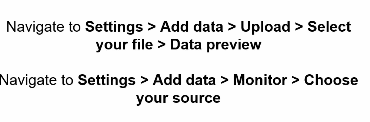
Splunk

Install splunk

Goto <https://www.splunk.com/>

Uploading data into splunk

We can also upload the log file to the splunk



Add this add on (splunk add on for cisco WSA)

Apps->Find more apps->search as cisco

Bucket

Bucket is nothing but a storage directory, residing in indexer and it is grouped by time

Standalone means on single local machine operating independently

Index

Index is something like hashtag, all the related data will be stored in same bucket

Raw data is nothing but the data that is not added into splunk, whatever data that is added to splunk will be indexed

While searching always remember index is mandatory,

Sourcetype

Source type is very very important, if u are uploading csv file, u should select the source type as CSV while uploading the file

Else data will not be indexed properly