

Oracle® Financial Services

Compliance Studio Installation Guide



Release 8.1.3.0.0
G23338-12
September 2025

ORACLE®

Copyright © 1994, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

Preface

Audience	i
Related Resources	i
Abbreviations	i
Documentation Accessibility	i
Diversity and Inclusion	ii
Conventions	ii
Comments and Suggestions	ii

1 Introduction

2 Installation

2.1 Prerequisites	1
2.1.1 Hardware and Software Requirements	1
2.1.2 Environmental Settings	2
2.1.3 System Configuration	2
2.1.4 Port Numbers for Application	3
2.2 Preparing for Installation	4
2.2.1 Download the Installer Kit	4
2.2.2 Extract the Installer Kit	4
2.3 Pre-Installation	5
2.3.1 Create Tablespace	5
2.3.2 Create Studio Schema	6
2.3.3 Assign Grants for Studio Schema	6
2.3.4 Create Sandbox Schema	7
2.3.5 Assign Grants for Sandbox Schema	8
2.3.6 Create Graph Schema	8
2.3.7 Assign Pre-installation Grants for Graph Schema	9
2.3.8 Create Filestore Directories in the Database Server for Graph	11
2.3.9 Assign Grants to Studio Schema to Access the Filestore Directories	12
2.4 Application User Access and Provisioning	12
2.4.1 Generating the Bearer Token	13

2.4.2	SAML for Authentication and AAI for Authorization	13
2.4.3	SAML for Authentication and SAML for Authorization	15
2.4.4	AAI for Authentication and AAI for Authorization	16
2.5	Database User Access	17
2.5.1	Setup Password Stores with Oracle Wallet	17
2.5.2	Setup the Password Stores for Database User Accounts	17
2.5.3	Verify the Connectivity of the Wallet	20
2.5.4	Create Wallet for ER/ESDF Schema	21
2.5.5	Create Wallet for Graph Schema	21
2.6	Validation Checklist	21
2.7	Installation Activity	22
2.7.1	Place Files in Wallet	22
2.7.2	Generate Compliance Studio Server SSL Configuration	22
2.7.2.1	Generate Self-signed Certificate	22
2.7.2.2	Generate Signed Certificate	23
2.7.3	Import the Certificate to JDK Security	25
2.7.4	Place the Key Store File for Secure Batch Service	25
2.7.5	Configure config.sh File	26
2.7.6	Run the Compliance Studio Installer	43
2.7.6.1	Trigger Installation	43
2.7.6.2	Start Compliance Studio	44
2.7.6.3	Stop Compliance Studio	44
2.7.6.4	Restart Compliance Studio	44
2.8	Post-Installation	44
2.8.1	Verify the Installation	45
2.8.2	Access Compliance Studio Application	45
2.8.2.1	Access Compliance Studio Application when Gateway is Enabled	45
2.8.2.2	Access Compliance Studio when Gateway is Disabled	46
2.8.3	Common for both Entity Resolution and Graph Use Cases	47
2.8.3.1	Copy Public and Private Keys	47
2.8.3.2	Configure the OpenSearch Component	48
2.8.3.3	Place admin.p12 file in the Installation Directories	51
2.8.3.4	Add Synonyms and Stopword files in OpenSearch	51
2.8.3.5	Configure Logstash	52
2.8.3.6	Registering the Conda Environment	52
2.8.3.7	ECM Patch	53
2.8.4	Entity Resolution Use Case	53
2.8.4.1	Create Entity Resolution Schema	53
2.8.4.2	Assign Grants for ER Schema	53
2.8.4.3	Uploading FSDF	54
2.8.4.4	Configure ER Schema Profile	55
2.8.4.5	Run ER Schema in Different Workspaces	55

2.8.5	Graph Use Case	56
2.8.5.1	Importing OOB Graph Definition and related Metadata	56
2.8.5.2	Assign Post-installation Grants for Graph Schema	69
2.8.5.3	Add the Studio Service (SSL) to PGX Configuration	69
2.8.5.4	Generate the graph-keystore.p12 File	70
2.8.5.5	Configure the PGX Service	71
2.8.5.6	Generating Certificate for PGX Server	74

3 Reinstall Compliance Studio with Updated Configuration

4 Frequently Asked Questions (FAQs) and Error Dictionary

4.1	Frequently Asked Questions in Compliance Studio	1
-----	---	---

A Appendix

A.1	Additional Configuration	A-1
A.2	Create Users, Groups, and Mappings	A-4
A.3	Generate an Encrypted Password for OpenSearch	A-6
A.4	Setup Compliance Studio Instance for Cloning the Filesystem	A-6
A.5	Generating Files for SAML Signed Request	A-12
A.6	Access Data Studio UI from Compliance Studio and ECM without Triggering Reinstallation	A-12
A.7	Support for POST and REDIRECT in SAML Request	A-13
A.8	Configuring Custom Ports	A-14
A.8.1	Compliance Studio Configuration	A-14
A.8.2	Custom Port Number Validation for Compliance Studio	A-15
A.8.3	MMG and Data Studio Configuration	A-20
A.8.4	Custom Port Number Validation for MMG and Data Studio Services	A-21
A.8.5	Database Validation	A-30

Document Control

The following table lists document control of this guide.

Table Document Control

Version Number	Revision Date	Change Log
8.1.3.0.0	September 2025	<p>Updated the Java version, Processing server, and PGX server in the Hardware and Software Requirements section.</p> <p>Added the Copy Public and Private Keys section.</p> <p>Removed the generation of the SSO token and public and private keys, as they are now generated automatically by the installer.</p> <p>Added the patch number for v8.1.3.0.0 in the Download the Installer Kit section.</p> <p>Removed the SSO_TOKEN parameter from the Configure config.sh File section.</p> <p>Updated the following parameters in the Configure config.sh File:</p> <p>SAML_IDP_URL, DATASTUDIO_SAML_AUTHZTYPE, DATASTUDIO_SCHEMA_WALLET_ALIAS, DATACATALOG_SERVICE_URL, AAI_AUTHZ_ENABLED, AAI_CLIENT_ID, AAI_CLIENT_SECRET, MMG_MODEL_ENDPOINT_REST_INTERVAL, ENABLE_POLICY_CREATION, and R_PYTHON_HOME.</p>

Preface

This section provides information on the Oracle Financial Services (OFS) Compliance Studio Installation Guide.

Audience

OFS Compliance Studio Installation Guide is intended for System Engineers who are responsible for installing and maintaining the application.

This document assumes that you have experience in installing Enterprise components and basic knowledge about the following:

- UNIX commands
- Database concepts

Related Resources

This section identifies additional resources to the OFS Compliance Studio. You can access additional documents from the [Oracle Help Center](#).

Abbreviations

The following table lists the abbreviations used in this document.

Table 1 Abbreviations

Abbreviation	Meaning
OFS	Oracle Financial Services
OFSA	Oracle Financial Services Analytical Application
BD	Behavior Detection
FCDM	Financial Crime Data Model
ICIJ	International Consortium of Investigative Journalists
IDCS	Oracle Identity Cloud Service
ECM	Enterprise Case Management
SSO	Single Sign-On
SSH	Secure Shell

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which user supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that user 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

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. It enables Contextual Investigations in one platform with complete and robust model management and governance functionality.

Users can perform the following actions:

- Install a new instance of Compliance Studio with OFSAA (Oracle Financial Services Analytical Application). Here, OFSAA is with Behavior Detection (BD) or Enterprise Case Management (ECM).

Note

If you want to install Compliance Studio without OFSAA, contact [My Oracle Support \(MOS\)](#).

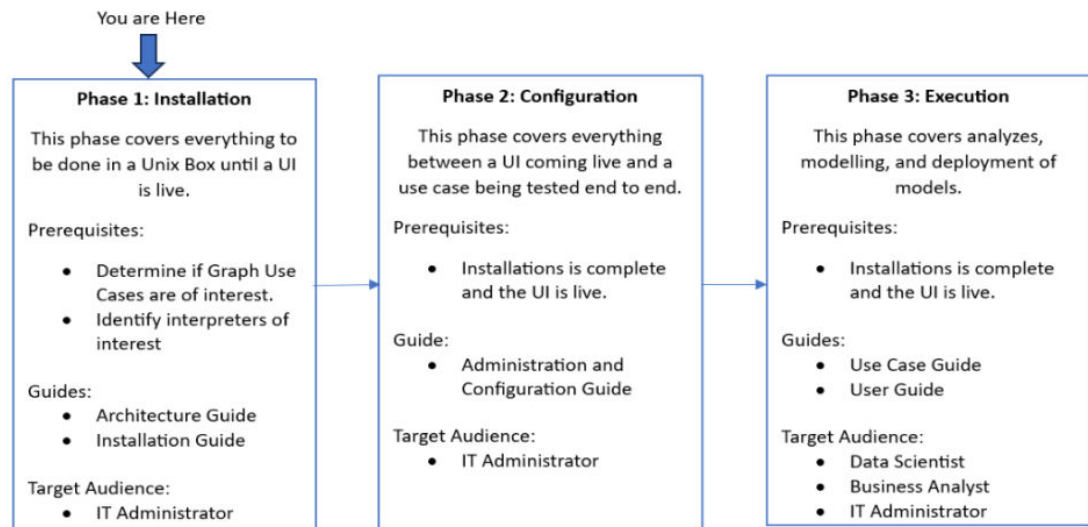
- If any issue occurs during installation, you can reinstall Compliance Studio with updated configuration.

The following use cases are supported in the Compliance Studio:

- **Entity Resolution**
- **Graph**
- **Investigation Toolkit Notebook**
- **Automated Scenario Calibration (ASC)**
- **Behavioral Model**
- **Sanctions Event Scoring**
- **AML Event Scoring**
- **Customer Segmentation and Anomaly Detection**
- **Customer Risk Scoring**
- **Shell Account Detection Scenario for AML**
- **Custom Scenario**

When to Use this Guide

The following illustration demonstrates when this guide should be used.

Figure 1-1 When to Use this Guide

2

Installation

This section explains step-by-step process for installing the Compliance Studio.

2.1 Prerequisites

Ensure your system meets the minimum hardware and software requirements and has the necessary environment and ports configured in the system before you begin installing the Compliance Studio.

Make sure that the application architecture is configured appropriately for the use cases of interest as outlined in the [OFS Compliance Studio Architecture Guide](#).

2.1.1 Hardware and Software Requirements

The installation environment or setup must have these requirements for an application to run smoothly and efficiently. The following hardware and software are required for this version of the Compliance Studio.

Table 2-1 Hardware and Software Requirements

Hardware/Software Category	Component Version	Use Case
Browser	Chrome	Applicable for all use cases
Java Version	JDK 17.0.12	Applicable for all use cases
Processing Server	RHEL 8+	Applicable for all use cases
Database Server	<ul style="list-style-type: none">Oracle Database Release 19c (19.3+)Enterprise EditionOracle Machine Learning for R (OML4R) (formerly ORE) 1.5.1 with Open source R or Oracle R Distribution 3.6.1	Applicable for all use cases
PGX (Graph) Server	<ul style="list-style-type: none">RHEL 8+Minimum gcc library v4.8.2	Applicable for Graph use case only
OpenSearch Version	Version: 2.19.1	Applicable for Entity Resolution and Graph use cases.
Logstash Version	Version: 7.16.3 Down load Logstash from here .	Applicable for Entity Resolution and Graph use cases.
Oracle Instant Client	instantclient-basic-linux.x64-19.8.0.0.0 Note: The version should be the same as the Database version, and this should be present in the processing server.	Applicable for all use cases
Oracle Database Client	Download the LINUX.X64_193000_client_home.zip file.	Applicable for all use cases

2.1.2 Environmental Settings

The following prerequisite environmental settings must be set before beginning the installation of Compliance Studio. These settings are the configuration that a system must have for an application to run smoothly and efficiently.

Table 2-2 Environmental Settings

Category	Expected Value
Java Settings	<p>PATH in the <code>.profile/.bash_profile</code> file must be set to include the Java Runtime Environment (JDK 17) absolute path.</p> <p>Supported version: jdk 17.0.12</p> <p>Note: Ensure the absolute path to JDK/bin is set at the beginning of the PATH variable.</p> <p>For example: <code>PATH=/scratch/fccstudio/jdk17.0.12/bin:\$PATH</code></p> <p>Ensure no SYMBOLIC links to Java installation are set in the PATH variable.</p>
Oracle Database Settings	<p>Oracle Processing Server</p> <p>ORACLE_HOME must be set in the <code>.profile</code> file pointing to the appropriate Oracle DB Client installation.</p> <p>PATH in the <code>.profile</code> file must be set to include the appropriate <code>\$ORACLE_HOME/bin</code> directory.</p>
Download Directory	<p>Indicates the directory where the product installer zip file is downloaded or copied. The user permission must be set to 755 for this directory.</p>
Installation Directory	<p>Indicates the directory where the product installer zip file is extracted, and the installation files are placed. The user permission must be set to 755 for this directory.</p> <p>Note: The Installation and the Download Directory can be the same if the product installer zip file is not copied separately to another directory.</p>
OS Locale	<p>Linux: <code>en_US.utf8</code></p> <p>Execute the following command to check the locale:</p> <pre>locale -a grep -i 'en_US.utf'</pre> <p>The locale is displayed.</p>
Oracle Instant Client	<p>Install oracle instant client in the server where compliance Studio is installed and provide the configuration <code>LD_LIBRARY_PATH</code> in <code>config.sh</code>.</p>

2.1.3 System Configuration

To configure the system:

1. Log in to the server as a root user.
2. Navigate to UNIX file path `/etc/security/limits.conf` to edit the file.
3. Add the following values at the end of the file for Compliance Studio:

```
<Username> hard nproc 65536
```

```
<Username> soft nproc 65536
```

For example:

```
compliancestudio hard nproc 65536
```

```
compliancestudio soft nproc 65536
```

2.1.4 Port Numbers for Application

To view default port number for available services in the application:

1. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
2. Open the additional_config.sh file and view list of ports as mentioned in the following table.

Table 2-3 List of Ports for Services

Service	Port Number
AUTH_SERVICE_PORT	7041
BATCH_SERVICE_PORT	7043
BE_PORT	7002
DATAPIPELINE_GATEWAY_SERVICE_PORT	7063
DATA_PIPELINE_UI_SERVICE_PORT	7067
ER_SERVICE_PORT	7051
GRAPH_SERVICE_PORT	7059
JDBC_EVENT_PORT	7031
JDBC_PORT	7011
LOAD_TO_OS_SERVICE_PORT	7053
MATCHING_SERVICE_PORT	7049
META_SERVICE_PORT	7045
PIPELINE_UI_SERVICE_PORT	7065
PYTHON_DEFAULT_EVENT_PORT	7030
PYTHON_DEFAULT_PORT	7010
PYTHON_DEFAULT_REST_PORT	7077
PYTHON_ML4AML_EVENT_PORT	7036
PYTHON_ML4AML_PORT	7016
PYTHON_ML4AML_REST_PORT	7097
PYTHON_SANE_EVENT_PORT	7037
PYTHON_SANE_PORT	7017
PYTHON_SANE_REST_PORT	7087
SCHEMA_PORT	7003
SESSION_SERVICE_PORT	7047
STUDIO_SERVICE_PORT	7008
UI_PORT	7001

Note

To customize the port number and other additional configuration, see [Additional Configuration](#) section in the [Appendix](#).

2.2 Preparing for Installation

This section describes how to download and extract the installer kit for Compliance Studio.

2.2.1 Download the Installer Kit

To download the software as .zip folders, download the latest installer **38357570** for the **v8.1.3.0.0** release from the [My Oracle Support \(MOS\)](#).

1. After downloading the installer kit (OFS_COMPLIANCE_STUDIO_8.1.3.0.0_LINUX.zip), unzip the file. It contains two folders as follows:
 - a. <p38357570_81300_Linux-x86-64>-1of2.zip
 - b. <p38357570_81300_Linux-x86-64>-2of2.zip
2. Rename the two folders as follows:
 - a. OFS_COMPLIANCE_STUDIO-8.1.3.0.0-1of2.zip
 - b. OFS_COMPLIANCE_STUDIO-8.1.3.0.0-2of2.zip

2.2.2 Extract the Installer Kit

To extract the downloaded .zip files:

1. Extract the OFS_COMPLIANCE_STUDIO-8.1.3.0.0-1of2.zip file from the installer in the download directory using the command.

```
unzip -a OFS_COMPLIANCE_STUDIO-8.1.3.0.0-1of2.zip
```
2. The OFS_COMPLIANCE_STUDIO-8.1.3.0.0-2of2.zip file should be placed in the same directory where OFS_COMPLIANCE_STUDIO-8.1.3.0.0-1of2.zip file is extracted.

Note

You do not need to unzip the OFS_COMPLIANCE_STUDIO-8.1.3.0.0- 2of2.zip file.

3. Navigate to the download directory where the installer archive is extracted, and assign execute permission to the installer directory using the following command:

```
chmod -R 0755 OFS_COMPLIANCE_STUDIO
```

After extracting .zip files, the folder structure should be as follows:

OFS_COMPLIANCE_STUDIO

OFS_COMPLIANCE_STUDIO-<version>-1of2.zip

OFS_COMPLIANCE_STUDIO-<version>-2of2.zip

The Compliance Studio installer file is extracted, and the OFS_COMPLIANCE_STUDIO directory is obtained and is referred to as <COMPLIANCE_STUDIO_INSTALLATION_PATH>.

Note

Do not rename the application installer directory name after extraction from the archive.

2.3 Pre-Installation

This section provides information about the tasks that must be performed before installing Compliance Studio. To install Compliance Studio with OFSAA, ensure the Behavior Detection (BD) or the Enterprise Case Management (ECM) application pack is installed.

2.3.1 Create Tablespace

Tablespace is required to manage and allocate space for its database objects efficiently. It plays crucial role in efficient database management, performance optimization, and scalability which are essential for the effective functioning of Compliance Studio.

To create a tablespace in the Oracle Database use the scripts as described in the following table.

Table 2-4 Create Tablespace

User	Script
AIF_USER_TEMP_TS	CREATE TABLESPACE AIF_USER_TEMP_TS DATAFILE '<Datafile Path>' SIZE <size in byte> REUSE AUTOEXTEND ON NEXT <size in megabyte> MAXSIZE UNLIMITED;
AIF_USER_TS	CREATE TABLESPACE AIF_USER_TS DATAFILE '<Datafile Path>' SIZE <size in byte> REUSE AUTOEXTEND ON NEXT <size in megabyte> MAXSIZE UNLIMITED;
<STUDIO TABLESPACE>	CREATE TABLESPACE <STUDIO TABLESPACE> DATAFILE '<Datafile Path>' SIZE <size in byte> REUSE AUTOEXTEND ON NEXT <size in megabyte> MAXSIZE UNLIMITED;
<GRAPH_SCHEMA_TS>	CREATE TABLESPACE <GRAPH_SCHEMA_TS> DATAFILE '<Datafile Path>' SIZE <size in byte> REUSE AUTOEXTEND ON NEXT <size in megabyte> MAXSIZE UNLIMITED;

Note

- The tablespace size should be defined based on the size of the data.
- AIF_USER_TS and AIF_USER_TEMP_TS tablespaces are required in all Production and Sandbox databases.

Verify the **AIF_USER_TS** and **AIF_USER_TEMP_TS** are available in the BD production database server. If not, then you need to create a tablespace. After creating a tablespace, you need to provide a quota on the tablespace AIF_USER_TS and AIF_USER_TEMP_TS.

For example:

```
ALTER USER <BD ATOMIC SCHEMA USER> QUOTA <size in megabyte> ON AIF_USER_TS; ALTER  
USER <BD ATOMIC SCHEMA USER> QUOTA <size in megabyte> ON AIF_USER_TEMP_TS;
```

2.3.2 Create Studio Schema

The studio schema stores all the metadata information related to Compliance Studio.

Note

The Compliance Studio schema and Atomic (BD/ECM) schema should be in the same database.

To create a studio schema, create a new Oracle Database schema user using the following script:

```
CREATE USER <STUDIO SCHEMA USER> IDENTIFIED BY <PASSWORD> DEFAULT TABLESPACE  
<STUDIO TABLESPACE>;  
ALTER USER <STUDIO SCHEMA USER> QUOTA 2000M ON <STUDIO TABLESPACE>;  
ALTER USER <STUDIO SCHEMA USER> QUOTA <SIZE IN MEGABYTE> ON AIF_USER_TS;
```

For example:

```
ALTER USER CS813_USER QUOTA 500M ON AIF_USER_TS;
```

Note

The tablespace and quota sizes should be defined based on the size of the data.

A new Oracle Database schema (Studio schema) is created.

2.3.3 Assign Grants for Studio Schema

This section describes how to assign grants for Studio schema.

Grant the following permissions to the newly created Oracle Database studio schema:

```
GRANT CREATE SESSION TO <STUDIO SCHEMA USER>;  
GRANT CREATE TABLE TO <STUDIO SCHEMA USER>;  
GRANT CREATE VIEW TO <STUDIO SCHEMA USER>;  
GRANT CREATE TRIGGER TO <STUDIO SCHEMA USER>;  
GRANT CREATE PROCEDURE TO <STUDIO SCHEMA USER>;  
GRANT CREATE SEQUENCE TO <STUDIO SCHEMA USER>;  
GRANT EXECUTE ON DBMS_RLS TO <STUDIO SCHEMA USER>;  
GRANT EXECUTE ON SYS.DBMS_SESSION TO <STUDIO SCHEMA USER>;  
GRANT CREATE SYNONYM TO <STUDIO SCHEMA USER>;  
GRANT EXECUTE ON DBMS_REDEFINITION TO <STUDIO SCHEMA USER>;  
GRANT REDEFINE TABLE TO <STUDIO SCHEMA USER>;  
GRANT CREATE MATERIALIZED VIEW TO <STUDIO SCHEMA USER>;  
GRANT SELECT ON SYS.V_$PARAMETER TO <STUDIO SCHEMA USER>;  
GRANT SELECT ON SYS.DBA_FREE_SPACE TO <STUDIO SCHEMA USER>;
```



```
GRANT SELECT ON SYS.DBA_TABLES TO <STUDIO SCHEMA USER>;
GRANT SELECT ON SYS.DBA_TAB_COLUMNS TO <STUDIO SCHEMA USER>;
GRANT CREATE RULE TO <STUDIO SCHEMA USER>;
GRANT DROP TRIGGER TO <STUDIO SCHEMA USER>;
GRANT SELECT ON SYS.DBA_RECYCLEBIN TO <STUDIO SCHEMA USER>;
GRANT CREATE JOB TO <STUDIO SCHEMA USER>;
GRANT EXECUTE ON DBMS_LOCK TO <STUDIO SCHEMA USER>;
GRANT EXECUTE ON DBMS_STATS TO <STUDIO SCHEMA USER>;
GRANT ANALYZE TO <STUDIO SCHEMA USER>;
GRANT CREATE TYPE TO <STUDIO SCHEMA USER>;
GRANT EXECUTE ON CTXSYS.CTX_DDL TO <STUDIO SCHEMA USER>;
```

Note

The following grants should be revoked after the successful installation of Compliance Studio.

```
REVOKE SELECT ON SYS.DBA_RECYCLEBIN FROM <STUDIO SCHEMA USER>;
REVOKE SELECT ON SYS.DBA_FREE_SPACE FROM <STUDIO SCHEMA USER>;
REVOKE SELECT ON SYS.DBA_TABLES FROM <STUDIO SCHEMA USER>;
REVOKE SELECT ON SYS.DBA_TAB_COLUMNS FROM <STUDIO SCHEMA USER>;
```

2.3.4 Create Sandbox Schema

This section describes how to create the Sandbox schema.

Note

- This section is applicable to all use cases with the exception of ASC. For ASC, the sandbox should be a valid prod-parallel BD schema.
- The Sandbox schema will always reside in a different database than the Atomic (BD/ECM) schema database.
- After creating a user for the sandbox schema, you must create a sandbox workspace.
- The tablespace and quota sizes should be defined based on the size of the data.

To create a sandbox schema, create a new Oracle Database sandbox schema user using the following script:

```
create user <SANDBOX SCHEMA USER>
IDENTIFIED BY <PASSWORD>
default tablespace AIF_USER_TS
temporary tablespace TEMP
profile DEFAULT
quota unlimited on AIF_USER_TS
quota unlimited on AIF_USER_TEMP_TS
```

A new Oracle Database schema (Sandbox schema) is created.

2.3.5 Assign Grants for Sandbox Schema

This section describes how to assign grants for Sandbox schema.

Note

This section is not applicable for ASC use case.

Grant the following permissions to the newly created Oracle Database sandbox schema:

```
GRANT CONNECT TO <SANDBOX SCHEMA USER>;
GRANT CREATE SESSION TO <SANDBOX SCHEMA USER>;
GRANT CREATE PROCEDURE TO <SANDBOX SCHEMA USER>;
GRANT CREATE SEQUENCE TO <SANDBOX SCHEMA USER>;
GRANT CREATE TABLE TO <SANDBOX SCHEMA USER>;
GRANT CREATE TRIGGER TO <SANDBOX SCHEMA USER>;
GRANT CREATE VIEW TO <SANDBOX SCHEMA USER>;
GRANT CREATE MATERIALIZED VIEW TO <SANDBOX SCHEMA USER>;
GRANT CREATE SYNONYM TO <SANDBOX SCHEMA USER>;
GRANT CREATE RULE TO <SANDBOX SCHEMA USER>;
GRANT CREATE ANY TRIGGER TO <SANDBOX SCHEMA USER>;
GRANT DROP ANY TRIGGER TO <SANDBOX SCHEMA USER>;
GRANT CREATE ANY TYPE TO <SANDBOX SCHEMA USER>;
```

2.3.6 Create Graph Schema

This section describes how to create Graph Schema.

Note

- This section is applicable only for Graph use case.
- The graph schema should be created based on which graph would be used:
 - For the BD graph, you should create a BD schema in the same database where the BD Atomic schema is present.
 - For the ECM graph, you should create an ECM schema in the same database where the ECM Atomic schema is present.
 - If both graphs are intended to be used, then the Graph, ECM and BD Atomic schemas should be on the same database.

Graph schema is a database schema where business data from either BD/ECM are extracted, transformed, and loaded (ETL) after the graph pipeline execution. The Compliance Studio installer requires the graph schema during the installation process; hence user should create the graph schema before the installation process.

If you are generating graph from business data of the BD application, then it is called as BD graph and similarly; if you are generating graph from business data of the ECM application, then it is called as ECM graph.

To create a graph schema, create a new Oracle Database schema user using the following script:

```
CREATE USER <GRAPH_SCHEMA_USER> IDENTIFIED BY <PASSWORD> DEFAULT TABLESPACE
<GRAPH_SCHEMA_TS>;
ALTER USER <GRAPH_SCHEMA_USER> QUOTA 2000M ON <GRAPH_SCHEMA_TS>;
For example:
ALTER USER GRAPH_SCHEMA_USER QUOTA 500M ON GRAPH_SCHEMA_TS;
```

Note

The tablespace and quota sizes should be defined based on the size of the data.

A new Oracle Database schema (Graph schema) is created.

2.3.7 Assign Pre-installation Grants for Graph Schema

This section describes how to assign pre-installation grants for the Graph schema.

Note

This section is applicable only for Graph use case.

Grant the following permissions to the newly created graph schema.

- **Pre-installation Grants for both BD and ECM Graphs**

```
GRANT ANALYZE TO <GRAPH_SCHEMA>;
GRANT CREATE SESSION TO <GRAPH_SCHEMA>;
GRANT CREATE TABLE TO <GRAPH_SCHEMA>;
GRANT CREATE VIEW TO <GRAPH_SCHEMA>;
GRANT CREATE PROCEDURE TO <GRAPH_SCHEMA>;
GRANT CREATE SEQUENCE TO <GRAPH_SCHEMA>;
GRANT CREATE JOB TO <GRAPH_SCHEMA>;
GRANT CREATE MATERIALIZED VIEW TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_SCHEDULER TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_COMPARISON TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_RLS TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON SYS.DBMS_SESSION TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_REDEFINITION TO <GRAPH_SCHEMA>;
GRANT REDEFINE TABLE TO <GRAPH_SCHEMA>;
GRANT SELECT ON SYS.V_$PARAMETER TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_ISCHED TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_PARALLEL_EXECUTE TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_STATS TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON SYS.DBMS_LOCK TO <GRAPH_SCHEMA>;
```

- **Pre-installation Grants for BD Graph**

Change the <BD_ATOMIC_SCHEMA> to the underlying schema of the data source of the BD graph pipeline.

Note

The following grants are applicable for the Out-of-the-box graph pipeline only. If the user has to execute the custom graph, the same permissions have to be provided for the input tables referred in Custom Graph Pipeline.

```
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.ACCT TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CUST_ACCT TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.ACCT_BAL_POSN_SMRY TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CUST TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.BACK_OFFICE_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.EMP TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CUST_CUST TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.KDD_CAL TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.KDD_REVIEW TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.EMP_ACCT TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.ACCT_SMRY_MNTH TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.ACCT_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.EXTERNAL_ENTITY TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CUST_EMAIL_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CUST_PHON TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CUST_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CASH_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.LINK_STAGE TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.WIRE_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.MI_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.INSTN_MASTER TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.EXTERNAL_ENTITY_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.DERIVED_ADDRESS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.CLIENT_BANK TO <GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.EXTERNAL_ENTITY_LINK TO <GRAPH_SCHEMA>;
GRANT ANALYZE TO <GRAPH_SCHEMA>;
```

- Pre-installation Grants for ECM Graph**

Change the <ECM_ATOMIC_SCHEMA> to the underlying schema of the data source of the ECM graph pipeline.

```
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_ACCT TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CUST_ACCT TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_ACCT_BAL_POSN_SMRY TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CUST TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_BACK_OFFICE_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EMP TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CUST_CUST TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EMP_ACCT TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_ACCT_SMRY_MNTH TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_ACCT_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EXTERNAL_ENTITY TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CUST_EMAIL_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CUST_PHON TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CUST_ADDR TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CASH_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_WIRE_TRXN TO <GRAPH_SCHEMA>;
```

```

GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_MI_TRXN TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_INSTN_MASTER TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EXTERNAL_ENTITY_ADDR TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_DERIVED_ADDRESS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CLIENT_BANK TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EXTERNAL_ENTITY_LINK TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.KDD_CASES TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.KDD_CASE_ACCOUNTS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_SCENARIO_MASTER TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EVENTS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EVENT_DETAILS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_EVENT_ENTITY_MAP TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_PRECASE_CASE_MAP TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.KDD_CASE_CUSTOMERS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.KDD_CASE_EXTERNAL_ENTITY TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.KDD_CASE_INSTN_MASTER TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CORRELATION_EVENT_MAP TO
<GRAPH_SCHEMA>;
GRANT EXECUTE ON DBMS_SCHEDULER TO <ECM_ATOMIC_SCHEMA>;
GRANT EXECUTE ON DBMS_ISCHED TO <ECM_ATOMIC_SCHEMA>;
GRANT EXECUTE ON DBMS_PARALLEL_EXECUTE TO <ECM_ATOMIC_SCHEMA>;
GRANT CREATE JOB TO <ECM_ATOMIC_SCHEMA>;

```

2.3.8 Create Filestore Directories in the Database Server for Graph

This section describes how to create Filestore Directories in the Database Server for Graph.

① Note

This section is applicable only for Graph use case.

To create filestore directories in the database server:

1. Log in as DB user in your DB server.
2. Create a new directory with preferred reference name (for example, datapipeline) at the preferred location.
3. Execute the following commands in putty session of the DB server:
 - Create a directory for the external table to write the logs - `mkdir -p ##<Location of the Created Directory>##/file_store/fs_list/ logs`
 - Create a directory to hold a pre-processor script used to list files in the directory and this requires read-execute permissions - `mkdir -p ##<Location of the Created Directory>##/file_store/fs_list/ script`
 - Create a directory to hold files to control which directories can be listed and this requires read permissions - `mkdir -p ##<Location of the Created Directory>##/file_store/fs_list/ control`

- Create a directory to hold files to control which directories can be listed and this requires read permissions - mkdir -p ##<Location of the Created Directory>##/file_store/fs_list/ fccm-data

2.3.9 Assign Grants to Studio Schema to Access the Filestore Directories

① Note

This section is applicable only for Graph use case.
Grant the following permissions to Studio Schema to access filestore directories.

```
CREATE OR REPLACE DIRECTORY fs_list_logs_dir AS '<Location of the
Created
Directory>/file_store/fs_list/logs/';
GRANT READ, WRITE ON DIRECTORY fs_list_logs_dir TO $STUDIO_DB_USERNAME;
CREATE OR REPLACE DIRECTORY fs_list_script_dir AS '< Location of the
Created
Directory >/file_store/fs_list/script/';
GRANT READ, EXECUTE ON DIRECTORY fs_list_script_dir
TO $STUDIO_DB_USERNAME;
CREATE OR REPLACE DIRECTORY fs_list_control_dir AS '<Location of the
Created
Directory >/file_store/fs_list/control/';
GRANT READ ON DIRECTORY fs_list_control_dir TO $STUDIO_DB_USERNAME;
CREATE OR REPLACE DIRECTORY external_tables_dir AS '<Location of the
Created
Directory >/file_store/fs_list/fccm-data/';
GRANT READ ON DIRECTORY external_tables_dir TO $STUDIO_DB_USERNAME;
```

2.4 Application User Access and Provisioning

The User Provisioning feature enables users and groups to be provisioned to Compliance Studio using REALM type.

① Note

Prerequisites: Pre-configure the REALM type as SAML for authentication.

The types are:

- SAML for Authentication and AAI for Authorization
- SAML for Authentication and SAML for Authorization
- AAI for Authentication and AAI for Authorization

2.4.1 Generating the Bearer Token

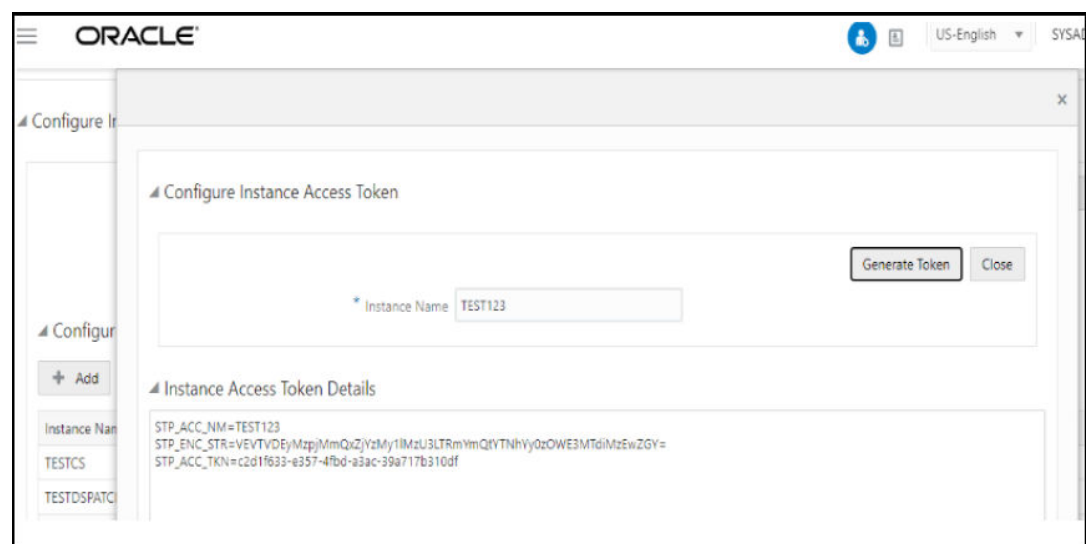
Bearer Token is required to configure the Compliance Studio for authentication and authorization.

To generate the bearer token:

1. Login to the BD/ECM application as **sysadmin**.
2. Select **Configure Instance Access Token** from the **System Configuration**.
3. Click **Add**.

The **Configure Instance Access Token** window is displayed.

Figure 2-1 Configure Instance Access Token



4. Provide the **Instance Name**.
5. Click **Generate Token**.
The Configure Instance Access Token Details are displayed.
6. Copy the **STP_ACC_NM** and **STP_ACC_TKN** for configuration.
7. Click **Close** to exit the screen.

2.4.2 SAML for Authentication and AAI for Authorization

This section describes the SAML for Authentication and AAI for Authorization.

If the REALM type is selected as **SAML for authentication and AAI for authorization**, configure:

1. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
2. Open the `config.sh` file and set the parameters as described in the following table.

Table 2-5 Parameters of config.sh file

Parameter	Significance	Value
AUTH_REALM	<p>Realm indicates the functional grouping of database schemas and roles that must be secured for an application. Realms protect data from access through system privileges; realms do not give its owner or participant's additional privileges.</p> <p>The Compliance Studio application can be accessed using the following realms:</p> <p>FCCMRealm Value=AAI FCCSamlRealm Value=SAML</p>	<p>SAML</p> <p>Note: This parameter is mandatory.</p>
SAML_DESTINATION	Indicates the SAML IDP URL that the Identity Provider provides after creating the SAML Application.	<p>Provide the IDCS-SSO URL.</p> <p>Note: This parameter is mandatory.</p>
SAML_ROLE_ATTRIBUTE	Indicates the SAML client identifier provided by the SAML Administrator for the Role and Attributes information while creating the SAML application for Compliance Studio.	<p>Provide the group name.</p> <p>Note: This parameter is mandatory.</p>
SAML_LOGOUT_URL	Indicates the SAML client identifier provided by the SAML Administrator for the Logout URL information while creating the SAML application for Compliance Studio.	<p>Provide the IDCS-SLO URL.</p> <p>Note: This parameter is mandatory.</p>
AAI_URL	<p>The Application URL of ECM/BD application.</p> <p>URL: http://<Server Hostname>:<Application URL PORT>/<Context Path></p>	<p>The value will be BD/ECM application where the USER-GROUP map/authentication is present.</p> <p>Note: This parameter is mandatory.</p>

3. Reinstall Compliance Studio with updated configuration.
4. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-ui/conf directory.
5. Open the application.properties file and add the following lines at the last:

```
#Fetching User-Groups from AAI using Bearer Token
aai.client.id=#client#
aai.client.secret=#secret#
aai.enable.fetchgroups=#true#/#false#
```
6. Replace the placeholder value as described in the following table.

Table 2-6 Parameter of application.properties file

Parameter	Value
aai.client.id	Provide Instance Name (STP_ACC_NM) of the Bearer Token. To get the instance name, see the Generating the Bearer Token .
aai.client.secret	Provide the Bearer token (STP_ACC_TKN). To get the instance name, see the Generating the Bearer Token .
aai.enable.fetchgroups	Set the value as true for AAI authorization.
aai.auth.url	Provide the AAI_URL.

7. Perform **Step 5** and **Step 6** in the `application.properties` file in the below location to take care of configuration whenever reinstall is required.

<COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-ui/conf

8. Restart Compliance Studio.

2.4.3 SAML for Authentication and SAML for Authorization

This section describes the SAML for Authentication and SAML for Authorization.

If the REALM type is selected as **SAML for authentication and SAML for authorization**, configure:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
2. Open the `config.sh` file and set the parameters as described in the following table.

Table 2-7 Parameters of the config.sh file

Parameter	Significance	Value
AUTH_REALM	Realm indicates the functional grouping of database schemas and roles that must be secured for an application. Realms protect data from access through system privileges; realms do not give its owner or participant's additional privileges. The Compliance Studio application can be accessed using the following realms: FCCMRealm Value=AAI FCCSamlRealm Value=SAML	SAML
SAML_DESTINATION	Indicates the SAML IDP URL that the Identity Provider provides after creating the SAML Application.	Provide the IDCS-SSO URL.

Table 2-7 (Cont.) Parameters of the config.sh file

Parameter	Significance	Value
SAML_ROLE_ATTRIBUTE	Indicates the SAML client identifier provided by the SAML Administrator for the Role and Attributes information while creating the SAML application for Compliance Studio.	Provide the group name.
SAML_LOGOUT_URL	Indicates the SAML client identifier provided by the SAML Administrator for the Logout URL information while creating the SAML application for Compliance Studio.	Provide the IDCS-SLO URL.

3. Reinstall Compliance Studio with updated configuration.
4. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-ui/conf` directory.
5. Open the `application.properties` file and add the following lines at the last:

```
#Fetching User-Groups from AAI using Bearer Token
aai.client.id=#client#
aai.client.secret=#secret#
aai.enable.fetchgroups=#true#/#false#
```
6. Replace the placeholder value as described in the following table.

Table 2-8 Parameter of application.properties file

Parameter	Value
aai.client.id	Retain the placeholder as it is.
aai.client.secret	Retain the placeholder as it is.
aai.enable.fetchgroups	Set the value as true for AAI authorization. Note: This parameter is mandatory.

7. Perform **Step 5** and **Step 6** in the `application.properties` file in the below location to take care of configuration whenever reinstall is required.

```
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-ui/conf
```
8. Restart Compliance Studio.

2.4.4 AAI for Authentication and AAI for Authorization

To enable REST API authorization by OFSAA in WebLogic, follow these steps:

1. Open the **config.xml** file located in the domain where OFSAA is deployed - `<domain_home>/config/config.xml`.
2. Add the security-configuration tag: `<enforce-valid-basic-authcredentials> false</enforce-valid-basic-auth-credentials>`

2.5 Database User Access

This section describes how users can access the database.

2.5.1 Setup Password Stores with Oracle Wallet

This section describes how to setup Password Stores with Oracle Wallet.

As part of an application installation, administrators must set up password stores for database user accounts using Oracle Wallet. These password stores must be installed on the application database side. The installer handles much of this process. The administrators must perform some additional steps.

A password store for the application and application server user accounts must also be installed; however, the installer takes care of this entire process.

User should create schema for pre-installation and post-installation activities as mentioned in the following table.

Table 2-9 Types of Schema for Installation Activity

Schema	Required for Pre-installation	Required for Post-installation
Studio Schema	Yes	Yes (It is already created in the pre-installation process).
Graph Schema	Yes	Yes (It is already created in the pre-installation process).
ECM/BD Atomic Schema	Yes	Yes (It is already created in the pre-installation process).
ER/FSDF Schema	No	Yes
Sandbox Schema	No	Yes

2.5.2 Setup the Password Stores for Database User Accounts

This section describes how to setup the Password Stores for Database User Accounts.

After the database is installed and the default database user accounts are set up, administrators must set up a password store using the Oracle Wallet. This involves assigning an alias for the username and associated password for each database user account. The alias is used later during the application installation. This password store must be created on the system where the application server and database client are installed. This section describes the steps to create a wallet and the aliases for the database user accounts.

For more information on configuring authentication and password stores, see [Oracle Database Security Guide](#).

Note

In this section, <wallet_location> is a placeholder text for illustration purpose. Before running the command, ensure that you have already created the <wallet_location> directory where you want to create and store the wallet.

To create a wallet:

1. Log in to the server as a Linux user.
2. Create a wallet in the <wallet_location> using the following command:

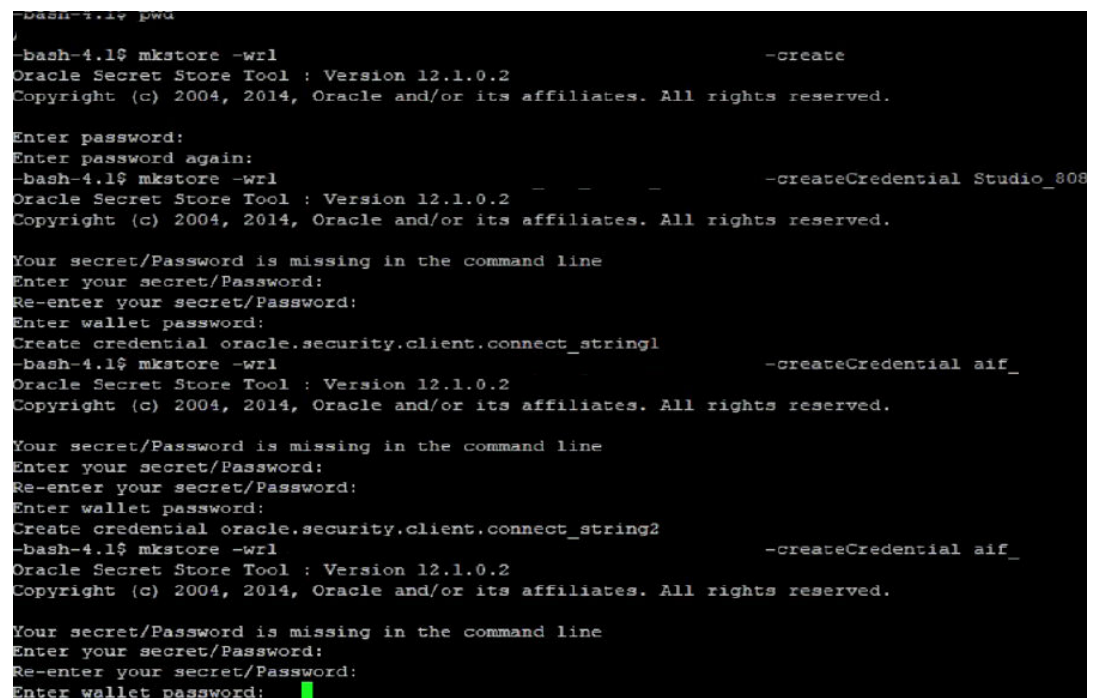
```
mkstore -wrl <wallet_location> -create
```

Note

The mkstore utility is included in the Oracle Database Client installation.

3. After you run the command, a prompt appears. Enter a password for the Oracle Wallet in the prompt.

Figure 2-2 Wallet Creation



```

-bash-4.1$ mkstore -wrl /u01/app/oracle/client/12.1.0.2/wallet -create
Oracle Secret Store Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

Enter password:
Enter password again:
-bash-4.1$ mkstore -wrl /u01/app/oracle/client/12.1.0.2/wallet -createCredential Studio_808
Oracle Secret Store Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

Your secret/Password is missing in the command line
Enter your secret/Password:
Re-enter your secret/Password:
Enter wallet password:
Create credential oracle.security.client.connect_string1
-bash-4.1$ mkstore -wrl /u01/app/oracle/client/12.1.0.2/wallet -createCredential aif_
Oracle Secret Store Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

Your secret/Password is missing in the command line
Enter your secret/Password:
Re-enter your secret/Password:
Enter wallet password:
Create credential oracle.security.client.connect_string2
-bash-4.1$ mkstore -wrl /u01/app/oracle/client/12.1.0.2/wallet -createCredential aif_
Oracle Secret Store Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

Your secret/Password is missing in the command line
Enter your secret/Password:
Re-enter your secret/Password:
Enter wallet password:

```

4. Create the database connection credentials for the studio schema/ER Schema alias using the following command:

```
mkstore -wrl <wallet_location> -createCredential <alias-name> <databaseuser-name>
```

After you run the command, a prompt appears. Enter the password associated with the database user account in the prompt. You are prompted to re-enter the password. You are prompted for the wallet password used in Step 1

5. Create the database connection credentials for the atomic schema alias using the following command:

```
mkstore -wrl <wallet_location> -createCredential <alias-name> <databaseuser-name>
```

Note

Creating an atomic schema is not required when installing Compliance Studio without OFSAA.

In this manner, create a wallet and associated database connection credentials for all the database user accounts.

The wallet is created in the <wallet_location> directory with the auto-login feature enabled. This feature enables the database client to access the wallet contents without using the password. For more information, see [Oracle Database Security Guide](#).


After the wallet is created, go to the <wallet_location> directory and click **Refresh**  to view the created wallet folder.

Figure 2-3 Location of the Created Wallet Folder

Name	Size	Changed	Rights	Owner
wallet_808_		12-08-2020 14:52:49	rwx-----	

The wallet folder contains two files - ewallet.p12 and cwallet.sso.

6. In the <wallet_location> directory, configure the **tnsnames.ora** file to include the entry for each alias name to be set up.

Figure 2-4 Snapshot of the tnsnames.ora file

```
Studio_808_ =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = ) (PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = )
    )
  )
aif_ =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = ) (PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = )
    )
  )
aif_ =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP) (HOST = ) (PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = )
    )
  )
)
```

Note

- You can either update the existing tnsnames.ora file with the above details or create new tnsnames.ora file and add the required entries.
- <alias-name> is a user-defined value.

7. Create a **sqlnet.ora** file in the wallet directory using the following content:

```
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY =  
<Wallet_Location>)) )  
  
SQLNET.WALLET_OVERRIDE=TRUE  
  
SSL_CLIENT_AUTHENTICATION=FALSE
```

2.5.3 Verify the Connectivity of the Wallet

This section describes how to verify the connectivity of the Wallet.

To verify the connectivity of the wallet.

1. Create a sqlnet.ora file in the wallet directory using the following content:

```
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY =  
<Wallet_Location>)) )  
  
SQLNET.WALLET_OVERRIDE=TRUE  
  
SSL_CLIENT_AUTHENTICATION=FALSE
```

2. Test the connectivity using the following command:

Note

The ORACLE_HOME used with the wallet must be the same version or higher than the wallet created.

```
$ export WALLET_LOCATION=<wallet_location>  
$ export TNS_ADMIN=<tnsnames.ora_location>. If you have created a new  
tnsnames.ora file, provide the location of the new file.  
$ sqlplus /@<alias_name>
```

The output is similar to:

```
SQL*Plus: Release 11  
Connected to:  
Oracle Database 12c  
To verify if you are connected to the correct user:  
SQL> show user  
The output is similar to:  
USER is "<database-user-name>"
```

2.5.4 Create Wallet for ER/ESDF Schema

This section describes how to create wallet for ER/ESDF schema.

To create a wallet for ER/ESDF, see **step 4** in the [Setup the Password Stores for Database User Accounts](#) section.

Note

- ER schema can be in the same database where CS is installed or a different database.
- You can create multiple ER schemas.

2.5.5 Create Wallet for Graph Schema

This section describes how to create wallet for Graph schema.

To create a wallet for Graph schema, see **step 4** in the [Setup the Password Stores for Database User Accounts](#) section.

Note

- Graph schema must be in the same database where Compliance Studio Schema is exists.
- You can refer only one Graph schema in Compliance Studio and it is applicable only for Graph use case.

2.6 Validation Checklist

The Validation Checklist section provides you with the parameters that you can validate to avoid installation issues.

This section explains the validation and actions that can be taken for some of the common parameters that are used in the `config.sh` file for the installation. The parameters that can be validated as mentioned in the following table.

Table 2-10 Required File Structure

Parameters	Validation
External Service (OFSAA_SERVICE URL)	The OFSAA_Service URL can be validated by clicking the URL for verification.
DB Details for Studio Schema	You can log in to SQL developer and verify the DB Details for Studio Schema.
Compliance Studio Schema Wallet Details	You can verify the Wallet details by reviewing the steps in Verify the Connectivity of the Wallet .
Atomic Wallet Detail	You can verify the Wallet details by reviewing the steps in Setup Password Stores with Oracle Wallet .

2.7 Installation Activity

This section explains step-by-step process to install Compliance Studio after completing the pre-installation activity.

2.7.1 Place Files in Wallet

This section describes how to place files in wallet.

To place the files in the wallet in the required locations:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>.
2. Create a folder 'wallet'.
3. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/wallet.
4. Place the following files, which are being generated from the <wallet_directory> in the [Setup the Password Stores for Database User Accounts](#) section:

```
tnsnames.ora  
ewallet.p12  
cwallet.sso  
ewallet.p12.lck  
cwallet.sso.lck
```

Note

This folder path will be referred to as "WALLET_LOCATION" and "TNS_ADMIN_PATH" in config.sh while configuring Compliance Studio. If you want to maintain tnsname.ora in a different folder, then "TNS_ADMIN_PATH" will be that folder location.

2.7.2 Generate Compliance Studio Server SSL Configuration

This section describes how to generate the Compliance Studio server SSL configuration.

2.7.2.1 Generate Self-signed Certificate

This section describes how to generate the Self-signed certificate.

To generate the self-signed certificate:

1. Run the following jks command in the Studio Server.

```
keytool -J-Dkeystore.pkcs12.legacy -genkey -alias <alias> -keyalg RSA -  
keystore <alias>.jks -dname "CN=<hostname>, OU=OR, O=OR L=OR, ST=OR, C=OR" -  
ext "SAN=IP:<ip address 1>,IP:<ip address 2>"
```


Note

- ip address 2 is optional and hostname is the fully qualified host name.
- You must use the same password and alias that is provided in the config.sh file.

2. Specify the keystore password.
3. When generating the keytool ensure to provide the hostname in the first name.

Question: What is your first and last name?

Answer: Provide the fully qualified studio server hostname.

For example: <hostname>.<domain name>

4. Specify any name for the other questions.
5. Specify the keystore password. The jks file is created in the Studio Server.

Note

You must use the same password and alias that is provided in the config.sh file.

6. Run the following jks command in the Studio Server to generate the .p12 file using the .jks file:

```
keytool -J-Dkeystore.pkcs12.legacy -importkeystore -srckeystore  
<alias>.jks -destkeystore <alias_name>.p12 -srcalias <alias> -  
srcstoretype jks -deststoretype pkcs12
```

7. Specify the keystore password. The .p12 file is created in the Studio Server.
8. Copy the .p12 files and place in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmghome/mmstudio/confdirectory.

2.7.2.2 Generate Signed Certificate

This section describes how to generate the Signed certificate.

To generate the signed certificate:

1. Log in to the server as a Linux user.
2. Generate the CSR file that describes the certificate requested and needed by the signing authority.
3. Openssl default configuration does not include subject alternative names by default.
4. SANs should be updated in cert.conf file. Additional SANs or IPs can be added through properties such as DNS.2, DNS.3, IP.1, and IP.2 in the [alt_names] section.
5. Once the configuration file is placed, generate the CSR file and associated private key by running the following command:

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr -  
config cert.conf
```

6. Provide the requested entries, and some entries can be left blank.

Note

- You can check the CSR contains SANs by running the command: `openssl req -text -noout -verify -in server.csr`
- This step is optional only.

7. Request certificate from the signing authority. Once the certificate is received, convert the `server.cer` into PEM format if required by running the command: `openssl x509 -in server.cer -out server.pem -outform PEM`

Note

- You can check the contents of the certificate to make sure that the SANs are included by running the command: `openssl x509 -in server.pem -text`
- This step is optional only.

8. Create `.p12` keystore.

Note

- The `-name` parameter must match the value of the **STUDIO_SERVER_SSL_ALIAS** variable from the path `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/ config.sh`
- To store the password, run the command: `openssl pkcs12 -export -out studio_server.p12 -inkey server.key -in server.pem -name studio_alias`
- The password must match the value of the **STUDIO_SERVER_SSL_PASSWORD** variable from `<COMPLIANCE_STUDIO_INSTALLATION_PATH >/bin/ config.sh`
- To check the keystore, run the command: `openssl pkcs12 -export -out studio_server.p12 -inkey server.key -in server.pem -name studio_alias`
- This step is optional only.

9. Copy `studio_server.p12` file and place in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-studio/conf/ studio_server.p12` and `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ mmg-home/mmg-studio/conf/studio_server.p12` directories.
10. Restart Compliance Studio. To do this, navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory and run the `./compliance-studio --restart` or `./compliance-studio -r`.

2.7.3 Import the Certificate to JDK Security

This section describes how to import the certificate to JDK security and it is required for both signed and self-signed certificates.

To import .p12 and .jks files:

1. Execute the following command to convert .p12 file to .cer format.

```
keytool -exportcert -keystore <Path of .p12 file >/<filename>.p12 -  
storetype PKCS12 -alias <alias> -file <Path where studiop.cer file should  
be created>/studiop.cer
```

For example:

```
keytool -exportcert -keystore /<COMPLIANCE_STUDIO_INSTALLATION_PATH>/  
studio_server.p12 -storetype PKCS12 -alias studio_server -file /  
<COMPLIANCE_ STUDIO_INSTALLATION_PATH>/studiop.cer
```

2. Execute the following command to import .cer to jdk security.

```
keytool -importcert -keystore <JAVA_HOME>/lib/security/cacerts - storepass  
changeit -alias studio_server -file <Path of studiop.cer file created from  
about command>/studiop.cer
```

For example:

```
keytool -importcert -keystore /Home/fccstudio/jdk-11.0.18/lib/security/  
cacerts -storepass changeit -alias studio_server -file /  
<COMPLIANCE_STUDIO_ INSTALLATION_PATH>/studiop.cer
```

Note

If you need to delete certificate from the JDK then execute the following command:

```
keytool -delete -noprompt -alias studio_server -keystore  
"<JAVA_HOME>/lib/security/cacerts" -storepass "changeit"
```

This can be helpful if you need to re-import a new certificate in the JDK.

2.7.4 Place the Key Store File for Secure Batch Service

This section describes how to place the Key Store file for Secure Batch service.

Place the .jks and .p12 files generated from the [Generate Compliance Studio Server SSL Configuration](#) section and place them in the batch service

<COMPLIANCE_STUDIO_INSTALLATION_PATH>/batchservice/conf path.

Note

If you have signed p12 certificate then .jks file is not required

2.7.5 Configure config.sh File

This section describes how to configure the config.sh file.

To configure the config.sh file for installing Compliance Studio:

1. Login to the server as a non-root user.
2. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
3. Configure the applicable config.sh attributes are shown in the following table.

A sample config.sh file is shown below for reference.

Figure 2-5 Snapshot of config.sh file

```

1  #!/usr/bin/env bash
2
3  ## COMPLIANCE_STUDIO_INSTALLATION_PATH path is absolute path including folder, 'OFS_COMPLIANCE_STUDIO'.
4  ## Example: /home/compliancestudio/OFS_COMPLIANCE_STUDIO
5  export COMPLIANCE_STUDIO_INSTALLATION_PATH=/scratch/focstudio/CS81300_C3_1908/compStudio_19081139/OFS_COMPLIANCE_STUDIO
6
7  ## MINICONDA_INSTALLATION_HOME is a configurable path for miniconda installation, within this "miniconda3" folder is created by the Miniconda
8  ## Example: /home/compliancestudio/conda
9  export MINICONDA_INSTALLATION_HOME=$HOME
10
11  ## NON_OFSAA: Accepted values: true or false
12  export NON_OFSAA=false
13
14  ## GRAPH_SOURCE Expected value : BD or ECM. This is source of data for ETL.
15  export GRAPH_SOURCE=BD
16  export ECM_SCHEMA_NAME=##ECM_SCHEMA_NAME##
17
18  ## Schema creator fcdm schema
19  export FCDM_SCHEMA=BD
20
21  ## SSL Configuration
22  ## Please place the SSL file after renaming it in 'COMPLIANCE_STUDIO_INSTALLATION_PATH/mmg-home/mmg-studio/conf' as file 'studio_server.p12'
23  export STUDIO_SERVER_SSL_SECRET=password
24  export STUDIO_SERVER_SSL_ALIAS=studio_server
25
26  ## Authentication Realm. Values are: SAML or AAI
27  export AUTH_REALM=SAML

```

Note

- You must manually set the parameter value in the config.sh file. If a value is not applicable, enter NA and ensure that the value is not entered as **NULL**.
- If the parameter STUDIO_DB_SERVICE_NAME has been filled, the parameter STUDIO_DB_SID should be left **blank**, and vice versa.
- If the parameter ATOMIC_DB_SERVICE_NAME has been filled, the parameter ATOMIC_DB_SID should be left **blank**, and vice versa.

Table 2-11 config.sh file

Parameter	Significance	Value
COMPLIANCE_STUDIO_INSTALLATION_PATH	Indicates the path where the Compliance Studio installer file is extracted.	Provide the path where the new installer is extracted. For example: /scratch/testuser/OFS_COMPLIANCE_STUDIO.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
MINICONDA_INSTALLATION_HOME	Indicates configured path for miniconda installation. By default, the value is set to \$HOME, which refers to the user's home directory.	By default, the value is \$HOME.
NON_OFSA	To install Compliance Studio with OFSA, enter " false ". To install Compliance Studio without OFSA, enter " true ".	Enter the value as false . For example: NON_OFSA=false
GRAPH_SOURCE	Indicates the source database for Compliance Studio.	Enter the value as BD . Note: This is a legacy ETL parameter, and the value should always be BD. This will not impact the Graph pipeline functionality with ECM.
ECM_SCHEMA_NAME	Indicates the name of the ECM Atomic Schema.	The value should be name of the ECM Atomic Schema. For example: ATOM8130 Note: If Legacy Graph (ETL connector job using Hadoop) is not required, then set the value as NA .
FCDM_SCHEMA	This indicates the datasource for the Production workspace. The available options are ECM and BD .	The value of this parameter should be provided either BD or ECM. For example: ECM.
STUDIO_SERVER_SSL_SECRET	Indicates the password for Studio Server P12 that is required for HTTPS configuration.	Enter the password created for the studio_server.p12 file. For example: password.
STUDIO_SERVER_SSL_ALIAS	Indicates the alias name for P12 for the Studio Server.	Enter alias name of the P12 file for the studio server. For example: studio_server.
AUTH_REALM	Realm indicates the functional grouping of database schemas and roles that must be secured for an application. Realms protect data from access through system privileges; realms do not give its owner or participant's additional privileges. Compliance Studio uses realm-based authorization and authentication for its users. The Compliance Studio application can be accessed using the following realms: FCCMRealm Value=AAI FCCSamlRealm Value=SAML	Enter AUTH_REALM value as SAML or AAI. For example: SAML.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
COOKIE_DOMAIN	The domain of the server where Compliance Studio is installed.	Enter the domain of the server where Compliance Studio is installed. For example: in.oracle.com.
AAI_URL	The Application URL of ECM/BD application. URL: http://<Server Hostname>:<Application URLPORT>/<Context Path>	Enter Application URL of ECM/BD. For example: http://testserver.in.oracle.com:4000/BDTEST Note: This parameter is applicable only if AUTH_REALM is AAI.
SAML_IDP_URL	Indicates the endpoint on the IDP side where SAML requests are posted. The Service Provider (SP) needs to obtain this information from the Identity Provider (IDP).	For example, http(s)://idcsxxxx.com/fed/v1/idp/so Note: This parameter is applicable only if AUTH_REALM is SAML .
SAML_DESTINATION	Indicates the SAML IDP URL that the Identity Provider provides after creating the SAML Application.	Enter the SAML Identity Provider URL. For example: http://<IDCS_APP_SSO_URL> Note: This parameter is applicable only if AUTH_REALM is SAML .
SAML_ROLE_ATTRIBUTE	Indicates the SAML client identifier provided by the SAML Administrator for the Role and Attributes information while creating the SAML application for Compliance Studio.	Enter the SAML client identifier. For example: group. Note: This parameter is applicable only if AUTH_REALM is SAML .
SAML_LOGOUT_URL	Indicates the SAML client identifier provided by the SAML Administrator for the Logout URL information while creating the SAML application for Compliance Studio.	Enter the Logout URL for SAML application. For example: http://<IDCS_APP_SLO_URL> Note: This parameter is applicable only if AUTH_REALM is SAML .
CS_SAML_SIGN_AUTHN_REQ	It is used to enable authentication through SAML signed request.	Set the value as true or false. By default, the value is false.
SAML_PRIVATE_KEY_PATH	Indicates the file path where the private key for signing SAML assertions or request is stored. For generating .pem file, see the Generating Files for SAML Signed Request section.	Enter the file path where private key is stored. For example, <COMPLIANCE_STUDIO_INSTALLATION_PATH>/spprivatekey.pem This parameter is applicable only when SAML_SIGN_AUTHN_REQ is set to true.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
SAML_SP_X509_CERT_PATH	Indicates the file path where the service provider's X509 certificate is stored. It is used by the service provider to validate the authenticity of the SAML assertions or to encrypt/decrypt information exchanged with the Identity Provider. For generating .cer file, see the Generating Files for SAML Signed Request section.	Enter the file path where service provider's X509 certificate is stored. For example, <COMPLIANCE_STUDIO_INSTALLATION_PATH>/spcertificate.cer
SAML_SIGN_ALGORITHM	Indicates algorithm for signing SAML assertions, request or responses.	Set this field as blank
DATASTUDIO_SAML_AUTHZTYPE	Indicates the Auth type for Data Studio and it is applicable when realm is OFSAASAMLRealm .	Set the value as SAML for SAML authN and SAML authZ, and AAI for SAML authN and AAI authZ.
API_USERS	Retain the default value	Retain the default value. In case of ECM-IH integration, add one more value to the parameter. i.e., ECM_API_USER. The values should be comma separated. For example: CS_API_USER, ECM_API_USER.
VALID_ROLES	Retain the default value	Retain the default value. For example: DSADMIN and DSUSER.
BATCH_ROLE	Retain the default value	Retain the default value. For example: DSBATCH
FTPSHARE	This can be any writable folder accessible to the process owner.	By default the value is \$COMPLIANCE_STUDIO_INSTALLATION_PATH/installed/workspace. For example, /scratch/users/ftpshare Note: Ensure that ftpshare folder is created before installation.
DATACATALOG_SERVICE_URL	Configuration is not required for this parameter	-
DATASTUDIO_SCHEMA_WALLET_ALIAS	Indicates the schema wallet alias of Datastudio.	Enter the schema wallet alias of Datastudio.
AAI_AUTHZ_ENABLED	Enables or disables AAI-based authorization when set to true; defaults to disabled. Note: Enable this setting only if the UI authentication type is SAML or LDAP, and you want to map additional user groups in AAI.	Set the value to true or false.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
AAI_CLIENT_ID	Indicates the instance name that the user provides when triggering the instance token in the AAI application. Note: This parameter can be configured when AAI_AUTHZ_ENABLED is set to true.	Enter the client ID for AAI-based authorization.
AAI_CLIENT_SECRET	Indicates the token generated when triggering an instance in the AAI application. Note: This parameter can be configured when AAI_AUTHZ_ENABLED is set to true.	Enter the client secret for AAI-based authorization.
SESSION_TOKEN_CREDENTIALS	Retain the default value	Retain the default value
FCC_API_USER	Retain the default value	Retain the default value. For example: CS_API_USER
MMG_DATASOURCE_MAX_POOL_SIZE	Maximum connection pool size allowed for Config Data Source.	Enter the maximum connection pool size for Config Data Source. For example: 50.
MMG_DATASOURCE_IDLE_TIMEOUT	Idle timeout for Config Data Source in a millisecond.	Enter Idle timeout for Config Data Source in a millisecond. For example: 30000.
MMG_DATASOURCE_CONNECTION_TIMEOUT	Connection timeout for Config Data Source in milliseconds.	Enter connection timeout for Config Data Source in milliseconds. For example: 30000.
EXT_DATASOURCE_MAX_POOL_SIZE	Maximum connection pool size allowed for Meta/Data Schemas.	Enter maximum connection pool size allowed for Meta/Data Schemas. For example: 50.
EXT_DATASOURCE_IDLE_TIMEOUT	Idle timeout for Meta/Data Schemas in milliseconds.	Enter Idle timeout for Meta/Data Schemas in milliseconds. For example: 30000.
EXT_DATASOURCE_CONNECTION_TIMEOUT	Connection timeout for Meta/Data Schemas in milliseconds.	Enter Connection timeout for Meta/Data Schemas in milliseconds. For example: 30000.
MMG_MODEL_ENDPOINT_RESTART_INTERVAL	Specifies the interval, in milliseconds, at which all model endpoints are automatically restarted in the model catalog to prevent disruptions caused by studio notebook expiration.	Enter the interval in milliseconds.
SERVER_COOKIE_TIMEOUT	Connection timeout for server cookie in milliseconds.	Enter connection timeout for server cookie in milliseconds. For example: 86400.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
DATASTUDIO_CSP_FRAME_A NCESTORS	This parameter allows Datastudio UI to be embedded as iFrame in any external application and this controls the allowed origins where datastudio UI can be embedded.	In case of ECM-IH integration use case, update the DATASTUDIO_CSP_FRAME_A NCESTORS parameter as follows: https://<Hostname>:<Compliance_Studio_Gateway_Port>,http://<ecm_webserver_hostname>:<ecm_ui_port> For example: DATASTUDIO_CSP_FRAME_A NCESTORS=https://testCSserver.oraclevcn.com:7071,http://testECMserver:8019
MMG_SPARK_ENABLED	It is used to enable or disable the spark interpreter.	The value is either true or false.
HADOOP_HOME	Indicates the directory path where Hadoop is installed.	Retain the placeholder as it is. For example, ##HADOOP_HOME##
SPARK_MASTER	Indicates master URL for the cluster or environment in which the spark job will run.	Retain the placeholder as it is. For example, ##SPARK_MASTER##
SPARK_DEPLOY_MODE	Indicates the mode how the spark application will be deployed.	Retain the placeholder as it is. For example, ##SPARK_DEPLOY_MODE##
SPARK_HOME	Indicates the absolute path of the Apache Spark library.	Retain the placeholder as it is. For example, ##SPARK_HOME##
STUDIO_DB_HOSTNAME	Indicates the hostname of the database where the Compliance Studio schema is created. Note: You must be logged in as SYSDBA to perform the Studio Schema configurations.	Enter hostname of the database where the Compliance Studio schema is created. For example: <testserver>.oraclevcn.com
STUDIO_DB_PORT	Indicates the port number where the Compliance Studio schema is created.	Enter port number where the Compliance Studio schema is created. For example: 1521.
STUDIO_DB_SERVICE_NAME	Indicates the service name of the database where the Studio schema is created.	Enter service name of the database where the Studio schema is created. For example: fccmdb.
STUDIO_DB_SID	Indicates the SID of the database where the Studio schema is created.	SID of the database where the Studio schema is created. For example: fccmdb. Note: Set this field as blank if there is no SID for Database.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
STUDIO_DB_USERNAME	Indicates the username of the Compliance Studio Schema	Enter username of the Compliance Studio Schema (newly created Oracle Schema). For example: CS8130_XXX_XX.
ATOMIC_DB_HOSTNAME	The hostname of the database where Atomic schema is present	Enter hostname of the database where Atomic schema is present (BD/ECM config). For example: <testserver>.oraclevcn.com
ATOMIC_DB_PORT	Port number of database where Atomic schema is present	Enter Port number of database where Atomic schema is present. For example: 1521.
ATOMIC_DB_SERVICE_NAME	The service name of the database where Atomic schema is present	Enter service name of the database where Atomic schema is present. For example: fccmdb.
ATOMIC_DB_SID	Service ID of database where Atomic schema is present. Note: Set this field as blank if there is no SID for Database.	Enter Service ID of database where Atomic schema is present. For example: fccmdb. Note: Set this field as blank if there is no SID for Database.
ATOMIC_DB_USERNAME	Username of the Atomic schema.	Enter Username of the Atomic schema. For example: XXX_ATOM8125.
STUDIO_ALIAS_NAME	Indicates the Studio alias name.	Enter Studio alias name. For example: CS8130_XXX_XX_alias Note: Enter the alias name that was created during wallet creation.
ATOMIC_ALIAS_NAME	Indicates alias name of FCDM source atomic schema given in wallet.	Enter alias name of FCDM source atomic schema given in wallet. For example: XXX_ATOM8125_alias Note: If Legacy Graph (ETL connector job using Hadoop) is not required, then set the value as NA .
TNS_ADMIN_PATH	Indicates the path of the tnsnames.ora file where an entry for the STUDIO_ALIAS_NAME is present.	Enter the path of the tnsnames.ora file where an entry for the STUDIO_ALIAS_NAME is present. For example: <COMPLIANCE_STUDIO_INSTALLATION_PATH>/wallet

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
WALLET_LOCATION	Indicates the Compliance Studio's wallet location. Note: For information on creating a wallet, Setup Password Stores with Oracle Wallet .	Enter wallet location of the Compliance Studio. For example: <COMPLIANCE_STUDIO_INSTALLATION_PATH>/wallet
LOGSTASH_HOME	Indicates the Logstash home. Note: Logstash is a supporting software for data ingestion to the OpenSearch.	Enter the path where Logstash is configured. For example: <COMPLIANCE_STUDIO_INSTALLATION_PATH>/Logstash/logstash-7.16.3 Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
GRAPH_DB_SERVER_NAME	Indicates the Graph Database server name. Note: The following parameters for graph service are mandatory for successful Compliance Studio installation, and the parameters cannot be set as blank or NA. If you do not want to use graph pipeline functionality, studio schema details should be provided for these parameters.	Enter the server name where the Graph Database is installed. For example: <testserver>.com
GRAPH_DB_PORT	Indicates the Graph Database server port	Enter the Graph Database server port. For example: 1521.
GRAPH_DB_SERVICE_NAME	Indicates the Graph Database service name	Enter the Graph Database service name. For example: fccmdb.
GRAPH_KEYSTORE_PASSWORD	Indicates the password of the keystore file, which stores the password of the graph schema.	Enter the password of the keystore file, which stores the password of the graph schema. For example: passwordXXX Note: If Graph Pipeline functionality is not required, then set the value as NA .
GRAPH_SCHEMA_DB_SCHEMA_NAME	Indicates the Database schema name of the graph schema.	Enter the Database schema name of the graph schema. For example: GSCS8130_XXX_XX.
GRAPH_SCHEMA_WALLET_ALIAS	Indicates the wallet alias of the graph schema.	Enter the wallet alias of the graph schema. For example: GSCS8130_XXX_XX_alias.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
GRAPH_SCHEMA_WALLET_LOCATION	Indicates the wallet location of the graph schema.	Enter the wallet location of the graph schema. For example: <COMPLIANCE_STUDIO_INSTALLATION_PATH>/wallet
GRAPH_SCHEMA_TNS_ADMIN_PATH	Indicates the TNS admin path of the graph schema.	Enter the TNS admin path of the graph schema. For example:<COMPLIANCE_STUDIO_INSTALLATION_PATH>/wallet
PGX_ENABLE_CP	It is used to enable or disable connection pooling for sub graph loading.	Set it to true for enabling the connection pooling for sub graph loading. The value for 'PGX_ENABLE_CP' is "true" or "false". For example: PGX_ENABLE_CP=true.
PGX_CP_INITIAL_SIZE	Indicates the initial number of connections that are created when the pool is started.	Enter the initial number of connections that are created when the pool is started. For example: 5.
PGX_CP_MAX_TOTAL	Indicates the maximum number of active connections that can be allocated from this pool at the same time or negative for no limit.	Enter the maximum number of active connections that can be allocated from this pool at the same time or negative for no limit. For example: 25.
PGX_CP_MAX_IDLE	Indicates the maximum number of connections that can remain idle in the pool, without extra ones being released or negative for no limit.	Enter the maximum number of connections that can remain idle in the pool, without extra ones being released or negative for no limit. For example: 10.
PGX_CP_MIN_IDLE	Indicates the minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none.	Enter the minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. For example: 5.
PGX_CP_MAX_WAIT_MILLIS	Indicates 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.	Enter 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. For example: 3000.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
PGX_CP_MIN_EVICTABLE_IDLE_TIME	Indicates 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 PGX_CP_MIN_IDLE.	Enter 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 PGX_CP_MIN_IDLE.
PGX_CP_SOFT_MIN_EVICTABLE_IDLE_TIME	Indicates the minimum amount of time a connection may sit idle in the pool before it is closed and a new connection is created.	Enter the minimum amount of time a connection may sit idle in the pool before it is closed and a new connection is created. For example: PT8H. Note: The values lesser than PGX_CP_MIN_EVICTABLE_IDLE_TIME will close all the idle connection and create connection to match PGX_CP_MIN_IDLE.
EXT_SCHEMA_ENABLE_CP	It is used to enable or disable connection pooling from any external schema. The parameters (Default Connection Pooling Configuration for External Schema) are applicable for enabling connection pool in graph service for any external schema. Note: The External Schema parameters are required for generating PDF in Investigation Toolkit notebooks.	The value is either true or false. If it is set to true, then configure the following parameters related to External Schema. If it is set to false, then configure the following parameters related to External Schema as NA .
EXT_SCHEMA_CP_MAX_IDLE	Indicates the maximum number of connections that can remain idle in the pool, without extra ones being released or negative for no limit.	Enter the maximum number of connections that can remain idle in the pool, without extra ones being released or negative for no limit. For example: 5.
EXT_SCHEMA_CP_MIN_IDLE	Indicates the minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none.	Enter the minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none. For example: 2.
EXT_SCHEMA_CP_INITIAL_SIZE	Indicates the initial number of connections that are created when the pool is started.	Enter the initial number of connections that are created when the pool is started. For example: 1.
EXT_SCHEMA_CP_MAX_TOTAL	Indicates the maximum number of active connections that can be allocated from this pool at the same time or negative for no limit.	Enter the maximum number of active connections that can be allocated from this pool at the same time or negative for no limit. For example: 10.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
EXT_SCHEMA_CP_MAX_WAIT_MILLIS	Indicates 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.	Enter 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. For example: 3000.
EXT_SCHEMA_CP_MIN_EVICTABLE_IDLE_TIME	Indicates 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 EXT_SCHEMA_CP_MIN_IDLE.	Enter 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 EXT_SCHEMA_CP_MIN_IDLE. For example: PT30M.
EXT_SCHEMA_CP_SOFT_MIN_EVICTABLE_IDLE_TIME	Indicates the minimum amount of time a connection may sit idle in the pool before it is closed and a new connection is created.	Enter the minimum amount of time a connection may sit idle in the pool before it is closed and a new connection is created. For example: PT6H. Note: The values lesser than EXT_SCHEMA_CP_MIN_EVICTABLE_IDLE_TIME will close all the idle connection and create connection to match EXT_SCHEMA_CP_MIN_IDLE.
PGX_ZEPPELIN_SCHEDULER_THREADPOOL_SIZE	Indicates the threadpool size of the PGX interpreter.	Enter the threadpool size of the PGX interpreter. For example: 200.
ENABLE_MATCHING_FOR_GRAPH	It is used to enable or disable matching for the graph.	The value is either true or false. For example: ENABLE_MATCHING_FOR_GRAPH=true
AUDIT_DATASOURCE_NAME	Indicates the datasource name which points to the database schema where Investigation Toolkit audit log is saved.	Enter the datasource name which points to the database schema where Investigation Toolkit audit log is saved. For example, GS is the datasource name which points to the Graph Schema.
ENABLE_POLICY_CREATION	This parameter is required for fine-grain access control.	By default, the value is false.
ENABLE_QUANTIFIND	It is used to enable or disable the quantifind integration. The parameters (Quantifind Details) are related to Quantifind Integration with Investigation Hub and these are optional.	Enable to integrate with quantifind. The value is "true" or "false". For example: Y.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
QUANTIFIND_URL	Indicates the quantifind API URL	Enter the quantifind API URL. For example: https://testserver.quantifind.com. Note: In Studio Schema, update Quantifind URL in V_URL column of the CS_IH_EXT_SRVC_APP_DET AILS table.
QUANTIFIND_APPNAME	Indicates the quantifind App Name	Enter the quantifind App Name. For example: OracleIntegrationTest. Note: In Studio Schema, update Quantifind App name in V_REQ_HDR_VALUE column of the CS_IH_EXT_SRVC_REQ_HEADERS table where V_REQ_HDR_KEY is X-QF-App-Name.
QUANTIFIND_TOKEN	Indicates the quantifind API token	Enter the quantifind API token Note: In Studio Schema, update Quantifind API token in V_REQ_HDR_VALUE column of the CS_IH_EXT_SRVC_REQ_HEADERS table where V_REQ_HDR_KEY is X-QF-App-Token.
HTTPS_PROXY_HOST	Indicates the proxy host that is used	Enter the proxy host that is used. For example: testproxyserver.com
HTTPS_PROXY_PORT	Indicates the proxy port that is used.	Enter the proxy port that is used. For example: 80.
HTTP_PROXY_USERNAME	Indicates the proxy username used, if there is any.	Enter the proxy username used, if there is any. For example: NA.
HTTP_PROXY_PASSWORD	Indicates the proxy password used if there is any.	Enter the proxy password used if there is any. For example: NA.
NO_PROXY	Indicates URLs with these domains and IP will be accessed without PROXY. Note: Configure this parameter when Quantifind is enabled.	The default value is "\"*.\$ (hostname - d) localhost \$(hostname - i) 127.0.0.1 0.0.0.0\""

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
NUM_CACHED_RESULTSET	<p>Indicates the cached result set. PGX (Parallel Graph AnalytiX) is a graph toolkit from Oracle that provides graph analysis on large scale graphs, to extract insights hidden in the connections across datasets between entities.</p> <p>Using built-in and custom graph algorithms, graph-pattern matching queries, and other enhanced graph analytics features, PGX helps investigators in conducting meaningful investigations and making actionable recommendations.</p> <p>Note: The parameter related to PGX server is applicable only for Graph use case.</p>	<p>Enter the cached result set.</p> <p>For example: 0.</p>
RESULTSET_EXPIRATION_TIME_SECS	Indicates the Result set expiration time.	<p>Enter the Result set expiration time.</p> <p>For example: 3600.</p>
MAX_TOTAL_SHARED_DATA_MEMORY_SIZE	The absolute memory limit of shared data (includes published graphs and pinned non-referenced graphs).	<p>Enter the absolute memory limit of shared data (includes published graphs and pinned non-referenced graphs).</p> <p>For example: 20G.</p>
MAX_TOTAL_PRIVATE_DATA_MEMORY_SIZE	The memory limit of private data (includes non-published graphs and PGQL results) relative to the total PGX engine memory limit.	<p>Enter the memory limit of private data (includes non-published graphs and PGQL results) relative to the total PGX engine memory limit.</p> <p>For example: 8G.</p>
MAX_PER_SESSION_DATA_MEMORY_SIZE	Absolute memory limit for any one session of the PGX engine.	<p>Enter the Absolute memory limit for any one session of the PGX engine.</p> <p>For example: 700M.</p>
MAX_DATA_MEMORY_SIZE_DSUSRGRP	Absolute memory limit for any user of the PGX engine whose role is DSUSRGRP.	<p>Enter the Absolute memory limit for any user of the PGX engine whose role is DSUSRGRP.</p> <p>For example: 2G.</p>
MAX_DATA_MEMORY_SIZE_DSBATCH	Absolute memory limit for any user of the PGX engine whose role is DSBATCH.	<p>Enter the Absolute memory limit for any user of the PGX engine whose role is DSBATCH.</p> <p>For example: 10G.</p>
MAX_DATA_MEMORY_SIZE_DSINTER	Absolute memory limit for any user of the PGX engine whose role is DSINTER.	<p>Enter the Absolute memory limit for any user of the PGX engine whose role is DSINTER.</p> <p>For example: 5G.</p>

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
MAX_DATA_MEMORY_SIZE_D SA PPROVER	Absolute memory limit for any user of the PGX engine whose role is DSAPPROVER.	Enter the Absolute memory limit for any user of the PGX engine whose role is DSAPPROVER. For example: 5G.
MAX_DATA_MEMORY_SIZE_D SUSER	Absolute memory limit for any user of the PGX engine whose role is DSUSER.	Enter the Absolute memory limit for any user of the PGX engine whose role is DSUSER. For example: 5G.
MAX_DATA_MEMORY_SIZE_I HUSRGRP	Absolute memory limit for any user of the PGX engine whose role is IHUSRGRP.	Enter the Absolute memory limit for any user of the PGX engine whose role is IHUSRGRP. For example: 10G.
PGX_SERVER_URL	Indicates the URL of the PGX server.	Enter URL of the PGX server. Note: If SSL is enabled, the URL should be provided with https . If SSL is disabled, the URL should be provided with http . Ensure to provide the correct hostname for the URL of the PGX service. If Legacy Graph (ETL connector job using Hadoop) and Graph Pipeline functionalities are not required, then set the value as NA .
R_ENABLED	It is used to enable or disable the R interpreter. Note: <ul style="list-style-type: none"> If this parameter is set to true, the R_PYTHON_HOME, RS_CONF_PATH, RS_KEYSTORE, and RS_KS_SECRET values must be provided If you are using an older Studio schema with an R interpreter already present and install with R_ENABLED set to false, the R interpreter will remain in Studio's interpreter menu and must be deleted manually. 	By default the value is set to true. Note: For configuration, see the R Interpreter section in the OFS Compliance Studio Administration and Configuration Guide .
R_PYTHON_HOME	Indicates the filesystem path to the Python environment used by R. Note: This parameter can be configured only when R_ENABLED is set to true.	Enter the filesystem path.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
RS_CONF_PATH	Absolute path to Rserve.conf file for running Rserve. Note: This parameter can be configured only when R_ENABLED is set to true.	Retain the default value. For example: /scratch/users/mmg-studio/conf/Rserve.conf
RS_KEYSTORE	Absolute path for the Keystore file made for Rserve.conf. Note: This parameter can be configured only when R_ENABLED is set to true.	Retain the default value. For example: / scratch/ users/ mmg-studio/ conf/ rinterpreterkeystore
RS_KS_SECRET	Keypass for rinterpreterkeystore. Note: This parameter can be configured only when R_ENABLED is set to true.	Retain the default value. For example: Change it. If the target AAI is https, then the certificate of the target machine needs to be imported to the DS Java keystore.
LD_LIBRARY_PATH	Indicates the Oracle Instant client path.	Enter the Oracle Instant client path. For example: /opt/oracle/instantclient_19_8:\$LD_LIBRARY_PATH
MATCHING_MECHANISM	Indicates the matching mechanism for Entity Resolution and Graph.	By default, the value is OS which refers to OpenSearch.
OPEN_SEARCH_HOSTNAME	Indicates the hostname of the server where the OpenSearch service is installed. OpenSearch is a distributed search and analytics engine. Compliance Studio leverages the search feature offered by OpenSearch. Note: The parameter related to OpenSearch is applicable for Entity Resolution and Graph use cases when MATCHING_MECHANISM is set to OS .	Enter the hostname of the server where the OpenSearch service is installed. For example: <testserver>.com. Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
OPEN_SEARCH_PORT	Indicates the port number where the OpenSearch service is installed.	Enter the port number where the OpenSearch service is installed. For example: 9202. Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
OPEN_SEARCH_HADOOP_CREDENTIAL_PATH	Indicates the open search hadoop credential path.	Enter the value as NA.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
OPEN_SEARCH_USERNAME	Indicates the OpenSearch Username.	Enter the OpenSearch Username. (It is Not Applicable when https enabled is false and authentication is not supported). For example: admin. Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
OPEN_SEARCH_ENCRYPTED_PASSWORD	Indicates the Encrypted password of the OpenSearch	Enter the Encrypted password. (It is Not Applicable when https enabled is false and authentication is not supported). Note: To generate an encrypted password, see Generate an Encrypted Password for OpenSearch . If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
OPEN_SEARCH_HADOOP_PASSWORD_ALIAS	Indicates the password alias for OpenSearch	Enter the value as NA.
OPEN_SEARCH_HTTPS_ENABLED	True (If OS is https enabled, else false)	Set it to True when Open Search is https enabled. Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as false .
OPEN_SEARCH_TRUSTSTORE_FILE_NAME	The filename of the OpenSearch keystore that contains the certificates of OS host to trust. (Not Applicable, if https enabled is false).	Enter the filename of the OpenSearch keystore that contains the certificates of OS host to trust. (Not Applicable, if https enabled is false). For example: admin.p12. Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
OPEN_SEARCH_TRUSTSTORE_SECRET	The password of the OpenSearch keystore file. (Not Applicable, if https enabled is false).	Enter the password of the OpenSearch keystore file. (Not Applicable, if https enabled is false). Note: If Graph Pipeline and Entity Resolution functionalities are not required, then set the value as NA .
OPEN_SEARCH_KEYSTORE_HADOOP_CREDENTIAL_ALIAS	Indicates the password alias for OpenSearch. (Not applicable if OS OPEN_SEARCH_HTTPS_ENABLED is false).	Enter the value as NA.

Table 2-11 (Cont.) config.sh file

Parameter	Significance	Value
ES Cluster Details Configuration is not required for the parameters related to Elastic Search as it is deprecated.	-	-
Additional MMG Configuration Configuration is not required for these EST_ENABLED, and EST_UI_URL parameters.	-	-
All Services Set the value of the parameter, DEPLOY_ALL_SERVICE, as true for starting all services and false for starting the selected services. For example: Compliance Studio independent of OFSAA: set "false" for service(s): entity resolution, matching service, and load-to-open Compliance Studio lite: set "false" for service(s): fcc-pgql, fcc-pgx-algorithm, fcc-pgx-java and pgx-server.	-	-
DEPLOY_ALL_SERVICE	Indicates the service to be started.	Set the value as true or false. Set it to true for starting all services. If it is false, then enable the following services based on the use case.
METASERVICE_ENABLED	This service has to be enabled for all use cases.	Set the value as true.
BATCHSERVICE_ENABLED	This service has to be enabled for all use cases.	Set the value as true.
GRAPH_SERVICE_ENABLED	This service has to be enabled for Graph use case.	Set the value as true.
ENTITY_RESOLUTION_ENABLED	This service has to be enabled for Entity Resolution use case.	Set the value as true.
MATCHING_SERVICE_ENABLED	This service has to be enabled for Entity Resolution and Graph use cases.	Set the value as true.
LOAD_TO_OPEN_SEARCH_ENABLED	This service has to be enabled for Entity Resolution and Graph use cases when MATCHING_MECHANISM is set to OS .	Set the value as true.
MMG_SERVICE_ENABLED	This service has to be enabled for all use cases.	Set the value as true.

2.7.6 Run the Compliance Studio Installer

This section provides information about how to install, start, restart and stop the Compliance Studio services.

The Compliance Studio application is installed with or without OFSAA, depending on the configuration provided in the `config.sh` file. The Compliance Studio application and all the interpreters are started.

After completing the Compliance Studio installation, the script displays a URL that can be used to access the Compliance Studio Application.

2.7.6.1 Trigger Installation

This section describes how to trigger installation.

For installation, you can pass argument `-i` or `--install`.

To run the Compliance Studio installer:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
2. Run the following command with a Linux user where Compliance Studio is installed:

```
./compliance-studio.sh -i
```

Or

```
./compliance-studio.sh --install
```

This will copy the whole compliance studio into the folder 'deployed' and then replaces the placeholders. Now, you can start Compliance Studio.

Note

- Run these commands only from `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin`.
- It should not be run from `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/bin`.
- Upon executing the `./compliance-studio.sh -i` command, a deployed folder is created that copies all the folders. And replaces placeholders inside the deployed folder.

Congratulations! Your installation is complete.

Note

For any help on installation commands, Run `./compliance-studio.sh --help`

3. To verify the installed patch version(s) of Compliance Studio, users can check this **FCC_COMPLIANCE_STUDIO_PATCHES** table in the Studio Schema.

2.7.6.2 Start Compliance Studio

This section describes how to start Compliance Studio.

Note

If any service fails to start, you need to wait 10 minutes to see the log file for the failure reason. After 20 minutes, the console will display the message as “Compliance Studio may have partially initiated or has encountered a startup failure,” in meantime you should not stop any activities.

- Switch to the Compliance Studio UNIX user home directory and run the user profile.
- Switch to Compliance Studio installed bin directory and run the command: `./compliance-studio.sh --start`

This will start the application and, on successful installation, will make the sensitive details blank in `config.sh`.

Note

If any of the services are not started/running and failed due to lock:

1. Log in to Studio schema.
2. Run the commands to truncate tables: `TRUNCATE TABLE DATABASECHANGELOGLOCK; TRUNCATE TABLE DATABASECHANGELOGLOCK_MMG;`
3. Log in to BD/ECM schema.
4. Run the command to truncate tables: `TRUNCATE TABLE DATABASECHANGELOGLOCK;`
5. Start the Compliance Studio.

2.7.6.3 Stop Compliance Studio

This section describes how to stop Compliance Studio.

To stop the application, you can run pass argument '-k' or '--stop'.

For example: `./compliance-studio.sh --stop`

2.7.6.4 Restart Compliance Studio

This section describes how to restart Compliance Studio.

To restart the application, you can run pass argument '-r' or '--restart'.

For example: `./compliance-studio.sh --restart`

2.8 Post-Installation

This section describes post-installation activities for Compliance Studio.

Note

After successful installation of Compliance Studio, a "deployed" folder is created and this directory is referred to as `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed`. You should not change any configurations/files outside of the deployed folder without specific instructions. If you modify configurations/files, the application may become unstable.

After successful installation of Compliance Studio, you must complete the following post-installation configurations based on the use cases.

2.8.1 Verify the Installation

This section describes how to verify the installation.

To verify the Compliance Studio installation with OFSAA, check the log files in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/logs` directory. If all the servers are up and running, it indicates that the installation is complete.

Note

If you notice any errors in the log files, do not proceed further. Contact [My Oracle Support \(MOS\)](#) provide the applicable error code and log files.

2.8.2 Access Compliance Studio Application

This section describes how to access the Compliance Studio application.

2.8.2.1 Access Compliance Studio Application when Gateway is Enabled

This section describes how to access the Compliance Studio application when Gateway is enabled.

The Compliance Studio Gateway serves as the central routing point for accessing the UI, ensuring a consistent origin for the Compliance Studio UIs. The introduction of the gateway addresses the security risks and inconsistencies by centralizing access and enhancing security.

This implementation, achieved via Spring Cloud Gateway, consolidates all UI access through a single port. By doing so, the gateway enforces security headers to mitigate clickjacking vulnerabilities. Specifically, it sets the Content Security Policy (CSP) with the frame-ancestors 'self' directive, ensuring that the UI can only be embedded within the same origin.

By default, `COMPLIANCE_STUDIO_GATEWAY_ENABLED` is set to **true** and `COMPLIANCE_STUDIO_GATEWAY_PORT` is **7071** in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/additional_config.sh` directory.

Note

Make sure that `COMPLIANCE_STUDIO_GATEWAY_PORT` and Datastudio default port should be opened in the firewall.

The Compliance Studio URL when gateway is enabled should be `https://<Hostname>:<COMPLIANCE_STUDIO_GATEWAY_PORT>/cs/home`.

Configure SAML Authentication

Note

This section is applicable only when **AUTH_REALM** is **SAML**.

To configure the SAML Authentication:

1. Navigate to the following directories:

```
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-ui/conf
```

```
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-ui/conf
```

2. Open the `application.properties` file and update port number in the following parameters:

```
saml.auth.sp.entity=https://<Hostname>:<COMPLIANCE_STUDIO_GATEWAY_PORT>/cs
```

```
saml.auth.consumerserviceurl=https://
```

```
<Hostname>:<COMPLIANCE_STUDIO_GATEWAY_PORT>/cs/home
```

For example:

```
saml.auth.sp.entity=https://<Hostname>:7071/cs
```

```
saml.auth.consumerserviceurl=https://<Hostname>:7071/cs/home
```

3. In IDCS configurations for Compliance Studio UI, update the Assertion consumer URL as `https://<Hostname>:<COMPLIANCE_STUDIO_GATEWAY_PORT>/cs/home`.

For example:

Assertion consumer URL: `https://<Hostname>:7071/cs/home`

Note

For Data Studio UI, keep the existing configuration as it is.

4. Restart the Compliance Studio services.

After restart, the Compliance Studio URL will be `https://`

```
<Hostname>:<COMPLIANCE_STUDIO_GATEWAY_PORT>/cs/home
```

2.8.2.2 Access Compliance Studio when Gateway is Disabled

This section describes how to access the Compliance Studio application when Gateway is enabled.

Note

This section is applicable only when `COMPLIANCE_STUDIO_GATEWAY_ENABLED` is set to **false** in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin/install.sh` directory.

To access the Compliance Studio UI when gateway is disabled:

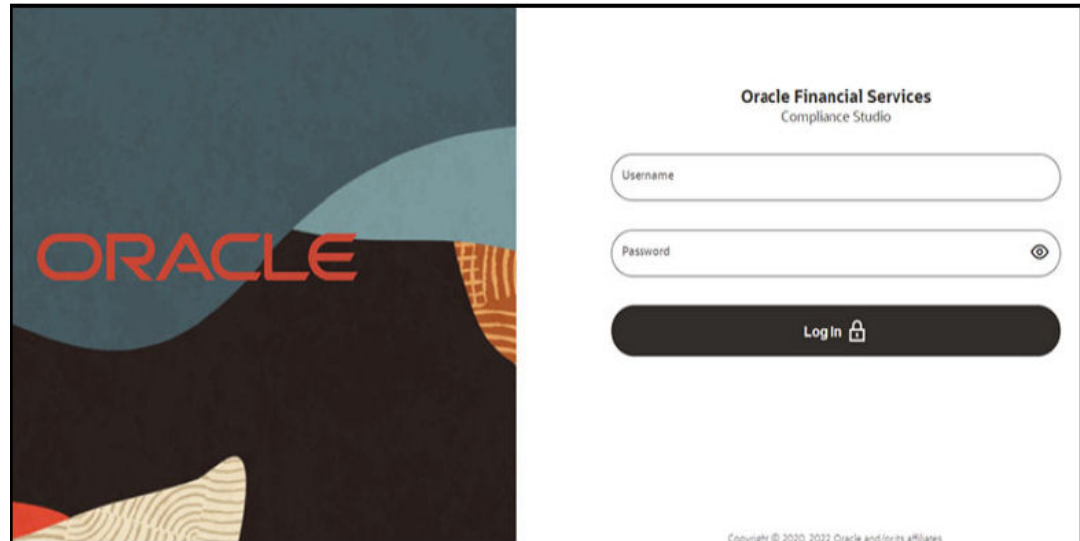
1. Enter the URL in the following format in the web browser:

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

Here, <Port_Number> is 7001 for the Compliance Studio application installed on-premise.

The Compliance Studio application login page is displayed.

Figure 2-6 Compliance Studio Application Login Page



2. Enter the Username and Password.

For Creating Users, Groups, and Mappings in AAI. See [Create Users, Groups, and Mappings](#).

3. Click **Login**.

After you access the application, you can view the ready-to-use notebooks. To check if you have been assigned any roles, create a notebook. If you cannot create a notebook, contact [My Oracle Support \(MOS\)](#).

2.8.3 Common for both Entity Resolution and Graph Use Cases

This section describes post-installation activities for both Entity Resolution and Graph use cases.

2.8.3.1 Copy Public and Private Keys

The `public.key` and `private.key` files are automatically generated by the installer and stored in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/conf` directory.

To copy the `public.key` and `private.key` files:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/conf` directory.
2. Copy the `public.key` and `private.key` files and paste them into the following directories:
 - `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/batchservice/conf`
 - `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/batchservice/conf`
3. Restart Compliance Studio.

2.8.3.2 Configure the OpenSearch Component

This section describes how to configure the OpenSearch component.

OpenSearch is a distributed search and analytics engine. Compliance Studio leverages the search feature offered by OpenSearch.

Note

- Ensure that a minimum of 4GB free RAM space is available for OpenSearch. If RAM is low, the shards of the OpenSearch fail, and the correct result is not fetched.
- You must manually clean the cache if facing a performance issue.
- **Prerequisites**
 - Download the analysis-icu and analysis-phonetic plugins. You can download the plugins from the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/opensearch` directory.
 - The Java version must be 11 and above.

To configure the OpenSearch component:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/opensearch` directory.
2. Untar the OpenSearch by executing the command: `tar -xvzf opensearch-
{<version>}.tar.gz`.
3. Install the following plugins:

```
<OPEN_SEARCH_EXTRACTED_PATH>/opensearch/opensearch-<version>/bin/  
opensearch-plugin install file:///<PATH>/analysis-icu-<version>.zip  
<OPEN_SEARCH_EXTRACTED_PATH>/opensearch/opensearch-<version>/bin/  
opensearch-plugin install file:///<PATH>/analysis-phonetic-  
<version>.zip
```

Where PATH specifies location of the plugins.

Note

- You can also install OpenSearch and the plugins on a different machine other than where the Compliance Studio is installed.
- The OpenSearch can be extracted in any directory outside the Compliance Studio path as well.

4. Navigate to the `<OPEN_SEARCH_EXTRACTED_PATH>/opensearch/opensearch-
<version>/config` directory.
5. Configure the `opensearch.yml` file with the following variables.

Table 2-12 opensearch.yml File

Interaction Variable Name	Significance
cluster.name	Indicates the name of the cluster.
node.name	Indicates the name given for the node.
path.data	Indicates the directory where you want to store the data.
path.logs	Indicates the directory where you want to store the logs.
network.host	Indicates the hostname of the machine where you want to install the OpenSearch service.
http.port	Indicates the port number where the OpenSearch service is installed.
discovery.seed_hosts	(Optional) Indicates the hostnames of the nodes of the cluster.
cluster.initial_cluster_manager_nodes	(Optional) Indicates the number given to the nodes of the cluster.

6. Configure the `jvm.options` file as follows.

Table 2-13 Configure `jvm.options` File

Interaction Variable Name	Significance
<ul style="list-style-type: none"> -Xms4g -Xmx4g 	<ul style="list-style-type: none"> Set the value for these parameters. The maximum value set can be up to 50% of the RAM size of the machine. Recommended value: Less than 32GB. <p>Note:</p> <ul style="list-style-type: none"> -Xms4g represents 4GB. The value for -Xms and -Xmx should be same.

7. After configuration changes, navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/opensearch/opensearch-<version>/bin` directory.
8. To start OpenSearch, execute the following command.
`nohup ./opensearch &`
9. To check the OpenSearch logs, execute the following command.
`tail -f nohup.out`

Enable SSL Configuration and Authentication

To enable SSL and Authentication for OpenSearch, configuration is required at both OpenSearch and Compliance Studio.

OpenSearch Configuration

To configure OpenSearch, [Download](#) the `opensearch-security` plugin zip file. For information about how to configure OpenSearch, see the [OpenSearch](#) documentation.

Compliance Studio Configuration

To configure Compliance Studio:

- Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
- Change the following property in the `config.sh` file.

```
OPEN_SEARCH_USERNAME=admin
```

3. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/ficdb/bin directory and encrypt the password (./FCCM_Studio_Base64Encoder.sh --admin) using FCCMBASEENCODER64.
4. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/opensearch/opensearch-<version>/config directory.
5. To generate the admin.p12 file, execute the following command.

```
openssl pkcs12 -export -out admin.p12 -inkey <path to/admin-key.pem> -in  
<path to/admin.pem>
```

6. To generate the ca.crt file, execute the following command.

```
openssl x509 -outform der -in <path to/admin.pem> -out ca.crt
```

7. Copy the admin.p12 file and place in the following directories.
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/load-to-open-search/conf
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/matching-service/conf
8. Copy the ca.crt file and place in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/<LOGSTASH_HOME>/config directory.
9. Configure the following parameters under **OpenSearch Cluster details** in the config.sh file.
OPEN_SEARCH_ENCRYPTED_PASSWORD='##ENCRYPTED_PASSWORD##'
OPEN_SEARCH_HTTPS_ENABLED=true
OPEN_SEARCH_TRUSTSTORE_FILE_NAME=admin.p12
OPEN_SEARCH_TRUSTSTORE_PASSWORD=password

Note

To generate an encrypted password, see [Generate an Encrypted Password for OpenSearch](#).

10. Install the Compliance Studio.

Cleanup for OpenSearch Indexes

To clean up the OpenSearch indexes, run the following command.

```
curl -XDELETE http://<FULLY QUALIFIED HOSTNAME OF STUDIO SERVER>:<PORT of  
Load To Open Search Service>/load-to-open-search/idx/deleteIndex/<INDEX NAME>
```

For example,

```
curl -XDELETE http://testserver.in.oracle.com:7053/load-to-open-search/idx/  
deleteIndex/test_index
```

Note

This command will work only if Compliance Studio is installed and all services are running.

2.8.3.3 Place admin.p12 file in the Installation Directories

This section describes how to place the `theadmin.p12` file in the installation directories.

To place the `admin.p12` file in the required locations when https is enabled for OpenSearch:

1. Copy the `admin.p12` file from the `<OpenSearch_Installation_path>/config` directory.
2. Place the `admin.p12` file in `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/matchingservice/conf` directory.
3. Place the `admin.p12` file in `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/load-to-open-search/conf` directory.

2.8.3.4 Add Synonyms and Stopword files in OpenSearch

This section describes how to add Synonyms and Stopword files in OpenSearch.

To consider the similarity when performing the OpenSearch, you can add the synonyms and stopword files in the OpenSearch.

To add synonyms and stopword files in OpenSearch:

1. Create a folder in the name of “analysis” in the `<OpenSearch_Installation_path>/config` directory.
2. You can add your synonyms and stopwords to these files and place the files in the analysis folder:
 - `Cardinal_ordinal.txt`
 - `Country.txt`
 - `Gender.txt`
 - `Namestop.txt`
 - `Name_synonym.txt`
 - `Organisation_strip.txt`
 - `Organisation_suffix.txt`
 - `Synonym.txt`
 - `Title.txt`

Note

- User can decide to provide any data in the Stopword or Synonym files.
- Each Stopword must be provided in a separate line.
- All related synonyms must be provided in the same line, separated by a comma.
- All the synonyms must be provided in the same line and ensure that there are no repetitions of the synonym. For example: rob, robi, robie, roby, robbi.

2.8.3.5 Configure Logstash

This section describes how to configure Logstash.

Logstash is a supporting software for data ingestion to the OpenSearch.

To configure logstash:

1. Navigate to **\$HOME**, which refers to the user's home directory. For example, /scratch/fccstudio/logstash-<version>.
2. Download the Logstash tar file from [here](#).
3. Untar contents of the tar file.
4. Provide this folder path for the parameter "Logstash_Home" in the config.sh file.

The Compliance Studio installer will automatically configure the Logstash properties where necessary.

Note

The ca.crt file should be copied from the open search server into the Logstash_Home/config path when https is enabled in OpenSearch.

2.8.3.6 Registering the Conda Environment

This section describes how to register the Conda environment.

Note

The User should not delete the pre-seeded conda environment.

To register the conda environment:

1. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
2. Execute the command: ./compliance-studio.sh -e or ./compliance-studio --enroll.

The Compliance Studio installer has three pre-seeded conda environments as follows:

- default_<CS Version>
- sane_<CS Version>
- ml4aml_<CS Version>

2.8.3.7 ECM Patch

This section describes the ECM patch-related information.

The following patches are required only when integrating with old versions for ECM:

- On top of ECM 8.0.8.0.0, apply the following ECM patch for ML-ECM integrations. 8.0.8.0.28 (BUG: **31497997**)
- On top of ECM 8.0.8.1.0, apply the following ECM patch for ML-ECM integrations. 8.0.8.1.4 (BUG: **33395125**)

Note

From ECM 8.1.1.0.0 and later versions, the above patches are not required for ML-ECM integrations.

- On top of ECM 8.1.2.0.0, apply the following ECM patch for ECM-IH integration. 8.1.2.0.8 (BUG: **34337520**)
- On top of ECM 8.1.2.4.0, apply the following ECM patch for ECM-IH integration. 8.1.2.4.5 (BUG: **35456951**)

2.8.4 Entity Resolution Use Case

This section describes post-installation activity for Entity Resolution use case.

2.8.4.1 Create Entity Resolution Schema

This section describes how to create the Entity Resolution schema.

Note

ER schema is nothing but FSDF schema and creation of ER schema can be skipped if the FSDF schema is already available. The grants mentioned in this section are required.

To create ER schema, create a new Oracle Database schema user using the following script:

```
CREATE USER <ER_SCHEMA_USERNAME> IDENTIFIED BY <PASSWORD>;
```

A new Oracle Database schema (ER schema) will be created.

2.8.4.2 Assign Grants for ER Schema

This section describes how to assign Grants for ER schema.

Grant the following permissions to the newly created Oracle Database ER schema:

```
GRANT CREATE SESSION TO <ER_SCHEMA_USER>;  
GRANT CREATE TABLE TO <ER_SCHEMA_USER>;  
GRANT CREATE VIEW TO <ER_SCHEMA_USER>;  
GRANT CREATE TRIGGER TO <ER_SCHEMA_USER>;  
GRANT CREATE PROCEDURE TO <ER_SCHEMA_USER>;
```

```

GRANT CREATE SEQUENCE TO <ER SCHEMA USER>;
GRANT EXECUTE ON DBMS_RLS TO <ER SCHEMA USER>;
GRANT EXECUTE ON SYS.DBMS_SESSION TO <ER SCHEMA USER>;
GRANT CREATE SYNONYM TO <ER SCHEMA USER>;
GRANT EXECUTE ON DBMS_REDEFINITION TO <ER SCHEMA USER>;
GRANT REDEFINE TABLE TO <ER SCHEMA USER>;
GRANT CREATE MATERIALIZED VIEW TO <ER SCHEMA USER>;
GRANT SELECT ON SYS.V_$PARAMETER TO <ER SCHEMA USER>;
GRANT SELECT ON SYS.DBA_FREE_SPACE TO <ER SCHEMA USER>;
GRANT SELECT ON SYS.DBA_TABLES TO <ER SCHEMA USER>;
GRANT SELECT ON SYS.DBA_TAB_COLUMNS TO <ER SCHEMA USER>;
GRANT CREATE RULE TO <ER SCHEMA USER>;
GRANT DROP TRIGGER TO <ER SCHEMA USER>;
GRANT SELECT ON SYS.DBA_RECYCLEBIN TO <ER SCHEMA USER>;
GRANT CREATE JOB TO <ER SCHEMA USER>;
GRANT EXECUTE ON DBMS_LOCK TO <ER SCHEMA USER>;
GRANT EXECUTE ON DBMS_STATS TO <ER SCHEMA USER>;
GRANT ANALYZE TO <ER SCHEMA USER>;
GRANT CREATE TYPE TO <ER SCHEMA USER>;
GRANT EXECUTE ON CTXSYS.CTX_DDL TO <ER SCHEMA USER>;

```

Note

The following grants should be revoked after the successful installation of Compliance Studio.

```

REVOKE SELECT ON SYS.DBA_RECYCLEBIN FROM <ER SCHEMA USER>;
REVOKE SELECT ON SYS.DBA_FREE_SPACE FROM <ER SCHEMA USER>;
REVOKE SELECT ON SYS.DBA_TABLES FROM <ER SCHEMA USER>;
REVOKE SELECT ON SYS.DBA_TAB_COLUMNS FROM <ER SCHEMA USER>;

```

2.8.4.3 Uploading FSDF

This section describes how to upload the FSDF data model.

Entity Resolution requires a set of pre-staging tables to be available in the OFSAA staging area and the pre-configured FSDF staging model.

The table definitions are available in terms of a data model file which can be uploaded to OFSAA with the help of AAI's Data model management.

Note

The **ER_81300.ODM** file is compatible only with **Behavior Detection version 8.1.2.9.0** and the **CSA_813** pipeline.

To upload the data model:

1. Copy ER_81300.ODM from <COMPLIANCE_STUDIO_INSTALLATION_PATH>/entityresolution/datamodels to <AAI Application Server>/<FSDF_STG_INFODOM>/ erwin/erwinXML
2. Model Upload using **JSON/Erwin XML**.

3. Select Upload Mode as **Sliced**.
4. Select **Object Registration Mode** as **Incremental Object Registration**.
5. Select **Upload File Type** as **JSON**.
6. Select the **erwin XML** or **Database XML** or **ODM** file for upload from the drop-down list.

Other options can be set to default and proceed to Upload.

For more information on uploading the Data Model, see the **Upload Business Model** section in the [OFS Analytical Applications Infrastructure User Guide](#).

2.8.4.4 Configure ER Schema Profile

This section describes how to configure the ER schema profile.

Set the SESSIONS_PER_USER limit to UNLIMITED for ER Schema:

1. Get the ER schema profile using the below query.

```
select profile from dba_users where username = '<ER_SCHEMA_USERNAME>';
```

2. Change the profile which is obtained from the step 1 using the below query.

```
ALTER PROFILE <profile> LIMIT SESSIONS_PER_USER UNLIMITED;
```

2.8.4.5 Run ER Schema in Different Workspaces

This section describes how to run the ER schema in different workspaces.

To run the ER schema in different workspaces:

1. The ER Data schema and Compliance Studio schema should be in the same wallet.
2. Update the following details for ER schema in the `resources.xml` file. The file can be found in: `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ficdb/conf`.

For example:

```
<Resource
id="ER2_CSA_ABCD"
name="jdbc/erdataschema"
auth="Container"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.OracleDriver"
url="jdbc:oracle:thin:@ER2_CSA_ABCD"
connectionProperties= "oracle.net.wallet_location
=<WALLET_PATH/ABCD>;
oracle.net.tns_admin=<WALLET_PATH/ABCD>;"
maxTotal="5"
maxIdle="0"
maxWaitMillis="-1" >
</Resource>
```

Note

Log in as either an SYS user or DBA user and grant these permissions to the ER schema created.

3. Ensure that the pre-staging and output tables are present in the given ER Data Schema.

a. The following are the pre-staging table names by version:

i. FSDf 81300:

- STG_PARTY_MASTER_PRE
- STG_PARTY_DETAILS_PRE
- STG_DELETED_PARTIES_PRE
- STG_CUSTOMER_IDENTIFCTN_DOC_PRE
- STG_ADDRESS_MASTER_PRE
- STG_PARTY_ADDRESS_MAP_PRE
- STG_PARTY_PHONE_MAP_PRE
- STG_PARTY_EMAIL_MAP_PRE
- FCC_ER_MAPPING
- FCC_ER_MANUAL_MAPPING

b. The following are the output table names by version:

i. FSDf 81300:

- STG_PARTY_MASTER
- STG_PARTY_DETAILS
- STG_PARTY_EMAIL_MAP
- STG_ADDRESS_MASTER
- STG_PARTY_ADDRESS_MAP
- STG_PARTY_PHONE_MAP
- STG_CUSTOMER_IDENTIFCTN_DOC
- FCC_ER_MAPPING
- FCC_ER_OUTPUT

2.8.5 Graph Use Case

This section describes post-installation activity for the Graph Use Case.

2.8.5.1 Importing OOB Graph Definition and related Metadata

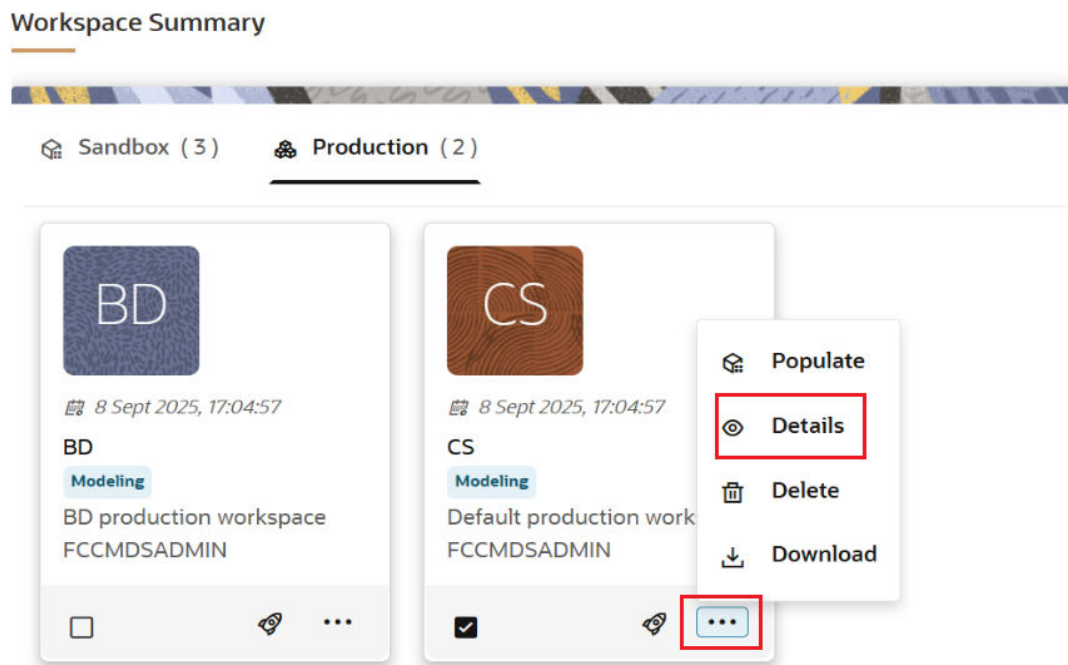
This section describes how to import OOB Graph Definition and its related Metadata.

Creating Graph Data Store

To create a data store for the graph:

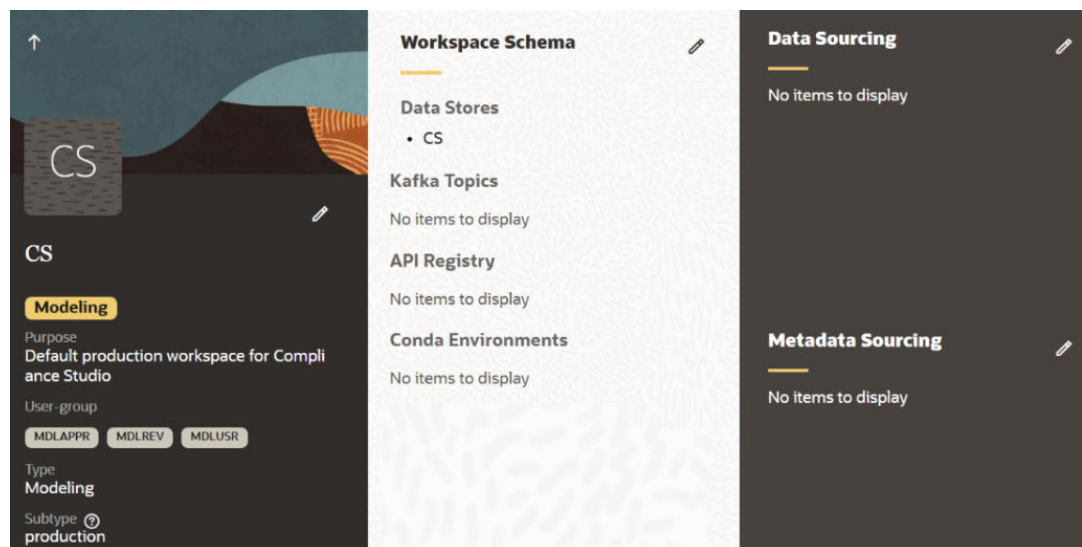
1. Log in to the Compliance Studio UI. The Workspace Summary page is displayed.

Figure 2-7 Workspace Summary



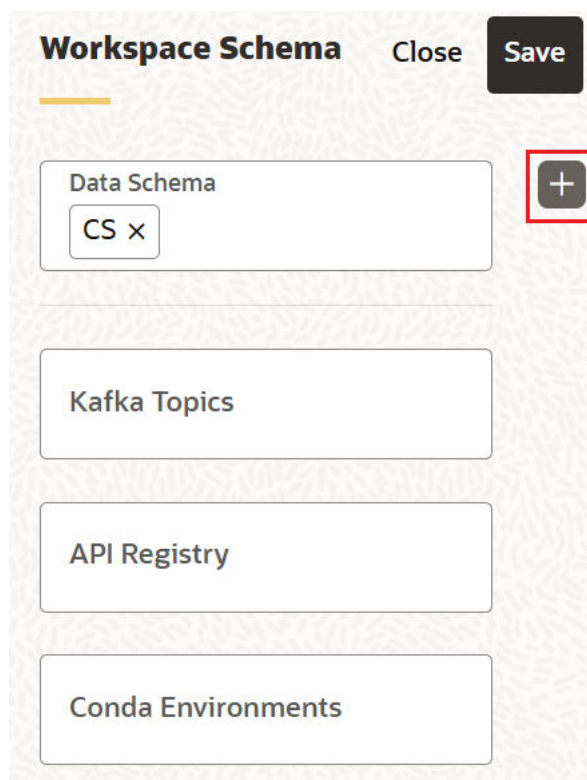
2. Click **Action** icon and then select **Details**. The Edit Workspace page is displayed.

Figure 2-8 Edit Workspace



3. In the Workspace Schema, click **Edit** icon. The Edit Workspace Schema pane is displayed.

Figure 2-9 Edit Workspace Schema

**Note**

By default, Studio Schema is mapped to the workspace and you need to map Graph Schema and Graph Data Store respectively for using graph functionality.


4. Click **Create Data Store**  The **Add Data Store** pane is displayed.

Figure 2-10 Add Data Store

Add Data Store

Data Store Name Required

Description Required

File Availability
JDBC

Database Type
Oracle

Wallet Alias Required

Table Owner

Additional Properties ⓘ

JDBC Connection String

User Name Password ⓘ

Test Connection Cancel Create

5. Enter **Data Store Name** and **Description** for the graph schema.

Note

Retain default settings in the **File Availability** and **Database Type** drop-down lists.

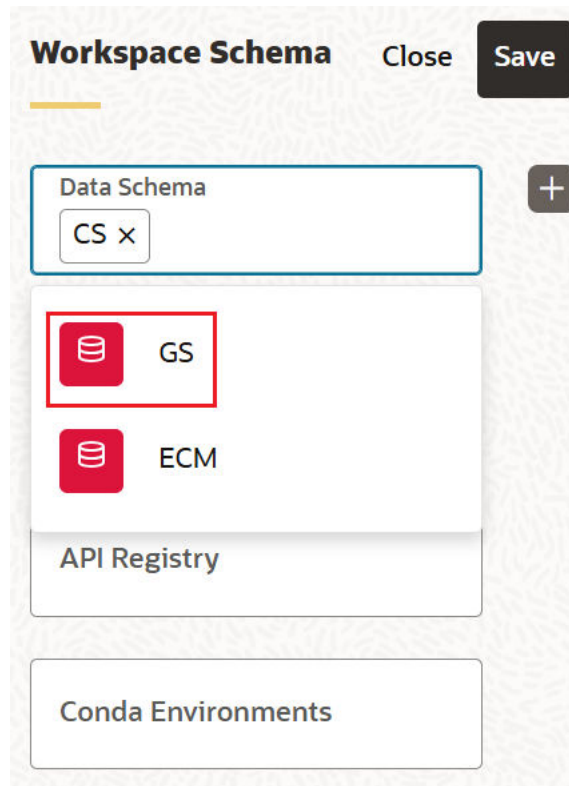
6. Enter the **Wallet Alias**.
7. Enter the Oracle Database schema name in the **Table Owner**.

Note

The **JDBC Connection String**, **User Name**, and **Password** fields are optional.

8. Click **Test Connection**. A **Success** confirmation message is displayed.
9. Click **Create**. The Data Store is created successfully.

Figure 2-11 Data Schema



10. From the **Data Schema** drop-down list, Select the **Graph Data Store**.
11. Click **Save**. The data store for the graph is saved successfully in the CS workspace.
12. Click **Close** to exit the process.

Note

If you are planning to use the OOB graph "FINANCIAL_CRIME_GLOBAL_GRAPH" based on the ECM data model or "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" based on the BD data model, then create the additional data store.

For "FINANCIAL_CRIME_GLOBAL_GRAPH," create the additional data store for ECM's Atomic Schema. This will be required later in the schedule part.

For "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION," create the additional data store for BD's Atomic Schema. This will be required later in the schedule part.

Importing OOB Graphs

Note

- If you want to import both graphs, execute the command: `./importGraph.sh`
- If you need any help about graphs, execute the command: `./importGraph.sh -h`

To import the OOB graphs:

1. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ficdb/graphmetadata/bin` directory.
2. If **ENABLE_MATCHING_FOR_GRAPH** parameter is set to "false" in the `config.sh` file, then import the graph as follows:

- a. If you are importing "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" OOB graph, then execute the following.

```
./importGraph.sh -b
```

- b. If you are importing "FINANCIAL_CRIME_GLOBAL_GRAPH" OOB graph, then execute the following.

```
./importGraph.sh -e
```

3. If **ENABLE_MATCHING_FOR_GRAPH** parameter is set to "true" in the `config.sh` file, then import the graph as follows:

- a. If you are importing "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" OOB graph with matching component enabled, then execute the following.

```
./importGraph.sh -b
```

(OR)

If you are importing "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" OOB graph with matching component disabled, then execute the following.

```
./importGraph.sh -b -sm
```

- b. If you are importing "FINANCIAL_CRIME_GLOBAL_GRAPH" OOB graph with matching component enabled, then execute the following.

```
./importGraph.sh -e
```

(OR)

If you are importing "FINANCIAL_CRIME_GLOBAL_GRAPH" OOB graph with matching component disabled, then execute the following.

```
./importGraph.sh -e -sm
```

Note

If you want to import both the graphs with matching component disabled, then execute the following.

```
./importGraph.sh -sm
```

The OOB graphs are imported to the Compliance Studio UI.

Registering Graph Data Store

To register graph data store:

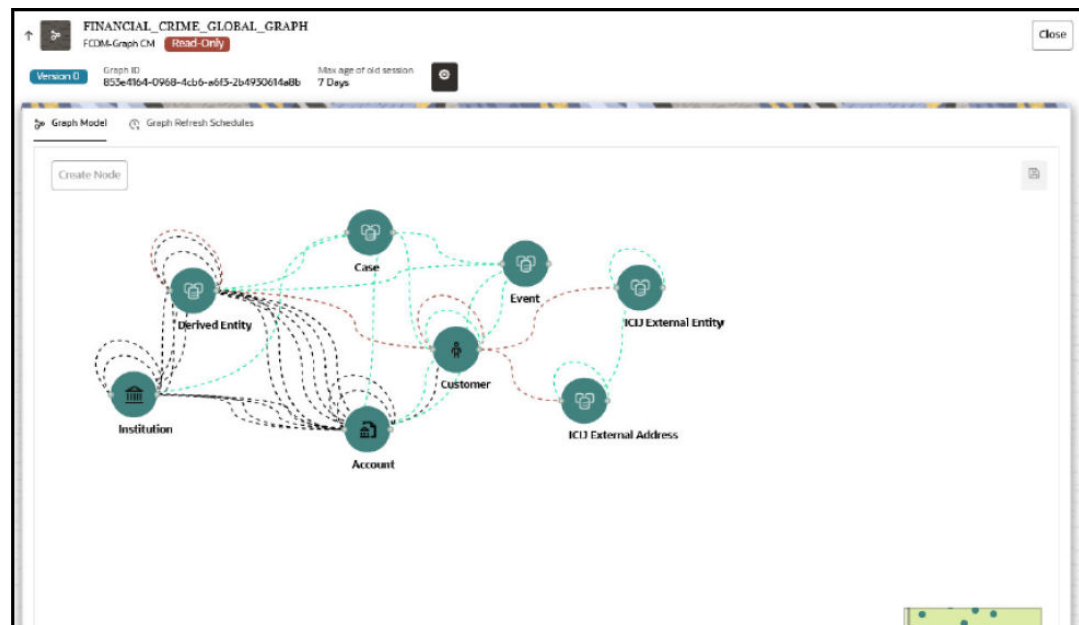
1. Log in to the Compliance Studio and navigate to the workspace summary.
2. On the **Modeling** menu, click **Graphs**. The Graph Summary page is displayed.

Figure 2-12 Graph Summary

Name	Number of Nodes	Number of Edges	Owner	Created Date	Action
FINANCIAL_CRIME_GLOBAL_GRAPH FCDM-Graph CM	8	39	MMGUSER	Apr 17, 2023, 5:02:26 PM	...
TEST_FINANCIAL_CRIME_GLOBAL_GRAPH FCDM-Graph CM	8	39	MMGUSER	Apr 17, 2023, 5:02:26 PM	...

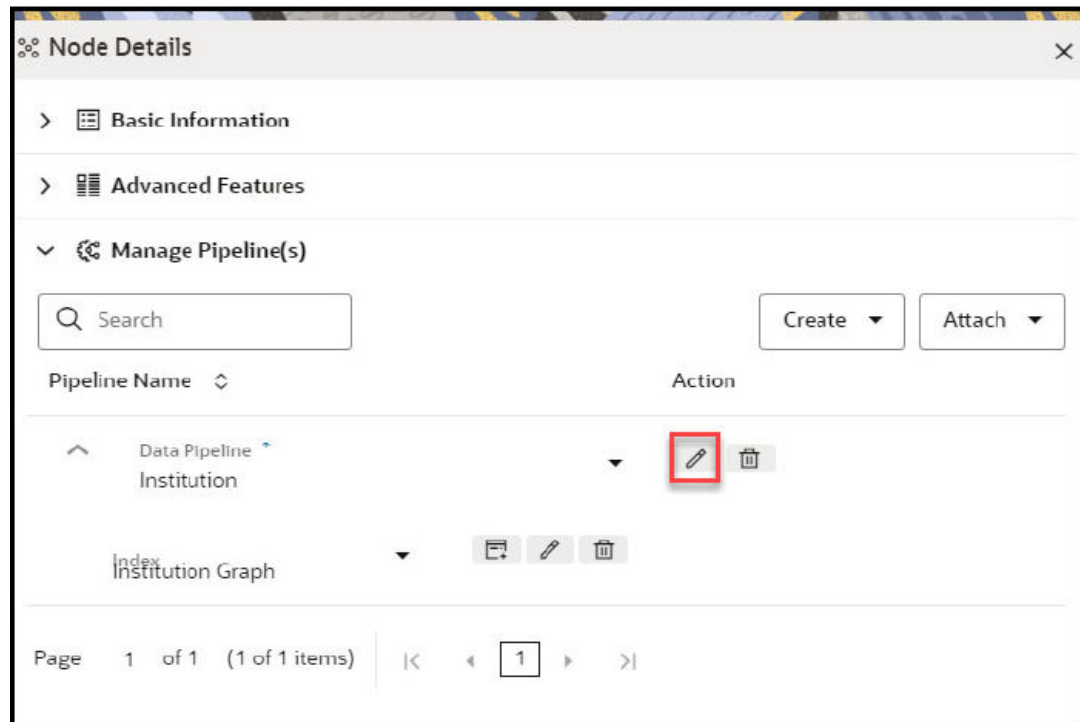
3. Select the appropriate graph, click **Action** icon **...** and select **Edit** to view the graph.

Figure 2-13 Graph Model



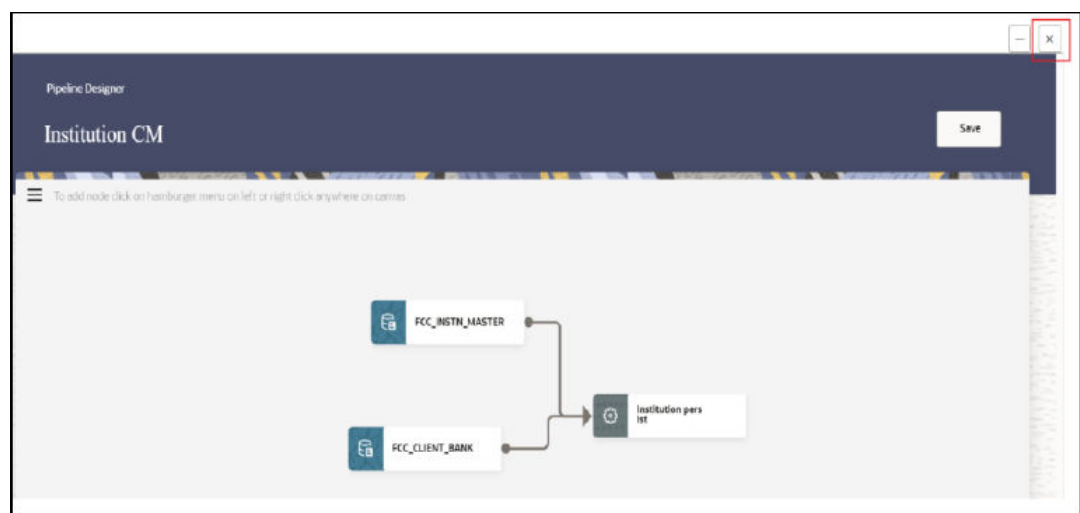
- To edit the Node, hover over the **Node** icon and click **Edit**. The Node Details page is displayed.

Figure 2-14 Node Details



- Expand Manage Pipeline(s) and click **Edit** icon on the data pipeline to view the Pipeline Designer page.

Figure 2-15 Pipeline Designer Page



- You need to wait for the UI to load, **Close** Pipeline Designer page and then **Close** the graph panel.

Initializing Metadata Indexes

① Note

Before executing the script, OpenSearch should be up and running.

To initialize metadata indexes:

1. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ficdb/graphmetadata/bin` directory.
2. Execute the following.

```
./CreateMetadataIndexes.sh
```

The metadata indexes will be created.

① Note

- If the **ENABLE_MATCHING_FOR_GRAPH** parameter is set to "false" in the `config.sh` file, then skip the **Step 2**.
- Before executing the command, if metadata indexes are available for OpenSearch, then it will not be updated until `F_IS_RECENTLY_CHANGED` column values are set to "Y" in the `FCC_IDX_M_LOOKUP` table.

Initializing Schemas

To initialize schemas:

1. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ficdb/graphmetadata/bin` directory.
2. If you are using "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" OOB graph, then execute the following.

```
./InitializeBDSchema.sh -bdw <bd_atomic_wallet_alias>
```

3. If you are using "FINANCIAL_CRIME_GLOBAL_GRAPH" OOB graph, then execute the following.

```
./InitializeECMSchema.sh -w <ecm_schema_wallet_alias>
```

4. To initialize graph schema based on the selected OOB graphs, execute the following.

- For initializing `FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION`,

```
./InitializeGraphSchema.sh -gw <graph_wallet_alias> -bs <bd_schema_name>
```

- For initializing `FINANCIAL_CRIME_GLOBAL_GRAPH`,

```
./InitializeGraphSchema.sh -gw <graph_wallet_alias> -es  
<ecm_schema_name>
```

- For initializing FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION and FINANCIAL_CRIME_GLOBAL_GRAPH in the **same** graph schema,

```
./InitializeGraphSchema.sh -gw <graph_wallet_alias> -es  
<ecm_schema_name> -bs <bd_schema_name>
```

Starting OpenSearch

To start OpenSearch:

1. Navigate to the <OPEN_SEARCH_EXTRACTED_PATH>/opensearch/opensearch-<version>/bin directory.
2. Execute the following.

```
nohup ./opensearch &
```

Note

To check the OpenSearch logs, execute the command - tail -f nohup.out.

Initializing OOB Graph Batch Schedules

Note

If you want help on the graph batch schedule, then execute the following commands:

- ./InitializeOOBGraphBatchScheduleECM.sh -h
- ./InitializeOOBGraphBatchScheduleBD.sh -h

To initialize OOB graph batch schedules:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ficdb/graphmetadata/bin directory.
2. If **ENABLE_MATCHING_FOR_GRAPH** parameter is set to "false" in the config.sh file, then initialize the graph batch schedule as follows:
 - a. If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" schedule, then execute the following.

```
./InitializeOOBGraphBatchScheduleBD.sh -bw <datasource name of the BD  
atomic schema> -s <start_date> -e <end_date> -gd <graph_datasource> -u  
<complianceStudioUserName> -sm
```

Note

The Data source value for BD atomic schema should be in exact same case where it was created while editing workspace from the UI.

- b. If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH" schedule, then execute the following.

```
./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM  
atomic schema> -sdg <Start-day-gap> -edg <End-day-gap> -u  
<complianceStudioUserName> -sm
```

Note

The Data source value for ECM atomic schema should be in exact same case where it was created while editing workspace from the UI.

The dates present in the batch schedule are only used to filter transaction edges. All the nodes are considered irrespective of the dates, and the dates are used to control the volume of transactions to be processed in a batch.

For example, if a customer has millions of transactions for each date, then instead of one batch that processes the complete date range, they can execute multiple batches in slices (let's say 3 months) for better performance, monitoring, and less resource constraint, etc.

By default, the graph has a retention period of 1 year which means transactions with a date older than 1 year will be ignored by the graph. So, if you want all the older transactions in the graph, then edit the OOB graph and update the retention period of transaction edges (pluggable edges) accordingly before executing the graph batch.

3. If **ENABLE_MATCHING_FOR_GRAPH** parameter is set to "true" in the `config.sh` file, then initialize the graph batch schedule as follows:
- a. If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" schedule with matching component enabled, then execute the following.

```
./InitializeOOBGraphBatchScheduleBD.sh -bw <datasource name of the BD  
atomic schema> -s <start_date> -e <end_date> -gd <graph_datasource> -u  
<complianceStudioUserName>
```

(OR)

If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH_BEHAVIOUR_DETECTION" schedule with matching component disabled, then execute the following.

```
./InitializeOOBGraphBatchScheduleBD.sh -bw <datasource name of the BD  
atomic schema> -s <start_date> -e <end_date> -gd <graph_datasource> -u  
<complianceStudioUserName> -sm
```

Note

The Data source value for BD atomic schema should be in exact same case where it was created while editing workspace from the UI.

- b. If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH" schedule with matching component enabled, then execute the following.

```
./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM  
atomic schema> -gd <graph_datasource> -sdg <Start-day-gap> -edg <End-  
day-gap> -u <complianceStudioUserName>
```

(OR)

If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH" schedule with matching component disabled, then execute the following.

```
./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM  
atomic schema> -gd <graph_datasource> -sdg <Start-day-gap> -edg <End-  
day-gap> -u <complianceStudioUserName> -sm
```

Note

The Data source value for ECM atomic schema should be in exact same case where it was created while editing workspace from the UI.

Auto Scheduling of Transactional Tasks in the Graph Batch

This section explains how to set up batch deltas to run for a specified period of time relative to the system date.

If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH" schedule with matching component enabled, then execute the following command.

```
./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM  
atomic schema> -sdg <Start-day-gap> -edg <End-day-gap> -gd <graph_datasource>  
-u <complianceStudioUserName>
```

The sample scripts for Weekly, Monthly, Yearly and, Periodically is given in the following table.

Table 2-14 Schedule Transactional Task

Batch Schedule	Sample Script
Weekly (7 Days)	<pre>./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM atomic schema> -sdg 7 -edg 0 -gd <graph_datasource> - u<complianceStudioUserName></pre> <p>For example, SYSDATE/ Current Date is 20/12/24 and you need to load one week data then use the following logic.</p> <p>Start Day Gap: 2024_12_20 - 7 = 2024_12_13</p> <p>End Day Gap: 2024_12_20 - 0 = 2024_12_20</p> <p>The transaction data from 2024_12_13 (12:00:00 AM) to 2024_12_19 (11:59:59 PM) will be considered for processing. As 2024_12_20 is the current date, complete data for the same date is not yet available in the Banking Domain for processing.</p>
Monthly (30 Days)	<pre>./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM atomic schema> -sdg 30 -edg 0 -gd <graph_datasource> -u <complianceStudioUserName></pre>
Yearly (365 Days)	<pre>./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM atomic schema> -sdg 365 -edg 0 -gd <graph_datasource> -u <complianceStudioUserName></pre>
Periodically	<pre>./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM atomic schema> -sdg 21 -edg 1 -gd <graph_datasource> -u <complianceStudioUserName></pre> <p>For example, Suppose today's date is 2024_12_20 and users want to load data from 2024_11_29 to 2024_12_18 (both dates are inclusive).</p> <p>You are running a batch on 2024_12_20, therefore end-day-gap should be given as edg=1 and start-day-gap should be given as -sdg=21 where number of days between two dates is 22.</p>

If you are initializing "FINANCIAL_CRIME_GLOBAL_GRAPH" schedule with matching component disabled, then execute the following command.

```
./InitializeOOBGraphBatchScheduleECM.sh -ew <datasource name of the ECM
atomic schema> -gd <graph_datasource> -sdg <Start-day-gap> -edg <End-day-gap>
-u <complianceStudioUserName> -sm
```

Start the PGX Service

To start the PGX service:

1. Navigate to the <PGX_INSTALLATION_PATH>/pgx/pgx-server/bin directory.

2. Execute the following.

```
./pgx-server.sh -s
```

The PGX service is up and running.

Note

To verify if PGX service is up, check the logs.

2.8.5.2 Assign Post-installation Grants for Graph Schema

This section describes how to assign the post-installation Grants for Graph schema.

Grant the following permissions to the newly created Graph schema.

- **Post-installation Grants for BD Graph**

```
GRANT EXECUTE ON <BD_ATOMIC_SCHEMA>.P_FCC_CS_BD_EXTERNAL_ENTITY TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.FCC_CS_BD_EXTERNAL_ENTITY TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <BD_ATOMIC_SCHEMA>.FCC_CS_BD_DERIVED_GROUP TO
<GRAPH_SCHEMA>;
```

- **Post-installation Grants for ECM Graph**

```
GRANT EXECUTE ON <ECM_ATOMIC_SCHEMA>.P_FCC_CS_CM_EXTERNAL_ENTITY TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CS_CM_EXTERNAL_ENTITY TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <ECM_ATOMIC_SCHEMA>.FCC_CS_CM_DERIVED_GROUP TO
<GRAPH_SCHEMA>;
GRANT DELETE ON <ECM_ATOMIC_SCHEMA>.FCC_GRAPH_M_TRXN_VIEWS TO
<GRAPH_SCHEMA>;
```

- **Post-installation Grants for both BD and ECM Graphs**

```
GRANT SELECT, INSERT, UPDATE, DELETE ON
<STUDIO_SCHEMA>.FCC_GRAPH_M_TRXN_VIEWS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.FCC_M_TABLES TO <GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.FCC_M_COLUMNS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.FCC_M_ATTRIBUTE TO <GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.FCC_M_ATTRIBUTE_COLUMN_MAP TO
<GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.FCC_M_COLUMNS_DETAILS TO <GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.FCC_M_MAP TO <GRAPH_SCHEMA>;
GRANT SELECT ON <STUDIO_SCHEMA>.MMG_GRAPH_SCHEMA TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON SYS.DBMS_LOCK TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON CTXSYS.CTX_DDL TO <GRAPH_SCHEMA>;
GRANT EXECUTE ON CTX_THES TO <GRAPH_SCHEMA>;
```

2.8.5.3 Add the Studio Service (SSL) to PGX Configuration

This section describes how to add the Studio Service (SSL) to PGX configuration.

Adding the Studio Service (SSL) to PGX Trust Store facilitates you to apply redaction on the graph batch service and connect with PGX.

To add the Studio Service to PGX Trust Store, copy the .p12 file from <Compliance_Studio Installation_path>/mmg-studio/conf directory to the <PGX Server path>/pgx-server/conf directory.

After generating the .p12 file and adding the Studio service to the PGX trust store.

2.8.5.4 Generate the graph-keystore.p12 File

This section describes how to generate the graph-keystore.p12 file.

Note

Before creating the graph-keystore.p12 file, ensure that the graph service is up and running.

To generate the graph-keystore.p12 file:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-load-to-graph/graph-service/utility/bin directory.
2. Execute the command: ./CreatePasswordlessKeystore.sh.
3. Enter the following values:
 - a. **Wallet Alias:** Enter the wallet alias of graph schema.
 - b. **Password:** Enter the graph schema password.
 - c. **Keystore Alias:** Enter an alias name for keystore.
4. The graph-keystore.p12 file is generated and available in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-load-to-graph/graph-service/conf directory.
5. Copy the graph-keystore.p12 file and place in the <PGX_HOME>/pgx/pgx-server/conf directory.

Note

- If you do not have any graph schema then create an empty file with a name "graph-keystore.p12" and place it in the <PGX_HOME>/pgx/pgx-server/deployed/conf directory.
- The path where the pgx-server-<version>.zip file is unzipped is referred as <PGX_HOME>.
- If you are updating credentials then copy the updated graphkeystore.p12 file and place in the <PGX_HOME>/pgx/pgxserver/conf directory.

2.8.5.5 Configure the PGX Service

This section describes how to configure the PGX service.

PGX (Parallel Graph AnalytiX) is a graph toolkit from Oracle that provides graph analysis on large scale graphs, to extract insights hidden in the connections across datasets between entities. Using built-in and custom graph algorithms, graph-pattern matching queries, and other enhanced graph analytics features, PGX helps investigators in conducting meaningful investigations and making actionable recommendations.

PGX service can be configured on the same server where Compliance Studio is installed or on a different server.

To install PGX service:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/pgx/pgx-server/` directory.
2. Perform the following:
 - If PGX service is to be installed on the same server where Compliance Studio is installed, extract the `pgx-server-<version>.zip` file.
 - If PGX service is to be installed on a different server:
 - Copy the `pgx-server-<version>.zip` file to the PGX server
 - Extract the `pgx-server-<version>.zip` file
3. Navigate to the `<PGX_HOME>/pgx-server/conf` directory and copy the following files:
 - `studio_server.pl2`
 - `graph-keystore.pl2`
 - `public.key`

Note

If applicable, configure the following properties.

In the `server.conf` file, configure the following properties:

- `enable_tls: false`
- `enable_client_authentication: false`
- The property value is true by default, which means that the SSL certificate is enabled and recommended. Change to false only if you do not have the SSL certificate enabled.

4. Navigate to the `<PGX_HOME>/pgx-server/bin` directory and configure the `config.sh` file as described in the following table.

Table 2-15 Config.sh file for PGX

Interaction Variable Name	Significance
PGX_SERVER_OFF_HEAP_MB	Indicates the maximum off-heap memory size in megabytes (mainly used for storing graphs except for their string properties) that PGX tries to respect. Recommended Value: 42% of the PGX server memory limit size above.
PGX_SERVER_ON_HEAP_MB	Indicates the maximum and minimum heap memory size (mainly used for storing graphs' string properties) for the Java process of PGX. Recommended Value: 58% of the PGX server memory limit size above.
PGX_SERVER_YOUNG_SPACE_MB	Indicates the amount of young space (new space) configured for the java heap.
GRAPH_SERVICE_URL	It indicates external service configuration where the Graph service is available. For example: https://<Compliance Studio fully qualified hostname>:7059/graph-service
GRAPH_KEYSTORE_PASSWORD	Indicates the password of the keystore file, which stores the password of the graph schemas.
PGX_SERVER_SSL_ENABLED	By default, the property value is true which means the SSL certificate is enabled and recommended. Note: Change it to false only if you do not required the SSL certificate.
PGX_SERVER_KEYSTORE_ALIAS	It indicates the alias name provided when generating a self- signed server keystore for PGX.
PGX_SERVER_KEYSTORE_FILE_PATH	It indicates the absolute path of the <code>server_keystore.jks</code> file, which is generated during Generating a Self-Signed Server Keystore for PGX.
PGX_SERVER_KEYSTORE_PASSWORD	It indicates the password created while generating a Self- signed server keystore for PGX.
SHUTDOWN_GRACE_PERIOD	It indicates the grace period in minutes for the graceful shutdown of the PGX Server. To set value, uncomment and set the value. Note: <ul style="list-style-type: none"> The value should be an integer. If the value is less than 1, then force shutdown is triggered immediately.

Note

You can generate the `graph-keystore.p12` file after starting the Compliance Studio.

5. Navigate to the `<PGX_Installation_Path>/pgx-server/bin` directory and run any one of the following commands:

- ```
./pgx-server.sh -install
```
- Or
- ```
./pgx-server.sh -i
```
6. Start the PGX service.
To start the PGX service:
 - a. Navigate to the path where the PGX service is installed.
 - b. Navigate to the following directory where the start service for PGX is located:
`<PGX_Installation_Path>/pgx-server/bin`
 - c. Run any one of the following commands:

```
./pgx-server.sh --start
```

Or

```
./pgx-server.sh -s
```

Figure 2-16 PGX start service

```
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.apache.logging.slf4j.Log4jLoggerFactory]
Oct 08, 2021 11:01:34 AM org.apache.coyote.AbstractProtocol init
INFO: Initializing ProtocolHandler ["http-nio-7007"]
Oct 08, 2021 11:01:34 AM org.apache.catalina.core.StandardService startInternal
INFO: Starting service [Tomcat]
Oct 08, 2021 11:01:34 AM org.apache.catalina.core.StandardEngine startInternal
INFO: Starting Servlet engine: [Apache Tomcat/9.0.44]
Oct 08, 2021 11:01:37 AM org.apache.catalina.startup.ContextConfig getDefaultWebXmlFragment
INFO: No global web.xml found
Oct 08, 2021 11:01:54 AM org.apache.jasper.servlet.TldScanner scanJars
INFO: At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this l
g unneeded JARs during scanning can improve startup time and JSP compilation time.
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/tmp/pgx_server7325961773484200210/ROOT/WEB-INF/lib/log4j-slf4j-
SLF4J: Found binding in [jar:file:/tmp/pgx_server7325961773484200210/ROOT/WEB-INF/lib/log4j-slf4j-
SLF4J: Found binding in [jar:file:/tmp/pgx_server7325961773484200210/ROOT/WEB-INF/lib/log4j-slf4j-
SLF4J: Found binding in [jar:file:/tmp/pgx_server7325961773484200210/ROOT/WEB-INF/lib/log4j-slf4j-
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.apache.logging.slf4j.Log4jLoggerFactory]
Oct 08, 2021 11:02:20 AM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-nio-7007"]
```

7. Stop the PGX service.
To stop the PGX service, run any one of the following commands:

```
./pgx-server.sh --stop
```

Or

```
./pgx-server.sh -k
```
8. Force Stop the PGX service.
To force stop the PGX service, run any one of the following commands:

```
./pgx-server.sh --force-stop
```

Or

```
./pgx-server.sh -f
```
9. Restart the PGX service.
To restart the PGX service, run any one of the following commands:

```
./pgx-server.sh --restart
```

Or

```
./pgx-server.sh -r
```

10. Reinstall PGX service with updated configuration.

To update configuration in PGX service in case of wrong configuration, run any one of the following commands:

```
./pgx-server.sh --update
```

Or

```
./pgx-server.sh -u
```

2.8.5.6 Generating Certificate for PGX Server

This section describes how to generate certificates for PGX server.

We recommend getting a certificate issued by a certificate authority (CA), which is trusted by your organization for the Linux server where the PGX server will be installed. If a CA certificate is not available, then generate it.

Generating a Self-Signed Server Keystore

To generate a self-signed server keystore:

1. Execute the following command.

```
keytool -genkey -alias pgx -keyalg RSA -keystore server_keystore.jks
```

2. Provide the requested details.
For example:

Enter keystore password:

Re-enter new password:

What is your first and last name?

[Unknown]: my.hostname.domain.com

What is the name of your organizational unit?

[Unknown]: OU What is the name of your organization?

[Unknown]: MyOrganization What is the name of your City or Locality?

[Unknown]: MyTown What is the name of your State or Province?

[Unknown]: MyState What is the two-letter country code for this unit?

[Unknown]: US

Is CN= my.hostname.domain.com, OU=OU, O=MyOrganization, L=MyTown, ST=MyState, C=US correct?

[no]: yes

Configuring PGX Server

Users need to update `config.sh` file for configuring the PGX server. For more information, see the [Configure the PGX Service](#) section.

Trust Compliance Studio's SSL Certificate

To trust Compliance Studio's SSL certificate:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgstudio/conf directory.
2. Obtain the Compliance Studio's SSL certificate, "studio_server.pl2".
3. Import the generated certificate to JAVA CA certs by executing the following command.

```
keytool -importcert -keystore $JAVA_HOME/lib/security/cacerts -storepass  
changeit -alias studio_server -file <ca_cert_dir>/studio_server.cer
```

Note

Replace <keystore path> with the absolute path of "studio_server.pl2" and replace <ca_cert_dir> with the directory where studio_server.cer should be generated.

Configuring Compliance Studio Server

Users need to trust PGX Server's certificate for configuring the Compliance Studio server.

Trust PGX Server's Certificate

To trust PGX Server's certificate:

1. Copy "ca_certificate.pem" from the PGX server to the Compliance Studio server.
2. Import the copied certificate to the java ca certs by executing the following command.

```
keytool -import -trustcacerts -keystore $JAVA_HOME/lib/security/cacerts  
-storepass changeit -alias pgx -file /path/of/ca_certificate.pem -  
noprompt
```

Note

Replace /path/of/ca_certificate.pem with the path where the certificate is copied.

3. If the PGX server keystore is generated, copy "server_keystore.jks" from the PGX server to the Compliance Studio server.
4. Import the copied keystore to the java ca certs by executing the following command.

```
keytool -importkeystore -srckeystore /path/of/server_keystore.jks -  
destkeystore $JAVA_HOME/lib/security/cacerts -deststorepass changeit -  
srcstorepass <keystore password> -noprompt
```

Note

Replace `<keystore password>` with the password generated while creating the PGX server keystore.

5. Update the PGX URL to set it as “https” using the following steps:
 - a. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
 - b. Open the `config.sh` file and update the “PGX_SERVER_URL” as `https://<FQDN of PGX Server>:7007`
 - c. Reinstall Compliance Studio with updated configuration.
(OR)
To Update the PGX URL in an alternative way as follows:
 - a. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgload-to-graph/graph-service/conf` directory.
 - b. Open the `application.yml` file and update the PGX_SERVER_URL.
 - c. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgstudio/server/builtin/interpreters` directory.
 - d. Open the `pgx.json` and update the PGX URL in the PGX interpreter’s JSON file.
 - e. Restart Compliance Studio.

3

Reinstall Compliance Studio with Updated Configuration

This section provides information about reinstall Compliance Studio with updated configuration settings when an incorrect configuration was applied or when new configuration details need to be implemented in the existing setup.

To reinstall Compliance Studio with updated configuration:

1. Stop Compliance Studio. To stop, execute the following command:
2. Update the `config.sh` file. Do not forget to reconfigure the sensitive details which were removed earlier.
3. To update configuration in the application, you can pass argument '-u' or '--update'

```
./compliance-studio.sh --stop
```

```
./compliance-studio.sh --update
```

Once reinstallation is done, you can start the application.

4

Frequently Asked Questions (FAQs) and Error Dictionary

This section consists of resolutions to the frequently asked questions and error codes noticed during the Compliance Studio installation.

The Compliance Studio installer performs all the pre-requisite validation checks during installation. Any error encountered in the process is displayed with an appropriate Error Code. You can refer to the Error Dictionary to find the exact cause and resolution to rectify the error.

4.1 Frequently Asked Questions in Compliance Studio

This section describes the Frequently Asked Questions (FAQs) in Compliance Studio.

You can refer to the Frequently Asked Questions, which are developed with interest to help you resolve some of the Compliance Studio Installation and Configuration issues. This intends to share problem resolution knowledge to a few of the known issues. This is not an official support document and just attempts to share problem resolution knowledge to a few known issues.

1. Why does my console show an unsuccessful message during wallet creation?

You can check if you have run the following commands correctly.

For more information on wallet creation, see [Setup Password Stores with Oracle Wallet](#).

- a. `mkstore -wrl <wallet_location> -create` //creates a wallet in the specified location.
- b. `mkstore -wrl <wallet_location> -createCredential <alias-name> <database-user-name>` //creates an alias in the studio schema.
- c. `mkstore -wrl <wallet_location> -createCredential <alias-name> <database-user-name>` //creates an alias in the atomic schema.
- d. `mkstore -wrl <wallet_location> -createCredential <alias-name> <database-user-name>` //creates an alias in the config schema.

If your issue is still not resolved, contact [My Oracle Support \(MOS\)](#).

2. Where can I find my created wallet?

Your wallet will be in the directory you have set as your wallet location.

If your issue is still not resolved, contact [My Oracle Support \(MOS\)](#).

3. When should I create a Database link, and if yes, how do I do it?

Create a Database link to connect the Atomic and Config database schemas to the Studio database schema if the databases are different. You must create the link in the Studio database.

In the following example, a link has been created from the config schema to the atomic schema by running the following script:

```
create public database link <studio database link>
connect to <Config Schema>
```



```

identified by password
using ' (DESCRIPTION = ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST
=<host name> (PORT = <port number>)) (CONNECT_DATA = (SERVICE_NAME =
<service name>))) ' ;
Config schema : <Config Schema>/password
' (DESCRIPTION = ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST =<host
name> (PORT = <port number>)) (CONNECT_DATA = (SERVICE_NAME = <service
name>))) ' ;

```

After running the script, run the FCDM connector and ICIJ connector jobs.

4. Why does my installed studio setup not have any notebooks?

Some default notebooks are ready to use when you install Compliance Studio. If you do not see any notebooks when you log in to the application, you may not be assigned any roles.

Check the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/logs directory to see if you have been assigned any roles, and if not, contact your administrator.

If your issue is still not resolved, contact [My Oracle Support \(MOS\)](#).

5. What can I do if the schema creation fails?

If the Atomic schema creation fails, login to the BD and ECM Atomic schemas and run the following query:

```
select * from fcc_orahive_datatypemapping;
```

The fcc_orahive_datatypemapping table must not have duplicate data types.

If the Compliance Studio schema creation fails, login as a Studio user and run the following query:

```
select * from fcc_datastudio_schemaobjects
```

Run the following query to replace all Y values with "":

```
update fcc_datastudio_schemaobjects set SCHEMA_OBJ_GENERATED=''
```

After the schema creation is successful, the value of the SCHEMA_OBJ_GENERATED attribute changes to Y.

You can also check for errors in the application log file in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/logs directory.

If your issue is still not resolved, contact [My Oracle Support \(MOS\)](#).

6. What can I do if the Import_training_model batch execution fails?

Batch execution status always displays success in case of success or failure.

You can also check for errors in the application log file in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/logs directory.

According to the log details, you can fix the failure and rerun the same batch.

7. Why is the PGX Server not starting?

The PGX server starts only after the FCDM tables are created after the FCDM connector job is run. Check if all FCDM tables are created, and start the PGX server.

You can also check for any errors in the application log file in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/logs directory.

If your issue is still not resolved, contact [My Oracle Support \(MOS\)](#).

8. What should I do if there is a below Error while selecting edges in manual DecisionUI?

```

java.lang.IllegalStateException: Unable to create
PgxFutureWrapperjava.lang.IllegalStateException: Unable to create
PgxFutureWrapper at
oracle.datastudio.interpreter.pgxFuture.CombinedPgxFutureDriver.getOrCreateSession(C
ombinedPgxFutureDriver.java:147) at
oracle.pgxFuture.graphviz.driver.PgxFutureDriver.getGraph(PgxFutureDriver.java:334) at
oracle.pgxFuture.graphviz.library.QueryEnhancer.createEnhancer(QueryEnhancer.j
ava:223) at
oracle.pgxFuture.graphviz.library.QueryEnhancer.createEnhancer(QueryEnhancer.j
ava:209) at
oracle.pgxFuture.graphviz.library.QueryEnhancer.query(QueryEnhancer.java:150)
at
oracle.pgxFuture.graphviz.library.QueryEnhancer.execute(QueryEnhancer.java:136
) at
oracle.pgxFuture.graphviz.interpreter.PgxFutureInterpreter.interpret(PgxFutureInterprete
r.java:131) at
oracle.datastudio.interpreter.pgxFuture.PgxFutureInterpreter.interpret(PgxFutureInterprete
r.java:120) at
org.apache.zepplin.interpreter.LazyOpenInterpreter.interpret(LazyOpenIn
terpreter.java:103) at
org.apache.zepplin.interpreter.remote.RemoteInterpreterServer$Interpret
Job.jobRun(RemoteInterpreterServer.java:632) at
org.apache.zepplin.scheduler.Job.run(Job.java:188) at
org.apache.zepplin.scheduler.FIFOScheduler$1.run(FIFOScheduler.java:140
) at java.base/
java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:515) at
java.base/java.util.concurrent.FutureTask.run(FutureTask.java:264) at
java.base/
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run
(ScheduledThreadPoolExecutor.java:304) at java.base/
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.jav
a:1128) at java.base/
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.ja
va:628) at java.base/java.lang.Thread.run(Thread.java:834)Caused by:
java.util.concurrent.ExecutionException:
oracle.pgxFuture.common.auth.AuthorizationException: PgxFutureUser(FCCMDSADMIN) does
not own session 6007f00a-8305-4576-9a56-9fa0f061586f or the session does
not exist code: PGX-ERROR-CQAZPV67UM4H at java.base/
java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:
395) at java.base/
java.util.concurrent.CompletableFuture.get(CompletableFuture.java:1999) at
oracle.pgxFuture.api.PgxFuture.get(PgxFuture.java:99) at
oracle.pgxFuture.api.ServerInstance.getSession(ServerInstance.java:670) at
oracle.datastudio.interpreter.pgxFuture.CombinedPgxFutureDriver.getOrCreateSession(C
ombinedPgxFutureDriver.java:145) ... 17 moreCaused by:
oracle.pgxFuture.common.auth.AuthorizationException: PgxFutureUser(FCCMDSADMIN) does
not own session 6007f00a-8305-4576-9a56-9fa0f061586f or the session does
not exist code: PGX-ERROR-CQAZPV67UM4H at
oracle.pgxFuture.common.marshalers.ExceptionMarshaller.toUnserializedException( Ex
ceptionMarshaller.java:107) at
oracle.pgxFuture.common.marshalers.ExceptionMarshaller.unmarshal(ExceptionMarsh
aler.java:123) at
oracle.pgxFuture.client.RemoteUtils.parseExceptionalResponse(RemoteUtils.java:
130) at

```

```
oracle.pgx.client.HttpRequestExecutor.executeRequest(HttpRequestExecutor
.java:198) at
oracle.pgx.client.HttpRequestExecutor.get(HttpRequestExecutor.java:165)
at
oracle.pgx.client.RemoteControlImpl$10.request(RemoteControlImpl.java:313)
at
oracle.pgx.client.RemoteControlImpl$ControlRequest.request(RemoteControl
Impl.java:119) at
oracle.pgx.client.RemoteControlImpl$ControlRequest.request(RemoteControl
Impl.java:110) at
oracle.pgx.client.AbstractAsyncRequest.execute(AbstractAsyncRequest.java
:47) at
oracle.pgx.client.RemoteControlImpl.request(RemoteControlImpl.java:107)
at
oracle.pgx.client.RemoteControlImpl.getSessionInfo(RemoteControlImpl.jav
a:296) at
oracle.pgx.api.ServerInstance.lambda$getSessionInfoAsync$14(ServerInstan
ce.java:490) at java.base/
java.util.concurrent.CompletableFuture.uniComposeStage(CompletableFuture
.java:1106) at java.base/
java.util.concurrent.CompletableFuture.thenCompose(CompletableFuture.jav
a:2235) at oracle.pgx.api.PgxFuture.thenCompose(PgxFuture.java:158)
```

You can perform the following steps as a workaround:

Export the "Manual Decision" Notebook.

Add the link parameter just below Description.

For example: "link": "manual Decision",

Figure 4-1 Link Parameter

```
[ {
  "name" : "manual Decision",
  "description" : null,
  "link": "manualDecision",
  "tags" : null,
  "version" : "5",
  "layout" : "zeppelin",
  "type" : "Default",
  "readOnly" : false,
```

Truncate the table "fcc_er_paragraph_manual" in Studio Schema.

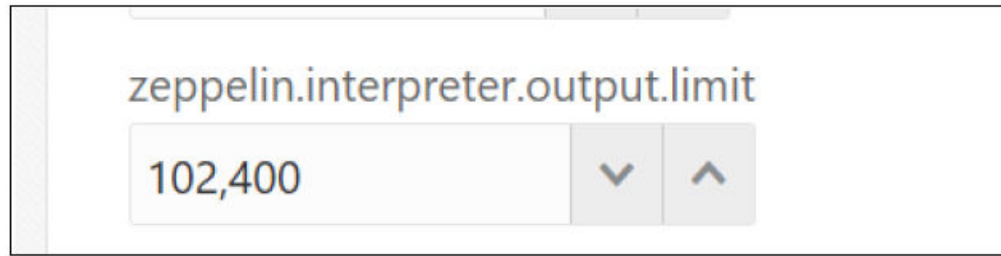
Import the modified notebook again.

9. What should I do when the result set is truncated if the size goes above '102400' bytes?

Perform the following steps:

Login to Compliance Studio.

Navigate to interpreter `zeppelin.interpreter.output.limit`.

Figure 4-2 Interpreter zeppelin parameter

Set the value to the required size.

Restart the Studio Application.

10. What should I do when the spark interpreter is not working?

- a. Log in to the server where Compliance Studio is installed.
- b. Navigate to \$SPARK_HOME directory. If the path is not set, then navigate to the <COMPLIANCE_ STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-studio/interpreter- server/spark-interpreter-<version>/extralibs directory.
- c. Export the following environment variables:

```
export HADOOP_CONF_DIR=<HADOOP Configuration Directory path>
export SPARK_HOME=<SPARK CLIENT DIRECTORY path>
export SPARK_CONF_DIR=<spark-defaults.conf directory path>
export SPARK_SUBMIT_OPTS="-Djava.security.krb5.conf=<kerberos directory path>/krb5.conf"
```

- d. Run the following commands for specific cases:

The result of the following command should be Pie value. (It ensures that the client is configured successfully.

```
./bin/run-example --master yarn SparkPi 10
```

The result of the following command is displayed as a Pie value. (It ensures that the client can successfully connect to the remote cluster.

```
./bin/spark-submit --class org.apache.spark.examples.SparkPi -- master
yarn <SPARK_HOME/examples/jars/>/spark-examples_<Version>.jar 10
```

For example, in case of spark 2.11-2.4.0, the command is as follows:

```
./bin/spark-submit --class org.apache.spark.examples.SparkPi -- master
yarn <SPARK_HOME/examples/jars/>/spark-examples_2.11- 2.4.0.jar 10
```

The result of the following command displays the list of databases that exist in HIVE.

```
./bin/spark-submit --class org.apache.spark.sql.hive.thriftserver.
SparkSQLCLIDriver --master yarn -e "Show databases"
```

The result of the following command ensures that the client can query from the HIVE schema.

```
./bin/spark-submit --class org.apache.spark.sql.hive.thriftserver.
SparkSQLCLIDriver --master yarn -e "select * from <hiveSchema>.<tableName>
limit 10"
```

11. How can I increase the memory of entity resolution and matching services?

For more information on increasing memory of entity resolution and matching services, see **Appendix - Setting Memory of Entity Resolution and Matching Services** in the [OFS Compliance Studio Administration and Configuration Guide](#).

12. What should I do when a runtime error occurs while executing a paragraph in Compliance Studio?

When Compliance Studio is just started (restart/upgrade/fresh installation), every interpreter gives a runtime error for the first time. Re-run the paragraph to get a result.

In addition, a user with admin privileges has to run a dummy notebook with a simple paragraph of all the used interpreters once.

13. What should I do if I encounter an error on the login?

If you log in to Compliance Studio for the first time, log out and log back in to resolve the error.

14. How can I retain the logs after restarting the Compliance Studio?

- a. Log in to the Compliance Studio.
- b. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
- c. Open the compliance-studio.sh file and modify the following for service(s) as per your requirement:

Search with "\$LOGS_FOLDER" text for each service and add > (Greater than) special character and space before the text as specified below:

```
"$DEPLOY_APP_HOME"/<service name>/bin/<service name> >> "$LOGS_FOLDER"/
<service name>.log
```

For example: batchservice, entity-resolution

```
function start_services() { service=$1 case $service in batchservice)
export JAVA_OPTS="-Djavax.net.ssl.trustStore=$DEPLOY_APP_HOME/ mmg-home/
mmg-studio/conf/<studio server> -
Djavax.net.ssl.trustStorePassword=$STUDIO_SERVER_SSL_PASSWORD" sh
"$DEPLOY_APP_HOME"/batchservice/bin/batchservice >> "$LOGS_FOLDER"/
batchservice.log 2>&1 & unset JAVA_OPTS ;; entity-resolution) export
JAVA_OPTS=<JAVA Options> export
ER_LOG_PATH="$COMPLIANCE_STUDIO_INSTALLATION_PATH/ deployed" export
ER_LOG_LEVEL=INFO export
LD_LIBRARY_PATH="$COMPLIANCE_STUDIO_INSTALLATION_PATH/ deployed/python-
packages/saneVirtualEnv/lib/python<version>/sitepackages/
jep:$COMPLIANCE_STUDIO_INSTALLATION_PATH/deployed/pythonpackages/
saneVirtualEnv/lib/" :$LD_LIBRARY_PATH export PATH_ORG=$PATH export
PATH=$DEPLOY_APP_HOME/python-packages/saneVirtualEnv/ bin:$PATH export
TNS_ADMIN=$TNS_ADMIN_PATH export PYTHONPATH_ORG=$PYTHONPATH
export PYTHONPATH="$DEPLOY_APP_HOME"/python-packages/
saneVirtualEnv/lib/python<version>/site-packages:$PYTHONPATH_ORG sh
"$DEPLOY_APP_HOME"/entity-resolution/bin/entity-resolution >>
"$LOGS_FOLDER"/entity-resolution.log & unset JAVA_OPTS export
PATH=$PATH_ORG ;;
```

- d. For load to OpenSearch, you need to add one more > (Greater than) special character as specified below:

```
sh "$DEPLOY_APP_HOME"/load-to-open-search/bin/load-to-open-search
>>"$DEPLOY_APP_HOME"/logs/load-to-open-search.log &
```

- e. Restart Compliance Studio. To do this, run the following command:

```
./compliance-studio.sh -restart
```

Or

```
./compliance-studio.sh -r script
```

15. What should I do if the following error message is displayed while starting Compliance Studio services? Java Memory error: unable to create new native thread

- Login to the Linux server as a root user where Compliance Studio is installed.
- Open the `/etc/security/limits.conf` file.
- Add the following parameters in the file:


```
soft nfile 65536
hard nfile 65536
<linux username> soft nproc 10240
@svrtech soft memlock 500000
@svrtech hard memlock 500000
```
- Save the file.
- Restart the Compliance Studio.

16. What should I do when unable to refresh Graph and fail due to the following error?

```
Failed to load graph '<Graph name>' in PGX server: http:// <hostname>:7007
08:22:54.878 [se-nio-7059-exec-1] ERROR
s.fccm.graphService.service.GraphExecutorService - Failed to refresh PGX
Graph, <Graph name>, in all PGX servers
```

- Stop the PGX server.
- Log in to Studio schema.
- Delete the entries that are related to the graph in the tables - **`fcc_graph_m_config_json`** and **`fcc_pgx_m_config`**.
- Start the PGX server.
- Re-execute the Batch for the Graph pipeline or Refresh the Graph task. See the **Managing Graph Pipeline** section in the [OFS Compliance Studio User Guide](#).

17. What should I do if there is a below error in the umm-service logs?

```
[29-06-22 07:30:48,095 GMT AM] [INFO ] [WEB] [UMM] [NA]
[GETUSERSESSION] Exception occurred while getting x-auth-token in
initSession method of GetUserSession classjavax.net.ssl.SSLKeyException:
Hostname verification failed:
HostnameVerifier=weblogic.security.utils.SSLWLSHostnameVerifier,
hostname=129.80.90.202.
```

Perform the steps described [here](#).

18. What should I do when upgrading the version JDK 11.0.13 to 11.0.15 using shellscript?

To upgrade bundled JDK:

- Use the `wget` command to download jdk 11.0.15 from [here](#).
- Change the directory where mmg-studio is installed and navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-studio/interpreter-server/pgx-interpreter-bundledJRE-<version>`.

- c. Run the `./update-jdk.sh [-j JDK11_HOME] [-o OUTPUT_DIR]` script.
`<JDK11_HOME>` specifies the downloaded JDK11 path, and `<OUTPUT_DIR>` specifies where the updated interpreter is saved.
 - d. Replace the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-studio/interpreter-server/pgx-interpreter-bundledJRE-<version>` directory with `<OUTPUT_DIR>/pgxjava`.
19. What should I do when unable to update the SSO token to the latest value while reinstalling the Compliance Studio?
- a. Log in to Studio schema.
 - b. Edit the table `NEXTGENEMF_CONFIG` and change the SSO token to the proper value.
 - c. Commit the changes.
 - d. Restart the Compliance Studio.
20. What should I do If it is a time-out issue observed in the Graph Pipeline?
- a. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgpipeline/pipeline/data-pipeline-service-<version>/conf/application.properties` directory.
 - b. Change the value from 1200000 to 120000000 in the `server.jetty.connectionidle-timeout=property` file.
 - c. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgpipeline/ pipeline/pipeline-service-<version>/conf/application.properties` directory.
 - d. Change the value from 1200000 to 120000000 in the `server.jetty.connectionidle-timeout= property` file.
21. What should I do if there is a below error in the Graph Pipeline?

```
08/Aug/2022 10:21:26,761- [LoggerConnection] LoggerConnection: Trying to
fetch connection for log.
08/Aug/2022 10:21:26,761- [LoggerConnection] LoggerConnection: isJNDI
value retrieved is true
08/Aug/2022 10:21:26,769- [LoggerConnection] LoggerConnection: Trying
to fetch connection for log.
08/Aug/2022 10:21:26,769- [LoggerConnection] LoggerConnection: isJNDI
value retrieved is true
08/Aug/2022 10:21:26,760- [DatabaseLogger] ExecutionLogger: Exception
while executing queries
java.lang.Exception:
at
com.oracle.fccm.amlxe.dataPipelineService.sequencer.impl.SequencerDAOImp
l.getQueries(SequencerDAOImpl.java:152) ~[classes!/:?]
at
com.oracle.fccm.amlxe.dataPipelineService.sequencer.impl.SequencerDAOImp
l$$FastClassBySpringCGLIB$$7e36e608.invoke(<generated>) ~[classes!/:?]
at
org.springframework.cglib.proxy.MethodProxy.invoke(MethodProxy.java:218)
~[spring-core-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.in
vokeJoinpoint(CglibAopProxy.java:771) ~[spring-aop-5.2.5.RELEASE.jar!/:]
```

```
:5.2.5.RELEASE]
at
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(Ref
lectiveMethodInvocation.java:163) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.pr
oceed(CglibAopProxy.java:749) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.dao.support.PersistenceExceptionTranslationIntercept
or.invoke(PersistenceExceptionTranslationInterceptor.java:139) ~[springtx-
5.2.5.RELEASE.jar!/5.2.5.RELEASE]
at
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(Ref
lectiveMethodInvocation.java:186) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.pr
oceed(CglibAopProxy.java:749) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.aop.framework.CglibAopProxy$DynamicAdvisedIntercepto
r.intercept(CglibAopProxy.java:691) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
com.oracle.fccm.amlxe.dataPipelineService.sequencer.impl.SequencerDAOImp
l$$EnhancerBySpringCGLIB$$c38b7c42.getQueries(<generated>) ~[classes!
:~]
at
com.oracle.fccm.amlxe.dataPipelineService.impl.ExecutorDAOImpl.executePi
pline(ExecutorDAOImpl.java:247) ~[classes!/:~]
at
com.oracle.fccm.amlxe.dataPipelineService.impl.ExecutorDAOImpl$$FastClas
sBySpringCGLIB$$14f27fdb.invoke(<generated>) ~[classes!/:~]
at
org.springframework.cglib.proxy.MethodProxy.invoke(MethodProxy.java:218)
~[spring-core-5.2.5.RELEASE.jar!/5.2.5.RELEASE]
at
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.in
vokeJoinpoint(CglibAopProxy.java:771) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(Ref
lectiveMethodInvocation.java:163) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.pr
oceed(CglibAopProxy.java:749) ~[spring-aop-5.2.5.RELEASE.jar!/
:5.2.5.RELEASE]
at
org.springframework.dao.support.PersistenceExceptionTranslationIntercept
or.invoke(PersistenceExceptionTranslationInterceptor.java:139) ~[springtx-
5.2.5.RELEASE.jar!/5.2.5.RELEASE]
at
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(Ref
```



```
lectiveMethodInvocation.java:186) ~[spring-aop-5.2.5.RELEASE.jar!/  
:5.2.5.RELEASE]  
at  
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.pr  
ceed(CglibAopProxy.java:749) ~[spring-aop-5.2.5.RELEASE.jar!/  
:5.2.5.RELEASE]  
at  
org.springframework.aop.framework.CglibAopProxy$DynamicAdvisedIntercepto  
r.intercept(CglibAopProxy.java:691) ~[spring-aop-5.2.5.RELEASE.jar!/  
:5.2.5.RELEASE]  
at  
com.oracle.fccm.amlxe.dataPipelineService.impl.ExecutorDAOImpl$$Enhancer  
BySpringCGLIB$$3277859b.executePipeline(<generated>) ~[classes!/:?]  
at  
com.oracle.fccm.amlxe.dataPipelineService.services.ExecutorService.execu  
tePipeline(ExecutorService.java:154) ~[classes!/:?]  
at sun.reflect.GeneratedMethodAccessor112.invoke(Unknown Source) ~[?:?]  
at  
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessor  
Impl.java:43) ~[?:1.8.0_321]  
at java.lang.reflect.Method.invoke(Method.java:498) ~[?:1.8.0_321]  
at  
org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(I  
nvocableHandlerMethod.java:190) ~[spring-web-5.2.5.RELEASE.jar!/  
:5.2.5.RELEASE]  
at  
org.springframework.web.method.support.InvocableHandlerMethod.invokeForR  
equest(InvocableHandlerMethod.java:138) ~[spring-web-5.2.5.RELEASE.jar!/  
:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHa  
ndlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:105)  
~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.mvc.method.annotation.RequestMappingHand  
lerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:879)  
~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.mvc.method.annotation.RequestMappingHand  
lerAdapter.handleInternal(RequestMappingHandlerAdapter.java:793)  
~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.  
handle(AbstractHandlerMethodAdapter.java:87) ~[spring-webmvc-  
5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherS  
ervlet.java:1040) ~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.DispatcherServlet.doService(DispatcherSe  
rvlet.java:943) ~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.FrameworkServlet.processRequest(Framework  
Servlet.java:1006) ~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]  
at  
org.springframework.web.servlet.FrameworkServlet.doPost(FrameworkServlet
```

```
.java:909) ~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at javax.servlet.http.HttpServlet.service(HttpServlet.java:652)
~[tomcat-embed-core-9.0.37.jar!/:4.0.FR]
at
org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883) ~[spring-webmvc-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at javax.servlet.http.HttpServlet.service(HttpServlet.java:733)
~[tomcat-embed-core-9.0.37.jar!/:4.0.FR]
at
org.eclipse.jetty.servlet.ServletHolder.handle(ServletHolder.java:755)
~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1617) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1604) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1604) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.springframework.boot.actuate.metrics.web.servlet.WebMvcMetricsFilter.doFilterInternal(WebMvcMetricsFilter.java:109) ~[spring-boot-actuator-2.2.6.RELEASE.jar!/:2.2.6.RELEASE]
at
org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1604) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119) ~[spring-web-5.2.5.RELEASE.jar!/:5.2.5.RELEASE]
at
org.eclipse.jetty.servlet.ServletHandler$CachedChain.doFilter(ServletHandler.java:1604) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.servlet.ServletHandler.doHandle(ServletHandler.java:545) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
```

```
at
org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java
:143) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.security.SecurityHandler.handle(SecurityHandler.java:5
90) ~[jetty-security-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.ja
va:127) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.
java:235) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.session.SessionHandler.doHandle(SessionHandler.
java:1607) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ScopedHandler.nextHandle(ScopedHandler.
java:233) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ContextHandler.doHandle(ContextHandler.
java:1297) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ScopedHandler.nextScope(ScopedHandler.j
ava:188) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.servlet.ServletHandler.doScope(ServletHandler.java:485
) ~[jetty-servlet-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.session.SessionHandler.doScope(SessionHandler.j
ava:1577) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ScopedHandler.nextScope(ScopedHandler.j
ava:186) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ContextHandler.doScope(ContextHandler.j
ava:1212) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.ScopedHandler.handle(ScopedHandler.java
:141) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.handler.HandlerWrapper.handle(HandlerWrapper.ja
va:127) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at org.eclipse.jetty.server.Server.handle(Server.java:500) ~[jettyserver-
9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.HttpChannel.lambda$handle$1(HttpChannel.java:38
3) ~[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at org.eclipse.jetty.server.HttpChannel.dispatch(HttpChannel.java:547)
[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at org.eclipse.jetty.server.HttpChannel.handle(HttpChannel.java:375)
[jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.server.HttpConnection.onFillable(HttpConnection.java:2
70) [jetty-server-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.io.AbstractConnection$ReadCallback.succeeded(AbstractC
```

```

onnection.java:311) [jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:103)
[jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.io.ssl.SslConnection$DecryptedEndPoint.onFillable(SslC
onnection.java:543) [jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.io.ssl.SslConnection.onFillable(SslConnection.java:398
) [jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.io.ssl.SslConnection$2.succeeded(SslConnection.java:16
1) [jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at org.eclipse.jetty.io.FillInterest.fillable(FillInterest.java:103)
[jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at org.eclipse.jetty.io.ChannelEndPoint$2.run(ChannelEndPoint.java:117)
[jetty-io-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.runTask(EatWhatYou
Kill.java:336) [jetty-util-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.doProduce(EatWhatY
ouKill.java:313) [jetty-util-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.tryProduce(EatWhat
YouKill.java:171) [jetty-util-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.run(EatWhatYouKill
.java:129) [jetty-util-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.ReservedThreadExecutor$ReservedThread.run(
ReservedThreadExecutor.java:388) [jetty-util-9.4.26.v20200117.jar!/:
9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.j
ava:806) [jetty-util-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at
org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPo
ol.java:938) [jetty-util-9.4.26.v20200117.jar!/:9.4.26.v20200117]
at java.lang.Thread.run(Thread.java:750) [?:1.8.0_321]
08/Aug/2022 10:21:26,786- [LoggerConnection] LoggerConnection: Trying
to fetch connection for log.
08/Aug/2022 10:21:26,786- [LoggerConnection] LoggerConnection: isJNDI
value retrieved is true

```

Re-execute the failed graph pipeline from the scheduler service.

To execute the Graph pipeline, see the **Using Scheduler Service** section in the [OFS Compliance Studio User Guide](#).

22. What should I do if there is a below error while executing the ER job 2 - ./ER_Run_Bulk_Similarity_Job.sh in matching-service.log?

```

ERROR ss.fccm.matchingservice.service.BulkQueryService - Exception
occurred in bulk processingERROR
ss.fccm.matchingservice.service.BulkQueryService - Exception occurred in
bulk processingjava.lang.IndexOutOfBoundsException: Index 1 out of

```

```

bounds for length 1 at
jdk.internal.util.Preconditions.outOfBounds(Preconditions.java:64)
~[?::?] at
jdk.internal.util.Preconditions.outOfBoundsCheckIndex(Preconditions.java
:70) ~[?::?] at
jdk.internal.util.Preconditions.checkIndex(Preconditions.java:248)
~[?::?] at java.util.Objects.checkIndex(Objects.java:372) ~[?::?] at
java.util.ArrayList.get(ArrayList.java:459) ~[?::?] at
com.oracle.ofss.fccm.matchingservice.service.BulkQueryService.preProcess
(BulkQueryService.java:159) [classes!/:?] at
com.oracle.ofss.fccm.matchingservice.controller.BulkUsingApiController2.
executeAsyncBulkQueryMatch(BulkUsingApiController2.java:76) [classes!/:
?] at jdk.internal.reflect.GeneratedMethodAccessor164.invoke(Unknown
Source) ~[?::?] at
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMetho
dAccessorImpl.java:43) ~[?::?] at
java.lang.reflect.Method.invoke(Method.java:566) ~[?::?] at
org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(I
nvocableHandlerMethod.java:205) [spring-w

```

This error is displayed only when the OpenSearch index does not have the proper data.

- a. Fix the data in the pre tables and cleanup the ER schema.
 - b. Re-run the job again. To run the job, see the **Perform Matching** section in the [OFS Compliance Studio Administration and Configuration Guide](#).
23. What should I do if interpreter settings are changed after restarting the Compliance Studio?

To retain the interpreter settings:

- a. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgstudio/conf directory.
- b. Open the application.yml file and change the value of **overwrite-builtin** to **false** in the interpreter parameter.

Note

While upgrading Compliance Studio, you should change the value to **true**.

- c. Restart Compliance Studio.
24. What should I do if ER Bulk similarity job fails due to metadata indices?

To load the indices:

- a. Execute the following cleanup scripts:
 - ER_Run_Bulk_Similarity_Job.sh
 - ER_Create_And_Load_Data_Into_Index.sh
- b. Delete the indices.
- c. Verify that the indices are deleted completely.
- d. Set the **F_IS_RECENTLY_CHANGED** flag to **Y** in the **fcc_idx_m_lookup**, and **fcc_idx_m_matching_lookup** tables.
- e. Execute ER_Create_And_Load_Data_Into_Index.sh.

- f. Ensure all the indices are created (Generally, it should create 19).
- g. If all the indices are available, then execute `ER_Run_Bulk_Similarity_Job.sh`.
- 25. Unable to open UI (Ruleset details, Manual Decisioning and Merge and Split Global Entities) in the Firefox browser?
Possible reason: Compliance Studio UI does not open in the Firefox browser if self-signed certificates are used while installation.
- 26. The UI (Ruleset details, Manual Decisioning and Merge and Split Global Entities) takes more time to load in other browsers?
Possible reason: The Compliance Studio UI screens are not cached if self-signed certificates are used and it takes time to load screen every time.
- 27. What should I do if the workspaces are not displayed and below error is encountered in the server.log?

```
12:02:16.272 [se-nio-7008-exec-2] ERROR
er.network.base.exception.ExceptionHandlerAdvice - Internal server
error.
io.jsonwebtoken.security.SignatureException: JWT signature does not
match locally computed signature. JWT validity cannot be asserted and
should not be trusted.
```

To resolve the error:

- a. Generate the public and private keys. For more information, see the [Generate Public and Private Keys](#) section.
- b. Replace the keys in the paths as mentioned in the see the [Generate Public and Private Keys](#) section.
- c. Generate the SSO (API) token. For more information, see the [Generate API Token for CS API User](#) section.
- d. Replace token in the `config.sh` file. For more information, see the parameter "SSO_TOKEN" in **Table 14** in [Configure config.sh File](#).
- e. Stop Compliance Studio.
- f. Reinstall Compliance Studio.
- g. Replace the value of SSO_TOKEN in the `nextgenemf_config` table in the studio schema.
- h. Start Compliance Studio.
- 28. What should I do if a particular patch version is not applied to the CS build?

To apply the patch:

- You must manually delete the entry for that particular patch version from the **FCC_COMPLIANCE_STUDIO_PATCHES** table in the Studio Schema.
- 29. How to configure a new/cloned interpreter?
To configure a new/cloned interpreter:
 - a. Create a new/clone an existing interpreter in the UI.
 - b. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgstudio/bin` directory.

- c. Open the `startup.sh` file and add the following line before the line containing `"counter=1";`

```
nohup <path_to_interpreter_binary_file> &> <path_to_save_the_logs>/
<log_file_name>.log &
```

Figure 4-3 Snapshot of startup.sh file

```
#export PLAINR_INTERPRETER_OPTS="$PLAINR_INTERPRETER_OPTS -DAPP_BASE_NAME='plainr-i
#nohup "$DIR"/../interpreter-server/plainr-interpreter-23.4.2/bin/plainr-interprete
# To start Spark interpreter
nohup "$DIR"/../interpreter-server/spark-interpreter-23.4.0/bin/spark-interpreter &
counter=1;
while [[ $counter -lt 20 ]]
do
  dsHealth=`curl -s --insecure https://ofss-mum-1779.snbomprshared1.gbucdsint02bc
```

- d. Save and close the file.
- e. Open the `shutdown.sh` file and add following line before the line containing `"SL="`.

```
I8004=`ps -eaf | grep java | grep RemoteInterpreterServer | grep 8004 |
awk '{print $2}'` if [[ "" != "$I8004" ]]; then kill -9 $I8004; fi
```

Figure 4-4 Snapshot of shutdown.sh file

```
# To shutdown Spark interpreter
I8004=`ps -eaf | grep java | grep RemoteInterpreterServer | grep 8004 | awk '{print $2}'`
if [[ "" != "$I8004" ]];
then kill -9 $I8004;
fi

SL=`ps -eaf | grep java | grep oracle.datastudio.starter.App | awk '{print $2}'`
if [[ "" != "$SL" ]];
then kill -9 $SL;
fi
```

Note

In the above steps, the port number for the new/cloned interpreter is assumed to be 8004, the default port that comes with the installer. If a different port is used, then change the configuration accordingly.

- f. Save and close the file.
 - g. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
 - h. Restart Compliance Studio using the command: `./compliance-studio.sh -restart`.
 - i. Verify if the spark-interpreter has started using the command: `netstat -nlt | grep 8004`.
- 30. What should I do if import failed in the Graph Pipeline?**

After installation, query the table `FCC_M_PIPELINE_IMPORT_LOG` to check the imported pipeline status. The `_V_IMPORT_STATUS_` column denotes the status and should be 'SUCCESS' for all the imported pipelines.

If any pipelines have the status of 'FAILED,' perform the following steps to reimport:

- a. Find the entry for the failed pipeline in the `FCC_M_EXTERNALSERVICE_RUN` table of the `_C_TABLELIST_` column.
- b. Remove that entry from the table. If the entry is not there, skip this step.
- c. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgpipeline/ pipeline/data-metadata-job-<version>/bin` directory.
- d. Run the `import_metadata.sh` shell script using the command: `./import_metadata.sh`.
- e. Once the script is executed, verify the status in the `FCC_M_PIPELINE_IMPORT_LOG` to ensure that the status is a success.

31. How do I update the BE_PORT value after reinstalling the Compliance Studio?

To update the BE_PORT value:

- a. Login to Compliance Studio schema.
- b. Open the `NEXTGENEMF_CONFIG` table.
- c. Verify the V_NAME columns (`EMFSTUDIO_SERVICE_URL` and `BASE_URL`).
If "BE_PORT" is not replaced, change V_VALUE to the required port number or set it to the default port value. i.e., **7002**.
- d. Restart the Compliance Studio.

32. What should I do if delta matches are not reflected in the sub graph (OOB)?

To reflect delta matches in the sub graph:

- a. Re-run the Refresh Graph task.
- b. Restart the PGX and then load the sub graph.

33. What should I do if any Compliance Studio service fails with the following error?

```
ERROR c.z.h.p.HikariPool - HikariPool-72 - Exception during pool
initialization.
java.sql.SQLException: ORA-02391: exceeded simultaneous SESSIONS_PER_USER
limit
https://docs.oracle.com/error-help/db/ora-02391/at
oracle.jdbc.driver.T4CTTIoer11.processError(T4CTTIoer11.java:709)
```

To Resolve this issue, follow these steps:

- a. Check the current value of `SESSION_PER_USER` for the Studio schema using the following query.

```
select PROFILE, LIMIT from dba_profiles a, dba_users b WHERE
a.PROFILE=b.PROFILE and a.RESOURCE_NAME = 'SESSIONS_PER_USER'and
a.PROFILE = '<Studio schema>';
```

- b. Get the Studio Schema profile using the following query.

```
select profile from dba_users where username = '<Studio schema>';
```


- c. Change the profile obtained in Step b using the following query.

```
ALTER PROFILE <profile> LIMIT SESSIONS_PER_USER UNLIMITED;
```

A

Appendix

This section provides additional information that supports the installation activity.

A.1 Additional Configuration

You can customize port number for the services and other additional configuration if required.

Customizable Parameters

Users can customize the parameters based on their preferences using **additional_config.sh** file.

After updating the **additional_config.sh** file, you must stop, trigger a reinstall, and then start Compliance Studio.

Note

The custom ports for the Batch Service and Meta Service are not replaced in the appropriate files, so the following changes must be made manually.

To update the custom port for Batch Service, follow these steps:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/batchservice/conf` directory.
2. Open the **server-config.properties** file.
3. Based on your preferences, update the custom port for the following parameters:
 - **server.http.port:**<Custom port for batch service to start>
 - **server.shutdownPort:**<Custom port for batch service to stop>For example,
server.http.port:16043
server.shutdownPort:16044
4. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/batchservice/conf` directory (outside the deployed location) and repeat step 3.

To update the custom port for Meta Service, follow these steps:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/metaservice/conf` directory.
2. Open the **server-config.properties** file.
3. Based on your preferences, update the custom port for the following parameters:
 - **server.http.port:**<Custom port for meta service to start>
 - **server.shutdownPort:**<Custom port for meta service to stop>For example,

server.http.port:16043**server.shutdownPort:16044**

4. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/metaservice/conf directory (outside the deployed location) and repeat step 3.

To customize the parameters, follow these steps:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
2. Open the **additional_config.sh** file and update the parameters as mentioned in the following table. The port number/value is provided for reference only; you need to configure it based on your preferences.

Table A-1 Additional Configuration File

Service / Parameter	Significance	Port Number/ Value
AUTH_SERVICE_PORT	Indicates the port number for authorization service.	7041
BATCH_SERVICE_PORT	Indicates the port number for batch service.	7043
BE_PORT	Indicates the port number for authorization service.	7002
DATAPIPELINE_GATEWAY_SERVICE_PORT	Indicates the port number for datapipeline gateway service.	7063
DATASTUDIO_SPARK_INTERPRETER_PORT	Indicates the port number for Datstudio's spark interpreter.	7014
DATASTUDIO_SERVER_PORT	Indicates the port number for Datstudio server.	7008
DATASTUDIO_MARKDOWN_INTERPRETER_PORT	Indicates the port number for Datstudio's markdown interpreter.	7009
DATASTUDIO_PYTHON_INTERPRETER_PORT	Indicates the port number for Datstudio's python interpreter.	7012
DATASTUDIO_JDBC_INTERPRETER_PORT	Indicates the port number for Datstudio's jdbc interpreter.	7011
DATASTUDIO_PYTHON_INTERPRETER_REST_SERVER_PORT	Indicates the port number for Datstudio's python interpreter of the server.	6012
DATASTUDIO_PGX_PYTHON_INTERPRETER_REST_SERVER_PORT	Indicates the port number for Datstudio's pgx-python interpreter of the server.	6022
DATASTUDIO_THRIFT_EVENT_HANDLER_PORT	Indicates the port number for Datstudio's thrift event handler.	8432
DATASTUDIO_PGX_INTERPRETER_PORT	Indicates the port number for Datstudio's pgx interpreter.	7022
DATAPIPELINE_HAZELCAST_PORT	Indicates the port number for datapipeline hazelcast.	5701
DATA_PIPELINE_UI_SERVICE_PORT	Indicates the port number for datapipeline UI service.	7067
ER_SERVICE_PORT	Indicates the port number for Entity Resolution service.	7051
GRAPH_SERVICE_PORT	Indicates the port number for Graph service.	7059
GRAPH_SERVICE_CACHE_SERVER_PORT	Indicates the port number for cache server of the Graph service.	7060
JDBC_EVENT_PORT	Indicates the port number for jdbc event.	7031

Table A-1 (Cont.) Additional Configuration File

Service / Parameter	Significance	Port Number/ Value
JDBC_PORT	Indicates the port number for jdbc.	7011
LOAD_TO_OS_SERVICE_PORT	Indicates the port number for load to OpenSearch service.	7053
MATCHING_SERVICE_PORT	Indicates the port number for matching service.	7049
META_SERVICE_PORT	Indicates the port number for meta service.	7045
MMG_COHERENCE_CLUSTER_PORT	Indicates the port number for MMG coherence cluster.	7574
PIPELINE_UI_SERVICE_PORT	Indicates the port number for pipeline UI service.	7065
PYTHON_DEFAULT_EVENT_PORT	Indicates the port number for python default event.	7030
PYTHON_DEFAULT_PORT	Indicates the port number for default python.	7010
PYTHON_DEFAULT_REST_PORT	Indicates the port number for default python rest.	7077
PYTHON_ML4AML_EVENT_PORT	Indicates the port number for python ML4AML event.	7036
PYTHON_ML4AML_PORT	Indicates the port number for python ML4AML.	7016
PYTHON_ML4AML_REST_PORT	Indicates the port number for python ML4AML rest.	7097
PYTHON_SANE_EVENT_PORT	Indicates the port number for python sane event.	7037
PYTHON_SANE_PORT	Indicates the port number for python sane.	7017
PYTHON_SANE_REST_PORT	Indicates the port number for python sane rest.	7087
SCHEMA_PORT	Indicates the port number for schema.	7003
SESSION_SERVICE_PORT	Indicates the port number for session service.	7047
STUDIO_SERVICE_PORT	Indicates the port number for studio service.	7008
UI_PORT	Indicates the port number for UI.	7001
CONNECTION_TIME_OUT	Indicates the connection time out.	50000
DS_API_VERSION	Indicates the API version for Data Studio.	20230913
HOSTNAME	Indicates the hostname of the application.	`hostname -f`
MD_VERSION	Indicates the version of the application.	21.4.9
READ_TIME_OUT	Indicates the read time out.	50000
LOG_LEVEL	Indicates the log level.	INFO
STUDIO_LOG_LEVEL	Indicates the log level of the Studio.	INFO
DATAPIPELINE_SERVICE_PORT1	Indicates the port number for datapipeline.	18005
DATAPIPELINE_SERVICE_PORT2	Indicates the port number for datapipeline.	18006
DATAPIPELINE_METADATA_IMPORT_SERVICE_PORT	Indicates the port number for importing metadata in the datapipeline	18007
DATASTUDIO_SERVER_TOMCAT_THREADS_MAX	Maximum amount of worker threads.	200
DATASTUDIO_HIKARI_MAX_LIFETIME_TIME	Maximum lifetime for a connection in the pool.	28800000

Table A-1 (Cont.) Additional Configuration File

Service / Parameter	Significance	Port Number/ Value
DATASTUDIO_HIKARI_MINIMUM_IDLE	Minimum number of idle connections that the pool should try to maintain.	10
DATASTUDIO_HIKARI_CONNECTION_TIMEOUT_MS	Maximum time application is willing to wait for a connection from the pool.	30000
DATASTUDIO_HIKARI_MAXPOOL_SIZE	Maximum number of connections that can be held in the connection pool.	350
DATASTUDIO_SERVER_ASYNC_THREADPOOL_SIZE	Number of threads in the thread pool used for asynchronous request.	128
DATASTUDIO_SERVER_SCHEDULED_THREADPOOL_SIZE	Number of threads in the thread pool used for scheduled execution.	128
DATASTUDIO_INTERPRETER_CLEANUP_CRON	Expression defines the schedule for the idle session cleanup.	"*/5 * * * *"
DATASTUDIO_INTERPRETER_CLEANUP_ENABLED	It is used to enable or disable the idle session cleanup.	TRUE
DATASTUDIO_INTERPRETER_IDLE_SESSION_TIMEOUT	Timeout duration for idle session. Longer sessions idle will be terminated.	PT1H
DATASTUDIO_ENABLE_INTERPRETER_RESTART	It is used to enable or disable the interpreter restart.	TRUE
DATASTUDIO_STARTUP_THRESHOLD_MS	The maximum time allowed for the interpreter to start in milliseconds. If the interpreter fails to start within this time, it is considered as unhealthy and restart is required. Note: This parameter is applicable only when this parameter (DATASTUDIO_ENABLE_INTERPRETER_RESTART) is enabled.	60000
DATASTUDIO_CHECK_ALIVE_INTERVAL	Indicates the time interval between health checks for the interpreter in milliseconds.	60000
DATASTUDIO_ZPLN_SCHEDULED_THREADPOOL_SIZE	Number of threads in the thread pool used by Zeppelin's scheduler.	10000

Non-customizable Parameters**Note**

Do not modify the parameters within the Non-customizable parameters section.

A.2 Create Users, Groups, and Mappings

This section describes how to create Users, Groups, and Mappings.

The AAI User Provisioning SQL Scripts Generator Utility allows you to use AAI for authN in the Compliance Studio. Identity administrators can create new user groups/roles, perform appropriate roles, usergroup and domain mapping, and so on.

This is provided as a SQL generator utility. This SQL scripts is executed in the AAI's config schema to create the required metadata.

You must execute this script multiple times against each username. Also, generate the merge scripts accordingly.

Execute the following command from <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/<mmg-home>/bin directory.

```
./userprovisioning-script-generator.sh <user> <comma separated list of user groups or ALL> <infodomain> <segment>
```

Sample Commands:

```
./userprovisioning-script-generator.sh SCRIPTUSER ALL OFSAAAIINFO EMFLD
./userprovisioning-script-generator.sh SCRIPTUSER
MDLREV,MDLUSR,IDENTITY_ADMIN OFSAAAIINFO EMFLD
```

Table A-2 Pre-configured Group

User Group	Description
IDNTYADMN	Identity Administrator group
IDNTYAUTH	Identity Authorizer group
MDLREV	The Modeling Reviewer Group. Users mapped to this group have access to the menu items in the application that are related to model review activities.
MDLAPPR	The Modeling Approver Group. Users mapped to this group have the rights to approve models created by the users.
MDLBATCHUSR	The Modeling Batch User. Scheduler can use this Group for executing batches. The Workspace Administrator Group.
WKSPADMIN	The Workspace Administrator Group. Users mapped to this group have access to create and populate workspaces. For viewing the landing page this group is required.
MDLUSR	The Modeling User Group. Users mapped to this group have access to all the menu items in the application that is related to model creation.
DSUSRGRP	Data Studio User Group. This User Group provide access to modify Interpreter configurations.
GRPADMIN	The Graph Administrator Group. Users mapped to this group have access to all the menu items in the application related to graph as well as Pipeline/Refresh graphs related health services.
GRPUSR	The Graph User Group. Users mapped to this group have access to all the menu items in the application related to graph as well as Pipeline/Refresh graphs related health services.

Table A-2 (Cont.) Pre-configured Group

User Group	Description
DSREDACTGRP	Roles for applying redaction in graph. This group will be applicable to only those users for whom graph redaction is required. Note: This group has to be created manually in AAI and map it to the users.
ERADMIN	Entity resolution admin group. Note: This group has to be created manually in AAI and map it to the users.
ERUSER	Entity resolution user group. Note: This group has to be created manually in AAI and map it to the users.

Note

For more information on adding, updating, and deleting users through AAI realm method, see the **System Configuration and Identity Management** section in the [OFSAAI User Guide](#).

A.3 Generate an Encrypted Password for OpenSearch

This section describes how to generate an encrypted password for OpenSearch.

Encrypted password is required during configuration.

For example: OPEN_SEARCH_ENCRYPTED_PASSWORD.

To generate an encrypted password:

1. Set the export FIC_DB_HOME path in the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/ficdb directory.
2. Run the echo \$FIC_DB_HOME command.
3. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/ficdb/bin directory and run the ./FCCM_Studio_Base64Encoder.sh <password to be encrypted> command.

A.4 Setup Compliance Studio Instance for Cloning the Filesystem

This section describes the process of cloning files from the Compliance Studio's Primary server to the Compliance Studio's Secondary server for the purpose of disaster recovery.

For more information about disaster recovery, see the **Setup Disaster Recovery (DR) in Compliance Studio** section in the [OFS Compliance Studio Architecture Guide](#).

Prerequisites

- OpenSearch should be installed in the Secondary server.

Note

The following prerequisites are applicable for the case where Database schemas (for example: Studio Schema, ECM/BD Atomic Schema, and Graph Schema) are cloned in a different database.

- Create a wallet for the Secondary Database. To create a wallet, see the [Setup the Password Stores for Database User Accounts](#) section.
- Add Secondary database credentials in the wallet.
- ER/FSDS Schema, Atomic Schema, Studio Schema, and Graph Schema names should be the same as the Primary Database.

Cloning Process**Note**

The Incremental file system changes from the Active Compliance Studio server should be synced/reflected in all the fail over Compliance Studio servers as well.

To clone files in the Compliance Studio, follow these steps:

1. Zip the **OFS_COMPLIANCE_STUDIO** and **Logstash-<version>** directories from the Compliance Studio's Primary Server.

Note

The Logstash for OpenSearch is different, so based on the configuration the respective logstash should be configured. Logstash version depends on the OpenSearch version.

2. To zip those directories, execute the following command.

```
zip -r <DIRECTORY_NAME>.zip <DIRECTORY_NAME>
```

For example, `zip -r OFS_COMPLIANCE_STUDIO.zip OFS_COMPLIANCE_STUDIO`

3. Copy the zip file into the Compliance Studio's Secondary server.
4. Unzip the file from the Compliance Studio's Secondary server by executing the following command.

```
unzip -a <zip_file_name>.zip
```

Cloning OpenSearch

To clone the OpenSearch, follow these steps:

1. Copy the folder "data" from this `<OS_Installation_Path>/opensearch-<version>` directory in the OpenSearch's Primary server.
Where `<OS_Installation_Path>` refers to OpenSearch installed path.
2. Place the copied "data" folder into `<OS_Installation_Path>/opensearch-<version>` directory of the OpenSearch's Secondary server.

If HTTPS and AUTH are enabled for OpenSearch, then follow these steps:

1. To generate **ca.crt** file in the OpenSearch's Secondary server, execute the following command.

```
openssl x509 -outform der -in <path to/admin.pem> -out ca.crt
```

2. Copy **ca.crt** file from OpenSearch's Secondary server and place in the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/logstash/config` directory.
3. To generate **admin.p12** file in the OpenSearch's Secondary server, execute the following command.

```
openssl pkcs12 -export -out admin.p12 -inkey <path to/admin-key.pem> -in  
<path to/admin.pem>
```

4. Copy **admin.p12** file and place it in the following directories of the Compliance Studio's server.

```
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/load-to-open-search/conf  
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/load-to-open-search/conf  
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/matching-service/conf  
<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/matching-service/conf
```

Cloning PGX Service

Note

This section is applicable only for Graph use case.

To clone the PGX service, follow these steps:

1. Copy the **studio_server.p12** file from `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-studio/conf` directory of the Compliance Studio's Primary server and place it to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/pgx-server/conf` directory in the Compliance Studio's Secondary server.
2. Generate the **graph-keystore.p12** file for PGX's Secondary server. To generate graph-keystore.p12 file, see the [Generate the graph-keystore.p12 File](#) section.
3. Navigate to the `<PGX_HOME>/pgx/pgx-server/bin` directory.
4. Open the **config.sh** file and update the following parameter.

```
GRAPH_SERVICE_URL=##SECONDARY_GRAPH_SERVICE_URL##  
  
GRAPH_KEYSTORE_PASSWORD=##SECONDARY_GRAPH_KEYSTORE_PASSWORD##
```

The path where the `pgx-server-<version>.zip` file is unzipped and it is referred to as **<PGX_HOME>**. For more information, see the [Configure the PGX Service](#) section.
5. To reinstall the PGX service, execute the following command.

```
./pgx-server --update
```

(OR)

```
./pgx-server -u
```

6. To start the PGX service, execute the following command.

```
./pgx-server --start
```

(OR)

```
./pgx-server -s
```

Cloning Conda Environment

To clone Conda environment, follow these steps:

1. Zip the miniconda directory from the Compliance Studio's Primary Server.
2. To zip the directory, execute the following command.

```
zip -r <DIRECTORY_NAME>.zip <DIRECTORY_NAME>
```

For example, `zip -r OFS_MINICONDA_INSTALLATION.zip MINICONDA_INSTALLATION`

3. Copy the zip file into the Compliance Studio's Secondary server.
4. Unzip the miniconda file from the Compliance Studio's Secondary server using the following command.

```
unzip -a <zip_file_name>.zip
```

Configure Wallet

Copy wallet from Primary server to Secondary server when database schemas are same between the servers.

If the database schemas are different, you have to create a new wallet for Secondary server. To create a wallet, see the [Setup Password Stores with Oracle Wallet](#) section.

① Note

Open the **sqlnet.ora** file in the wallet location and update the path with wallet location path of the Secondary server.

Generate SSL Certificate

If SSL certificate generated in the Primary server is exclusive to that server only, then a new certificate has to be generated for the Secondary server.

To generate SSL certificate, see the [Generate Compliance Studio Server SSL Configuration](#) section.

Configuring config.sh File

To configure the config.sh file, follow these steps:

1. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory in Compliance Studio's Secondary server.
2. Open the **config.sh** file and update parameters as mentioned in the following table.

Note

For the parameter description, see the section.

Table A-3 Parameter and its Values in Config.sh File

Parameter	Placeholder Value
COMPLIANCE_STUDIO_INSTALLATION_PATH	##SECONDARY_COMPLIANCE_STUDIO_PATH## Note: If the OFS_COMPLIANCE_STUDIO path is same in the Compliance Studio's Primary and Secondary Servers, then this parameter need not be changed.
MINICONDA_INSTALLATION_HOME	##SECONDARY_MINICONDA_INSTALLATION_PATH## Note: If miniconda path is different between Primary and Secondary servers, open the config.sh file and update the MINICONDA_INSTALLATION_HOME with the path in the Secondary server.
LOGSTASH_HOME	##SECONDARY_LOGSTASH_HOME##
LD_LIBRARY_PATH	##SECONDARY_LD_LIBRARY_PATH##
SSL Configuration	-
STUDIO_SERVER_SSL_ALIAS	##SECONDARY_STUDIO_SERVER_SSL_ALIAS##
DB Details of Studio Schema Note: This parameter is applicable when Database schemas are cloned to the different databases.	-
STUDIO_DB_HOSTNAME	## SECONDARY_STUDIO_DB_HOSTNAME ##
STUDIO_DB_PORT	## SECONDARY_STUDIO_DB_PORT##
STUDIO_DB_SERVICE_NAME	## SECONDARY_STUDIO_DB_SERVICE_NAME##
STUDIO_DB_SID	## SECONDARY_STUDIO_DB_SID##
STUDIO_DB_USERNAME	## SECONDARY_STUDIO_DB_USERNAME##
DB Details of Atomic Schema Note: This parameter is applicable when Database schemas are cloned to the different databases.	-
ATOMIC_DB_HOSTNAME	## SECONDARY_ATOMIC_DB_HOSTNAME##
ATOMIC_DB_PORT	## SECONDARY_STUDIO_DB_PORT##
ATOMIC_DB_SERVICE_NAME	## SECONDARY ATOMIC_DB_SERVICE_NAME ##
ATOMIC_DB_SID	## SECONDARY_ATOMIC_DB_SID##
ATOMIC_DB_USERNAME	## SECONDARY_ATOMIC_DB_USERNAME##
Graph Schema Configuration Note: This parameter is applicable when Database schemas are cloned to the different databases.	-
GRAPH_DB_SERVER_NAME	## SECONDARY_GRAPH_DB_SERVER_NAME##
GRAPH_DB_PORT	## SECONDARY_GRAPH_DB_PORT##
GRAPH_DB_SERVICE_NAME	## SECONDARY_GRAPH_DB_SERVICE_NAME##

Table A-3 (Cont.) Parameter and its Values in Config.sh File

Parameter	Placeholder Value
GRAPH_KEYSTORE_PASSWORD	## SECONDARY_GRAPH_KEYSTORE_PASSWORD##
GRAPH_SCHEMA_DB_SCHEMA_NAME	##SECONDARY_GRAPH_SCHEMA_DB_SCHEMA_NAME# #
GRAPH_SCHEMA_WALLET_ALIAS	## SECONDARY_GRAPH_SCHEMA_WALLET_ALIAS##
Wallet Details Note: This parameter is applicable when Database schemas are cloned to the different databases. OR If the filesystem of the secondary server has a different folder structure than the Primary server.	-
WALLET_LOCATION	##WALLET_PATH_CONTAINING_SECONDARY_DB_CREDENTIALS##
TNS_ADMIN_PATH	##TNS_ADMIN_PATH_CONTAINING_SECONDARY_DB_CREDENTIALS##
GRAPH_SCHEMA_WALLET_LOCATION	##GRAPH_SCHEMA_WALLET_PATH_CONTAINING_SECONDARY_DB_CREDENTIALS##
GRAPH_SCHEMA_TNS_ADMIN_PATH	##GRAPH_SCHEMA_TNS_ADMIN_PATH_CONTAINING_SECONDARY_DB_CREDENTIALS##
Service Urls	-
PGX_SERVER_URL	##SECONDARY_PGX_SERVER_URL##

3. Add Secondary Database credentials in the wallet. To add credentials, see the [Setup the Password Stores for Database User Accounts](#) section.
4. In Studio Schema, delete the following row from the DATABASECHANGELOG table.
author = 'Compliance Studio 8.1.3.0' and id = 'FCC_DATASTUDIO_CONFIG_8130'
5. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
6. Reinstall Compliance Studio's Secondary Server. To reinstall, execute the following command.

```
./compliance-studio.sh --update
```

(OR)

```
./compliance-studio.sh -u
```

7. Start Compliance Studio's Secondary Server. To start, execute the following command.

```
./compliance-studio.sh --start
```

8. Navigate to the <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ficdb/confdirectory.
9. Open the **resources.xml** file and update the following details for ER/FSDF schema. Example,

```
<Resource
id="##ER_DATA_SCHEMA_ALIAS_NAME##"
```

```
name="jdbc/erdataschema"
auth="Container"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.OracleDriver"
url="jdbc:oracle:thin:@##ER_DATA_SCHEMA_ALIAS_NAME##"
connectionProperties="oracle.net.wallet_location=/scratch/fccstudio/
CS81300_CS_Cloning_0204/compStudio_02040741/OFS_COMPLIANCE_STUDIO/
wallet;oracle.net.tns_admin=/scratch/fccstudio/CS81300_CS_Cloning_0204/
compStudio_02040741/OFS_COMPLIANCE_STUDIO/wallet;"
maxTotal="20"
maxIdle="0"
maxWaitMillis="-1">
</Resource>
```

A.5 Generating Files for SAML Signed Request

Security Assertion Markup Language (SAML) signed request that is cryptographically signed to ensure its authenticity and integrity. It is typically used to authenticate and authorize users between the Identity Provider and Service Provider.

To create .cer and .pem files for SAML signed request:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH> directory.
2. Execute the following command.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout spprivatekey.
pem -out sp-certificate.cer
```

A.6 Access Data Studio UI from Compliance Studio and ECM without Triggering Reinstallation

To access Datastudio UI from Compliance Studio and ECM application without triggering reinstallation:

1. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-ui/conf directory.

Note

Make sure that you have taken backup of this application.properties file before updating any changes.

2. Open the application.properties file and update value for **mmg.datastudio.ui.url** as `https://<hostname>:<Datastudio Port>/cs`. For example, `https://testserver.com:7008/cs`.
3. Save the file.
4. Navigate to <COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgstudio/conf directory.

Note

Make sure that you have taken backup of this `application.yml` file before updating any changes.

5. Open the `application.yml` file and update the directives parameter as follows:

```
"frame-ancestors 'self' https://  
<Hostname>:<Compliance_Studio_Gateway_Port>"
```

This parameter allows Datastudio UI to be embedded as iFrame in any external application and this controls the allowed origins where datastudio UI can be embedded.

In case of ECM-IH integration use case, update the directives parameter as follows:

```
"frame-ancestors 'self' https://  
<Hostname>:<Compliance_Studio_Gateway_Port> http://  
<ecm_webserver_hostname>:<ecm_ui_port>"
```

6. Restart Compliance Studio services.

After restart, the Compliance Studio URL will be `https://<Hostname>:<COMPLIANCE_STUDIO_GATEWAY_PORT>/cs/home`.

A.7 Support for POST and REDIRECT in SAML Request

SAML assertions contain authentication and authorization information, which is transmitted using a request method. This enables a secure and standardized exchange of identity and access data between systems or domains.

After generating certificates for a SAML signed request, users need to configure SAML with request type.

To update the request type, follow these steps:

1. Navigate to the `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmgui/conf` directory.
2. Open **application.properties** file and add the following parameters at the end of the file.

```
saml.request.type=POST  
saml.include.sp.cert=Y
```

Note

- SAML requests can be sent using different methods, called bindings. Currently, we support REDIRECT and POST bindings, with REDIRECT being the default method.
- The possible values for `saml.request.type` are **POST** and **REDIRECT** and possible value for `saml.include.sp.cert` is either **Y** or **N**.

A.8 Configuring Custom Ports

Customizing the port number in the Compliance Studio offers flexibility in network configuration, enhances security, prevents conflicts, and guarantees compliance with organizational policies.

Follow the standard installation process for the Compliance Studio, and then use this section to reconfigure the server port based on your preferences.

Note

- By default, port number used in the Compliance Studio is 7XXX. If user wants to customize the port number, then you can update based on your preferences. For example, change the port number starts with 7XXX to 3XXX and change the port number starts with 18XXX to 8XXX. The same example has been used in the document for reference.
- If port numbers are not replaced properly, then you need to update it manually.
- Restart Compliance Studio is required whenever you updated the port number.

A.8.1 Compliance Studio Configuration

To update port number for Compliance Studio service, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
2. Open **compliance-studio.sh** file and update port numbers as mentioned in the following table.

Table A-4 compliance-studio.sh file

Service	Port Number
PGX_INTERPRETER_OPTS	3059
curl --location --insecure URL	3002

3. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin` directory.
4. Open **additional_config.sh** file and update port numbers as mentioned in the following table.

Table A-5 additional_config.sh file

Service	Port Number
AUTH_SERVICE_PORT	3041
BATCH_SERVICE_PORT	3043
BE_PORT	3002
DATAPIPELINE_GATEWAY_SERVICE_PORT	3063
DATA_PIPELINE_UI_SERVICE_PORT	3067
ER_SERVICE_PORT	3051
GRAPH_SERVICE_PORT	3059

Table A-5 (Cont.) additional_config.sh file

Service	Port Number
JDBC_EVENT_PORT	3031
JDBC_PORT	3011
LOAD_TO_OS_SERVICE_PORT	3053
MATCHING_SERVICE_PORT	3049
META_SERVICE_PORT	3045
PIPELINE_UI_SERVICE_PORT	3065
PYTHON_DEFAULT_EVENT_PORT	3030
PYTHON_DEFAULT_PORT	3010
PYTHON_DEFAULT_REST_PORT	3077
PYTHON_ML4AML_EVENT_PORT	3036
PYTHON_ML4AML_PORT	3016
PYTHON_ML4AML_REST_PORT	3097
PYTHON_SANE_EVENT_PORT	3037
PYTHON_SANE_PORT	3017
PYTHON_SANE_REST_PORT	3087
SCHEMA_PORT	3003
SESSION_SERVICE_PORT	3047
STUDIO_SERVICE_PORT	3008
UI_PORT	3001
DATAPIPELINE_SERVICE_PORT1	8005
DATAPIPELINE_SERVICE_PORT2	8006
DATAPIPELINE_METADATA_IMPORT_SERVICE_PORT	8007
LOADGRAPH_BASE_URL	3059
MATCHRULE_BASE_URL	3051

5. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/bin directory.
6. Open **config.sh** file and update port numbers as mentioned in the following table.

Table A-6 config.sh.sh file

Service	Port Number
PGX_SERVER_URL	3007
Opensearch port	##OPEN_SEARCH_PORT##

A.8.2 Custom Port Number Validation for Compliance Studio

This section helps to validate port number changes for Compliance Studio service.

Batch Service

To view updated port number for batch service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/ batchservice/ conf directory.

2. Open **server-config.properties** file and view the port numbers as mentioned in the following table.

Table A-7 server-config.properties file

Service	Port Number
server.http.port	3043
server.shutdownPort	3044

Note

If the port numbers are not updated, manually update them and restart the Compliance Studio.

Entity Resolution Service

To view updated port number for entity resolution service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/entity-resolution/conf directory.
2. Open **application.yml** file and view the port numbers as mentioned in the following table.

Table A-8 application.yml file

Service	Port Number
port	3051
matchingService	3049
graphService	3059

3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/bin directory.
4. Open **config.sh** file and view the ER_SERVICE_PORT as 3051.

FCC UI Service

To view updated port number for FCC UI service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/fcc-ui/conf directory.
2. Open **application.yml** file and view port numbers as mentioned in the following table.

Table A-9 application.yml file

Service	Port Number
port	3061
erserviceUrl	3051
metaserviceUrl	3045
batchserviceUrl	3043
loadToOsServiceUrl	3053
graphserviceUrl	3059
mmgUIServiceUrl	3002

Table A-9 (Cont.) application.yml file

Service	Port Number
BASE_URL	3002
mmg url	3001

3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/bin directory.
4. Open **config.sh** file and view port numbers as mentioned in the following table.

Table A-10 config.sh file

Service	Port Number
ER_SERVICE_URL	3051
MMG_SVC_URL	3002
META_SERVICE_URL	3045
GRAPH_SERVICE_URL	3059
LOAD_TO_OS_SERVICE_URL	3053
BATCH_SERVICE_URL	3043
MMG_UI_URL	3001

Note

If the port numbers are not updated, follow these steps:

- a. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/mmg-gateway/conf/routes directory.
- b. Open the **fcc-routes.csv** file and update the port numbers manually.
- c. Restart Compliance Studio.

Load to Elastic Search Service

To view updated port number for load to elastic search service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/load-to-es/ conf directory.
2. Open **application.yml** file and view port numbers as mentioned in the following table.

Table A-11 application.yml file

Service	Port Number
server.port	3053
index.logstash-conf.port	##LOGSTASH_PORT##
index.es-conf.port	##ELASTIC_SEARCH_PORT##
dataPipelineService.url	8006
pipelineService.url	8005

Load to OpenSearch Service

To view updated port number for load to opensearch service, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/load-to- open-search/conf` directory.
2. Open **application.yml** file and view port numbers as mentioned in the following table.

Table A-12 application.yml file

Service	Port Number
server.port	3053
index.logstash-conf.port	##LOGSTASH_PORT##
index.open-search-conf.port	##OPEN_SEARCH_PORT##
dataPipelineService.url	8006
pipelineService.url	8005

Matching Service

To view updated port number for matching service, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/matching-service/conf` directory.
2. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-13 application.yml file

Service	Port Number
opensearch.port	##OPEN_SEARCH_PORT##
server.port	3049

Note

If the port numbers are not updated, manually update them and restart the Compliance Studio.

Matching Service for Elastic Search

To view updated matching service port number for elastic search, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/matching-service-es/conf` directory.
2. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-14 application.yml file

Service	Port Number
es.port	##ELASTIC_SEARCH_PORT##
server.port	3049

Meta Service

To view updated port number for meta service, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/metaservice/conf` directory.
2. Open **server-config.properties** file and view port numbers as mentioned in the following table.

Table A-15 application.yml file

Service	Port Number
server.http.port	3045
server.shutdownPort	3046

Note

If the port numbers are not updated, manually update them and restart the Compliance Studio.

Scheduler Service

Users need to view port numbers in the `aaicl_ss_batch_url` table as follows:

- WORKSPACE URL: `https://<Test Server>.com:3002/cs`
- MMG_SERVICE_URL: `https://<Test Server>.com:3002/cs`
- CS_SERVICE_URL: `https://<Test Server>.com:3002/cs`

PGX Service

To view updated port number for PGX service, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/pgx/pgx-server/bin` directory.
2. Open **config.sh** file and view port number in the `GRAPH_SERVICE_URL` as 3059.

For In-memory Graph Service

If PGX is already running in-memory graph, you need to truncate the following tables to generate the views again:

- `fcc_pgx_m_config`
- `fcc_graph_m_config_json`

Scenario Conversion Utility (SCU) Notebook

To view updated port numbers in the SCU notebooks, follow these steps:

1. Open SCU notebook and navigate to **Generate Scenario(s)** paragraph.
2. Click **Visibility** icon and select **Code** option.
3. View port numbers in the following urls:

- `obj_url= "https://<Test Server>.com:3002/cs/v1/model-service/ModelController/ADD_OBJECTIVES"`
- `url= "https://<Test Server>.com:3002/cs/v1/model-service/ ModelController/CREATE_NOTEBOOK"`

Note

If the port numbers are not updated, manually update them and restart the Compliance Studio.

A.8.3 MMG and Data Studio Configuration

To update port number for MMG and Data Studio services, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/bin` directory.
2. Open **config.sh** file and update port numbers as mentioned in the following table.

Table A-16 config.sh file

Service	Port Number
BE_PORT	3002
UI_PORT	3001
SCHEMA_PORT	3003
SAML_SP_ENTITY	3001
SAML_SRV_URL	3001
AUTH_SERVICE_URL	3001
META_SERVICE_URL	3045
ER_SERVICE_URL	3051
BATCH_SERVICE_URL	3043
SAML_ISSUER	3008
SAML_ASSERTION	3008
DATAPIPELINE_SERVICE_PORT1	8005
DATAPIPELINE_SERVICE_PORT2	8006
DATAPIPELINE_METADATA_IMPORT_SERVICE_PORT	8007
DATAPIPELINE_GATEWAY_SERVICE_PORT	3063
PIPELINE_UI_SERVICE_PORT	3065
DATA_PIPELINE_UI_SERVICE_PORT	3067
MATCHRULE_BASE_URL	3051
LOADGRAPH_BASE_URL	3059
MATCHSRVC_UI_URL	3061
GRAPH_INDEX_BASE_URL	3053
LOADINDEX_UI_URL	3061
GRAPH_SERVICE_PORT	3059
PGX_SERVER_URLS	3007

3. Open **EICSchedulerService.sh** file and update `BASE_URL` as 3001.

4. Open **Shutdown.sh** file and update port numbers as mentioned in the following table.

Table A-17 Shutdown.sh file

Service	Port Number
uiHealth	3001
serviceHealth	3002
schemaHealth	3003
dsHealth	3008
dpHealth	8005

5. Open **install.sh** file and update DATASTUDIO_URL as 3008.

A.8.4 Custom Port Number Validation for MMG and Data Studio Services

This section helps to validate port number changes for MMG and Data Studio services.

MMG Graph Service

To view update port number for MMG graph service, follow these steps:

1. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-load-to-graph/graph-service/bin` directory.
2. Open **config.sh** file and view port numbers as mentioned in the following table.

Table A-18 config.sh file

Service	Port Number
GRAPH_SERVICE_URL	3059
GRAPH_SERVICE_PORT	3059
ER_SERVICE_URL	3051
GRAPH_DATA_PIPELINE_URL	8006
MMG_SERVICE_URL	3002
PGX_SERVER_URL	3007

3. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-load-to-graph/graph-service/conf` directory.
4. Open **application.yml** file and view port numbers as mentioned in the following table.

Table A-19 application.yml file

Service	Port Number
port	3059
mmg-url	3002
jdbcUrl	##JDBC_PORT##
dataPipeline-url	8006
pgx-url	3007
entityResolution-url	3051

5. Navigate to `<OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-load-to-graph/graph-service/utility/bin` directory.

6. Open **CreatePasswordlessKeystore.sh** file and view graphServiceUrl port number as 3059.
7. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-load-to-graph/graph-service/utility/bin directory.
8. Open **ResetGraphMetadata.sh** file and view graphServiceUrl port number as 3059.
9. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-load-to-graph/graph-service/utility/bin directory.
10. Open **SetConnectionPoolConfig.sh** file and view graphServiceUrl port number as 3059.

MMG Pipeline Service

Note

Users cannot update hazelcast port number manually.

To view updated port number for MMG pipeline, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/data-metadata-job-<version>/conf directory.
2. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-20 application.properties file

Service	Port Number
server.port	8007
pipeline.url	8005

3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/data-pipeline-service-<version>/conf directory.
4. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-21 application.properties file

Service	Port Number
server.port	8006
mmg.url	3002
pipeline.url	8005
cors.url	3063
datapipeline.url	8006

5. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/data-pipeline-service-UI-<version>/conf directory.
6. Open application.properties file and view port numbers as mentioned in the following table.

Table A-22 application.properties file

Service	Port Number
server.port	3067
mmg.url	3002
pipeline.url	8005
cors.url	3063
datapipeline.url	8006

7. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/pipelinegateway/conf directory.
8. Open application.properties file and view port numbers as mentioned in the following table.

Table A-23 application.properties file

Service	Port Number
server.port	3063
mmgservice.uri	3002
pipelineservice.uri	8005
pipelineserviceui.uri	3065
datapipelineservice.uri	8006
datapipelineserviceui.uri	3067

9. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/pipeline-service-<version>/conf directory.
10. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-24 application.properties file

Service	Port Number
server.port	8005
mmgurl	3002
pipeline.url	8005
cors.url	3063
datapipeline.url	8006
gatewayUrl	8006

11. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/pipeline-service-<version>/files directory.
12. Open **Metadata_DATA_3.json** file and view "nPortNumber" as "8080".
13. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-pipeline/pipeline/pipeline-service-UI-<version>/conf directory.
14. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-25 application.properties file

Service	Port Number
server.port	3065
mmr.url	3002
pipeline.url	8005
cors.url	3063
datapipeline.url	8006
gatewayUrl	8006

MMG Schema Creator Service

To view updated port number for MMG schema creator, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-schema-creator/conf directory.
2. Open **application.properties** file and view server.port as 3003.
3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-schema-creator/bin directory.
4. Open **config.sh** file and view port numbers as mentioned in the following table.

Table A-26 config.sh file

Service	Port Number
SCHEMA_PORT	3003
DATASTUDIO_URL	3008
BE_PORT	3002
UI_PORT	3001
DATAPIPELINE_UI_URL	3063

5. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-schema-creator/bin directory.
6. Open **startup.sh** file and view port numbers as mentioned in the following table.

Table A-27 startup.sh file

Service	Port Number
schemaHealth	3003
	Note: Search and view in two places
graphschemaHealth	3003

MMG Service

To view updated port number for MMG service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-service/conf directory.
2. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-28 application.properties file

Service	Port Number
server.port	3002
BASE_URL	3002
GRAPH_DATA_PIPELINE_URL	3063
GRAPH_MR_PIPELINE_URL	3051
GRAPH_MATCH_RULE_BASE_URL	3051
GRAPH_LOAD_GRAPH_BASE_URL	3059
GRAPH_DATAPIPELINE_SERVICE_URL	8006
GRAPH_INDEX_BASE_URL	3053

3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-service/bin directory.
4. Open **config.sh** file and view port numbers as mentioned in the following table.

Table A-29 config.sh file

Service	Port Number
DATASTUDIO_URL	3008
BE_PORT	3002
DATAPIPELINE_URL	3063
MATCHRULE_BASE_URL	3051
LOADGRAPH_BASE_URL	3059
DATAPIPELINE_SERVICE_URL	8006
GRAPH_INDEX_BASE_URL	3053

5. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-service/bin directory.
6. Open **startup.sh** file and view serviceHealth port number as 3002 in two places.

MMG Studio Service

To update port number for MMG studio service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/conf directory.
2. Navigate to line 9, press **Enter** and add the following lines.

```
thrift-server:
enabled: true
port: 3432
mode: TCP
```

3. Open **application.yml** file and view port numbers as mentioned in the following table.

Table A-30 application.yml file

Service	Port Number
mmgserviceUrl	3002

Table A-30 (Cont.) application.yml file

Service	Port Number
authserviceUrl	3041
metaserviceUrl	3045
erserviceUrl	3051
batchserviceUrl	3043
saml-issuer	3008
saml-assertion-consumer-service-url	3008

4. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/bin directory.
5. Open **config.sh** file and view port numbers as mentioned in the following table.

Table A-31 config.sh file

Service	Port Number
MMG_SVC_URL	3002
DATASTUDIO_URL	3008
PGX_SERVER_URL	3007
AUTH_SERVICE_URL	3041
META_SERVICE_URL	3045
ER_SERVICE_URL	3051
BATCH_SERVICE_URL	3043
SAML_ISSUER	3008
SAML_ASSERTION	3008

6. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/bin directory.
7. Open **Startup.sh** file, navigate to line 14 and press **Enter**.
8. Add the following lines.

```
export STUDIO_INTERPRETER_PYTHON_INTERPRETER_REST_SERVER_PORT=3038
export STUDIO_INTERPRETER_PGX_PYTHON_INTERPRETER_REST_SERVER_PORT=3039
export DS_EVENT_HANDLER_HOST=localhost
export DS_EVENT_HANDLER_PORT=3432
```

9. Search dsHealth and view port number as 3008.
10. Navigate to HADOOP_HOME parameter and press **Enter**.
11. Add the following lines.

```
. ./"$DIR"/datastudio --jdbc -1 --shell -1 --external --port 3008 --jdbc
3011 --python 3012 --markdown 3009 --spark 3014 --pgx 3022 --url http://
localhost:3007
exec "$JAVACMD" "$@" &> "$DIR"/nohup.out &
```

12. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/bin directory.
13. Open **Shutdown.sh** file and view port numbers as mentioned in the following table.

Table A-32 Shutdown.sh file

Service	Port Number
I7009	3009
I7011	3011
I7012	3012
I7013	3013
I7019	3019
I7022	3022

14. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/bin directory.
15. Open **install.sh** file and view DATASTUDIO_URL as 3008.

Interpreter Service

To view updated port number for interpreter service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/jdbc-interpreter-<version>/bin directory.
2. Open **jdbc-interpreter** file and view 3011 port number in the classpath.
3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/fcc-interpreter-<version>/bin directory.
4. Open **fcc-interpreter** file and view 3011 port number in the classpath.

Note

If the port numbers are not updated, manually update them and restart the Compliance Studio.

5. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/markdown-interpreter-<version>/bin directory.
6. Open **markdown-interpreter** file and view 3009 port number in the classpath.
7. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/pgx-interpreter-<version>/bin directory.
8. Open **pgx-interpreter** file and view 3022 port number in the classpath.
9. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/plainr-interpreter-<version>/bin directory.
10. Open **plainr-interpreter** file and view 3019 port number in the classpath.
11. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/python-interpreter-<version>/bin directory.
12. Open **python-interpreter** file and view 3012 port number in the classpath.
13. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/spark-interpreter-<version>/bin directory.
14. Open **spark-interpreter** file and view 3014 port number in all three places.
15. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/interpreter-server/pgx-interpreter-<version>/conf directory.

16. Open **graph-client.properties** file and view port numbers as mentioned in the following table.

Table A-33 graph-client.properties file

Service	Port Number
graphServiceUrl	3059
erserviceUrl	3051

17. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
18. Open **spark.json** file, view port number 3014 under "lifecycleConfig" and port number 3077 under "spark.master".
19. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
20. Open **python.json** file and view port number 3012 under "lifecycleConfig".
21. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
22. Open **pgx.json** file, view port number 3022 under "lifecycleConfig" and port number 3077 under "interpreterClientConfigs".
23. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
24. Open **markdown.json** file view port number 3009 under "lifecycleConfig".
25. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
26. Open **jdbc.json** file and view port number 3012 under "lifecycleConfig".
27. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
28. Open **fcc-python-sane.json** file view port number 3017 under "lifecycleConfig".
29. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
30. Open **fcc-python-ml4aml.json** file and view port number 3016 under "lifecycleConfig".
31. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-studio/server/builtin/interpreters directory.
32. Open **fcc-python.json** file and view port number 3010 under "lifecycleConfig".

MMG UI Service

To view updated port number for MMG UI service, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-ui/conf directory.
2. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-34 application.properties file

Service	Port Number
server.port	3001
BASE_URL	3002
saml.auth.sp.entity	3001
saml.auth.consumerserviceurl	3001
DP_UI_URL	3063
MATCHSRVC_UI_URL	3061
LOADINDEX_UI_URL	3061

3. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-ui/conf directory.
4. Open **application.properties** file and view port numbers as mentioned in the following table.

Table A-35 application.properties file

Service	Port Number
DATASTUDIO_URL	3008
BE_PORT	3002
UI_PORT	3001
SAML_SP_ENTITY	3001
SAML_SRV_URL	3001
DATAPIPELINE_URL	3063
DATAPIPELINE_UI_URL	3063
MATCHSRVC_UI_URL	3061
LOADINDEX_UI_URL	3061

5. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ mmg-ui/bin directory.
6. Open **startup.sh** file and view uiHealth port number as 3001 in two places.

Notification Service

To update coherence cluster port, follow these steps:

1. Navigate to <OFS_COMPLIANCE_STUDIO_INSTALLATION_PATH>/deployed/mmg-home/ conf/ aai-notifications-service directory.
2. Open **cache-config-notif.xml** file, navigate to line 12 and add the following lines.

```
<cluster-config>
<multicast-listener>
<port system-property="coherence.clusterport">3206</port>
</multicast-listener>
</cluster-config>
```

3. Restart Compliance Studio.

A.8.5 Database Validation

Connect to Studio Schema and view updated port numbers in the **MMG_MENU** table as mentioned in the following table.

Table A-36 MMG_MENU Table

Service URL	Port Number
Match Rules	3001
Merge Rules	3001
Data Survival	3001
Manual Decisioning	3001
Merge and Split Global Entities	3001

Connect to Studio Schema and view updated port numbers in the **nextgenemf_config** table as mentioned in the following table.

Table A-37 nextgenemf_config Table

Service	Port Number
EMFSTUDIO_SERVICE_URL	3002
BASE_URL	3002
DATASTUDIO_URL	3008