Oracle Financial Services Investigation Hub

Administration and Configuration Guide

Release 8.0.8.0.0

September 2020

F28095-01

ORACLE
Financial Services

Oracle Financial Services Investigation Hub Administration and Configuration Guide

Document Control

The following table provides the version control details of the document.

Table 1: Document Control

Version Number	Revision Date	Changes Done
8.0.8.0.0	Updated: September 2020	The Dynamic Search parameters can be added to the Notebook. For more information, see Dynamic Search Parameters.
8.0.7.4.0	Updated: April 2020	The Investigation Hub application is integrated with the ECM application to investigate the ECM cases using Investigation Hub. For more information, see Integrating Investigation Hub with ECM.
8.0.7.3.0	Created: March 2020	Created the first version of the Investigation Hub Administration Guide for 8.0.7.3.0 Release.

This table records the number of revisions or changes done to this document as part of a release. The version control specifies that the document is last updated as part of the v8.0.7.4.0 release in April 2020.

Table of Contents

1 About this Guide 5

1.1 Who Should Use This Guide 5

1.2 Scope of This Guide 5

1.3 How this Guide is Organized 5

1.4 Where to Find More Information 5

1.5 Conventions Used in this Guide 6

1.6 Abbreviations 6

2 About Oracle Financial Services Investigation Hub 7

2.1 Introduction 7

2.1.1 Key Features 7

2.2 Administration and Configuration Activities 7

2.3 Providing Permissions to a Notebook 8

3 Managing User Administration 10

4 Configuring the Notebook Parameters 11

4.1 Configuring the Investigation Recommendation Score 11

4.2 Configuring the Red Flag 12

4.3 Configuring the Risk Factors 13

4.4 Configuring the Network Disposition Score 14

4.5 Dynamic Search Parameters 15

5 Additional Configuration 17

5.1 Configuring Interpreters 17

5.2 Managing Graphs 17

5.3 Managing Templates 17

6 Integrating Investigation Hub with ECM 18

6.1 Prerequisites 18

6.2 Updating the Database Tables in ECM 18

6.2.1 Creating an Encrypted Password 20

6.3 Mapping IH Entity/Tab in ECM Case Designer 20

7 Appendix - Generating Correlation Networks 21

8 Appendix - API for Running All Paragraphs 22
9 OFSAA Support Contact Details 23
10 Send Us Your Comments 24

1 About this Guide

This guide gives comprehensive instructions for system administration, daily operations, and maintenance of Oracle Financial Services Investigation Hub application.

Topics:

- Who Should Use This Guide
- Scope of This Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide
- Abbreviations

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. Also, the System Administrator 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 details about 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

The following table lists the conventions used in this guide and their associated meanings.

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

The following table lists the abbreviations used in this guide.

Table 2: Abbreviations Used in This Guide

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
IH	Investigation Hub

2 About Oracle Financial Services Investigation Hub

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

Topics:

- Introduction
- Administration and Configuration Activities
- Providing Permissions to a Notebook

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 generate case narratives and insights, highlights risk factors, and red flags which are meaningful to the investigation and recommend 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.

- **ECM Integration:** Enable Case Investigators to access additional rich information about a case such as, case summary, a detailed narrative about case entities, graph view of a case, and so on, which is otherwise not available in ECM.

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

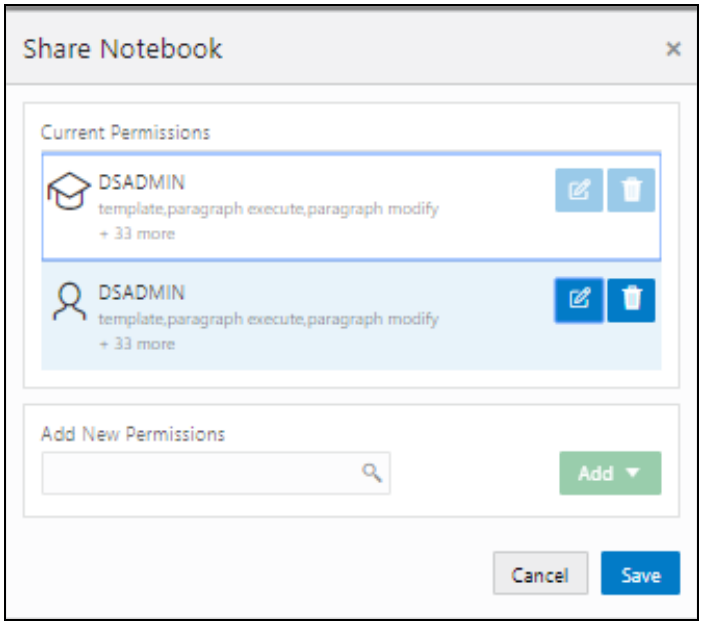
The Share button allows you to share a notebook with another user, user group, or role. This option helps you to provide the permission of a notebook to a specific user.

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:

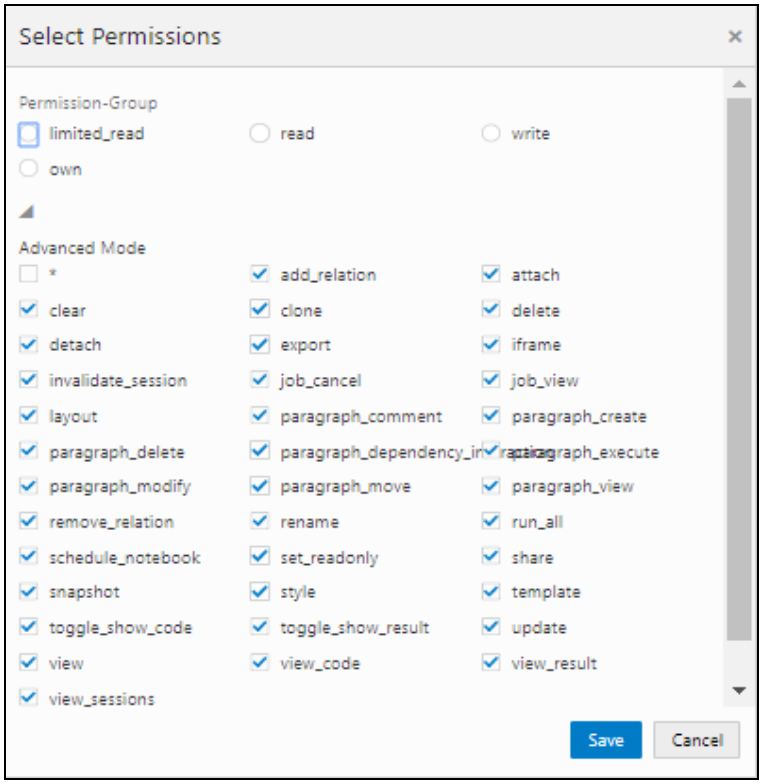
1. Navigate to Investigation Hub application home page.
2. Navigate to any notebook of application.
3. Click **Share**.

Figure 1: Share Notebook Window



4. Click **Add** icon.

Figure 2: Select Permissions Window



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 the *Oracle Financial Services Investigation Hub User 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, and map users to groups, domains and roles, grant permissions based on user roles and requirements, and so on.

For more information, see *Managing User Administration* chapter in the *OFS Crime and Compliance Studio Administration Guide*.

4 Configuring the Notebook Parameters

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

- Special Investigation Notebook
- Level 1 Case Investigation
- Level 2 Case Investigation

> **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* in the *Oracle Financial Services Crime and Compliance Studio Installation and Configuration Guide*.

Topics:

- Configuring the Investigation Recommendation Score
- Configuring the Red Flag
- Configuring the Risk Factors
- Configuring the Network Disposition Score
- Dynamic Search Parameters

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 in 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, follow these steps:

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

Figure 1: Configure Recommendation Score in the Initialization-I Paragraph

```
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 the **Red Flag** paragraph of the **Special Investigation** notebook. An Investigator can view these details during the investigation process.

To configure the Red Flag indicator, follow these steps:

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

Figure 2: Configure Red Flag in the Initialization-I Paragraph

```
/***********************************************
 * 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 code to add a query for the red flag parameter and execute the paragraph.
4. Navigate to the Red Flags paragraph.

Figure 3: 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 given 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 a 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 the Risk Factors paragraph of the Special Investigation notebook.

To configure the risk factors, follow these steps:

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

Figure 4: Configure Risk Factors in the Initialization-I Paragraph

```
/*********************************************
 * 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 the risk factors parameter and execute the paragraph.
4. Navigate to the Risk Factors paragraph.

Figure 5: 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 the **Initialization - I** paragraph.

4.4 Configuring the Network Disposition Score

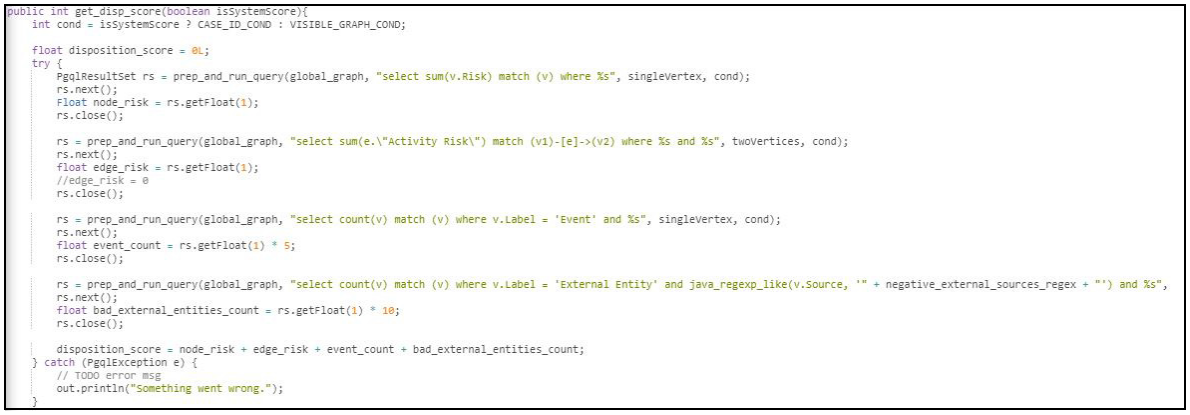
Network disposition is calculated using the following formula:

```
Sum of Node Risk/Node Count
```

To configure the Network Disposition Score, follow these steps:

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

Figure 6: 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 {
        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 Dynamic Search Parameters

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=}"
```

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

To add a new search criterion, follow these steps:

1. Navigate to the **Special Investigation** notebook.
2. Open the codes of the **Input Search Results** paragraph notebook.
3. Add new variable and getter setter methods for the input field in `searchEntry` class and result class in Initialization 3.
4. Add a new field in input search results. For example: `String givenTaxId = cleanString("${Tax Id}");)`.
5. 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..
6. Add the query for the input field in the `getMatchesForPGQLQuery`..

7. Update the merging answers section and add the new search field functions (getter and setter).
8. Update the `readInResultData` function and add the new search field to the `VertexBuilder` node.

5 Additional Configuration

This chapter provides information about additional configuration for Investigation Hub.

Topics:

- Configuring Interpreters
- Managing Graphs
- 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 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 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 Managing Template section in the *Oracle Financial Services Crime and Compliance Studio User Guide*.

6 Integrating Investigation Hub with ECM

Investigation Hub (IH) is integrated with Enterprise Case Management (ECM) to enable Case Investigators to access additional rich information about a case such as, 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

Download and apply the patch **31185239** on the Oracle Financial Services Enterprise Case Management 8.0.8.0.0 application. For more information, see the Readme file packaged with the `OFS ECM 8.0.8.0.4` Patch Installer Archive File.

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.

- This table 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 1: FCC_CM_STUDIO Table

PlaceHolder	Description
##URL##	Replace the placeholder with the FCC Studio URL. For example: http://<Host_Name>:7008
##SSOHEADER##	Replace the placeholder with the SSOHEADER to access FCC Studio For example: oam_remote_user **NOTE:** If SSO is enabled for Studio and ECM, ensure to replace the ##SSO-HEADER## placeholder value with the relevant SSOHEADER, and provide null for ##PASSWORD##.
##USERNAME##	Use the Studio user details to login (provisioned to DSADMIN or DSUSER role). **NOTE:** The Username must be NULL if SSO is used.
##PASSWORD##	The encrypted password that you must use to login to the Notebook. To create the encrypted password, see Creating an Encrypted Password.

- This table 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 pro-

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

Table 2: FCC_CM_CTYPE_NB_MAPPING Table

Placeholder	Description
For the ECM user roles: CMANALYST1 and CMANALYST2	
##CASE_TYPE##	Replace the placeholder with the case type for which you want to enable the IH 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. **NOTE:** You must provide the notebook ID of the ECM_Integration_L1 notebook for the Analyst role.
For the ECM user role: CMSUPRVISR	
##CASE_TYPE##	Replace the placeholder with the case type for which you want to enable the IH 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. **NOTE:** You must provide the Notebook ID of the ECM_Integration_L2 notebook for the Supervisor role.

- This table 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. 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 3: FCC_CM_CTYPE_NB_MAPPING Table

Table Entry	Description
V_NB_TOOLBAR	• '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.

Table 3: FCC_CM_CTYPE_NB_MAPPING Table

Table Entry	Description
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 for the user.
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_NOTEBOOK_ID,V_CREATED_DATE,V_CREATED_BY,V_UPDATED_BY,V_UPDATED_DATE,V_NB_TOOLBAR,V_ADD_PARA,V_PARA_ACTIONS,V_PARA_CODE) values ('<User_Role>','##CASE_TYPE##','##notebookId##',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 `/Studio Installation path>/OFS_FCCM_STUDIO/ficdb/bin` directory.
3. Execute the following command:

   `./FCCM_Studio_Base64Encoder.sh <password to encrpt>`
4. Copy the encrypted password from the putty session and use it in the password field in **fcc_cm_studio** table.

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 - 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, follow these 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.

8 Appendix - 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.

OFSAA Support Contact Details

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.