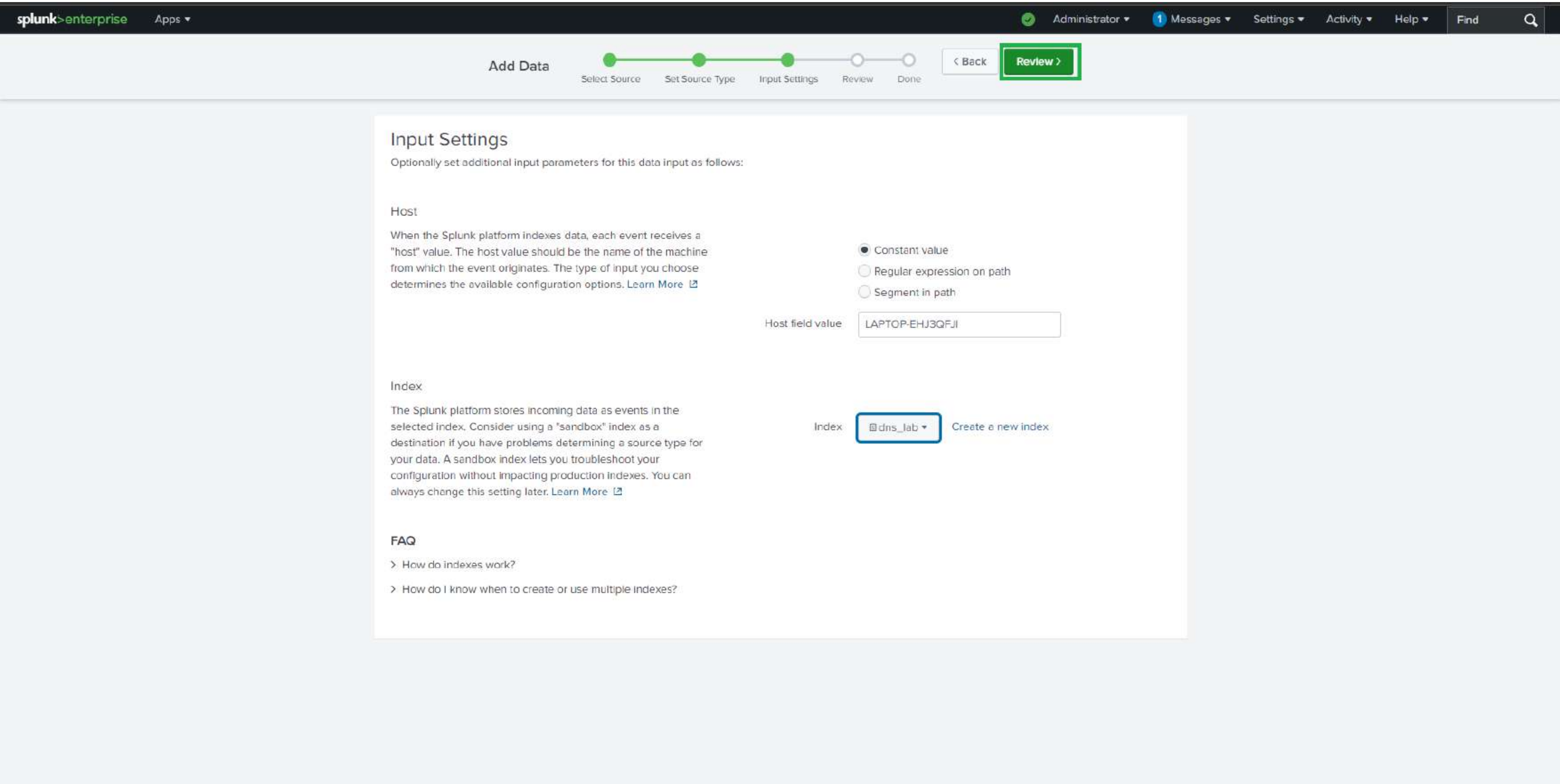
Index: Default ▾ Create a new index

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

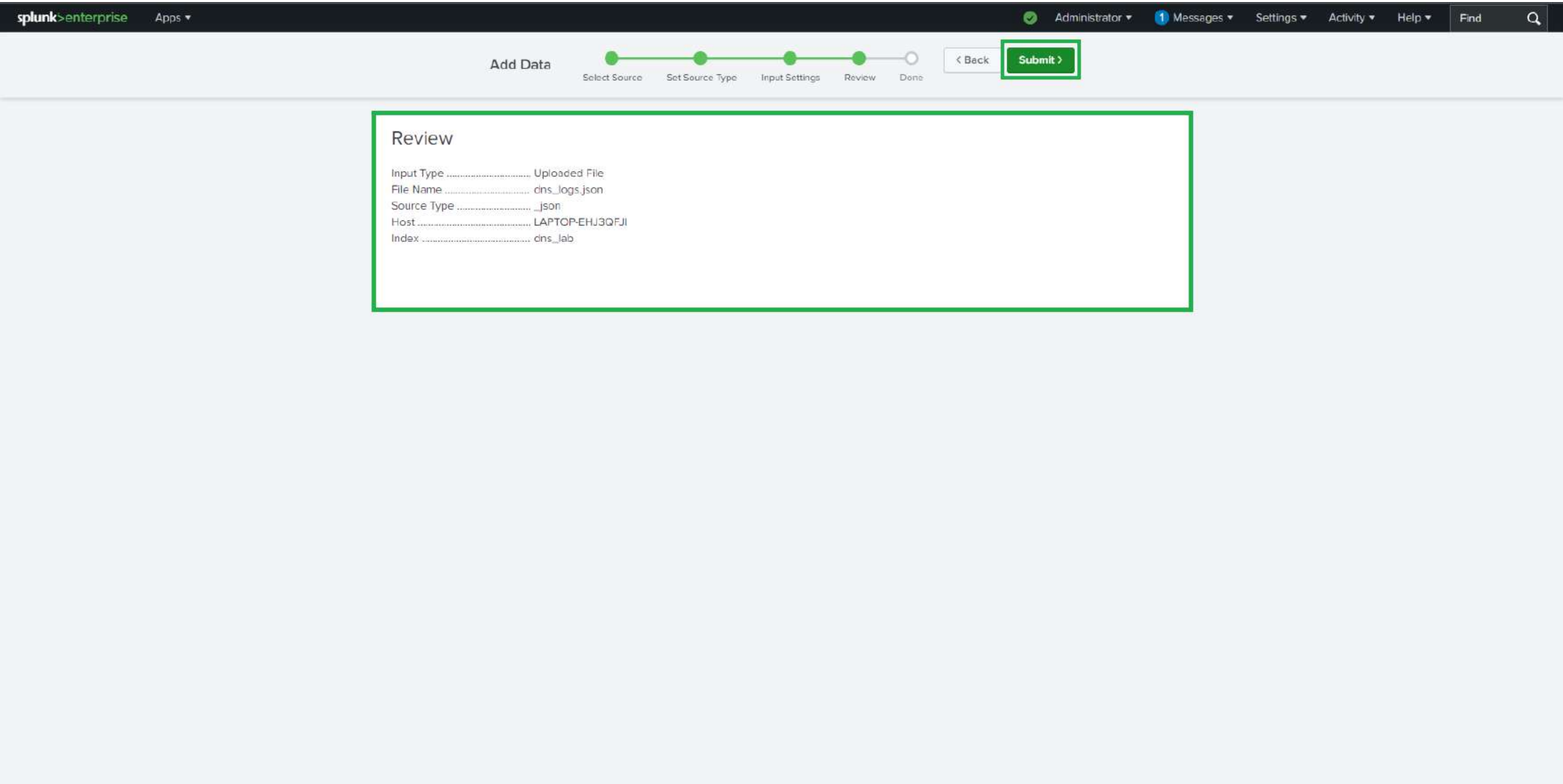
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change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

Index: dns_lab ▾ Create a new index

FAQ

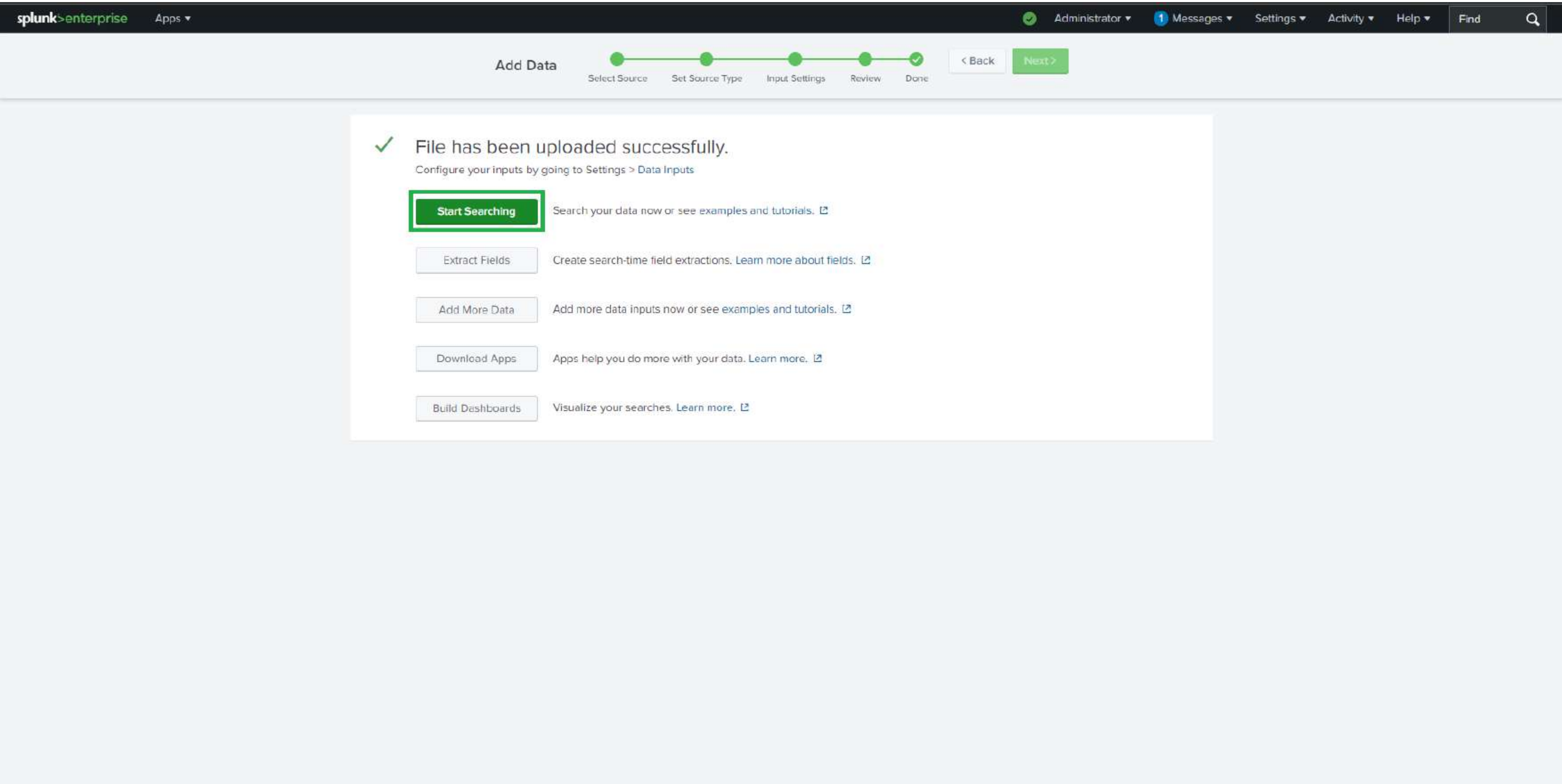
› How do indexes work?

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



Review

Input Type .... Uploaded File
File Name .... dns_logs.json
Source Type .... _json
Host LAPTOP-EHJ3QFJI
Index .... dns_lab



✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

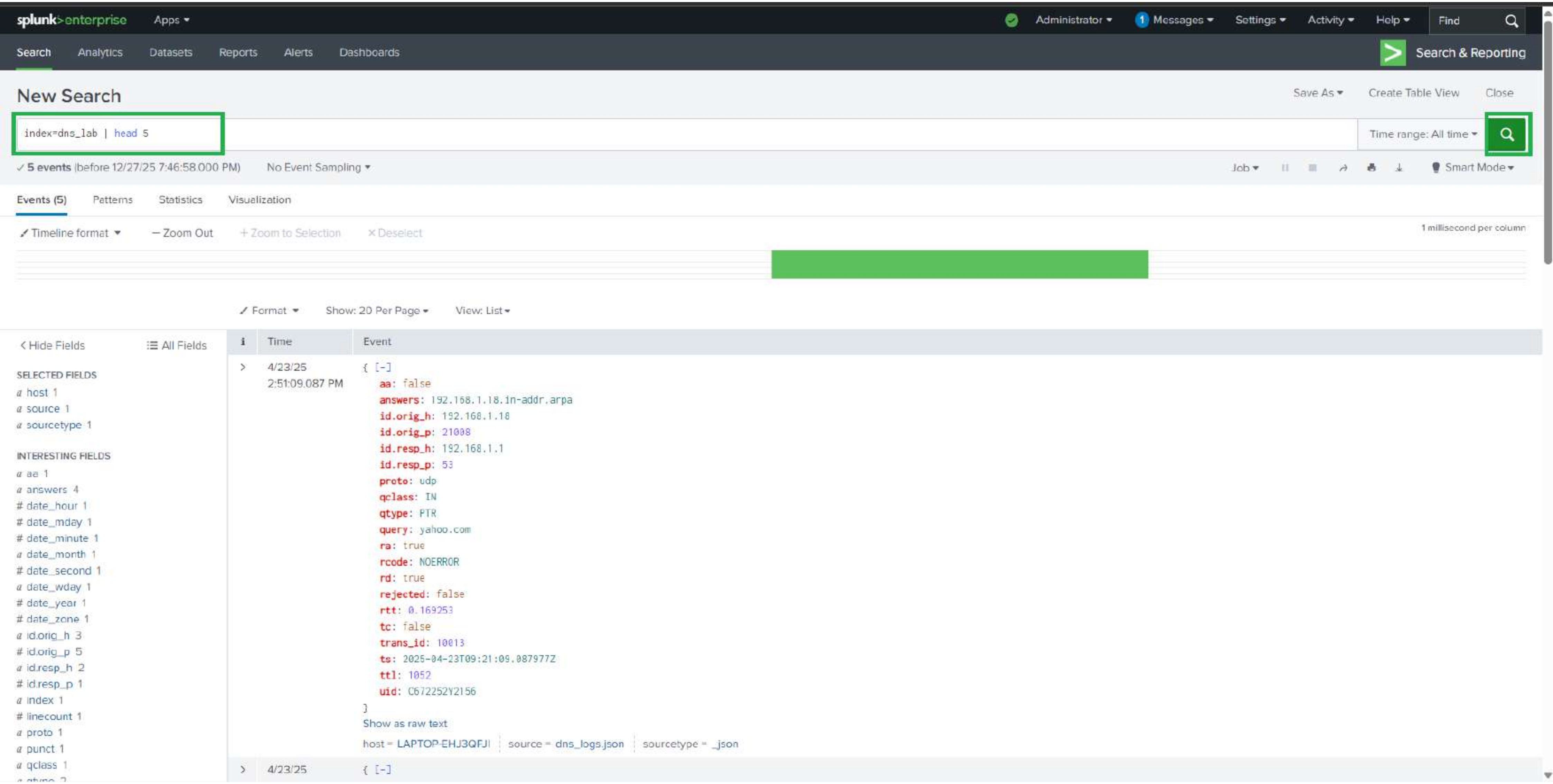
Search your data now or see examples and tutorials.

Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

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

Visualize your searches. Learn more.



New Search

```
index=dns_lab | head 5
```

Time range: All time

✓ 5 events (before 12/27/25 7:46:58.000 PM)   No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a aa 1
a answers 4
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
# date_zone 1
a id.orig_h 3
# id.orig_p 5
a id.resp_h 2
# id.resp_p 1
a index 1
# linecount 1
a proto 1
a punct 1
a qclass 1

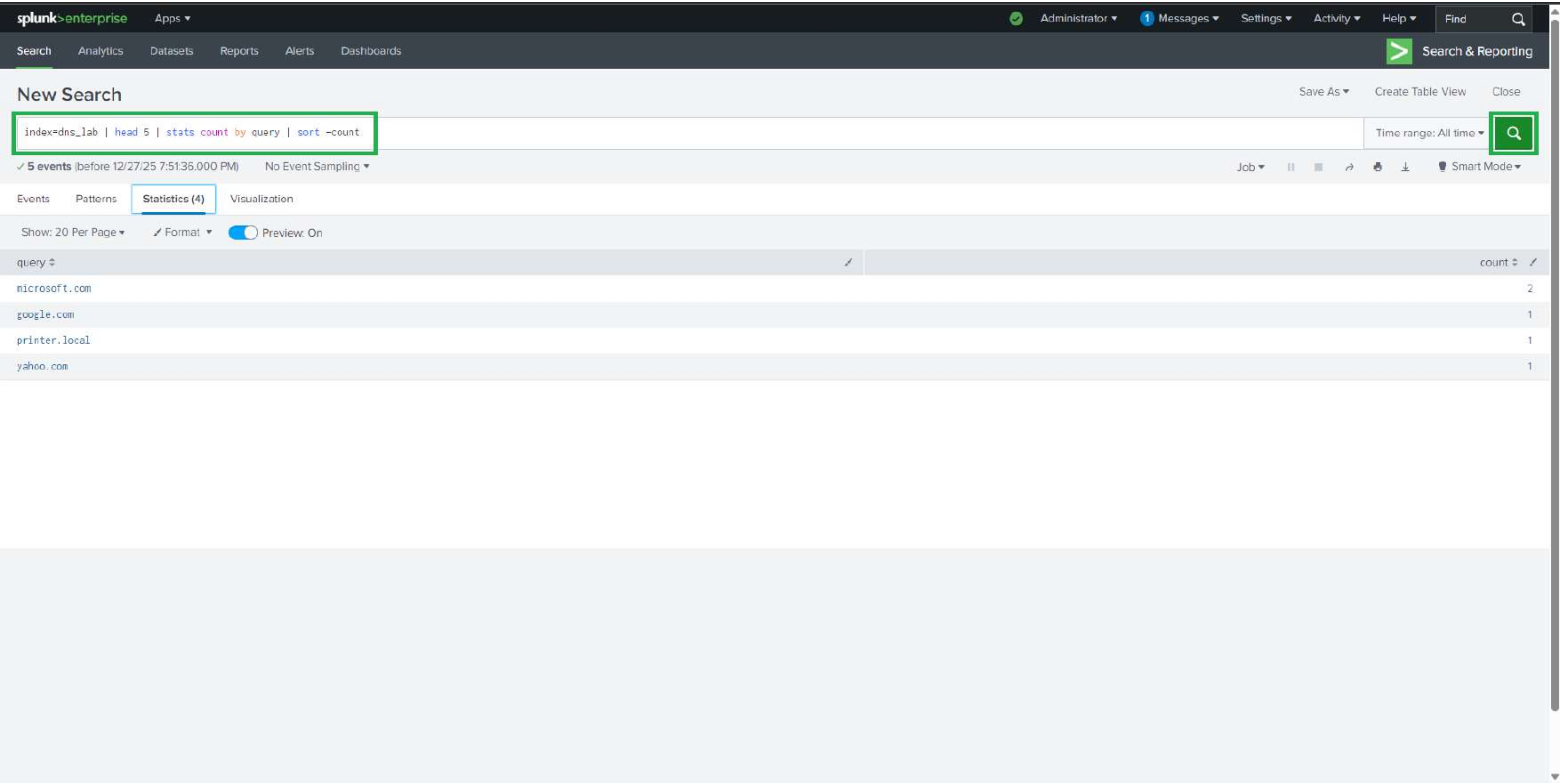
4/23/25
2:51:09.087 PM

```
{ [-]
  aa: false
  answers: 192.168.1.18.in-addr.arpa
  id.orig_h: 192.168.1.18
  id.orig_p: 21008
  id.resp_h: 192.168.1.1
  id.resp_p: 53
  proto: udp
  qclass: IN
  qtype: PTR
  query: yahoo.com
  ra: true
  rcode: NOERROR
  rd: true
  rejected: false
  rtt: 0.169253
  tc: false
  trans_id: 10013
  ts: 2025-04-23T09:21:09.087977Z
  ttl: 1052
  uid: C672252Y2156
}
```

host = LAPTOP-EHJ3QFJI | source = dns_logs.json | sourcetype = _json

4/23/25

```
{ [-]
```

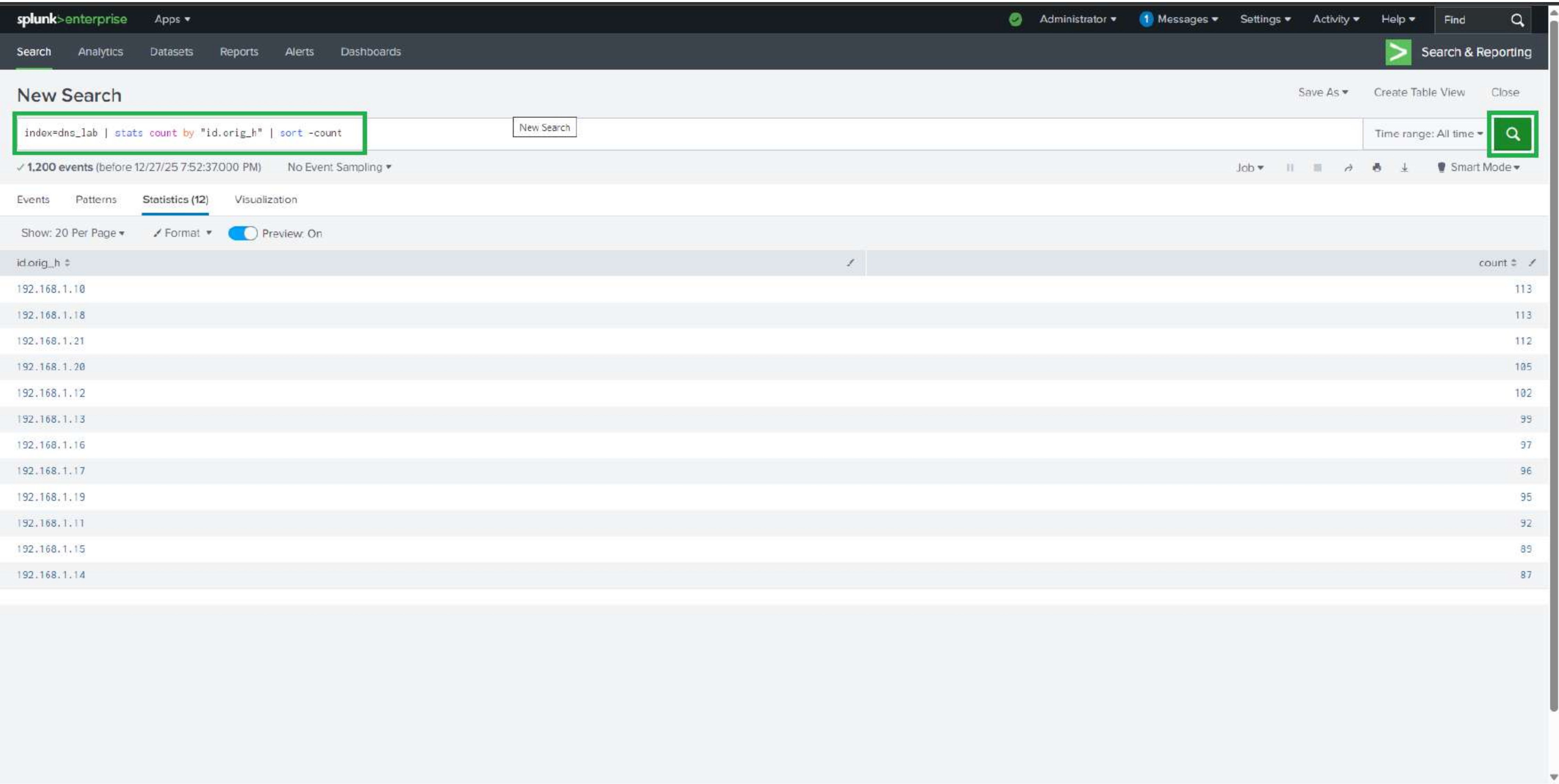


New Search

```
index=dns_lab | head 5 | stats count by query | sort -count
```

✓ 5 events (before 12/27/25 7:51:36.000 PM)

query	count
microsoft.com	2
google.com	1
printer.local	1
yahoo.com	1

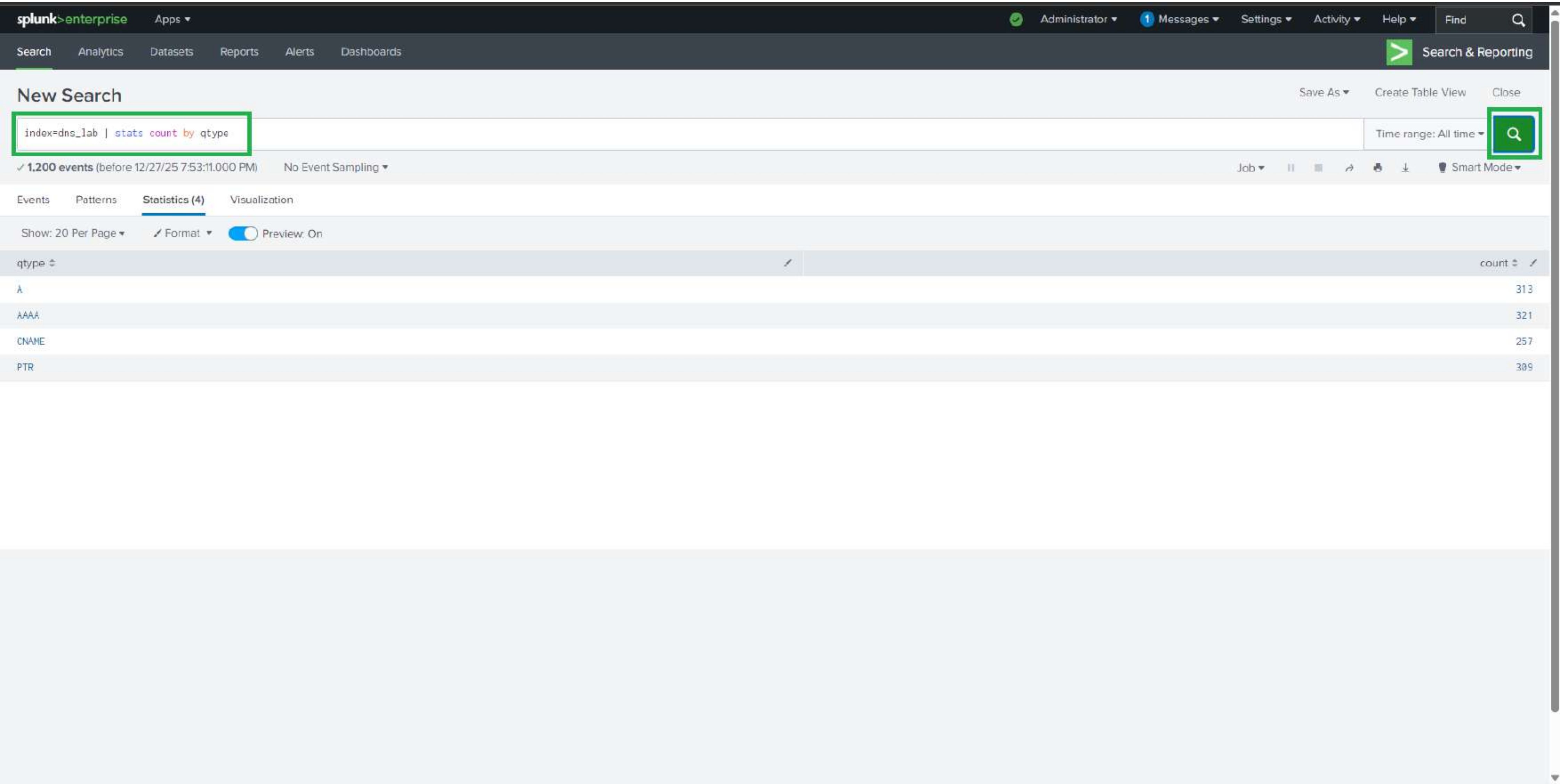


New Search

```
index=dns_lab | stats count by "id.orig_h" | sort -count
```

✓ **1,200 events** (before 12/27/25 7:52:37.000 PM) No Event Sampling ▾

id.orig_h	count
192.168.1.10	113
192.168.1.18	113
192.168.1.21	112
192.168.1.20	105
192.168.1.12	102
192.168.1.13	99
192.168.1.16	97
192.168.1.17	96
192.168.1.19	95
192.168.1.11	92
192.168.1.15	89
192.168.1.14	87



```
index=dns_lab | stats count by qtype
```

Time range: All time

✓ 1,200 events (before 12/27/25 7:53:11.000 PM) No Event Sampling ▾

qtype	count
A	313
AAAA	321
CNAME	257
PTR	309