Oracle Financial Services Investigation Hub

Administration and Configuration Guide

Release 8.0.7.3.0

March 2020

F28095-01

ORACLE
Financial Services

Oracle Financial Services Investigation Hub

Document Control

Table 1: Document Control

Version Number	Revision Date	Changes Done
8.0.7.3.0	Created: February 2020	Created the first version of the Investigation Hub Administration Guide for 8.0.7.3.0 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.

Table of Contents

1 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:

1.1 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.

1.2 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.

1.3 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.
- Configuring the Notebook Parameters describes the configurable notebook parameters.
- Additional Configuration details the additional configurations.

1.4 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*

1.5 Conventions Used in this Guide

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

Table 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

1.6 Abbreviations Used in this Guide

Abbreviations used in this guide are listed here.

Table 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

2 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:

2.1 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.

2.1.1 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

2.2 Administration and Configuration Activities

An administrator should configure the following Notebooks:

- **Special Investigation:** 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 Investigation** notebook to users (investigators) and users will clone the notebook for their investigation.

Adminstrator loads the graph into memory and publishes it so other notebooks can access and use it.

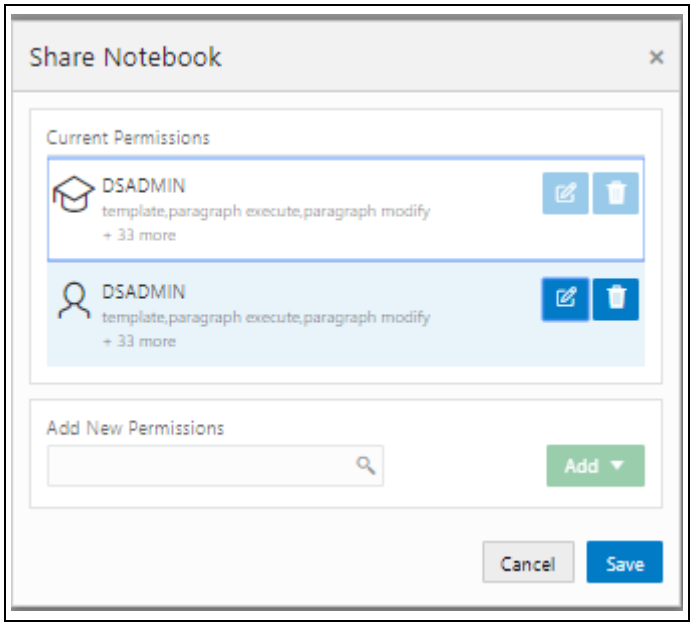
2.3 Providing Permissions to a Notebook

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.

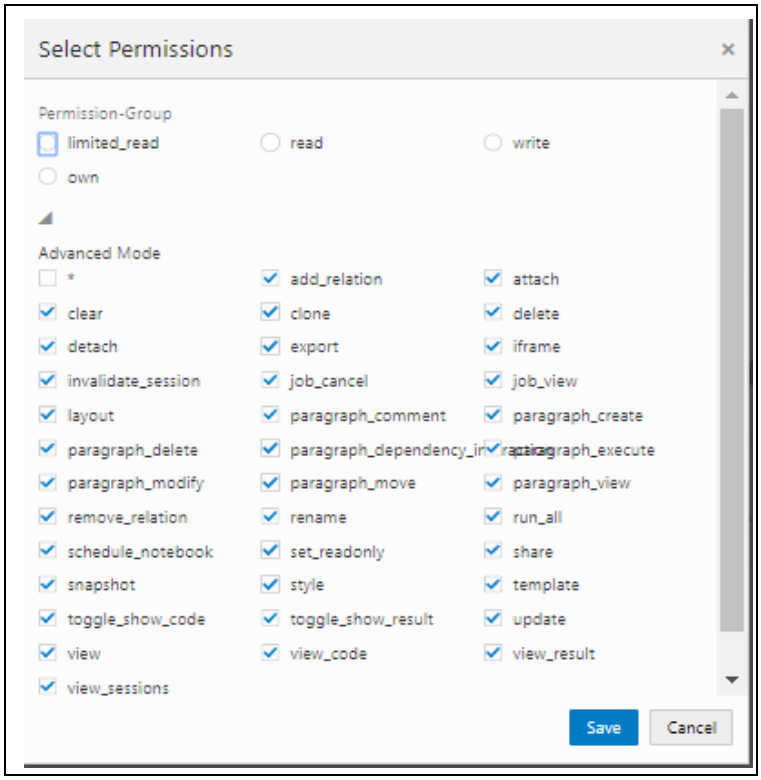
For more information on permissions, see the Oracle Financial Services Crime and Compliance Studio Administration and Configuration Guide

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.

3 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

3.1 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

3.1.1 Identity and Authorization Process

The following figure shows the process flow of identity management and authorization.

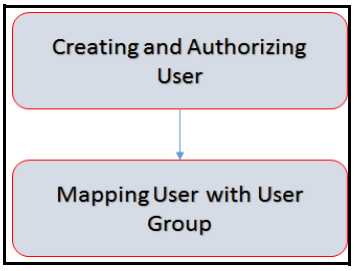


Table 3 lists the various actions involved in the user administration process flow:

Table 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.

3.1.2 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.

3.2 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.

4 Configuring the Notebook Parameters

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

> **NOTE:** In an Investigation Hub notebook, the graph is lost whenever a session is reset and this occurs as part of the session clean-up. You must execute the Graph_Alive notebook to retain the link to the graph even when a session is reset. For more information, see the Appendix - Executing Graph_Alive Notebook of Oracle Financial Services Crime and Compliance Studio Installation and Configuration Guide.

This chapter covers the following sections:

- Configuring the Investigation Recommendation Score
- Configuring the Red Flag
- Configuring the Risk Factors
- Configuring the Network Disposition Score
- Adding a New Search Criteria

4.1 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 Investigation** notebook.
3. Open the codes of **Initialization - I** paragraph and edit it as required. The following figure shows an example.

```
public String get_recommendation(int case_disp_system, int case_disp_analyst, int red_flags, int risk_factors, int external_data, int internal_data, boolean initial) {
    String color = "seagreen";
    String ret = "Close Case (Reason: False Positive)";

    int disposition_score = (case_disp_analyst > 0 ? case_disp_analyst : case_disp_system);

    // 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 < 76) {
        ret = "Special Investigation Needed";
        color = "darkorange";
    } else if (disposition_score > 76) {
        ret = "Consider Escalation";
        color = "crimson";
    }
```

4. Execute the paragraph.

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

4.2 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 Investigation** 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*: Property status on event = SAR
2. *Entities who are Oligarchs and political figures*: isPep = true and list = SDN
3. *Shell companies  owned/controlled by a Russian UBOs*: source = BvD (for now Panama Papers), edge from company to individual to where address.country = RUS*/
Workload<Long> sar_wl = new Workload<> (
    "select count(*) match (v) where v.Status = 'SAR' and %s",
    singleVertex,
    get_long_scala
);
Workload<List<String>> sar_list_wl = new Workload<> (
    "select v.Name match (v) where v.Status = 'SAR' and %s",
    singleVertex,
    get_string_list
);
Workload<Long> oligarchs_and_political_figures_wl = new Workload<> (
    "select count(*) match (v) where java_regexp_like(v.\"Is PEP\", 'PEP') or java_regexp_like(v.List, 'sar') and %s",
    singleVertex,
    get_long_scala
);
Workload<List<String>> oligarchs_and_political_figures_list_wl = new Workload<> (
    "select v.Name match (v) where java_regexp_like(v.\"Is PEP\", 'PEP') or java_regexp_like(v.List, 'sar') and %s",
    singleVertex,
    get_string_list
);
Workload<Long> ru_ubo_wl = new Workload<> (
    "select count(*)"
    + "match (v) -[e1]- (external) -[e2]- (ubo) -[e3]- (address) "
    + "where e1.Label = 'match name' and external.Label = 'External Source' and e3.Label = 'address of' and address.Country = 'RU' and external.Source = 'BvD' and %s",
    singleVertex,
    get_long_scala
);
Workload<List<String>> ru_ubo_list_wl = new Workload<> (
```

3. If required, edit the codes to add a query for red flag parameter and execute the paragraph.
4. Navigate to Red Flags paragraph.

Red Flags

```
%pgx-java

Map<String, Workload<Long>> red_flag_workloads = new HashMap<>() {{
    put("Entities with SARs filed related to FRTTH", sar_wl);
    put("Entities who are Oligarchs or political figures", oligarchs_and_political_figures_wl);
    put("Shell companies owned/controlled by Russian UBOs" , ru_ubo_wl);
    put("Transactions with payer in risky country and beneficiary in tax haven", transaction_wl);
    put("Accounts interacting with sanctioned Russian banks and entities", interaction_sanctioned_ru_banks_wl);
}};

out.println(get_table(resultGraph, red_flag_workloads, "Red Flags"));
```

Type to search

Red Flags	Hits (Initial)	Hits (Investigator)
Shell companies owned/controlled by Russian UBOs	0	0
Entities with SARs filed related to FRTTH	0	0
Entities who are Oligarchs or political figures	0	0
Transactions with payer in risky country and beneficiary in tax haven	0	0
Accounts interacting with sanctioned Russian banks and entities	0	0

Page 1 of 1 (1-5 of 5 items) 1

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.

4.3 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 Investigation** 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 -- update this w/ udf
Workload<Long> country_risk_wl = new Workload<> (
    "select count(distinct v) match (v) <-[e]- (v2) where "
        + "(v2.Country = 'RU' or v2.Country = 'CY' or v2.Country = 'EE' or java_regexp_like(v2.Country,'IVOIRE')) and "
        + "(e.Label = 'address of' or e.Label = 'match name') and %s",
    singlevertex,
    get_long_scala
);
// count where list = regex SDN
Workload<Long> sanction_hit_risk_wl = new Workload<> (
    "select count(*) match (v) where java_regexp_like(v.List,'sdn') and %s",
    singlevertex,
    get_long_scala
);
Workload<List<String>> sanction_hit_risk_list_wl = new Workload<> (
    "select v.Name match (v) where java_regexp_like(v.List, 'sdn') and %s",
    singlevertex,
    get_string_list
);
Workload<Long> terrorism_risk_wl = new Workload<> (
    "select count(*) match (v) where v.Category = 'TERRORISM' and %s",
    singlevertex,
    get_long_scala
);
Workload<List<String>> terrorism_risk_list_wl = new Workload<> (
    "select v.Name match (v) where v.Label = 'Customer' and v.Category = 'TERRORISM' and %s",
    singlevertex,
    get_string_list
);
Workload<Long> prohibited_business_risk_wl = new Workload<> (
    "select count(*) match (v) where v.\"Customer Type\" = 'IND' and (v.Industry = 'NAVY' or v.Industry = 'WHL') and %s",
    singlevertex,
    get_long_scala
```

3. If required, 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.

4.4 Configuring the Network Disposition Score

Network disposition is calculated using the following formula:

Sum of Node Risk/Node Count

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

1. Navigate to the **Special Investigation** notebook.
2. Open the codes of **Initialization - I** paragraph notebook.

```
public int get_disp_score(boolean isSystemScore){
    int cond = isSystemScore ? CASE_ID_COND : VISIBLE_GRAPH_COND;

    float disposition_score = 0L;
    try {
        PgqlResultSet rs = prep_and_run_query(global_graph, "select sum(v.Risk) match (v) where %s", singleVertex, cond);
        rs.next();
        float node_risk = rs.getFloat(1);
        rs.close();

        rs = prep_and_run_query(global_graph, "select sum(e.\"Activity Risk\") match (v1)-[e]->(v2) where %s and %s", twoVertices, cond);
        rs.next();
        float edge_risk = rs.getFloat(1);
        //edge_risk = 0
        rs.close();

        rs = prep_and_run_query(global_graph, "select count(v) match (v) where v.Label = 'Event' and %s", singleVertex, cond);
        rs.next();
        float event_count = rs.getFloat(1) * 5;
        rs.close();

        rs = prep_and_run_query(global_graph, "select count(v) match (v) where v.Label = 'External Entity' and java_regexp_like(v.Source, '" + negative_external_sources_regex + "') and %s",
        rs.next();
        float bad_external_entities_count = rs.getFloat(1) * 10;
        rs.close();

        disposition_score = node_risk + edge_risk + event_count + bad_external_entities_count;
    } catch (PgqlException e) {
        // TODO error msg
        out.println("Something went wrong.");
    }
```

3. If required, edit the codes and execute the paragraph.

4.5 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 Investigation** notebook.
2. Open the codes of **Input Search Results** paragraph notebook.

3. If required, edit the codes and execute the paragraph.

5 Additional Configuration

This chapter provides information on additional configuration for Investigation Hub.

This chapter covers the following sections:

5.1 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, 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.

5.2 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.

5.3 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.

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

7 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.