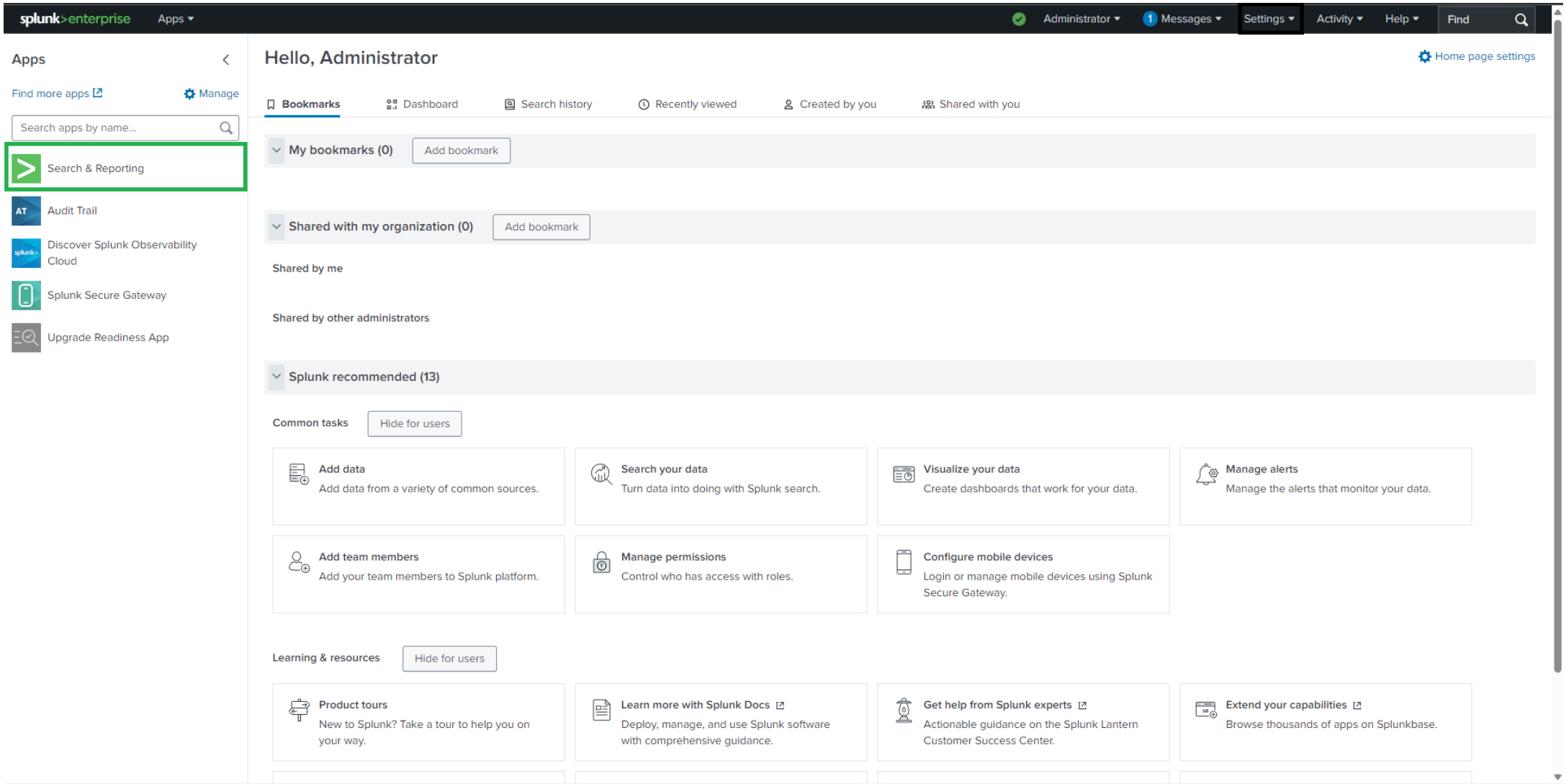
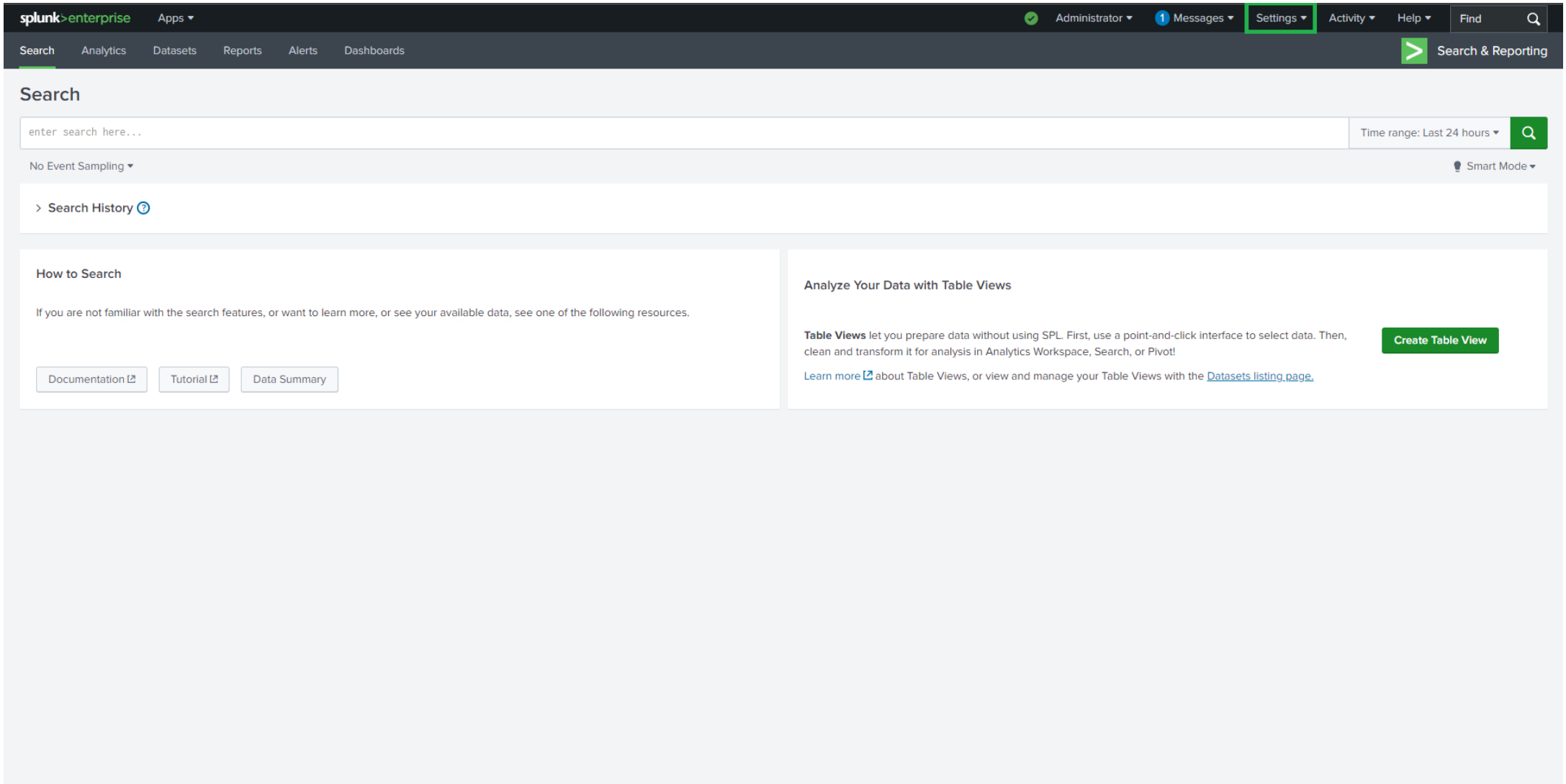
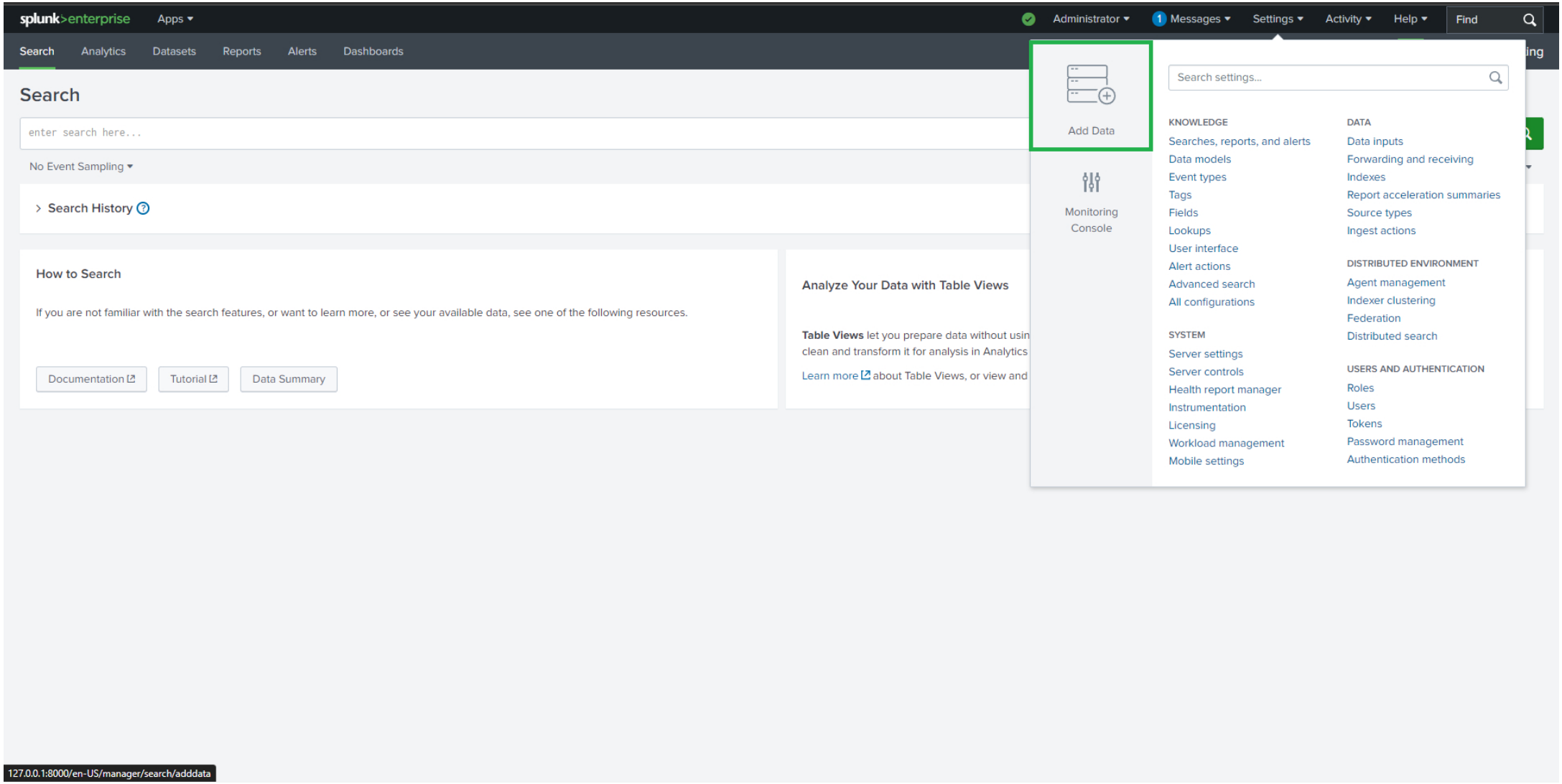
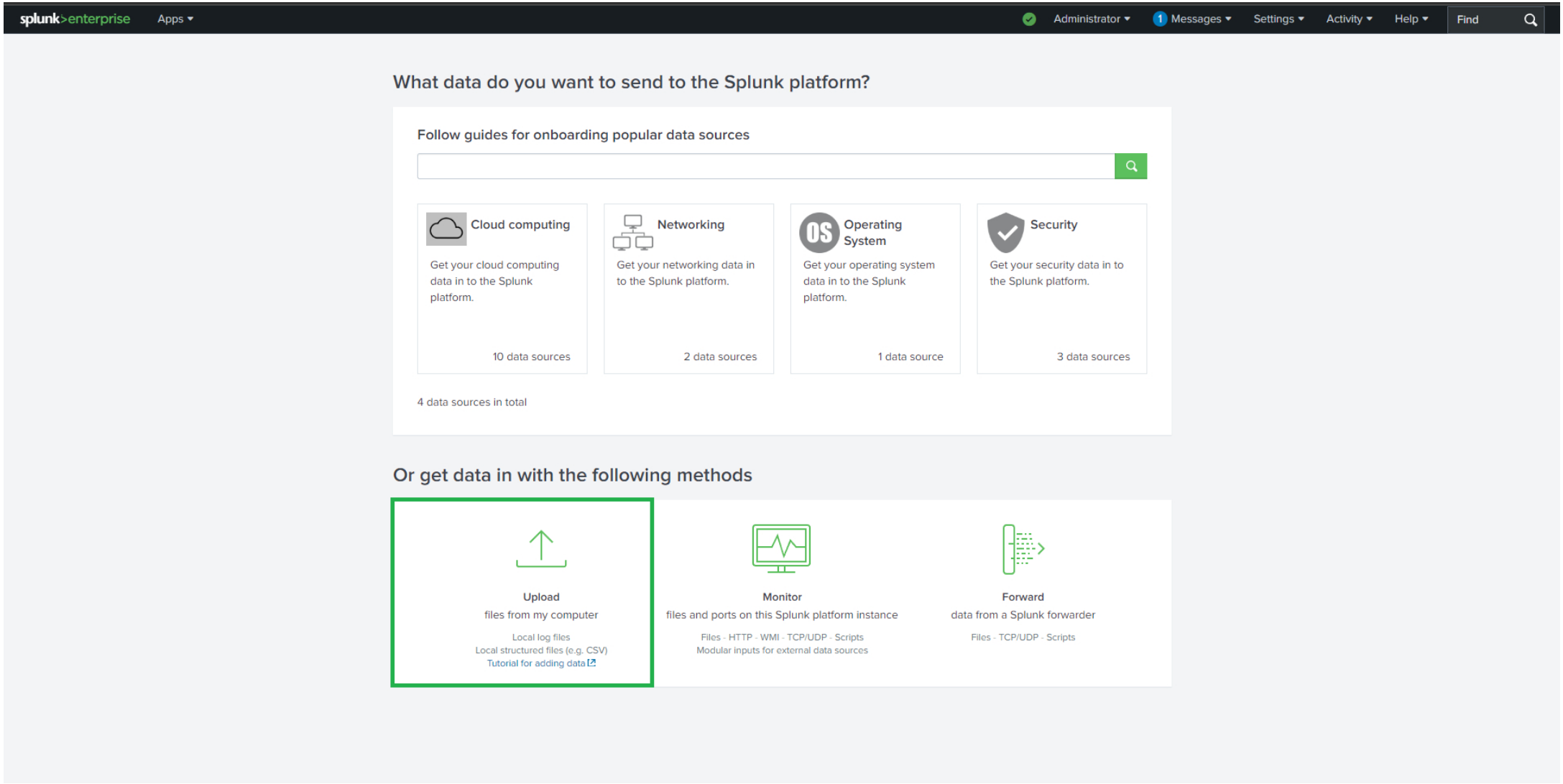
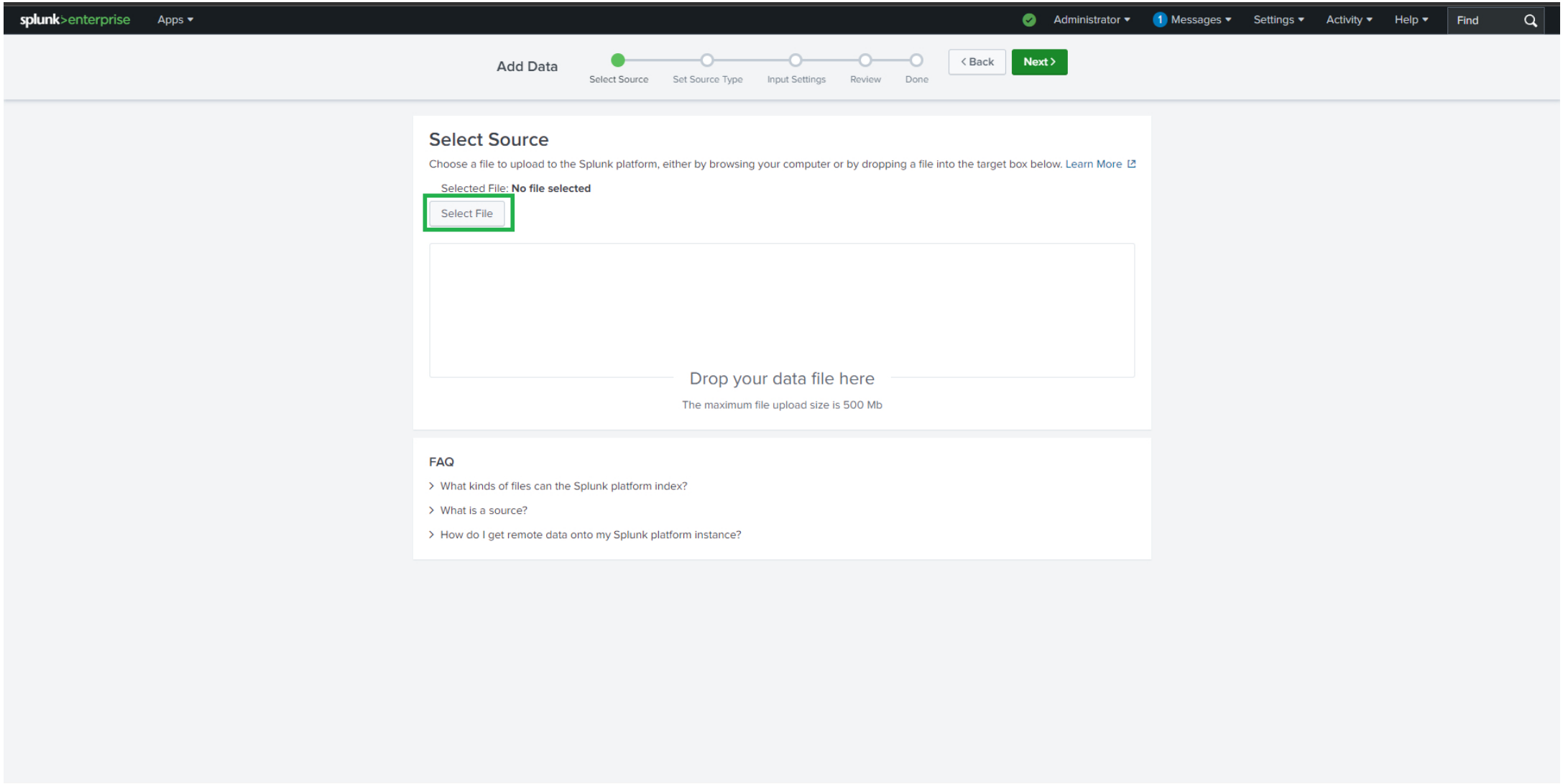
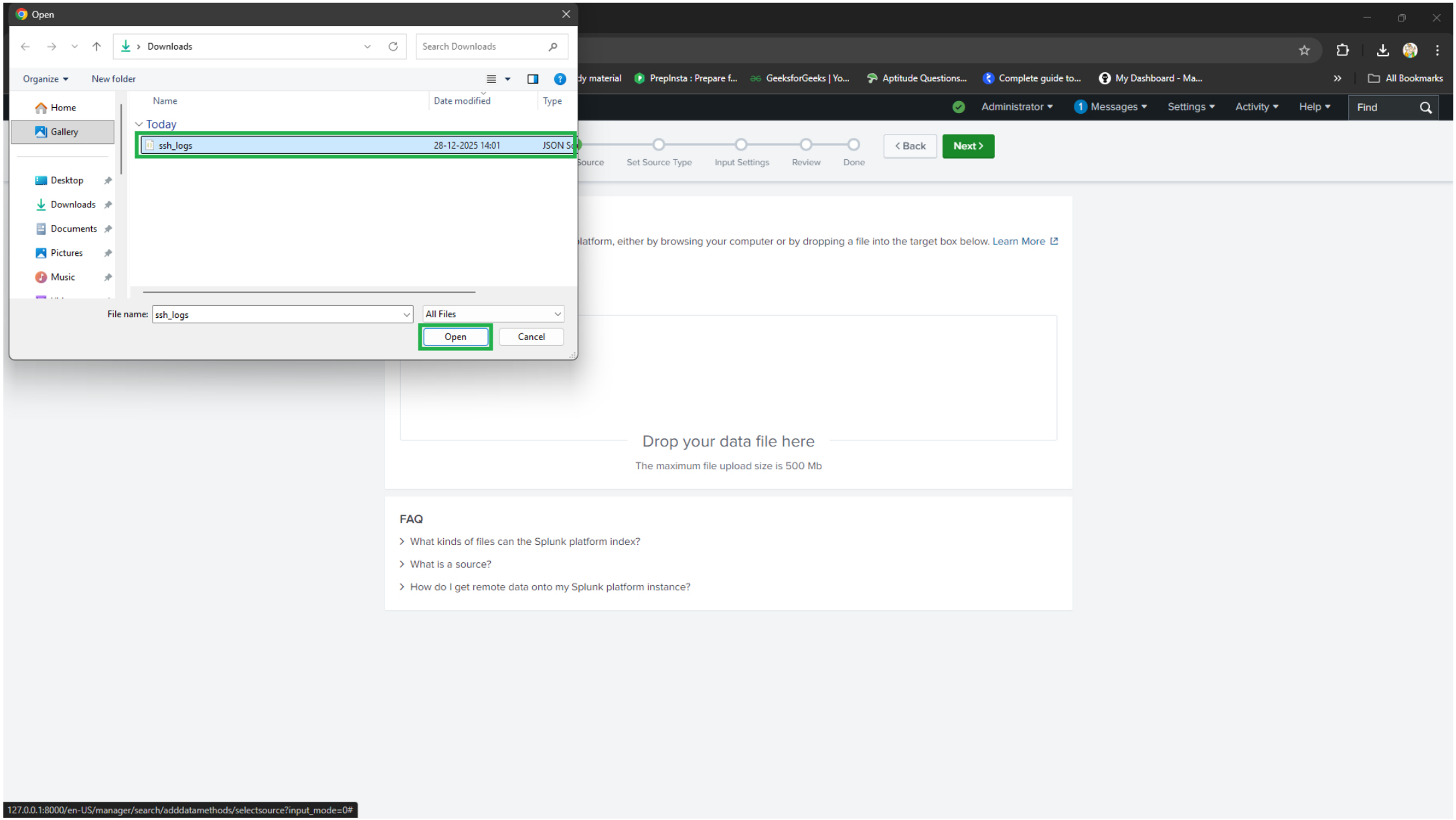

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search 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.

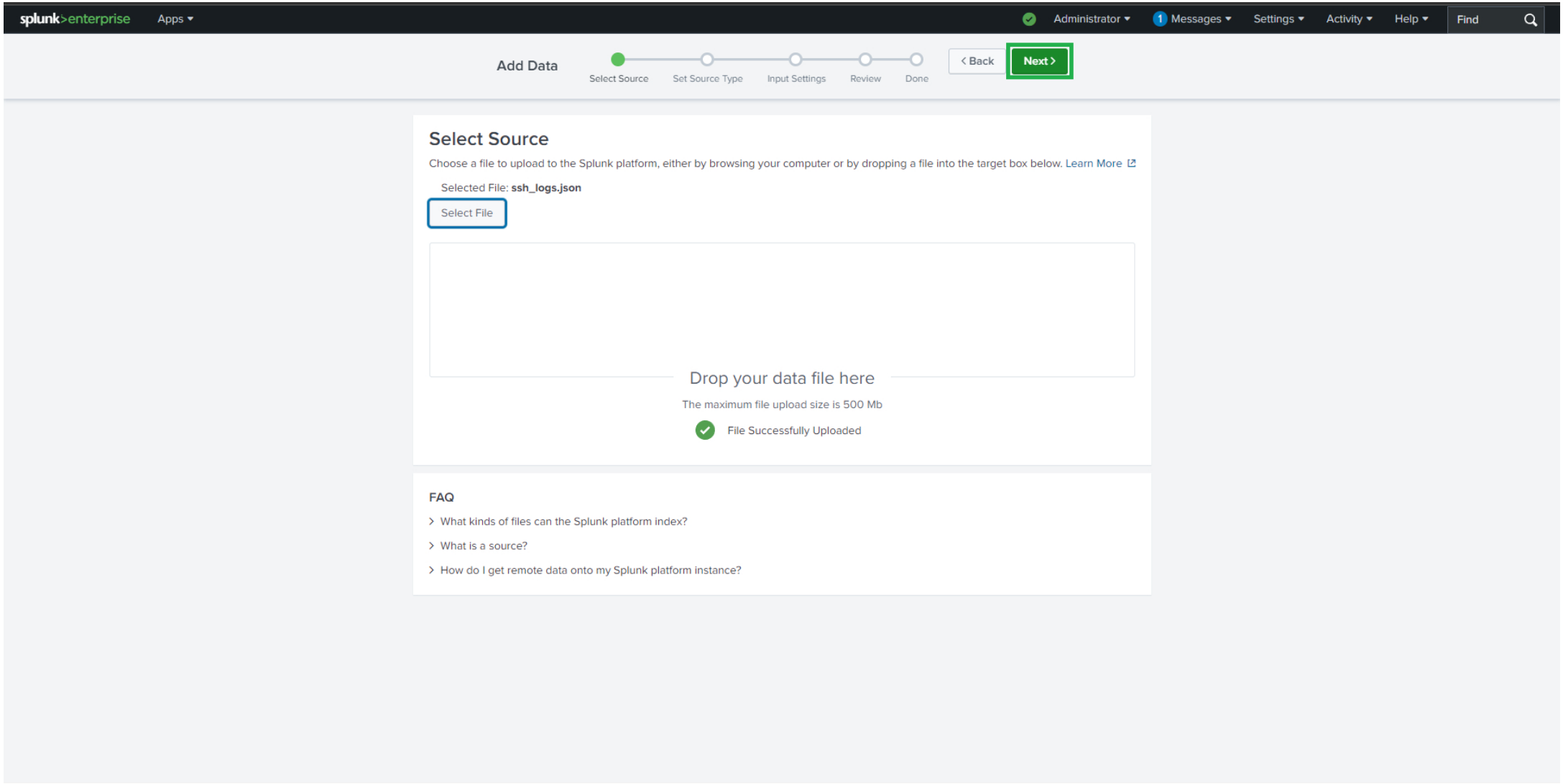

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Search
enter search here...
Time range: Last 24 hours
No Event Sampling
Smart Mode
Search History
How to Search
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.
Documentation
Tutorial
Data Summary
Analyze Your Data with Table Views
Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!
Create Table View
Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

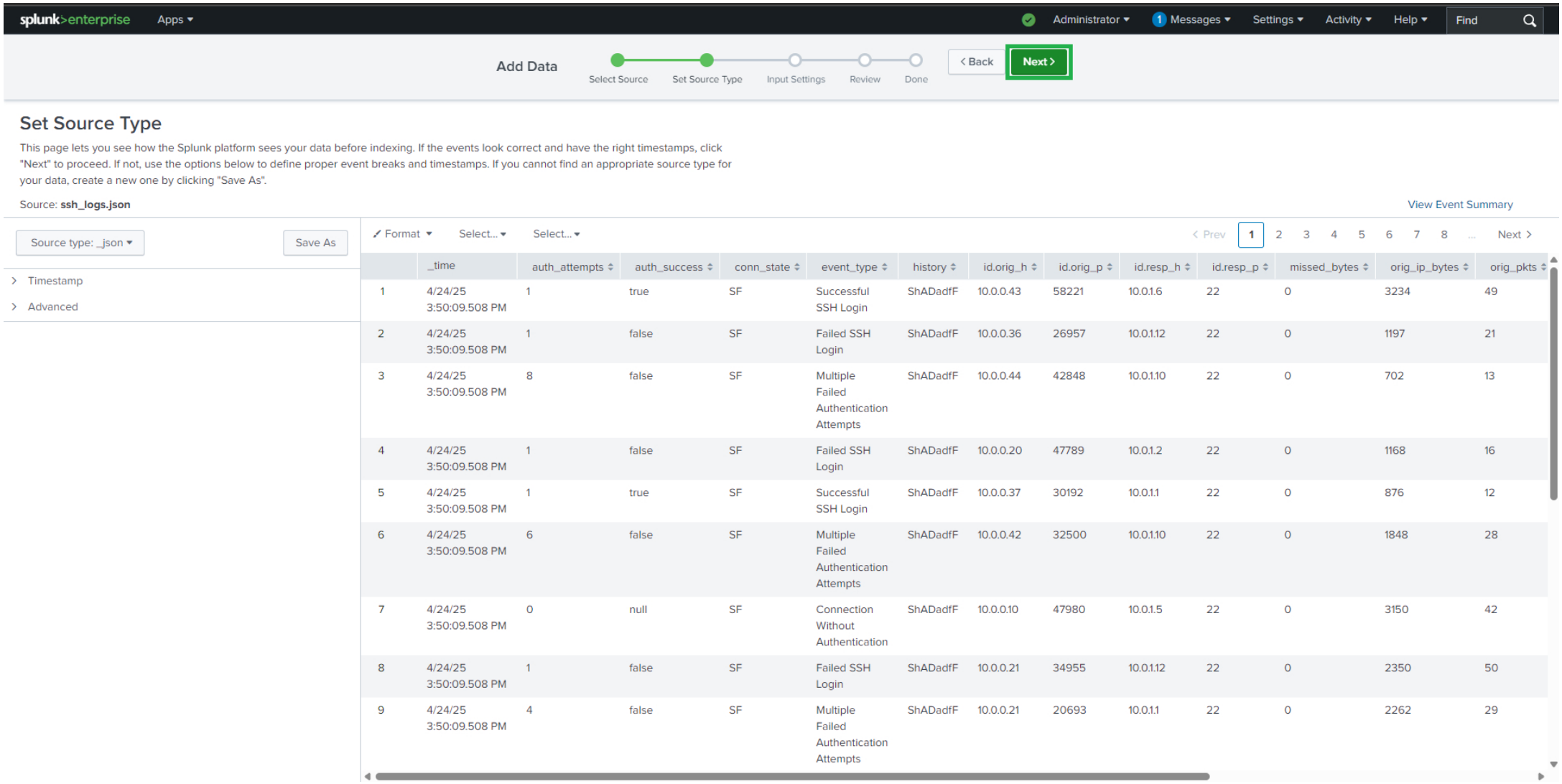

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search
enter search here...
No Event Sampling
Search History
How to Search
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.
Documentation
Tutorial
Data Summary
Analyze Your Data with Table Views
Table Views let you prepare data without usin
clean and transform it for analysis in Analytics
Learn more about Table Views, or view and
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

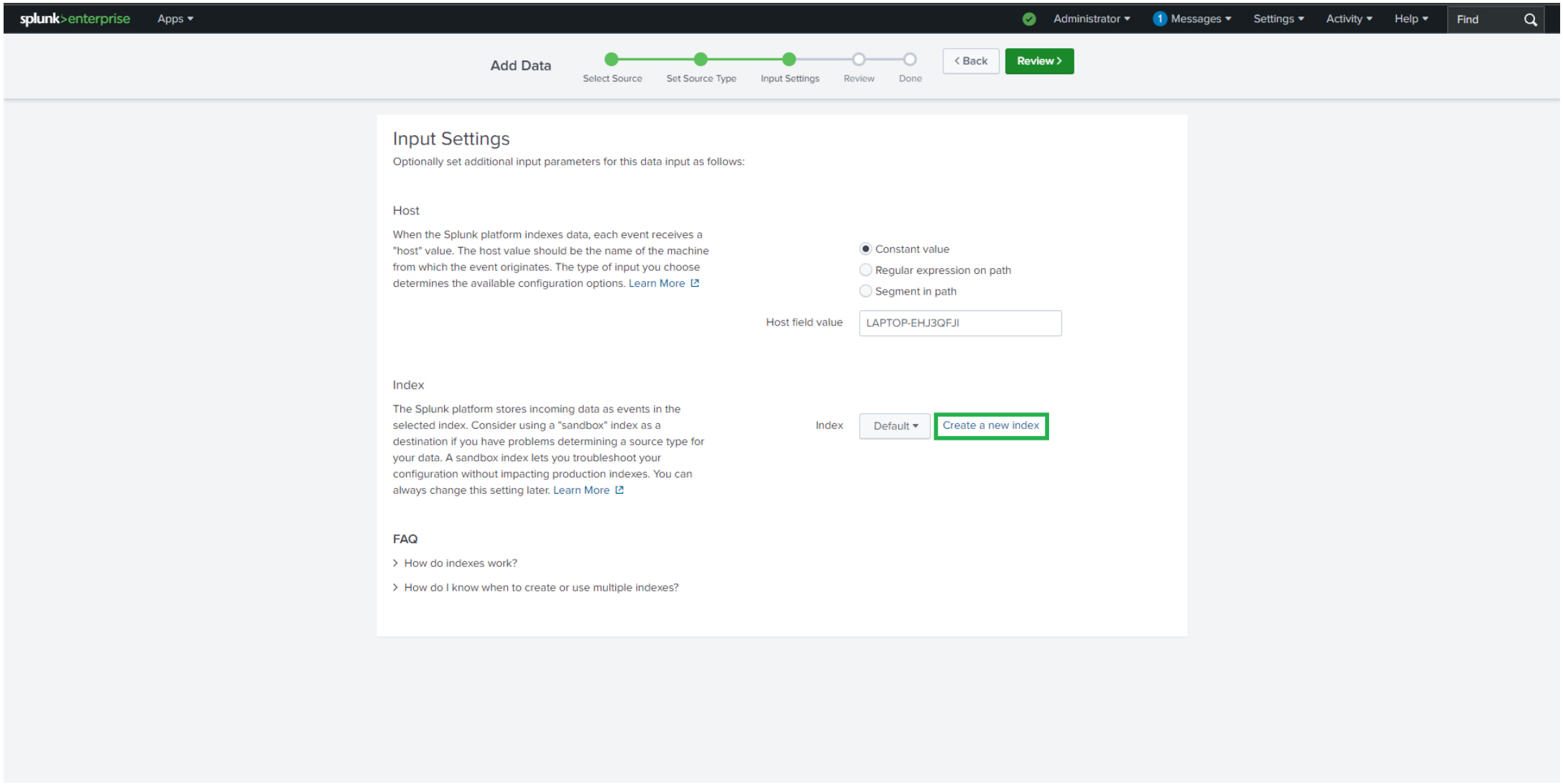

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
What data do you want to send to the Splunk platform?
Follow guides for onboarding popular data sources
Cloud computing
Get your cloud computing data in to the Splunk platform.
10 data sources
Networking
Get your networking data in to the Splunk platform.
2 data sources
OS
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

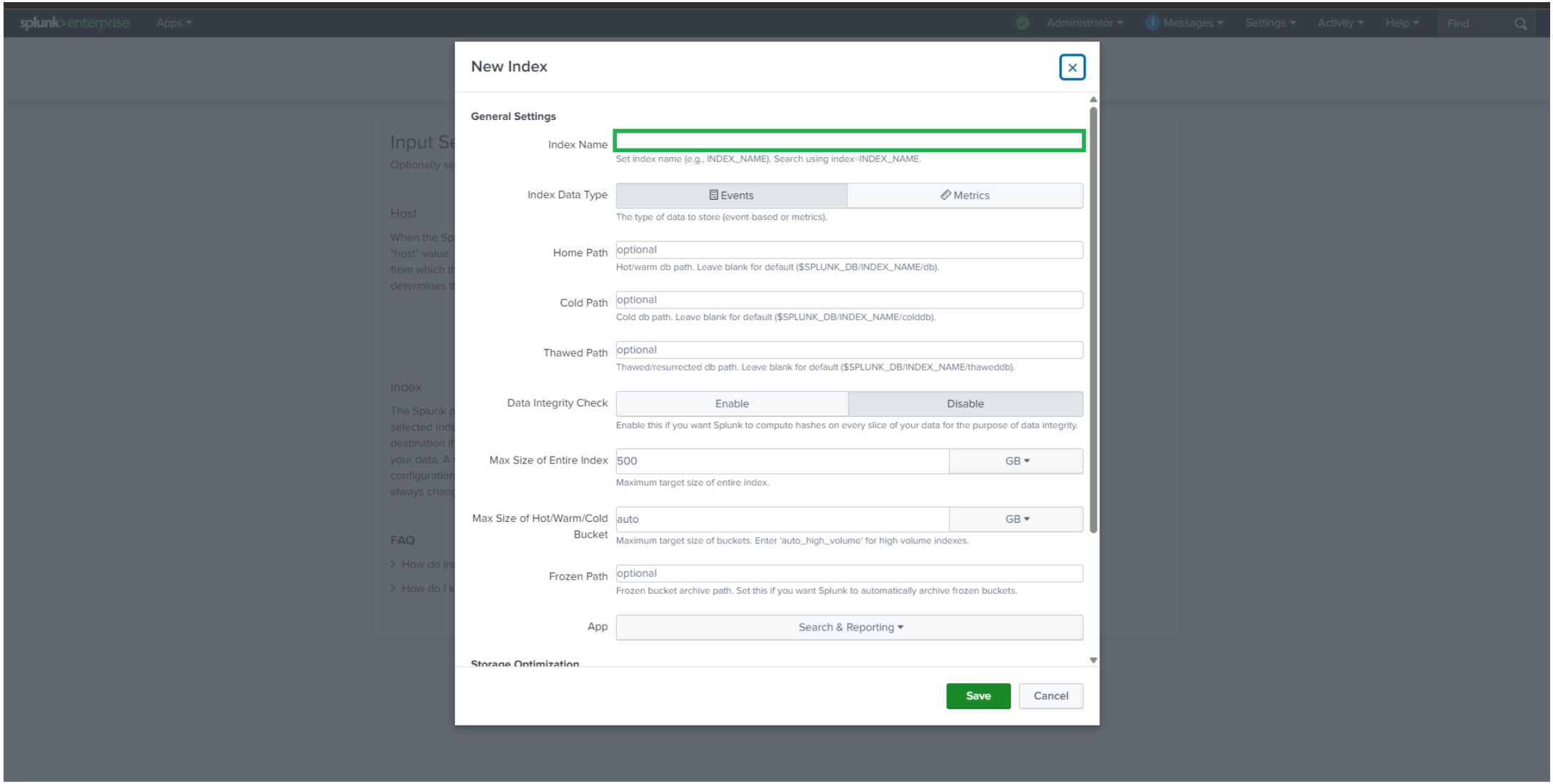

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Select Source
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More
Selected File: No file selected
Select File
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?

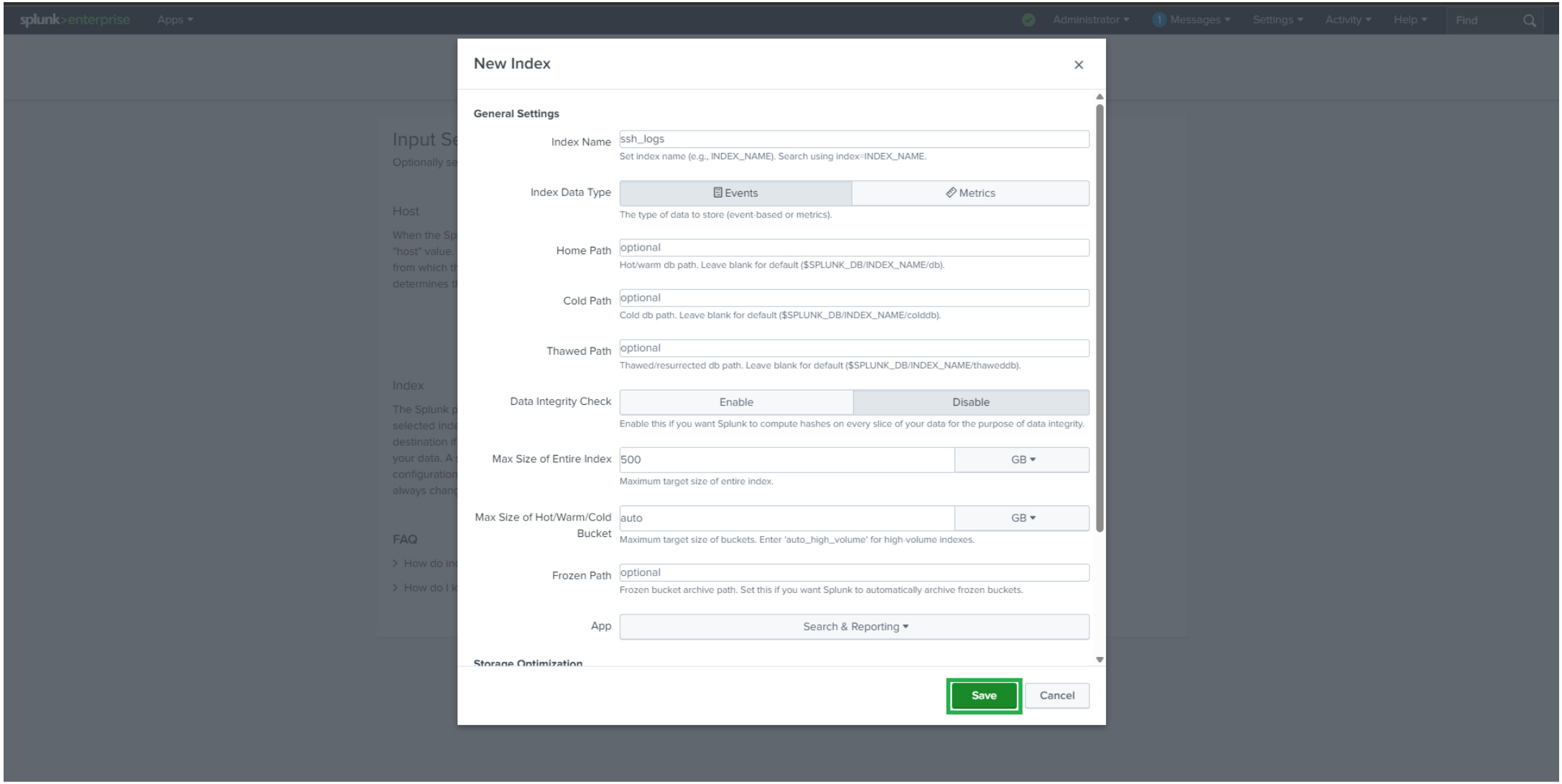

Open
Downloads
Search Downloads
Organize
New folder
Home
Gallery
Desktop
Downloads
Documents
Pictures
Music
Name
Date modified
Type
Today
ssh_logs
28-12-2025 14:01
File name: ssh_logs
All Files
Open
Cancel
Administrator
Messages
Settings
Activity
Help
Find
Back
Next
Set Source Type
Input Settings
Review
Done
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#

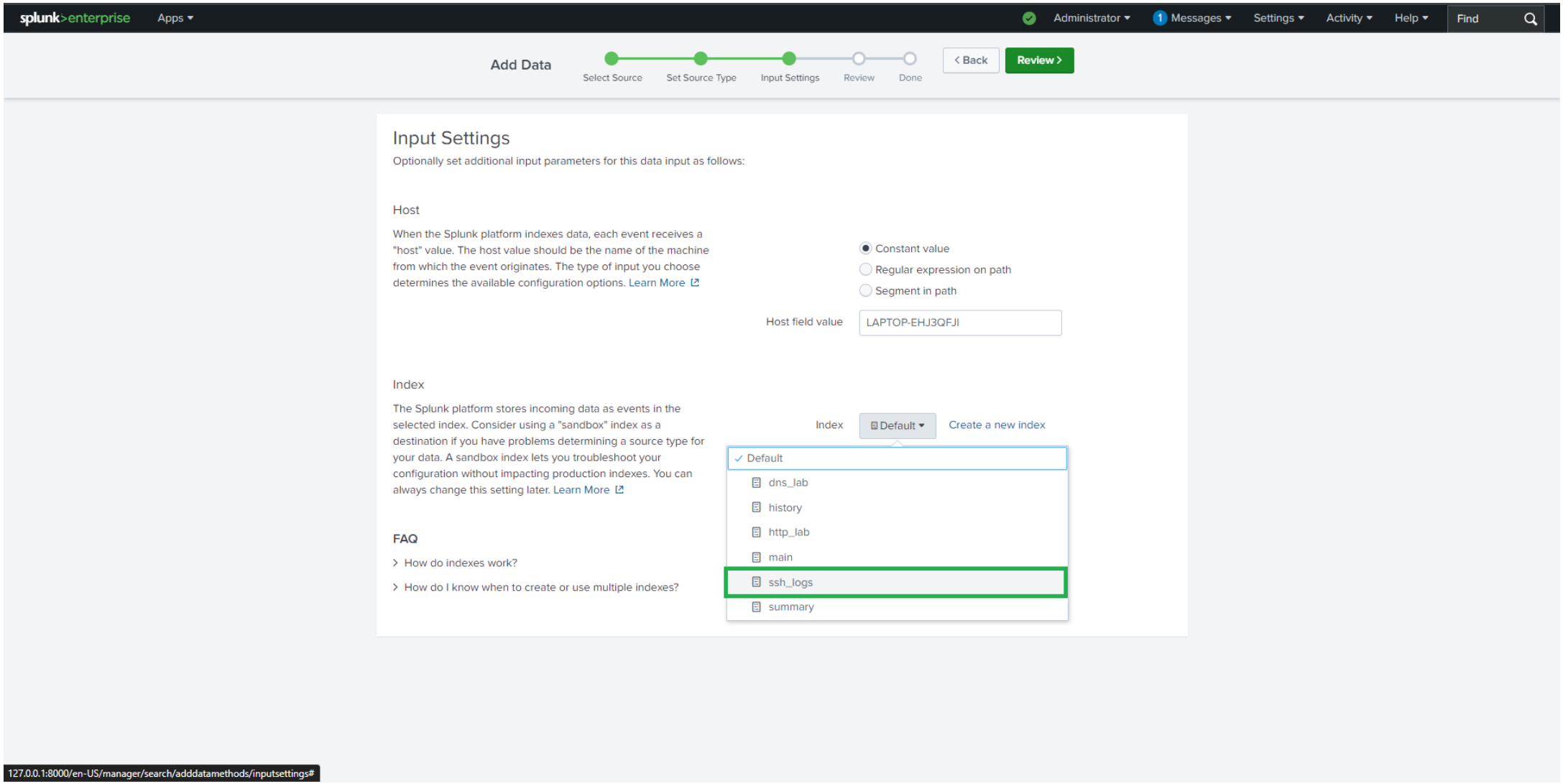

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Select Source
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More
Selected File: ssh_logs.json
Select File
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?

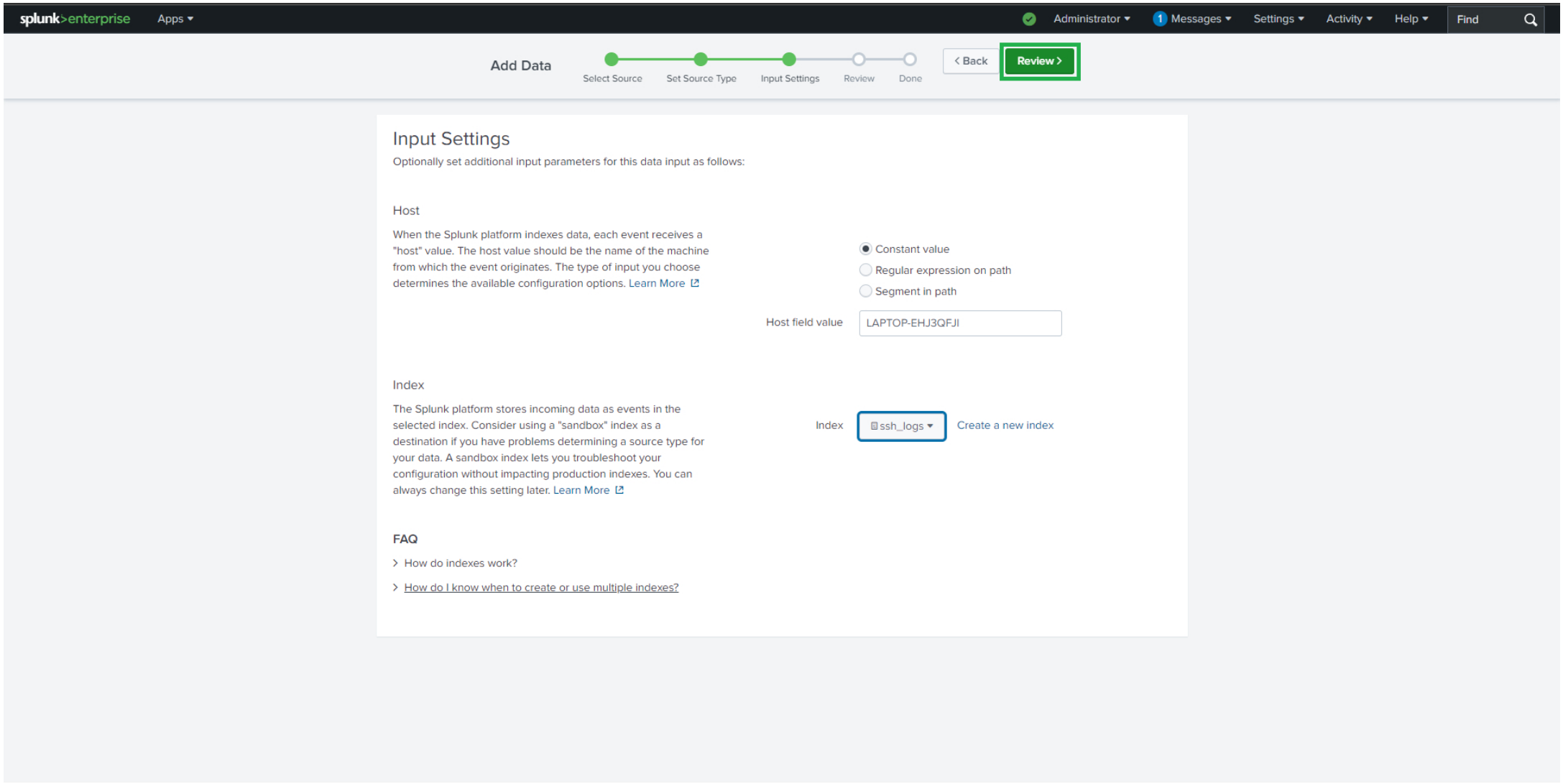

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, 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: ssh_logs.json
View Event Summary
Source type: _json
Save As
Timestamp
Advanced
Format
Select...
Select...
< Prev
1 2 3 4 5 6 7 8 ... Next >
_time
auth_attempts
auth_success
conn_state
event_type
history
id.orig_h
id.orig_p
id.resp_h
id.resp_p
missed_bytes
orig_ip_bytes
orig_pkts
1 4/24/25 3:50:09.508 PM 1 true SF Successful SSH Login ShADadfF 10.0.0.43 58221 10.0.1.6 22 0 3234 49
2 4/24/25 3:50:09.508 PM 1 false SF Failed SSH Login ShADadfF 10.0.0.36 26957 10.0.1.12 22 0 1197 21
3 4/24/25 3:50:09.508 PM 8 false SF Multiple Failed Authentication Attempts ShADadfF 10.0.0.44 42848 10.0.1.10 22 0 702 13
4 4/24/25 3:50:09.508 PM 1 false SF Failed SSH Login ShADadfF 10.0.0.20 47789 10.0.1.2 22 0 1168 16
5 4/24/25 3:50:09.508 PM 1 true SF Successful SSH Login ShADadfF 10.0.0.37 30192 10.0.1.1 22 0 876 12
6 4/24/25 3:50:09.508 PM 6 false SF Multiple Failed Authentication Attempts ShADadfF 10.0.0.42 32500 10.0.1.10 22 0 1848 28
7 4/24/25 3:50:09.508 PM 0 null SF Connection Without Authentication ShADadfF 10.0.0.10 47980 10.0.1.5 22 0 3150 42
8 4/24/25 3:50:09.508 PM 1 false SF Failed SSH Login ShADadfF 10.0.0.21 34955 10.0.1.12 22 0 2350 50
9 4/24/25 3:50:09.508 PM 4 false SF Multiple Failed Authentication Attempts ShADadfF 10.0.0.21 20693 10.0.1.1 22 0 2262 29

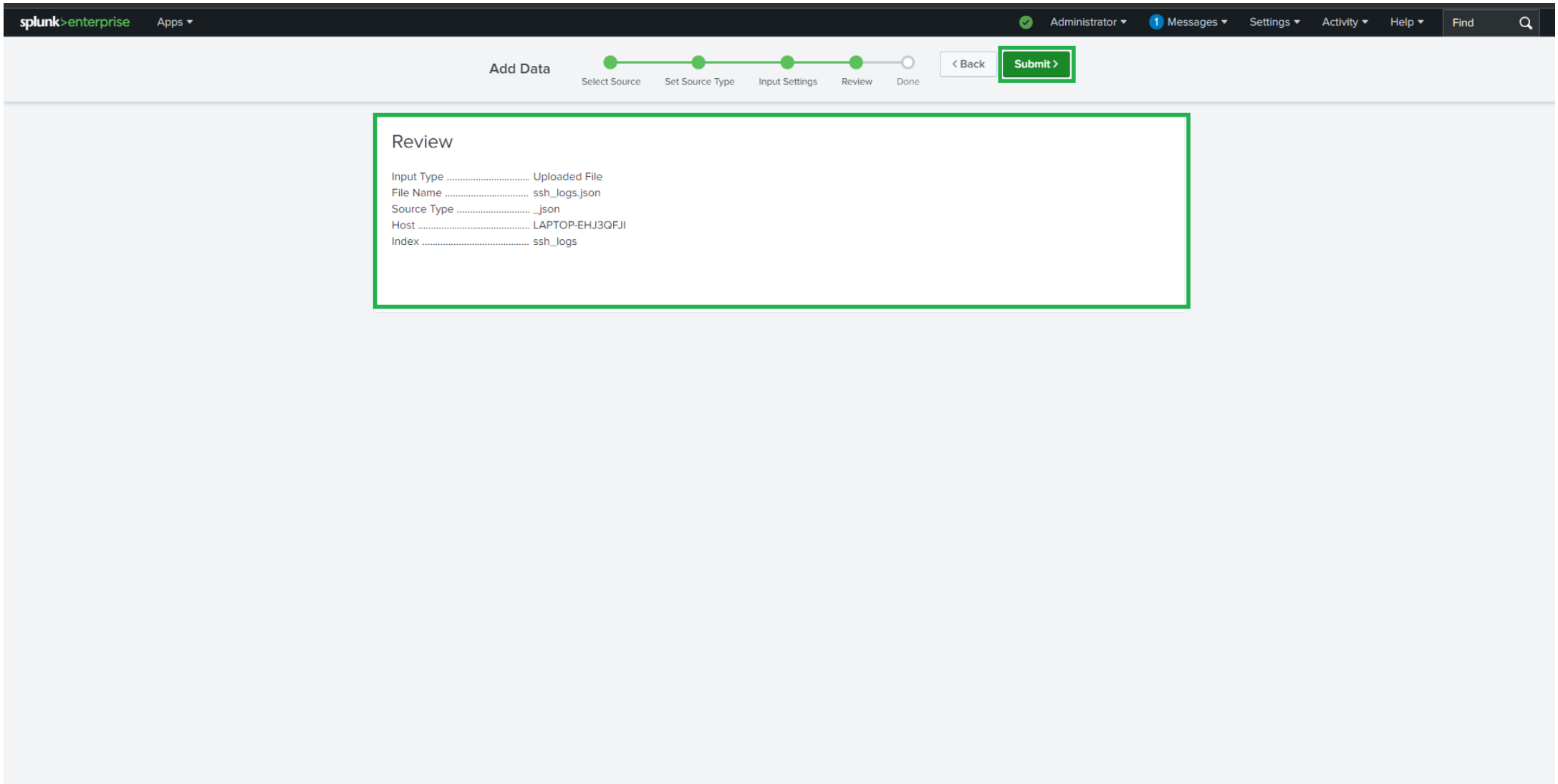

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event 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?

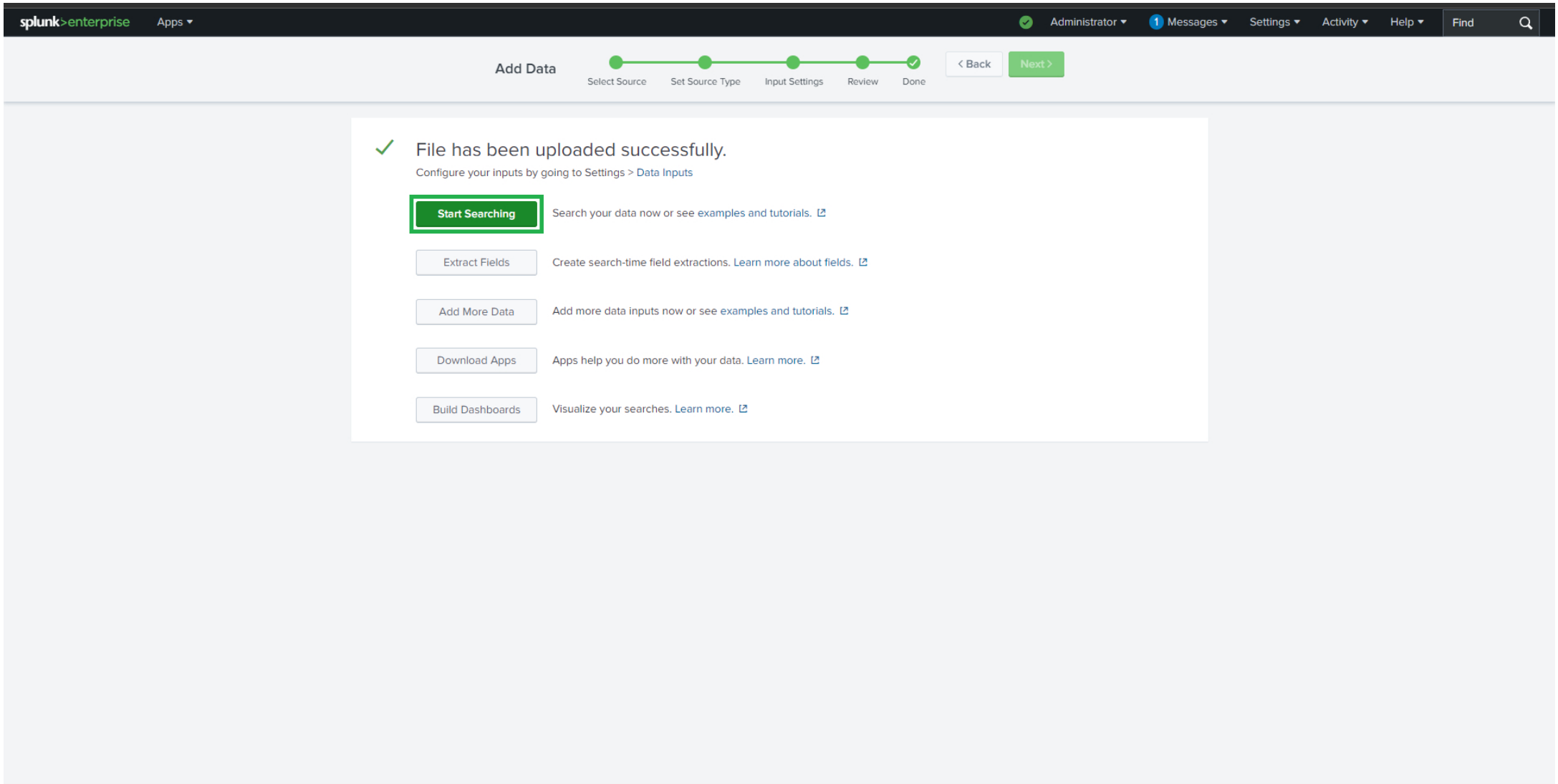

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
New Index
General Settings
Index Name
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.
Index Data Type
Events
Metrics
The type of data to store (event-based or metrics).
Home Path
optional
Hot/warm db path. Leave 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
Save
Cancel

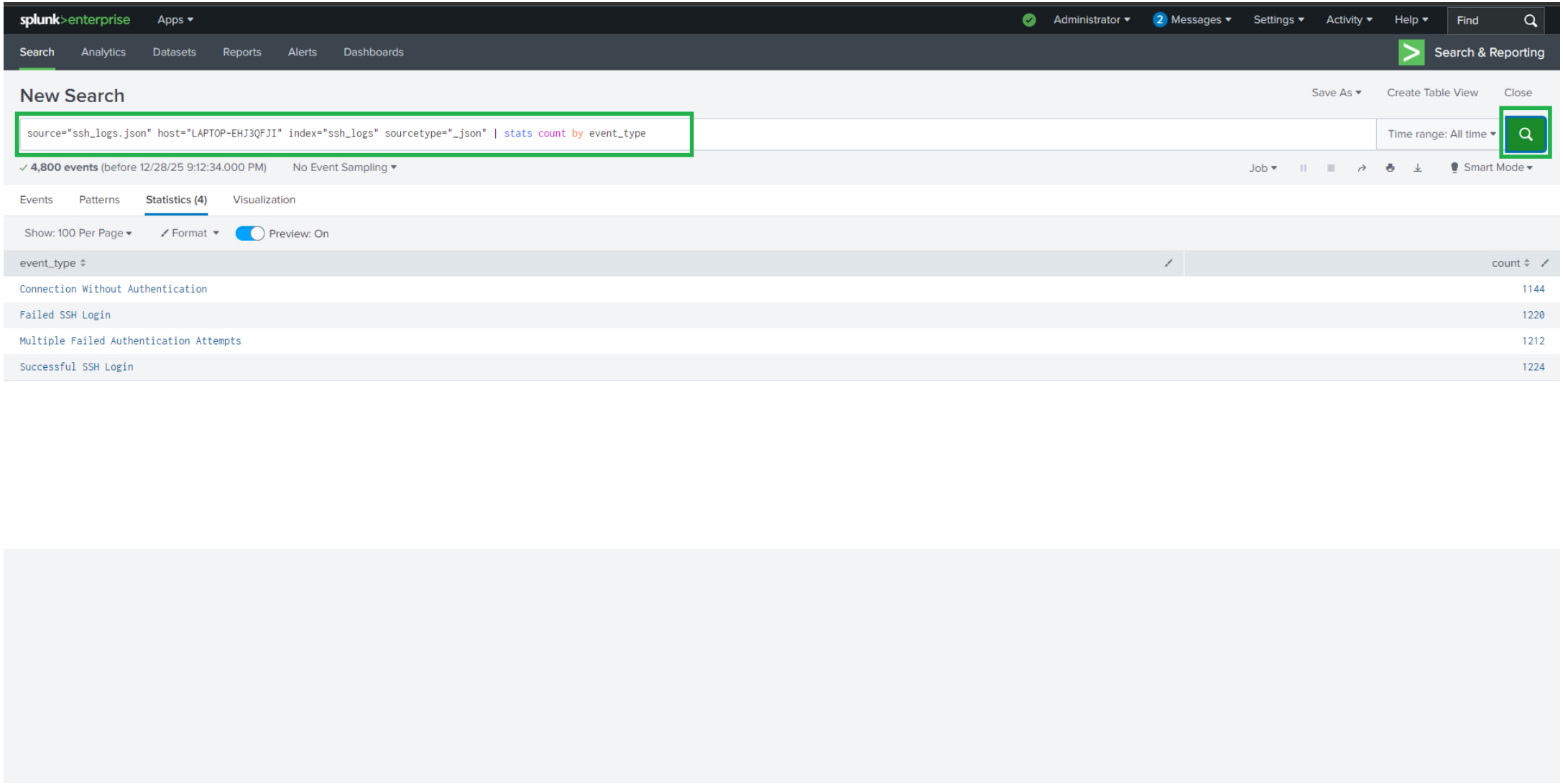

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
New Index
General Settings
Index Name
ssh_logs
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.
Index Data Type
Events
Metrics
The type of data to store (event-based or metrics).
Home Path
optional
Hot/warm db 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
Save
Cancel

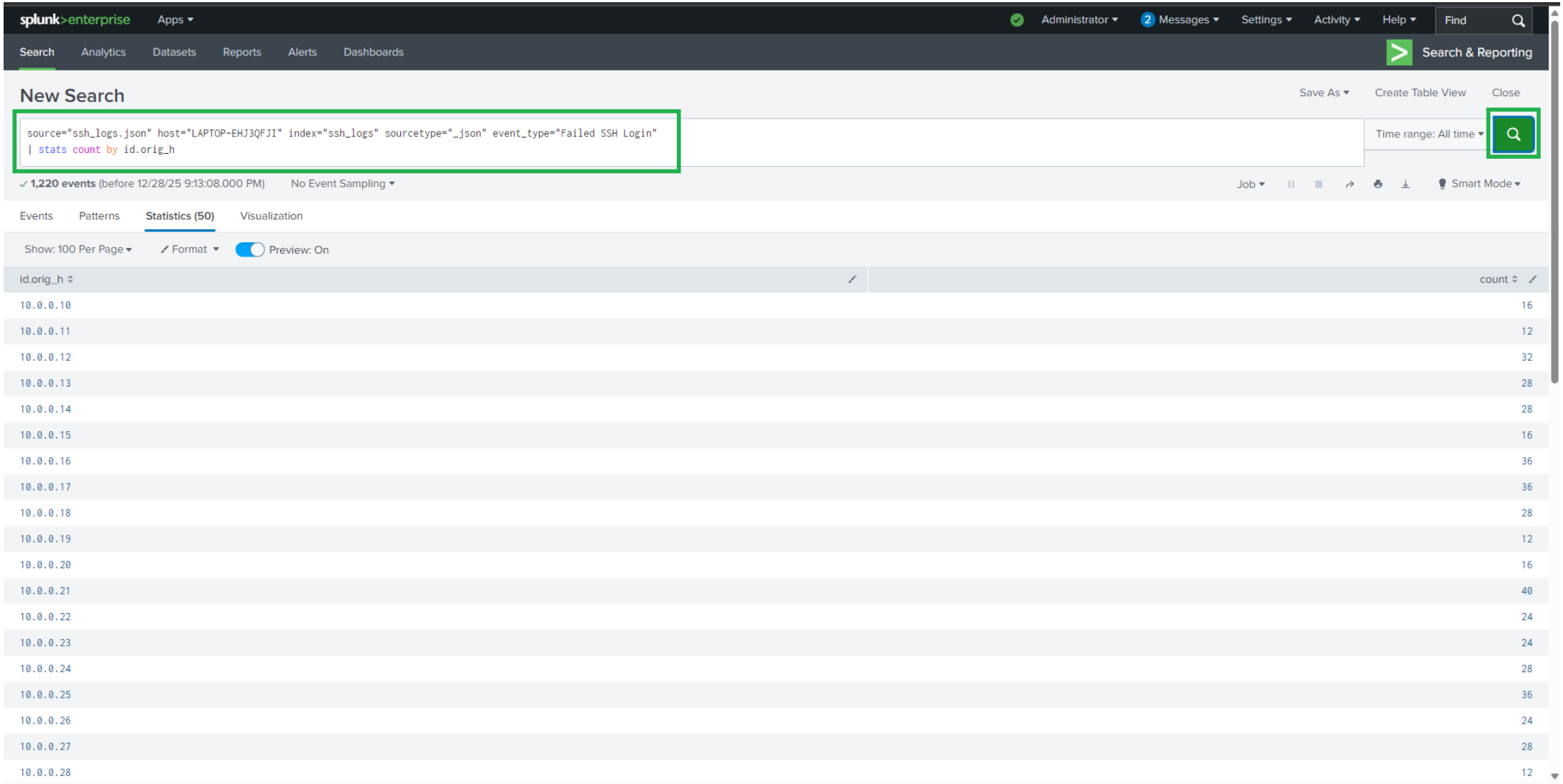

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event 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
Default
dns_lab
history
http_lab
main
ssh_logs
summary
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#

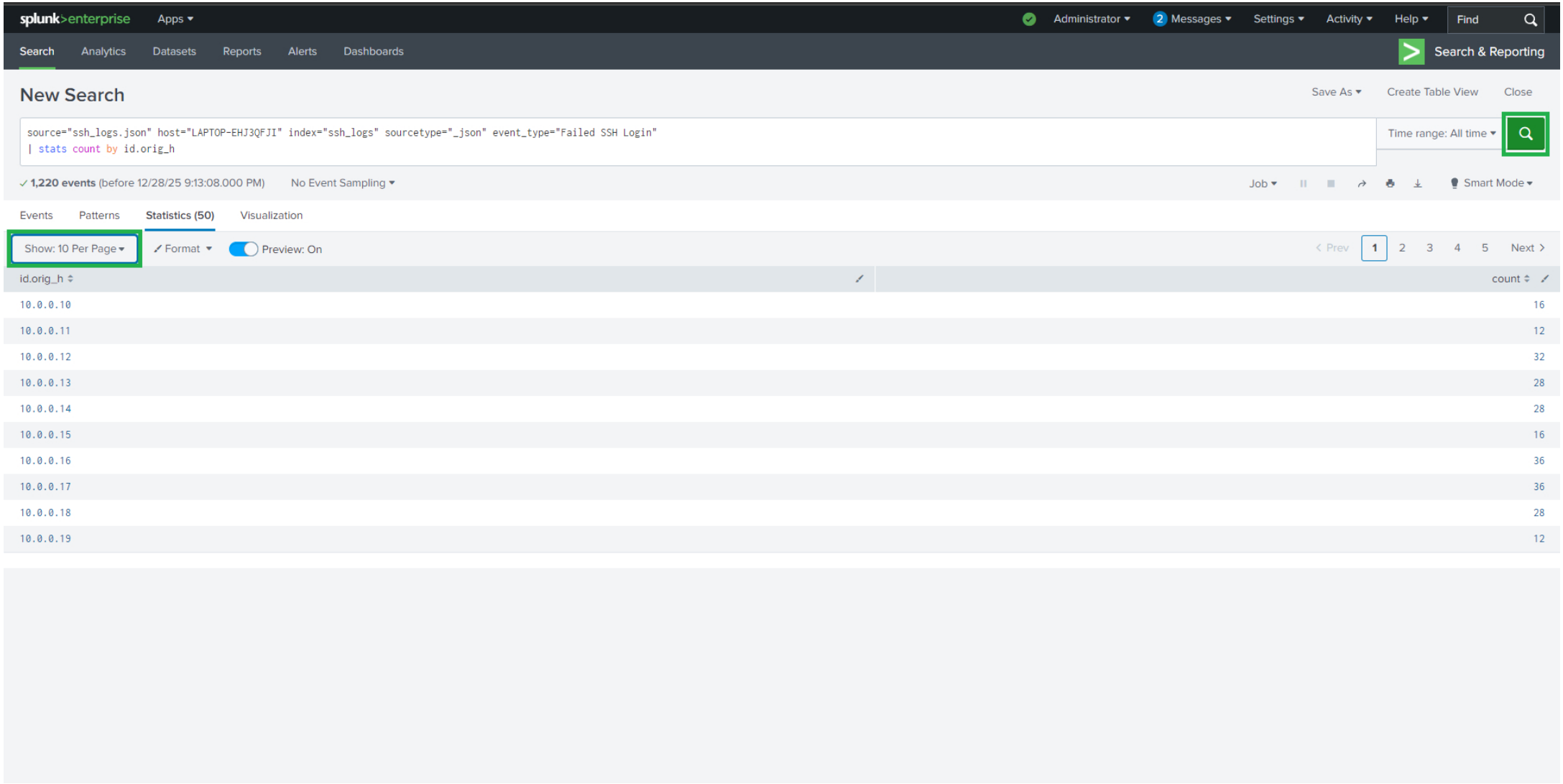

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event 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
ssh_logs
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?

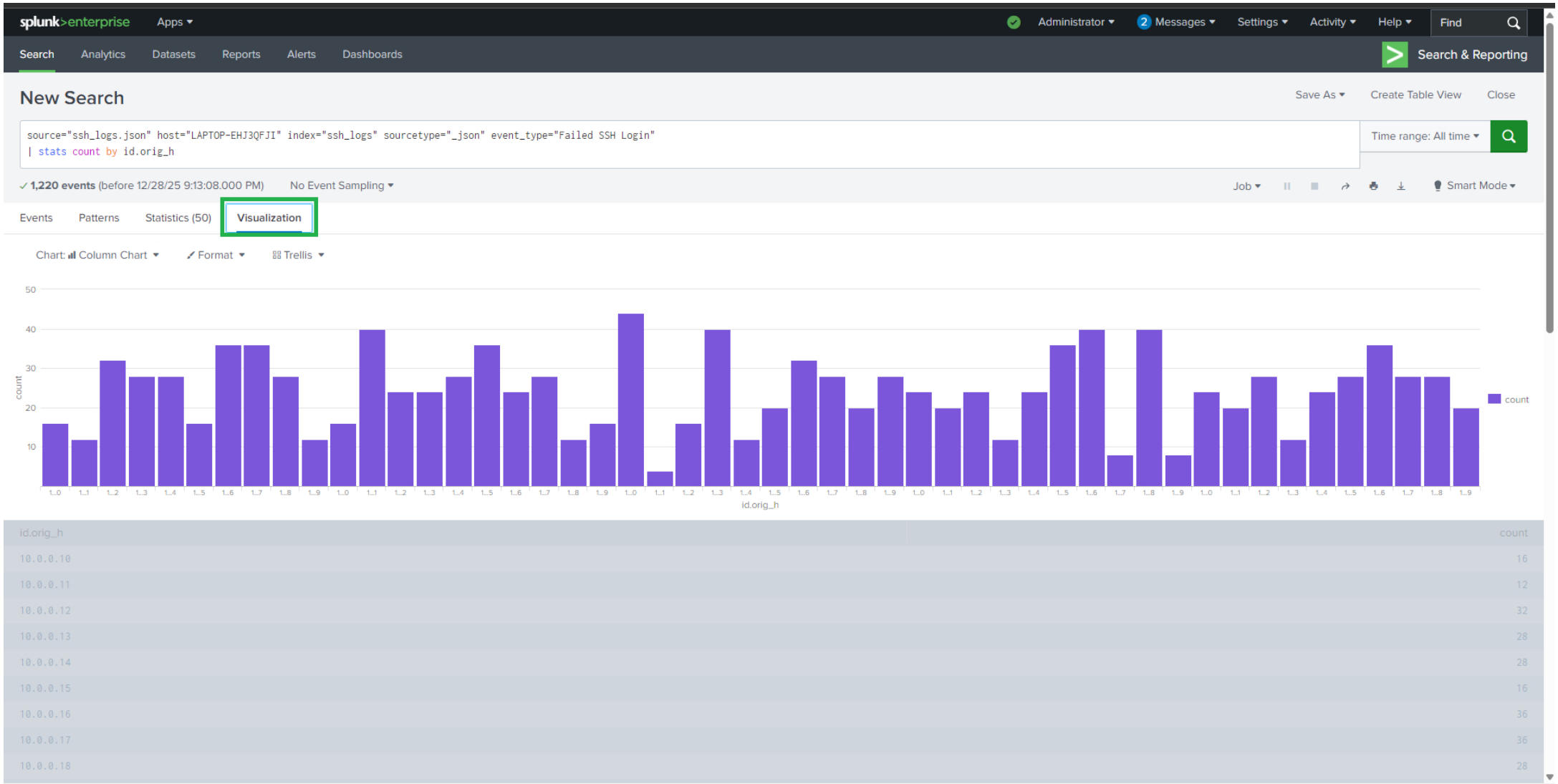

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... Uploaded File
File Name ..... ssh_logs.json
Source Type ..... _json
Host LAPTOP-EHJ3QFJI
Index ..... ssh_logs

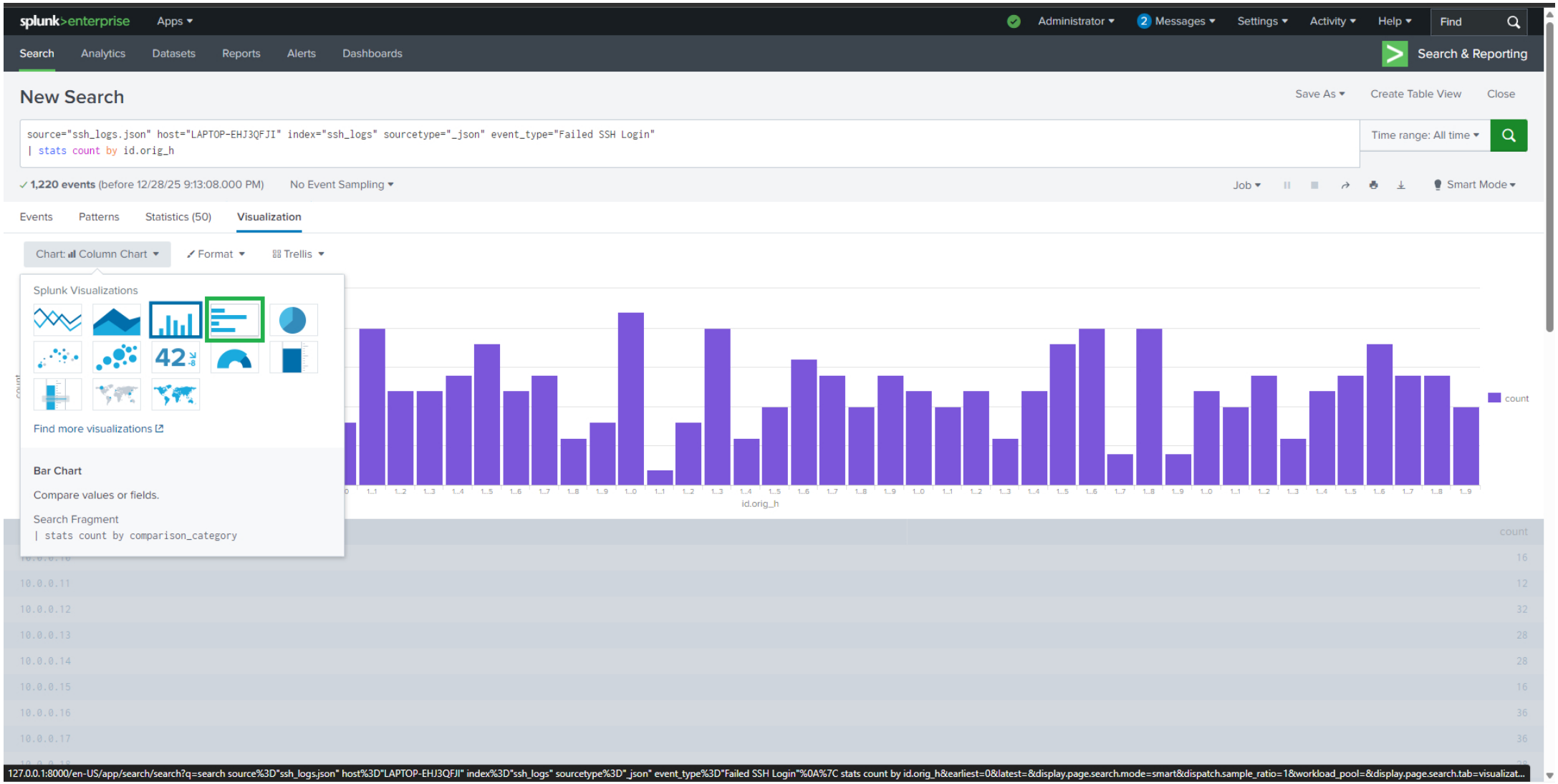

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples 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.

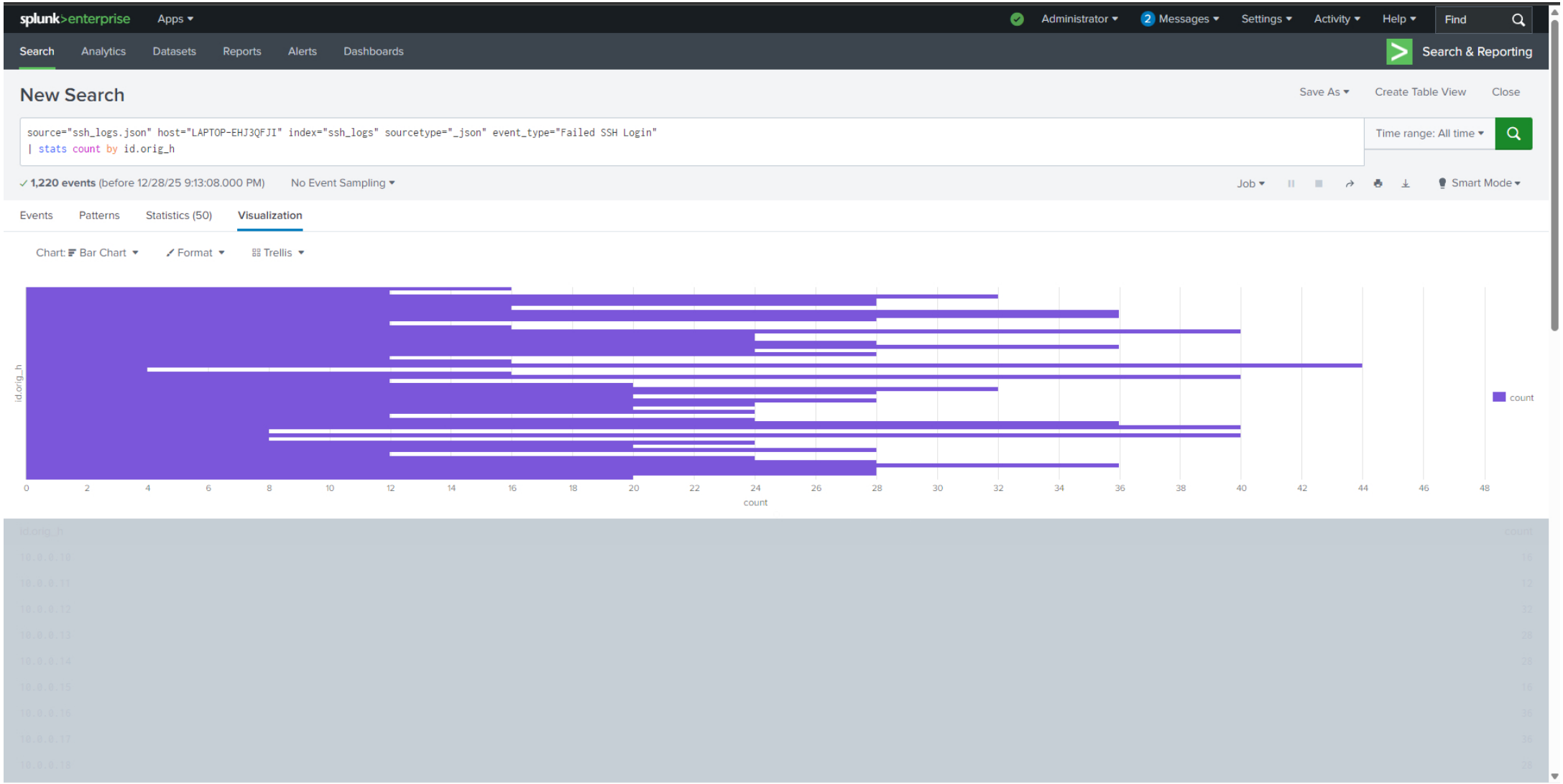

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" | stats count by event_type
Time range: All time
4,800 events (before 12/28/25 9:12:34.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (4)
Visualization
Show: 100 Per Page
Format
Preview: On
event_type
count
Connection Without Authentication
1144
Failed SSH Login
1220
Multiple Failed Authentication Attempts
1212
Successful SSH Login
1224

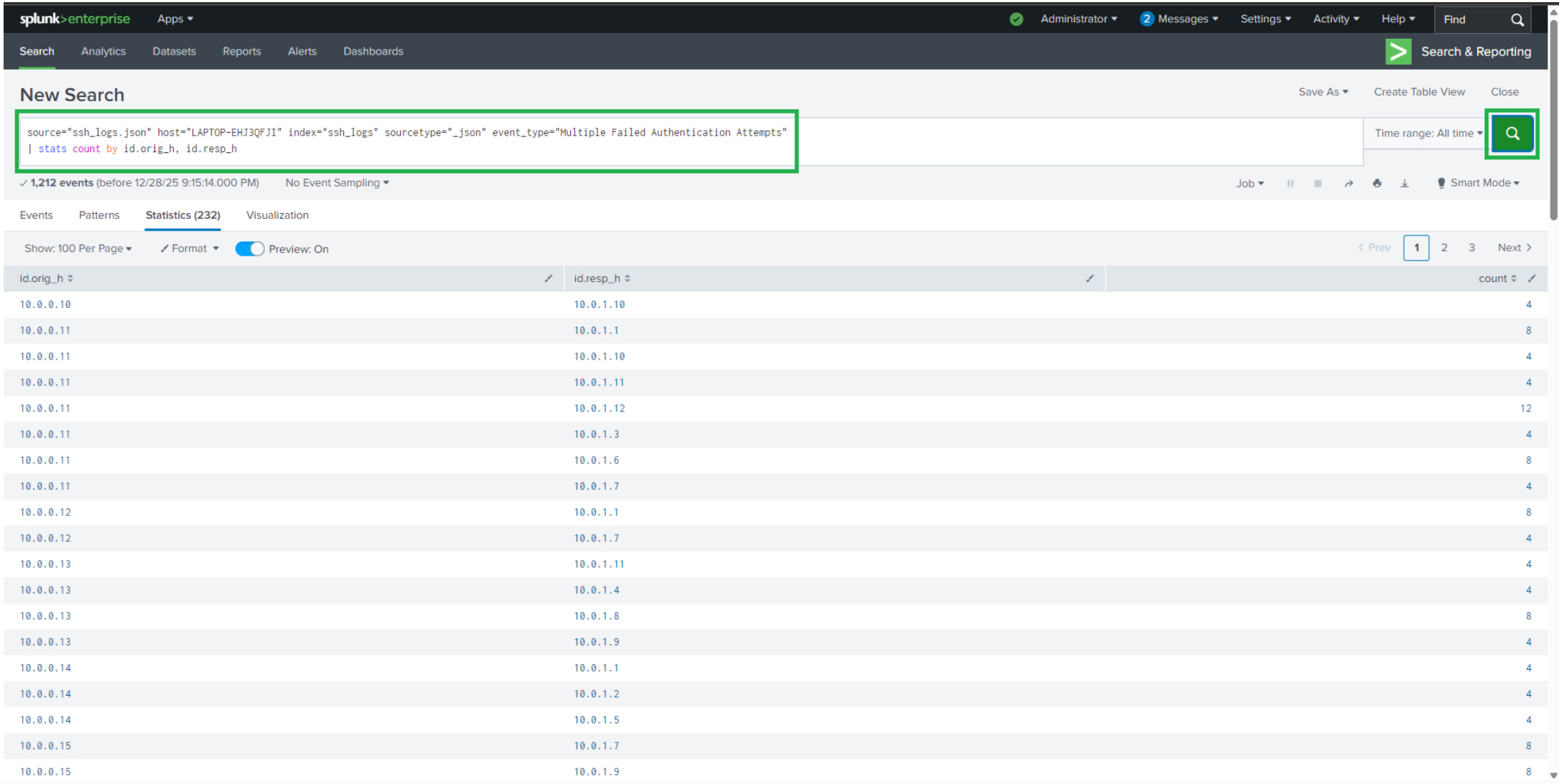

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Failed SSH Login"
| stats count by id.orig_h
Time range: All time
1,220 events (before 12/28/25 9:13:08.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (50)
Visualization
Show: 100 Per Page
Format
Preview: On
id.orig_h
count
10.0.0.10 16
10.0.0.11 12
10.0.0.12 32
10.0.0.13 28
10.0.0.14 28
10.0.0.15 16
10.0.0.16 36
10.0.0.17 36
10.0.0.18 28
10.0.0.19 12
10.0.0.20 16
10.0.0.21 40
10.0.0.22 24
10.0.0.23 24
10.0.0.24 28
10.0.0.25 36
10.0.0.26 24
10.0.0.27 28
10.0.0.28 12


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Failed SSH Login"
| stats count by id.orig_h
Time range: All time
1,220 events (before 12/28/25 9:13:08.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (50)
Visualization
Show: 10 Per Page
Format
Preview: On
Prev
1
2
3
4
5
Next
id.orig_h
count
10.0.0.10 16
10.0.0.11 12
10.0.0.12 32
10.0.0.13 28
10.0.0.14 28
10.0.0.15 16
10.0.0.16 36
10.0.0.17 36
10.0.0.18 28
10.0.0.19 12

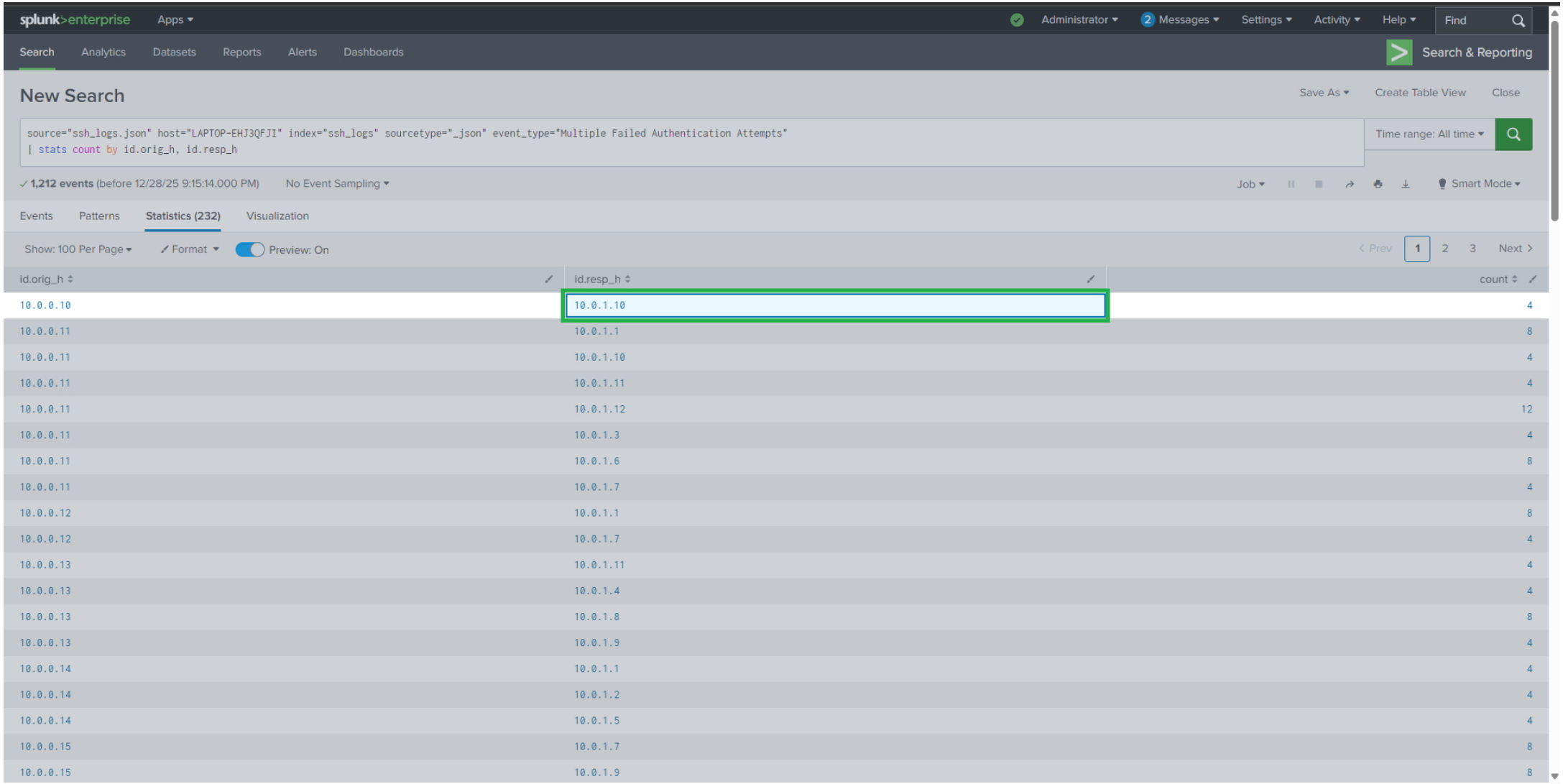

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Failed SSH Login"
| stats count by id.orig_h
Time range: All time
1,220 events (before 12/28/25 9:13:08.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (50)
Visualization
Chart: Column Chart
Format
Trellis
50
40
30
20
10
count
id.orig_h
count
id.orig_h
count
10.0.0.10
16
10.0.0.11
12
10.0.0.12
32
10.0.0.13
28
10.0.0.14
28
10.0.0.15
16
10.0.0.16
36
10.0.0.17
36
10.0.0.18
28


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Failed SSH Login"
| stats count by id.orig_h
Time range: All time
✓ 1,220 events (before 12/28/25 9:13:08.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (50)
Visualization
Chart: Column Chart
Format
Trellis
Splunk Visualizations
Find more visualizations
Bar Chart
Compare values or fields.
Search Fragment
| stats count by comparison_category
count
id.orig_h
10.0.0.11
10.0.0.12
10.0.0.13
10.0.0.14
10.0.0.15
10.0.0.16
10.0.0.17
127.0.0.1:8000/en-US/app/search/search?q=search source%3D"ssh_logs.json" host%3D"LAPTOP-EHJ3QFJI" index%3D"ssh_logs" sourcetype%3D"_json" event_type%3D"Failed SSH Login"%0A%7C stats count by id.orig_h&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&display.page.search.tab=visualizat...

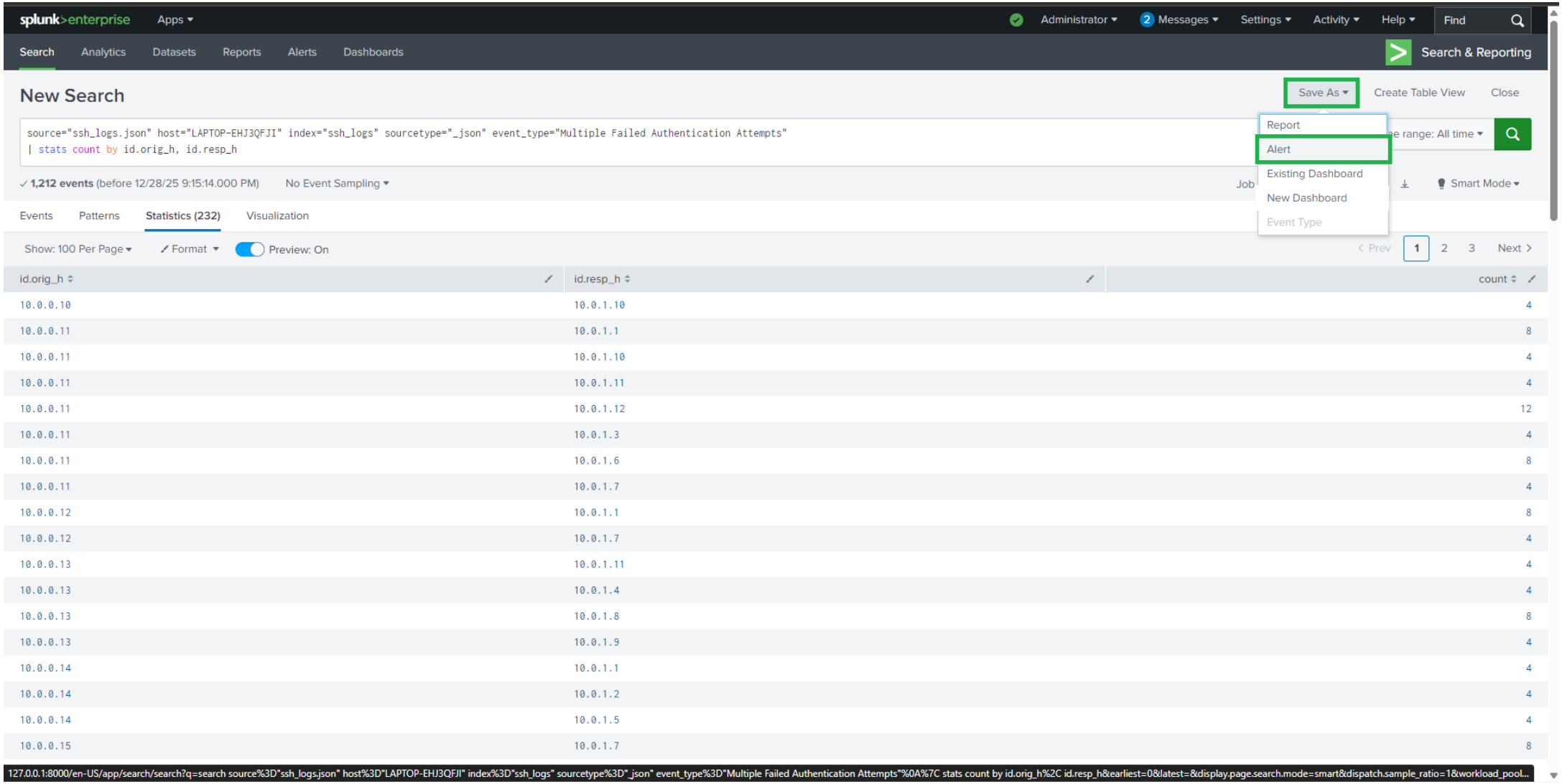

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Failed SSH Login"
| stats count by id.orig_h
Time range: All time
1,220 events (before 12/28/25 9:13:08.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (50)
Visualization
Chart: Bar Chart
Format
Trellis
id.orig_h
count
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
42
44
46
48

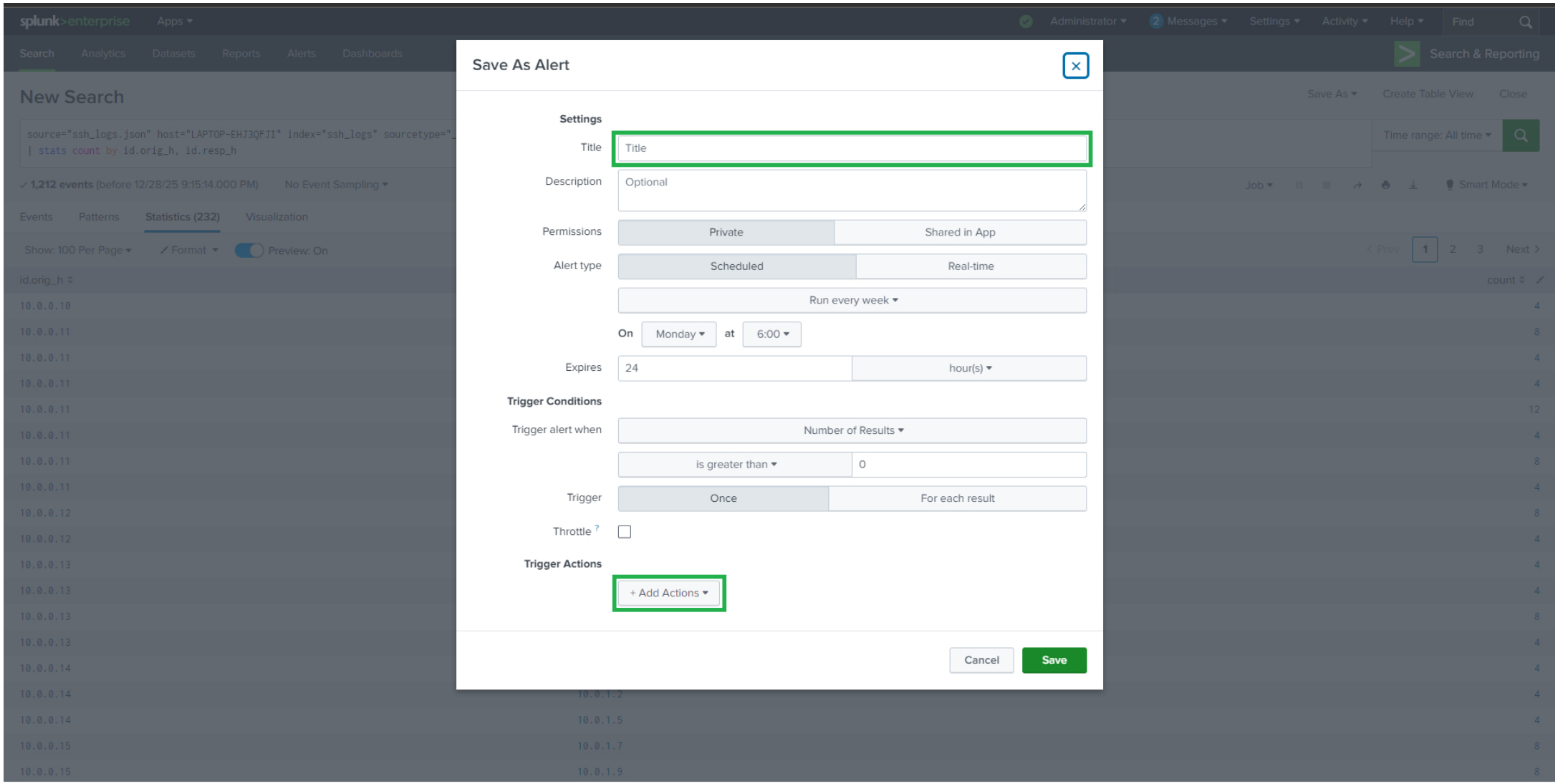


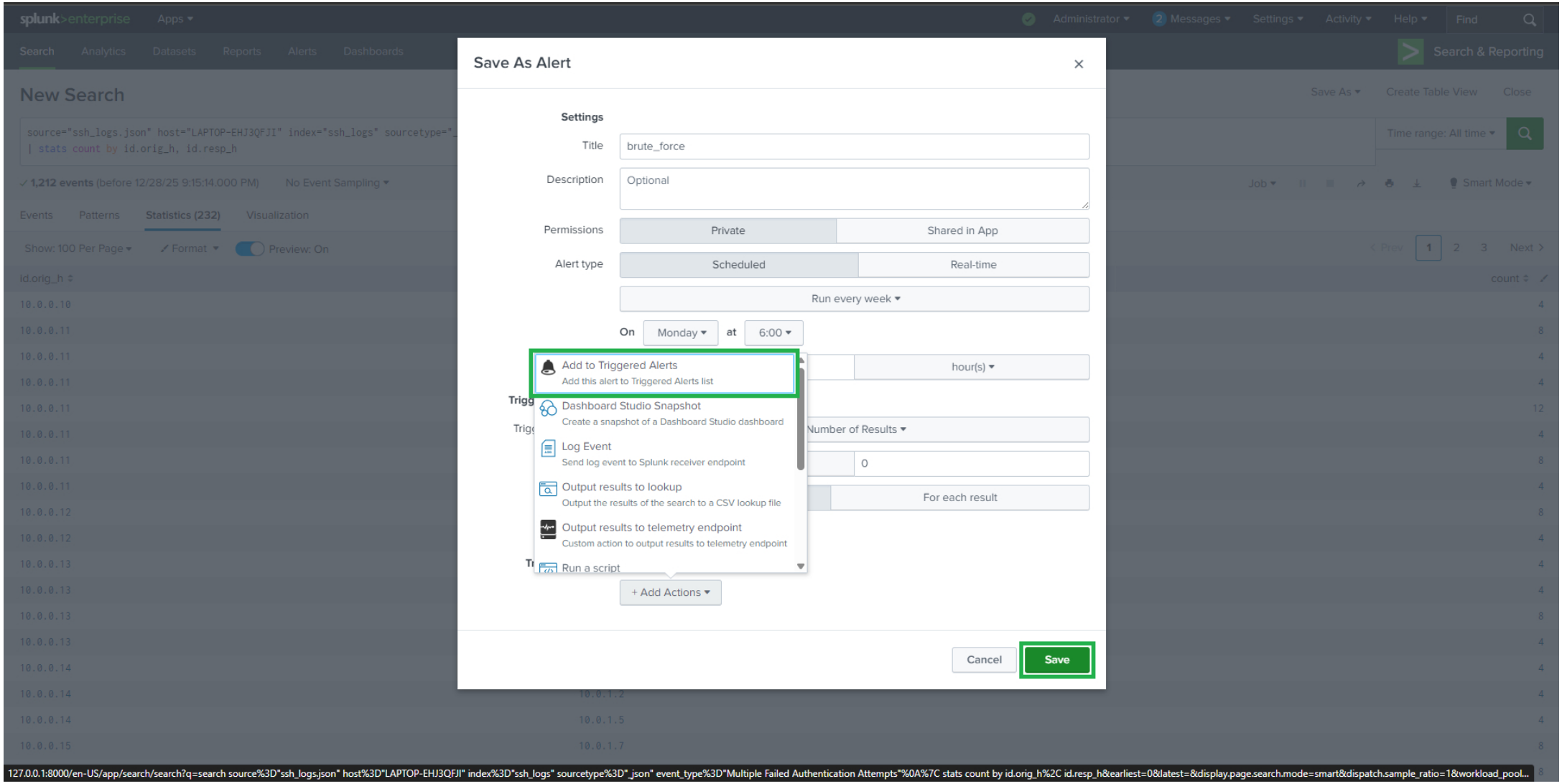
id.orig_h	id.resp_h	count
10.0.0.10	10.0.1.10	4
10.0.0.11	10.0.1.1	8
10.0.0.11	10.0.1.10	4
10.0.0.11	10.0.1.11	4
10.0.0.11	10.0.1.12	12
10.0.0.11	10.0.1.3	4
10.0.0.11	10.0.1.6	8
10.0.0.11	10.0.1.7	4
10.0.0.12	10.0.1.1	8
10.0.0.12	10.0.1.7	4
10.0.0.13	10.0.1.11	4
10.0.0.13	10.0.1.4	4
10.0.0.13	10.0.1.8	8
10.0.0.13	10.0.1.9	4
10.0.0.14	10.0.1.1	4
10.0.0.14	10.0.1.2	4
10.0.0.14	10.0.1.5	4
10.0.0.15	10.0.1.7	8
10.0.0.15	10.0.1.9	8

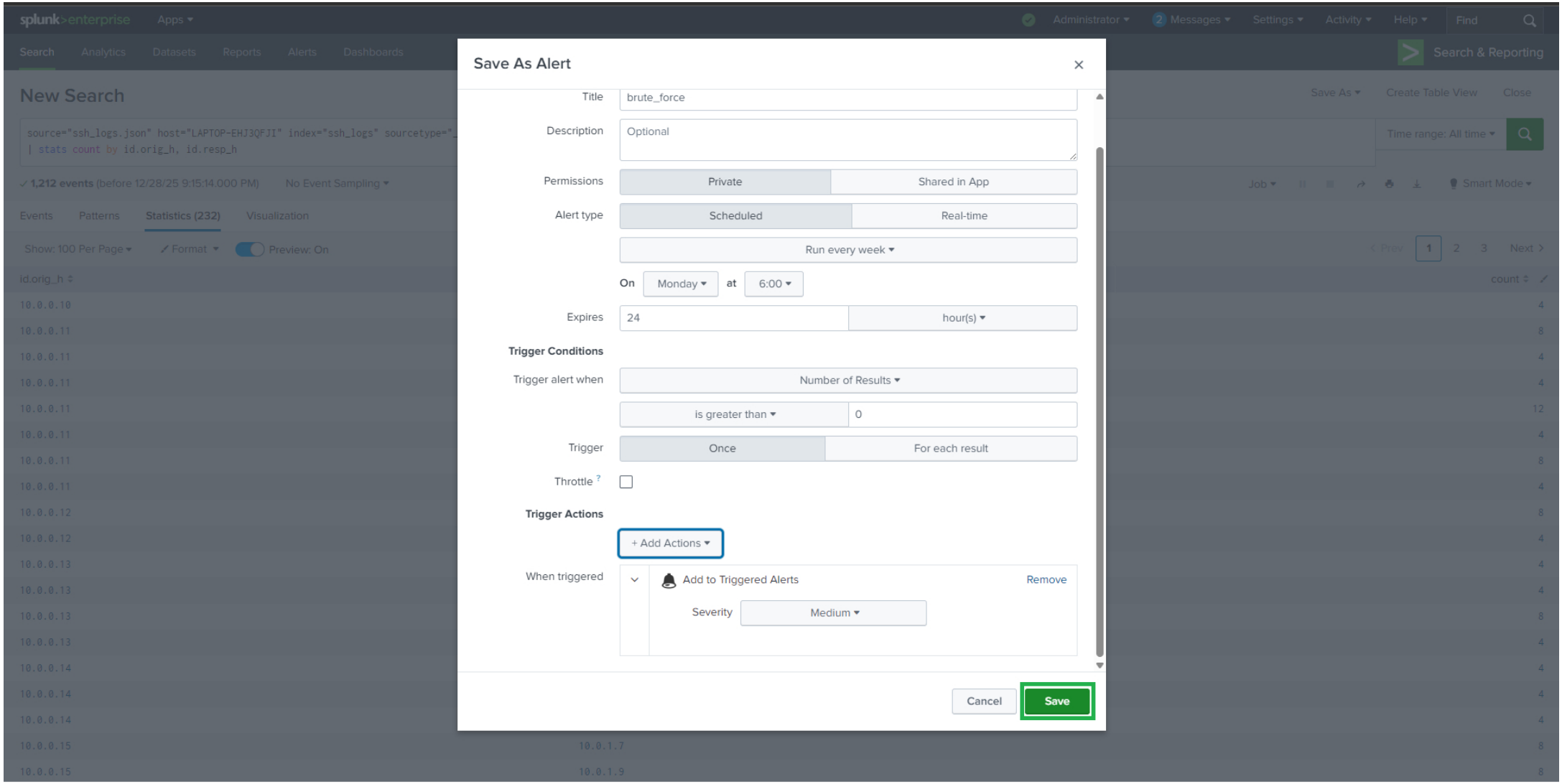


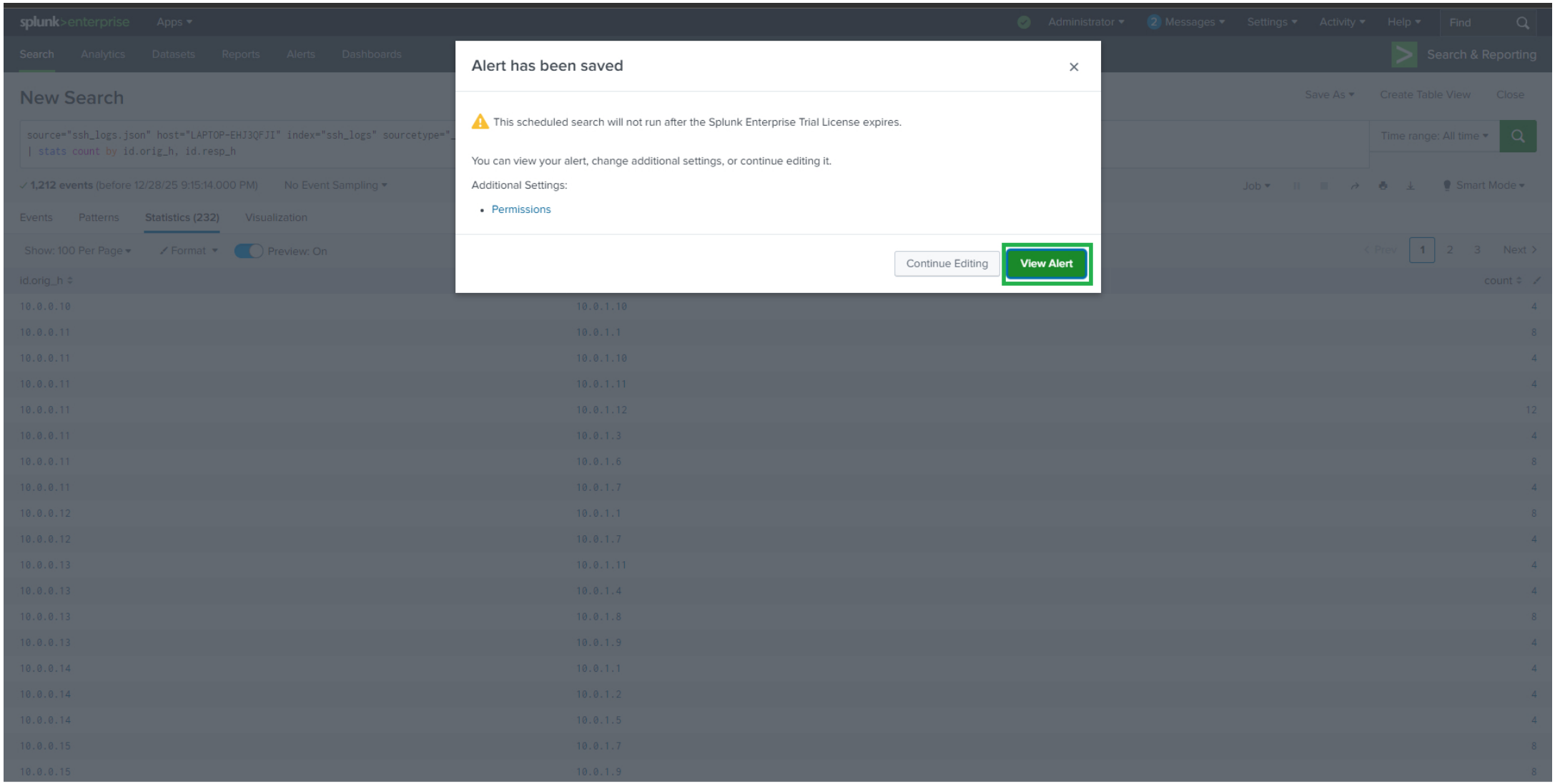
id.orig_h	id.resp_h	count
10.0.0.10	10.0.1.10	4
10.0.0.11	10.0.1.1	8
10.0.0.11	10.0.1.10	4
10.0.0.11	10.0.1.11	4
10.0.0.11	10.0.1.12	12
10.0.0.11	10.0.1.3	4
10.0.0.11	10.0.1.6	8
10.0.0.11	10.0.1.7	4
10.0.0.12	10.0.1.1	8
10.0.0.12	10.0.1.7	4
10.0.0.13	10.0.1.11	4
10.0.0.13	10.0.1.4	4
10.0.0.13	10.0.1.8	8
10.0.0.13	10.0.1.9	4
10.0.0.14	10.0.1.1	4
10.0.0.14	10.0.1.2	4
10.0.0.14	10.0.1.5	4
10.0.0.15	10.0.1.7	8
10.0.0.15	10.0.1.9	8

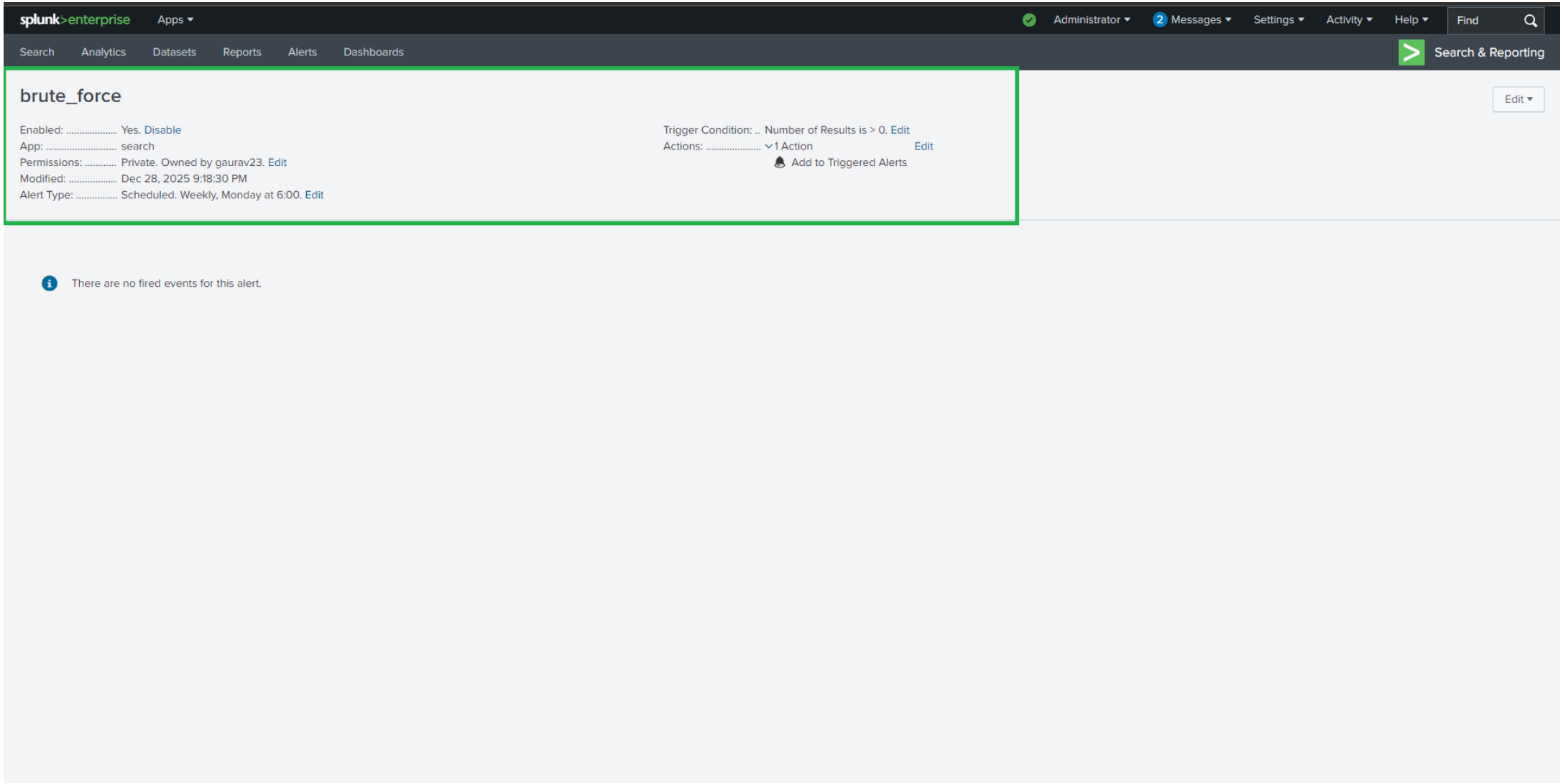

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Multiple Failed Authentication Attempts"
| stats count by id.orig_h, id.resp_h
Report
Alert
Existing Dashboard
New Dashboard
Event Type
e range: All time
✓ 1,212 events (before 12/28/25 9:15:14.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (232)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
id.resp_h
count
10.0.0.10 10.0.1.10 4
10.0.0.11 10.0.1.1 8
10.0.0.11 10.0.1.10 4
10.0.0.11 10.0.1.11 4
10.0.0.11 10.0.1.12 12
10.0.0.11 10.0.1.3 4
10.0.0.11 10.0.1.6 8
10.0.0.11 10.0.1.7 4
10.0.0.12 10.0.1.1 8
10.0.0.12 10.0.1.7 4
10.0.0.13 10.0.1.11 4
10.0.0.13 10.0.1.4 4
10.0.0.13 10.0.1.8 8
10.0.0.13 10.0.1.9 4
10.0.0.14 10.0.1.1 4
10.0.0.14 10.0.1.2 4
10.0.0.14 10.0.1.5 4
10.0.0.15 10.0.1.7 8
127.0.0.1:8000/en-US/app/search/search?q=search source%3D"ssh_logs.json" host%3D"LAPTOP-EHJ3QFJI" index%3D"ssh_logs" sourcetype%3D"_json" event_type%3D"Multiple Failed Authentication Attempts"%0A%7C stats count by id.orig_h%2C id.resp_h&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool...

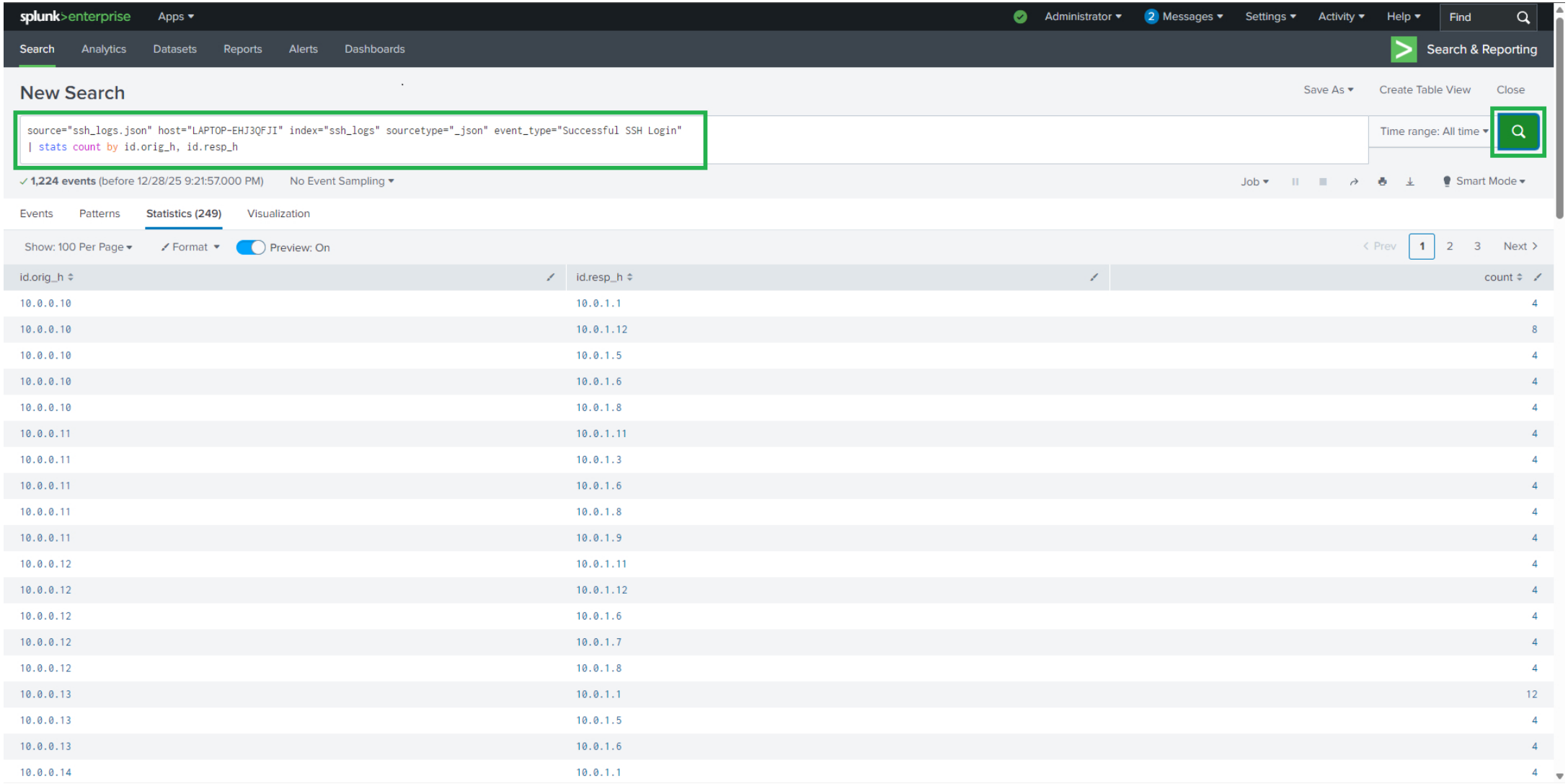

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_
| stats count by id.orig_h, id.resp_h
Time range: All time
1,212 events (before 12/28/25 9:15:14.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (232)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
count
10.0.0.10
10.0.0.11
10.0.0.12
10.0.0.13
10.0.0.14
10.0.0.15
10.0.1.2
10.0.1.5
10.0.1.7
10.0.1.9
Save As Alert
Settings
Title
Title
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
Cancel
Save

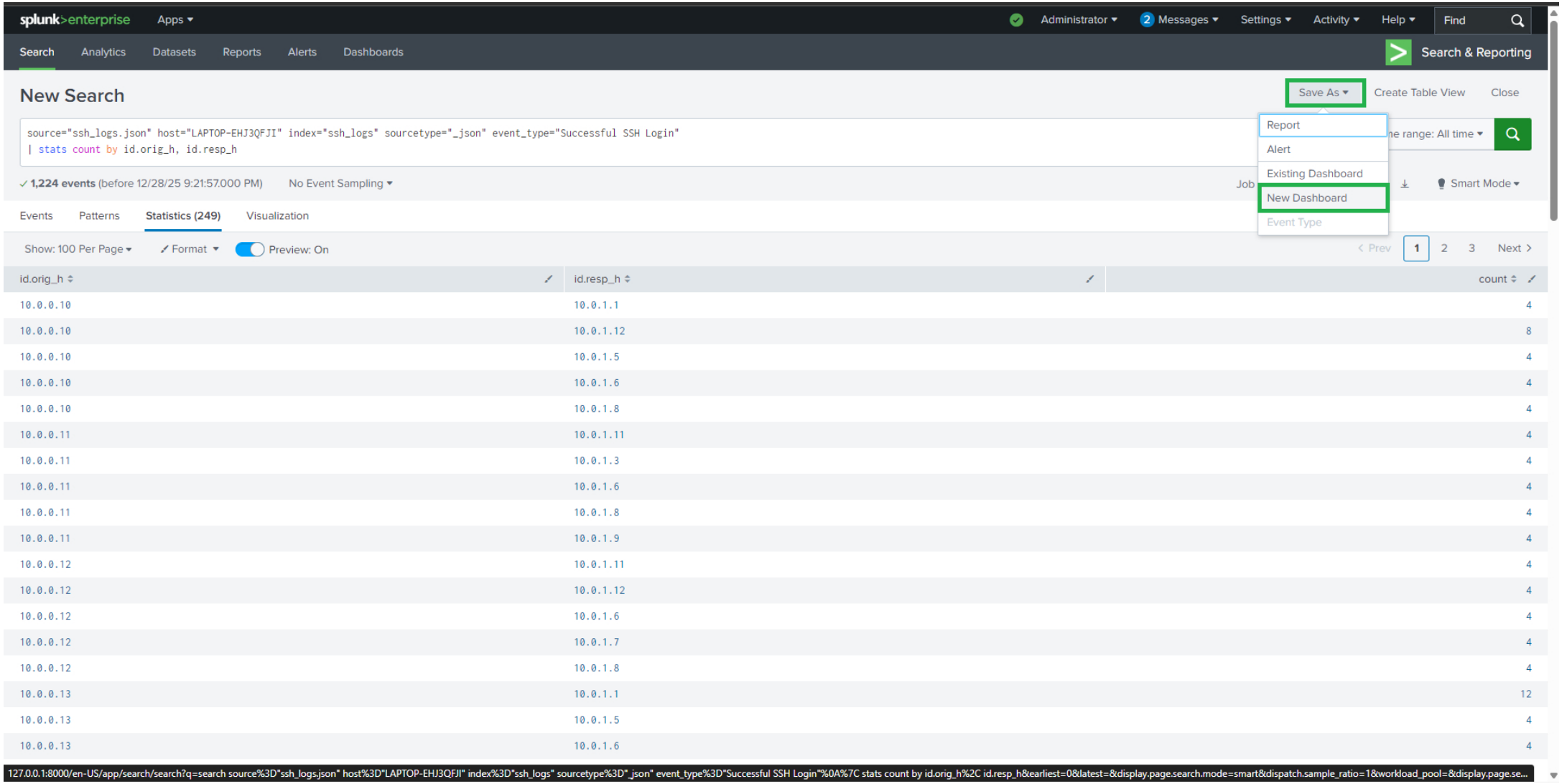

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_
| stats count by id.orig_h, id.resp_h
Time range: All time
1,212 events (before 12/28/25 9:15:14.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (232)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
count
10.0.0.10
10.0.0.11
10.0.0.12
10.0.0.13
10.0.0.14
10.0.0.15
10.0.1.2
10.0.1.5
10.0.1.7
Save As Alert
Settings
Title
brute_force
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
hour(s)
Add to Triggered Alerts
Add this alert to Triggered Alerts list
Dashboard Studio Snapshot
Create a snapshot of a Dashboard Studio dashboard
Log Event
Send log event to Splunk receiver endpoint
Output results to lookup
Output the results of the search to a CSV lookup file
Output results to telemetry endpoint
Custom action to output results to telemetry endpoint
Run a script
Number of Results
0
For each result
+ Add Actions
Cancel
Save
127.0.0.1:8000/en-US/app/search/search?q=search source%3D"ssh_logs.json" host%3D"LAPTOP-EHJ3QFJI" index%3D"ssh_logs" sourcetype%3D"_json" event_type%3D"Multiple Failed Authentication Attempts"%0A%7C stats count by id.orig_h%2C id.resp_h&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool...

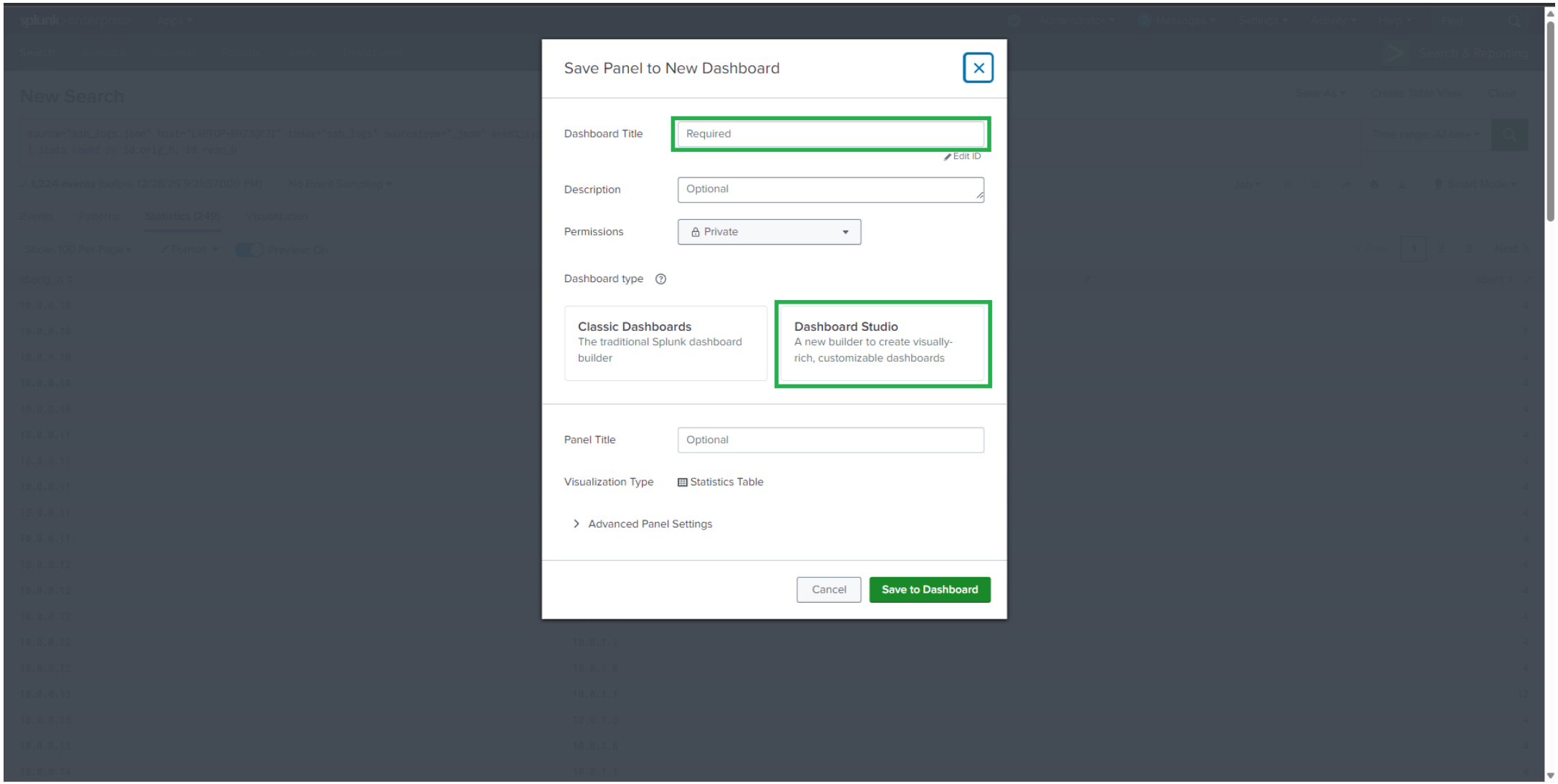

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_
| stats count by id.orig_h, id.resp_h
Time range: All time
1,212 events (before 12/28/25 9:15:14.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (232)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
count
10.0.0.10
10.0.0.11
10.0.0.12
10.0.0.13
10.0.0.14
10.0.0.15
10.0.1.7
10.0.1.9
Save As Alert
Title
brute_force
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Add to Triggered Alerts
Remove
Severity
Medium
Cancel
Save

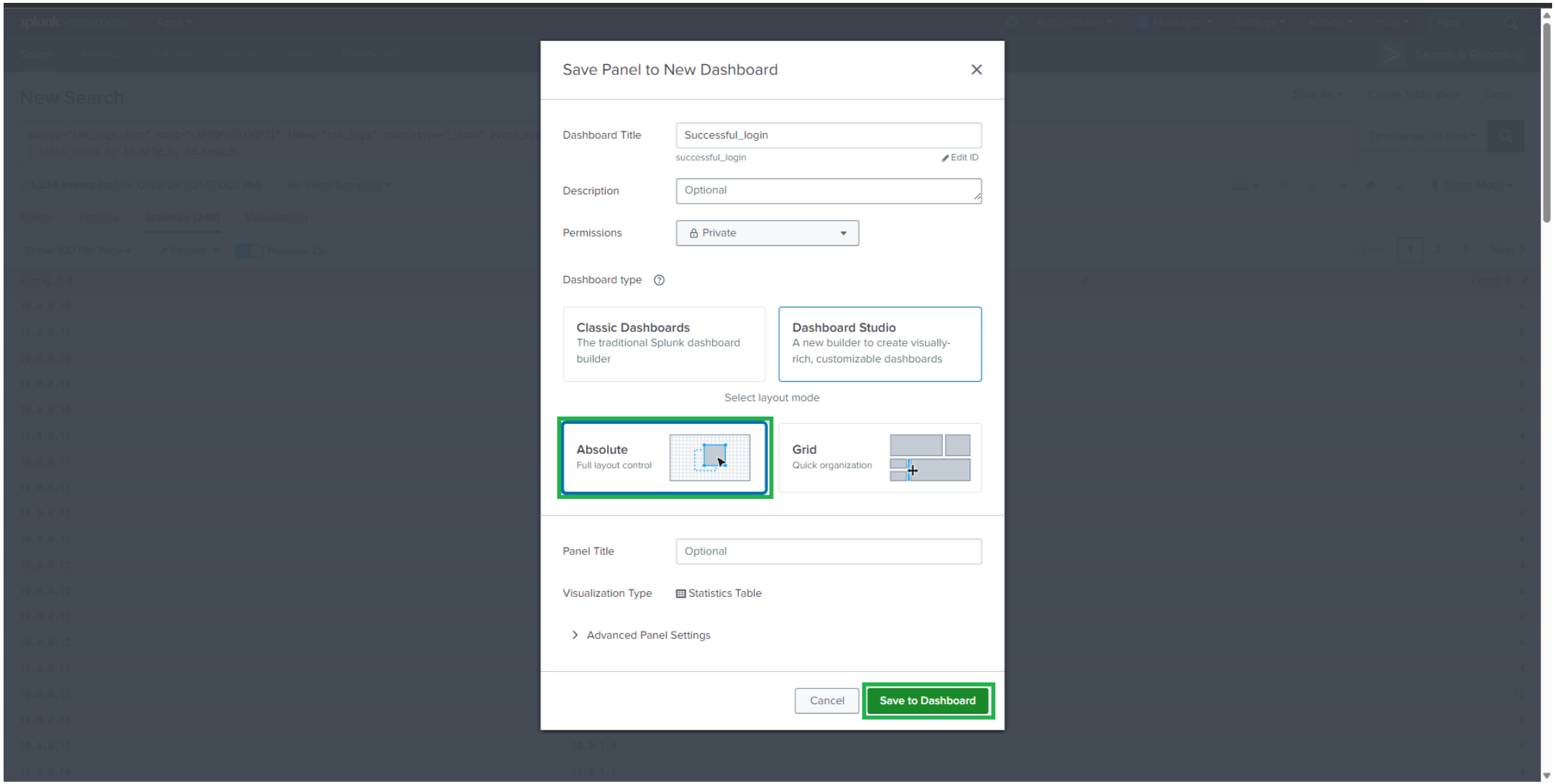

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_
| stats count by id.orig_h, id.resp_h
Time range: All time
1,212 events (before 12/28/25 9:15:14.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (232)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
count
10.0.0.10 10.0.1.10 4
10.0.0.11 10.0.1.1 8
10.0.0.11 10.0.1.10 4
10.0.0.11 10.0.1.11 4
10.0.0.11 10.0.1.12 12
10.0.0.11 10.0.1.3 4
10.0.0.11 10.0.1.6 8
10.0.0.11 10.0.1.7 4
10.0.0.12 10.0.1.1 8
10.0.0.12 10.0.1.7 4
10.0.0.13 10.0.1.11 4
10.0.0.13 10.0.1.4 4
10.0.0.13 10.0.1.8 8
10.0.0.13 10.0.1.9 4
10.0.0.14 10.0.1.1 4
10.0.0.14 10.0.1.2 4
10.0.0.14 10.0.1.5 4
10.0.0.15 10.0.1.7 8
10.0.0.15 10.0.1.9 8
Alert has been saved
This scheduled search will not run after the Splunk Enterprise Trial License expires.
You can view your alert, change additional settings, or continue editing it.
Additional Settings:
Permissions
Continue Editing
View Alert

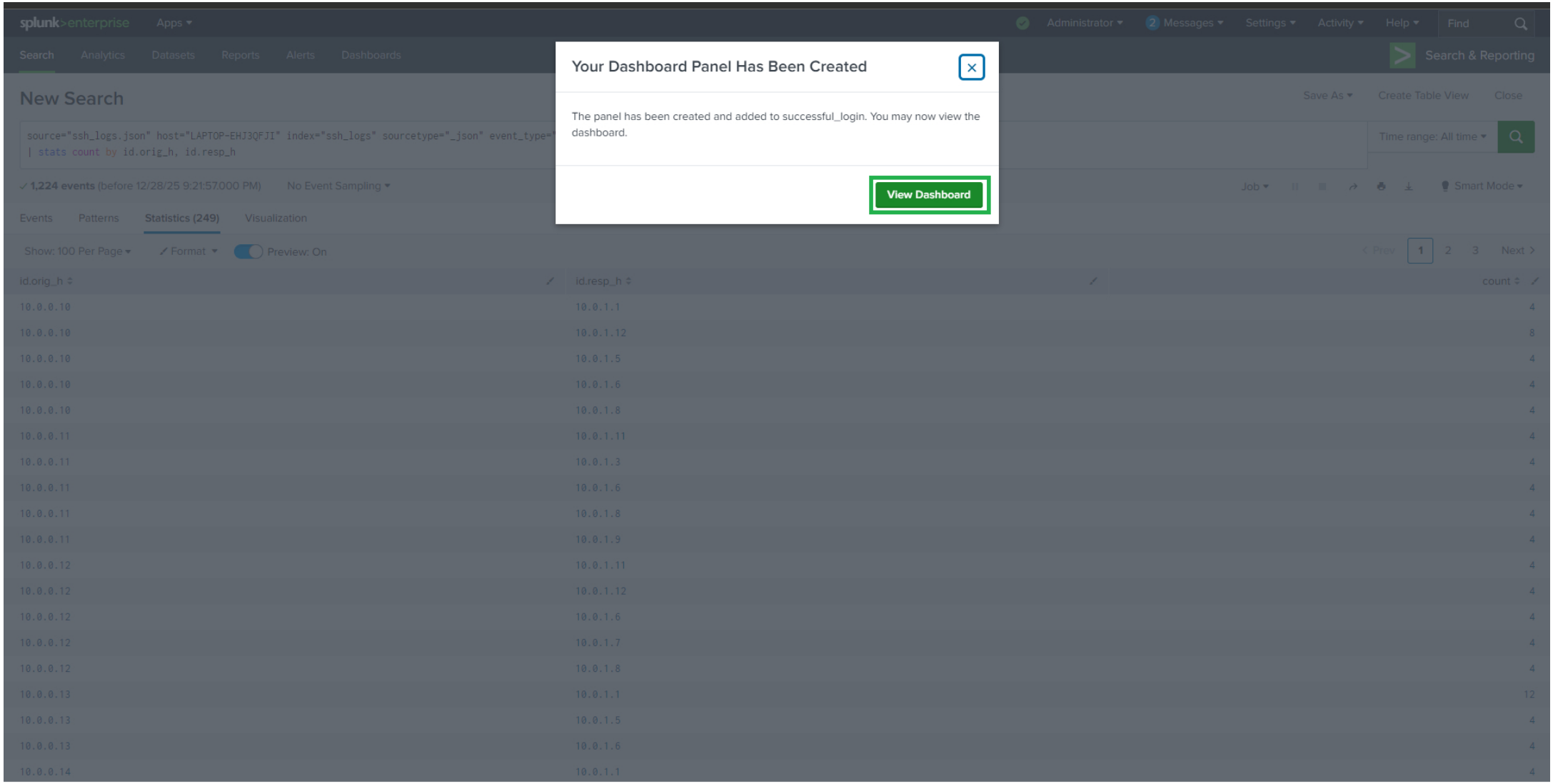

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
brute_force
Edit
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by gaurav23. Edit
Modified: Dec 28, 2025 9:18:30 PM
Alert Type: Scheduled. Weekly, Monday at 6:00. Edit
Trigger Condition: Number of Results is > 0. Edit
Actions: 1 Action Edit
Add to Triggered Alerts
There are no fired events for this alert.

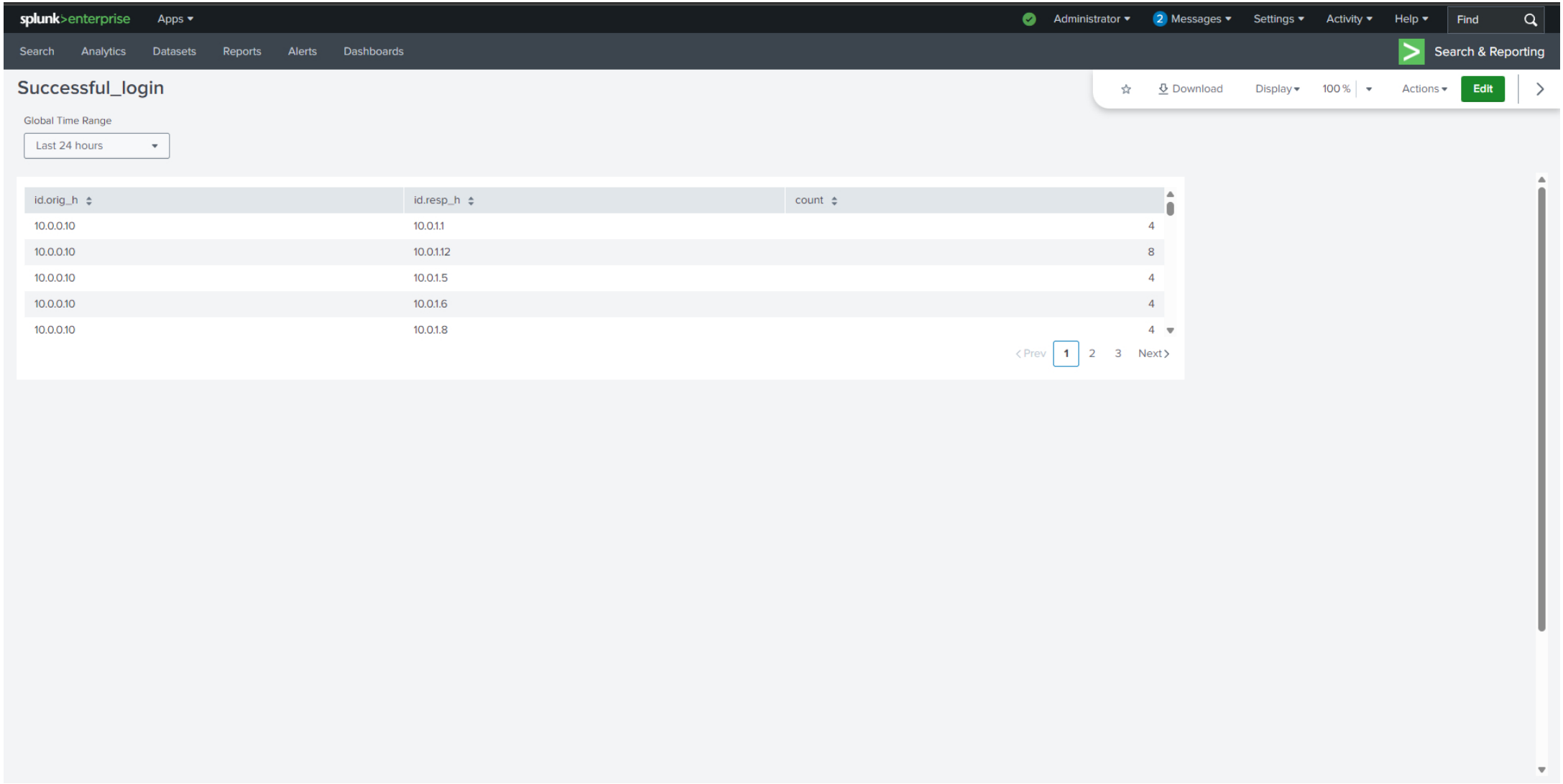

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Successful SSH Login"
| stats count by id.orig_h, id.resp_h
Time range: All time
1,224 events (before 12/28/25 9:21:57.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (249)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
id.resp_h
count
10.0.0.10 10.0.1.1 4
10.0.0.10 10.0.1.12 8
10.0.0.10 10.0.1.5 4
10.0.0.10 10.0.1.6 4
10.0.0.10 10.0.1.8 4
10.0.0.11 10.0.1.11 4
10.0.0.11 10.0.1.3 4
10.0.0.11 10.0.1.6 4
10.0.0.11 10.0.1.8 4
10.0.0.11 10.0.1.9 4
10.0.0.12 10.0.1.11 4
10.0.0.12 10.0.1.12 4
10.0.0.12 10.0.1.6 4
10.0.0.12 10.0.1.7 4
10.0.0.12 10.0.1.8 4
10.0.0.13 10.0.1.1 12
10.0.0.13 10.0.1.5 4
10.0.0.13 10.0.1.6 4
10.0.0.14 10.0.1.1 4

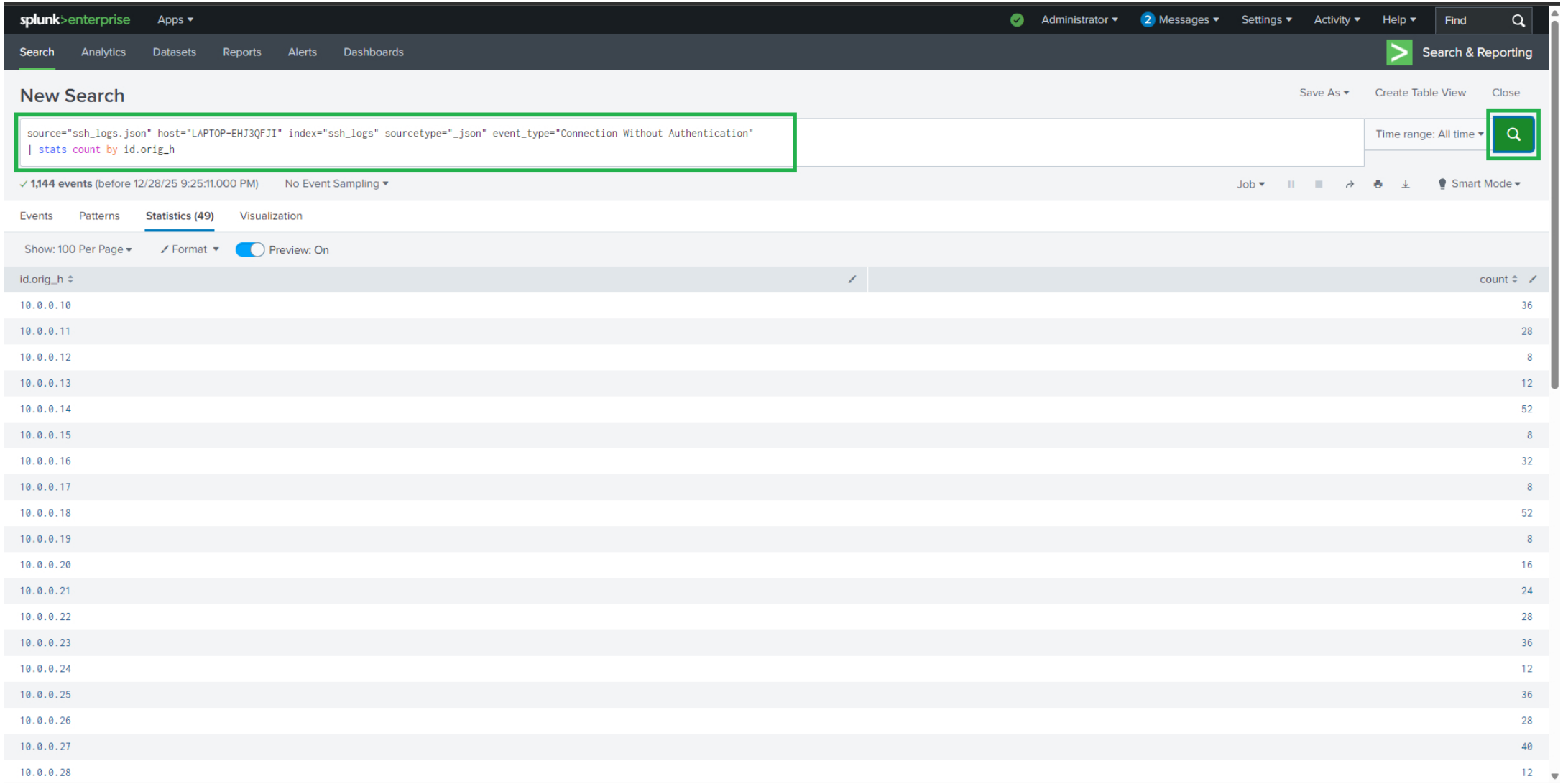

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Successful SSH Login"
| stats count by id.orig_h, id.resp_h
Report
Alert
Existing Dashboard
New Dashboard
Event Type
1,224 events (before 12/28/25 9:21:57.000 PM)
No Event Sampling
Smart Mode
Events
Patterns
Statistics (249)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
id.orig_h
id.resp_h
count
10.0.0.10 10.0.1.1 4
10.0.0.10 10.0.1.12 8
10.0.0.10 10.0.1.5 4
10.0.0.10 10.0.1.6 4
10.0.0.10 10.0.1.8 4
10.0.0.11 10.0.1.11 4
10.0.0.11 10.0.1.3 4
10.0.0.11 10.0.1.6 4
10.0.0.11 10.0.1.8 4
10.0.0.11 10.0.1.9 4
10.0.0.12 10.0.1.11 4
10.0.0.12 10.0.1.12 4
10.0.0.12 10.0.1.6 4
10.0.0.12 10.0.1.7 4
10.0.0.12 10.0.1.8 4
10.0.0.13 10.0.1.1 12
10.0.0.13 10.0.1.5 4
10.0.0.13 10.0.1.6 4
127.0.0.1:8000/en-US/app/search/search?q=search source%3D"ssh_logs.json" host%3D"LAPTOP-EHJ3QFJI" index%3D"ssh_logs" sourcetype%3D"_json" event_type%3D"Successful SSH Login"%0A%7C stats count by id.orig_h%2C id.resp_h&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&display.page.se...

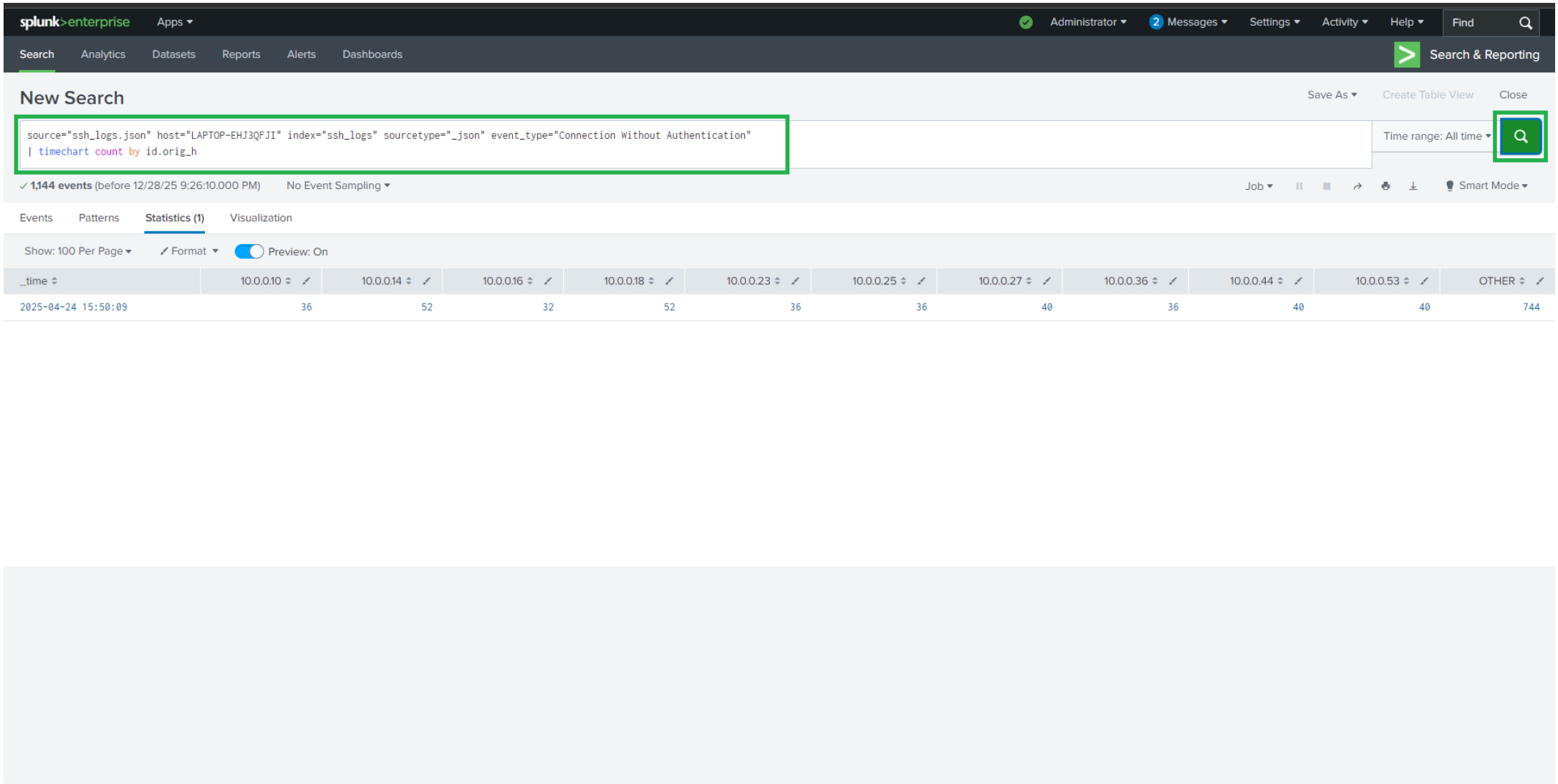

Save Panel to New Dashboard
Dashboard Title
Required
Edit ID
Description
Optional
Permissions
Private
Dashboard type
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
A new builder to create visually-rich, customizable dashboards
Panel Title
Optional
Visualization Type
Statistics Table
Advanced Panel Settings
Cancel
Save to Dashboard


Save Panel to New Dashboard
Dashboard Title
Successful_login
successful_login
Edit ID
Description
Optional
Permissions
Private
Dashboard type
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
A new builder to create visually-rich, customizable dashboards
Select layout mode
Absolute
Full layout control
Grid
Quick organization
Panel Title
Optional
Visualization Type
Statistics Table
Advanced Panel Settings
Cancel
Save to Dashboard


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="
| stats count by id.orig_h, id.resp_h
Time range: All time
✓ 1,224 events (before 12/28/25 9:21:57.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (249)
Visualization
Show: 100 Per Page
Format
Preview: On
Prev
1
2
3
Next
Your Dashboard Panel Has Been Created
The panel has been created and added to successful_login. You may now view the dashboard.
View Dashboard
id.orig_h
id.resp_h
count
10.0.0.10 10.0.1.1 4
10.0.0.10 10.0.1.12 8
10.0.0.10 10.0.1.5 4
10.0.0.10 10.0.1.6 4
10.0.0.10 10.0.1.8 4
10.0.0.11 10.0.1.11 4
10.0.0.11 10.0.1.3 4
10.0.0.11 10.0.1.6 4
10.0.0.11 10.0.1.8 4
10.0.0.11 10.0.1.9 4
10.0.0.12 10.0.1.11 4
10.0.0.12 10.0.1.12 4
10.0.0.12 10.0.1.6 4
10.0.0.12 10.0.1.7 4
10.0.0.12 10.0.1.8 4
10.0.0.13 10.0.1.1 12
10.0.0.13 10.0.1.5 4
10.0.0.13 10.0.1.6 4
10.0.0.14 10.0.1.1 4


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Successful_login
Download
Display
100 %
Actions
Edit
Global Time Range
Last 24 hours
id.orig_h
id.resp_h
count
10.0.0.10 10.0.1.1 4
10.0.0.10 10.0.1.12 8
10.0.0.10 10.0.1.5 4
10.0.0.10 10.0.1.6 4
10.0.0.10 10.0.1.8 4
Prev
1
2
3
Next


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Connection Without Authentication"
| stats count by id.orig_h
Time range: All time
✓ 1,144 events (before 12/28/25 9:25:11.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (49)
Visualization
Show: 100 Per Page
Format
Preview: On
id.orig_h
count
10.0.0.10 36
10.0.0.11 28
10.0.0.12 8
10.0.0.13 12
10.0.0.14 52
10.0.0.15 8
10.0.0.16 32
10.0.0.17 8
10.0.0.18 52
10.0.0.19 8
10.0.0.20 16
10.0.0.21 24
10.0.0.22 28
10.0.0.23 36
10.0.0.24 12
10.0.0.25 36
10.0.0.26 28
10.0.0.27 40
10.0.0.28 12


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="_json" event_type="Connection Without Authentication"
| timechart count by id.orig_h
Time range: All time
✓ 1,144 events (before 12/28/25 9:26:10.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
Show: 100 Per Page
Format
Preview: On
_time
10.0.0.10
10.0.0.14
10.0.0.16
10.0.0.18
10.0.0.23
10.0.0.25
10.0.0.27
10.0.0.36
10.0.0.44
10.0.0.53
OTHER
2025-04-24 15:50:09
36
52
32
52
36
36
40
36
40
40
744