Oracle® Financial Services Investigation Hub

Administration and Configuration Guide

Release 8.0.7.1.0

December 2019

ORACLE

Administration and Configuration Guide, Release 8.0.7.1.0

Copyright © 2019 Oracle and/or its affiliates. All rights reserved.

Primary Author: Arpana Danayak

Contributor: Pankaj Chhangwani, Swetha Yatham, Parthik Davda

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Document Control

This section provides the revision details of the document.

Version Number	Revision Date	Changes Done
8.0.7.1.0	Created: December 2019	Created the first version of the Investigation Hub Administration Guide for 8.0.7.1.0 Release.

This document provides functional information about the Investigation Hub application and enables you to navigate through the various sections of the application. The latest copy of this guide can be accessed from the Oracle Help Center (OHC) Documentation Library.

About this Guide

This guide gives comprehensive instructions for system administration, daily operations, and maintenance of Oracle Financial Services Investigation Hub application. This section focuses on the following topics:

Who Should Use This Guide

This guide is intended for administrators and implementation consultants. Their roles and responsibilities, as they operate within Investigation Hub, include the following:

- Implementation Consultant: Installs and configures the Investigation Hub application at a deployment site. The consultant also installs and upgrades any additional Oracle Financial Services solution sets, and requires access to deployment-specific configuration information. For example, machine names and port numbers.
- System Administrator: Configures and maintains the system. The System Administrator maintains user accounts and roles, monitors data management, archives data, loads data feeds, and performs post-processing tasks. In addition, the System Administrator also reloads the cache.

Scope of This Guide

This guide describes the physical and logical architecture of the Investigation Hub application. It also provides instructions for maintaining and configuring Investigation Hub, its subsystem components, and any third-party software required for operations.

How this Guide is Organized

The Administration Guide includes the following chapters:

- About Oracle Financial Services Investigation Hub provides a brief overview of the Investigation Hub and its components.
- Managing User Administration provides the details on user roles.

- Loading Data to Graphs provides instructions on loading graphs.
- Configuring the Notebook Parameters describes the configurable notebook parameters.
- Additional Configuration details the additional configurations.

Where to Find More Information

This section identifies additional documents related to the Investigation Hub application. You can access the following documents from the Oracle Help Center (OHC) Documentation Library:

- *Oracle Financial Services Investigation Hub Release Notes Guide*
- *Oracle Financial Services Investigation Hub Installation Guide*
- *Oracle Financial Services Investigation Hub User Guide*

Conventions Used in this Guide

Conventions used in this guide and their associated meanings are listed in the following table.

Table 0–1 Conventions Used in this Guide

Convention	Meaning
Boldface	Boldface type indicates graphical user interface elements associated with an action (menu names, field names, options, button names), or terms defined in text or glossary.
Italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates the following: • Directories and subdirectories • File names and extensions • Process names • Code sample, that includes keywords, variables, and user-defined program elements within the text
<variable>	Substitute input value

Abbreviations Used in this Guide

Abbreviations used in this guide are listed here.

Table 0–2 Abbreviations and their meaning

Abbreviation	Meaning
OFS	Oracle Financial Services
T2T	Table to Table
AAI	Analytical Applications Infrastructure
PGX	Parallel Graph AnalytiX
PGQL	Property Graph Query Language
LHS	Left Hand Side

1

About Oracle Financial Services Investigation Hub

This chapter provides a brief overview of the Oracle Financial Services Investigation Hub (OFS IH) application.

This chapter covers the following topics:

Introduction

Oracle Financial Services Crime and Compliance Investigation Hub is an application built on FCC Studio which allows investigators to rapidly view the case and Adhoc information within the Financial Crime and Compliance Graph. The in-built scoring, matching and correlation engines create meaningful units of investigation and pre-configured red flags and risk factors target investigative effort effectively. The Financial Crime and Compliance Graph on which it is built accelerates investigations by bringing relevant information sources together, preventing the need for the manual collation of information from disparate sources for ad hoc investigations. Oracle Financial Services Crime and Compliance Investigation automatically generates case narratives and insights, highlights risk factors and red flags which are meaningful to the investigation and recommends actions based on graph scoring algorithms.

Key Features

- Pre-built user interfaces for case investigation, special and Adhoc investigations and sanctions
- Configurable red flags and risk factors to highlight key areas for investigation
- Case summary in narrative format and case recommendation
- In-built correlation and scoring algorithms
- Exploration of the financial crimes global-graph using an interactive and visual graph explorer tool
- Integrates fully with Oracle Financial Crimes Application Data and external data sources such as watchlist and company hierarchy data and is readily usable across the enterprise financial crimes data lake

- Built on Oracle Financial Service Crime and Compliance Studio which includes a highly scalable in-memory Oracle Graph Analytics Engine (PGX), AI and machine learning.
- Utilizes proven Enterprise Financial Crimes Graph model which accelerates financial crime investigation use cases

Administration and Configuration Activities

An administrator should configure the following Notebooks:

- **Publishing Graph:** Loads the graph into memory and publishes it so other notebooks can access and use it.
- **Special Investigations:** Enables the investigator to search for one or multiple names and/or addresses to examine the network, red flags, and risk factors
- **Level 2 Case Investigations:** Allows the investigator to explore a case - including graph, risk factors, and red flags.

Note: Administrator must share only the **Special Investigations** notebook to users (investigators) and users will clone the notebook for their investigation.

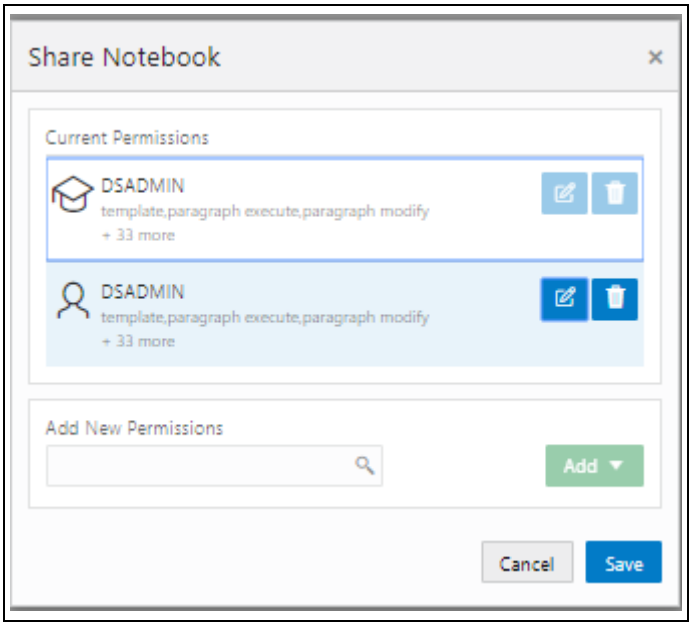
Providing Permissions to a Notebook

Share button allows you to share a notebook with another user, user group, or role. This option helps you to provide the permission of a notebook to specific user.

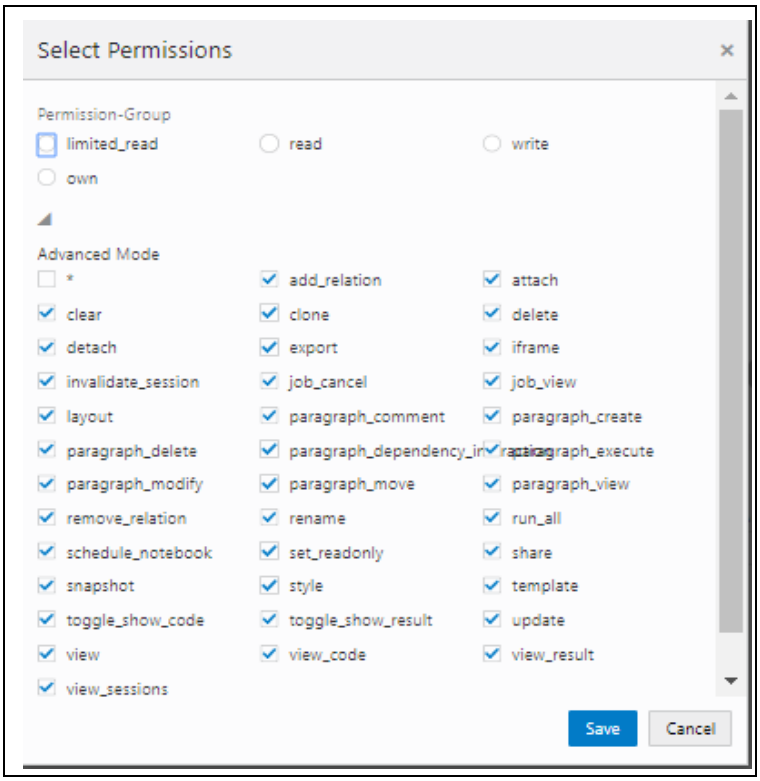
For more information on permissions, see the ***Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide***

To share a note, perform the following steps:

1. Navigate to Investigation Hub application home page.
2. Navigate to any notebook of application.
3. Click Share button.



4. Click **Add** icon.



5. Select the required permissions and click Save.

After sharing the notebook, an Investigator must clone the notebook and start using that notebook for investigation. For more information, see the Cloning of Notebook in *Oracle Financial Services Investigation Hub User Guide*.

2

Managing User Administration

This chapter provides information on creating users who can access the Investigation Hub application and execute batches required for Investigation Hub. You must create users and execute batches in the OFSAA environment.

User administration involves creating and managing users, and providing access to Investigation Hub based on assigned roles.

The following topics are covered in this section:

- Managing Identity and Authorization
- Granting Permissions

Managing Identity and Authorization

This section provides information on creating, mapping and authorizing users, and providing access to the Investigation Hub application.

This section covers the following topics:

- Identity and Authorization Process
- Creating and Authorizing User
- Mapping User with User Group

Identity and Authorization Process

Figure 2–1 shows the process flow of identity management and authorization.

Figure 2–1 Managing Identity and Authorization Process Flow

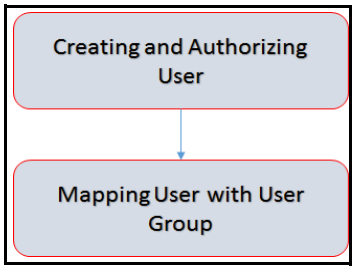


Table 2–1 lists the various actions involved in the user administration process flow:

Table 2–1 User Administration Process Flow

Action	Description
Creating and Authorizing User	Create a user by providing the user name, user designation, and the date during which the user is active in Investigation Hub.
Mapping User with User Group	Map user with a user group that provides the user with the privileges of the mapped user group.

Creating and Authorizing User

Users with SYSADMN and SYSAUTH functional roles can create and authorize users in Investigation Hub, respectively. For more information on creating and authorizing users, see *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

Granting Permissions

1. Log in to Oracle Database from sys as a SYSDBA user.
2. Execute the following command:

   ```
   grant execute dbms_rls to <Studio DB Username>
   ```

   The Execute permission is granted to VPD.
3. Execute the following command:

   grant create any context to <STUDIO_DB_USER_NAME>;

   The Create permission is granted to context.

3

Loading Data to Graphs

Graph load is used to create a graph from the underlying data. It gives the .pgb file and config.json of the GLOBALGRAPH, which are further used in Investigation Hub to view or query using PGQL and PGX interpreters. This chapter provides information on configuring graphs in the application.

Data is loaded from the landing area to the consolidated area in Investigation Hub using processors and they are called connectors. For more information, see the Configuring Data Sources for Graph of ***Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide*.**

Note: A new graph is loaded everyday, so you must run the **Load Graph** paragraph manually.

For more information on scheduling, see the Managing the batches section in ***Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide.***

This chapter covers the following sections:

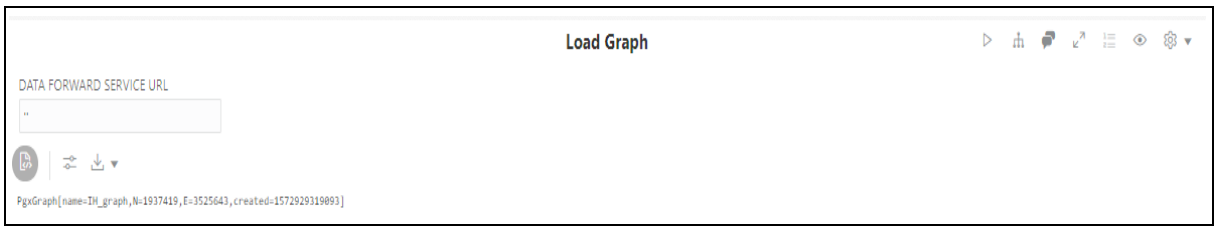
Loading the Graph

To load the data into the graphs, perform the following steps:

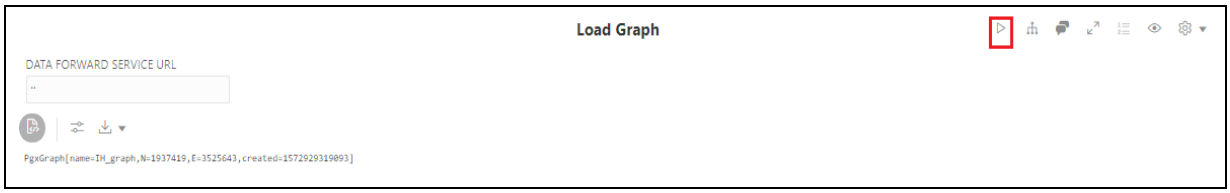
1. Login to the Investigation Hub application.
2. Click the **Investigation Hub** folder.
3. Navigate to the **Publishing Graph** notebook.
4. Enter the following details:

   DATA FORWARD SERVICE URL: URL of the config file created from the data forward service

   GRAPH NAME: Provide a graph name for the investigation hub graph



5. Click **Execute Paragraph** to execute the **Load Graph** paragraph.



6. Execute the P**ublishing Graph** notebook. See Configuring the Notebook Parameters.

The graphs will be loaded in IH. After executing the Publishing Graph notebook, generate the correlation network using the **Generate Correlated Networks** notebook. For more information, see **Appendix A**.

For more information on batch execution, see the Managing Studio Batches section in ***Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide***.

4

Configuring the Notebook Parameters

This chapter provides information on configuring the notebook parameters for Investigation Hub.

This chapter covers the following sections:

Configuring the Investigation Recommendation Score

Scoring is a methodology to calculate the score of events, correlation, and entity (for example, customer). You can define the score range based on which a case can be recommended for investigation. The investigation recommendation will be displayed on the **Recommendation** paragraph of the **Special Investigation** notebook.

For example,

If you have defined the investigation score range as 10-25 and case status as “Further Investigation”, then the case investigation recommendation will be set to “Further Investigation" when a case score falls in the 10-25 range.

To define the investigation recommendation, perform the following steps:

1. Click the **Investigation Hub** folder.
2. Navigate to the **Special Investigations** notebook.
3. Open the codes of **Initialization - I** paragraph and edit it as required. The following figure shows an example.

```
get_recommendation = { disp_score, red_flags, risk_factors,
    color = 'seagreen'
    ret = "Close Case (Reason: False Positive)"

    score = disp_score

    // TODO: Improve case recommendation logic
    if (disposition_score > 25 && disposition_score < 51) {
        ret = "Unknown - Further Investigation Needed"
        color = "gold"
    } else if (disposition_score > 50 && disposition_score <
        ret = "Special Investigation Needed"
        color = "darkorange"
    } else if (disposition_score > 76) {
        ret = "Consider Escalation"
        color = 'crimson'
    }
    return """<font color="${color}" style="font-weight:bold
}
```

4. Execute the paragraph.

An Investigator can view the investigation status based on this recommendation scoring.

Configuring the Red Flag

The Red Flag indicator suggests a potential problem with a business entity. When you see a red flag indication, you must view the investigation recommendation and take the appropriate action. The Red Flag details will be displayed on **Red Flag** paragraph of the **Special Investigation** notebook. An Investigator can view these details during investigation process.

To configure Red Flag, perform the following steps:

1. Navigate to the **Special Investigations** notebook.
2. Open the codes of **Initialization - I** paragraph notebook. The following figure shows an example.

```
/*********************************************
 * RED FLAGS
 *********************************************/
/*Red Flags:
1. *Count of entities with SARs filed related to FRTTH*: Pro
2. *Entities who are Oligarchs and political figures*: isPep
3. *Shell companies  owned/controlled by a Russian UBOs*: so
sar_wl = new Workload (
    '''\
    select count(*) match (v) where %1$s and v.Status = 'SAR
    ''',
    ['v'],
    get_long_scala
)
sar_list_wl = new Workload (
    '''\
    select v.Name match (v) where %1$s and v.Status = 'SAR'
    ''',
    ['v'],
    get_string_list
)
oligarchs_and_political_figures_wl = new Workload (
    '''\
    select count(*) match (v) where %1$s and java_regexp_lik
    ''',
    ['v'],
    get_long_scala
)
oligarchs_and_political_figures_list_wl = new Workload (
    '''\
```

3. Edit the codes to add a queryfor red flag parameter and execute the paragraph.
4. Navigate to Red Flags paragraph.

5. Enter the Red Flag names (for example, "Accounts interacting with sanctioned Russian banks and entities") and the query details. This query name should be the same as mentioned in the **Initialization - I** paragraph. This is used for calling the red flag query defined in **Initialization - I** paragraph.

Configuring the Risk Factors

You can configure the risk factor of business entity. The risk factor can lower organization profits or lead it to fail. Based on risk factor details, you should view the

investigation recommendation and take the appropriate action. The risk factor details will be displayed on Risk Factors paragraph of Special Investigation notebook.

1. Navigate to the **Special Investigations** notebook.
2. Open the codes of **Initialization - I** paragraph notebook. The following figure shows an example.

```
/
 * RISK FACTORS
 ********************************************/
// count number of high risk countries (>3) in case -- updat
country_risk_wl = new Workload (
    '''\
    select count(distinct s)
    match (s) <-[e]- (d)
    where
        %1$s and (d.Country = 'RU' or d.Country = 'CY' or d.
        (e.Label = 'address of' or e.Label = 'match name')
    '''
    ,
    ['s'],
    get_long_scala
)
// Count where list = regex SDN
sanction_hit_risk_wl = new Workload (
    '''\
    select count(*) match (s) where %1$s and java_regexp_lik
    '''
    ,
    ['s'],
    get_long_scala
)
sanction_hit_risk_list_wl = new Workload (
    '''\
    select v.Name match (v) where %1$s and java_regexp_like(
    '''
    ,
    ['v'],
    get_string_list
)
```

3. Edit the codes to add a query for risk factors parameter and execute the paragraph.
4. Navigate to Risk Factors paragraph.

5. Enter the Risk Factor names (for example, "Sanction Hits") and the query details. This query name should be the same as mentioned in the **Initialization - I**

paragraph. This is used for calling the risk factor query defined in **Initialization - I** paragraph.

Configuring the Network Disposition Score

Network disposition is calculated using the following formula:

Sum of risk of all the entities in the result graph/Number of entities in the result graph

To configure the Network Disposition Score, perform the following steps:

1. Navigate to the **Special Investigations** notebook.
2. Open the codes of **Initialization - I** paragraph notebook.
3. Edit the codes and execute the paragraph.

Adding a New Search Criteria

The default, search criteria available to search a business entity are: Tax ID, Name, Address, and Date.

You can add new search criteria. For example, if you want to add customer DOB as a new search criterion, use the following format:

givenDOB = "@{Date=}"

To add a new search criterion, perform the following steps:

1. Navigate to the **Special Investigations** notebook.
2. Open the codes of **Entity Search** paragraph notebook.

3. Edit the codes and execute the paragraph. After executing the Entity Search paragraph, add the relevant program code of that search criterion in the **Initial Screening Results** paragraph.

5

Additional Configuration

This chapter provides information on additional configuration for Investigation Hub.

This chapter covers the following sections:

Configuring Interpreters

An interpreter is a program that directly reads and executes the instructions written in a programming or scripting language without previously compiling the high-level language code into a machine language program.

Interpreters supported by Investigation Hub are PGX, PGQL, GreenMarl, OFSAA Interpreter, OFSAA SQL Interpreter, Markdown and so on.

For more information, see the Configuring Interpreters section in the ***Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide***.

Managing Graphs

You can view the graphs that are created using Investigation Hub data in the Investigation Hub interface.

To create custom graphs, you must manually configure the Data Store. For more information on configuring graphs, see the ***Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide***.

Managing Templates

Investigation Hub offers various formats using which you can view the result after the execution of a paragraph. Templates enable you to define parameters and use these parameter to customize the result formats. You can customize the visualization of the result by defining parameters in a template and then applying the template to a Notebook. The customized parameters in the template are applied to the result format in the Notebook.

For more information, see the Managing Template section in the ***Oracle Financial Services Crime and Compliance Studio User Guide***.

A

Generating Correlation Networks

After event data is loaded from different applications into Investigation Hub, you can correlate events based on business entities using configurable rule sets. This functionality is performed by the event correlation process. The group of events is identified for correlation-based on business entities in the application.

Note: This correlation is applicable only if you are not using the ECM application.

The Generate Correlation Network notebook creates the correlated networks of related events (alerts) for next-level investigators as a starting point of the investigation. It can be mapped to existing cases or used to generate new cases. These generated correlation networks are used in Special Investigation and Level 2 Case Investigations notebooks. To generate the correlation network, perform the following steps:

1. Navigate to the Investigation Hub home page.
2. Navigate to the **Generate Correlated Networks** notebook.
3. Enter the graph name in the Load the Global Graph section as shown here. This graph name should be the same as mentioned in Graph Loading notebook. For more information, see Loading Data to Graphs).

4. Click Execute Paragraph to execute the Load the Global Graph paragraph.

5. Execute the notebook.

6. After executing the notebook, the correlation network will be generated for loaded data.

B

API for Running All Paragraphs

The following methods are available in the REST API for running all paragraphs at once:

Run all notebook paragraphs:

/v2/notebooks/run with {notebookId: notebookId, paragraphs: [{paragraphId: paragraphId , params: {}}]}

For more information, see the API documentation of Data Studio.

> **Note:** Before running the API, values must be defined in notebooks.