USER GUIDE
TO
INSTALL AND SET-UP
AUTHENTIC8
SPLUNK ADD-ON

REVISION HISTORY

Version	Date	Author	Summary
1.0	1-Jul-2020	Divya Pandia	Initial Draft

TABLE OF CONTENTS

1. INTRODUCTION

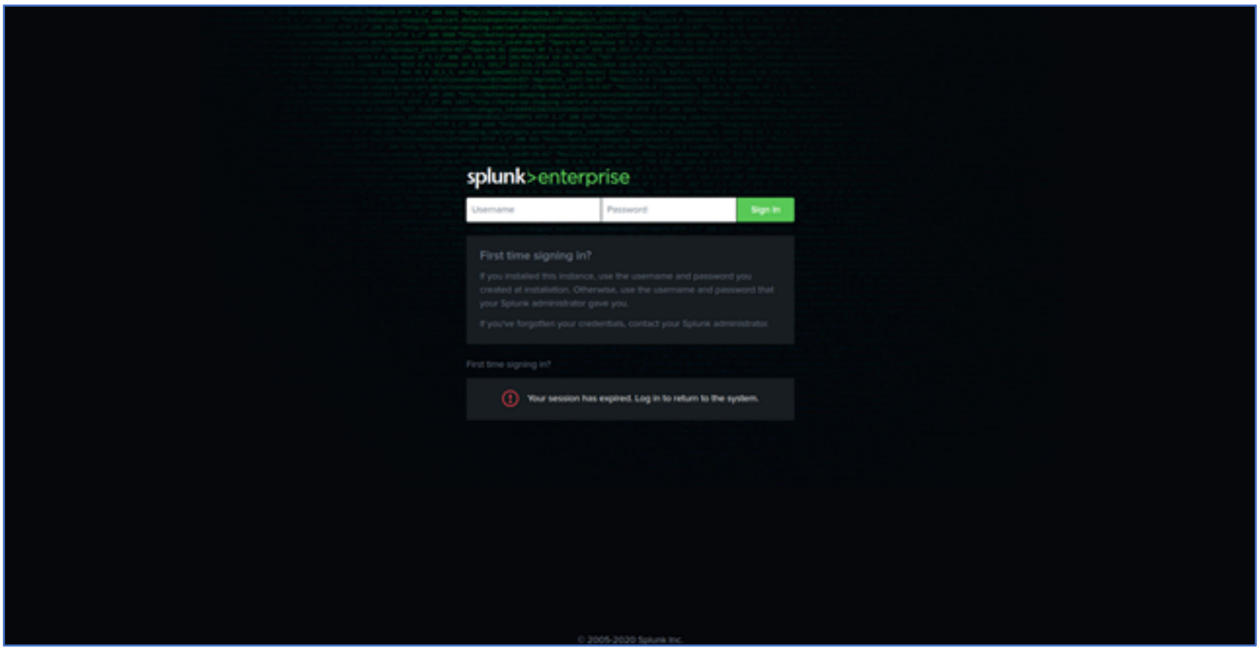
This User Guide is designed to provide documentation for anyone who needs to install and set-up Authentic8 add-on in Splunk. This guide provides you with all the details needed to successfully setup the Splunk Addon on a local Splunk Enterprise 8.x instance and will also provide a quick overview of the Splunk addon.

2. PRE-REQUISITES

2.1 Prior to the install and setup of Splunk Addon of Authenticate8 you will need to have access to an instance Splunk Enterprise 8.x or above as an administrator. Please follow the instructions as provided by Splunk for the installation of Splunk Enterprise 8.x or above.

2.2 To be able to view the CIM visualizations, the CIM package needs to be installed from the following link: https://splunkbase.splunk.com/app/1621/#/overview .

2.3 In order to successfully access Splunk for installing the addon, you must have the administrator credentials of the Splunk Enterprise 8.x local instance. Below is a typical screenshot of the Splunk Enterprise login page.



First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you.

If you've forgotten your credentials, contact your Splunk administrator.

Your session has expired. Log in to return to the system.

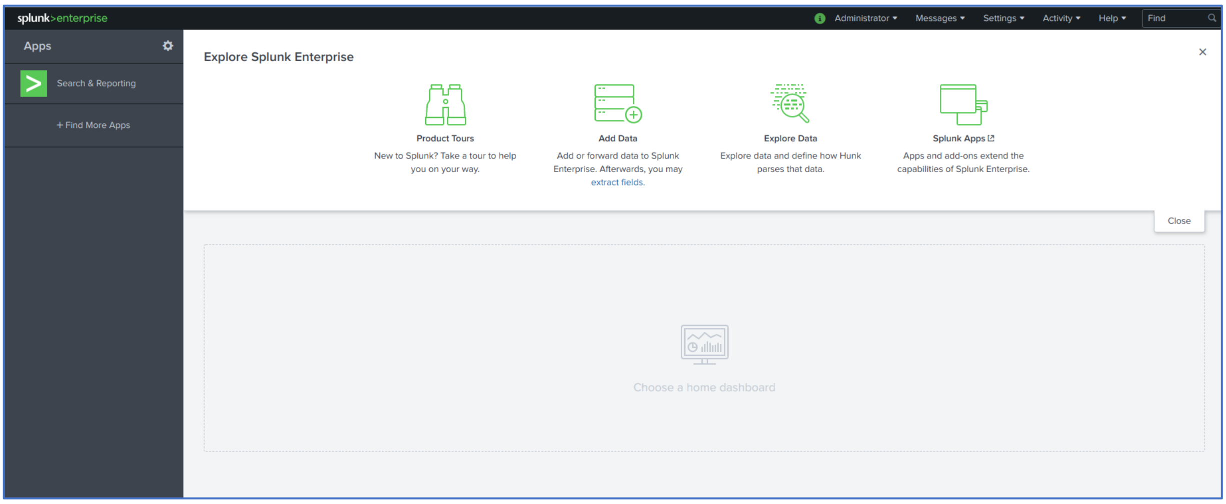
© 2005-2020 Splunk Inc.

2.4 There are few libraries should be installed in the linux environment where the Splunk instance has been deployed and below are the commands to install them using the root user.

- `sudo apt-get install libgmp-dev`
- `sudo apt-get install libmpfr-dev`
- `sudo apt-get install libmpc-dev`

3. INSTALL AUTHENTIC8 ADDON

3.1 Login with your administrator credentials into the Splunk enterprise and you will be navigated to the dashboard page as shown below.



Explore Splunk Enterprise

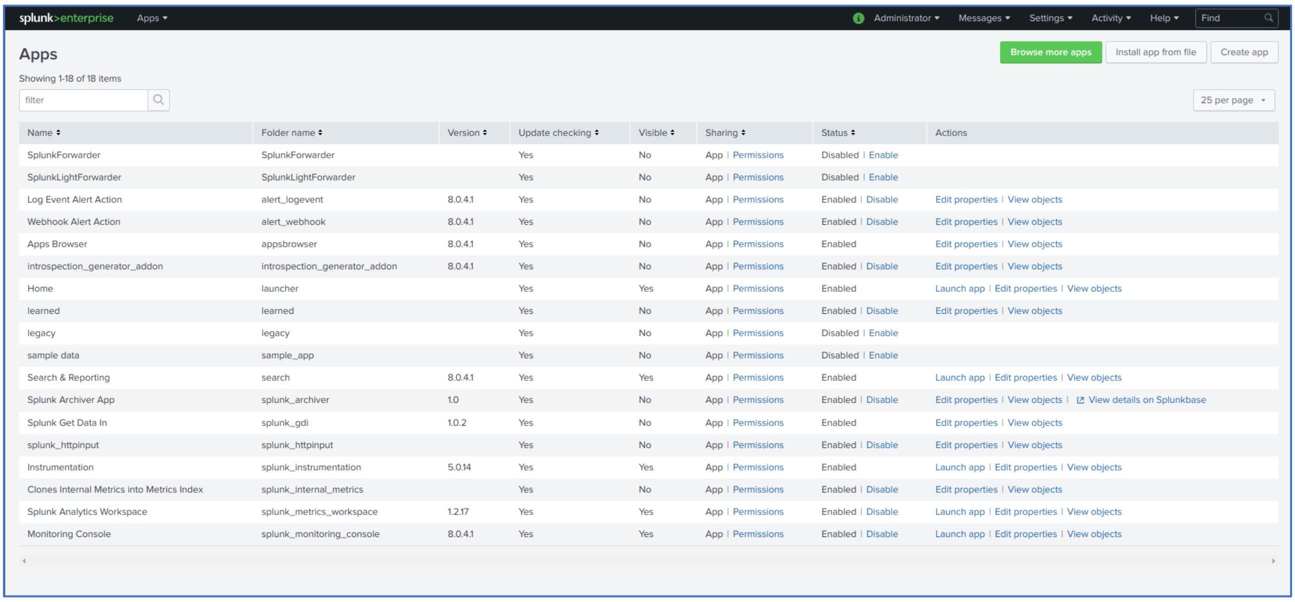
Product Tours
New to Splunk? Take a tour to help you on your way.

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

Explore Data
Explore data and define how Hunk parses that data.

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

3.2 On the dashboard screen on the left top corner click on the settings icon and you will be navigated to the Manage Apps screen. On the page you will notice a few Splunk apps already installed by default as shown in the figure below.

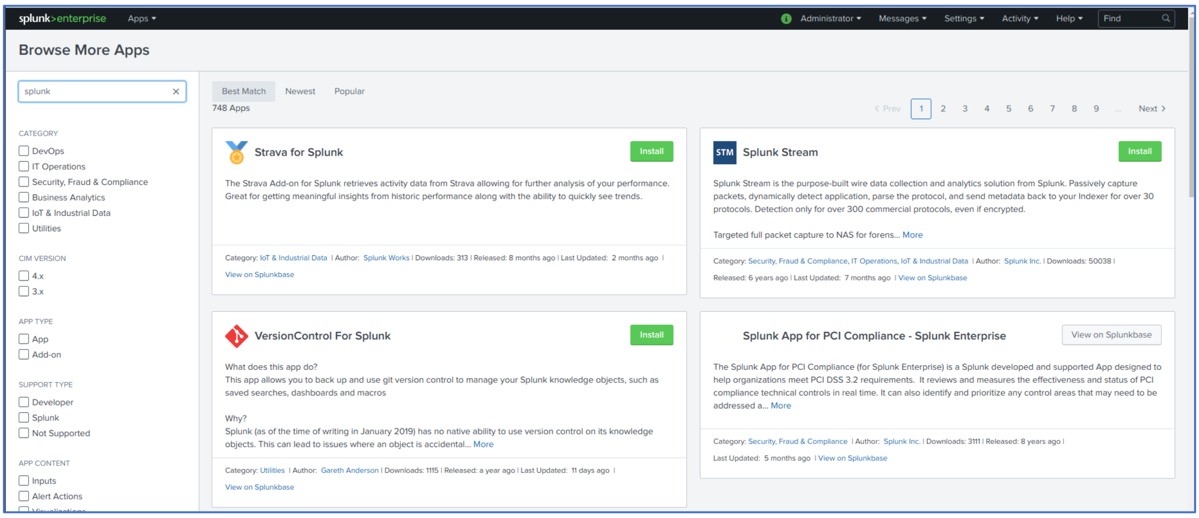


Apps

Showing 1-18 of 18 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Log Event Alert Action	alert_logevent	8.0.4.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	8.0.4.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Apps Browser	appsbrowser	8.0.4.1	Yes	No	App | Permissions	Enabled	Edit properties | View objects
introspection_generator_addon	introspection_generator_addon	8.0.4.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	
sample data	sample_app		Yes	No	App | Permissions	Disabled | Enable	
Search & Reporting	search	8.0.4.1	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase
Splunk Get Data In	splunk_gdi	1.0.2	Yes	No	App | Permissions	Enabled	Edit properties | View objects
splunk_httpinput	splunk_httpinput		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Instrumentation	splunk_instrumentation	5.0.14	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
Clones Internal Metrics into Metrics Index	splunk_internal_metrics		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Splunk Analytics Workspace	splunk_metrics_workspace	1.2.17	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Monitoring Console	splunk_monitoring_console	8.0.4.1	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects

3.3 Click on the Browse more apps button on the top right corner of the dashboard screen to navigate to the Splunk Marketplace, where we will search for the authentic8 addon from the search bar of the top left of the screen as shown in the figure below. Once you can see the Authentic8 addon you can install the addon to add it to your Splunk instance.



Strava for Splunk

The Strava Add-on for Splunk retrieves activity data from Strava allowing for further analysis of your performance. Great for getting meaningful insights from historic performance along with the ability to quickly see trends.

Category: IoT & Industrial Data | Author: Splunk Works | Downloads: 313 | Released: 8 months ago | Last Updated: 2 months ago | View on Splunkbase

Splunk Stream

Splunk Stream is the purpose-built wire data collection and analytics solution from Splunk. Passively capture packets, dynamically detect application, parse the protocol, and send metadata back to your Indexer for over 30 protocols. Detection only for over 300 commercial protocols, even if encrypted.

Targeted full packet capture to NAS for forens... More

Category: Security, Fraud & Compliance, IT Operations, IoT & Industrial Data | Author: Splunk Inc. | Downloads: 50038 | Released: 6 years ago | Last Updated: 7 months ago | View on Splunkbase

VersionControl For Splunk

What does this app do?
This app allows you to back up and use git version control to manage your Splunk knowledge objects, such as saved searches, dashboards and macros

Why?
Splunk (as of the time of writing in January 2019) has no native ability to use version control on its knowledge objects. This can lead to issues where an object is accidental... More

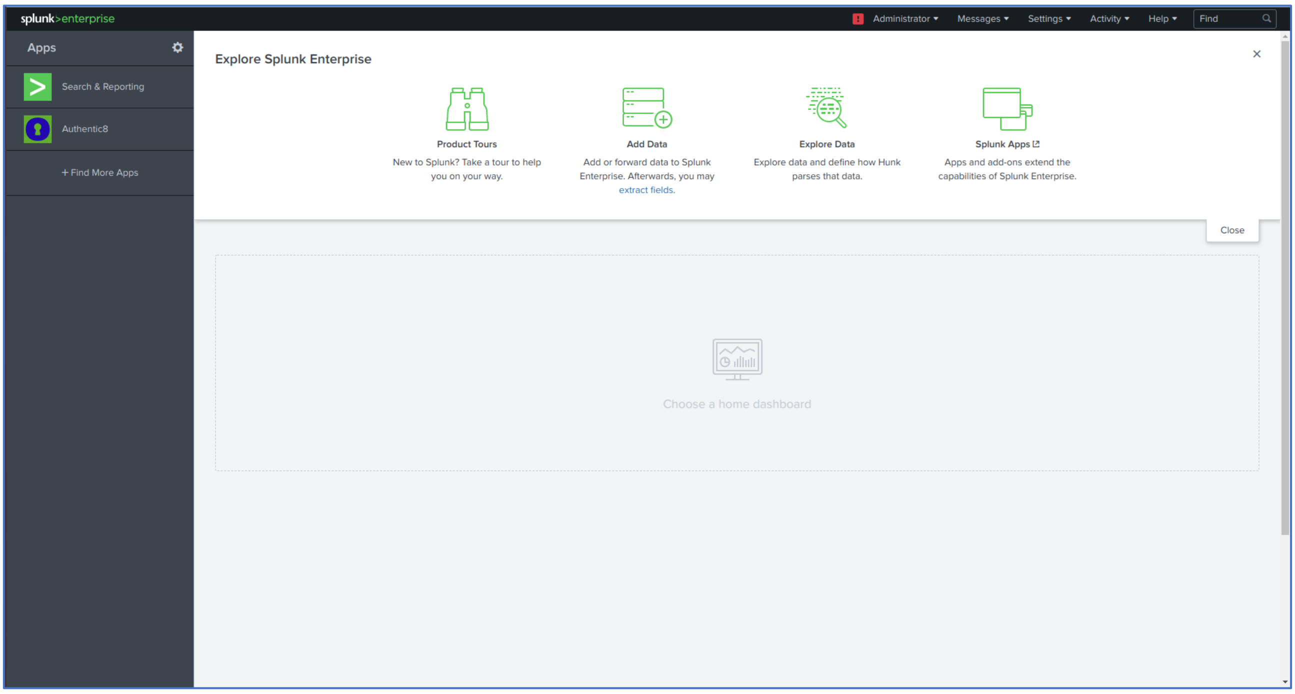
Category: Utilities | Author: Gareth Anderson | Downloads: 1115 | Released: a year ago | Last Updated: 11 days ago | View on Splunkbase

Splunk App for PCI Compliance - Splunk Enterprise

The Splunk App for PCI Compliance (for Splunk Enterprise) is a Splunk developed and supported App designed to help organizations meet PCI DSS 3.2 requirements. It reviews and measures the effectiveness and status of PCI compliance technical controls in real time. It can also identify and prioritize any control areas that may need to be addressed a... More

Category: Security, Fraud & Compliance | Author: Splunk Inc. | Downloads: 3111 | Released: 8 years ago | Last Updated: 5 months ago | View on Splunkbase

3.4 After the install you will be taken back to the dashboard screen with the list of apps and you should now be able to see Authentic8 listed as one of the apps on the Splunk instance as depicted in the figure below.



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

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

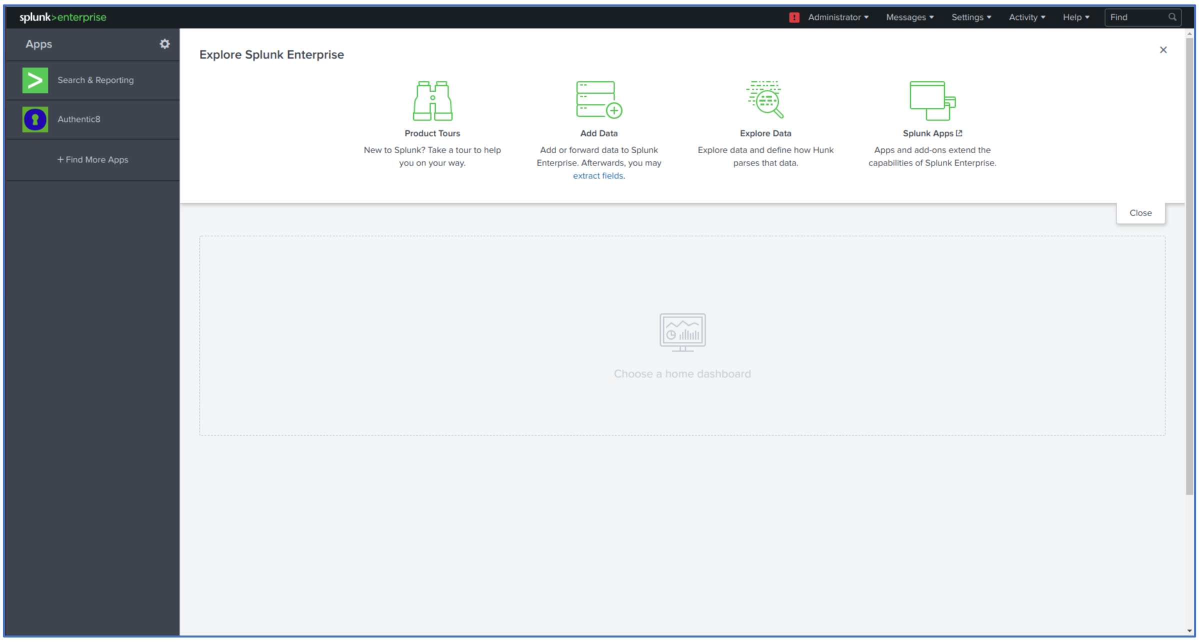
Explore data and define how Hunk parses that data.

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

4. CONFIGURE AUTHENTIC8 ADDON

4.1 Verify Authentic8 Addon installed:

Login into the Splunk instance and you should be able to see Authentic 8 addon listed as apps on your left pane as shown in the figure below.



Explore Splunk Enterprise

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

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

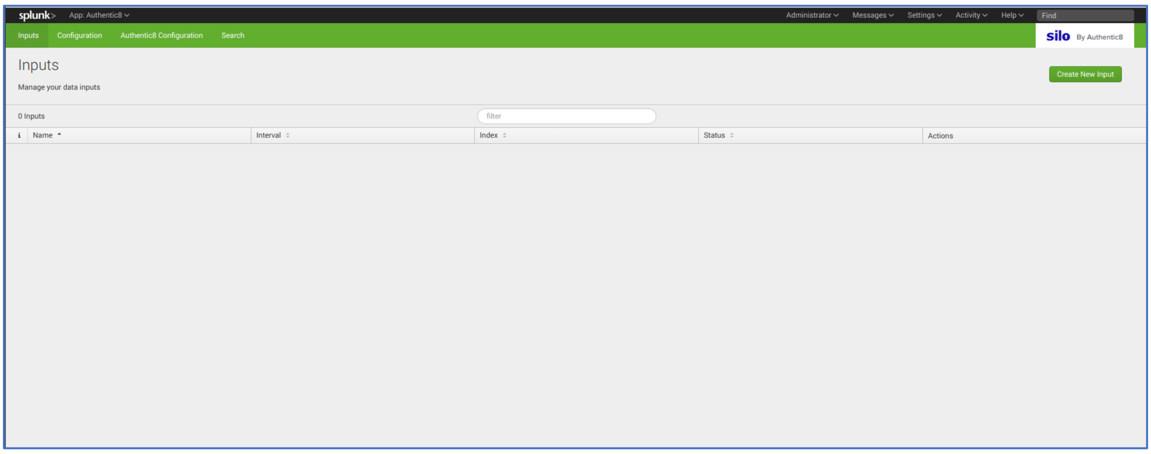
Explore Data
Explore data and define how Hunk parses that data.

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

Choose a home dashboard

4.2 Configure inputs for the Authentic8 addon:

4.2.1 When you click on the addon you will be navigated to the configurations screen as shown below. Here you can configure the Authentic8 addon



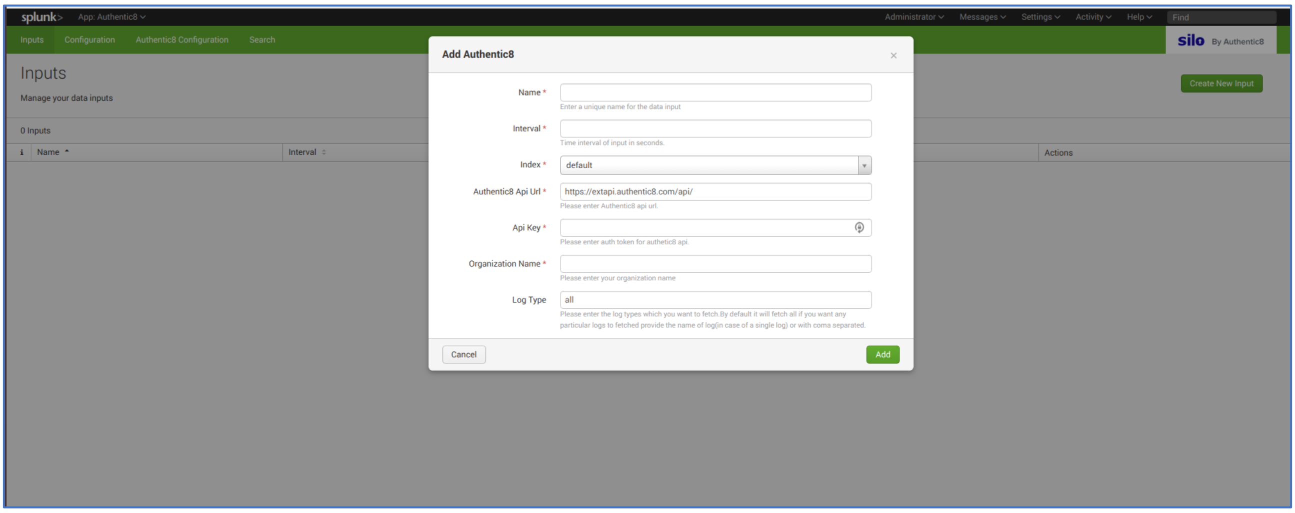
Inputs

Manage your data inputs

0 Inputs

i	Name	Interval	Index	Status	Actions

4.2.2 The first step in configuring the addon is to Create New Input, by clicking on the button in the top right corner. This will open the configuration screen for the user to Add a new configuration for the addon.



Add Authentic8

Name *
Enter a unique name for the data input

Interval *
Time interval of input in seconds.

Index * default

Authentic8 Api Url * https://extapi.authentic8.com/api/
Please enter Authentic8 api url.

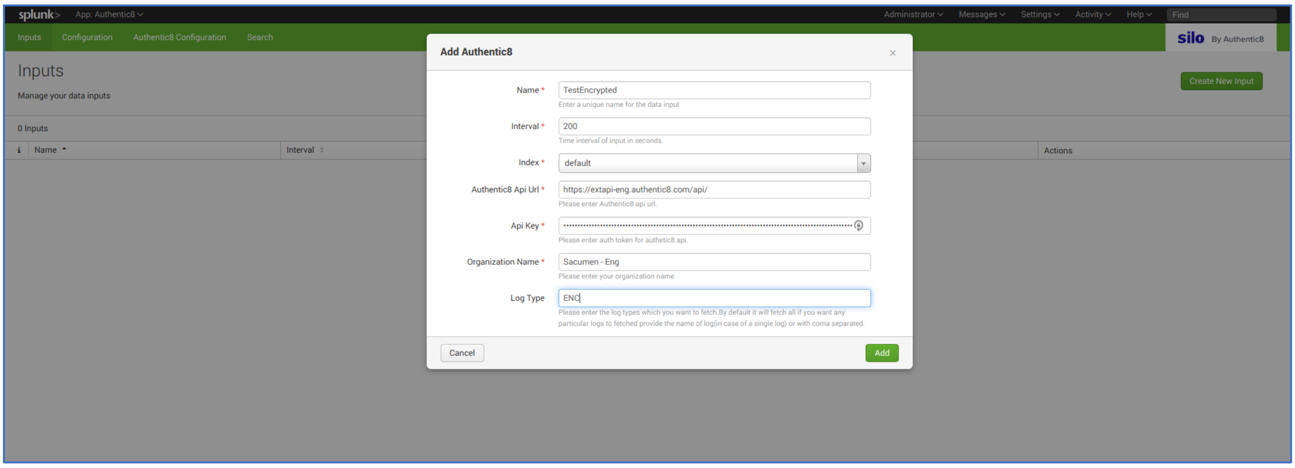
Api Key *
Please enter auth token for authetic8 api.

Organization Name *
Please enter your organization name

Log Type all
Please enter the log types which you want to fetch.By default it will fetch all if you want any particular logs to fetched provide the name of log(in case of a single log) or with coma separated.

The configuration screen consists of the following fields:

Field Name	**Description**
Name	The user needs to provide a name for the input. (Any name can be entered here)
Interval	User need to provide the interval after which the data will be pulled to Splunk. (For example, if 100 is given, after every 100 seconds, data will be pulled in Splunk.)
Index	Splunk has an index feature. The log types which will be retrieved in Splunk saves against an index. The index is set to default.
Authentic8 API URL	User need to provide the API URL which fetches the log types from Silo Browser. The default string is 'https://extapi.authentic8.com/api/'. It is preferred to use https URL only.
API Key	User need to provide the API Key provided by Authentic8 to authorise the user for retrieving log data via the API.
Organization Name	User need to provide their organization name as set in the Silo system from which the log types are to be retrieved.
Log type	User need to provide the log type which needs to be retrieved from Silo system (Individual log types, multiple log types separated by comma can be provided and 'ALL' value is to fetch all the log types) Supported Log types values: URL, EXPLOIT, DOWNLOAD, UPLOAD, POSTDATA, ENC, COOKIES, ADMIN_AUDIT, BLOCKED_URL, TRANSLATION, A8SS, AUTH, PRINT, LOCATION_CHANGE, HARVEST and ALL



Add Authentic8

Name * TestEncrypted
Enter a unique name for the data input

Interval * 200
Time interval of input in seconds.

Index * default

Authentic8 Api Url * https://extapi-eng.authentic8.com/api/
Please enter Authentic8 api url.

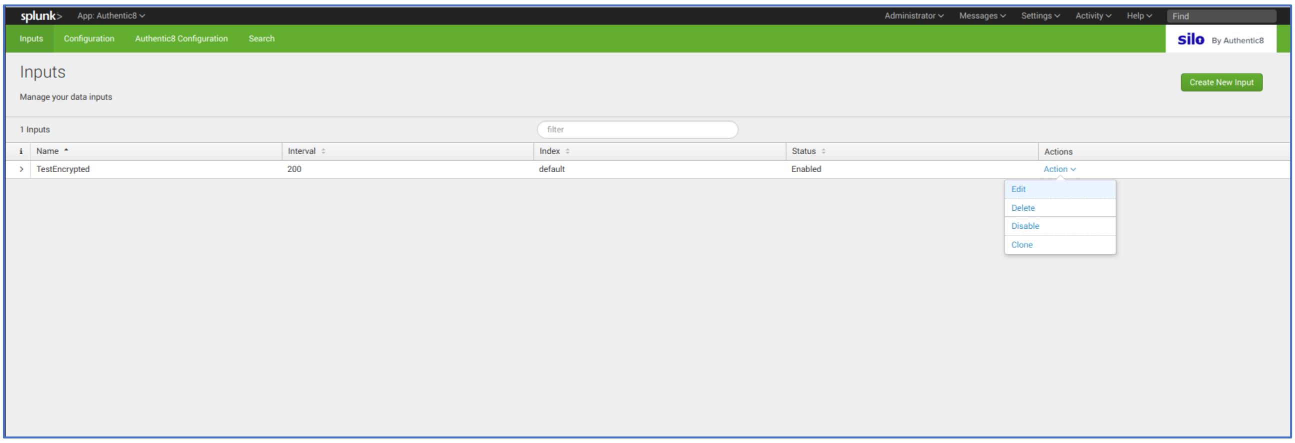
Api Key * ••
Please enter auth token for authetic8 api.

Organization Name * Sacumen - Eng
Please enter your organization name

Log Type ENC
Please enter the log types which you want to fetch.By default it will fetch all if you want any particular logs to fetched provide the name of log(in case of a single log) or with coma separated.

4.2.3 Once the input is created it is enabled by default. Only for the first time the input is created, it will retrieve log types for the last 90 days per the earlier configurations. We can create multiple inputs for the same addon and the other inputs will retrieve data based on the sequence id already retrieved by the addon.. Each of the inputs have a few operations that can be performed.

- User can click on “Edit” to edit the input.
- User can click on “Delete” to delete the input.
- User can click on “Disable” to disable the input. This will restrict the log types to be added to Splunk.
- User can click on “Clone” to create a duplicate input.



Inputs

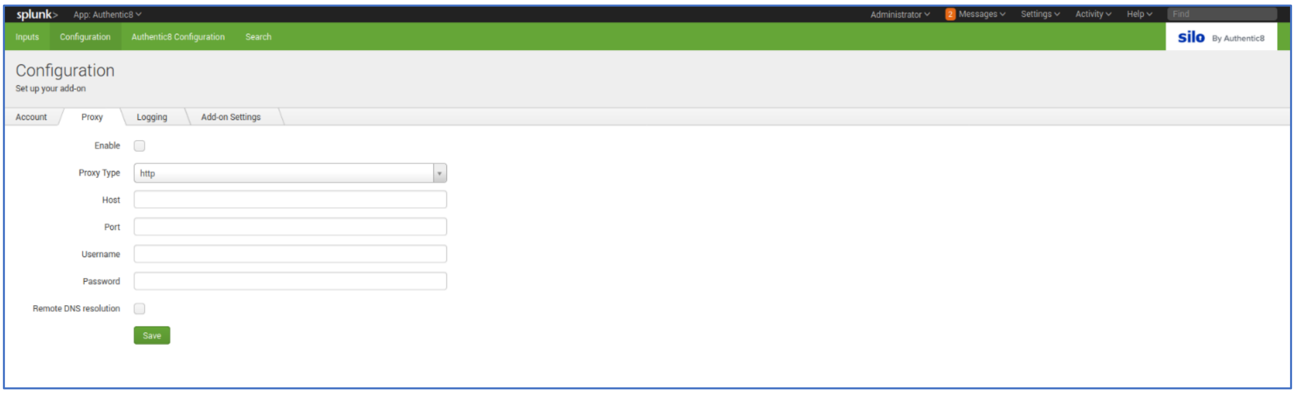
Manage your data inputs

1 Inputs

i	Name	Interval	Index	Status	Actions
>	TestEncrypted	200	default	Enabled	Action

4.3 Configuring settings

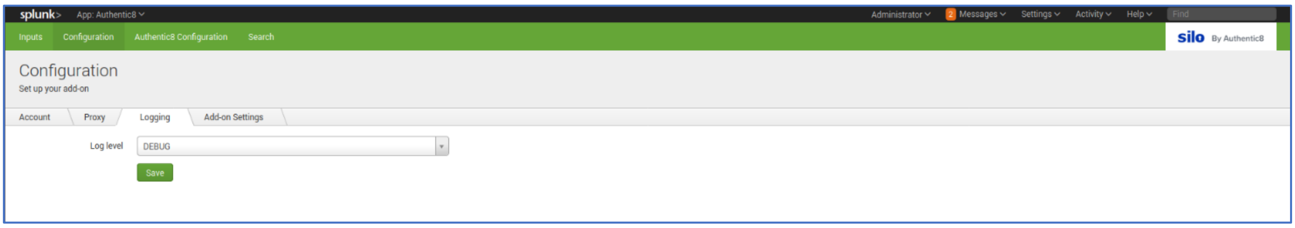
4.3.1 User needs to navigate to Configuration tab to provide additional configuration on Proxy settings if proxy is being used.



Configuration
Set up your add-on

Enable ☐
Proxy Type: http
Host
Port
Username
Password
Remote DNS resolution ☐

4.3.2 User needs to changing the logging level to enable a higher level of logging as required in the Splunk instance.



Configuration
Set up your add-on

Log level: DEBUG

4.3.3 The Account tab and the Addon configuration tab are blank as there is no other configuration required.

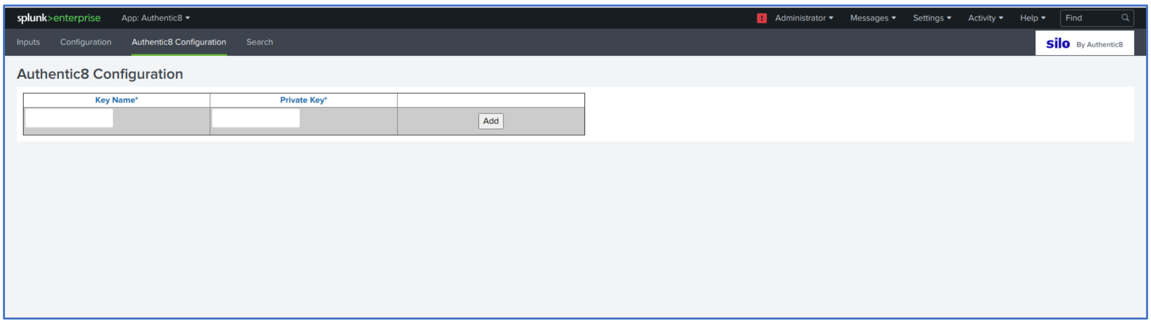
4.4 Configuring Encryption keys for Encrypted log type

4.4.1 When the user navigates to the ‘Authentic8 configuration’ tab, the user will be presented with an option to add multiple key name and private key the addon can use for decryption of encrypted log types depending on the configuration in the Silo system.

Field /button name	**Description**
Key Name	User need to enter the Key Name (same as entered in Silo Browser).
Private Key	User need to enter the Private Key (same as entered in Silo Browser).
Add button	Enables addition of the Key Name and Private Key for an Organization for the addon to decrypt encrypted log types.
Edit button	User can edit the already created key name / private key entry to rectify any errors while entering the values

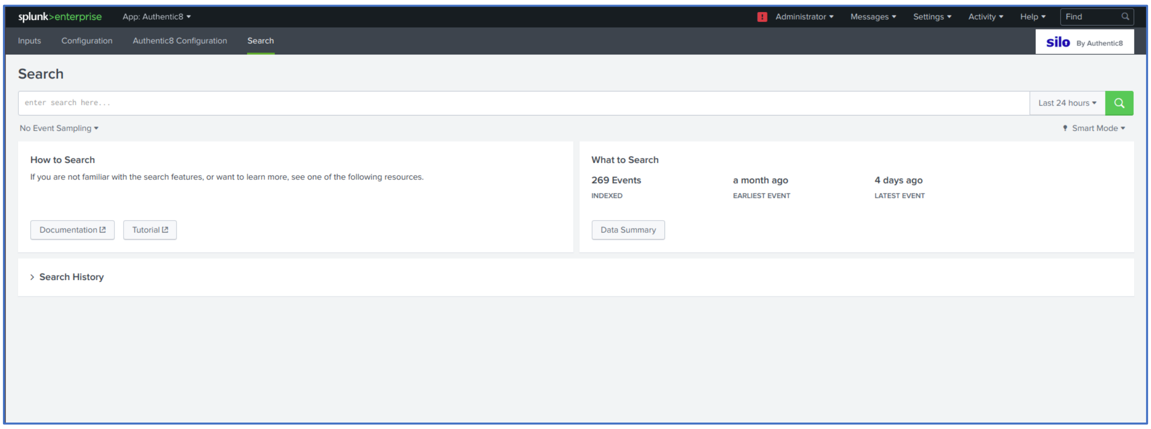
Delete button	User can delete an already existing key name/ private key combination in the configuration as it might have expired.

If the organization in the silo system is encrypted and the key name /private key combination is not provided the addon will not be able to decrypt the data received from the Silo system.



4.5 Verifying on the search tab

4.5.1 Navigate to the search tab and user should be able to see log type events being retrieved from the Silo System. This confirms that the configuration and addon is setup and working.

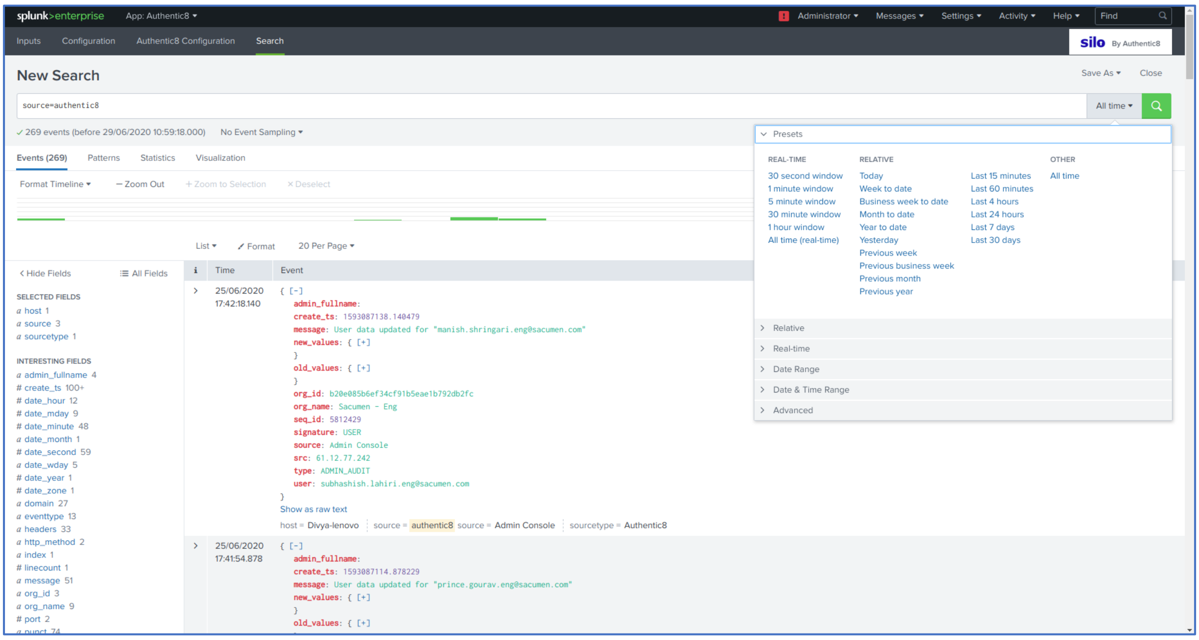


If you are not familiar with the search features, or want to learn more, see one of the following resources.

269 Events	a month ago	4 days ago
INDEXED	EARLIEST EVENT	LATEST EVENT

5. ANALYSE LOGTYPES IN SPLUNK

5.1 We can check the log types by adding “source=”authentic8” in the search box. We can see the data of all time and different time frames by selecting the pop-up as shown in the figure below.



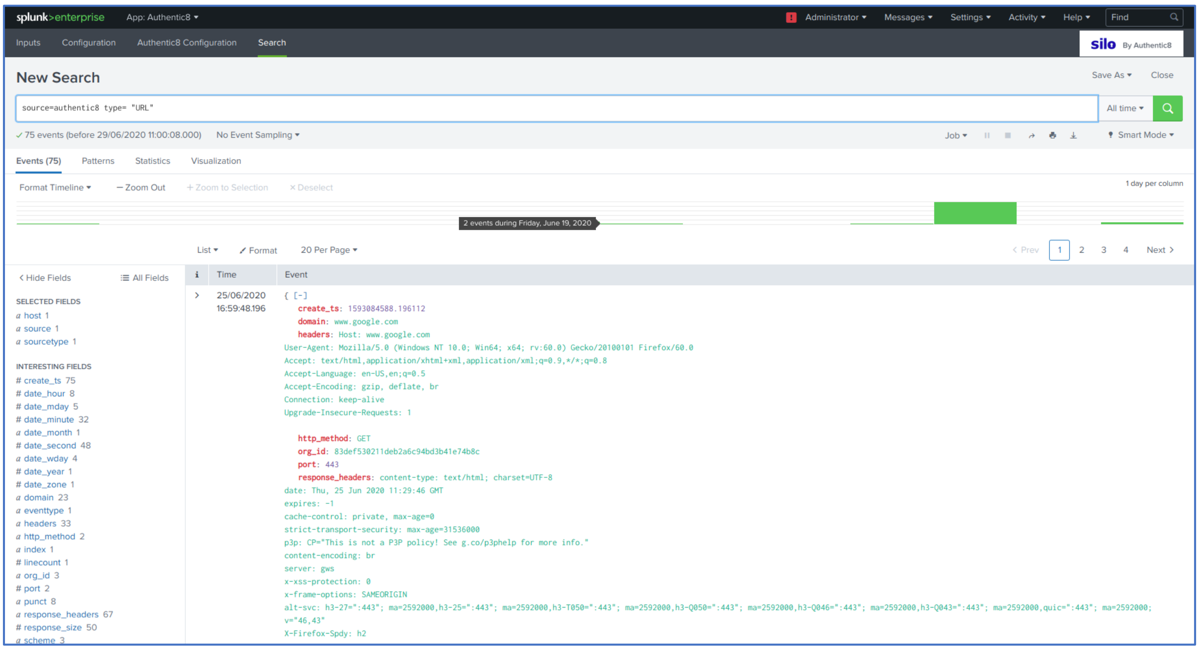
```
source=authentic8
```

✓ 269 events (before 29/06/2020 10:59:18.000) No Event Sampling ▾

```
25/06/2020 17:42:18.140
{ [-]
   admin_fullname:
   create_ts: 1593087138.140479
   message: User data updated for "manish.shringari.eng@sacumen.com"
   new_values: { [+]
   }
   old_values: { [+]
   }
   org_id: b20e085b6ef34cf91b5eae1b792db2fc
   org_name: Sacumen - Eng
   seq_id: 5812429
   signature: USER
   source: Admin Console
   src: 61.12.77.242
   type: ADMIN_AUDIT
   user: subhashish.lahiri.eng@sacumen.com
}
Show as raw text
host = Divya-lenovo   source = authentic8 source = Admin Console   sourcetype = Authentic8

25/06/2020 17:41:54.878
{ [-]
   admin_fullname:
   create_ts: 1593087114.878229
   message: User data updated for "prince.gourav.eng@sacumen.com"
   new_values: { [+]
   }
   old_values: { [+]
```

5.2 We can also search a log type by adding to the search tab type= “URL” as shown in the figure below.



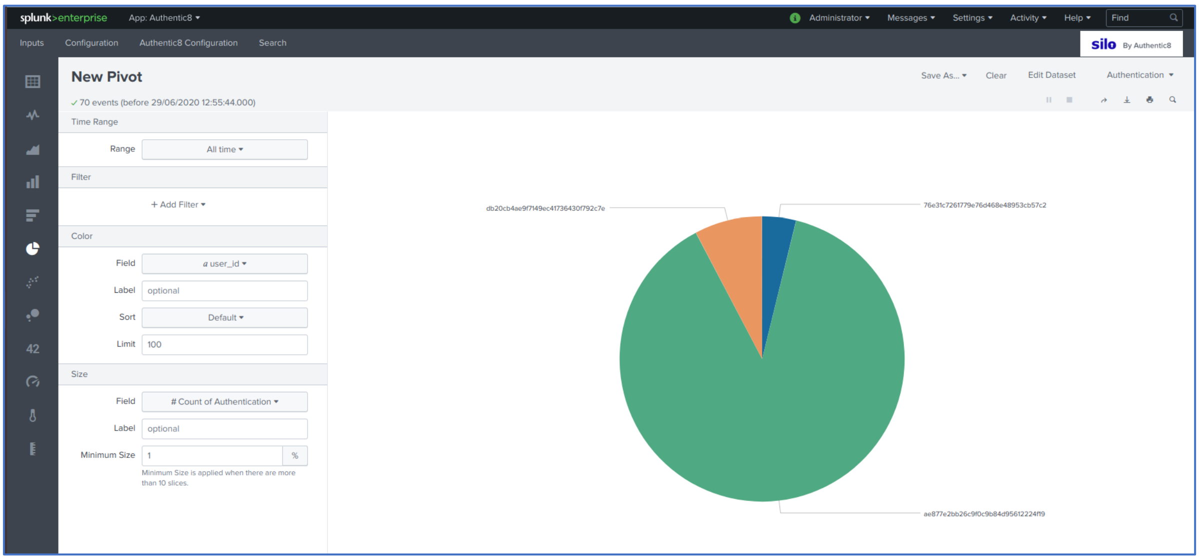
```
source=authentic8 type= "URL"
```

✓ 75 events (before 29/06/2020 11:00:08.000) No Event Sampling ▾

```
25/06/2020 16:59:48.196
{ [-]
   create_ts: 1593084588.196112
   domain: www.google.com
   headers: Host: www.google.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1

   http_method: GET
   org_id: 83def530211deb2a6c94bd3b41e74b8c
   port: 443
   response_headers: content-type: text/html; charset=UTF-8
date: Thu, 25 Jun 2020 11:29:46 GMT
expires: -1
cache-control: private, max-age=0
strict-transport-security: max-age=31536000
p3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
content-encoding: br
server: gws
x-xss-protection: 0
x-frame-options: SAMEORIGIN
alt-svc: h3-27=":443"; ma=2592000,h3-25=":443"; ma=2592000,h3-T050=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;
v="46,43"
X-Firefox-Spdy: h2
```

5.3 The Authentic8 addon has mapped some of the fields of the log types to the Splunk Common information model (CIM) in order to provide for visualizations on the log data.



New Pivot

✓ 70 events (before 29/06/2020 12:55:44.000)

Time Range

Range: All time

Filter

Color

Field: a user_id

Label: optional

Sort: Default

Limit: 100

Size

Field: # Count of Authentication

Label: optional

Minimum Size: 1 %

Minimum Size is applied when there are more than 10 slices.