Oracle Financial Services Advanced Analytical Applications Infrastructure Pack

Installation and Configuration Guide

Version 8.0.6.0.0

ORACLE
FINANCIAL SERVICES

DOCUMENT CONTROL

Version Number	Revision Date	Changes Done
1.0	Created: May 2018	Added 8.0.6.0.0 Minor Release installation procedure and configuration details.
2.0	Modified: June 2018	Added info about mandatory one-off patch 28079607.
3.0	Modified: July 2018	Updated the document for mandatory compatibility patch 28033582 and mandatory installer patch 28398331.
4.0	Modified: Sep 2018	Added a post install step to install 8.0.6.1.0 ML instead of applying the mandatory patches like **28079607**, **27938294** and **28033582**.
4.1	Modified: July 2020	Added information to download, install, and apply patch 31606017 (Doc 31647393).
4.2	December 2021	Updated the How to Apply This Release? Section for 33663417 Mandatory Patch instructions (Doc 33668822).

Executive Summary

This document includes the necessary instructions to apply 8.0.6.0.0 Minor Release for OFS Advanced Analytical Applications Infrastructure Application Pack and perform the required post install configurations. You can find the latest copy of this document in the OHC Documentation Library.

ORACLE®

TABLE OF CONTENTS

ORACLE

Preface

This document provides step-by-step instructions to install the Oracle Financial Services Advanced Analytical Applications Infrastructure (OFS AAAI) Application Pack 8.0.6.0.0 Minor Release.

This chapter discusses the following topics:

- Audience
- How this Guide is Organized
- Related Documents
- Conventions Used

Audience

The OFS AAAI Application Pack Installation and Configuration Guide is intended for administrators and implementation consultants who are responsible for installing and maintaining the application pack components.

Prerequisites for the Audience

It is assumed that you have experience in installing Enterprise components and basic knowledge about the following is recommended:

- Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack components
- Oracle Financial Services Analytical Applications (OFSAA) Architecture
- UNIX Commands
- Database Concepts
- Web Server/Web Application Server

How this Guide is Organized

The OFS AAAI Application Pack Installation and Configuration Guide includes the following topics:

- OFS AAAI Application Pack Minor Release 8.0.6.0.0
- Appendix A – Frequently Asked Questions (FAQ)

ORACLE®

Conventions and Acronyms

Conventions	Description
Actions are indicated in **Bold.** Command or query is indicated in `Courier New font.`	
AIX	Advanced Interactive eXecutive
MFA	Multi-Factor Authentication
OFSAA	Oracle Financial Services Analytical Applications
OFSAAI	Oracle Financial Services Analytical Applications Infrastructure
OFS AAAI	Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack
OHC	Oracle Help Center
RHEL	Red Hat Enterprise Linux
R	Third-party open source software. Open source R is governed by GNU General Public License (GPL).
Oracle R Distribution	Oracle R Distribution is Oracle's free distribution of open source R.
Oracle R Enterprise (ORE)	Oracle R Enterprise integrates R, the open source scripting language and environment, with Oracle Database.
Atomic Schema	Database schema where the application data model is uploaded.
Config Schema	Database schema which contains setup related configurations and metadata.
Infodom	Information Domain
TDE	Transparent Data Encryption

ORACLE®

1 OFS AAAI Application Pack Minor Release 8.0.6.0.0

This release of OFS AAAI Application Pack is cumulative and includes all enhancements and bug fixes done since the OFS AAAI Application Pack v8.0.0.0.0 release.

1.1 Pre Installation Requirements

1. OFS AAAI Application Pack version 8.0.2.0.0 or higher must be installed.

2. Refer to the Technology Matrix for Hardware and Software Requirements for this release.

3. To install this release on Oracle Solaris OS, refer to the following list for version specific information:

   ▪ **Solaris 11** – Upgrade to Oracle Solaris 11.3 with SRU09 or higher. See https://docs.oracle.com/cd/E60778_01/html/E60743/gouaw.html#scrolltoc to upgrade to SRU09 if you have a lower SRU version. Additionally, install the required runtime libraries. For more information, see Installing Only the Runtime Libraries on Oracle Solaris 11.

   ▪ **Solaris 10** – Install the required OS patches. For more information, see Installing the Required Oracle Solaris 10 Patches. Additionally, install the required runtime libraries. For more information, see Installing Only the Runtime Libraries on Oracle Solaris 10.

   NOTE: In an OFSAA instance where multiple OFSAA application packs have been installed/ deployed, it is mandatory to upgrade all OFSAA application packs to 8.0.4.0.0 or higher version.

4. If you want to enable TDE or Data Redaction, ensure the required Oracle Database Server versions are installed and mandatory patches are applied as listed out in *Prerequisites* section mentioned in Enabling Transparent Data Encryption (TDE) and Data Redaction section.

5. Following step is applicable *only* if existing OFSAAI setup version is 8.0.5.x.x and Configuration and Atomic Schema(s) were restored from exported dumps of other environment:

   Login to Configuration Schema and execute the following SQL statements:

   ```
   alter table AAI_AOM_APP_COMP_ATTR_MAPPING drop constraint
   AOM_APP_COMP_ATTR_PK drop index
   /
   ```

ORACLE

```
alter table AAI_AOM_APP_COMP_ATTR_MAPPING add constraint
AOM_APP_COMP_ATTR_PK primary key (APP_COMP_ATTR_MAP_ID)
/
```

6. Download the mandatory OFSAAI Maintenance Level release version 8.0.6.1.0 (28033370) from My Oracle Support.

> **NOTE:** OFSAAI 8.0.6.1.0 ML is regularized with all the mandatory patches released on top of 8.0.6.0.0 release. This ML has the compatibility patch as well, which enables you to upgrade selected packs in your OFSAA instance to 8.0.6.x.x and makes the existing packs from earlier versions compatible with 8.0.6.x.x.

> **NOTE:** Execute the DMT Migration Utility to manually migrate the DMT metadata of the Applications which are not upgraded to 8.0.6.0.0.

7. *Bug 23251358-Object Registration is failing with duplicate Constraint Names* is regularized in this OFS AAAI application pack 8.0.6.0.0. This is bundled as a utility - **Update Constraints Utility**, and is executed as part of the 8.0.6.0.0 patch installation.

> **NOTE:** Skip the following steps if the existing platform version is 8.0.3.x.x.

Perform the following steps and apply the change before you proceed further with the patch upgrade.

   a. Backup the Atomic Schema for each Information Domain in the OFSAA instance before applying the patch.
   b. Execution of the utility is a memory intense process as the entire steps involved for performing a full model upload is carried out as part of the utility for each of the Infodom. The OFSAA installation server needs to have twice the allocated memory, which is assigned using parameter `X_ARGS_APPS`.
   c. Utility creates three temporary tables- `REV_TAB_CONSTRAINTS_U`, `REV_TAB_REF_CONSTRAINTS_U`, and `REV_TAB_CONSTRAINT_COLUMNS_U`. If the Atomic Schema has any of these tables already created for a different purpose, take a backup and drop/rename.
   d. For the applications that follow logical model upload like OFS_AML in BD pack, the utility does not play any role, since persistence of the model is outside the purview of the utility.
   e. For more information about the utility execution and log files information, see Update Constraints Utility section.

8. Connect to the database as user with DBA privileges. Execute the following grant statement:

```
GRANT CREATE TYPE TO [<ATOMIC SCHEMA>];
```

> **NOTE:** This grant should be executed for all existing Atomic Schemas.

9. As part of the OFSAAI upgrade installer, DMT migration utility gets invoked to migrate existing Data Sources data from XML to database. Hence, if your OFSAA environment contains Data Source definitions of source type File and Table based on HDFS, copy the `log4j-1.2.17.jar` file from the Apache installation directory into `$FIC_HOME/ext/lib` directory.

1.2 How to Apply This Release?

1.2.1 Installing OFS AAAI Application Pack

See the following instructions to download, extract, install, and configure this release.

1. Log in to https://support.oracle.com/ and search for **23036940** under the *Patches & Updates* tab.

2. Download the OFS AAAI Application Pack v8.0.6.0.0 archive file and copy it to your OFSAA server in **Binary** mode.

> **NOTE:** The archive files are different for every operating system like AIX, Solaris, and RHEL/Oracle Linux.

3. Search and download the mandatory installer patch **28398331** from https://support.oracle.com/.

4. Search and download the mandatory patch **31606017** from https://support.oracle.com/.

5. Log in to My Oracle Support, search for the **33663417** Mandatory Patch in the **Patches & Updates** Tab and download it.

> **ATTENTION** On the 10th of December 2021, Oracle released Security Alert CVE-2021-44228 in response to the disclosure of a new vulnerability affecting Apache Log4J before version 2.15. The application of the **33663417** Mandatory Patch fixes the issue.
>
> For details, see the My Oracle Support Doc ID 2827801.1.
>
> Ensure that you reapply the **33663417** Mandatory Patch whenever you install or upgrade the application, or apply an incremental patch.

6. Log in to the OFSAA Server.

7. Shut down all the OFSAAI Services. For more information, refer to the *Start/Stop Infrastructure Services* section in the OFS Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide.

ORACLE®

8. Execute the following command:

   ```
   chmod -R 750 $FIC_HOME
   ```

9. If you have Unzip utility, skip to the next step. Download the Unzip utility (OS specific) and copy it in **Binary** mode to the directory that is included in your PATH variable, typically **$HOME** path or directory in which you have copied the 8.0.6.0.0 installer.

   a. Uncompress the unzip installer file using the command:

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

NOTE:	In case you notice an error message "**uncompress: not found [No such file or directory]**" when the package is not installed, contact your UNIX administrator.

   b. Give EXECUTE permission to the file using the command:

      ```
      chmod 751 OFS_AAAI_80600_<OperatingSystem>.zip.
      ```

10. Extract the contents of the 8.0.6.0.0 archive file using the command:

    ```
    unzip_<os> -a <name of the file to be unzipped>
    ```

NOTE:	The above "**-**a" option is mandatory to unzip the archive file. For example: `unzip_aix -a OFS_AAAI_80600_<OperatingSystem>.zip`

11. Apply the patch **28398331**. Refer to the *Readme.txt* file packaged with the patch for details on how to apply the patch.

12. Navigate to the path where the directory *OFS_AAAI_PACK* exists and execute the command:

    ```
    chmod -R 755 OFS_AAAI_PACK
    ```

13. Execute **OFSAAIUpdate.sh** file using the following command.

    ```
    ./OFSAAIUpdate.sh
    ```

    Verify if the release is applied successfully by checking the log file generated in the installation directory in the path `<PATCH_EXTRACTED DIRECTORY>/OFS_AAAI_PACK/logs/OFSAAIUpdate.log`. You can ignore ORA-00001, ORA-00955, ORA-02260, ORA-01430, and ORA-01031 errors in the log file. In case of any other errors, contact Oracle Support.

14. Install the mandatory OFSAAI Maintenance Level release version 8.0.6.1.0 (28033370). For instructions on how to install it, see OFS Analytical Applications Infrastructure Maintenance Level Release 8.0.6.1.0.

15. DMT migration utility is available as part of the OFSAAI 8.0.6.0.0 upgrade to migrate the DMT metadata (PLC/Data Source/Data Mapping/Data File Mapping) to be persisted

ORACLE®

in tables instead of XML. To identify when to migrate, what/how to migrate, and how to handle migration issues, see OFSAA DMT Metadata Migration Guide.

NOTE:	Execute the DMT Migration Utility to manually migrate the DMT metadata of the Applications which are not upgraded to 8.0.6.0.0.

16. Verify the `Update.log` file located at `$FIC_HOME/utility/UpdateConstraints/logs` directory which is created by Update Constraint utility.

    Execution status information of the utility is available against each Information domain. For success, "*Update successful*" message is displayed. If it is successful, verify the following references for new constraint names:

    - `ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml`

    - Constraint scripts under `ftpshare/<INFODOM>/erwin/scripts/table`

    - Constraint scripts under `ftpshare/<INFODOM>/scripts`

    - Object registration tables for constraints, REV_TAB_CONSTRAINTS, REV_TAB_REF_CONSTRAINTS, REV_TAB_CONSTRAINT_COLUMNS.

    - Oracle Data Dictionary in the respective Atomic Schemas for each Infodom.

    If you encounter errors in the `Update.log` file, identify and troubleshoot the failed Infodoms. Once you have completed the troubleshooting, execute the standalone utility for the failed Infodoms. For more information on executing the update constraints utility, see the section Update Constraints Utility.

NOTE:	If you are upgrading from 8.0.3.0.0, 8.0.4.0.0 or 8.0.5.0.0 version to 8.0.6.0.0 version, you may find the following error in the `Update.log` file and `upgrade.log` file:
	`Unable to fetch execution status of utility on this`
	`infodom.`
	`java.lang.Exception: Unable to get the records in`
	`aai_mu_util_update_cons Table for infodom.`
	You can ignore this error and proceed.

17. Verify `MF_xml_migration.log` file available in the `$FIC_HOME/utility/modelutil/log folder`. If any errors are there in the log file, you should re-run the utility. For more information on how to run the utility, see *Model Venue Migration Utility* section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

18. Secure your OFSAA Infrastructure. For more information, refer to the Security Guide in the OHC Documentation Library.

ORACLE

19. After successful installation, follow these steps:

- Clear the application cache. Navigate to the following path depending on the configured web application server and delete the files.

  - **Tomcat**:
    ```
    <Tomcat installation
    directory>/work/Catalina/localhost/<Application
    name>/org/apache/jsp
    ```

  - **WebLogic**:
    ```
    <WebLogic installation location>/domains/<Domain
    name>/servers/<Server name>/tmp/_WL_user/<Application
    name>/<auto generated directory>/jsp_servlet
    ```

    In case of WebLogic version 12.2.x.x, delete the folder named ".WL_internal" present in the path `<WebLogic installation location>/user_projects/domains/<Domain name >/applications/<context_name>.ear/META-INF/`, if it exists.

  - **WebSphere**:
    ```
    <WebSphere installation
    directory>/AppServer/profiles/<Profile name>/temp/<Node
    name>/server1/<Application name>/<.war file name>
    ```

20. Add umask 0027 in the `.profile` of the UNIX account which manages the WEB server to ensure restricted access permissions.

21. Perform the necessary additional configurations as mentioned in the following sections:

- Additional Configurations for Web Servers

- Configurations for Enterprise Modeling

- Configurations for Inline Processing Engine (IPE)

- Configurations for Process Modeling Framework

- Configurations for Forms Manager

22. Generate the application EAR/WAR file and redeploy the application onto your configured web application server. For more information on generating and deploying EAR/WAR file, refer to the *Post Installation Configuration* section in the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide.

23. Apply the mandatory patch **31606017**. See the Readme available with the patch for further instructions on how to install and apply the patch.

24. Apply the **33663417** Mandatory Patch.

ORACLE®

See the Readme that is packaged with the patch for further instructions on how to install and apply it.

25. After the successful installation of the release, restart all the OFSAAI 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.

26. For enabling Oracle Advanced Security features in OFSAA, see Enabling Transparent Data Encryption (TDE) and Data Redaction section.

27. Perform the necessary additional configuration as mentioned in Configurations for Enterprise Modeling section.

ORACLE

1.3 Additional Configurations for Application Packs

This section provides information for additional configurations required for the OFSAA application packs.

1.3.1 Configurations for Enterprise Modeling

This section is applicable only if OFS Enterprise Modeling is licensed and enabled in your OFSAA instance. See the OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0 for information on additional configurations.

Perform the following configurations before you start using Enterprise Modeling framework on 8.0.6.0.0:

1. Install OFS AAAI Runner package in the database server to execute ORE models. This is a mandatory step and you can find the Runner package in the `$FIC_HOME/ficdb/lib` directory. For more information, refer to the section *Installing OFS AAAI Runner Package* in the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide v8.0.2.0.0.

2. Configure ORE 1.5 to load the Cairo library in Oracle Linux/RHEL 7 by creating a symbolic link from `libtiff.so.3` to `libtiff.so.5` for the ORE executions to succeed. Follow the steps given below to create a symbolic link:

   a. Log in as root and change directory to `/usr/lib64`.
   b. Execute the following command:
      ```
      ln -s libtiff.so.5 libtiff.so.3
      ```

NOTE: Contact Oracle Support Services if you require further assistance on ORE 1.5.

---

3. The following steps are not required if you have configured this as part of 8.0.3.0.0 version.

   a. Sandbox Resave Utility is included in the 8.0.6.0.0 upgrade patch. If the log file in the path `$FIC_HOME/utility/sandboxutil/logs` has any error messages, execute the Sandbox Resave utility. For details, see How to Run the Utility section.
   b. Resave all ORE-based models, if you are upgrading to OFS AAI 8.0.6.0.0 from an older version. For more information on running the model resave utility, see Model Resave Utility section.

4. Execute Variable Migration Utility to migrate the variables defined in previous versions to 8.0.6.0.0 version. For more details, see Variable Migration utility section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

1.3.2 Configurations for Inline Processing Engine (IPE)

See the OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0 for information on configuration for IPE.

1.3.3 Configurations for Process Modeling Framework

You can see the OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0 for information on configuration for Process Modeling Framework.

1.3.4 Configurations for Forms Manager

You can see the OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0 for information on configuration for Forms Manager.

1.4 Additional Configurations for Web Servers

This section provides information for additional configuration required for the web servers on OFS AAAI.

1.4.1 Configuration for Tomcat

For successful execution of Data Mapping in Tomcat, perform the configurations mentioned in *Configuration for Tomcat* section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

For additional configurations, see the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide v8.0.2.0.0.

1.4.2 Configuration for WebLogic

To configure WebLogic, see the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide v8.0.2.0.0. Additionally, configure for REST services. For details, see *Configuring WebLogic for REST Services Authorization* section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

Additionally, you need to configure Work Manager in WebLogic. For details, see *Work Manager Configurations* section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

1.4.3 Configuration for WebSphere

To configure WebSphere, see the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide v8.0.2.0.0. Additionally, configure for REST services. For details, see *Configuring WebSphere for REST Services Authorization* section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

ORACLE

Additionally, you need to configure Work Manager in WebSphere and map it to OFSAA instance. For details, see *Work Manager Configurations* section in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

1.4.3.1   Configuring Application Security in WebSphere

This is a mandatory security procedure for WebSphere to restrict the unauthorized access of configuration files in directories. For detailed information, see the Oracle Financial Services Analytical Applications Infrastructure Security Guide.

1.4.3.2   Configuring WebSphere Shared Library to Support Jersey 2x and Jackson 2.9x Libraries

Perform the following configuration to set WebSphere shared library to support jersey 2x and Jackson 2.9x libraries.

1. Click **Environment** from the menu on the left to expand and view the list. Click **Shared Libraries** to open the *Shared Libraries* window.
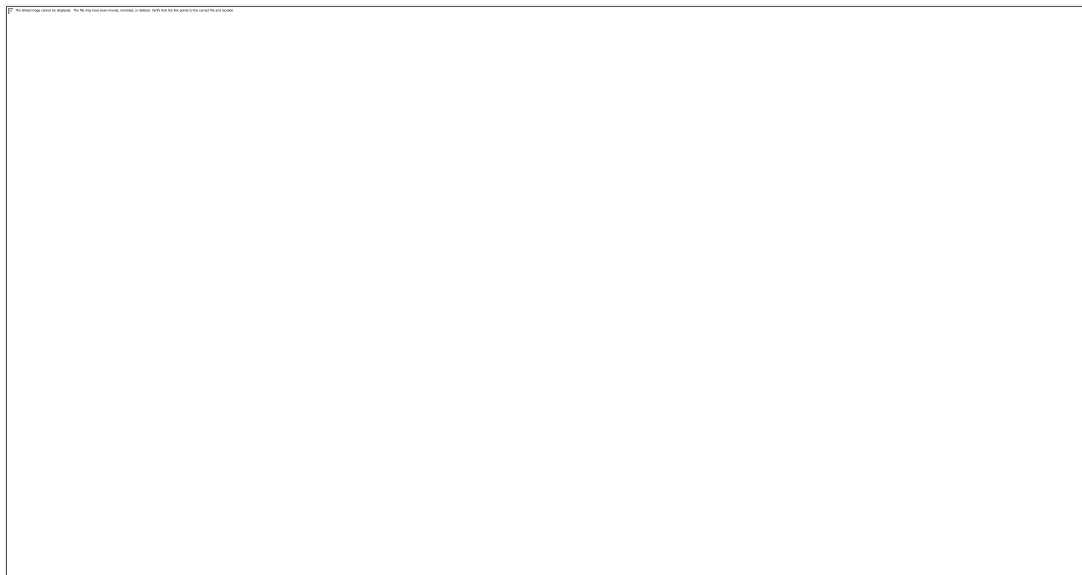
2. Enter details as shown in the following:

   - **Name**: Enter a unique identifiable name.

   - **Description**: Enter a valid description.

   - **Classpath**: Enter the absolute path where the JARs related to Jersey 2.x and Jackson 2.9x are copied. These jars are available in the *<OFSAA_HOME>/utility/externallib/WEB-INF/lib* directory after creation of the EAR file.

3. Select **Use an isolated class loader for this library**.

4. Click **OK** to save to master configuration.

ORACLE

5. Select the application or module and map the shared libraries. Click **OK**. In the following illustration, **ofsa** is selected.
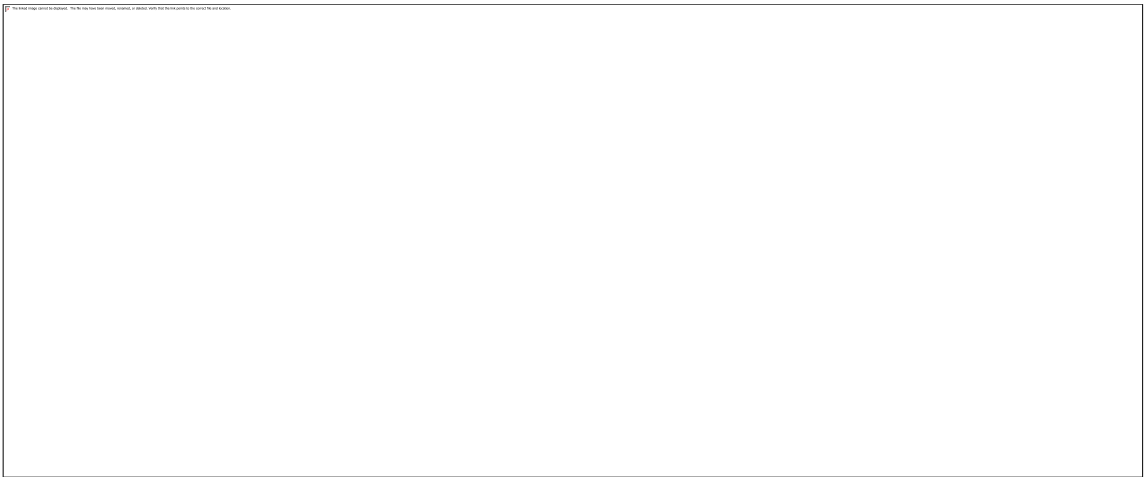
6. From the *Shared Library Mapping* window, move the required shared libraries from **Available** to **Selected**. In the following illustration, JERSEY2x is selected.
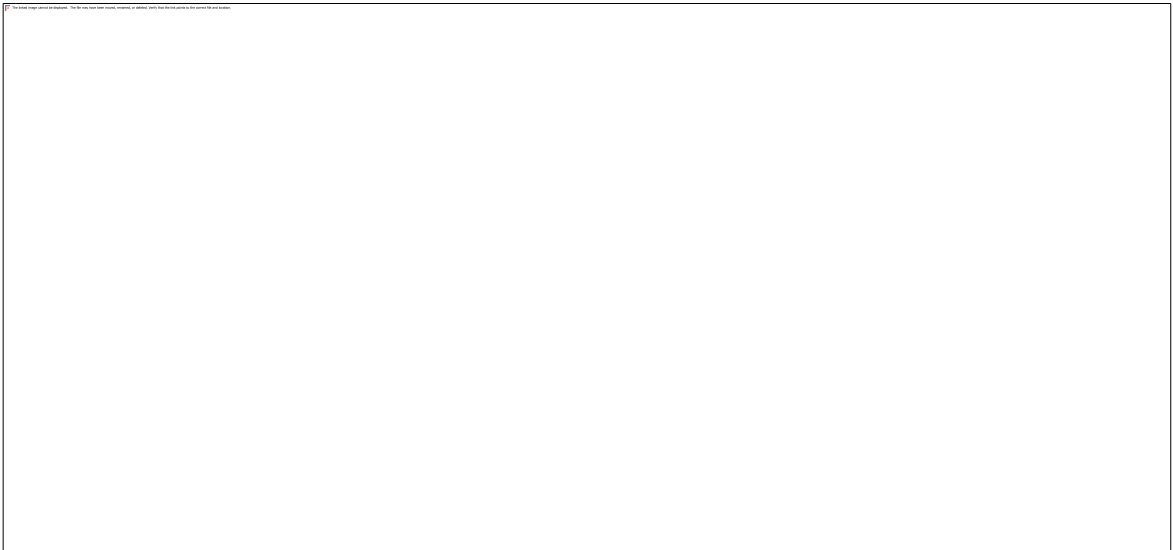
7. Click **OK**.

8. Similarly, select the next application or module and repeat the procedure from steps 5 to 7.

9. Disable the built-in JAX-RS via JVM property.

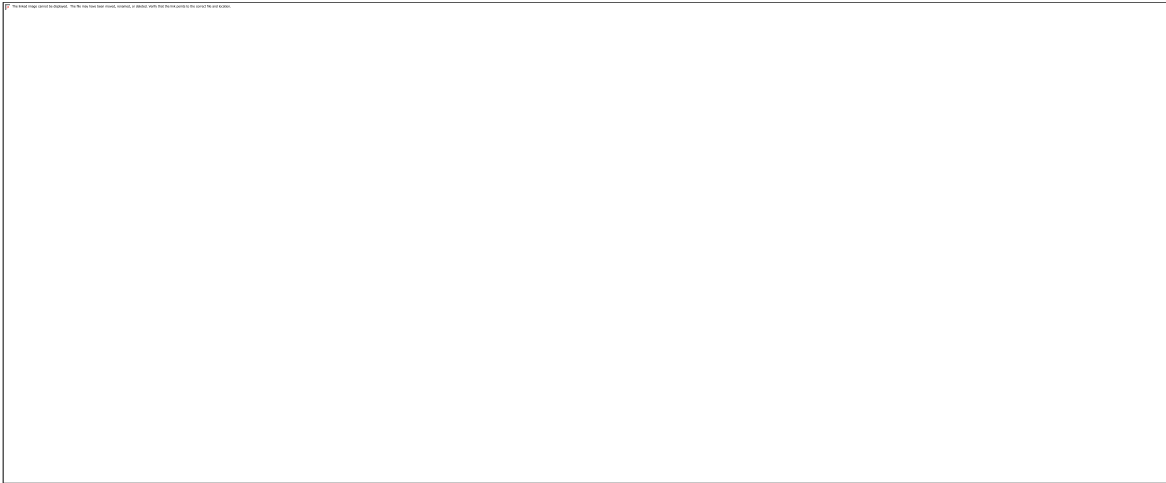   a. Go to WebSphere admin console in **Servers > WebSphere Application Servers > yourServerName**.

    b. In **Server Infrastructure** section, go to **Java and Process Management > Process definition > Java Virtual Machine > Custom properties**.

    c. Add the following property:

    ```
    com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine=true
    ```

10. Restart the application.

1.5   Update Constraints Utility

This utility applies a new naming convention to constraints (PK and FK) to resolve the following issues:

- For tables with similar names which are relatively long (>27 characters) where initial few characters differ (for example, STG_COMMON_ACCOUNT_SUMMARY, FCT_COMMON_ACCOUNT_SUMMARY), the constraint names get generated as same causing an Oracle error of duplicate constraints.

- When number of foreign keys for a table is more than 100, the length of the constraint name exceeds the permissible limits allowed by Oracle Database.

The new naming convention has the following logic. A Unique ID gets generated for each data model entities. The new constraint name will be generated by appending the unique ID with 'FK' or 'PK' (along with a sequence for FK). For example PK on DIM_ACCOUNT will be formed as PK_101, where 101 is the unique id of DIM_ACCOUNT. Similarly, FKs on FCT_ACCOUNT_SUMMARY will be FK_206_01, FK_206_02, FK_206_03, FK_206_04, where 206 is the unique id of FCT_ACCOUNT_SUMMARY and the table has 4 FKs.

ORACLE®

This utility is executed during the OFSAAI 8.0.6.0.0 patch installation. After successful installation of the OFSAAI 8.0.6.0.0 installer patch, verify the messages in the `Update.log` file in the directory `$FIC_HOME/utility/UpdateConstraints/logs` for any errors or failures. This directory is created by the Update Constraints Utility. You can also verify the installation status from the value in AAI_MU_UTIL_UPDATE_CONS. V_FLAG_VALUE from the **Config Schema** table. If the value is **N** for an Infodom, it is a failure.

In case of errors, identify and troubleshoot the failed Infodoms. Once you have completed the troubleshooting, execute the standalone utility for the failed Infodoms.

1.5.1 How to Execute the Utility

Utility performs the backup of the following files under `ftpshare/<INFODOM>_encon_bkp` but restoration is not done.

- ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml

- Constraint scripts under ftpshare/<INFODOM>/erwin/scripts/table

- Constraint scripts under ftpshare/<INFODOM>/scripts

To execute the utility, perform the following steps:

1. Navigate to `$FIC_HOME/utility/UpdateConstraints/bin/` directory and grant RWX (755) permissions for all executables (.sh files).

2. Execute the utility manually for each of the failed information domains.

   `$FIC_HOME/utility/UpdateConstraints/bin/execute.sh $INFODOM`

3. If the process is successful, verify the following references for new constraint names:

   - ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml

   - Constraint scripts under ftpshare/<INFODOM>/erwin/scripts/table

   - Constraint scripts under `ftpshare/<INFODOM>/scripts`

   - Object registration tables for constraints, REV_TAB_CONSTRAINTS, REV_TAB_REF_CONSTRAINTS, REV_TAB_CONSTRAINT_COLUMNS.

   - Oracle Data Dictionary in respective Atomic Schema for each Infodoms.

4. In case of failure, refer the utility's log and identify the cause of the failure. Resolve the issues before proceeding with the re-run of the utility. For more queries, contact Oracle Support Services.

1.5.2 Troubleshooting

Utility goes through six different steps, which can be traced with the below messages.

> **NOTE:** At every stage identify the cause of the failure and resolve the issues before proceeding with the re-run of the utility.

Steps	Description	Action to be taken
1	Generate Scripts and updating DATABASE.XML	**Step 1**: Restore the file backed up at **ftpshare/<INFODOM>_encon_bkp/erwin/fipxml/<INFODOM>_DATABASE.xml** to the destination **ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml**. **Step 2**: Restore the directories backed up at **ftpshare/<INFODOM>_encon_bkp/erwin/scripts/table** to the destination directory **ftpshare/<INFODOM>/erwin/scripts/table**. **Step 3**: Restore the directories backed up at **ftpshare/<INFODOM>_encon_bkp/scripts** to the destination directory **ftpshare/<INFODOM>/scripts**. **Step 4**: Re-run the utility.
2	Triggering Object Registration	**Step 1**: Restore the file backed up at **ftpshare/<INFODOM>_encon_bkp/erwin/fipxml/<INFODOM>_DATABASE.xml** to the destination **ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml**. **Step 2**: Restore the directories backed up at **ftpshare/<INFODOM>_encon_bkp/erwin/scripts/table** to the destination directory **ftpshare/<INFODOM>/erwin/scripts/table**. **Step 3**: Restore the directories backed up at **ftpshare/<INFODOM>_encon_bkp/scripts** to the destination directory **ftpshare/<INFODOM>/scripts**. **Step 4**: Re-run the utility.

Steps	Description	Action to be taken
3	Gathering information about previous constraint names	**Step 1**: Restore the file backed up at **ftpshare/<INFODOM>_encon_bkp/ erwin/fipxml/<INFODOM>_DATABASE.xml** to the destination **ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml**. **Step 2**: Restore the directories backed up at **ftpshare/<INFODOM>_encon_bkp/erwin/scripts/table** to the destination directory **ftpshare/<INFODOM>/erwin/scripts/table**. **Step 3**: Restore the directories backed up at **ftpshare/<INFODOM>_encon_bkp/scripts** to the destination directory **ftpshare/<INFODOM>/scripts**. **Step 4**: Re-run the utility.

Steps	Description	Action to be taken

4	Alter constraints	**Step 1:**
		Execute the following statements to drop the back up tables in Atomic Schema:
		
		`Drop table REV_TAB_CONSTRAINTS_U;`
		
		`Drop Table REV_TAB_REF_CONSTRAINTS_U ;`
		
		`Drop table REV_TAB_CONSTRAINT_COLUMNS_U;`
		
		Step 2:
		Restore the file backed up at
		ftpshare/<INFODOM>_encon_bkp/erwin/fipxml/<INFODOM>_DATABASE.xml to the destination
		ftpshare/<INFODOM>/erwin/fipxml/<INFODOM>_DATABASE.xml.
		
		Step 3:
		Restore the directories backed up at
		ftpshare/<INFODOM>_encon_bkp/erwin/scripts/table to the destination directory **ftpshare/<INFODOM>/erwin/scripts/table**.
		
		Step 4:
		Restore the directories backed up at
		ftpshare/<INFODOM>_encon_bkp/scripts to the destination directory **ftpshare/<INFODOM>/scripts**.
		
		Step 5:
		Modify `r_rename_cons.sql` that is available in the `$FIC_HOME/utility/UpdateConstraints/Scripts/<INFODOM>` directory by adding semicolon at the end of each line.
		
		Step 6:
		Execute the file `r_rename_cons.sql` in the Infodom Atomic Schema.
		Note: Ignore any ORA errors related to 'constraint does not exist'.
		
		Step 7:
		Re-run the utility.

Steps	Description	Action to be taken

5	Clear data of previous constraints	This can be considered as a successful case. However, user needs to execute the following SQL commands.
		
		Step 1:
		Execute the following statements to drop the back up tables in Atomic Schema:
		
		`Drop table REV_TAB_CONSTRAINTS_U;`
		
		`Drop Table REV_TAB_REF_CONSTRAINTS_U ;`
		
		`Drop table REV_TAB_CONSTRAINT_COLUMNS_U;`
		
		Step 2 :
		Execute the statement in Configuration Schema, after replacing <INFODOM> with the respective information domain:
		
		`UPDATE aai_mu_util_update_cons SET`
		`V_FLAG_VALUE='Y',V_UPDATE_DATE=SYSDATE where`
		`DSNID='<INFODOM>'`

6	Update Successful	-

1.6 Sandbox Resave Utility

A utility is provided to regenerate the CONSTRAINTS.XML as per the changes done as part of Update Constraints utility. The constraint xml is required for sandbox data population which will store the foreign key names of all the tables.

The xml files which will be re-generated are:

```
ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/CONSTRAINTS.xml
```

```
ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/<TABLE_NAME>.xml
```

1.6.1 Prerequisites

Update Constraints utility should have been run successfully on all the sandbox and production Infodoms.

1.6.2 How to Run the Utility

1. Navigate to `$FIC_HOME/utility/sandboxutil/bin` directory and grant RWX (755) permissions for all executables (.sh files).

2. Execute the utility using the following command:

    ```
    ./updatesandbox.sh
    ```

3. Verify logs from `$FIC_HOME/utility/sandboxutil/logs/Update.log` directory.

4. If the process is successful, verify the following references for new constraint names:

    ```
    ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/CONSTRAINTS.xml
    ```

    ```
    ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/<TABLE_NAME>.xml
    ```

5. In case of failure, refer the utility's log and restore the backups for file system. Execute the utility for the failed infodoms one by one using the following command:

    ```
    $FIC_HOME/utility/sandboxutil/bin/updatesandbox.sh $INFODOM.
    ```

NOTE:	Utility does the backup of `ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox` directory as `ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox_bkp`, but restore is not done. Restore should be done manually in case of any failure. The backup directory will be created in the app ftpshare area. In case of any failure the backup has to be replaced in the db ftpshare area also.

For more queries, contact Oracle Support Services.

ORACLE®

1.7 Model Resave Utility

If you upgrade OFS AAI to 8.0.6.0.0 from an older version, you have to resave all ORE based models. To resave, you have to use the utility `modelresave.sh`, which is available in the directory `$FIC_DB_HOME/bin`.

NOTE:	You cannot trigger the model resave utility if the *RQADMIN* role is not granted to Configuration Schema. For more information on granting the role, refer to the section *Configuration for Oracle R Distribution and Oracle R Enterprise (ORE)* in the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide v8.0.2.0.0

To run the utility from the console:

1. Navigate to `$FIC_DB_HOME/bin` directory and grant RWX (755) permissions for all executables (.sh files).

2. Execute the utility using the following command:

   `./modelresave.sh`

   This will resave all the available ORE models.

3. Provide the following parameter if you want to resave ORE models that are present in a particular information domain:

   ▪ INFODOM- Specify the information domain name if you want to resave the models only in a particular information domain.

   For example, `./modelresave.sh <infodom>`

You can find the logs in `$FIC_DB_HOME/log/migration.log`.

1.8 Enabling Transparent Data Encryption (TDE) and Data Redaction

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 after upgrade to OFSAA 8.0.6.0.0 version from a previous version.

1.8.1 Prerequisites

1. Ensure the required Oracle Database Server versions are installed :

   - Oracle Database Server Enterprise Edition 11g Release 2 (11.2.0.4.0 +) - 64 bit RAC/Non-RAC with/ without partitioning option, Advanced Security Option

   - Oracle Database Server Enterprise Edition 12c Release 1 (12.1.0.1.0 +) - 64 bit RAC/ Non-RAC with/ without partitioning option, Advanced Security Option

2. Ensure the required patches are applied for your respective Oracle DB versions:

   - For Oracle DB Serve 11.2.0.4, the patch 22205607 should have been applied.

   - For Oracle DB Server 12.1.0.1 and 12.1.0.2, the patches 27010930 and 22205607 should have been applied.

1.8.2 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.

Perform the following steps to configure TDE for OFSAA:

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.
NOTE:	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 under *Generic Configurations* chapter in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.

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.

1.8.2.1   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: 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

---

ORACLE

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:

Step 1: Setting the COMPATIBLE initialization parameter for tablespace encryption

Step 2: Setting the tablespace TDE master encryption key

Step 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:

   ```
   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:

   a. 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`).

b. 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`

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

   For example:

   `COMPATIBLE = 12.2.0.0`

d. 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`

e. 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.

See the following reference link for details on manually creating encrypted tablespaces:

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

ORACLE®

1.8.2.2 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, which indicates whether the TABLESPACE is encrypted or not in the ENCRYPTED column:

```
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.

1.8.3 Enabling Data Redaction

OFSAAI 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.

To enable Data Redaction, 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.sq`
   `l` 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 8.0.6.0.0.

Appendix A – Frequently Asked Questions (FAQ)

Which release version of OFS AAAI 8.x on OSDC should I choose to install?

You can choose OFS AAAI 8.0 or higher versions. However, Oracle recommends that you install OFS AAAI 8.0.2.0.0.

What are the browsers supported for OFS AAAI?

OFS AAAI supports web browsers Microsoft Internet Explorer™, Google Chrome™ and Mozilla Firefox™. For detailed information, refer to the Technology Matrix.

NOTE: The support information for browsers mentioned here is applicable only for OFS AAAI. For browser support information on other OFSAA applications, refer to the respective application pack documentation. Oracle provides Web Browser support in accordance with the vendor support policy listed on Oracle Software Web Browser Support Policy.

What is the screen resolution supported for OFS AAAI?

OFS AAAI supports screen resolutions of 1024 x 768 and 1280 x 1024 pixels.

Should I select inbuilt browser-based property 'Prevent this page from creating additional dialogs' in Chrome and FireFox?

No, this will block the OFS AAAI dialogs from displaying on the screen and impact the functionality.

What checks does the 8.0.6.0.0 Release patch perform?

- Environment Check- As part of environment check, it performs Java validation, Environment Variables validation, OS specific validation, DB specific validation, and it shuts down all OFSAAI Services (Infrastructure Server, ICC Server, and back-end services).

- Post Install check- As part of Post Installation check, it checks if OFSAAI services can be successfully started.

Which version of ERwin Data Modeler does OFSAAI support?

The references to Data Modeler ERwin versions 70, 71, 72, 90, 92 and 96 are provided for the AAI framework to support these for backward compatibility. However, the data model-slices shipped with OFS AAAI 8.0.6.0.0 application packs are compatible with Erwin versions 9.5, 9.6, and 9.7.

What should I do for viewing the log files in Debug level for troubleshooting?

By default, the log level is set as INFO. You need to manually change it to Debug to view the log files in debug level. Based on your requirement, you can change the log level to Warn, Error, or Fatal as well.

1. Navigate to *$FIC_HOME/conf* in the APP layer of your OFSAAI installation.

     ▪   Change the **priority value** to **Debug** in the *RevLog4jConfig.xml* file.

For example:

```
<root>
  <priority value ="debug" />
  <appender-ref ref="ConsoleAppender1"/>
</root>
```

     ▪   Change the value of **LOGGERLEVEL** in the *DynamicServices.xml* file from **20** to **0**. (**20** is the value for Info and **0** for Debug.)

NOTE: For multi-tier installation, you need to change the log level to Debug in the *DynamicServices.xml* and *RevLog4jConfig.xml* files, which are present in *$FIC_APP_*HOME*/conf*, *$FIC_DB_HOME/conf*, and *$FIC_WEB_HOME/conf* as well.

---

2. Navigate to *$FIC_WEB_HOME/webroot/conf* and change the **priority value** to **Debug** in the *ExportLog4jConfig.xml* , *MDBLogger.xml*, and *PR2Logger.xml* files for viewing log files in Debug level for the modules Archive/Restore, Metadata Browser and RRF respectively.

3. Generate the application EAR/WAR file and redeploy the application onto your configured web application server. For more information on generating and deploying EAR / WAR file, refer to the *Post Installation Configuration* section in the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide.

4. Restart the OFSAAI Services (APP and WEB). 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.

Can I install OFSAA 8.0.0.0.0 release Application Packs on an OFSAA instance which is already upgraded to a higher version say 8.0.6.0.0?

Yes. You can install an OFSAA 8.0.0.0.0 release Application Packs on an OFSAA instance which is already upgraded to a higher version. Refer the *Installer and Installation Prerequisites* table *(*section Installer and Installation Prerequisites >> Category Others >> Sub-Category OFSAA) in the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide for more details prior to proceeding with the installation.

While executing an ORAAH model created in a Hive sandbox, a message [1] "package 'ORE' not found" is displayed in the log file generated in Remote R server. What should I do?

This has no impact on the model execution. You can ignore the log file message and proceed further. Please verify if the OJDBC6 jar is placed in the lib path of the remote box.

What should I do when model execution fails in ICC?

If model execution fails in ICC, check whether the optional parameter is set to $MODE=M. If not, set it to $MODE=M and run the model execution.

ORACLE®

OFSAAI
8.0.6.0.0 Installation and Configuration Guide

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com/us/industries/financial-services/

Oracle Financial Services Software