Mambu-Audit-Trail-Collector

Release 0.1

Graziella

Sep 15, 2021

CONTENTS

Mambu-Audit-Trail-Collector This Splunk Add-On is to bridge Mambu Audit Trail project to understand what the users are doing and how they are using the platform.

Check out the *Mambu Audit Trail Collector for Splunk* section for further information, including how to installation the project.

Note: This project is under active development.

CHAPTER

ONE

CONTENTS

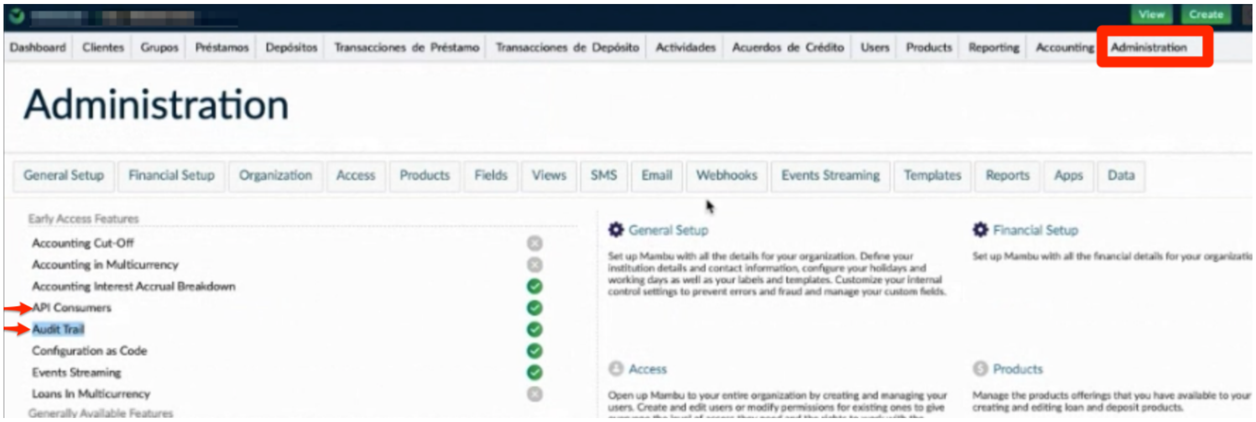
1.1 Mambu Audit Trail Collector for Splunk

Collecting audit data is a great way to correlate all kinds of information so that analysts and auditors will be able to retrieve the necessary information in a timely and efficient manner to investigate a potential fraud or other specific suspicious action.

With that in mind, the purpose of this Splunk Add-On is to bridge Mambu Audit Trail project to understand what the users are doing and how they are using the platform.

1.1.1 Check status/enable Audit Trail API Consumer

To authenticate Audit Trail requests you must use an API key generated by an API consumer of the type ‘audit trail’. So, first of all (and the most important thing) is to check if the API Consumers and Audit Trail features are already enabled.



Early Access Features

Accounting Cut-Off	⊗
Accounting in Multicurrency	⊗
Accounting Interest Accrual Breakdown	✓
API Consumers	✓
Audit Trail	✓
Configuration as Code	✓
Events Streaming	✓
Loans In Multicurrency	⊗

Set up Mambu with all the details for your organization. Define your institution details and contact information, configure your holidays and working days as well as your labels and templates. Customize your internal control settings to prevent errors and fraud and manage your custom fields.

Set up Mambu with all the financial details for your organizatio

Open up Mambu to your entire organization by creating and managing your users. Create and edit users or modify permissions for existing ones to give

Manage the products offerings that you have available to your creating and editing loan and deposit products.

Go to Administration on the top menu bar and verify this.

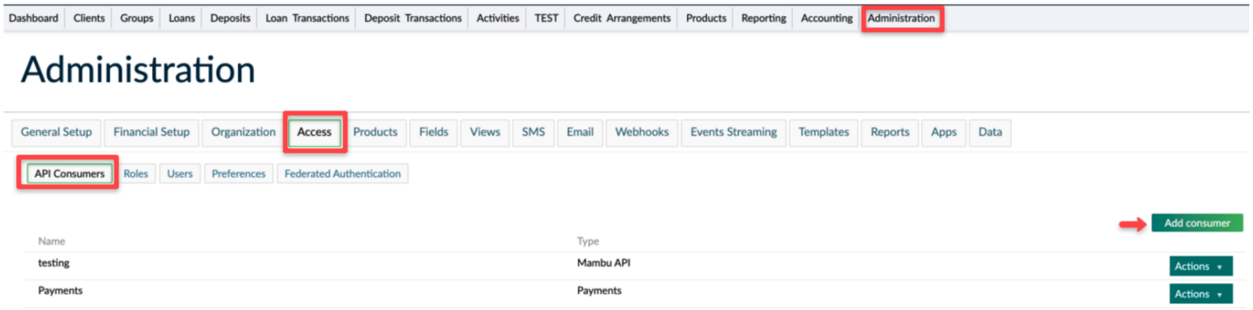
API Consumers	✓
Audit Trail	✓

If for some reason one of the features is disabled, you should contact Mambu support team.

1.1.2 Managing Audit Trail API credentials

You may configure relevant settings in Administration > Access > Preferences

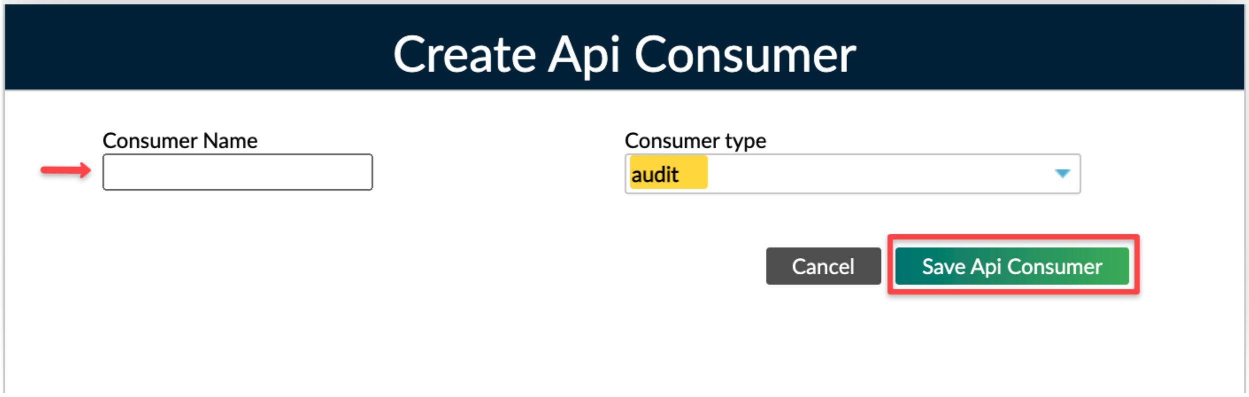
To create an API Consumer:



Name	Type
testing	Mambu API
Payments	Payments

On the main menu, go to Administration > Access > API Consumers Select Add consumer Enter all the necessary information in the Create Api Consumer dialog (Some name and Consumer Type -in our case- Audit) Select Save Api Consumer

To generate an API key:



Consumer Name

Consumer type: audit

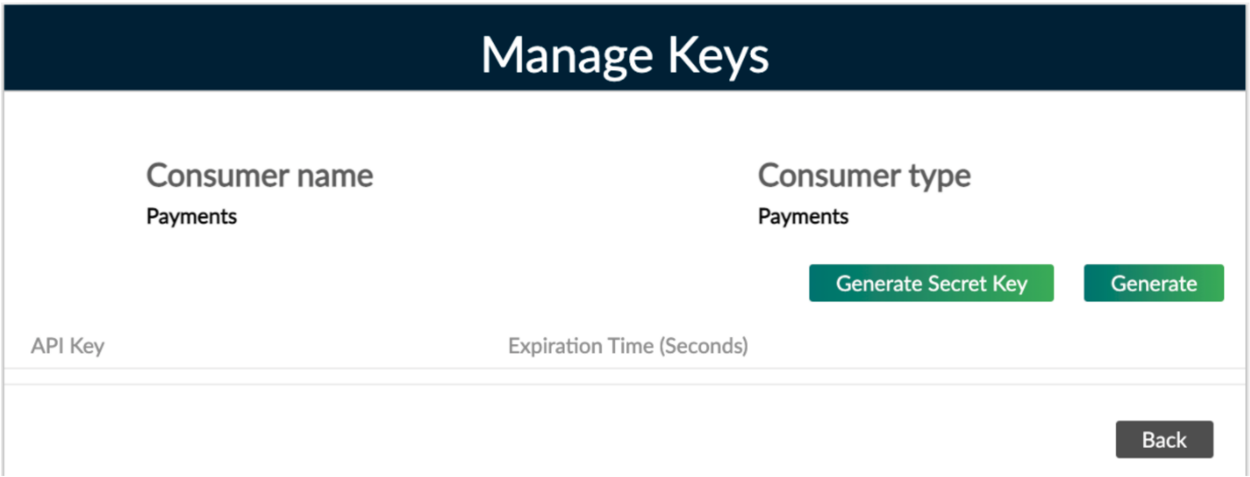
On the main menu, go to Administration > Access > API Consumers Find the API consumer in the list that you would like to make an API key for, select Actions > Manage keys In the Manage Keys dialog, select Generate In the Generate New API Key dialog, you can optionally choose whether you want to enter an expiration time to live (TTL) in seconds Select Generate to finish generating the key

1.1.3 Splunk Add-On installation

1. Download Mambu Audit Trail Collector from Splunkbase
2. Within Splunk go to Manage Apps menu and click on Install app from file.
3. Select the Add-On file you've just downloaded and click on Upload.
4. You must restart Splunk server to enable the Add-On.

1.1.4 Step by step Configuration

Once Splunk restarted you will see a new app within the left menu.

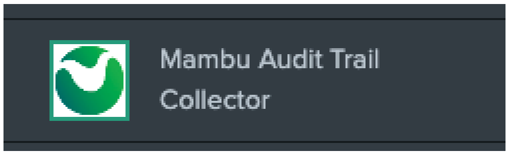


Manage Keys

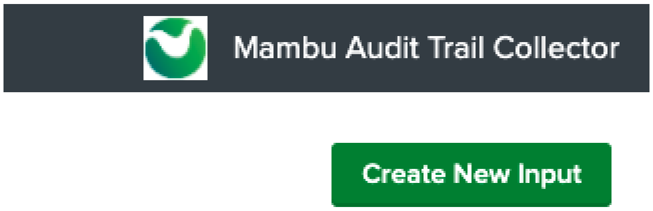
Consumer name
Payments

Consumer type
Payments

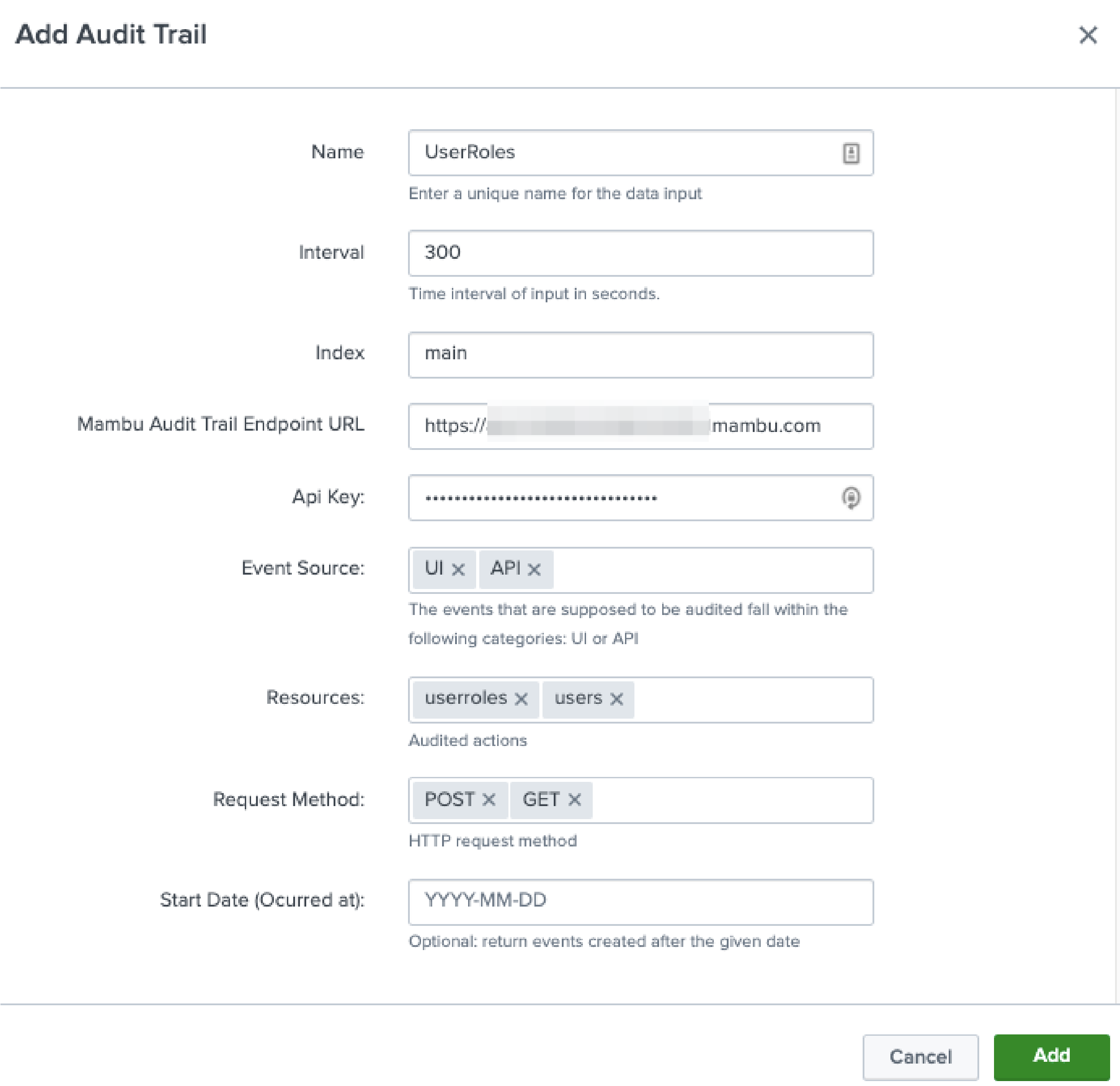
Now it's time to configure our data source (Input). First, click on the Add-On name to access.



Click on Create New Input



Fill the corresponding form and enter your Mambu Audit Trail Endpoint and API Key. Also, you'll need to select through different event categories (like User Interface / API, Resource and Request Method) to monitor.



Add Audit Trail

Name: UserRoles

Enter a unique name for the data input

Interval: 300

Time interval of input in seconds.

Index: main

Mambu Audit Trail Endpoint URL: https://[redacted]mambu.com

Api Key: ••••••••••••••••••••••••••••••••

Event Source: UI × API ×

The events that are supposed to be audited fall within the following categories: UI or API

Resources: userroles × users ×

Audited actions

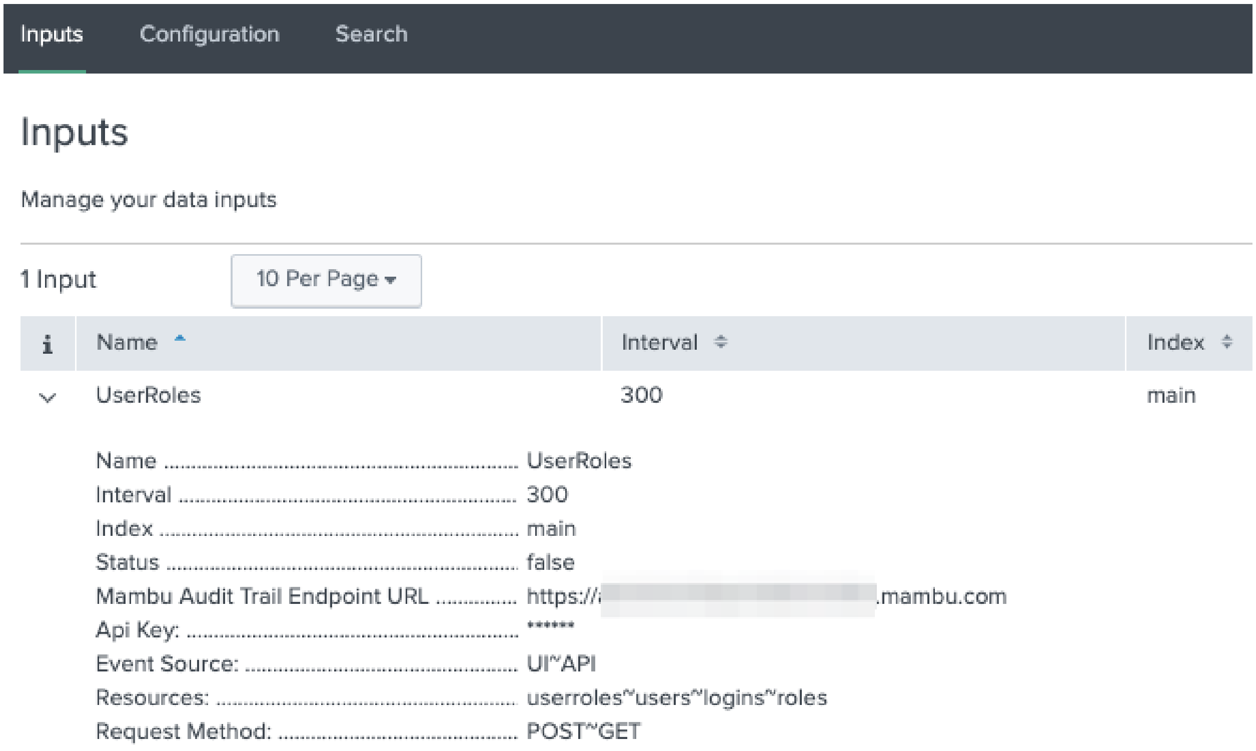
Request Method: POST × GET ×

HTTP request method

Start Date (Ocurred at): YYYY-MM-DD

Optional: return events created after the given date

Last, click on Add



Inputs

Manage your data inputs

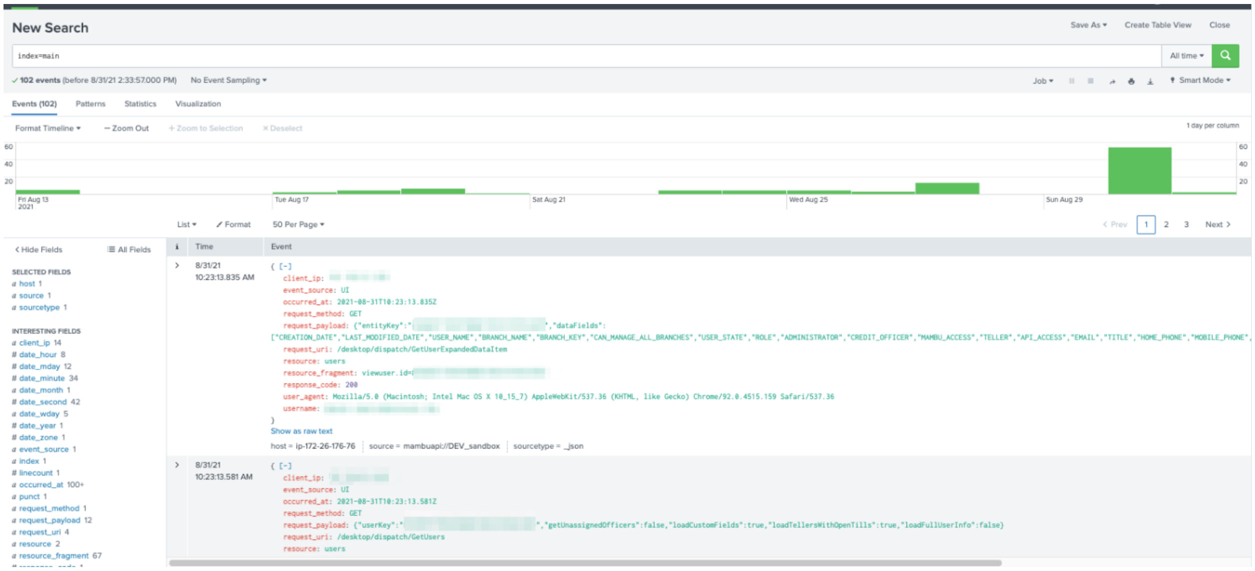
1 Input   10 Per Page ▾

i	Name ▴	Interval ⇕	Index ⇕
⌄	UserRoles	300	main

```
Name ......................................... UserRoles
Interval ..................................... 300
Index ........................................ main
Status ....................................... false
Mambu Audit Trail Endpoint URL ............... https://[redacted].mambu.com
Api Key: ..................................... ******
Event Source: ................................ UI~API
Resources: ................................... userroles~users~logins~roles
Request Method: .............................. POST~GET
```

Congratulations! you have successfully configure Mambu Audit Trail Collector input.

And lastly it's time to run some Splunk searches…



```
index=main
```

✓ 102 events (before 8/31/21 2:33:57.000 PM)   No Event Sampling ▾

i	Time	Event
›	8/31/21 10:23:13.835 AM	see below
›	8/31/21 10:23:13.581 AM	see below

```
{ [-]
   client_ip: [redacted]
   event_source: UI
   occurred_at: 2021-08-31T10:23:13.835Z
   request_method: GET
   request_payload: {"entityKey":"[redacted]","dataFields":
["CREATION_DATE","LAST_MODIFIED_DATE","USER_NAME","BRANCH_NAME","BRANCH_KEY","CAN_MANAGE_ALL_BRANCHES","USER_STATE","ROLE","ADMINISTRATOR","CREDIT_OFFICER","MAMBU_ACCESS","TELLER","API_ACCESS","EMAIL","TITLE","HOME_PHONE","MOBILE_PHONE",
   request_uri: /desktop/dispatch/GetUserExpandedDataItem
   resource: users
   resource_fragment: viewuser.id=[redacted]
   response_code: 200
   user_agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
   username: [redacted]
}
Show as raw text
host = ip-172-26-176-76 | source = mambuapi://DEV_sandbox | sourcetype = _json
```

```
{ [-]
   client_ip: [redacted]
   event_source: UI
   occurred_at: 2021-08-31T10:23:13.581Z
   request_method: GET
   request_payload: {"userKey":"[redacted]","getUnassignedOfficers":false,"loadCustomFields":true,"loadTellersWithOpenTills":true,"loadFullUserInfo":false}
   request_uri: /desktop/dispatch/GetUsers
   resource: users
```

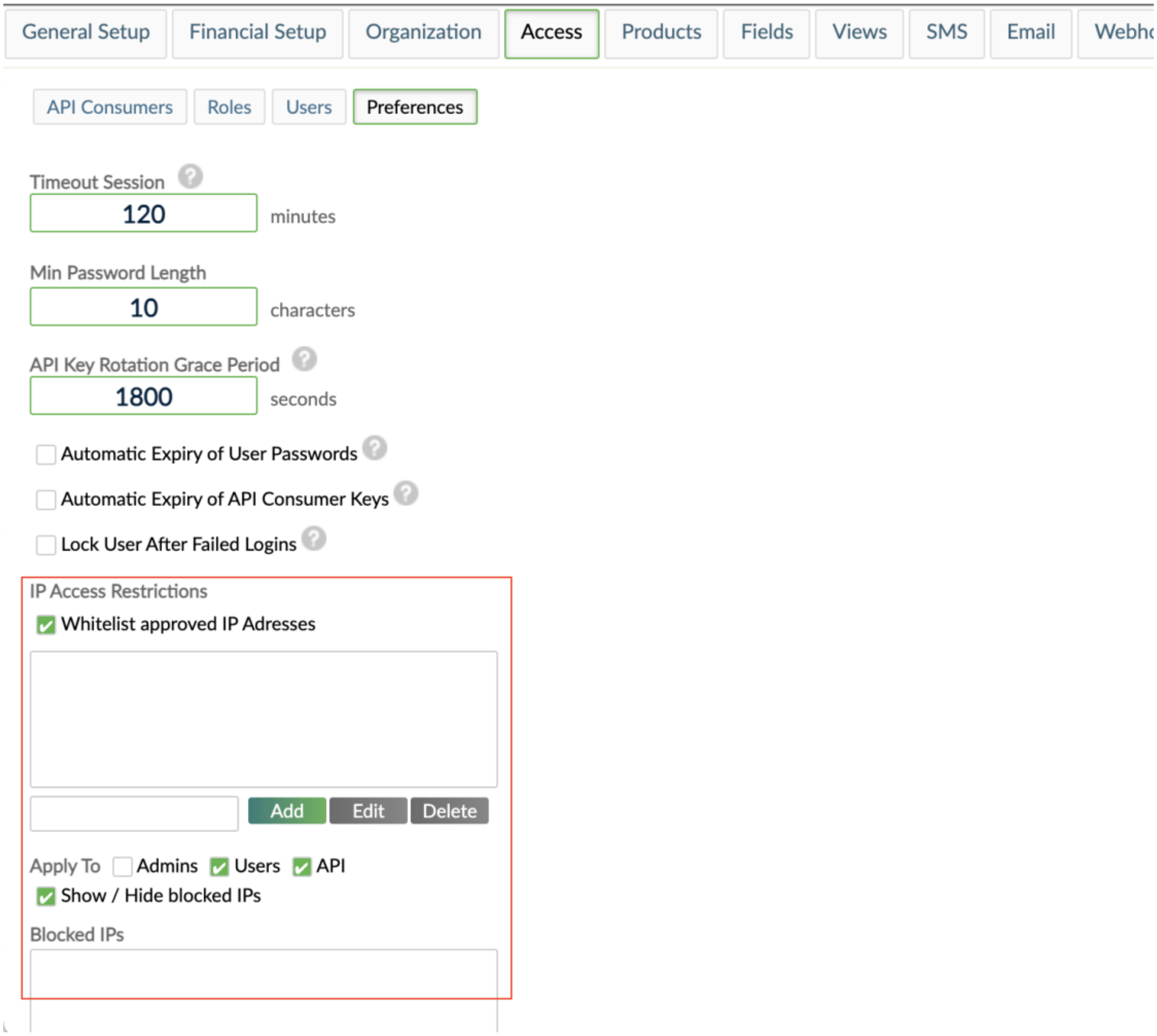
NOTE: *Keep in mind that the audit events should be available for making request, as soon as one of the audited action occurs, e.g after a user logs in.*

Happy Splunking!!!

1.1.5 Connection Troubleshooting

If you faced timeout issues from the Splunk client host, you'd probably need to validate the IP Whitelisting configuration in your tenant/environment.

To do that, you will need to check the following section: Administration > Access > Preferences, specifically the IP Access Restrictions configuration:



Timeout Session 120 minutes

Min Password Length 10 characters

API Key Rotation Grace Period 1800 seconds

□ Automatic Expiry of User Passwords

□ Automatic Expiry of API Consumer Keys

□ Lock User After Failed Logins

IP Access Restrictions

☑ Whitelist approved IP Adresses

Apply To □ Admins ☑ Users ☑ API

☑ Show / Hide blocked IPs

Blocked IPs

For more information check the Mambu's Access Preferences documentation