KPMG

cutting through complexity

Saviynt Splunk Integration & Prerequisites

<Client>
KPMG Build

July 2022
Version: 1.0

Table of Contents

1 Document Control

1.1 Document Review & Feedback

An updated version of this document has been created and will be reviewed by the team members and stakeholders listed below. The feedback obtained from their review will be incorporated.

Manjunath Madiraju	07/27/2022	Architect	07/27/2022
Architect	Date	<Title>	Date
Security Architect	Date	<Title>	Date
<Title>	Date	<Title>	Date

1.2 Document Acceptance

Representative Approvers

By signing this document, you confirm that you have read, reviewed, and approved the contents of this deliverable.

AGREED TO AND ACCEPTED BY:

Client Project Management

By: ________________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

AGREED TO AND ACCEPTED BY:

Vendor Project Management

By: ______________________________

Name: ____________________________

Title: _____________________________

Date: _____________________________

1.3 Modification History

Change Date	Author	Version Modified	Description of Changes
July 27, 2022	Manjunath Madiraju	1.0	Initial Creation

2 Document Purpose

Enabling access to technology resources in a secure and efficient manner is at the core of a strong cyber security program. An organization must provide its workforce (employees, contractors and business partners) with the required access to securely enable business operations and collaboration. The purpose of this document is to provide Splunk Prerequisites for <Client>.

3 Introduction

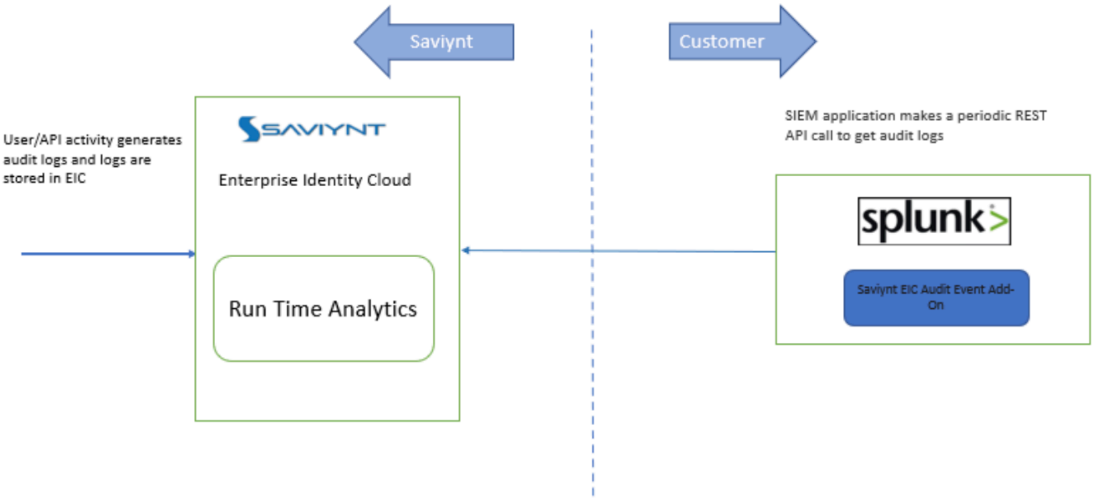
Saviynt Enterprise Identity Cloud (EIC) generates audit logs that records all actions performed by a user such as changes to SAV role, changes to global configurations, changes to connections. These audit logs include the following entries: OBJECT TYPE, OBJECT NAME, ACTION, ATTRIBUTE, ACCESS BY, ACCESS TIME, IP ADDRESS, and MESSAGE.

4 Splunk Architecture

Saviynt provides a REST API to allow the Splunk application to fetch audit logs.

Perform the following steps to fetch audit logs:

1. Setup up a runtime Analytics in Saviynt Enterprise Identity Cloud (EIC) to fetch the data using Saviynt REST API. For more information, see Creating an Analytics Record.
2. Setup an API user with appropriate permissions. For more information, see Setup a User to Manage the SIEM Integration.
3. Use the Splunk add-on to collect data from EIC and to feed the data to the Splunk application.


Saviynt
Customer
User/API activity generates audit logs and logs are stored in EIC
SAVIYNT
Enterprise Identity Cloud
Run Time Analytics
SIEM application makes a periodic REST API call to get audit logs
splunk>
Saviynt EIC Audit Event Add-On

Splunk Integration Architecture

4.1 Creating an Analytics Record (Saviynt Action)

Create a new runtime analytics control (V2) using an SQL Query. For more information, see Analytics Control V2 using SQL query. While creating an analytics control, copy the following query in the **Analytics Query** parameter.

```
select ua.TYPEOFACCESS as 'Object Type',ua.ActionType as 'Action Taken',u.username as 'Accessed By',
ua.IPADDRESS as 'IP Address',ua.ACCESSTIME as 'Event Time',ua.DETAIL as 'Message' from users u ,
userlogin_access ua, userlogins l where l.loginkey = ua.LOGINKEY and l.USERKEY = u.userkey and
ua.AccessTime >= (NOW() - INTERVAL ${timeFrame} Minute) and ua.Detail is not NULL
```

4.2 Setting up Permissions (Saviynt Action)

Saviynt recommends that you create a dedicated user with the least privileges required to call the Saviynt API and get audit logs. In EIC, you can associate a Role Admin SAV Role or a custom SAV Role to a user.

Perform the following steps to set up permissions:

1. Create a user ID, for example, siem-sid. For more information on creating users, see Creating Users. For more information on changing the password of the user, see Managing Users.
2. Create an SAV Role, for example, ROLE_SIEM.
3. Assign SAV Role permissions.
    1. Assign the SAV Role the permission to access the web service URL of the API. For more information, see Creating SAV Roles - Web Service Access.
    2. Assign the SAV Role the permission to verify the analytics record that you created. For more information, see Creating SAV Roles - Analytics.
4. Add the SAV Role to the user. For more information, see Creating SAV Roles - Users.

Note: If you want to associate a Role Admin SAV Role to a user, you have to only add the SAV Role to the user while creating the SAV Role. You need not perform steps 3a and 3b listed above.

4.3 Invoke the Saviynt API (Splunk Action)

EIC maintains an audit log of all security activities performed by a user within the identity warehouse of EIC. You can send these logs from EIC to your SIEM application using the Saviynt REST API.

Perform the following steps to create a REST-based integration with the SIEM application:

Invoke the authentication API to get the authorization token to make a REST API call.
Method: POST
Endpoint: {{url}}/ECM/api/login

Syntax used in the API URLs:

{{url}}/ECM/{{path}}/apiName

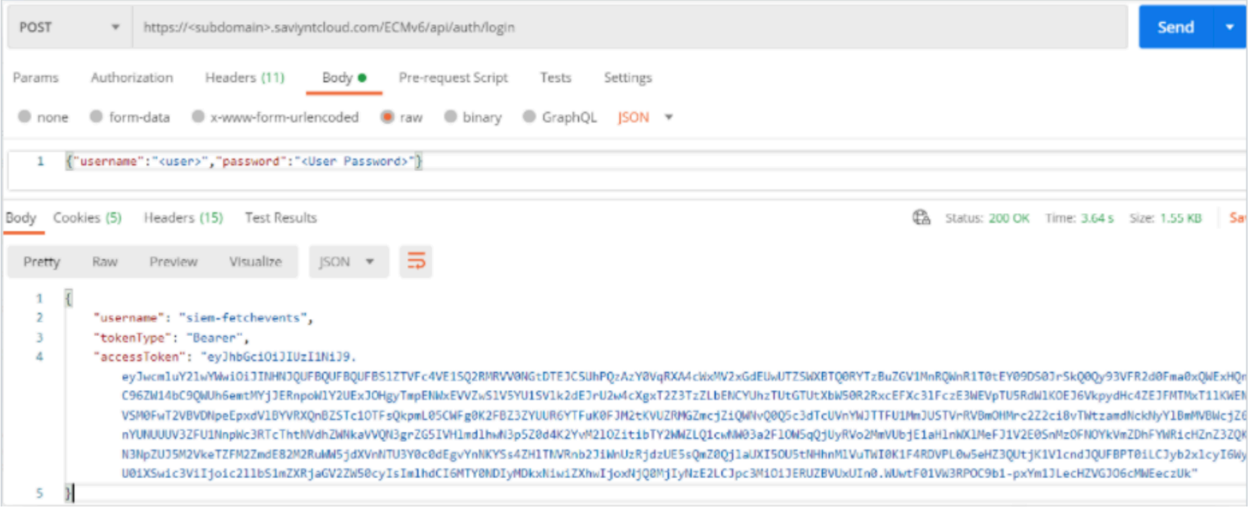
Example:

{{url}} - https://example.saviyntcloud.com

{{path}} - Use api/v5 for EIC v5.2 onwards. Use api for older versions of EIC.
Body:

{"username":"admin","password":"password"}

For more information about the request and response details, see API document.
Sample screenshot taken from the Postman tool:



POST https://<subdomain>.saviyntcloud.com/ECMv6/api/auth/login

```
{"username":"<user>","password":"<User Password>"}
```

```
{
    "username": "siem-fetchevents",
    "tokenType": "Bearer",
    "accessToken": "eyJhbGciOiJIUzI1NiJ9.
        eyJwcmluY2lwYWwiOiJINHNJQUFBQUFBQUFBS1ZTVFc4VE1SQ2RMRVV0NGtDTEJCSUhPQzAzY0VqRXA4cWxMV2xGdEUwUTZSWXBTQ0RYTzBuZGV1MnRQWnR1T0tEY09DS0JrSkQ0Qy93VFR2d0Fma0xQWExHQn
        C96ZW14bC9QWUh6emtMYjJERnpoW1Y2UExJOHgyTmpENWxEVVZwS1V5YU1SV1k2dEJrU2w4cXgxT2Z3TzZLbENCYUhzTUtGTUtXbW50R2RxcEFXc31FczE3WEVpTU5RdW1KOEJ6VkpydHc4ZEJFMTMxT11KWEN
        VSM0FwT2VBVDNpeEpxdV1BYVRXQnBZSTc1OTFsQkpmL05CWFg0K2FBZ3ZYUUR6YTFuK0FJM2tKVUZRMGZmcjZiQWNvQ0Q5c3dTcUVnYWJTTFU1MmJUSTVrRVBmOHMrc2Z2ci8vTWtzamdNckNyY1BmMVBWcjZ6
        nYUNUUUV3ZFU1NnpWc3RTcThtNVdhZWNkaVVQN3grZG5IVHlmdlhwN3p5Z0d4K2YvM21OZitibTY2MWZLQ1cwNW03a2FlOW5qQjUyRVo2MmVUbjE1aHlnWXlMeFJ1V2E0SnMzOFNOYkVmZDhFYWRicHZnZ3ZQK
        N3NpZUJ5M2VkeTZFM2ZmdE82M2RuWW5jdXVnNTU3Y0c0dEgvYnNKYSs4ZHlTNVRnb2JiWnUzRjdzUE5sQmZ0QjlaUXI5OU5tNHhnM1VuTWI0K1F4RDVPL0w5eHZ3QUtjK1V1cndJQUFBPT0iLCJyb2xlcyI6Wy
        U01XSwic3ViIjoic2llbS1mZXRjaGV2ZW50cyIsImlhdCI6MTY0NDIyMDkxNiwiZXhwIjoxNjQ0MjIyNzE2LCJpc3MiOiJERUZBVUxUIn0.WUwtF01VW3RPOC9b1-pxYm1JLecHZVGJO6cMWEeczUk"
}
```

1. Invoke the fetchRuntimeControlsDataV2 API to fetch data.
   Method: POST
   Endpoint: {{url}}/ECM/{{path}}/fetchRuntimeControlsDataV2
   Body:

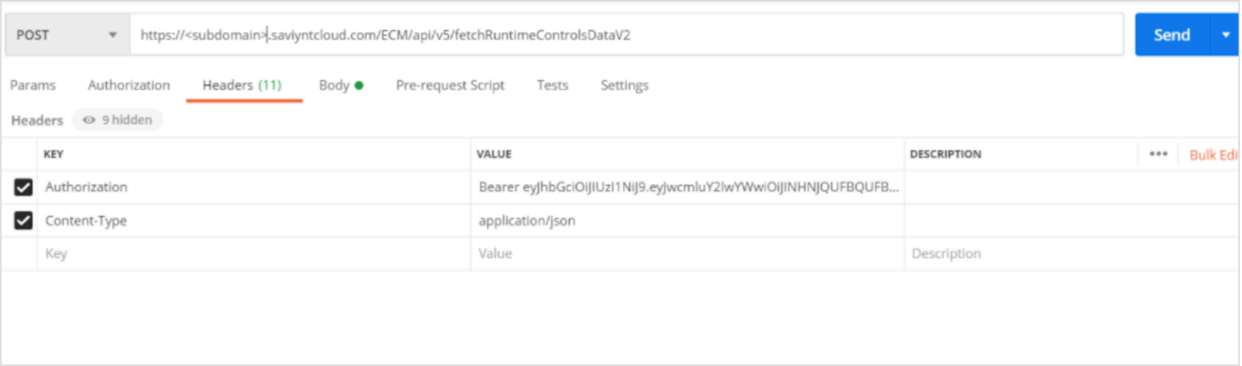
```
{
  "analyticsname": "<Analytics Name>",
   "attributes": {
      "timeframe": "<INTERVAL in minutes>"
   }
}
```

Ensure that you add the following in the body of the API:

Variable	Details
analyticsname	Specify the name of analytic control created in Step 1.
timeframe	Specify a timeframe in minutes to schedule the API at regular intervals. **Note:** Saviynt recommends that this timeframe must neither be lesser than 15 minutes nor greater

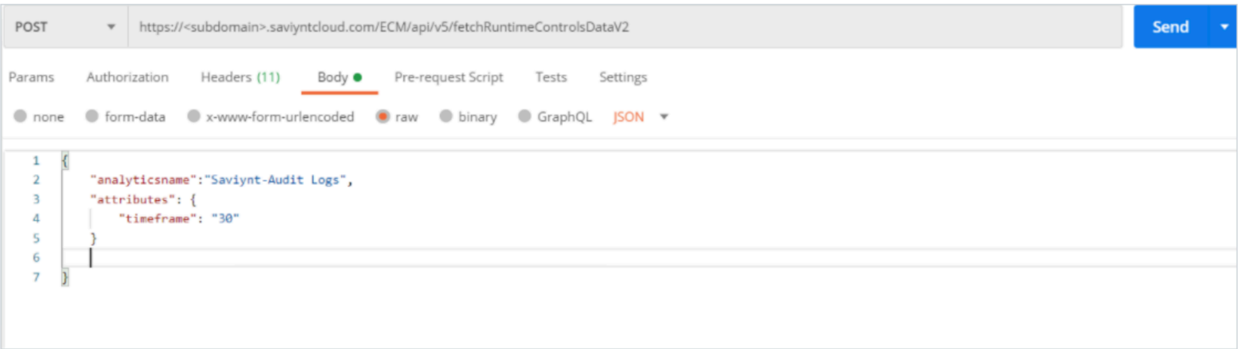
For more information about the request and response details, see API document.

Sample screenshot taken from the Postman tool:



https://<subdomain>.saviyntcloud.com/ECM/api/v5/fetchRuntimeControlsDataV2

	KEY	VALUE	DESCRIPTION
☑	Authorization	Bearer eyJhbGciOiJIUzI1NiJ9.eyJwcmluY2lwYWwiOiJINHNJQUFBQUFB...	
☑	Content-Type	application/json	
	Key	Value	Description



https://<subdomain>.saviyntcloud.com/ECM/api/v5/fetchRuntimeControlsDataV2

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
    "analyticsname":"Saviynt-Audit Logs",
    "attributes": {
        "timeframe": "30"
    }

}
```

5 Splunk Prerequisites (Splunk Action)

Supported Software Versions

Software	Version
EIC	Release v5 and later

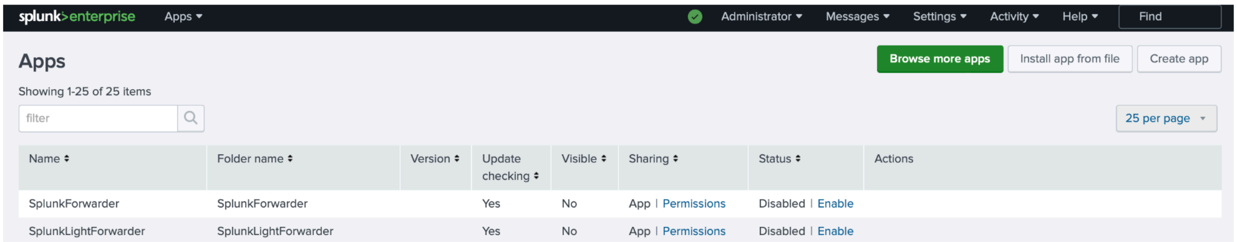
Setting up Saviynt Add-on for Data Collection

This section describes the steps required to install and configure the Saviynt EIC add-on for Splunk to extract audit logs from EIC.

Step 1: Download the Splunk EIC Add-on.

Step 2: Login to Splunk Enterprise with Admin privileges.

Step 3: Go to Apps and Select Install app from file

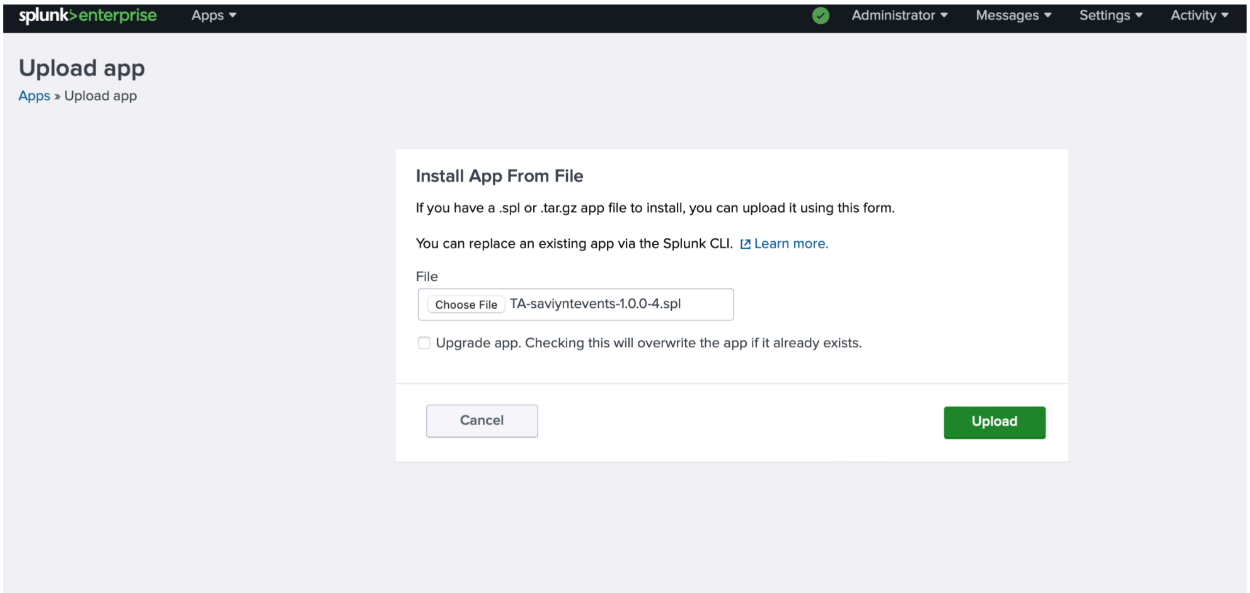


Apps

Showing 1-25 of 25 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	

Step 3: Select the file downloaded in Step 1 and upload



Upload app

Apps » Upload app

Install App From File

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

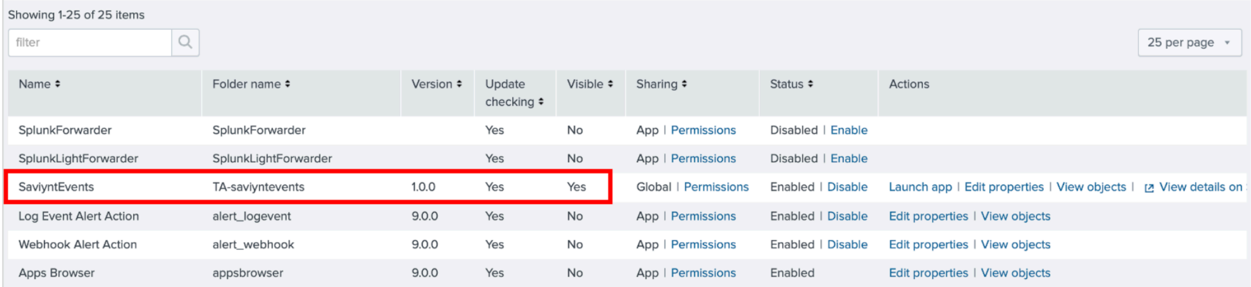
You can replace an existing app via the Splunk CLI. Learn more.

File

Choose File TA-saviyntevents-1.0.0-4.spl

□ Upgrade app. Checking this will overwrite the app if it already exists.

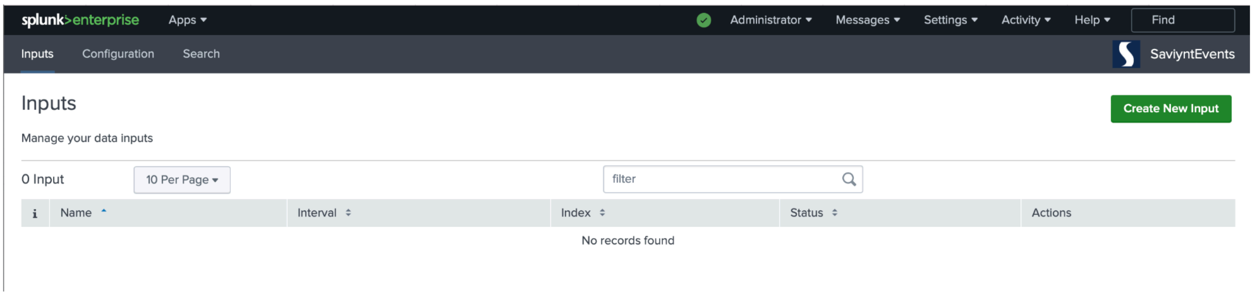
Step 4: Once successfully uploaded, the Saviynt Add-on will appear in the apps/add-on.



Showing 1-25 of 25 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	
SaviyntEvents	TA-saviyntevents	1.0.0	Yes	Yes	Global | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on
Log Event Alert Action	alert_logevent	9.0.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	9.0.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Apps Browser	appsbrowser	9.0.0	Yes	No	App | Permissions	Enabled	Edit properties | View objects

Step 5: Click on the SaviyntEvents Add-on and Create a New Input



Inputs

Manage your data inputs

0 Input

i	Name ˄	Interval ⇕	Index ⇕	Status ⇕	Actions

No records found

Step 6: Add the configuration values specific to your Saviynt tenant and Splunk setup

Name: Name of the input

Interval - Time interval when this add-on will be

Index - Choose the appropriate index

Saviynt Tenant - The Saviynt tenant URI - https://<<Saviynt Tenant>> (without the forward slash / at the end)

Username - API user name that has the appropriate permissions to use the APIs and execute the runtime analytics. Refer to documentation for more details.

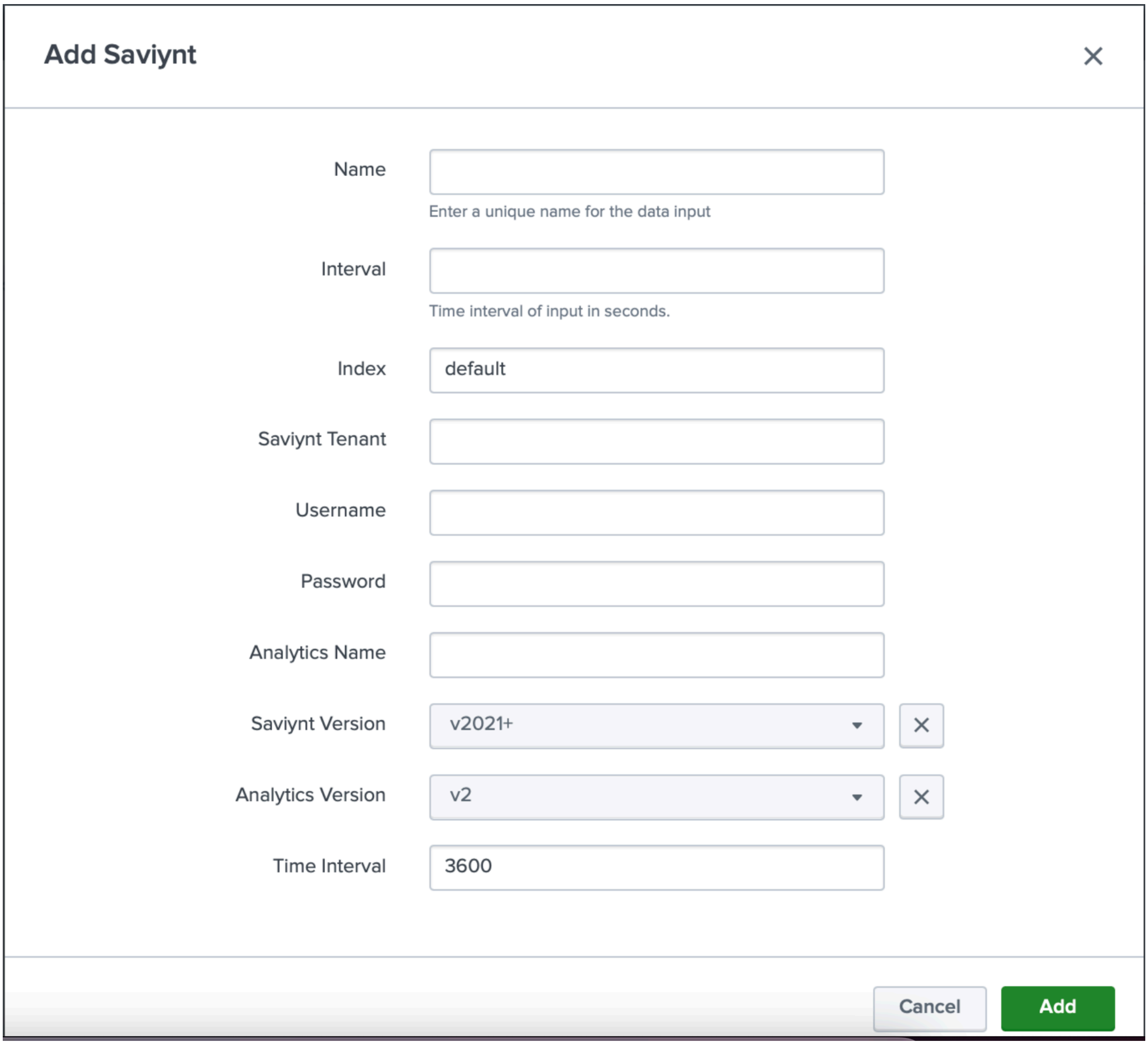
Password - API user credentials

Analytics Name - Frequency to pull Audit Events from Saviynt (this is in seconds)

Saviynt Version - Select the version of your Saviynt tenant from drop down

Analytics Version - Version of the RunTime Analytics used

Time Interval - This is the time interval in minutes when the Saviynt Analytics will collect the data, except for testing purposes set it same as Interval.



Add Saviynt

Name:
Enter a unique name for the data input

Interval:
Time interval of input in seconds.

Index: default

Saviynt Tenant:

Username:

Password:

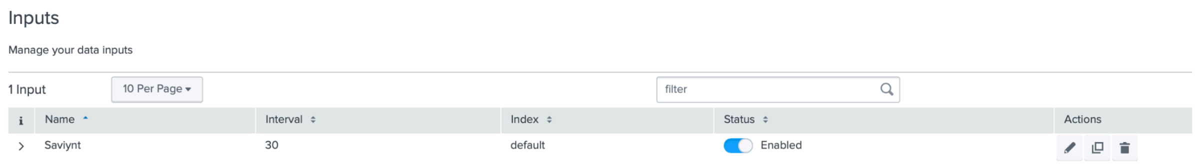
Analytics Name:

Saviynt Version: v2021+

Analytics Version: v2

Time Interval: 3600

Step 7: Click **Add** to finish setting up the SaviyntEvents Add-on



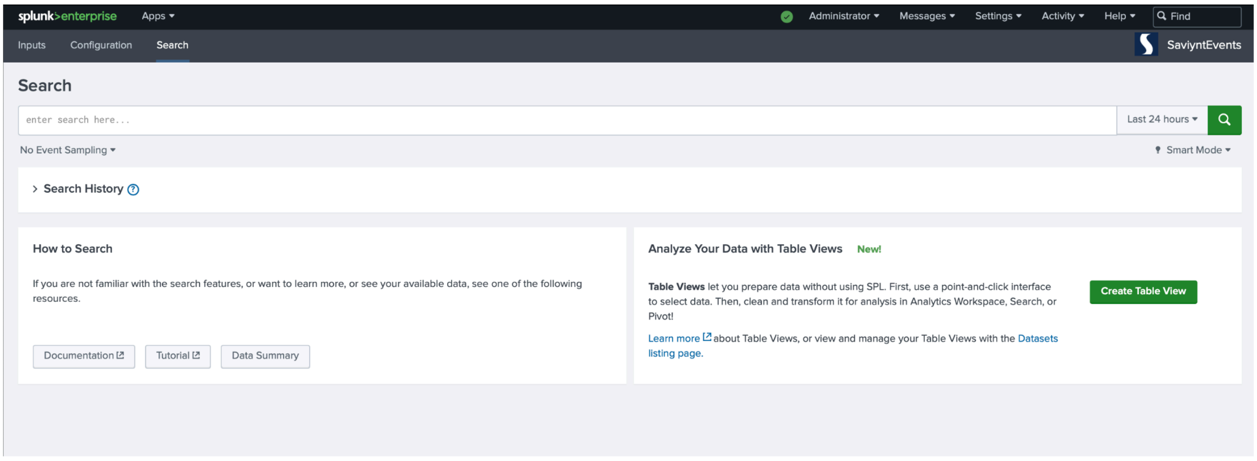
Inputs

Manage your data inputs

1 Input

i	Name	Interval	Index	Status	Actions
›	Saviynt	30	default	Enabled	

Step 8: Validate by Searching for an event once the add-on has executed



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.

Analyze Your Data with Table Views New!

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!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Contact us

Manjunath Madiraju
Manager, Technical Architect

Email mmadiraju@kpmg.com

Ken Dunbar
Engagement Director

Email kbdunbar@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.