Oracle® Financial Services Crime and Compliance Studio Application

Installation Guide

Release 8.0.6.0.0

E91246-01

Dec 2018

ORACLE®

Installation Guide, Release 8.0.6.0.0

E91246-01

Primary Author: Nethravathi G

Contributor: Swetha Yatham, Parthik Davda

Contents

List of Figures

List of Tables

Document Control

This section provides the revision details of the document.

Version Number	Revision Date	Changes Done
8.0.6.0.0	Created: May 2018	Created first version of Oracle Financial Services Crime and Compliance Studio Installation Guide for 8.0.6.0.0 Release.
8.0.6.0.1	Created: Dec 2018	▪ Created the Hive Data Movement and Oracle DB Data Movement sections in the Post Installation Configuration chapter. ▪ Created the Enabling VPD section in the Post Installation configuration chapter.

This document includes the necessary instructions to install the OFS Crime and Compliance Studio application and perform the required post installation configurations.

Preface

This section provides supporting information for the OFS Crime and Compliance Studio application Installation Guide and includes the following topics:

Summary

Before you begin the installation, ensure that you have access to the Oracle Support Portal with valid login credentials to quickly notify us of any issues at any stage. You can obtain the login credentials by contacting Oracle Support.

Audience

The Installation Guide is intended for System Engineers who are responsible for installing and configuring the OFS Crime and Compliance Studio Application's components.

Prerequisites for the Audience

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

- Scala, PGQL, and PGX
- UNIX commands
- Database concepts
- Web Application Server
- Big Data

Related Documents

This section identifies additional documents related to OFS Crime and Compliance Studio application. You can access the following documents from Oracle Help Center (OHC) Documentation Library:

- *Oracle Financial Services Crime and Compliance Studio Administration Guide*

- *Oracle Financial Services Crime and Compliance Studio User Guide*
- *Oracle Financial Services Crime and Compliance Studio Release Notes*

Conventions

The following table lists the text conventions used in this document:

Table 0–1 Conventions Used in this Guide

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Abbreviations

The following table lists the abbreviations used in this document:

Table 0–2 Abbreviations and Their Meaning

Abbreviation	Meaning
OFS	Oracle Financial Services
HTTPS	Hypertext Transfer Protocol Secure
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
LHS	Left Hand Side
MOS	My Oracle Support
OS	Operating System
SFTP	Secure File Transfer Protocol
URL	Uniform Resource Locator
WAR	Web application ARchive
JAR	Java ARchive
PGX	Parallel Graph AnalytiX
PGQL	Property Graph Query Language
XML	Extensible Markup Language

1

Understanding Crime and Compliance Studio Application Installation

This chapter provides necessary information required to understand the installation of the Oracle Financial Service (OFS) Crime and Compliance Studio application.

This chapter includes the following topics:

Installation Overview

You can download this installer to install a new instance of the OFS Crime and Compliance Studio application. Figure 1–1 shows the order of procedures required to install a new instance of the Studio application.

Figure 1–1 **Installation Overview**

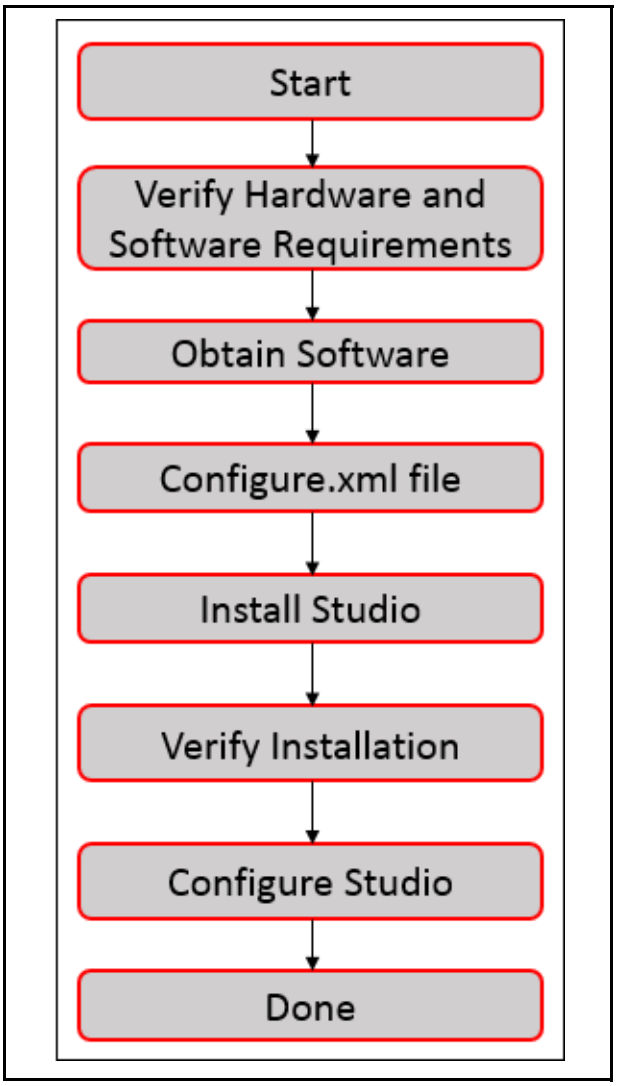


Table 1–1 provides additional information to specific documentation for each task in the flowchart.

Table 1–1 Studio Application Installation Tasks and Descriptions

Tasks	Details and Documentation
Verify Hardware and Software requirements	To verify that your system contains the required hardware and software requirements to install the Studio application, see Hardware and Software Requirements.
Obtain the Software	To access and download the Crime and Compliance Studio application, see Obtaining the Software.
Configure.XML File	To configure the XML file, see Configuring InstallConfig.xml.
Install Studio Application	To install the Crime and Compliance Studio application, see Installing the Studio Application.
Verify Installation	To verify installation of Crime and Compliance Studio application, see Verifying Installation.

Table 1–1 Studio Application Installation Tasks and Descriptions

Tasks	Details and Documentation
Configure Studio Application	To configure Crime and Compliance Studio application, See Post Installation Configurations.

Hardware and Software Requirements

This section describes the various Operating Systems, Database, Web Server, and Web Application Server versions, and other variant details on which this release of the Studio application is qualified. For information on the requirements, see Oracle Help Center (OHC) Documentation Library.

Configurations Supported for Java 8

Table 1–2 Configurations Supported for Java 8

BIG DATA	
Cloudera Distribution Hadoop 5.12	▪ CDH Version 5.12 ▪ Hadoop-2.5.0+cdh5.3.3+844 ▪ Hive-0.13.1+cdh5.3.3+350 ▪ Sqoop1 V 1.4.4+cdh5.3.3+67
Cloudera Hive Connectors	Hive JDBC Connectors V 2.5.15
Oracle R Advanced Analytics for Hadoop	Oracle R Advanced Analytics for Hadoop (ORAAH) 2.4.0
Hadoop Security Protocol	▪ Kerberos R release 1.6.1 ▪ Sentry-1.4.0
Hortonworks Data Platform (HDP 2.5)	▪ CDH Version 2.5 ▪ Hadoop-2.7.3+hdp2.5+844 ▪ Hive-1.2.1+hdp2.5+350 ▪ Sqoop1 V 1.4.4+hdp2.5+67 ▪ Sqoop2 V 1.99.4+hdp2.5+23 ▪ Oracle Loader For Hadoop (OLH) V 3.2
Hortonworks Hive Connectors	Hive JDBC Connectors V 2.5.15
Oracle R Advanced Analytics for Hadoop	Oracle R Advanced Analytics for Hadoop (ORAAH) 2.4.0
Hadoop Security Protocol	▪ Kerberos 5 release 1.6.1 ▪ Sentry-1.4.0

2

Preparing for Installation

Note:

Release 8.0.6.0.0 of OFS Crime and Compliance Studio is not fully backward compatible with earlier versions of FCCM application. You must upgrade all of your FCCM application from existing 8.0.x versions to 8.0.6.0.0 version and cannot choose to upgrade only selective application packs to v8.0.6.0.0.

This chapter provides necessary information to review before installing the OFS Crime and Compliance Studio application.

This chapter includes the following sections:

- Installer and Installation Prerequisites
- Obtaining the Software
- Performing Common Pre-Installation Tasks

Installer and Installation Prerequisites

Table 2–1 provides the list of prerequisites required before beginning the installation of the Studio application. The Installer or Environment Check Utility notifies you if any requirements are not met.

Table 2–1 Prerequisite Information

Category	Sub-Category	Expected Value
Environment Settings	PGX Settings	PGX_HOME path and SPARK_HOME path needs to be set in the Environment variables
	Java Settings	▪ PATH in .profile to be set to include the Java Runtime Environment absolute path. The path should include java 8. **Note:** ▪ Ensure the absolute path to JRE/bin is set at the beginning of PATH variable. ▪ For example, PATH=/usr/java/jre1.8/bin:$ORACLE_HOME/bin:$PATH ▪ Ensure no SYMBOLIC links to JAVA installation is being set in the PATH variable
	Oracle Database Settings	**Oracle Database Server** ▪ TNS_ADMIN to be set in .profile file pointing to appropriate tnsnames.ora file. ▪ Enable Transparent Data Encryption (TDE) and/ or Data Redaction** ** Note: For more information, see Appendix F, "Configuring TDE and Data Redaction in OFSAA". **Oracle Processing Server** ▪ ORACLE_HOME to be set in .profile file pointing to appropriate Oracle DB Client installation. ▪ PATH in .profile to be set to include appropriate $ORACLE_HOME/bin path ▪ Ensure to add an entry (with SID/ SERVICE NAME) is added in the tnsnames.ora file.
	MySQL Database Schema Settings	Install a MYSQL Database on server and create a schema. This schema will be used by Data Studio to store the metadata. Enter the URL of the newly created schema in the MYSQL_JDBC_URL parameter in InstallConfig.xml file.
	Tomcat Settings	Set the following in .profile file: CATALINA_HOME=<TOMCAT_PATH> export CATALINA_HOME
	Installation Directory	A directory where the installation files will be installed. User permission is set to 755 on the installation directory.
	Download Directory	A directory where the product installer file will be downloaded/ copied. Ensure user permission is set to 755 on the Download directory.
	OS Locale	▪ Linux: en_US.utf8 To check the locale installed, execute the following command: locale -a | grep -i 'en_US.utf'

Table 2–1 (Cont.) Prerequisite Information

Category	Sub-Category	Expected Value
	Oracle Database Schema Settings	Grant the following permissions to the newly created Oracle Database Schema: ■ GRANT create session TO <Schema User>; ■ GRANT create table TO <Schema User>; ■ GRANT create view TO <Schema User>; ■ GRANT create any trigger TO <Schema User>; ■ GRANT create any procedure TO <Schema User>; ■ GRANT create sequence TO <Schema User>; ■ GRANT ALL privileges TO <Schema User>; ■ Grant execute on dbms_rls to <Schema User>; ■ Grant execute on sys.dbms_session to <Schema User>; ■ ALTER USER <Schema User> QUOTA 100M ON users; ■ Grant create sequence to <Schema User>; ■ Grant create SYNONYM to <Schema User>; ■ Grant create any context to <Schema User>; ■ Grant execute on dbms_rls to <Schema User>;
Web Application Server	Tomcat	Apache Tomcat version must be 8.0 or above.

Obtaining the Software

This release of the Studio application can be downloaded from My Oracle Support. You must have a valid Oracle account to download the software and then search for the Bug ID **28082337** under the *Patches & Updates* tab.

Performing Common Pre-Installation Tasks

The common pre-installation activities that you must carry out before installing the Studio application are:

- Identifying the Installation, Download and Metadata Repository Directories
- Downloading Crime and Compliance Studio Application Installer
- Extracting the Software

Identifying the Installation, Download and Metadata Repository Directories

To install the Crime and Compliance Studio Application Pack, create the following directory which is typically the user home directory:

- **Studio Download Directory (Optional)**: Create a download directory and copy the Crime and Compliance Studio Application Installer File (archive). This is the directory where the downloaded installer/patches can be copied.

Downloading Crime and Compliance Studio Application Installer

To download and copy the Studio Application Installer, follow these steps:

1. Login to the My Oracle Support with a valid Oracle account and search for the Bug ID **28082337** under the *Patches & Updates* tab.
2. Download the installer archive OFS_FCCM_STUDIO_8.0.6.0.0.LINUX.zip file to the download directory (in Binary Mode) on the setup identified for Studio installation.

Extracting the Software

Note:

You must be logged in to the UNIX operating system as a non-root user.

---

1. Download the unzip utility (OS specific) `unzip_<os>.Z` and copy it in Binary mode to the directory where you want to install the application. If you already have the unzip utility to extract the contents of the downloaded archive, skip to Step 4.
2. Uncompress the unzip installer file with the following command:

   ```
   uncompress unzip_<os>.Z
   ```

   Note:

   In the error message, "uncompress: not found [No such file or directory]" is displayed, contact your UNIX administrator.

   ---

3. Assign EXECUTE permission to the file with the following command:

   ```
   chmod 751 unzip_<OS>
   ```

   For example, `chmod 751 unzip_sparc`
4. Extract the contents of the OFS_FCCM_STUDIO_8.0.6.0.0 installer archive file in the download directory with the following command:

   ```
   unzip OFS_FCCM_STUDIO_8.0.6.0.0.zip
   ```

   Note

   Do not rename the Application installer folder name on extraction from the archive.

   ---

5. Navigate to the download directory where the installer archive is extracted and assign execute permission to the installer directory with the following command:

   ```
   chmod -R 750 OFS_FCCM_STUDIO_PACK
   ```

3

Installing the Crime and Compliance Studio Application

This chapter provides the instructions to install the OFS Crime and Compliance Studio application.

This chapter includes the following topics:

- Installing the Studio Application
- Verifying Installation

Installing the Studio Application

This section provides instructions to install the OFS Services Crime and Compliance Studio application.

This topic includes the following sections:

- Configuring InstallConfig.xml
- Running the Installer
- Completing the Installation

Configuring InstallConfig.xml

> **Note:** While configuring for 8.0.6.0.1, make the following changes in the `PatchConfig.xml` file.

To configure the `InstallConfig.xml file`, follow below steps:

1. Log in to the system as non-root user.
2. Navigate to the `OFS_FCCM_STUDIO_PACK/OFS_FCCM_STUDIO/conf/InstallConfig.xml` file
3. Configure the `InstallConfig.xml` file as mentioned in Table 3–1.

   You must manually set the InteractionVariable parameter values as mentioned in the Table 3–1. If a value is not applicable, enter NA and ensure that the value is not entered as NULL.

Table 3–1 InstallConfig.xml Parameters

InteractionVariable Name	Significance	Used for Hive DataBase	Used for Oracle Database
##PGX_REQD##	Indicates whether PGX must be installed along with the installer Example: "true" The value true indicates that PGX must be installed with the installer. The value false indicates that PGX must not be installed with the installer.	Yes	Yes
##PGX_ INSTALATION_ PATH##	Indicates the installation path of the PGX server. Example: <Studio_Installed_Path>/studio	Yes	Yes
##PGX_PGB_PATH##	Indicates the PGB file path on HDFS. Example: hdfs:/user/ofsaa	Yes	Yes
##PGX_SERVER_ URL##	Indicates the URL of the PGX server. Example: http://<HOSTName>:<PortNo>/ The value for the PortNo must be 7007.	Yes	Yes
##DATA_STUDIO_ INSTALLATION_ PATH##	Indicates the path where Studio is to be installed.	Yes	Yes
##OFSAA_SERVICE_ URL##	Indicates the URL of the OFSAA instance. Do not enter '/' at the end of the URL. **Note:** ■ For OFSAAI version 8.0.6.0.0., the value must be in the following format: https://<HOSTName>:<PortNo>/<ContextName>/rest-api	Yes	Yes
##META_SERVICE_ URL##	Indicates the metaservice URL which will get activated after deployment of the .war file in TOMCAT. The format for the metaservice URL is as follows: http://<HOSTName>:<PortNo>/metaservice	Yes	Yes
##SESSION_SERVICE_ URL##	Indicates the session service URL which will get activated after deployment of the .war file in TOMCAT.	Yes	Yes
##AUTH_SERVICE_ URL##	Indicates the AUTH service URL which will get activated after deployment of the .war file in TOMCAT.	Yes	Yes
##SOURCE_ DATABASE_URL##	Indicates the JDBC URL of the OFSAA instance.	Yes	Yes
##STUDIO_ DATABASE_URL##	Indicates the newly created schema database URL.	Yes	Yes
##JDBC_DRIVER##	Indicates the Oracle database driver. This must be a unique value.	Yes	Yes
##STUDIO_DB_ USERNAME##	Indicates the username for the newly created schema.	Yes	Yes

Table 3–1 (Cont.) InstallConfig.xml Parameters

InteractionVariable Name	Significance	Used for HIve DataBase	Used for Oracle Database
##STUDIO_DB_ PASSWORD##	Indicates the password for the newly created schema.	Yes	Yes
##SRC_DB_CONFIG_ USRNAME##	Indicates the config schema username of the OFSAA or BD instance.	Yes	Yes
##SRC_DB_CONFIG_ PASSWORD##	Indicates the config schema password of the OFSAA or BD instance.	Yes	Yes
##DATAMOVEMENT_ LINK_NAME##	If the newly created schema is in a different database host, then you must create a DB link and provide the same link in this parameter. Alternatively, you can provide the source schema name.	Yes	Yes
##DATAMOVEMENT_ LINK_TYPE##	If DB link is used, enter DBLINK in this field. If DB link is not used, enter SCHEMA in this field.	Yes	Yes
##SQOOP_TRG_ HOSTNAME##	Indicates the host name of the SQOOP web server. Example: `<HOSTName>`	Yes	No
##SQOOP_ PARAMFILE_PATH##	Indicates the path of the SQOOP property file. The path should point to the `datamovement_ properties` file, which will be made available in the `<Studio_Installed_Path>/studio` path after completion of the installation. Example: `<Studio_Installed_ Path>/datamovement_properties/`	Yes	No
##SQOOP_WORKDIR_ HDFS##	Indicates the SQOOP working directory in HDFS.	Yes	No
##SQOOP_ PARTITION_COL##	Indicates the column in which the HIVE table is partitioned. The value must be `SNAPSHOT_DT`	Yes	No
##LIVY_HOST_URL##	Indicates the URL of the Livy application. The format for the URL is as follows: `http://<HOSTName>:<PortNo>`	Yes	No
##HIVE_SCHEMA##	Indicates to create schema in HIVE.	Yes	No
##FSINFODOM##	Indicates the name of the OFSAA or BD Infodom.	Yes	Yes
##FSSEGMENT##	Indicates the name of the OFSAA or BD segment.	Yes	Yes
##JAAS_CONF_FILE_ PATH##	Created for future use.	No	No
##KRB5_CONF_FILE_ PATH##	Created for future use.	No	No
##security_krb5_ realm##	Created for future use.	No	No
##server_kerberos_ keytab_file##	Created for future use.	No	No
##security_krb5_kdc_ server##	Created for future use.	No	No
##server_kerberos_ principal##	Created for future use.	No	No

Table 3–1 (Cont.) InstallConfig.xml Parameters

InteractionVariable Name	Significance	Used for HIve DataBase	Used for Oracle Database
##MYSQLDB_JDBC_ URL##	Enter details for the MYSQL database created schema. This schema will be used by Data Studio to store the metadata.	Yes	Yes
##MYSQLDB_ROOT_ PASSWORD##	Enter password for the MYSQL database created schema.	Yes	Yes
BDSCHEMA_DB_ HOST_NAME	Indicates the BD Schema database host name.	Yes	Yes
BDSCHEMA_DB_ PORT_NUMBER	Indicates the BD Schema port number.	Yes	Yes
BDSHEMA_DB_ SERVICE_NAME	Indicates the BD Schema database service name.	Yes	Yes
HADOOP_ CREDENTIAL_ PROVIDER_PATH	Indicates the path where Hadoop credential is stored like	Yes	No
HADOOP_ PASSWORD_ALIAS	Indicates the Hadoop alias given while creating the hadoop credentials like	Yes	No
SQOOP_ HOSTMACHINE_ USER_NAME	Indicates the user name of Host machine where sqoop will run.	Yes	No
BDSCHEMA_DB_ USER_NAME	Indicates the BD Schema database username.	Yes	Yes
BATCH_SERVICE_URL	Indicates the batch service URL.	Yes	Yes
Hive_Host_Name	Indicates the Hive host name.	Yes	No
Hive_Port_number	Indicates the Hive port number.	Yes	No
Krb_Service_Name	Indicates the Krb service name.	Yes	No
Krb_Host_FQDN_ Name"	Indicates the Krb host FQDN name.	Yes	No
Krb_Realm_Name	Indicates the Krb realm name.	Yes	No
HIVE_PRINCIPAL	Indicates the Hive Principal.	Yes	No
SOL_VERSION	Indicates the SQL version.	Yes	Yes

Running the Installer

To run the installer, follow these steps:

1. Navigate to the `OFS_FCCM_STUDIO_PACK/OFS_FCCM_STUDIO/bin` directory.
2. Execute the following command in the console:

```
./setup.sh
```

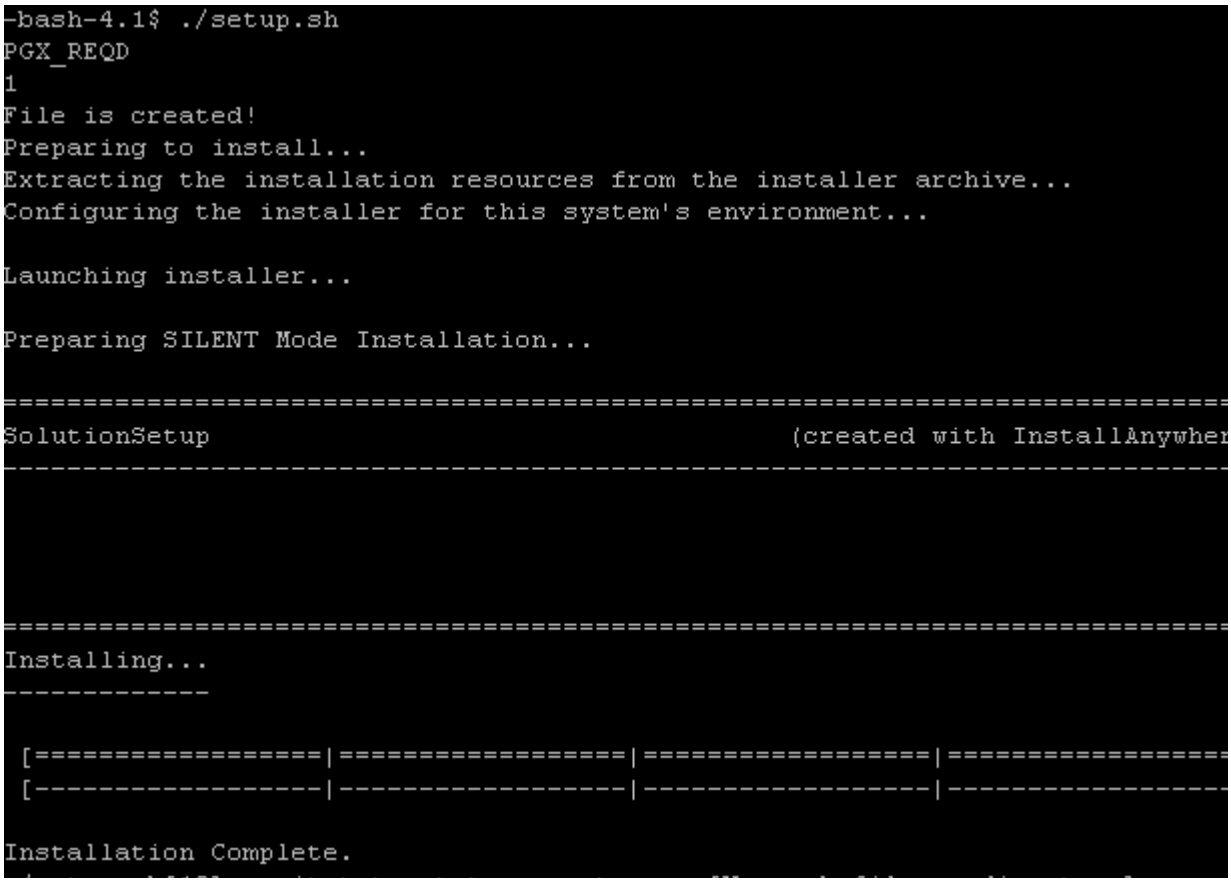
Note:: While running the installer for 8.0.6.0.1, execute the following command in the console:

```
./install.sh
```

Completing the Installation

A confirmation message is displayed to indicate the completion of the installation. On launching the installer, the environment check utility is executed. Figure 3–1 shows the success message displayed after successful installation.

Figure 3–1 Installation Complete



Verifying Installation

To verify the installation, verify the following log files:

See the `OFS_CCMS_LOG.log` file located in the `/OFS_FCCM_STUDIO_PACK/OFS_FCCM_STUDIO/logs` directory.

Note: Any errors encountered in the process is displayed with an appropriate error code. Do not proceed with further installation and contact Oracle Support with relevant log files.

4

Post Installation Configurations

On successful installation of the OFS Crime and Compliance Studio application, follow these post installation steps:

This chapter includes the following sections:

- Configuring Resource Reference
- Deploying the Application Pack Web Archive
- Hive Data Movement
- Oracle DB Data Movement
- Enabling VPD
- Configuring PGX
- Starting Studio Services

> **Note:** Ensure to clear the application cache prior to the deployment of Application Pack Web Archive. This is applicable for all Web Servers (Weblogic and Tomcat). For more information on clearing application cache, see Appendix E, "Clearing Application Cache".

Configuring Resource Reference

Configure the resource reference in the Web Application Server (Weblogic and Tomcat) configured for the Studio application. For details on configuring the resource reference in WebLogic and Tomcat Application Servers, see Appendix A, "Configuring Resource Reference in Web Application Servers".

Deploying the Application Pack Web Archive

On successful installation of the Studio application, the Studio metaservice application pack web archive is automatically generated. However you must deploy the generated Studio metaservice application pack web archive on the web application server (Weblogic and Tomcat).

To deploy the Studio metaservice application pack web archive, follow these steps:

1. Navigate to the `<Studio_Installed_Path>/datastudio_metaservice` directory.
2. Deploy the generated metaservice `EAR/WAR` file on to the web application server (Weblogic and Tomcat). For detailed information, see Appendix B, "Deploying EAR/ WAR File".

Hive Data Movement

This section includes the following topics:

Obtain Required Files

To obtain required files, follow these steps:

1. Rename the keytab file as `ofsaa.keytab`.
2. Place the `krb5.conf` and `keytab` file in the `$$<CATALINA_HOME/conf` path.

Configuring Schema Creation

To configure Schema Creation, follow these steps:

1. Set `FIC_DB_HOME` path to `<Studio_Installed_Path>/ficdb`.
2. Copy all the jar files located in the `<Studio_Installed_Path>/ficdb/lib` path to the `<OFSAA_FIC_HOME_PATH>/ficdb/lib` path.
3. Create a Hive Schema with the name mentioned in the `HIVE_SCHEMA` parameter in the `InstallConfig.xml` file.

   For information on InstallConfig.xml file, see Configuring InstallConfig.xml.
4. Create tables in Hive Schema by executing the shell script in `<Studio_Installed_PATH>/ficdb/bin/FCCM_Studio_SchemaCreation.sh HIVE`.

   This creates tables in the Hive Schema.

Creating Credential Keystore

To create credential keystore, follow these steps:

1. Login as HDFS SuperUser.
2. Create a credential keystore on HDFS by executing the following command:

   ```
   hadoop credential create mydb.password.alias -provider
   jceks://hdfs/user/root/oracle.password.jceks
   ```
3. Verify the credential keystore file by executing the following list command:

   ```
   hadoop credential list -provider
   jceks://hdfs/user/root/oracle.password.jceks
   ```
4. Grant Read permission to the keystore file by executing the following command:

   ```
   hadoop fs -chmod 744 /user/root/oracle.password.jceks
   ```

Note: Ensure the credential keystore file path and the alias is given correctly in the `Installconfig.xml` file.

Performing Data Movement and Graph Load

To perform Data Movement and Graph Load, follows these steps:

1. Go to the <Studio_Installed_Path>/ficdb/bin/ path.
2. Execute the FCCM_Studio_SqoopJob.sh file with the required parameters as follows:

   ```
   ./FCCM_Studio_SqoopJob.sh <Batch Name> <Batch ID> EXEC <FIC_MIS_Date>
   SNAPSHOT_DT=<SNAPSHOT_Date>,DATAMOVEMENTCODE=ALL
   ```

Oracle DB Data Movement

This section includes the following topics:

Configuring Schema Creation

To configure Schema Creation, follow these steps:

1. Set FIC_DB_HOME path to <Studio_Installed_Path>/ficdb in.profile.
2. Copy all the jar files located in the <Studio_Installed_Path>/ficdb/lib path to the <OFSAA_FIC_HOME_PATH>/ficdb/lib path.
3. Create tables in Oracle DB Studio Schema by executing the shell script in <Studio_Installed_PATH>/ficdb/bin/FCCM_Studio_SchemaCreation.sh ORACLE.

   This creates tables in the Studio Schema.

Performing Data Movement

To perform Data Movement, follows these steps:

1. Go to the <Studio_Installed_Path>/ficdb/bin/ path.
2. Provide select grant from the Source Atomic Schema as follows:

   ```
   GRANT select ON <TABLE NAME> to <STUDIO SCHEMA NAME>;
   ```

   Note:

   - The Table Name can be obtained from the SCHEMA_SRC_OBJ_NAME column of the fcc_datastudio_schemaobjects table.
   - Ensure to provide Grants to any newly added tables as well.

3. Execute the FCCM_Studio_DB_DataMove.sh file with the required parameters as follows:

   ```
   ./FCCM_Studio_DB_DataMove.sh <Batch Name> <Batch ID> EXEC <FIC_MIS_
   Date> SNAPSHOT_DT=<SNAPSHOT_Date>,DATAMOVEMENTCODE=ALL or <Data
   Movement Code of a Table>
   ```

Note: DATAMOVEMENTCODE of each table can be found in the DMCODE column of the FCC_DM_DEFINITION.

Creating and Loading Graph

To create and load graph, follow these steps:

1. Go to <STUDIO_INSTALLED_PATH>/datastudio/conf.
2. Modify the values of the below mentioned parameters in the OFSAAGLOBALGRAPH.json file:

   ```
   "jdbc_url" : <Provide JDBC URL of Studio schema>

   "username" : <Provide Studio Schema user name>

   "password" : <Provide Studio Schema user password>
   ```

3. Go to the $FIC_DB_HOME/bin.
4. Execute ./FCCM_Studio_GraphLoad.sh <Batch Name> <Batch ID> EXEC <FIC_MIS_Date> SNAPSHOT_DT=<SNAPSHOT_Date>.

Enabling VPD

To Enable VPD, enter the following in the table *FCC_GROUPFILTER*:

1. **GroupCode** must be the same group code as defined in *csms_group_master*.
2. **GroupFilter** must be a username and the user should be mapped to a specific jurisdiction.
3. **Jurisdiction** is a user defined value and must be set as required. For example, US or AMEA.

Configuring PGX

To configure PGX, follow below steps:

1. Navigate to the <Studio_Installed_Path>/pgx/pgx-2.6.0-server/pgx-2.6.0/conf/server.conf file.
2. Configure the following properties as per the requirement:

   In server.conf file:

   ```
   enable_tls=false

   enable_client_authentication=false
   ```

   In pgx.conf file:

   ```
   allow_local_filesystem": true
   ```

   Here, true is to enable, and false is to disable.

3. Copy the pgx-2.6.0-java-client directory from the <Studio_Installed_Path>/pgx path to any location inside the node servers.

   This is performed to copy the PGX Client to all the nodes in the cluster.

4. Set the values for the SPARK_CLASSPATH and JAVA_HOME parameters in the spark-env.sh file as follows:

```
export SPARK_CLASSPATH=<Studio_Installed_
Path>/pgx/pgx-2.6.0-java-client/pgx-2.6.0/lib/*:$HADOOP_CONF_DIR

export JAVA_HOME=<JAVA_INSTALLED_PATH>/jdk1.8.0_101
```

5. Place the `ojdbc7` jar file in the `<Cloudera_Installation_Path>/sqoop/jars` path.

Starting Studio Services

Start the Studio services in the order mentioned in Appendix C, "Starting/Stopping Infrastructure Services".

You can now view the Studio interface. You can access the Studio application from the URL as follows:

`http://<HOST>:7008`

A

Configuring Resource Reference in Web Application Servers

This section covers the following topics:

- Configuring Resource Reference in Tomcat Application Server

Configuring Resource Reference in Tomcat Application Server

To configure the resource reference in Web Application Servers, refer the following sections:

- Creating Data Source
- Configuring Class Loader for Apache Tomcat

Copy the Oracle JDBC driver file, "ojdbc<version>.jar" from `<Oracle Home>/jdbc/lib` and place it in `<Tomcat Home>/lib`.

> **Note:** Refer Appendix D, "JDBC Jar Files" for identifying the correct `ojdbc<version>.jar` version to be copied.

Creating Data Source

- Creating Data Source for Metaservice
- Creating Data Source for Batchservice

Creating Data Source for Metaservice

To create "data source" for metaservice of Studio application, follow these steps:

1. Navigate to `<Tomcat Home>/conf` and edit the `server.xml` file by replacing the actual values with the following block of text:

```
<Context path ="/<context name>" docBase="<Tomcat Installation
Directory>/webapps/<context name>" debug="0" reloadable="true"
crossContext="true">

<Resource auth="Container"

name="jdbc/FCCM_STUDIO_SCHEMA"

type="javax.sql.DataSource"

driverClassName="oracle.jdbc.driver.OracleDriver"
```

```
username="<user id for the studio schema>"
password="<password for the above user id>"
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100"
maxIdle="30"
maxWait="10000"/>
</Context>
```

Note:

- The <Resource> tag must be repeated for each Information Domain created.
- After the above configuration, the "WAR" file has to be created and deployed in Tomcat.

Creating Data Source for Batchservice

To create "data source" for batchservice of Studio application, follow these steps:

1. Navigate to `<Tomcat Home>/conf` and edit the `server.xml` file by replacing the actual values with the following block of text:

```
<Context path ="/<context name>" docBase="<Tomcat Installation
Directory>/webapps/<context name>" debug="0" reloadable="true"
crossContext="true"><Resource auth="Container"
name="jdbc/FCCM_BD_SCHEMA"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver"
username="<user id for the BD schema>"
password="<password for the above user id>"
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100"
maxIdle="30"
maxWait="10000"/>
<Resource auth="Container"
name="jdbc/FCCM_STUDIO_SCHEMA"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver"
username="<user id for the studio schema>"
password="<password for the above user id>"
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100"
maxIdle="30"
```

```
maxWait="10000"/>

</Context>
```

Note:

- The <Resource> tag must be repeated for each Information Domain created.
- After the above configuration, the "WAR" file has to be created and deployed in Tomcat.

Configuring Class Loader for Apache Tomcat

To configure Class Loader for Apache Tomcat, follow these steps:

1. Edit the `server.xml` available in `$TOMCAT_HOME/conf/` folder.
2. Add tag `<Loader delegate="true" />` within the `<Context> tag`, above the <Resource> tag.

   This is applicable only when the web application server is Apache Tomcat 8.

Note: This configuration is required if Apache Tomcat version is 8.

B

Deploying EAR/ WAR File

This section covers the following topics:

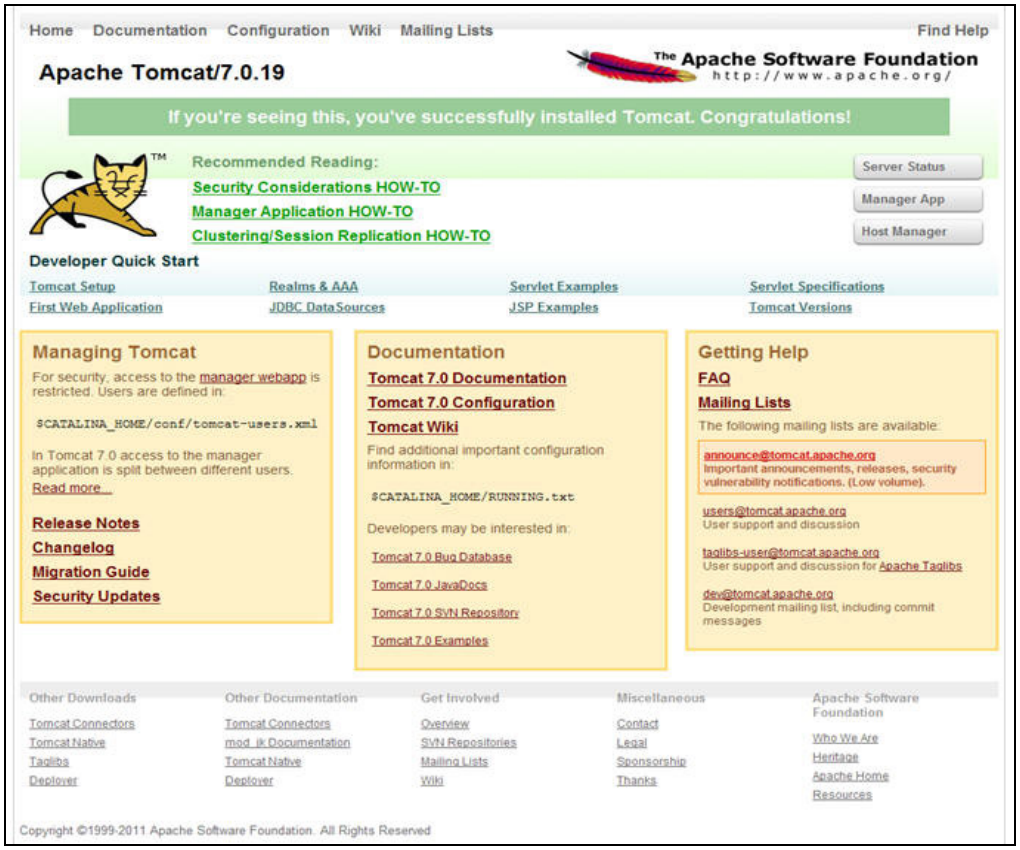
Deploying EAR/WAR Files on Tomcat

Before deploying the WAR files, ensure that the previously deployed application of Infrastructure are uninstalled.

On the machine that hosts Tomcat, follow these steps to deploy Infrastructure application:

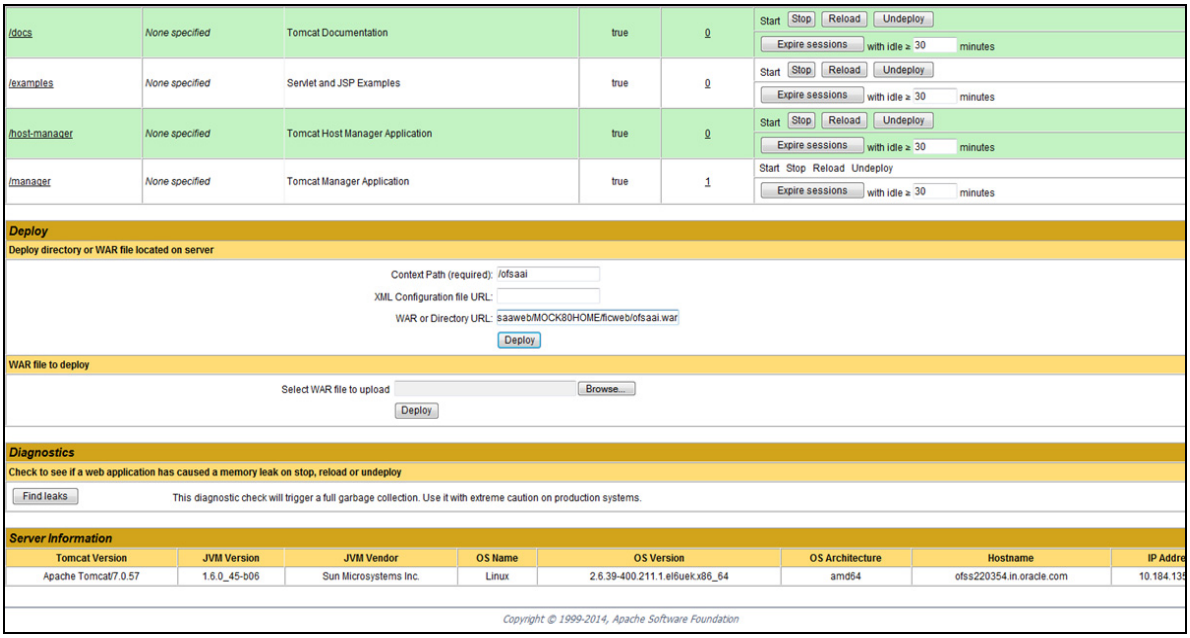
1. Copy the `<context-name>.war` from `<Studio_Installed_Path>/datastudio_metaservice/<metaservice.war>` to `<Tomcat Installation Directory>/webapps/` directory.

Figure B–1 Tomcat Home Page



2. Copy the <context-name>.war from <Studio_Installed_Path>/datastudio_batchservice/<batchservice.war> to <Tomcat Installation Directory>/webapps/ directory.
3. Click **Manager App**. The Connect to dialog box is displayed.
4. Enter the **User Id** and **Password** that has admin rights and click **OK**. The Tomcat Web Application Manager window is displayed with the list of all the applications deployed.

Figure B–2 Tomcat Web Application Manager



5. In the *Deploy* section, enter the **Context Path** provided during the installation as "/<context-name>".
6. Enter the path where the `<context-name>.war` file resides (by default `<Studio_Installed_Path>/datastudio_metaservice/<metaservice.war>`) in the **WAR or Directory URL** field and click **Deploy**.
7. On successful application deployment, a confirmation message is displayed.

   Start the Tomcat server.

C

Starting/Stopping Infrastructure Services

This section details about how to start and stop the infrastructure services needed for OFS Crime and Compliance Studio application.

This section covers the following topics:

- Starting/Stopping Livy Service
- Starting/Stopping PGX Service
- Starting/Stopping Data Studio Service
- Starting/Stopping MetaService Service

Starting/Stopping Livy Service

The Livy service is installed with Cloudera.

To start the Livy service, navigate to the path where Livy service is installed and run the following:

```
./livy-server start
```

To stop the Livy service, navigate to the path where Livy service is installed and run the following:

```
./livy-server stop
```

Starting/Stopping PGX Service

To start the PGX service, navigate to the path where PGX service is installed and run the following:

```
./start-server
```

The start service for PGX will be located in the path as follows:

```
##PGX_INSTALATION_PATH##/pgx/pgx-2.6.0-server/pgx-2.6.0/bin
```

To stop the PGX service, kill the process.

Starting/Stopping Data Studio Service

To start the Data Studio service, navigate to the path where Studio is installed and run the following:

```
./datastudio --external
```

The start service for Data Studio will be located in the path as follows:

```
##DATA_STUDIO_INSTALLATION_PATH##/datastudio/bin
```

To stop the service, kill the process.

Starting/Stopping MetaService Service

To start the Metaservice service, navigate to path where Metaservice service is installed and run the following:

```
./startup.sh
```

The start service for Metaservice service will be located in the path as follows:

```
<Metaservice Deployed Area>/bin
```

To stop the service, navigate to the path where Metaservice service is installed and run the following:

```
./shutdown.sh
```

Once all the Services are up and running, Studio Application can be accessed with the following URL:

```
http://<HOST>:<7008>
```

D

JDBC Jar Files

Overview

The `ojdbc<version>.jar` file should be copied based on the Oracle Database version and the supported Java (JDK/JRE) version. See the following table for details:

Table D–1 JDBC Jar files version details

Oracle Database Version	JDK/JRE Version Supported	JDBC Jar files specific to the release
12.1 or 12cR1	JDK 8 and JDK 7	ojdbc7.jar for JDK 7 and JDK 8

E

Clearing Application Cache

Overview

Clearing application cache is applicable to all Web Servers (WebLogic and Tomcat).

Prior to the deployment of Infrastructure or Application Service Packs/One-off patches, navigate to the following path depending on the WebServer configured and clear the cache:

- **WebLogic**: `<Weblogic installation location>/domains/<Domain name>/servers/<Server name>/tmp/_WL_user/<Application name>/qaelce/jsp_servlet`
- **Tomcat**: `<Tomcat installation folder>/work/Catalina/localhost/<Application name>/org/apache/jsp`

F

Configuring TDE and Data Redaction in OFSAA

Two features comprise Oracle Advanced Security: Transparent Data Encryption and Oracle Data Redaction

This section details about the configurations required in case you want to enable TDE or Data Redaction in OFSAA applications.

This section includes the following:

- Transparent Data Encryption (TDE)
- Data Redaction

Transparent Data Encryption (TDE)

Transparent Data Encryption (TDE) enables you to encrypt sensitive data, such as Personally Identifiable Information (PII), that you store in tables and tablespaces. After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data. To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a Keystore. For more details on TDE, see the Database Advanced Security Guide. TDE tablespace encryption enables you to encrypt all of the data stored in a tablespace. To control the encryption, you use a Keystore and TDE master encryption key. Oracle Database supports both software keystores and hardware, or HSM-based, keystores. A software keystore is a container for the TDE master encryption key, and it resides in the software file system.

Configuring TDE During Enterprise Case Management Installation Using Full Installer

This section provides information on how to enable TDE (Transparent Data Encryption) in the database. This section consists of the following sub sections:

- Configuring a Software Keystore and Encrypted Tablespace Creation
- Running the Schema Creator Utility With Encryption
- Testing the Encryption

Configuring a Software Keystore and Encrypted Tablespace Creation

A software keystore is a container for the TDE master encryption key, and it resides in the software file system. You must define a location for the key in the `sqlnet.ora` file so that the database locates the keystore (one per database) by checking the keystore

location in the sqlnet.ora file. After defining the location, create the keystore and open it. Set the TDE master key after opening it and then encrypt the data

To find whether a wallet is already existing, check the following entries:

1. The location specified by the ENCRYPTION_WALLET_LOCATION parameter in the sqlnet.ora file.
2. The location specified by the WALLET_LOCATION parameter in the sqlnet.ora file.

Encrypted tablespaces can share the default database wallet. However, Oracle recommends that you use a separate wallet for transparent data encryption functionality by specifying the ENCRYPTION_WALLET_LOCATION parameter in the sqlnet.ora file.

Note: NOTE: You should have proper privileges to perform the following actions.

For details to configure the software keystore, perform the following steps:

Step 1: Set the Software keystore location in the sqlnet.ora file

The first step is to designate a location for software keystore in the sqlnet.ora file. The Oracle Database will check the sqlnet.ora file for the directory location of the keystore to determine whether it is a software keystore or a hardware module security (HSM) keystore

Note: Ensure that the directory location which you want to set for software keystore exists beforehand. Preferably, this directory should be empty.

In a multitenant environment, the keystore location is set for the entire multitenant container database (CDB), not for individual pluggable databases (PDBs).

By default, the sqlnet.ora file is located in the ORACLE_HOME/network/admin directory or in the location set by the TNS_ADMIN environment variable. Ensure that you have properly set the TNS_ADMIN environment variable to point to the correct sqlnet.ora file.

To create a software keystore on a regular file system, use the following format when you edit the sqlnet.ora file:

```
ENCRYPTION_WALLET_LOCATION=
  (SOURCE=
    (METHOD=FILE)
    (METHOD_DATA=
    (DIRECTORY=<<path to keystore>>)))
```

Examples:

For regular file system in which the database name is orclb:

```
ENCRYPTION_WALLET_LOCATION=
```

```
  (SOURCE=
   (METHOD=FILE)
    (METHOD_DATA=
     (DIRECTORY=/etc/ORACLE/WALLETS/orcl)))
```

When multiple databases share the `sqlnet.ora` file:

```
ENCRYPTION_WALLET_LOCATION=
  (SOURCE=
   (METHOD=FILE)
    (METHOD_DATA=
     (DIRECTORY=/etc/ORACLE/WALLETS/orcl)))
```

When Oracle Automatic Storage Management (ASM) is configured:

```
ENCRYPTION_WALLET_LOCATION=
 (SOURCE=
  (METHOD=FILE)
   (METHOD_DATA=
    (DIRECTORY=+disk1/mydb/wallet)))
```

For ASM Diskgroup:

```
ENCRYPTION_WALLET_LOCATION=
 (SOURCE=
  (METHOD=FILE)
   (METHOD_DATA=
    (DIRECTORY=+ASM_file_path_of_the_diskgroup)))
```

Step 2: Create the Software Keystore

There are three different types of Software Keystores:

- Password-based Software Keystores
- Auto-login Software Keystores
- Local Auto-login Software Keystores

Perform the following steps to create a software keystore:

1. Login as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. Use the following command to create password-based software keystore:

   ```
   CONN sys/password@serviceid AS SYSDBA

   ADMINISTER KEY MANAGEMENT CREATE KEYSTORE 'keystore_location'
   IDENTIFIED BY software_keystore_password;
   ```

   - `keystore_location` is the path of the keystore directory you want to create
   - `software_keystore_password` is the password of the keystore that you want to create.

   For example, to create the keystore in the `/etc/ORACLE/WALLETS/orcl` directory:

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/etc/ORACLE/WALLETS/orcl'
IDENTIFIED BY password;
```

After you run this statement, the ewallet.p12 file, which is the keystore, appears in the keystore location.

Alternatively, you can create an Auto-Login or Local-Login Keystore to avoid opening the Keystore manually every time. Use the following command:

```
ADMINISTER KEY MANAGEMENT CREATE [LOCAL] AUTO_LOGIN KEYSTORE FROM
KEYSTORE 'keystore_location' IDENTIFIED BY keystore_password;
```

`LOCAL` enables you to create a local auto-login software keystore. Otherwise, omit this clause if you want the keystore to be accessible by other computers.

After you run this statement, the `cwallet.sso` file appears in the keystore location.

Note: It is important to remember the master key password (<keystore_password>) used during creation of the keystore. There are no ways to retrieve the password if forgotten.

Step 3: Open the Software Keystore

Depending on the type of keystore you create, you must manually open the keystore before you can use it.

You do not need to manually open auto-login or local auto-login software keystores. These keystore are automatically opened when it is required, that is, when an encryption operation must access the key. If necessary, you can explicitly close any of these types of keystores. You can check the status of whether a keystore is open, closed, open but with no master key, or open but with an unknown master key by querying the STATUS column of the V$ENCRYPTION_WALLET view.

Note: After you open a keystore, it remains open until you manually close it. Each time you restart a database instance, you must manually open the password keystore to re-enable encryption and decryption operations.

Perform the following steps to open the software wallet:

1. Login as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. Use the following command to open password-based software keystore:

   ```
   CONN sys/password@serviceid AS SYSDBA
   ```

   ```
   ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY software_
   keystore_password [CONTAINER = ALL | CURRENT];
   ```

   - `software_keystore_password` is the same password that you used to create the keystore in "Step 2: Create the Software Keystore".
   - `CONTAINER` is for use in a multitenant environment. Enter ALL to set the keystore in all of the PDBs in this CDB, or CURRENT for the current PDB.

Note: In a CDB, open the Keystore in the ROOT (CDB$ROOT) container and in all the associated PDBs, where TDE is enabled.

You do not need to manually open auto-login or local auto-login software Keystores.

Step 4: Set the Software TDE Master Encryption Key

Once the keystore is open, you can set a TDE master encryption key for it. The TDE master encryption key is stored in the keystore. This key protects the TDE table keys and tablespace encryption keys. By default, the TDE master encryption key is a key that Transparent Data Encryption (TDE) generates.

In a multitenant environment, you can create and manage the TDE master encryption key from either the root or the PDB.

Ensure that the database OPEN_MODE is set as READ WRITE. To find the status for a non-multitenant environment, query the OPEN_MODE column of the V$DATABASE dynamic view. If you are using a multitenant environment, then query the V$PDBS view. (If you cannot access these views, then connect as SYSDBA and try the query again. In order to connect as SYSKM for this type of query, you must create a password file for it. See Oracle Database Administrator's Guide for more information.)

Perform the following steps to set the encryption key:

1. Login as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege
2. Use the following command to set the encryption key:

```
CONN sys/password@serviceid AS SYSDBA
```

```
ADMINISTER KEY MANAGEMENT SET KEY [USING TAG 'tag'] IDENTIFIED BY
password [WITH BACKUP [USING 'backup_identifier']] [CONTAINER = ALL |
CURRENT];
```

   - `tag` is the associated attributes and information that you define. Enclose this setting in single quotation marks (' ').
   - `password` is the mandatory keystore password that you created when you created the keystore in "Step 2: Create the Software Keystore".
   - `WITH BACKUP` creates a backup of the keystore. You must use this option for password-based keystores. Optionally, you can use the USING clause to add a brief description of the backup. Enclose this description in single quotation marks (' '). This identifier is appended to the named keystore file (for example, ewallet_time_stamp_emp_key_backup.p12, with emp_key_backup being the backup identifier). Follow the file naming conventions that your operating system uses.
   - `CONTAINER` is for use in a multitenant environment. Enter ALL to set the key in all of the PDBs in this CDB, or CURRENT for the current PDB.

   For example,

```
ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY password WITH BACKUP
USING 'emp_key_backup';
```

Step 5: Encrypting your Data

After completing the keystore configuration, encrypt the data. You can encrypt individual columns in a table or entire tablespaces. OFSAA recommends encrypting entire tablespaces and the description in this section covers encrypting entire tablespaces.

Note the following restrictions on using Transparent Data Encryption when you encrypt a tablespace:

- Transparent Data Encryption (TDE) tablespace encryption encrypts or decrypts data during read and write operations, as compared to TDE column encryption, which encrypts and decrypts data at the SQL layer. This means that most restrictions that apply to TDE column encryption, such as data type restrictions and index type restrictions, do not apply to TDE tablespace encryption.
- To perform import and export operations, use Oracle Data Pump.

Encrypting data involves the following steps:

1. Setting the COMPATIBLE initialization parameter for tablespace encryption
2. Setting the tablespace TDE master encryption key
3. Creating the Encrypted Tablespace

Step 1: Setting the COMPATIBLE initialization parameter for tablespace encryption

Prerequisite- You must set the COMPATIBLE initialization parameter for the database to 11.2.0.0 or later. Once you set this parameter to 11.2.0.0, the change is irreversible.

Perform the following steps to set the `COMPATIBLE` initialization parameter:

1. Log into the database instance. In a multitenant environment, log into the PDB.
2. Check the current setting of the `COMPATIBLE` parameter.

   For example:

Table F–1 SHOW PARAMETER COMPATIBLE

Name	Type	Value
Compatible	String	12.0.0.0
noncdbcompatible	Boolean	False

3. If you want to change the `COMPATIBLE` parameter, perform the following steps:
   1. Locate the initialization parameter file for the database instance.

      UNIX systems: This file is in the `ORACLE_HOME/dbs` directory and is named `initORACLE_SID.ora` (for example, initmydb.ora).
   2. In SQL*Plus, connect as a user who has the SYSDBA administrative privilege, and then shut down the database.

      ```
      For example:

      CONNECT /AS SYSDBA

      SHUTDOWN
      ```
   3. Edit the initialization parameter file to use the correct `COMPATIBLE` setting.

      For example:

      ```
      COMPATIBLE = 12.2.0.0
      ```

4. In SQL*Plus, ensure that you are connected as a user who has the SYSDBA administrative privilege, and then start the database.

   For example:

   ```
   CONNECT /AS SYSDBA

   STARTUP
   ```

5. If tablespace encryption is in use, then open the keystore at the database mount. The keystore must be open before you can access data in an encrypted tablespace.

   ```
   STARTUP MOUNT;

   ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY password;

   ALTER DATABASE OPEN;
   ```

Step 2: Setting the tablespace TDE master encryption key

Make sure that you have configured the TDE master encryption key as shown in Step 4: Setting the software TDE master encryption key.

Step 3: Creating the Encrypted Tablespace

After you have set the `COMPATIBLE` initialization parameter, you are ready to create the encrypted tablespace.

Follow the instruction given in Running the Schema Creator Utility with Encryption section for configuring the schema creator file to create tablespaces.

If you are enabling TDE in case of upgrade or you did not enable it during installation and want to enable at a later point of time, see the following reference link for details on manually creating encrypted tablespaces:

https://docs.oracle.com/cloud/latest/db121/ASOAG/asotrans_config.htm#ASOAG9555

Running the Schema Creator Utility With Encryption

This section is applicable only if you want to enable TDE during installation.

Run the schema creator utility by including the **encrypt=on** option in the Tablespace tag in the `<<APP PACK>>_SCHEMA_IN.xml` file. You have to perform this procedure manually as it is not a part of the `<<APP PACK>>_SCHEMA_IN.xml.TEMPLATE` originally.

Following is an example for `OFS _AAAI_PACK_ SCHEMA_IN.xml`

```
<APPPACKSCHEMA>

<APP_PACK_ID>OFS_AAAI_PACK</APP_PACK_ID>

<JDBC_URL>jdbc:oracle:thin:@<DB_Server_IP>:1521:<DB_NAME></JDBC_URL>

<JDBC_DRIVER>oracle.jdbc.driver.OracleDriver</JDBC_DRIVER>

<HOST><OFSAA_Server_IP/HOST Name></HOST>

<SETUPINFO NAME="<PREFIX_NAME>" PREFIX_SCHEMA_NAME="Y"/>

<PASSWORD APPLYSAMEFORALL="Y" DEFAULT="<PASSWORD>"/>

<TABLESPACES>

<TABLESPACE NAME="OFS_AAI_TBSP" VALUE="TS_USERS1" DATAFILE="<ABSOLUTE PATH
to TABLESPACE>/<TABLESPACE_DATA_FILE_NAME>.dbf" SIZE="500M"
AUTOEXTEND="OFF" ENCRYPT="ON" />

</TABLESPACES>
```

```
<SCHEMAS>

<SCHEMA TYPE="CONFIG" NAME="ofsaaconf" PASSWORD="" APP_ID="OFS_AAI"
DEFAULTTABLESPACE="##OFS_AAI_TBSP##" TEMPTABLESPACE="TEMP"
QUOTA="unlimited"/>

<SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_AAAI"
DEFAULTTABLESPACE="##OFS_AAI_TBSP##" TEMPTABLESPACE="TEMP"
QUOTA="unlimited" INFODOM="OFSAAAIINFO"/>

<SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_IPE"
DEFAULTTABLESPACE="##OFS_AAI_TBSP##" TEMPTABLESPACE="TEMP"
QUOTA="unlimited" INFODOM="OFSAAAIINFO"/>

</SCHEMAS>

</APPPACKSCHEMA>
```

Testing the Encryption

Test the encryption by checking if a tablespace is encrypted or not. Execute the following query to check:

```
SELECT tablespace_name, encrypted FROM dba_tablespaces;
```

The following result is displayed, where ENCRYPTED column indicates whether the TABLESPACE is encrypted or not.

Table F–2 TABLESPACE Encryption

TABLESPACE_NAME	ENCRYPTED
SYSTEM	No
SYSAUX	No
UNDOTBS1	No
TEMP	No
USERS	No
ENCRYPTED_TS	Yes
6 rows selected.	

The above example indicates TABLESPACE `ENCRYPTED_TS` is created with Encryption ON.

Configuring TDE in Case of Upgrade

This section details about the configurations required in case you want to enable TDE in OFSAA applications after upgrade to OFSAA 8.0.6.0.0 version from a previous version. Additionally, these configurations are required in case you did not enable TDE during 8.0.6.0.0 installation and want to enable at a later point of time.

1. Create a new PDB (12c)/ instance (11g) on same or different Database Server for TDE. For more information, see Configuring Software Keystore and Encrypted Tablespace Creation.
2. Shutdown the OFSAAI Services.
3. Export all Configuration, Atomic and Sandbox Schemas as per the applications installed in your OFSAA instance.

   For example:

```
expdp SYSTEM/oracle@OFSA12C2DB  DIRECTORY=data_pump_dir
DUMPFILE=ofsaaconf_ofsaaatm_%U.dmp filesize=2G
SCHEMAS=ofsaaconf,ofsaaatm LOGFILE=ofsaaconf_ofsaaatm_exp.log
```

Note: The above command will create data dumps as files of 2GB size each (multiples). Any other commands/ tools as appropriate may be used to archive the schemas.

4. Import all schemas that are exported using the above command, into the new DB instance.

   For example:

   ```
   impdp SYSTEM/oracle@OFSA12nDB  DIRECTORY=data_pump_dir
   DUMPFILE=ofsaaconf_ofsaaatm_%U.dmp  SCHEMAS=ofsaaconf,ofsaaatm
   LOGFILE=ofsaaconf_ofsaaatm_imp.log
   ```

   Note:
   - Restoring the exported dumps creates Configuration and Atomic Schema(s) with the same user credentials as that of the source, along with the existing grants.
   - If schemas are restored using a tool/ mechanism other than as mentioned in the Step 1 and 2, retain the user credentials of Configuration and Atomic Schemas same as in the Source environment, along with the Schema grants.

5. Provide select grants on `sys.V_$parameter` to view Configuration and Atomic Schemas of Target Environment database

   For example:

   Login as sys user:

   ```
   SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaaconf;

   Grant succeeded

   SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaaatm;

   Grant succeeded
   ```

6. Update `.profile` for `ORACLE_SID` environment variable with new ORACLE_SID.
7. Update JDBC URL by executing Port Changer utility. For details on how to execute Port Changer utility, see Changing IP/ Hostname, Ports, Deployed paths, Protocol of the OFSAA Instance section.
8. Navigate to the `$FIC_WEB_HOME` directory and execute the following command to trigger the creation of EAR/WAR file:

   ```
   ./ant.sh
   ```

9. The EAR/WAR file - <contextname>.ear/.war - is created in `$FIC_WEB_HOME` directory.
10. On completion of EAR/WAR file creation, the message "BUILD SUCCESSFUL" will be displayed.
11. Edit the existing Connection Pool settings to point to new JDBC URL and verify connections.

12. Clear the webserver cache and redeploy the application onto your configured web application server.
13. Restart the OFSAA Services. For more information, refer to the Start/Stop Infrastructure Services section in the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide 8.0.2.0.0.

Data Redaction

OFSAA is enhanced to enable masking of sensitive data and Personal Identification Information (PII) to adhere to Regulations and Privacy Policies. Oracle Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed to a pattern that does not contain any identifiable information.

Enabling Data Redaction in case of Upgrade

This section details about the configurations required in case you want to enable Data Redaction in OFSAA applications after upgrade to OFSAA 8.0.6.0.0 version from a previous version. Additionally, these configurations are required in case you did not enable TDE during ECM Application Pack 8.0.6.0.0 installation and want to enable at a later point of time.

Perform the following steps:

1. Login as SYSDBA into the database.
2. Execute the file `$FIC_HOME/utility/data_security/scripts/create_data_sec_roles.sql` only once per database (PDB in case of 12c).
3. Execute the following sql statement to find out the list of atomic users from the table:

   ```
   select v_schema_name from aai_db_detail where V_DB_NAME <> 'CONFIG' AND V_DB_TYPE = 'ORACLE'
   ```

4. Execute the `file $FIC_HOME/utility/data_security/scripts/grant_data_sec_roles.sql` for all atomic users found in the previous step.
5. From the *Configuration* window in the *System Configuration* module, select the **Allow Data Redaction** checkbox.
6. Run the Data Redaction utility. For more details on how to run the utility, see *Data Redaction* section under *Data Security and Data Privacy* chapter in OFS Analytical Applications Infrastructure Administration Guide.