Oracle Financial Services Compliance Studio

Architecture Guide

Release 8.1.2.8.0

August 2024

F48788-01

ORACLE
Financial Services

OFS Compliance Studio Architecture Guide

and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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

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

Document Control

Table 1 lists document control of this guide.

Table 1: Document Control

Revision Number	Revision Date	Change Log
8.1.2.8.0	August 2024	There is no feature update and only updated version number (8.1.2.8.0) in the document.

Table of Contents

1 Preface

This preface provides information on the Oracle Financial Services (OFS) Compliance Studio Architecture Guide.

1.1 About this Guide

This document provides the architecture details and the key components of OFS Compliance Studio. In addition, it also describes the application authentication process and various use cases supported in the Compliance Studio.

1.2 Audience

Oracle Financial Services Compliance Studio Architecture Guide is intended for implementation consultants and administrators who can view the high-level architecture of the Compliance Studio solution.

1.3 Related Documents

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

1.4 Conventions

Table 2 explains text conventions used in this guide.

Table 2: Document Conventions

Convention	Description
Italics	Names of books, chapters, and sections as references
Bold	Emphasis and need for attention
Hyperlink	Hyperlink type indicates the links to external websites, and internal document links to sections.

1.5 Abbreviations

Table 3 lists abbreviations used in this document.

Table 3: Abbreviations

Abbreviation	Meaning
OFS	Oracle Financial Services
OFSAAI	Oracle Financial Services Analytical Applications Infrastructure
OHC	Oracle Help Center
MOS	My Oracle Support
OFSAA	Oracle Financial Services Analytical Application

Table 3: Abbreviations

Abbreviation	Meaning
BD	Behavior Detection
FCDM	Financial Crime Data Model
MMG	Model Management and Governance
SSO	Single Sign-On
SSH	Secure Shell
OOB	Out of the Box
PGX	Parallel Graph Analytics
AML	Anti-Money Laundering
ML	Machine Learning
ML4AML	Machine Learning for AML
ORE	Oracle R Enterprise
SAML	Security Assertion Markup Language
AAI	Advanced Analytics Infrastructure
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL or HTTP Secure
SSL	Secure Socket Layer
TLS	Transport Layer Security
ETL	Extract, Transform and Load
SSH	Secure Shell Protocol
UI	User Interface
IDP	Identity Provider
REST	Representational State Transfer
GER	Global Entity Resolution
LDAP	Lightweight Directory Access Protocol
SID	System Identifier
REPL	Read Eval Print Loop

2 OFS Compliance Studio Architecture

This chapter describes architecture, components, and various use cases supported in the Compliance Studio.

2.1 Introduction

OFS Compliance Studio is an advanced analytics application that supercharges anti-financial crime programs for better customer due diligence, transaction monitoring, and investigations by leveraging the latest innovations in artificial intelligence, open-source technologies, and data management. It combines Oracle's Parallel Graph Analytics (PGX), Machine Learning for AML, Entity Resolution, and notebook-based code development and enables Contextual Investigations in one platform with complete and robust model management and governance functionality.

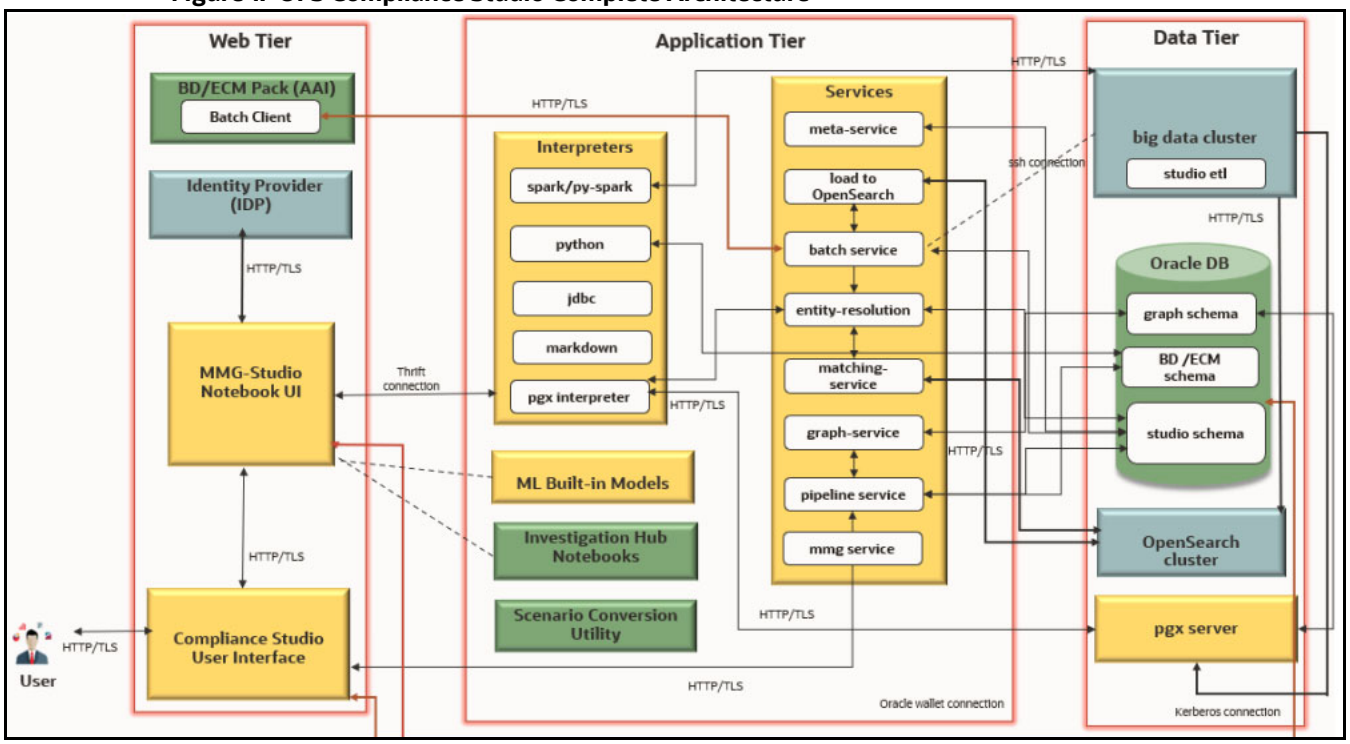
2.2 Architecture Overview

This topic provides details for native and simplify architectures.

2.2.1 Native Architecture

The following diagram exhibits the complete architecture of OFS Compliance Studio.

Figure 1: OFS Compliance Studio Complete Architecture



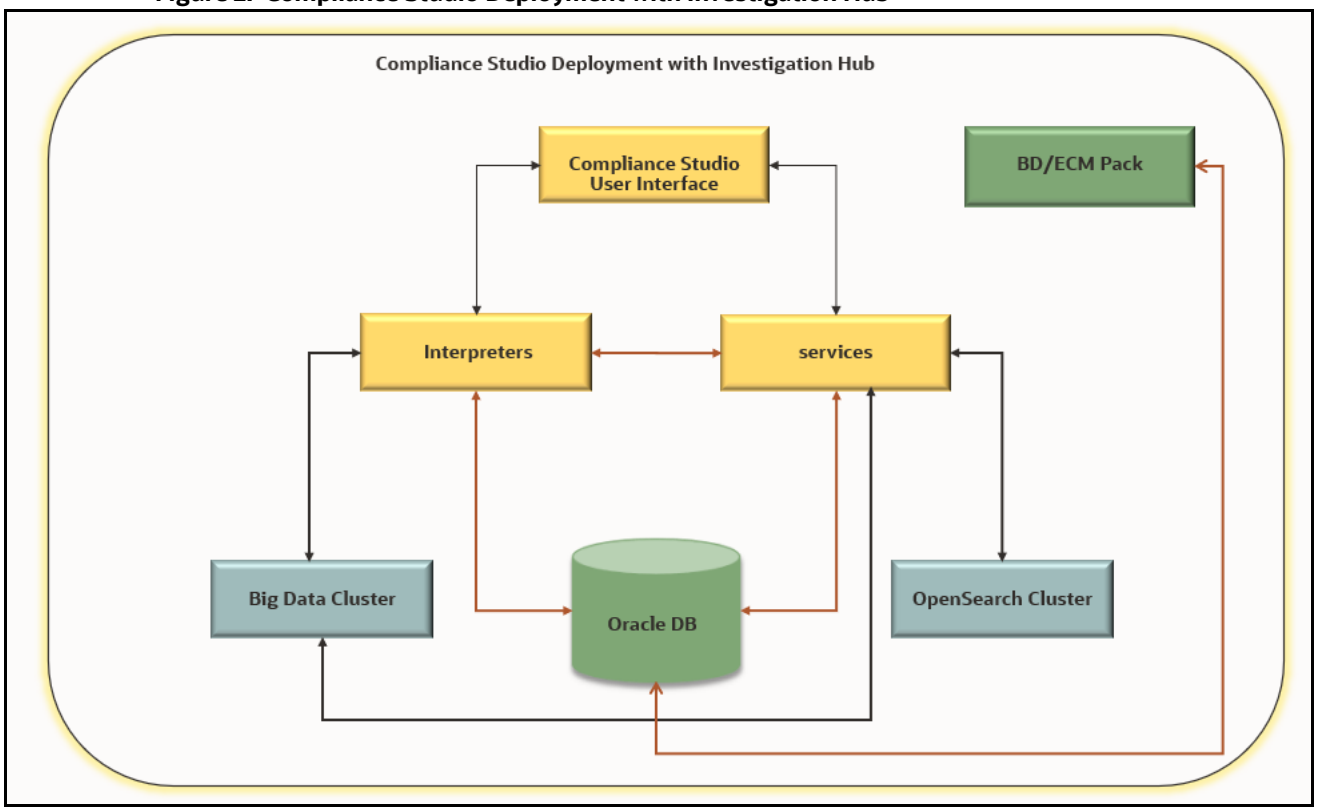
NOTE

- Compliance Studio components (indicated in the yellow color) are deployed on the same server.
- PGX Server can be deployed on the same server or other server based on Graph Sizing requirement.

2.2.2 Simplify Architecture

The following diagram exhibits the Simplified architecture of OFS Compliance Studio.

Figure 2: Compliance Studio Deployment with Investigation Hub



2.3 Components

This topic provides list of key components and third-party components in the Compliance Studio.

2.3.1 Key Components

The following components are bundled in the OFS Compliance Studio installer:

- OFS Compliance Studio Front End Service
  - Compliance Studio UI
  - Notebook Server UI
- OFS Compliance Studio Back End Service
  - Interpreters
  - Services
  - MMG Service
- ML4AML Models
- Python
- Parallel Graph Analytics Server

2.3.2 Other Oracle Components

- Behavior Detection (DB) Pack
- Enterprise Case Management (ECM) Pack
- Investigation Hub
- Scenario Conversion Utility
- Oracle DB

2.3.3 Third-party Components

- OpenSearch Cluster
- Identity Provider (IDP)

2.4 Component Details

Table 4 shows the component details for Compliance Studio.

Table 4: Component Details

Component/Service	Details
OFS Compliance Studio Front End Service	
Compliance Studio UI	You can access the Compliance Studio UI via browser and enter the login credentials along with the language. For valid login credentials, it navigates to the Workspace Summary page.
Notebook Server UI	You can access Notebook Server UI through the Compliance Studio UI.
OFS Compliance Studio Back End Service - Interpreters	
Spark Interpreter	You can connect to a big data cluster and create the models to perform analytics on data present in the Big data clusters.
Python Interpreter	You can create/execute the Python models using this Interpreter. Analytics can be done with any python library. By default, python interpreters are configured with predefined conda environments as follows: • default_8.1.2.8.0 • ml4aml_8.1.2.8.0 • sane_8.1.2.8.0 For more information, see the OFS Compliance Studio Administration and Configuration Guide.

Table 4: Component Details

Component/Service	Details
JDBC Interpreter	You can create/execute the SQL models using this Interpreter. By default, this is connecting to Studio schema. You can connect to any schema by changing the interpreter configuration. For example, BD or ECM schema. **NOTE:** This feature is not recommended approach because it can only be used to connect to a single schema, and all users will have access to that, rather than access being managed per user. In future releases this interpreter will not be enabled by default but instructions will be given to enable if required. **Limitation** • Data source configuration is not dynamic; instead, it is static from the Interpreter Configuration screen. • There is no restriction or secure access of data provided with this interpreter. **Recommendation** Users are recommended to use a python interpreter to get dynamic data source configuration; even data access permission features can also be used with this interpreter.
PGX Interpreter	• **pgx-java**: Java-based Interpreter, you can create/execute Java-based models and interact with the PGX server for graph analytics • **pgql**: SQL is like an interpreter to query on the graph • **pgx-python**: python based Interpreter with a PGX python client embedded in it to query on graph present in the PGX server. • **pgx-algorithm**: Graph toolkit that provides a graph query language and optimized analytics algorithms. For more information, see the website.
OFS Compliance Studio Back End Service	
Meta Service	This service is responsible for setting up metadata related to Compliance Studio in Studio schema.
Load to OpenSearch	This service manages OpenSearch indexes used to resolve the entity based on the matching rules.
Batch Service	This service is responsible for executing some of the batch jobs of Compliance Studio. For example, ETL for graph analytics or entity resolution

Table 4: Component Details

Component/Service	Details
Entity Resolution	It is responsible for resolving entities using matching and merging rules. • **Graph ER**: It creates Similarity Edges between nodes by comparing the attributes of the nodes and identifying where the similarity is significant enough to create an edge so the nodes are linked with the graph model and can be analyzed as a single entity. • **Global Party ER**; It creates a Global Party of similar entities by comparing multiple attributes of entities using matching and merging rules. For more information on merging and matching rules, see OFS Compliance Studio Matching Guide.
Matching Service	It is responsible for scoring in ER based on matching rules. It has the following scoring methods: • Jaro-Winkler • ML-Boosted Name • ML-Boosted Address • Levenshtein • Individual • Name • Entity • Name • Default For more information on merging and matching rules, see the OFS Compliance Studio Matching Guide.
Graph Service	This service is used for managing graphs in Compliance Studio.
Pipeline Service	This service is used for extract transform and load data into target tables.
ML4AML Models	
ML Model Templates	The prepackaged Model templates allow you to perform the following: • Model segmentation (model grouping) • Load and Preview data • User-defined transformation (deriving additional features) • EDA • Feature selections • Model training and • Evaluation • Model Agnostics (Explainability) • On-going validations
Python	Python contains all packages required to execute ML4AML models. For example, scikit-learn pandas
MMG Service	

Table 4: Component Details

Component/Service	Details
MMG Service	This service is used to manage the following functions: • Workspaces and sandbox • Data sources (external, local file, relational, and distributed) • Model complete lifecycle, governance, and execution • Batch and Scheduler services • User roles and accesses • User Provisioning and authentication
Other Oracle Components	
Parallel Graph Analytics Server	Graph analysis lets you reveal latent information that is not directly apparent from fields in your data but is encoded as direct and indirect relationships - metadata - between elements of your data. This connectivity-related information is not apparent to the naked eye but can have tremendous value when uncovered. PGX is a toolkit. For graph analysis, It supports both efficient graph algorithms and fast SQL-like graph pattern matching queries. FCGM is loaded into the PGX server for analytics.
BD PACK	In Compliance Studio, the graph model is based on the BD Pack's FCDM model and ML4AML using the same data model. For more information, see the Behavior Detection Application Pack.
ECM PACK	In Compliance Studio, the graph model is based on the ECM Pack's FCDM model. ECM is also used to correlate events generated via Compliance Studio and for case investigation. For more information, see the Enterprise Case Management Application Pack.
Oracle DB	Compliance Studio stores the metadata in the Oracle DB.
Investigation Hub	OFS Investigation Hub is an application built on Compliance Studio, allowing investigators to view the case and adhoc information within, then creates case narratives and insights, highlight risk factors and red flags meaningful to the investigation, and recommend actions based on graph scoring algorithms. For more information, see the Investigation Hub Application Pack.
Scenario Conversion Utility	This utility converts the Behavior Detection scenario into Compliance Studio scenario.
Third-party Components	
Identity Provider	Identity Provider (IdP or IDP) is required for SSO/SAML authentication.
OpenSearch Cluster	An OpenSearch cluster is a group of nodes that have the same cluster name attribute. As nodes join or leave a cluster, they reorganize to evenly distribute the data across the available nodes. If you are running a single instance of OpenSearch, you have a cluster of one node. It is used for a matching service engine used for Entity Resolution and Similarity Edge for Graph Nodes.

2.5 Communication Details

Table 5 shows the communication details in the Compliance Studio.

Table 5: Communication Details

Connection/Interface	Details
HTTP	Hypertext Transfer Protocol (HTTP) is a communication protocol in the application.
HTTPS	HTTPS (HTTP over SSL or HTTP Secure) uses a Secure Socket Layer (SSL), a secure protocol that works on top of HTTP to provide security. That means SSL encrypted data will be routed using protocols like HTTP for communication.
TLS	Transport Layer Security (TLS) encrypts data for private and sensitive information such as passwords, credit card numbers, and personal correspondence in the application.
Thrift connection	Thrift supports clean abstractions and implementations for data transport, data serialization, and application-level processing.
Oracle Wallet connection	Oracle Wallet is a file that stores database authentication and signing credentials. It allows users to securely access databases without providing credentials to third party software and quickly connects to Oracle products.
SSH connection	Secure Shell Protocol (SSH) hosts multiple channels simultaneously and transfers data in both directions.

2.6 Application Deployment

A separate installer is provided for the On-premise deployment.

For more installation information, you can see the OFS Compliance Studio Installation Guides.

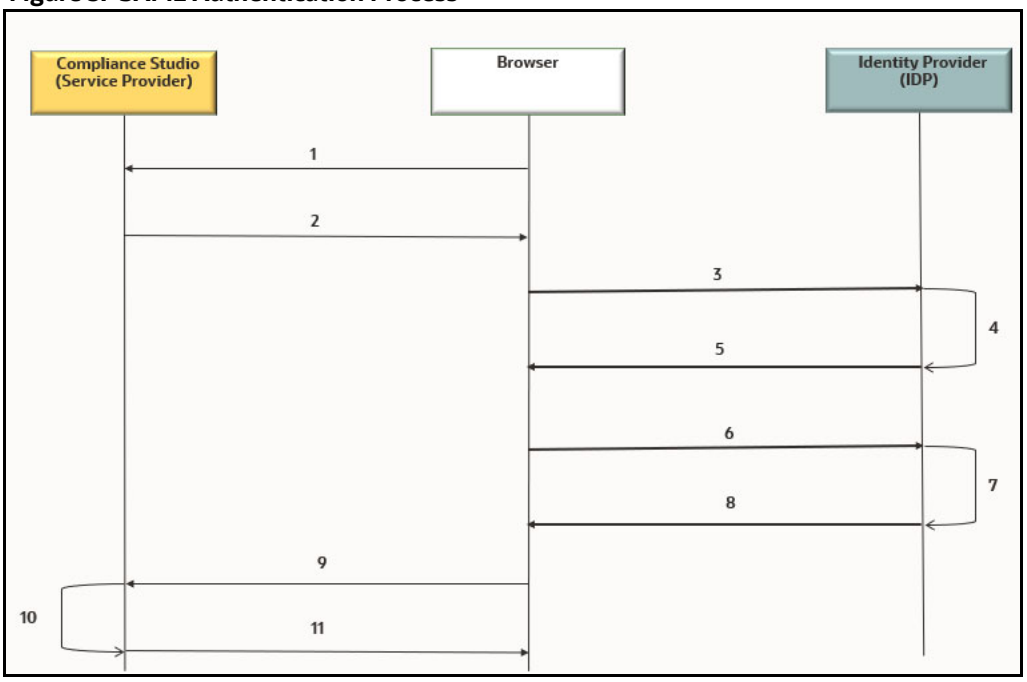
2.7 Application Authentication

This topic provides the authentication details in the Compliance Studio.

2.7.1 SSO/SAML

Single Sign-On (SSO)/Security Assertion Markup Language (SAML) is a type of authentication supporting the OFS Compliance Studio. It is an open standard for exchanging authentication and authorization between the user and the Compliance Studio application, such as logins, authentication state, identifiers, and other relevant attributes.

Figure 3: SAML Authentication Process



The entities are as follows:

- End-User
- OFS Compliance Studio application
- SAML

The SAML authentication process is as follows:

1. A user sends a request to access the OFS Compliance Studio application.
2. The application redirects the request to IDP for authentication with SAML request:
3. The application sends the request to IDP for the SSO login page.
4. IDP validates the SAML request for the login page.
5. IDP sends the response to the user with the SSO login page.
6. The user enters the credentials on the SSO login page.
7. IDP validates the credentials and generates the SAML response.
8. IDP sends the SAML response is as follows:
   - For valid credentials, it sends the response to the application for validating the SAML response.
   - For invalid credentials, it displays an authentication error.
9. It posts SAML response to Assertion Consumer URL for valid credentials.
10. The application verifies the user signature in the SAML response.
11. The application displays the OFS Compliance Studio home page to the user.

2.7.2 OFSAAI

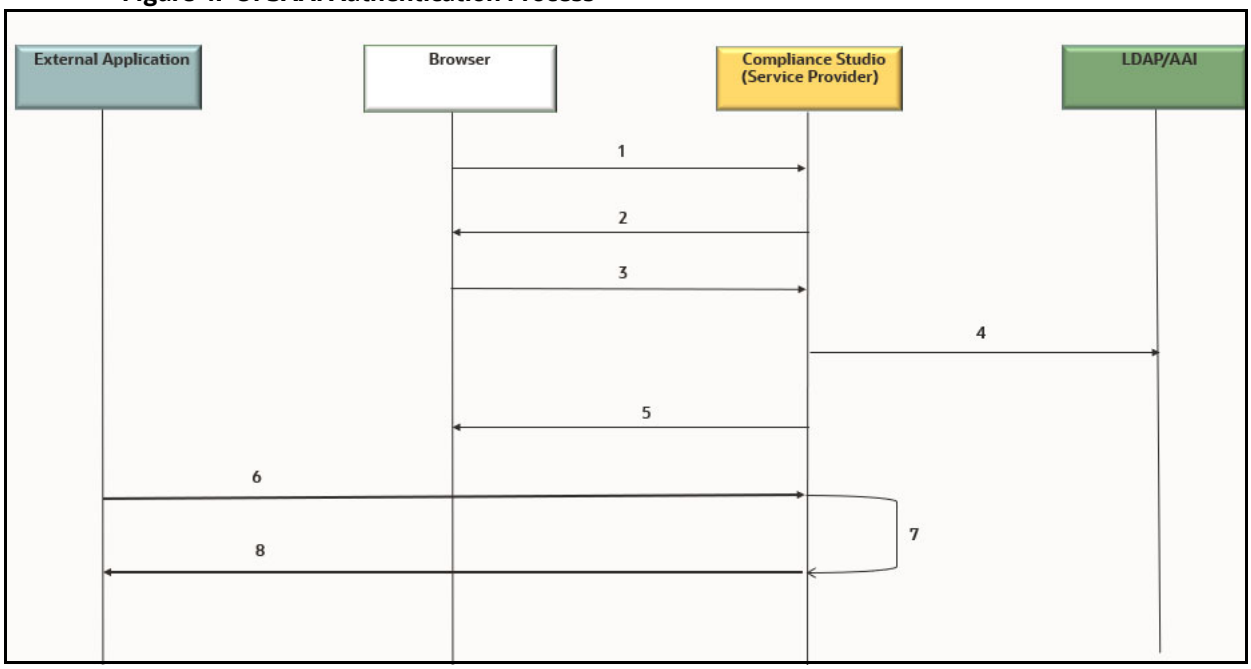
Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) authenticates users using any web browser with a username/password to login into the application. It is also possible to restrict access to content and services based on user attributes or, conversely, make them accessible internationally.

You can authenticate the OFS Compliance Studio with the following:

- Existing OFSAAI
- Install OFSAAI and authenticate

OFSAAI is available with a pre-installed BD Pack or ECM Pack.

Figure 4: OFSAAI Authentication Process



The entities are as follows:

- End-User
- OFS Compliance Studio application
- AAI
- External Application

The AAI authentication process is as follows:

1. A user sends a request to access the OFS Compliance Studio application.
2. The application displays the OFS Compliance Studio application login page:
3. The user enters the credentials on the login page.
4. The application sends the request to AAI for validation.
5. AAI validates the credentials:
    a. For valid credentials, it displays the OFS Compliance Studio home page to the user.
    b. For invalid credentials, it displays an authentication error.

6. The External Application sends the request with Bearer/Basic token to access the application through REST API.
7. The application validates the Authorization Header using Pre-Filters.
8. The application sends the response to the External Application.

   REST API: Representational State Transfer (REST) is a software architectural style that defines a set of constraints to create Web services. Web services that conform to the REST architectural style, called RESTful Web services, provide interoperability between computer systems on the internet.

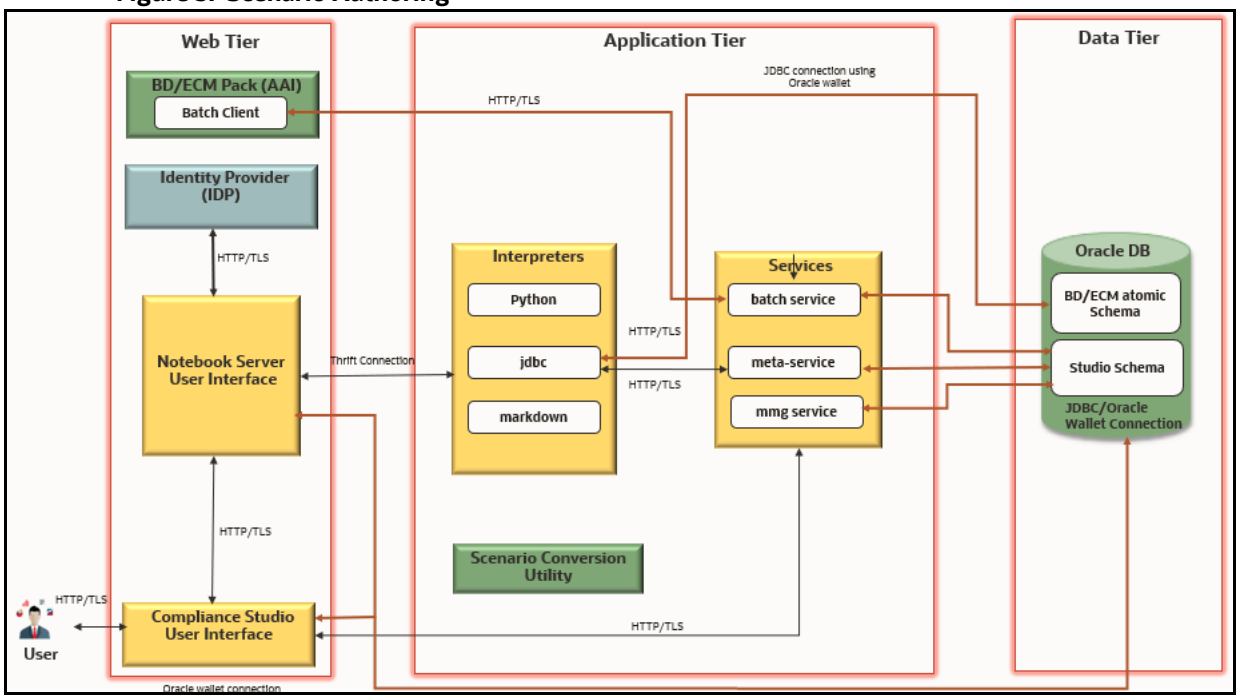
2.8 Use Cases

2.8.1 Scenario Authoring

OFS Compliance Studio supports Polyglot Scenario Authoring to author new scenarios in various languages like SQL, Scala, Python, and R.

It is used with Oracle's Behavior Detection or other FCC product. There are pre-built integrations for Scenario Authoring and creating events, posting them into our Enterprise Case Management system, and further creating cases for investigation. However, Compliance Studio can be used with any financial crime platform for Scenario Authoring.

Figure 5: Scenario Authoring



The following components are involved in this use case:

- OFS Compliance Front End Service
- OFS Compliance Back End Service
- IDP
- ECM/BD Pack
- Oracle DB

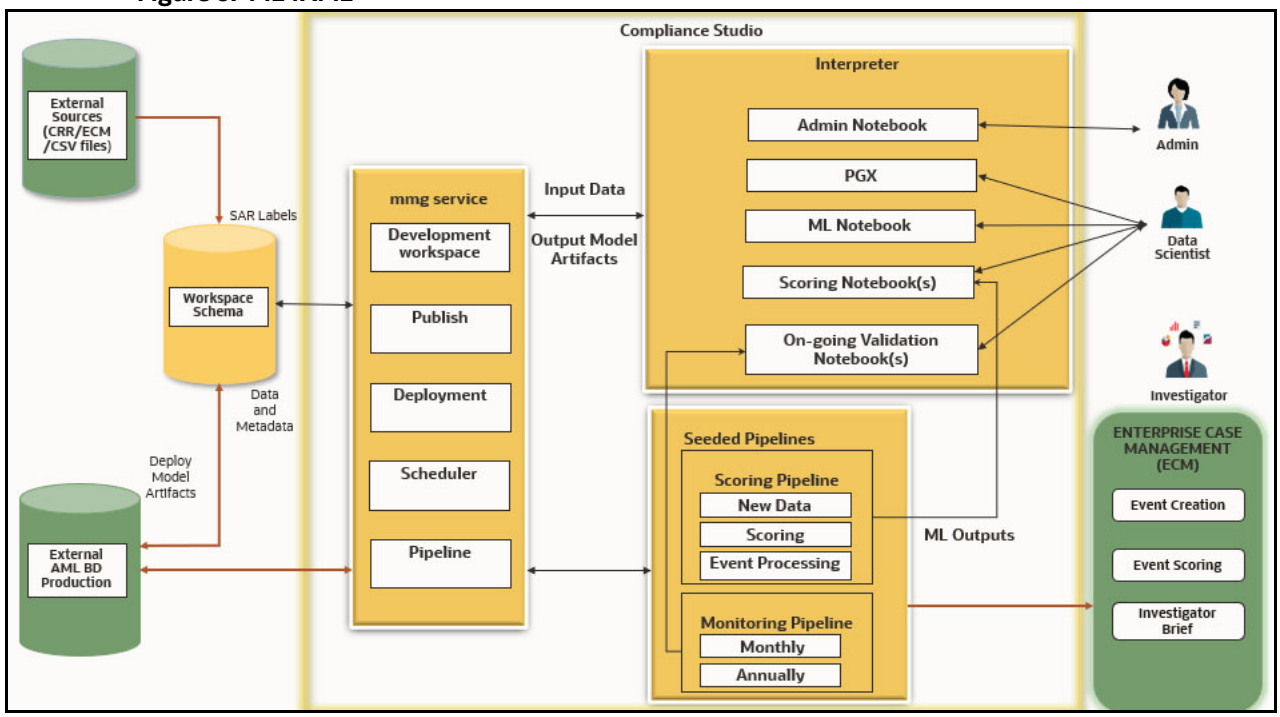
- Scenario Conversion Utility

For more information on each component, see the Component Details section.

2.8.2 Machine Learning for AML

Compliance Studio supports Machine Learning for AML (ML4AML). It is collection of use cases. For more information about use cases, see the OFS Compliance Studio ML4AML Use Case Guide.

Figure 6: ML4AML



The following components are involved in this use case:

- OFS Compliance Front End Service
- OFS Compliance Back End Service
- Database -External sources (ECM/CRR CSV file)/AML BD production
- ECM

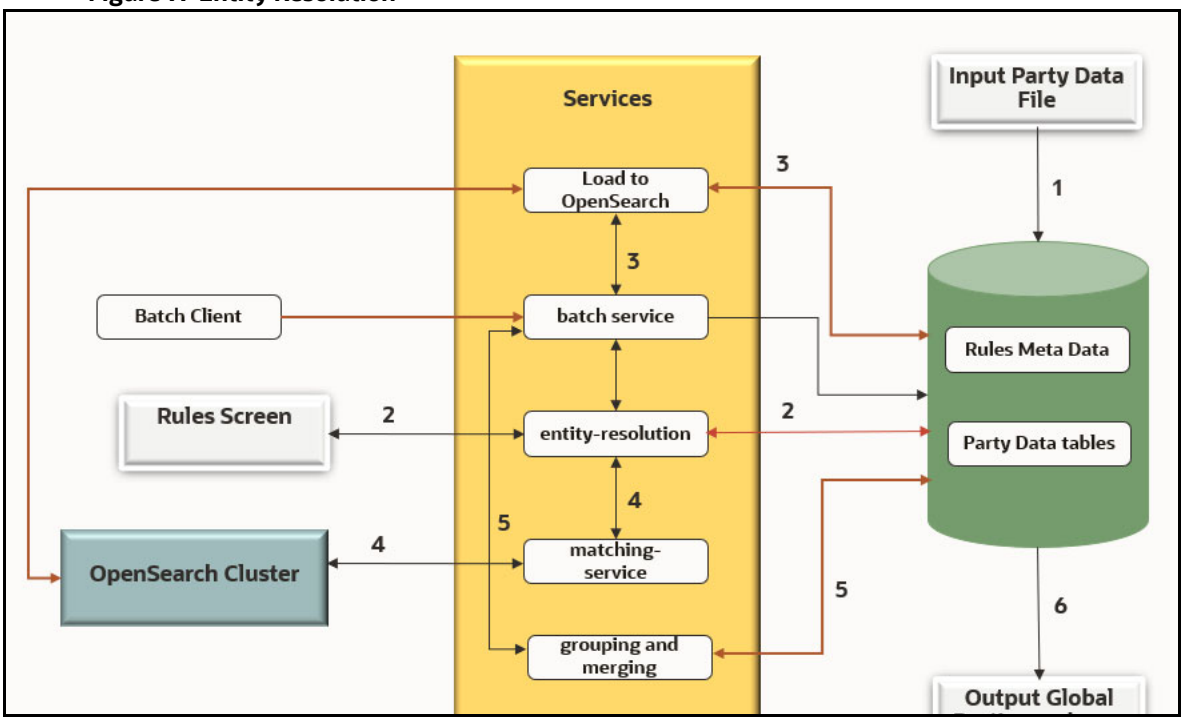
For more information on each component, see the Component Details section.

2.8.3 Entity Resolution

OFS Compliance Studio supports Entity Resolution. It allows firms to break through barriers in their data by gaining single views of their customers and their external entities and have the choice of monitoring them both under one consolidated Global Party.

Entity Resolution leverages ideas and concepts from entity resolution, machine learning, and graph analytics to resolve parties across vast datasets where customers, to avoid detection, may misidentify parties due to segmented business processes or malicious attempts. The new features allow firms to have rich visualization around complex networks and truly gain an entity view across varied datasets. This new clear customer view also can be weaponized within AML detection systems by using this resolved data to drive down false positives and ensure entities are being monitored holistically.

Figure 7: Entity Resolution



The following are reference points for Figure 7:

1. Load input data
2. Input rules
3. Create and load Index
4. Match and generate similarities
5. Group and merge based on similarities
6. Persist Global parties in the file system

The following components are involved in this use case:

- OFS Compliance Back End Service
- ECM/BD Pack
- Oracle DB
- OpenSearch Cluster

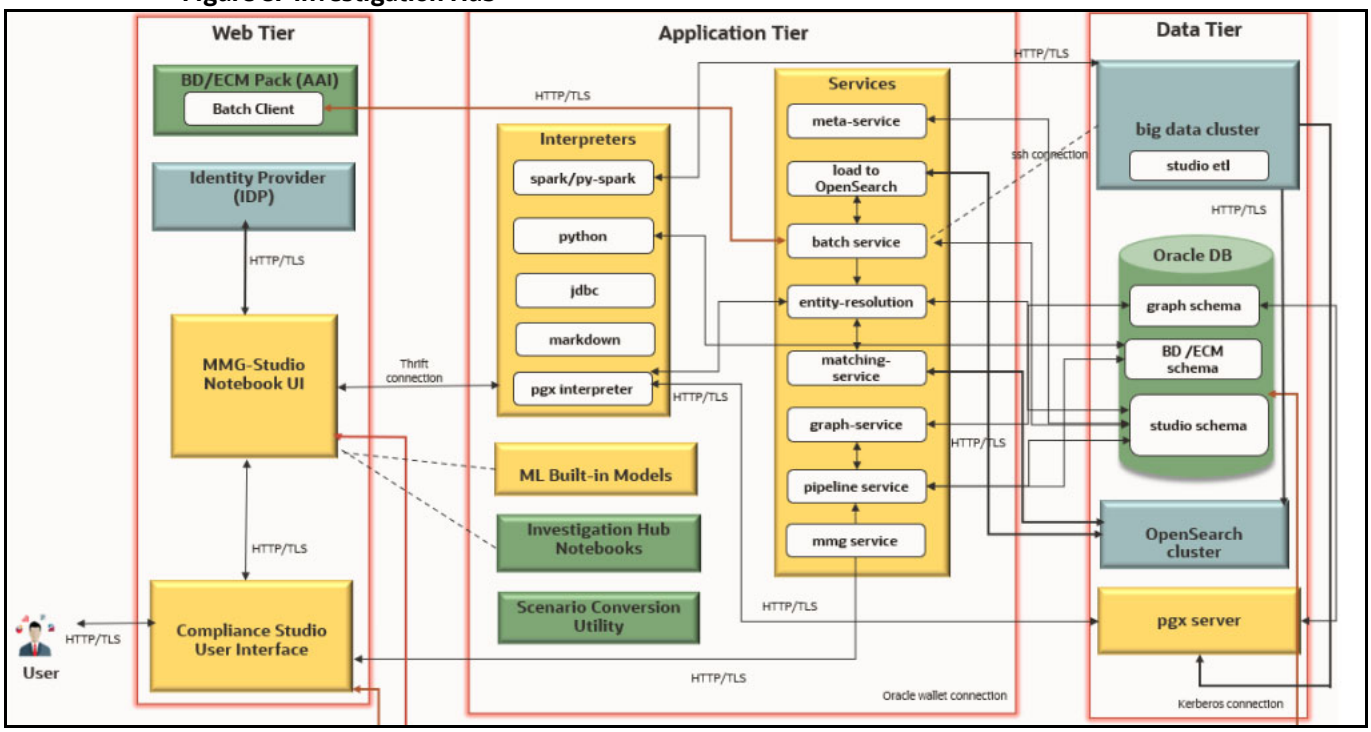
For more information on each component, see the Component Details section.

2.8.4 Investigation Hub

OFS Investigation Hub is an application built on Compliance Studio, allowing investigators to view the case and adhoc information within the FCGM rapidly. The in-built scoring, matching, and correlation engines create meaningful investigation units, and pre-configured red flags and risk factors target investigative efforts effectively. The FCGM on which it is built accelerates investigations by bringing relevant information sources together, preventing the need for the manual collation of information from disparate sources for adhoc investigations. OFS IH automatically generates case narratives and

insights, highlights risk factors and red flags meaningful to the investigation, and recommends actions based on graph scoring algorithms.

Figure 8: Investigation Hub



The following components are involved in this use case:

- OFS Compliance Front End Service
- OFS Compliance Back End Service
- IDP
- ECM/BD Pack
- Oracle DB
- OpenSearch
- PGX
- Investigation Hub
- Scenario Conversion Utility

For more information on each component, see the Component Details section.

OFSAA Support

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

Send Us Your Comments

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

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

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

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