Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack

Administration and Configuration Guide

Release 8.0 - 8.0.5.x.x

ORACLE
FINANCIAL SERVICES

DOCUMENT CONTROL

Version Number	Revision Date	Changes Done
1.0	Created Jan 2015	Captured the administration configurations for OFS AAAI Application Pack 8.0.0.0.0.
1.1	Sep 2015	Restructured the guide and removed irrelevant sections.
2.0	Dec 2015	Added 8.0.2.0.0 related configurations
3.0	Dec 2015	Added a new section Changing IP/ Hostname, Ports, Deployed paths of the OFSAA Instance
4.0	Jan 2016	Added Workflow Manager Configurations chapter.
5.0	Feb 2016	Added Transferring Batch Ownership section as per Bug 22103206.
6.0	Feb 2016	Added SCD Execution on Hive Information Domain section.
7.0	May 2016	Added a prerequisite for PortC utility based on Bug 22554485. Added LDAP Configuration section, which was earlier present in I&C guide.
8.0	July 2016	Added configurations required for 8.0.3.0.0 release.
9.0	Oct 2016	Updated as per Bug 22554485.
10.0	Jan 2017	Added 8.0.4.0.0 related changes: ▪ Updated section ‘LDAP Configuration’ with a note for being not applicable for Release 8.0.4.0.0 and later. ▪ Updated LDAP to SMS information in section ‘Migrate Data from CSSMS tables to LDAP server and from LDAP to SMS. ▪ Public Key Authentication configurations are introduced. ▪ Sqoop 1 in cluster mode configurations are introduced.
11.0	June 2017	Added the following sections for Bug 25699783: ▪ Enable and Disable Users ▪ Password Reset Updated section ‘Questionnaire Setup and Configuration Details’ for Bug 26200436. Updated Jars details as per Bug 25835648.

Version Number	Revision Date	Changes Done
12.0	Aug 2017	▪ Added configurations required for Distributed AM processing. ▪ Added section Configuring Components, Dimensions, and Static Options for JIRA OFSAAAAI-8431. ▪ Added details for Bug 25768642.
13.0	Sep 2017	Added section 5.1 ‘Using X-Frame-Options to Embed OFSAA Content on your Site’ for Bug 26788350.
14.0	Oct 2017	▪ Added section ‘Registering and Invoking your Application's Customized Workflow’ (JIRA OFSAAAAI-9113). ▪ Modified *Distributed AM Based Processing* section ▪ Added *Configuring Attributes for Attribute Expression Application Rule* section ▪ Added section ‘Configuring OFSAA OIM Connector’ (JIRA OFSAAAAI-10062).
15.0	Jan 2018	Added 8.0.2.2.0, 8.0.3.3.0, 8.0.4.2.0 and 8.0.5.1.0 ML changes.
16.0	Feb 2018	Added updates for JIRA OFSAAAAI-12376.
17.0	Apr 2018	▪ Added configurations for CMIS Integration in Forms Framework. ▪ Added Enabling Proxy for Webservices Rule section
18.0	Jun 2018	Added updates for JIRA OFSAAAAI-14207 and OFSAAAAI-13230.
19.0	Jul 2018	Updated for OFSAAAAI-13230.
20.0	Sep 2018	Added HTTPS Protocol section based on Bug 27821807.
21.0	Jun 2019	Added additional information for Tectia configuration in section Other SSH Software (Doc 29771662).
22.0	Jan 2020	Added for Doc 30881993: ▪ Information to create and deploy EAR/WAR in the sections Running Port Changer Utility and Running Port Changer Utility for 8.0.2.2.0, 8.0.3.3.0, 8.0.4.2.0 and 8.0.5.1.0. ▪ Note for table batch_parameter in the section Running Port Changer Utility.
Created by: Brijesh/Gitcy	Reviewed by: Jeev/Suresh	Approved by: Subhashini/Virupaksha

NOTE: For the configurations for OFSAA Release 8.0.6.0.0, see OFS Analytical Applications Infrastructure Administration Guide.

TABLE OF CONTENTS

Preface

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

- Summary
- Audience
- Related Documents
- Conventions

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.

Audience

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

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

Conventions

The following text conventions are 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.

Abbreviations

The following table lists the abbreviations used in this document:

Abbreviations	Meaning
AIX	Advanced Interactive eXecutive
CDH	Cloudera Distribution Including Apache Hadoop
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
KBD	Key Business Dimensions
OEL	Oracle Enterprise Linux
OFSAAI	Oracle Financial Services Analytical Applications Infrastructure
OLH	Oracle Loader for Hadoop
RDBMS	Relational Database Management System
RHEL	Red Hat Enterprise Linux
RRF	Run Rule Framework
SCD	Slowly Changing Dimension

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

1 Data Management Tools Module Configurations

This chapter details about the configurations required in the Data Management Tools module. It includes the following sections:

- Data Mapping Configurations
- Data File Mapping Configurations
- Oracle® Loader for Hadoop (OLH) Configuration
- Sqoop Configuration
- SCD Execution on Hive Information Domain

1.1 Data Mapping Configurations

This is applicable from OFSAAI version 8.0.2.0.0.

This section talks about the configurations required for data movement involving Hive based source or target. This is required only if you have enabled Big Data Processing within your application pack.

- HDFS-Hive source to RDBMS target(H2T)
- HDFS-Hive source to HDFS target (H2H)
- RDBMS source to HDFS-Hive target (T2H)
- HDFS-Hive source to Flat File target (H2F)
- HDFS/Local-WebLog Source to HDFS Target (L2H)

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

1.1.1.1 Default Implementation

The following property needs to be set in the ETLLoader.properties file which is present in `$FICDB_HOME/conf`:

- `H2TMode=default`

1.1.1.2 OLH (Oracle Loader for Hadoop) Implementation

OLH (Oracle Loader for Hadoop) should have been installed and configured in your system. For more information, see Oracle® Loader for Hadoop (OLH) Configuration.

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, Data Type DATE (that is supported in HIVE 12) is not supported by OLH.

1.1.1.3 Sqoop Implementation

Sqoop should have been installed and configured in your system.

Two types of Sqoop implementations are supported:

- **Sqoop 1** (Sqoop 1.4x) – in Client mode. Using Sqoop export
- **Sqoop 1** (Sqoop 1.4x) – in Cluster mode. OFSAAI first SSHs to the Sqoop node on the cluster, and then executes the export command.

For more information, see Sqoop Configuration.

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

1.1.2.1 Default Implementation

The following property needs to be set in the ETLLoader.properties file which is present in `$FICDB_HOME/conf`:

- `T2HMode=default`
- `ISHIVELOCAL`
  - YES - If Hive and OFSAA are installed on the same Virtual Machine (VM)
  - NO - If Hive and OFSAA are on different VM’s
- `HIVESERVER_NAME` – IP address of the Hive Server
- `HIVESERVE_PORT` – FTP Port of the Hive Server
- `HIVESERVER_FTPDRIVE` – The shared path on the Hive VM
- `HIVESERVER_FTPSHARENAME` – Used only in windows, this is not supported now.
- `HIVESERVER_FTP_USERID` – FTP User ID
- `HIVESERVER_FTP_PASSWORD` – Password required for FTP connection

1.1.2.2 Sqoop Implementation

Sqoop should have been installed and configured in your system. For more information, see Sqoop Configuration.

Three types of Sqoop implementations are supported:

1. **Sqoop 1** (Sqoop 1.4x) – in Client mode. Using Sqoop import
2. **Sqoop 1** (Sqoop 1.4x) – in Cluster mode. OFSAAI first SSHs to the Sqoop node on the cluster, and then executes the import command.

Limitations of Sqoop 1:

- 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.

3. **Sqoop 2** (Sqoop 1.9 x)

   Limitations of Sqoop 2:

   - It does not support Secured Clusters.

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

This is applicable from OFSAAI version 8.0.3.0.0.

1.1.3.1 Prerequisites

- CDH4 or Apache Hadoop 2.2.0
- Create a Folder /<Weblog Working Directory> in HDFS and provide 0777 permissions for the same.

1.1.3.2 Configurations

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

1. Set the following properties in the `ETLLoader.properties` file that is present in `$FICDB_HOME/conf`:
   - `WEBLOG_WORKING_DIR`- Temporary working directory in HDFS
   - `KEEP_WEBLOG_PROCESSED_FILES`
     - YES- The working directory will be retained with the processed WebLog files. If the data loading was successful, the WebLog file name will be appended with Processed. Else, the WebLog file name will be appended with Working.
     - NO- The working directory will be deleted after data loading.

   For example,

   ```
    <PROPERTY ID="WEBLOG_WORKING_DIR" VALUE="/user/ofsaa/WebLogWork"/>
   <PROPERTY ID="KEEP_WEBLOG_PROCESSED_FILES" VALUE="YES"/>
   ```

2. Configure the `Clusters.XML` file located at `$FIC_HOME/conf/folder.`

   Clusters.XML file is used to configure Hadoop Cluster information in OFSAA. The file will have configuration tags to configure both secured and non-secured Hadoop Clusters.

NOTE: Execution of L2H (with a Local File System based WebLog source) expects an entry with CLUSTER ID as "DEFAULT", and the cluster tag should contain cluster details of the target information domain.

For the Secured Hadoop Cluster tag, enter the details as tabulated:

Tag Name	Description	Example
`Cluster ID`	Unique ID to identify the Hadoop Cluster	`DEFAULT`
`Name`	Name of the cluster	
`AUTHTYPE`	Supported Authentication Types are Kerberos with Keytab (KRB) and Default (non-secured).	`KRB-` Kerberos with Key Tab
`PRINCIPAL`	Kerberos Principal name	
`CONFPATH`	Path where Kerberos Configuration files reside.	`/scratch/ofsaaapp/AAAI_HOME/conf`
`KEYTAB`	Name of the Key Tab file.	`xxxx.keytab`
`REALM`	Name of the Kerberos Realm file.	`krb5.conf`
`CORESITE`	Name of `core-site.xml`	`core-site.xml`
`HDFSSITE`	Name of `hdfs-site.xml`	`hdfs-site.xml`
`MAPREDSITE`	Name of `mapred-site.xml`	`mapred-site.xml`
`YARNSITE`	Name of `yarn-site.xml`	`yarn-site.xml`
`DESCRIPTION`	Description for the cluster tag	
`CREATEDBY`	Date on which the cluster tag is created	
`CREATETIME`	Time on which the cluster tag is created	

For example:

```
<CLUSTER ID="DEFAULT">
<NAME>DEFAULT</NAME>
<AUTHTYPE>KRB</AUTHTYPE>
<PRINCIPAL>ofsaa</PRINCIPAL>
<CONFPATH>/scratch/ofsaaapp/AAAI_HOME/conf</CONFPATH>
<KEYTAB>ofsaa2.keytab</KEYTAB>
<REALM>krb5_All.conf</REALM>
```

```
<CORESITE>core-site.xml</CORESITE>
<HDFSSITE>hdfs-site.xml</HDFSSITE>
<MAPREDSITE>mapred-site.xml</MAPREDSITE>
<YARNSITE>yarn-site.xml</YARNSITE>
<DESCRIPTION>Cloudera   Distribution   for   Hadoop   with   Hive
0.13.1</DESCRIPTION>
<CREATEDBY>sysadmn</CREATEDBY>
<CREATETIME>2015/05/18 04:24:49 PM</CREATETIME>
```

For the non-secured Cluster tag, enter the details as tabulated:

Tag Name	Description	Example
Cluster ID	Unique ID to identify the Hadoop Cluster	DEFAULT
Name	Name of the cluster	
AUTHTYPE	Supported Authentication Types are Kerberos with Keytab (KRB) and Default (non-secured).	DEFAULT- for non-secured
CONFPATH	Path where Kerberos Configuration files such as core-site.xml, hdfs-site.xml reside.	/scratch/ofsaaapp/AAAI_HOME/conf
CORESITE	Name of core-site.xml	core-site.xml
HDFSSITE	Name of hdfs-site.xml	hdfs-site.xml
MAPREDSITE	Name of mapred-site.xml	mapred-site.xml
YARNSITE	Name of yarn-site.xml	yarn-site.xml
DESCRIPTION	Description for the cluster tag	
CREATEDBY	Date on which the cluster tag is created	
CREATETIME	Time on which the cluster tag is created	

For example:

```
<CLUSTER ID="NONSECURECLUSTER">

<NAME>NONSECURECLUSTER</NAME>
<AUTHTYPE>DEFAULT</AUTHTYPE>
<CONFPATH>/scratch/ofsaaapp/AAAI_HOME/conf</CONFPATH></CONFPATH>
<CORESITE>core-site.xml</CORESITE>
```

```
<HDFSSITE>hdfs-site.xml</HDFSSITE>
<MAPREDSITE>mapred-site.xml</MAPREDSITE>
<YARNSITE>yarn-site.xml</YARNSITE>
<DESCRIPTION>Details of the Non-Secure Cluster</DESCRIPTION>
<CREATEDBY>NA</CREATEDBY>
<CREATETIME>NA</CREATETIME>
```

Add additional CLUSTER tags to add more clusters.

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

   - `avro-1.7.4.jar`
   - `commons-cli-1.2.jar`
   - `commons-httpclient-3.1.jar`
   - `hadoop-hdfs-2.0.0-cdh4.7.0.jar`
   - `jackson-core-asl-1.8.8.jar`
   - `jackson-mapper-asl-1.8.8.jar`
   - `protobuf-java-2.4.0a.jar`
   - `servlet-api.jar`
   - `htrace-core-3.0.4.jar`

NOTE: Version of Jars depends on the CDH Version and the Drivers used. For CDH 5.8.4 version, additionally `htrace-core4-4.0.1-incubating.jar` has to be copied.

Below jars are needed but will already be present in the `$FIC_HOME/ext/lib` folder as part of CDH Enablement.

- `commons-configuration-1.6.jar`
- `commons-collections-3.2.2.jar`
- `commons-io-2.4.jar`
- `commons-logging-1.0.4.jar`
- `hadoop-auth-2.0.0-cdh4.7.0.jar`
- `hadoop-common-2.0.0-cdh4.7.0.jar`
- `hadoop-core-2.0.0-mr1-cdh4.7.0.jar`
- `libfb303-0.9.0.jar`
- `libthrift-0.9.0-cdh4-1.jar`

- `slf4j-api-1.6.4.jar`

NOTE: The version of jars to be copied will differ depending upon the version of CDH configured.

4. Copy `core-site.xml, hdfs-site.xml, mapred-site.xml, hive-site.xml`, and `yarn-site.xml` from the Hadoop Cluster to the path mentioned in the `Clusters.XML` file. Note that only Client Configuration Properties are required.

   If Cloudera Manager is used, the same can be downloaded directly which will contain only the client properties.

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.

For more information, refer http://www.cloudera.com/content/cloudera/en/documentation/cdh4/v4-3-0/CDH4-Security-Guide/cdh4sg_topic_3_16.html

1.1.3.3 Logger Types Seeded Table

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

Below are the sample entries for the logger types.

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,	DELIMITED~,

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

- `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 will be 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 the 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. User 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 will be displayed as **Input Regex** in the *Source Model Generation* window.

1.2 Data File Mapping Configurations

This is applicable from OFSAAI version 8.0.2.0.0.

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

1.2.1 Flat File Present in the Local File System (LFS)

The following property needs to be set in the ETLLoader.properties file which is present in $FICDB_HOME/conf:

- ISHIVELOCAL
  - YES - If Hive and OFSAA are installed on the same Virtual Machine (VM)
  - NO - If Hive and OFSAA are on different VM's
- HIVESERVER_NAME – IP address of the Hive Server
- HIVESERVE_PORT – FTP Port of the Hive Server
- HIVESERVER_FTPDRIVE – The shared path on the Hive VM
- HIVESERVER_FTPSHARENAME – Used only in windows, this is not supported now.
- HIVESERVER_FTP_USERID – FTP User ID
- HIVESERVER_FTP_PASSWORD – Password required for FTP connection

NOTE: Set the properties depending on whether the HIVE server and OFSAA are running on the same Virtual Machine (VM).

1.3 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 RDBMS Tables from Hive Tables.

1.3.1 Prerequisite

- CDH4.7 or CDH 5.2.1 should have been installed.
- Apache Hive 0.10.0 should have been installed.
- Hadoop Client (version compatible with the Hadoop Cluster) should have been installed on OFSAAI VM. (If OFSAAI and Hadoop are not on the same VM)
- Oracle Loader for Hadoop v 3.0 should have been installed on the OFSAAI VM.

1.3.2 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 OFSSAI is installed.

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

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

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

Step 2 : Configuring the Properties Files

1. Set the following property in the ETLLoader.properties file which is present in the location `$FIC_DB_HOME/conf/`:

   ```
   <PROPERTY ID="H2TMode" VALUE="OLH"/>
   ```

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

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

STEP 3: Copy Configuration xmls from Hadoop Cluster

1. Copy the following files from the Hadoop Cluster to `$FIC_HOME/conf folder`.

   - core-site.xml
   - hdfs-site.xml

- mapred-site.xml
- hive-site.xml
- yarn-site.xml

NOTE: Only Client Configuration Properties are required. If Cloudera Manager is used, the same can be downloaded directly which will contain only the client properties.

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

```
<property>
    <name>mapred.child.java.opts</name>
    <value>-Xmx4096m</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. For more information, see CDH4 Security Guide.
The version of jars to be copied will differ depending upon the version of CDH configured.

STEP 4: Copy the required Jars

- If OFSSAI 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, do the following steps:

  - Edit the `oracle.hadoop.loader.libjars` property present in `OLH_HOME/doc/oraloader-conf.xml` 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 `FIC_DB_HOME/conf/dtextInput.xml`

- If OFSSAI is using Cloudera Connectors

  OLH is not qualified on Cloudera Connectors. Perform the following workaround:

  - Copy the following jars (Apache Drivers) to `OLH_HOME/jlib`.

    ```
    hive-exec-*.jar, libfb303-*.jar, hive-service-*.jar, hive-metastore-*.jar
    ```

  Usually these jars are added to the Classpath. In case of any ClassNotFound Exception, do the following steps:

- Edit the `oracle.hadoop.loader.libjars` property present in `OLH_HOME/doc/oraloader-conf.xml` to accommodate the newly added jars. That is, `${oracle.hadoop.loader.olh_home}/jlib/ hive-exec-*.jar`
- Copy the entire property to `FIC_DB_HOME/conf/dtextInput.xml`

NOTE: Add the above mentioned 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`.

1.3.3 Limitations

- Mapping a Hive column with Data Type STRING (even if it contains a single character) to a RDBMS Column with 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.
- OLH is not supported with Cloudera Connectors. As a workaround, perform Step 4.

1.4 Sqoop Configuration

Sqoop installation through Cloudera® Manager allows the user to load Data into Hive Tables from RDBMS Tables.

1.4.1 Prerequisites

- CDH4 or Apache Hadoop 2.2.0.
- Sqoop 1 & Sqoop 2(installed with CDH)
- Create a Folder /<Sqoop Working Directory> in HDFS and provide 0777 permissions for the same.
- Sqoop Server should be up and running.
- Make sure that an appropriate jdbc driver is present in Sqoop library path on the cluster.

1.4.2 Steps for Configuring Sqoop

1.4.2.1 Sqoop 1 Cluster Mode

```
<PROPERTY ID="H2TMode" VALUE="SQOOP"/>
<PROPERTY ID="T2HMode" VALUE="SQOOP"/>
<PROPERTY ID="SQOOP_VERSION" VALUE="1.44SSH"/>
<PROPERTY ID="SQOOPSERVER_NAME" VALUE=""/>
<PROPERTY ID="SQOOPSERVER_SSH_PORT" VALUE="<SSH Port of the
SQOOP Server>"/>
```

```
<PROPERTY ID="SQOOPSERVER_SSH_USERID" VALUE="<SSH User ID of the
SQOOP Server>"/>
<PROPERTY ID="SQOOPSERVER_SSH_PASSWORD" VALUE="<SSH Password of
the Sqoop Server>"/>
<PROPERTY ID="SQOOPSERVER_SSH_ALIAS" VALUE="<Create Auth
Alias.>"/>
```

Perform the following steps to create Auth Alias:

a) Login 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** button for **Alias Name**.
e) Enter an **Auth Alias**, enter a valid SSH username in **User/Principal Name** and enter 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 anything else.

NOTE: The `SQOOPSERVER_SSH_ALIAS` is introduced in 8.0.5.2.0 and 8.0.4.3.0. You need to manually add the property tag `SQOOPSERVER_SSH_ALIAS` as given above. It should be used instead of `SQOOPSERVER_SSH_USERID` and `SQOOPSERVER_SSH_PASSWORD` properties. Restart of OFSAA services is not required after this change in `ETLLoader.properties` file.
If the `SQOOPSERVER_SSH_ALIAS` is not set or an invalid value is provided and `SQOOPSERVER_SSH_USERID` and `SQOOPSERVER_SSH_PASSWORD` properties have valid values, Sqoop execution will be successful.

```
<PROPERTY ID="SQOOP_PARAMS" VALUE="< any global sqoop
configuration to passed for sqoop execution. E.g. --direct --
compress. >"/>
<PROPERTY ID="SQOOP_USE_STAGING" VALUE="<Indicates if the sqoop
export creates a temporary staging table before inserting into
the destination table. Value can be YES or NO.>"/>
```

NOTE: `SQOOP_PARAMS` is supported for H2T/T2H only in SQOOP 1.44SSH mode.
`SQOOP_USE_STAGING` is supported only for H2T in SQOOP 1.44SSH mode.

In case, the cluster is Kerberos secured, add an additional property,

```
<PROPERTY ID="SQOOPSERVER_SSH_KINIT_COMMAND" VALUE="<Command to
be executed on the shell for Kerberos authentication. For
example, kinit -kt /home/ofsaa.keytab ofsaa@DEV.ORACLE.COM>"/>
```

All the above properties, except SQOOP_USE_STAGING, are valid for both Sqoop import and export. SQOOP_USE_STAGING is applicable only for Sqoop export.

NOTE: Copying of any Sqoop jars and Hadoop/Hive configuration XMLs to OFSAAI is not required in cluster mode.

1.4.2.2 Sqoop 1 Client Mode

STEP 1: Configuring the Properties File:

Set the following property in the `ETLLoader.properties` file which is present in the location `$FIC_DB_HOME/conf/`:

```
<PROPERTY ID="T2HMode" VALUE="SQOOP"/> or <PROPERTY ID="H2TMode"
VALUE="SQOOP"/>
<PROPERTY ID="SQOOPURL" VALUE="<Ip>:<Port>"/>
<PROPERTY ID="SQOOP_VERSION" VALUE="1.44"/>
<PROPERTY ID=”SQOOP_WORKING_DIR” VALUE=”<Path of a working
directory in HDFS, with 777 permissions for ofsaa>”
```

STEP 2: Copy Third Party Jars

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

- `avro-1.7.4.jar`
- `commons-cli-1.2.jar`
- `commons-httpclient-3.1.jar`
- `hadoop-hdfs-2.0.0-cdh4.7.0.jar`
- `jackson-core-asl-1.8.8.jar`
- `jackson-mapper-asl-1.8.8.jar`
- `protobuf-java-2.4.0a.jar`
- `servlet-api.jar`
- `sqoop-test-1.4.3-cdh4.7.0.jar`
- `sqoop-1.4.3-cdh4.7.0.jar`
- `htrace-core-3.0.4.jar`

NOTE: Version of Jars depends on the CDH Version and the Drivers used. For CDH 5.8.4 version, you should copy `htrace-core4-4.0.1-incubating.jar` instead of `htrace-core-3.0.4.jar`.

Following jars are needed, but may be present in the `$FIC_HOME/ext/lib` folder as part of CDH Enablement.

- `commons-configuration-1.6.jar`

- `commons-collections-3.2.2.jar`
- `commons-io-2.4.jar`
- `commons-logging-1.0.4.jar`
- `hadoop-auth-2.0.0-cdh4.7.0.jar`
- `hadoop-common-2.0.0-cdh4.7.0.jar`
- `hadoop-core-2.0.0-mr1-cdh4.7.0.jar`
- `libfb303-0.9.0.jar`
- `libthrift-0.9.0-cdh4-1.jar`
- `slf4j-api-1.6.4.jar`

NOTE: The version of jars to be copied will differ depending upon the version of CDH configured.

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 `$FIC_HOME/conf` folder. Note that only Client Configuration Properties are required.

If Cloudera Manager is used, the same can be downloaded directly which will contain only the client properties.

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.

1.4.2.3 Sqoop 2

STEP 1: Configuring the Properties File:

Set the following property in the `ETLLoader.properties` file which is present in the location `$FIC_DB_HOME/conf/`:

```
<PROPERTY ID="T2HMode" VALUE="SQOOP"/>
<PROPERTY ID="SQOOPURL" VALUE="<Ip>:<Port>"/>
<PROPERTY ID="SQOOP_VERSION" VALUE="1.99"/>
<PROPERTY ID=”SQOOP_WORKING_DIR” VALUE=”<Path of a working
directory in HDFS, with 777 permissions for ofsaa>”
```

STEP 2: Copy Third Party Jars

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

- `avro-1.7.4.jar`

- `commons-cli-1.2.jar`
- `commons-httpclient-3.1.jar`
- `hadoop-hdfs-2.0.0-cdh4.7.0.jar`
- `jackson-core-asl-1.8.8.jar`
- `jackson-mapper-asl-1.8.8.jar`
- `protobuf-java-2.4.0a.jar`
- `servlet-api.jar`
- `sqoop-test-1.4.3-cdh4.7.0.jar`
- `sqoop-1.4.3-cdh4.7.0.jar`
- `htrace-core-3.0.4.jar`

NOTE: Version of Jars depends on the CDH Version and the Drivers used. For CDH 5.8.4 version, you should copy `htrace-core4-4.0.1-incubating.jar` instead of `htrace-core-3.0.4.jar`.

Following jars are needed, but may be present in the `$FIC_HOME/ext/lib` folder as part of CDH Enablement.

- `commons-configuration-1.6.jar`
- `commons-collections-3.2.2.jar`
- `commons-io-2.4.jar`
- `commons-logging-1.0.4.jar`
- `hadoop-auth-2.0.0-cdh4.7.0.jar`
- `hadoop-common-2.0.0-cdh4.7.0.jar`
- `hadoop-core-2.0.0-mr1-cdh4.7.0.jar`
- `libfb303-0.9.0.jar`
- `libthrift-0.9.0-cdh4-1.jar`
- `slf4j-api-1.6.4.jar`

NOTE: The version of jars to be copied will differ depending upon the version of CDH configured.

1.4.3 Limitations:

Sqoop2 does not support Kerberized Clusters.

1.5 SCD Execution on Hive Information Domain

This is applicable from OFSAAI 8.0.2.0.0 version.

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

1.5.1 Prerequisites

- SCD on Hive Information Domain requires table to be present in the Datadom of Hive Information Domain. Execute the following create table script on Datadom of Hive Information Domain.:

```
CREATE TABLE DIM_SCD_SEEDED
(
SEEDED_SKEY BIGINT,
SEEDED_CODE String,
SEEDED_DESC String
)
ROW FORMAT DELIMITED FIELDS TERMINATED BY ',' STORED AS
INPUTFORMAT
'org.apache.hadoop.mapred.TextInputFormat' OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat';
```

- `DIM_SCD_SEEDED` table columns should be loaded with data values as mentioned in the following table:

SEEDED_SKEY	SEEDED_CODE	SEEDED_DESC
0	MSG	Missing
-1	OTH	Other

1.5.2 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.

1.5.3 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.

2 Dimension Management Module Configurations

This chapter details about the configurations required in the Dimension Management Module. It consists of the following sections:

- Configurations to use Alphanumeric and Numeric Codes for Dimension Members
- General Configurations for Dimension Management Module

2.1 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 external source systems, for which the members may be 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 will additionally store an alphanumeric member code. After performing the Dimension configuration explained in this section, the Alphanumeric Code field in the Member Definition (New Mode) window becomes editable. For more information, see *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 which 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 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.

2.1.1 Configure Alphanumeric Dimensions

To configure a numeric dimension as alphanumeric and to remove the optional code attribute from prior releases you have to 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 8.0, 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;
   ```

2.1.2 Configure Numeric Dimensions

If REV_DIMENSIONS_B.Member_Code_Column is populated for a dimension, any UI which displays an alphanumeric code will look in the specified column for the member's alphanumeric code. If REV_DIMENSIONS_B.Member_Code_Column is null, the UI will assume no alphanumeric code column exists in the member table and will display the alphanumeric code with the same value as the numeric code. Therefore, for numeric dimensions, you may want to 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 Rev_Dimensions_B for Numeric dimension, since the REV_DIMENSIONS_B.MEMBER_CODE_COLUMN column has value 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 value are stored in the same <DIM>_ID column.

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

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), this will cause the dimension loaders and seeded T2T extracts to 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 table REV_DIMENSIONS_B, if you have not done it already.
- Populate the Member Code Column entries for applicable dimensions.

  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;
    ```

2.1.3 Configure Alphanumeric Code in Simple Dimension Tables

For some editable seeded and user-defined simple dimensions, the alphanumeric code column currently might not be present in the data model. To add this column to a user-defined simple dimension table, you can use Model Upload. You will also need to 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.

2.1.4 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;
```

2.2 General Configurations for Dimension Management Module

These configuration changes are applicable when Dimension Management features provided in OFSAAI are used. You can open `AMHMConfig.properties` file present in the `$FIC_WEB_HOME/webroot/conf` directory to set the properties for the following:

- Member Deletion
- Attribute Default Date Format
- Members Reverse Population
- Hierarchy Reverse Population
- Maximum levels allowed in Hierarchies
- Node Limit for a Hierarchy Tree

Configuration for Dimension and Hierarchy Management has to be done only after the Application Pack installation is done. The properties specific to Information Domain are:

- `$INFODOM$`=<Name of the Information Domain>
- `$DIMENSION_ID$`=<Dimension ID for which the property to be set>

2.2.1.1 Configure Member Deletion

This property should be set to allow the user to delete the Members for the Dimension.

Value	Code	Example
# Member Deletion Configuration - VALUE- Y/N	MEMBER_DEL-$INFODOM$-$DIMENSION_ID$=$VALUE$	MEMBER_DEL-ORAFUSION-1=Y

2.2.1.2 Configure Attribute Default Date Format

This property should be set to display the Default Date Format for Date type Attribute in Attributes window.

Value	Code	Example
# Attribute Default Date Format - DB_DATE_FORMAT:DD-MON-YYYY	ATTR_DEF_DATE_FORMAT-$INFODOM$=DB_DATE_FORMAT	ATTR_DEF_DATE_FORMAT-ORAFUSION=DD/MON/YYYY

2.2.1.3 Configure Members Reverse Population

This property should be set for reverse population of Members for the Dimensions in required Information Domains.

Value	Code	Example
# Members Reverse population - VALUE- Y/N	MEMBER_REVERSE_POP-$INFODOM$-$DIMENSION_ID$=$VALUE$	MEMBER_REVERSE_POP-ORAFUSION-1=Y

2.2.1.4 Configure Hierarchy Reverse Population

This property should be set for reverse population of Hierarchies for the Dimensions in required Information Domains.

Value	Code	Example
#Hierarchy Reverse population - VALUE- Y/N	HIERARCHY_REVERSE_POP-$INFODOM$-$DIMENSION_ID$=$VALUE$	HIERARCHY_REVERSE_POP-ORAFUSION-1=Y

2.2.1.5 Configure Maximum Levels allowed in Hierarchies

This property is required to set the maximum levels allowed to build the Hierarchies tree structure.

Value	Code	Example
#Hierarchy Maximum level allowed for the hierarchy in particular Information Domain - VALUE - Integer number	MAX_DEPTH-$INFODOM$=$VALUE$	MAX_DEPTH-FUSION=15

The Maximum Levels allowed in the hierarchies is less than or equal to 15. If the Hierarchy Reverse population is set as "**Y**" and more than 15 levels are created. Then an alert is displayed as "The number of levels exceeding the limit".

If the maximum level allowed is set as more than 15 and hierarchy reverse population is set as "**Y**" then an error is displayed as "Error occurred in Reverse populating the hierarchy".

2.2.1.6 Configure Node Limit for a Hierarchy Tree

This property is required 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.

Value	Code	Example
#Tree node limit for the hierarchy - Values is Integer number	TREE_NODE_LIMIT=$VALUE$	TREE_NODE_LIMIT=30

3 Rule Run Framework Configurations

This chapter details about the configurations required in the Rule Run Framework module. It consists of the following sections:

- Performance Optimization Setting for RRF Module
- Component Registration in RRF
- Configure Forms XML to Execute Server Side Rule

3.1 Performance Optimization Setting for RRF Module

This is an enhancement introduced in 8.0.1.0.0 release.

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 MERGE 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:

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.	

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).

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 like 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.

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.

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.

3.2 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

3.2.1.1 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.

3.2.1.1.1 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.

3.2.1.1.2 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.

3.2.1.1.3 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.

3.2.1.1.4 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.

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.

3.2.1.1.5 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.

3.2.1.1.6 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 dependant 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.

3.2.1.2 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.

3.2.1.3 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.

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

Column Name	Type	Description	Null
`V_LAST_MODIFIED_BY`	VARCHAR2(30)	Stores the modifier username.	Y
`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')

3.2.1.4 Sample Code

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

ComponentSample.txt

3.3 Configure Forms XML to Execute Server Side Rule

You can execute database stored procedure and RRF Run using the Forms Framework server side rule configuration.

In order to execute RRF Run using Forms xml, the Form where server side rule is being executed with Type as "**REVELEUS_RULE**" you need to manually update the Type as "**FIRERUN**".

For example, the `RiskRecalculate.xml` having server side rule is used to re-calculate the risk. Here the Type needs to be changed as suggested below.

Replace the following attribute **Type** value:

```
<RULESET ID="110" TYPE="REVELEUS_RULE">
```

With

```
<RULESET ID="110" TYPE="FIRERUN">
```

4 Operations

This section is applicable only from OFS AAAI 8.0.5.0.0 version.

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.

4.1 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 the 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.

4.1.1 Setting Up of Secondary AM Server

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,PMEMORY,
CACHE,NOOFTHREADS,IOTRANSFER,MAXTRANSPERSEC,DISKSDBSTRIPING,DISKSFILESTRIPI
NG,MAXFILESIZE,MAXFTPFILESIZE,MAXFILENAMELEN,OSDATABLOCKSIZE,DATASETTYPE,ST
AGEPATH,DBFTPSHARE,DBFTPUSERID,DBFTPPASSWD,DBFTPPORT,DBFTPDRIVE,APPFTPSHARE
,APPFTPPORT,APPFTPDRIVE,APPFTPUSERID,APPFTPPASSWD,WEBFTPSHARE,WEBFTPPORT,WE
BFTPUSERID,WEBFTPDRIVE,WEBFTPPASSWD,OSTYPE,SOCKETSERVERPORT,SEC_SHARE_NAME,
SEC_USERID,SEC_PASSWD,F_ISPRIMARY,N_PRECEDENCE)
```

```
SELECT
WEBIPADDRESS,APPIPADDRESS,'<NEWAMIPADDRESS>',ETLAPPHOME,NOOFCPUS,VMEMORY,PM
EMORY,CACHE,NOOFTHREADS,IOTRANSFER,MAXTRANSPERSEC,DISKSDBSTRIPING,DISKSFILE
STRIPING,MAXFILESIZE,MAXFTPFILESIZE,MAXFILENAMELEN,OSDATABLOCKSIZE,DATASETT
YPE,STAGEPATH,DBFTPSHARE,DBFTPUSERID,DBFTPPASSWD,DBFTPPORT,DBFTPDRIVE,APPFT
PSHARE,APPFTPPORT,APPFTPDRIVE,APPFTPUSERID,APPFTPPASSWD,WEBFTPSHARE,WEBFTPP
ORT,WEBFTPUSERID,WEBFTPDRIVE,WEBFTPPASSWD,OSTYPE,SOCKETSERVERPORT,SEC_SHARE
_NAME,SEC_USERID,SEC_PASSWD,F_ISPRIMARY,N_PRECEDENCE 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>'
```

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:

   h) Modify the following variables in the `.profile` file:

   i) 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.

   ii) 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
```

iii) 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
```

iv) Set `JARPATH` variable to `$FIC_DB_HOME/lib`.

v) 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.

i) 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.

3. 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.

4.1.2 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.

4.1.3 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 8.0.5.0.0

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 8.0.5.0.0.

5 Unified Analytical Metadata Configurations

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

- Hierarchy Node Internationalization
- Data Element Filters Classification

5.1 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.

5.1.1 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, Forms Framework, and Hierarchy Maintenance.

5.1.2 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.

5.1.3 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.

5.1.3.1 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.

5.1.3.2 MLS Table Configuration

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

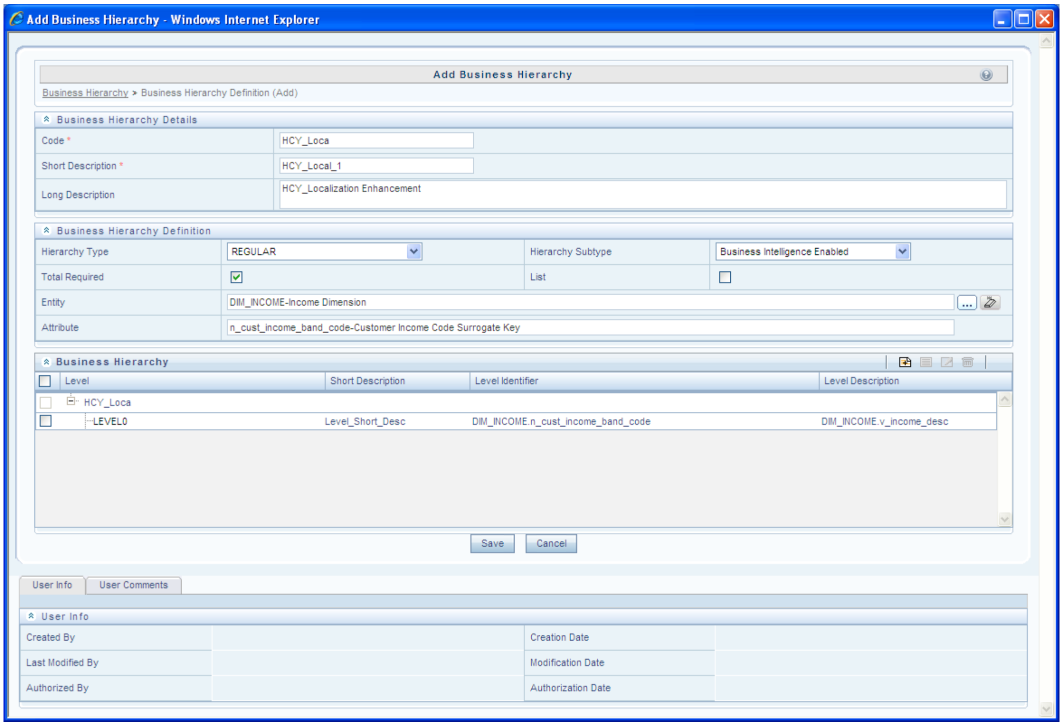
Column Name	Primary Key	Datatype
N_CUST_INCOME_BAND_CODE	PK	Number(5,0)
FIC_MIS_DATE		Date
V_CUST_INCOME_SHORT_DESC		Varchar2(80)
V_INCOME_DESC		Varchar2(80)
N_D_INCOME_UPPER_VALUE		Number(22,3)
N_D_INCOME_LOWER_VALUE		Number(22,3)

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:

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 following figure represents the **Income** Hierarchy definition:



Add Business Hierarchy

Business Hierarchy > Business Hierarchy Definition (Add)

Business Hierarchy Details

Code *	HCY_Loca
Short Description *	HCY_Local_1
Long Description	HCY_Localization Enhancement

Business Hierarchy Definition

Hierarchy Type	REGULAR	Hierarchy Subtype	Business Intelligence Enabled
Total Required	☑	List	□
Entity	DIM_INCOME-Income Dimension		
Attribute	n_cust_income_band_code-Customer Income Code Surrogate Key		

Business Hierarchy

□	Level	Short Description	Level Identifier	Level Description
□	HCY_Loca			
□	LEVEL0	Level_Short_Desc	DIM_INCOME.n_cust_income_band_code	DIM_INCOME.v_income_desc

User Info

Created By		Creation Date	
Last Modified By		Modification Date	
Authorized By		Authorization Date	

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).

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.

5.1.4 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

5.1.4.1 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.

5.1.4.2 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.

5.1.5 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.

5.1.6 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.

5.1.7 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.

5.2 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* screen 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* screen 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.

5.2.1 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 in to 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 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:

- Configuration of Oracle R distribution and Oracle R enterprise (ORE)
- Configurations for OFSAAI Remote Invocation of Scripted Models Using Standard R Distributions
- Configurations for Open-R with HDFS
- Support for Scripts which work on HDFS Files Directly
- User Configurable Execution Implementation
- Configuration for Parallel Execution of Models
- Configurations for ORE Execution
- Configuring the 8.0.6.0.0 Variable Migration Utility

6.1 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.

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

This is applicable from OFSAAI version 8.0.1.0.0.

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.

6.2.1 Prerequisite

1. Following packages should be installed 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. If you want 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.

6.2.2 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 on the R directories.

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 `ojdbc6.jar` file to the lib directory in the remote file path configured.
- 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.

6.2.3 Framework Specific Configurations

Following tags should be updated with appropriate values in **`ModelingFramework.xml`** located at `/webroot/conf` (WEB layer) and `/ficdb/conf`(in DB layer). By default, the XML configuration comes with pre-configured for R scripts for data frame and HDFS based executions.

```
<Target id = "$HOST$" PRIMARY_NODE = "$TRUE/FALSE$" LANGUAGE = "R"
EXE_ENV = "Standard R Engine" INPUT_DATA_TYPE = "DF / HDFS" NAME =
"$Logical Name for the target$" >
```

- `Target id =` Replace `$HOST$` with IP address / host name of remote machine where Rserve is running.
- `PRIMARY_NODE` = set as `TRUE` to indicate this is the primary node where execution will happen if host is not passed as a runtime execution parameter.
- `LANGUAGE =` Enter the language in which the script is written. The supported languages are Standard R and ORE.
- `EXE_ENV` = Enter the execution engine in which the script should be executed. The supported execution engines are Standard R and ORE.
- `INPUT_DATA_TYPE` = Enter the data type format as `DF or HDFS`. In case the type is 'HDFS' user has to configure the `<HDFS_LOCATION>` tag.
- `NAME` = a unique name for the combination of language, execution engine and input data type.

```
<REMOTE_FILE_PATH>$FILE_PATH$</REMOTE_FILE_PATH>
```

- Replace `$FILE_PATH$` with the path in Remote Machine/Server which has got complete access rights to all users.

  (Output of the executions will be created under this configured directory)

  In this case, Remote Machine/server refers to the execution engine like Rserve.

  Configured path should end with a directory separator at the end.

  Format : `<REMOTE_FILE_PATH>/user1/OFSAA/R/</REMOTE_FILE_PATH>`

```
<IS_OUTPUT_REQ_IN_OFSAA>N</IS_OUTPUT_REQ_IN_OFSAA>
```

The flag value indicates whether the outputs have to be written back to framework tables.

```
<IS_DETAILED_OUTPUT_REQUIRED>Y</IS_DETAILED_OUTPUT_REQUIRED>
```

The flag value indicates whether the outputs has to be written in the .csv format in the machine in which the model is executed.

```
<DELETE_OUTPUTFILES>N</DELETE_OUTPUTFILES>
```

The flag value indicates whether to delete the output files (only the files will be deleted not the folders) from the machine in which the model is executed.

NOTE: Once the configurations are done in `FIC_DB_LAYER`, copy the same to the deployed path `webroot/conf` folder or copy the file to `$FIC_WEB_HOME/webroot/conf` folder and re-deploy.

6.2.4 Configurations for R Script

```
<PRE_SCRIPT_FILE>REXECUTION_PREFIX</PRE_SCRIPT_FILE>
```

By default, OFSAA pre-script will be considered. If you want your own pre- script, it needs to be configured with this tag.

```
<POST_SCRIPT_FILE>REXECUTION_SUFFIX</POST_SCRIPT_FILE>
```

By default, OFSAA post script will be considered. If you want your own post- script, it needs to be configured with this tag.

```
<REMOTESERVICE_PORT>$PORT$</REMOTESERVICE_PORT>
```

Replace `$PORT$` with the port configured for Rserve. (The default Rserve port is 6311.)

```
<USER>

<NAME>$USERNAME$</NAME>

<PASSWORD>$PASSWORD$</PASSWORD>

</USER>
```

Replace `$USERNAME$` and `$PASSWORD$` with the credentials of the user who can connect to Rserve. It should be same as the entry made in the `Rserveusers` file.

The password should be in encrypted format. To encrypt the password, do the following steps:

1. Go to `$FIC_DB_HOME/bin` and execute the command:

   ```
   .\hostconfig.sh
   ```

2. Provide the unique name given in the **`ModelingFramework.xml`** in the 'NAME' attribute of 'TARGET' tag and password. Once these values are provided the password will be stored in the encrypted format in **`ModelingFramework.xml`**.

6.2.5 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;

};
```

- If the cloudera jdbc connector version is 2.5.x:

```
Client {
   com.sun.security.auth.module.Krb5LoginModule required
   useKeyTab=true
   useTicketCache=false
   doNotPrompt=true
   keyTab=""
   debug=true;
};
```

6.3 Configurations for Open-R with HDFS

This is applicable from OFSAAI version 8.0.3.0.0.

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

6.3.1 Prerequisites

Following are the installation requirements for external dependencies:

- CDH (Version: OFSAA qualified CDH version)
- 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.
  Note: ORAAH 2.7.0 is compatible only with OFSAAI 8.0.5.0.0 and later versions.
- 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
  ```

6.3.2 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. Log in 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
   ```

6.3.3 Framework Specific Configurations

Following are the additional tags in ModelingFramework.xml applicable for ORAAH:

```
<HIVE_HOST>$HIVE_HOST$</HIVE_HOST>
```

Replace `$HIVE_HOST$` with Hive server Host Name or IP Address.

```
<HIVE_PORT>$HIVE_PORT$</HIVE_PORT>
```

Replace `$HIVE_PORT$` with Hive server running port.

```
HIVE_PRINCIPAL>$HIVE_PRINCIPAL$</HIVE_PRINCIPAL>
```

Replace `$HIVE_PRINCIPAL$` with the Kerberos server principal for the host where the HiveServer2 is running.

```
<DFS_NAME_NODE>$DFS_NAME_NODE$</DFS_NAME_NODE>
```

Replace `$DFS_NAME_NODE$` with default HDFS Name-node to use when converting HDFS object into RDD object.

```
<SPRK_MEMORY_PER_PROCESS>2G</SPRK_MEMORY_PER_PROCESS>
```

Amount of memory to use per executor process, in the same format as JVM memory strings (for example 512m, 2g). Or in byte if specified as integer. Default is 2 G.

Pre/Post Script Tags

```
<PRE_SCRIPT_FILE>REXEC_PREFIX_HDFS,REXECUTION_PREFIX_2</PRE_SCRIPT_FILE
>
```

By default, OFSAA pre-script will be considered. If you want your own pre- script, it needs to be configured with this tag.

```
<POST_SCRIPT_FILE>REXECUTION_SUFFIX_0,REXECUTION_SUFFIX</POST_SCRIPT_FI
LE>
```

By default, OFSAA post script will be considered. If you want your own post- script, it needs to be configured with this tag.

6.3.4 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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. Log in 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 Process Modeling Framework Configurations

This is applicable from OFSAAI version 8.0.2.0.0. In 8.0.2.0.0, it was called Workflow and Process Orchestration.

This chapter details about the configurations required for Process Modeling Framework module. It includes the following sections:

- SMTP Server Configurations
- Work Manager Configurations

7.1 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. For example, task, bulk task, and single.
   - 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.

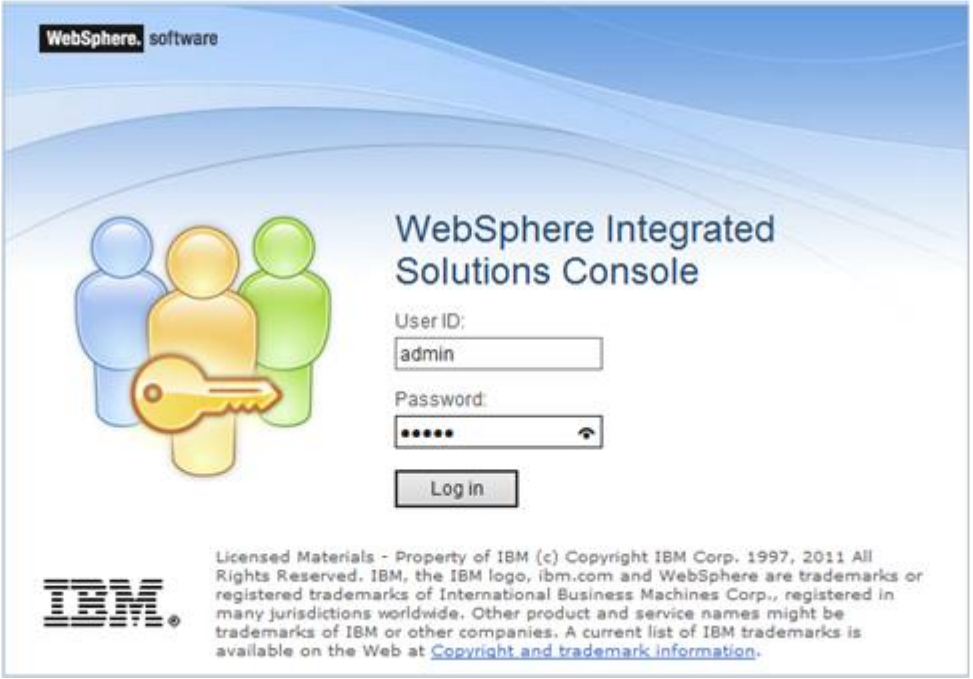
7.2 Work Manager Configurations

This is applicable from OFSAAI version 8.0.3.0.0.

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.

7.2.1 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.

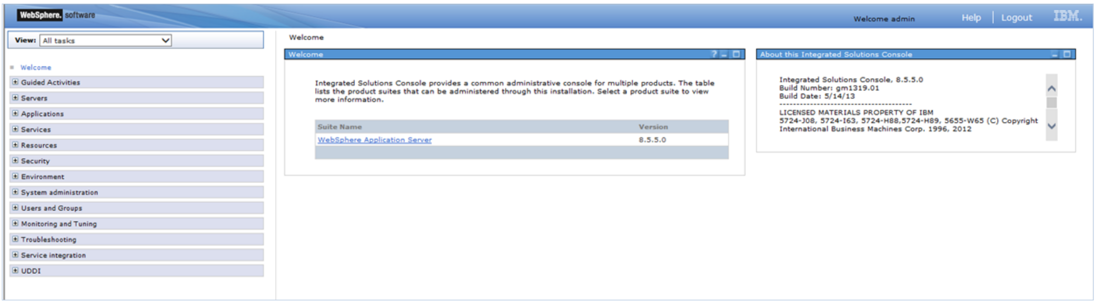


User ID: admin

Password: •••••

Licensed Materials - Property of IBM (c) Copyright IBM Corp. 1997, 2011 All Rights Reserved. IBM, the IBM logo, ibm.com and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information.

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



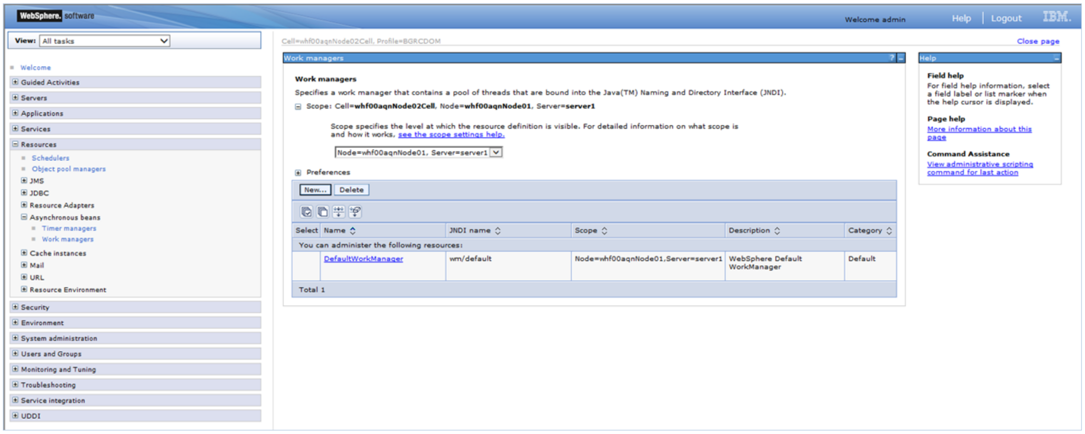
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.0

Integrated Solutions Console, 8.5.5.0
Build Number: gm1319.01
Build Date: 5/14/13

LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88,5724-H89, 5655-W65 (C) Copyright International Business Machines Corp. 1996, 2012

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



Cell=whf00aqnNode02Cell, Profile=BGRCDOM

Work managers

Work managers

Specifies a work manager that contains a pool of threads that are bound into the Java(TM) Naming and Directory Interface (JNDI).

Scope: Cell=**whf00aqnNode02Cell**, Node=**whf00aqnNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=whf00aqnNode01, Server=server1

Preferences

Select	Name	JNDI name	Scope	Description	Category
You can administer the following resources:					
	DefaultWorkManager	wm/default	Node=whf00aqnNode01,Server=server1	WebSphere Default WorkManager	Default
Total 1					

Help

Field help
For field help information, select a field label or list marker when the help cursor is displayed.

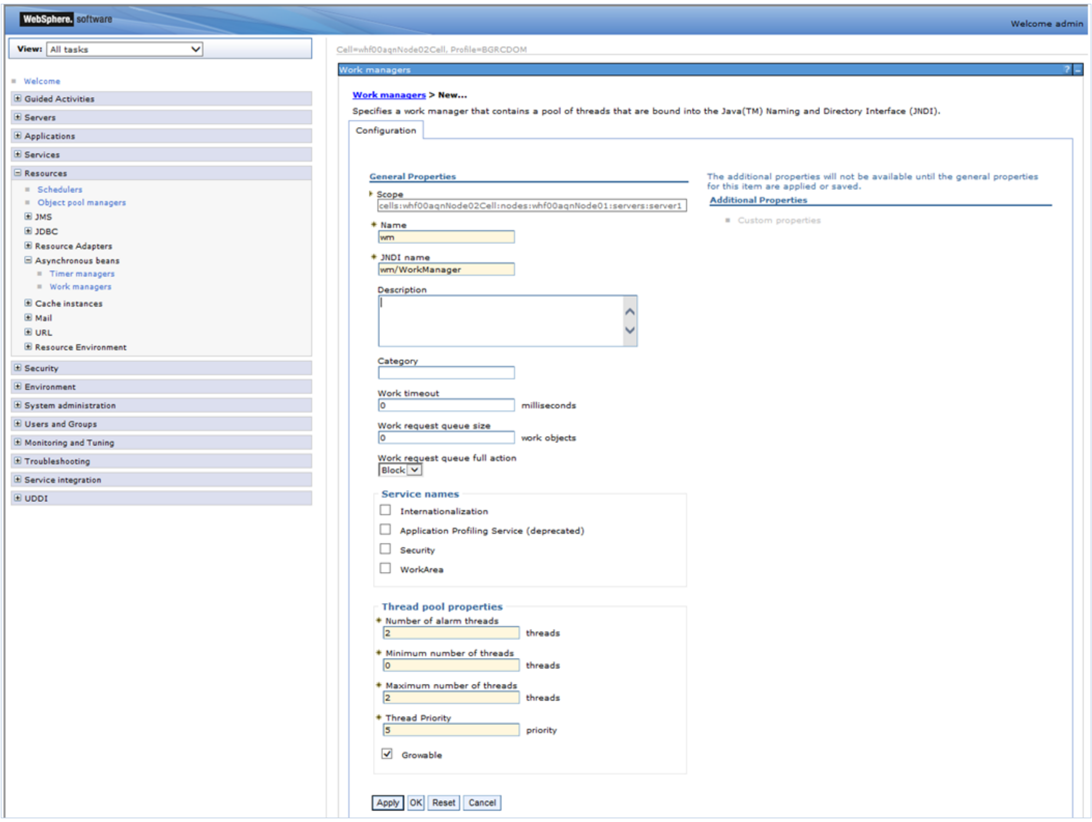
Page help
More information about this page

Command Assistance
View administrative scripting command for last action

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

   For example, Node=whf00aqnNode01, Server=server1.

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



Cell=whf00aqnNode02Cell, Profile=BGRCDOM

Work managers

Work managers > **New...**

Specifies a work manager that contains a pool of threads that are bound into the Java(TM) Naming and Directory Interface (JNDI).

General Properties

Scope
cells:whf00aqnNode02Cell:nodes:whf00aqnNode01:servers:server1

* Name
wm

* JNDI name
wm/WorkManager

Description

Category

Work timeout
0 milliseconds

Work request queue size
0 work objects

Work request queue full action
Block

The additional properties will not be available until the general properties for this item are applied or saved.

Additional Properties

Service names

□ Internationalization
□ Application Profiling Service (deprecated)
□ Security
□ WorkArea

Thread pool properties

* Number of alarm threads
2 threads

* Minimum number of threads
0 threads

* Maximum number of threads
2 threads

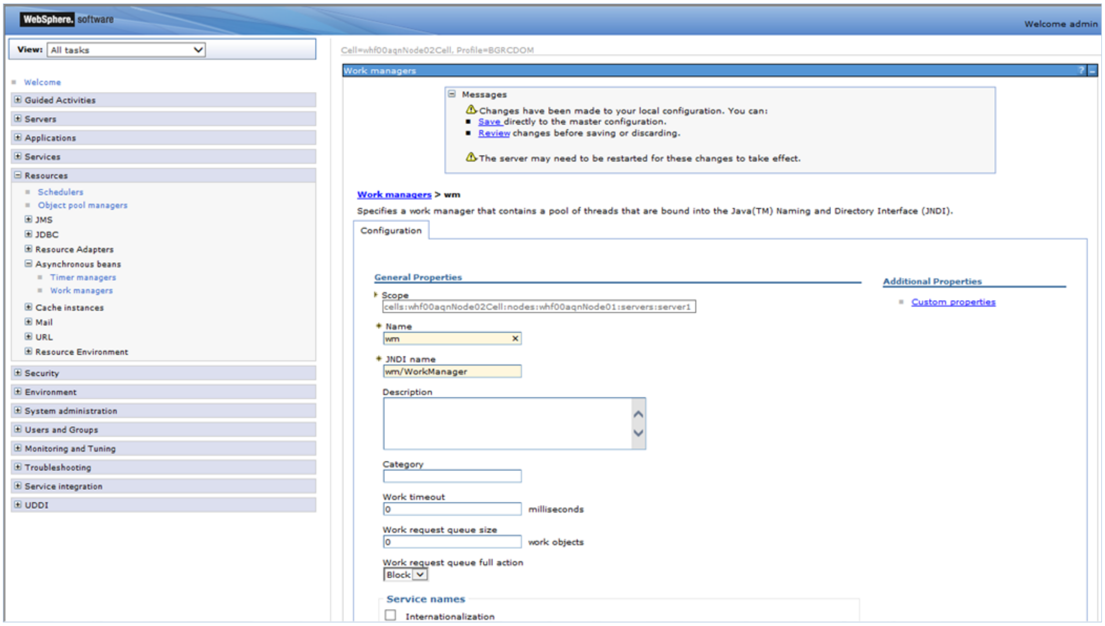
* Thread Priority
5 priority

☑ Growable

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**.



Cell=whf00aqnNode02Cell, Profile=BGRCDOM

Work managers

Messages

⚠Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠The server may need to be restarted for these changes to take effect.

Work managers > wm

Specifies a work manager that contains a pool of threads that are bound into the Java(TM) Naming and Directory Interface (JNDI).

Configuration

General Properties

Scope: cells:whf00aqnNode02Cell:nodes:whf00aqnNode01:servers:server1

* Name: wm

* JNDI name: wm/WorkManager

Description:

Category:

Work timeout: 0 milliseconds

Work request queue size: 0 work objects

Work request queue full action: Block

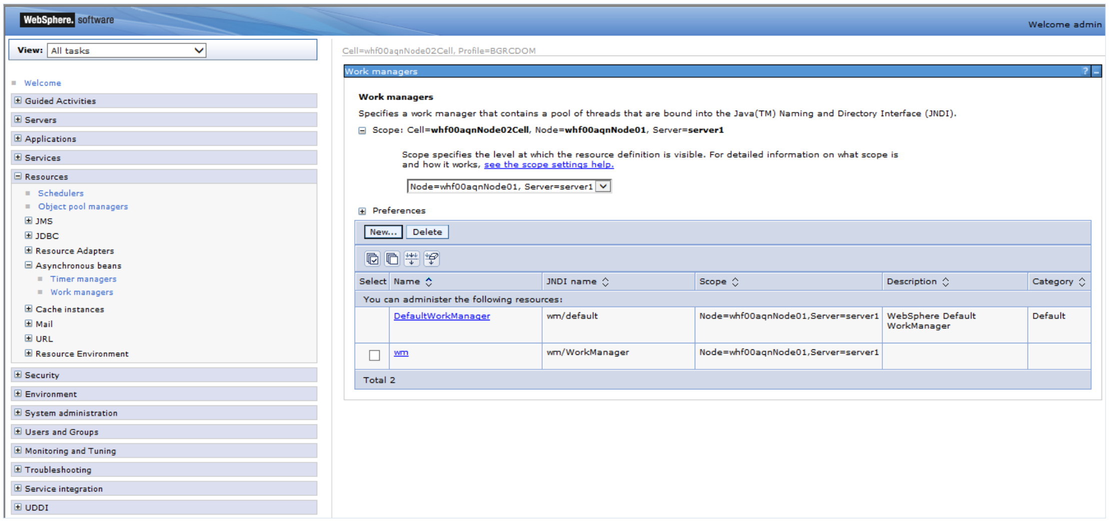
Service names

□ Internationalization

Additional Properties

- Custom properties

9. Click **Save**.



Cell=whf00aqnNode02Cell, Profile=BGRCDOM

Work managers

Work managers

Specifies a work manager that contains a pool of threads that are bound into the Java(TM) Naming and Directory Interface (JNDI).

Scope: Cell=**whf00aqnNode02Cell**, Node=**whf00aqnNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=whf00aqnNode01, Server=server1

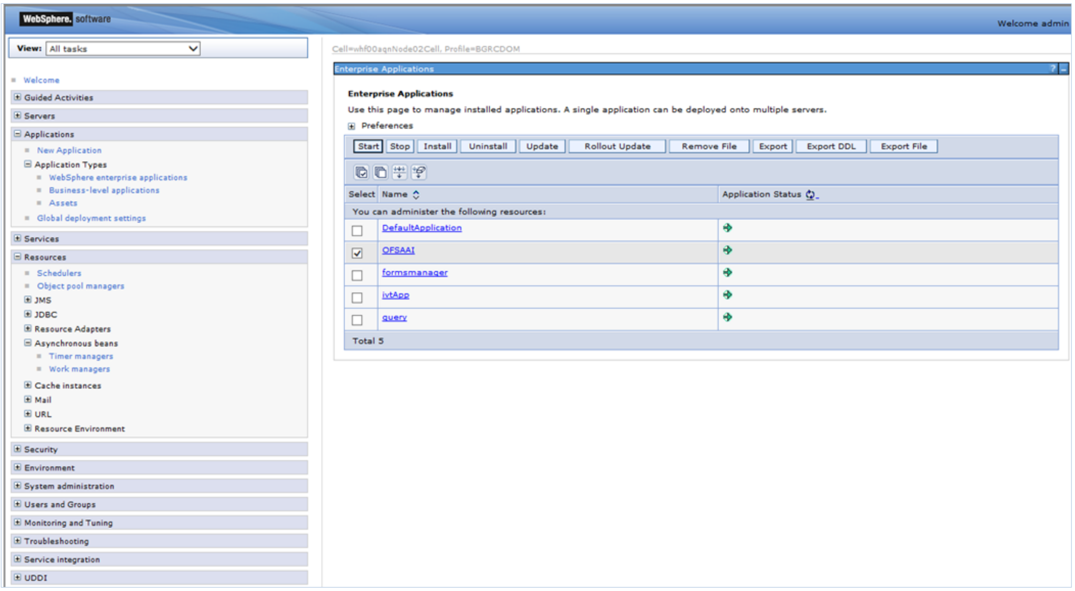
Preferences

Select	Name	JNDI name	Scope	Description	Category
You can administer the following resources:					
	DefaultWorkManager	wm/default	Node=whf00aqnNode01,Server=server1	WebSphere Default WorkManager	Default
□	wm	wm/WorkManager	Node=whf00aqnNode01,Server=server1		
Total 2					

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

7.2.2 Mapping Work Manager to OFSAA WebSphere Instance

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

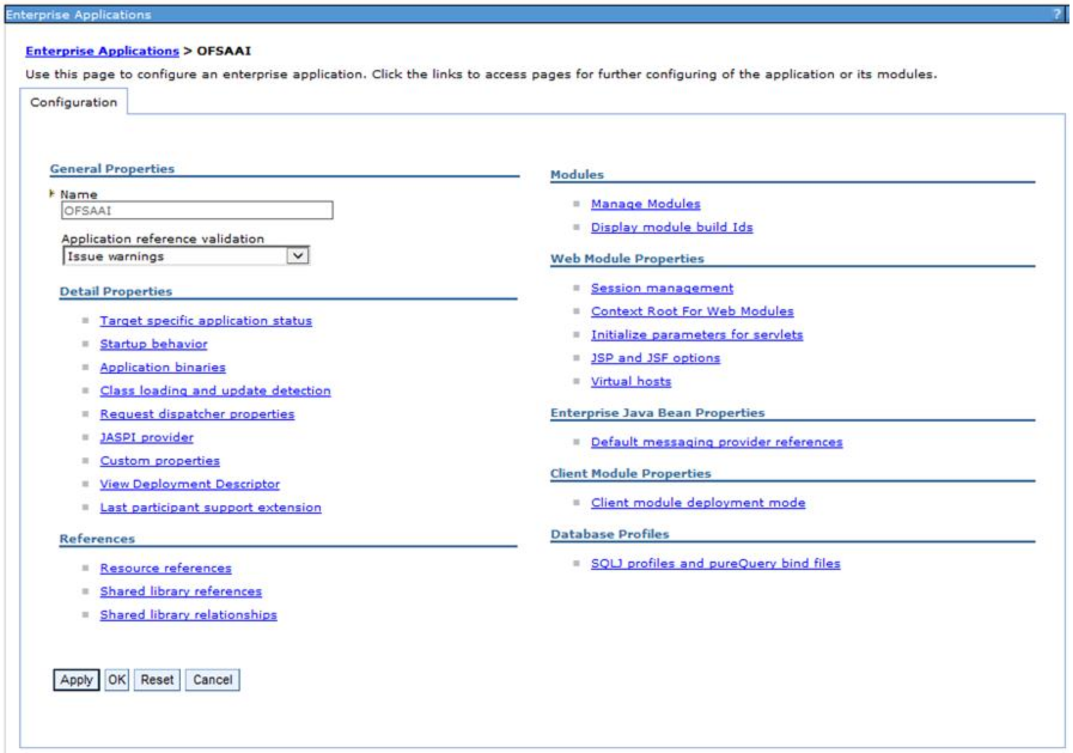


Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Select	Name	Application Status
You can administer the following resources:		
□	DefaultApplication	➔
☑	OFSAAI	➔
□	formsmanager	➔
□	ivtApp	➔
□	query	➔
Total 5		

2. Click OFSAAI instance hyperlink.


Enterprise Applications
Configuration
General Properties
Detail Properties
Target specific application status
Startup behavior
Application binaries
Class loading and update detection
Request dispatcher properties
JASPI provider
Custom properties
View Deployment Descriptor
Last participant support extension
References
Resource references
Shared library references
Shared library relationships
Modules
Manage Modules
Display module build Ids
Web Module Properties
Session management
Context Root For Web Modules
Initialize parameters for servlets
JSP and JSF options
Virtual hosts
Enterprise Java Bean Properties
Default messaging provider references
Client Module Properties
Client module deployment mode
Database Profiles
SQLJ profiles and pureQuery bind files
Apply
OK
Reset
Cancel

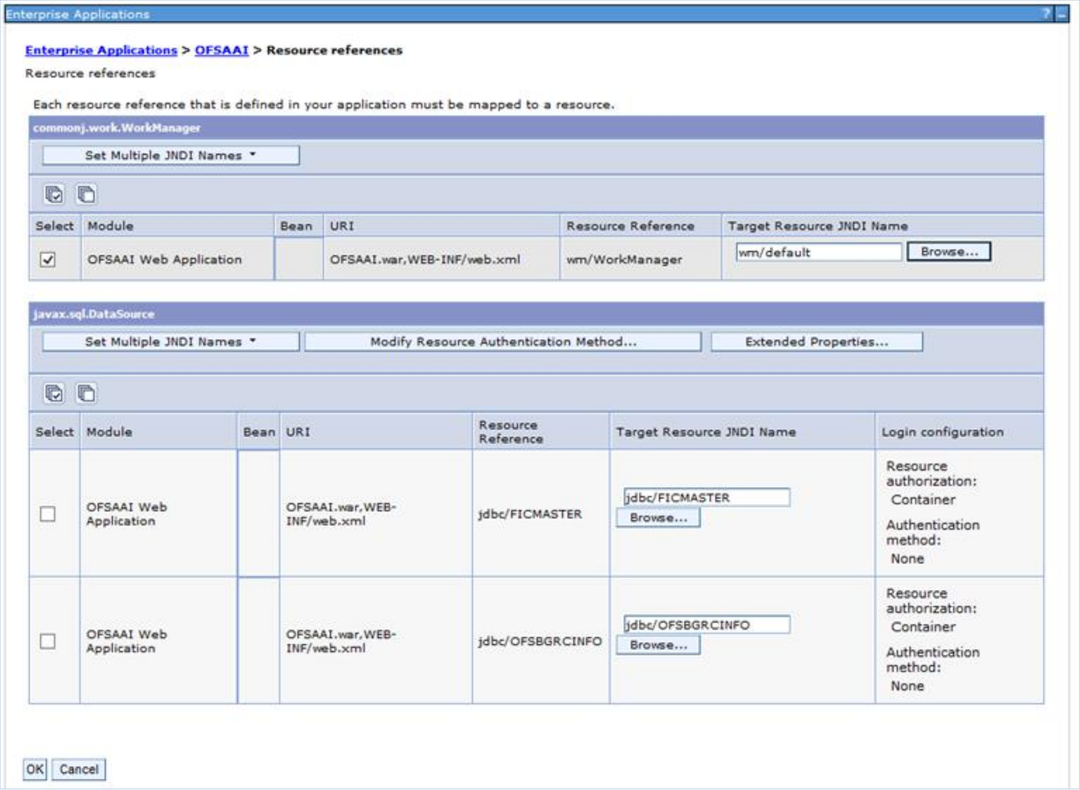
Enterprise Applications > OFSAAI

Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.

Name: OFSAAI

Application reference validation: Issue warnings

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



Enterprise Applications

Enterprise Applications > OFSAAI > Resource references

Resource references

Each resource reference that is defined in your application must be mapped to a resource.

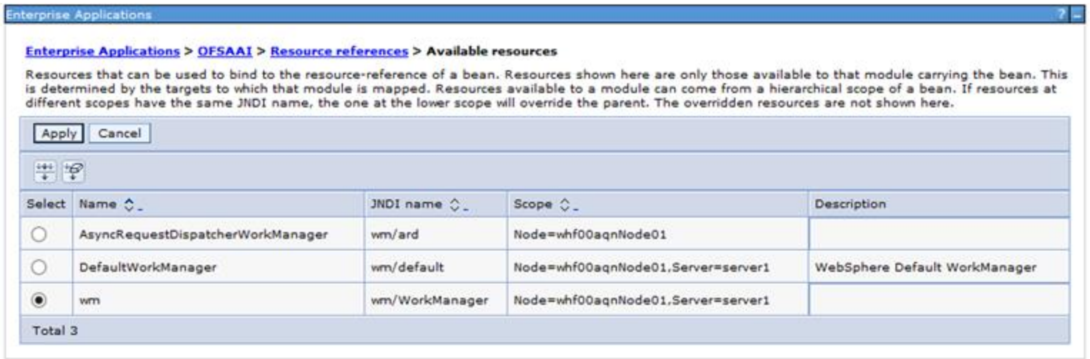
commonj.work.WorkManager

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name
☑	OFSAAI Web Application		OFSAAI.war,WEB-INF/web.xml	wm/WorkManager	wm/default Browse...

javax.sql.DataSource

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name	Login configuration
☐	OFSAAI Web Application		OFSAAI.war,WEB-INF/web.xml	jdbc/FICMASTER	jdbc/FICMASTER Browse...	Resource authorization: Container Authentication method: None
☐	OFSAAI Web Application		OFSAAI.war,WEB-INF/web.xml	jdbc/OFSBGRCINFO	jdbc/OFSBGRCINFO Browse...	Resource authorization: Container Authentication method: None

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



Enterprise Applications

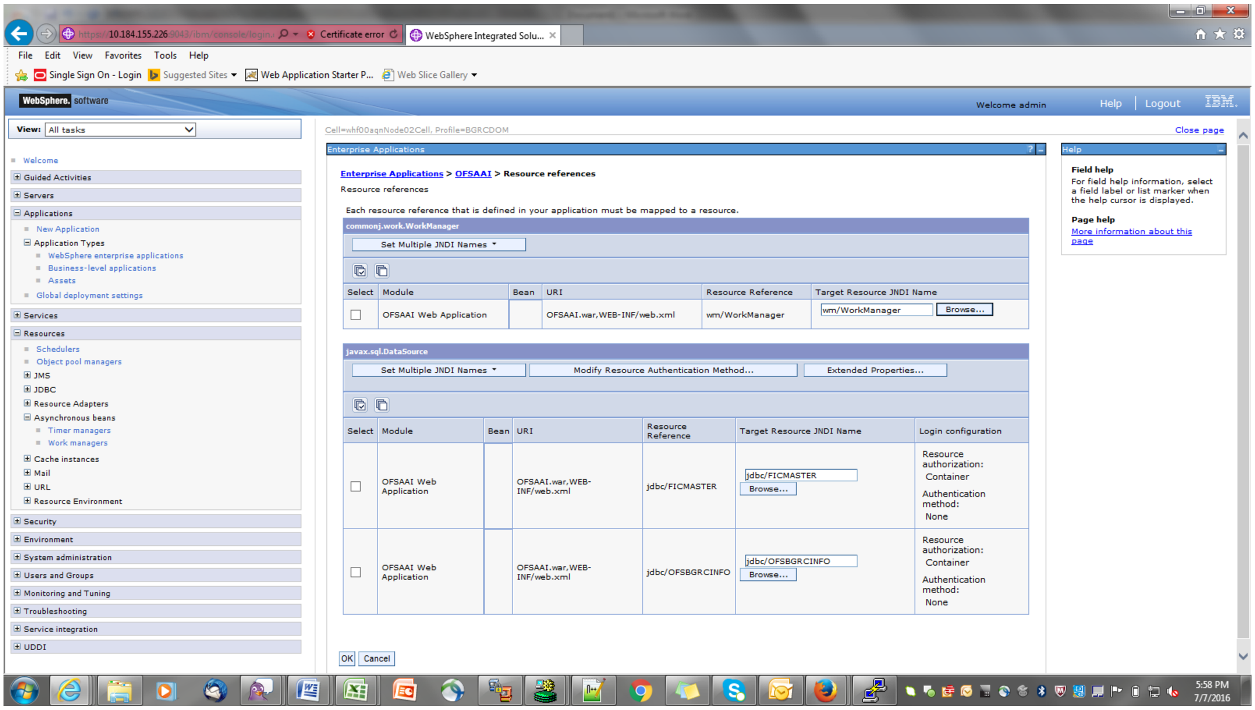
Enterprise Applications > OFSAAI > Resource references > Available resources

Resources that can be used to bind to the resource-reference of a bean. Resources shown here are only those available to that module carrying the bean. This is determined by the targets to which that module is mapped. Resources available to a module can come from a hierarchical scope of a bean. If resources at different scopes have the same JNDI name, the one at the lower scope will override the parent. The overridden resources are not shown here.

Select	Name	JNDI name	Scope	Description
○	AsyncRequestDispatcherWorkManager	wm/ard	Node=whf00aqnNode01	
○	DefaultWorkManager	wm/default	Node=whf00aqnNode01,Server=server1	WebSphere Default WorkManager
●	wm	wm/WorkManager	Node=whf00aqnNode01,Server=server1	

Total 3

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



Cell=whf00aqnNode02Cell, Profile=BGRCDOM

Enterprise Applications

Enterprise Applications > OFSAAI > Resource references

Resource references

Each resource reference that is defined in your application must be mapped to a resource.

commonj.work.WorkManager

Set Multiple JNDI Names

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name
□	OFSAAI Web Application		OFSAAI.war,WEB-INF/web.xml	wm/WorkManager	wm/WorkManager Browse...

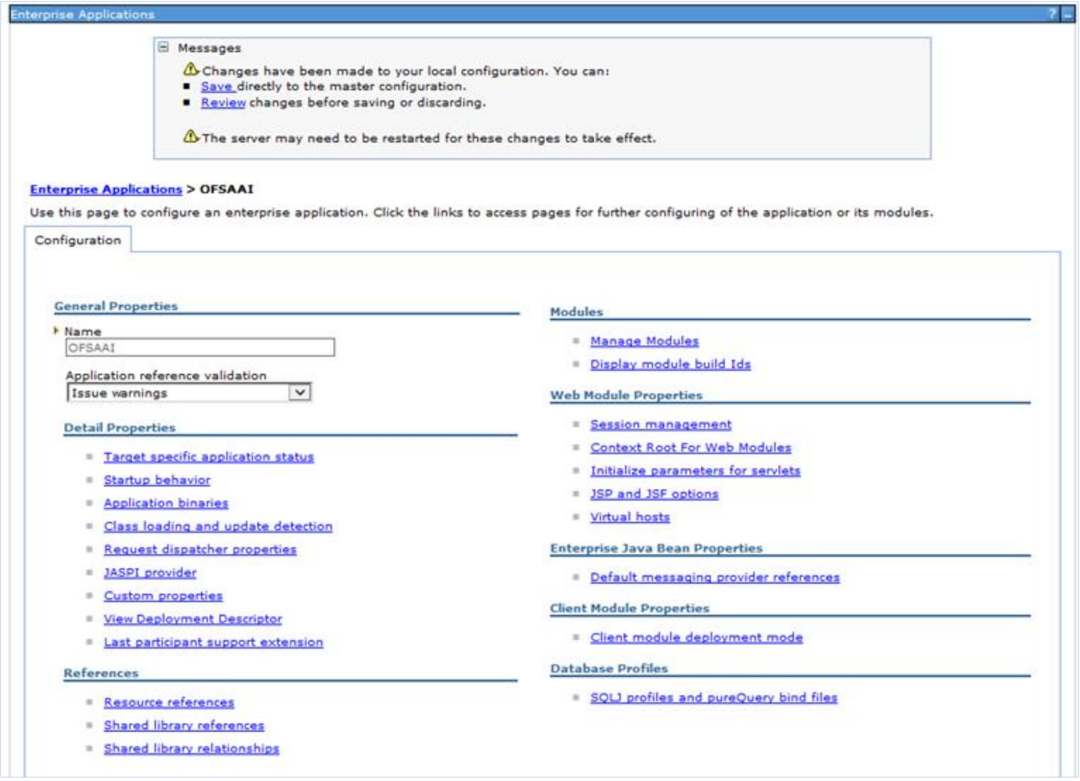
javax.sql.DataSource

Set Multiple JNDI Names | Modify Resource Authentication Method... | Extended Properties...

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name	Login configuration
□	OFSAAI Web Application		OFSAAI.war,WEB-INF/web.xml	jdbc/FICMASTER	jdbc/FICMASTER Browse...	Resource authorization: Container Authentication method: None
□	OFSAAI Web Application		OFSAAI.war,WEB-INF/web.xml	jdbc/OFSBGRCINFO	jdbc/OFSBGRCINFO Browse...	Resource authorization: Container Authentication method: None

OK Cancel

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



Enterprise Applications

Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

Enterprise Applications > OFSAAI

Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.

Configuration

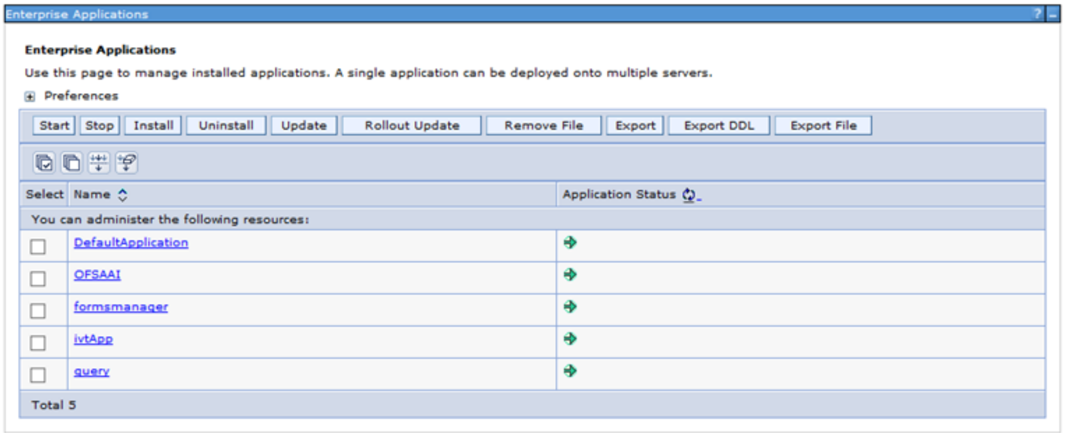
General Properties

Name: OFSAAI

Application reference validation: Issue warnings

Detail Properties
Target specific application status
Startup behavior
Application binaries
Class loading and update detection
Request dispatcher properties
JASPI provider
Custom properties
View Deployment Descriptor
Last participant support extension
References
Resource references
Shared library references
Shared library relationships
Modules
Manage Modules
Display module build Ids
Web Module Properties
Session management
Context Root For Web Modules
Initialize parameters for servlets
JSP and JSF options
Virtual hosts
Enterprise Java Bean Properties
Default messaging provider references
Client Module Properties
Client module deployment mode
Database Profiles
SQLJ profiles and pureQuery bind files

7. Click **Save**.



Enterprise Applications

Enterprise Applications

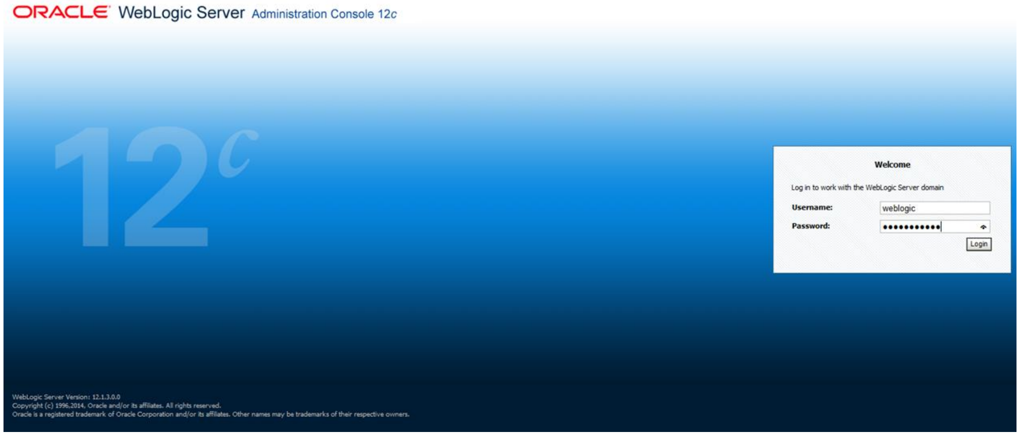
Use this page to manage installed applications. A single application can be deployed onto multiple servers.

⊞ Preferences

Select	Name	Application Status
You can administer the following resources:		
□	DefaultApplication	➜
□	OFSAAI	➜
□	formsmanager	➜
□	ivtApp	➜
□	query	➜
Total 5		

7.2.3 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.



Welcome

Log in to work with the WebLogic Server domain

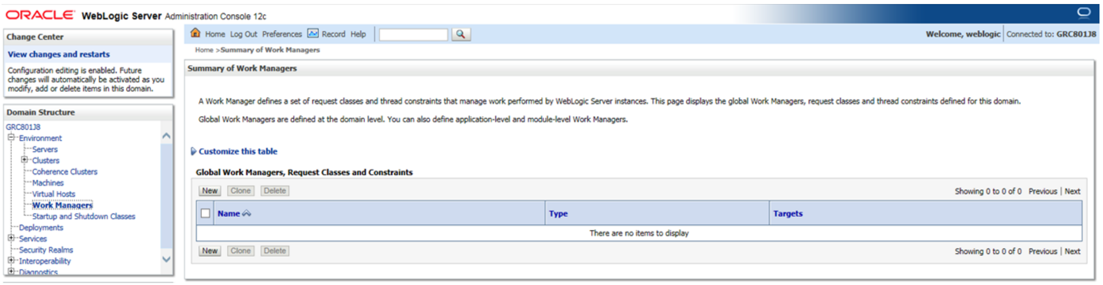
Username: weblogic

Password: ●●●●●●●●●●●●

WebLogic Server Version: 12.1.3.0.0
Copyright (c) 1996,2014, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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.



ORACLE WebLogic Server Administration Console 12c
Home
Log Out
Preferences
Record
Help
Welcome, weblogic
Connected to: GRC801J8
Home >Summary of Work Managers
Change Center
View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Summary of Work Managers

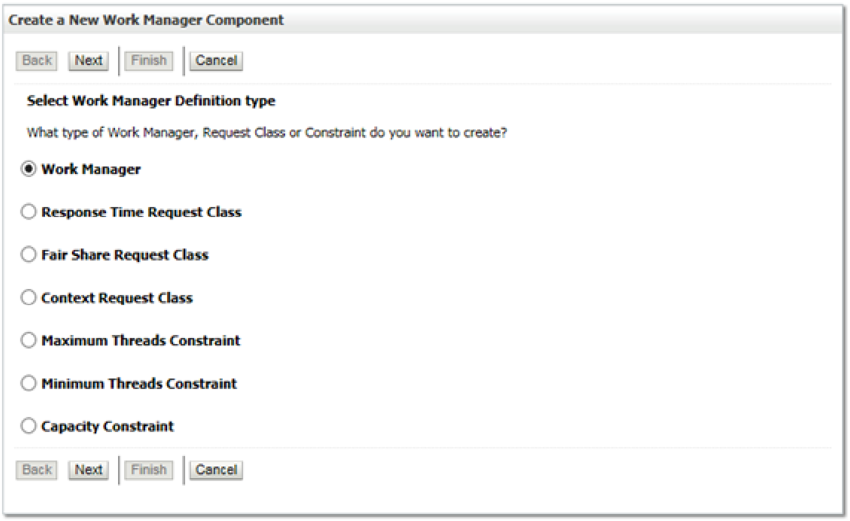
A Work Manager defines a set of request classes and thread constraints that manage work performed by WebLogic Server instances. This page displays the global Work Managers, request classes and thread constraints defined for this domain.

Global Work Managers are defined at the domain level. You can also define application-level and module-level Work Managers.

Global Work Managers, Request Classes and Constraints

□ Name	Type	Targets
There are no items to display		

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



Create a New Work Manager Component

Select Work Manager Definition type

What type of Work Manager, Request Class or Constraint do you want to create?

● Work Manager

○ Response Time Request Class

○ Fair Share Request Class

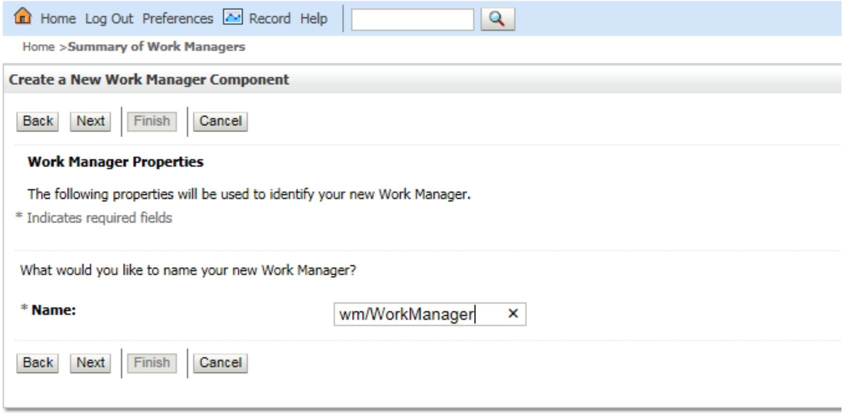
○ Context Request Class

○ Maximum Threads Constraint

○ Minimum Threads Constraint

○ Capacity Constraint

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



Create a New Work Manager Component

Work Manager Properties

The following properties will be used to identify your new Work Manager.

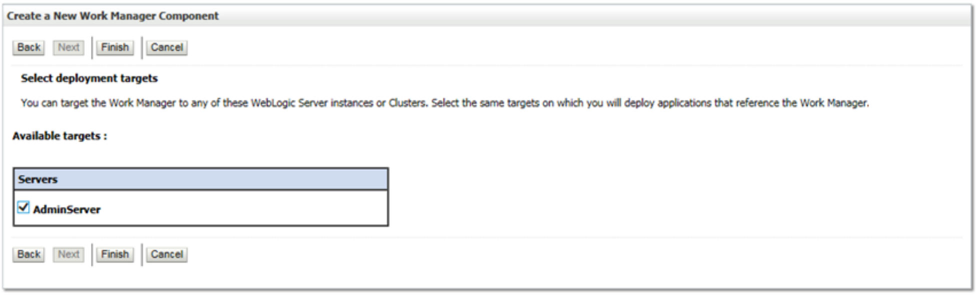
* Indicates required fields

What would you like to name your new Work Manager?

* **Name:** wm/WorkManager

6. Enter the **Name** as ‘wm/WorkManager’.

7. Click **Next**.



Create a New Work Manager Component

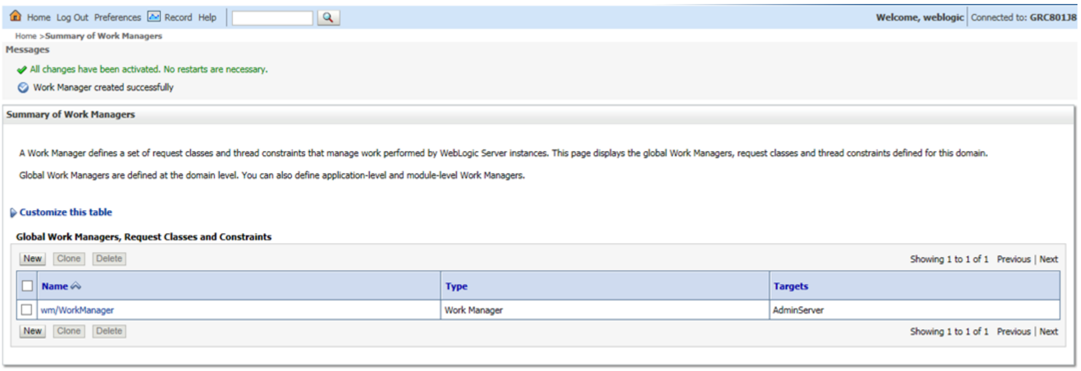
Select deployment targets

You can target the Work Manager to any of these WebLogic Server instances or Clusters. Select the same targets on which you will deploy applications that reference the Work Manager.

Available targets :

Servers
☑ AdminServer

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


Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: GRC801J8
Home >Summary of Work Managers

Messages

✓ All changes have been activated. No restarts are necessary.

Work Manager created successfully

Summary of Work Managers

A Work Manager defines a set of request classes and thread constraints that manage work performed by WebLogic Server instances. This page displays the global Work Managers, request classes and thread constraints defined for this domain.

Global Work Managers are defined at the domain level. You can also define application-level and module-level Work Managers.

Global Work Managers, Request Classes and Constraints

□	Name	Type	Targets
□	wm/WorkManager	Work Manager	AdminServer

7.3 Configuring Attributes for Attribute Expression Application Rule

This section explains how to configure attributes for creating Decision Rules on those attributes for application specific workflows. Each application and its respective components can have many attributes configured. Each attribute is identified with an ID `app_comp_attr_map_id`, based on which the values for attributes can be fetched.

Enter attribute information in the `AAI_AOM_APP_COMP_ATTR_MAPPING` table. Enter values as tabulated:

Column Name	Description
`APP_COMP_ATTR_MAP_ID`	ID of the attribute
`V_ATTR_CODE`	Name of the attribute
`N_ATTR_TYPE_ID`	ID of the attribute type. The values of the attributes are fetched based on attribute type. 1001- Static 1002- Query 1003- JavaAPI For more information, see Attribute Types.
`V_ATTRIBUTE_VALUE1` `V_ATTRIBUTE_VALUE2`	Values to be fetched for the attribute. Based on the attribute type, you need to pass the values.
`N_APP_ID`	Application code for which the current attribute is configured.
`N_COMP_ID`	Component code for which the attribute is configured.
`V_UDP_CODE`	Special property used by applications (user defined). For example, 'GET_STATUS' –to get the status for the workflow.

7.3.1 Attribute Types

The values of attributes are fetched based on the attribute types. Following are the attribute types with their IDs:

Attribute Type ID	Attribute Type Name
1001	Static
1002	Query
1003	JavaAPI

- **1001 (Static)** - Store attribute values in the `AAI_AOM_STATIC` table as `V_STATIC_ID` and `V_STATIC_VAL`.
- **1002 (Query)** - Enter the SQL query in `V_ATTRIBUTE_VALUE1` in the `AAI_AOM_APP_COMP_ATTR_MAPPING` table, which has to be fired to fetch the attribute values.
- **1003 (JavaAPI)** – Enter the method that is configured for `V_ATTRIBUTE_VALUE1` for the required attribute. The configured method in the class path is invoked to get the attribute values in this case.

7.4 Enabling Proxy for Webservices Rule

This is applicable from OFSAAI version 8.0.5.2.0 onwards.

This section explains how to configure the Proxy details if it is required for the Webservices/Rest Service Application Rule.

Add the following entries in the `AAI_WF_GLOBAL_SETTINGS` table:

V_PARAM_NAME	V_PARAM_VALUE	Description
PROXY_SERVER_IP	For example, www.proxy.myserver.com	Provide the IP address of the Proxy server.
PROXY_SERVER_PORT	For example, 80	Provide the port number of the Proxy server.

8 Inline Processing Engine Configurations

You should create an additional resource reference as `JDBC/<INFODOMNAME>` pointing to the same infodom in which IPE is installed. For information on creating resource reference, see *Appendix B* of the OFS AAI Application Pack Installation and Configuration Guide.

9 Forms Manager Configurations

9.1 Creating EAR/WAR File

To create the EAR/WAR file, follow these steps:

1. Navigate to the `$FIC_HOME/FMStandalone` directory on the OFSAA Installed server.
2. Execute. /`ant.sh` to trigger the creation of EAR/ WAR file.
3. On completion of the EAR files creation, the "BUILD SUCCESSFUL" and "Time taken" messages are displayed and you will be returned to the prompt.

   The EAR/WAR file – `formsmanager.ear/.war` - is created.

NOTE: This process overwrites any existing version of EAR file that exists in the path. If OFSAA is configured on Tomcat installation, `formsmanager.war` will be created.

9.2 Deploying Ear/WAR File

Deployment of the `formsmanager.ear/war` file is similar to the deployment of the OFSAA ear/war file. To deploy the `formsmanager.ear/war` file, follow the steps mentioned in Appendix C of OFS AAAI Installation and Configuration Guide.

NOTE: Apply the respective Application patches for Forms Manager if any other application is running in 8.0.2.0.0, before redeploying FM 2.0.

9.3 Migrating from FM 1.0 to FM 2.0

This is applicable from OFSAAI version 8.0.3.0.0.

Follow the step to migrate from FM 1.0 to FM 2.0:

Execute the following script in Configuration Schema:

```
declare
n varchar2(50);
BEGIN
pkg_createfrm_pages.createPagesInConfig('<appId>','<sourcedsnId>','<ta
rgetdsnId>',n);
dbms_output.put_line('DONE');
END;
```

where `appId` refers to Application ID, `sourcedsnId` refers to source dsnId and `targetdsnId` refers to target Id.

NOTE: Apply the respective Application patches for Forms Manager before migrating from FM 1.0 to FM 2.0.

10 Forms Framework Configurations

This is applicable from OFSAAI 8.0.5.2.0 version.

10.1 Content Management Integration

CMIS (Content Management Interoperability Services) is an OASIS standard enabling information sharing between different Content Management Systems. Forms Framework has been enhanced 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. Make sure the URL is up & 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 Oracle Financial Services Analytical Applications Infrastructure Installation & Configuration Guide 8.0.2.0.0.

4. Restart all the OFSAAI services. For more information, refer to the Start/Stop Infrastructure Services section in the Oracle Financial Services Analytical Applications Infrastructure Installation & Configuration Guide 8.0.2.0.0.

11 Flexible KBD Configurations

This is applicable from OFSAAI version 8.0.2.0.0.

Perform the following configurations required for Flexible KBD utility:

1. Add entries to the following tables to create the tree structure according to the application requirements:
   - aai_menu_b
   - aai_menu_tl
   - aai_menu_tree
   - insert_aai_obj_type_action_func_map
   - insert_aai_obj_type_b
   - insert_aai_obj_type_tl
2. Map the required User Groups to the respective User Roles to provide access to KBD Preference module. The User Roles mapped to KBD Preference module are:
   - F_KBDACC -Flex KBD Access
   - F_KBDAUTH- Flex KBD Authorize
   - F_KBDREAD- Flex KBD Read
   - F_KBDWRITE- Flex KBD Write

   If you already have User Group Role mapping, map your user group to `FlexKBD` folder. For more information, see the *Identity Management* section in OFS Analytical Applications Infrastructure User Guide. You can also populate the following tables to seed the appropriate user function mapping to FlexKBD folder:
   - insert_cssms_function_mast
   - insert_cssms_group_role_map
   - insert_cssms_role_function_map
   - insert_cssms_role_mast
   - cssms_folder_function_map

   If data is seeded into the system, then the sequences for the following tables should be reinitialized:
   - flexkbd_ctrl_loc
   - flexkbd_dim_info
   - flexkbd_pref_master

Following table describes the column name for the corresponding Table and Sequence that needs to be reinitialized:

Sequence name	**Table name**	**Column name**
FLEXKBD_CTRL_LOC_SEQ	flexkbd_ctrl_loc	CONTROL_ID
FLEXKBD_DIM_INFO_SEQ	flexkbd_dim_info	KBDID
FLEXKBD_PREF_MASTER_SEQ	flexkbd_pref_master	PREF_ID

12 Questionnaire Setup and Configuration Details

The information in this section is applicable for OFSAAI Release 8.0.4.0.0 and later.

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:

- Launching Questionnaire Menu
- Mapping Roles to Access Questionnaire
- Configuring Components, Dimensions, and Static Options

12.1 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.

12.2 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 the System Administrator & Identity Management tab and click Identity Management.
3. Click User Group Role Map from the User Administrator LHS menu. The User Group Role Map window is displayed.

4. Map users to User or Approver roles.

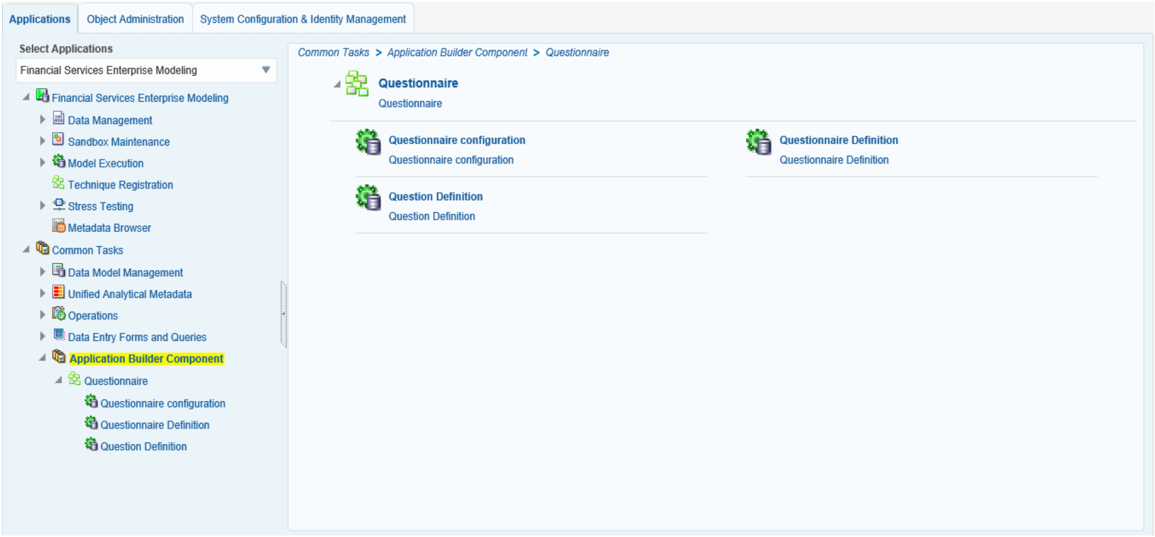
   a) Users of applications mapped to groups can access the Questionnaire menu by mapping the groups to following roles:

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.

5. 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.



Applications | Object Administration | System Configuration & Identity Management

Select Applications

Financial Services Enterprise Modeling

- Financial Services Enterprise Modeling
  - Data Management
  - Sandbox Maintenance
  - Model Execution
  - Technique Registration
  - Stress Testing
  - Metadata Browser
- Common Tasks
  - Data Model Management
  - Unified Analytical Metadata
  - Operations
  - Data Entry Forms and Queries
  - Application Builder Component
    - Questionnaire
      - Questionnaire configuration
      - Questionnaire Definition
      - Question Definition

Common Tasks > Application Builder Component > Questionnaire

Questionnaire
Questionnaire

Questionnaire configuration
Questionnaire configuration

Questionnaire Definition
Questionnaire Definition

Question Definition
Question Definition

NOTE: 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.

12.3 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.

12.3.1 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.

12.3.2 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.

12.3.3 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.

12.4 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.

13 Generic Configurations

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

- Query Performance Optimization
- Multiple Language Support (MLS) Utility
- Transferring Batch Ownership
- Database Password Reset/ Change
- Changing IP/ Hostname, Ports, Deployed paths of the OFSAA Instance
- Configure Stylesheet
- LDAP Configuration
- Using X-Frame-Options to Embed OFSAA Content on your Site
- Configuration for Tomcat
- Configuring WebLogic
- SSO Authentication (SAML) Configuration
- Public Key Authentication
- Enable and Disable Users
- Password Reset
- Configuring OFSAA OIM Connector
- Using REST APIs for user management from third-party IDMs
- Configuring the Logout URL for OBIEE in OFSAA

13.1 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.

Parameters	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
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.

13.2 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>

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 8.0.0.0.0 LP on an OFSAA setup where the OFSAA version is 8.0.1.0.0.

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 8.0.1.0.0 and have installed OFSAA 8.0.0.0.0 language packs for French and Spanish (since the latest 8.0.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 8.0.0.0.0 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 8.0.0.0.0 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 log into 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 log in with any of the above languages. For example, if you log in 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 8.0.0.0.0 (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.

13.2.1 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/`.

13.3 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;
```

13.4 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. Log in to the database and change the config schema password.
2. Log in 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. Log in to the database and change the ATOMIC schema password.
3. Log in 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. Modify the **Password** field with the new password and click **Save**. For more information, see OFSAAI User Guide.
6. Navigate to *Data Management Framework* > *Data Sources*.
7. Select the appropriate Data Source pointing to the ATOMIC Schema for which the password was reset from the *Data Sources* tree.
8. Click **Edit**.
9. Modify the **Password** field with the new password and click **Save**. For more information, see OFSAAI User Guide.

Resource Reference/ JNDI 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 Tomcat Web Server.
  - Stop the Tomcat Server.
  - Update the `Server.xml` file present in `$CATALINA_HOME/conf` with the latest config schema and atomic schema passwords.
- For WebSphere / WebLogic
  - Access the server specific “Admin” console.
  - Log in to the server with Administrative privileges.
  - Update DataSources with the latest config schema and atomic schema passwords. For more information, refer the *Configuring Resource Reference* sections in Appendix B in *OFS AAAI Application Pack Installation and Configuration Guide* available in OHC Documentation Library.

13.5 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 .

13.6 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.

Prerequisite

- You should have minimum version as OFSAAI 8.0.
- Ensure `RevLog4jConfig.xml` is configured with default log paths before executing the utility. 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.

13.6.1 Running Port Changer Utility

NOTE: The instructions in this section are not applicable to OFSAAI 8.0.2.2.0, 8.0.3.3.0, 8.0.4.2.0 and 8.0.5.1.0. For information on Running Port Changer Utility for the versions mentioned previously, see Running Port Changer Utility for 8.0.2.2.0, 8.0.3.3.0, 8.0.4.2.0, and 8.0.5.1.0.

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

   ```
   java -jar PortC.jar 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.jar** utility using the command:

   ```
   java -jar PortC.jar 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.

NOTE: The table `batch_parameter` is not updated with the new IP after you run the file `portc.jar`. The table holds the batch execution details of the batches that were executed earlier. The table `batch_parameter_master` holds the new IP after you run `portc.jar`.

Check the logs for more information, and contact My Oracle Support if you encounter any errors.

13.6.2 Running Port Changer Utility for 8.0.2.2.0, 8.0.3.3.0, 8.0.4.2.0 and 8.0.5.1.0

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.

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.

13.7 Configure Stylesheet

You will have two stylesheets theme or UI skin as mentioned below:

- Default Existing Blue theme (stylesheetAAI)
- New White & Red Theme (stylesheetAAI2) - This is configurable.

By default, the existing Blue theme is selected.

The steps to configure the new white & red theme are as follows:

1. Set the paraname key `DEFAULT_AAICSS_INFO` in the Configuration table to ‘stylesheetAAI2’. The paraname value for default theme is ‘stylesheetAAI’.

2. Restart the OFSAAI services.

13.8 LDAP Configuration

This section is not applicable for Release 8.0.4.0.0 and later. The functionality is now available from the user – interface of the OFSAAI application and you can see the LDAP Configuration section in the OFSAAI User Guide 8.0.4.0.0 for more information.

This section details about the configuration required if you want to use LDAP (Lightweight Directory Access Protocol) authentication for logging on to Infrastructure.

Before doing the following configuration, it is required to select the **Authentication Type** as **LDAP Authentication and SMS Authorization** in the Configuration window of Infrastructure. For more information, see Configuration section in the OFS Analytical Applications Infrastructure User Guide.

13.8.1 Prerequisites

- LDAP system should be installed successfully.
- One set of LDAP User credentials which can perform search on complete LDAP system and retrieve user details.

NOTE: Password for this user should never expire.

- Ensure the following entries are present in the Configuration Schema:

PARAMNAME	Description	PARAM Value Example
AUTHENTICATIONTYPE	Authentication type	3 - AUTHENTICATIONTYPE value must be 3 for LDAP. This is populated from the value entered in the Authentication Type drop-down list in the Configuration window.
ROOTCONTEXT	The Root Context for the LDAP Directory.	`dc=<OFSAA>, dc=<com>`
ROOTDN	The Root dn for LDAP directory	`cn=<Manager>, dc=<Reveleus>, dc=<com>`
ROOTPASS	Password for the Root	<secret> This is populated from the value entered in the **LDAP Password** field in the *Configuration* window.
LDAPURL	LDAP URL	`<ldap://192.0.2.1:1234/>`
LDAPSERVERURL	LDAP Server URL	`<ldap://192.0.2.2:1234/>`

PARAMNAME	Description	PARAM Value Example
LDAP_SSL_MODE	LDAP in SSL Mode	**N** for non - SSL and **Y** for SSL This is populated from the value selected for the **LDAP SSL Mode** checkbox in the *Configuration* window. **Note**: If LDAP_SSL_Mode is Y, SSL certificate needs to be imported to the JVM used by OFSAA Server.
HASHPASS	Should the user password be Hashed	FALSE or TRUE. When HASSPASS is set as FALSE, we need to have the ROOTDN value as "uid=ORCLADMIN, ou =Users, dc=OFSAAI, dc=com". ORCLADMIN is a dummy user, it will be replaced dynamically with the logged in user. When HASSPASS is set as TRUE, we need to have the ROOTDN value as "cn=orcladmin, cn=Users, dc=i-flex,dc=com" and proper ORCLADMIN LDAP password as ROOTPASS. First OFSAAI connects to LDAP directory using orcladmin user and fetches the login user details and verifies the entered password.
RETRIEVE_DN	To retrieve Distinguished Name	TRUE RETRIEVE_DN value can be FALSE if both login user id and CN value in LDAP system are the same, and all LDAP users are present under same directory structure.

NOTE: ROOTCONTEXT, ROOTDN, and ROOTPASS entries should be same as in the slapd.conf file.

13.8.2 Configure LDAP Properties File

The LDAPProperties.properties file is present in the $FIC_HOME/ficapp/common/FICServer/conf folder. Modify the following parameters in the Properties file:

- GROUPDN_USER – Should be ROOTCONTEXT value.

- USER - Should be User/Person (LDAP User Object Class).
- USER_ID – Should be `uid/cn/sAMAccountName` (which LDAP user attribute is equivalent of OFSAAI login user id).
- USER_NAME - Should be name/givenName/displayName (Which LDAP user attribute is equivalent of OFSAAI login user name).
- DISTINGUISHED_NAME - Should be dn/distinguishedName. (Which LDAP user attribute represents distinguished name).

13.8.3 Configure OpenLDAP Files

1. Copy the `reveleusSchema.schema` from <`Infrastructure Installation Directory> /ficapp/common/FICServer/conf/LDAP_LDIF` folder to `LDAPServer Schema` folder.
2. Copy the `Domains.ldif` and `Reveleus.ldif` files from `<Infrastructure Installation Directory>/ficapp/common/FICServer/conf/LDAP_LDIF` folder to `OpenLDAPServer` folder.

NOTE: Make sure that the `ROOTCONTEXT` in the `Domains.ldif` and `Reveleus.ldif` files are the same as `slapd.conf` file.

3. Provide the appropriate entries for `ROOTDN`, `ROOTPASS`, and `ROOTCONTEXT` in `slapd.conf` file in the `OpenLDAPServer` folder.
4. Add the text "include schema/reveleusSchema.schema" as the first line of the `slapd.conf` file

NOTE: The aforementioned steps of the configuration are for OpenLDAP Server only. If you need to configure Infrastructure for any other LDAP Server, you will have to make the changes appropriately.

5. In the command prompt, navigate to the LDAP installation directory and execute the following command :

```
ldapadd -D"ROOTDN"  -w ROOTPASS -f/data/Reveleus.ldif
```

This is for creating the entries for Users, User Groups, Functions, Profiles, Segments, Domains, Roles, and HolidayMaster in the Data information Tree of LDAP.

6. Make an entry in the `Domains.ldif` file for each Information Domain that is created through the Infrastructure UI.
7. To add an entry corresponding to the new Information Domain to the `Domains.ldif` file, add the following block of text with the appropriate values:

NOTE: DSNID refers to Information Domain name.

```
dn: DSNID=<DSN ID>,ou=Domains,@LDAP_DIRECTORY_ROOTCONTEXT@
changetype: add
mappedsegments: <Mapped segments/~>
dsnid: <DSN ID>
infodomname: < Information Domain Name>
objectClass: Infodom
objectClass: top
infodomdescription: < Information Domain Description>
```

Example:

```
dn: DSNID=FUSIONMOCK, ou=Domains, dc=FTP1,dc=com
mappedsegments: ~
dsnid: FUSIONMOCK
infodomname: FUSIONMOCK
objectClass: Infodom
objectClass: top
infodomdescription: FUSIONMOCK
```

8. Navigate to LDAP installation directory and execute the following command:

```
D"ROOTDN" -w ROOTPASS -f/data/Domains.ldif
```

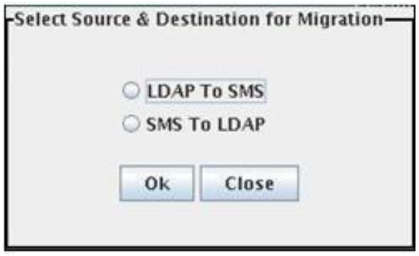
NOTE: You can add entries for multiple Information Domains at the same time.

13.8.4 Migrate Data from CSSMS tables to LDAP server and from LDAP to SMS

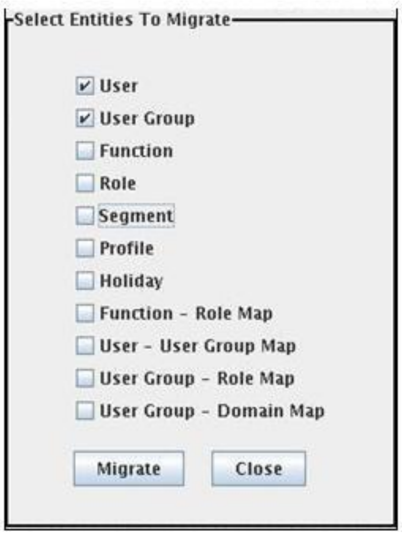
If you are using LDAP authentication, it is required to migrate all the details from the CSSMS table, which contains the information entered using the Infrastructure Identity Management module to the LDAP Server. Similarly, you can migrate the details from LDAP to SMS.

To migrate data from the CSSMS tables to LDAP server and vice versa:

1. Invoke the `LDAP_Migration.sh` file in `$FIC_HOME/MigrationUtilities/Migration_LDAP/ bin` folder. The *Select Source & Destination for Migration* window is displayed with the option to migrate the data from SMS to LDAP and vice versa.



2. Select the **SMS to LDAP** option to migrate from SMS to LDAP or select the **LDAP To SMS** option to migrate from LDAP to SMS and click **OK**. The *Select Entities to Migrate* window is displayed.



☑ User
☑ User Group
□ Function
□ Role
□ Segment
□ Profile
□ Holiday
□ Function - Role Map
□ User - User Group Map
□ User Group - Role Map
□ User Group - Domain Map

You can select the data that you wish to migrate such as Users, User Groups, Functions, Roles, Segment, Profiles, Holiday Master, Function Role Maps, User - User Group Maps, User Group Role Map, and User Group- Domain Map.

3. Select the entities that you wish to migrate and click **Migrate**. The data is migrated and a confirmation dialog is displayed.

You can verify the data migrated to LDAP server through the LDAP Browser and the data migrated to SMS in the OFSAAI tables.

NOTE: You should also enter the passwords for all the users since the passwords are not migrated in migration process.

13.9 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.

13.9.1 Knowing the Prerequisites

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

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

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]

13.9.2 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.

13.10 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>
   ```

13.11 Configuring WebLogic

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

13.11.1 Knowing the Prerequisites for OFSAA on WebLogic

Download and install the one-off patch **25343603** from My Oracle Support if OFSAA is deployed on **Oracle WebLogic Server version 12.2.x**. See the Readme available with the patch for further instructions on installing the patch.

NOTE: See the Technology Matrix for a list of supported servers for OFSAAI 8.x.

13.11.2 Configuring WebLogic for REST Services Authorization

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

1. Open the *config.xml* file located in the domain where OFSAA is deployed.
2. Directory: *<domain_home>/config/config.xml*
3. Add the following in the security-configuration tag:
4. `<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>`
5. Disable **Encrypt Login Password** on the *Configuration* screen.

NOTE: To disable Encrypt Login Password, see the *Configuration* section in the OFS Analytical Applications Infrastructure User Guide.

13.12 SSO Authentication (SAML) Configuration

This feature has been introduced in 8.0.3.0.0 release.

OFSAA can be configured as “Service Provider” using SAML 2.0 protocol. Following is the configuration required if you want to register OFSAA as Service Provider.

To register OFSAA as Service Provider, update `sp_metadata.xml` file which is located in `$FIC_HOME/conf/` folder.

```
<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/<context>/logout.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 attribute (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”.

13.13 Public Key Authentication

This section is applicable for versions 8.0.4.0.0 and later.

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

13.13.1 Prerequisite

You have a working SSH server and client installed.

13.13.2 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. Log in 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/AAI
AKG/MYKey/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.

13.13.3 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:

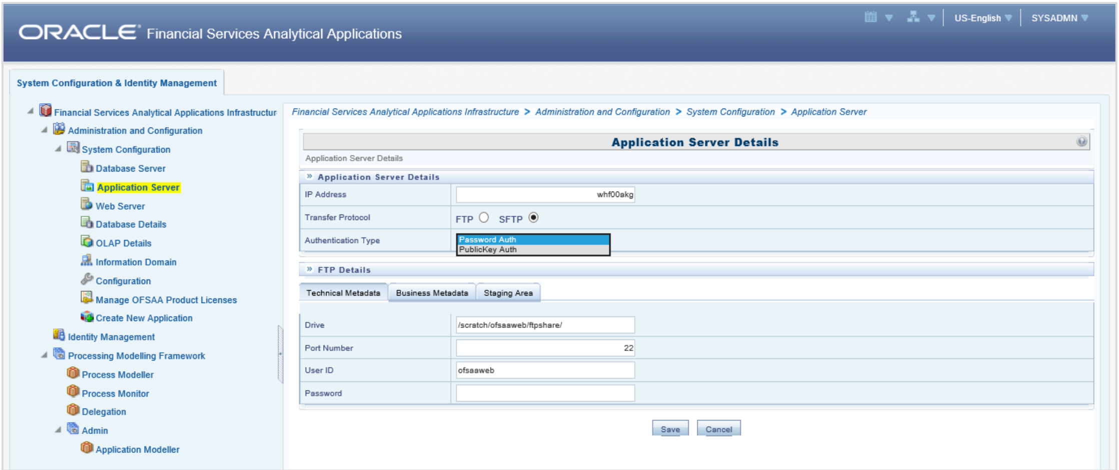
1. Convert private key to OpenSSH format.
2. Change passphrase using the following OpenSSH command:

   ```
   $ ssh-keygen -f <PRIVATE_KEY_PATH> -p
   ```

   `<private_key_path>` refers to path where private key is located including private key name.

13.13.4 Configurations Required in OFSAA Setup

1. Navigate to **System Configuration & Identity Management** tab, expand **Administration and Configuration** > **System Configuration** and select **Application Server**.
2. In the *Application Server Details* window, click **Modify**.


ORACLE Financial Services Analytical Applications
US-English
SYSADMN
System Configuration & Identity Management
Financial Services Analytical Applications Infrastructur
Administration and Configuration
System Configuration
Database Server
Application Server
Web Server
Database Details
OLAP Details
Information Domain
Configuration
Manage OFSAA Product Licenses
Create New Application
Identity Management
Processing Modelling Framework
Process Modeller
Process Monitor
Delegation
Admin
Application Modeller
Financial Services Analytical Applications Infrastructure > Administration and Configuration > System Configuration > Application Server
Application Server Details
Technical Metadata
Business Metadata
Staging Area
Save
Cancel

Application Server Details

» Application Server Details

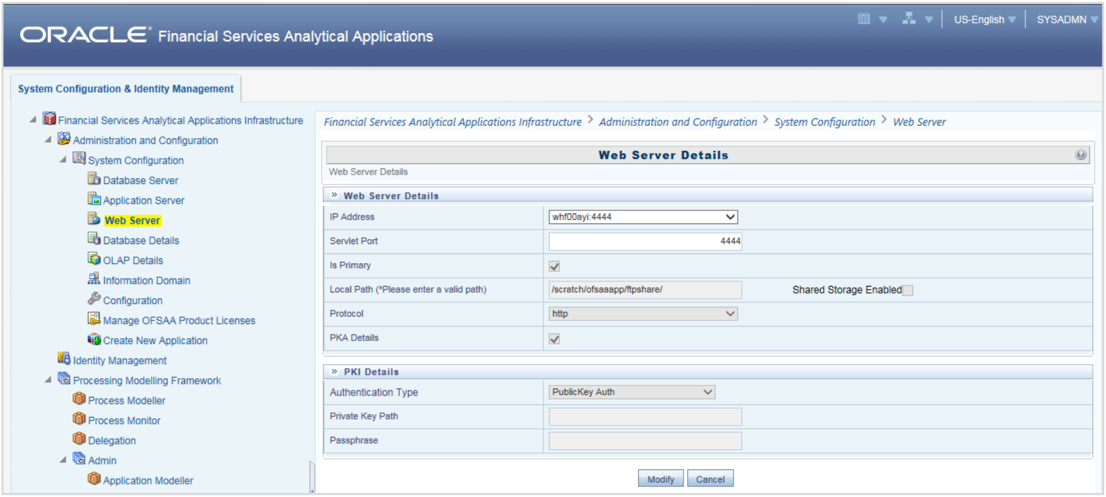
IP Address	whf00akg
Transfer Protocol	FTP ○ SFTP ●
Authentication Type	Password Auth PublicKey Auth

» FTP Details

Drive	/scratch/ofsaaweb/ftpshare/
Port Number	22
User ID	ofsaaweb
Password	

3. Select **Authentication Type** as **Publickey Auth.**
4. Click **Save**.
5. A confirmation message is displayed to inform that you need to provide the PKI details in the *Web Server Details* window. Click **OK**.

6. Click **Web Server** from the LHS menu. The *Web Server Details* window is displayed.


ORACLE Financial Services Analytical Applications
US-English
SYSADMN
System Configuration & Identity Management
Financial Services Analytical Applications Infrastructure
Administration and Configuration
System Configuration
Database Server
Application Server
Web Server
Database Details
OLAP Details
Information Domain
Configuration
Manage OFSAA Product Licenses
Create New Application
Identity Management
Processing Modelling Framework
Process Modeller
Process Monitor
Delegation
Admin
Application Modeller
Financial Services Analytical Applications Infrastructure > Administration and Configuration > System Configuration > Web Server
Web Server Details
Web Server Details
Modify
Cancel

» Web Server Details

IP Address	whf00ayi:4444	
Servlet Port	4444	
Is Primary	☑	
Local Path (*Please enter a valid path)	/scratch/ofsaaapp/ftpshare/	Shared Storage Enabled □
Protocol	http	
PKA Details	☑	

» PKI Details

Authentication Type	PublicKey Auth
Private Key Path	
Passphrase	

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.

7. Click **Modify**.

8. Enter **Private Key Path** and **Passphrase** which you created during Step 1.

9. Click **Save**.

13.14 Enable and Disable Users

Note: This feature is applicable to OFSAA 8.0.4.0.0 and later releases.

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.

13.14.1 Prerequisites

The following prerequisites must be met before you proceed with the password reset:

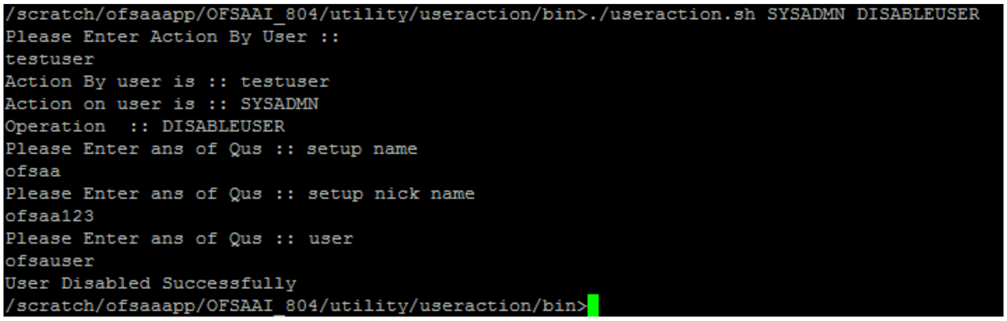
- Check if the Authentication Type selected is **SMS Authentication & Authorization**. Enabling and disabling users does not work for other authentication types. For more details, see the information on **Authentication Type** field in the **Configuration** subsection in **System Configuration** in the 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.

13.14.2 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.
   The following illustration displays a disable user action:



```
/scratch/ofsaaapp/OFSAAI_804/utility/useraction/bin>./useraction.sh SYSADMN DISABLEUSER
Please Enter Action By User ::
testuser
Action By user is :: testuser
Action on user is :: SYSADMN
Operation  :: DISABLEUSER
Please Enter ans of Qus :: setup name
ofsaa
Please Enter ans of Qus :: setup nick name
ofsaa123
Please Enter ans of Qus :: user
ofsauser
User Disabled Successfully
/scratch/ofsaaapp/OFSAAI_804/utility/useraction/bin>
```

13.15 Password Reset

Note: This feature is applicable for OFSAA 8.0.4.0.0 and later releases.

The password for users can be reset from the command prompt. Only users with the requisite administrator role can perform this action.

13.15.1 Prerequisites

The following prerequisites must be met before you proceed with the password reset:

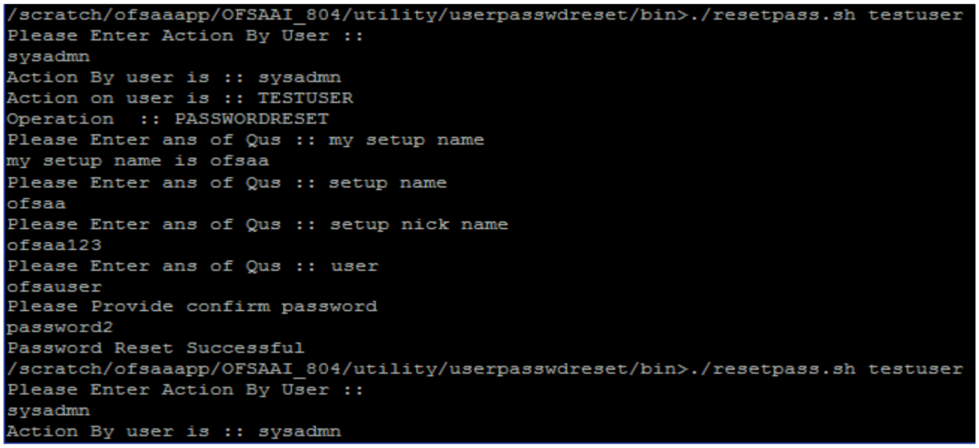
- Check if the Authentication Type selected is **SMS Authentication & Authorization**. Password reset does not work for other authentication types. For more details, see the information on **Authentication Type** field in the **Configuration** subsection in **System Configuration** in the OFS Analytical 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.

13.15.2 Resetting a User Password

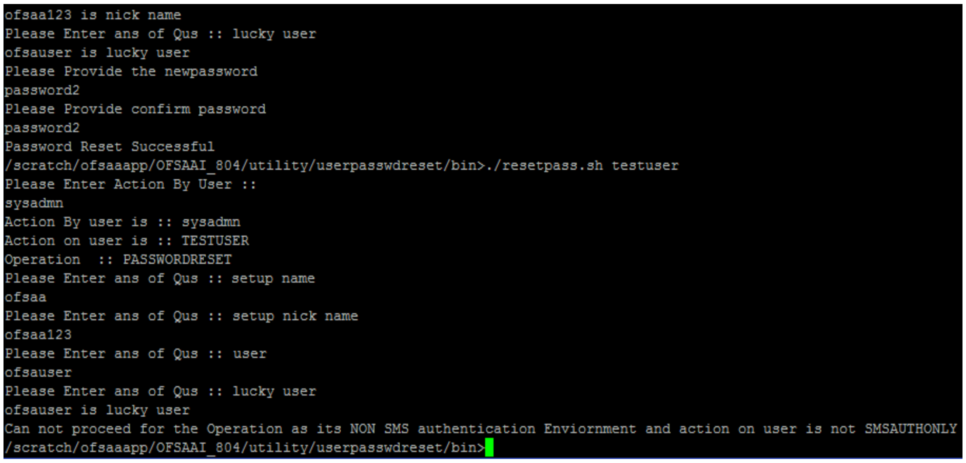
Perform the following procedure to reset the password for a user:

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>
   ```
   For example:
   ```
   ./resetpass.sh johnsmith
   ```
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:



```
/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:



```
ofsaa123 is nick name
Please Enter ans of Qus :: lucky user
ofsauser is lucky user
Please Provide the newpassword
password2
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
Action on user is :: TESTUSER
Operation  :: PASSWORDRESET
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 Enter ans of Qus :: lucky user
ofsauser is lucky user
Can not proceed for the Operation as its NON SMS authentication Enviornment and action on user is not SMSAUTHONLY
/scratch/ofsaaapp/OFSAAI_804/utility/userpasswdreset/bin>
```

13.16 Configuring OFSAA OIM Connector

Note: This feature is applicable for OFSAA Release 8.0.4.1.0, 8.0.5.0.1 and 8.0.5.1.0.

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.

13.16.1 Knowing the Prerequisites

The following are the prerequisites for this configuration:

1. You must have the user credentials with which you installed IDM Suite.
2. You must have the user credentials with which you installed OFSAA 8.0.4.1.0 AAI ML.
3. You must download and install the one-off patch **26531002** from My Oracle Support.

NOTE: The installation of the preceding one-off patch is required only for OFSAA Release 8.0.4.1.0. Skip this step for other releases.

4. You must have the host information for OIM and OFSAA server(s).

13.16.2 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. Log in to the OFSAA host with your OFSAA user credentials.
    a. Navigate to *$FIC_HOME/util*ity.
    b. Copy the **OFSConnector** directory to your local system.
2. Log in to the OIM host with OIM user credentials.
3. Copy the **OFSConnector** directory from your local system to *$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.ide
ntityconnectors.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>>
```

For example,

```
sh deploySchTask.sh -username xelsysadm -password Welcome1 -
serverURL t3://whf00aum:14000 –id DEV
```

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:
   1. For SSO, <OFS_USER > is a valid OIM user. If the setup is non-SSO, then <OFS_USER> is SYSADMN.
   2. Based on the OIM version 11.1.2.2 or 11.1.2.3, select the appropriate version of the files to upload.

   For example,

   ```
   $OIM_ORACLE_HOME/connectors/OFSConnector/ImportMetadata.sh xelsysadm
   Welcome t3://whf00aum:14000 OFS-ConnectorConfig_11.1.2.2.xml DEV
   sysadmn password http://whf00abc:7001/ofsaa
   ```

   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:
    1. For SSO, <OFS_USER > is a valid OIM user. If the setup is non-SSO, then <OFS_USER> is SYSADMN.
    2. <OFSAA_ID> should always be unique for each environment. For example, UAT01.
    3. Based on the OIM version 11.1.2.2 or 11.1.2.3, select the appropriate version of the files to upload.

    For example,

    ```
    $OIM_ORACLE_HOME/connectors/OFSConnector/ImportMetadata.sh xelsysadm
    Welcome t3://whf00aum:14000 OFS-ITResource_11.1.2.2.xml UAT sysadmn
    password http://whf00xyz:7001/ofsaa
    ```

11. Set the System Property **XL.AllowAPHarvesting** to **TRUE**. See the following steps for the procedure to set the property:

    a. Log in to the **SYSADMIN** console.

    b. Click **System Configuration** to view *System Properties*.

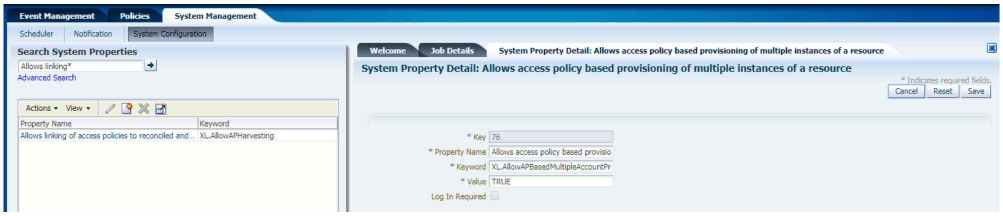
c. Enter **XL.AllowAPHarvesting** in **Search System Properties** and click ➡ to view the property name in the search results pane.

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.



Search System Properties

Allows linking*

Property Name	Keyword
Allows linking of access policies to reconciled and...	XL.AllowAPHarvesting

System Property Detail: Allows access policy based provisioning of multiple instances of a resource

* Indicates required fields.

* Key: 76

* Property Name: Allows access policy based provisio

* Keyword: XL.AllowAPBasedMultipleAccountPr

* Value: TRUE

Log In Required: □

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>')
```

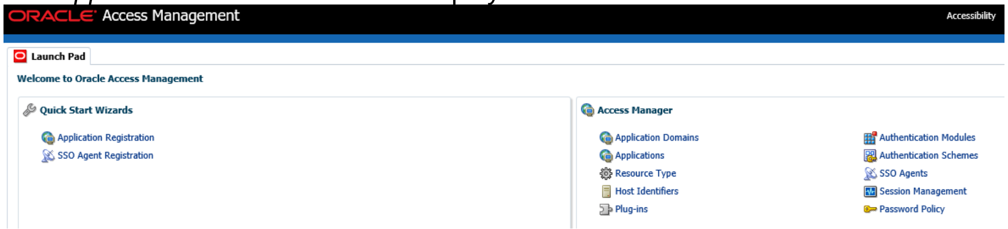
d. Import the OAM Policies using the following:

```
wls:/idm_domain/serverConfig>
importPolicy(pathTempOAMPolicyFile="/<path>/oam-policies.xml")
```

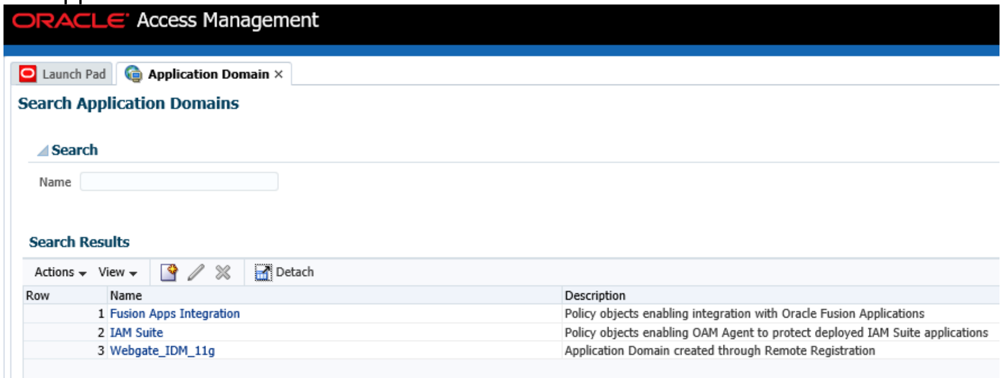
13. Perform OFSAA User Provisioning Configuration by applying Pre-authentication Advanced Rules to the basic Authorization Policy for users in the system. It is applied from the OAM console after IDM Provisioning and is done to switch to a form-based authentication scheme if the authorization header is not a basic scheme. Update the pre-authentication advanced rules to a form-based authentication scheme using the following steps:

a. Log in to the **OAM Administrator Console**.

b. From the **Launch Pad**, click **Application Domains** from the **Access Manager** widget. The *Application Domain* window is displayed.

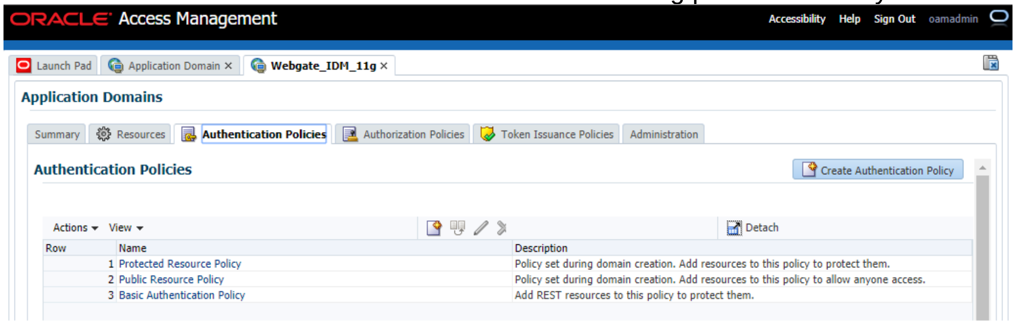


c. Search for the required application domain for which you want to switch the authentication scheme and click **Name** from the search results to display the details for the application domain.



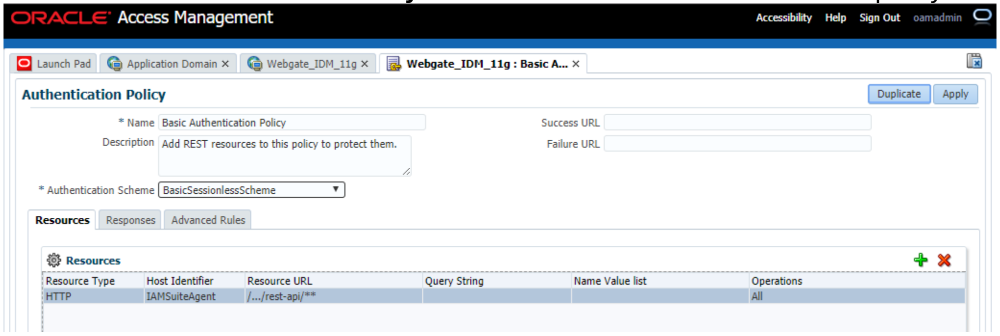
Row	Name	Description
1	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
2	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications
3	Webgate_IDM_11g	Application Domain created through Remote Registration

d. Click the **Authentication Policies** tab to view the existing policies in the system.



Row	Name	Description
1	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.
2	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
3	Basic Authentication Policy	Add REST resources to this policy to protect them.

e. Click **Basic Authentication Policy** from the list to view the details for the policy.



* Name: Basic Authentication Policy

Description: Add REST resources to this policy to protect them.

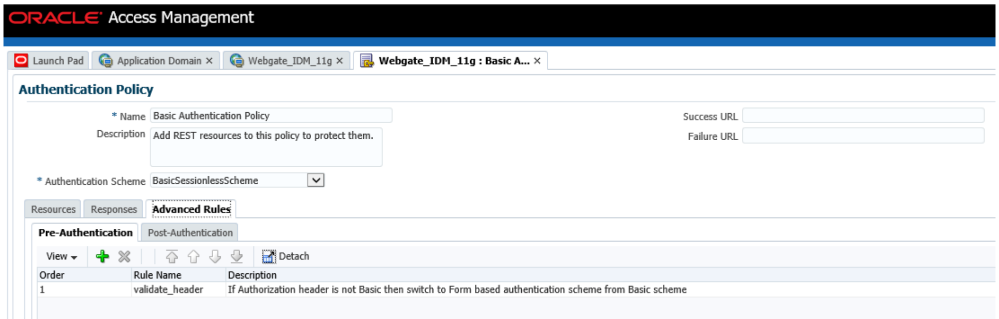
* Authentication Scheme: BasicSessionlessScheme

Success URL:

Failure URL:

Resource Type	Host Identifier	Resource URL	Query String	Name Value list	Operations
HTTP	IAMSuiteAgent	/.../rest-api/**			All

f. Click **Advanced Rules** tab to view the details for Pre-Authentication.



Authentication Policy

* Name: Basic Authentication Policy
Description: Add REST resources to this policy to protect them.
* Authentication Scheme: BasicSessionlessScheme
Success URL:
Failure URL:

Order	Rule Name	Description
1	validate_header	If Authorization header is not Basic then switch to Form based authentication scheme from Basic scheme

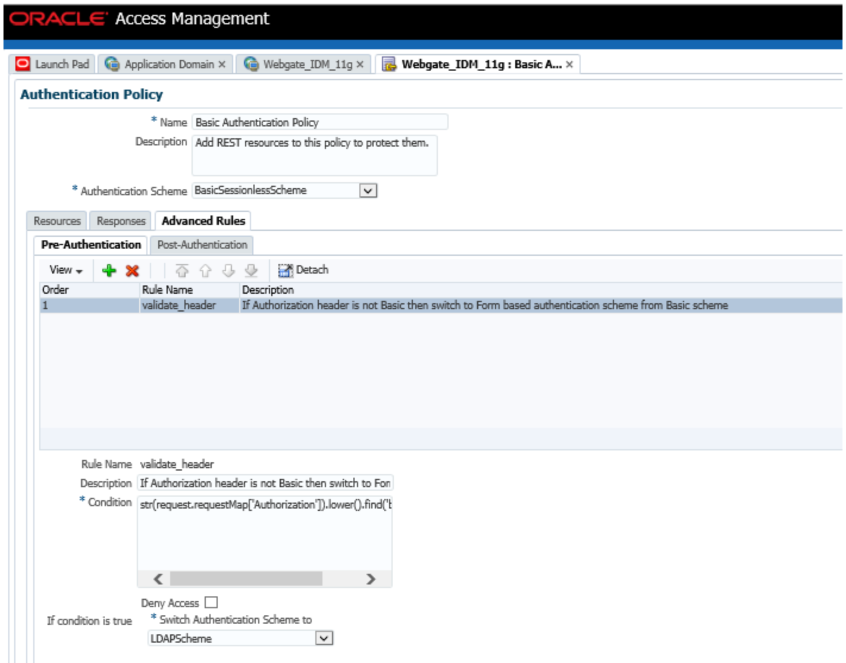
g. Click the **Add** ✚ button and create a rule with the following information:

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)



Authentication Policy

* Name: Basic Authentication Policy
Description: Add REST resources to this policy to protect them.
* Authentication Scheme: BasicSessionlessScheme

Order	Rule Name	Description
1	validate_header	If Authorization header is not Basic then switch to Form based authentication scheme from Basic scheme

Rule Name: validate_header
Description: If Authorization header is not Basic then switch to For
* Condition: str(request.requestMap['Authorization']).lower().find('b
Deny Access □
If condition is true: * Switch Authentication Scheme to: LDAPScheme

h. Click **Apply** to save.

13.16.3 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.

13.16.3.1 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.

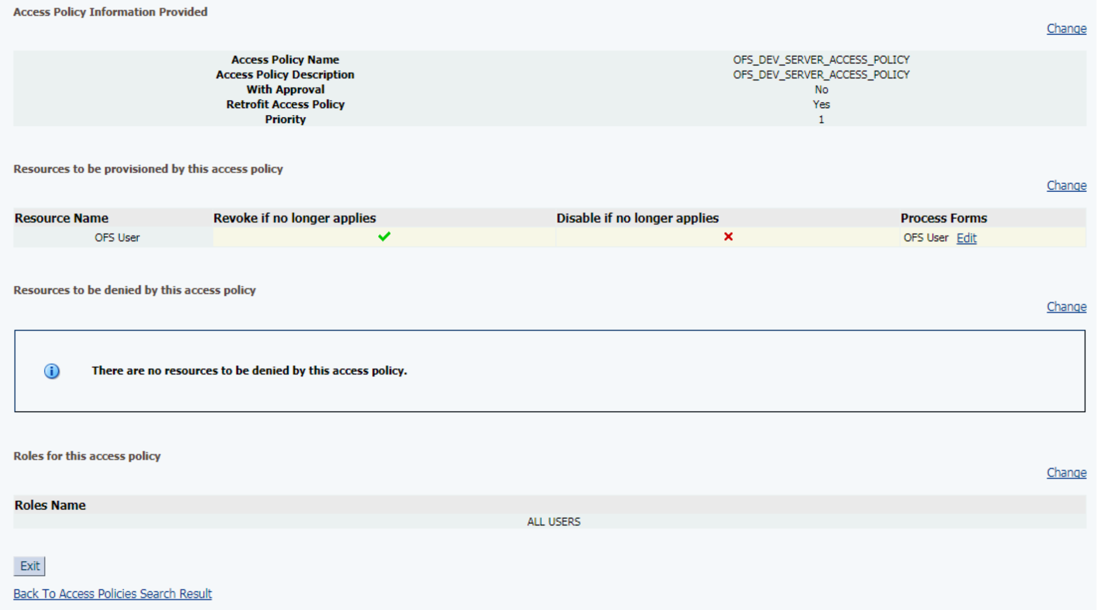
NOTE: If you use OFSAA Native Authentication (SMS), then the password policy for OIM and OFSAA should be the same.

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. Log in 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.



Access Policy Information Provided

Access Policy Name	OFS_DEV_SERVER_ACCESS_POLICY
Access Policy Description	OFS_DEV_SERVER_ACCESS_POLICY
With Approval	No
Retrofit Access Policy	Yes
Priority	1

Resources to be provisioned by this access policy

Resource Name	Revoke if no longer applies	Disable if no longer applies	Process Forms
OFS User	✓	✗	OFS User Edit

Resources to be denied by this access policy

There are no resources to be denied by this access policy.

Roles for this access policy

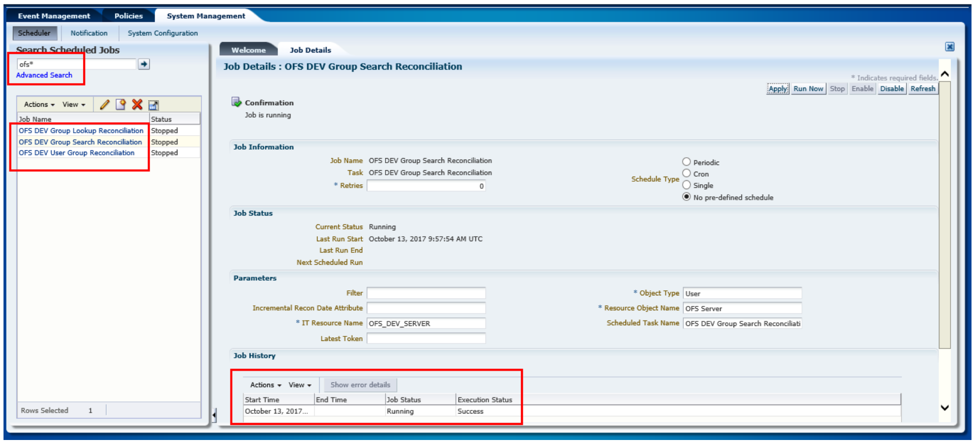
Roles Name
ALL USERS

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.



Search Scheduled Jobs

ofs*

Job Name	Status
OFS DEV Group Lookup Reconciliation	Stopped
OFS DEV Group Search Reconciliation	Stopped
OFS DEV User Group Reconciliation	Stopped

Rows Selected 1

Job Details : OFS DEV Group Search Reconciliation

* Indicates required fields.

Confirmation
Job is running

Job Information

Job Name OFS DEV Group Search Reconciliation
Task OFS DEV Group Search Reconciliation
* Retries 0

Schedule Type
○ Periodic
○ Cron
○ Single
● No pre-defined schedule

Job Status

Current Status Running
Last Run Start October 13, 2017 9:57:54 AM UTC
Last Run End
Next Scheduled Run

Parameters

Filter
Incremental Recon Date Attribute
* IT Resource Name OFS_DEV_SERVER
Latest Token
* Object Type User
* Resource Object Name OFS Server
Scheduled Task Name OFS DEV Group Search Reconciliati

Job History

Start Time	End Time	Job Status	Execution Status
October 13, 2017...		Running	Success

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:

   i. mins

   ii. hrs

   iii. 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:

   i. Daily

   ii. Weekly

   iii. Monthly on given dates

   iv. Monthly on given weekdays

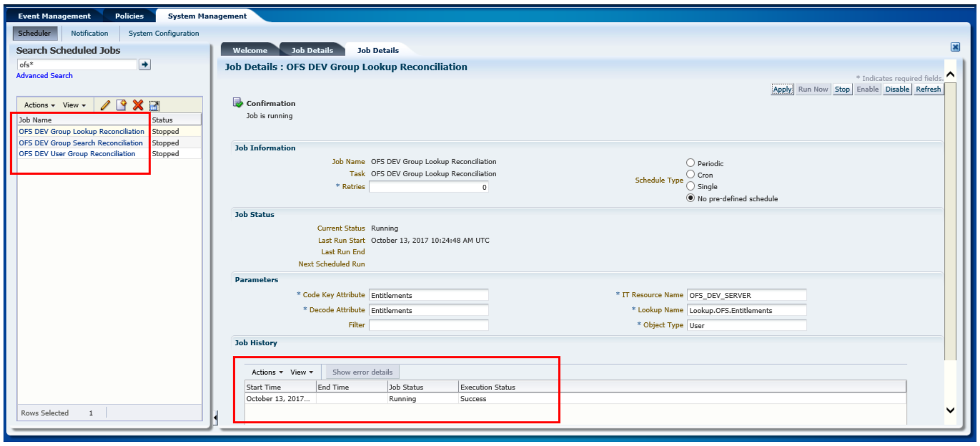
   v. Yearly
   After selecting a value, you can enter an integer value in the Days between runs field.

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.



Search Scheduled Jobs

ofs*

Job Name	Status
OFS DEV Group Lookup Reconciliation	Stopped
OFS DEV Group Search Reconciliation	Stopped
OFS DEV User Group Reconciliation	Stopped

Rows Selected 1

Job Details : OFS DEV Group Lookup Reconciliation

* Indicates required fields.

Confirmation
Job is running

Job Information

Job Name OFS DEV Group Lookup Reconciliation
Task OFS DEV Group Lookup Reconciliation
* Retries 0

Schedule Type ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status

Current Status Running
Last Run Start October 13, 2017 10:24:48 AM UTC
Last Run End
Next Scheduled Run

Parameters

* Code Key Attribute Entitlements
* Decode Attribute Entitlements
Filter
* IT Resource Name OFS_DEV_SERVER
* Lookup Name Lookup.OFS.Entitlements
* Object Type User

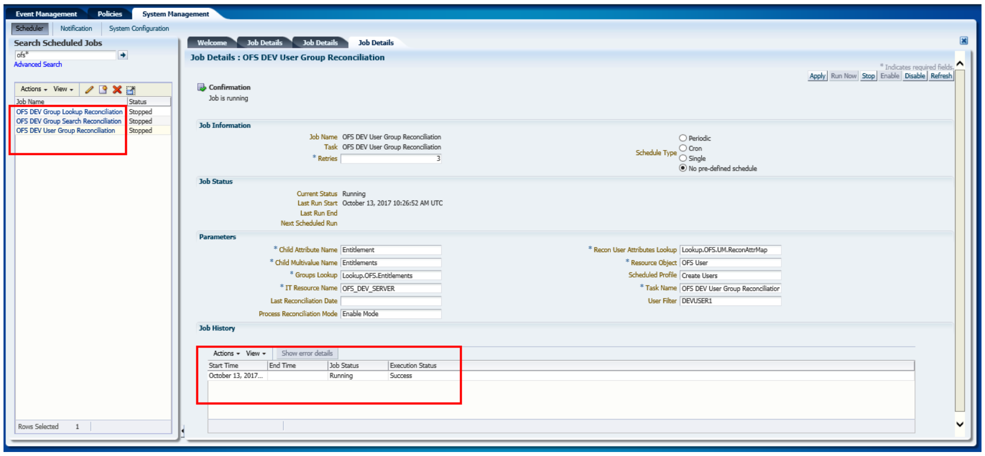
Job History

Start Time	End Time	Job Status	Execution Status
October 13, 2017...		Running	Success

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.



Search Scheduled Jobs

ofs*

Job Name	Status
OFS DEV Group Lookup Reconciliation	Stopped
OFS DEV Group Search Reconciliation	Stopped
OFS DEV User Group Reconciliation	Stopped

Rows Selected 1

Job Details : OFS DEV User Group Reconciliation

* Indicates required fields.

Confirmation
Job is running

Job Information

Job Name OFS DEV User Group Reconciliation
Task OFS DEV User Group Reconciliation
* Retries 3

Schedule Type ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status

Current Status Running
Last Run Start October 13, 2017 10:26:52 AM UTC
Last Run End
Next Scheduled Run

Parameters

* Child Attribute Name Entitlement
* Child Multivalue Name Entitlements
* Groups Lookup Lookup.OFS.Entitlements
* IT Resource Name OFS_DEV_SERVER
Last Reconciliation Date
Process Reconciliation Mode Enable Mode
* Recon User Attributes Lookup Lookup.OFS.UM.ReconAttrMap
* Resource Object OFS User
Scheduled Profile Create Users
* Task Name OFS DEV User Group Reconciliatior
User Filter DEVUSER1

Job History

Start Time	End Time	Job Status	Execution Status
October 13, 2017...		Running	Success

14. Select from **Schedule Type**, the frequency at which you want to run the job. For description, see Schedule Type.

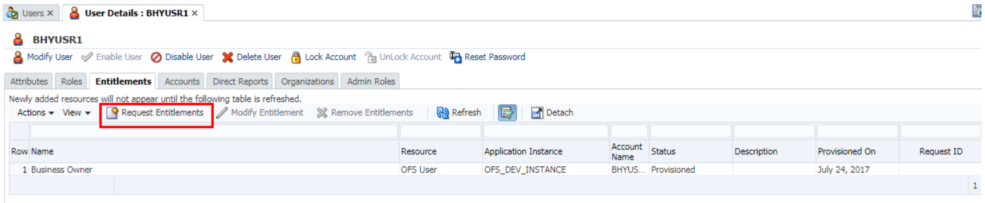
15. Enter the login user name in **User Filter** to apply the user group reconciliation to. To add more than one user name, separate by using commas (,). Leave the field empty to apply to all users.

16. Run **OFS {OFSAA_ID} User Group Reconciliation** and check for successful execution of the run.

13.16.3.2 Provisioning Entitlement Requests

The following is the procedure to provision entitlement requests for Users:

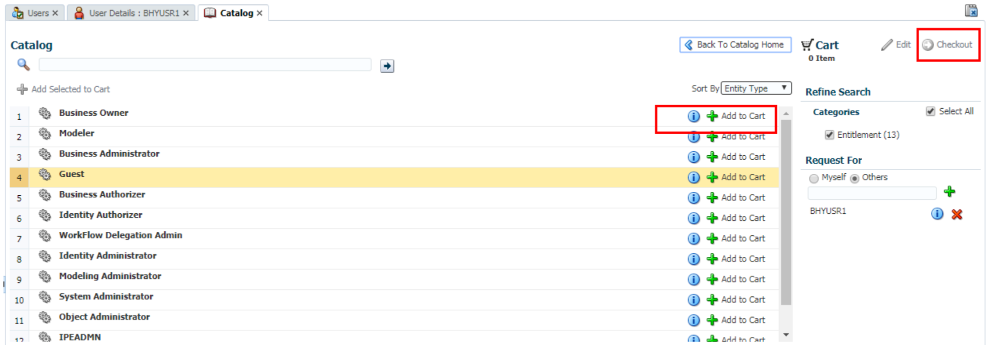
1. Log in to **OIM Identity Console**.
2. Select the User and click **Request Entitlements** on the Entitlements window to display the *Catalog* window. **Catalog** displays a list of all OFSAA group as Entitlements.



Newly added resources will not appear until the following table is refreshed.

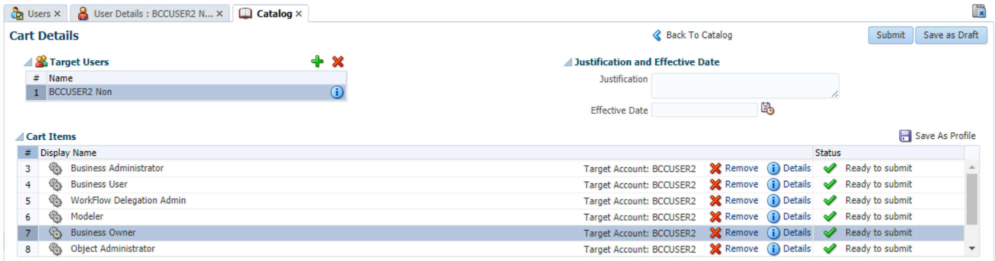
Row	Name	Resource	Application Instance	Account Name	Status	Description	Provisioned On	Request ID
1	Business Owner	OFS User	OFS_DEV_INSTANCE	BHYUS...	Provisioned		July 24, 2017	

3. Select User and click **Add to Cart**. Click **Checkout** to view the *Cart Details* window.



1	Business Owner	Add to Cart
2	Modeler	Add to Cart
3	Business Administrator	Add to Cart
4	Guest	Add to Cart
5	Business Authorizer	Add to Cart
6	Identity Authorizer	Add to Cart
7	WorkFlow Delegation Admin	Add to Cart
8	Identity Administrator	Add to Cart
9	Modeling Administrator	Add to Cart
10	System Administrator	Add to Cart
11	Object Administrator	Add to Cart
12	IPEADMN	Add to Cart

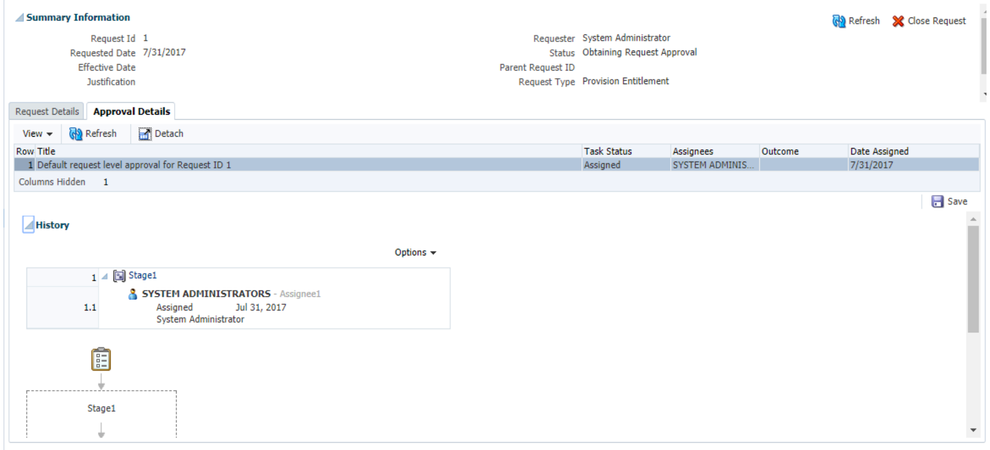
4. Click **Submit**. The request is processed for approval. See [Approving Request Entitlements]() for more details.



#	Name
1	BCCUSER2 Non

#	Display Name				Status
3	Business Administrator	Target Account: BCCUSER2	Remove	Details	✓ Ready to submit
4	Business User	Target Account: BCCUSER2	Remove	Details	✓ Ready to submit
5	WorkFlow Delegation Admin	Target Account: BCCUSER2	Remove	Details	✓ Ready to submit
6	Modeler	Target Account: BCCUSER2	Remove	Details	✓ Ready to submit
7	Business Owner	Target Account: BCCUSER2	Remove	Details	✓ Ready to submit
8	Object Administrator	Target Account: BCCUSER2	Remove	Details	✓ Ready to submit

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.



Summary Information

Request Id 1
Requested Date 7/31/2017
Effective Date
Justification

Requester System Administrator
Status Obtaining Request Approval
Parent Request ID
Request Type Provision Entitlement

Row	Title	Task Status	Assignees	Outcome	Date Assigned
1	Default request level approval for Request ID 1	Assigned	SYSTEM ADMINIS...		7/31/2017

Columns Hidden 1

History

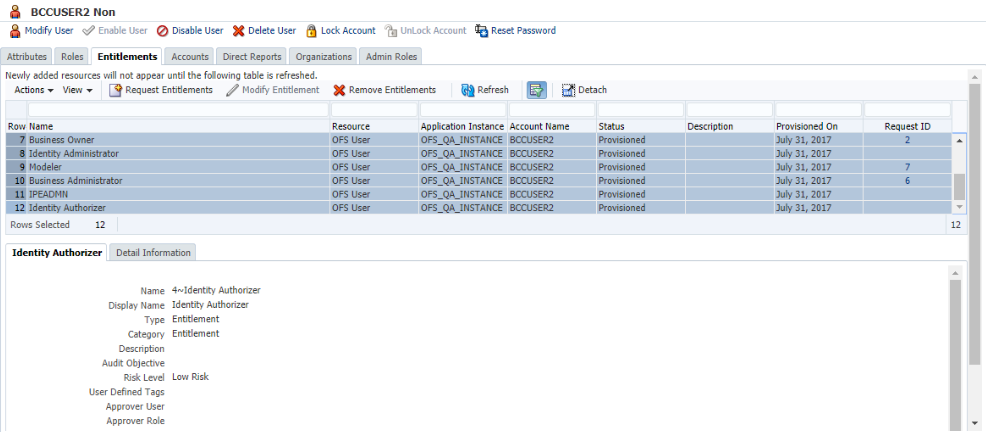
1 Stage1
1.1 SYSTEM ADMINISTRATORS - Assignee1
Assigned Jul 31, 2017
System Administrator

13.16.3.3 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. Log in 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.



BCCUSER2 Non

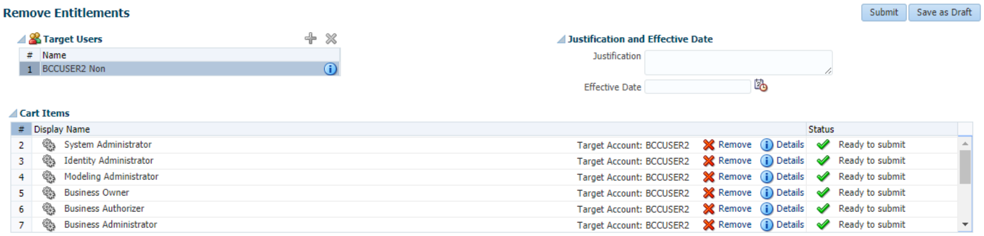
Newly added resources will not appear until the following table is refreshed.

Row	Name	Resource	Application Instance	Account Name	Status	Description	Provisioned On	Request ID
7	Business Owner	OFS User	OFS_QA_INSTANCE	BCCUSER2	Provisioned		July 31, 2017	2
8	Identity Administrator	OFS User	OFS_QA_INSTANCE	BCCUSER2	Provisioned		July 31, 2017	
9	Modeler	OFS User	OFS_QA_INSTANCE	BCCUSER2	Provisioned		July 31, 2017	7
10	Business Administrator	OFS User	OFS_QA_INSTANCE	BCCUSER2	Provisioned		July 31, 2017	6
11	IPEADMN	OFS User	OFS_QA_INSTANCE	BCCUSER2	Provisioned		July 31, 2017	
12	Identity Authorizer	OFS User	OFS_QA_INSTANCE	BCCUSER2	Provisioned		July 31, 2017	

Rows Selected 12 12

Name 4~Identity Authorizer
Display Name Identity Authorizer
Type Entitlement
Category Entitlement
Description
Audit Objective
Risk Level Low Risk
User Defined Tags
Approver User
Approver Role

3. Click **Submit**. The request is processed for approval. See Approving Request Entitlements for more details.



#	Name
1	BCCUSER2 Non

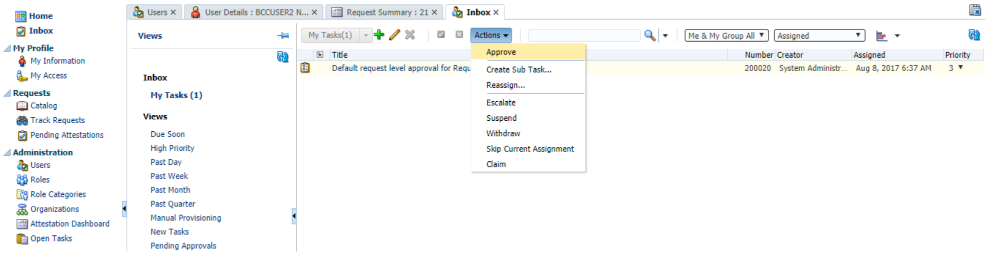
#	Display Name				Status
2	System Administrator	Target Account: BCCUSER2	Remove	Details	Ready to submit
3	Identity Administrator	Target Account: BCCUSER2	Remove	Details	Ready to submit
4	Modeling Administrator	Target Account: BCCUSER2	Remove	Details	Ready to submit
5	Business Owner	Target Account: BCCUSER2	Remove	Details	Ready to submit
6	Business Authorizer	Target Account: BCCUSER2	Remove	Details	Ready to submit
7	Business Administrator	Target Account: BCCUSER2	Remove	Details	Ready to submit

13.16.3.4 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.

The procedure to approve an entitlement request is in the following:

1. Log in 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.



Title	Number	Creator	Assigned	Priority
Default request level approval for Requ	200020	System Administr...	Aug 8, 2017 6:37 AM	3

13.17 Using REST APIs for user management from third-party IDMs

> **NOTE:** The APIs listed in this topic are available from release 8.0.4.0.0 and later. However, in release 8.0.5 and later, “rest” has been modified to “rest-api” in the REST URLs.

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.

13.17.1 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 should be mapped to the IDMGMTADVN role.

13.17.2 Understanding REST API Specifications

The following table provides details for the REST APIs:

Number	Requirement	URL	Method Type	Request	Sample Request JSON	Comments

1	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)
					}
					}
						All FIELDS are mandatory.
						Date format is mm/dd/yyyy. If user_is_authorized is set to true, then user is authorized during creation.

Number	Requirement	URL	Method Type	Request	Sample Request JSON	Comments

2	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)
					}
					}
						All FIELDS are mandatory.
						Date format is mm/dd/yyyy. If user_is_authorized is set to true, then user is authorized during creation.

3	Delete User	/rest-api/idm/service/delete/user	POST	TEXT	USERID	User ID is mandatory.
4	Authorize User	/rest-api/idm/service/authorize/user	POST	TEXT	USERID	User ID is mandatory.
5	Reinstate user	/rest-api/idm/service/reinstate/user	POST	TEXT	USERID	User ID is mandatory.

Number	Requirement	URL	Method Type	Request	Sample Request JSON	Comments

6	Map user to group	/rest-api/idm/service/map/groupmembers	POST	JSON	{
					"user_id": "user_id",
					"group": [
					{
					"group_id": "group_id",
					"group_name": "groupname"
					},
					...
					]
					}
						Mapping of user id to groups.

13.18 Configuring the Logout URL for OBIEE in OFSAA

Note: This feature is applicable for OFSAA Release 8.0.2.2.0, 8.0.4.2.0 and 8.0.5.1.0.

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. Log in to the OFSAA database with CONFIG user credentials:
2. In the database, update the configuration table with 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

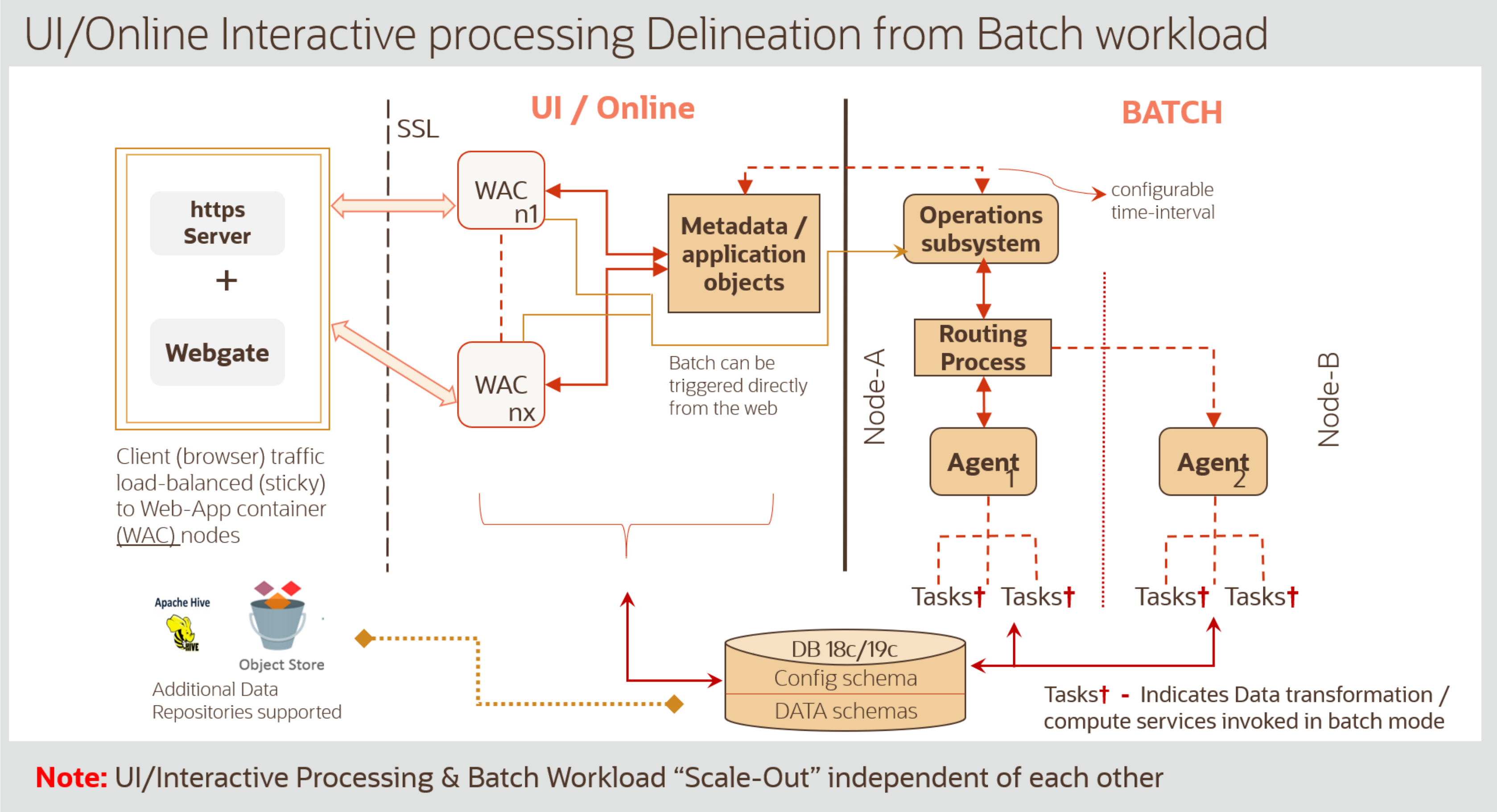
Replace `<IS_CROSSDOMAIN>` with **true** if OBIEE is on another server.

For example,

```
update configuration set paramvalue = 'true' where paramname =
   'OBIEE_CROSS_DOMAIN_VAL';
```

14 Appendix A – Distributed Activation Manager Deployment

Illustration of Distributed Activation Manager Deployment



UI/Online Interactive processing Delineation from Batch workload

UI / Online

BATCH

SSL

https Server

+

Webgate

WAC n1

WAC nx

Metadata / application objects

Batch can be triggered directly from the web

Operations subsystem

configurable time-interval

Routing Process

Agent 1

Agent 2

Node-A

Node-B

Task† Task† Task† Task†

Client (browser) traffic load-balanced (sticky) to Web-App container (WAC) nodes

Apache Hive

Object Store

Additional Data Repositories supported

DB 18c/19c

Config schema

DATA schemas

Task† - Indicates Data transformation / compute services invoked in batch mode

Note: UI/Interactive Processing & Batch Workload “Scale-Out” independent of each other

OFSAAI
Administration Guide

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

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

Due care has been taken to make this Administration Guide and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this Administration Guide and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.