crest(data)

Splunk To Datadog Migration Platform User Guide

Last Updated: 10/07/2024

Contact Information

USA

Crest Data
3031, Tisch Way, #602,
San Jose, CA 95128

India

Crest Data Pvt. Ltd.
CDS House, Sarkhej - Gandhinagar Hwy,
Nr. Sanand - Sarkhej Road, Makarba,
Ahmedabad, Gujarat 382210

Have any feedback or questions for us? Reach us at https://www.crestdata.ai/contact-us

Table Of Content

Overview

The Splunk to Datadog Migration Platform is an advanced software tool engineered to streamline the process of transitioning visualizations from Splunk to Datadog. Both Splunk and datadog are robust solutions for handling and interpreting substantial datasets. However, the intricacies involved in migrating visualizations arise due to the disparate system architectures and distinct query languages utilized by each platform.

The platform serves as an intermediary, enabling users to effortlessly convert and migrate their Splunk visualizations—encompassing dashboards, charts, and graphs—into formats compatible with Datadog. It significantly simplifies the migration workflow by automating the conversion process. This includes the translation of Splunk-specific configurations and syntactic elements of queries into their Datadog counterparts, ensuring functional and visual fidelity.

Goals

The principal objective of the Splunk to Datadog Migration Platform is to demystify and simplify the complex task of migrating visualizations between two leading data analytics platforms. It is designed to streamline the transition, making it more accessible and less error-prone for organizations.

The ultimate aim of this platform is to facilitate an untroubled and efficient migration experience. Organizations seeking to transition from Splunk to Datadog for their data analysis requisites will find their journey greatly eased by the functionalities offered by this migration tool. It ensures that the valuable insights represented in Splunk visualizations are preserved and seamlessly adapted to the Datadog environment.

Prerequisites

Data should be available & should be in sync between both the platforms before starting the migration journey.

Ensure you have access to your Splunk account with sufficient permissions to read the dashboards and queries.

Compatibility Matrix

Supported Splunk Versions

	Minimum Supported Version	Maximum Supported version
Splunk On-Prem	9.0.0	9.3.0
Splunk Cloud	9.0.0	9.3.0

Migration Capabilities and Limitations

Splunk to Datadog Migration Options

Remote Option:

- Supports migration of Dashboards & Alerts.

Offline Option:

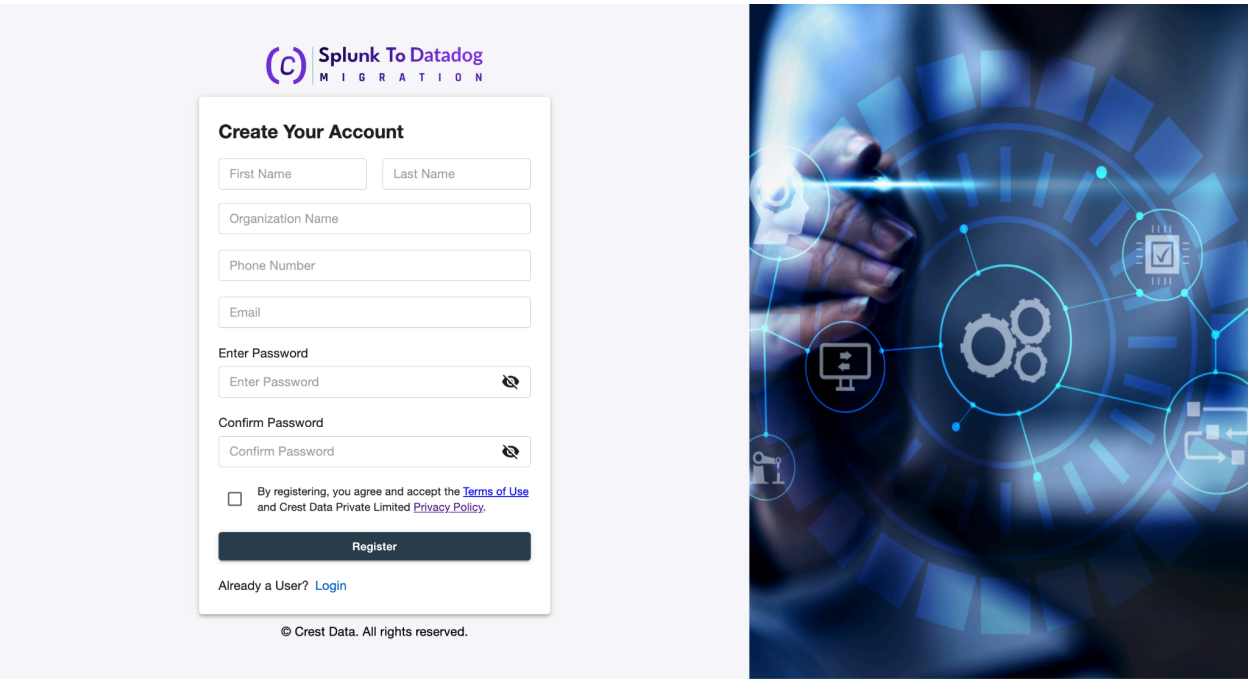
- Supports migration of dashboards using `.zip` or `.tar` files.
- Supports migration of any type of query, including panel and saved search queries, using `.csv` files.

Configuration Guide

I. Signing Up

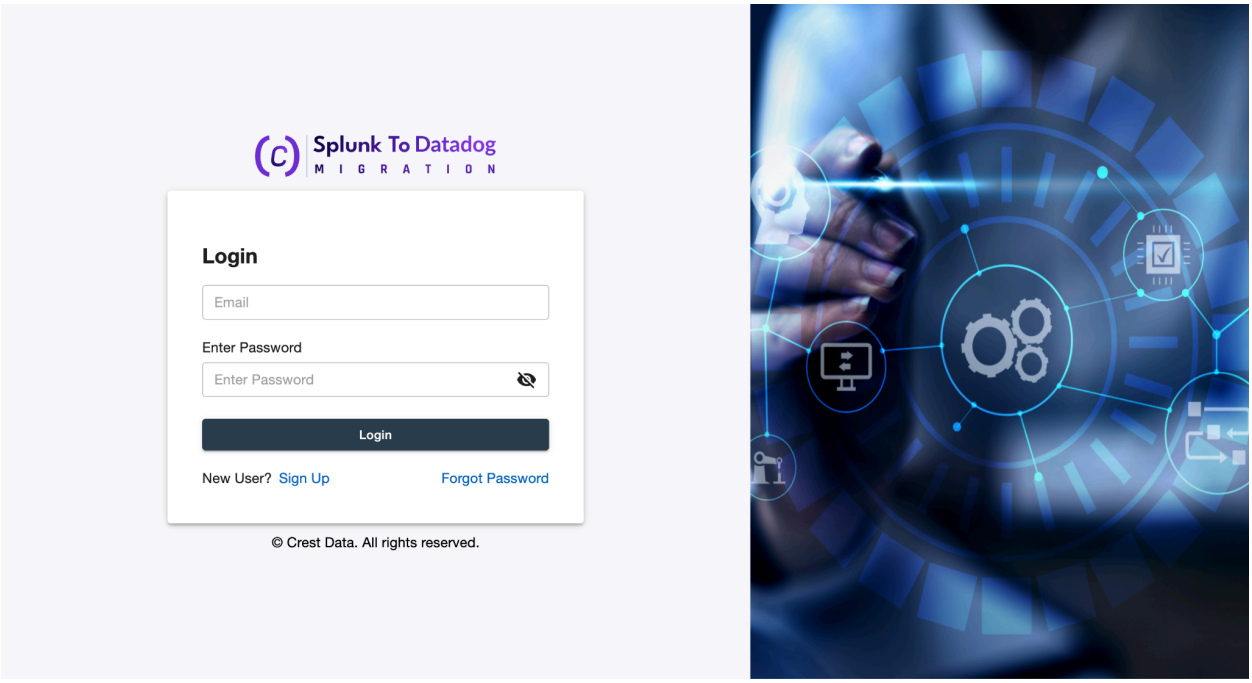
- Enter your First name, Last name, Organization name, phone number, Organization email address, Address & a secure password.
- Accept the Terms of Use.
- Email and password are required to login so keep them handy and other details would be part of your invoice.
- Hit the Register button to submit your form and create a user.

- A verification mail would be sent to your organization email address. If not found in inbox check spam and mark it as not spam to click on the button.
- You will be redirected to the login page once the email is verified successfully.



II. Login

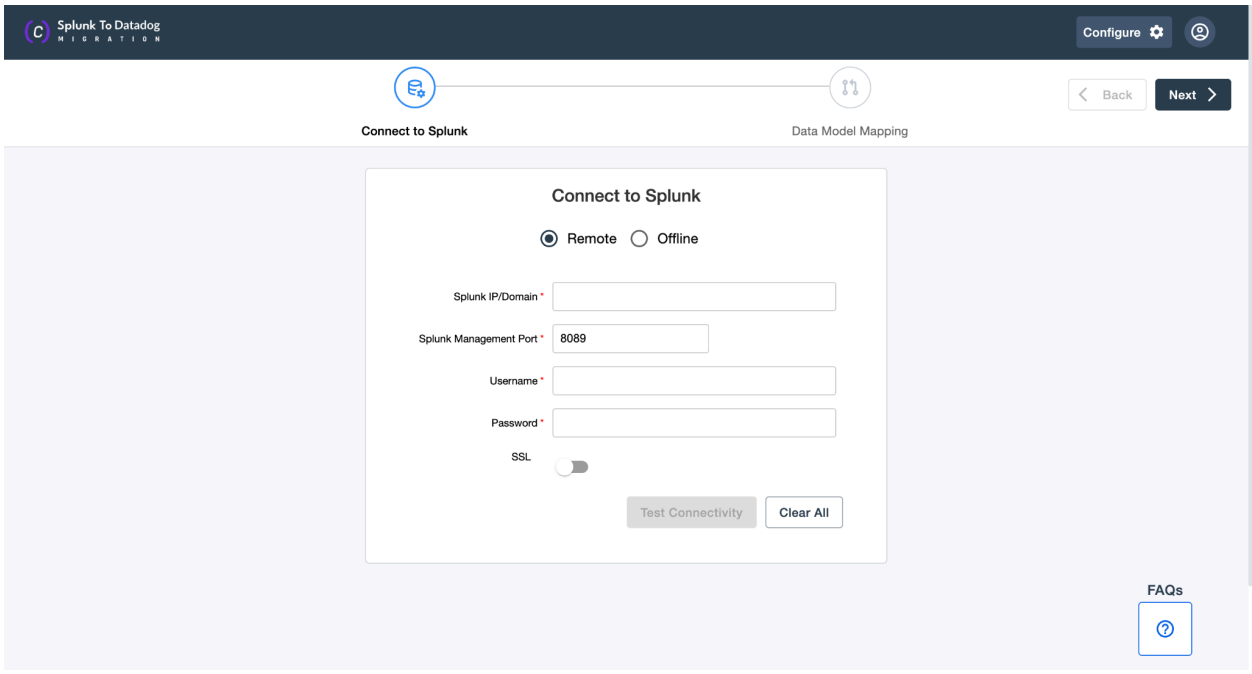
- Enter email address and password
- Hit login to start exploring



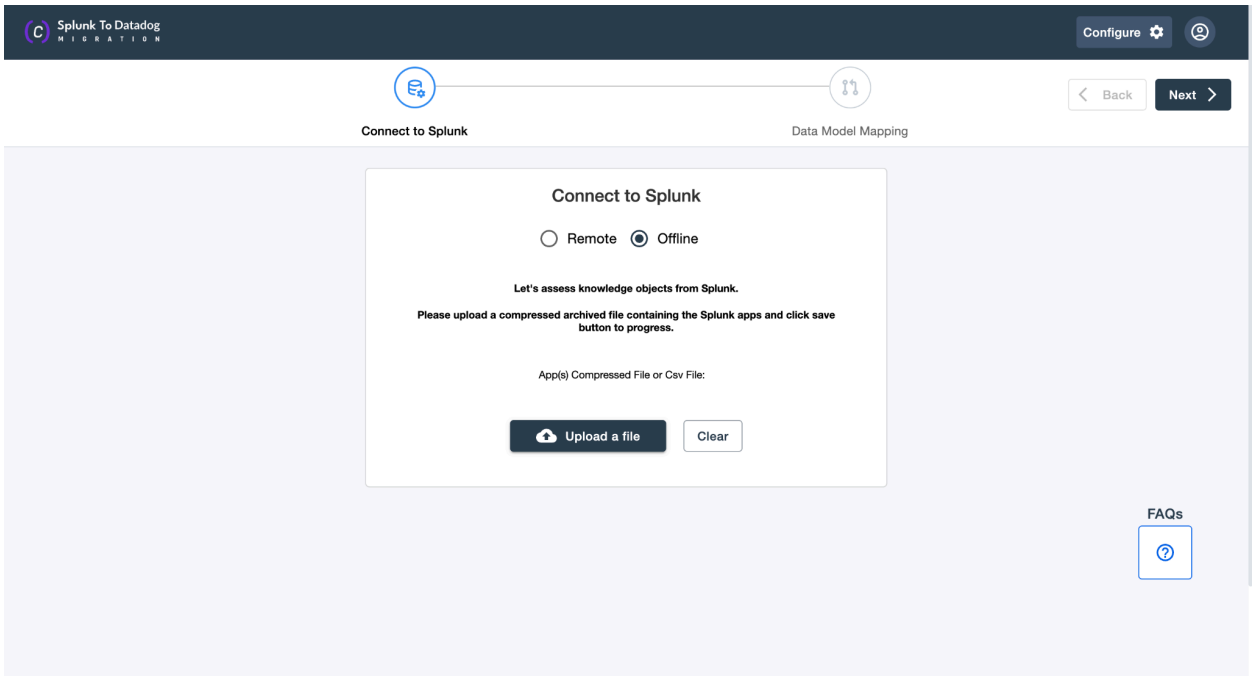
III. Configuration Wizard

Configure Splunk: We require splunk details to fetch Apps/Dashboards/Panels for a particular instance. User will have two options to provide those details

- **Option-1: Splunk Remote:** For Splunk Remote we need a few details mentioned as below
    - **Splunk IP/Host:** We will request apps/dashboards/panels (artifacts) from this IP/host
    - **Splunk Management Port:** Port is as critical as host and we need this to request data.
    - **Splunk Username:** The data will be fetched from the user which you mentioned in the username field as we might have multiple users for one splunk instance.
    - **Splunk Password:** Enter the Password for the Username that you configure above so we can get access to the artifacts
    - **Splunk SSL:** Enable this to make secure requests to your splunk deployment.
    - **Splunk SSL Pem file:** Upload the .PEM file to make secure request which host can identify



- **Option-2: Splunk Local:** For Splunk local you need to upload the tar.gz or .tgz file which has the Splunk apps in it
    - **.tgz/tar.gz File:** Upload the file and the platform will extract the file to get the artifacts i.e. apps/dashboards/panels

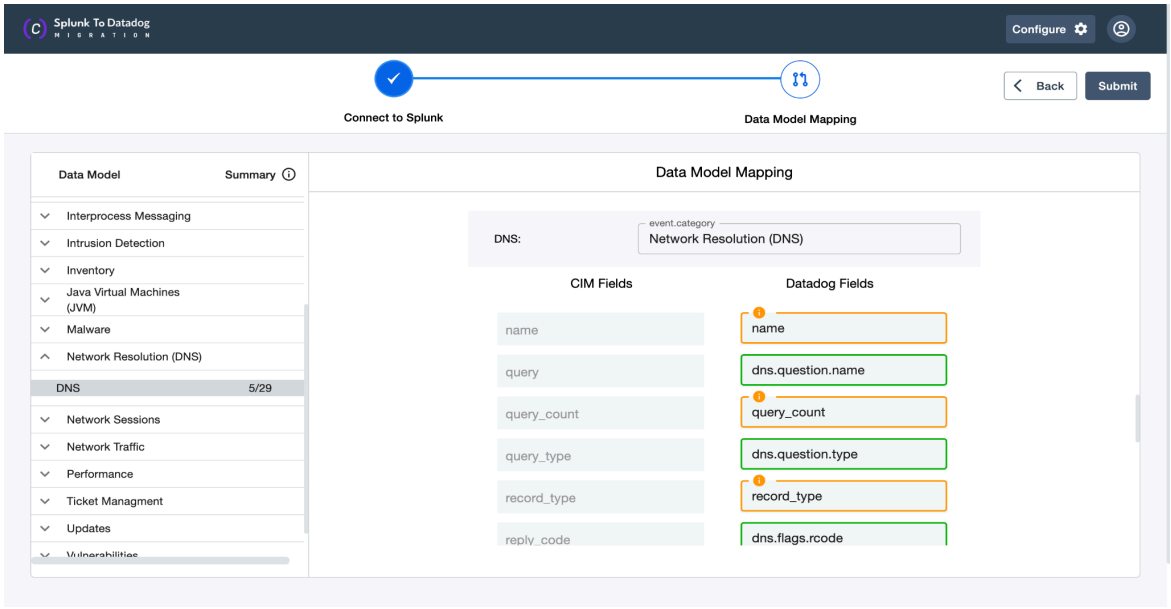


NOTE: Upon entering and saving your Splunk instance details into the platform, the synchronization process will commence automatically. This process is designed to retrieve artifacts from the specified Splunk instance for subsequent migration activities.

NOTE: When undertaking the migration of several applications or dashboards from different Splunk instances, it is essential to configure each one individually. Furthermore, migration is contingent upon the completion of payment for each app or dashboard that is being transferred. It is important to be cognizant of the fact that any unpaid assessments and their associated statuses will be expunged from our database in the event of changes to the configuration settings, such as the IP address, Port number, or Username. Users are encouraged to ensure all assessments are paid for before making any such changes to avoid loss of data.

CIM-Datadog standard Field Mapping: The Common Information Model and Datadog standard Field Mapping is a critical procedure that encompasses the alignment of field names from Splunk to the canonical fields defined by the Datadog standard fields. This meticulous process of field correlation guarantees the standardization and coherence of data drawn from various types and sources. It is particularly vital when utilizing the tstats command in Splunk, as this command is integral to querying data models and datasets.

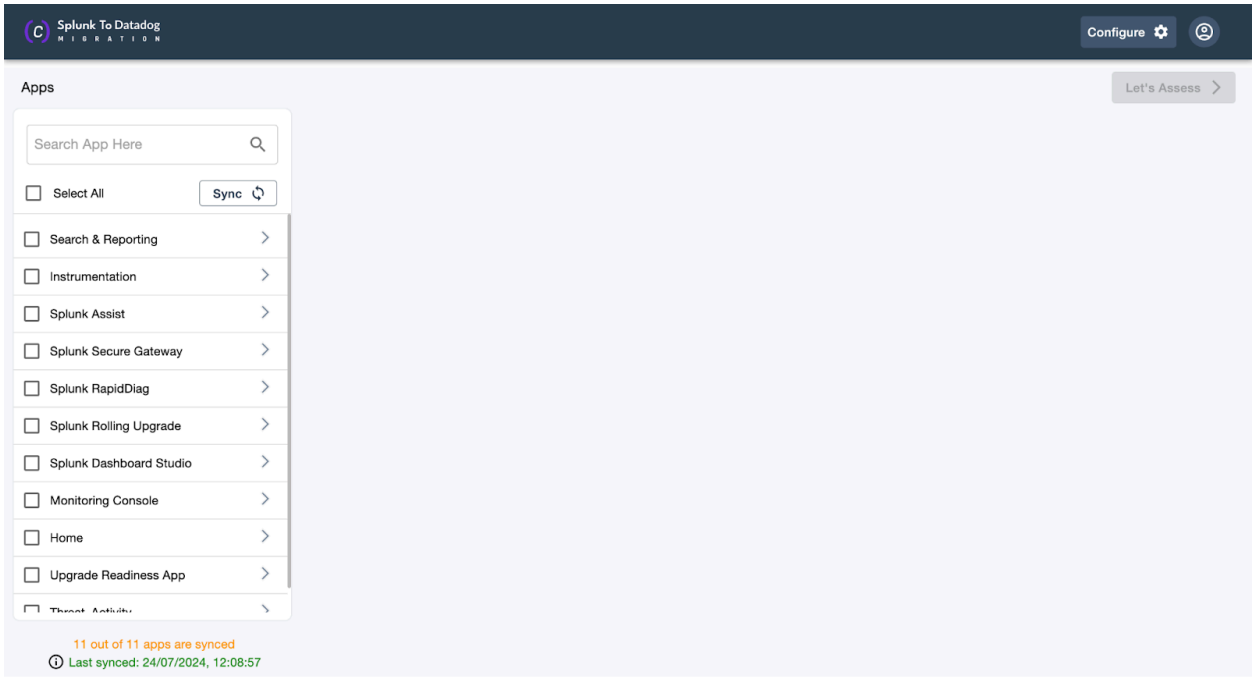
- On the current interface, the left-hand side displays a hierarchical arrangement of all data models and datasets. The "Summary" section indicates the count of fields for which the CIM-Datadog standard field mapping has been confidently established in relation to the total number of fields available.
- By selecting a specific dataset, you will be directed to the CIM-Datadog standard field mapping interface. Here, it is imperative that you review and, if necessary, adjust the mappings to ensure accuracy and relevance.



NOTE: Upon saving your configuration settings, you will be automatically redirected to a page that displays all the Splunk applications sourced from the configured IP address or from an uploaded local file.

IV. Sync Apps

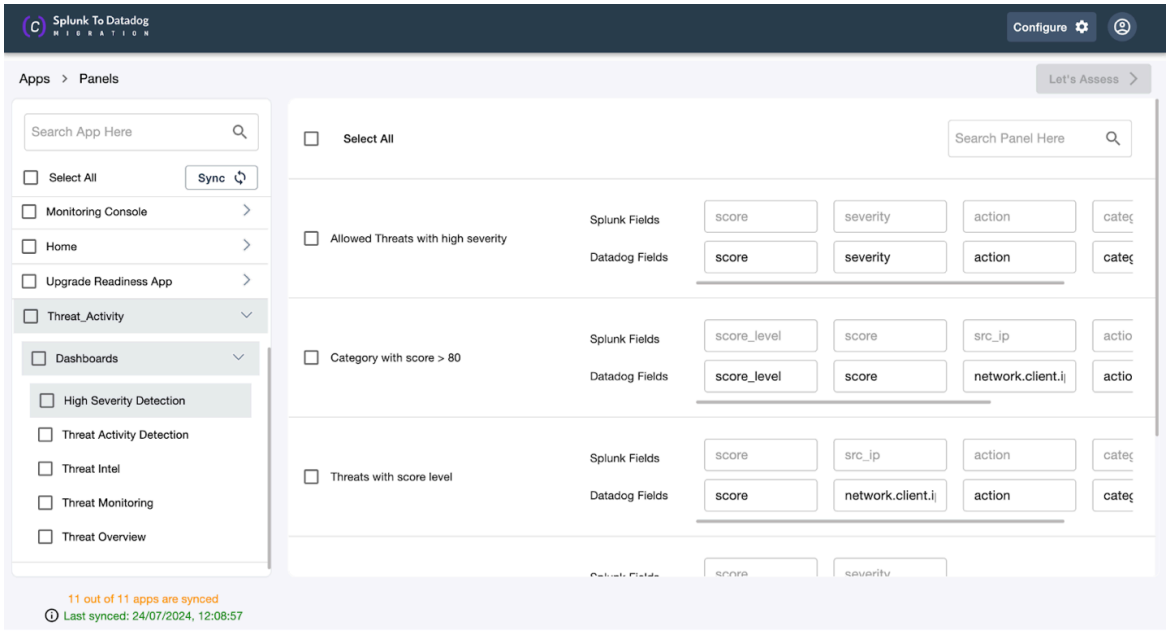
Sync Apps/Dashboard/Panel: To ensure comprehensive synchronization, it is necessary to identify the dashboards and panels within Splunk applications that require updating. This identification process should include all associated visualizations and the specific fields utilized within those visualizations.



The Apps listing page presents an overview of all applications. Once the synchronization process is complete, you may search for your specific app.

- Click on the app to see its dashboards
- Click on the particular dashboard to see the panels belonging to that dashboard.
- You will see all the panels and their **fields mapping**. You need to select the panels that you want to migrate and verify the mappings.

Field Mapping: The field mapping procedure must account for discrepancies in field names or structural differences between Splunk and Datadog. This can necessitate the formulation of custom mappings or the application of transformations to achieve precise correspondence between the data representations in the two systems.



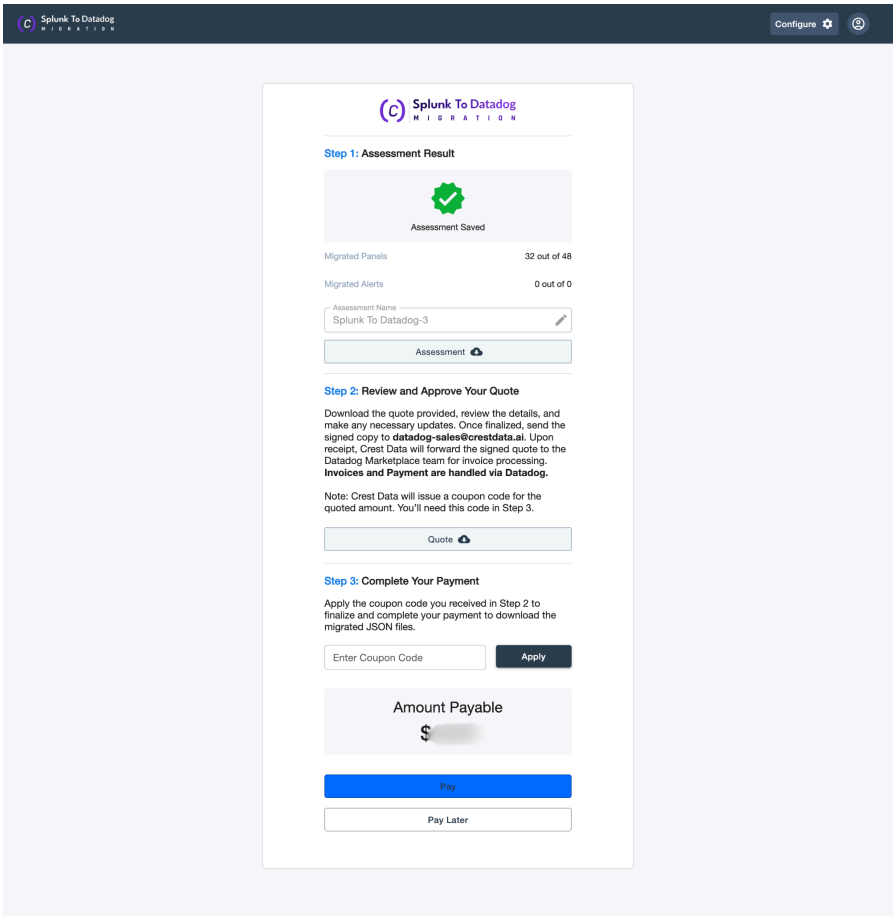
NOTE: Once you're ready with your selection Click on the "Let's Assess" button top right corner.

V. Assessment Process

Automated Conversion: The platform is equipped with a sophisticated translation engine that applies a predefined set of conversion rules or logic to transform Splunk-specific visualizations, including dashboards and charts, into formats that are compatible with Datadog

For instance:

The platform identifies Splunk-specific chart types, such as bar charts, line graphs, pie charts, and others. It then converts these visual elements into the corresponding visualization types recognized by Datadog, ensuring that the visual representation of data is maintained.



Query Translation:

The platform internally performs the query translation by converting the Splunk queries and search language into Datadog's equivalent query language. The platform examines Splunk queries, dissecting the syntax and structure to grasp the various elements, such as operators and functions, within the search language. It then executes a set of predefined translation rules and logic to adapt Splunk-specific syntax, like commands, operators, and functions, into the equivalent constructs in Datadog JSON.

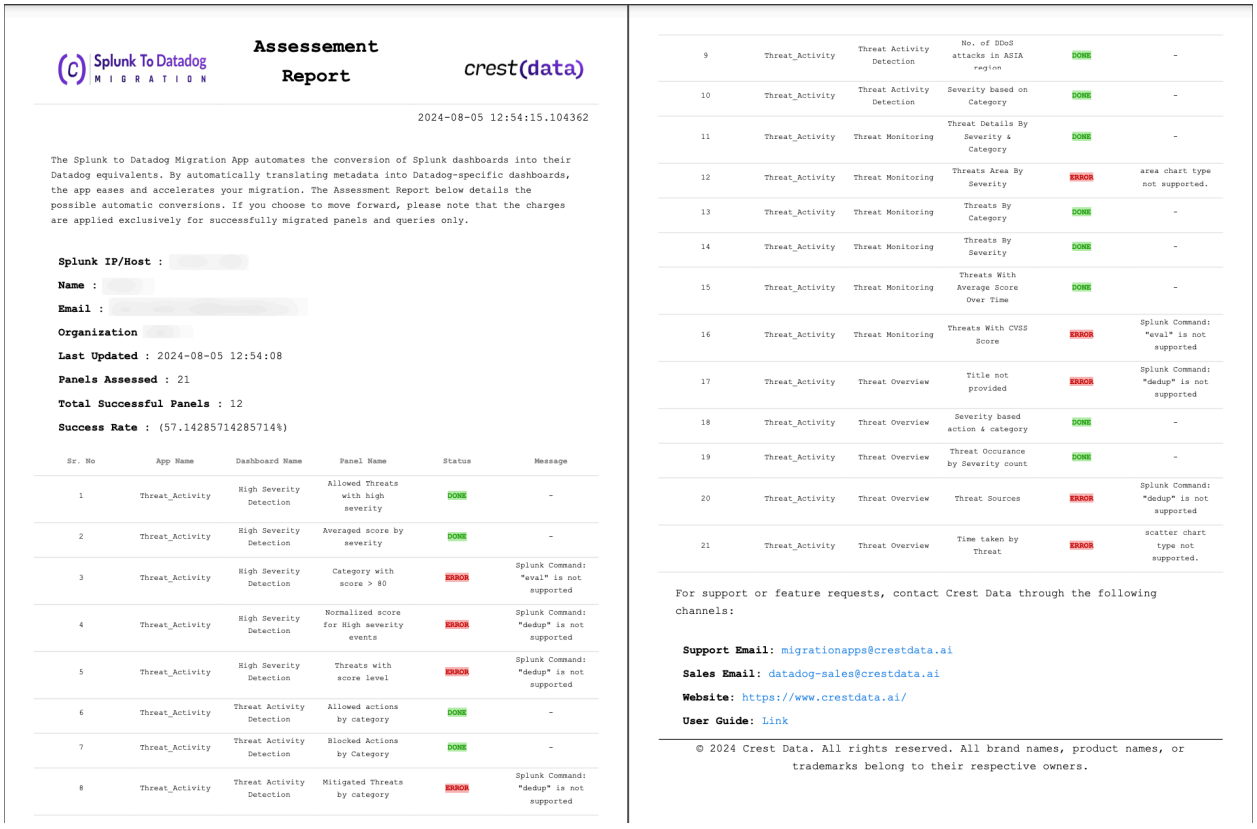
Edit Assessment Name: Users will be provided with the ability to customize the name of the assessment they create.

Assessment Report:

Users will have the option to download an assessment report that details which panels can be migrated and which cannot, along with explanations for any errors.

Note that users will only be charged for panels for which the platform can perform a successful migration; the platform will not require payment for panels that cannot be migrated.

The assessment report acts as an in-depth record, often in PDF format, summarizing the outcomes of the panel conversion process from Splunk to Datadog. It includes a thorough account of successful migrations as well as any errors or failures, accompanied by detailed descriptions of any conversion issues, potentially with error codes, messages, or logs for further clarity on the unsuccessful conversions.



Splunk To Datadog MIGRATION

Assessement Report

crest(data)

2024-08-05 12:54:15.104362

The Splunk to Datadog Migration App automates the conversion of Splunk dashboards into their Datadog equivalents. By automatically translating metadata into Datadog-specific dashboards, the app eases and accelerates your migration. The Assessment Report below details the possible automatic conversions. If you choose to move forward, please note that the charges are applied exclusively for successfully migrated panels and queries only.

Splunk IP/Host :
Name :
Email :
Organization
Last Updated : 2024-08-05 12:54:08
Panels Assessed : 21
Total Successful Panels : 12
Success Rate : (57.142857142857142%)

Sr. No	App Name	Dashboard Name	Panel Name	Status	Message
1	Threat_Activity	High Severity Detection	Allowed Threats with high severity	DONE	-
2	Threat_Activity	High Severity Detection	Averaged score by severity	DONE	-
3	Threat_Activity	High Severity Detection	Category with score > 80	ERROR	Splunk Command: "eval" is not supported
4	Threat_Activity	High Severity Detection	Normalized score for High severity events	ERROR	Splunk Command: "dedup" is not supported
5	Threat_Activity	High Severity Detection	Threats with score level	ERROR	Splunk Command: "dedup" is not supported
6	Threat_Activity	Threat Activity Detection	Allowed actions by category	DONE	-
7	Threat_Activity	Threat Activity Detection	Blocked Actions by Category	DONE	-
8	Threat_Activity	Threat Activity Detection	Mitigated Threats by category	ERROR	Splunk Command: "dedup" is not supported
9	Threat_Activity	Threat Activity Detection	No. of DDoS attacks in ASIA region	DONE	-
10	Threat_Activity	Threat Activity Detection	Severity based on Category	DONE	-
11	Threat_Activity	Threat Monitoring	Threat Details By Severity & Category	DONE	-
12	Threat_Activity	Threat Monitoring	Threats Area By Severity	ERROR	area chart type not supported.
13	Threat_Activity	Threat Monitoring	Threats By Category	DONE	-
14	Threat_Activity	Threat Monitoring	Threats By Severity	DONE	-
15	Threat_Activity	Threat Monitoring	Threats With Average Score Over Time	DONE	-
16	Threat_Activity	Threat Monitoring	Threats With CVSS Score	ERROR	Splunk Command: "eval" is not supported
17	Threat_Activity	Threat Overview	Title not provided	ERROR	Splunk Command: "dedup" is not supported
18	Threat_Activity	Threat Overview	Severity based action & category	DONE	-
19	Threat_Activity	Threat Overview	Threat Occurance by Severity count	DONE	-
20	Threat_Activity	Threat Overview	Threat Sources	ERROR	Splunk Command: "dedup" is not supported
21	Threat_Activity	Threat Overview	Time taken by Threat	ERROR	scatter chart type not supported.

For support or feature requests, contact Crest Data through the following channels:

Support Email: migrationapps@crestdata.ai
Sales Email: datadog-sales@crestdata.ai
Website: https://www.crestdata.ai/
User Guide: Link

VI. Quote Generation

Review and Approve Your Quote

Download the quote provided, review the details, and make any necessary updates. Once finalized, send the signed copy to datadog-sales@crestdata.ai. Upon receipt, Crest Data will forward the signed quote to the Datadog Marketplace team for invoice processing. Invoices and Payment are handled via Datadog

crest(data)

Quote

crest(data)

Crest Data Systems Pvt Ltd.
Email : datadog-sales@crestdata.ai
Date : 2024-09-18

Customer Organization:
Customer Contact:
Billing Address

Customer Contact Name	
Customer Email	

Quote Expiration	2025-09-18
Start Date of Service	2024-09-18
End Date of Service	2025-09-18
Payment Frequency	One-Time
Payment Term	Net 30
Payment Method	Invoice

COMMITTED SERVICES

Fees for Committed Services are based on quantities purchased, not actual usage, at the Sales Prices listed below.

SERVICE/FEATURE	QUANTITY	UNIT LIST PRICE	TOTAL PRICE
Dashoboard - Panels OR Query	3	$	$
Alerts	2	$	$
		NET AMOUNT DUE:	**$ USD**

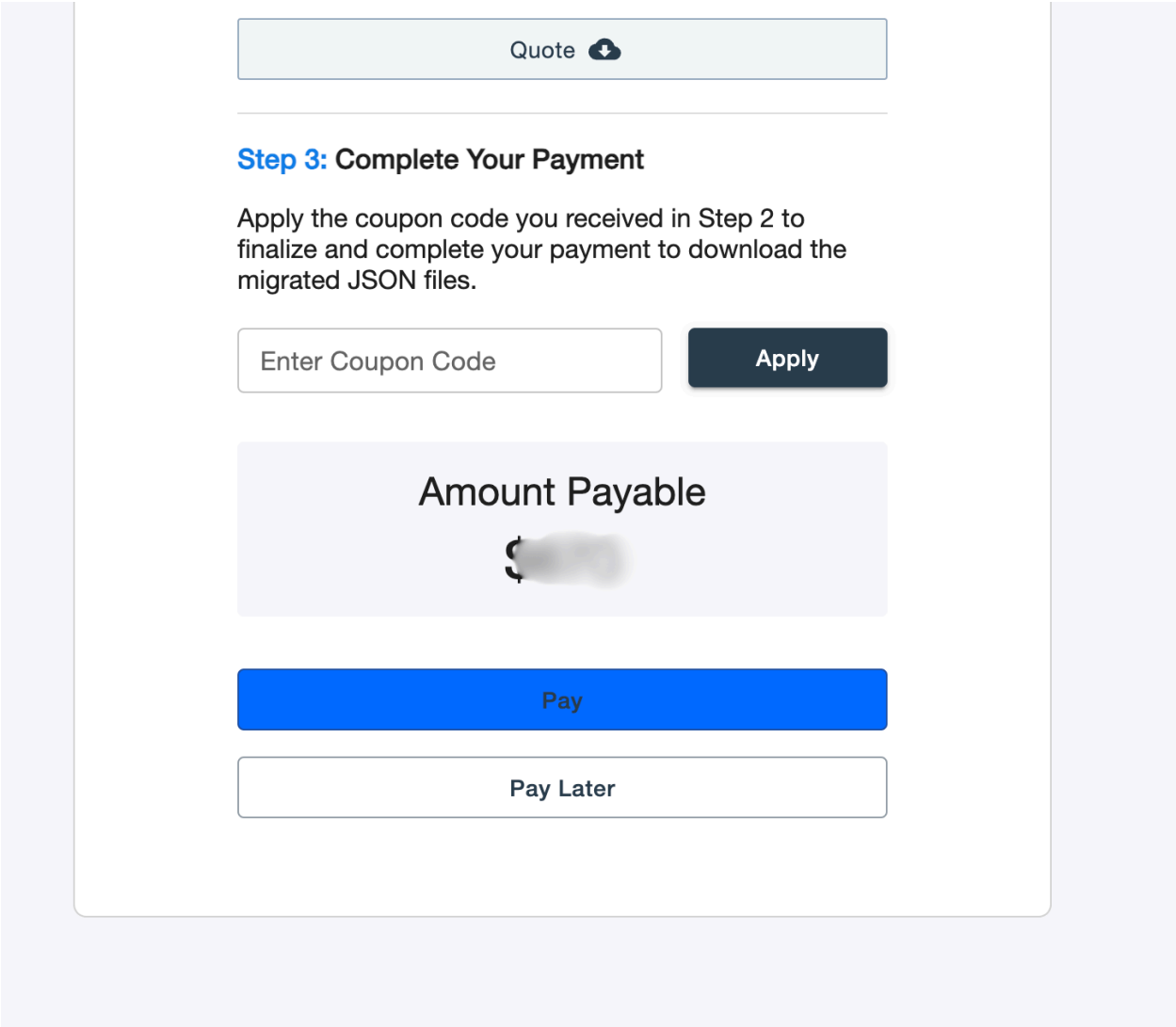
The Net Amount Due will be due and payable according to the Payment Frequency, Term, and Method stated above. This Quote will become effective when signed by both Parties. Unless both Parties sign this Quote, the pricing and terms offered in this Quote expire on the Quote Expiration date stated above.
Invoices and Payment are handled via Datadog.

Customer:	Supplier: **Crest Data Systems Pvt Ltd.**
By :	**By :**
Name :	**Name :**
Title :	**Title :**
Date :	**Date :**

VII. Payment Process

Success-Based Billing: The billing model is structured so that charges are applied exclusively for panels that have been successfully and fully translated from Splunk to Datadog. Panels that do not convert successfully or need additional modifications will not be included in the payment calculation.

Note: Currently, the platform supports the payment through Coupon Codes only. Once the Payment is completed & invoice is generated by Datadog, Admin from the Crest will generate a coupon for the user to make the payment.



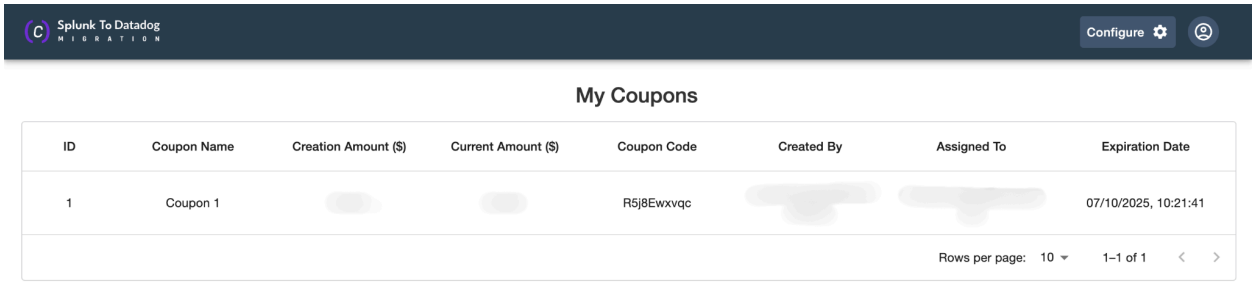
VIII. Coupon Code

Users can get/retrieve the coupons by following ways:

1. **Email Notification**: Once Crest Data issues a coupon, you will receive an email notification with the coupon details. Be sure to check your inbox for this information.

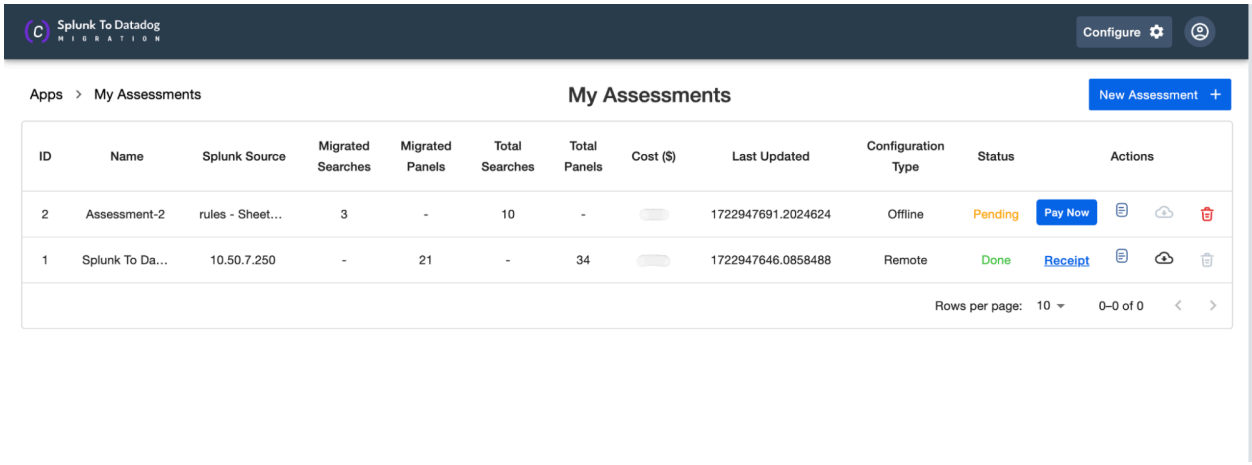
2. **Coupon Page**: You can also find all available coupons listed on the **My Coupons** page within your account. This page will display all active coupons along with their expiration dates and any applicable usage restrictions.

Make sure to check both the email and the coupon page for the latest coupons.



IX. My Assessments

List of all the Paid/Unpaid Assessments: Users will be presented with a list displaying all assessments, distinguishing between those that are paid and unpaid, along with various actionable options. From this interface, users will have the capability to settle payments for their outstanding assessments.



Invoicing or Billing Statements: Users will be provided with the functionality to download invoices or billing statements, which will itemize the count of successfully converted panels along with the associated fees. These documents will also specify the payment deadline and include any additional pertinent billing details.

Exporting as a Zip File: Users can begin the export procedure, which compiles the visualizations—like dashboards, charts, or reports—into a compressed zip file. The resulting zip file organizes the exported visualizations in an orderly fashion. Within the archive, each visualization may be encapsulated in an individual file or a set of files.

NOTE: The Zip file containing the visualizations can be downloaded only after payment has been made for the respective assessment.

- **Uploading the json File:** Users commence the upload procedure for the json file(s) that embody the visualizations. This process may require utilizing designated tools or interfaces that the Datadog system offers to import these json files.

Delete Assessment: Users will have the option to delete assessments that have not been paid.

Troubleshooting Guidelines

1. Encountering difficulty accessing the system due to login issues.

The user must be registered and should login with valid credentials.

Incase of a new user registration or losing your password, please reach out to <> inorder to reset your password.

2. Encountering connectivity issues during the configuration of Splunk, receiving an error indicating that Splunk is unreachable.

Make sure that the provided splunk details are correct, the Splunk IP should not have scheme or any leading or trailing slash and is reachable in the same network.
In order to configure Splunk remotely, the Splunk machine must have sufficient storage available to run the queries used to fetch the app dashboards into our platform.

Check the “Messages” on your Splunk Machine to confirm if there is any warning regarding insufficient space. If it is the case, kindly free some space for our platform to run queries successfully to fetch the app details.

3. Is there an alternative method for configuring Splunk that does not necessitate the disclosure of credentials?

If you prefer not to disclose your Splunk details, kindly select the “Splunk Local” as an alternative option.

4. How can I generate a tarball file of my Splunk machine

1. Go to the apps directory under splunk directory i.e. "$SPLUNK_HOME/etc/apps"

2. Run the following command from the apps folder

"sudo tar -cvf <tar_file_name>.tar.gz <app1_name> <app2_name> <app3_name>"

5. Encountering difficulty in saving the configuration with SSL enabled.

Confirm the SSL certificate file is correct.
If still issue persist contact our support at migrationapps@crestdata.ai

6. Following a successful configuration, the Dashboard page displays "No Apps Found."

Once the Splunk configuration is saved successfully, the process of fetching the app's details from the Splunk machine is initiated which would reflect on the

Dashboards page. The app is made visible on the UI once it is synced with complete details and is ready to undergo the migration process. Hence, incase of apps with huge dashboards, it would take a considerable amount of time to reflect on the UI.

7. I am not able to see the apps coming real-time after the synchronization process.

Once an app is synced successfully, it will be visible to the user without the need of page refresh. If page refreshes are required to update the Dashboard page with synced apps, kindly contact your IT team and get the host of our application whitelisted from the “Netscope Client” or similar installed on your system.

8. The sync button continues to display a loading state.

The sync button keeps loading until the ongoing sync process finishes successfully.

9. Among a total of n apps present on the splunk machine, the platform has successfully synchronized only m apps.

Incase of total n apps installed on your Splunk machine, only those apps will be fetched that have XML files with at least one panel in it.

10. Sync takes a long time to finish the process.

Incase of apps with huge dashboards, the sync process takes a considerable amount of time to finish its process.

11. Can I stop the sync process?

Currently, there is no way to stop an ongoing sync process. The process itself finishes once all the apps are synced successfully.

12. I am unable to start a new sync process.

Incase of an ongoing sync process, the user will not be able to initiate a new process until the previous process finishes.

13. What does partially synced mean?

Partially synced refers to an ongoing sync process where some apps have been synced completely and are ready to be migrated whereas the sync process of other apps are in progress.

14. Why do I see different App counts between local and remote configurations of Splunk?

The total app count varies sometimes between local and remote configurations in Splunk.

15. Why can I not see some filters/dashboard inputs of a dashboard?

Since static dashboard inputs do not have any fields to map, they are processed in the backend itself and are not visible to the user on UI.

16. How can I fetch new apps from my splunk instance?

Three ways to fetch new apps from existing Splunk configuration.
> Click on the “sync” button which would just fetch the new apps that are not present in the platform
> Select app/s and click on the “sync” button to resync them and fetch new apps that are not present in the platform
> Select all the apps and click on the “sync” button to resync all of them and fetch new apps that are not present in the platform.

17. How can I resync app/s to retrieve their latest updates?

Select the app to be resynced and click on the “sync” button which would fetch the latest details of the app and other new apps that are not present in the platform.

18. Why can I not see the app/s that I just resynced?

On resyncing the selected app/s, the platform runs a query on the Splunk machine with the app name and if the app is not present on the Splunk machine, it gets removed from our platform as well and hence, it gets removed from the list.

19. What happens when I update my configurations?

On updating the Splunk IP/domain or the Splunk Management Port for existing Splunk IP or the Splunk username for existing Splunk IP/domain, the sync process is initiated again and the current apps collection gets dropped. Additionally, all the unpaid assessments for that configuration are removed.

20. What is the significance of the status icons appearing alongside my synchronized apps?

Once an app undergoes the migration process and an assessment is created for the same, the app gets a status icon next to it indicating if it is successfully migrated, partially migrated or completely failed to migrate. This helps the user to understand progress made with the migration process on the apps.

21. Why did the status of migrated apps get reset?

On resyncing the app or initiating a global sync for the same Splunk configuration, the app is dropped from the platform and synced again which causes the status icon to reset.

22. What can I do for my failed migrated panels?

The migration for some panels may fail because of the limitations mentioned in the guide. If you still require those failed panels to migrate successfully, you can reach out to migrationapps@crestdata.ai OR datadog-sales@crestdata.ai to get it migrated manually.

23. I am unable to find my unpaid assessments.

Unpaid assessments shall be removed from the records once you update either of the configurations, Splunk or Datadog. Moreover, you can also delete unpaid assessments manually.

24. I am unable to export the migrated dashboards.

Migrated Dashboards can be exported only after the payment is done successfully. Incase of any other error, kindly reach out to migrationapps@crestdata.ai OR datadog-sales@crestdata.ai.