Oracle® Financial Services

Investigation Toolkit Administration and Configuration Guide

Release 8.1.2.9.0
G30141-02
April 2025

ORACLE

Oracle Financial Services Investigation Toolkit Administration and Configuration Guide, Release 8.1.2.9.0

G30141-02

Contents

Preface

1 Overview

2 Manage User Administration

3 General Configurations for All Notebooks

4 Configuring and Customization of ECM Integration L1, Special Investigation, and ECM Case Narrative Notebooks

5 Configuration for Investigation Flow Notebook Template

6 ECM Investigation Toolkit Configuration

Document Control

This topic lists the document control of this guide.

Version Number	Revision Date	Change Log
8.1.2.9.0	April 2025	Added the **Configuration for Investigation Flow Template** chapter.

Preface

This section provides information of the Oracle Financial Services (OFS) Investigation Toolkit Administration and Configuration Guide.

Audience

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

Related Resources

This section identifies additional resources to the OFS Investigation Toolkit. You can access additional documents from the Oracle Help Center.

Abbreviations

The following table lists the abbreviations used in this document.

Table 1 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
FCGM	Financial Crime Graph Model
FCDM	Financial Crime Data Model
SQL	Structured Query Language
ECM	Enterprise Case Management
AML	Anti-money Laundering
BD	Behavior Detection
OOB	Out-of-the-Box

Documentation Accessibility

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.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

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.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: https://support.oracle.com/portal/.

1 Overview

OFS Investigation Toolkit accelerates investigations by bringing relevant information sources together (including external API calls to sources such as Quantifind), and preventing the need for the manual collation of information from disparate sources (where data is not available in OFS Enterprise Case Management). OFS Investigation Toolkit automatically generates case narratives and insights, highlights risk factors, and red flags that are meaningful to the investigation, and recommends actions based on the scoring algorithms as required.

Investigation Toolkit comes with a selection of notebook templates for customers to adapt for their own Investigative needs. Multiple types of notebooks or configurations of the same notebook can be configured and are permission driven.

The Notebook templates available are:

- Investigation Flow Template - Focused on case information, configurable narratives and highlighting of case risk factors. It follows the flow of a typical investigation.
- ECM Integration L1 Template - Primarily for users who would heavily leverage the graph in their Case Investigations, expanding beyond the boundaries of the original case.
- Special Investigation Template - Like the L1 Template but the starting point would be an entity name search rather than a case id.
- Case Narrative Template - Simple template which does not include a graph but is focused on providing a case summary as a narrative.

The L1 and Special Investigations Notebooks are built on the Financial Crime Graph Model Schema which is configurable within OFS Compliance Studio and optionally provides the capability for matching to third-party sources of data like ICIJ and well as linking internal similar internal parties.

Key Features

Investigation Toolkit includes the following key features:

- Pre-built notebooks 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
- 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
- Built on OFS Compliance Studio, which includes a highly scalable in-memory Oracle Graph Analytics Engine (PGX), AI, and machine learning
- Integrated with Quantifind API for additional information on case entities

Import Notebooks

To import notebooks, see the *Importing Notebooks* section in the *OFS Investigation Toolkit Installation Guide*.

Administration and Configuration Activities

An administrator can 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.
- ECM_Case_Narrative: Enables the investigators to access only case summary and a detailed narrative about case entities. The graph view for the case is not available in this notebook.
- Investigation Flow Template: Enables analysts to investigate cases through end-to-end process.

> **Note:**
>
> Administrators must share only the Special Investigation notebook with users (investigators) and ECM clones the Notebook for their investigation.

2

Manage 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 **IHUSRGRP** group must be assigned to the user using Investigation Toolkit.

> **Note:**
>
> Ensure that no investigation toolkit user is part of the **DSUSRGRP** group since this is an admin group.

For more information, see the **Mapping User Groups** section in the OFS Compliance Studio Administration and Configuration Guide.

2.1 Investigation Toolkit User Group Mapping

To access the Investigation Toolkit notebook template in the ECM application, ensure that you map IHUSRGRP to the respective user in ECM.

To map a user group:

1. Create new user group with name **IHUSRGRP** in ECM and authorize the group.
2. Map **IHUSRGRP** group to **DSUSER** role in ECM and authorize it.
3. Map the created **IHUSRGRP** to the ECM user.

    > **Note:**
    >
    > If it is already mapped, unmap DSUSRGRP from ECM user.

3

General Configurations for All Notebooks

This chapter lists all the common configurations related to all the notebooks.

1. For importing any notebook template and getting the notebook id, see the OFS Investigation Toolkit Installation Guide.
2. To configure specific notebook template such as L1, SI, ECM Case Narrative Notebook template, Investigation Flow Notebook Template, follow the below chapters.
3. To configure specific notebook template with ECM, follow ECM Toolkit Integration chapter.

4

Configuring and Customization of ECM Integration L1, Special Investigation, and ECM Case Narrative Notebooks

This chapter lists all the configurations applicable for ECM Integration L1, Special Investigation, and ECM Case Narrative Notebooks.

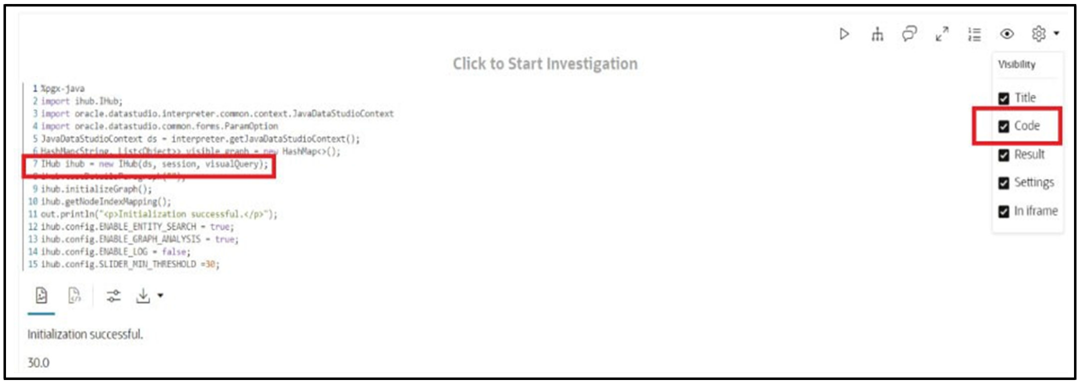
4.1 Configure the Investigation Toolkit Parameters

This chapter provides information on configuring and customization of the Investigation Toolkit parameters for Special Investigation, ECM Integration L1, and ECM Case Narrative seeded notebooks.

Updating Notebook Parameters Configuration

An admin user can configure the parameters of the Investigation Toolkit notebooks by updating the values. To update the value, follow these steps:

1. Login to Data Studio.
2. Navigate to the **Investigation Toolkit** folder.
3. Open the desired notebook.
4. Open the notebook and navigate to the **Click to Start Investigation** paragraph in ECM Integration L1 and Special Investigation notebooks or **Entity Summary Risk Report** paragraph in the ECM Case Narrative notebook.



```
%pgx-java
import ihub.IHub;
import oracle.datastudio.interpreter.common.context.JavaDataStudioContext
import oracle.datastudio.common.forms.ParamOption
JavaDataStudioContext ds = interpreter.getJavaDataStudioContext();
HashMap<String, List<Object>> visible_graph = new HashMap<>();
IHub ihub = new IHub(ds, session, visualQuery);
[illegible]
ihub.initializeGraph();
ihub.getNodeIndexMapping();
out.println("<p>Initialization successful.</p>");
ihub.config.ENABLE_ENTITY_SEARCH = true;
ihub.config.ENABLE_GRAPH_ANALYSIS = true;
ihub.config.ENABLE_LOG = false;
ihub.config.SLIDER_MIN_THRESHOLD =30;
```

```
Initialization successful.

30.0
```

5. Click on the **Visibility** icon and select the **Code** option.
6. Navigate to the line `IHub ihub = new Ihub(ds, session, visualQuery);`
7. Update the value by adding a line just after the above line with `ihub.config.` followed by `variable_name` and then the value.
   For example, `ihub.config.DATE_DISPLAY_FORMAT = "MM-dd-yyyy";`
8. To update another value, add the additional line as above.

For example, with multiple parameter updates as follows:

```
IHub ihub = new IHub(ds, session, visualQuery);
ihub.config.DATE_DISPLAY_FORMAT = "MM-dd-yyyy";
ihub.config.HIGH_RISK_MIN_SCORE_BOUNDARY = 5;
```

4.1.1 Add Parameters to the Notebooks

An admin user can configure the parameters of the notebook as described in the following table.

Table 4-1 Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override
Generic Configuration	ENABLE_GRAPH_ANALYSIS	It enables graph analysis if the value is set to “true”. The value is either true or false. **NOTE:** Set the value as “false” for the ECM case narrative notebook. Set the value as “True” for the ECM Integration L1 and Special Investigation notebooks.	To disable it in the ECM Integration L1 notebook. `ihub.config.ENABLE_GRAPH_ ANALYSIS = false;`
Generic Configuration	ENABLE_ENTITY_SEARCH	It enables additional entity search if the value is set to “true”. The value is either true or false. By default, it is set to true.	To disable it in ECM Integration L1 notebook. `ihub.config.ENABLE_ENTITY_SEARCH = false;`

Generic Configuration	RISK_PROHIBITED_LIST_OF_BUSINESS	It indicates the prohibited list of businesses. For example, Bank.	To update the list.
			`ihub.config.RISK_PROHIBITED_LIST_OF_BUSINESS =new ArrayList();`
			`ihub.config.RISK_PROHIBITED_LIST_OF_BUSINESS.add(" BANK");`
			`ihub.config.RISK_PROHIBITED_LIST_OF_BUSINESS.add(" AGRI");`
			`ihub.config.RISK_PROHIBITED_LIST_OF_BUSINESS.add(" GOVT");`
			Or
			`ihub.config.RISK_PROHIBITED_LIST_OF_BUSINESS = List.of("BANK","AGRI","GO VT");`

Generic Configuration	TAX_HAVEN_COUNTRY_LIST	It indicates the list of countries having taxes. For example: CHE, BHS, ANB, US, etc.	To update the list. `ihub.config.TAX_HAVEN_COUNTRY_LIST = List.of("CHE", "BHS","ANB", "US");`

Table 4-1 (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override
Generic Configuration	DATE_DISPLAY_FORMAT	It indicates the date format to display in the narrative/tabular format. The format isYYYY-MMM-DD. **NOTE:** For more information on formatting the string, see the *DateTimeFormatter*.	Set the date format as follows. `ihub.config.DATE_DISPLAY_FORMAT =MM-dd-yyyy;`
Generic Configuration	ENABLE_LOG	It enables logs in to the paragraph output if the value is set to "true". The value is true or false. It helps to debug the notebook. By default, set it to false.	To enable: `ihub.config.ENABLE_LOG = true;`
Generic Configuration	HIGH_RISK_MIN_SCORE_BOUNDARY	It indicates the risk score. If the values are more than HIGH_RISK_MIN_SCORE_BOUNDARY,it is considered as high risk. The values are 7 - 10.	To set the minimum score boundary to 6: `ihub.config.HIGH_RISK_MIN_SCORE_BOUNDARY = 6;`

Sub Graph Loading	NODE_PROVIDER_EXPAND_EXCLUSION_LIST	It indicates subgraph loading for investigation; neighbors of the node providers mentioned in this list will be excluded from subsequent loading.
		The values are:
		• "Derived Entity"
		• "Institution"
		• "ICIJ External Address"
		• "ICIJ External Entity"
			To override the exclusion list:
			`ihub.config.NODE_PROVIDER_EXPAND_EXCLUSION_LIST =List.of("DerivedEntity","ICIJ External Entity", "ICIJ External Address");`
			Or
			`ihub.config.NODE_PROVIDER_EXPAND_EXCLUSION_LIST.remove("Institution");`

Sub Graph Loading	INITIAL_LOAD_HOPS	It indicates the number of hops to load for the initial step while creating the sub graph. The recommended values are between 0 to 2.The default value is 1. **Note:**This affects the sub graph loading time. For example: The value can be set to 0 to load entities without any edges.	To override the value: `ihub.config.INITIAL_LOAD_HOPS = 0;`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	SEARCH_TYPE	It indicates the search type for matching. The value is fuzzy.	To update it to "exact": `ihub.config.SEARCH_TYPE = "exact";`

Table 4-1 (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override
Real-time Matching **NOTE:** It is applicable for Entity Search only.	NAME_SEARCH_METHOD	It indicates the scoring method for the name search. The values are: • mlboostednamematching • jaroWinkler	To update the scoring method to “jaroWinkler”: `ihub.config.NAME_SEARCH_METHOD = “jaroWinkler”;`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	ADDRESS_SEARCH_METHOD	It indicates the scoring method for address search. The values are: • mlboostednamematching • jaroWinkler	To update the scoring method to “jaroWinkler”: `ihub.config.ADDRESS_SEARCH_METHOD = “jaroWinkler”;`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	CONFIGURABLE_CED	CED for address matching, where CED stands for Character Edit Distance. Comparison is good for matching textual values that may be misspelled and thus have one or two character differences between each other. The value is auto. For more information, see the *OFS Compliance Studio Matching Guide.*	To set the value to 2: `ihub.config.CONFIGURABLE_CED = 2`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	SLIDER_MIN_THRESHOLD	It indicates the match score minimum value on the slider. For example, 50.	To set the minimum value to 70%: `ihub.config.SLIDER_MIN_THRESHOLD = 70;`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	SLIDER_MAX_THRESHOLD	It indicates match score maximum value on the slider. For example, 100.	To set the maximum value to 90%: `ihub.config.SLIDER_MAX_THRESHOLD = 90;`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	SLIDER_THRESHOLD_STEP	It indicates the slider step size. For example, 5.	To set the slider step to 10%: `ihub.config.SLIDER_THRESHOLD_STEP = 10;`
Real-time Matching **NOTE:** It is applicable for Entity Search only.	SLIDER_THRESHOLD_DEFAULT	It indicates the match score default value on the slider. For example, 50.	To set the max value to 80%: `ihub.config.SLIDER_THRESHOLD_DEFAULT = 80;`

Table 4-1 (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override

Status Code Mapping	STATUS_CODE_MAPPING	It indicates the value of the status code. It is used to show Account and Customer status in the narrative paragraph. The status codes are as follows:
		• l A -Active
		• l I -Inactive
		• l N - Not a customer
		• l P -Pending
			To set the more mapping:
			`ihub.config.STATUS_CODE_MAPPING.put("C","Priority Customer");`
			To override the mapping:
			`ihub.config.STATUS_CODE_MAPPING= new HashMap<>;`
			`ihub.config.STATUS_CODE_MAPPING.put("A""Active");`
			`ihub.config.STATUS_CODE_MAPPING.put("D","Dormant");`
			`ihub.config.STATUS_CODE_MAPPING.put("P","Priority Customer");`

Color and Weight for Risk Factor and Red Flags	DEFAULT_SCORE_FONT_COLOUR	It indicates the default score font color .For example, seagreen. For more information, see *Color Names* for other color code.	To set the default color to blue: `ihub.config.DEFAULT_SCORE_FONT_COLOUR = blue;`
Color and Weight for Risk Factor and Red Flags	HIGHLIGHTED_SCORE_FONT_COLOUR	It indicates the highlighted score font color. For example, crimson.	To set the default color to red: `ihub.config.DEFAULT_SCORE_FONT_COLOUR = red;`
Color and Weight for Risk Factor and Red Flags	DEFAULT_SCORE_FONT_WEIGHT	It indicates the default score font weight. The supported values are normal and bold. For example, normal.	To set the default font to bold: `ihub.config.DEFAULT_SCORE_FONT_WEIGHT = bold;`
Color and Weight for Risk Factor and Red Flags	HIGHLIGHTED_SCORE_FONT_WEIGHT	It indicates the highlighted score font weight. The supported values are normal and bold. For example, bold.	To set the highlighted font to normal: `ihub.config.HIGHLIGHTED_S CORE_FONT_WEIGHT =normal;`
Color and Weight for Risk Factor and Red Flags	HIGHLIGHTED_SCORE_MIN_VALUE	It indicates the highlighted score minimum value. If the value is less than HIGHLIGHTED_SCORE_MIN_VALUE, it will be displayed with default color and weight. The minimum value is 6.	To set the min value to highlight as 3: `ihub.config.HIGHLIGHTED_S CORE_MIN_VALUE = 3;`

Table 4-1 (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override

Disposition Score	DISPOSITION_COLOUR_MAP	It indicates a color map for disposition.
		To set the color depending on score boundaries, add the minimum score as 1 and color in the hashmap. The higher value for the boundary will be less than the next boundary.
		For example, the color and its boundary values are:
		• l seagreen[0,25]
		• l gold(25,51]
		• l darkorange(51,76]
		• l crimson(76,100]
		• If mapping is 0, the minimum value is 0 and maximum value is 25 for seagreen color.
		• If mapping is 25, the minimum value is 26 and maximum value is 51 for gold color.
		• If mapping is 51, the minimum value is 52 and maximum value is 76 for dark orange color.
		• If mapping is 76, the minimum value is 77 and maximum value is 100 for crimson color.
			To override the color:
			• Sea Green
			– Mapping: 0
			– Color: seagreen
			– Min Value: 0
			– Max Value: 24
			• Yellow
			– Mapping: 24
			– Color: yellow
			– Min Value: 25
			– Max Value: 39
			• Gold
			– Mapping: 39
			– Color: gold
			– Min Value: 40
			– Max Value: 59
			• Dark Orange
			– Mapping: 59
			– Color: darkorange
			– Min Value: 60
			– Max Value: 74
			• Crimson
			– Mapping: 74
			– Color: crimson
			– Min Value: 75
			– Max Value: 89
			• Brown
			– Mapping: 89
			– Color: brown
			– Min Value: 90
			– Max Value: 100
			`ihub.config.DISPOSITION_COLOUR_MAP = newHashMap<>;`
			`ihub.config.DISPOSITION_COLOUR_MAP .put(0,"seagreen");`
			`ihub.config.DISPOSITION_COLOUR_MAP .put(24,"yellow");`
			`ihub.config.DISPOSITION_COLOUR_MAP .put(39,"gold");`
			`ihub.config.DISPOSITION_COLOUR_MAP .put(59,"darkorange");`
			`ihub.config.DISPOSITION_COLOUR_MAP .put(74,"crimson");`
			`ihub.config.DISPOSITION`

Table 4-1 (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override
			`_COLOUR_MAP .put(89,"brown");`
Disposition Score	RECOMMENDATION_CLOSE_MESSAGE	It indicates the default recommendation message. This is recommended when the disposition score is less than the first declared range. For example, Close Case (Reason: False Positive)	To update the recommendation close message: `ihub.config.RECOMMENDATION_CLOSE_MESSAGE = "False Positive, Close Case";`

Table 4-1 (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override

Disposition Score	DISPOSITION_RECOMMENDATION_MAP	It indicates a recommendation map for disposition.
		To set the message depending on score boundaries, add the minimum score as 1 and the message in the hashmap. The higher value for the boundary will be less than the next boundary.
		For example, the message and its boundary values are:
		• Close Case (Reason:False Positive) [0,25]
		• l Low Risk Network(25,51]
		• l Medium Risk Network(51,76]
		• Potential High Risk Network (76,100]
		If mapping is 0, the minimum value is 0 and maximum value is 25 for Close Case (Reason: False Positive) message.
		If mapping is 25, the minimum value is 26 and maximum value is 51 for Low Risk Network message.
		If mapping is 51, the minimum value is 52 and maximum value is 76 for Medium Risk Network message.
		If mapping is 76, the minimum value is 77 and maximum value is 100 for Potential High Risk Network message.
			To override the recommendation message:
			• If mapping is 0, the minimum and maximum values of the Close Case (Reason: False Positive) message are 0 and 24.
			• If mapping is 24, the minimum and maximum values of the Low Risk Network message are 25 and 39.
			• If mapping is 39, the minimum and maximum values of the Medium Risk Network message are 40 and 59.
			• If mapping is 59, the minimum and maximum values of the Potential High Risk Network message are 60 and 74.
			• If mapping is 74, the minimum and maximum values of the High Risk Network message are 75 and 89.
			• If mapping is 89, the minimum and maximum values of the Very High Risk Network message are 90 and 100.
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP = new HashMap<>;`
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP.put(0,"CloseCase (Reason: FalsePositive)");`
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP.put(24, "Low RiskNetwork");`
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP.put(39, "Medium RiskNetwork");`
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP.put(59, "Potential HighRisk Network");`
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP.put(74, "High Risk`

Table 4-1   (Cont.) Configure Parameter for Notebook

Type	Parameter	Description	Example Code Snippet to Override

			`Network");`
			`ihub.config.DISPOSITION_RECOMMENDATION_MAP.put(89, "Very High Risk Network");`

Disposition Score	COUNTRY_SEPARATOR	It indicates the delimiter for the attribute "Country". The value is ~ ;	-
Advance Configuration **NOTE:** The parameters should be updated only when the graph pipeline is customized.	GRAPH_NAME	It indicates the PG graph name. For example, FINANCIAL_CRIME_GLOBAL_GRAPH.	-
Advance Configuration **NOTE:** The parameters should be updated only when the graph pipeline is customized.	GRAPH_PIPELINE_ID	It indicates the graph pipeline ID. For example, 853e4164-XXXX-XXXX- XXXX-XXXXXXXXXXXX	-
Advance Configuration **NOTE:** The parameters should be updated only when the graph pipeline is customized.	RESULT_CASE_GRAPH	It indicates the subgraph name. For example, caseGraph.	-
Advance Configuration **NOTE:** The parameters should be updated only when the graph pipeline is customized.	SEPARATOR	It indicates the separator used in the graph pipeline. For example,~	-
Advance Configuration **NOTE:** The parameters should be updated only when the graph pipeline is customized.	KEY_COLUMN_ID	It indicates the key attribute for the node name. For example, id.	-

4.1.2 Rename Input Parameters

An admin user can rename the input parameters in the notebooks.

1. Login to **Data Studio**.
2. Navigate to the **Investigation Toolkit** folder.
3. Open the desired notebook.
4. Open the notebook and navigate to the **Click to Start Investigation** paragraph in ECM Integration L1 and Special Investigation notebooks or **Entity Summary Risk Report** paragraph in the ECM Case Narrative notebook.
5. Click on the **Visibility** icon and select the **Code** option.
6. Navigate to the line `IHub ihub = new Ihub(ds, session, visualQuery);`

7. Update the value by adding a line just after the above line with `ihub.dynamicForms.` followed by `variable_name` and then the value.

   For example:

   ```
   ihub.dynamicForms.addressTextBox = "Complete Address";
   ```

8. To update another value, add the additional line as above.

   For example, with multiple parameter updates as follows:

   ```
   IHub ihub = new IHub(ds, session, visualQuery);
   ihub.dynamicForms.addressTextBox = "Complete Address";
   ihub.config.nameTextBox = "Full Name";
   ```

4.1.2.1 Configure Parameters for Entity Search

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

Users can customize the dynamic forms for the notebook as described in the following table.

Table 4-2 Configure Parameters for Entity Search

Parameter	Significance
nameTextBox	It indicates the label of the text box for Name. The value is Name.
addressTextBox	It indicates the label of the text box for the Address. The value is Address..
dateTextBox	It indicates the label of the Date and Time picker for Date. The value is Date.
defaultDateFormat	It indicates the format for the Date and Time picker. The value is yyyy-MM-dd HH:mm:ss
defaultDateValue	It indicates the default Date and Time Value. The value is 1970-01-01 00:00:00
useDateCheckBox	It indicates the check box's label to suggest if to use the Date value for “Non-Case Entity”. The value is Use Date?
emptyListCheckBox	It indicates the label of the check box for resetting the non-case entities in the L1 notebook or List of Search Entity in the SI notebook. The value is Empty the existing entities list?
matchScoreThresholdSlider	It indicates the label of the slider for threshold score. The value is Minimum Match Score Cutoff in %
taxIdTextBox	It indicates the label of the text box for Tax ID. The value is Tax Id.
maxMatchCountTextBox	It indicates the label of the text box for Top Critical Matches. The value is Top Critical Matches.
noOfHopsToPreFetch	It indicates the label of the text box for number of hops to be considered in the case graph. The value is the Number of Hops to Pre-Fetch.

Table 4-2 (Cont.) Configure Parameters for Entity Search

Parameter	Significance
noOfHopsToDisplay	It indicates the label of the text box for the number of hops to be displayed initially. The value is the Number of Hops to Display.
additionalEntitiesTextBox	It indicates the label of the text box for additional Customer or Account internal ids for historical summary report. The value is Additional Entity Ids (supports multiple comma-separated Customer or Account entities).
minTransactionAmountTextBox	It indicates the label of the text box for "Minimum transaction Amount". The value is the Minimum transaction amount.
maxTransactionAmountTextBox	It indicates the label of the text box for "Maximum transaction Amount". The value is the Maximum transaction amount.
searchIndexCheckBox	It indicates the label of the check boxes to select the target search entities (Opensearch Indexes). The value is Target search entities (selected targets are used for "Name" and "Address" matching).

4.2 Customize Investigation Toolkit Notebook Template

An admin user can refer to the Investigation Toolkit notebook template with source code to understand and customize the output of each paragraph.

Once satisfied with the customization, an admin user can compile the code which is present in the notebook template to create a jar and then configure it in Compliance Studio to publish the changes for the Investigation Toolkit user.

> **Note:**
>
> For more information on customization reach out to My Oracle Support (MOS).

Investigation Toolkit notebook template with source code is present inside the directory, Investigation Toolkit/Source Code in the Data Studio.

Customizing and publishing changes for Investigation Toolkit users involves the following process:

1. Customize Notebook Template
2. Prepare Java Archive (jar)
3. Update Investigation Toolkit Jar in the Compliance Studio
4. Update Investigation Toolkit Notebook Template (without source code)
5. Add/Update Case-Notebook Template Mapping

4.2.1 Customize Notebook Template

An admin user can refer to the Investigation Toolkit notebook template with source code to understand and customize the output of each paragraph.

The Investigation Toolkit notebook template (with source code) has complete java code in the "Entity Summary Risk Report" paragraph of the ECM Case Narrative notebook template or "Click to Start Investigation" paragraph in the ECM Integration L1 or Special Investigation notebook template. The code has multiple java classes for different entities. An admin user can go through the code to understand the implementation of each paragraph. The changes may be simple or complex based on the nature of customization. In this section, we will discuss a few common customizations.

An admin user who wants to customize the notebook template should have experience with the following:

- Java
- SQL
- PGQL (required for graph-based analysis)

If customizations are complex, we recommend to setup IDE and then do the customization. For more information, see the Setup an Integrated Development Environment section.

Customize Entity Summary Risk Report (Narrative)

Entity Summary Risk Report is also referred to as Narrative and is generated in two step process. We collect all the information first and then generate the narrative. This section discusses the following scenarios:

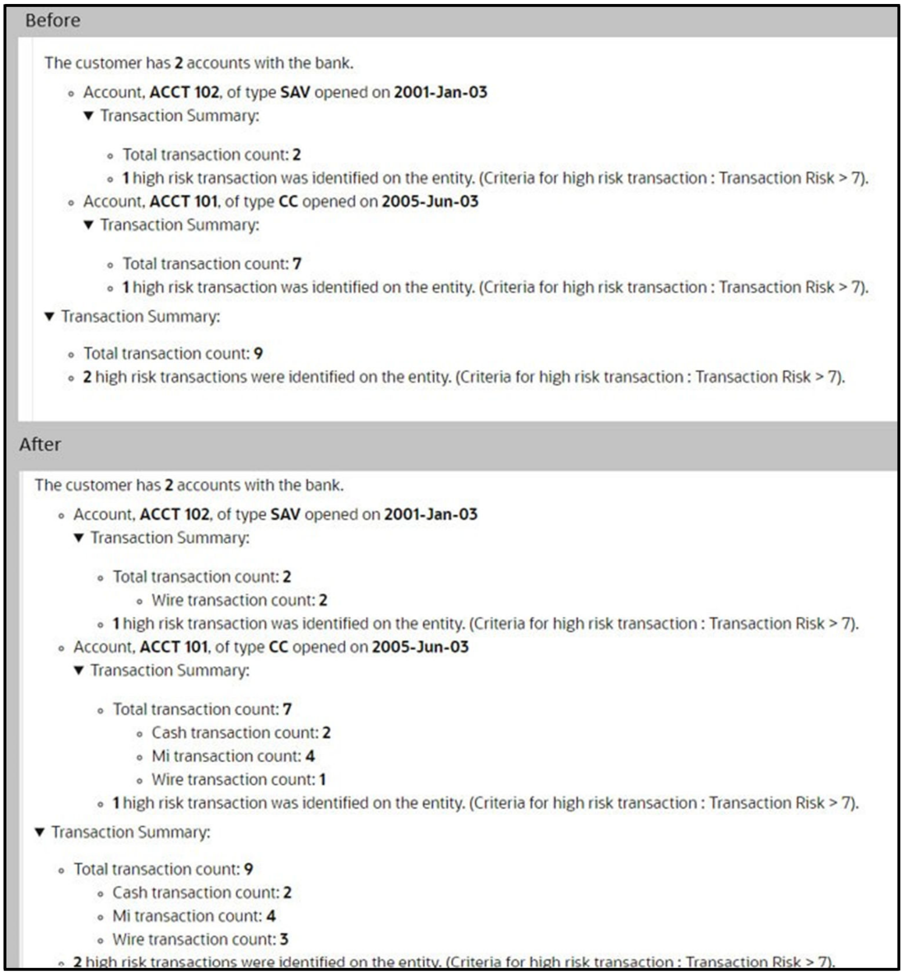
- Customer Transaction Summary should show transaction type wise distribution
- Additional Attributes in Account Summary

Customer Transaction Summary should show transaction type wise distribution

In this example, in the pre-configured narrative, you want to see the transaction type wise count for each account-wise Customer's transaction summary.

To update the pre-configured Investigation Toolkit notebook template, enable the flag to show transaction breakup in the `SummaryGenerator#getAcctWiseDetail()` method as given below.

```
// Replace below line
getTransactionDetails(detail.transactionDetail, reportStringBuilder,
false);
// with below lines
getTransactionDetails(detail.transactionDetail, reportStringBuilder,
true);
```



Before

The customer has **2** accounts with the bank.

- Account, **ACCT 102**, of type **SAV** opened on **2001-Jan-03**
  - ▼ Transaction Summary:
    - Total transaction count: **2**
    - **1** high risk transaction was identified on the entity. (Criteria for high risk transaction : Transaction Risk > 7).
- Account, **ACCT 101**, of type **CC** opened on **2005-Jun-03**
  - ▼ Transaction Summary:
    - Total transaction count: **7**
    - **1** high risk transaction was identified on the entity. (Criteria for high risk transaction : Transaction Risk > 7).

▼ Transaction Summary:

- Total transaction count: **9**
- **2** high risk transactions were identified on the entity. (Criteria for high risk transaction : Transaction Risk > 7).

After

The customer has **2** accounts with the bank.

- Account, **ACCT 102**, of type **SAV** opened on **2001-Jan-03**
  - ▼ Transaction Summary:
    - Total transaction count: **2**
      - Wire transaction count: **2**
    - **1** high risk transaction was identified on the entity. (Criteria for high risk transaction : Transaction Risk > 7).
- Account, **ACCT 101**, of type **CC** opened on **2005-Jun-03**
  - ▼ Transaction Summary:
    - Total transaction count: **7**
      - Cash transaction count: **2**
      - Mi transaction count: **4**
      - Wire transaction count: **1**
    - **1** high risk transaction was identified on the entity. (Criteria for high risk transaction : Transaction Risk > 7).

▼ Transaction Summary:

- Total transaction count: **9**
  - Cash transaction count: **2**
  - Mi transaction count: **4**
  - Wire transaction count: **3**
- **2** high risk transactions were identified on the entity. (Criteria for high risk transaction : Transaction Risk > 7).

Additional Attributes in Account Summary

This example shows the account opening method in the account summary. To update the pre-configured Investigation Toolkit notebook template, follow these steps:

1. Check if the attribute is defined in the graph definition. Since the attribute **account opening method** is not defined in the Account node provider, update the graph pipeline to add the property. For more information, see the *Graphs* section in the *OFS Compliance Studio User Guide*.
   Let's say it was added as an attribute, **Opening Method**.
2. Query Update: Update the query for information collection.
   - **PGQL Query**: Modify the query in the `GraphPgqlQueries#getAccountDetails()method` to add the attribute Opening Method as shown below.

     ```
     public String getAccountDetails(
     Set<String> nodeIds, PgxGraph resultGraph, GetInfoFromGraph
     getInfo) {
     if (getInfo.verifyIfNodeProviderExist(List.of("Account"),
     resultGraph, false, false)) {
     return "SELECT "
     + "n.Name,"
     + "n.Status,"
     ```

```
+ "n.\"Tax Id\","
+ "n.Address,"
+ "n.\"Entity Type\","
+ "n.City,"
+ "n.Country,"
+ "n.State,"
+ "n.Jurisdiction,"
+ "n.\"Business Domain\","
+ "n.Risk,"
+ "n.D_date,"
+ "n.\"Original Id\","
+ "n.\"Opening Method\""
+ "id(n) "
+ "MATCH (n:Account) where id(n) in ('"
+ String.join("','", nodeIds)
+ "')";
} else {
return null;
}
}
```

- **SQL query:** Modify the query in the `SqlQueries#getAccountDetails()method` to add the attribute Opening Method as shown below.

```
public String getAccountDetails(Set<String> nodeIds, HashSet<String>
tableHashSet) {
StringBuilder queryString = new StringBuilder();
if
(tableHashSet.contains("VW_FCC_ACCOUNT853E4164_0968_4CB6_A6F3_2B49306
14A8B")) {
queryString
.append("SELECT /*+ parallel(")
.append(config.PARALLEL_HINT)
.append(
") */ n.\"Name\", n.\"Status\", n.\"Tax Id\",
n.\"Address\", n.\"Entity Type\", n.\"City\", n")
.append(
".\"Country\", n.\"State\", n.\"Jurisdiction\",
n.\"Business Domain\", n.\"Risk\", n.\"D_date\", n")
.append(
".\"Original Id\", n.\"Id\" , n.\"Label\", n.\"Opening
Method\" FROM vw_fcc_account853e4164_0968_4cb6_a6f3_2b4930614a8b n ")
.append("WHERE n.\"Id\" IN ( '")
.append(String.join("','", nodeIds))
.append("')");
}
return queryString.toString();
}
```

- Update the entity, Account, to store the value: Add a variable for `openingMethod` and respective `getter` and `setter` in class `AccountDetail` as shown below.

```
String openingMethod;
public String getOpeningMethod() {
return openingMethod ;
}
```

```
public void setOpeningMethod(String openingMethod ) {
this.openingMethod = openingMethod ;
}
```

- Setting the value: Modify these methods, `GetInfoFromDb#gatherAccountDetails()` and `GetInfoFromGraph#gatherAccountDetails()` to set the value as shown below respectively:
  - Set the value in

    ```
    GetInfoFromDb#gatherAccountDetails()
    accountDetail.setOriginalId(result.getString(13));
    accountDetail.setOpeningMethod(result.getString(16));
    ```

  - Set the value in

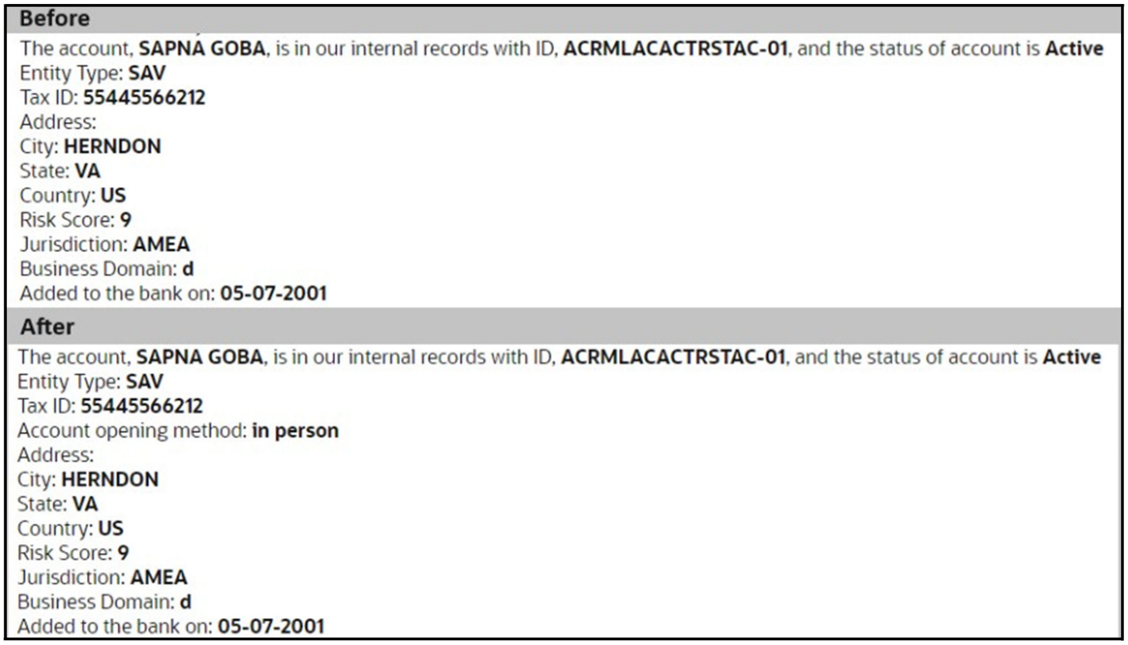
    ```
    GetInfoFromGraph#gatherAccountDetails()
    accountDetail.setOriginalId(result.getString(13));
    accountDetail.setOpeningMethod(result.getString(14));
    ```

- Risk Report update: Modify the risk report in the `SummaryGenerator#getAccountReport()` method by appending the message and the value as shown below.

  ```
  public void getAccountReport(AccountDetail accountDetail, StringBuilder
  reportStringBuilder) {
  if (accountDetail != null) {
  reportStringBuilder
  .append("<details>")
  .append("<summary>Account Summary of <b>")
  .append(accountDetail.getName())
  .append("</b></summary>")
  .append("<p>")
  .append("The account, <b>")
  .append(accountDetail.getName())
  .append("</b>, is in our internal records with ID, <b>")
  .append(accountDetail.getOriginalId())
  .append("</b>, and the status of account ");
  String acctStatus = accountDetail.getStatus();
  reportStringBuilder
  .append(acctStatus.startsWith("code") ? "has <b>" : "is <b>")
  .append(accountDetail.getStatus())
  .append("</b>")
  .append("</br>")
  .append("Entity Type: <b>")
  .append(accountDetail.getEntityType())
  .append("</b>")
  .append("</br>")
  .append("Tax ID: <b>")
  .append(accountDetail.getTaxId())
  .append("</b>")
  .append("</br>")
  .append("Account opening method: <b>")
  .append(accountDetail.getOpeningMethod())
  .append("</br>")
  .append("Address: ")
  ```

```
.append(getList(accountDetail.getAddresses()))
.append("</br>")
.append("City: <b>")
.append(getList(accountDetail.getCities()).append("</b>"))
.append("</br>")
.append("State: <b>")
.append(getList(accountDetail.getStates()).append("</b>"))
.append("</br>")
.append("Country: <b>")
.append(getList(accountDetail.getCountries()).append("</b>"))
.append("</br>")
.append("Risk Score: <b>")
.append(accountDetail.getRiskScore())
.append("</b>")
.append("</br>")
.append("Jurisdiction: <b>")
.append(accountDetail.getJurisdiction())
.append("</b>")
.append("</br>")
.append("Business Domain: <b>")
.append(accountDetail.getBusinessDomain())
.append("</b>")
.append("</br>")
.append("Added to the bank on: <b>")
.append(accountDetail.getAddedDate())
.append("</b>");
getTransactionDetails(accountDetail.transactionDetail,
reportStringBuilder, true);
getRelatedCustSummary(accountDetail, reportStringBuilder);
getComplianceSummary(accountDetail.getEventDetails(),
reportStringBuilder, false);
getRiskFactorsAndRedFlags(accountDetail.getCustomerDetails(),
reportStringBuilder, true);
reportStringBuilder.append("</p>").append("<hr>").append("</
details>");
} else {
ihubUtil.log("Skipping Account report as passed account detail is
null.");
}
}
```

After all the changes are done, value of the account opening method will be shown in the account summary.



Before

The account, **SAPNA GOBA**, is in our internal records with ID, **ACRMLACACTRSTAC-01**, and the status of account is **Active**
Entity Type: **SAV**
Tax ID: **55445566212**
Address:
City: **HERNDON**
State: **VA**
Country: **US**
Risk Score: **9**
Jurisdiction: **AMEA**
Business Domain: **d**
Added to the bank on: **05-07-2001**

After

The account, **SAPNA GOBA**, is in our internal records with ID, **ACRMLACACTRSTAC-01**, and the status of account is **Active**
Entity Type: **SAV**
Tax ID: **55445566212**
Account opening method: **in person**
Address:
City: **HERNDON**
State: **VA**
Country: **US**
Risk Score: **9**
Jurisdiction: **AMEA**
Business Domain: **d**
Added to the bank on: **05-07-2001**

4.2.1.1 Additional Risk Factor and High Risk Entities

This example shows how to add an additional risk factor, which shows the count of high-risk entities, where entities are either Customers or Accounts.

To update, follow these steps:

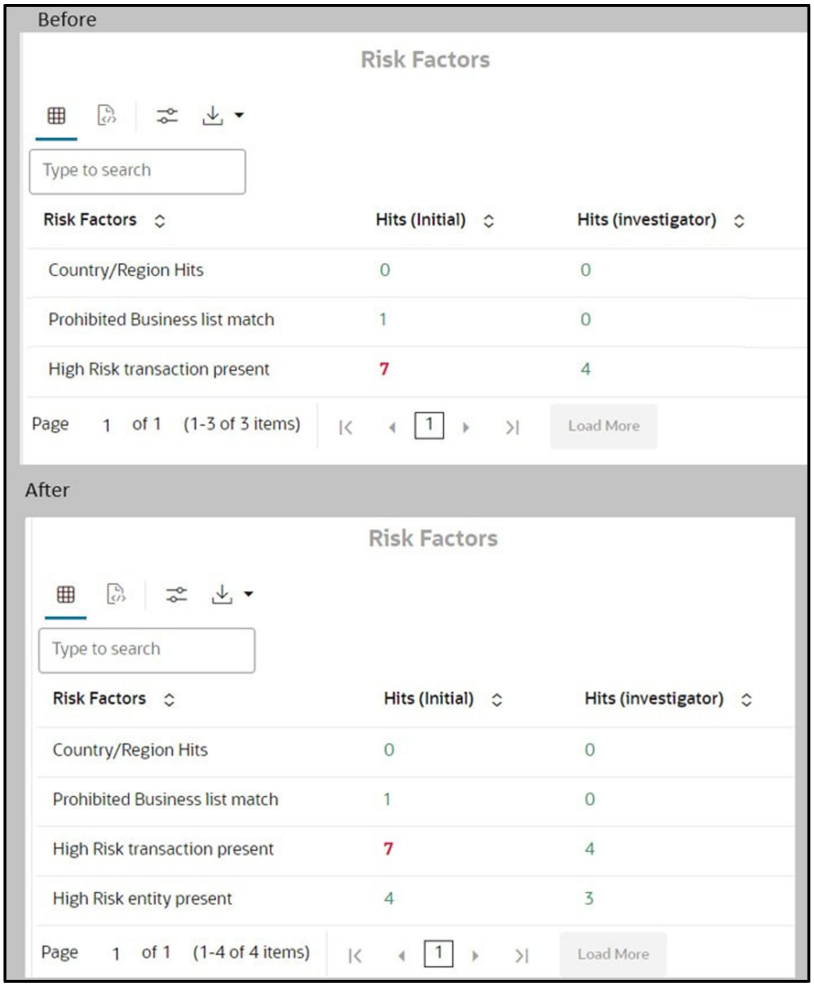
1. Add a query to get the count: Add a method in `GraphPgqlQueries#getHighRiskEntitiesCount()` as given below.

```
public String getHighRiskEntityCount(
        boolean forVisibleGraph,
        long minRiskBoundary,
        PgxGraph resultGraph,
        GetInfoFromGraph getInfo) {
if (getInfo.verifyIfNodeProviderExist(
        List.of("Account", "Customer"), resultGraph, false, false)) {
StringBuilder queryBuilder = new StringBuilder();
queryBuilder
        .append("SELECT ")
        .append("count(n.\"Original Id\")")
        .append(" MATCH (n) ")
        .append(
                "WHERE n.Label in ('Account', 'Customer') ")
        .append("and n.\"Risk\" > ")
        .append(minRiskBoundary);
if (forVisibleGraph) {
queryBuilder.append(" and id(n) in ? ");
}
return queryBuilder.toString();
} else {
 return null;
}
}
```

2. To add a row in Risk Factors, either modify the `IHub#getRiskFactormethod` or add a new method and then call that method inside the `getRiskFactormethod` as given below. Add the following lines at the end of the method to add new rows, before the line `printStatement(report.printTable(true));`

```
log("Fetching high risk entity count.");
        long highRiskEntityCaseGraph =
                getCountBasedOnQuery(
                        false,
                        graphPgqlQueries.getHighRiskEntityCount(
                                true,
                                config.HIGH_RISK_MIN_SCORE_BOUNDARY,
                                resultGraph,
                                (GetInfoFromGraph) getInfo),
                        null);
        long highRiskEntityVisibleGraph =
                getCountBasedOnQuery(
                        true,
                        graphPgqlQueries.getHighRiskEntityCount(
                                true,
                                config.HIGH_RISK_MIN_SCORE_BOUNDARY,
                                resultGraph,
                                GetInfoFromGraph) getInfo),
                        List.of(visibleNodeList));
                report.addRow(
                        "High Risk entity present",
                        formatScore(highRiskEntityCaseGraph),
                        formatScore(highRiskEntityVisibleGraph));
```

After all the changes are done, the **Risk Factors** section will show additional row as shown in the following figure



Before

Risk Factors

Risk Factors	Hits (Initial)	Hits (investigator)
Country/Region Hits	0	0
Prohibited Business list match	1	0
High Risk transaction present	7	4

After

Risk Factors

Risk Factors	Hits (Initial)	Hits (investigator)
Country/Region Hits	0	0
Prohibited Business list match	1	0
High Risk transaction present	7	4
High Risk entity present	4	3

.

4.2.1.2 Additional Red Flag: Customer with more than certain No. of Accounts

This example tells how to add an additional red flag, which shows the number of customers with more than a certain number of accounts.

To update, follow these steps:

1. Configuration for the Number of Accounts: Instead of fixing the value, add it as a dynamic form where Investigation Toolkit users can update if required.
   Update it as given below.

   // Code snippet to add a text box, with default value 3 and then additional validation to validate the user input is a valid integer.

   ```
   String textBoxMessage = "Minimum number of associated account to
   consider it as a red flag";
   String minAccountCountString = ds.textbox(textBoxMessage, "3",
   textBoxMessage).trim();
   int minAccountCount = 0;
   minAccountCount =
   validateTextBoxAndGetIntValue(minAccountCountString, 3,
   textBoxMessage);
   ```

2. Add a query to get the customer IDs with more than certain number of accounts: Add a method in `GraphPgqlQueries#getCustomerCountWithMoreThanCertainAccount()` as given below.

```
public String getCustomerCountWithMoreThanCertainAccount(
PgxGraph resultGraph,
GetInfoFromGraph getInfo,
Integer minAccountCount,
boolean forVisibleGraph) {
if (getInfo.verifyIfNodeProviderExist(
List.of("Customer", "Account"), resultGraph, true, false)
&& getInfo.verifyIfEdgeProviderExists("Cust Has Acct", resultGraph,
false)) {
return "SELECT n.\"Original Id\", count(n.\"Original Id\") as
count_id "
+ " FROM MATCH (n:Customer) - [e] -> (acct: Account) "
+ (forVisibleGraph ? " where id(n) in ?" : "")
+ " group by n.\"Original Id\" "
+ " having count_id > " + minAccountCount;
} else {
return null;
}
}
```

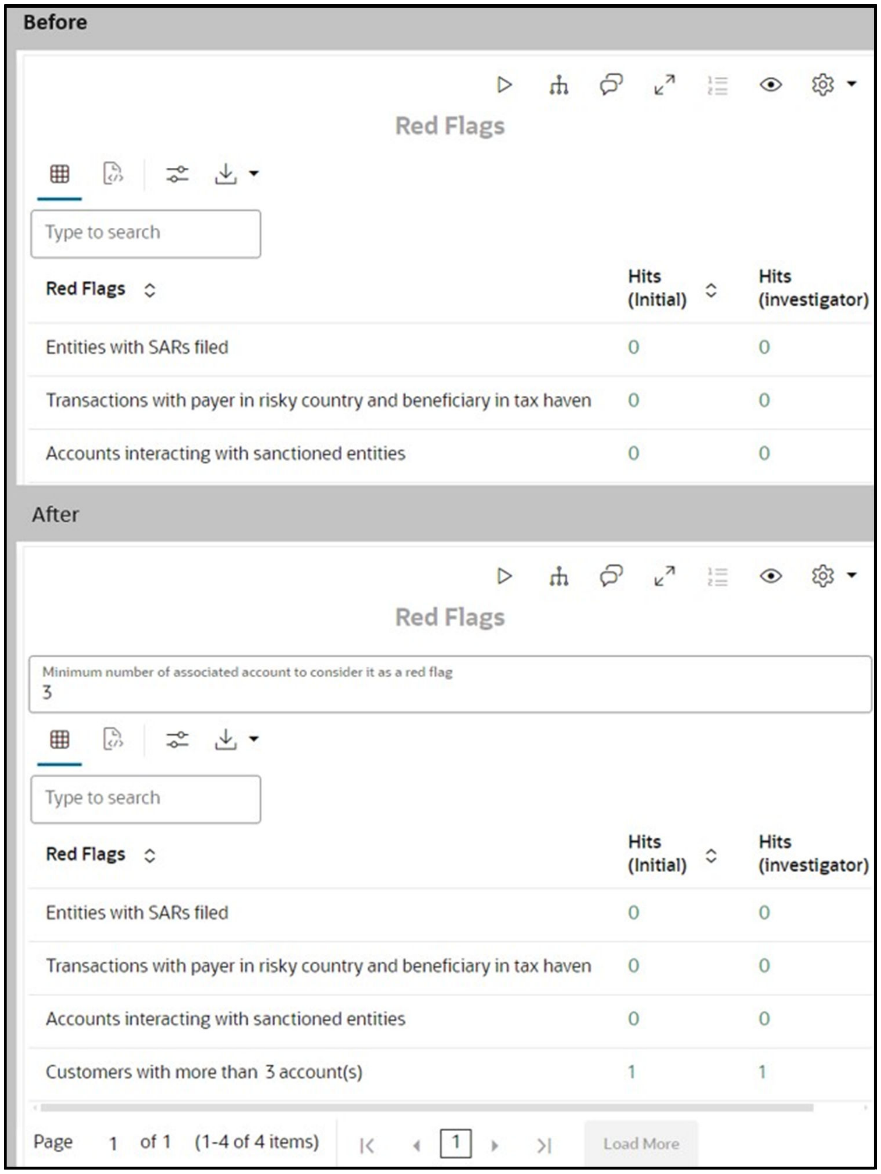
3. To add a row in the Red flag, either modify the `IHub#getRedFlag()` method or add a new method and then call that method inside the `getRedFlag()` method.

```
public void addRedFlag(Table report, List<String> visibleNodeList)
throws DynamicFormsException {
String textBoxMessage = "Minimum number of associated account to
consider it as a red flag";
String minAccountCountString = ds.textbox(textBoxMessage, "3",
textBoxMessage).trim();
int minAccountCount = 0;
minAccountCount =
validateTextBoxAndGetIntValue(minAccountCountString, 3,
textBoxMessage);
log("Fetching entities with more than " + minAccountCount + "
accounts");
long countVisibleGraph = queryVisibleGraph(resultGraph,
graphPgqlQueries.getCustomerCountWithMoreThanCertainAccount(resultGraph,
(GetInfoFromGraph) getInfo,minAccountCount, true),
List.of(visibleNodeList)).getRows().size();
long countCaseGraph = queryCaseGraph(resultGraph,
graphPgqlQueries.getCustomerCountWithMoreThanCertainAccount(resultGraph,
(GetInfoFromGraph) getInfo,minAccountCount,
false)).getRows().size();
report.addRow(
"Customers with more than " + minAccountCount + " account(s)",
formatScore(countCaseGraph), formatScore(countVisibleGraph));
}
public void getRedFlag() {
...
addRedFlag(report, visibleNodeList);
```

// calling the method, `addRedFlag()`, before printing the final statement.

```
printStatement(report.printTable(true));
 }
```

After all the changes are done, the **Red Flag** section will show an additional row as shown below.



Before

Red Flags

Type to search

Red Flags	Hits (Initial)	Hits (investigator)
Entities with SARs filed	0	0
Transactions with payer in risky country and beneficiary in tax haven	0	0
Accounts interacting with sanctioned entities	0	0

After

Red Flags

Minimum number of associated account to consider it as a red flag
3

Type to search

Red Flags	Hits (Initial)	Hits (investigator)
Entities with SARs filed	0	0
Transactions with payer in risky country and beneficiary in tax haven	0	0
Accounts interacting with sanctioned entities	0	0
Customers with more than 3 account(s)	1	1

Page 1 of 1 (1-4 of 4 items)

4.2.1.3 Network Disposition Score and Breakdown

Disposition score should consider only Customers and Accounts and the Breakdown must show an additional column to show contribution.

This example shows how to change the score of disposition score to consider only Customers and Account and the breakdown must show an additional column to contribute toward the final risk score.

To update, follow these steps:

1. Modify the `GraphPgqlQueries#getDispositionScore()` and `GraphPgqlQueries#getDispositionScoreBreakdown()` queries for disposition score and its breakdown, respectively, as shown below:
   - // Modified method

     ```
     public String getDispositionScore(boolean forVisibleGraph) {
     return "SELECT sum(n.Risk * 10)/count(n) as "
     + "network_disposition_score "
     + "FROM MATCH (n) "
     + "where n.Label in ('Customer', 'Account') and n.Risk is not
     null"
     + (forVisibleGraph ? " and id(n) in ?" : "");
     }
     ```

   - // A new method to get the node count of Customer and Account present in the graph/visible graph

     ```
     public String getNodeCount(boolean forVisibleGraph) {
     return "SELECT count(n) as "
     + " node_count "
     + " from match(n) "
     + " where n.Label in ('Customer', 'Account') and n.Risk is not
     null "
     + (forVisibleGraph ? " and id(n) in ?" : "");
     }
     ```

   - // Modified method

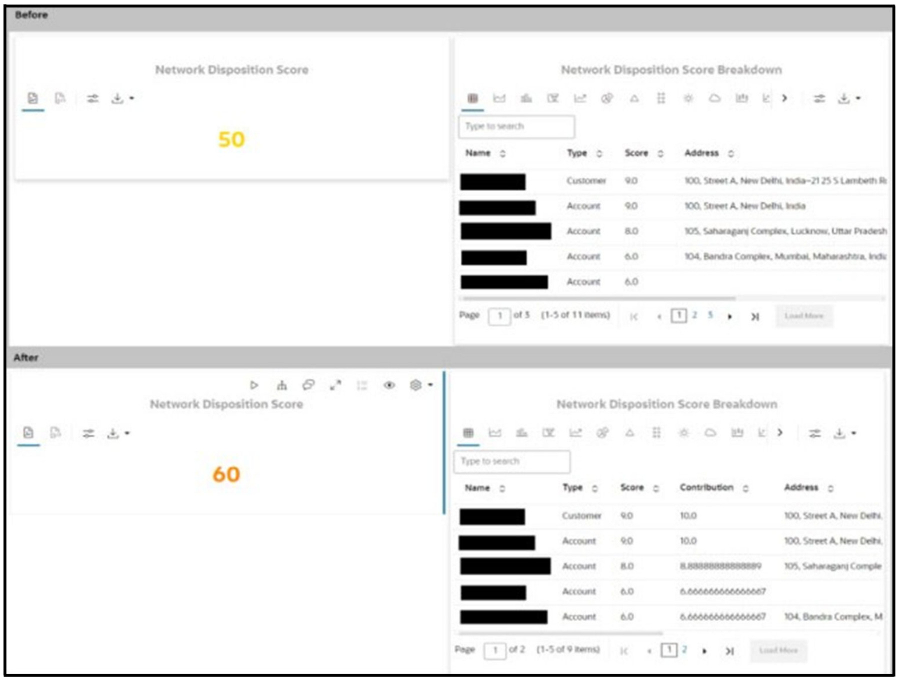
     ```
     public String getDispositionScoreBreakdown(long nodeCount, boolean
     forVisibleGraph) {
     return "SELECT "
     + "n.Name as Name, "
     + "n.Label as Type, "
     + "n.Risk as Score, "
     + "(n.Risk * 10)/" + nodeCount + " as Contribution, "
     + "n.Address as Address, "
     + "n.D_date as \"Opened Date\", "
     + "CASE WHEN n.Label = 'Account' THEN '2' ELSE '0' END as Acct, "
     + "CASE WHEN n.Label = 'Customer' THEN '1' ELSE '0' END as Cust "
     + "FROM MATCH (n) "
     + "where n.Label in ('Customer', 'Account') and n.Risk is not
     null"
     + (forVisibleGraph ? " and id(n) in ? " : "")
     + " order by Score desc";
     }
     ```

2. Update the `IHub#getNetworkDispositionScoreBreakdown()` method to get the count and pass it to the updated `GraphPgqlQueries#getDispositionScoreBreakdown()` method as shown below.

   ```
   public void getNetworkDispositionScoreBreakdown() {
   if (validateIfGraphAnalysisIsEnabled() && resultGraph != null) {
   long nodeCount = getCountBasedOnQuery(true,
   ```

```
graphPgqlQueries.getNodeCount(true), List.of(getVisibleGraphNode()));
String query =
graphPgqlQueries.getDispositionScoreBreakdown(nodeCount,true);
queryVisibleGraphAndPrintTable(resultGraph, query,
List.of(getVisibleGraphNode()));
}
}
```

After all the changes are done, the network disposition score and the breakdown are updated as shown in the following figure.


Before
Network Disposition Score
50
Network Disposition Score Breakdown
Type to search
Page 1 of 3 (1-5 of 11 items)
1 2 3
Load More
After
Network Disposition Score
60
Network Disposition Score Breakdown
Type to search
Page 1 of 2 (1-5 of 9 items)
1 2
Load More

Before

Name	Type	Score	Address
[redacted]	Customer	9.0	100, Street A, New Delhi, India~21 25 S Lambeth R
[redacted]	Account	9.0	100, Street A, New Delhi, India
[redacted]	Account	8.0	105, Saharaganj Complex, Lucknow, Uttar Pradesh
[redacted]	Account	6.0	104, Bandra Complex, Mumbai, Maharashtra, Indi
[redacted]	Account	6.0	

After

Name	Type	Score	Contribution	Address
[redacted]	Customer	9.0	10.0	100, Street A, New Delhi,
[redacted]	Account	9.0	10.0	100, Street A, New Delhi,
[redacted]	Account	8.0	8.88888888888889	105, Saharaganj Comple
[redacted]	Account	6.0	6.666666666666667	
[redacted]	Account	6.0	6.666666666666667	104, Bandra Complex, M

4.2.2 Prepare Java Archive (jar)

The code must be complied as a java archive (jar) to publish the changes after customization.

Setup an Integrated Development Environment

> **Note:**
>
> An admin user can use the java principle to extend the default classes and override or add additional methods as required. This will reduce the effort for re-applying the customization on future upgrades.

To setup an Integrated Development Environment (IDE) to compile, follow these steps:

1. Download and Install JDK 11 and your choice of IDE with Java Support.
2. Download the jars from `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmghome/mmg-studio/interpreter-server/pgx-interpreter-*/lib` and`<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-studio/interpreter-server/pgx-interpreter-*/extralibs` directories into your local directory.

3. Add these jars as default jars (default class path of JDK) in the IDE.
4. Copy the code from the notebook template and create the respective java class in IDE.

Create the Java Archive

As per your IDE, run the respective command to create a jar.

4.2.3 Update Investigation Toolkit Jar in the Compliance Studio

To update the complied jar, follow these steps:

1. Copy the compiled jar and paste it in the following directories:

   ```
   <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-studio/
   interpreter-server/pgx-interpreter-*/extralibs
   <COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-studio/
   interpreterserver/
   pgx-interpreter-*/extralibs
   ```

   > **Note:**
   >
   > Take a backup of the existing investigation jar into the folder outside of `<COMPLIANCE_STUDIO_INSTALLATION_PATH>` for safekeeping.

2. Restart Compliance Studio.

4.2.4 Update Investigation Toolkit Notebook Template Without Source Code

To update Investigation Toolkit notebook template (without source code), follow these steps:

1. Clone the without source code notebook template and create a new notebook template.
2. Update the code in the notebook template (without source code) in respective paragraphs, if new methods were added to support additional paragraphs or customization.
3. Verify the changes with this notebook template.

4.2.5 Add/Update Case-Notebook Template Mapping

If customization was done in the separate notebook template, then configure this notebook template against required case type and role in **FCC_CM_CTYPE_NB_MAPPING** table in the ECM Atomic Schema. For more information, see the Map Notebook Template and User Groups section.

Once the mapping is updated, the Investigation Toolkit users with role for that case type will see the updated notebook template for case investigation.

5 Configuration for Investigation Flow Notebook Template

Admin users configure the following sections to access the investigation flow notebook template.

5.1 Flow Template Notebook Configuration

This section outlines the configuration steps required to successfully set up and operate the Flow Template Notebook. All administrators must ensure the correct setup of Mandatory Configuration, while Additional Configuration offers advanced customization for auditability, performance, validation, and formatting.

5.1.1 Investigation Flow Template

This section lists the configurations required to enable Investigation Flow Template.

5.1.1.1 Mandatory Configuration

The following table, CS_IH_CONFIG in Studio schema lists the essential parameters that must be configured during setup. These settings are crucial for integrating with Investigation Flow Template Notebook and establishing the necessary data sources for business data, ECM integration, and audit records.

Table 5-1 Mandatory Configurations

Description	Name	Default Value	Comment
FCC UI Narrative URL for accessing investigation details in the FCC web application	FCC_NARRATIVE_UI_URL	https://##FCC_UI_HOST_NAME##:##FCC_UI_PORT_NO##/fcc/ihNarrativeView.jsp	Action Required: Replace ##FCC_UI_HOST_NAME## with the fully qualified domain name (FQDN) of your FCC UI server, and ##FCC_UI_PORT_NO## with the correct port number (default is 7061 unless otherwise set during installation). This ensures users can access narrative views directly from the FCC UI.

Table 5-1   (Cont.) Mandatory Configurations

Description	Name	Default Value	Comment
Datasource for storing Investigation Toolkit data; must reference a dedicated business schema, not the Studio Schema	IH_DATASOURCE	CS	Action Required: Set this value to the name of a business data schema such as ECM Atomic Schema or a newly created Toolkit Schema. Do not use the Studio Schema as it is only for metadata. If you create a new schema, grant it the same privileges as the Studio Schema and register the new database connection in the Oracle wallet. This ensures proper data segregation and secure connectivity.
Datasource for accessing ECM toolkit integration configuration	ECM_DATASOURCE	E_D	Action Required: Enter the datasource name that connects to your ECM toolkit configuration schema. If any changes are made to this schema or its connection parameters, update the Oracle wallet accordingly to maintain secure and successful access to ECM configuration data.
Datasource for storing Flow Template Notebook audit records; should use a dedicated audit schema, not the Studio Schema	auditDatasourceName	CS	Action Required: Set this to the schema where audit records for the Flow Template Notebook will be persisted, such as an ECM Atomic Schema or a new dedicated Toolkit Schema. Avoid using the Studio Schema. If you create a new schema, assign privileges at least equivalent to those of the Studio Schema, and update the Oracle wallet with this new connection information.

Note:

- It is mandatory to review and configure each of the above settings to ensure secure and correct functioning of the Flow Template Notebook.
- The above data source must be created in Compliance Studio and mapped to `CS` production workspace. For more information about how to create and map data source in compliance studio UI, see the Compliance Studio User Guide.

5.1.1.2 Additional Configuration

The parameters in this section allow administrators to enhance, customize, or optimize the notebook’s behavior for their operational environment. These configurations cover attribute handling, validation, audit or process tracking, and user environment defaults.

Note:

(Optional) Review and adjust these settings based on your compliance, audit, UI, and performance requirements.

Sr. No.	Description	Name	Default Value	Comment
Overridable and Additional Attribute Value Handling (Store user-provided overrides and remarks in the IH Data Schema. Use these settings to control value saving behavior.)				
1	Flag to save values for overridable entity attributes	enableSaveOverrideValues	TRUE	Disabling may prevent storage of user input overrides.
2	Flag to save values for additional attributes such as user remarks, risk scores, or flags	enableSaveAdditionalAttrValues	TRUE	Set to FALSE if not tracking any supplementary information.
Restricted Word Validation Settings (Control restricted word validation and handling in user inputs.)				
3	Flag to validate restricted words in override attribute values	enableRestrictedWordValidationInOverride	TRUE	Set to FALSE to skip restricted word checks in overrides.
4	Flag to validate restricted words in additional attribute values	enableRestrictedWordValidationInAdditional	TRUE	Set to FALSE to skip restricted word checks in additional attributes.
5	Flag to treat restricted words in override attributes as errors (otherwise tracked as warnings)	restrictedWordValidationErrorModeInOverride	FALSE	If TRUE, validation failures will result in errors and may block processing.

Sr. No.	Description	Name	Default Value	Comment
6	Flag to treat restricted words in additional attributes as errors (otherwise tracked as warnings)	restrictedWordValidationErrorModeInAdditional	FALSE	If TRUE, validation failures will result in errors and may block processing.
Attribute Formatting and Default Value Controls (Manage delimiters and assign default values when source data is null.)				
7	Delimiter character for splitting multi-valued strings	ATTRIBUTE_DELIMITER	~	Modify only if the default delimiter conflicts with data.
8	Default value if date is null	DATE	01-01-1970	Use a value consistent with your business rules for missing dates.
9	Default date format	DATE_FORMAT	yyyy-MM-dd	Ensure this format matches expectations for data integration and reporting.
10	Default value if time is null	TIME	00:00.0	
11	Default time format	TIME_FORMAT	HH:mm:ss.S	
12	Default value if timestamp is null	DATE_TIME	00:00.0	
13	Default timestamp format	DATE_TIME_FORMAT	yyyy-MM-dd HH:mm:ss.S	
14	Default string value	STRING	Use only if null/ empty string values must be replaced.	
15	Default long value	LONG	0	
16	Default float value	FLOAT	0	
17	Default integer value	INTEGER	0	
18	Default double value	DOUBLE	0	
19	Default boolean value	BOOLEAN	FALSE	
Audit & Process Tracking Configuration (Manage audit and process tracking behavior and storage.)				
20	Maximum records to collect before writing audit or process tracking batches	N_AUDIT_BATCH_SIZE	1000	Adjust based on memory, performance, and system load.
21	Time interval before saving audit or process tracking batches	V_AUDIT_SAVE_INTERVAL	PT20S	ISO-8601 duration string, e.g., PT20S means 20 seconds.
22	Maximum concurrent threads for batch processing	N_AUDIT_MAX_THREAD	4	Increase with caution; higher values may impact database performance.

Sr. No.	Description	Name	Default Value	Comment
23	Maximum retry attempts for batch writes to database	N_AUDIT_MAX_RETRY	3	Higher values may prolong processing time in the event of repeated failures.
24	Flag to log audit records in the log file if unsaved after all retries	F_LOG_UNSAVED_AUDIT_RECORDS	TRUE	Set to TRUE to avoid data loss, but monitor log file growth.
25	Wait time before retrying a failed batch write	V_AUDIT_RETRY_DELAY	PT15S	ISO-8601 duration; adjust based on retry policy.
26	Flag to store attribute values in audit records in the table	saveValueInAudit	FALSE	Recommended FALSE to prevent storing potential PII in audit logs.
27	Flag to track processing of all toolkit processes such as narrative generation and risk evaluation	saveProcessTracking	TRUE	To reduce overhead, set FALSE unless detailed tracking is required.
28	Process tracking detail level for records saved in the audit table (0-5)	process_level	1	Level 0=Minimal, 5=Most granular; recommend minimal in production.
29	Process tracking detail level for records saved in logs (0-5)	log_level	1	Level 0=Minimal, 5=Most granular; increase for diagnostics.
30	Flag to log process tracking records if unsaved after retries	F_LOG_UNSAVED_PROCESS_TRACKING_RECORDS	TRUE	Set to TRUE to retain failure cases for further investigation.
General and Performance Configuration (Control display, concurrency, caching, and environment context.)				
31	Default styling for the narrative iframe	NARRATIVE_IFRAME_STYLE	frameborder="0" style="height: 100vh; width: 100%;"	Adjust to meet UI/UX requirements.
32	Batch size for entity processing during narrative generation	NARRATIVE_BATCH_SIZE	1000	Larger batches may improve performance but increase memory usage.
33	Batch size to save and read values during PDF generation	PDF_BATCH_SIZE	1000	Balance throughput and resource usage.
34	SQL parallelism execution hint	PARALLEL_HINT	8	Match to database and hardware capabilities for best results.

Sr. No.	Description	Name	Default Value	Comment
35	Flag to cache narrative responses on the interpreter side for improved performance	enableNarrativeResponseCache	TRUE	Recommended TRUE for optimal performance; set FALSE to always regenerate.
36	Flag to enable database connection pool	enableConnectionPool	TRUE	Set to FALSE only if connection pooling is managed externally.
37	Feature name for the HTML table generator	HTML_TABLE_FEATURENAME	htmlTableGenerator	Change only if using a custom implementation.
38	Feature name for the DS table generator	DS_TABLE_FEATURENAME	dsTableGenerator	Change only if using a custom implementation.
39	Default INFODOM value used to fetch configuration from MMG	infodom	CS	
40	Default locale value used to fetch configuration from MMG	locale	en_US	Set to your application's localization needs.
41	Workspace identifier value	workspace	CS	
42	Default user identifier value used to fetch configuration from MMG	user	MMGUSER	Change if using a dedicated technical username for configuration fetch.
43	Flag to track changes to original attribute values (if disabled, updates may overwrite prior values during restoration)	enableTracking	TRUE	Keeping TRUE ensures auditability of source value changes.

5.1.1.2.1 Update ECM Atomic Schema Datasource in Toolkit Metadata

If you set ECM_DATASOURCE in the above table to a value other than E_D, follow these steps to ensure all Toolkit Metadata references are updated to the correct datasource for investigation reads.

To update ECM Atomic Schema Datasource:

1. Skip this section if you are using E_D as your ECM_DATASOURCE.
2. If you have set ECM_DATASOURCE to a different datasource name, perform the following updates in the Toolkit Metadata tables:
   - In the table `CS_IH_ENTITY_SQL_QUERY_MAPPING`, update the value of the column `V_DATASRC_NM` from `E_D` to your chosen datasource name for all relevant records.
   - In the table `CS_IH_SQL_DATASOURCE_MAP`, update the value of the column `V_DATASRC_NM` from `E_D` to your chosen datasource name for all relevant records.

This ensures that the Flow Template Notebook references the correct schema when reading data for investigations, preventing unresolved lookups or data access issues.

5.2 Post-Installation Steps for Investigation Toolkit

Follow the steps below to complete the setup and initialize required components.

After installing the Investigation Toolkit, the following post-installation steps must be performed by the administrator to complete the setup and enable all features of Investigation Toolkit.

Prerequisite:
Ensure that you have the correct data source names available in the `CS_IH_CONFIG` table (mandatory configurations). And, these data sources have been mapped with the CS workspace in compliance studio UI.

> **Note:**
>
> Ensure that you have the correct data source names available in the `CS_IH_CONFIG` table (mandatory configurations). And, these data sources have been mapped with the CS workspace in compliance studio UI.

1. **Initialize Audit**

   The audit functionality tracks and logs all user access events within the Investigation Toolkit. Audit details are stored in the `CS_IH_AUDIT_DETAILS` table.

   Table 5-2 CS_IH_AUDIT_DETAILS

V_CASE_ID	V_USR_NM	V_ACTN	V_PRCS_NM	T_EXEC_TM	V_MSG
CA101	DSADMIN	EXECUTE	Override	22-APR-24 09.19.26.5240 00000 PM	

   To create the audit table:

   a. Navigate to the following path `##CS_INSTALLATION_PATH##/OFS_COMPLIANCE_STUDIO/deployed/mmg-home/mmg-load-to-graph/graph-service/utility/bin` and execute the following shell script:

      ```
      ./InitializeIhAudit.sh --datasource <DATASOURCE_NAME>
      ```

      > **Note:**
      >
      > Ensure the <DATASOURCE_NAME> argument matches the data source name stored with the key `auditDatasourceName` in the `CS_IH_CONFIG` table.

   b. The audit table will be created in the specified data source. Another table by the name CS_IH_PROCESS_LOG will be initialized in the same data source which keep track of all the process logs. This will be initialized while running the `InitializeIhAudit.sh` script

> **Note:**
>
> The following tables `CS_IH_AUDIT_DETAILS` and `CS_IH_PROCESS_LOG` are created in the schema mapped with the specified data source provided as argument. The `CS_IH_PROCESS_LOG` table is used to record all process-related logs.

2. **Configure Investigation Hub (IH) Data Schema**

   This is used for saving User input while Case Investigation and tracking change. The IH Data Schema stores values for overridable and additional user-defined attributes. Data related to overridden or updated attributes is saved in the tables `CS_IH_UPDTD_ENTITY_ATTR_VAL` and `CS_IH_ENTITY_ADDITIONAL_ATTR_VAL`. The original values from previous execution are saved in the `V_ORIGINAL_ATTR_VAL` column of `CS_IH_UPDTD_ENTITY_ATTR_VAL` table.
   This table saves the overriden attribute values.

Table 5-3 CS_IH_UPDTD_ENTITY_ATTR_VAL

V_CASE_ID	V_USER NAME	V_ENTITY_PROVIDER	V_ENTITY_ID	V_ATTRIBUTE_NAME	V_ATTRIBUTE_VALUE	V_ORIGINAL_ATTR_VAL	D_TIME STAMP
CA121	User A	FocalEntity	CUST101	Alias	Shyam ~ Krishna	Syam	03-07-24 1:59:33.844 PM

This table saves the additional attribute values.

Table 5-4 CS_IH_ENTITY_ADDITIONAL_ATTR_VAL

V_CASE_ID	V_USER NAME	V_ENTITY_PROVIDER	V_ENTITY_ID	V_ATTRIBUTE_NAME	V_ATTRIBUTE_VALUE	D_TIME STAMP
CA121	User A	FocalEntity	CUST101	Alias	Shyam ~ Krishna	03-07-24 1:59:33.844 PM

> **Note:**
>
> Only updated attributes are stored in the tables.

To initialize these tables:

- Navigate to the following path `##CS_INSTALLATION_PATH##/OFS_COMPLIANCE_STUDIO/deployed/mmg-home/mmg-load-to-graph/graph-service/utility/bin` and execute the following script:

  ```
  ./ExecuteIhDataSchema.sh --datasource <DATASOURCE_NAME>
  ```

> **Note:**
>
> Use the data source name stored with the key `IH_DATASOURCE` in the `CS_IH_CONFIG` table.

3. **Initialize ECM Data Schema**

   The ECM Data Schema is required for reading source data from ECM atomic schema in Flow notebook template.

   To initialize:

   - Navigate to the following location `##CS_INSTALLATION_PATH##/OFS_COMPLIANCE_STUDIO/deployed/mmg-home/mmg-load-to-graph/graph-service/utility/bin` and execute the following script:

     ```
     ./InitializeEcmDataSchema -d <DATASOURCE_NAME>
     ```

   > **Note:**
   >
   > Use the data source name stored with the key `ECM_DATASOURCE` in the `CS_IH_CONFIG` table.

4. **Initialize Archival**

   Archival helps manages active record count by hiding inactive, redundant or historical records, thereby improving the table performance.

   To set up archival tables and procedures:

   - Navigate to the following location `##CS_INSTALLATION_PATH##/OFS_COMPLIANCE_STUDIO/deployed/mmg-home/mmg-load-to-graph/graph-service/utility/bin` and run the following shell script:

     ```
     ./InitializeIhArchival.sh -d <DATASOURCE_NAME>
     ```

   > **Note:**
   >
   > Update to archival must be initialized in all 3 schemas. For example, in data schema, ECM schema and audit schema. Since the tables are distributed across multiple schemas, this script must be used to initialize objects required for archival in all schema.

   > **Note:**
   >
   > Create a separate data source for archival or use the existing ones from `CS_IH_CONFIG` table.

5. **Connection Pooling**

   Connection pooling is implemented in the Investigation Toolkit to efficiently manage database connections. When multiple users investigate cases simultaneously, connection pooling ensures performance and resource optimization by reusing established connections, thus reducing the overhead associated with frequently creating and closing connections. Investigation toolkit maintains a pool of connections for it's operations.

During installation, the CS_CON_POOL_DETAILS table is created and populated with a DEFAULT entry.

> **Note:**
>
> If connection pool details are not provided for any datasource, the properties for that datasource will default to those of the default datasource.

To configure or update connection pooling for any additional data sources, use the provided shell script. This script will insert or update a record in the `CS_CON_POOL_DETAILS` table for the specified data source.

Path: `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgload-to-graph/graph-service/utility/bin`

Execute the following shell script `./SetConnectionPoolConfigForDatasource.sh -h`. This list down the shell script usage information.

For example: `./SetConnectionPoolConfigForDatasource.sh --username fccuser --datasource-name ECM_datasource --initial-size 25 --max-total 50 --max-idle 35 --min-idle 10 --max-wait-millis 3000 --min-evict-idle-time PT30M --soft-min-evict-idle-time PT8H`

> **Note:**
>
> Use same shell script to update connection pooling details. Restart the compliance studio to reflect updated changes.

Parameters

Table 5-5 Parameters

Parameter	Default Value/ example	Description	Comment
--username	MMGUSER	compliance studio username	
--initial-size (IH_CP_INITIAL_SIZE)	10	The initial number of connections that are created when the pool is started.	
--max-idle (IH_CP_MAX_IDLE)	20	The maximum number of connections that can remain idle in the pool, without extra ones being released, or negative for no limit.	

Table 5-5 (Cont.) Parameters

Parameter	Default Value/ example	Description	Comment
--max-total (IH_CP_MAX_TOTAL)	50	The maximum number of active connections that can be allocated from this pool at the same time, or negative for no limit.	
--max-wait-millis (IH_CP_MAX_WAIT_MILLIS)	3000	The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely.	

--min-evict-idle-time (IH_CP_MIN_EVICTABLE_IDLE_TIME)	PT30M	The minimum amount of time a connection may sit idle in the pool before it is closed and a new connection is created if count of connections is less than IH_CP_MIN_IDLE.	PT30M = 30 minutes
			PT55S = 55 seconds
			PT2H = 2 hours

--min-idle (IH_CP_MIN_IDLE)	10	The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none.	
--soft-min-evict-idle-time (IH_CP_SOFT_MIN_EVICTABLE_IDLE_TIME)	PT8H	The minimum amount of time a connection may sit idle in the pool before it is closed and a new connection is created. Note: Values lesser than IH_CP_MIN_EVICTABLE_IDLE_TIME will close all the idle connection and create connection to match IH_CP_MIN_IDLE	

> **Note:**
>
> Reset cache or restart Compliance Studio to update connection pool details.

Review Connection pooling for External Schema:

Connection pooling is used at multiple places in compliance studio, One such service of our interest is graph service. Connection pooling details for graph service (uses external schema) are present in `##CS_INSTALLATION_PATH##/OFS_COMPLIANCE_STUDIO/bin/config.sh`. These connection pooling settings are used by investigation toolkit, when fetching values while rendering narrative on UI and reading data information for PDF generation.

Table 5-6 Sample External Schema Pooling Parameters

Key	Default Value	Comment
EXT_SCHEMA_ENABLE_CP	TRUE	Enables pooling for external schema connections.
EXT_SCHEMA_CP_SOFT_MIN_EVICTABLE_IDLE_TIME	PT6H	Soft minimum idle time before eviction.
EXT_SCHEMA_CP_MIN_IDLE	2	Minimum idle connections maintained.
EXT_SCHEMA_CP_MIN_EVICTABLE_IDLE_TIME	PT30M	Minimum idle time before eviction.
EXT_SCHEMA_CP_MAX_WAIT_MILLIS	3000	Max wait time (ms) for an available connection.
EXT_SCHEMA_CP_MAX_TOTAL	10	Maximum number of pooled connections.
EXT_SCHEMA_CP_MAX_IDLE	5	Maximum connections allowed idle.
EXT_SCHEMA_CP_INITIAL_SIZE	1	Initial number of connections in the pool.

> **Note:**
>
> For updating the connection pooling configuration for external schema (e.g for graph service), update the value in Compliance Studio's `config.sh` and run update configuration command `compliance-studio.sh -u` from the path `##CS_INSTALLATION_PATH##/OFS_COMPLIANCE_STUDIO/bin`.

6. Import Investigation Flow Template Notebook

   Import the investigation flow template notebook in data studio. For instructions on how to import the notebook, refer the investigation toolkit installation guide.

5.3 Advanced configuration

5.3.1 Managing Restricted Words

The investigation template notebook allows users to provide input for overriding attributes or supplying values for additional attributes. Before saving these inputs, the Restricted Word Manager validates whether any restricted words are present in the input.

Features:

- Configure restricted word validation globally via `CS_IH_CONFIG` table.
- Validation is performed only on user-provided input.
- Define restricted words in tables `cs_ih_constants` or via custom SQL.
- Select error or warning actions if restricted words are detected.

- Customize case sensitivity according to your requirements.

The list of restricted words is defined either in the `cs_ih_constants` table against the key `RS_WORD` in studio schema or is dynamically fetched from another table using an SQL identifier. If any restricted words are detected, the system saves the input but displays a warning or error message to inform the user.

The restricted words can be stored against a key in the `CS_IH_CONSTANT` table in Studio schema.

5.3.1.1 Restricted words validation

> **Note:**
>
> Restricted words validation is done on the user inputs instead of generated narrative to restrict the validation on user input. Since, the narrative is generated by using seeded templates, selection values and the values of attributes, implementer should ensure that seeded template and selection values mustn't have restricted words. The validation will validate usage of restricted words in user input but will skip the values from source system.

Enable restricted word validation for overridable attribute

Restricted word validation for overridable attribute can be enabled by setting the key `enableRestrictedWordValidationInOverride` to `true` in `CS_IH_CONFIG` table. This global configuration will enable restricted word validation for overridable attribute throughout the investigation toolkit notebook.

Enable restricted word validation for additional attributes

Restricted word validation for additional attributes like user remarks can be enabled by setting the key `enableRestrictedWordValidationInAdditional` to `true` in the `CS_IH_CONFIG` table. This global configuration will ensure restricted word validation for all additional attributes within the Investigation Toolkit notebook.

Error or Warning mode for Overridable attributes

You can control the system’s response when restricted words are found in overridable attributes by configuring the error mode in the CS_IH_CONFIG table by setting the key `restrictedWordValidationErrorModeInOverride` value. Set this value to `true` to enforce ERROR mode (which blocks the entry), or to `false` for WARNING mode (which logs a warning but allows the input to be saved).

- When set to true (ERROR mode):
  - The system throws an exception if any restricted word is detected in the input.
  - The value is not saved.
  - An error message is recorded in the log.
  - No audit entry is created, as the update did not occur.
- When set to false (WARNING mode):
  - The system logs a warning but still saves the value.
  - An audit entry is created to record the update.

Error or Warning mode for Additional attributes

For additional attributes, you can control how the system handles restricted words by configuring the error mode in the CS_IH_CONFIG table by setting the `restrictedWordValidationErrorModeInAdditional` value. Set the value to `true` to enforce ERROR mode (which blocks the entry) or to `false` for WARNING mode (which logs a warning but still allows the entry to be saved).

Condition	Description
ERROR	• A consolidated Exception is thrown with restricted word details • An error message is logged in the log file. • The value is not saved in the table. • Audit message is not added as the value wasn't updated.
WARN	• A warning message is logged in the log file. • The value is saved in the table. • Audit message is added as the value was updated.

Case Sensitivity

Note:

Restricted word comparison is **case-insensitive by default**.

5.3.1.2 Examples

Restricted words

SAR, Suspicious, 314(a), 314(b), 311, Hold Open, National Security letter, Subpoena , Disclosure, Disclosed, Disclosing, File, Filed, Filing, Report, Reported, Reporting.

Expected behaviors

Table 5-7 Expected behaviors

Value	Datatype	Restricted words
SAR was reported on the user, as the account was hold opened. The account holder had received letter from National security letter. Categorized as 314(a) and 51314(b) account.	String	SAR, reported, National security letter, 314(a)
893110. 311	Number	311
314(a), undisclosed road, national security block, restricted Nagar~House no 42A, XYZ Street, ABC	Array	314(a)

5.3.2 Caching

Caching is enabled in graph service to improve the performance of execution by caching the metadata like entity details, sql queries, and configuration, etc.

The configuration related to caching is maintained in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-load-to-graph/graph-service/conf/application.yml` directory.

5.3.3 Enable or Disable Caching

By default, caching is enabled in the graph service and you can see the following configuration in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-load-to-graph/graph-service/conf/application.yml` directory.

```
cache:
  enable: true
```

> **Note:**
>
> It is recommended to always enable the cache.

(Optional) To disable caching:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-load-to-graph/graph-service/conf` directory.
2. Open the `application.yml` file and update the configuration as follows.

   ```
   cache:
     enable: false
   ```

3. Restart Graph Service by restarting the Compliance Studio.

5.3.3.1 Reset Cache

The toolkit caches metadata like SQL queries, Entity Structure and attributes, and so on and configuration values like data source name, connection pool details, and so on. To reset the cache follow either ways:

You can reset cache in one of the following ways:

- **Using Shell Script Utility**
  To execute the shell script utility:
  1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/ /deployed/mmg-home/mmg-load-to-graph/graph-service/utility/bin` directory.

2. Execute the following script: `./resetCache.sh -a` OR `./resetCache.sh --all`

   OR

- **Restart Compliance Studio**

5.3.4 Managing Transaction Trends List

The Investigation template notebook allows configuration of transaction trend values, which are used during case analysis and attribution within the investigation notebook. These trends help categorize cases based on observed transactional behaviors, supporting more accurate assessments and actions during investigations.

5.3.4.1 Configuration

Storage Location: Transaction trend values are stored in the `CS_IH_CONFIG` table under the key `IT_TRNS_TRENDS` in studio schema.

Add or Modify existing transaction trend value: To update transaction trend values, add or modify the value associated with the IT_TRNS_TRENDS key in the CS_IH_CONFIG table

5.3.4.2 Usage in Investigation toolkit Notebook

- The transaction trend values stored in `CS_IH_CONFIG` are accessed by the Investigation toolkit and are made available in the investigation template notebook.
- Users analyzing a case can reference these values to attribute cases with one or more relevant transaction trends.
- This enables structured and consistent trend analysis across cases.

5.3.4.3 Example

If the following value is set in `CS_IH_CONSTANTS`:

```
Key: IT_TRNS_TRENDS
Value: ["Round Dollar", "Possible Structuring", "Interpersonal Transfer"]
```

In the notebook:

Users will see ["Round Dollar", "Possible Structuring", "Interpersonal Transfer"] as selectable transaction trends during case attribution.

> **Note:**
>
> - There are no advanced modes or validation settings for transaction trend configuration; simply update the key-value pair in `CS_IH_CONFIG` as needed.
> - Ensure the trend values entered are well-defined and meaningful for your business use case to maximize the effectiveness of trend analysis during investigations.
> - Ensure that there are no restricted words.

5.3.5 Case Category Configuration

Case categories help classify cases in the Investigation toolkit notebook, enabling better organization, filtering, and reporting. The values for case categories are centrally configured and made available in investigation notebooks for consistent case labeling.

5.3.5.1 Overview

Case categories play a vital role in classifying and organizing cases within the Flow Template Notebook. By standardizing case categorization, your investigation team can efficiently filter, analyze, and report on cases across various business, compliance, and operational needs. The case category configuration enables administrators to centrally manage the list of possible categories, ensuring that users label each case consistently during workflow execution.

5.3.5.2 Configuration

- Storage Location:
  Case category values are stored in the `CS_IH_CONSTANTS` table using the key `IT_CASE_CATEGORY`.
- How to Update:
  To add, update, or remove case categories, modify the value associated with the `IT_CASE_CATEGORY` key in the `CS_IH_CONSTANTS` table.

> **Note:**
>
> Periodically review and update the list to match evolving regulatory, compliance, or business requirements.

5.3.5.3 Usage in Investigation Flow Notebook

- The values defined for `IT_CASE_CATEGORY` are automatically retrieved by the Flow Template Notebook when users access or initiate a new case.
- Investigators are presented with these predefined categories as selection options, streamlining the case labeling process.

5.3.5.4 Example

If the following value is set in `CS_IH_CONSTANTS`:

```
Key: IT_CASE_CATEGORY
Value: ["Shell Companies", "Human Trafficking", "Unlawful Internet Gambling"]
```

In the Investigation Notebook:

Users will be able to choose "Shell Companies", "Human Trafficking", "Unlawful Internet Gambling" as the case category when labeling a case.

Note:

- Case category configuration is a simple key-value setup with no additional validation or advanced settings.
- Ensure that the case categories are reviewed and maintained to align with your investigative and reporting needs.

Note:

For more information on customization reach out to My Oracle Support (MOS).

6

ECM Investigation Toolkit Configuration

An Admin user configure the following sections to access the investigation flow notebook template notebook through ECM application.

6.1 Integrating Investigation Toolkit with ECM

Investigation Toolkit 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.

Prerequisites

For more information on the ECM patch, see the **Prerequisites** section in the OFS Investigation Toolkit Installation Guide.

Enable Investigation Toolkit Tab in ECM Case Designer

> **Note:**
>
> If ECM 8.0.7.* version is used; the Investigation Toolkit tab configuration in the ECM Case Designer has to be done manually. To configure manually, see **Adding Optional Entities to the Case Type** section in the OFS ECM Administration And Configuration Guide.

For ECM 8.0.8.* and above versions, the pre-configured ECM patch enables the Investigation Toolkit tab for AMLSURV case types. An admin user can add the tab for other case types by using the Case Designer component in the ECM. For more information, see **Adding Optional Entities to the Case Type** section in the OFS ECM Administration And Configuration Guide.

> **Note:**
>
> Pre-configured Investigation Toolkit Notebook Template may not be applicable to all case types.

6.1.1 Map Notebook Template and User Groups

This section can be used to configure notebook template for specific case and case subtype and specify user groups fr access. An admin user can map the Investigation Toolkit notebook template against a role and case type.

Map additional case types, roles, and respective notebook template ID in the table.

> **Note:**
>
> The configuration of the FCC_CM_STUDIO table is described in the Installation Guide.

Table 6-1 Configuration Table for ECM-Investigation Toolkit Integration

Schema	Table Name	Description
Atomic Schema	FCC_CM_STUDIO	Configuration related to Compliance Studio and ECM Toolkit.
Atomic Schema	FCC_CM_CTYPE_NB_MAPPING	This table stores the mapping between case type and template notebook id.
Atomic Schema	FCC_CM_NB_GROUPS	This table stores the mapping between notebook id and user group.
Atomic Schema	CS_IH_KDD_CASE_STATUS_MAP	This table store mappings for read-only case status.
Atomic Schema	FCC_CM_NB_AND_PDF_TMPLT_MAPPING	This table stores mapping between pdf template Id and notebook id. **Note**: The FCC_CM_NB_AND_PDF_TMPLT_MAPPING table is applicable only to the Investigation Flow Template.
Atomic Schema	FCC_CM_NB_CODE_MAPPING	This table will store the mapping between template notebook, interpreter, case initialization and case update code snippet.

6.1.1.1 Configuring Case Type and Template Notebook Template ID Mapping in FCC_CM_CTYPE_NB_MAPPING Table

This table stores mapping between case type and template notebook template id.

The FCC_CM_CTYPE_NB_MAPPING table contains mapping of template notebook, corresponding case and case subtype.

> **Note:**
>
> This table has undergone structural changes for this release. Hence, if you are upgrading from a previous version, follow the steps mentioned in the `readmeUpgrade.txt` file of the ECM toolkit patch and validate the mapping after migration.

Table 6-2 FCC_CM_CTYPE_NB_MAPPING Table Details

Column Name	Column Description	Default Value/placeholder
V_CASE_TYPE	ECM Case Type. Ex: AML_SURV	##CASE_TYPE##
V_CASE_SUB_TYPE	ECM Case Sub Type. Ex: SURV	##CASE_SUB_TYPE##
V_NOTEBOOK_ID	Notebook template id.	##notebookId##
F_USE_CUSTOM_FUNCTION	If value is set to Y, the template notebook id is fetched from the function, instead of V_NOTEBOOK_ID column.	N
V_CREATED_DATE	Created Date	
V_CREATED_BY	Created BY	
V_UPDATED_BY	Updated BY	
V_UPDATED_DATE	Updated Date	

> **Note:**
>
> The columns **V_CASE_TYPE**, **V_CASE_SUB_TYPE**, and **V_NOTEBOOK_ID** are mandatory and must be configured by the user. The remaining columns are optional, and some have default values assigned. Optional columns should be updated only when necessary.
>
> 1. `V_CASE_TYPE`: Replace the placeholder with the case type for which you want to enable the Investigation Toolkit tab. This corresponds to the `CASE_TYPE_CD` in the `KDD_CASES` table in ECM schema. For example enter the ECM case sub-type as `AML_SURV`.
> 2. `V_CASE_SUB_TYPE`: Replace the placeholder with the case subtype. This corresponds to the `CASE_SUBTYPE_CD` in the `KDD_CASES` table in ECM schema. For example enter the ECM case sub-type as `SURV`.
> 3. `V_NOTEBOOK_ID`: Enter the notebook template ID. For more information, about getting the notebook Id, see the OFS Investigation Toolkit Installation Guide.

The template notebook ID is mapped against case type and case subtype in the `FCC_CM_CTYPE_NB_MAPPING` table. To map a template notebook ID for different case types and case subtypes, add a new entry to the table with the corresponding case type and case subtype values. Here, the case type refers to `CASE_TYPE_CD`, and the case subtype refers to `CASE_SUBTYPE_CD` in the `KDD_CASES` table.

Example:

To illustrate the configuration of the `FCC_CM_CTYPE_NB_MAPPING` table, let's consider an example with two notebook templates:

1. ds1gbNB1 (or NB1)
   - Associated with two case types: `AML_SURV` and `YML_SURV`
   - For `AML_SURV`, the case subtypes are `SURV`, `SURV_2`, and `SURV_3`.
   - For `YML_SURV`, the case subtypes are `YS_A`, `YS_B`, and `YS_C`.
2. ds2pqNB2 (or NB2)

- Associated with one case type: `CASE_TYPE2`.
- For `CASE_TYPE2`, the case subtype is `SUB_CASE_TYPE2`.

The corresponding table entries would look like:

Table 6-3 FCC_CM_CTYPE_NB_MAPPING table

V_CASETYPE	V_CASE_SUB_TYPE	V_NOTEBOOK_ID	F_USE_CUSTOM_FUNCTION	V_CREATED_DATE	V_CREATED_BY	V_UPDATED_BY	V_UPDATED_DATE
AML_SURV	SURV	ds1gbNB1	N	24-MAY-25 12.50.19.000000000 PM	SYS	SYS	24-MAY-25 12.50.19.000000000 PM
AML_SURV	SURV_2	ds1gbNB1	N	SYS	SYS		
AML_SURV	SURV_3	ds1gbNB1	N	SYS	SYS		
YML_SURV	YS_A	ds1gbNB1	N	SYS	SYS		
YML_SURV	YS_B	ds1gbNB1	N	SYS	SYS		
YML_SURV	YS_C	ds1gbNB1	N	SYS	SYS		
CASE_TYPE2	SUB_CASE_TYPE2	ds2pqNB2	N	SYS	SYS		

Note:

- Each case subtype requires an explicit entry in the `FCC_CM_CTYPE_NB_MAPPING` table with the notebook id being used.
- The `V_CASE_TYPE` and `V_CASE_SUB_TYPE` columns must match the corresponding values in the `KDD_CASES` table.
- The `V_NOTEBOOK_ID` column specifies the notebook template ID associated with the case type and subtype.

Customizing Template ID Selection:

In cases where the selection of a template ID depends on custom conditions (e.g., case ID or user ID), you can enable a custom function to determine the template ID.

To determine the template ID:

1. Set the `F_USE_CUSTOM_FUNCTION` flag to `Y` in the `FCC_CM_CTYPE_NB_MAPPING` table.
2. Implement a custom function named `f_cs_ih_get_ds_notebook_id` in the Studio schema. This function should contain the logic to select the appropriate template ID based on your specific requirements.
   By implementing this custom function, you can dynamically determine the template ID for a given case, providing greater flexibility in your workflow.

6.1.1.2 Configuring Notebook Template ID and User Group Mapping in FCC_CM_NB_GROUPS Table

This table stores mapping between notebook template id and user group.

The FCC_CM_NB_GROUPS table maps the groups required for investigating cases.

The following table describes the entities in the FCC_CM_NB_GROUPS tale.

Table 6-4 FCC_CM_NB_GROUPS Table Details

Column Name	Column Description	Default Value/Placeholder
V_NB_ID	Template notebook id. Replace the placeholder to the template notebook id.	##NOTEBOOK_ID##
V_USR_GRP	ECM user group	OOB groups. CMSUPERVISORUG, CMANALYST1UG, CMANALYST2UG

Let's continue with the previous example, where we have two notebook templates: NB1 and NB2. To control access to these notebooks, we will configure the `FCC_CM_NB_GROUPS` table.

Sample Access Requirements:

- NB1: Grant access to user groups `UG1` and `UG2`.
- NB2: Grant access to user groups `UG1`, and `UG3`.

By mapping user groups to notebook templates in the `FCC_CM_NB_GROUPS` table, you can effectively manage access and ensure that the right users have the necessary permissions to work with the corresponding notebooks.

Table 6-5 Mapping user groups to notebook templates

V_NB_ID	V_USR_GRP
NB1	UG1
NB2	UG1
NB1	UG2
NB2	UG3

6.1.1.3 Configuring Read-only Case Status in CS_IH_KDD_CASE_STATUS_MAP Table

This table stores the mapping for read only case status.

This table stores the mapping for read-only case status.

For example all closed cases and cases in review should be marked as read only.

The status table maps the status of all the investigation cases.

This table stores KDD_CASE_STATUS that is closed or should be enabled for READ_ONLY notebook.

Table 6-6   KDD_CASE_STATUS Table Details

Table Entry	Description
IH_CASE_STATUS	IH case status. Accepted value: READ_ONLY
KDD_CASE_STATUS	KDD case status code. OOB case status that are mapped for READ only are CCFSAR, CCM, CCNSAR

Note:

Ensure that the Admin reviews and updates all the read-only case statuses.

6.1.1.4 Configuring PDF Template ID and Notebook ID Mapping in FCC_CM_NB_AND_PDF_TMPLT_MAPPING Table

Note:

This section is applicable only to the Investigation Flow Template.

This table stores mapping between pdf template id and notebook id.

The PDF and Template table maps the template for the PDF document.

The following table describes the entries in the FCC_CM_NB_AND_PDF_TMPLT_MAPPING table.

Table 6-7   FCC_CM_NB_AND_PDF_TMPLT_MAPPING Table Details

Table Entry	Description
V_NOTEBOOK_ID	Notebook id of a notebook
PDF_TEMPLATE_ID	Template Id mapped with notebook

Note:

The default PDF Template ID for Flow template notebook is 1000.

6.1.1.5 Configuring Code Snippet for Notebook in FCC_CM_NB_CODE_MAPPING Table

The code mapping table maps the code to cases.

> **Note:**
>
> The FCC_CM_NB_CODE_MAPPING table is used to customize code snippets for use during various operations.

The following table describes the entries in the FCC_CM_NB_CODE_MAPPING table.

Table 6-8 FCC_CM_NB_CODE_MAPPING Table Details

V_TEMPLATE_NB_ID	Notebook id of template notebook. P.K of the table.
V_INTERPRETER	Interpreter used for this notebook.
V_CASE_INIT_CODE	Case initialization code snippet for the interpreter.
V_UPDATE_CASE_CODE	Case update code snippet for the interpreter.

6.1.2 Authenticate User Access to Investigation Tab in ECM

This section tells how to authenticate users to access the 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, follow these steps:

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" must 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

Additional Configuration

This section provides information about additional configurations for OFS Investigation Toolkit.

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.

The supported interpreters are PGX, PGQL, Python, Markdown, and so on.

For more information, see the **Configure Interpreters** section in the OFS Compliance Studio Administration and Configuration Guide.

Managing Templates

Templates (**FCGM Default Template**) allow you to create a common way of viewing data in Investigation Toolkit and cover both graphs and other visualizations.

For more information, see the **Configuring Templates** section in the OFS Compliance Studio User Guide.

A

Appendix

This section provides additional information for configuration.

A.1 Frequently Asked Questions

You can refer to the Frequently Asked Questions, which are developed with interest to help you resolve some of the Investigation Toolkit Installation and configuration issues.

1. What happens when a case is opened by two different users who have different roles and mappings?
   - If two users have different roles mapped to two different notebook IDs, a case is opened with a different notebook for the two users.
   - If two users have different roles mapped to same notebook IDs, a case is opened with a same notebook for the two users.
   - User with multiple roles where each role is mapped with a different notebook, then the case is opened for the role with the highest precedence.
   - Two users open a case with different roles and different mapped notebooks at different point of time, then both users will see different notebooks for the same case.
2. How do I update mapping while an upgrade or customization is made in the case?
   In case of an upgrade, update notebook ID mappings in the FCC_CM_CTYPE_NB_MAPPING table.

   > **Note:**
   >
   > When the user opens a case which is already opened by another user, then it clones the new notebook ID mapped to the role and opens the cloned notebook for the case.

3. What should I do if ORA_OLDS_SESSION cookie is missing when user login in Compliance Studio?
   To resolve the issue:
   a. Take copy of deployed folder for backup.
   b. Generate private and public key outside deployed folder and place it in the following directories.

      ```
      <COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-studio/conf
      <COMPLIANCE_STUDIO_INSTALLATION_PATH>/batchservice/conf
      <COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-load-to-graph/
      graphservice/conf
      <COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-ui/conf
      ```

   c. Generate SSO token and update in config.sh file. The config.sh file directory is <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin.

- d. Update cookie_domain value in config.sh file to **snlhrprshared2.gbucdsint02lhr.oraclevcn.com**.
- e. Reinstall compliance studio `(./compliance-studio.sh --reinstall from <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin)`
- f. Complete post installation steps as per OFS Compliance Studio Installation Guide.
- g. Verify token in Nextgenemf_config table (if mismatch, then update manually and restart services).

4. What should I do if Compliance Studio - 8127* - ORA_OLDS_SESSION cookie is missing when user login in CS if DNS Alias (Domain) is used instead of the server domain?
   For example: Server name - test.server.oracle.com, DNS Alias name - test.server.dns.alias.oracle.com

   To resolve the issue:

   - a. Take copy of deployed folder for backup.
   - b. Update **cookie_domain** value in config.sh file to **oracle.com**. Since "oracle.com" is common between the server name and dns alias name, this will solve the problem of cookie creation.
   - c. Since DNS Alias name will be used to hit the UI, make sure to change the value of HOSTNAME parameter from 'hostname -f' to "<DNS ALIAS NAME>" in the install.sh file inside path <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin.
     Forexample: export HOSTNAME="test.server.dns.alias.oracle.com"
   - d. Stop the Compliance studio instance.
   - e. Reinstall compliance studio (./compliance-studio.sh --reinstall from <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin.
   - f. Make sure to check the cookie domain after the reinstall in the following directories.

     ```
     <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/deployed/mmg-home/bin/config.sh
     <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/deployed/mmg-home/mmg-studio/bin/config.sh
     <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/deployed/mmg-home/mmg-studio/conf/application.yml
     <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/deployed/mmg-home/mmg-ui/conf/application.properties
     <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/deployed/mmg-home/mmg-ui/bin/config.sh
     ```

   - g. Verify SSO_TOKEN in Nextgenemf_config table. The Compliance Studio schema if the SSO_TOKEN value is not present, please copy it from config.sh file from `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` path.
   - h. Start Compliance Studio.

5. How can we change color of the table cell?
   For html table, you can add template as follows.

   html template

   ```
   <td class="val-##BODY COLUMN##"> ##BODY
             COLUMN##</td>CSS:<div><style>.val-False
   ```

```
{color: red;} .val-True {color:
green;}</style></div>
```

css template must be added in **cs_ih_ext_srvc_summary_css_template** table

and add css_template_id it in **cs_ih_ext_srvc_summary_html_template** table.

6. What should I do if Compliance Studio - 8127* - ECM Investigation Toolkit Integration certificate Issue occurs?
Issue - Certificate issue while accessing the Investigation Toolkit tab after opening a case from ECM.

   There could be a scenario where there is a difference in Java version between the Compliance Studio and the ECM (Application and Web Layer) server. For Ex - In compliance studio server it's JDK11.0.18 and in ECM sever (Both Application and Web Server) its Java 8.

   Solution: In order to resolve this the studio_server.p12 which is created in Compliance studio server has be created which supports Java8 as well. In order to do this below command has to be used during the creation of studio_server.p12 file. "-J-Dkeystore.pkcs12.legacy" parameter should be used in the key tool command.

```
keytool -genkey -alias studio_server
          -keyalg RSA -keystore studio_server.jkskeytool -J-
Dkeystore.pkcs12.legacy
          -importkeystore -srckeystore studio_server.jks -destkeystore
studio_server.p12 -srcalias
          studio_server -srcstoretype jks -deststoretype pkcs12keytool -
exportcert -keystore <Path of
          .p12 file >/<filename>.p12 -storetype PKCS12 -alias <alias> -
file <Path where studiop.cer file
          should be created>/studiop.cerFor example:keytool -exportcert
        -keystore /scratch/fccstudio/CS_8126_Cloned_Patches/
compStudio_15050706/OFS_COMPLIANCE_STUDIO/mmg-home/mmg-studio/conf/
studio_server.p12
          -storetype PKCS12 -alias studio_server -file
        /scratch/fccstudio/CS_8126_Cloned_Patches/compStudio_15050706/
OFS_COMPLIANCE_STUDIO/mmg-home/mmg-studio/conf/studiop.cerkeytool -
importcert -keystore
          <JAVA_HOME>/lib/security/cacerts -storepass changeit -alias
studio_server -file <Path of
          studiop.cer file created from about command>/studiop.cerFor
example:
    keytool -importcert -keystore /scratch/fccstudio/jdk-11.0.22/lib/
security/cacerts
        -storepass changeit -alias studio_server -file /scratch/fccstudio/
CS_8126_Cloned_Patches/compStudio_15050706/OFS_COMPLIANCE_STUDIO/mmg-home/
mmg-studio/conf/studiop.cer
```

   If user wants to delete the certificate from JDK then below command can be used. This could be helpful if user wants to reimport a new certificate in JDK.

```
keytool -delete -noprompt -alias studio_server  -keystore
          "/scratch/fccstudio/jdk-11.0.22/lib/security/cacerts" -storepass
          "changeit"Also, the certificate needs to be imported in the Java
        security in ECM server for both Application server and Web server
as
```

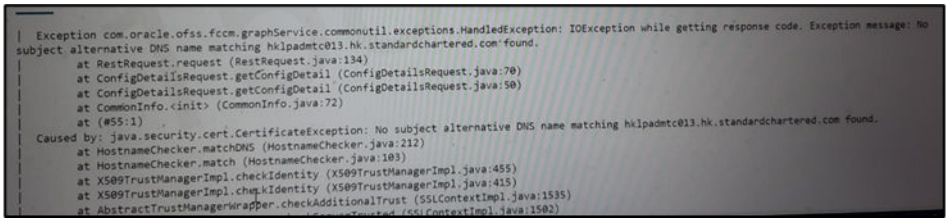
```
        follows.openssl pkcs12 -in studio_server.p12
          -nokeys -out server_cert.pemopenssl pkcs12 -in studio_server.p12
          -nodes -nocerts -out server_key.pem keytool -certreq -keystore
          studio_server.jks -alias studio_server -keyalg RSA -file
        client.csropenssl x509 -req -CA server_cert.pem
          -CAkey server_key.pem -in client.csr -out client_certificate.pem
-days 365
          -CAcreateserialkeytool -import -file
          "/scratch/ofsaauser/BDECM8125P/Studio_Certificates/
studio_1780_cpu_certificates/client_certificate.pem"
          -alias studio_server -keystore "/scratch/ofsaauser/
jdk-11.0.19/lib/security/cacerts"
          -storepass "changeit"
```

If user wants to delete the certificate from JDK then below command can be used. This could be helpful if user wants to reimport a new certificate in JDK.

```
keytool -delete -noprompt -alias
            studio_server  -keystore
          "/scratch/ofsaauser/jdk-11.0.19/lib/security/cacerts" -storepass
          "changeit"
```

7. What should I do if Compliance Studio - 8127* - PGX Interpreter issue occurs?
   This is issue comes up when there is a change from Server name to the DNS ALIAS name and then the reinstall is triggered.

   Figure A-1   PGX Interpreter issue

```
|  Exception com.oracle.ofss.fccm.graphService.commonutil.exceptions.HandledException: IOException while getting response code. Exception message: No
subject alternative DNS name matching hklpadmtc013.hk.standardchartered.com found.
|          at RestRequest.request (RestRequest.java:134)
|          at ConfigDetailsRequest.getConfigDetail (ConfigDetailsRequest.java:70)
|          at ConfigDetailsRequest.getConfigDetail (ConfigDetailsRequest.java:50)
|          at CommonInfo.<init> (CommonInfo.java:72)
|          at (#55:1)
|  Caused by: java.security.cert.CertificateException: No subject alternative DNS name matching hklpadmtc013.hk.standardchartered.com found.
|          at HostnameChecker.matchDNS (HostnameChecker.java:212)
|          at HostnameChecker.match (HostnameChecker.java:103)
|          at X509TrustManagerImpl.checkIdentity (X509TrustManagerImpl.java:455)
|          at X509TrustManagerImpl.checkIdentity (X509TrustManagerImpl.java:415)
|          at AbstractTrustManagerWrapper.checkAdditionalTrust (SSLContextImpl.java:1535)
```

   To resolve this issue:

   a. Navigate to the `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory and open **compliance-studio.sh** file.
   b. Navigate to line number 196 and view the export parameter **PGX_INTERPRETER_OPTS**.
   c. Change server name as DNS alias name in the PGX_INTERPRETER_OPTS parameter.
      For example: `export PGX_INTERPRETER_OPTS="$PGX_INTERPRETER_OPTS - DAPP_BASE_NAME='pgx-interpreter' - Dgraph-service.url=https://<DNS ALIAS NAME>:7059/graph-service`

8. What should I do if ECM Investigation Toolkit Integration issue occurs when Case ID is not passed automatically in the Investigation Toolkit notebook whenever a user opens a case for the first time?
   Issue - This is happening because the user which is logged in Datastudio/Compliance Studio is in lowercase and the same user is logged in ECM in uppercase.

Solution - The user login is case sensitive so the user which is used for login has to be in same case for Data Studio/Compliance Studio and ECM.

A.2 Graph Service REST-API

Get Entity Details Based on Objective ID

Method: GET

URL: `https://<graph-service-url>/ih/entity/details/objectiveId/${objectiveId}Return "payload" contains "GraphMetadata"`

Get all configs

Method: GET

URL: `https://<graph-service-url>/ih/config`

Return "payload" contains "HashMap" of config and its value

Get specific config value

Method: GET

URL: `https://<graph-service-url>/ih/config/paramname/${paramname}`

Return "payload" contains value ("String") of the config param if found, else null

Get all active SQL queries

Method: GET

URL: https://<graph-service-url>/ih/queries/active/

Return "payload" contains "?" details about all the active queries

Get specific active SQL queries

Method: GET

URL: https://<graph-service-url>/ih/queries/active/sqlId/$sqlId

Return "payload" contains "?" details about specific active query based on sql id

Get all active Entity-SQL Mapping

Method: GET

URL: `https://<graph-service-url>/ih/entity/sql-mapping/active/objective/{$objective-id}[HttpHeaders headers]`

Return "payload" contains "?" details about all the active entity sql mapping. It contains datasource details and SQL IDs.

Get specific active Entity-SQL Mapping

Method: GET

URL: `https://<graph-service-url>/ih/entity/sql-mapping/active/objective/{$objective-id}/entity-id/{$entity-id}[HttpHeaders headers]`

Return "payload" contains "?" details about all the active entity sql mapping. It contains datasource details and SQL IDs.

A.3 Cache

Additional REST API related to cache.

Logging cache value

Log all the cache

Method: GET

Path: /ih/cache/log/cache

> **Note:**
>
> The cached values are logged not returned as response.

Log specific cache (based on cache-name)

Method: GET

Path: /ih/cache/log/cache/{cache-name}

For cache name and its description, see **List of cache-name** section.

> **Note:**
>
> The cached values are logged but not returned as response.

List of cache-name

- **ihConfigs**: cache related to config present in the table, CS_IH_CONFIG
- **ihGraphMetadata**: cache related to objective id, entity providers and associated attributes.
- **ihEntitySqlMap**: cache related to entity and sql query mapping.
- **ihSql**: cache related to sql query and associated bind value mapping.

B OFSAA Support

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

B.1 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 My 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 or recently released documents.