

# **Oracle Financial Services Investigation Hub**

**Administration and Configuration Guide**

**Release 8.1.2.4.0**

**November 2023**

**F49104-01**

**ORACLE<sup>®</sup>**  
Financial Services

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, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

# Document Control

Table 1 lists the document control of this guide:

**Table 1: Document Control**

Version Number	Revision Date	Change Log
8.1.2.4.0	November 2023	Updated a note in the <a href="#">Managing User Administration</a> section.
8.1.2.4.0	July 2023	Updated the investigation score in the <a href="#">Configuring the Investigation Recommendation based on Network Disposition Score</a> section.
8.1.2.4.0	June 2023	Deprecated L2 and Generate Correlation Networks notebooks. Updated api_version in the <a href="#">Updating the Database Tables in ECM</a> section. Added a note (step 1) in the <a href="#">Authenticating the User to Access Investigation Tab in ECM</a> section. Updated note in the <a href="#">Administration and Configuration Activities</a> section. Removed the following sections: <ul style="list-style-type: none"><li>• Generating Correlation Networks</li><li>• Creating a New CSV</li><li>• Loading Data to Graphs</li></ul>
8.1.2.1.0	December 2022	<ul style="list-style-type: none"><li>• OJET Upgrade (all UI elements are updated according to UI in the entire document).</li><li>• Updated URL, api_version in the Table 4 and notebookId in the Table 5 of the <a href="#">Updating the Database Tables in ECM</a> section.</li><li>• Updated step 1 in the <a href="#">Authenticating the User to Access Investigation Tab in ECM</a> section.</li><li>• Updated the <a href="#">PGX Data Memory Limit</a> section.</li></ul>
8.1.2.0.0	April 2022	Added a new <a href="#">PGX Data Memory Limit</a> section.
8.1.1.1.0	December 2021	There is no content update from the previous version. Only version number has been changed.
8.1.1.0.0	October 2021	This is the first version created for IH 8.1.1.0.0 release based on OFS Compliance Studio 8.1.1.0.0 release.

---

# Table of Contents

<b>1</b>	<b>Preface .....</b>	<b>7</b>
1.1	Summary.....	7
1.2	Documentation Accessibility .....	7
1.3	Audience .....	7
1.4	Related Documents.....	7
1.5	Conventions .....	8
1.6	Abbreviations .....	8
<b>2</b>	<b>About Oracle Financial Services Investigation Hub .....</b>	<b>9</b>
2.1	Introduction.....	9
2.1.1	<i>Key Features</i> .....	9
2.2	Access the OFS Compliance Studio application .....	10
2.3	Import Notebooks .....	10
2.4	Access the Notebook.....	11
2.5	Administration and Configuration Activities.....	12
<b>3</b>	<b>Managing User Administration .....</b>	<b>13</b>
<b>4</b>	<b>Configuring the Notebook Parameters.....</b>	<b>14</b>
4.1	Configuring the Investigation Recommendation based on Network Disposition Score .....	14
4.2	Configuring the Red Flags.....	15
4.3	Configuring the Risk Factors .....	16
4.4	Configuring the Network Disposition Score.....	17
4.5	Adding New Dynamic Search Parameters.....	18
<b>5</b>	<b>Additional Configuration .....</b>	<b>19</b>
5.1	Configuring Interpreters.....	19
5.2	Managing Graphs.....	19
5.3	Data visualization .....	19
5.4	Managing Templates.....	20
<b>6</b>	<b>Integrating OFS IH with ECM .....</b>	<b>21</b>
6.1	Prerequisites.....	21
6.2	Updating the Database Tables in ECM.....	21
6.2.1	<i>Creating an Encrypted Password</i> .....	23

---

6.2.2	<i>Assign Grants to BD and ECM Atomic Schema</i> .....	24
6.3	Mapping IH Entity/Tab in ECM Case Designer.....	24
<b>7</b>	<b>Appendix</b> .....	<b>25</b>
7.1	Authenticating the User to Access Investigation Tab in ECM .....	25
7.2	Executing the Notebook .....	26
7.3	PGX Data Memory Limit .....	26
<b>8</b>	<b>OFSAA Support</b> .....	<b>27</b>
<b>9</b>	<b>Send Us Your Comments</b> .....	<b>28</b>

# 1 Preface

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

## Topics:

- [Summary](#)
- [Documentation Accessibility](#)
- [Audience](#)
- [Related Documents](#)
- [Conventions](#)
- [Abbreviations](#)

## 1.1 Summary

You can find the latest copy of this document in the Oracle Help Center (OHC) Documentation Library which includes all the recent additions/revisions (if any) done to date.

## 1.2 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the [Oracle Accessibility Program website](#).

## 1.3 Audience

The Oracle Financial Services Investigation Hub Administration and Configuration Guide is intended for System Administrator and Implementation Consultant.

## 1.4 Related Documents

This section identifies additional documents related to the OFS IH application. Oracle Financial Services Analytical Applications Infrastructure Related Documents.

The following OFS IH documents are available in Oracle Help Center Documentation Library:

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

## 1.5 Conventions

Table 2 lists the conventions used in this document.

**Table 2: Conventions Used in This Guide**

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text on the screen, or text you enter.

## 1.6 Abbreviations

Table 3 lists the abbreviations used in this document.

**Table 3: Abbreviations Used in This Guide**

Abbreviation	Meaning
OFS	Oracle Financial Services
AAI	Analytical Applications Infrastructure
PGX	Parallel Graph Analytics
PGQL	Property Graph Query Language
LHS	Left Hand Side
OFSAA	Oracle Financial Services Analytical Applications
OFS IH	Oracle Financial Services Investigation Hub
FCGM	Financial Crime Graph Model
FCDM	Financial Crime Data Model
SQL	Structured Query Language
IH	Investigation Hub
ECM	Enterprise Case Management
AML	Anti-money Laundering
BD	Behavior Detection
OOB	Out-of-the-Box



## 2 About Oracle Financial Services Investigation Hub

This chapter provides a brief overview of the OFS IH application.

### Topics:

- [Introduction](#)
- [Access the OFS Compliance Studio application](#)
- [Import Notebooks](#)
- [Access the Notebook](#)
- [Administration and Configuration Activities](#)

### 2.1 Introduction

OFS Investigation Hub is an application built on OFS Compliance Studio, allowing investigators to rapidly view the case and ad-hoc information within the FCGM. 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 FCGM 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. OFS IH automatically generates case narratives and insights, highlights risk factors, red flags that 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 and special investigation
- 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. It is applicable only for non-ECM customers
- Exploration of the financial crimes global-graph using an interactive and visual Graph Explorer tool.
- Integrates fully with FCDM (data can be loaded directly from Behavior Detection (AML) or ECM instance) and ICIJ data sources. It can be enhanced to support other data sources such as watchlist and company hierarchy data
- It is built on OFS Compliance Studio, including a highly scalable in-memory Oracle Graph Analytics Engine (PGX).

## 2.2 Access the OFS Compliance Studio application

To access the OFS Compliance application, follow these steps:

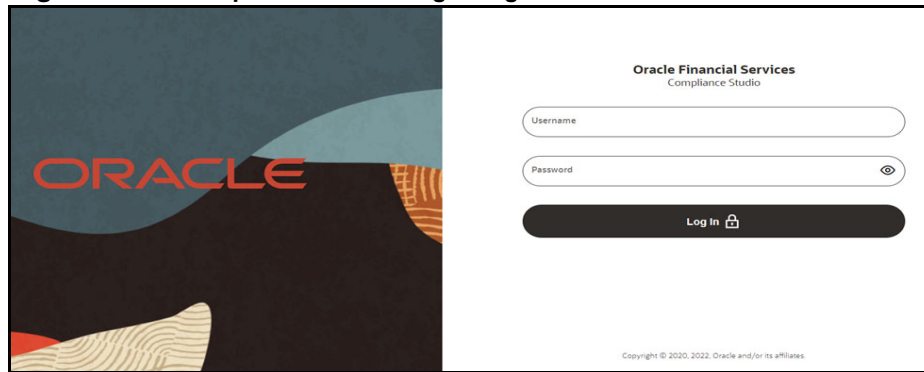
1. Enter the URL in the following format in the web browser:

`https://<Host_Name>:<Port_Number>/cs/home`

Here <Port\_Number> is **7001** for the OFS Compliance Studio application installed on-premise.

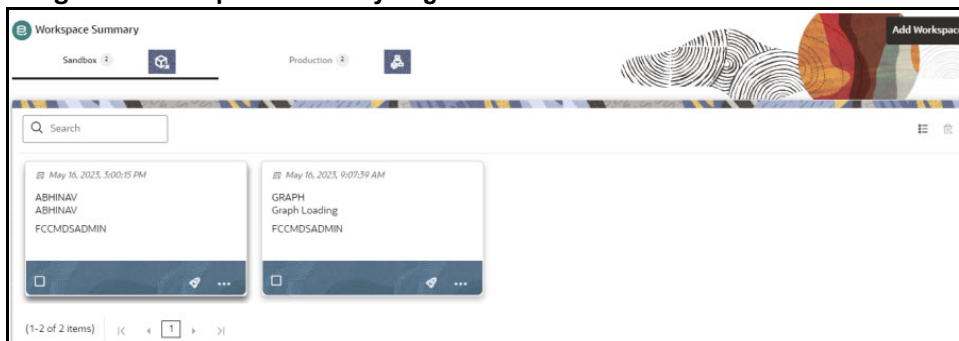
2. The OFS Compliance Studio application login page is displayed.

**Figure 1: OFS Compliance Studio Login Page**



3. Enter the **Username** and **Password**.
4. Click **Login**.
5. After login into the OFS Compliance Studio application, the Workspace Summary page is displayed.

**Figure 2: Workspace Summary Page**



## 2.3 Import Notebooks

### NOTE


- An Administrator can also import the IH notebooks for all users.
- In the case of the Special Investigation notebook, creating an Objective and Draft to import the Notebook must be performed for each user separately.

For more information on how to import notebooks, see the **Importing the Notebook** section in the [Oracle Financial Services Investigation Hub Installation Guide](#).


## 2.4 Access the Notebook

The Investigation Hub objective (folder) displays the notebooks that are mapped to the logged-in user's role and displays the details of each Notebook, such as Notebook name, Notebook details, date when the Notebook is published, and related tags. The Detailed Information section includes the date and time of Notebook creation, the number of compilations performed using different interpreters in a Notebook, and the username of the Notebook creator.

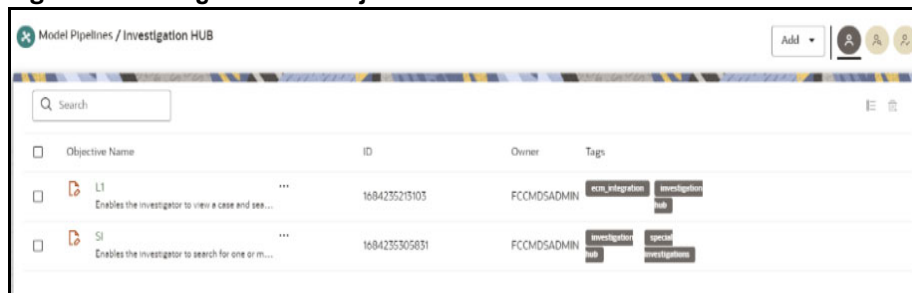
To access the Notebook, follow these steps:

1. Log in to the Compliance Studio application.
2. On the **Workspace Summary** page, click  Launch for the corresponding Sandbox workspace. The Workspace Dashboard is displayed.

**NOTE** For IH Notebook to be executable, it needs to be imported into the **Sandbox** workspace.

3. Click **Model Pipelines**  to display the **Model Pipelines** page.
4. Click the **Investigation Hub** Objective. The following notebooks are available in the Investigation Hub objective:
  - Investigation Hub\_ECM\_Integration\_L1
  - Investigation Hub\_Special\_Investigation

**Figure 3: Investigation Hub Objective**



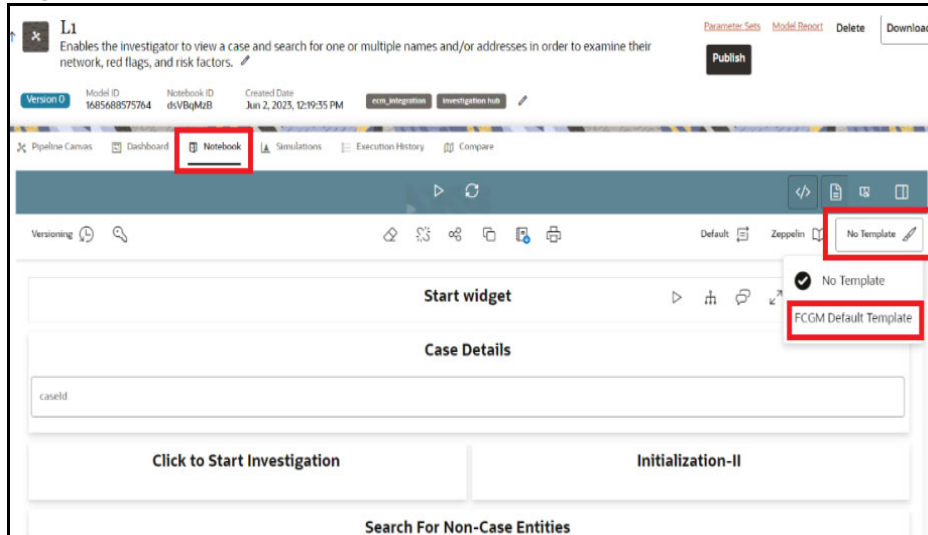
5. Click **...** next to the corresponding Notebook and select the **Open in Pipeline Designer** option. The following window is displayed.

**Figure 4: Pipeline Canvas window**



6. Click on the **Notebook** tab to view the notebook. The notebook window is displayed.

Figure 5: Notebook Tab



7. Click **No Template** and select **FCGM Default Template** from the drop-down list to access the notebook.

## 2.5 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.
- **ECM Integration\_L1:** Enable Level 1 Case Investigators to access additional rich information about a case such as a case summary, a detailed narrative about case entities, graph view of a case, and so on, which is otherwise not available in ECM. Allows the investigator to explore a case - including graph, risk factors, and red flags.

### NOTE

- Administrators must share only the Special Investigation notebook with users (investigators) and users will clone the Notebook for their investigation.
- Administrator loads the graph into memory and publishes it so other notebooks can access and use it.
- For IH Notebook to be executable, it needs to be imported into the **Sandbox** workspace.
- For L2 user, the L1 notebook can be reused. For more information, see the Importing IH Notebooks section in the [OFS Investigation Hub Installation Guide](#).

## 3 Managing User Administration

User Administration refers to the process of controlling the user privileges in accessing the application resources and is based on business requirements to provide access to view, create, edit, or delete confidential data.

User Administration involves administrator tasks to create user definitions, user groups, maintain profiles, authorize users and user groups, map users to groups, domains and roles, grant permissions based on user roles and requirements, etc.

---

**NOTE**

The **DSUSRGRP** group must be assigned to the user for using the Investigation Hub.

For more information, see the **Managing User Administration** section in the [OFS Compliance Studio Administration and Configuration Guide](#).

## 4 Configuring the Notebook Parameters

This chapter provides information on configuring the notebook parameters for the following seeded notebooks of the OFS IH application:

- Special Investigation Notebook
- ECM\_Integration\_L1

### Topics:

- [Configuring the Investigation Recommendation based on Network Disposition Score](#)
- [Configuring the Red Flags](#)
- [Configuring the Risk Factors](#)
- [Configuring the Network Disposition Score](#)
- [Adding New Dynamic Search Parameters](#)

### 4.1 Configuring the Investigation Recommendation based on Network Disposition 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 in the Recommendation paragraph of the Special Investigation notebook.

Following is the criteria for recommendation:

- If the investigation score is between 0 to 24, the case status is displayed as **Further Investigation**.
- If the investigation score is between 25 to 50, the case status is displayed as **Low Risk Network**.
- If the investigation score is between 51 to 76, the case status is displayed as **Medium Risk Network**.
- If the investigation score is greater than 76, the case status is displayed as **High Risk Network**.


An Investigator can print or save the Notebook after viewing the investigation recommendation.

To define the investigation recommendation, follow these steps:

1. Log in to the **OFS Compliance Studio** application.
2. On the **Workspace Summary** page, select **Launch workspace**  to display the application configuration and model creation menu.

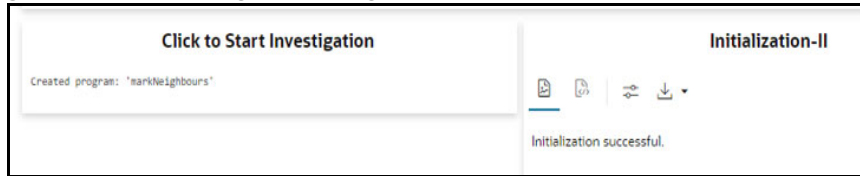
---

**NOTE** For IH Notebook to be executable, it needs to be imported into the **Sandbox** workspace.

3. Click **Model Pipelines**  to display the **Model Pipelines** page.
4. Navigate to the **Investigation Hub** objective.
5. Navigate to the **Special Investigation** notebook that is assigned for a particular user role.
6. Click on the **Notebook** tab.

7. Execute **Click to Start Investigation** paragraph. It executes the **Click to Start Investigation** paragraph and also the initialization paragraph automatically.  
The successful initialization message is displayed.

**Figure 6: Start Investigation Paragraph**



8. Execute all subsequent paragraphs. The Network Disposition score is displayed.  
An Investigator can view the investigation recommendation status based on this Network Disposition score.

**Figure 7: Investigation Recommendation**



## 4.2 Configuring the Red Flags

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 the Red Flags paragraph of the Special Investigation, and ECM\_Integration\_L1 notebooks. An Investigator can view the following details during the investigation process:

- Entities with SARs filed
- Transactions with the payer in risky country and beneficiary in tax haven
- Accounts interacting with sanctioned entities

To configure **Transactions with payer in risky country and beneficiary in tax haven** in the Red Flag indicator, follow these steps:

1. Navigate to the **Special Investigation** notebook.

**NOTE** You can follow the same steps for ECM\_Integration\_L1 notebook.

2. Open the code of the Red Flag paragraph notebook. The following figure shows an example.

Figure 8: Configure Red Flag Paragraph

```
String txn_query_visible="select count(e) "
+ "match (v1)-[e]-(v2) "
+ "where e.\"Original Id\" is not null and "
+ "e.Label in ('end to end wire txn', 'end to end ml txn','cash txn') "
+ " and v2.Country in ('CHE','BHS','ANB','US') "
+ " and v1.Country in "+ countryListString
+ " AND id(e) in ? and ( id(v1) in ? or id(v2) in ? ) GROUP BY e.\"Original Id\" ";

PgsqlResultSet txn_query_visible_result = prep_and_run_query(resultGraph, txn_query_visible, threeEdgeVertices, VISIBLE_GRAPH_CMD);

for(PgsqlResult r:txn_query_visible_result){
    count_txn_visible++;
    r.getLong(1);
}

String txn_query="select count(e) "
+ "match (v1)-[e]-(v2) "
+ "where e.\"Original Id\" is not null and "
+ "e.Label in ('end to end wire txn', 'end to end ml txn','cash txn') "
+ " and v2.Country in ('CHE','BHS','ANB','US') "
+ " and v1.Country in "+ countryListString
+ " GROUP BY e.\"Original Id\" ";

PgsqlResultSet txn_query_result = prep_and_run_query(resultGraph, txn_query, twoVertices, CASE_ID_CMD);

for(PgsqlResult r:txn_query_result){
    count_txn++;
}

}

out.println(String.join("\t","Red Flags", "Hits (Initial)", "Hits (Investigator)"));

String redFlags = String.join("\n",
String.join("\t", "Entities with SARs filed", format_score(count_sar_wl),format_score(count_sar_wl_visible)),
String.join("\t", "Transactions with payer in risky country and beneficiary in tax haven", format_score(count_txn),format_score(count_txn_visible)),
String.join("\t", "Accounts interacting with sanctioned entities", format_score(count_sanctioned), format_score(count_sanctioned_visible))
);
out.println(redFlags);
```

3. Edit the code to configure the **Transactions with payer in risky country and beneficiary in tax haven** parameter.

For example:

```
v2.Country in ('CHE','BHS','ANB')"
```

4. Execute the Red Flags paragraph.

Figure 9: Red Flags Paragraph

```
86 String redFlags = String.join("\n",
87 String.join("\t", "Entities with SARs filed", format_score(count_sar_wl),format_score(count_sar_wl_visible)),
88 String.join("\t", "Transactions with payer in risky country and beneficiary in tax haven", format_score(count_txn),format_score(count_txn_visible)),
89 String.join("\t", "Accounts interacting with sanctioned entities", format_score(count_sanctioned), format_score(count_sanctioned_visible))
90 );
91 out.println(redFlags);
92
```

Red Flags	Hits (Initial)	Hits (Investigator)
Entities with SARs filed	1	1
Transactions with payer in risky country and beneficiary in tax haven	101	6
Accounts interacting with sanctioned entities	3	3

## 4.3 Configuring the Risk Factors

You can configure the risk factor of a business entity. The risk factor can lower an organization's profits or lead it to fail. Based on risk factor details, you should view the investigation recommendation and take the appropriate action. The following risk factor details will be displayed on the Risk Factors paragraph of the Special Investigation, and ECM\_Integration\_L1 notebooks:

- Country/Region Hits
- Prohibited Business List Match
- High Risk Transaction Present

To configure **Prohibited Business List Match** in the risk factors, follow these steps:

1. Navigate to the **Special Investigation** notebook.

**NOTE** You can follow the same steps for ECM\_Integration\_L1 notebook.



- Open the code of the Risk Factors paragraph notebook. The following figure shows an example.

**Figure 10: Configure Risk Factors**

```

2
3 /*****
4 * This need to be Customize as Per Customer Data
5 Entity Type and Industry can be customise here by putting values in below query
6 *****/
7
8 String prohibited_business_risk_wl_visible="select count(*) match (v) where v.\"Entity Type\" = <Customize_Entity_Type> and (v.Industry = <Customize_I
9 PgqlResultSet prohibited_business_risk_wl_visible_result = prep_and_run_query(resultGraph, prohibited_business_risk_wl_visible, singleVertex, VISIBLE_GR
10
11 String prohibited_business_risk_wl_graph="select count(*) match (v) where v.\"Entity Type\" = <Customize_Entity_Type> and (v.Industry = <Customize_Ind
12 PgqlResultSet prohibited_business_risk_wl_result_graph = prep_and_run_query(resultGraph, prohibited_business_risk_wl_graph, singleVertex, CASE_ID_COND);
13
14 Long count_prohibited_visible=0L;
15 for(PgxResult r:prohibited_business_risk_wl_visible_result){
16     // count_prohibited_visible++;
17     count_prohibited_visible=r.getLong(1);
18 }
19
20 Long count_prohibited_graph=0L;
21 for(PgxResult r:prohibited_business_risk_wl_result_graph){
22     // count_prohibited_graph++;
23     count_prohibited_graph=r.getLong(1);
24 }
25

```

- Edit the codes to configure the **Prohibited Business List Match** (Entity Type and Industry) parameters.

For example:

v.\"Entity Type\" = <Customize\_Entity\_Type> and (v.Industry = <Customize\_Industry> or v.Industry = '<Customize\_Industry>')

- Execute the Risk Factors paragraph.

**Figure 11: Risk Factors Paragraph**

Risk Factors	Hits (Initial)	Hits (Investigator)
Country/Region Hits	213	38
Prohibited Business List Match	49	1
High Risk Transaction Present	122	6

Page 1 of 1 (1-3 of 3 items) | < 1 >

## 4.4 Configuring the Network Disposition Score

This paragraph shows the network disposition score based on the nodes' risk on the **Visible Graph**.

Network disposition is calculated using the following formula:

The formula to calculate the network disposition score is "(Total risk of nodes in Visible Graph/Number of nodes in the Visible Graph) \* 10."

For example:

Divide the total risk of nodes by the number of nodes in the Visible Graph and multiply the output by 10.

To configure the Network Disposition Score, follow these steps:

- Navigate to the **Special Investigation** notebook.
- Open the codes of the Network Disposition Score paragraph.

**Figure 12: Configure Network Disposition Score in the Initialization Paragraph**

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

    float disposition_score = 0L;
    try {
        PsqlResultSet rs = prep_and_run_query(resultGraph, "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(resultGraph, "select count(v) match (v) where %s", singleVertex, cond);
        rs.next();
        float node_count = rs.getFloat(1);
        rs.close();

        disposition_score = (node_risk/node_count)*10;
    } catch (PgqlException e) {
        // TODO error msg
        out.println("Something went wrong.");
    }
}
```

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

## 4.5 Adding New Dynamic Search Parameters

The Dynamic Search enables you to identify non-case entities within the Notebook.

**NOTE** These parameters can only be added to the ECM Integration and Special Investigation Notebooks.

Out of the box, the four search parameters (Tax Id, Name, Address, and Date) are provided and add the Dynamic Search parameters within the graph by performing the following steps.

1. Add new variable and getter setter methods for the input field in `SearchEntry` class and result class in Initialization 3.
2. Add a new field in input search results. For example: `String givenTaxId = cleanString("${Tax Id}");`.
3. Make the required changes in blacklist object of `searchEntry` class in input search results.
  - For fuzzy matching, update the `getMatches` function and add the new input field entries in the required places.
  - For exact matching, update the `getMatchesForPGQLQuery` function and add the new input field entries in the required places.
4. Add the query for the input field in the `getMatchesForPGQLQuery`.
5. Update the `merging answers` section and add the new search field functions (getter and setter).
6. Update the `readInResultData` function and add the new search field to the `VertexBuilder` node.

## 5 Additional Configuration

This chapter provides information about additional configurations for OFS IH.

### Topics:

- [Configuring Interpreters](#)
- [Managing Graphs](#)
- [Data visualization](#)
- [Managing Templates](#)

### 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 OFS IH are PGX, PGQL, OFSAA Interpreter, OFSAA SQL Interpreter, Markdown, etc.

For more information, see the **Configure Interpreters** section in the [Oracle Financial Services Compliance Studio Administration and Configuration Guide](#).

### 5.2 Managing Graphs

You can view the graphs that are created using OFS IH data in the OFS IH interface.

To create custom graphs, you must manually configure the Data Store. For more information on Configuring graphs, see the [Oracle Financial Services Compliance Studio Administration and Configuration Guide](#).

### 5.3 Data visualization

You can view the transactions in the following formats.

- Table
- Area Chart
- Bar Chart
- Funnel Chart
- Line Chart
- Pie Chart
- Pyramid Chart
- Treemap Diagram
- Sunburst Diagram
- Tag Cloud
- Box Plot
- Scatter Plot
- Map Visualizer

- Text

For more information, see the **Data Visualization** section in the [Oracle Financial Services Investigation Hub User Guide](#).

## 5.4 Managing Templates

OFS IH 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 parameters 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 **Templates** section in the [Oracle Financial Services Compliance Studio User Guide](#).

## 6 Integrating OFS IH with ECM

OFS IH is integrated with ECM to enable Case Investigators to access additional rich information about a case such as a case summary, a detailed narrative about case entities, graph view of a case, and so on, which is otherwise not available in ECM.

### Topics:

- [Prerequisites](#)
- [Updating the Database Tables in ECM](#)
- [Mapping IH Entity/Tab in ECM Case Designer](#)

### 6.1 Prerequisites

For more information on ECM patches, see the **Prerequisites** section in [Oracle Financial Services Investigation Hub Installation Guide](#).

### 6.2 Updating the Database Tables in ECM

Update the following database tables in ECM by replacing the placeholders with the user-specified values to integrate IH with ECM.

[Table 4](#) describes the placeholders that must be replaced with the required values, which will replace the corresponding rows in the FCC\_CM\_STUDIO database table.

**Table 4: FCC\_CM\_STUDIO Table**

Placeholder	Description
##URL##	Replace the placeholder with the OFS Compliance Studio URL. For example: http://<Host_Name>:7008/cs
##SSOHEADER##	Replace the placeholder with the SSOHEADER to access OFS Compliance Studio. For example: oam_remote_user NOTE: If SSO is enabled for OFS Compliance Studio and ECM, ensure to replace the ##SSO- HEADER## placeholder value with the relevant SSOHEADER, and provide null for ##PASSWORD##.
##USERNAME##	Use the OFS Compliance Studio user details to login (provisioned to DSADMIN or DSUSER role).
##PASSWORD##	The encrypted password that you must use to login to the Notebook. To create the encrypted password, see <a href="#">Creating an Encrypted Password</a> .
api_version	The API version number is 20220914.

[Table 5](#) describes the placeholders that must be replaced with the required values, which will replace the corresponding rows in the FCC\_CM\_CTYPE\_NB\_MAPPING database table. This provides access to

the Investigation Hub tab in ECM for the default out-of-the-box ECM user roles, CMANALYST1, CMANALYST2, and CMSUPRVISR.

**Table 5: FCC\_CM\_CTYPE\_NB\_MAPPING Table**

Placeholder	Description
For the ECM user roles: CMAN- ALYST1 and CMAN- ALYST2	
##CASE_TYPE##	Replace the placeholder with the case type for which you want to enable the Investigation Hub tab. For example: AML_SURV
##notebookId##	<p>Replace the placeholder with the notebook ID of the IH notebook that must be cloned for all the cases of the specified case type.</p> <p>Follow the below steps:</p> <ol style="list-style-type: none"> <li>1. Navigate to the Data Studio URL(<a href="https://&lt;Data Studio server hostname&gt;:&lt;DataStudioPort&gt;/cs">https://&lt;Data Studio server hostname&gt;:&lt;DataStudioPort&gt;/cs</a> Example, <a href="https://&lt;testserver.oracle.com&gt;:7008/cs">https://&lt;testserver.oracle.com&gt;:7008/cs</a></li> <li>2. Navigate to the path where L1 notebook were imported through Compliance Studio. For more information on how to import notebooks, see the <b>Access the Investigation Hub Objective</b> section in the <a href="#">Oracle Financial Services Investigation Hub User Guide</a>.</li> <li>3. Click ECM_Integration_L1 Notebook. The notebook window is displayed.</li> <li>4. Copy notebook id from the URL <a href="https://Testserver:7008/?root=notebooks&amp;notebook=&lt;Notebook ID&gt;">https://Testserver:7008/?root=notebooks&amp;notebook=&lt;Notebook ID&gt;</a> For example, <a href="https://Testserver:7008/?root=notebooks&amp;notebook=abcde12">https://Testserver:7008/?root=notebooks&amp;notebook=abcde12</a> <b>Notebook ID:</b> abcde12</li> </ol> <p><b>NOTE:</b> You must provide the notebook ID of the ECM_Integration_L1 Notebook for the Analyst role.</p>
For the ECM user role: CMSUPRVISR	
##CASE_TYPE##	Replace the placeholder with the case type for which you want to enable the Investigation Hub tab. For example: AML_SURV
##notebookId##	Replace the placeholder with the notebook ID of the IH notebook that must be cloned for all the cases of the specified case type.

Table 6 describes the placeholders that must be replaced with the required values, which will replace the corresponding rows in the FCC\_CM\_CTYPE\_NB\_MAPPING table. You can modify the permissions

granted to a user role by changing the default assigned values, 'Y' or 'N', to restrict the actions that a user role can perform in the Investigation Hub tab.

**Table 6: FCC\_CM\_CTYPE\_NB\_MAPPING Table**

Table Entry	Description
V_NB_TOOL- BAR	'Y' indicates to grant permission to the user role for the actions that can be performed on a notebook such as Publish Notebook, Clear Result, Share Notebook, and so on. 'N' indicates to deny the permission.
V_ADD_PARA	'Y' indicates to grant permission to the user role to add new paragraphs to a notebook. 'N' indicates to deny the permission. The Interpreter toolbar is not visible to the user.

Table 7 describes the placeholders that must be replaced with the required values, which will replace the corresponding rows in the FCC\_CM\_CTYPE\_NB\_MAPPING table. You can modify the permissions granted to a user role by changing the default assigned values, 'Y' or 'N', to restrict the actions that a user role can perform in the Investigation Hub tab.

**Table 7: FCC\_CM\_CTYPE\_NB\_MAPPING Table**

Table Entry	Description
V_PARA_ACTIONS	'Y' indicates to grant permission to the user role for the actions that can be performed in a paragraph such as Execute Paragraph, Enter Dependency Mode, Comment, and so on. 'N' indicates to deny the permission.
V_PARA_CODE	'Y' indicates to grant permission to the user role to view the paragraph code in the IH notebook. 'N' indicates to deny the permission.

To add a new user role who needs access to the Investigation Hub tab in ECM, you must insert new entries for that user role, case type, and notebook ID in the FCC\_CM\_CTYPE\_NB\_MAPPING table as follows:

```
Insert into FCC_CM_CTYPE_NB_MAPPING (V_USERROLE,V_CASETYPE,V_NOTE-
BOOK_ID,V_CREATED_DATE,V_CREATED_BY,V_UPDATED_BY,V_UPDATED_DATE,V_N-
B_TOOLBAR,V_ADD_PARA,V_PARA_ACTIONS,V_PARA_CODE) values
('<User_Role>','##CASE_TYPE##','##note- bookId##',null,null,null,null,'Y/
N','Y/N','Y/N','Y/N')
```

## 6.2.1 Creating an Encrypted Password

To use a non-SSO setup, you must provide the encrypted password for the notebook login.

To create an encrypted password, follow these steps:

1. Export the **FIC\_DB\_HOME**.
2. Navigate to the <Compliance\_Studio\_Installation\_path>/deployed/ficdb/bin directory.

3. Run the following command:

```
./FCCM_Studio_Base64Encoder.sh <password to encrypt>
```

4. Copy the encrypted password from the putty session and use it in the password field in **fcc\_cm\_studio** table.

---

**NOTE** Ignore this section if both BD and ECM are installed as pack on pack.

## 6.2.2 Assign Grants to BD and ECM Atomic Schema

### 6.2.2.1 BD Atomic Schema

1. Login to BD Atomic Schema.
2. Run the following command:

```
GRANT SELECT ON FCC_AM_EVENTS to ECM_ATOMIC_SCHEMA_NAME
```

### 6.2.2.2 ECM Atomic Schema

1. Login to ECM Atomic Schema.
2. Run the following command:

```
CREATE SYNONYM FCC_AM_EVENTS FOR BD_ATOMIC_SCHEMA_NAME.FCC_AM_EVENTS
```

## 6.3 Mapping IH Entity/Tab in ECM Case Designer

Using the Case Designer component in ECM, you must add the "Investigation Hub" entity to the Case Type for which you want the Investigation Hub tab to be enabled. For more information, see Adding Optional Entities to the Case Type section in the **Managing Case Designer** chapter in the [OFS Enterprise Case Management Administration Guide](#).



## 7 Appendix

### Topics:

- [Authenticating the User to Access Investigation Tab in ECM](#)
- [Executing the Notebook](#)
- [PGX Data Memory Limit](#)

### 7.1 Authenticating the User to Access Investigation Tab in ECM

**NOTE** The user needs a self-signed certificate to authenticate the user for accessing Investigation Tab in ECM.

If the user is not using the self-signed certificate, perform the following:

1. Copy the following files from `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-studio/conf` to the server where ECM is installed.
  - `studio_server.p12`
  - `studio_server.jks`

**NOTE** Make sure that the "studio\_server.p12" and "studio\_server.jks" certificates are compatible with Java 8. This is applicable only if the Compliance Studio server is in JDK 11 and the ECM application server is in Java 8. If there is a difference in Java versions, then both the files "studio\_server.p12" and "studio\_server.jks" need to be recreated in Compliance Studio server and replaced in all necessary locations. For more information about these certificates, see **Generate Self-signed Certificate** section in the [OFS Compliance Studio Installation Guide](#).

2. Run the following command to create certificate files:

```
openssl pkcs12 -in studio_server.p12 -nokeys -out server_cert.pem
openssl pkcs12 -in studio_server.p12 -nodes -nocerts -out server_key.pem
keytool -certreq -keystore studio_server.jks -alias studio_server -
keyalg RSA -file client.csr
openssl x509 -req -CA server_cert.pem -CAkey server_key.pem -in
client.csr -out client_certificate.pem -days 365 -CAcreateserial
```

3. Modify the path and run the following command

```
keytool -import -file "<ECM Installation Path>/client_certificate.pem"
-alias studio_server -keystore "<JDK Installed Directory>/lib/security/
cacerts" -storepass "changeit"
```

For example,

```
keytool -import -file "Testserver/client_certificate.pem" -alias
studio_server -keystore "jdk-11.0.10/lib/security/cacerts" -storepass
"changeit"
```

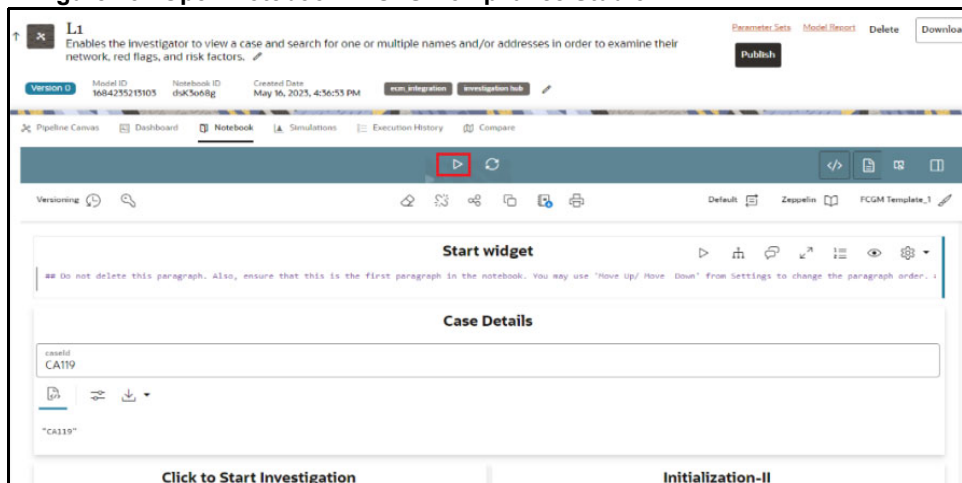
## 7.2 Executing the Notebook

The published scenario notebook can be scheduled for execution with a set of threshold values as seemed required for generating alerts or trends.

To execute a Notebook, perform the following steps:

1. Log in to the **OFS Compliance Studio** application.
2. Navigate to the **Model Pipelines** and click **Investigation Hub** objective.
3. Click **⋮** next to the corresponding Notebook and select **Open in Pipeline Designer** option.
4. Click on the **Notebook** tab. The notebook window is displayed.

**Figure 13: Open Notebook in OFS Compliance Studio**



5. Click **Run Paragraphs** icon to execute the complete Notebook.

## 7.3 PGX Data Memory Limit

While executing IH notebooks, the following error might occur with respect to PGX:

```
18:43:09,450 [http-nio-7007-exec-8] ERROR AbstractExceptionHandler - exception
mapper caught exception with code PGX-ERROR-3UU16PP39FUT218:43:09,450 [http-
nio-7007-exec-8] ERROR AbstractExceptionHandler - exception mapper caught
exception with code PGX-ERROR-
3UU16PP39FUT2java.util.concurrent.ExecutionException:
java.lang.RuntimeException: java.util.concurrent.CompletionException:
java.lang.AssertionError: accessing index: 41 that is out of bounds: [0, 41]
at
java.util.concurrent.CompletableFuture.reportGet (CompletableFuture.java:357)
~[?:1.8.0_201] at java.util
```

To resolve this issue, see the **PGX Advanced Configurations** section in the [OFS Compliance Studio Administration and Configuration Guide](#).

## OFSAA Support

Raise a Service Request (SR) in [My Oracle Support \(MOS\)](#) for queries related to OFSAA applications.

## Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.

