

Integrate SSH Jump server with splunk for SIEM

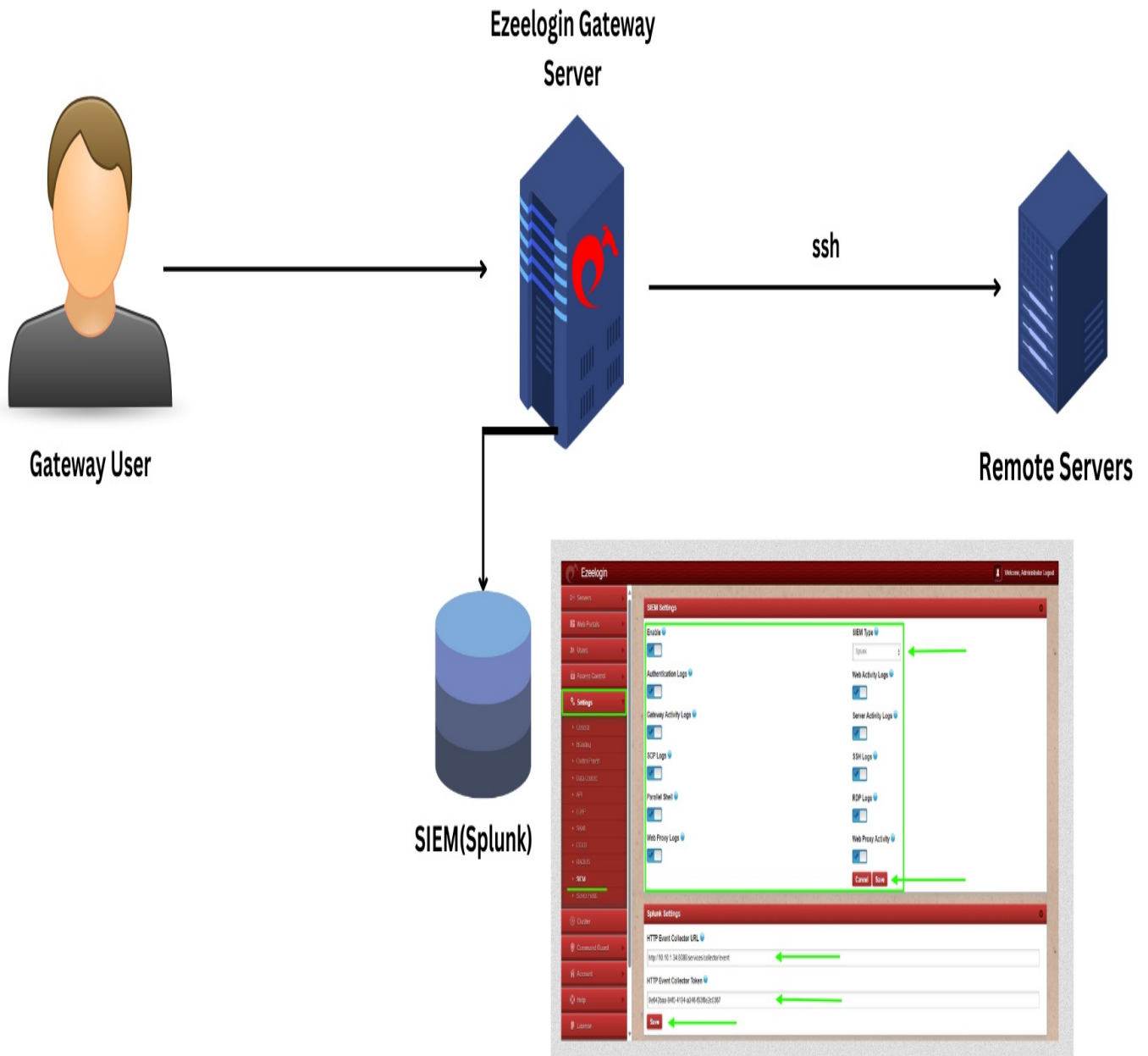
📄 652 👤 Manu Chacko 📅 May 14, 2025 📁 [Features & Functionalities](#)

👁 10173

How to forward SSH Jump Server logs to Splunk?

Overview: This article explains how to configure Splunk HTTP Event Collector (HEC) to forward Ezeelogin SSH Jump Server logs for real-time monitoring and analysis.

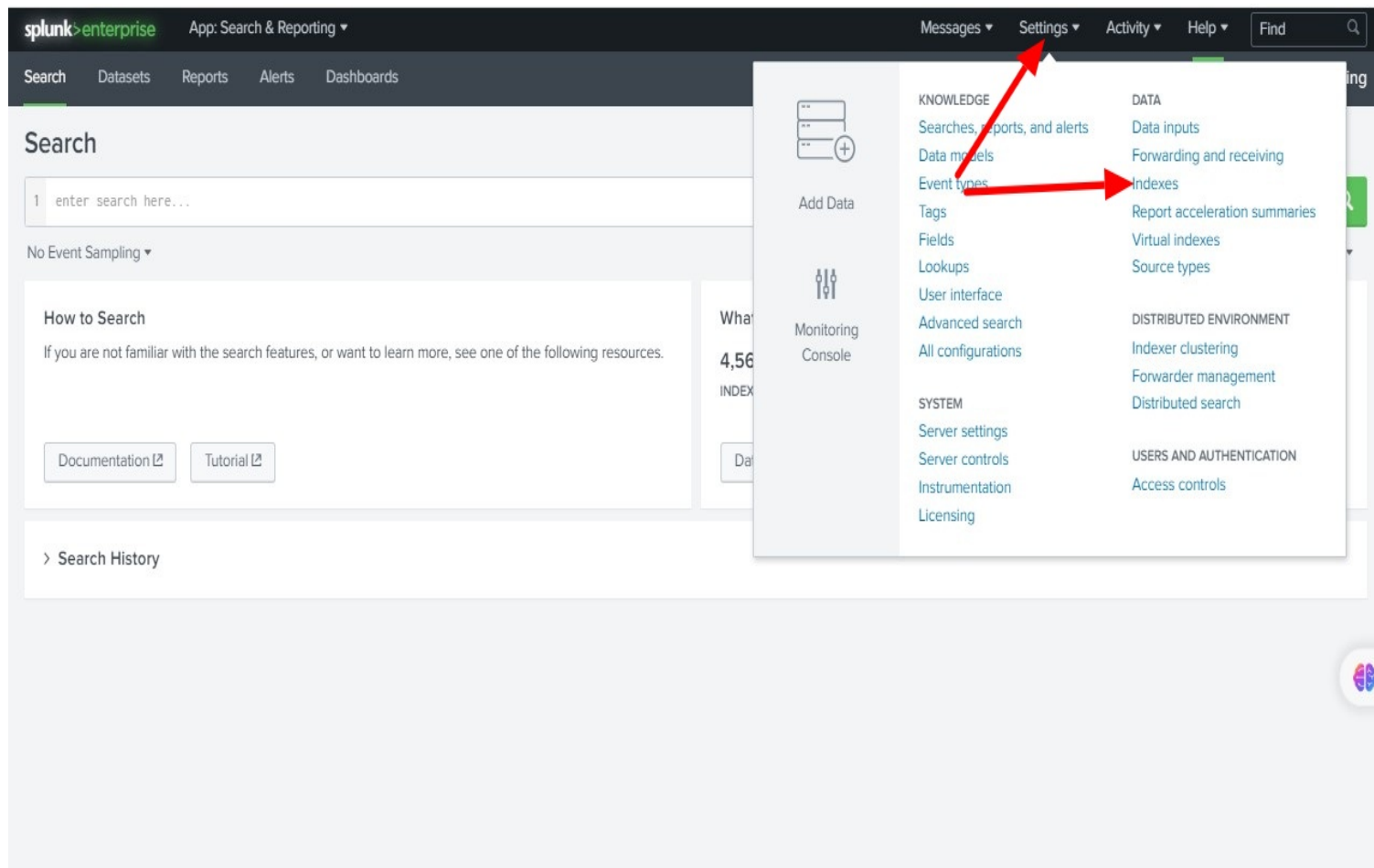
Splunk is a software platform designed for searching, monitoring, and analyzing machine-generated data in real time. It provides insights into various data sources, including logs, events, and metrics, allowing organizations to gain information and troubleshoot efficiently. Splunk is widely used for log management, security information and event management (SIEM), and business analytics.



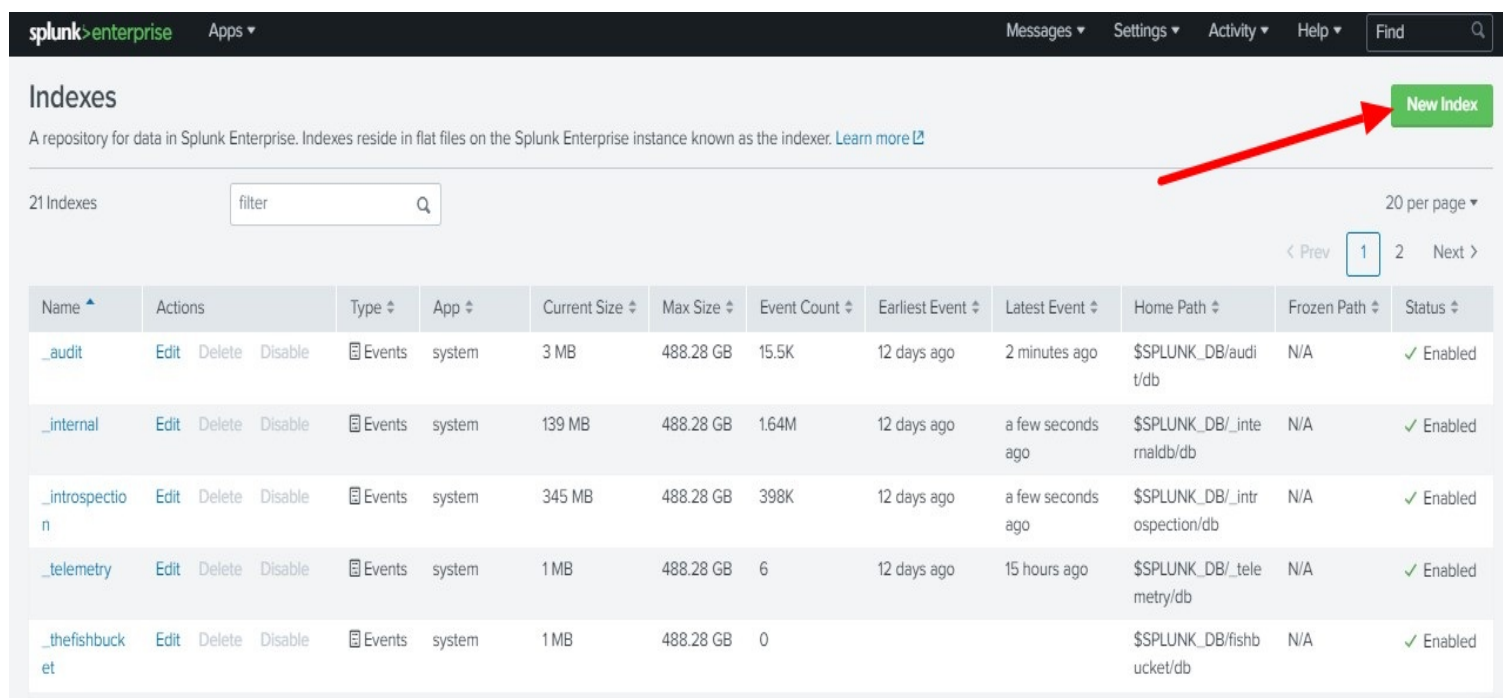
We are configuring Splunk HTTP Event Collector (HEC) which allows Ezeelogin logs to be streamed to Splunk

Step 1: Log in to **Splunk** and refer to the steps to create an index for Ezeelogin.

Click on **Settings -> Indexes**



Step 2: Click on **New Index** to create a new index.



Step 3: Enter the Index Name and Save it. We need to add the following indexes for streaming Ezeelogin Logs

authlog

ezsh_activity

sshlogs

web_activity

server_activity

parallel_shell

rdplogs

web_proxy

web_proxy_activity

scplogs

Add all the above indexes one by one as follows.

Indexes
A repository for data in Splunk Enterprise. Indexes

21 Indexes

Name	Actions
_audit	Edit Delete Disable
_internal	Edit Delete Disable
_introspection	Edit Delete Disable
_telemetry	Edit Delete Disable
_thefishbucket	Edit Delete Disable
authlog	Edit Delete Disable
ez	Edit Delete Disable
ezsh_activity	Edit Delete Disable
hec	Edit Delete Disable
history	Edit Delete Disable
main	Edit Delete Disable
parallel_shell	Edit Delete Disable

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

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

Thawed Path
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 GB
Maximum target size of entire index.

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

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

Step 4: Create **HTTP Event Collector** and enable **Global Settings**

Step 4 A: Click on **Settings -> Data inputs**

splunk>enterpriseApps

MessagesSettingsActivityHelpFind

Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexes.

22 Indexesfilter

Name	Actions	Type	App	Current Size	Max Size	Event Count
_audit	Edit Delete Disable	Events	system	3 MB	488.28 GB	15.5K
_internal	Edit Delete Disable	Events	system	139 MB	488.28 GB	1.64M
_introspection	Edit Delete Disable	Events	system	345 MB	488.28 GB	398K
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	6
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0
authlog	Edit Delete Disable	Events	search	1 MB	500 GB	52
ez	Edit Delete Disable	Events	search	1 MB	500 GB	6
ezsh_activity	Edit Delete Disable	Events	search	1 MB	500 GB	14
hec	Edit Delete Disable	Events	search	1 MB	500 GB	0
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0
indexadd	Edit Delete Disable	Events	search	1 MB	500 GB	0

Add DataMonitoring Console

KNOWLEDGE

Searches, reports, and alertsData modelsEvent typesTagsFieldsLookupsUser interfaceAdvanced searchAll configurations

SYSTEM

Server settingsServer controlsInstrumentationLicensing

DATA

Data inputsForwarding and receivingIndexesReport acceleration summariesVirtual indexesSource types

DISTRIBUTED ENVIRONMENT

Indexer clusteringForwarder managementDistributed search

USERS AND AUTHENTICATION

Access controls

Step 4 B: Click on **HTTP Event Collector**

Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Local inputs

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	6	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	3	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	5	+ Add new

Forwarded inputs

Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	0	+ Add new

Step 4 C: Enable Global Settings

click on **Global Settings**

splunk>enterprise Apps ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

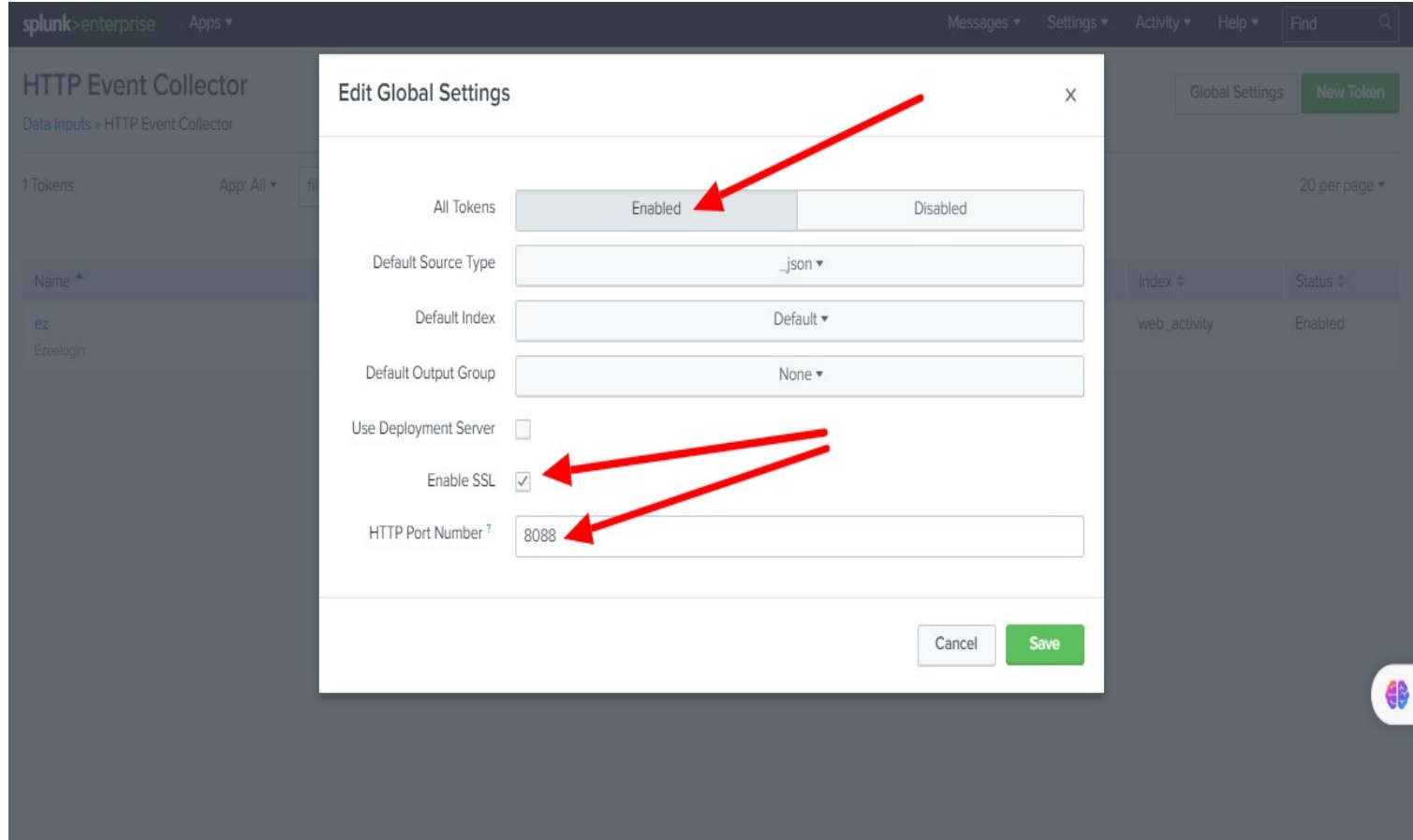
HTTP Event Collector

Data Inputs » HTTP Event Collector

1 Tokens App: All ▾ filter 🔍 20 per page ▾

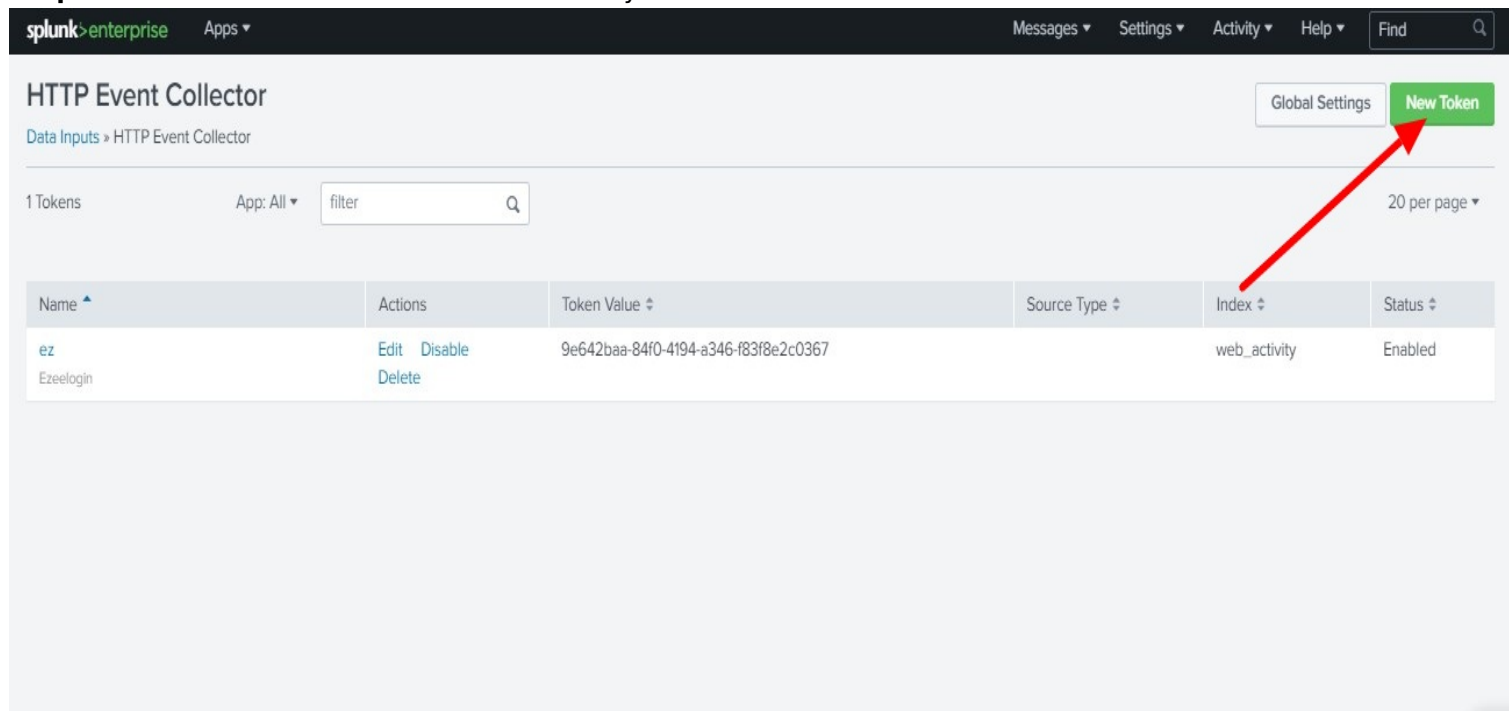
Name ▲	Actions	Token Value ↕	Source Type ↕	Index ↕	Status ↕
ez Ezeelogin	Edit Disable Delete	9e642baa-84f0-4194-a346-f83f8e2c0367		web_activity	Enabled

Step 4 D: Click Enabled -> Enable SSL (optional) -> Specify HTTP Port Number (8088) -> Save



Create HEC Token

Step A: Click on **New Token** to create a security token.



Step B: Enter **Name** (Ezeelogin) -> Description (optional) - > click **Next**

splunk>enterprise Apps Messages Settings Activity Help Find

Add Data Select Source Input Settings Review Done < Back Next >

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

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

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

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

Configure a new token for receiving data over HTTP. [Learn More](#)

Name Ezeelogin

Source name override ? optional

Description ? Ezeelogin logs

Output Group (optional) None

Enable indexer acknowledgement ☐

FAQ

- > What is the HTTP Event Collector?
- > How do I set up the HTTP Event Collector?
- > How do I view and configure the tokens that I can use to send data to the HTTP Event Collector?
- > What clients can send data to the HTTP Event Collector?
- > What port and protocol does the HTTP Event Collector receive data on and how can I change that?
- > What is an output group?

Step C: Select and Add the Indexes which created for Ezeelogin " **authlog, ezsh_activity, sshlogs, web_activity, server_activity, parallel_shell, rdplogs, web_proxy, web_proxy_activity, scplogs** " -> Click **Review**.

Add Data

Select Source Input Settings Review Done

< Back

Review >

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

Automatic Select New

App context

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

App Context

Search & Reporting (search) ▾

Index

Splunk 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](#)

Select Allowed
Indexes

Available item(s)

add all >

main
parallel_shell
rdplogs
scplogs
server_activity

Select indexes that clients will be able to select from.

Default Index

authlog ▾

[Create a new index](#)

Selected item(s)

< remove all

authlog
ezsh_activity
parallel_shell
rdplogs
scnlogs

Step D: Review and make sure that you have selected all the indexes created for Ezeelogin and click **Submit**.

splunk>enterprise Apps Messages Settings Activity Help Find

Add Data Select Source Input Settings Review Done < Back Submit >

Review

Input Type Token
Name Ezeelogin
Source name override N/A
Description Ezeelogin logs
Enable indexer acknowledg..... No
Output Group N/A
Allowed indexes
Default index authlog
Source Type Automatic
App Context search

sshlogs
web_activity
web_proxy
web_proxy_activity
parallel_shell

You can view a success message **"Token has been created successfully."** on the next window. You can find a Token and copy the **Token Value** from the window.

splunk>enterprise Apps Messages Settings Activity Help Find

Add Data Select Source Input Settings Review Done < Back Next >

✓ Token has been created successfully.
Configure your inputs by going to Settings > [Data Inputs](#)

Token Value f2d12883-55c2-4273-b9f5-7c098b9

Start Searching Search your data now or see [examples and tutorials](#). [🔗](#)

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](#). [🔗](#)

You can also view the tokens created from **Settings > Data Inputs > HTTP Event Collector**

splunk>enterprise Apps Messages Settings Activity Help Find

HTTP Event Collector

Data Inputs > HTTP Event Collector

2 Tokens App: All filter 20 per page

Name	Actions	Token Value	Source Type	Index	Status
ez Ezeelogin	Edit Disable Delete	9e642baa-84f0-4194-a346-f83f8e2c0367		web_activity	Enabled
Ezeelogin Ezeelogin logs	Edit Disable Delete	f2d12883-55c2-4273-b9f5-7c098b936b1b		authlog	Enabled

Step 5: Log in to Ezeelogin GUI to configure the Splunk settings in Ezeelogin.

Login to **Ezeelogin GUI > Settings > SIEM > Enable SIEM, Web Activity Logs, Server Activity Logs, SSH Logs, RDP logs, Web Proxy Activity, Authentication Logs, Gateway Activity Logs, SCP Logs, Parallel Shell, Web Proxy Logs > Save.**

Splunk Settings

Add **HTTP Event Collector URL:** **https://mysplunkserver:8088/services/collector/event** (Replace "**mysplunkserver:8088**" with the **URL** and **Port** of your Splunk server)

Add **HTTP Event Collector Token:** **9e642baa-84f0-4194-a346-f83f8e2c0367** (you can find the HTTP Event Collector Token from your Splunk server **Settings > Data Inputs > HTTP Event Collector**)

Ezeelogin Welcome, Administrator Logout

Servers Web Portals Users Access Control Settings General Branding Control Panels Data Centers API LDAP SAML FIDO2 RADIUS SIEM Server Fields Cluster Command Guard Account Help License

SIEM Settings

Enable ☒ SIEM Type Splunk

Authentication Logs ☒ Web Activity Logs ☒

Gateway Activity Logs ☒ Server Activity Logs ☒

SCP Logs ☒ SSH Logs ☒

Parallel Shell ☒ RDP Logs ☒

Web Proxy Logs ☒ Web Proxy Activity ☒

Cancel Save

Splunk Settings

HTTP Event Collector URL

HTTP Event Collector Token

Save

Now you can view the Ezeelogin logs on Splunk.

For example: Ezeelogin Authentication logs can be viewed by searching the **index="authlog"**

splunk>enterprise App: Search & Reporting Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Close

1 index="authlog" during Nov 2023

52 events (11/1/23 12:00:00.000 AM to 12/1/23 12:00:00.000 AM) No Event Sampling Job Fast Mode

Events (52) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 50 Per Page Prev 1 2 Next

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a index 1
- # linecount 1
- a source 1
- a sourcetype 1
- a splunk_server 1

+ Extract New Fields

i	Time	Event
>	11/22/23 12:25:35.000 PM	<pre>{ [-] client_addr: 10.10.1.1 created: 2023-11-22 12:25:35 email: john@jacobs.com expiry: 2023-11-22 14:25:35 id: 52 interface: WEB mode: node: primary nodestate: master reason: server_addr: 10.10.12.3:80 status: success type: logout uid: 0 user_id: 3 usergroup: Admins usergroup_id: 1 username: john }</pre> Show as raw text host = 10.10.134.8088 index = authlog linecount = 1 source = http:ez sourcetype = _json splunk_server = ubuntu
>	11/22/23 12:25:28.000 PM	<pre>{ [-] client_addr: 10.10.1.1 created: 2023-11-22 12:25:28 email: john@jacobs.com expiry: 2023-11-22 14:25:28 id: 51 interface: WEB</pre>

You can create visualizations from the data using the "**Visualization**" feature
Click on **Visualization** then click **Pivot**

splunk>enterprise App: Search & Reporting ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Datasets Reports Alerts Dashboards **Search & Reporting**

New Search

Save As ▾ Close

1 index="ezsh_activity" Previous year 🔍

✓ 38,026 events (Partial results for 1/1/22 12:00:00.000 AM to 1/1/23 12:00:00.000 AM) No Event Sampling ▾ Job ▾ || ▮ ↻ 🖨️ ⬇️ 🔍 Smart Mode ▾

Events (38,026) Patterns Statistics **Visualization**

📘 Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.



Pivot

Build tables and visualizations using multiple fields and metrics without writing searches.



Quick Reports

Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'.

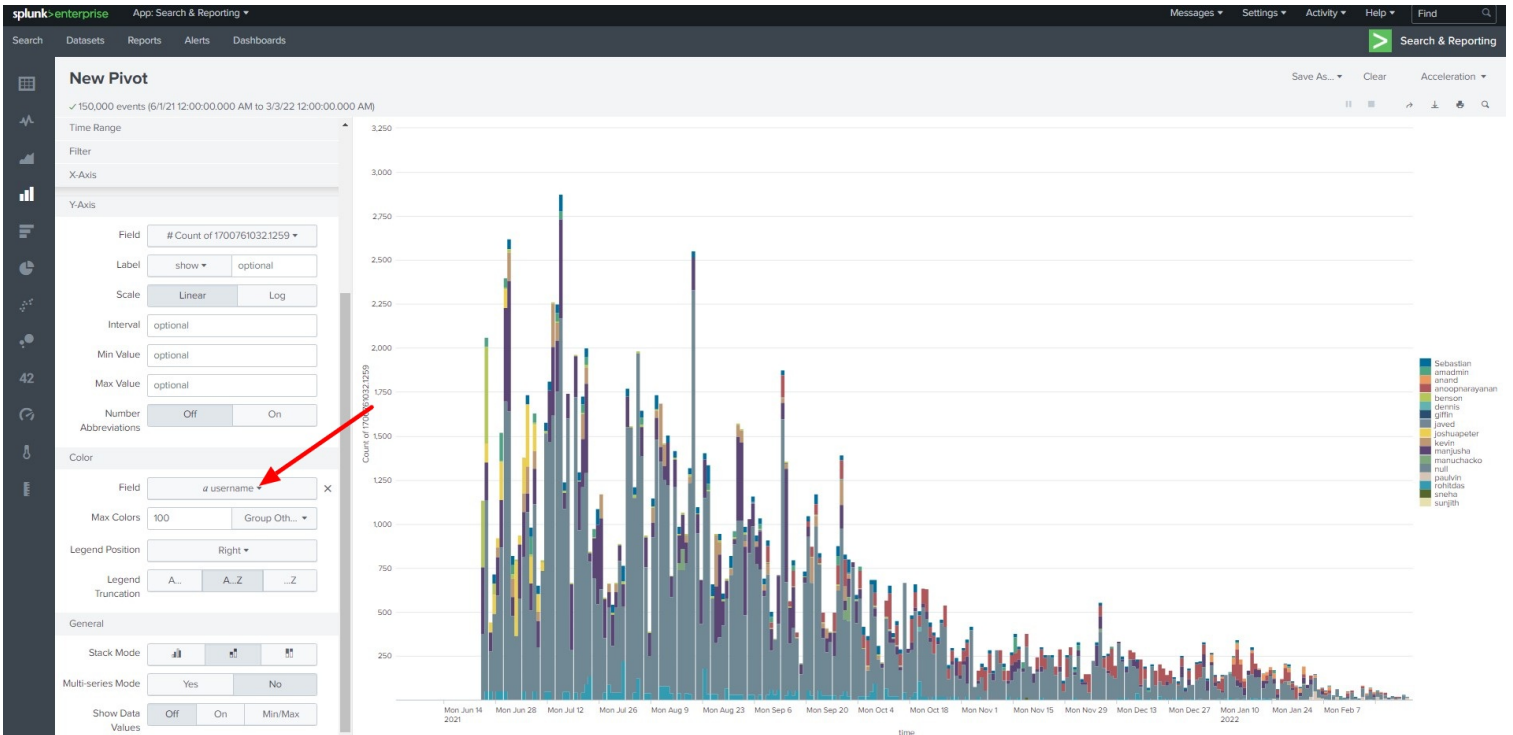


Search Commands

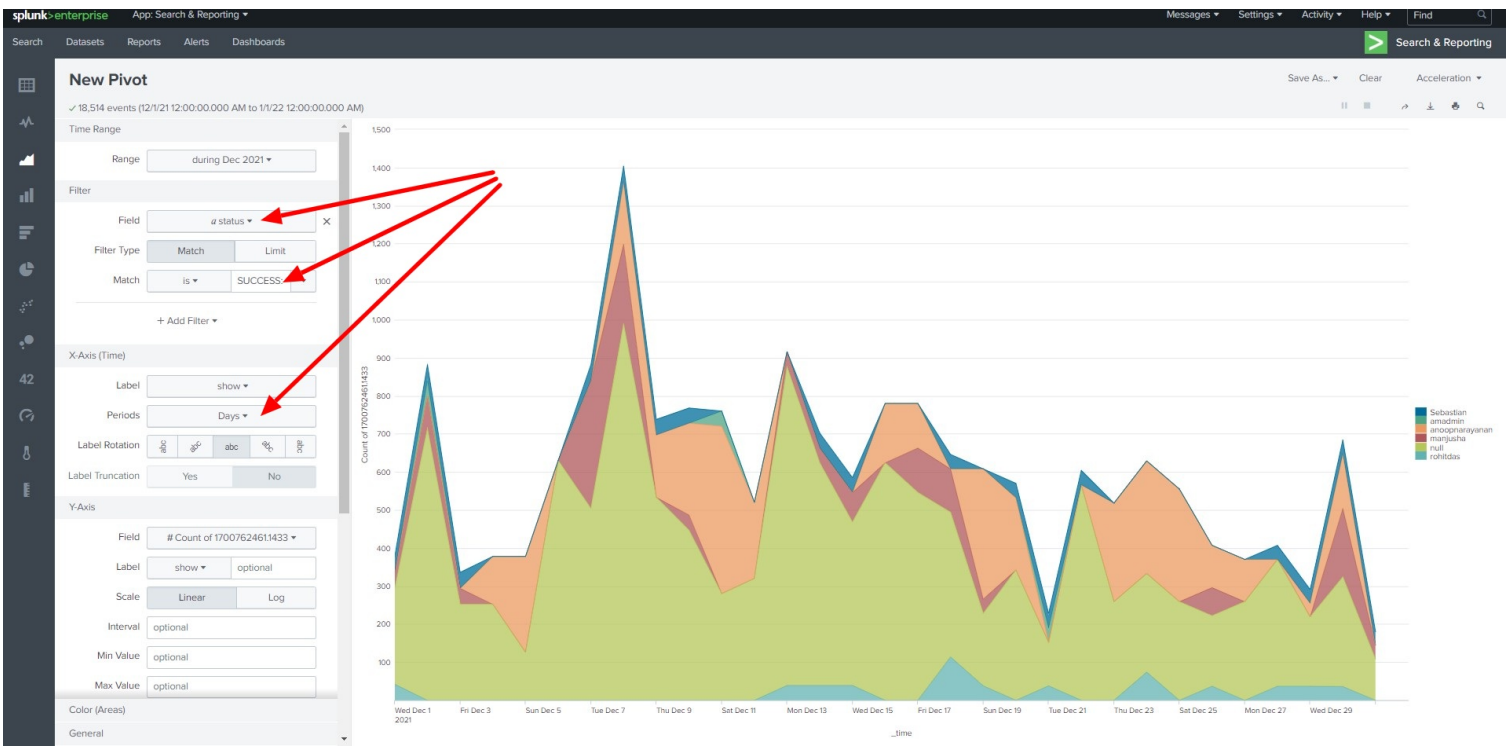
Use a transforming search command, like timechart or stats, to summarize the data.

You can create different types of Visualizations from the data

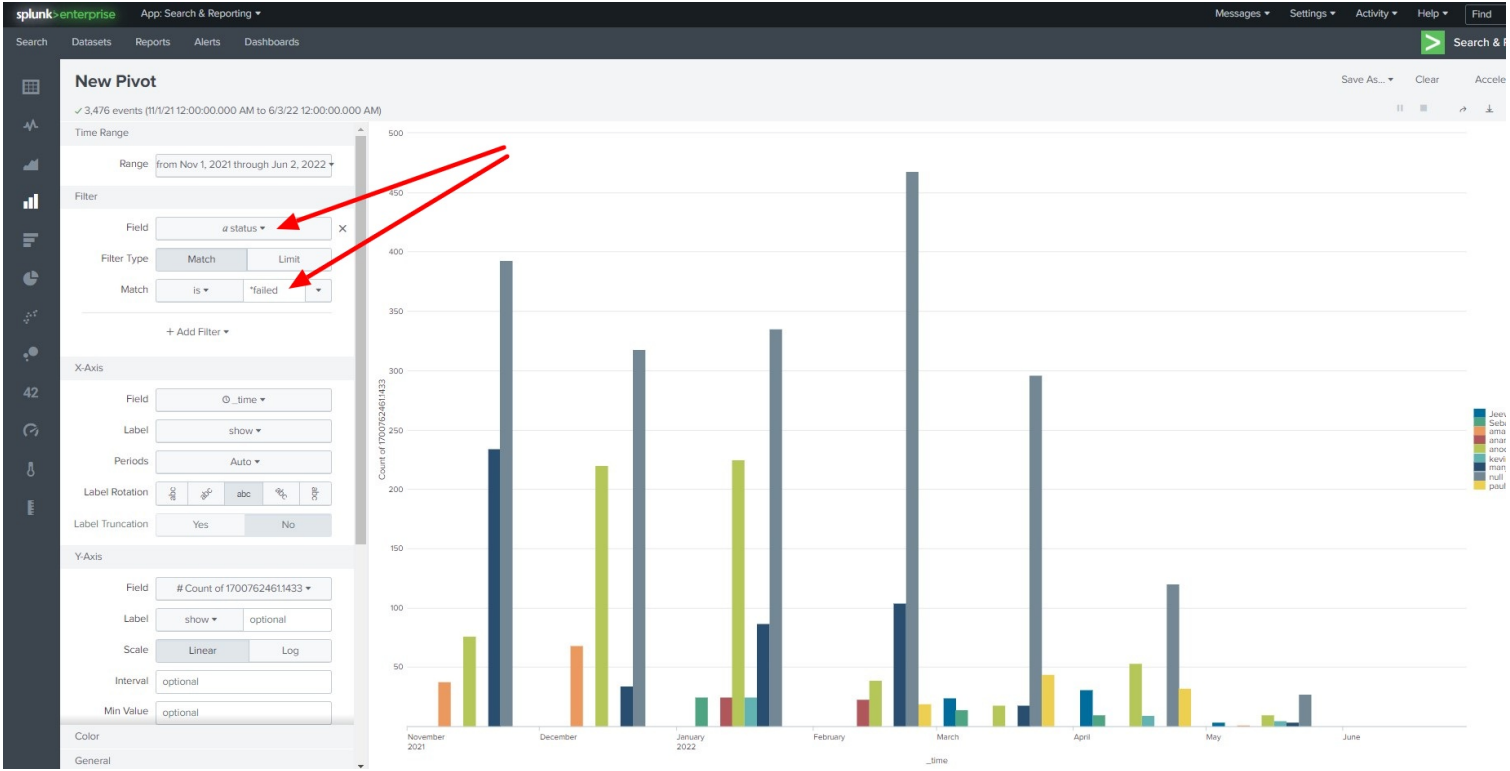
Top user access to Ezeelogin shell



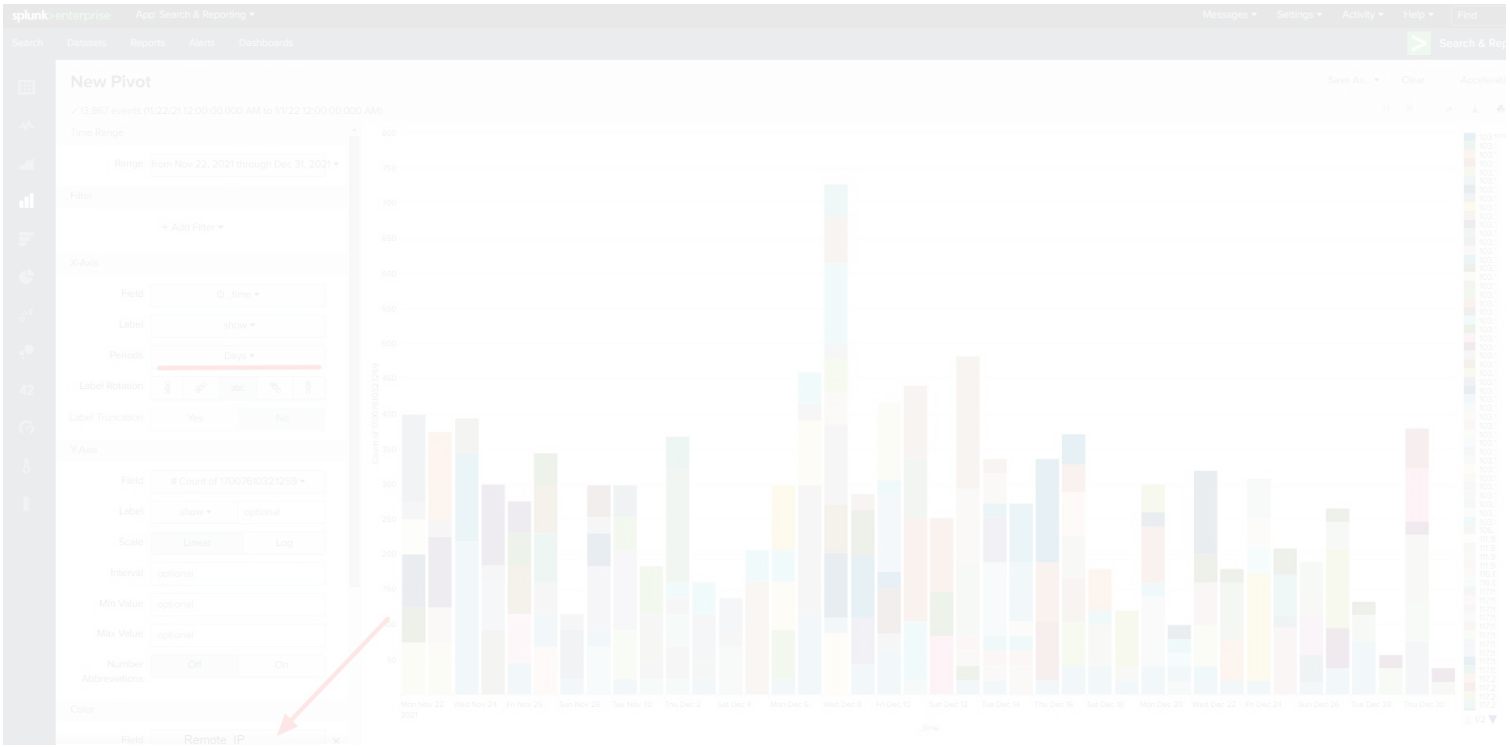
Successful Login attempts to the Ezeelogin gateway per day



Failed Login attempts to the Ezeelogin shell



Top Daily access from IP address



This feature is available from **Ezeelogin version 7.36.1**. Refer the article to **[upgrade Ezeelogin version](#)**.

Related Articles:

[Integrate Ezeelogin SSH Jump host with syslog](#)

[Audit logs and configurations](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-ssh-jump-server-with-splunk-for-siem-652.html>