Oracle Financial Services Analytical Applications Infrastructure

Administration and Configuration Guide

Release 8.1.x

April 2024

ORACLE
Financial Services

ORACLE

OFS Analytical Applications Infrastructure Administration Guide

Document Control

Version Number	Revision Date	Change Log
2.0	April 2024	• Included topic for adding FIC_MIS_DATE Option During Batch Creation IN AAI Run Framework (36419221) • Updated addition of PMF process details in the Audit trail report (36491694)
1.9	March 2024	Updated steps to update atomic schema password (36119985)
1.8	December 2023	Added section for System for Common Domain Identity Management (SCIM) (36067267)
1.7	October 2023	Added patch details to prevent creating AAI and other related tables, while creating Infodom in Using REST APIs for User Management from Third-Party IDMs. (35877027)
1.6	September 2023	A note has been added under Understanding REST API Specifications section.
1.5	August 2023	Updated the following API details in Using REST APIs for User Management from Third-Party IDMs. (35493671) • Create Application • Delete Application • Create Infodom • Delete Infodom • Create segment • Authorize role group • Authorize domain group • Create Database Details
1.4	March 2023	Replaced/deleted references to include Apache big data in the relevant sections.
1.21	March 2023	Updated the information related to PortC utility running without manual intervention. (34193711)
1.20	February 2023	Updated information for enabling and disabling users with Sysadmn and Sysauth roles without answering the security questions (35033898)
1.19	January 2023	Added the following sections: • Reverting the Data Redaction for an individual Policy • Reverting the Data Redaction for an individual Column
1.18	December 2022	Added **Force User Delete** REST API under Understanding REST API Specifications section – (34801724).
1.17	November 2022	Updated Configuring Password Changes Section with information for changing the password for config and atomic schema of a target environment - (34489091)

Version Number	Revision Date	Change Log
1.16	August 2022	Updated following sections : • Added information related Oracle Wallet - Configurations for Connecting OFSAA to Oracle Database using Secure Database Connection (TCPS) • Updated information in Note section for SYSDBA during Schema creator execution in online and offline mode -Configure OFSAA to Store Config Schema, Atomic Schema, and SysDBA Credentials with Oracle Wallet • Added information about standard alias names - Configuring OFSAA and various Web Application Servers with Oracle Wallet
1.15	August 2022	Updated encryption information in Key Management Section.
1.14	April 2022	Added the Appendix B – Additional Information in REST APIs for User Status and User Access Reports Section (Doc 33531880).
1.13	March 2022	Updated the Resetting a User Section (Doc 33786717).
1.12	February 2022	Added the Configuring Password Changes Section (Doc 33796200 and 33858601).
1.11	December 2021	Updated the Setting Up of Secondary AM Server Section (33035719).
1.10	November 2021	Updated the Understanding REST API Specifications section (Doc 33544923 and Doc 33544922).
1.9	October 2021	Updated the Executing EncryptC Utility (Doc 33479398).
1.8	September 2021	Updated the Understanding REST API Specifications section (Doc 32820508).
1.7	August 2021	• Added a note in the Configuring OFSAA and various Web Application Servers with Oracle Wallet section (Doc 32638370). • Updated the Understanding REST API Specifications section (Doc 32769246 and Doc 33181636). • Updated the General Configurations for Dimension Management Module section (DOC 32404359). • Updated the Changing IP/ Hostname, Ports, and Deployed paths of the OFSAA Instance section (Doc 33165413).
1.6	July 2021	Updated the Understanding REST API Specifications section for Doc 32769246.
1.5	June 2021	Updated the Configurations for Connecting OFSAA to Oracle Database using Secure Database Connection (TCPS) section for Doc 32956215.
1.4	January 2021	• Updated the guide for the OFS AAI v8.1.1.0.0 release. • Added a note for JCE enabled by default for Java versions in the Enabling Unlimited Cryptographic Policy for Java for Java section (Doc 32353959). • Updated the Sqoop 1 Cluster Mode section for SSH Auth Alias (Doc 32418654).
1.3	October 2020	Added the Delink ICC Server from FICServer section (Doc 32006156).

Version Number	Revision Date	Change Log
1.2	July 2020	Added the Configure Document Upload File Timeout and File Transfer section.
1.1	June 2020	Added the Configure Document Upload Settings section (Doc 31379149).
1.0	May 2020	Created the document for the OFS AAI v8.1.0.0.0 release.

Table of Contents

1 Preface

This Preface provides supporting information for the Oracle Financial Services Analytical Applications Infrastructure (OFS AAI) Administration Guide and includes the following topics:

1.1 What is New in this Release of OFSAAAI Application Pack

This section lists new features and changes in the OFSAAAI Application Pack for Release 8.1.2.0.0.

1.1.1 New Features in Release 8.1.2.0.0

This section lists the new features described in this Administration Guide.

Table 1: New features in the OFSAAAI Application Pack Release 8.1.2.0.0

Feature	Description
Using REST APIs for User Management from Third-Party IDMs	• Configure the value for 'SMS AUTH ONLY' through the Identity Management (IDM) RESTful API. • Map Users to a Group through the RESTful API.

For more details, see the Oracle Financial Services Advanced Analytical Applications Infrastructure Release 8.1.2.0.0 Readme.

1.1.2 Deprecated Features

There are no Deprecated Features in this release.

1.1.3 Desupported Features

There are no Desupported Features in this release.

1.2 Summary

This document includes the necessary instructions for module specific configurations. We recommend you to download the latest copy of this document from OHC Documentation Library which includes all the recent revisions (if any) done till date.

1.3 Audience

Oracle Financial Services Analytical Applications Infrastructure Administration Guide is intended for administrators and implementation consultants who are responsible for installing and maintaining OFSAAI.

1.4 Related Documents

This section identifies additional documents related to OFSAA Infrastructure. You can access the following documents from OHC Documentation Library.

- Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide
- Oracle Financial Services Analytical Applications Environment Check Utility Guide
- Oracle Financial Services Analytical Applications Infrastructure User Guide
- Oracle Financial Services Analytical Applications Infrastructure Security Guide

1.5 Conventions

The following text conventions are used in this document:

Table 2: Conventions used in this document

Conventions	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.

1.6 Abbreviations

The following table lists the abbreviations used in this document:

Table 3: Abbreviations used in this document

Abbreviations	Meaning
AIX	Advanced Interactive eXecutive
EPM	Enterprise Performance Management
F2H	HDFS File/Flat File to HDFS target
HDFS	Hadoop Distributed File System
H2T	HDFS-Hive source to RDBMS target mapping
H2H	HDFS-Hive source to HDFS target
H2F	HDFS-Hive source to Flat File target
JCE	Java Cryptography Extension
KBD	Key Business Dimensions
MFA	Multi-Factor Authentication
OEL	Oracle Enterprise Linux
OFSAAI	Oracle Financial Services Analytical Applications Infrastructure
OLH	Oracle Loader for Hadoop
PII	Personally Identifiable Information
RDBMS	Relational Database Management System
RHEL	Red Hat Enterprise Linux
RRF	Run Rule Framework
SCD	Slowly Changing Dimension

Abbreviations	Meaning
SQL	Structured Query Language
TDE	Transparent Data Encryption
T2H	RDBMS source to HDFS-Hive target
UDP	User Defined Properties
UMM	Unified Metadata Manager
VM	Virtual Machine

2 Data Management Tools (DMT) Module Configurations

This chapter details about the configurations required in the Data Management Tools module.

Topics:

2.1 Data Mapping Configurations

This section details about the configurations required for the following Data Mapping Definitions:

2.1.1 Data Movement from RDBMS Source to HDFS Target (T2H)

2.1.1.1 Default Implementation

Step 1: Configure the Properties

1. From *DMT Configurations* window, set **T2H mode** as **Default**.
2. From the *Register Cluster* tab in the *DMT Configurations* window, register a cluster with Target Information domain name as the Cluster **Name**.

   For more information, see the *DMT Configurations* section in the OFS Analytical Applications Infrastructure User Guide.

Step 2: Copy the required Jars

Copy the following Third-Party Jars from the Apache installation libraries into the `$FIC_HOME/ext/lib` folder:

- `re2j-1.1.jar`
- `commons-cli-1.2.jar`
- `htrace-core4-4.1.0-incubating.jar`

- `hadoop-hdfs-3.1.1.jar`

2.1.1.2 Sqoop Implementation

1. From *DMT Configurations* window, set **T2H Mode** as **Sqoop**.
2. Sqoop must have been installed and configured in your system. For more information on how to use Sqoop for T2H, see Sqoop Configuration.

2.1.2 Data Movement from HDFS Source to RDBMS Target (H2T)

2.1.2.1 Default Implementation

From *DMT Configurations* window, set **H2T mode** as **Default**. For more information, see the *DMT Configurations* section in the OFS Analytical Applications Infrastructure User Guide.

2.1.2.2 OLH (Oracle Loader for Hadoop) Implementation

1. From *DMT Configurations* window, set **H2T Mode** as **OLH**.
2. OLH (Oracle Loader for Hadoop) must have been installed and configured in your system. For more information on required configurations, see Oracle® Loader for Hadoop (OLH) Configuration.

2.1.2.3 Sqoop Implementation

3. From *DMT Configurations* window, set **H2T Mode** as **Sqoop**.
4. Sqoop must have been installed and configured in your system. For more information on how to use Sqoop for H2T, see Sqoop Configuration.

2.1.3 Data Movement from File to HDFS Target (F2H)

This section talks about the configurations required for data movement involving Hive based source or target (F2H).

- HDFS-File to HDFS target
- Local Flat File to HDFS Target

Step 1: Configure Properties

1. From *DMT Configurations* window, select **Is Hive Local** as **Yes** if Hive Server is running locally to OFSAA, else select **No,** from the drop-down list.

   For more information, see the *DMT Configurations* section in the OFS Analytical Applications Infrastructure User Guide.

2. From the *Register Cluster* tab in the *DMT Configurations* window, register a cluster with Target Information domain name as the Cluster **Name** for the following scenarios:
   - If Flat File is local and **Is Hive Local** is set as **No**

- If Flat File is Remote and **Is Hive Local** is set as **Yes**

Step 2: Copy the required Jars

Copy the following Third-Party Jars from the Apache installation libraries into the `$FIC_HOME/ext/lib` folder:

```
commons-cli-1.2.jar
hadoop-hdfs-3.1.1.jar
htrace-core4-4.1.0-incubating.jar
```

2.1.4 Data Movement of WebLog Source to HDFS Target (L2H)

2.1.4.1 Prerequisites

- Apache Hadoop
- Create a folder (`/<Weblog Working Directory>`) in HDFS and provide 777 permissions for the same.

2.1.4.2 Configurations

Following are the configurations required in case of HDFS based WebLog source:

1. From the *Register Cluster* tab in the *DMT Configurations* window, register a cluster with Target Information domain name as the Cluster **Name**.

   For details, see *Cluster Registration* section in the OFS Analytical Applications Infrastructure User Guide.

2. Copy the required Third-Party Jars from the Apache installation libraries into the following location `$FIC_HOME/ext/lib`:

   ```
   commons-httpclient-3.1.jar
   commons-cli-1.2.jar
   hadoop-hdfs-3.1.1.jar
   protobuf-java-2.5.0.jar
   htrace-core4-4.1.0-incubating.jar
   jackson-mapper-asl-1.9.13.jar
   jackson-core-2.3.1.jar
   avro-1.8.1.jar
   ```

   ```
   hadoop-mapreduce-client-core-3.1.1.jar
   ```

NOTE	Ensure the jars are part of Big Data installation is also present in the above location.

NOTE	The version of the aforementioned Jars to be copied differs depending upon the version of the Apache configured based on the Technology Matrix.

3. Copy `core-site.xml, hdfs-site.xml, mapred-site.xml, hive-site.xml`, and `yarn-site.xml` from the Hadoop Cluster to the location mentioned in the **Configuration File Path** field in the *Cluster Configurations* window and the `<deployed location>/conf` folder. Note that only Client Configuration Properties are required.

> **NOTE** If the proxy user option is enabled and the Job is submitted by the same, the user should be created in every node of the Hadoop Cluster.

4. 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, see the *Post Installation Configuration* section in OFS AAAI Installation and Configuration Guide.
5. Restart all the OFSAAI services. For more information, see the *Start/Stop Infrastructure Services* section in the OFS AAAI Installation and Configuration Guide.

2.1.4.3 Logger Types Seeded Table

Standard logger types and their details are seeded in the `AAI_DMT_WEBLOG_TYPES` table. By default, the details for the Apache and Microsoft-IIS logs are pre-populated. You can add other logger methods to the table to make them visible in the UI.

The sample entries for the logger types are given in the following table:

Table 4: Logger Types Seed table

V_LOG_TYPE	V_LOG_COLUMNS	V_LOG_COL_DATATYPE	V_LOG_REGEX
Apache Sample	IP,Identity,User,Time,URL,Status,Size,Referer,Agent,Bytes	string,string,string,string,string,string,string,string,string,string	([^]*) ([^]*) ([^]*) (-|\[[^\]]*\]) ([^ \"]*|\"[^\"]*\") ([0-9]*) ([0-9]*) ([^ \"]*|\"[^\"]*\") ([^ \"]*|\"[^\"]*\") ([0-9]*)
Microsoft-IIS Sample	IP,User,Date,Time,Service,ServerName,ServerIP,TimeTaken,ClientBytesSent,ServerBytesSent,ServiceStatus,WindowsStatus,RequestType,TargetOperation,Parameters	string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,	DELIMITED~,

To add a new logger type, add a new entry in the AAI_DMT_WEBLOG_TYPES table as follows:

- `V_LOG_TYPE`- Enter a name for the custom logger type. The values in this column are displayed as **Logger Type** drop-down list in the *Preview* pane of *Source Model Generation* window for WebLogs.

- V_LOG_COLUMNS- Enter appropriate column names separated by commas, which is displayed in the *Data Model Preview* pane as **Column Names**.
- V_LOG_COL_DATATYPE- Enter the data type for the corresponding column names entered in V_LOG_COLUMNS, separated by commas. The supported Data Types are String and Int. The values in this column are displayed as the **Data Type** for the corresponding **Column Names.** If you do not specify Data Type for a column, Integer is selected by default. You can change it to String if required from the *Source Model Generation* window.
- V_LOG_REGEX- Enter the Regular expression for each Column Name separated by a space. This is displayed as **Input Regex** in the *Source Model Generation* window.

2.2 Oracle® Loader for Hadoop (OLH) Configuration

Oracle® Loader for Hadoop (OLH) is a Map Reduce utility to optimize data loading from Hadoop into Oracle Database. OFSAAI supports OLH as one of the modes for loading data into the RDBMS Tables from Hive Tables.

2.2.1 Prerequisite

- Apache Hive
- Hadoop Client (version compatible with the Hadoop Cluster) on OFSAAI VM (If OFSAAI and Hadoop are not on the same VM)
- Oracle Loader for Hadoop v 3.9.0 on the OFSAAI VM

2.2.2 Steps for Configuring OLH

Step 1: Installing OLH in the OFSAAI VM

1. Unzip the OLH Package downloaded from the Oracle site in the VM where OFSAAI is installed.

   Location: Inside the Home Directory of the user where OFSAAI is installed.

2. Set OLH_HOME environment variable in the .profile file.

   OLH_HOME contains the directories such as bin, examples, jlib and lib.

Step 2: Configuring the Property

1. Set the following property in the jdbcOutput.xml file, which is present in the $FIC_DB_HOME/conf/ location:

```
<property>
<name>oracle.hadoop.loader.connection.defaultExecuteBatch</name>
 <value>100</value>
</property>
```

2. From the *DMT Configurations* window, set **H2T Mode** as **OLH**.
3. From the *Register Cluster* tab in the *DMT Configurations* window, register a cluster with Source Information domain name as the Cluster **Name**.

For more information, see the *DMT Configurations* section in the OFS Analytical Applications Infrastructure User Guide.

Step 3: Copy Configuration XMLs from Hadoop Cluster

1. Copy the following files from the Hadoop Cluster to the **Configuration File Path** given in the *Cluster Configurations* window of the registered cluster.
   - `core-site.xml`
   - `hdfs-site.xml`
   - `mapred-site.xml`
   - `hive-site.xml`
   - `yarn-site.xml`

> **NOTE** Only Client Configuration Properties are required.

2. Modify the following property in the `mapred-site.xml` file in the `$FIC_HOME/conf` folder:

```
<property>
    <name>mapred.child.java.opts</name>
    <value>-Xmx4096m</value>
  </property>
<property>
<name>mapreduce.job.outputformat.class</name>
<value>oracle.hadoop.loader.lib.output.JDBCOutputFormat</value>
</property>
<property>
 <name>mapreduce.output.fileoutputformat.outputdir</name>
 <value>(Any temporary directory)</value>
 </property>
<property>
    <name>oracle.hadoop.loader.defaultDateFormat</name>
    <value>yyyy-MM-dd</value>
  </property>
```

> **NOTE** If proxy user is enabled and the Job is submitted by the same, the user should be created in every node of the Hadoop Cluster.

Step 4: Copy the required Jars

1. Copy `commons-httpclient-3.1.jar` from the Apache installation libraries into the `$OLH_HOME/jlib` folder.
2. If OFSAA is using Apache driver:
   - Usually jars such as `hive-exec-*.jar, libfb303-*.jar, hive-service-*.jar, hive-metastore-*.jar` are present in the `ext/lib` folder and are added to the Classpath. In case of any ClassNotFound Exception, perform the following steps:
     — Edit the `oracle.hadoop.loader.libjars` property present in the `OLH_HOME/doc/oraloader-conf.xml` file to accommodate the newly added jars. That is, `$FIC_HOME/ext/lib/ hive-exec-*.jar` (repeat for each of the mentioned jars)
   - Copy the entire property to the `FIC_DB_HOME/conf/dtextInput.xml` file.

> **NOTE** Add the aforementioned jars only if OLH task is to be run. If any other OFSAA task is running, do not keep a copy of the jars in the `OLH_HOME/jlib` folder.

2.2.3 Limitations

- OLH can read data from a Single Source Table (ANSI joins are not supported) and load it into a single target RDBMS table.
- OLH 2.3.1 is built against HIVE 0.10. It works well with HIVE 0.12 too; however, the Data Type DATE (that is supported in HIVE 12) is not supported by OLH.
- Mapping a Hive column with the Data Type STRING (even if it contains a single character) to an RDBMS column with the Data Type CHAR is not allowed. The Destination Column should be at least VARCHAR2 (1), or the Source Column Data Type should be CHAR.
- Joins/Filters/Expressions are not supported in OLH.

2.3 Sqoop Configuration

Apache Sqoop installation allows the user to load data from the RDBMS tables into Hive tables.

Two types of Sqoop implementations are supported:

- **Sqoop** in Client mode. This mode uses Sqoop export.
- **Sqoop** in Cluster mode. OFSAAI first SSHs to the Sqoop node on the cluster, and then executes the export command.

2.3.1 Prerequisites

- Apache Sqoop server must be up and running.
- Ensure that an appropriate JDBC driver is present in the Sqoop library path on the cluster.

2.3.2 Steps for Configuring Sqoop

2.3.2.1 Sqoop Cluster Mode

1. From the *DMT Configurations* window, set **Sqoop Mode** as **Cluster**.
2. Specify the path of the HDFS working directory for Sqoop related operations in the **Sqoop Working Directory** field.
3. Register a cluster with Target Information domain name as the Cluster **Name** in case of T2H from the **Register Cluster** tab in the **DMT Configurations** window. You can also register a cluster with Source Information domain name as the Cluster **Name** in case of H2T.

   To enable the Sqoop Cluster in SSH mode, provide the appropriate SSH details in the **SSH Server name**, **SSH Port**, and **SSH Auth Alias** fields.

   To create **SSH Auth Alias**, follow these steps:

   a. Log in as SYSADMN and navigate to the **Database Details** window.

   b. Click **Add** (+ symbol) to view the **Database Details** window.

   c. Do not enter **Name** or **Schema** name. Select **ORACLE** for **DB Type** and **DEFAULT** for **Auth Type**.

   d. Click **Add** for **Alias Name**.

   e. Enter an auth alias in **Auth Alias**, enter a valid SSH username in **User/Principal Name**, and enter an SSH password in **Auth String**.

   f. Click **Save** to create and register a new Auth Alias in OFSAA.

   g. Close the **Database Details** window without saving the details in any of the other fields.

   For details, see the *DMT Configurations* section in the OFS Analytical Applications Infrastructure User Guide.
4. Open the command prompt and execute a manual **kinit** on the Sqoop node with SSH user credentials before Sqoop execution. Execute kinit periodically based on the Kerberos settings for the lifetime of the ticket. Also, ensure that the Sqoop commands are executable from the default shell of the SSH user.
5. Copy the following Third-Party Jars from the Apache installation libraries into the `$FIC_HOME/ext/lib` folder:

```
hadoop-mapreduce-client-core-3.1.1.jar
re2j-1.1.jar
commons-cli-1.2.jar
hadoop-hdfs-3.1.1.jar
hadoop-hdfs-client-3.1.1.jar
protobuf-java-2.5.0.jar
htrace-core4-4.1.0-incubating.jar
commons-net-3.6.jar
commons-codec-1.11.jar
sqoop-test-1.4.7.jar
sqoop-1.4.7.jar
jackson-mapper-asl-1.9.13.jar
```

```
jackson-core-2.3.1.jar
avro-1.8.1.jar
```

2.3.2.2 Sqoop Client Mode

Step 1: Configuring the Properties

1. From the *DMT Configurations* window, set **Sqoop Mode** as **Client**.
2. Specify the path of the HDFS working directory for Sqoop related operations in the **Sqoop Working Directory** field.
3. From the *Register Cluster* tab in the *DMT Configurations* window, register a cluster with Target Information domain name as the Cluster **Name** in case of T2H or register a cluster with Source Information domain name as the Cluster **Name** in case of H2T.

   For details, see *DMT Configurations* section in the OFS Analytical Applications Infrastructure User Guide.

Step 2: Copy Third Party Jars

Copy the following Third-Party Jars from the Apache installation libraries into the `$FIC_HOME/ext/lib` folder:

```
hadoop-mapreduce-client-core-3.1.1.jar
re2j-1.1.jar
commons-cli-1.2.jar
hadoop-hdfs-3.1.1.jar
hadoop-hdfs-client-3.1.1.jar
protobuf-java-2.5.0.jar
htrace-core4-4.1.0-incubating.jar
commons-net-3.6.jar
commons-codec-1.11.jar
sqoop-test-1.4.7.jar
sqoop-1.4.7.jar
jackson-mapper-asl-1.9.13.jar
jackson-core-2.3.1.jar
avro-1.8.1.jar
```

> **NOTE** Ensure the jars are part of Big Data installation is also present in the above location.

Step 3: Copy Configuration XMLs from Hadoop Cluster

Copy `core-site.xml, hdfs-site.xml, mapred-site.xml, hive-site.xml,` and `yarn-site.xml` from the Hadoop Cluster to the **Configuration File Path** given in the *Cluster Configurations* window of the registered cluster. Note that only Client Configuration Properties are required.

> **NOTE** If proxy user is enabled and the Job is submitted by the same, the user should be created in every node of the Hadoop Cluster.

2.3.2.2.1 Limitations of Sqoop

- Derived Column cannot be used as the split by column, hence should not have field order 1.
- Date Type Column cannot be used as the split by column. (Sqoop Limitation: Sqoop-1946). Hence it should not have field order 1.

2.4 SCD Execution on Hive Information Domain

You need to consider the following constraints and assumptions for Slow Changing Dimension (SCD) execution on Hive Infodom:

2.4.1 Constraints

1. Default Columns with Surrogate Key (SK) as 0 and -1 will be inserted into destination (DIM) table, only if data is present in the table `DIM_SCD_SEEDED`.
2. `PRTY_LOOKUP_REQD_FLG` should always be set to 'N'.
3. The data type of SK column in destination (DIM) table should always be INT/BIGINT and it will be generated using the following logic:

   `MAX_SKEY + row_number(n)` where (n) is rowid.
4. Query to fetch Maximum SKEY value will give performance improvement, if indexing is done on DIM table.
5. Stage Column where Column Type = 'ED' should be updated with Date in Hive Format – 'yyyy-mm-dd'.

   Apart from this only 'dd-Mon-yyyy' format is supported to keep the current seeding intact. Final data in Date column will always be inserted in 'yyyy-mm-dd' format.
6. Columns which are not part of STG and DIM mapping will be passed as '' (empty strings).
7. Columns with column type STRING/VARCHAR/CHAR will be inserted as empty strings and all other column types will be inserted as NULL.
8. Stage table should not contain duplicate records for the same MISDATE.
9. Two or more SCDs executing in parallel should not update the same Dimension table. In such cases, ensure the processing is sequential. Similar limitation is applicable for the option Map Ref No: =-1.

2.4.2 Assumptions:

1. Primary Key (PK) and Surrogate Key (SK) Columns are mandatory to map, else SCD will fail.

2. Since Hive does not have PK functionality, you should map an ID Column as PK, on the basis of which STG and DIM tables will be matched for TYPE1 and TYPE2.
3. SK column in destination (DIM) table will always be of data type INT/BIGINT.
4. `DIM_SCD_SEEDED` table will be created automatically. You need to insert data manually as mentioned in the following table:

Table 5: Seeded Key and Code

SEEDED_SKEY	SEEDED_CODE	SEEDED_DESC
0	MSG	Missing
-1	OTH	Other

2.5 Heterogeneous Support for SCD to RDBMS

After SCD execution on Hive Information Domain, user can update the data from Hive DIM table to RDBMS DIM table. Consider the following assumptions:

2.5.1 Assumptions

DIM table in Hive and RDBMS should have the same table and column names, though column order may differ but not the data type.

User needs to pass 2 extra parameters `DBSERVERNAME` and `DBSERVERIP` in SCD call to update data from Hive to RDBMS. This is done using RUN EXECUTABLE.

```
<SCD EXECUTABLE NAME>,<REFRENCE NUMBER>,<TARGET RDBMS NAME>,<TARGET RDBMS SERVER>
```

For example:

```
scd,78,devofsatm,192.0.2.1
```

Relevant entry should be present in `AAI_DB_DETAIL` table corresponding to `<TARGET RDBMS SERVER>` and `<TARGET RDBMS NAME>`.

2.6 Configuring DMT Optimization Parameter

To reduce the memory consumption by the decrypt function, the optimization parameter X_ARGS_CPPENC is introduced. By default, the values for Xms is 32m and Xmx is 64m, where 32m and 64m indicates 32 MB and 64 MB of memory respectively.

To override the default values, add the environment variable X_ARGS_CPPENC in the `.profile` file on the server where OFSAA is installed in the following format:

```
X_ARGS_CPPENC="-Xms256m -Xmx512m"
export X_ARGS_CPPENC
```

Note that 256m and 512m are the new values given for Xms and Xmx respectively.

3 Dimension Management Module Configurations

This chapter details about the configurations required in the Dimension Management Module.

Topics:

3.1 Configurations to use Alphanumeric and Numeric Codes for Dimension Members

This section explains the configuration required if you want to enable alphanumeric codes for Dimension Members in the Dimension Management module. This feature can be used if you want to use dimensions that are available in the external source systems, for which the members are maintained as a Number or alpha numeric text. For example, for dimensions like currency, alphanumeric codes can be used to denote the currency codes such as INR, USD, and so on, along with the exact amount.

OFSAAI supports both numeric and alphanumeric codes for Members of a Dimension. Both dimension types require a numeric member code. An alphanumeric dimension additionally stores an alphanumeric member code. After performing the Dimension configurations explained in this section, the **Alphanumeric Code** field in the *Member Definition (New Mode)* window becomes editable. For more information, see the *Adding Member Definition* section in OFS Analytical Applications Infrastructure User Guide.

The REV_DIMENSIONS_B table stores the required dimension metadata including dimension member data type and the member column names for dimension member tables where the numeric and alphanumeric codes are stored.

In the REV_DIMENSIONS_B table:

- The column MEMBER_DATA_TYPE_CODE with value 'NUMBER' identifies a dimension as numeric and value 'VARCHAR2' identifies a dimension as alphanumeric.
- MEMBER_CODE_COLUMN specifies the member table column that holds the alphanumeric member code. This is optional for numeric dimensions, where alphanumeric and numeric member codes would be equivalent.
- MEMBER_COL specifies the numeric member code column.

> **NOTE** Any change done in the REV_DIMENSIONS_B table requires restart of the web server because the dimension definitions data in cache memory has to be refreshed.

A new installation by default will have the seeded key dimensions configured as numeric, although those dimension member tables include a column for alphanumeric member codes. You can configure any of these dimensions as alphanumeric. For more information, see Configure Alphanumeric Dimensions.

You might also need to run some SQL updates for numeric dimensions. For more information, see Configure Numeric Dimensions.

3.1.1 Configure Alphanumeric Dimensions

To configure a numeric dimension as alphanumeric and to remove the optional code attribute from prior releases, you should back up the affected dimension tables (like REV_DIMENSIONS_B, REV_DIM_ATTRIBUTES_B, REV_DIM_ATTRIBUTES_TL, and DIM_<DIMENSION>_ATTR) and perform the following steps on each applicable dimension.

1. Set the member type as alphanumeric (VARCHAR2) in REV_DIMENSIONS_B and identify the member table's alphanumeric code column name, if it is not populated already using the following code:

   ```
   Update REV_DIMENSIONS_B SET
   Member_Data_Type_Code = 'VARCHAR2' [, Member_Code_Column =
   '{Alphanumeric Column Name}'] Where Dimension_ID = {Dimension ID}
   ```

   Example:

   ```
   Update REV_DIMENSIONS_B SET
   Member_Data_Type_Code = 'VARCHAR2', Member_Code_Column =
   'TP_PRODUCT_CODE' Where Dimension_ID = 5;
   ```

   > **NOTE** In OFSAAI 8.1.x, the seeded key dimensions have already populated MEMBER_CODE_COLUMN.

2. In case, any rows in the Dimension member table contain a null alphanumeric code, you can populate the Numeric Member ID itself as alphanumeric member code as illustrated in the following example. This is to ensure that there is no null value for the Alphanumeric Member Code:

   ```
   Update DIM_GENERAL_LEDGER_B set GL_Account_Code = GL_Account_ID Where
   GL_Account_Code is null;
   Commit;
   ```

3.1.2 Configure Numeric Dimensions

If REV_DIMENSIONS_B.Member_Code_Column is populated for a dimension, any UI that displays an alphanumeric code check in the specified column for the member's alphanumeric code. If REV_DIMENSIONS_B.Member_Code_Column is null, the UI assumes no alphanumeric code column exists in the member table and displays the alphanumeric code with the same value as the numeric code. Therefore, for numeric dimensions, you should update the metadata.

There are two options available to configure Numeric dimension.

- Option 1: When the dimension does not have <DIM>_CODE column in <DIM>_B table
- Option 2: When the dimension have <DIM>_CODE column in <DIM>_B table

> **NOTE** By default, no configuration changes are required in the Rev_Dimensions_B table for Numeric dimension, since the REV_DIMENSIONS_B.MEMBER_CODE_COLUMN column has value as either <Dim>_Code or null depending on the availability of <Dim>_Code column.

Option 1: When the dimension does not have <DIM>_CODE column in <DIM>_B table.

In this case, the alphanumeric and numeric code values are stored in the same <DIM>_ID column.

- Back up the REV_DIMENSIONS_B table, if you have not done it already.
- Clear the Member Code Column entries for applicable dimensions.

  For example:

  - For specific numeric dimensions, use the following code:

    ```
    Update REV_DIMENSIONS_B Set Member_Code_Column = null Where
    Dimension_ID in([values]);

    Commit;
    ```

  - For all editable numeric dimensions, use the following code:

    ```
    Update REV_DIMENSIONS_B Set Member_Code_Column = null Where
    Member_Data_Type_Code = 'NUMBER' and DIMENSION_EDITABLE_FLAG = 'Y';

    Commit;
    ```

> **NOTE** If the dimension has <Dim>_Code column and Option 1 is used (that is, the REV_DIMENSIONS_B.MEMBER_CODE_COLUMN is set to null), then the dimension loaders and seeded T2T extracts will fail.

Option 2: When the dimension have <DIM>_CODE column in <DIM>_B table.

In this case, the alphanumeric and numeric code value are stored separately in <DIM>_CODE and <DIM>_ID column (though both the values are same).

- Back up the REV_DIMENSIONS_B table, if you have not done it already.
- Populate the Member Code Column entries for applicable dimensions.

  For example:

  - For specific numeric dimensions:

    ```
    Update REV_DIMENSIONS_B Set Member_Code_Column = <dim>_code Where
    Dimension_ID in([values]);

    Commit;
    ```

  - For all editable numeric dimensions:

    ```
    Update REV_DIMENSIONS_B Set Member_Code_Column = <dim>_code Where
    Member_Data_Type_Code = 'NUMBER' and DIMENSION_EDITABLE_FLAG = 'Y';

    Commit;
    ```

3.1.3 Configure Alphanumeric Code in Simple Dimension Tables

For some editable seeded and user-defined simple dimensions, the alphanumeric code column may not be currently present in the data model. To add this column to a user-defined simple dimension table, you can use Model Upload. Also, you should update the REV_DIMENSIONS_B table as indicated in Dimension Configuration section, to configure alphanumeric properties.

> **NOTE** You should not modify the structure of any seeded simple dimensions.

3.1.4 Create Index on Code Column

You need to create a unique index on the alphanumeric code column if an index does not exist. While creating index, you need to ensure that the index uniqueness should be case insensitive.

Example:

```
Create unique index IDX1_DIM_PRODUCTS_B on DIM_PRODUCTS_B
Upper(PRODUCT_CODE)

Commit;
```

3.2 General Configurations for Dimension Management Module

These configurations are applicable only if you are using the Dimension Management features provided in OFSAAI.

A new table called AAI_AMHM_PROPS table is introduced to configure properties related to the Dimension Management module. Note that in 8.0.x versions, the `AMHMConfig.properties` file was used. The attributes in this table are as follows:

- V_PARAM_NAME- Enter the parameter name. See the succeeding table for the parameter names for the available properties.
- V_INFODOM- Enter the Information Domain name for which you want to apply the property. For each Infodom, you should add a new row with the required Information Domain name in the table.
- N_DIMENSION_ID- Enter the dimension ID of the Dimension for which you want to apply a property. For each dimension, you should add a new row with the Dimension ID in the table.
- V_PARAM_VALUE- Enter the value for the corresponding parameter name. See the following table for the available values for various properties.

Table 6: Parameter value and their description for configuring the Dimension Management module

V_PARAMNAME	V_PARAM_VALUE	Description	Example
TREE_NODE_LIMIT	An integer number	Specify the maximum number of tree nodes that should be allowed for the hierarchy. **NOTE:** This property is used to display the Hierarchy as a small or a large Hierarchy. If the tree node limit exceeds the set limit, the Hierarchies are treated as large Hierarchy. The value of **V_INFODOM** and **DIMENSION_ID** must be **NULL** in the **AAI_AMHM_PROPS** table.	30
SEARCH_TREE_NODE_LIMIT	An integer number	Specify the maximum number of tree nodes that should be allowed for the Hierarchy during search. **NOTE:** The value of **V_INFODOM** and **DIMENSION_ID** must be **NULL** in the **AAI_AMHM_PROPS** table.	50
MEMBER_DEL	Y or N	Set this property to Y to allow the user to delete the Members of the Dimension. **NOTE:** The value of **V_INFODOM** and **DIMENSION_ID** must be given in the **AAI_AMHM_PROPS** table.	Y
ATTR_DEF_DATE_FORMAT	Date format	Specify the default date format for the date type Attributes in the *Attributes* window. **NOTE:** The value of **V_INFODOM** must be given in the **AAI_AMHM_PROPS** table.	DD/MON/YYYY
MEMBER_REVERSE_POP	Y or N	Set this property to Y to allow the reverse population of the Members of the Dimensions. **NOTE:** The value of **V_INFODOM** and **DIMENSION_ID** must be given in the **AAI_AMHM_PROPS** table.	Y

V_PARAMNAME	V_PARAM_VALUE	Description	Example
HIERARCHY_REVERSE_POP	Y or N	Set this property to Y to allow the reverse population of Hierarchies of the Dimensions. **NOTE:** The value of **V_INFODOM** and **DIMENSION_ID** must be given in the **AAI_AMHM_PROPS** table.	Y
MAX_DEPTH-FUSION	An integer number	Specify the maximum level to be allowed to build the Hierarchy tree structure. The maximum levels allowed in the Hierarchies should be less than or equal to 15. If the HIERARCHY_REVERSE_POP parameter is set as "Y" and more than 15 levels are created, then an alert is displayed as "The number of levels is exceeding the limit". If the maximum level allowed is set as more than 15 and the HIERARCHY_REVERSE_POP parameter is set as "Y", then an alert is displayed as "Error occurred in Reverse populating the hierarchy". **NOTE:** The value of **V_INFODOM** must be given in the **AAI_AMHM_PROPS** table.	15
HIERARCHY_IN_FILTER_SORT	Y or N	Set this property to Y to sort the nodes alphabetically. **NOTE:** The value of **V_INFODOM** and **DIMENSION_ID** must be given in the **AAI_AMHM_PROPS** table.	Y

NOTE During the upgrade from 8.0.x versions, the properties already configured in the `AMHMConfig.properties` file are automatically populated into the AAI_AMHM_PROPS table.

The following figure shows a sample of the AAI_AMHM_PROPS table:

Figure 1: Parameter value for configuring the Dimension Management module

	V_PARAM_NAME	V_INFODOM	N_DIMENSION_ID	V_PARAM_VALUE
1	SEARCH_TREE_NODE_LIMIT			100
▶ 2	MEMBER_DEL	OFSAAAIINFO	3	Y

4 Rule Run Framework Configurations

This chapter details about the configurations required in the Rule Run Framework module.

Topics:

4.1 Performance Optimization Setting for RRF Module

The Process engine and Rule engine has been enhanced to take advantage of ORACLE's fast insertion into table and partition swap mechanism.

Based on the new enhancement, Rule and Process Execution supports two additional execution modes (apart from the Merge execution mode where Oracle MERFGE query is used). They are:

- Select (select insert query is used) - In this execution mode, all records are moved to a temporary table with the updated records and then moved back to the original table. This improves the performance since INSERT is faster than MERGE. In this execution mode, the actual updated record count cannot be known since all records are moved back from the temporary table to the original.
- Partition (partition swap query is used) - This is somewhat similar to Select execution mode. This also moves all the records to a temporary table with the updated records. However, while moving back, the whole temporary table will be moved as a partition of the original table using the Oracle Partition Swap mechanism. In this mode the record count cannot be known as you are swapping the partitions.

The execution mode can be set in the `QRY_OPT_EXEC_MODE` parameter of the CONFIGURATION table as well as `V_EXECUTION_MODE` parameter in the `AAI_OBJ_QUERY_OPTIMIZATION` table. The parameter value can be set as SELECT, MERGE or PARTITION. The optimization table is newly introduced. Both the tables reside in the Configuration schema.

The Configuration table setting is for global level (applies to all rules and processes execution) and the Optimization setting is for rule/process level.

> **NOTE** The Optimization table setting has preference over the Configuration table setting. That is, if `V_EXECUTION_MODE` in `AAI_OBJ_QUERY_OPTIMIZATION` table is set, that will be considered. If it is not set, then the execution mode will be as per the value given in the `QRY_OPT_EXEC_MODE` parameter in the Configuration table. By default, its value will be MERGE.

The columns and the values to be given in the AAI_OBJ_QUERY_OPTIMIZATION table are indicated as follows:

Table 7: Column name, values, and their description Performance Optimization Setting for RRF Module.

Column Name	Description	Value
V_OBJ_CODE	Rule/Process/Run Code	Rule(PR2_RULE_B.V_RULE_NAME) Process(PR2_PROCESS_B.V_PROCESS_NAME) Run (PR2_RUN_B.V_RUN_NAME)
V_INFODOM_CODE	Infodom Code	Infodom
V_OBJ_TYPE	Rule/Process/Run Type	Rule(RL) Process(PT) Run (RN)
V_EXECUTION_MODE	Type of query used while executing.	MERGE- Merge statement will be used SELECT- Select Insert will be used PARTITION- Partition swap will be used
F_USE_PARTITION	If partition is used as a filter	Y/N
F_USE_ROWID	If ROWID is used other than primary key in MERGE. This is used only for MERGE query execution.	Y/N
V_MERGE_HINT	Used for MERGE or INSERT hint.	
V_SELECT_HINT	Used for SELECT hint	
V_PRE_SCRIPT	Used for alter statements executed before rule execution	
V_POST_SCRIPT	Used for alter statements executed after rule execution.	

4.1.1 Behavior of Execution Modes

Merge, Select and Partition execution modes are supported. If any value is there in the Optimization table, then the execution mode set in the Configuration table will be ignored and it follows a waterfall model as explained:

For Rule Execution:

With Rule Code - checks if rule level execution mode is set. If it is not set, it checks for the next level.

With Process Code - checks if process level execution mode is set. If it is not set, it checks for the next level.

With Run Code - checks if run level execution mode is set. If it is not set, it checks for the next level, that is, `QRY_OPT_EXEC_MODE` parameter in the Configuration table.

For Process Execution:

With Process Code (Process Execution) - checks if process level execution mode is set. If it is not set, it checks for the next level.

With Run Code - checks if run level execution mode is set. If it is not set, it checks for the next level, that is, `QRY_OPT_EXEC_MODE` parameter in the Configuration table.

Consider an example where you have a Run definition (say Run1) with two rules (Rule1 and Rule 2). For Rule1, the execution mode is set as SELECT and Rule 2, it is not set. For Run1, the execution mode is set as PARTITION. In this case, Rule1 will be executed using Select query (as it is set in rule level) and Rule 2 will be executed using PARTITION query (as it is set in the Run level).

4.1.2 Use ROWID

If this is set to Y, ROWID will also be used along with Primary Key in MERGE query. This entry should be made for MERGE execution mode only. This also follows a waterfall model same as execution mode.

- If Use ROWID is set (as Y/N) in the Optimization table, it will take preference over the Configuration table entry.
- If Use ROWID is set as N in Optimization table and
  - It is set to Y in Configuration table, for all the rules ROWID will be used, irrespective of what is set in rule level.
  - It is set to N in Configuration table, then it will check for rule level setting and behave accordingly.
- If Use ROWID is left blank in the Optimization table, it will be considered as N.

4.1.3 Use PARTITION

This has been newly introduced. If a table used in a Rule has partition and is registered with OFSAA Object Registration, then the partition columns will be added as a filter to all the type of rule queries (MERGE/SELECT/PARTITON); provided the USE PARTITION is set to Y. The behavior is same as that of Use ROWID.

4.1.4 Hints/ Scripts

You can enter Merge/ Select Hints and Post/ Pre Scripts in the Optimization table.

- If Hints/ Scripts are given in the Optimization table, those will be considered, and it will not check in the Configuration table.
- If no entry is there in the Optimization table, it will check in the Configuration table and Rule level, and both will be considered during execution.

4.2 Component Registration in RRF

A Component in the context of OFSAAI is an entity which can be executed individually in Operations module to carry out some definite job for which it has been formed. Components within OFSAAI and its application need to be registered so that it is configurable for different installations with very minimal change.

The component registration process helps you to make the components of Process and Run module configurable inside Run Rule Framework (RRF). With component registration, components can be added, modified and deleted from RRF by doing very minimal changes to the system. For registering a component in RRF, the same should be present in ICC also.

Steps to Register Component

Registering Component has been divided into the following steps respectively:

- Component Detailed Implementation Class
- Deployment
- Entry to PR2_COMPONENT_MASTER Table

4.2.1 Component Detailed Implementation Class

The component implementation class has to be made for all the components which are inserted to the `PR2_COMPONENT_MASTER` table.

This class has to extend **com.ofs.aai.pr2.comp.PR2ComponentProps**, in turn to implement the following methods.

- getComponentDescription
- getPorbableParamValues (optional)

Implementation of interface com.ofs.aai.pr2.comp.PR2Component is optional. This interface will be implemented for only the components which can be directly used in a Process or Run. By implementing this class file following methods has to be over written.

- getSummay
- getCompDescMap
- fillTaskParameter
- getUsedTables

Each method takes current username and locale by default.

4.2.1.1 getComponentDescription

This method is used to get the description for all the components which are show in the component tree.

The Input Parameters are:

- String username
- String locale

Return is:

- String

It returns the localized string that has to be displayed for the component in the component tree.

4.2.1.2 getPorbableParamValues

This method is used to identify if a parameter input should be a text box or a drop-down field.

The Input Parameters are:

- String username
- String locale
- String infodom

Return is:

- Map<String, String>

It returns map containing entry key as the value which is shown to the user. The entry value is stored in database.

4.2.1.3 getSummary

This method is used to get all existing definition of the component type existing in the system.

The Input Parameters are:

- String username
- String locale
- String infodom

Return is:

- Hashtable<String, Vector<com.ofs.aai.pr2.comp.bean.TaskDefinition>>

It returns a Hashtable of <String, Vector<TaskDefinition>>. Where key denotes any specific sub-levels to be shown, which in turn contains a JSON object with compName, compDesc, isDinamic, levelImg properties for that sub-level and the Vector<TaskDefinition> contains all the data needed for using the component in a process or run.

4.2.1.4 getCompDescMap

This method is used to find all details about all specified definitions.

The Input Parameters are:

- String username
- String locale
- String infodom
- Map<String, String> descMap
- Boolean allData

Return is:

- Map<String, String>

Passed to the method in Map<String, String>, where key is the definition unique code. The value is a JSON object with defnDesc property with the value same as code. The same JSON has to be replaced with another JSON object containing defnDesc, defnSubType, defnRef1Name, defnRef1Value, defnRef2Name, defnRef2Value, defnRef3Name, defnRef3Value, defnRef4Name, defnRef4Value, defnOptParamName properties. The values populated for these properties as follows.

Table 8: Property Name and their description

Property Name	Description
defnDesc	Populated with <name> for the <code> of the definition, if <name> exists. If <name> does not exist, then populated with <code>:SD. If definition does not exist, then populated with <code>:NA.
defnSubType	Sub-Type of the definition
defnRef1Name defnRef1Value defnRef2Name defnRef2Value defnRef3Name defnRef3Value defnRef4Name defnRef4Value	Any references which can be used to Identify the definition uniquely. There are four of them. So can be put as name and value pairs.
defnOptParamName	If any optional parameter exits and has to be taken as input from user, then only the name can be provided by this property.

There is another input called **allData**, which is a flag. If it is false, then only **defnDesc** has to be passed and when true all the data has to be passed.

After putting the corresponding JSON Object to its <code> the same map is returned back.

4.2.1.5 fillTaskParameter

This method is used to get the parameters for the component which will be used to execute the component in Operations module.

The Input Parameters are:

- String username

- String locale
- String infodom
- String uniqueName
- String subtype
- Map<String, String> allParams

Return is:

- Map<String, String>

It takes uniqueName which is nothing but the <code> of the definition. It also takes subType of the definition and an allParams which is of data type Map<String, String>. This map contains all the probable parameters with it, where key is the parameter name and value is the parameter value. This map contains following params.

- Dollar variables ($RUNID, $RUNSK, $EXEID, $RUNEXECID, $MODE).
- All reference name and value.
- Optional parameter if any.

By using the map another LinkedHashMap will be created in this method with all the parameters needed to run the component in Operations module. Al the parameter in this map has to be put in correct order. This LinkedHashMap will be returned back to the calling method.

4.2.1.6 getUsedTables

This method is used to get the dependent tables for specified definition of the component type.

The Input Parameters are:

- String username
- String locale
- String infodom
- String uniqueName
- Map<String, String> allParams

Return is:

- Set<String>

It takes uniqueName which is <code> of the definition and the same allParam map which is used in fillTaskParameter method. By using these inputs a Set<String> will be formed with all the dependent table data. This data is used to identify a Rule Filter / Process Filter can be applied to this component. This Set will be returned to the calling method.

4.2.2 Deployment

Below steps should be followed for deployment of the component.

1. Place all the image files to the folders mentioned in `V_TREE_IMAGE` column of `PR2_COMPONENT_MASTER` table, relative to <`FIC_WEB_HOME>/webroot folder` of the application.

2. The jar containing the component implementation classes has to be placed into `<FIC_WEB_HOME>\webroot\WEB-INF\lib f`older.
3. Rebuild and redeploy the application.

4.2.3 Entry to PR2_COMPONENT_MASTER Table

`PR2_COMPONENT_MASTER` is the table for storing all components which are used in RRF. You can enter either through backend which is explained here or through UI which is explained in the Component Registration section under RRF module in the OFS Analytical Applications Infrastructure User Guide.

An entry contains the following fields.

Table 9: Column name, type, and their description

Column Name	Type	Description	Null
V_PR2_COMPONENT_ID	VARCHAR2(30)	Represents component type in a Process or Run.	N
V_PR2_COMPONENT_PARENT_ID	VARCHAR2(30)	Indicates parentage which refers to V_PR2_COMPONENT_ID.	Y
V_COMPONENT_ID	VARCHAR2(30)	Existing ICC Component Id.	Y
V_PR2_COMPONENT_CLASS	VARCHAR2(100)	Fully qualified class path of the implementation class for this component.	N
V_TREE_IMAGE	VARCHAR2(100)	Name with relative path (with respect to web context) of the image which will be displayed in the component tree.	N
N_TREE_ORDER	NUMBER(9)	Display order of the component in the tree. The order is done upon the peers.	N
V_SEEDED_BY	VARCHAR2(8)	Differentiates user created and system created. The system created will have this field filled with an application name which cannot be edited from the front-end utility. The components created from front-end utility will not populate any value in this field which can be edited or deleted from front-end.	Y
V_CREATED_BY	VARCHAR2(30)	Stores the creator username.	N
D_CREATED_DATE	TIMESTAMP(6)	Stores created date and time.	N
V_LAST_MODIFIED_BY	VARCHAR2(30)	Stores the modifier username.	Y

Column Name	Type	Description	Null
D_LAST_MODIFIED_DATE	TIMESTAMP(6)	Stores modified date and time.	Y

Example:

```
insert into PR2_COMPONENT_MASTER (V_PR2_COMPONENT_ID,
V_PR2_COMPONENT_PARENT_ID, V_COMPONENT_ID, V_PR2_COMPONENT_CLASS,
V_TREE_IMAGE, N_TREE_ORDER, V_SEEDED_BY, V_CREATED_BY) values ('COMPTYP',
null, 'Component Sample', 'com.sample.ComponentSample',
'sampleImages/sampleComp.gif', 0, 'SEEDEDBY', 'USER')
```

4.2.4 Sample Code

The COMPONETSAMPLE.txt file contains the sample code of a created component.

5 Operations

This chapter details about the configurations required in the Operations module.

> **NOTE** To use the features explained in this section, additional licenses may apply. For details, contact My Oracle Support.

5.1 Delink ICC Server from FICServer

This section is applicable to 8.1.0.1.0+ versions only.

OFSAA predominantly has been a batch centric application that runs in the Application layer. With the increase in the number of batches running concurrently, the memory usage within the Application layer is adversely affected and this results in the slow performance of the applications. ICC server also has to-and-fro traffic requests to FICServer during batch executions to fetch its own metadata, which further degrades the performance of the application.

A way to improve the performance is to separate or de-link the ICC server from FICServer. ICC Server is enhanced to get its own metadata during batch executions without any dependency with FICServer.

Following are the advantages of delinking the ICC server from FICServer:

1. The load on FICServer during batch execution is reduced.
2. ICC server deployed on a different instance to FICServer helps in controlling the memory surge observed on FICServer.
3. You can execute batches concurrently even when the load on FICSERVER is at the peak level.
4. Execution engines with component types such as Load Data, Transform Data, Data Quality and RULE_EXECUTION can be successfully executed without any dependency on FICServer.
5. In case the FICServer is down,
   - You can create batches using the Manage Run Execution (`WSMRERequest.sh`) command line utility with any available component types.
   - You can execute batches through the ESIC (External Scheduler Interface Component) command line utility.

This enhancement is available as a licensed option and the existing architecture of co-existence of ICC and FICServer continues as the default option.

5.1.1 Configure ICC Server on a Separate OFSAA Node

5.1.1.1 Prerequisites

1. A separate OFSAA node must be available where ICC server can be run independent of FICServer.
2. Batches for execution should have the component types as Load Data, Transform Data, Data Quality and RULE_EXECUTION.
3. Ensure the new tier on which the ICC server is running is on similar tech stack as the OFSAA application deployed node.

5.1.2 Steps to Deploy ICC Server in Separate OFSAA Node

> **NOTE** In this section, the App layer refers to the OFSAA node where FICServer is already running, and the ICC layer refers to the new OFSAA node where ICC server will be deployed.

1. Copy the `.profile` file from the App layer to the new ICC layer.
2. Copy the following Jars from the `$FIC_HOME/ficapp/common/FICServer/lib` folder in the App layer to the `$FIC_HOME/ficapp/common/FICServer/lib` folder in the ICC layer.
   - `icccomm.jar`
   - `FICServer.jar`
   - `aai-core.jar`
   - `AESCryptor.jar`
   - `scheduler.jar`
3. Copy the following libraries from the `$FIC_HOME/ficdb/lib` folder in the App layer to the `$FIC_HOME/ficdb/lib` in the ICC layer.
   - `libDatabase.so`
   - `libI18N.so`
   - `libmisc.so`
   - `librevlog.so`
   - `libSms.so`
4. Copy the following folders from the App layer to ICC layer:
   - `$FIC_HOME/ficapp/icc`
   - `$FIC_HOME/conf`
   - `$FIC_HOME/utility/ES`
5. Modify the following parameters specific to the ICC layer in the `.profile` file:
   a. Set `FIC_HOME` variable to the directory that is created as OFSAA home.

b. Set `FIC_DB_HOME` variable to the directory where the ficdb folder is copied.

c. Set `FIC_APP_HOME` variable to the directory where the ficapp folder is copied.

d. Set `JARPATH` variable to the `$FIC_APP_HOME/lib` path.

e. Set `ES_HOME` to the directory where the `utility/ES` folder is copied.

```
ES_HOME=$FIC_HOME/utility/ES
export ES_HOME
```

f. Configure `ORACLE_HOME` and `JAVA_BIN` to the PATH environment variable as follows:

```
PATH=$JAVA_BIN:$ORACLE_HOME/bin:/usr/bin:/bin:/usr/sbin:$FIC_APP_HOM
E/icc/bin

export PATH
```

g. Modify the `LD_LIBRARY_PATH` to point it to the Java installation directory in the ICC layer as shown:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/java/jdk1.8.0_172/jre/lib/amd6
4/server
```

6. In ICC layer, modify the `File name` in the `ICCLog4jConfig.xml` file available in the `$FIC_APP_HOME/icc/conf` folder to point it to the new ICC layer `$FIC_HOME` path.
7. In ICC layer, modify the following variables in the `server.conf.properties` file available in the `$FIC_APP_HOME/icc/conf` path:

Table 10: Variable name and their description with the example.

Variable Name	Description	Example
ICC_SERVER_HOST	The IP address of the ICC server.	ICC_SERVER_HOST=192.0.2.1
OBJECT_SERVER_PORT	The port on which ICC is listening.	OBJECT_SERVER_PORT=6666
ICC_ROUTER_HOST	The IP address of the Router.	ICC_ROUTER_HOST=192.0.2.2
ICC_ROUTER_PORT	The port on which router is listening.	ICC_ROUTER_PORT=7777
MESSAGE_SERVER_HOST	The IP Address of the message server	MESSAGE_SERVER_HOST=192.0.2.3
MESSAGE_SERVER_PORT	The port on which the message server is listening	MESSAGE_SERVER_PORT=8888

8. Execute the following SQL script in the Configuration Schema by replacing <ICCSERVERHOSTIP> with IP address/Hostname of the new ICC layer.

```
UPDATE CONFIGURATION SET PARAMVALUE = '<ICCSERVERHOSTIP>'
WHERE PARAMNAME = '&ICC_SERVER_HOST'
```

9. Update the ICC host name and port as shown in the following in the `AAI_SETUP_PROPS` table of the Config Schema:

V_PROP_NAME	Description	Example
ICC_SERVER_HOST	The IP address of the ICC server.	192.0.2.1
ICC_SERVER_PORT	The port on which ICC is listening.	6666

10. Navigate to `$FIC_APP_HOME/icc/bin` folder and start the ICC server by executing the following command:

    ```
    ./iccserver.sh
    ```

11. Verify the log file `iccserver.log` under `$FIC_HOME/logs/` folder for any errors.

5.2 Distributed Activation Manager (AM) Based Processing

Distributed AM based processing feature allows you to configure AM engines to run on multiple OFSAA nodes and then ICC Batch Tasks can be configured to get distributed across AM engines on multiple nodes to enable distributed/ parallel task executions. Distributed AM based processing is achieved in OFSAA by two mechanisms.

1. Configuring OFSAA processing tier through Load Balancer where Batch Tasks are distributed across multiple AM nodes
2. Manually configuring Batch tasks to run on specific AM nodes

For both mentioned mechanisms, you should configure the Secondary AM server. For details, see the following section.

> **NOTE** For an illustration of the Distributed Activation Manager deployment, see Appendix A.

5.2.1 Setting Up of Secondary AM Server

5.2.1.1 Prerequisites

- For information on hardware and software requirements for setting up of secondary AM server, see *Hardware and Software Requirements* section in OFS AAAI Application Pack Installation Guide.
- Execute the following SQL script on Configuration Schema by replacing `<NEWAMIPADDRESS>` with the IP address/Hostname of the new AM node you want to set up and `<EXISTINGAMIPADDRESS>` with the IP address/IP address of the existing AM server:

  ```
  INSERT INTO ficsysmaster
  (WEBIPADDRESS,APPIPADDRESS,DBIPADDRESS,ETLAPPHOME,NOOFCPUS,VMEMORY,PMEM
  ORY,CACHE,NOOFTHREADS,IOTRANSFER,MAXTRANSPERSEC,DISKSDBSTRIPING,DISKSFI
  LESTRIPING,MAXFILESIZE,MAXFTPFILESIZE,MAXFILENAMELEN,OSDATABLOCKSIZE,DA
  TASETTYPE,STAGEPATH,DBFTPSHARE,DBFTPUSERID,DBFTPPASSWD,DBFTPPORT,DBFTPD
  RIVE,APPFTPSHARE,APPFTPPORT,APPFTPDRIVE,APPFTPUSERID,APPFTPPASSWD,WEBFT
  ```

```
PSHARE,WEBFTPPORT,WEBFTPUSERID,WEBFTPDRIVE,WEBFTPPASSWD,OSTYPE,SOCKETSE
RVERPORT,SEC_SHARE_NAME,SEC_USERID,SEC_PASSWD,F_ISPRIMARY,N_PRECEDENCE)

SELECT
WEBIPADDRESS,APPIPADDRESS,'<NEWAMIPADDRESS>',ETLAPPHOME,NOOFCPUS,VMEMOR
Y,PMEMORY,CACHE,NOOFTHREADS,IOTRANSFER,MAXTRANSPERSEC,DISKSDBSTRIPING,D
ISKSFILESTRIPING,MAXFILESIZE,MAXFTPFILESIZE,MAXFILENAMELEN,OSDATABLOCKS
IZE,DATASETTYPE,STAGEPATH,DBFTPSHARE,DBFTPUSERID,DBFTPPASSWD,DBFTPPORT,
DBFTPDRIVE,APPFTPSHARE,APPFTPPORT,APPFTPDRIVE,APPFTPUSERID,APPFTPPASSWD
,WEBFTPSHARE,WEBFTPPORT,WEBFTPUSERID,WEBFTPDRIVE,WEBFTPPASSWD,OSTYPE,SO
CKETSERVERPORT,SEC_SHARE_NAME,SEC_USERID,SEC_PASSWD,F_ISPRIMARY,N_PRECE
DENCE FROM ficsysmaster

WHERE DBIPADDRESS='<EXISTINGAMIPADDRESS>'
```

To set the newly added AM node as primary node, execute the following SQL script by replacing `<NEWAMIPADDRESS>` with the IP address/Hostname of the newly added AM node:

```
UPDATE FICSYSMASTER SET F_ISPRIMARY = 'Y', N_PRECEDENCE=200 WHERE
DBIPADDRESS = '<NEWAMIPADDRESS>'
```

- Update the `IS_DISTRIBUTED_AM_SUPPORTED` Parameter in the **Configuration** Table.

Following are the steps involved in setting up of secondary AM servers:

1. Copy the following folders to the secondary AM server from the primary OFSAA server:
   - `$FIC_HOME/conf`
   - Entire `ficdb` and its sub-directories
   - `.profile` file from `$HOME` directory of primary OFSAA server
2. Perform the following configurations in the secondary AM server:
   - Modify the following variables in the `.profile` file:
     - Set `FIC_HOME` variable to the directory which is created as OFSAA home (should contain `ficdb` and `conf` folders).

> **NOTE** It is advisable to setup the OFSAA secondary AM under the same user as in the primary server. For example, if OFSAA is installed on the primary server under `/scratch/ofsaausr`, you can setup the secondary OFSAA instance as well under `/scratch/ofsaausr` user.

3. Set `FIC_DB_HOME` variable to the directory where the `/ficdb` folder is copied under secondary AM server.

```
AM_HOME=$FIC_HOME/ficdb
export AM_HOME
AM_CONF_FILE=$FIC_DB_HOME/conf/am.conf
export AM_CONF_FILE
FICTEMP=$FIC_DB_HOME/conf
export FICTEMP
```

4. Ensure the following variables are pointed to valid hostname/IP address on which Message Server and Router server and Router engines are running.

```
MESSAGE_SERVER_HOST=10.XXX.XXX.XXX
export MESSAGE_SERVER_HOST
MESSAGE_SERVER_PORT=6666
export MESSAGE_SERVER_PORT
FIC_ROUTER_HOST=10.XXX.XXX.XXX
export FIC_ROUTER_HOST
FIC_ROUTER_PORT=7777
export FIC_ROUTER_PORT
```

5. Set `JARPATH` variable to `$FIC_DB_HOME/lib`.
6. Ensure ORACLE_SID variable is pointed to correct Oracle Instance and user can successfully connect to this instance from the Secondary AM server using sql/plus.
7. Update secondary AM node details in the `AM.conf` file present under `$FIC_HOME/ficdb/conf` path.

```
<AM_HOST>`<Secondary AM node host name/IP Address>`
<AM_PORT>`<Secondary AM node Port number>`
```

> **NOTE** Do not alter `<ROUTER_NAME>` and `<ROUTER_PORT>` values.

8. Modify the logger XML files such as `MFLogger.xml`, `OFSAALogger.xml`, `DQLogger.xml`, and `PR2Logger.xml` available under `$FIC_DB_HOME/conf` folder with the secondary AM Server `$FIC_HOME` path.

5.2.2 Configuring OFSAA Instance through Load *Balancer* to Distribute Batch Tasks on Multiple AM Nodes

See *Configuring OFSAA Load Balancer* section in the Configuration for High Availability (HA) Best Practices Guide for details on how to configure the Load Balancer.

> **NOTE** Message Server should be running in all the nodes where AM servers are configured.

5.2.3 Executing Batches on Multiple AM Nodes

While defining a Task in a Batch from the *Task Definition* window in the Operations module, you can choose on which node each task needs to be executed. The **Primary IP for Runtime Processes** drop-down list in the *New Task Definition* window displays all the registered AM Server nodes. Select the IP

address of the AM node where you want the task to be executed. For more information on how to define a Batch, see OFS Analytical Applications Infrastructure User Guide.

> **NOTE** Crash handling of backend servers is supported. For more information, see *Crash Handling of Backend Servers* section in OFS Analytical Applications Infrastructure User Guide.

6 Unified Analytical Metadata Configurations

This chapter details about the configurations required in the Unified Analytical Metadata module. It consists of the following sections:

6.1 Hierarchy Node Internationalization

Hierarchy Node Internationalization is a feature available for Business Hierarchies in Oracle Financial Services Analytical Applications Infrastructure. This feature is introduced to internationalize the node description of Regular Business Intelligence Enabled (BI) and Parent Child (PC) Hierarchies and to display them in Hierarchy Browser.

Each Node has a description. Previously, the node descriptions were fetched from the Description column of the Dimension table to facilitate the node description generation in `REV_LOCALE_HIER` table. Hierarchy node Internationalization feature changes the way in which these descriptions are stored in the `REV_LOCALE_HIER` table. The locale specific node descriptions are fetched from Multi Language Support table (`MLS` table). This table holds the node descriptions in all the installed locales, that is, in the locales in which OFSAAI is available.

6.1.1 Scope

The scope of this enhancement is limited to the Hierarchy Browser window. The hierarchies defined are displayed in Hierarchy Browser and the Hierarchy Browser is used in modules such as Unified Metadata Manager, Rules Framework, Metadata Browser, Map Maintenance, and Hierarchy Maintenance.

6.1.2 Prerequisites

Following are the prerequisites for creating a Hierarchy with Multi Language Support Descriptions:

- The Hierarchy under creation should be either Regular Business Intelligence Enabled (BI) or Parent Child (PC).
- The Multi Language Support table MLS should be created either through Data Model Upload or manually in atomic schema. For more information on MLS table and structure, refer to Multi Language Support (MLS) Table.
- The Description columns used for node generation should be of **Varchar** / **Varchar2** data type.

6.1.3 Multi Language Support (MLS) Table

The MLS table which is meant to provide multi language support can have any name as per Oracle database nomenclature and details of this table need to be configured for further usage. More details about the configuration are explained below:

> **NOTE** The insertion of data into MLS tables should be performed manually.

6.1.3.1 MLS Table Structure

Following points must be taken care during MLS table creation:

- Description columns on which the Hierarchy definition is based should also be present in the MLS table.
- A column of data type **Varchar** / **Varchar2** should be present in the MLS table. This column should contain the information about the locale (such as **fr_FR**, **ko_KR**). Refer to the MLS Table Configuration section for more details.
- Going forward Dimension related information will be maintained in OFSAAI tables. Before proceeding with the configuration of Dimension and its MLS table, the following master tables need to have data.
  - CSSMS_SEGMENT_MAST

    This table holds information about the segments present in OFSAAI and an entry needs to be present in this table for mapping a dimension to a segment/ folder. The Dimension data to be seeded into AAI tables can be mapped to the folder/segment 'DEFAULT'. So the entry for 'DEFAULT' folder needs to be included in this table.
  - AAI_OBJ_TYPE_B

    This table holds information about various object types supported in OFSAAI such as Dataset, Business Measure, and so on. For Dimension management, the object type will be DIMENSION.
  - AAI_OBJ_TYPE_TL

    This table holds locale specific information about various object types present in OFSAAI. Locale specific information about the object type 'DIMESNION' needs to be added here.
  - AAI_OBJ_SUBTYPE_B

    This table holds information about different objects' sub types supported in OFSAAI. The different sub types associated with a 'DIMENSION' object will be mentioned in this table.
  - AAI_OBJ_SUBTYPE_TL

    This tables hold locale specific information about various object sub types present in OFSAAI and information on the subtypes of 'DIMESNION' are maintained in this table.

> **NOTE** Refer to the HNL_Data for more information on the sample data. The data provided in each of these tables is not exhaustive and has been provided as per requirements of Hierarchy Node Localization only.

6.1.3.2 MLS Table Configuration

Consider a Hierarchy "**Income"** defined on a dimension table "DIM_INCOME". The table structure is as indicated in the following table:

Table 11:Column Name, Primary Key, and Datatype information for MLS Table Configuration

Column Name	Primary Key	Datatype
N_CUST_INCOME_BAND_CODE	PK	Number(5,0)
FIC_MIS_DATE		Date
V_CUST_INCOME_SHORT_DESC		Varchar2(80)
V_INCOME_DESC		Varchar2(80)
N_D_INCOME_UPPER_VALUE		Number(22,3)
N_D_INCOME_LOWER_VALUE		Number(22,3)

The primary key of `DIM_INCOME` table is `PK_DIM_INCOME` and is enforced on the column `N_CUST_INCOME_BAND_CODE`.

An MLS table with name, say "`DIM_INCOME_LANG`" can be created in the atomic schema to provide MLS support for `DIM_INCOME`. The structure of this table can be as indicated in the following table:

Table 12: Column Name, Primary Key, and Datatype information for MLS Table Configuration

Column Name	Primary Key	Datatype
N_INCOME_BAND_CODE	PK	Number(5,0)
LOCALE_CD		Varchar2(10)
V_CUST_INCOME_SHORT_DESC		Varchar2(80)

The MLS table corresponding to the Dimension DIM_INCOME can be created as follows:

- Create a table to provide MLS support for the Dimension DIM_INCOME. For example, assume the name of the table is `DIM_INCOME_LANG`. This table which is to provide MLS related information for DIM_INCOME ,needs to be configured:
  - AAI_OBJECT_B

    This table registers information about an AAI object. Since Dimension is considered as an AAI object, the data corresponding to the Dimension DIM_INCOME needs to be maintained in this table.
  - AAI_OBJECT_TL

    This table holds locale specific information about an object in AAI. So locale specific information pertaining to the Dimension, DIM_INCOME, needs to be maintained in this table.
  - AAI_DIMENSION

This table will provide further information about the DIMENSION table. Information such as whether the data in dimension table is in PC structure, whether the members are acquired in the dimension, and so on are maintained in this table.

- AAI_DIM_META_TABLE

  This is the metadata table for a DIMESNION. Information about the table such as the MLS table meant for the Dimension, the hierarchy table, the attribute table, and so on will be maintained in this table.

- AAI_DIM_META_COLUMN

  This table provides information about various columns that will be used for a Dimension table. From Hierarchy Node Localization perspective, the name of the locale column which will hold locale information needs to be maintained here.

- AAI_DIM_META_JOIN

  This table holds information about the columns that will be used for joining the Dimension table with other tables such as the MLS table, Hierarchy table, Attribute table, and so on. Here multiple join conditions can be specified as well. Refer to HNL_Data excel for further information on providing joining columns information with respect to Hierarchy Node Localization.

The following table displays sample data which can be populated in `DIM_INCOME_MLS` table in a setup where there are 2 locales installed say, English (en_US) and Chinese (zh_CN).

Table 13: Sample data that is populated in the MLS Table

N_CUST_BAND_CODE	V_INCOME_DESC	LOCALE_CD
1	AAA	en_US
2	BBB	en_US
1	CCC	zh_CN
2	DDD	zh_CN

Note the following:

- In Regular BI enabled and PC Hierarchies, the Level Description expression **should not** contain columns with Number or Date data types. The inclusion of such a column in the Level Description expression would prevent the Business Hierarchy from generating nodes.
- There is no concept of **default** locale. Whenever a Hierarchy is saved, the translated node descriptions present in MLS table are saved in the corresponding columns of the `REV_LOCALE_HIER` table depending on the availability of translated values in the MLS table.
- The inclusion or exclusion of nodes from a Hierarchy will be reflected in Forms once the Hierarchy is resaved.

6.1.4 Node Generation Process

During Hierarchy definition, the nodes get generated depending on the structure of the Hierarchy. Node generation is possible in the following two scenarios:

- Node Generation when <DIM>_MLS Table is Present & Configured

- Node Generation when <DIM>_MLS Table is Not Present or Not Configured

6.1.4.1 Node Generation when MLS Table is Present and Configured

When MLS table is present, the nodes are generated by fetching the Description from the MLS table. Thus, entry in the Description columns of MLS table is mandatory.

6.1.4.2 Node Generation when MLS Table is Not Present or Not Configured

When MLS table is not present, by default the nodes are generated by fetching the Description from the Dimension table.

6.1.5 Configure Mapper for Multiple Locales

This step is optional and is required if Node Generation Process explained in the previous section is done.

To configure mapper for multiple locales:

1. Duplicate the data in `REVELEUS_MASTER` table with different locales in `LOCALE_ID` column.
2. Translate `V_OBJECT_DESC` column in `REVELEUS_MASTER` table to the desired locale.
3. Duplicate data in `LOCALE_ID` column in `REV_MAST_MAP_ITEMS` table for different `LOCALE_ID`.

Example:

An existing mapper namely **Mapper A** (created in any locale) can be translated into other locales as indicated in the following example:

1. Login to the configuration schema and duplicate the data in `REVELEUS_MASTER` table by changing the locale in `LOCALE_ID` column.
2. Change `V_OBJECT_DESC` for the corresponding locale in `REVELEUS_MASTER` table.
3. Duplicate the data in `REV_MAST_MAP_ITEMS` table by changing locale in `LOCALE_ID` column.

> **NOTE** 2nd and 3rd steps need to be performed for all the locales to which you wish to translate mapper A.

6.1.6 Update Nodes in Existing Regular BI and PC Hierarchies

Currently, the node description is generated only for one locale on which the Hierarchy is saved. With the introduction of Hierarchy Node Internationalization, the nodes will be generated in all the installed locales.

To generate the localized node descriptions for the existing Hierarchies, you need to edit and re-save the Hierarchies post MLS table creation and configuration. You can also mass update the existing Hierarchies from **Administration** > **Save Metadata** section. The node description data for all the installed locales will be populated in `REV_LOCALE_HIER` table.

> **NOTE** If an SCD (Slowly Changing Dimension) is configured on a Dimension table, synchronize the new entries with the corresponding MLS table also.

6.1.7 Limitations

If the Hierarchies are accessed via Modeling Framework module, the node descriptions of the same will be displayed only in English, despite the locale you have logged in to the application.

6.2 Data Element Filters Classification

This section explains the option to categorize "Filter classification Types" as **Classified, UnClassified**, or **All** which can be used to define Data Element filters on Business Metadata Management objects.

To classify the tables available for a Filter in an existing information domain, perform a Model upload (Incremental / Sliced / Complete) to trigger object registration, which in turn will populate all the necessary entries to the registration tables. This is an optional one-time activity required to register all the tables, so that the tables without classification code are also made available in the Data Element filters.

During Model upload, Object Registration is done for all Tables and columns.

- Tables with the classification code will continue to have entry in `REV_TABLE_CLASS_ ASSIGNMENT` with the appropriate classification code.
- Tables without classification code will also have entry in `REV_TABLE_CLASS_ ASSIGNMENT` with the value as 1000 (UnClassified).

Once tables are registered successfully, you can go to the *Filter* window to Define Data Element Filters on any tables and columns. Based on the Classification, the appropriate Classification type option has to be selected in the *Data Element Selection* window to list the tables.

Note the following:

- If the field value in `CLASSIFICATION_FLG` column of `REV_TABLE_CLASSIFICATION_B` table is set to '**1**', then it is considered as a **Classified** table.

  By Default, the classification codes 20, 200, 210, 310, 370, 50, 300, and 500 will have the `CLASSIFICATION_FLG` set to "**1**".
- The `REV_TABLE_CLASSIFICATION_TL` table will have an entry `TABLE_CLASSIFICATION_CD` = "**1000**", `TABLE_DESCRIPTION` = "**UnClassified**" to identify UnClassified Tables (that is, tables which are not classified in the ERwin through UDP).
- The category "**All**" option will select all the tables available in the infodom, irrespective of whether table is classified or not.

  Since the previous option doesn't check the classification type, even the table which has `CLASSIFICATION_FLG` = **Blank**, in the `REV_TABLE_CLASSIFICATION_B` table will also be listed. These tables will not be displayed under Classified or Unclassified Category.

6.2.1 Limitations

Following are the limitations with Data Element Filters classification:

- While defining Data Element Filter/Group Filter, it is not recommended to use features like using an Expression in a Filter and Macro Columns, since the generated SQL query for these features is unresolved.
- Defining Hierarchy/Attribute Filter is not recommended using BMM objects since the underlying Dimension and Hierarchy data are more specific to EPM Apps, and data will be available only if EPM Apps are installed in same Information Domain.
- Dependency check is not available when any of the BMM objects uses Filters. To maintain dependency between parent and child objects, an appropriate entry has to be added into the `REV_OBJECT_DEPENDENCIES` table. Since the BMM object definition details are stored in Config schema, and do not populate entry into the `FSI_M_OBJECT_DEPENDENCY_B/TL` tables, the dependency check will not happen especially while deleting a Filter.

6.3 Configuring Essbase Connectivity Check

Essbase connectivity check is required to verify if the client is successfully connecting to the server. Server connectivity is required for creating and maintaining Essbase Cube details in OFSAA.

> **NOTE** Essbase Cube is available to users in the path `OFSAA Applications > Common Tasks > Unified Analytical Metadata > Analytics Metadata`.

6.3.1 Settings in .profile File

Perform the following settings in the `.profile` file:

1. Open `.profile` file from $HOME directory of primary OFSAA server.
2. Set `ARBORPATH` to `EPMSystem11R1/common/EssbaseRTC-64/11.1.2.0` path.
3. Set `ESSBASEPATH` to `EPMSystem11R1/common/EssbaseRTC-64/11.1.2.0` path.
4. Set `export ESSLANG=English_UnitedStates.Latin1@Binary`.
5. Save and close the file.

6.3.2 Checking the Connection

Perform the following procedure on the command prompt to check the connection:

1. Login to the OFSAA Server.
2. Navigate to `$HYPERION_HOME/products/Essbase/EssbaseServer/bin` directory.
3. Execute command `./ESSCMD`.
4. Enter `:::[0]-> login`.

5. Enter the following details for the Login:
   a. Host Node ><ESSBASE_SERVER_HOST_NAME>
   b. User ><ADMINISTRATOR_USER_NAME>
   c. Password ><PASSWORD>

7 Enterprise Modeling Framework Configurations

This chapter details about the configurations which are required only if OFS Enterprise Modeling is licensed and enabled in the OFSAA instance on which this release is being installed. This chapter includes the following sections:

7.1 Configuration of Oracle R distribution and Oracle R enterprise (ORE)

You can refer the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide for information on configuration of Oracle R distribution and Oracle R Enterprise.

7.2 Configurations for OFSAAI Remote Invocation of Scripted Models Using Standard R Distributions

OFSAAI Remote invocation of "R" distribution (Open-R, Revo-R & others) is an enhancement to the framework which enables execution of "R" scripted Models to be executed on a remote "R" server instance (node). By configuring the OFSAAI with a run time parameter, models can be executed on any node. You can distribute the models for execution on multiple nodes. The settings are applicable for the entire OFSAA installation.

> **NOTE** The reference implementation provided by Oracle is for Open-R distribution. Any other distribution would require custom plug-in based well-published interface-spec to interchange data/parameters and output handling.

7.2.1 Prerequisite

1. Install the following packages along with R (R version 3.0.1):
   - rJava - version 0.9-8

- RJDBC- version 0.2-5
- DBI- version 0.4-1
- Cairo- version 1.5-9

  The packages are available to download from https://cran.r-project.org/.
- Rserve – version 1.8-x (download link - http://rforge.net/Rserve/files/)

2. To execute R scripted models, ensure that the Rserve related jar files such as `REngine.jar` and `RserveEngine.jar` are copied into the `$FICDB_HOME/lib` folder.
3. Install the OFSAAIRunnerOpenR R Package in the remote box where Rserve is running. For more information, see Installing OFSAAIRunnerOpenR R Package.

7.2.1.1 Installing OFSAAIRunnerOpenR R Package

OFSAAIRunnerOpenR is a mandatory R package required to execute models in the Open-R Framework. This package (`OFSAAIRunnerOpenR_1.0.0.tar.gz`) is available in the `$FIC_DB_HOME/lib` directory. Install this package on a machine which runs **Rserve** or **client R Engine**.

Perform the following instructions to install OFSAAIRunnerOpenR R Package:

1. Login to the OFSAA Server.
2. Navigate to the `$FIC_DB_HOME/lib` directory.
3. Copy the file `OFSAAIRunnerOpenR_1.0.0.tar.gz` in default mode to Rserve box (node where Rserve is installed/running).

> **NOTE** The preceding action requires UNIX root login.

4. Navigate to the directory where the file `OFSAAIRunnerOpenR_1.0.0.tar.gz` is copied.
5. Install the package by executing the command as a root user:

```
R CMD INSTALL OFSAAIRunnerOpenR_1.0.0.tar.gz
```

> **NOTE** The OFSAAIRunnerOpenR package is installed in the `/usr/lib64/R/library` directory.

6. Navigate to the directory `$R_HOME/library` and check whether the OFSAAIRunneOpenR package is listed in the directory by executing the command as root user:

```
ls -l
```

7.2.2 Configurations

Following configurations are required for Rserve in remote nodes where Open-R engine is installed:

1. Create **Rserv.conf** file in `/etc` and make following entries:

```
workdir /tmp/Rserv
pwdfile /etc/Rserveusers
remote enable
auth enable
plaintext enable
port 6311
maxsendbuf 0
interactive no
```

For more details, refer the link: http://rforge.net/Rserve/doc.html.

> **NOTE** The user who starts the R Server should have the read-write permissions for the working directory.

2. Set the Environment variables for R:

```
JAVA_HOME={java home path}
JAVA_BIN={java bin path}
LD_LIBRARY_PATH={LD library path}
```

Note the following:

- If RJDBC connection is required, copy the `ojdbc<version>.jar` file to the lib directory in the remote file path configured. The version of `ojdbc<version>.jar` file is based on the Java version.
- The `lib` and `conf` folders have to be created under the path mentioned in `<REMOTE_FILE_PATH>` tag.
- For the Kerberos authentication the required `jaas-conf, krb-conf` and `keytab` files have to be placed under `conf` folder. The `jaas-conf` file name should be same as that of the `keytab` file name. It should be placed under the `conf` folder in the read-write path in remote machine or in the `$FIC_DB_HOME/conf` folder in case of local executions. The `krb5 conf` file name should be same as the name configured in the table.
- Hive and Hadoop related jars should be copied to the `lib` folder mentioned in the `<REMOTE_FILE_PATH>` tag.

7.2.3 Structure of the gss-jass.conf File

- If sun JDK for Linux is used:

```
com.sun.security.jgss.initiate {
  com.sun.security.auth.module.Krb5LoginModule required
  useKeyTab=true
  useTicketCache=false
```

```
   doNotPrompt=true
   keyTab="<KeyTab File Path>"
   debug=true;
};
```

- If IBM JDK for Linux is used:

```
com.ibm.security.jgss.initiate {
   com.ibm.security.auth.module.Krb5LoginModule required
credsType=both
useKeytab="<KeyTab File Path>"
   debug=true;
};
```

7.3 Configurations for Open-R with HDFS

Oracle R Advanced Analytics for Hadoop (ORAAH)/Oracle R Connector for Hadoop (ORCH) is the default approach for running Open-R on HDFS.

7.3.1 Prerequisites

The installation requirements for external dependencies are in the following list:

- Apache Big Data
- ORAAH – Versions supported: 2.6.0 and 2.7.0.
  Download it from http://www.oracle.com/technetwork/database/database-technologies/bdc/r-advanalytics-for-hadoop/downloads/index.html

  For more information on installation and configuration of ORAAH, see ORAAH Installation Guide.
- Cairo- The package is available to download from https://cran.r-project.org/. Download and transfer it to Rserve box. Install the package using the following command:

  ```
  R CMD INSTALL Cairo_Package_Name
  ```

  Or

  ```
  install.packages( "Cairo", dependencies = T)  #using R session
  ```

The installation requirements for internal dependencies are in the following list:

- OFSAAIRunnerHDFS_1.0.0.tar.gz
- OFSAAIRunnerOpenR_1.0.0.tar.gz

> **NOTE** The packages in the preceding list are mandatory for executions to work. For more information, see section Installing OFSAAIRunnerOpenR R Package.

7.3.2 Installing OFSAAIRunnerHDFS Package

OFSAAIRunnerHDFS is an R package required for executing models in Open-R Framework with HDFS Option. This package (`OFSAAIRunnerHDFS_1.0.0.tar.gz`) is available under `$FIC_DB_HOME/lib`. This package needs to be installed on a machine which is running Rserve or client R Engine.

Refer to the following instructions to install OFSAAIRunner package:

1. Login to the OFSAA Server. Navigate to the folder `$FIC_DB_HOME/lib`.
2. Copy the file `OFSAAIRunnerHDFS_1.0.0.tar.gz` in in default mode to Rserve box (node where Rserve is installed/running).

> **NOTE** UNIX root login is required.

3. Navigate to the directory where the file `OFSAAIRunnerHDFS_1.0.0.tar.gz` is copied.
4. Install the package by executing the command as root user:

```
R CMD INSTALL OFSAAIRunnerHDFS_1.0.0.tar.gz
```

> **NOTE** The OFSAAIRunnerHDFS package is installed in /usr/lib64/R/library.

5. Navigate to the directory `$R_HOME/library` and check whether OFSAAIRunnerHDFS package is listed there by executing the command as root user:

```
ls -l
```

7.3.3 Additional Configurations for ORAAH Executions

The following configurations are mandatory for model executions using ORAAH.

Set the following environment variables in `$R_HOME/etc/Renviron.site` file:

- `HIVE_HOME, SPARK_HOME, HADOOP_HOME` with the respective paths
- `HIVE_CONF_DIR, HADOOP_CONF_DIR, YARN_CONF_DIR, SPARK_CONF_DIR` with their respective configuration directory paths
- `CLASSPATH` and `HADOOP_CLASSPATH` with all the hadoop/hdfs/yarn/hive jars, Hadoop configuration directory (HADOOP_CONF_DIR) and spark configuration directory (SPARK_CONF_DIR)
  For example,

  ```
  CLASSPATH=$HADOOP_CONF_DIR:$SPARK_CONF_DIR:All_hadoop_jars
  ```

- `SPARK_JAVA_OPTS` variable with `$R_HOME/lib`

  For example, `SPARK_JAVA_OPTS="-Djava.library.path=/usr/lib64/R/lib"`

- For **Kerberos** enabled cluster, initializing the ticket should be done in `Renviron/Renviron.site` file.

7.4 Support for Scripts which work on HDFS Files Directly

The framework supports scripts which work directly on the HDFS files. In the technique registration UI and model definition UI there will be a provision to specify what is the input data type – data-frame or HDFS file.

The default pre-script and post-script which comes with the patch set will work only with data frame approach. For the script to work on HDFS files, custom pre and post scripts have to be written and configured in the `ModelingFramework.xml`. Also, the HDFS location has to be configured in the XML.

The HDFS location should have complete access and the necessary packages should have been installed in the server.

7.5 User Configurable Execution Implementation

If you want your own implementation to execute the scripts, you can configure the `<CLASS_NAME>` tag in the `ModelingFramework.xml` with the java class name to be instantiated. Also, the jar file containing this class file should be placed in `$FIC_DB_HOME/lib` folder.

7.6 Configuration for Parallel Execution of Models

If Rserve version is 1.8.x and above, the control feature should not be enabled for parallel execution of models. You should remove the tag `control enable/disable` entry from the `Rserv.conf` file in the `/etc` folder.

7.7 Configurations for ORE Execution

This is an optional step and required only if you have installed and configured Oracle R distribution and Oracle R Enterprise:

1. Login to the Oracle Database Server.
2. Add an entry in `tnsnames.ora` file with same name as that of the value set for `ORACLE_SID`.

> **NOTE** For a RAC database, follow the aforementioned configuration in all nodes of the RAC cluster.

7.8 Variable Migration Utility

The Variable Migration utility is provided to migrate the variables defined in OFSAAI 8.0.5.0.0 and previous versions to the Variables Definition compatible with OFSAAI 8.0.6.0.0 and later. The utility `variableresaveutil.sh` is available in the `$FIC_HOME/utility/variable/bin/` folder.

The following are the steps to run the migration utility:

1. Navigate to `$FIC_HOME/utility/variable/bin` directory.
2. Execute `variableresaveutil.sh` (UNIX).

```
./variableresaveutil.sh
```

This command will migrate all available variables from all Infodoms, which are in the `ftpshare/<infodom>/erwin/variable/` directory.

3. Provide the following parameter if you want to migrate variables that are present in a particular information domain:
   - INFODOM- Specify the information domain name if you want to migrate variables present only in a particular information domain.

     ```
     ./variableresaveutil.sh <INFODOM >
     ```

4. Check the status, and errors if any, in the `migration.log` file available in the `$FIC_HOME/utility/variable/logs/` folder.

> **NOTE** After you have triggered this utility and migrated all variables successfully, any subsequent run of the utility will throw SQL constraint violation errors for Variables that have been migrated. You can ignore this error if you do not want to change any details in migrated variables. If you want to update or correct an existing variable, then delete the migrated variable from UI and retrigger the utility.

7.9 Model Execution Venue Migration Utility

The Model Execution Venue Migration utility helps to migrate the `ModelingFramework.xml` entries configured in previous versions to the table definition compatible with OFSAAI 8.0.6.0.0 and later. This utility `ExecutionConfig.sh` is available in the `$FIC_HOME/utility/ modelutil/bin/` folder. This utility gets executed as part of OFS AAAI Application Pack 8.0.6.0.0 patch installation. If you encounter any errors, you should run the utility again.

Following are the steps to run the utility:

1. Navigate to `$FIC_HOME/utility/modelutil/bin` directory.
2. Execute `ExecutionConfig.sh` (UNIX).

   ```
   ./ExecutionConfig.sh
   ```

   This command migrates all available ModelingFramework.xml target entries to table.

   Check the status, and errors if any, in the `MF_xml_migration.log` file available in the `$FIC_HOME/utility/modelutil/log folder`.

7.10 Data Redaction Grants to Sandbox Schema

The configuration discussed in this section is required if you have selected Data Redaction while installing OFSAA. Data Redaction is an Advanced Security option (see Data Redaction for more details). You have to give grants related to Data Redaction to the Sandbox schema for model execution to execute.

Perform the following procedure to give grants for Data Redaction to the Sandbox schema:

1. Login with System Database Administrator (SYSDBA) rights to the database where the Sandbox schema is created.
2. Give the following Grants:

```
grant execute on DBMS_REDACT to &atomicUser
/
Create role OFS_SEC_DATA
/
grant OFS_SEC_DATA to &atomicUser
/
create role OFS_NOSEC_DATA
/
grant EXEMPT REDACTION POLICY to OFS_NOSEC_DATA
/
grant OFS_NOSEC_DATA to &atomicUser
/
alter user &atomicUser default role none
/
```

8 Process Modeling Framework Configurations

This chapter details about the configurations required for Process Modeling Framework module.

Topics:

8.1 SMTP Server Configurations

Task notifications can be sent as Email to the assigned users. To receive notifications as email, perform the following configurations:

1. Add the following entries in `AAI_EMAIL_CONFIG` table:

   `V_PROTOCOL` - SMTP

   `V_HOST` –SMTP/ Mail Server ID

   `V_PORT` - SMTP Server Port

   `V_AUTHENTICATION` - Either False or True

   `V_USER_NAME` - Login name to SMTP/ Mail Server ID from which mail will be triggered. This is required if `V_AUTHENTICATION` is set as True.

   `V_PASSWORD` - Password to login into SMTP/ Mail Server. This is required if `V_AUTHENTICATION` is set as True.

   `V_SECURITY` -

2. Add the following entries in the `AAI_USER_PREFERENCE` table:

   In this table, you can set the user preference of how to receive the notification mails.

V_USER_ID	N_EMAIL_NOTIF_REQ
USER1	1
USER2	2

   - 0 – To receive no notification mails
   - 1 – To get mails instantly
   - 2 – To get bulk mail (Additionally, you need to set `V_BULK_MAIL_TRIGGER` value to Y in the `AAI_WF_BULK_MAIL_TRIGGER` table). A single mail will be sent with all the pending notifications from last trigger, as a PDF attachment. Once the bulk mail is sent, `V_BULK_MAIL_TRIGGER` value is automatically set to N.
   - 3 – To get mail with attachment

3. Add the email id of the user, to which the notification mails need to be sent, in the `CSSMS_USR_PROFILE` table.

V_USR_ID	V_EMAIL
USER1	user1@oracle.com
USER2	user2@oracle.com

4. Add the following entries in the `AAI_WF_EMAIL_TEMPLATE` table:
   - V_MAIL_FROM- Email id from which the mail is sent
   - V_MAIL_MESSAGE- Email message template
   - V_MAIL_SUBJECT- Subject of the mail
   - V_APP_PACKAGE_ID- Application package ID
   - V_MAIL_TYPE- Email type such as task or bulk task.
   - N_TEMPLATE_ID- A unique Email Template ID
   - V_TEMPLATE_NAME- Email Template name
5. Set the `V_EMAIL_REQUIRED` value to Y in `AAI_WF_APP_PACKAGE_B` (for app level setting), `AAI_WF_APP_REGISTRATION` (for entity type level setting) and `AAI_WF_ACTIVITY_TASK_B` (for task level setting) tables.

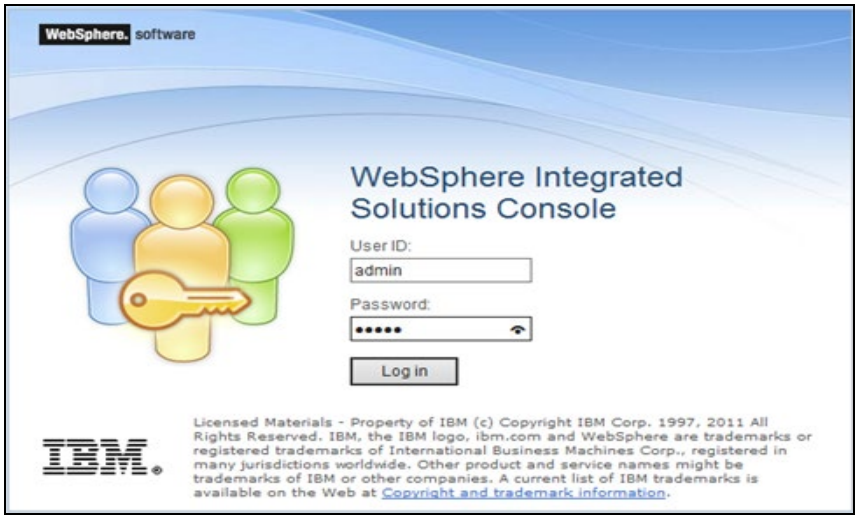
8.2 Work Manager Configurations

Process Modelling framework requires creation of Work Manager and mapping it to OFSAA instance. This configuration is required for Web Application Server type as WebSphere and WebLogic.

8.2.1 Creating Work Manager in WebSphere Application Server

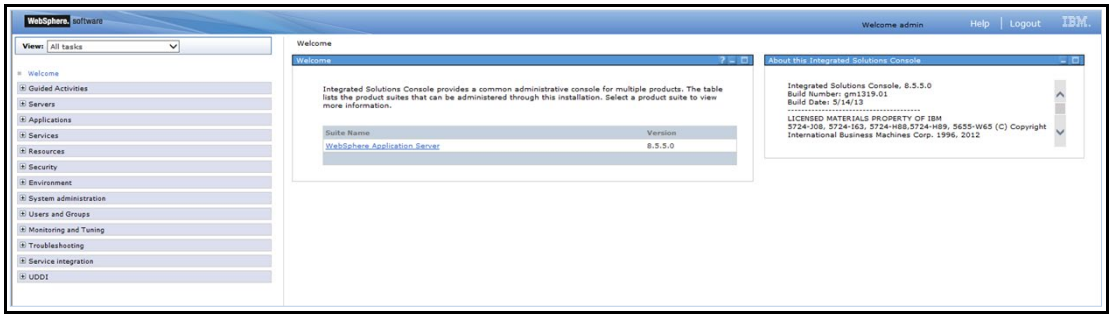
1. Open the WebSphere admin console in the browser window: http://<ipaddress>:<administrative console port>/ibm/console. (https if SSL is enabled). The *Login* window is displayed.

Figure 2: IBM WebSphere Integrated Solutions Console window



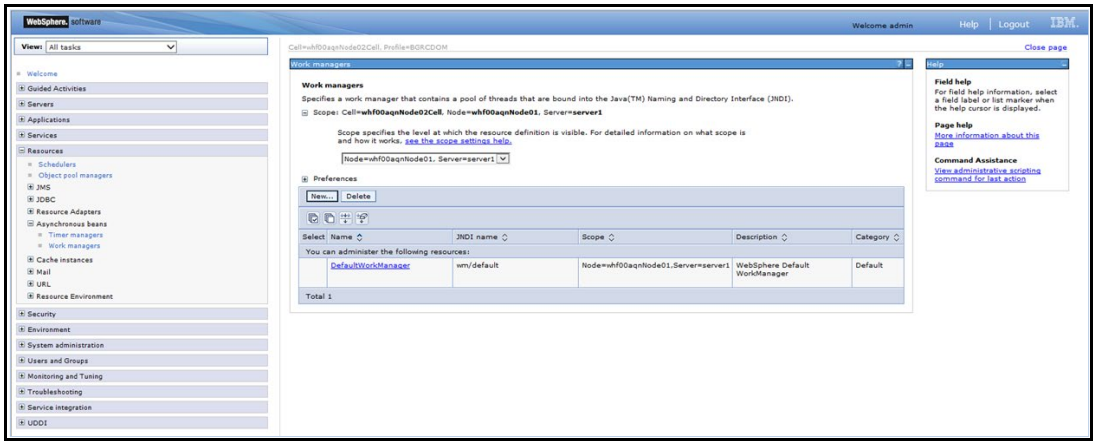
2. Login with the user id that has admin rights.

Figure 3: WebSphere Homepage



3. From the LHS menu, expand **Resources** and **Asynchronous beans** and then, select **Work Managers**.

Figure 4: WebSphere Homepage Work Managers option

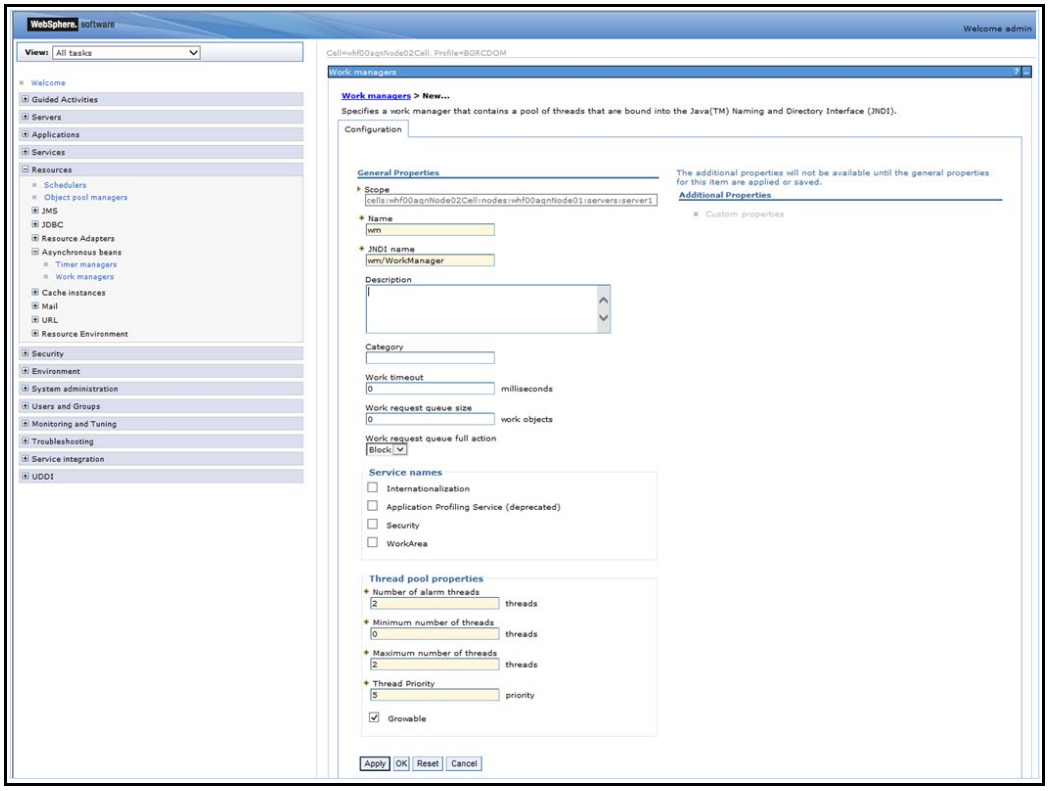


4. Select the required **Scope** from the drop-down list.

   For example, `Node=whf00aqnNode01, Server=server1.`

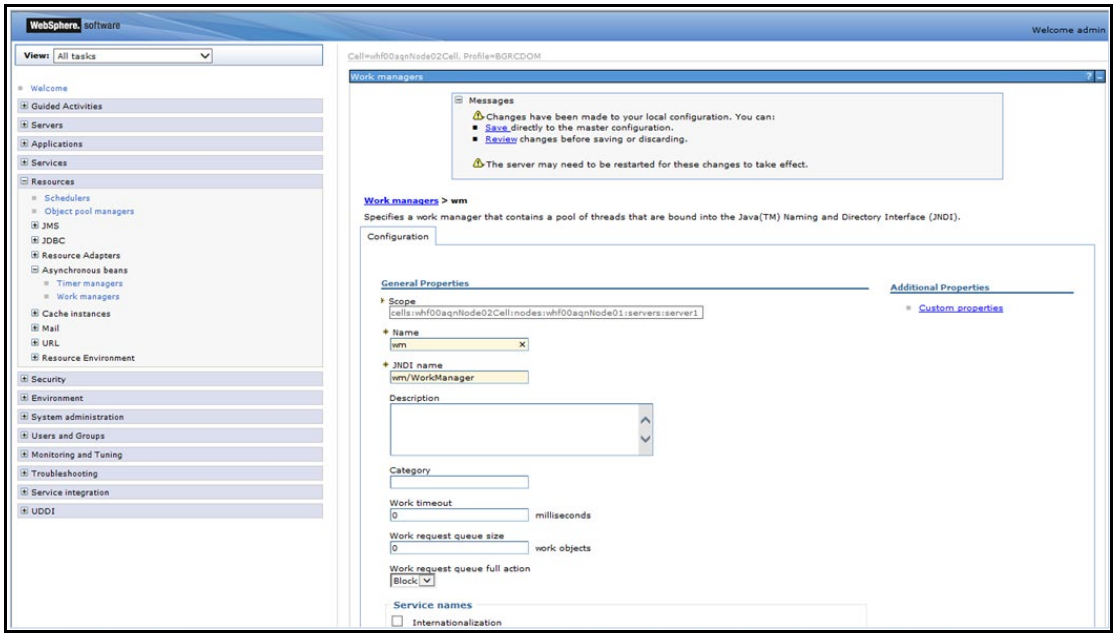
5. Click **New** in the *Preferences* section.

Figure 5: Work Managers Configuration page



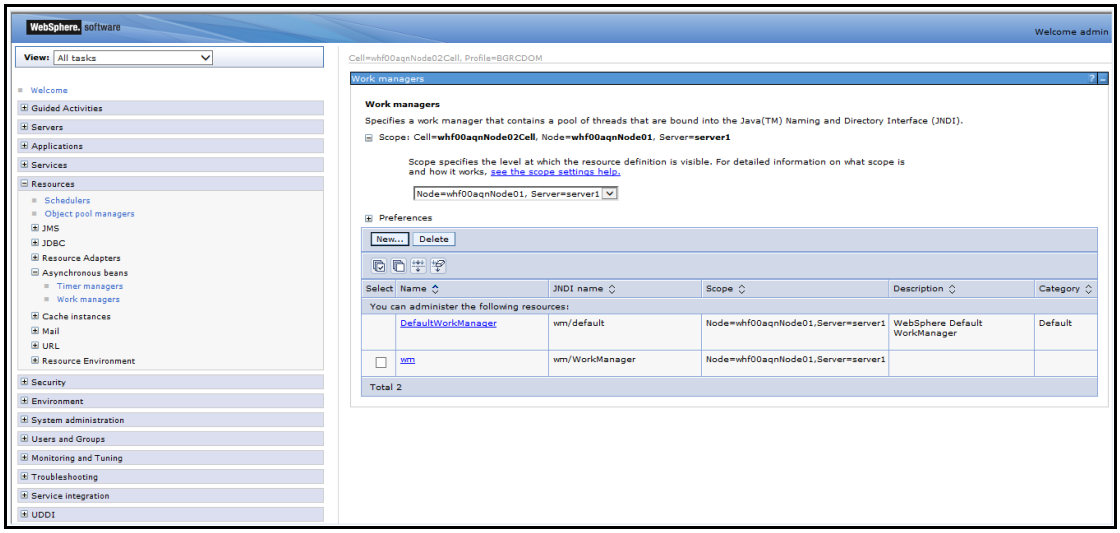
6. Enter the **Name** as 'wm' and **JNDI name** as 'wm/WorkManager ' in the respective fields.
7. Enter the **Thread pool properties**.
8. Click **Apply**.

Figure 6: Work Managers Configuration page



9. Click **Save**.

Figure 7: Work Managers Configuration page

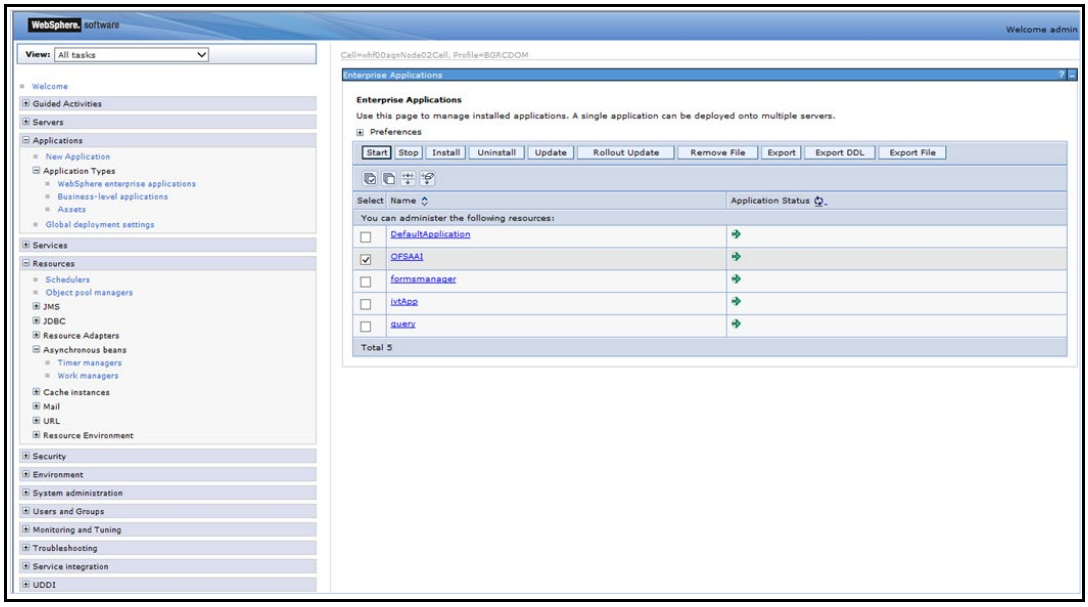


After creating work manager successfully, you have to map it to OFSAA instance.

8.2.2 Mapping Work Manager to OFSAA WebSphere Instance

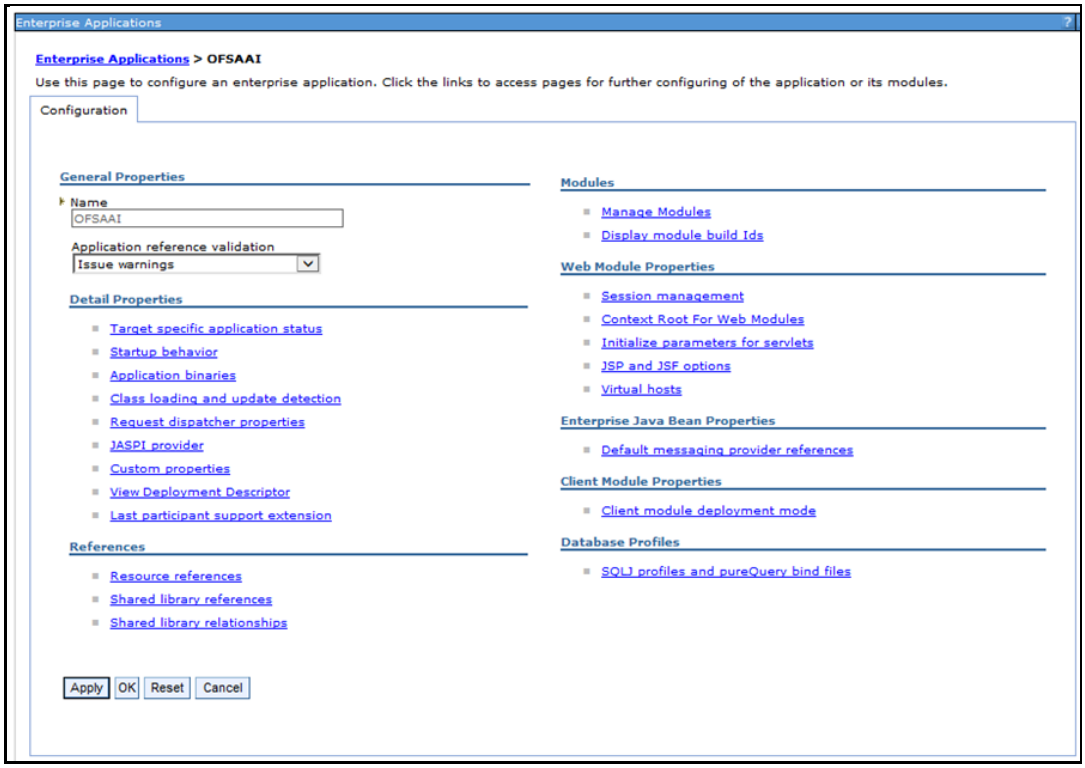
1. From the LHS menu, expand **Applications** > **Application Types** and select **WebSphere enterprise applications**.

Figure 8: Work Managers Configuration page



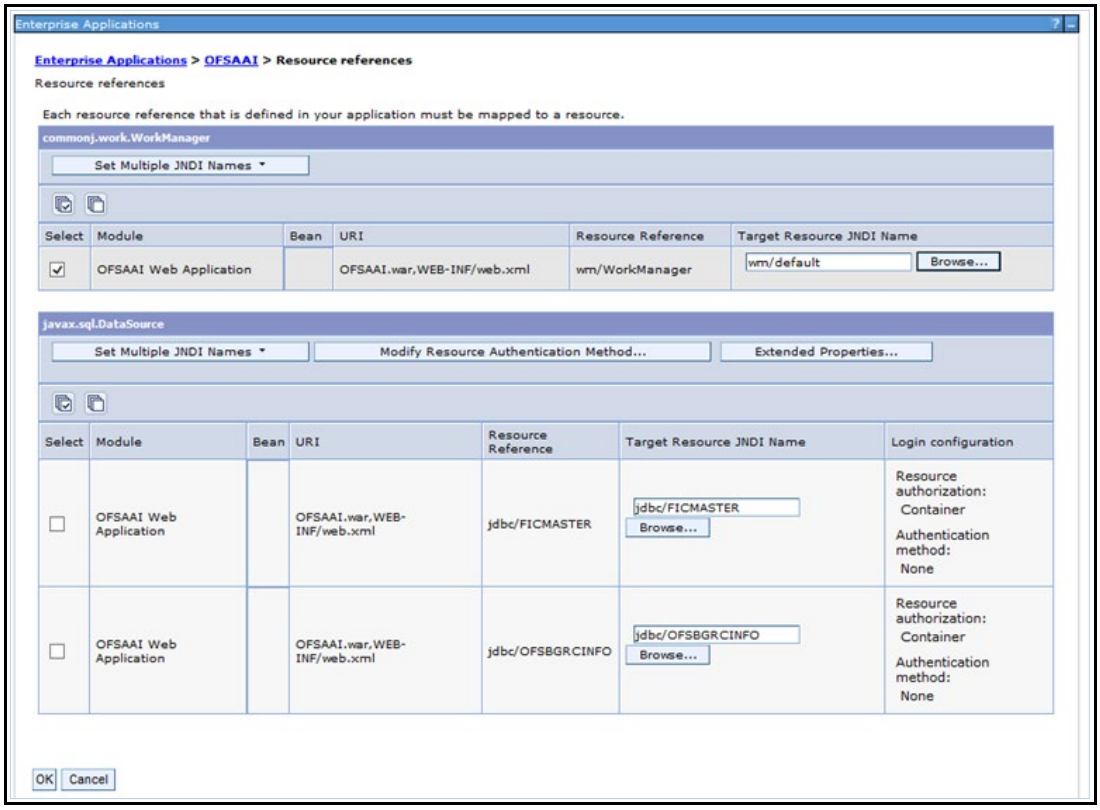
2. Click **OFSAAI instance** hyperlink.

Figure 9: Enterprise Applications page



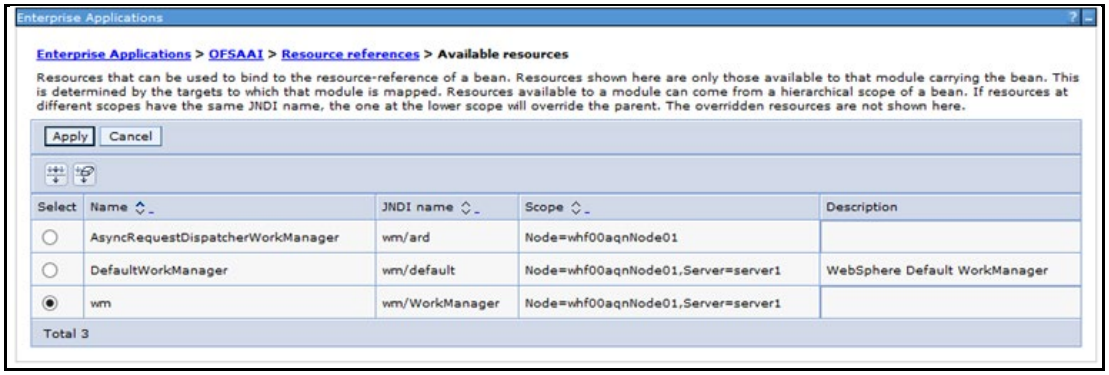
3. Click **Resource references** link under *References* section.

Figure 10: Enterprise Applications page for Resource reference configuration



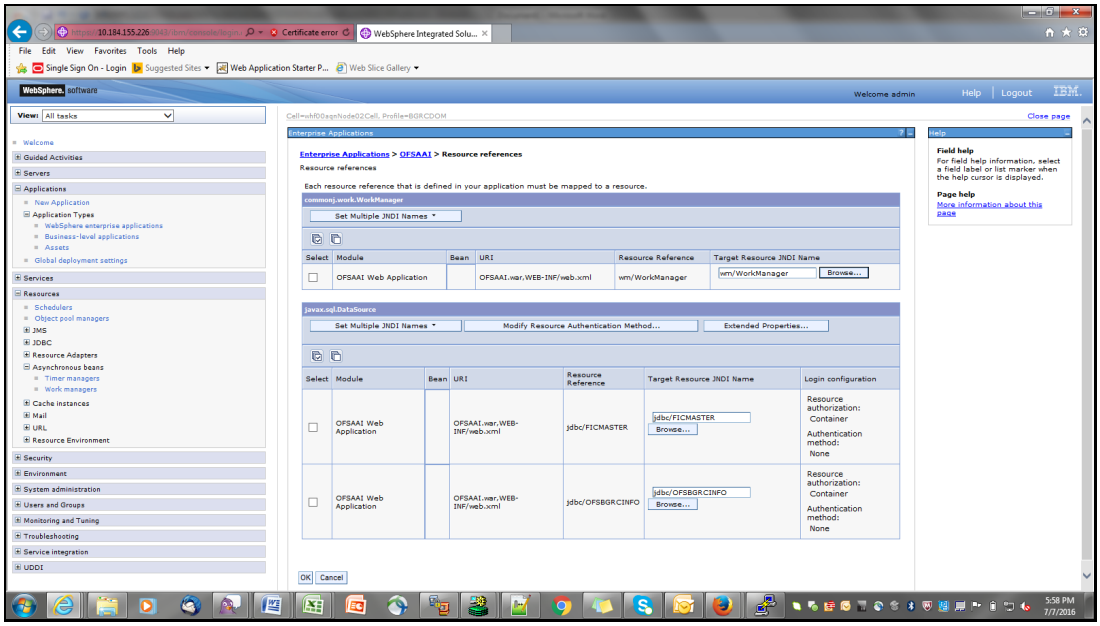
4. Click **Browse** corresponding to the Work Manager Resource Reference. The available resources are displayed.

Figure 11: Enterprise Applications page for Available reference configuration



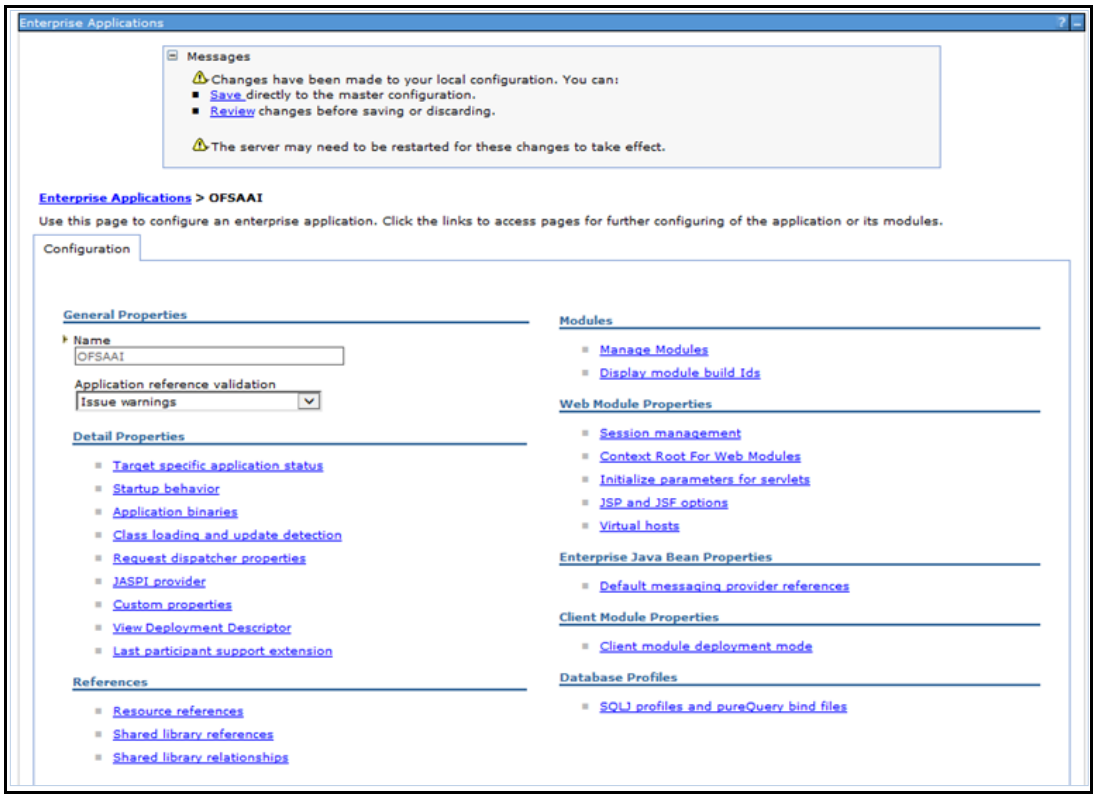
5. Select the newly created Work Manager ('wm') and click **Apply**.

Figure 12: Enterprise Applications page for Resource reference configuration



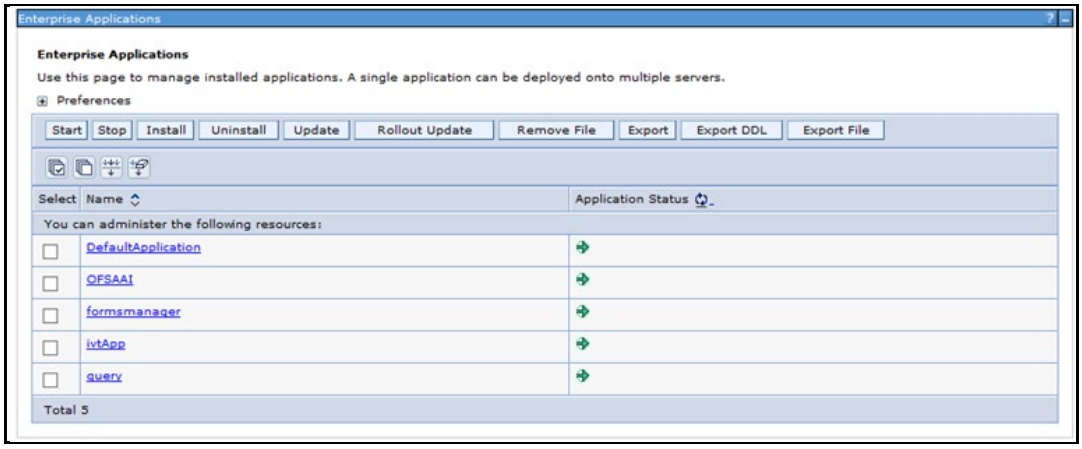
6. Select the Work Manager ('wm/WorkManager') and click **OK.**

Figure 13: : Enterprise Applications page



7. Click **Save**.

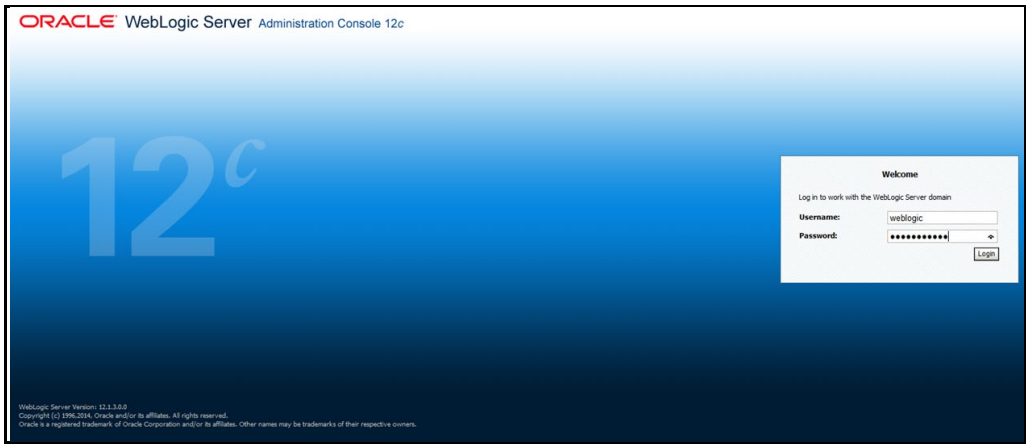
Figure 14: Preferences page



8.2.3 Creating Work Manager in WebLogic Application Server

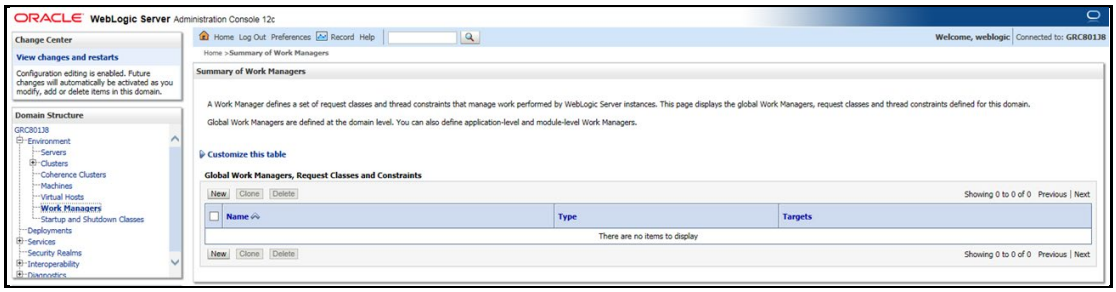
1. Open the WebLogic admin console in the browser window: `http://<ipaddress>:<administrative console port>/console`. (https if SSL is enabled). The *Welcome* window is displayed.

Figure 15: WebLogic Application Server



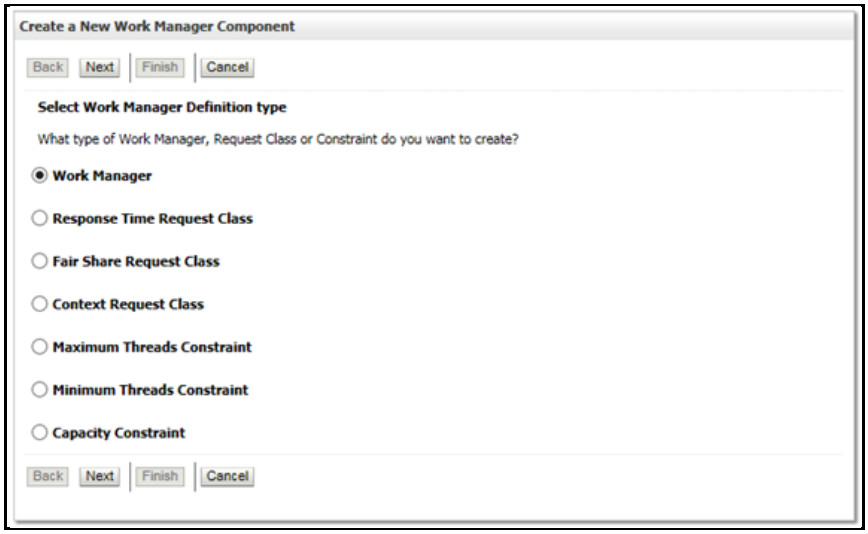
2. Login with the user id that has admin rights.
3. From the *Domain Structure* menu in the LHS, expand **Environment** and select **Work Managers**. The *Summary of Work Managers* window is displayed.

Figure 16: WebLogic Application Server Homepage



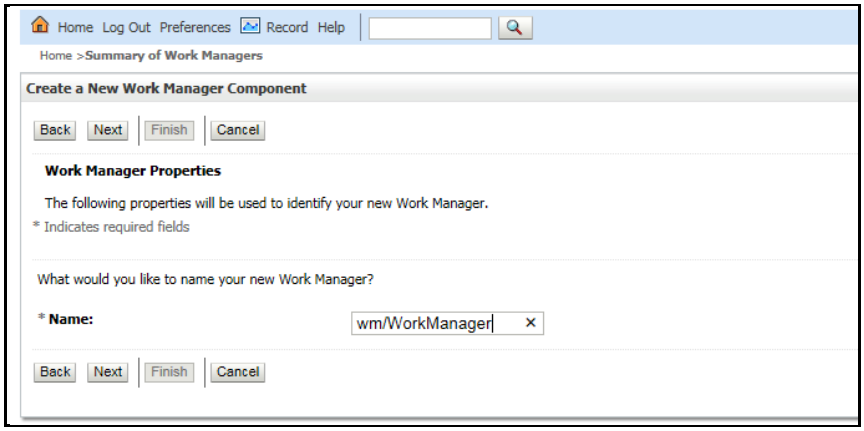
4. Click **New** to create a new work manager component.

Figure 17: New Work Manager Component window



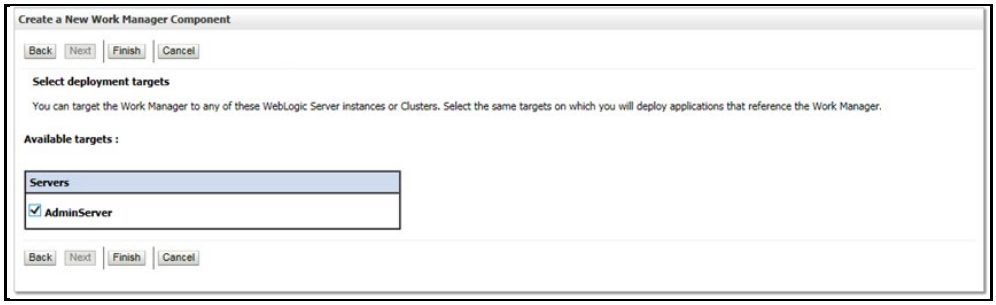
5. Select **Work Manager** and click **Next**.

Figure 18: New Work Manager Component window



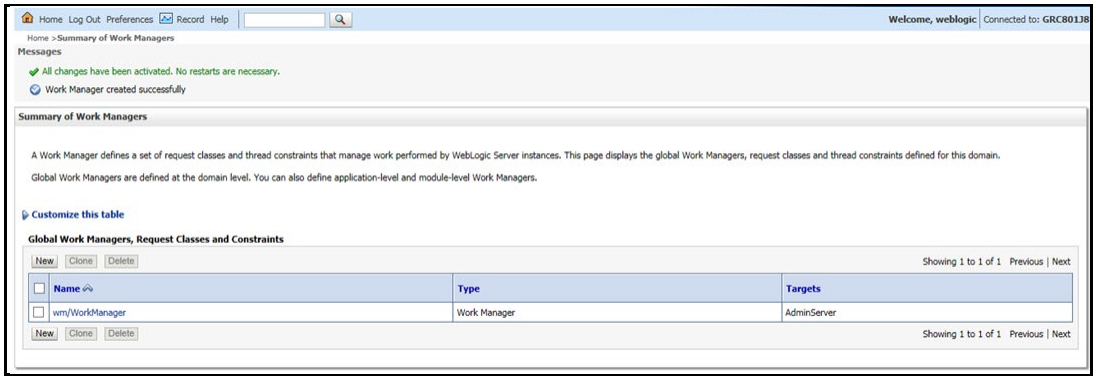
6. Enter the **Name** as 'wm/WorkManager'.
7. Click **Next**.

Figure 19: New Work Manager Component window



8. Select the required deployment target and click **Finish**.

Figure 20: New Work Manager Component window



9 Document Management Configurations

Documents are required to support transactions and you can upload or download them in OFSAA configuring the various document management properties.

Topics:

9.1 Configure Document Upload Settings

Configure the document upload settings for the location of the files, types of files, and the size of the files in the configuration table of the Config Schema.

> **NOTE** Restart the OFSAA services after updating the document upload settings.

9.1.1 Configure Document Upload Location Properties

A document upload in the OFSAA is initially stored in a temporary directory in the web local path of the web layer. After the document copying process to the temporary directory is complete, it is copied to the ftpshare location of the application layer. This is a two-stage process.

To configure the temporary and permanent directories to save the uploaded documents, set the parameters DOCUMENT_UPLOAD_TEMP and DOCUMENT_Upload_Save in the configuration table of the Config Schema as shown in the following table:

Table 14: Parameter name, value, and their description for Document Upload location properties

PARAMNAME	PARAMVALUE	DESCRIPTION
DOCUMENT_UPLOAD_TEMP	/TEMPFOL	Set the value of the temporary directory. The directory is created in the web local path of the web tier. To find the web local path, execute the following query in the CONFIG schema: `SELECT LOCALPATH FROM WEB_SERVER_INFO;`
DOCUMENT_UPLOAD_SAVE	/DocStorage	Set the value of the document storage directory. The directory is created in the FTPSHARE path of the application tier. To find the FTPSHARE path, execute the following query in the CONFIG schema: `SELECT FTPDRIVE FROM APP_SERVER_INFO;`

9.1.2 Configure Document Upload File Formats and Size

To configure the file types (formats) and the file size that you can upload, set the DOCUMENT_ALLOWED_EXTENSION and DOCUMENT_MAX_SIZE parameters in the configuration table of the Config Schema as shown in the following table:

Table 15: Parameter name, value, and their description for Document Upload file formats and size properties

PARAMNAME	PARAMVALUE	DESCRIPTION
DOCUMENT_ALLOWED_EXTENSION	• txt • pdf • doc • Doc • html • htm • xls • zip	Set the file format extension values separated by commas for the file types allowed for upload.
DOCUMENT_MAX_SIZE	10096000	Set the maximum size of the document that can be uploaded in bytes.

9.1.3 Configure Document Upload File Timeout and File Transfer

To configure the file time out and the file transfer that you can upload, set the TP_SOCKET_TIMEOUT and F_IS_ASYNC_FILETRANSFER parameters in the configuration table of the Config Schema as shown in the following table.

Table 16: Parameter name, value, and their description for Document Upload file time and file transfer

PARAMNAME	PARAMVALUE	DESCRIPTION	DEFAULT VALUE
FTP_SOCKET_TIMEOUT	10000000	Default File Transfer Socket timeout value	By default, the value is 10000000 milliseconds.
F_IS_ASYNC_FILETRANSFER	FALSE	File transfer mode Synchronous or Asynchronous	By default, the value is FALSE, which means Synchronous file upload.

9.2 Content Management Integration

Content Management Interoperability Services (CMIS) is an OASIS standard enabling information sharing between different Content Management Systems. Document management within OFSAA can integrate with CMIS services to support document upload and download to the CMIS repository.

> **NOTE** To use the features explained in this section, additional licenses may apply. For details, contact My Oracle Support.

Perform the following configurations:

1. Set the following parameters in the configuration table in the Config Schema to enable CMIS:
   a. Set the value of `IS_CMIS_ENABLED` parameter to TRUE. If this is set to FALSE, document upload will happen on ftpshare.
   b. Update the value of `CMIS_ATOMPUB_URL` parameter with the repository URL. Ensure the URL is up and running.

      For example: http://192.0.2.1:7777/service/cmis
2. Modify the property file `INFODOM_cmis.properties`, which is available inside `$FIC_HOME/ficweb/webroot/conf` folder.
   a. Rename the file by replacing the INFODOM with actual name of Infodom. For example if Infodom name is "OFSAAINFO", rename the file to `OFSAAINFO_cmis.properties`.
   b. The property file will contain the following entries. Update them as per the CMIS URL.

      `REPOSITORY_ID=`*5*

      `USER=`*admin*

      `PASSWORD=`*password*

      `DEFAULTPATH=`*/Default*

      `DOC_OBJ_TYPE_ID=`*cmis:document*

      `FLDR_OBJ_TYPE_ID=`*cmis:folder*
3. Redeploy the application onto your configured web application server. For more information on generating and deploying the EAR/ WAR file, refer to the Post Installation Configuration section in the OFS Analytical Applications Infrastructure Installation and Configuration Guide.
4. Restart all the OFSAAI services. For more information, refer to the Start/Stop Infrastructure Services section in the OFS Analytical Applications Infrastructure Installation and Configuration Guide.

9.2.1 Configurations for Document Upload to Multiple Libraries

Documents can be uploaded to multiple libraries instead of single library. This way, the number of documents within each library can be controlled within the threshold.

Enter values for the following parameters in the AAI_CMIS_REPO_MASTER table in the Config Schema as given:

- V_REPO_ID -- Unique value for identification of Library
- V_REPO_URL -- Update the value with the repository URL
- V_DEF_PATH -- Update the folder path
- D_START_DATE -- Upload start date for the library/folder
- D_END_DATE -- Upload end date for the library/folder
- V_INFODOM -- Update Infodom name

- V_CMIS_REPO_ID -- Update the value with REPOSITORY_ID (note that this value is case-sensitive)

> **NOTE** For old documents, in DOCUMENT_MASTER, only V_DOC_CMIS_ID column is updated in case of CMIS integrated uploads. After applying 80710 ML patch, V_REPO_ID column in DOCUMENT_MASTER should be updated with value as updated in AAI_CMIS_REPO_MASTER.V_REPO_ID column. This needs to be updated for all rows that are having value in V_DOC_CMIS_ID column of DOCUMENT_MASTER.

10 Questionnaire Setup and Configuration Details

This section provides details to set up Questionnaire in your system environment and map groups to roles, which lets you access the feature.

You have to launch the Questionnaire menu and map it to roles. The following subsections provide details for the procedures:

10.1 Launching Questionnaire Menu

You can configure Questionnaire to appear in any relevant menu of your choice in the application. For example, you can configure Questionnaire to appear in the PMF menu or in the Common Tasks menu.

The following menus are available for Questionnaire:

1. **OFS_ABC_QTNR_CONF** – You can access the Questionnaire Configuration screen from this menu. It is used to define components and attributes, which are used to create a Questionnaire.
2. **OFS_ABC_QTNR_DEFN** – You can access the Questionnaire Library screen from this menu.
3. **OFS_ABC_QTN_DEFN** – You can access the Questions Library screen from this menu.

Add the menus mentioned in the preceding list to the **aai_menu_tree** table to enable the Questionnaire menus to appear in the OFSAAI LHS menu.

After you have launched the menu, follow the instructions described in the section Mapping Roles to Access Questionnaire.

10.2 Mapping Roles to Access Questionnaire

Access to Questionnaire requires mapping groups to roles. The step-by-step description of the procedure is in the following list:

1. Login to OFSAA with your system administrator credentials.
2. Click  from the header to display the administration tools in a Tiles menu.
3. Click **Identity Management** to view the *Security Management* menu in a separate window.
4. Click **User Administrator** to expand the list further.
5. Click **User Group Role Map** to display the *User Group Role Map* window.
6. Map users to User or Approver roles.
    a. Users of applications mapped to groups can access the Questionnaire menu by mapping the groups to following roles:

Table 17: Mapping Roles and their Description

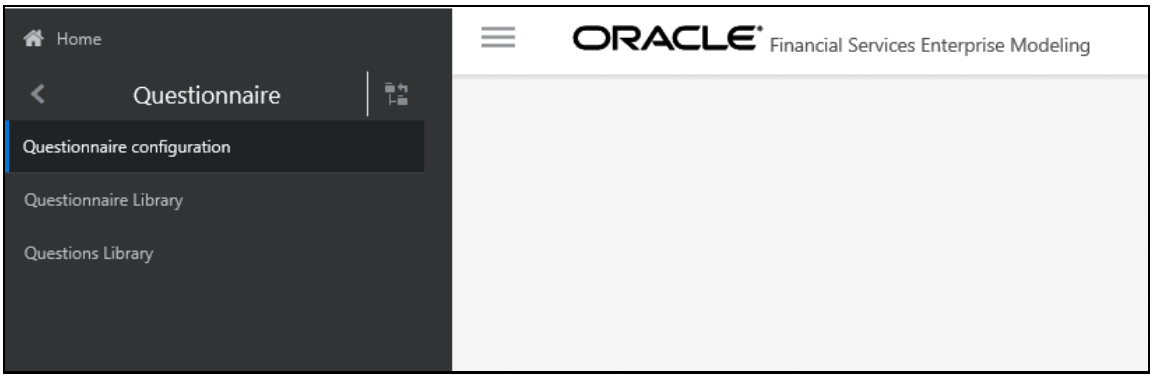
Number	Role Codes	Description
1	QTNRADMNRL	ABC Questionnaire Administrator
2	QUESTMATRL	ABC Questionnaire Maintenance
3	QTNRCONFRL	Questionnaire Configuration Execute

b. Users of applications can be configured to be approvers by mapping their group to the QLOCAUTHRL role.

7. Authorize the user groups and role mapping. (You or another user with authorizer role (*sysauth*) has to login to OFSAA and authorize the mapping).

Configured users can login with the credentials created and access Questionnaire with the roles assigned. The **Questionnaire** window is displayed as shown.

Table 18: Questionnaire configuration navigation



In the preceding illustration, the **Questionnaire** window is configured to appear in **Application Builder Component** in **Common Tasks**. Similarly, you can configure Questionnaire to appear in the menu item of your choice. For example, you can configure it to appear in the Know Your Customer (KYC) menu list.

10.3 Configuring Components, Dimensions, and Static Options

Users have to configure the data in the drop-down fields such as Components, Dimensions and Static options on the Questionnaire window. The following subsections provide configuration information for the various options.

10.3.1 Configuring Components for Questionnaire

Component is a drop-down list. Seed the data for Components in the tables DIM_COMPONENT_INFO and DIM_COMPONENT_INFO_MLS. For table details, see the spreadsheet AAI_Questionnaire_Data_Model_Sheet.xlsm.

10.3.2 Configuring Dimensions for Questionnaire

Dimensions is a drop-down list. Seed the data for Dimensions in the tables QTNR_DIM_SRC and QTNR_DIM_SRC_MLS. For table details, see the spreadsheet AAI_Questionnaire_Data_Model_Sheet.xlsm.

10.3.3 Configuring Static Options for Questionnaire

Static Options is a drop-down list. Seed the data for Static Options in the following tables and in the order specified:

1. QTNR_STATIC_GRP
2. QTNR_STATIC_GRP_MLS
3. QTNR_STATIC_SRC
4. QTNR_STATIC_SRC_MLS

For table details, see the spreadsheet AAI_Questionnaire_Data_Model_Sheet.xlsm.

10.4 Registering and Invoking your Application's Customized Workflow

You can define customized workflows in your application and apply in Questionnaire by registering it. Questionnaire has a workflow definition seeded by AAI, where object type is defined as QTNR. If you choose not to define your workflow, Questionnaire defaults to the workflow defined by AAI.

Perform the following steps in your application to register the customized workflow:

1. Create a new package in the table **aai_wf_app_package_b**.
   Note: Name **OBJECT_TYPE** for workflow definition in the convention **$APP_CODE_QTNR**. For example, if your APP_CODE is OFS_KYC, name the Object Type as OFS_KYC_QTNR.
2. Register a new object **V_OBJECT_TYPE** in the table **aai_wf_app_registration**.
3. Create a new process or copy it to the PMF application.
4. Add the entry with the object **V_OBJECT_TYP**E in the table **aai_wf_app_definition_map**.

Questionnaire validates the Object Type before invoking the workflow. If the naming convention of the workflow definition matches with the naming convention defined in the preceding steps, it invokes the registered workflow from your application. However, if the naming convention does not match the registered workflow, Questionnaire invokes the default reference workflow with object type **QTNR**.

To check for the creation of the new process, perform the following steps:

1. Create a new questionnaire in Draft status.
2. Check in the Process Monitor that the Questionnaire is running in the new process.

11 Data Security and Data Privacy

Data Security refers to the protection of data against unauthorized access and data theft. OFSAA ensures Data Security with the following features:

- Multi-Factor Authentication
- Transparent Data Encryption (TDE)
- Data Redaction
- File Encryption
- Key Management
- HTTPS
- Logging

11.1 Multi-Factor Authentication

This section is applicable only if you are using SSO enabled with multi factor authentication in OAM/OIM.

Multi-Factor Authentication (MFA) is a method of confirming a user's identity for login, by verifying 2 or more pieces of evidence (or factors) to an authentication mechanism. Two-Factor Authentication in OFSAA requires users to provide two levels of authentication. The subsections in this topic provide information to configure Two-Factor Authentication in OFSAA using OAM/OIM.

11.1.1 Prerequisites

The following list mentions the prerequisites required for this configuration:

1. All Oracle IDM Suite 11.1.2.3 related services should be running and OFSAA setup should be SSO enabled.
2. WebLogic or Tomcat as Web Application Server identified for the deployment of OFSAA.

11.1.2 Configuring OTP through Email using OAM Adaptive Authentication Service

The OAM Oracle Adaptive service uses SOA User Messaging Service (UMS) to send notifications. This requires that you must configure the SOA server to UMS to enable this feature.

11.1.2.1 Enabling Adaptive Authentication Service

The Adaptive Authentication Service is enabled using the Oracle Access Management Console.

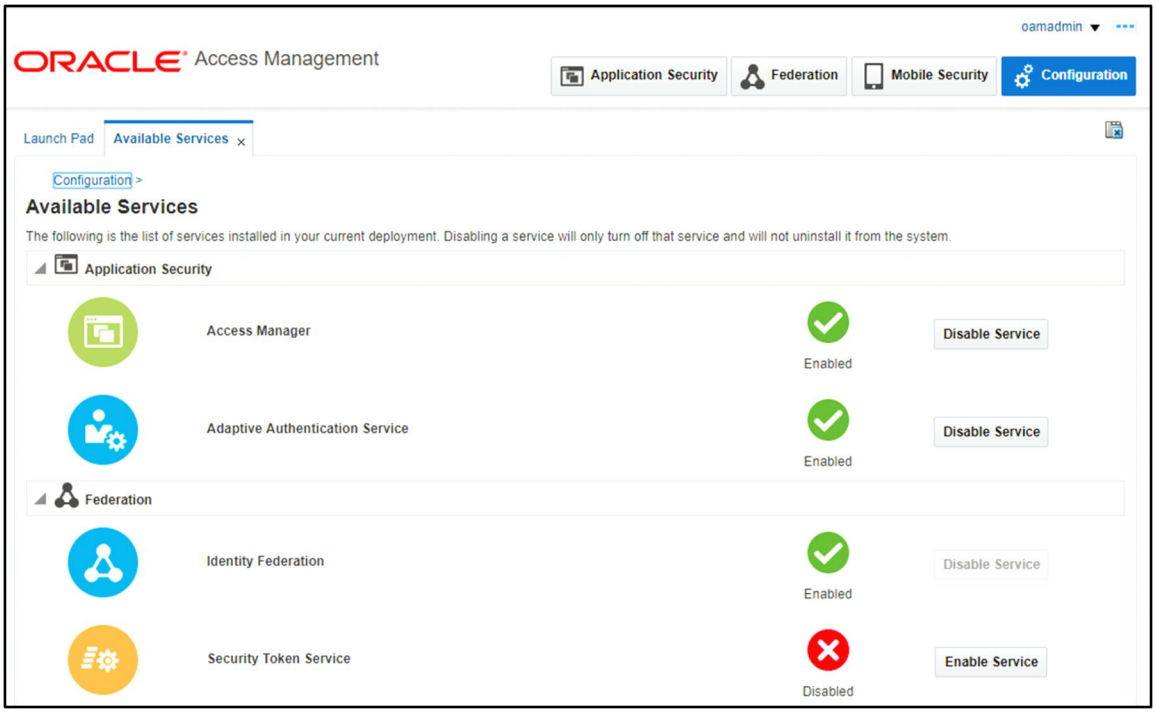
The Adaptive Authentication Service has to be licensed separately to use the two-factor authentication feature.

To enable the Adaptive Authentication Service, perform the following steps:

1. Login in to *OAM Admin Console* and click **Configuration** tab.
2. Navigate to **Configuration** and select **Available Services**.

3. Click **Enable Service** against **Adaptive Authentication Service**.

Figure 21: Oracle Access Management Available Services pane

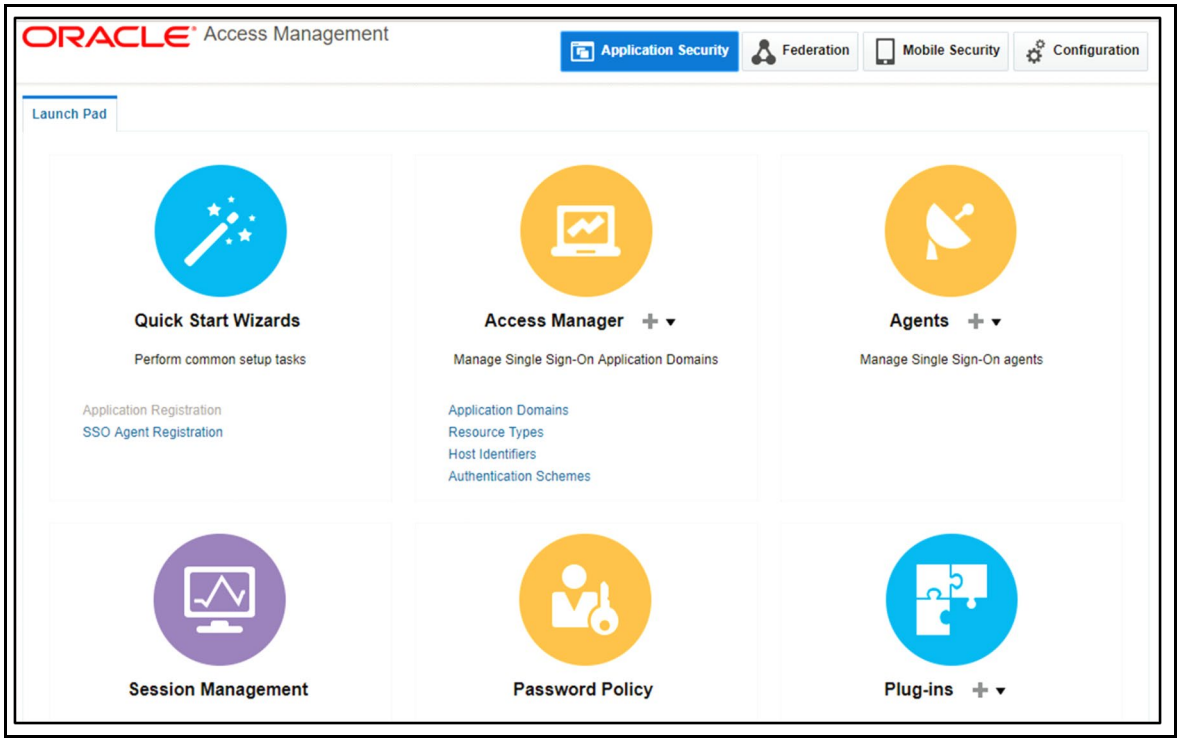


11.1.2.2 Configuring Adaptive Authentication Plugin

To configure email related settings in the Adaptive Authentication plugin, perform the following steps:

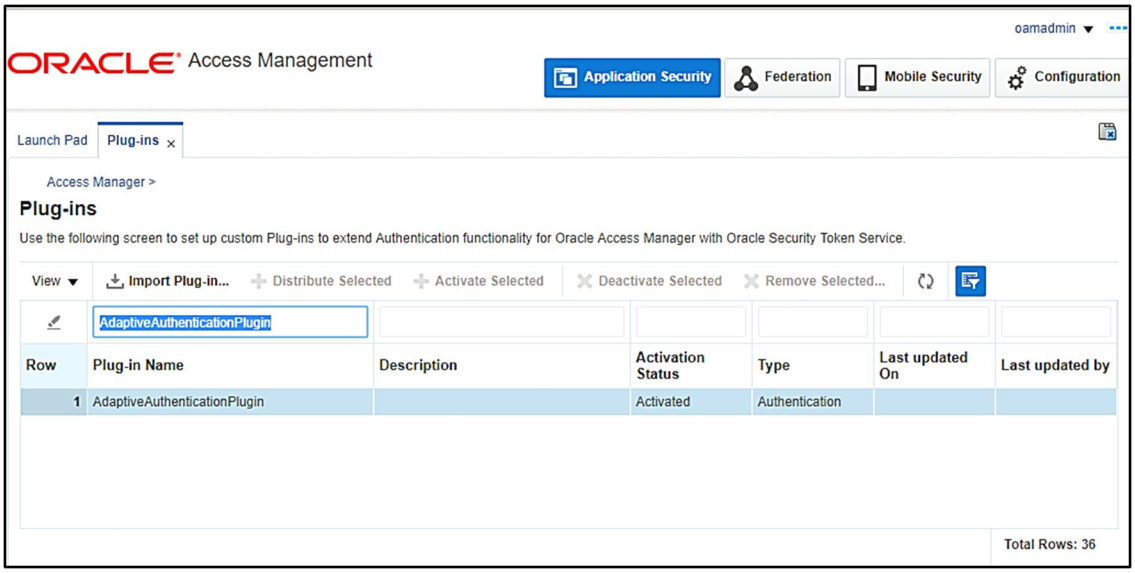
1. Login to *OAM Admin Console* and click **Application Security** tab.

Figure 22: Access Management - Application Security tab



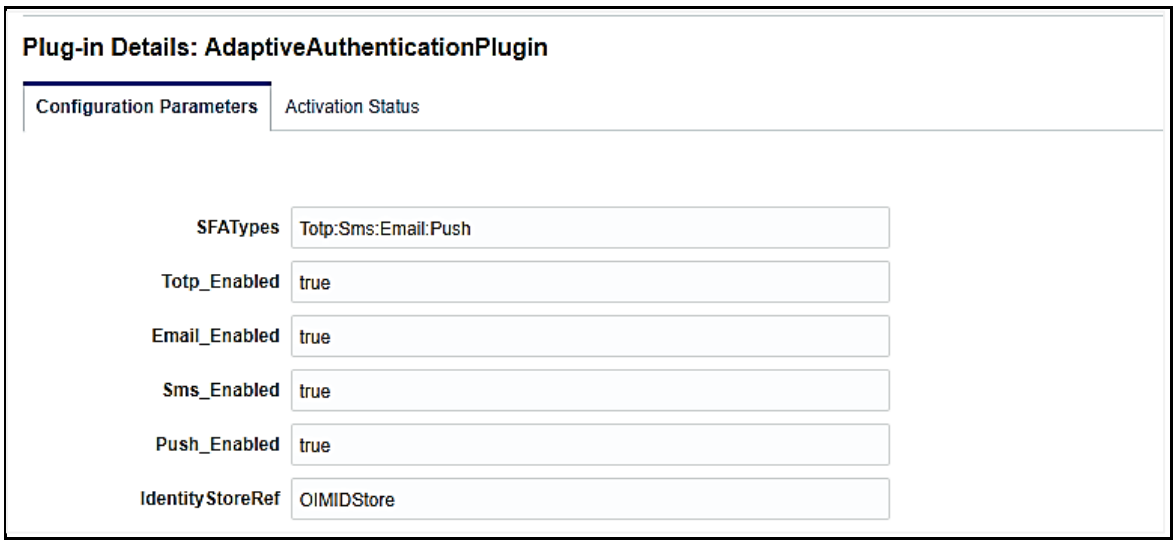
2. Click **Authentication Plug-ins** under *Plug-ins* tile. The *Plug-ins* window is displayed.

Figure 23: Plug-ins window



3. Search for **AdaptiveAuthenticationPlugin**.
4. Click the **AdaptiveAuthenticationPlugin** link. The *Plug-in Details: AdaptiveAuthenticationPlugin* window is displayed.

Figure 24: Plug-in Details: Configuration Parameters



5. Configure OTP through Email by updating the following *Configuration Parameters*:

   a. **SFATypes** - Types of Second Factor Authentication methods. To send OTP through Email, add Email to the list. Add Email if you are not using other SFA types.

   b. **Email_Enabled** - Set this attribute to **true** to send OTP through Email.

   c. **IdentityStoreRef** - Enter the user Identity store where your user details are stored, and user is authenticated in First-level authentication.

> **NOTE** After the first-level authentication, the adaptive authentication plug-in searches for the Email (required attributes for other types of SFA). If the **IdentityStoreRef** detail is not correct, then an error page is displayed after the First level authentication.

   d. **UMSAvailable** - Set the value to **true**

   e. **UmsClientUrl -** Enter the value for **UmsClientUrl**.
   Adaptive Authentication Service uses Oracle SOA User Messaging Services to send the Email notification.

   f. **EmailField** – Enter the value for Email Address attribute in the User Identity Store. The Adaptive Authentication plugin fetches the value for this field to send the email notification.

   g. **PinLength** – Specify the length of the OTP pin sent through Email.

   h. **PinChars** – Specify the characters to generate the OTP. If you want only digits in the OTP, enter only "0123456789".

   i. **EmailMsgSubject** – Email Subject for the OTP notification.

   j. **EmailMsgFrom** – From email address in the email notification.

   k. **EmailMsgFromName** – From name in the email notification

Figure 25: SMS Details

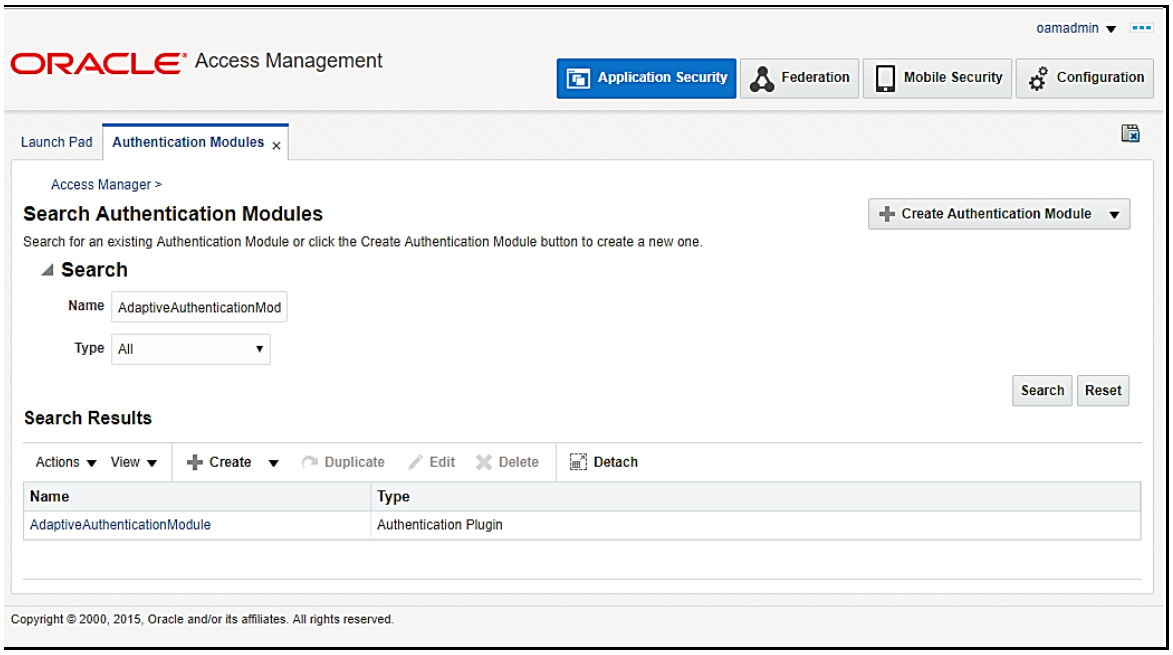
6. Click **Save**.

11.1.3 Configuring AdaptiveAuthenticationModule

To configure the Adaptive Authentication Module, perform the following steps:

1. Navigate to **Application Security > Plug-ins > Authentication Modules**.
2. Search for **AdaptiveAuthenticationModule**.

Figure 26: Authentication Modules tab



3. Click **AdaptiveAuthenticationModule**.
4. Click *Steps* tab and validate the configuration details entered. Update any Email related parameter if it is missing.
5. Validate **IdentityStoreRef**, **UmsAvailable**, **UmsClientUrl**, **EmailField**, **Email_Enabled** and so on. Update the values if required.

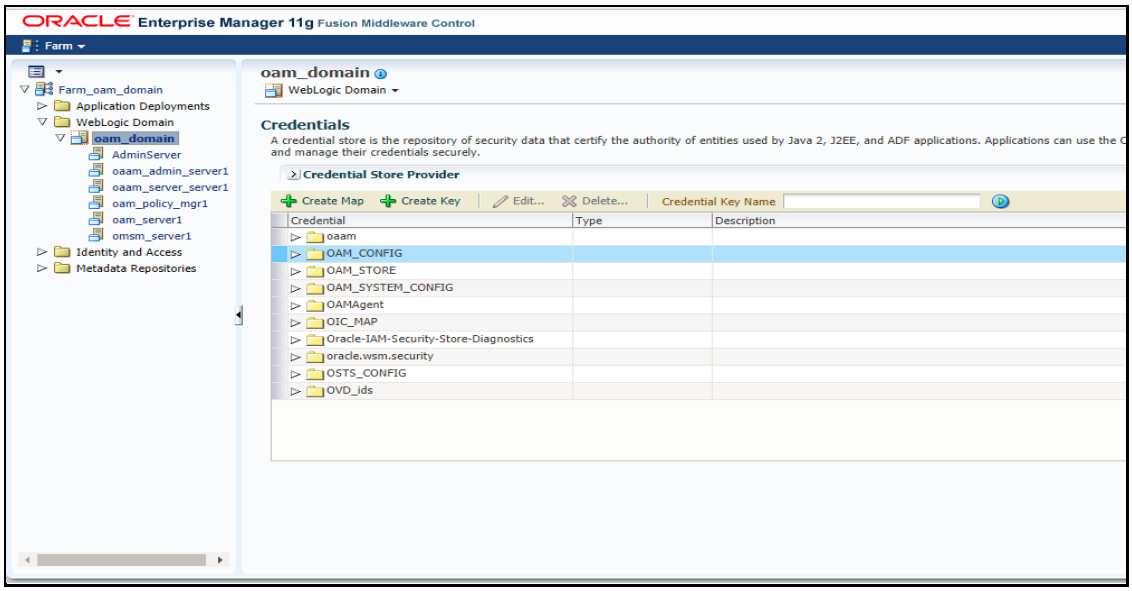
11.1.3.1 Configuring Credentials for UMS

Adaptive Authentication Service uses Oracle SOA **User Messaging Service (UMS)** to send Email notifications. The OAM server needs the UMS credentials to send the notifications.

To update the UMS credentials for OAM server, perform the following steps:

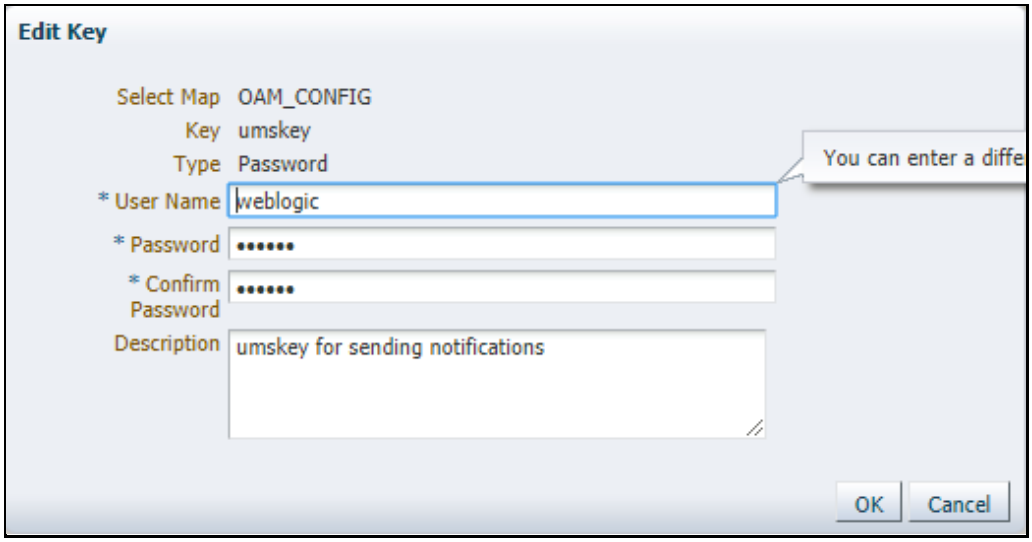
1. Login to OAM EM console.
2. Expand **Weblogic Domain** and then right click on **<Domain_Name>** and navigate to **Security > Credentials**.

Figure 27: Credentials for UMS window



3. From the *Credentials* window, click **OAM_CONFIG** and then click **Create Key**. The *Edit Key* window is displayed.

Figure 28: Edit Key window



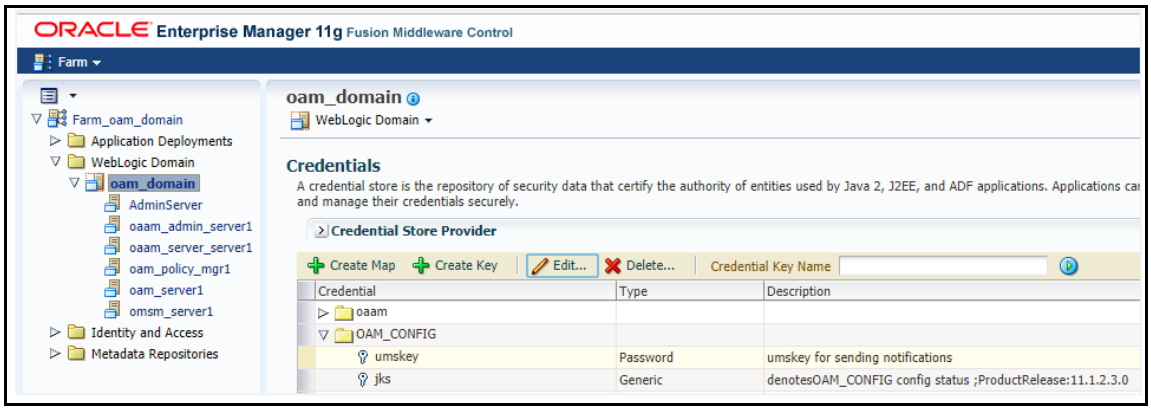
4. Enter the UMS key credentials such as **User Name, Password, Confirm Password** and **Description**. Make sure that **OAM_CONFIG** is selected in **Select Map** and **Type** is selected as Password.
5. Click **OK** to save.

For creating **umsKey** using the *wlst scripts,* perform the following steps:

1. Navigate to `<MiddleWare_HOME>/common/bin`.
2. Execute the following command:

   `./wlst.sh`
3. Connect to WebLogic server using `connect()` and enter the following WebLogic Admin server details:
   `createCred(map="OAM_CONFIG",key="umsKey",user="weblogic",password="welcome1" )`

Figure 29: Credentials for UMS window



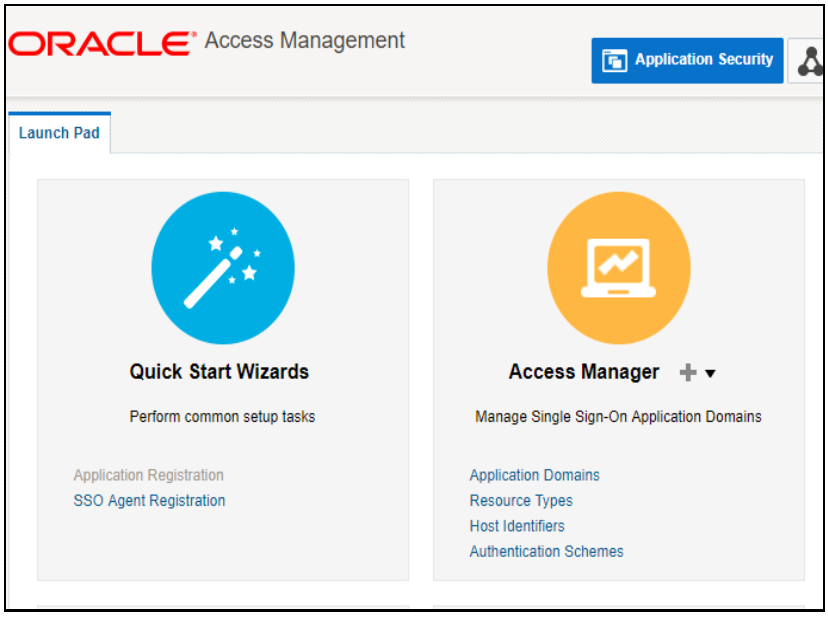
11.1.3.2 Protecting the Resource with AdaptiveAuthenticationScheme

The adaptiveAuthentication Scheme is used for two-factor authentication.

To configure, perform the following steps:

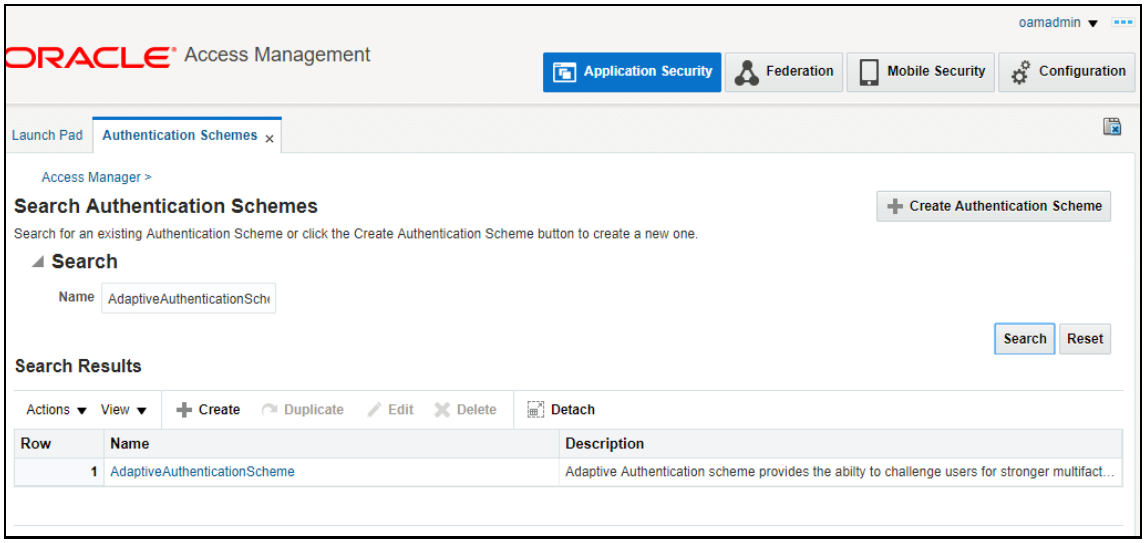
1. Login to *OAM Admin Console* and click **Application Security**.

Figure 30: Application Security page



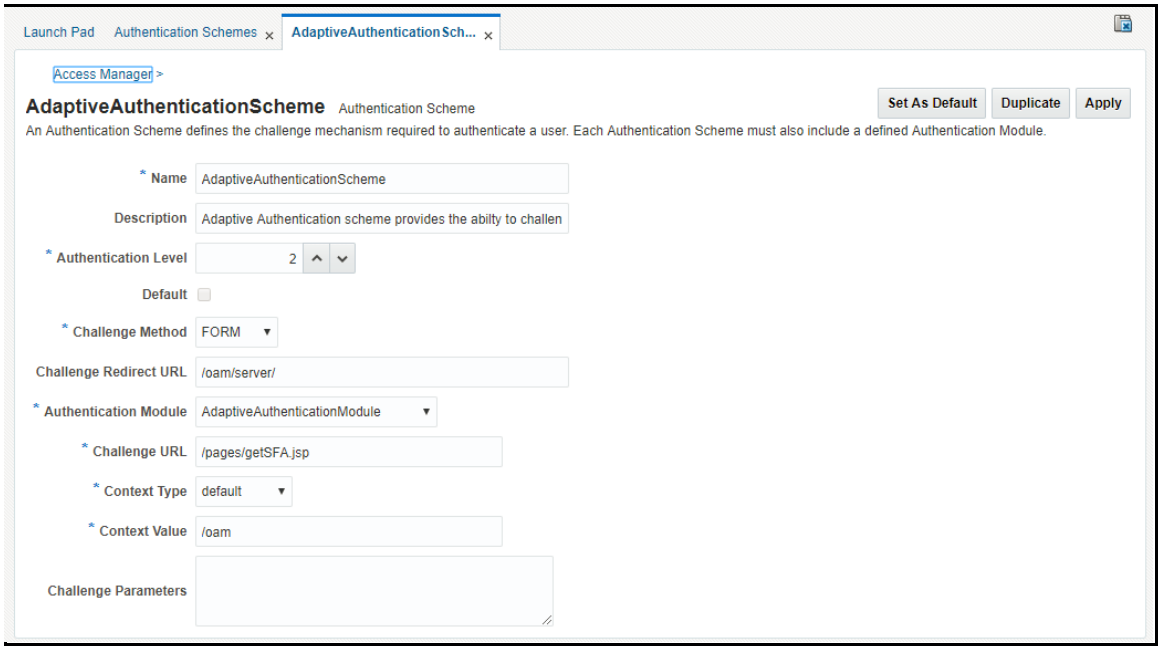
2. From the **Application Security** tab and click **Access Manager > Authentication Schemes**.
3. Search for **AdaptiveAuthenticationScheme**.

Figure 31: Authentication Schemas tab



4. Click **AdaptiveAuthenticationScheme** to view the details.

Figure 32: Authentication Schemas window



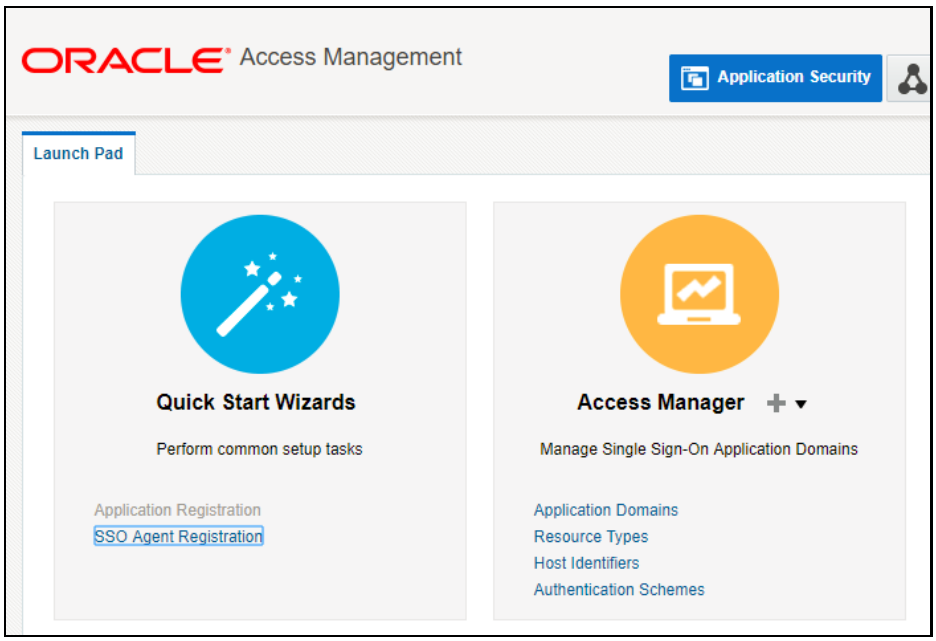
5. Verify the details and click **Apply**.

11.1.3.3 Enabling Two-Factor Authentication to a Protected Resource

To enable two-factor authentication to a protected resource, perform the following steps:

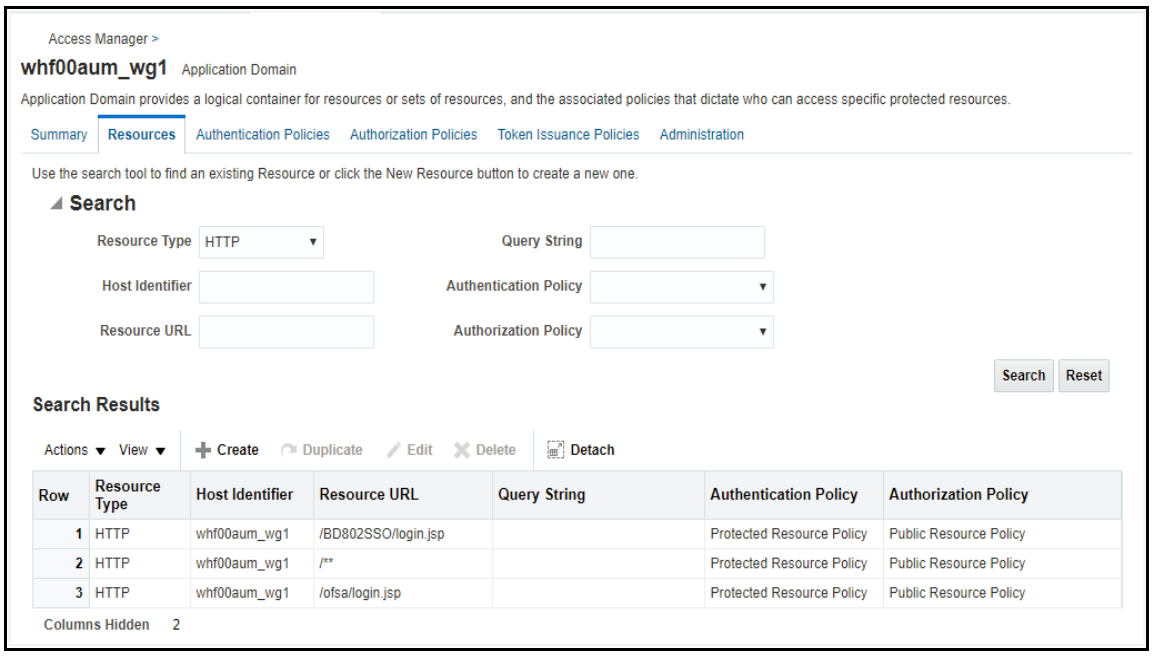
1. Login to *OAM Admin Console* and click **Application Security** tab.

Figure 33: Application Security page



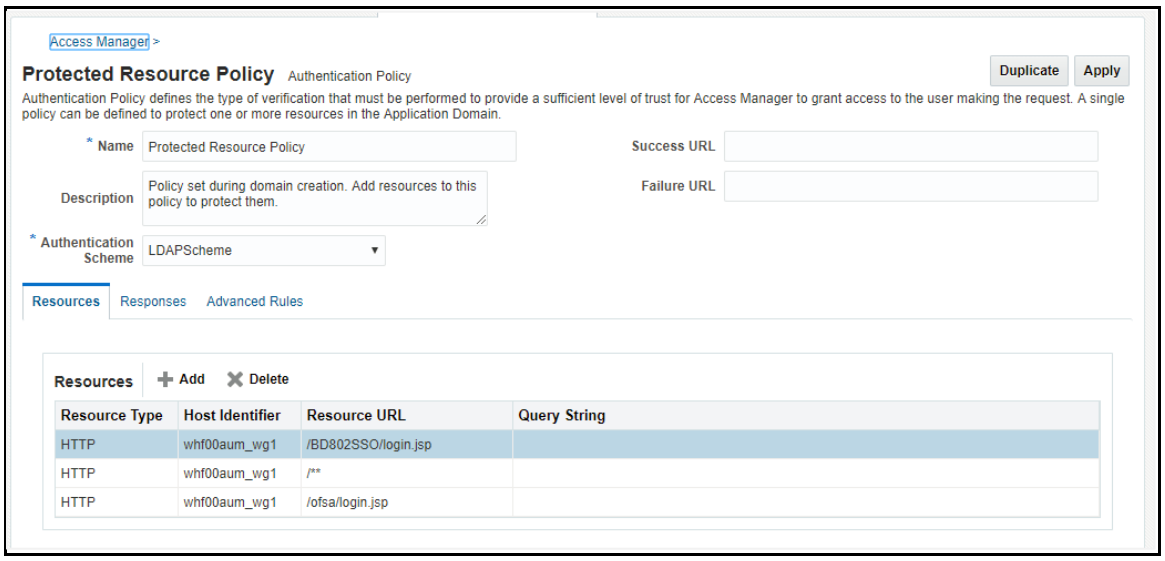
2. Click **Access Manager > Application Domains**.

Figure 34: Access Manager - Application Domains window



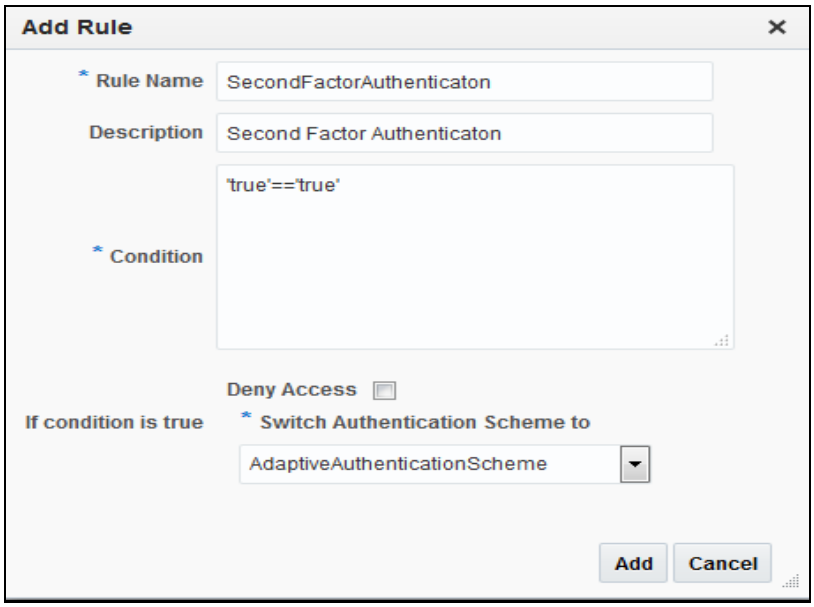
3. From the *Resources* tab, search for your SSO added Resource Type.
4. Select *Authentication Policies* tab and then click **Protected Resource Policy**.

Figure 35: Protected Resource Policy window



5. Click **Advanced Rules tab.**
6. **From the** *Post-Authentication* tab in the created Authentication Policy, click **Add**.

Figure 36: Add Rule window



7. Enter the required details as shown and click **Add** to save.

11.1.3.4 Accessing the UI

To access the UI, perform the following steps:

1. Access the UI by using the IP Address/ Host Name, Port, and Context Name of SSO enabled Setup.

```
http://<IPADDRESS/HOSTNAME hosting IDM OHS>:<OHSPORT>/<OFSAACONTEXT
NAME>/login.jsp
```

For example:

```
http://<SERVER_HOME>:7777/<CONTEXT>/login.jsp
```

2. Login with User Name and Password. After successful OIM login, the application prompts for Second Factor Authentication through OTP.

Figure 37: Oracle Access Manager Second Factor Authentication

3. Select the method to receive the OTP from the options: SMS or Email.

Figure 38: Oracle Access Manager Second Factor Authentication

4. Enter the OTP which you received through SMS or Email.
5. Click **Login**. The *OFSAA Landing Screen* is displayed.

11.2 Transparent Data Encryption (TDE)

OFSAAI is enhanced to support Transparent Data Encryption (TDE) feature of Oracle Advanced Security option. 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.

In case you did not enable TDE or Data Redaction during OFSAA installation and want to enable at a later point of time, see *Configure Transparent Data Encryption (TDE) and Data Redaction in OFSAA* section in OFS AAAI Application Pack Installation and Configuration Guide.

11.3 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.

11.3.1 Prerequisites

1. Ensure the required Oracle Database Server versions are installed :
   - Oracle Database Server Enterprise Edition 18c Release 3 - 64 bit RAC/Non-RAC with/without partitioning option, Advanced Security Option.
   - Oracle Database Server Enterprise Edition 19c Release 3 - 64 bit RAC/Non-RAC with/without partitioning option, Advanced Security Option.
2. You must have performed all configurations mentioned in the *Data Redaction* section in OFS AAAI Application Pack Installation and Configuration Guide.
3. The DATASECURITYADMIN user role must be mapped to the user to run the Data Redaction utility.
4. From the *Configuration* window in the *System Configuration* module, select the **Allow Data Redaction** checkbox. For more information, see *Configuration* section in the OFS Analytical Applications Infrastructure User Guide.

11.3.2 Input for Data Redaction

Following are the tables that are seeded as part of Data Redaction:

Table 19: Data Redaction table name and their description

Table Name	Description
AAI_DRF_FUNCTION_MASTER	This table holds the Redaction function definitions. Generic Functions can be email, card number, phone number etc.
AAI_DRF_FUNCTION_COLUMN_MAP	This table holds the Redaction Function- Column mappings. The columns will be redacted according to the Function mapping.
AAI_DRF_TABLE_ACCESS_CD_MAP	This table holds the mapping of tables having columns marked for redaction to the Access codes. These access codes are SMS function codes and are expected to be mapped to the role DATASECURITY. The policy expression would be created

Table Name	Description
	based on this role and would be evaluated in order to access unredacted data.

11.3.3 Data Redaction utility

This utility can be executed by running the seeded Batch with Batch Name as "##INFODOM##_DATA_REDACTION" if it is available as part of application common metadata. If it is not available, you have to create a new Batch as mentioned in the Creating Batch for Executing Data Redaction Utility section.

The task in the Batch has three parameters: `dataredaction.sh`, `true/false` and OFSAA User ID.

- **true/false flag**
  - False- By default, `false` is seeded. False indicates policy scripts will be generated and executed.
  - True- Specify `true` to generate policy scripts, but will not be executed. You can use this option if the logged-in user does not have script execution rights on Atomic Schema. See Executing Data Redaction utility with TRUE flag section to execute the scripts later.
- **User ID**- OFSAA user who is the batch owner

Note the following:

If any application specific database roles are granted to atomic schema, they should be granted as default roles after enabling data redaction.

```
Alter user << atomic schema user >> default role <<role1>>, <<role2>>.
```

For example, RQADMIN database role is granted to atomic schema user for ORE executions. In this case, post enabling data redaction, RQADMIN should be granted as a default role to atomic schema.

```
Alter user <<atomic schema user>> default role RQADMIN
```

11.3.3.1 Executing Data Redaction Utility with False Flag

Following are the steps if you want to execute Data Redaction utility with False flag:

1. From the *Batch Execution* window, search for Batch Name as "##INFODOM##_DATA_REDACTION".
2. Select the Batch and click **Execute Batch**.

   All policy scripts will be generated and executed in the Atomic Schema and the identified table data will be redacted.

11.3.3.2 Executing Data Redaction utility with TRUE flag

Following are the steps involved if dataredaction utility is executed with TRUE flag

1. From the *Configuration* window of System Configuration module, enter the absolute path where the encryption key is stored in the **Encryption Key Path** field. If this is not provided, default key will be used which is available in `$fic_home/conf` folder.

2. From the *Batch Maintenance* window, search for Batch ID as "##INFODOM##_DATA_REDACTION".
3. Select the Batch.
4. Select the task from the *Task Details* pane and click **Edit**.
5. In the Executable field in the Dynamic Parameters List, specify as `dataredaction.sh,true,<<ofsaa user id>>`.
6. Click **Save**.
7. From the *Batch Execution* window, search for Batch ID as <>>.
8. Select the Batch and click **Execute Batch**.
9. Navigate to `FTPshare/DataRedaction` folder. You can find 2 folders called Scripts and Postscripts inside DataRedaction folder.
10. Decrypt "create scripts" in the `FTPshare/DataRedaction/scripts` folder using `dmtfileencryption.sh` with the following arguments:

    `./dmtfileencryption.sh decrypt_file <INPUTFILE> <OUTPUTFILE> <KEYFILE>`

    - <INPUTFILE>- Provide the absolute path of the input file. Since all "create scripts" in the scripts folder need to be decrypted, you can provide the folder path, that is, `FTPshare/DataRedaction/scripts`.
    - <OUTPUTFILE>- Provide the absolute path of the input file.
    - <KEYFILE>- Provide the absolute path of key file with key file name. This should be same as that is provided in the Configuration window. If nothing was provided in the Configuration window, specify the default key path as `$fic_home/conf/ofsaa8xkey.ext`.

      For more details, see *Command Line Utility for DMT File Encryption* section in OFS Analytical Applications Infrastructure User Guide.
11. Execute the decrypted "create scripts" in the Atomic Schema.
12. Execute scripts in the `FTPshare/DataRedaction/postscripts` folder for populating required OFSAA metadata.

    The identified table data will be redacted.

11.3.4 Creating Batch for Executing Data Redaction Utility

If the seeded Batch is not available, create a Batch to execute Data Redaction utility.

Following are the steps required to create a Batch

1. From the *Batch Maintenance* window, click ➕ **Add** button in the *Batch Name* tool bar. The *Add Batch Definition* window is displayed.
2. Enter **Batch Name** and **Batch Description**.
3. Click **Save.** The newly added Batch will be listed in the *Batch Maintenance* window.
4. Select the Batch and click ➕ **Add** from the *Task Details* tool bar. The *Add Task Definition* window is displayed.

5. Enter **Task Description** and select **Component** as RUN EXECUTABLE from the drop-down list.
6. In the **Executable** field in the *Dynamic Parameters List*, specify as `dataredaction.sh,false/true,<<ofsaa user id>>`.
7. See *Adding Task Details* section in the *Operations* Chapter in the OFS Analytical Applications Infrastructure User Guide for details on other fields.

11.3.5 Logs

You can find the logs in `/ftpshare/logs/<ExecutionDate>/<Infodom Name>/RUN EXECUTABLE` folder.

11.3.6 Disabling Data Redaction

For disabling data redaction, perform the following steps:

1. From the *Configuration* window in the *System Configuration* module, de-select the **Allow Data Redaction** checkbox.
2. Run the Data Redaction utility. For details on running the Data Redaction utility, see Data Redaction utility section.

11.3.7 Reverting the Data Redaction for an individual Policy

To revert the data redaction for an individual policy, perform the following steps:

1. Run the below query as a SYS user.

   ```
   select * from REDACTION_POLICIES t where t.object_name='##TABLE_NAME##';
   ```

2. Fetch the policy name from the table.
3. Update the below query and run in the atomic schema.

   ```
   begin
     dbms_redact.DROP_POLICY (
       object_schema => '##USER_NAME##',
       object_name   => '##TABLE_NAME##',
       policy_name   => '##POLICY_NAME##'
     );
   end;
   /
   ```

11.3.8 Reverting the Data Redaction for an individual Column

To revert the data redaction for an individual column, perform the following steps:

1. Run the below query as a SYS user.

   ```
   select * from REDACTION_POLICIES t where t.object_name='##TABLE_NAME##';
   ```

2. Fetch the policy name from the table.

3. Update the below procedure and run in the atomic schema.

```
begin
  dbms_redact.ALTER_POLICY (
    object_schema => '##USER_NAME##',
    object_name   => '##TABLE_NAME##',
    policy_name   => '##POLICY_NAME##',
action => dbms_redact.drop_column,
column_name          => '##COULMN_NAME##'
  );
end;
/
```

11.4 Data File Encryption

OFSAAI supports encryption of Data files. A stand-alone File Encryption utility is provided to encrypt and decrypt the Data files.

To configure File encryption:

1. From the *DMT Configurations* window under *File Encryption* grid, enter the following details:
   a. Select **Yes** from the **Encryption at Rest** drop-down list.
   b. Enter the **Key File Name** and **Key File Path** of the key that is used to encrypt or decrypt the Data File. You can use File Encryption utility to generate key in AES 256-bit format. For details, see *Command Line Utility for File Encryption* section in OFS Analytical Applications Infrastructure User Guide.
2. For F2T or F2H, encrypt your Data File using File Encryption utility and place the Key used for encryption in the **Key File Path** given in the DMT Configurations window. Then place the encrypted Data File in `/ftpshare/<INFODOM>/dmt/source/<SOURCE_NAME>/data/<MIS_DATE>/`.
3. For T2F or H2F, the output Data file will be encrypted. Use the File Encryption utility to decrypt the data file.

   For details on how to execute File Encryption Utility, see *Command Line Utility for File Encryption* section in OFS Analytical Applications Infrastructure User Guide.

11.5 Key Management

The OFSAA Configuration Schema (CONFIG) is the repository to store passwords for users and application database schemas centrally. These values are AES 256 bit encrypted using an encryption key uniquely generated for each OFSAA instance during the installation process.

The OFSAA platform provides a utility (EncryptC.sh) to rotate/ generate a new encryption key if needed.

> **NOTE** Integration with any other Key management solution is out of scope of this release.

This section details about the EncryptC Utility, which is used to:

- Generate keystore from `AESCryptkey.ext` key.
- Retrieve `AESCryptkey.ext` if it is deleted using the keystore.
- Generate new `AESCryptKey.ext` and update the keystore.

11.5.1 Executing EncryptC Utility

The procedure to execute the EncryptC utility is described in the following subsections.

11.5.1.1 Knowing the Prerequisites

- Ensure that the `Keystore.properties` file is present in the `$FIC_HOME/conf` directory.
- Enter the keystore path where you want to generate AESkeystore.ks.

  For example,

  `keystorepath=/scratch/ofsaaweb/OFSAAI_810`
- Ensure that **EncryptC** utility is present in the `$FIC_HOME/utility/EncryptC` directory.

11.5.1.2 Generating Keystore

Generate keystore using the following procedure:

1. Navigate to the `$FIC_HOME/utility/EncryptC/bin` directory.
2. Execute the command:

   `./EncryptC.sh –genkeystore keystorepassword keypassword`
3. Expected output and actions required are listed:
   a. A prompt appears to enter the keystore path if the path is not mentioned in `keystore.properties`.
   b. Keystore path is read from `KeyStore.properties` file and name of keystore is **AESKeyStore.ks**. So this generates keystore at specified location.

11.5.1.3 Retrieving AESCryptKey.ext

Retrieve `AESCryptKey.ext` using the following procedure:

1. Navigate to the `$FIC_HOME/utility/EncryptC/bin` directory.
2. Execute the command:

   `./EncryptC.sh –retrieve keystorepassword keypassword`
3. Expected output and actions required are listed:
   a. `AESCryptKey.ext` is retrieved to all locations where it was originally present.

11.5.1.4 Generating new AESCryptKey.ext and updating the keystore

Generate new `AESCryptKey.ext` and update the keystore using the following procedure:

1. Navigate to `$FIC_HOME/utility/EncryptC/bin` directory.
2. Execute the command:

   ```
   ./EncryptC.sh -genkey keystorepassword keypassword
   ```

3. Expected output and actions required are listed:
   a. The system checks whether keystore exists or not. If it does not, then it prompts for generating keystore using the `-genkeystore` option.
   b. The system rotates the existing `AESCryptKey.ext` and generates a new `AESCryptKey.ext` key.
   c. Then it updates the keystore with the new key.

> **NOTE** If you provide an option other than the ones discussed in the preceding sections, the system prompts to enter the correct option.

11.6 HTTPS Protocol

HTTP Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a network.

To change protocol from HTTP to HTTPS, follow these steps:

1. Create SSL related certificates and import to respective servers.
2. Enable SSL on a desired Port (example 9443) on your existing and already deployed web application servers.
3. Execute PortC Utility to change the Servlet port to hold new SSL port and Servlet Protocol from http to https. For details, see Changing IP/ Hostname, Ports, Deployed paths, Protocol of the OFSAA Instance.
4. When SSL/TLS is configured on Java 7, navigate to `$FIC_HOME/utility/Migration/bin` path and modify the `ObjectMigration.sh` file as given:

   ```
   $JAVA_BIN/java $X_ARGS_OBJMIG -Dhttps.protocols=TLSv1.2 -classpath
   $_CLASSPATH $MAIN_JAVA_CLASS $MIGRATION_HOME> $LOG_FILE
   ```

> **NOTE** For more information, see the link:
> https://bugs.openjdk.java.net/browse/JDK-8151387.

11.7 Logging

Logging in OFSAA is done using Log4J. The log files are available in the following locations:

- **UI/Web Logs**: `<DEPLOYED LOCATION>/<Context>.ear/<Context>.war/logs`
- **Application Logs**: `$FIC_HOME/logs`
- **Execution Logs**: `/ftpshare/logs/<MISDATE>/<INFODOM>/<COMPONENT NAME>/<LOG FILE NAME>.log`

11.7.1 Purging of Logs

Configure the logger related attributes in the `RevLog4jConfig.xml` file available in the `$FIC_HOME/conf/` folder. Each of log file will have appenders in this file and attributes pertaining to this particular appender can be changed.

The default size of the log files is set to 5000 KB and number of maximum backup log files retained is set to 5, both of which are configurable. Increasing these parameters to a higher value should depend on the server hardware configurations and may reduce the performance.

> **NOTE** Similar settings are also available in `OFSAALogger.xml` file available in the `$FIC_HOME/conf/` folder which contains configuration for additional loggers used in OFS AAI. You can configure the Log file size as explained in the following section.

To configure the Logs file size, follow these steps:

1. Navigate to `$FIC_HOME/conf` folder or `<DeployedLocation>/<context.war>/<context>/` and locate `RevLog4jConfig.xml` file.
2. Configure the logger related attributes in the `RevLog4jConfig.xml` file. This file will have Appenders for each log files.

   Sample Appender for UMM log file is shown:

```
<RollingFile name="UMMAPPENDER"
fileName="/scratch/ofsaaweb/weblogic/user_projects/domains/cdb/applications/cdb.ear/cdb.war/logs/UMMService.log"

filePattern="/scratch/ofsaaweb/weblogic/user_projects/domains/cdb/applications/cdb.ear/cdb.war/logs/UMMService-%i.log" >

<PatternLayout>

  <Pattern> [%d{dd-MM-yy HH:mm:ss,SSS zzz aa}{GMT}] [%-5level] [WEB] %m%n </Pattern>

  </PatternLayout>

  <Policies>

       <SizeBasedTriggeringPolicy size="5000 KB" />

  </Policies>

   <DefaultRolloverStrategy max="5"> <!-- number of backup files -->

       </DefaultRolloverStrategy>

  </RollingFile>
```

3. To change the log file size, modify the value set for `SizeBasedTriggeringPolicy size`.
4. To change the number of backup files to be retained, modify the value set for `DefaultRolloverStrategy max`.

11.7.2 Log File Format

In OFSAA, log format is standardized and can be read by any standard log analysis tool. The standard log format is as follows:

```
[GMT TIMESTAMP] [LOGGER LEVEL] [LOGGER LOCATION]  [MODULE/COMPONENT]
[LOGGED IN USER] [JAVA CLASS] <LOG MESSAGE>
```

Sample:

```
[25-04-18 10:08:41,066 GMT AM] [INFO    ] [WEB]  [UMM]  [UMMUSER]
[BUSINESSMETADATA] Inside createImplicitObjectsForAllInfodom

[25-04-18 10:08:41,069 GMT AM] [INFO    ] [WEB]  [UMM]  [UMMUSER]
[BUSINESSMETADATA] Call createImplicitObjectsForMapper for infodom =
TESTCHEF

[25-04-18 10:08:42,142 GMT AM] [DEBUG] [WEB]  [UMM]  [UMMUSER]
[BUSINESSMETADATA] Source created successfully for infodom TESTCHEF

[25-04-18 10:08:42,142 GMT AM] [INFO    ] [WEB]  [UMM]  [UMMUSER]
[BUSINESSMETADATA] Start - code added to create user group hierarchy for
this infodom

[25-04-18 10:08:42,142 GMT AM] [INFO    ] [WEB]  [UMM]  [UMMUSER]
[BUSINESSMETADATA] Inside createUserGroupHierarchyForInfodom
```

12 Generic Configurations

This chapter describes about generic configurations required for OFS AAAI Application pack. It consists of the following sections:

12.1 OFSAA Global Performance Optimization

OFSAA execution performance can be enhanced by providing optimization parameters specifically at information domain level, database level, object level or object sub type level. This is done by updating the `AAI_GLOBAL_EXEC_OPTIMIZATION` table with appropriate values.

The columns and the values to be given in the `AAI_GLOBAL_EXEC_OPTIMIZATION` table are indicated as follows:

Table 20: Global Performance Optimization name, value, and their description

Column Name	Description	Value
`V_INFODOM_CODE`	Information Domain code	ALL or specific information domain code.

Column Name	Description	Value
V_DB_TYPE	Database type of the Information Domain	ORACLE or HIVE
V_OBJ_TYPE_CODE	Object type for which you want to apply execution optimization.	For example, Rule (RL). This is referred from AAI_OBJ_TYPE_SUBTYPE_MAP. V_ OBJ_TYPE_CODE.
V_OBJ_SUBTYPE_CODE	Object sub type for which you want to apply execution optimization.	For example, for Rule (RL) Object type, TYPE2 and TYPE3 are subtype codes. This is referred from AAI_OBJ_TYPE_SUBTYPE_MAP. V_ OBJ_SUBTYPE_CODE.
V_EXEC_OPTIM_PARAM_NAME	Name of the parameter using which optimization is done.	This is referred from AAI_EXEC_OPTIM_PARAM_B. V_EXEC_OPTIM_PARAM_NAME. Currently supported parameters are POSTSCRIPT, PRESCRIPT, MERGE, HINT and SELECT.
V_EXEC_OPTIM_PARAM_VALUE	Value for the optimization parameter mentioned in V_EXEC_OPTIM_PARAM_NAME column.	

12.2 Query Performance Optimization

A configuration file, **OracleDB.conf** has been introduced to accommodate any configurable parameter related to operations for Oracle database. If you do not want to set a parameter to a specific value, then the respective parameter entry can be removed/commented from the **OracleDB.conf** file which resides in the path $FIC_DB_HOME/conf.

The following table details the configurable OFSAA parameters in **OracleDB.conf** file with its purpose and the way it maps to Oracle Database Parallelism settings.

Table 21: Query Performance Optimization parameters and their description

Parameters	Description
CNF_PARALLEL_DEGREE_POLICY	Sets the parallel degree policy. Possible values – **MANUAL**, **LIMITED**, or **AUTO**. Query fired on the database - ALTER SESSION SET PARALLEL_DEGREE_POLICY=<<CNF_PARALLEL_DEGREE_POLICY>>
CNF_PARALLEL_QUERY	Sets parallelism for queries. Possible values – **DISABLE**, **ENABLE**, or **FORCE**. Query fired on the database - ALTER SESSION <<CNF_PARALLEL_QUERY>> PARALLEL QUERY

Parameters	Description
CNF_PARALLEL_DML	Sets parallelism for DML operations. Possible values – **DISABLE**, **ENABLE**, or **FORCE**. Query fired on the database - ALTER SESSION <<CNF_PARALLEL_QUERY>> PARALLEL DML
CNF_DEGREE_OF_PARALLELISM	Sets the degree of parallelism. Possible values – Value can be any positive integer. The default mode of a session is *DISABLE PARALLEL DML*. If *CNF_DEGREE_OF_PARALLELISM* is not set, then the default degree, as decided by Oracle will be used. Queries fired on the database - ALTER SESSION <<CNF_PARALLEL_QUERY>> PARALLEL QUERY PARALLEL <<CNF_DEGREE_OF_PARALLELISM>> ALTER SESSION <<CNF_PARALLEL_QUERY>> PARALLEL DML PARALLEL <<CNF_DEGREE_OF_PARALLELISM>>

For more information, see the **Using Parallel Execution** section in Oracle Database VLDB and Partitioning Guide.

12.3 Adding FIC_MIS_DATE Option During Batch Creation IN AAI Run Framework

To add the execution date to the FIC_MIS_DATE using the FIRERUN_DEFAULT_MISDATE in the configuration table:

- Set the parameter to Y, to assign the user provided MIS Date as the default execution date, in the DIM RUN table.
- Set the parameter to N, to assign the system date as the execution date, in the DIM RUN table.

12.4 Multiple Language Support (MLS) Utility

Multiple Language Support (MLS) refers to the ability to run multiple languages in the same Application instance. MLS provides multiple language architecture, while specific language packs provide the individual language translations.

Multiple Language Support (MLS) is supported for the following objects:

- Unified Metadata Manager- All Objects.
- Run Rule Framework- Run, Process and Rule definitions.
- Financial Services Applications- Dimension Management - Attributes, Members, Hierarchies; Filters, Expressions and Object Migration.

The MLS Utility can be invoked through the execution of the following steps with an appropriate parameter. The purpose and the parameters are listed below.

To execute the MLS utility, perform the following steps:

1. Navigate to `$FIC_HOME/MLS_ofsaai` directory of OFSAAI APP tier.

2. Execute the MLS utility <Command> <parameter>.

12.4.1 Available Parameters

MES

You need to invoke the utility with this parameter for population of seeded text such as menu labels and popup messages.

You need to execute this utility with this parameter only after you install an OFSAA language pack, where the language pack has a version lower than the installed OFSAAI software version. For example, you are installing the OFSAA 8.1.0.0.0 LP on an OFSAA setup where the OFSAA version is 8.1.1.0.0.

There are additional labels and messages that have been added or modified as part of previous release. In order to update/ populate the `messages_<locale>` table with delta records, you need to run the utility with this parameter. Running this utility will copy the incremental set of text to the language-specific `messages_<locale>` tables as a placeholder, so you will see an American English message (default for base install) until the translation is available in language packs.

For example, if you are on OFSAA 8.1.1.0.0 and have installed OFSAA 8.1.0.0.0 language packs for French and Spanish (since the latest 8.1.x language pack may not yet be available), running the utility with the MES parameter will duplicate the incremental labels and messages from the `messages_en_US` table to the language specific tables for French and SpanishCommand:

```
./MLS_ofsaai.sh MES
```

MLS

You need to execute the MLS utility with this parameter in order to pseudo-translate the translatable attributes of user-defined metadata objects. For example, this will copy Names and Descriptions as placeholders in rows for other installed languages.

See the above list of MLS-enabled OFSAAI object types. After installation of 8.1.0.0.0 release for any application, the base metadata and translatable data for these object types will have rows for US (American English) only. Executing the utility with the MLS parameter will duplicate the translatable attributes of the metadata objects for other installed locales.

Command:

```
./MLS_ofsaai.sh MLS
```

Multilingual Support (MLS) architecture has been enabled by segregation of the metadata definitions into non-translatable content (such as Codes), and translatable content (such as Names and Descriptions) for the en_US and other installed languages. The object information has been organized with a single row of base information (containing non-translatable attributes) and multiple associated language rows for holding translatable content (one for each language including a row for en_US.).

For example, you have a Hierarchy which has been defined in en_US (US English) language and then you install 8.1.0.0.0 language packs for 2 more languages, say fr-FR (French), and es-ES (Spanish). Post execution of the utility with the MLS parameter, the same Hierarchy rule will be available in the two additional languages that you have installed. You can then login to each locale (language) and edit the Hierarchy definition to enter translated text for the Hierarchy Name and Description.

Before you run the utility, you will have only one row for English, for example:

LANGUAGE=US, Description="Organization Hierarchy – Level 1", SOURCE_LANG=US

After you run the utility, you will have two more rows: One for French, and one for Spanish:

LANGUAGE=FR, Description="Organization Hierarchy – Level 1", SOURCE_LANG=US

LANGUAGE=ES, Description="Organization Hierarchy – Level 1", SOURCE_LANG=US

That is, the utility has created a copy of the source row for each target language. The source language in each row is American English (US), the Description data is American English, and the LANGUAGE column contains the target language code. The Hierarchy rule will be available when you login with any of the above languages. For example, if you login with French, you can select and edit the object definition, then update the Name and Description to a French translation of the text.

> **NOTE** As in the above example, running with MLS is necessary for objects (such as a Hierarchy rule) that exist in OFSAAI 8.1.0.0.0 (or later release) prior to applying a language pack for a new locale. If you create a Hierarchy after you apply the language pack, OFSAAI will automatically replicate text (such as Name and Description) into the new locale.

12.4.2 AAIPI.sh Utility

AAIPI.sh utility can be executed instead of executing MLS utility with different parameters. This utility will internally call the MLS utility in the following order:

```
./MLS_ofsaai.sh MIG
./MLS_ofsaai.sh MLS
./MLS_ofsaai.sh MES
```

To execute this utility:

1. Navigate to `$FIC_HOME/Post_AAI_Migration` directory of OFSAAI APP tier.
2. Execute command:

   ```
   ./aaipi.sh
   ```

You can find the log file `Post_AAI_Migration.log` in the following location `$FIC_HOME/Post_AAI_Migration/logs/`.

12.5 Transferring Batch Ownership

A procedure called TRANSFER_BATCH_OWNERSHIP is available in Configuration Schema to transfer the batch ownership of specific batches in an information domain or across information domains.

To execute the procedure:

1. Login to Configuration Schema.
2. Execute the procedure TRANSFER_BATCH_OWNERSHIP by entering following command:

   ```
   begin
   AAI_TRANSFER_BATCH_OWNER.TRANSFER_BATCH_OWNERSHIP
   ('<fromuser>','<touser>','<batchid>','<infodom>');
   end;
   ```

- `<fromuser>` - Specify the ID of the user whose batch ownership you want to transfer.
- `<touser>` - Specify the ID of the user to whom the ownership has to be transferred.
- `<batchid>` - This is an optional parameter. Specify the ID of the batch whose ownership you want to transfer. If `<batchid>` is not specified, all batches owned by the `<fromuser>` will be transferred to the `<touser>`.
- `<infodom>` - This is an optional parameter. Specify the information domain name if ownership of all batches in that information domain needs to be transferred to the `<touser>`. If `<infodom>` is not specified, ownership of batches across all information domains will be transferred.

For example,

To transfer a single batch ownership, execute the following command:

```
begin
AAI_TRANSFER_BATCH_OWNER.TRANSFER_BATCH_OWNERSHIP
('<fromuser>','<touser>','<batchid>');
end;
```

To transfer all batch ownerships across infodoms, execute the following command:

```
begin
AAI_TRANSFER_BATCH_OWNER.TRANSFER_BATCH_OWNERSHIP
('<fromuser>','<touser>');
end;
```

To transfer all batches in a specific infodom, execute the following command:

```
begin
AAI_TRANSFER_BATCH_OWNER.TRANSFER_BATCH_OWNERSHIP
('<fromuser>','<touser>','','<infodom>');
end;
```

12.6 Database Password Reset/ Change

The database password for config schema and atomic schema should be changed periodically for security. The following configurations are required on changing the database passwords:

For changing CONFIG schema password:

1. Login to the database and change the config schema password.
2. Login to the OFSAA server.
3. Stop all OFSAA services.
4. Delete `Reveleus.sec` from `FIC_HOME/conf`.
5. Restart OFSAA service in foreground (without the nohup option).
6. Enter the latest config schema password when you are prompted at the console.

For changing the ATOMIC schema password:

1. Ensure the OFSAA services are running, and application can be accessed.
2. Login to the database and change the ATOMIC schema password.
3. Login to the OFSAA application as any user with System Administrator privilege.
4. Navigate to *System Configuration and Identity Management* > *Administration and Configuration* > *Database Details*.
5. Select the appropriate connection and edit the **Password**.

Resource Reference/ Web Server JDBC Connection details

On change of the CONFIG/ ATOMIC schema passwords, the corresponding Resource Reference/ JNDI connection entries made in the Web Application Servers need to be updated.

- For Apache Tomcat Web Server.
  - Stop the Tomcat Server.
  - Update the `<Context> -> Resource tag` details in the `Server.xml` file present in `$CATALINA_HOME/conf` directory with the latest config schema and atomic schema passwords. For Tomcat, both Config Schema (FICMASTER resource) and Atomic Schema (<INFODOM_NAME> resource) exist.
- For WebSphere / WebLogic
  - Access the server specific Admin console.
  - Login to the server with Administrative privileges.
  - Under Domain Structure list box, expand the appropriate Domain and navigate to Services > JDBC >Data Sources. A list of data sources are populated on the right side. Select the appropriate Data Source and update the connection details. with the latest config schema and atomic schema passwords. For more information, see the *Configuring Resource Reference* section in the *OFS AAAI Application Pack Installation and Configuration Guide* available in OHC Documentation Library.
  - Restart OFSAA services.

12.7 Changing IP/ Hostname, Ports, Deployed paths of the OFSAA Instance

The Port Changer utility can be used to change IP/ Hostname, Ports, and Deployed paths of the OFSAA instance.

This Utility is only meant for replacing the Platform Framework related files and tables of the Pack Name OFS_AAAI_Pack. If your setup has other Application Packs kindly check the respective documents for the Applications or Application Support Team My Oracle Support.

Prerequisites

- Ensure that the `RevLog4jConfig.xml` of the `$FIC_HOME/conf` and the **AAI_SETUP_PROPS** Table of the Config Schema for the param name `LOGHOME` is configured with the default log paths before executing the utility.

The default log path for `RevLog4jConfig.xml` is `$FIC_HOME/logs` and the default log path to be set for the **AAI_SETUP_PROPS** Table of the Config Schema for the param name LOGHOME is `<deployed area of web server>/logs`.

- For more information, see *How to Find and Maintain OFSAA and OFSAAI Log and Configuration Files (Doc ID 1095315.1)* available in My Oracle Support.

12.7.1 Running Port Changer Utility

Port Changer (PortC) utlity is enhanced to run as an automated job without any manual intervention.

Complete the following steps to run the PortC utility.

1. Navigate to `$FIC_HOME/utility/PortC/bin` folder on *Target*.
2. Run the **PortC.sh** utility using command:

   `./PortC.sh DMP`

   A file with the name `DefaultPorts.properties` will be created under `$FIC_HOME` directory which will contain the ports, IPs and paths currently being used.

   NOTE It is mandatory to run the Port Changer utility using the DMP parameter every time before executing the utility using UPD command.

3. Make the necessary changes to those ports, IPs, and paths in the `DefaultPorts.properties` file as per the Target environment. Save the changes.

   NOTE In the properties file, make sure that the JDBC_URL parameter does not contain space(s). If you enter JDBC_URL with space(s), then you might experience errors in accessing the System Configuration window.

4. Run the **PortC.sh** utility using the command:

   `./PortC.sh UPD`

   This will change the ports, IPs and paths in `.profile` (under home directory), all files under `$FIC_HOME` directory, and tables in the database according to the values mentioned in `DefaultPorts.properties` file.

5. Execute the `.profile` file and create the EAR/WAR file. Then restart the OFSAA services and redeploy to the configured web application server.

12.8 Using X-Frame-Options to Embed OFSAA Content on your Site

By default, the OFSAA configuration does not allow you to embed OFSAA Content on your site. However, you can modify the web.xml file to enable this option. For more information about X-Frame-Options, see https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options.

12.8.1 Knowing the Prerequisites

The following is the prerequisite to configure X-Frame-Options to embed OFSAA content on your site:

You can embed the OFSAA Content only on the following browsers that support X-Frame-Options headers:

Table 22: Browser Details and their Supported Versions

Number	Browser	DENY and SAMEORIGIN Support Introduced Version	ALLOW-FROM Support Introduced Version
1	Chrome	4.1.249.1042 [3]	Not supported or Bug reported [4]
2	Firefox (Gecko)	3.6.9 (1.9.2.9) [5]	18.0 [6]
3	Internet Explorer	8.0 [7]	9.0 [8]
4	Opera	10.50 [9]	
5	Safari	4.0 [10]	Not supported or Bug reported [11]

12.8.2 Enabling or Disabling X-Frame-Options in the web.xml File

You have to change the default OFSAA setting for X-Frame-Options from **SAMEORIGIN** to **ALLOW-FROM** in the *web.xml* file to embed OFSAA content on your site.

The following is the procedure to modify the *web.xml* file:

1. Open the `web.xml` file in an editor.
2. Search for the following tag:

```
<filter>
<filter-name>FilterServlet</filter-name>
<filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
</filter>
```

3. Add the following tag before the tag shown in the preceding step:

```
<filter>
   <filter-name>FilterServletAllowFrom</filter-name>
   <filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
   <init-param>
       <param-name>mode</param-name>
       <param-value>ALLOW-FROM https://example.com/</param-value>
   </init-param>
</filter>
<filter-mapping>
   <filter-name>FilterServletAllowFrom</filter-name>
   <url-pattern>/url1</url-pattern>
```

```
</filter-mapping>
```

4. Replace **https://example.com/** with the URL of your site and replace **/url1** with the OFSAA relative URL. This embeds OFSAA content on your site.

12.9 Setting Access-Control-Allow-Origin Header

Setting the Access-Control-Allow-Origin header value allows browsers to get responses from the origin and access it for the request codes sent.

The following is the procedure to set Access-Control-Allow-Origin header:

1. Open the `web.xml` file in an editor.
2. Search for the following tag:

```
<filter>
<filter-name>FilterServlet</filter-name>
<filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
</filter>
```

3. Add the <init-param> tag values within the filterservlet tag as shown in the following:

```
<filter>
<filter-name>FilterServletAllowFrom</filter-name>
<filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
<init-param>
<param-name>AllowOrigin</param-name>
<param-value><origin></param-value>
</init-param>
</filter>
```

4. Replace <origin> in the preceding tag with the URL of your website. This allows the request of code from the origin.

12.9.1 Knowing Additional Cross-Origin Resource Sharing (CORS) Configuration

Setting the Access-Control-Allow-Origin header value described previously allows for responses of all requests. Configuring CORS renders more security to the application and reduces vulnerability to CSRF and XSS attacks. It also allows only specific sharing of resources such as script_font and CSS.

> **NOTE** The CORS configuration is preset in OFSAA and does not require any action. The information presented here is for your understanding.

The following headers have been added to make the shared resource and response restricted to specific http method types and also to be accessible through authentication:

1. Access-Control-Allow-Credentials
2. Access-Control-Allow-Methods

12.10 Configuration for Tomcat

To stop generating static content with one print statement per input line, you need to configure the `web.xml` file.

To configure `web.xml` file, perform the following steps:

1. Navigate to `tomcat/conf` folder.
2. Edit `web.xml` file as explained below:

   Set the mapped file parameter to **False** in the servlet tag mentioned with

   ```
   <servlet-name>jsp</servlet-name>.
   <init-param>
   <param-name>mappedfile</param-name>
   <param-value>false</param-value>
   </init-param>
   ```

12.11 Configuring WebLogic

This section provides information for generic configurations required for OFSAA deployed on WebLogic server.

12.11.1 Configuring WebLogic for REST Services Authorization

To enable REST API authorization by OFSAA in WebLogic server, perform the following steps:

1. Open the `config.xml` file located in the domain where OFSAA is deployed, that is, `<domain_home>/config/config.xml`.
2. Add the following in the security-configuration tag:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   ```

12.12 Configuring WebSphere

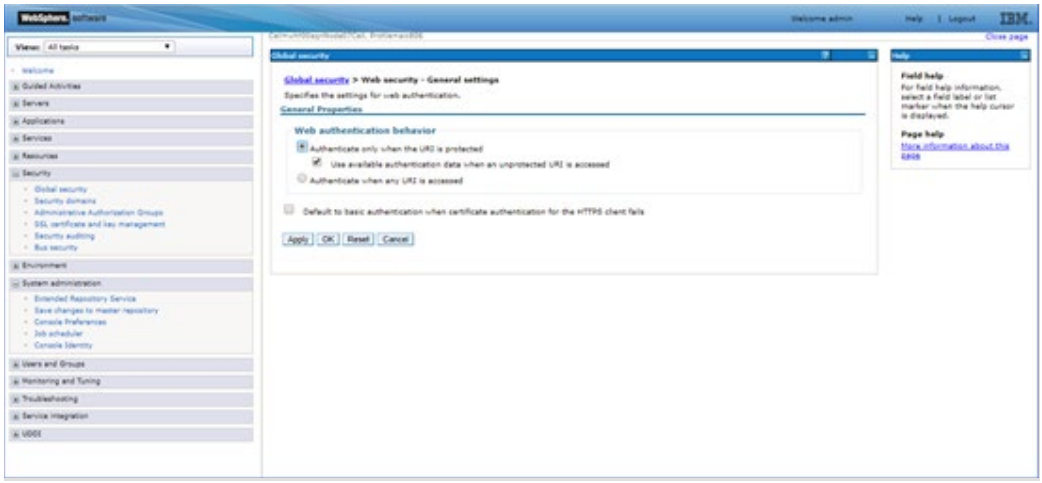
This section provides information for generic configurations required for OFSAA deployed on WebLogic server.

12.12.1 Configuring WebSphere for REST Services Authorization

Configure the following in WebSphere to enable REST API authorization by OFSAA:

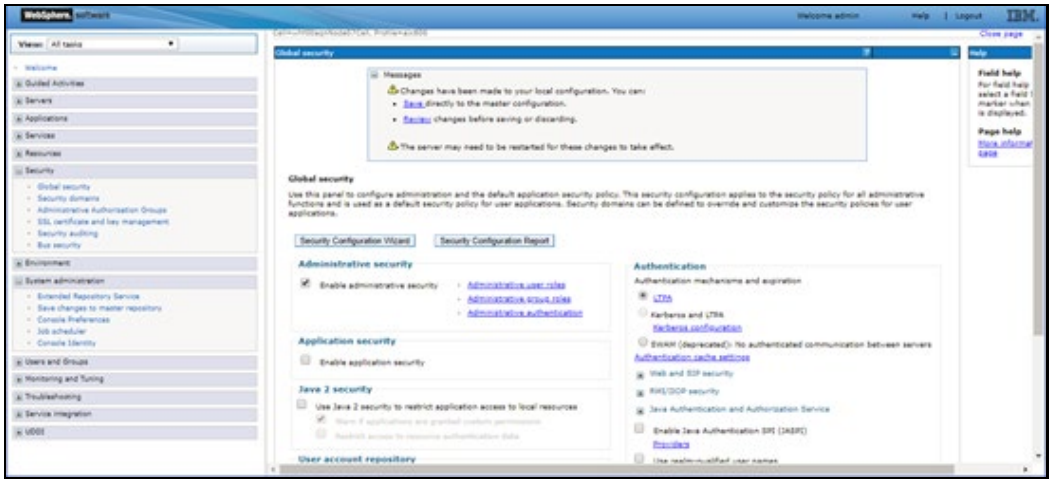
1. Log on to WebSphere console with the **User ID** provided with the admin rights.
2. Expand Security menu in the LHS and click **Global security** > **Web and SIP security** > **General settings**.

Figure 39: WebSphere REST Service Details page



3. De-select the **Use available authentication data when an unprotected URI is accessed** checkbox.
4. Click **OK.**

Figure 40: WebSphere REST Service Details page



5. Click **Save** to save the changes to master configuration.

12.13 SSO Authentication (SAML) Configuration

OFSAA can be configured as "Service Provider" using the SAML 2.0 protocol. To register OFSAA as the Service Provider, update the `sp_metadata.xml` file, which is located in the `$FIC_HOME/conf/` directory. The following options are available:

1. SAML Service Provider Metadata Configuration with Certificate
2. SAML Service Provider Metadata Configuration without Certificate

12.13.1 SAML Service Provider Metadata Configuration with Certificate

For SAML Service Provider Metadata Configuration with Certificate, update the `sp_metadata.xml` file with the X509 Certificate, which is available on the *OFSAA Configuration* window. For more information, see the section *Update General Details* in the OFS Analytical Applications Infrastructure User Guide.

The following code snippet shows the format of the tags in the XML file:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="$ENTITYID$">
  <md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:KeyDescriptor use="signing">
          <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
               <ds:X509Data>
                    <ds:X509Certificate></ds:X509Certificate>
               </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
               <ds:X509Data>
                    <ds:X509Certificate></ds:X509Certificate>
               </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
        <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="$CONSUMERSERVICEURL$" index="0"/>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="$LOGOUTSERVICEURL$"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

> **NOTE** Do not copy `----Begin Certificate----` and `----End Certificate----`. It may lead to issues during authentication.

The following code snippet is an example of the XML file with X509 Certificate values embedded in the tags:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://example.com:3333/ofsa8100">

<md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

  <md:KeyDescriptor use="signing">

    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

         <ds:X509Data>
  <ds:X509Certificate>MITFpTCCA42gAwIBAgIJAKhGKZaNnbRxMA0GCSqGSIb3DQEBCwUAMG
kxCzAJBgNVBAYTAklOMRIwEAYDVQQIDAlLYXJuYXRha2ExEjAQBgNVBAcMCUJhbmdhbG9yZTEPMA
0GA1UECgwGT3JhY2xlMQ4wDAYDVQQLDAVGU0dCVTERMA8GA1UEAwwId2hmMDBvZnMwHhcNMTkxMT
A4MDc1NzE5WhcNMjExMTA3MDc1NzE5WjBpMQswCQYDVQQGEwJJTjESMBAGA1UECAwJS2FybmF0YW
thMRIwEAYDVQQHDAlCYW5nYWxvcmUxDzANBgNVBAoMBk9yYWNsZTEOMAwGA1UECwwFRlNHQlUxET
APBgNVBAMMCHdoZjAwb2ZzMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuctabBwiZp
v0wk4fBdqXmHTNAb/3Rj+SvgVAxmL5ix09Z6bS+x26oHmxBHSY2zXlz5ArXeHzKpGgm0D/zSeSxv
s9v1SqrFxjjFakYNmzP361VptOpu53njZ+3f+WMXocHSTvOFsRRfzRfNTpvmXSiVzvKUtqgT8QgP
MHTR5MuLWDYiz3RLzTnN/rJ/oO4+2fQmOeo9GRkeO41SAI+SPDnOSMjycGq7rlmqnJCAfV4OVJ2w
SfuQLieNkfJUWINEiF7UT+/5IlSHjlpo6YJRVMXT51KD6Rx3i31FEzJaTaWJoDA2C7YA6xs7DYfr
bTenPKxwtue99stJDoeMKS8cGG8UK8N12BvlaLraaasmr/cDdBV89VRoP+6eDQEwhXHT834ruZ6o
M0p+TzyHztYNur9BJKtMqGlzyX+wGMGu9FFjLu5pxwtJw1qxMv9ti35yLMVUVOYAjMSHtqj+I9d1
zBLNOQMs4sPxzIZgmGMuZ0TM4kgsSNl4LuAPbFw4wDG4Q/oJYBiBMifzPC3OytYjcDTqNtl5i40i
MLMbw0bLWqFW39z0GhrNoCko6DcLTRLLtB1ERw/AmGKBdP8T66kz7hEy9C/SkyP+75qJxhjEDMN2
Ha+wwrrat3Yg+H+n7OM+xJJScerK3ZiiqkEGCA69gjvaCBKp/v/pEL/wepHZV6aGECAwEAAaNQME
4wHQYDVR0OBBYEFEi7rT1QIjudl3jn6UTRP4sw9CzeMB8GA1UdIwQYMBaAFEi7rT1QIjudl3jn6U
TRP4sw9CzeMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggIBADeHLz7k3/iOessnp8dRei
GGpf+fIzib+whbUcaVMrNzGk86WQb8zNXGExcZV3RX9l35zW2hDwQUDpdl25lHpvDTo4xIvBOMi4
P49rz0SMVYiXVAPY7sy+cidjmcATI4UXxeGD3g+gvzv3z9l6Mg19ivits5BFUksIHMY+rgMewj2+
ovSeo8RJd8rjeG7z7JDKlOj1PUPfjpEB9nY+V6tTuqYopcJU6ln3zyN4ngcrJEahY15jeRBzkdzA
QRoIRnEjFEob6lCxdkciupl2IdOz6c2kkYQnMcDjyT8jfMQffFMAV/rcE6RS+w4+Ear0/q3svukG
YpZnpGpEdxhIV4uo0TwSZo6cE1cj1LGRPNYP/2Cfd6Gp1qJBUxrFKjYx1v9c0KJEnGVUuhNRKxcP
facHloJmNHS5Z2xVQrY+eBSuR+TtKTaio9FWigU3Nx6v1LkbvC7265N38Is3Gkhk5KbN+G4Xet6T
X3LcRx0MDqfRfZT3Q+7elFFEunxeBaXg6OaTKbxhHtskgAi1+4z/acrYKC/yjNn8F7qJNkhsFovV
HwqPItx517XZzsNjVcp3V+oFfPZdw6MQtp7zSqB+GnM52OrT77X3hGe7+B+PpTARueth2trsiNag
qrumAKV8DdtS0Q4XCQ++mmKmm8n/5Epq10Sagbf1D46q+iawIgZf1E</ds:X509Certificate>

         </ds:X509Data>

    </ds:KeyInfo>

  </md:KeyDescriptor>

  <md:KeyDescriptor use="encryption">

    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

         <ds:X509Data>
<ds:X509Certificate>MITFpTCCA42gAwIBAgIJAKhGKZaNnbRxMA0GCSqGSIb3DQEBCwUAMGkx
CzAJBgNVBAYTAklOMRIwEAYDVQQIDAlLYXJuYXRha2ExEjAQBgNVBAcMCUJhbmdhbG9yZTEPMA0G
A1UECgwGT3JhY2xlMQ4wDAYDVQQLDAVGU0dCVTERMA8GA1UEAwwId2hmMDBvZnMwHhcNMTkxMTA4
MDc1NzE5WhcNMjExMTA3MDc1NzE5WjBpMQswCQYDVQQGEwJJTjESMBAGA1UECAwJS2FybmF0YWth
MRIwEAYDVQQHDAlCYW5nYWxvcmUxDzANBgNVBAoMBk9yYWNsZTEOMAwGA1UECwwFRlNHQlUxETAP
BgNVBAMMCHdoZjAwb2ZzMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuctabBwiZpv0
wk4fBdqXmHTNAb/3Rj+SvgVAxmL5ix09Z6bS+x26oHmxBHSY2zXlz5ArXeHzKpGgm0D/zSeSxvs9
v1SqrFxjjFakYNmzP361VptOpu53njZ+3f+WMXocHSTvOFsRRfzRfNTpvmXSiVzvKUtqgT8QgPMH
```

```
TR5MuLWDYiz3RLzTnN/rJ/oO4+2fQmOeo9GRkeO41SAI+SPDnOSMjycGq7rlmqnJCAfV4OVJ2wSf
uQLieNkfJUWINEiF7UT+/5IlSHjlpo6YJRVMXT51KD6Rx3i31FEzJaTaWJoDA2C7YA6xs7DYfrbT
enPKxwtue99stJDoeMKS8cGG8UK8N12BvlaLraaasmr/cDdBV89VRoP+6eDQEwhXHT834ruZ6oM0
p+TzyHztYNur9BJKtMqGlzyX+wGMGu9FFjLu5pxwtJw1qxMv9ti35yLMVUVOYAjMSHtqj+I9d1zB
LNOQMs4sPxzIZgmGMuZ0TM4kgsSNl4LuAPbFw4wDG4Q/oJYBiBMifzPC3OytYjcDTqNtl5i40iML
Mbw0bLWqFW39z0GhrNoCko6DcLTRLLtB1ERw/AmGKBdP8T66kz7hEy9C/SkyP+75qJxhjEDMN2Ha
+wwrrat3Yg+H+n7OM+xJJScerK3ZiiqkEGCA69gjvaCBKp/v/pEL/wepHZV6aGECAwEAAaNQME4w
HQYDVR0OBBYEFEi7rT1QIjudl3jn6UTRP4sw9CzeMB8GA1UdIwQYMBaAFEi7rT1QIjudl3jn6UTR
P4sw9CzeMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggIBADeHLz7k3/iOessnp8dReiGG
pf+fIzib+whbUcaVMrNzGk86WQb8zNXGExcZV3RX9l35zW2hDwQUDpdl25lHpvDTo4xIvBOMi4P4
9rz0SMVYiXVAPY7sy+cidjmcATI4UXxeGD3g+gvzv3z9l6Mg19ivits5BFUksIHMY+rgMewj2+ov
Seo8RJd8rjeG7z7JDKlOj1PUPfjpEB9nY+V6tTuqYopcJU6ln3zyN4ngcrJEahY15jeRBzkdzAQR
oIRnEjFEob6lCxdkciupl2IdOz6c2kkYQnMcDjyT8jfMQffFMAV/rcE6RS+w4+Ear0/q3svukGYp
ZnpGpEdxhIV4uo0TwSZo6cE1cj1LGRPNYP/2Cfd6Gp1qJBUxrFKjYx1v9c0KJEnGVUuhNRKxcPfa
cHloJmNHS5Z2xVQrY+eBSuR+TtKTaio9FWigU3Nx6v1LkbvC7265N38Is3Gkhk5KbN+G4Xet6TX3
LcRx0MDqfRfZT3Q+7elFFEunxeBaXg6OaTKbxhHtskgAi1+4z/acrYKC/yjNn8F7qJNkhsFovVHw
qPItx517XZzsNjVcp3V+oFfPZdw6MQtp7zSqB+GnM52OrT77X3hGe7+B+PpTARueth2trsiNagqr
umAKV8DdtS0Q4XCQ++mmKmm8n/5Epq10Sagbf1D46q+iawIgZf1E</ds:X509Certificate>
         </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
        <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://example.com:3333/ofsa8100/login.jsp" index="0"/>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://example.com:3333/ofsa8100/signoff.jsp"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

After updating the file, upload it to the **Trusted Providers** table under **Identity Federation** in the Identity Manager application.

12.13.2 SAML Service Provider Metadata Configuration without Certificate

For SAML Service Provider Metadata Configuration without Certificate, update the following information in the `sp_metadata.xml` file:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="$ENTITYID$">
   <md:SPSSODescriptor
   protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
        format:unspecified</md:NameIDFormat>
```

```
            <md:AssertionConsumerService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="$CONSUMERSERVICEURL$" index="0"/>

            <md:SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="$LOGOUTSERVICEURL$"/>

        </md:SPSSODescriptor>
</md:EntityDescriptor>
```

- `$ENTITYID$` - OFSAAI URL till context name.

  For example, `http(s)://hostname:port/<context>`

- `$CONSUMERSERVICEURL$` - OFSAAI login URL

  For example, `http(s)://hostname:port/<context>/login.jsp`

- `$LOGOUTSERVICEURL$` - OFSAAI logout URL

  For example: `http(s)://hostname:port//signoff.jsp`

OFSAA generated SAMLRequest is unsigned and sent to "Identity Provider (IdP)" using "HTTP Redirect" method. "Identity Provider (IdP)" sends back SAMLResponse using "HTTP POST" method. Authenticated user can be sent as one of the attributes (e.g. "uid") in SAMLResponse or in "Subject".

If user is sent in attribute, same user attribute has to be specified in "SAML User Attribute" in OFSAA Configuration screen.

If user is sent in subject, then NameID format in SAML response should be "`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`".

12.14 System For Cross-Domain Identity Management (SCIM)

The System for Cross-domain Identity Management (SCIM) simplifies the process of managing user identities in On-Premise applications and services. This system can use the existing schemas and deployments and utilize the existing authentication, authorization, and privacy models. This helps to reduce the cost and complexity of user management operations as it consumes a common user schema and extension model, as well as links the documents to provide patterns for exchanging this schema using standard protocols.

> **NOTE** The SCIM configuration applies only to Oracle IAM (SaaS) and does not apply to other SCIM software applications. For other SCIM software/SaaS applications, refer to respective documentation.

12.14.1 Prerequisites

- Ensure to have an environment with OFSAA version 8.1.2.3.0 with one off **36029065**. Refer to My Oracle Support, to install the one-off patch.

- Disable JIT Unmapping Operation and JIT Provisioning in OFSAA. For more information, refer to **Update General Details** in Oracle Financial Services Analytical Applications Infrastructure User Guide.
- All the groups created in OFSAA must also be created in Oracle IAM. Generate `groups.csv` file by executing the IDCS command line utility:
  a. Navigate to `$FIC_HOME/utility/IDCS_Utility` directory.
  b. Execute `IDCSUtility.sh` (UNIX)in the following format:

```
./IDCSUtility.sh
http://<OFSAA_Webserver_IP>:<SERVLET_PORT>/<Context_name> SYSADMN
<password>
```

  The groups.csv file is saved in the `$FIC_HOME/utility/IDCS_Utility/` directory.
  c. Click **Groups** > **More actions** > **Import Groups** in Oracle IAM, to import the `groups.csv` file to Oracle IAM, using Import CSV option.

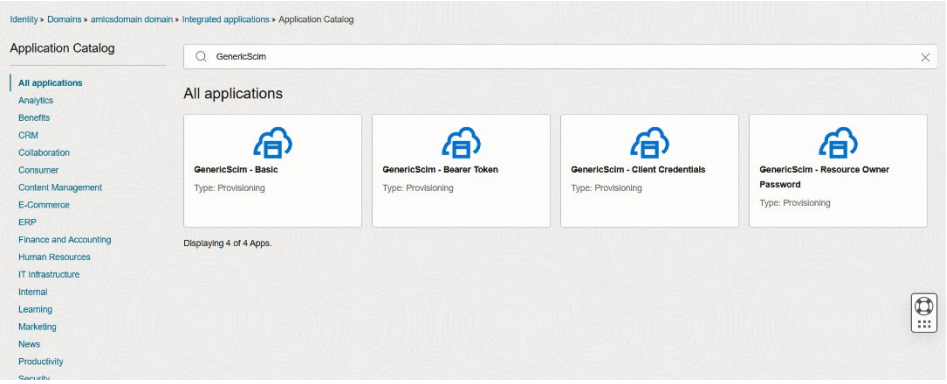
12.14.2 Create Generic SCIM application in Oracle IAM

You can use the following SCIM applications:

- GenericScim - Basic : uses user credentials
- GenericScim - Bearer Token : uses Token generated from OFSAA application. To create a token, refer to **Creating the Instance Access Token** in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

To create GenericScim basic application:

1. Click **Integrated Application** > **Add Application** > **Application Catalog**, to access the list of applications present in Oracle IAM.



2. Select **GenericScim – Basic**, in IAM console.
3. Select **Configure Provisioning** > **Enable provisioning** option and enter the following details:
   - **Hostname** : `<OFSAA_Webserver_IP>`
   - **Base URL** : /<context_name>/rest-api/v1/scim
   - **Adminstrator Username** : SYSADMN
   - **Administrator Password** : <password>

4. Perform the Test Connectivity:

   a. For Weblogic WebServer:

      Set the `enforce-valid-basic-auth-credentials` flag to `False`, in `/domains/{weblogic_domain_name}/config/config.xml` file within the `<security-configuration>` tag:

      ```
      <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
      ```

      After setting the flag, restart all the servers in the domain.

   b. If your OFSAA application is not HTTPS and Port is not 443, execute the following PATCH request:

      ```
      URL: {{IDCS-HOST}}/admin/v1/Apps/{{SCIM-APP-ID}}

      Authorization : OAuth 2.0 [Client-Credentials]

      Json_body : {
        "schemas": [
          "urn:ietf:params:scim:api:messages:2.0:PatchOp"
        ],
        "Operations": [
           {
            "op": "replace",
            "path":
      "urn:ietf:params:scim:schemas:oracle:idcs:extension:managedapp:App:bundleConfigurationProperties[name eq \"sslEnabled\"].value",
            "value": [ "false"] --false, if OFSAA runs on HTTP
          },
           {
            "op": "replace",
            "path":
      "urn:ietf:params:scim:schemas:oracle:idcs:extension:managedapp:App:bundleConfigurationProperties[name eq \"port\"].value",
            "value": [ "4488"] --WebServer Port of OFSAA application
          }
        ]
      }
      ```

5. Click **Test Connectivity**. A confirmation message is displayed when the connection is established successfully.
6. Select **Configure Attribute Mapping** and use the default values.
7. Select Provisioning Operations and enable all options except Authoritative sync.
8. **Enable Synchronization** option, to synchronize the users and groups present in OFSAA to Oracle IAM.

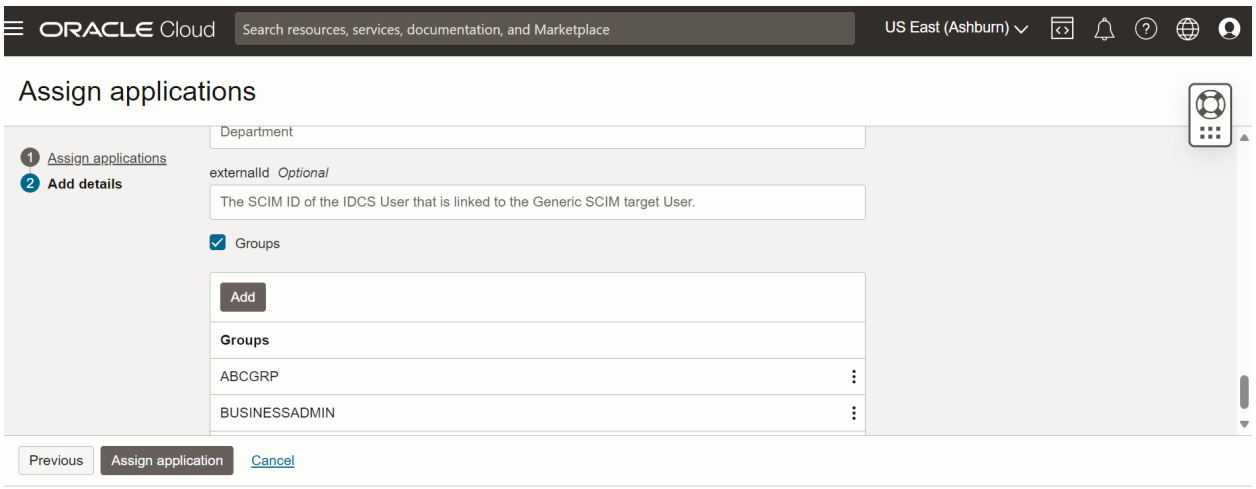
9. Select **Configure synchronization**, and select the following details:
   - **User identifier** : Username
   - **Application identifier** : name
   - **When exact match is found** : Link and Confirm
   - **Synchronization Schedule** : Never [If required, schedule it]
10. Click **Save Changes** and activate the application.

Refer to Use the SCIM Interface to Integrate Oracle Identity Cloud Service with Custom Applications for more information.

12.14.3 Assign Groups from Oracle IAM to the existing groups in OFSAA

It is recommended to have the groups from Oracle IAM assigned to the same group in OFSAA.

1. Navigate to the group to be assigned and select **Integrated Application**.
2. Click **Assign application** and select **SCIM application**.
3. In the **Add Details** page goto **Groups** and add all the OFSAA groups to be mapped with ORACLE IAM groups.
4. Click **OK**.

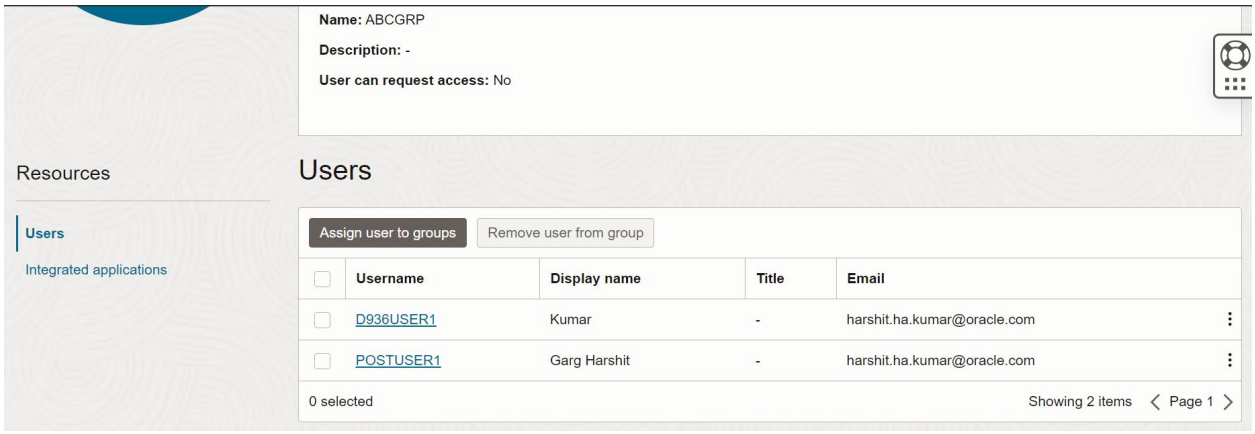


12.14.4 User - User Group Mapping in Oracle IAM

All the users mapped with the Oracle IAM group, will be created in OFSAA application along with group mapping. It is recommended to manage users from the groups, which are already mapped to SCIM application.

To map users with the Oracle IAM group:

1. Navigate to the group to be mapped and select **Users**.
2. Click **Assign users to groups**. Select the required user.
3. Login with this user to OFSAA application.

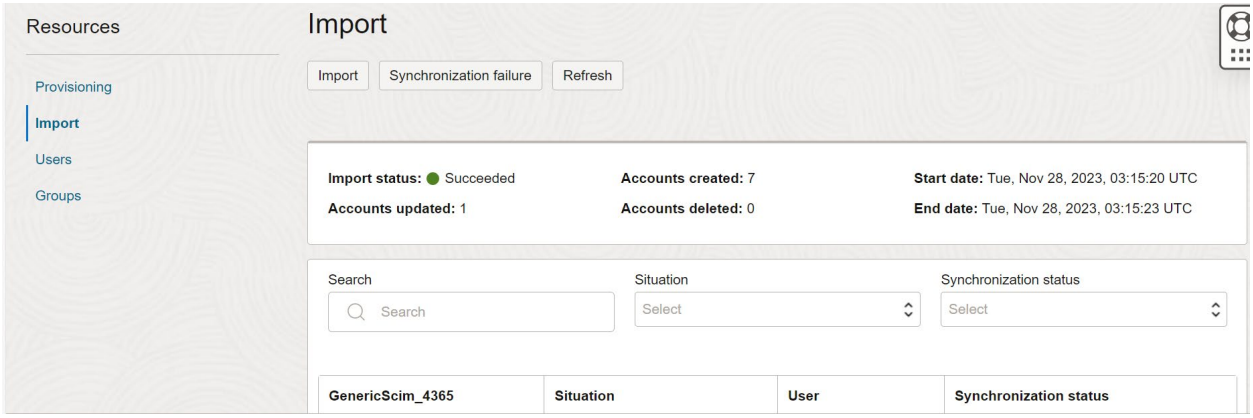


12.14.5 Synch Users from OFSAA to Oracle IAM

Sync the users manually, if users are already created in OFSAA and needs to be synced in Oracle IAM.

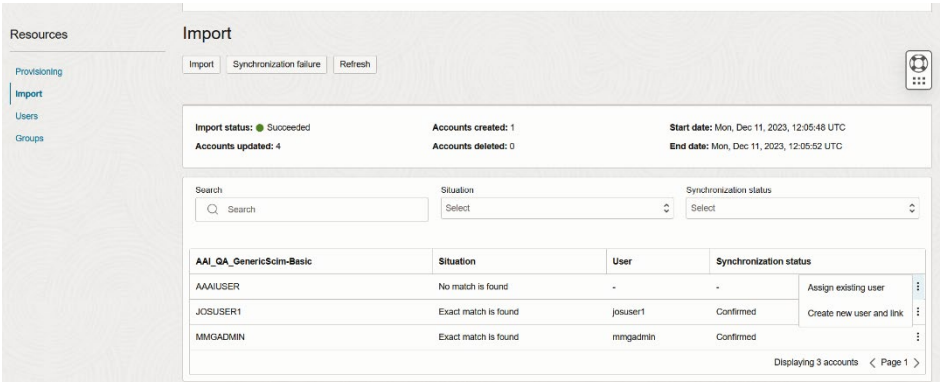
To sync the users:

1. Navigate to your SCIM application and go to **Import** tab.



2. Click **Import** to fetch all the users to Oracle IAM.
3. Click **Refresh**, to check the import status of all the users.

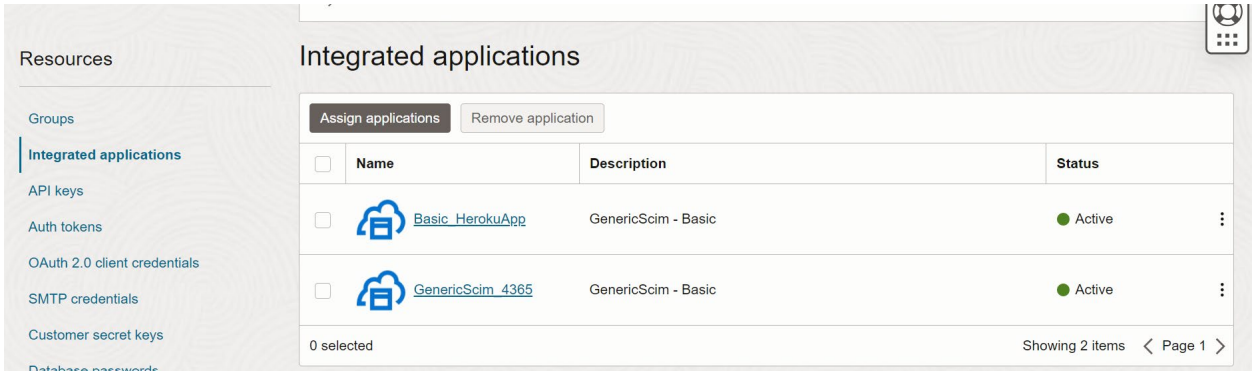
   All the existing users in Oracle IAM will be mapped with the users in OFSAA and the remaining ones can be manually created and linked with them.



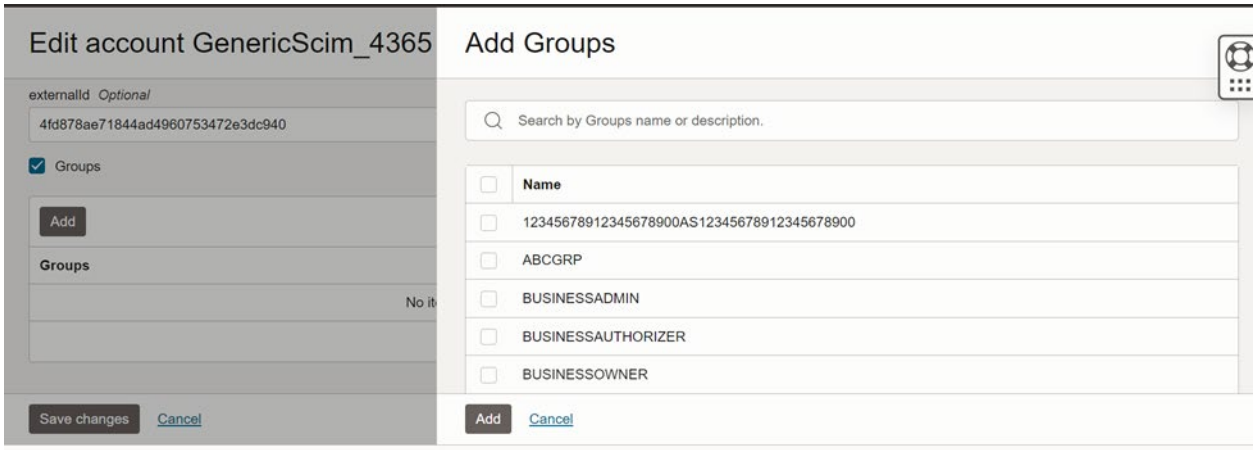
12.14.6 Create Users

Complete the following steps, to create users in IAM console.

1. Navigate to **User** and open **Integrated application**s tab.



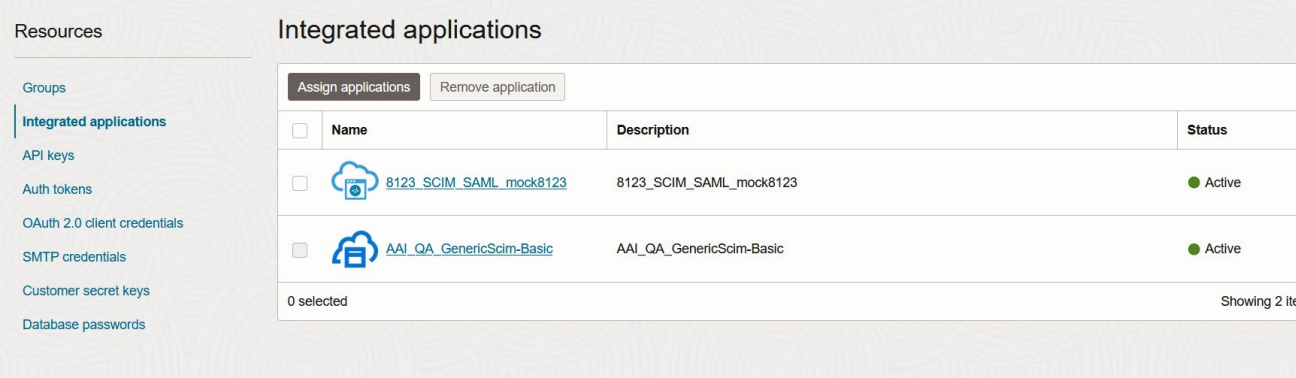
2. Click **Assign Application** and select the Generic SCIM Application.
3. Proceed with mapping the OFSAA groups.



12.14.7 Modify Users

To modify the users using SCIM application, in Oracle IAM console:

1. Navigate to the users to be modified and click **Integrated application**s.
2. Click **Options** (three dots) of the SCIM application and click **Edit**.

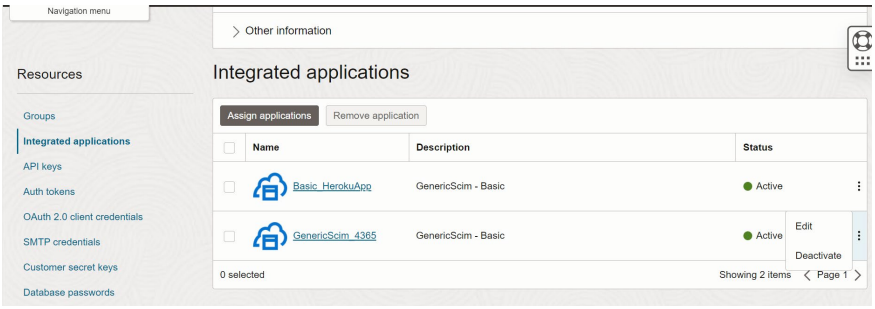


12.14.8 Enable/Disable Users

You can enable/disable users using SCIM application, in Oracle IAM console.

1. Navigate to a user to be enabled/disabled and select **Integrated Application**.
2. Click **Options** (three dots) and click **Activate/Deactivate** to enable/disable the specific user.

   SYSAUTH action is NOT required in OFSAA again to authorize the enabled/disabled user.



   The user status is also updated in OFSAA. You can verify the user status in the **Identity Management**.

12.14.9 Delete Users

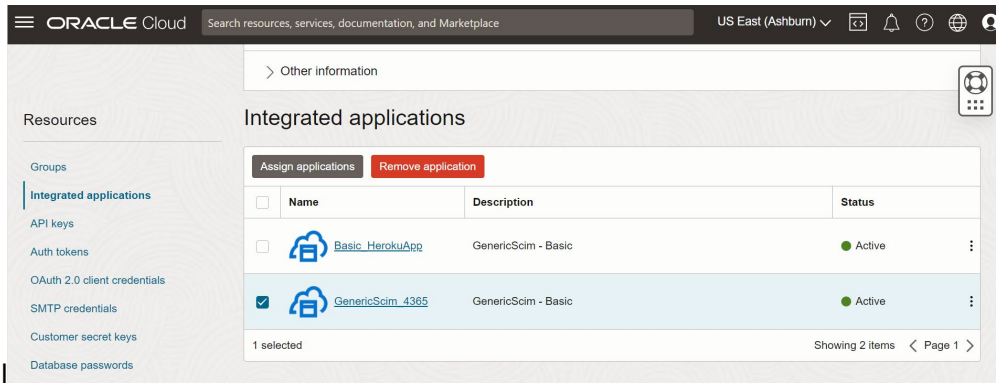
To delete users in Oracle IAM console, using SCIM application:

1. Navigate to user to be deleted and select **Integrated Application**.
2. Select the SCIM application and click on remove application button.

   SYSAUTH action is NOT required in OFSAA again to authorize the deleted user.

   To verify, go to **OFSAA > User Maintenance > User**, and the deleted user is removed from user list.

   To access the list of deleted users, go to **OFSAA > User Reinstate**.



12.15 Public Key Authentication

This section is meant for users who want to configure Public Key Authentication for OFSAAI on UNIX machine.

12.15.1 Prerequisite

You have a working SSH server and client installed.

12.15.2 Setting Up Public Key Authentication on Client Server

Setting up public key authentication to access a particular remote host is a one-time procedure comprising of three steps.

Step 1: Generate a public/private key pair on your webserver.

Use the `ssh-keygen` command to generate public/private key pair. The key-type flag -t is mandatory, accepting either "rsa" or "dsa" as an argument. In the example given, the -f option is also used to override the default name and location for the resulting private-key file.

When prompted for a passphrase, you can enter appropriate phrase or keep it empty.

```
$ ssh-keygen -t dsa -f ./<KEY_NAME>
```

The command produces two text files in current folder: The `<KEY_NAME>` folder contains the private key, and `<KEY_NAME>.pub` folder contains the public key. The private key must be kept secret. Accordingly, access to private key is restricted to the file owner and its contents are encrypted using the passphrase.

You can recreate `<KEY_NAME>.pub` from `<KEY_NAME>` by executing the following command:

```
$ ssh-keygen -y -f ./<KEY_NAME> > <KEY_NAME>.pub
```

Step 2: Install the public key on the remote host to which you want to connect.

1. Copy `mykey.pub` to your home directory on the remote host and append its contents to the `authorized_keys` file in the `.ssh` directory. If authorized_keys file is not present in `.ssh` directory, you can create it manually by executing the following command:

   ```
   $ scp <key_name>.pub <remote_user>@<remote_host>:<Remote_PATH>
   ```

   Here, <remote_host> is the IP address of the remote server.<remote_user> is the user name of the <remote_host> to which you want to connect.

2. Login to remote host by executing the following command:

   ```
   $ ssh -l <remote_user> <remote_host>
   ```

3. Append public key by executing the command on remote host (Server) to append public key.

   ```
   $ cat <KEY_NAME>.pub >> $HOME/.ssh/authorized_keys
   ```

   For example :

   ```
   $ cat ofsa.pub >> $HOME/.ssh/authorized_keys
   ```

   The private key is not installed on any remote host.

> **NOTE** Set the following permissions on App Server:
>
> ```
> $ chmod –R 755 <remote_user_home>
> $ chmod 700 .ssh
> $ chmod 755 authorized_keys
> ```

> **NOTE** Set the following permissions required on Web Server:
>
> ```
> $ chmod 600 <PRIVATE_KEY>
> ```

Step 3: Verify whether Public Key authentication works from Web Server

Public Key authentication is invoked by using the -i flag with the ssh command, specifying <PRIVATE_KEY_PATH> as the flag's argument.

Execute the following command from Web Server to check remote App Server:

```
$ ssh -x -l <REMOTE_USER> -i <PRIVATE_KEY_PATH> <REMOTE_HOST>
```

For example :

```
$ ssh -x -l ofsaaweb -i
/scratch/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/AAIAKG/M
YKey/ofsa whf00akg
```

<PRIVATE_KEY_PATH> is the fully qualified name of the private key file.

> **NOTE** If you see a password prompt instead of a passphrase prompt, the administrators of the remote host may have disallowed public key authentication.

12.15.3 Other SSH Software

Refer the documentation of SSH software for Configuration of Public Key Authentication.

If you want to use Public Key authentication on other SSH software such as Tectia, you have to convert private key file to OpenSSH format.

> **NOTE** You can use Tectia SSH if your application server and web server are running on the same machine. However, if they are on separate machines, you have to convert the private key file to OpenSSH format.

Use the following command to convert private key to OpenSSH format:

`ssh-keygen -i -f [filename]` (key must be unencrypted)

If key is encrypted, perform the following steps:

1. Convert private key to OpenSSH format.
2. Change passphrase using the following OpenSSH command:

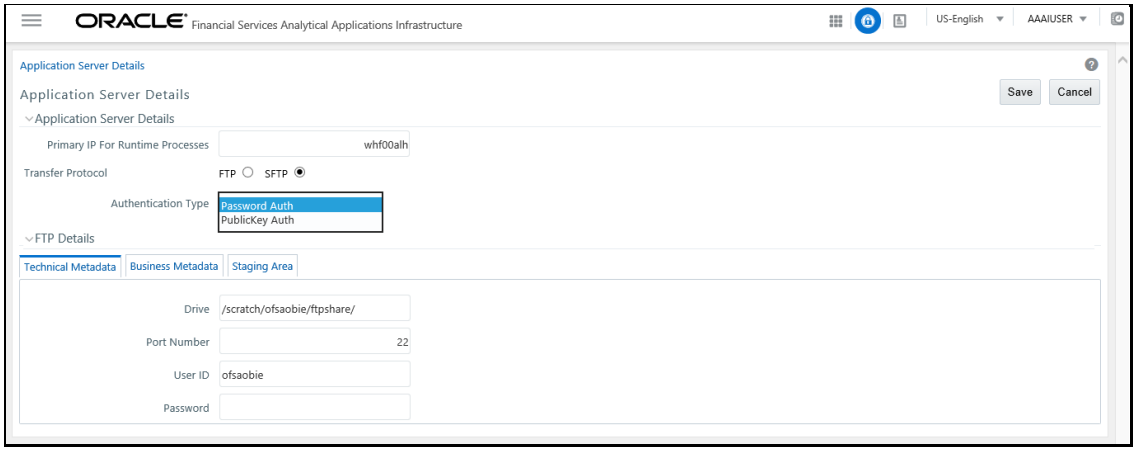
   `$ ssh-keygen -f <PRIVATE_KEY_PATH> -p`

   `<private_key_path>` refers to path where private key is located including private key name.

12.15.4 Configurations Required in OFSAA Setup

1. Login to OFSAA with your system administrator credentials.
2. Click  from the header to display the administration tools in a Tiles menu.
3. Click **System Configuration** to view the menu.
4. Click **Configure Application Server** from the menu to view the *Application Server Details* window.
5. In the *Application Server Details* window, click **Modify**.

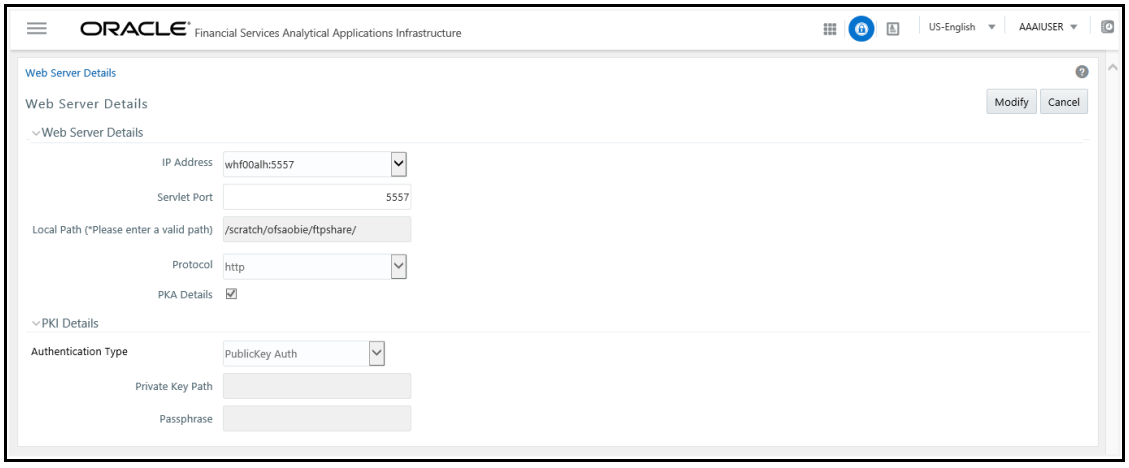
Figure 41: Application Server Details page



6. Select **Authentication Type** as **Publickey Auth.**
7. Click **Save**.

8. A confirmation message is displayed to inform that you need to provide the PKI details in the *Web Server Details* window. Click **OK**.
9. Click **Hamburger Icon** to view the Navigation list.
10. Click **Configure Web Server** from the Application Navigation Drawer. The *Web Server Details* window is displayed.

Figure 42: Web Server Details page



If you have selected **Authentication Type** as **Public Key Auth** in the *Application Server Details* window, the **PKA Details** check box gets automatically selected and the *PKI Details* pane is displayed.

11. Click **Modify**.
12. Enter **Private Key Path** and **Passphrase** which you created during Step 1 (Generate a public/private key pair on your webserver).
13. Click **Save**.

12.16 Enable and Disable Users

The users with System Administrator (sysadmn) and System Authorizer (sysauth) functional roles can be enabled or disabled using the command line prompt. Only users with the requisite administrator role to perform this action can disable or enable users with sysadmn and sysauth roles.

12.16.1 Prerequisites

The following prerequisites must be met before you proceed with the password reset:

- Check if the Authentication Type selected is **SMS Authentication & Authorization**. Enabling and disabling users does not work for other authentication types. For more details, see the information on **Authentication Type** field in the **Configuration** subsection in **System Configuration** in the OFS Analytical Applications Infrastructure User Guide.
- Check if Security Questions are enabled and configured. For more details, see the information on **Security Questions Enable** field in the **Configuration** subsection in **System Configuration** the OFS Analytical Applications Infrastructure User Guide.

12.16.2 Enabling or Disabling Users with System Administrator and System Authorizer Roles

Perform the following procedure to enable or disable a sysadmn or sysauth user:

1. Open the Command Prompt window and go to the folder `FIC_HOME/utility/useraction/bin`.
2. Execute the following command:

   ```
   ./useraction.sh <ACTION ON USER> <OPERATION>
   ```

   For example:

   To disable a user:

   ```
   ./useraction.sh johnsmith disableuser
   ```

   To enable a user:

   ```
   ./useraction.sh johnsmith enableuser
   ```

3. A prompt (**Please Enter Action by User**) appears, which requires that you enter your User Id. Your User ID must have the requisite role with permissions to perform the enable or disable action. Enter the User ID and the three questions for authentication appear. Enter the correct answers to complete the password reset.
4. To enable or disable the users with the Sysadmn or the Sysauth users by skipping the 3 security questions, use the following command.

   ```
   ./useraction.sh <usr_ID> ENABLEUSER/DISABLEUSER SYSADMN N/Y
   ```

   - Usr_ID – the user who needs to be enabled/disabled.
   - The user is prompted to answer the security questions if the 4th parameter is set to Y.

Note: This feature is available with versions v8113+, v8121+one-off[35073367], v8122+

12.17 Password Reset

The password for users can be reset from the command prompt. Only users with the requisite administrator role can perform this action.

12.17.1 Prerequisites

The following prerequisites must be met before you proceed with the password reset:

- Check if the Authentication Type selected is **SMS Authentication & Authorization**. Password reset does not work for other authentication types. For more details, see the information on **Authentication Type** field in the **Configuration** subsection in **System Configuration** in the OFS Analytical Applications Infrastructure User Guide.
- Check if Security Questions are enabled and configured. For more details, see the information on **Security Questions Enable** field in the **Configuration** subsection in **System Configuration** in the OFS Analytical Applications Infrastructure User Guide.

12.17.2 Resetting a User Password

Perform the following procedure to reset the password for a user:

1. Open the Command Prompt window and go to the folder `FIC_HOME/utility/userpasswdreset/bin`.
2. Execute the following command:

   `./resetpass.sh <ACTION ON USER> <ACTION TAKEN BY USER> N <NEW PASSWORD>`

   For example:

   `./resetpass.sh johnsmith sysadmn N password1`
3. A prompt (**Please Enter Action by User**) appears, which requires that you enter your User Id. Your User ID must have the requisite role with permissions to perform the password reset action. Enter the User ID to display the three questions for authentication. Enter the correct answers to complete the password reset.

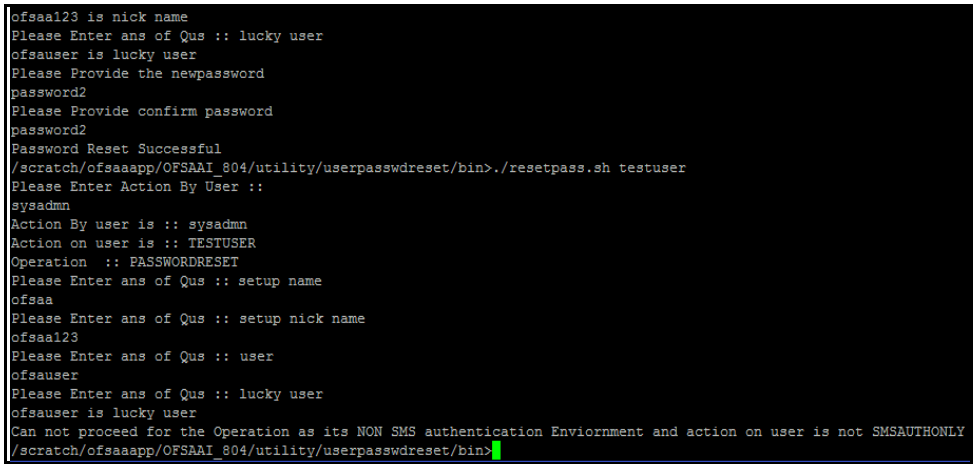
   The following illustration displays a password reset on the command prompt that was successful:

Figure 43: Password Reset command

```
/scratch/ofsaaapp/OFSAAI_804/utility/userpasswdreset/bin>./resetpass.sh testuser
Please Enter Action By User ::
sysadmn
Action By user is :: sysadmn
Action on user is :: TESTUSER
Operation  :: PASSWORDRESET
Please Enter ans of Qus :: my setup name
my setup name is ofsaa
Please Enter ans of Qus :: setup name
ofsaa
Please Enter ans of Qus :: setup nick name
ofsaa123
Please Enter ans of Qus :: user
ofsauser
Please Provide confirm password
password2
Password Reset Successful
/scratch/ofsaaapp/OFSAAI_804/utility/userpasswdreset/bin>./resetpass.sh testuser
Please Enter Action By User ::
sysadmn
Action By user is :: sysadmn
```

The following illustration displays a password reset that was not successful since the environment did not meet the authentication type prerequisite - SMS Authentication and Authorization:

Figure 44: Password Reset - Not successful



12.18 Configuring OFSAA OIM Connector

OFSAA OIM Connector is used for provisioning users in the Oracle Financial Services Analytical Applications (OFSAA) from Oracle Identity Manager (OIM). For information on OIM, see http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-098451.html.

This section provides information to configure the OFSAA Connector with OIM. The connector supports OIM versions 11.1.2.2 and 11.1.2.3 on WebLogic Server. This section also provides information on configuring Entitlements.

12.18.1 Knowing the Prerequisites

The following are the prerequisites for this configuration:

- You must have the user credentials with which you installed IDM Suite.
- You must have the host information for OIM and OFSAA server(s).

12.18.2 Configuring the Connector

This section provides information to configure the OFSAA Connector with OIM that enables mapping of policies from OFSAA and user configuration.

The following steps describe the procedure to configure the OFSAA OIM Connector:

1. Login to the OFSAA host with your OFSAA user credentials.
   a. Navigate to `$FIC_HOME/utility` folder.
   b. Copy the `OFSConnector` directory to your local system.
2. Login to the OIM host with OIM user credentials.
3. Copy the `OFSConnector` directory from your local system to `$OIM_ORACLE_HOME/connectors`.
4. Check and ensure that the following environment variables are set in the OIM host:

   ```
   JAVA_HOME= <Path to Java Dir>
   ```

For example, `/u01/java/jdk1.7.0_91`

`MW_HOME=<Middleware Home Path>`

For example, `/u01/oracle/products/fmw/10.3.6`

`WL_HOME=<Weblogic Home Dir>`

For example, `$MW_HOME/wlserver_10.3`

`LD_LIBRARY_PATH=<Webtier lib path>`

For example, `/u01/oracle/products/fmw/Oracle_WT1/lib`

`APP_SERVER=<App server>`

For example, `weblogic/websphere`

`OIM_ORACLE_HOME=< OIM install dir>`

For example, `/u01/oracle/products/fmw/10.3.6/Oracle_IDM`

`DOMAIN_HOME=<OIM Domain path>`

For example, `/u01/oracle/domains/idm_domain`

`ANT_HOME=<Ant Home>`

For example, `$MW_HOME/modules/org.apache.ant_1.7.1`

`PATH=$JAVA_HOME/bin:$ANT_HOME/bin:$PATH:$OIM_ORACLE_HOME/OPatch`

5. Generate `wlfullclient.jar` by using the following procedure:
   a. Navigate to the `$DOMAIN_HOME/bin` directory and run the following command: `./setDomainEnv.sh`
   b. Navigate to the `$WL_HOME/server/lib` directory and run the following command: `java -jar wljarbuilder.jar`
   c. Copy the newly created `wlfullclient.jar` from `$WL_HOME/server/lib` to the path `$OIM_ORACLE_HOME/designconsole/ext`.
6. Execute the following command from the `$OIM_ORACLE_HOME/server/bin` directory to upload the OFSAA connector to OIM:

```
sh UploadJars.sh -username << Xellerate admin username>> -password <<
admin password>> -serverURL << serverURL>> -ctxFactory << context>> -
ICFBundle <<Full path of OFS connector>>
```

For example,

```
sh UploadJars.sh -username xelsysadm -password Welcome1 -serverURL
t3://whf00aum:14000 -ctxFactory weblogic.jndi.WLInitialContextFactory -
ICFBundle
/scratch/software/weblogic10.3.6/iam/connectors/OFSConnector/org.identi
tyconnectors.ofs-1.0.0.jar
```

NOTE `ctxFactory` value is `weblogic.jndi.WLInitialContextFactory` for WebLogic and `com.ibm.websphere.naming.WsnInitialContextFactory` for WebSphere.

7. Navigate to the `$OIM_ORACLE_HOME/server/plugin_utility` directory and set the following values in the `ant.properties` file:

   ```
   wls.home=<Path to WebLogic Server Dir>
   ```

   For example, `/u01/oracle/products/fmw/10.3.6/wlserver_10.3`

   ```
   oim.home=<OIM Home Path>
   ```

   For example, `/u01/oracle/products/fmw/10.3.6/Oracle_IDM/server`

   ```
   login.config=<Login Configuration File Home Path>
   ```

   For example, `${oim.home}/config/authwl.conf`

   ```
   mw.home=<Middleware Home Path>
   ```

   For example, `/u01/oracle/products/fmw/10.3.6`

8. Execute the following command from the `$OIM_ORACLE_HOME/connectors/OFSConnector/` directory and upload the schedule task in OIM:

   ```
   sh deploySchTask.sh -username << Xellerate admin username>> -password
   << admin password>> -serverURL <<oim_server_url>> -id <<OFSAA_ID>>
   ```

9. Upload the OFSAA Connector metadata to OIM by executing the following command from the `$OIM_ORACLE_HOME/connectors/OFSConnector` directory:

   ```
   sh ImportMetadata.sh <xellerate admin username> <admin password>
   <oim_server_url> OFS-ConnectorConfig_<OIM_VERSION>.xml <OFSAA_ID>
   <OFS_USER> <OFS_PASSWD> <OFS_URL>
   ```

> **NOTE** For SSO, <OFS_USER > is a valid OIM user. If the setup is non-SSO, then <OFS_USER> is SYSADMN.
> Based on the OIM version 11.1.2.2 or 11.1.2.3, select the appropriate version of the files to upload.

   If the file upload from the shell script is successful, the following message is printed:
   `File imported successfully: OFS-ConnectorConfig_11.1.2.2.xml`

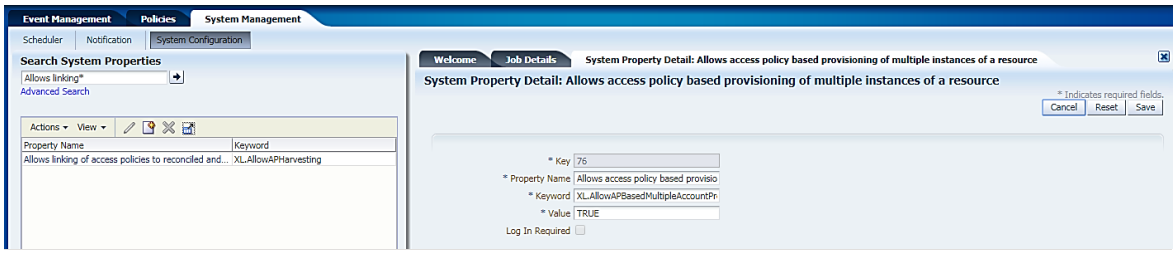
10. For other OFSAA environments such as DEV, UAT and PROD, use the following command to create IT Resource and Access Policy:

    ```
    sh ImportMetadata.sh <xellerate admin username> <admin password>
    <oim_server_url> OFS-ITResource_<OIM_VERSION>.xml <OFSAA_ID> <OFS_USER>
    <OFS_PASSWD> <OFS_URL>
    ```

> **NOTE**
> - For SSO, <OFS_USER > is a valid OIM user. If the setup is non-SSO, then <OFS_USER> is SYSADMN.
> - <OFSAA_ID> should always be unique for each environment. For example, UAT01.
> - Based on the OIM version 11.1.2.2 or 11.1.2.3, select the appropriate version of the files to upload.

11. Set the System Property `XL.AllowAPHarvesting` to **TRUE**. See the following steps for the procedure to set the property:
    a. Login to the **SYSADMIN** console.
    b. Click **System Configuration** to view *System Properties*.
    c. Enter **XL.AllowAPHarvesting** in **Search System Properties** and click to view the property name in the search results pane.
    d. Click **Allows access policy-based provisioning of multiple instances of a resource** in the results pane to view the *System Property Detail: Allows access policy-based provisioning of multiple instances of a resource* window.
    e. Enter **TRUE** in the **Value** field.
    f. Click **Save**.
    g. Restart the OIM Server.

Figure 45: System Management window



> **NOTE** Further instructions apply only if SSO is configured in OFSAA. If you use Native Authentication, skip these instructions and proceed to Configuring Entitlements.

12. Upload the OAM Policy file to set the authentication for REST APIs, which the OFSAA Connector uses. The following is the procedure to upload:
    a. Edit the `oam-policies.xml` file in a text editor. Replace the placeholders ${OHS_PORT}, ${OHS_HOST}, and ${IDM_HOST} with the respective values of OHS Port, OHS Host Name, and IDM Host Name of the server where the IDM is hosted and the Oracle HTTP Server (OHS)) is configured.
    b. Execute the command **wlst**.

       For example, `$OIM_ORACLE_HOME/common/bin/wlst.sh`
    c. Connect to the **OAM Admin** server using the following:

```
wls:/offline>
connect('<user_id>','<password>','t3://<IDM_HOST>:<ADMIN_PORT>')
```

    d. Import the OAM Policies using the following:

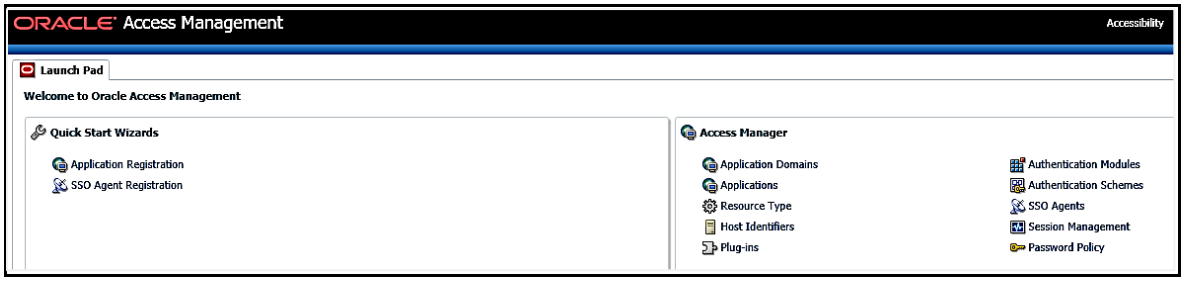
```
wls:/idm_domain/serverConfig>
importPolicy(pathTempOAMPolicyFile="/<path>/oam-policies.xml")
```

13. Perform OFSAA User Provisioning Configuration by applying Pre-authentication Advanced Rules to the basic Authorization Policy for users in the system. It is applied from the OAM console after IDM Provisioning and is done to switch to a form-based authentication scheme if the authorization header is not a basic scheme. Update the pre-authentication advanced rules to a form-based authentication scheme using the following steps:

    a. Login to the **OAM Administrator Console**.

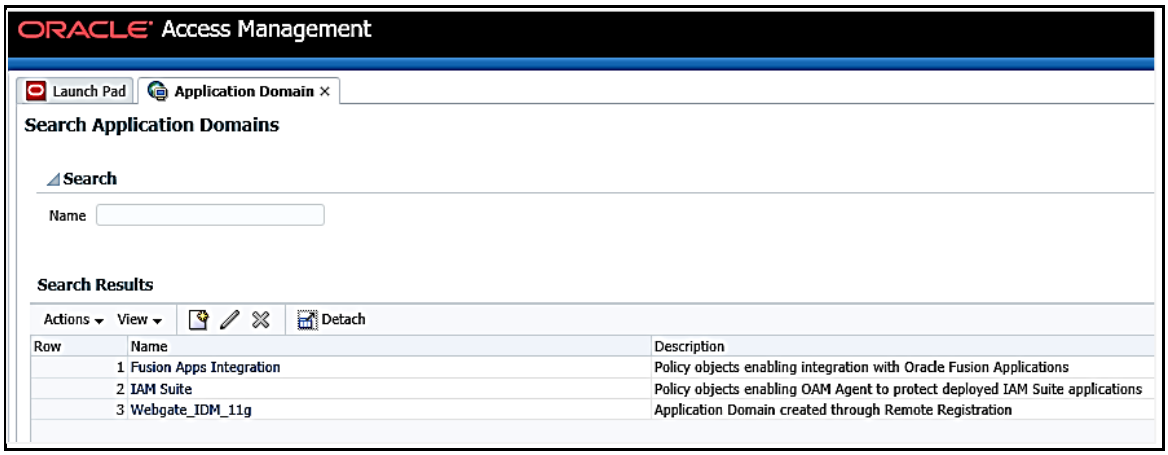
    b. From the **Launch Pad**, click **Application Domains** from the **Access Manager** widget. The *Application Domain* window is displayed.

Figure 46: Access Management Launch Pad



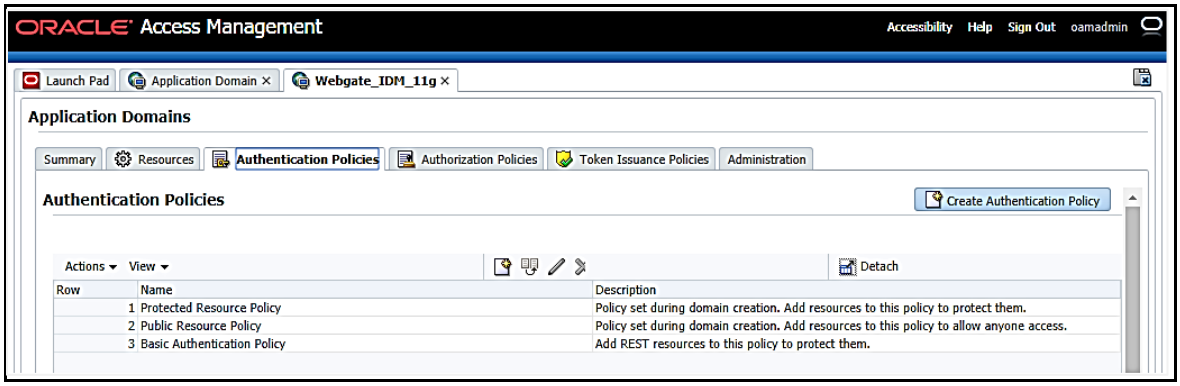
    c. Search for the required application domain for which you want to switch the authentication scheme and click **Name** from the search results to display the details for the application domain.

Figure 47: Application Domain tab



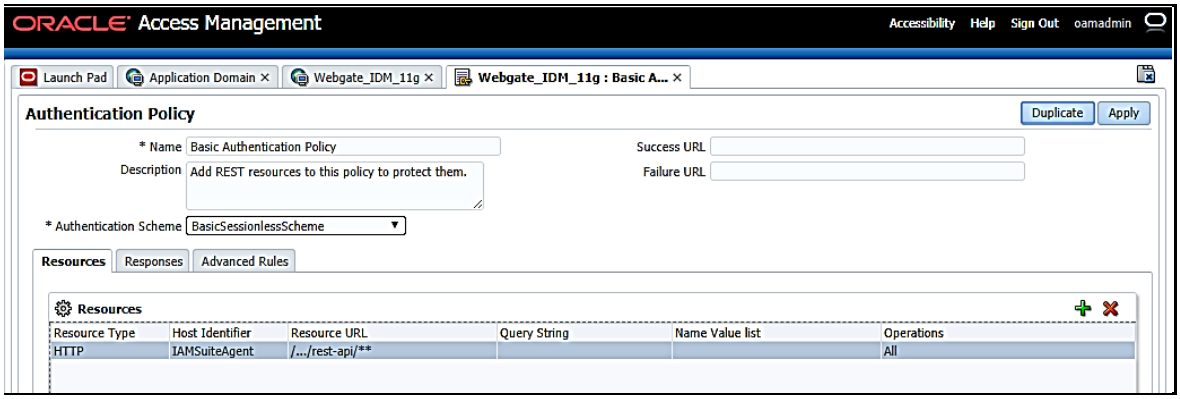
    d. Click the **Authentication Policies** tab to view the existing policies in the system.

Figure 48: Authentication Policies tab



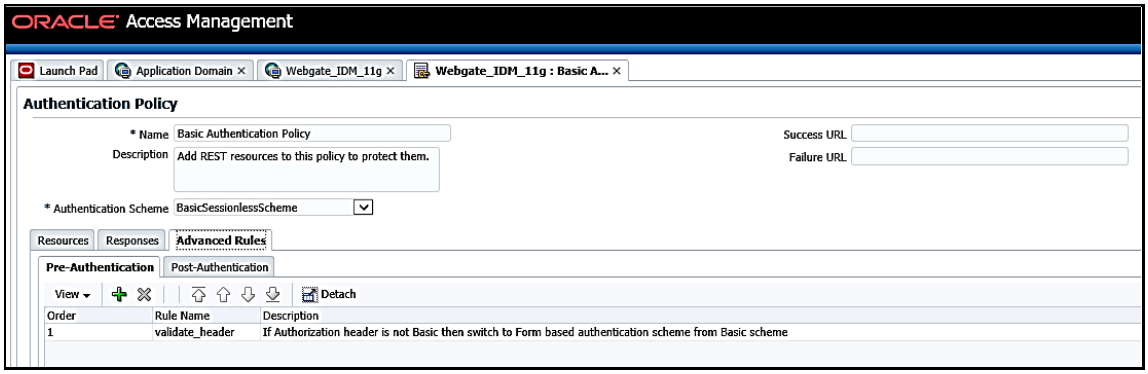
e. Click **Basic Authentication Policy** from the list to view the details for the policy.

Figure 49: Authentication Policies tab



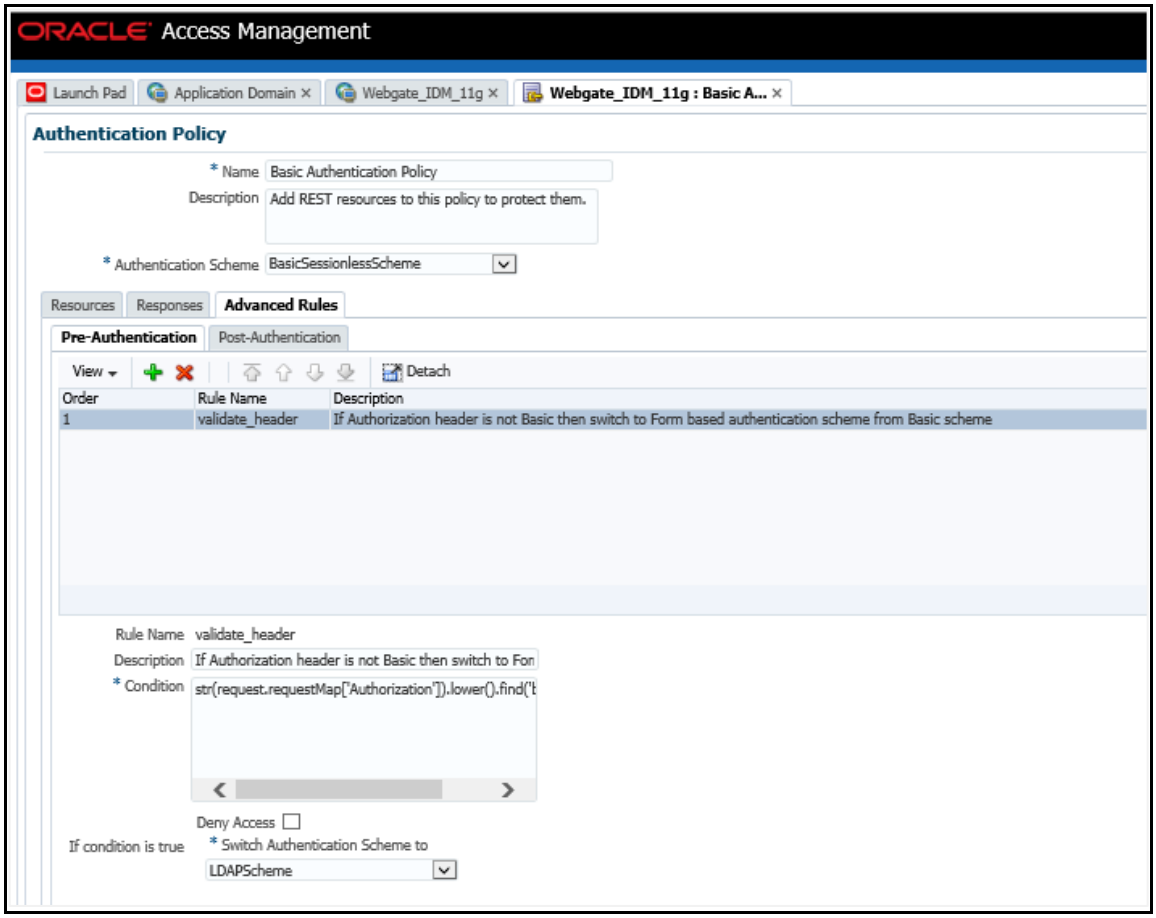
f. Click **Advanced Rules** tab to view the details for Pre-Authentication.

Figure 50: Authentication Policies - Advanced Rules tab



g. Click the **Add** + button and create a rule with the following information:

Figure 51: Authentication Policies - Advanced Rules tab



- Rule Name: validate_header
- Description: If Authorization header is not Basic then switch to Form based authentication scheme from Basic scheme
- Condition: str(request.requestMap['Authorization']).lower().find('basic') == -1
- Switch Authentication Scheme to: (select LDAPScheme from drop down)

h. Click **Apply** to save.

12.18.3 Configuring Entitlements

This section explains how you can provision Entitlements to users in OIM. Users are provisioned with Entitlements to enable them to be grouped for specific privileges, which allows them to perform certain restricted functions.

The subsections in this section provide information for the various operations required to configure Entitlements.

12.18.3.1 Performing User Group and User-User Group Mapping Reconciliation

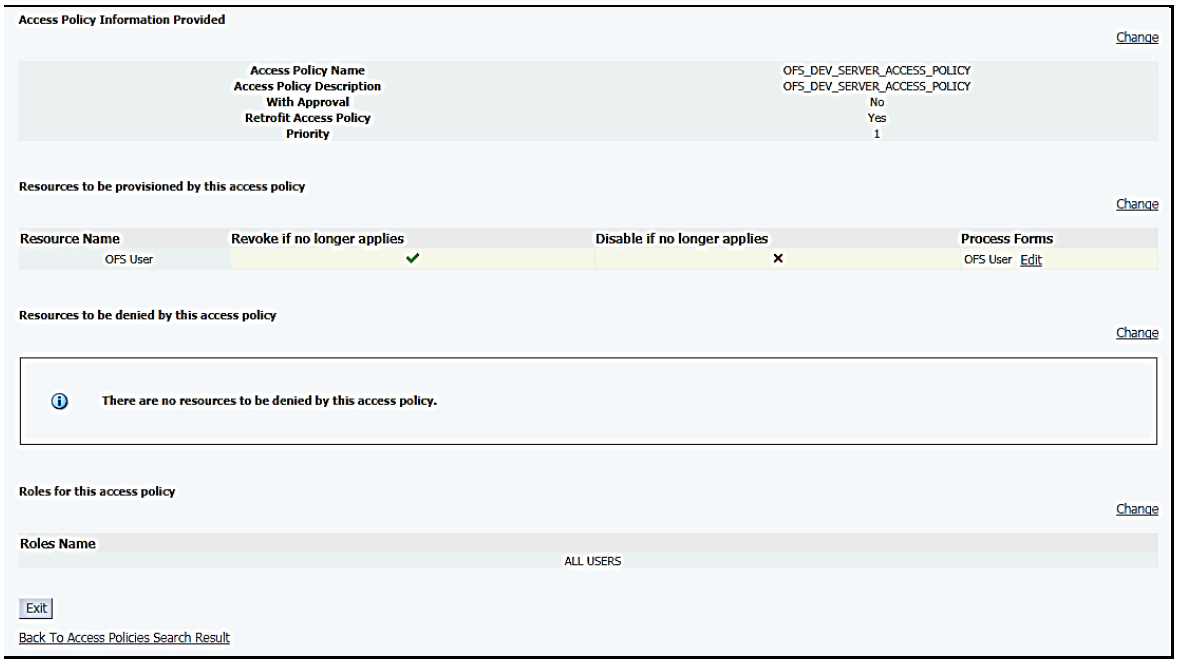
Performing reconciliation activity creates accounts in OIM, and if a user exists, the OIM account is mapped to the user. If a user doesn't exist, create the user profile in OIM, where the user login is the same as the user account. This maps the user to the OIM account created during reconciliation.

> **NOTE** If you use OFSAA Native Authentication (SMS), then the password policy for OIM and OFSAA should be the same.
>
> If OFSAA is deployed on WebLogic, then add the following tag in the **security-configuration** tag in the `<domain_home>/config/config.xml` file to enable REST API authorization by OFSAA:
> `<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>`

The following is the procedure to perform user group reconciliation, and user-user group mapping reconciliation:

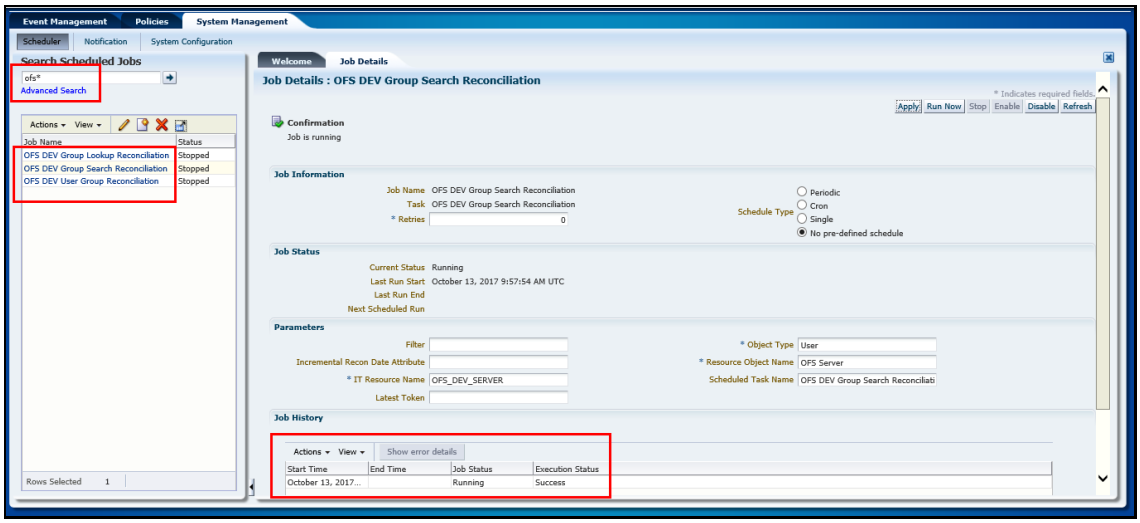
1. Login to **OIM SYSADMIN Console**.
2. Click **Access Policies** in **Policies** from the left menu to view the *Manage Access Polices* window.
3. Search for server access policy in the window and click the server access policy name to view the *Access Policy Information* window.

Figure 52: Access Policy Information window



4. By default, **All Users** role is mapped to the server access policy. To create and map Roles to provision specific users, see https://docs.oracle.com/cd/E40329_01/user.1112/e27151/role_mangmnt.htm#OMUSG3006.
5. Click **System Management** to view the window and click the **Scheduler** tab to view the *Scheduler* window.
6. Enter **OFS*** in **Search Scheduled Jobs** and click  to view the OFSAA group jobs.
7. Click **OFS {OFSAA_ID} Group Search Reconciliation** to view the *OFS {OFSAA_ID} Group Search Reconciliation* window.

Figure 53: OFS {OFSAA_ID} Group Search Reconciliation window.



8. Select from **Schedule Type**, the frequency at which you want to run the job. Select one from the following options:
   a. **Periodic** - Select this option if you want to run the job at a specific time and on a recurring basis. Enter an integer value in the Run every field in the Job Periodic Settings section and select one of the following values:
      - mins
      - hrs
      - days
   b. **Cron** - Select this option if you want to run the job at a particular interval and on a recurring basis. For example, you can create a job that runs at 8:00 A.M. every Monday through Friday, or at 1:30 A.M. every last Friday of the month. Specify the recurrence of the job in the Cron Settings section. Select any of the following values in the Recurring Interval field:
      - Daily
      - Weekly
      - Monthly on given dates
      - Monthly on given weekdays
      - Yearly

After selecting a value, you can enter an integer value in the Days between runs field.

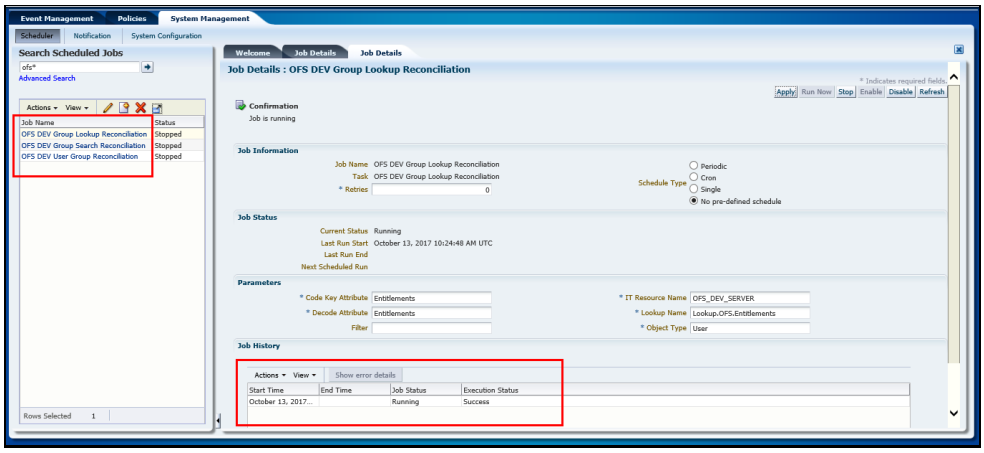
c. **Single** - Select this option if you want to run the job only once at a specific start date and time.

d. **No pre-defined schedule** – Select this option if you do not want to create a schedule that triggers the job automatically. To trigger the job, click **Save and Run Now**.

9. Run **OFS {OFSAA_ID} Group Search Reconciliation** and check for successful execution of the run.

10. Click **OFS {OFSAA_ID} Lookup Search Reconciliation** to view the *OFS {OFSAA_ID} Lookup Search Reconciliation* window.

Figure 54: OFS {OFSAA_ID} Group Search Reconciliation window.

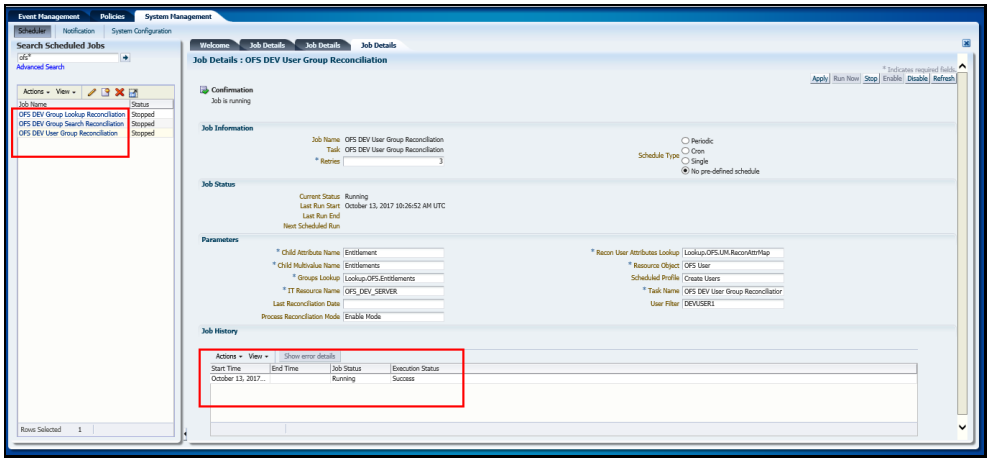


11. Select from **Schedule Type**, the frequency at which you want to run the job. For description, see Schedule Type.

12. Run **OFS {OFSAA_ID} Lookup Search Reconciliation** and check for successful execution of the run.

13. Click **OFS {OFSAA_ID} User Group Reconciliation** to view the *OFS {OFSAA_ID} User Group Reconciliation* window. Reconcile existing user-group mapping from OFSAA to OIM based on the User Filter field on this window.

Figure 55: OFS {OFSAA_ID} Group Search Reconciliation window.



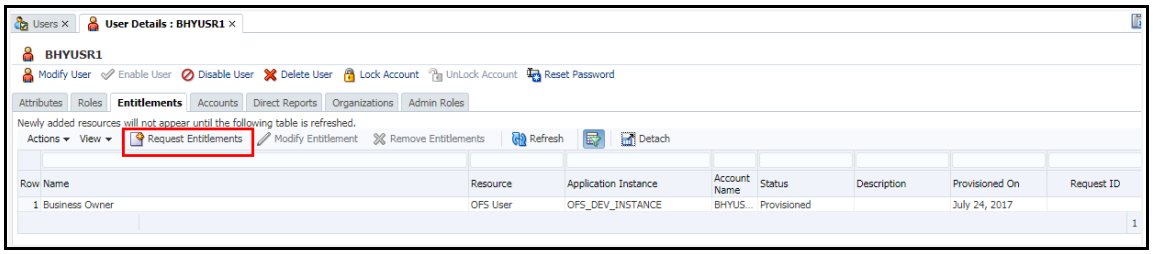
14. Select from **Schedule Type**, the frequency at which you want to run the job. For description, see Schedule Type.
15. Enter the login user name in **User Filter** to apply the user group reconciliation to. To add more than one user name, separate by using commas (,). Leave the field empty to apply to all users.
16. Run **OFS {OFSAA_ID} User Group Reconciliation** and check for successful execution of the run.

12.18.3.2 Provisioning Entitlement Requests

The following is the procedure to provision entitlement requests for Users:

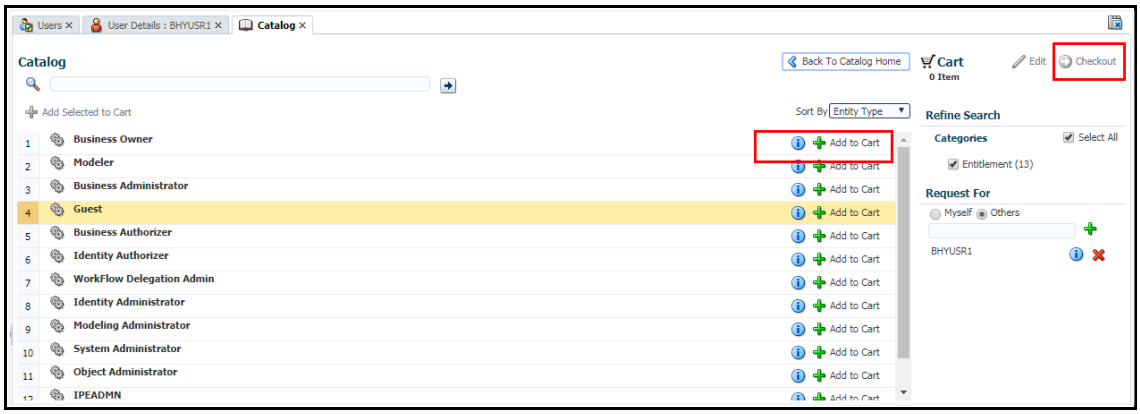
1. Login to **OIM Identity Console**.
2. Select the User and click **Request Entitlements** on the Entitlements window to display the *Catalog* window. **Catalog** displays a list of all OFSAA group as Entitlements.

Figure 56: OIM Identity Console



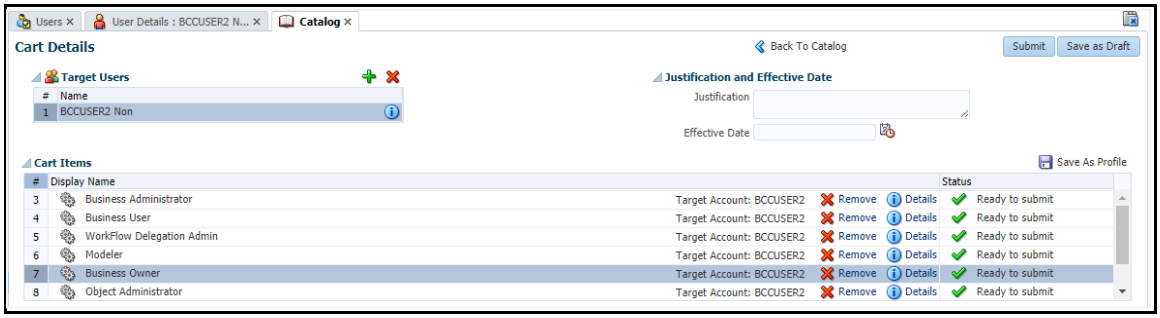
3. Select User and click **Add to Cart**. Click **Checkout** to view the *Cart Details* window.

Figure 57: Catalog- Cart Details window



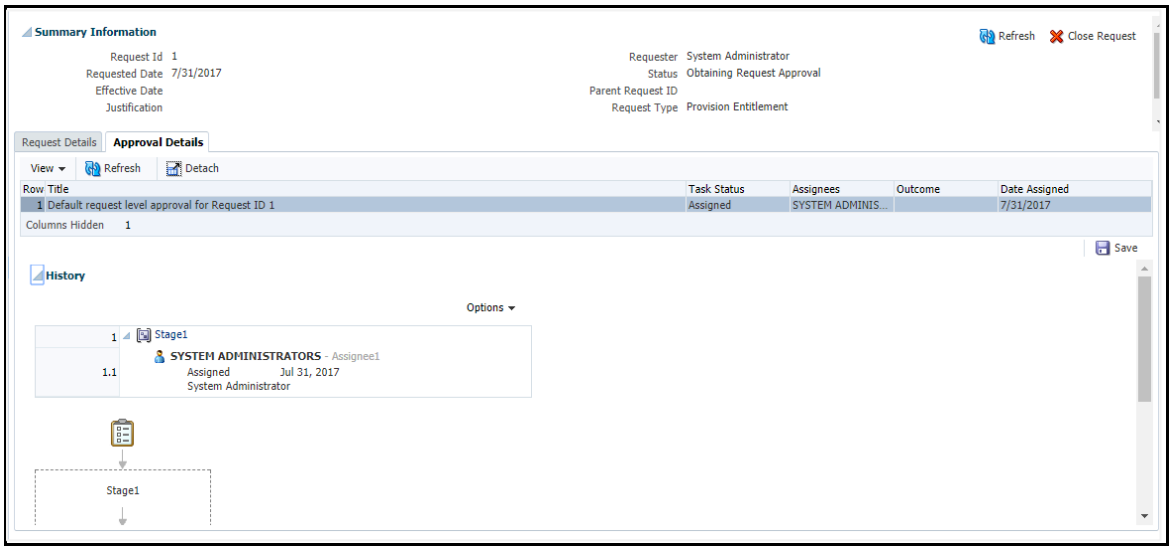
4. Click **Submit**. The request is processed for approval. See Approving Request Entitlements for more details.

Figure 58: Catalog- Cart Details window



5. Verify and confirm that the user group mapping is completed in OFSAA. Use the *Summary Information* window to check the stage that the request is in.

Figure 59: Catalog- Cart Details Summary window



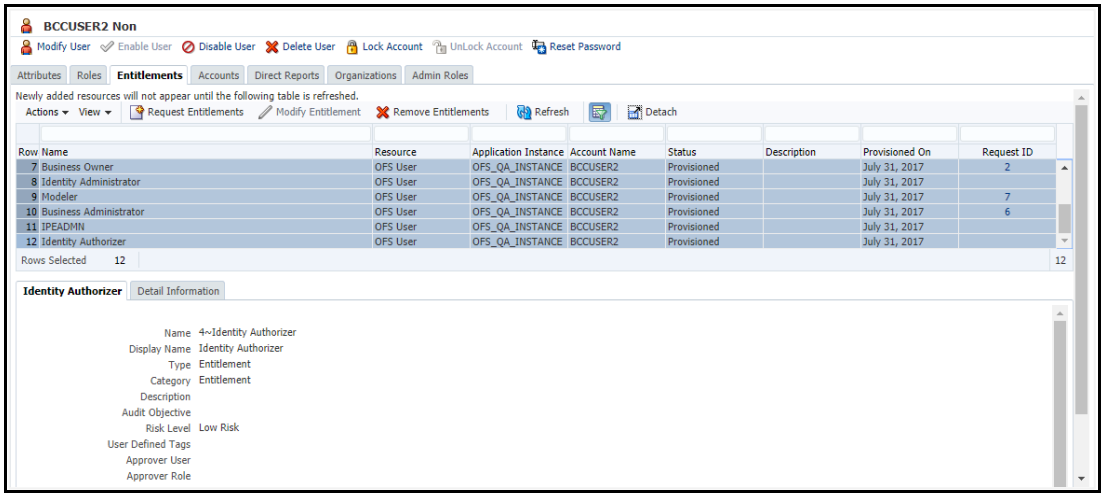
12.18.3.3 Removing Provisioned (Deprovisioning) Entitlements

Remove Entitlements provisioned to users if you want to update the system for changes in user's status.

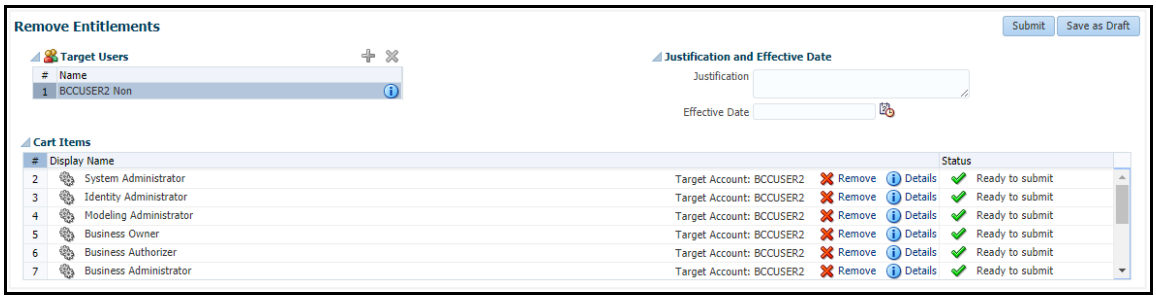
The following is the procedure to remove entitlements:

1. Login to **OIM Identity Console**.
2. Select the User to deprovision and check for status **Provisioned** to confirm that the User is assigned to an Entitlement. Click **Remove Entitlements** to display the *Remove Entitlements* window.

Figure 60: OIM Identity Console



3. Click **Submit**. The request is processed for approval. See Approving Request Entitlements for more details.



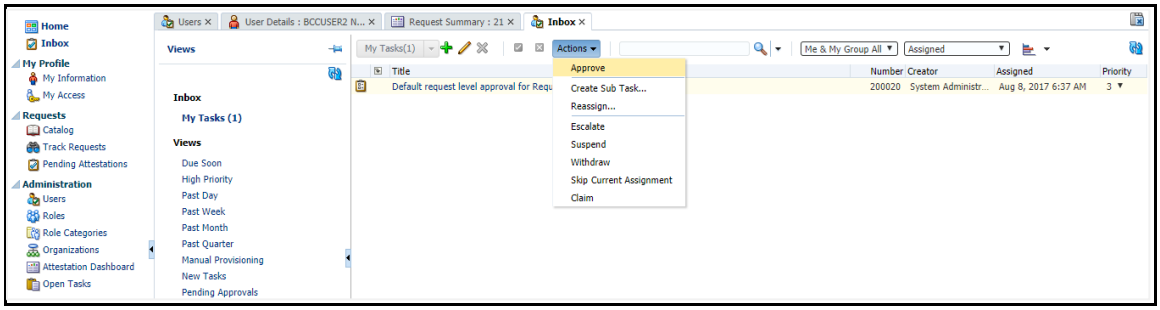
12.18.3.4 Approving Request Entitlements

User submitted entitlement requests are processed for approval. Only a user with approver role can approve and activate the request in OFSAA.

Following is the procedure to approve an entitlement request:

1. Login to **OIM Identity Console**.
2. Click **Inbox** from the left menu to display the Inbox window with tasks assigned to you.
3. Select the task that requires you to approve and click the **Actions** drop-down list. Select **Approve** to approve the Request Entitlement.

Figure 61: OIM Identity Console



12.19 Using REST APIs for User Management from Third-Party IDMs

OFSAA provides connectors which integrates with OIM. However, if you want to integrate OFSAA with any other Identity Management (IDM) System, then you have to use the APIs listed in this topic to develop connectors that can connect with OFSAA for user provisioning.

12.19.1 Knowing the Prerequisites

The following are the prerequisites to configure the REST APIs for third-party IDM Solutions:

1. The REST APIs referred to in this topic are protected by Basic Authentication, it requires administrator user ID and password to access.
2. To access these services, administrator users must be mapped to the IDMGMTADVN Role.
3. Select **Enable Native Authentication for Rest API** in the **OFSAA System Configuration** Window for the REST APIs to authenticate the password.

12.19.2 Understanding REST API Specifications

NOTE

Prefix `http://<Webserverip>:<servletport>/<context>` to the values in the URL column.

For example, `/rest-api/idm/service/create/user` must be `http://<Webserverip>:<servletport>/<context>/rest-api/idm/service/create/user`.

The following table provides details for the REST APIs:

Table 23: REST API specifications

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Create User	/rest-api/idm/service/create/user	POST	JSON	{ "attributes": { "user_id": "user_id", "user_name": "user_name", "user_password": "password", "user_start_date": "start_date", "user_end_date": "End_date", "user_is_authorized": true(/false), "user_is_enabled": true(/false), "user_logon_holiday": true(/false) "smsauthonly": true(/false) } }	All fields are mandatory. The Date format is mm/dd/yyyy. If user_is_authorized is set to **true**, then the User is authorized during User creation. If smsauthonly is set to **true**, then the User is authenticated only using the SMS Authentication type. If it is set to **false**, then the User can be authenticated using the SMS, LDAP and SSO authentication types. However, the smsauthonly configuration feature is available in the OFS AAI Release 8.1.1.1 and later versions.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Update User	/rest-api/idm/service/update/user	POST	JSON	{ "attributes": { "user_id": "user_id", "user_name": "user_name", "user_password": "password", "user_start_date": "start_date", "user_end_date": "End_date", "user_is_authorized": true(/false), "user_is_enabled": true(/false), "user_logon_holiday": true(/false) "smsauthonly": true(/false) } }	All fields are mandatory. The Date format is mm/dd/yyyy. If user_is_authorized is set to **true**, then the User is authorized during User creation. If smsauthonly is set to **true**, then the User is authenticated only using the SMS Authentication type. If it is set to **false**, then the User can be authenticated using the SMS, LDAP and SSO authentication types. However, the smsauthonly configuration feature is available in the OFS AAI Release 8.1.1.1 and later versions.
Delete User	/rest-api/idm/service/delete/user	POST	TEXT	USERID	The User ID is mandatory.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Authorize User	/rest-api/idm/service/authorize/user	POST	TEXT	USERID	The User ID is mandatory.
Force User Delete	rest-api/idm/service/delete/user/force	POST	TEXT	USERID	The User ID is mandatory. **NOTE:** This is applicable only after applying Oracle Financial Services Analytical Applications Infrastructure 8.1.2.2.0 Maintenance Release (ID 34572960).
Reinstate User	/rest-api/idm/service/reinstate/user	POST	TEXT	USERID	The User ID is mandatory.
Map User to Group	/rest-api/idm/service/map/groupmembers	POST	JSON	{ "user_id": "user_id", "group": [{ "group_id": "group_id", "group_name": "groupname" }, ...] }	The mapping of the User ID to Groups.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Unmap User from Group	/rest-api/idm/service/unmap/groupmembers	POST	JSON	{ "user_id": "user_id", "group": [{ "group_id": "group_id", "group_name": "groupname" }, ...] }	The unmapping of the User IDs from Groups.

User Status Report	`/rest-api/v1/user/status?userId=<USERID>&userName=<USERNAME>&idledays=<Number of days idle>&gsUserID=<Logged-in user>&loggedIp=<IP Address>&enable=<Y/N>&delete=<Y/N>&loggedIn=<Y/N>`	GET	-	For example: `https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/status?userId=exampleUserID&userName=exampleUserName&idledays=&gsUserID=SYSADMN&loggedIp=<192.0.2.1>&enable=Y&delete=N&loggedIn=Y`	The JSON request displays the Report for the deleted, disabled, currently logged in, and idle Users. **Note**: • The Get Response populates additional fields in v8.1.2.0.0+ on applying the **33150367** One-off Patch. See the Appendix B – Additional Information in REST APIs for User Status and User Access Reports Section for more details. • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • idledays is the number of days (INTEGER) the user has not logged into the system. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • enable is the flag to determine if the user is enabled or disabled in the system. The valid values are **Y** for yes and **N** for no. • delete is the flag to determine if the user is deleted in the system. The valid values are **Y** for yes and **N** for no. • loggedIn is the flag to determine if the user is currently logged into the system. The valid values are **Y** for yes and **N** for no. • Oracle recommends that you copy and paste the URL and modify the placeholders.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
User Attribute Report	`/rest-api/v1/user/attributes?userId=<USERID>&userName=<USERNAME>&gsUserID=<Logged-in User>&loggedIp=<IP Address>`	GET	-	For example: `https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/attributes?userId=exampleUserID&userName=exampleUserName&gsUserID=SYSADMN&loggedIp=<192.0.2.1>`	The JSON request displays the Report for the various User attributes. **Note**: • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Oracle recommends that you copy the URL and modify the placeholders.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
User Admin Activity Report	/rest-api/v1/user/useradminactivity?userId=<USERID>&userName=<USERNAME>&startdate=<mm/dd/yyyy>&enddate=<mm/dd/yyyy>&gsUserID=<Logged-in User>&loggedIp=<IP Address>	GET	-	For example: https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/useradminactivity?userId=exampleUserID&userName=exampleUserName&startdate=01/01/2020&enddate=12/31/2020&gsUserID=SYSADMN&loggedIp=<192.0.2.1>	The JSON request displays the Report for the various activities of the User. **Note**: • The values for the **startdate** and **enddate** attributes in this API are required. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • startdate is the date from which the report is to be considered. The Date format is mm/dd/yyyy. • enddate is the end date to be considered for the report. The Date format is mm/dd/yyyy. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Oracle recommends that you copy the URL and modify the placeholders.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
User Access Report	`/rest-api/v1/user/useraccess?userId=<USERID>&userName=<USERNAME>&gsUserID=<Logged-in User>&loggedIp=<IP Address>`	GET	-	For example: `https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/useraccess?userId=exampleUserID&userName=exampleUserName&gsUserID=SYSADMN&loggedIp=<192.0.2.1>`	The JSON request displays the Report for User Access Rights. **Note**: • The Get Response populates additional fields in v8.1.2.0.0+ on applying the **33150367** One-off Patch. See the Appendix B – Additional Information in REST APIs for User Status and User Access Reports Section for more details. • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Oracle recommends that you copy the URL and modify the placeholders.

Audit Trail Report	/rest-api/v1/audit/summary	POST	JSON	{
				
				"userId":"<User Id>",
				
				"fromdate":"<Date>",
				
				"todate":"<Date>",
				
				"action":"<add/copy/delete/authorize and other actions>",
				
				"strlocale": "en_US",
				
				"msgsearchfld":"",
				
				"loggedIP":"<IP Address>",
				
				"gsUsrID":"<Logged-in User Id>"
				}
					The JSON request displays the Report for Audit Trail.
					Note:
					• The values for the **fromdate**, **todate**, and **strlocale** attributes in this API are required.
					• If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit.
					• If you do not enter the value for the **userId** attribute in this API, the records for all the users is displayed
					• userID is the OFSAA identifier of the User for whom the report is to be generated.
					• userName is the OFSAA login name for the above User ID.
					• fromdate is the date from which the report is to be considered. The Date format is mm/dd/yyyy.
					• todate is the end date to be considered for the report. The Date format is mm/dd/yyyy.
					• Action is the type of method. The valid options are as follows:
					Note: If you do not enter any value for this attribute, all records for the actions is displayed.
					Displays all actions performed by the selected user.
					When the audit trail report is generated the details of the associated activity/data field and the application IDs of the PMF process is also added as the **Action details** for all the displayed actions.
					▪ Add
					Displays add events performed by the selected user.
					▪ Advanced
					Displays advanced events performed by the selected user.
					▪ Authorize

					Displays authorization performed by the selected user. ▪ Archive Displays archive actions performed by the selected user. ▪ Compare Displays compare actions performed by the selected user. ▪ Copy Displays copy events performed by the selected user. ▪ Disable Displays any disable actions performed by the selected user. ▪ Download Displays downloads done by the selected user. ▪ Edit Displays any edits done by the selected user. ▪ Enable Displays any enable actions done by the selected user. ▪ Execute Displays execute actions performed by the selected user. ▪ Export Displays export events performed by the selected user. ▪ Generate Displays generate events performed by the selected user. ▪ Ignore access Displays ignore access events performed by the selected user. ▪ Ignore lock Displays ignore lock events performed by the selected user.

					▪ Import Displays import events performed by the selected user. ▪ Latest Displays the latest events performed by the selected user. ▪ Link Displays any link events performed by the selected user. ▪ Lock Displays any lock events linked to the selected user. ▪ Login Displays login events performed by the selected user. ▪ Logout Displays logout events performed by the selected user. ▪ Publish Displays publish events performed by the selected user. ▪ Purge Displays purge events performed by the selected user. ▪ Reject Displays reject events performed by the selected user. ▪ Delete Displays delete events performed by the selected user. ▪ Restore Displays restore events performed by the selected user. ▪ Review Displays review events performed by the selected user.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
					▪ Revoke Displays revoke events performed by the selected user. ▪ Submit Displays submit events performed by the selected user. ▪ Summary Displays summary modifications performed by the selected user. ▪ Trace Displays trace events performed by the selected user. ▪ Upload Displays uploads performed by the selected user. ▪ Validate Displays validate events performed by the selected user. ▪ View Displays view events performed by the selected user. • strlocale is the language code string such as en_US. • msgsearchfld is the search field string. This value is optional. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • gsUserID is the User ID of the user logged in and accessing the system. • Oracle recommends that you copy the URL and modify the placeholders.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
NOTE : • The below APIs are applicable on 8.1.2.3.0 after applying the **35322369** One-off Patch. • Apply the patch **35829211** to prevent creating AAI and related tables, when you are creating INFODOM.					

Requirement	URL	Method Type	Request	Sample Request JSON	Comments

Create Application	/rest-api/v1/app/create	POST	JSON	{
				"appId": "application id",
				"appName": "application name",
				"appDesc": "application desc",
				"infodomId": "Infodom name",
				"enabled": true/false,
				"userLocale":"locale (en_US)"
				}
					All fields are mandatory.
					If Enabled is set to true then created application will be enabled else it will be disabled.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Delete Application	/rest-api/v1/app/delete/app_Id	DELETE	Path param	Url Params are used so sample request will be as follows: rest-api/v1/app/app_id	app id is mandatory

Create Infodom	/rest-api/v1/infodom/create	POST	JSON	{
				"appLogPath": "/scratch/test8123/ftpshare/PAERTHTESTINFO/logs",
				"dbLogPath": "/scratch/test8123/ftpshare/PAERTHTESTINFO/logs",
				"infodomName": "PAERTHTESTINFO",
				"infodomDesc": "PAERTHTESTINFO DESC",
				
				"authRSNRequired": false,
				
				"infodomTypeStaging": true,
				
				"dbName":"testparth",
				
				"dbServer":"100.76.146.194", --FIC_HOME IP
				
				"olapServer":"127.0.0.1",
				"olapType":"ESSBASE",
				"scriptRequired": false --default is true [which creates AAI related tables]
				}	

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Delete Infodom	`/rest-api/v1/infodom/delete/infodom_name`	DELETE	Path param	`Url Params are used so sample request will be as follows: rest-api/v1/app/infodom_name`	Infodom name is mandatory

Requirement	URL	Method Type	Request	Sample Request JSON	Comments

Create segment	/rest-api/v1/segment /create	POST	JSON	{
				
				"segmentCode":"segment_code",
				
				"segmentName":"segment_name",
				
				"segmentDesc":"segment_desc",
				
				"segmentType":"segment_type",
				
				"dsnID":"infodom_id",
				
				"ownerCode":"user_id"
				}
					All fields are
					Three types of segmentType (PUBLIC, PRIVATE, SHARED)
					ownerCode is user id if you have selected segmentType as private

Requirement	URL	Method Type	Request	Sample Request JSON	Comments

Authorize role group	/rest-api/v1/group/role/authorize?operation=map&auth=A	POST	JSON	{
				"groupid":"BUSINESSADMIN",
				"rolecodes" : ["QLOCAUTHRL","QLOCVIEWRL"]
				}
					operation=map/unmap[based on roles are mapped or unmapped
					auth=A/R [A:authorize, R:reject]

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
Authorize domain group	/rest-api/v1/group/domain/authorize?operation=map&auth=A	POST	JSON	{ "groupid":"IDENTITYMGMTAUTH", "domainnames" : ["PARTHTESTINFO-PTFLD","PARTHTESTINFO-PARFLD"] }	operation=map/unmap[based on domains are mapped or unmapped] auth=A/R [A:authorize, R:reject]

Create Database Details	/rest-api/v1/database-details/create	POST	JSON	{ "dbServer":"100.76.146.194", "dbName":"aaipatest", "dbSchemaName":"aaiptest", "dbDateFormat":"mm-dd-yyyy", "authAliasName":"aaipatest", "authAliasUserName":"aaipatest", "authAliasPassword":"aaipatest", "dataSourceString":"SMSOCI19PDB", "jdbcConnString":"jdbc:oracle:thin:@100.76.146.194:1521/SMSOCI19PDB", For Wallet: jdbc:oracle:thin:/@july25_als where july25_als is the alias created for new schema user created.	All Fields Are required.

Requirement	URL	Method Type	Request	Sample Request JSON	Comments
				"jndiName":"AAIPATESTINFO" }	

12.20 Configuring the Logout URL for OBIEE in OFSAA

Logging out from OFSAA does not logout a user from Oracle Business Intelligence Enterprise Edition (OBIEE) if the OBIEE Logout URL is not configured in OFSAA.

Perform the following configuration in OFSAA to enable logging out of OBIEE when you logout of OFSAA:

1. Login to the OFSAA database with CONFIG user credentials:
2. In the database, update the configuration table by running the script in the following format:

```
update configuration set paramvalue = '<OBIEE_LOGOUT_URL>' where paramname =
'OBIEE_LOGOUT_URL_VAL';

/

update configuration set paramvalue = '<IS_CROSSDOMAIN>' where paramname =
'OBIEE_CROSS_DOMAIN_VAL';
```

Replace `<OBIEE_LOGOUT_URL>` with the OBIEE logout URL.

For example,

```
update configuration set paramvalue = 'http://obieehost:port/analytics/saw.dll?Logoff'
where paramname = 'OBIEE_LOGOUT_URL_VAL';
```

and

Replace `<IS_CROSSDOMAIN>` with **true** if OBIEE is on another server.

For example,

```
update configuration set paramvalue = 'true' where paramname = 'OBIEE_CROSS_DOMAIN_VAL';
```

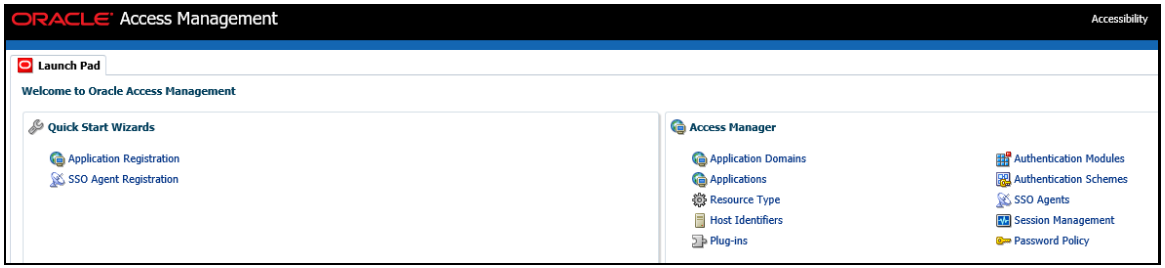
12.21 Enabling Deep Linking in OFSAA

When a user logs into OFSAA, by default, the application opens the default landing page or the preferred landing page. However, it is possible to open a specific page (show requested resource URL) other than the default or preferred landing page by using Deep Linking in an SSO-enabled setup.

To enable deep linking, perform the following procedure:

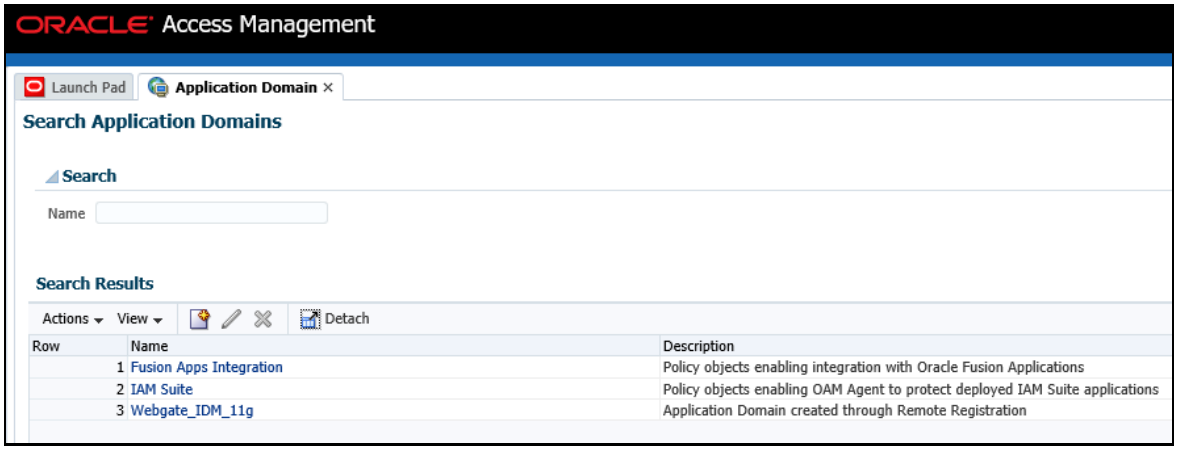
1. Login to the **OAM Administrator Console**.
2. From the **Launch Pad**, click **Application Domains** from the **Access Manager** widget. The *Application Domain* window is displayed.

Figure 62: Access Management Launch Pad



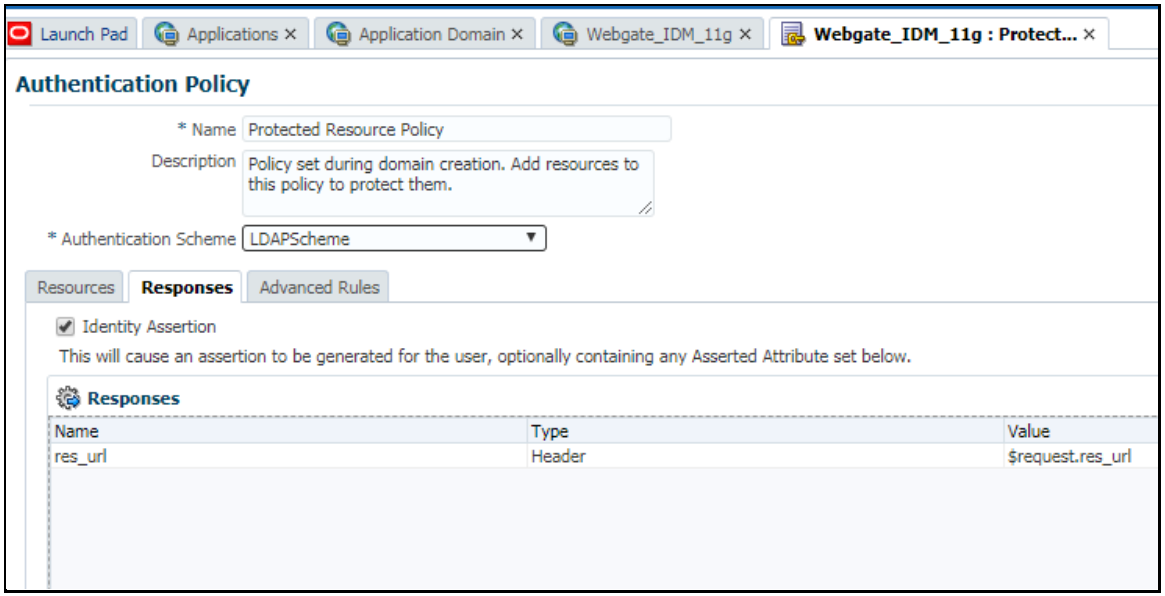
3. Search for the required application domain for which you want to switch the authentication scheme and click **Name** from the search results to display the details for the application domain.

Figure 63: Application Domain tab



4. Click the **Authentication Policies** tab to view the existing policies in the system.

Figure 64: Authentication Policies tab



5. Click **Protected Resource Policy** from the list to view the details for the policy.
6. Click **LDAPScheme** from Authentication Scheme.
7. Click **Responses** tab and click **Add** button.
8. To configure deep linking in your OFSAA, set **res_url** header in response to send Requested resource URL path. In the popup, select **Header** for **Type**. Enter **res_url** for **Name** and enter **$request.res_url** for **Value**. Click **OK**.
9. Click **Apply** to save.

For reference information on the preceding instructions, see the following link for OAM:

https://docs.oracle.com/cd/E52734_01/oam/AIAAG/GUID-30AA255E-677D-4054-8C3E-2D991F50BCA8.htm#GUID-26E22714-19DF-42DB-98DE-1C8DF67DDF1F

12.22 Enabling Unlimited Cryptographic Policy for Java

Enabling the Unlimited Cryptographic Policy for Java enables you to use the AES-256 keys for encryption.

NOTE Skip the steps mentioned in this section as JCE is enabled by default for the following Java versions:

- Java 7:

  7u171 and later

- Java 8:

  8u161 and later

You can download the JCE Policy JAR files, for the current and later Java versions required for OFSAA, from the following web page:

https://bugs.java.com/view_bug.do?bug_id=JDK-8170157

For Java versions, where Unlimited Cryptographic Policy is not enabled by default, follow these steps to enable it:

1. Download the JCE Policy related JARs `local_policy.jar` and `US_export_policy.jar`.
   - For Oracle Java 7, download it from the following web page:

     https://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.
   - For Oracle Java 8, download it from the following web page:

     https://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html.
   - For IBM Java, download it from the following web page:

     https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk.
2. Copy (or replace) the downloaded JCE Policy related JARs `local_policy.jar` and `US_export_policy.jar` into the `/jre/lib/security` directory of the Java installation directory used for OFS AAI and the Web Application Servers.

13 Configurations for Connecting OFSAA to Oracle Database using Secure Database Connection (TCPS)

13.1 Prerequisites

The following are the prerequisites for this configuration:

1. UNIX user credentials with which OFSAA was installed.
2. UNIX user credentials with which Web Application Server (Oracle WebLogic (WLS)/Apache Tomcat/ IBM WebSphere) was installed.
3. OFSAAI version should be 8.1.0.0.0 and later.
4. Ensure OFSAA installed and deployed is having JAVA 8 (Java version must support Java unlimited cryptographic policy. Java version 1.8.0_161+ supports unlimited cryptographic policy.)
5. Create Oracle Wallet on the OFSAA processing tier. It is mandatory to create an oracle wallet to connect with OFSAA and TCPS Database Server.

   For information on Creating and Managing Oracle Wallet, see https://blogs.oracle.com/dev2dev/ssl-connection-to-oracle-db-using-jdbc,-tlsv12,-jks-or-oracle-wallets and https://blogs.oracle.com/weblogicserver/weblogic-jdbc-use-of-oracle-wallet-for-ssl.
6. Configure the Oracle Wallet with trusted certificates between the database server with TCPS configured and the database client to enable communication through the SSL protocol. For example, all the database utils such as sqlplus, tnsping, and sqlldr must work between the Client and the Server.

13.2 Configure OFSAA to Store Config Schema, Atomic Schema, and SysDBA Credentials with Oracle Wallet

To configure the OFSAA to store the Config and Atomic Schema credentials with Oracle Wallet, follow these steps:

1. Log in as a UNIX user with the permission to modify the Oracle Wallet.
2. Execute the following command to configure Config Schema credentials. Enter the password to store the credentials in the Wallet when prompted.

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -createCredential  -nologo CONFIG
<CONFIG_DATABASE_USERNAME>  <CONFIG_DATABASE_PASSWORD>
```

3. Execute the following command to configure the Atomic Schema credentials. Enter the password to store the credentials in the Wallet when prompted.

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -createCredential  -nologo <ATOMICALIASNAME>
<ATOMIC_DATABASE_USERNAME>  <ATOMIC_DATABASE_PASSWORD>
```

4. Configure SysDBA credentials. Execute the following command to configure SysDBA Schema credentials. Enter the password to store the credentials in the Wallet when prompted.

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -createCredential  -nologo SYS
<SYS_DATABASE_USERNAME>  <SYS_DATABASE_PASSWORD>
```

NOTE

- CONFIG value is a TNS alias for Config Schema. Do not change this value.
- SYS value is a TNS alias for SYSDBA Schema user. Do not change this value. This is required only to execute Schema Creator Utility in Online mode. If Schema creation is executed in Offline mode, this alias is not required.
- ATOMICALIASNAME value is a TNS alias for Atomic Schema. It must not contain underscores.

  For example, if the Atomic Schema Name is PROD_OFSAAATM, then the value for ATOMICALIASNAME must be entered as PRODOFSAAATM.
- In case of Config and Atomic Schema passwords are changed over a period of time, new password credentials needs to be updated for Config and Atomic Schema in the Oracle Wallet so that OFSAA and Webserver takes the new credentials.

1. Execute the following command to update passwords of Config and Atomic Schema users.

1. Enter the password to store the credentials in the Wallet when prompted.

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -
modifyCredential -nologo CONFIG
<CONFIG_DATABASE_USERNAME>
<CONFIG_DATABASE_PASSWORD>
```

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -
modifyCredential -nologo <ATOMICALIASNAME>
<ATOMIC_DATABASE_USERNAME>
<ATOMIC_DATABASE_PASSWORD>
```

13.3 Configuring OFSAA and various Web Application Servers with Oracle Wallet

The following are the details to configure OFSAA and various Web Application Servers with Oracle Wallet:

1. Import all the Wallet Certificates from the Oracle Database and Oracle Database Client into the JDK cacert store:
   a. Log in as a UNIX User with the required permission configured to access the **cacerts of Java** file.
   b. Execute the following command to add the Wallet Certificates to the JDK store of the JRE used in the OFSAA Processing Server:

```
/usr/java/jdk1.8.0_161/bin/keytool -importcert -trustcacerts -alias sslorclserver -file
<locationofservercerts>/server_certs/ dbsrvhostname-certificate.crt -keystore
/usr/java/jdk1.8.0_161/jre/lib/security/cacerts -storepass changeit
```

```
/usr/java/jdk1.8.0_161/bin/keytool -importcert -trustcacerts -alias ssloraclclient -file
<locationofclientcerts>/client_certs/ dbclthostname-certificate.crt -keystore
/usr/java/jdk1.8.0_161/jre/lib/security/cacerts -storepass changeit
```

```
/usr/java/jdk1.8.0_161/bin/keytool -importcert -trustcacerts -alias sslorclcdb -file
<locationofservercerts>/server_certs/ dbsrvhostname-certificate_xdb.crt -keystore
/usr/java/jdk1.8.0_161/jre/lib/security/cacerts -storepass changeit
```

> **NOTE** For information on Creation of Certificates, contact your Database Administrator (DBA).
>
> The alias names – sslorclcdb, ssloraclclient, and sslorclserver are given as reference names and you can choose any other names.

2. Login to the OFSAA Processing Tier with the same user credentials with which the OFSAA processes run.
3. Verify the location of the wallet in the `sqlnet.ora` file found (location: `$TNS_ADMIN`) usually in the path `ORACLE_HOME/network/admin`. This file might have entries in the following format:

```
WALLET_LOCATION =
   (SOURCE =
     (METHOD = FILE)
     (METHOD_DATA =
       (DIRECTORY = /scratch/ssldbtest/clientwallet)
     )
   )
```

```
SQLNET.WALLET_OVERRIDE = TRUE

SSL_CLIENT_AUTHENTICATION = FALSE

SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA)
```

4. Modify the tns entry in `tnsnames.ora` file for connecting the database with secured database connection (TCPS).

```
DBAAIB =
(DESCRIPTION =

 (ADDRESS = (PROTOCOL = TCPS)(HOST = dbsrvhostname.in.oracle.com)
            (PORT = 2484)
 )

 (CONNECT_DATA =
   (SERVER = DEDICATED)
   (SERVICE_NAME = DBAAIB)
 )
 (security=(ssl_server_cert_dn= "CN=dbsrvhostname"))
)
dbtyofsaaatm =
(DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCPS)(HOST = dbsrvhostname.in.oracle.com)
   (PORT = 2484)
  )
 (CONNECT_DATA=
   (SERVER = DEDICATED)
   (SERVICE_NAME=DBAAIB)
 )
 (security=(ssl_server_cert_dn= "CN=dbsrvhostname"))
)

CONFIG =  (DESCRIPTION =  (ADDRESS = (PROTOCOL = TCPS)(HOST = dbsrvhostname.in.oracle.com)
(PORT = 2484)  )  (CONNECT_DATA =    (SERVER = DEDICATED)    (SERVICE_NAME = DBAAIB)  )
(security=(ssl_server_cert_dn= "CN=dbsrvhostname")) )


SYS =  (DESCRIPTION =    (ADDRESS = (PROTOCOL = TCPS)(HOST = dbsrvhostname.in.oracle.com)
(PORT = 2484)   )  (CONNECT_DATA=    (SERVER = DEDICATED)    (SERVICE_NAME=DBAAIB)  )
(security=(ssl_server_cert_dn= "CN=dbsrvhostname")) )
```

5. Enable Java Security Provider as Oracle PKI Provider statically on machines hosting OFSAA and the Web Application Servers, by performing the following step:

- Since SSO wallets (`cwallet.sso`) are used, add the OraclePKIProvider at the end of the provider list in the `java.security` file (this file is part of your JRE install located at `$JRE_HOME/jre/lib/security/java.security`) which typically looks like:

Figure 65: JRE install located in the Java.Security file

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
security.provider.7=oracle.security.pki.OraclePKIProvider
```

For more information, refer the following link:

https://blogs.oracle.com/dev2dev/ssl-connection-to-oracle-db-using-jdbc,-tlsv12,-jks-or-oracle-wallets#Wallets

6. Connect to the OFSAA database and modify the existing JDBC connect string value in the following columns:
   - Update the **JDBC_CONN_STR** values in the **AAI_DB_PROPERTY** and **DB_MASTER** tables from the Configuration Schema as shown in the following example:

     Syntax: `jdbc:oracle:thin:@<tns entry DBserver points to tcps>`

     Example: `jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)(HOST = dbsrvhostname.in.oracle.com)(PORT = 2484)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME=DBAAIB)) (security=(ssl_server_cert_dn=CN=dbsrvhostname)))`
   - Update **V_PRMVALUE** for the parameter V_PRMVKEY=DEFAULT_CONNECTION_URL in the table **AAI_DYN_SVCS_PARAMS**.
7. Modify **DEFAULT_CONNECTION_URL** in the `$FIC_HOME/conf/DynamicServices.xml` file from the Configuration Schema as follows:

   Syntax: `jdbc:oracle:thin:@< tns entry DBServer points to tcps>`

   Example: `jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)(HOST = dbsrvhostname.in.oracle.com)(PORT = 2484)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = DBAAIB)) (security=(ssl_server_cert_dn=CN=dbsrvhostname)))`
8. Add or modify the environment variables **wallet_loc** and **X_ARGS_GEN** in `.profile` of OFSAA user and web server user. Add `-Doracle.net.tns_admin, -Doracle.net.ssl_server_dn_match, -Djavax.net.ssl.trustStoreType`

-Djavax.net.ssl.trustStore, -Doracle.net.ssl_version and -Doracle.net.wallet_location locations as given below.

```
wallet_loc="(SOURCE=(METHOD=file)(METHOD_DATA=(DIRECTORY=/scratch/ssldbtest/clientwallet)))"

export wallet_loc

X_ARGS_GEN="-Doracle.net.tns_admin=$TNS_ADMIN

   -Doracle.net.wallet_location=$wallet_loc

   -Doracle.net.ssl_server_dn_match=true

   -Djavax.net.ssl.trustStoreType=SSO

   -Djavax.net.ssl.trustStore=cwallet.sso

   -Doracle.net.ssl_version=1.2"

export X_ARGS_GEN
```

9. Update the variables to append **X_ARGS_GEN** value in **X_ARGS_APP** and other X_ARGS property in .profile of the OFSAA user as shown in the following:

```
X_ARGS_APP="-Xms200m -Xmx8g -XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=1024M -
XX:+UseParallelOldGC  -XX:+DisableExplicitGC $X_ARGS_GEN"

export X_ARGS_APP

X_ARGS_OBJMIG="-Xms256m -Xmx512m -XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=1024M -
XX:+UseParallelOldGC  -XX:+DisableExplicitGC $X_ARGS_GEN"

export X_ARGS_OBJMIG

X_ARGS_RLEXE="-Xms512m -Xmx1024m -XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=1024M -
XX:+UseParallelOldGC  -XX:+DisableExplicitGC $X_ARGS_GEN"

export X_ARGS_RLEXE

X_ARGS_RNEXE="-Xms256m -Xmx512m -XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=1024M -
XX:+UseParallelOldGC  -XX:+DisableExplicitGC $X_ARGS_GEN"

export X_ARGS_RNEXE

X_ARGS_WSEXE="-Xms256m -Xmx512m -XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=1024M -
XX:+UseParallelOldGC  -XX:+DisableExplicitGC $X_ARGS_GEN"

export X_ARGS_WSEXE
```

10. Execute the .profile and restart OFSAA Services.

13.3.1 Configuring OFSAA and Tomcat as Web Application Server with Oracle Wallet

1. On Primary Tomcat Server instance, since there is no Oracle Client on the Tomcat Server instance, manually create a directory called "network" and copy `tnsnames.ora`, `sqlnet.ora` files into the "network" folder. Copy complete wallet directory "clientwallet" configured from OFSAA layer.
2. Modify `sqlnet.ora` with new WALLET_LOCATION path.
3. Add the following Java properties in `catalina.sh` file after `-Djava.io.tmpdir="\"$CATALINA_TMPDIR\"" \` entry. This needs to be added in multiple places in the same file.

```
-Doracle.net.tns_admin="\"$TNS_ADMIN\"" \
-Doracle.net.wallet_location="\"$wallet_loc\"" \
-Djavax.net.ssl.trustStoreType="SSO" \
-Djavax.net.ssl.trustStore="/scratch/ssldbtest/clientwallet/cwallet.sso" \
-Djavax.net.ssl.keyStore="/scratch/ssldbtest/clientwallet/cwallet.sso" \
-Djavax.net.ssl.keyStoreType="SSO" \
-Doracle.net.ssl_version="1.2" \
-Doracle.net.ssl_server_dn_match="true" \
```

4. Specify the fully qualified JDBC URL in Connection pool settings of Tomcat `server.xml` or `Context.xml` used for DataSources.

   For example:

```
url="jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)(HOST =
dbsrvhostname.in.oracle.com)(PORT = 2484)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME=DBAAIB)) (security=(ssl_server_cert_dn=CN= dbsrvhostname)))"
```

13.3.2 Configuring OFSAA and WebLogic as Web Application Server with Oracle Wallet

1. On Primary WebLogic Server instance, since there is no Oracle Client on the WebLogic Server instance, manually create a directory called "network" and copy `tnsnames.ora`, `sqlnet.ora` files into the "network" folder. Copy complete wallet directory "clientwallet" configured from OFSAA layer.
2. Modify `sqlnet.ora` with new WALLET_LOCATION path.

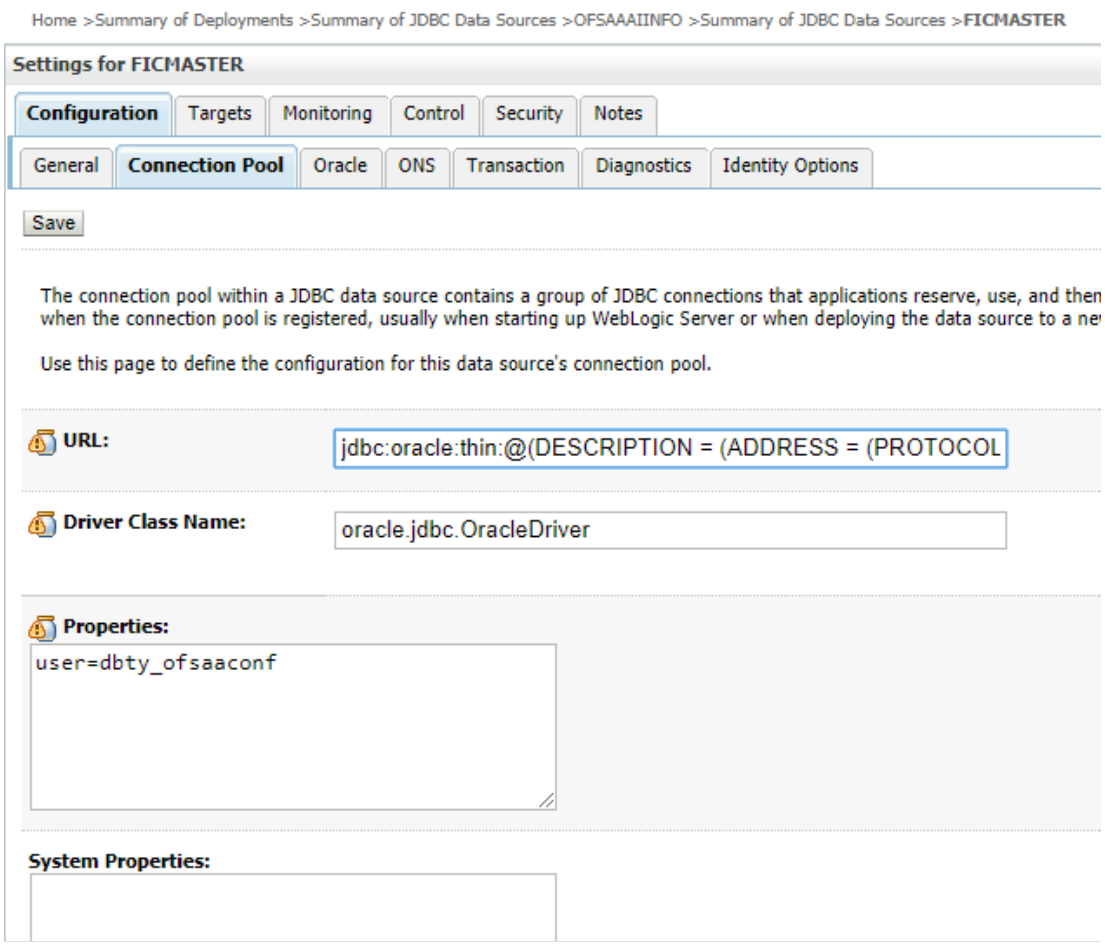
NOTE Make sure the TNS_ADMIN and WALLET LOCATION are under *Domain* directory so that after Cluster configuration it is being copied to secondary Weblogic Server instances manually. For more information on clustered setup configuration, see Configuring OFSAA in Clustered Environment Guide .

3. Add parameters and its values (`-Doracle.net.tns_admin`, `- Doracle.net.ssl_server_dn_match`, `-Djavax.net.ssl.trustStoreType`, `- Djavax.net.ssl.trustStore`, `-Doracle.net.ssl_version` and `-Doracle.net.wallet_location`) in the `setDomainEnv.sh` file as given:

```
JAVA_PROPERTIES="${JAVA_PROPERTIES} ${EXTRA_JAVA_PROPERTIES}
-Doracle.net.tns_admin=
/scratch/ssldbtest/Oracle/Middleware/Oracle_Home/user_projects/domains/DBAAAIB/network
-Doracle.net.wallet_location=
  (SOURCE=(METHOD=file)
  (METHOD_DATA=(DIRECTORY=
   /scratch/ssldbtest/Oracle/Middleware/Oracle_Home/user_projects/domains/DBAAAIB/clientwall
   et)
  )
-Djavax.net.ssl.trustStoreType=SSO
-
Djavax.net.ssl.trustStore=/scratch/ssldbtest/Oracle/Middleware/Oracle_Home/user_projects/dom
ains/DBAAAIB/clientwallet/cwallet.sso
-Doracle.net.ssl_version=1.2
-Doracle.net.ssl_server_dn_match=true
"
export JAVA_PROPERTIES
```

4. Copy the `ojdbc8.jar` file from the `$FIC_HOME/ficapp/common/FICServer/lib` directory into the <WL_HOME>/common/lib/oracle.jdbc located jdbc drivers directory.
5. Login to the **WLS Admin console** and edit the **WLS JNDI Data Source** connection pool details.

Figure 66: OFSAA and WebLogic as Web Application Server Configuration window

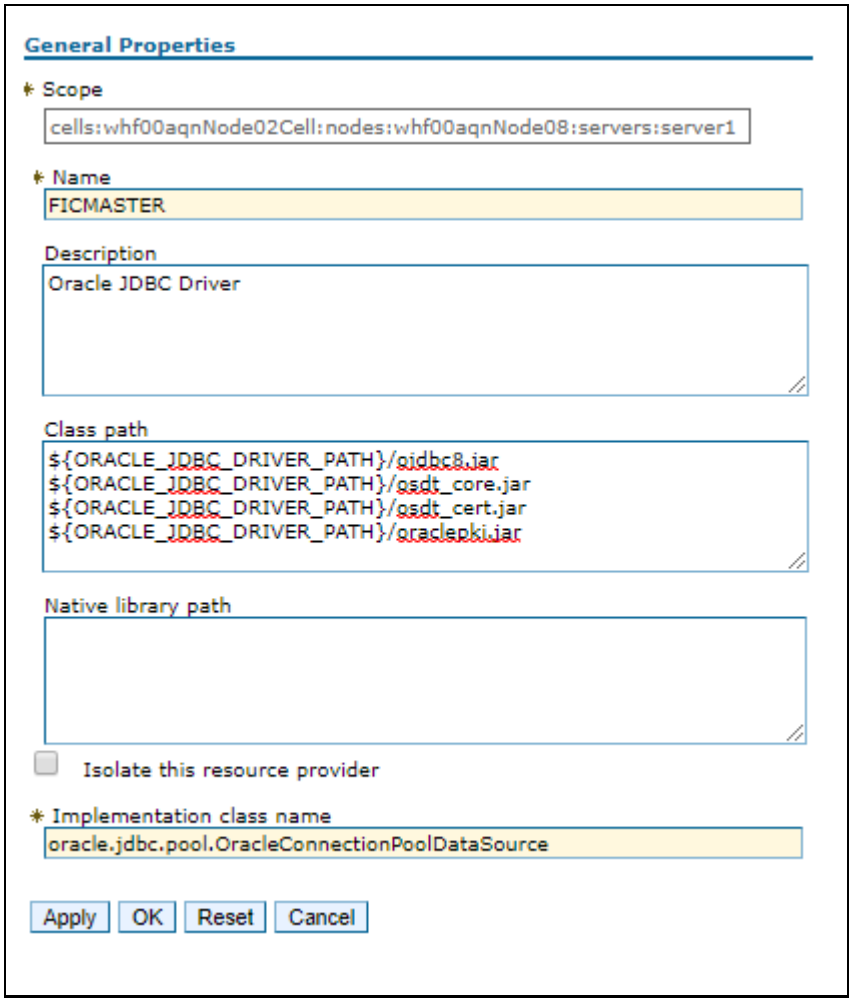


6. Modify **URL** and **Properties** values as displayed in the figure.
7. Similarly, edit the **WLS JNDI Data Source** connections **ATOMIC** and **SANDBOX** schemas, and perform a Test Connection on each data source.

13.3.3 Configuring OFSAA and WebSphere as Web Application Server with Oracle Wallet

1. Since there is no Oracle Client on the WebSphere server instance, manually create a directory called "network" and copy `tnsnames.ora`, `sqlnet.ora` files into the "network" folder. Copy complete wallet directory "clientwallet" configured from OFSAA layer.
2. Modify `sqlnet.ora` with new WALLET_LOCATION path.
3. Copy `ojdbc8.jar` and oracle PKI related jars `oraclepki.jar`, `osdt_cert.jar` and `osdt_core.jar` from `$FIC_HOME/ficapp/common/FICServer/lib` into <WebSphere located jdbc drivers> (that is usually referred in WebSphere as `${ORACLE_JDBC_DRIVER_PATH})`.
4. In the WebSphere console, navigate to *Resources >JDBC>JDBC Providers*, and click the link that corresponds to OFSAA Config, Atomic and Sandbox. Then add the references of oracle PKI related jars. Click OK and save to Master configuration.

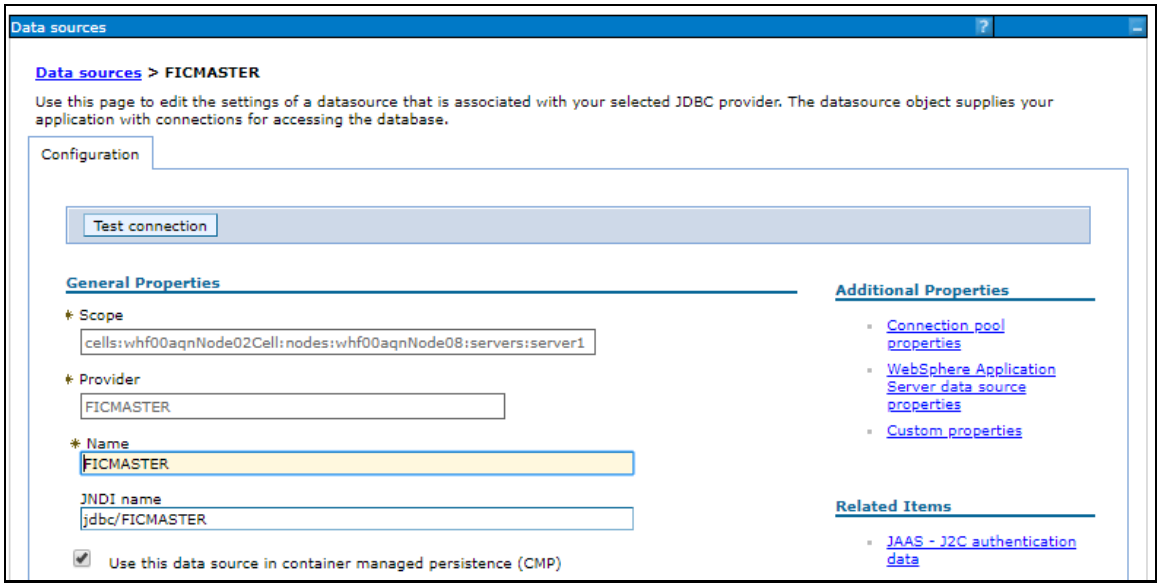
Figure 67: General Properties window



TIP This Step requires restart of WebSphere profile restart.

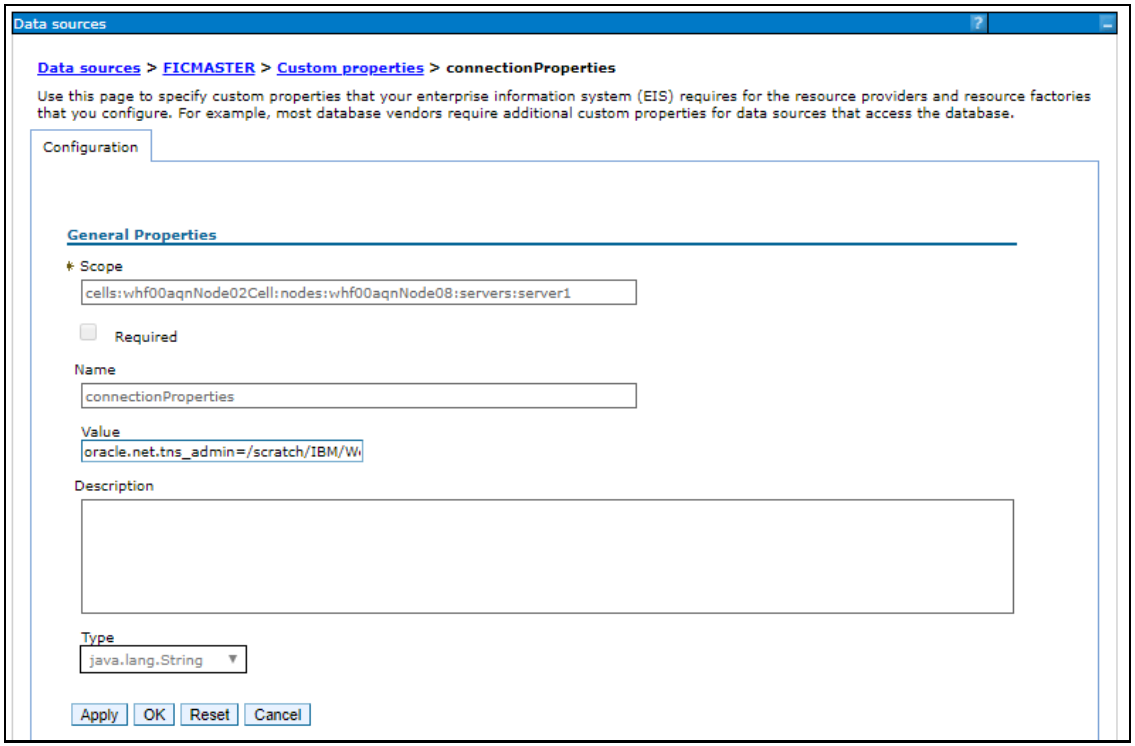
5. Navigate to *Resources>JDBC>Data sources*, and click the link that corresponds to Config, Atomic and Sandbox Datasource to update to use SSL.

Figure 68: Data Source Configuration window



6. From the *Additional Properties* pane, click **Custom properties**.
7. Add "connectionProperties" with a value of
`javax.net.ssl.trustStore=<wallet_locatioin>/cwallet.sso;javax.net.ssl.trustStoreType=SSO;oracle.net.ssl_version=1.2;oracle.net.ssl_server_dn_match=true; oracle.net.tns_admin=<path of network folder>;oracle.net.wallet_location=(SOURCE=(METHOD=file)(METHOD_DATA=(DIRECTORY=<wallet_locatioin>)))`

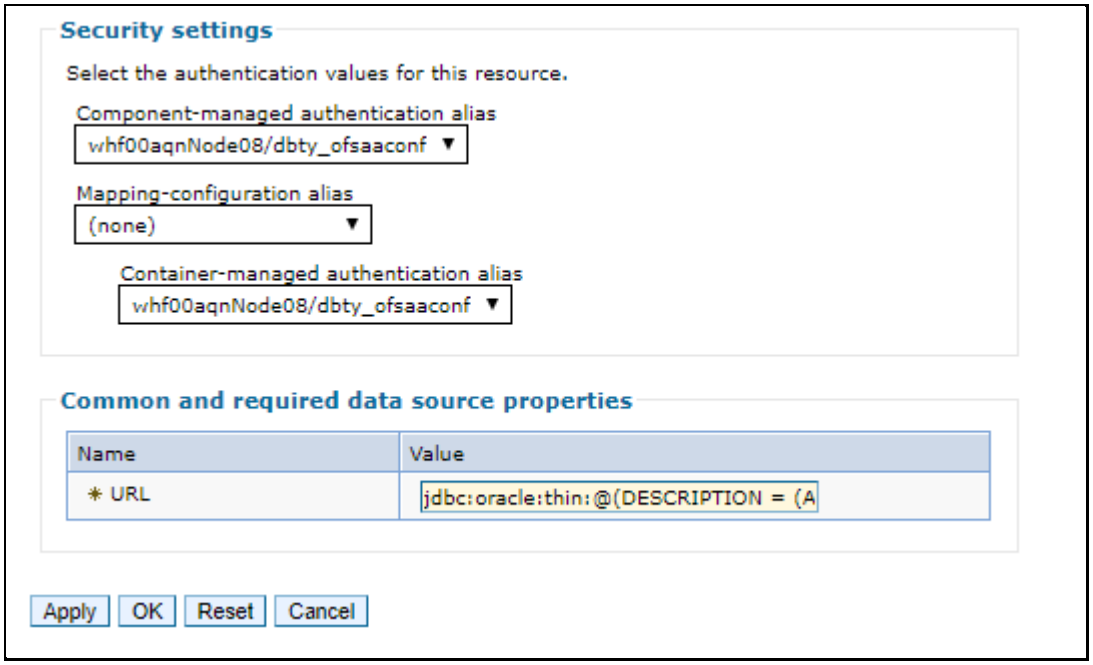
Figure 69: Data Source Configuration window



8. Click **OK** and return to the main Datasource configuration page. Scroll down to the bottom where the connection properties are displayed and update the **URL** to the SSL value.

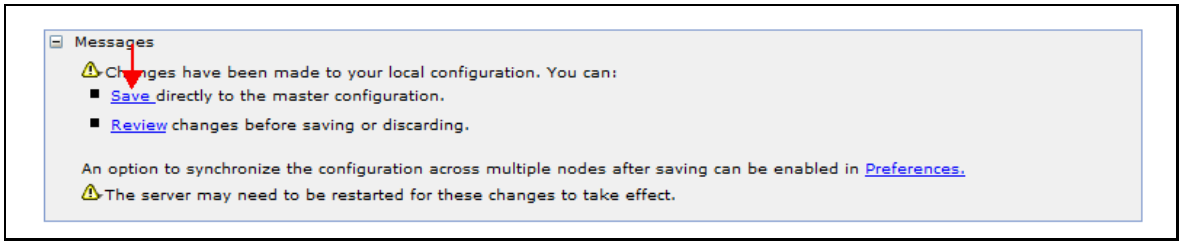
   For example,
   `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=db_host_name)(PORT=security_port))(CONNECT_DATA=(SERVICE_NAME=database_alias)))`

Figure 70: Security settings window



9. Click **Save directly to the master configuration**.

Figure 71: Messages pane



10. Click **Test connection** to test the connection to Oracle server through secured port.

13.4 Generating EAR/WAR Files

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.

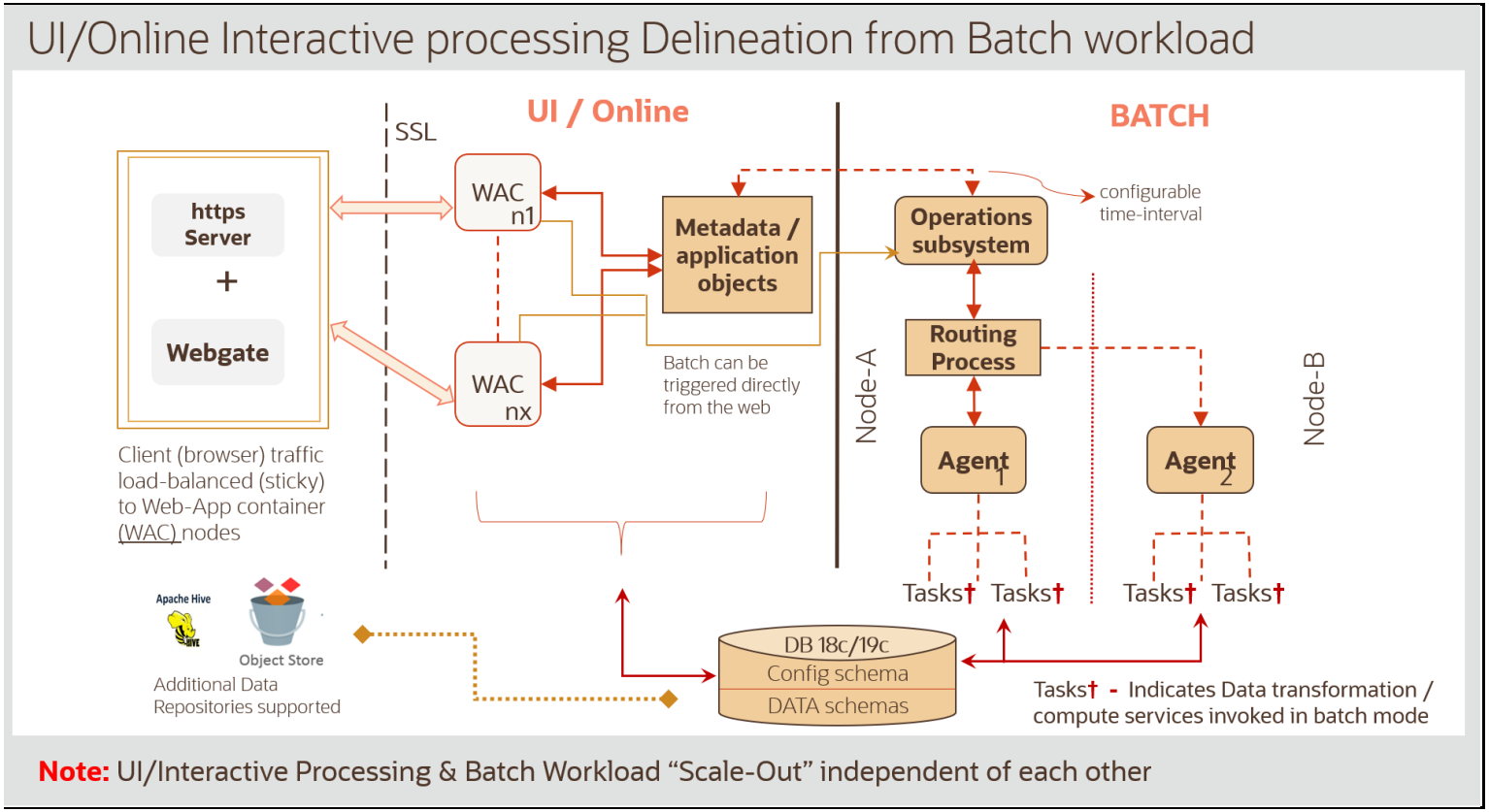
13.5 Configuring Password Changes

If you want the change the password for config and atomic schema of a target environment, refer to **Modify OFSAA Infrastructure Config Schema Password in a Non Wallet-Based Setup and** section and **Modify OFSAA Infrastructure Atomic Schema Password in a Non Wallet-Based Setup** in Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide for the specific release at the Oracle Help Center.

> **NOTE** The information in this section applies to OFSAAI v8.1.1.0.0 and later versions.

14 Appendix A – Distributed Activation Manager Deployment

Figure 72: Illustration of Distributed Activation Manager Deployment



15 Appendix B – Additional Information in REST APIs for User Status and User Access Reports

In addition to the REST API Endpoints discussed in the Using REST APIs for User Management from Third-Party IDMs Section, the User Status Report and User Access Report have more fields that are part of the Get Response populates additional fields in v8.1.2.0.0+ on applying the **33150367** One-off Patch from My Oracle Support.

Topics:

15.1 Prerequisites

- See the Using REST APIs for User Management from Third-Party IDMs Section for information about REST APIs in OFSAA.
- You must apply the **33150367** One-off Patch from My Oracle Support.
-

15.2 Reference Table

The following table provides details for the Additional REST API Specifications for User Status Report and User Access Report:

Table 24: User Status and User Access Reports - Additional REST API Specifications

No	Requirement	URL	Method Type	Request	Sample Request JSON	Comments
1	User Status Report	/rest-api/v1/user/status?userId=<USERID>&userName=<USERNAME>&idledays=<Number of days idle>&gsUserID=<Logged-in user>&loggedIp=<IP Address>&enable=<Y/N>&delete=<Y/N>&loggedIn=<Y/N>	GET	-	For example: https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/status?userId=exampleUserID&userName=exampleUserName&idledays=&gsUserID=SYSADMN&loggedIp=<192.0.2.1>&enable=Y&delete=N&loggedIn=Y	The JSON request displays the Report for the deleted, disabled, currently logged in, and idle Users. **Note**: • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • idledays is the number of days (INTEGER) the user has not logged into the system. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • enable is the flag to determine if the user is enabled or disabled in the system. The valid values are **Y** for yes and **N** for no. • delete is the flag to determine if the user is deleted in the system. The valid values are **Y** for yes and **N** for no. • loggedIn is the flag to determine if the user is currently logged into the system. The valid values are **Y** for yes and **N** for no. • Oracle recommends that you copy and paste the URL and modify the placeholders. • In addition, the fields shown in the next row are added to the User Status Report:

No	Requirement	URL	Method Type	Request	Sample Request JSON	Comments
						• Start Date - Displays the Start Date configured of the period for the User to be active in the system. • End Date - Displays the End Date configured of the period for the User to be active in the system. • Login Holidays - Displays whether the user is allowed to access the system on holidays or not. • SMS Auth Only - Displays if the User can be authenticated through SMS. • Created Date - Displays the date on which the User was created in the system. • Last Modified Date - Displays the date on which the details of the User were last updated in the system. • Last Password Change Date - Displays the date when the password was changed the last time around for the User. • Last Enabled Date - Displays the date when the User was last enabled in the system. • Last Disabled Date - Displays the date when the User was last disabled in the system. • Deleted Date - Displays the date when the User was deleted from the system.

No	Requirement	URL	Method Type	Request	Sample Request JSON	Comments
2	User Access Report	/rest-api/v1/user/useraccess?userId=<USERID>&userName=<USERNAME>&gsUserID=<Logged-in User>&loggedIp=<IP Address>	GET	-	For example: https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/useraccess?userId=exampleUserID&userName=exampleUserName&gsUserID=SYSADMN&loggedIp=<192.0.2.1>	The JSON request displays the Report for User Access Rights. **Note**: • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Oracle recommends that you copy the URL and modify the placeholders. • In addition to the textbox Search Filters such as User ID and User Name, you can also search with the check box Search Filters: Group, Role, and Functions. See the following rows for details.

No	Requirement	URL	Method Type	Request	Sample Request JSON	Comments
3	User Access Report – group=Y	/rest-api/v1/user/useraccess?userId=<USERID>&userName=<USERNAME>&gsUserID=<Logged-in User>&loggedIp=<IP Address>&group=Y	GET		For example: https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/useraccess?userId=exampleUserID&userName=exampleUserName&gsUserID=SYSADMN&loggedIp=<192.0.2.1>&group=Y	The JSON request displays the Report for User Access Rights. **Note**: • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Groups mapped to the selected user are displayed. The valid value is Y. • Oracle recommends that you copy the URL and modify the placeholders.

No	Requirement	URL	Method Type	Request	Sample Request JSON	Comments
4	User Access Report – role=Y	/rest-api/v1/user/useraccess?userId=<USERID>&userName=<USERNAME>&gsUserID=<Logged-in User>&loggedIp=<IP Address>&role=Y	GET		For example: https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/useraccess?userId=exampleUserID&userName=exampleUserName&gsUserID=SYSADMN&loggedIp=<192.0.2.1>&role=Y	The JSON request displays the Report for User Access Rights. **Note**: • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Groups and Roles mapped to the selected user are displayed The valid value is Y. • Oracle recommends that you copy the URL and modify the placeholders.

No	Requirement	URL	Method Type	Request	Sample Request JSON	Comments
5	User Access Report – function=Y	/rest-api/v1/user/useraccess?userId=<USERID>&userName=<USERNAME>&gsUserID=<Logged-in User>&loggedIp=<IP Address>&function=Y	GET		For example: https://<HOST_NAME:PORT>/<CONTEXTNAME>/rest-api/v1/user/useraccess?userId=exampleUserID&userName=exampleUserName&gsUserID=SYSADMN&loggedIp=<192.0.2.1>&function=Y	The JSON request displays the Report for User Access Rights. **Note**: • If you do not enter the values for the **gsUserID** and **loggedIp** attributes in this API, the transaction is not recorded in audit. • If you do not enter the values for the **userId** and **userName** attributes in this API, the records for all the users is displayed. • userID is the OFSAA identifier of the User for whom the report is to be generated. • userName is the OFSAA login name for the above User ID. • gsUserID is the User ID of the user logged in and accessing the system. • loggedIP is the IPv4 address of the workstation from where the RESTful API IP is invoked. An alternative is to configure it to the loopback address 127.0.0.1. • Groups, Roles, and Functions mapped to the selected user are displayed. The valid value is Y. • Oracle recommends that you copy the URL and modify the placeholders.

OFSAA Support

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

Send Us Your Comments

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

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

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

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

ORACLE