

Oracle Financial Services Investigation Hub

Administration and Configuration Guide

Release 8.0.8.3.0

June 2021

F28095-01

ORACLE
Financial Services

Copyright © 2021 Oracle and/or its affiliates. All rights reserved.

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 de-compilation of this software, unless required by law for interoperability, is prohibited.

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information 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 on third party licenses, click [here](#).

Document Control

Version Number	Revision Date	Change Log
8.0.8.3.0	Created: June 2021	The following chapters are updated with new images and respective parameters: <ul style="list-style-type: none">• Configuring the Red Flag• Configuring the Risk Factors• Configuring the Network Disposition Score
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 OFS IH application is integrated with the ECM application to investigate the ECM cases using OFS IH. For more information, see Integrating OFS IH 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.

Table of Contents

1	Preface	6
1.1	Summary	6
1.2	Documentation Accessibility	6
1.3	Audience	6
1.4	Related Documents	6
1.5	Conventions	7
1.6	Abbreviations	7
2	About Oracle Financial Services Investigation Hub	8
2.1	Introduction	8
2.1.1	Key Features	8
2.2	Administration and Configuration Activities	8
2.3	Providing Permissions to a Notebook	9
3	Managing User Administration	11
4	Configuring the Notebook Parameters	12
4.1	Configuring the Investigation Recommendation based on Network Disposition Score	12
4.2	Configuring the Red Flags	13
4.3	Configuring the Risk Factors	14
4.4	Configuring the Network Disposition Score	15
4.5	Adding New Dynamic Search Parameters	15
5	Additional Configuration	17
5.1	Configuring Interpreters	17
5.2	Managing Graphs	17
5.3	Data visualization	17
5.4	Managing Templates	18
6	Integrating OFS IH with ECM	19
6.1	Prerequisites	19
6.2	Updating the Database Tables in ECM	19
6.2.1	Creating an Encrypted Password	21
6.3	Mapping IH Entity/Tab in ECM Case Designer	21

7 Appendix22

- 7.1 Generating Correlation Networks 22
- 7.2 Creating a New CSV 22
- 7.3 Load Data to Graphs..... 23
- 7.4 Execute the Notebook.....24

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

The following table lists the conventions used in this document.

Table 1: 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 that appears on the screen, or text that you enter.

1.6 Abbreviations

The following table lists the abbreviations used in this document.

Table 2: Abbreviations Used in This Guide

Abbreviation	Meaning
OFS	Oracle Financial Services
FCC Studio	Financial Crime and Compliance Studio
AAI	Analytical Applications Infrastructure
PGX	Parallel Graph Analytics
PGQL	Property Graph Query Language
LHS	Left Hand Side
OFSCC	Oracle Financial Services Crime and Compliance
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](#)
- [Administration and Configuration Activities](#)
- [Administration and Configuration Activities for new Notebook](#)
- [Providing Permissions to a Notebook](#)

2.1 Introduction

OFS IH is an application built on FCC Studio which allows investigators to rapidly view the case and adhoc 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 adhoc investigations. OFS IH 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 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 FCC Studio, which includes a highly scalable in-memory Oracle Graph Analytics Engine (PGX), AI, and machine learning.
- Utilizes the proven FCGM, 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.
- **ECM Integration_L1:** Enable Level 1 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. Allows the investigator to explore a case - including graph, risk factors, and red flags.

- **ECM Integration_L2:** Enable Level 2 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. 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.
- Administrator loads the graph into memory and publishes it so other notebooks can access and use it.

2.3 Providing Permissions to a Notebook

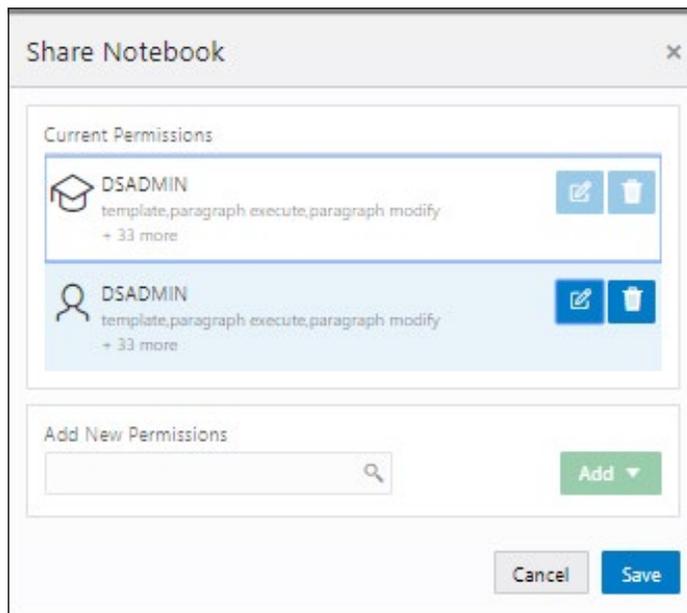
The Share button allows you to share a notebook with another user, user group, or role. This option helps you to provide the permission of a notebook to a specific user.

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 OFS IH application home page.
2. Navigate to any notebook of application.
3. Click **Share**. The Share Notebook window is displayed.

Figure 1: Share Notebook Window



4. Click **Add** icon. The Select Permissions window is displayed.

Figure 2: Select Permissions Window

The screenshot shows a 'Select Permissions' dialog box with the following content:

Permission-Group

- limited_read
- own
- read
- write

Advanced Mode

- *
- clear
- detach
- invalidate_session
- layout
- paragraph_delete
- paragraph_modify
- remove_relation
- schedule_notebook
- snapshot
- toggle_show_code
- view
- view_sessions
- add_relation
- clone
- export
- job_cancel
- paragraph_comment
- paragraph_dependency_invalidate
- paragraph_move
- rename
- set_readonly
- style
- toggle_show_result
- view_code
- attach
- delete
- iframe
- job_view
- paragraph_create
- paragraph_execute
- paragraph_view
- run_all
- share
- template
- update
- view_result

Buttons: Save, Cancel

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 a 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** section 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 OFS IH application:

- Special Investigation Notebook
- ECM_Integration_L1
- ECM_Integration_L1

Topics:

- [Configuring the Investigation Recommendation Score](#)
- [Configuring the Red Flag](#)
- [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 in between 0 to 25, the case status is displayed as **Further Investigation**.
- If the investigation score is in between 25 to 51, the case status is displayed as **Low Risk Network**.
- If the investigation score is in between 50 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. Navigate to the Special Investigation notebook that is assigned for a particular user role.
2. 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 3: Start Investigation Paragraph



- Execute all subsequent paragraphs. The Network Disposition score is displayed.

An Investigator can view the investigation recommendation status based on this Network Disposition score.



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, ECM_Integration_L1, and ECM_Integration_L2 notebooks. An Investigator can view following details during the investigation process:

- Entities with SARs filed
- Transactions with 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:

- Navigate to the Special Investigation notebook.

NOTE You can follow the same steps for ECM_Integration_L1, and ECM_Integration_L2 notebooks.

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

Figure 4: Configure Red Flag Paragraph

```

66
67 String   txn_query="select count(e) "
68         + "match (v1)-[e]-(v2) "
69         + "where e.\"Original ID\" is not null and "
70         + "e.Label in ('end to end wire txn', 'end to end mi txn', 'cash txn', 'send mi to', 'transfer mi to', 'receive mi from', 'send wire
71         + " and v2.Country in ('CHE', 'BHS', 'ANB', 'US') "
72         + " and v1.Country in "+ countryListString
73         + " GROUP BY e.\"Original ID\" ";
74
75 PgqlResultSet txn_query_result = prep_and_run_query(resultGraph, txn_query, twoVertices, CASE_ID_COND);
76
77 for(PgxResult r:txn_query_result){
78     count_txn++;
79 }
80
81 }
82
83
84 out.println(String.join("\t", "Red Flags", "Hits (Initial)", "Hits (Investigator)"));
85
86 String redflags = String.join("\n",
87     String.join("\t", "Entities with SARs filed", format_score(count_sar_w1),format_score(count_sar_w1_visible)),
88     String.join("\t", "Transactions with payer in risky country and beneficiary in tax haven", format_score(count_txn),format_score(count
89     String.join("\t", "Accounts interacting with sanctioned entities", format_score(count_sanctioned), format_score(count_sanctioned_visibl
90 );
    
```

- 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')
```

- Execute the Red Flags paragraph.

Figure 5: 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_trxn),format_score(count
89   String.join("\t", "Accounts interacting with sanctioned entities", format_score(count_sanctioned), format_score(count_sanctioned_visibl
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 organization 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, ECM_Integration_L1, and ECM_Integration_L2 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, and ECM_Integration_L2 notebooks.

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

Figure 6: Configure Risk Factors

```

2
3 /*****
4 * This need to be Customize as Per Customer Data
5 Entity Type and Industry can be custmise 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_CON
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

```

3. 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>')

4. Execute the Risk Factors paragraph.

Figure 7: 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

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:

1. Navigate to the Special Investigation notebook.
2. Open the codes of the Network Disposition Score paragraph.

Figure 8: 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 {
        PgsqlResultSet 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 (PgsqlException 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 for non-case entities within the notebook.

NOTE

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

Out of 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 configuration for OFS IH.

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 OFS IH 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 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 Crime and 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 **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 **Managing Template** section in the [Oracle Financial Services Crime and 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, 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 **32559114** 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 8.0.8.0.41 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).
##PASSWORD##	The encrypted password that you must use to login to the Notebook. To create the encrypted password, see Creating an Encrypted Password.
api_version	The API version number is 20210315.

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 provides 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: 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##	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 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. 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 following 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 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 for the user.

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 <Studio Installation path>/OFS_FCCM_STUDIO/ficdb/bin directory.
3. Run 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

7.1 Generating Correlation Networks

This is a sample notebook and an example of how users can correlate cases in the graph when not using ECM.

After event data is loaded from different applications into OFS IH, 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, ECM_Integration_L1, and ECM_Integration_L2 notebooks. To generate the correlation network, follow these steps:

1. Navigate to the OFS IH Home page.
2. Navigate to the Generate Correlated Networks notebook.
3. Execute the notebook.

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

After the notebooks are created you can carry out the following tasks to load data into your notebook and also execute to view the insights:

- Create New CSV file
- Load the Graphs
- Execute the Notebook

Topics:

- [Creating a New CSV](#)
- [Load Data to Graphs](#)
- [Execute the Notebook](#)
- [Adding New Dynamic Search Parameters](#)

7.2 Creating a New CSV

The data is loaded into the graphs using the CSV files. You can create a new CSV file as per requirements, which can be used for loading data into the graphs.

To create a new CSV file, perform the following steps:

1. Create an Excel file with required data and save it as .csv.

2. Place this CSV file at following location `<IH_Installation_Path>/Datasource` directory.
3. Navigate to `<IH_Installation_Path>/Datasource` directory and modify `CONFIG.JSON` file.

When you are creating a new CSV file, the attributes (column names of Excel) of this CSV file must be manually entered in `CONFIG.JSON` file in below mentioned format:

```
{"name" : "Tax Country", "type" : "string"},
```

Here,

Name should be same as attribute of CSV file

Type is the data type (string, float, Boolean, and so on)

NOTE

- Column headers are not required in CSV files.
- Last column of the CSV file cannot be blank (including space).
- Update the blank columns of CSV file with Null or Space.

7.3 Load Data to Graphs

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

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

1. Log in to the **OFS Studio** application.
2. Navigate to **OFS Investigation Hub** tab.
3. Create a notebook with type as **Default**.

Figure 9: Create a new notebook

NOTE

You can either load a graph in the Investigation Hub notebook or create a separate notebook with the Default type.

4. Edit the code for attributes, **dataSourceName** and **graphName** in the `pgx - java` paragraph as shown in Figure 10:

Figure 10: PGX-Java paragraph

```
%pgx-java  
PgxGraph graph = session.readGraphWithProperties(dataSourceName, "graphName");
```

NOTE If the paragraph does not exist, then create a pgx - java paragraph as shown in Figure 10.

5. Enter the name of the data source and the graph.
6. Click **Execute Paragraph** to execute the paragraph. The graph is loaded and displayed wherever you run the pgql query as shown in Figure 11:

Figure 11: PGQL Query

```
%pgql  
SELECT n,e,m FROM graphName MATCH (n)-[e]->(m)
```

7.4 Execute the Notebook

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

To execute a Notebook, perform the following steps:

1. Log in to the **OFS Studio** application.
2. Navigate to OFS Investigation Hub tab.
3. Select the Notebook that you want to execute.
4. Click the **Execute Notebook** icon to execute the complete notebook.

OFSAA Support

Raise a Service Request (SR) in [My Oracle Support \(MOS\)](#) for queries related to the 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 that has all the revised/recently released documents.

