
Mambu-Audit-Trail-Collector

Release 0.1

Graziella

Sep 15, 2021

CONTENTS

1	Contents	3
1.1	Mambu Audit Trail Collector for Splunk	3

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.

CONTENTS

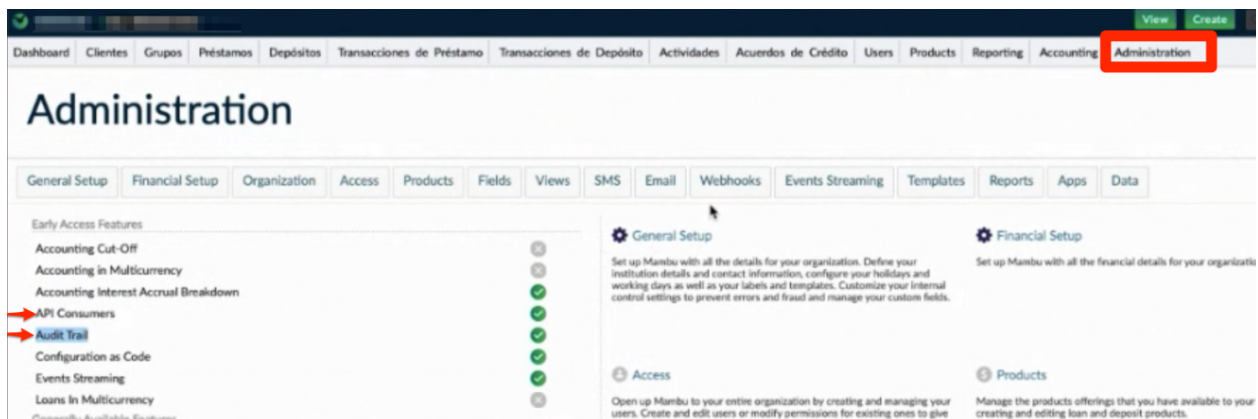
1.1 Mambu Audit Trail Collector for Splunk

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.



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

API Consumers



Audit Trail

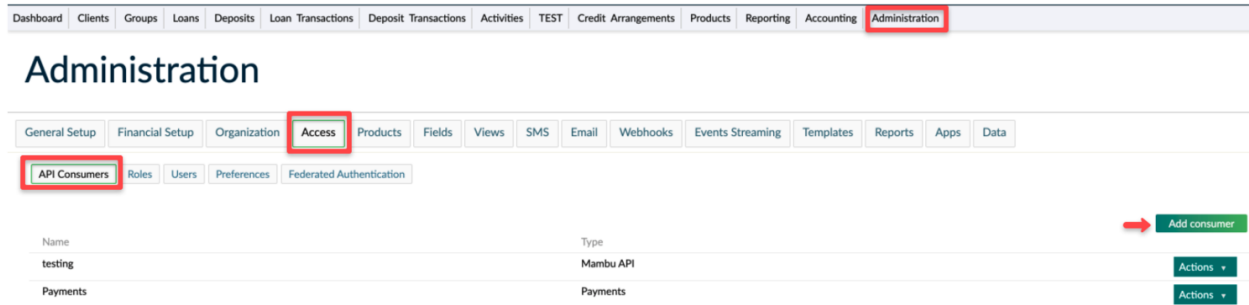


If for some reason one of the features is disabled, you should contact Mambu support team.

1.1.2 Managing Audit Trail API credentials

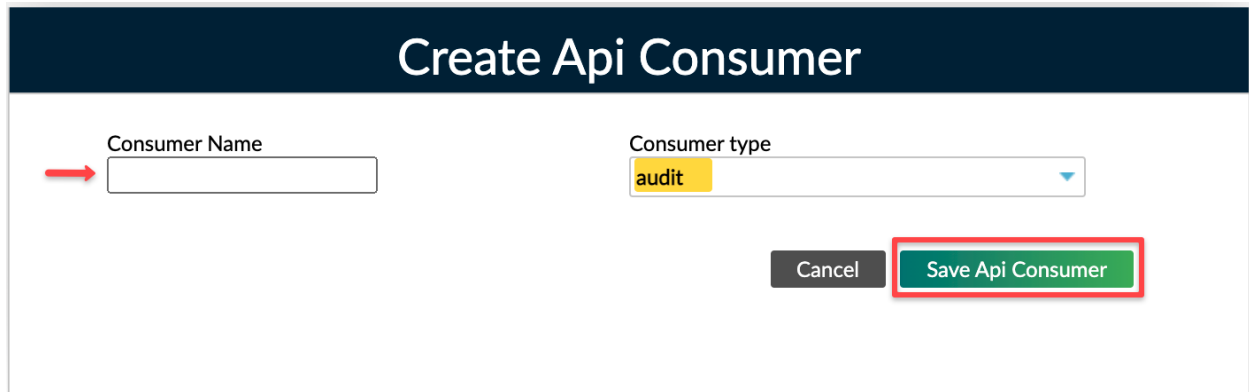
You may configure relevant settings in Administration > Access > Preferences

To create an API Consumer:



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:



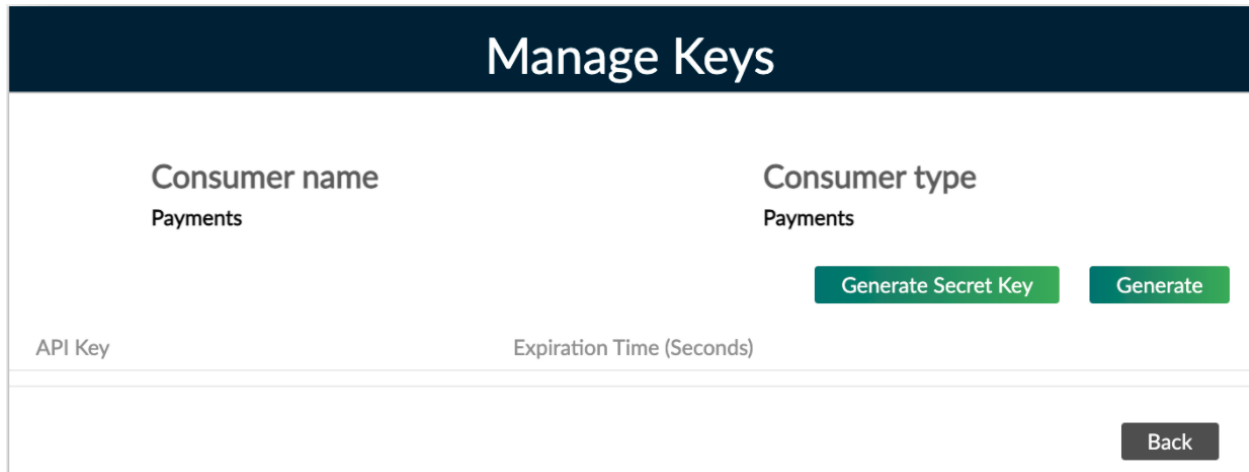
On the main menu, go to Administration > Access > API Consumers Find the API consumer in the list that you would like to make an API key for, select Actions > Manage keys In the Manage Keys dialog, select Generate In the Generate New API Key dialog, you can optionally choose whether you want to enter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

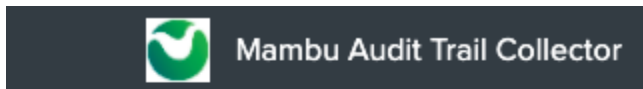
Once Splunk restarted you will see a new app within the left menu.



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



Click on Create New Input



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	<input type="text" value="UserRoles"/>
	Enter a unique name for the data input
Interval	<input type="text" value="300"/>
	Time interval of input in seconds.
Index	<input type="text" value="main"/>
Mambu Audit Trail Endpoint URL	<input type="text" value="https://[redacted]mambu.com"/>
Api Key:	<input type="text" value="....."/>
Event Source:	<input type="text" value="UI x API x"/>
	The events that are supposed to be audited fall within the following categories: UI or API
Resources:	<input type="text" value="userroles x users x"/>
	Audited actions
Request Method:	<input type="text" value="POST x GET x"/>
	HTTP request method
Start Date (Occurred at):	<input type="text" value="YYYY-MM-DD"/>
	Optional: return events created after the given date

Last, click on Add

Inputs Configuration Search

Inputs

Manage your data inputs

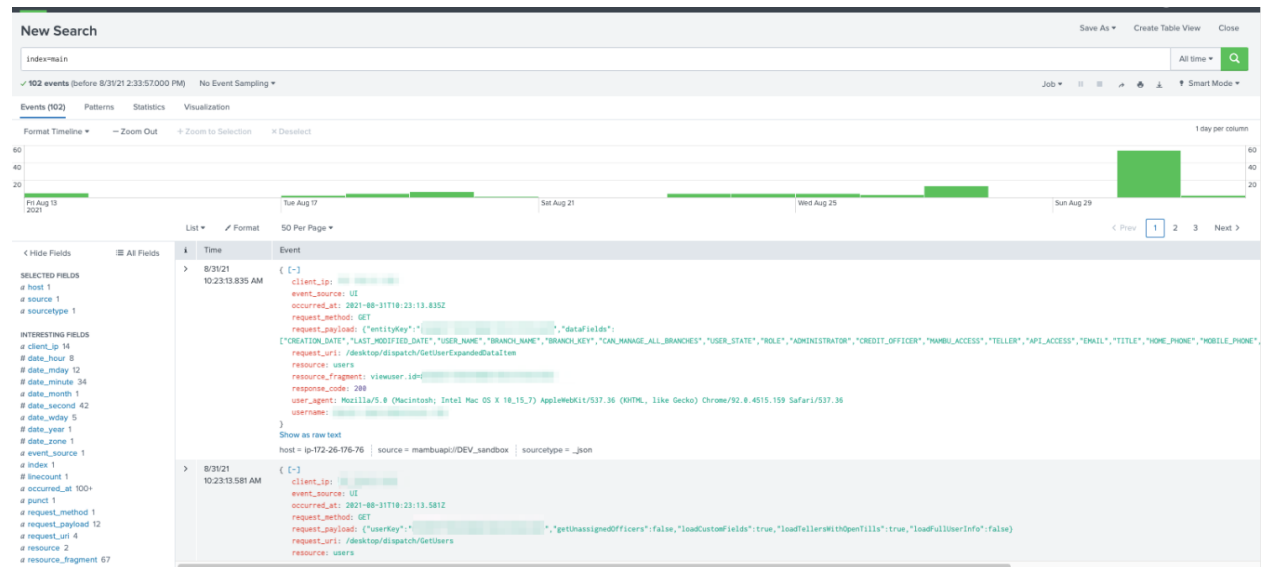
1 Input

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...



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:

The screenshot shows the 'Access' tab in the Mambu configuration interface. Under the 'Preferences' sub-tab, several settings are visible: 'Timeout Session' is set to 120 minutes, 'Min Password Length' is 10 characters, and 'API Key Rotation Grace Period' is 1800 seconds. There are three unchecked checkboxes for 'Automatic Expiry of User Passwords', 'Automatic Expiry of API Consumer Keys', and 'Lock User After Failed Logins'. The 'IP Access Restrictions' section is highlighted with a red box and contains the following elements: a checked checkbox for 'Whitelist approved IP Addresses', a large empty text area for IP addresses, a small input field, and 'Add', 'Edit', and 'Delete' buttons. Below this, the 'Apply To' section has 'Admins' unchecked and 'Users' and 'API' checked. The 'Show / Hide blocked IPs' checkbox is also checked. At the bottom, there is a 'Blocked IPs' label and an empty text area.

General Setup Financial Setup Organization **Access** Products Fields Views SMS Email Webhook

API Consumers Roles Users **Preferences**

Timeout Session [?]
 minutes

Min Password Length
 characters

API Key Rotation Grace Period [?]
 seconds

☐ Automatic Expiry of User Passwords [?]

☐ Automatic Expiry of API Consumer Keys [?]

☐ Lock User After Failed Logins [?]

IP Access Restrictions

☒ Whitelist approved IP Addresses

Add **Edit** **Delete**

Apply To ☐ Admins ☒ Users ☒ API

☒ Show / Hide blocked IPs

Blocked IPs

For more information check the [Mambu's Access Preferences documentation](#)