Oracle Financial Services
Advanced Analytical
Applications Infrastructure
Application Pack

Administration and
Configuration Guide

Release 8.0.6.0.0+
## Document Control

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Revision Date</th>
<th>Changes Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Created May 2018</td>
<td>Added Configurations for 8.0.6.0.0 version.</td>
</tr>
<tr>
<td>2.0</td>
<td>Updated July 2018</td>
<td>Updated for OFSAAAAAI-13230 and OFSAAAAAI-15150.</td>
</tr>
<tr>
<td>3.0</td>
<td>Updated Aug 2018</td>
<td>Updated for 8.0.6.1.0 ML changes.</td>
</tr>
<tr>
<td>4.0</td>
<td>Updated Sep 2018</td>
<td>Updated the HTTPS Protocol section for Bug 27821807.</td>
</tr>
</tbody>
</table>

Created by: Brijesh/Gitcy  
Reviewed by: Bharath/Suresh  
Approved by: Jeev/Subhashini/Viru
TABLE OF CONTENTS

PREFACE ...................................................................................................................... 8
Summary ......................................................................................................................... 8
Audience ......................................................................................................................... 8
Related Documents ................................................................................................ ...... 8
Conventions .................................................................................................................. 9
Abbreviations ............................................................................................................... 9

1 DATA MANAGEMENT TOOLS (DMT) MODULE CONFIGURATIONS ......................... 11
  1.1 Data Mapping Configurations .............................................................................. 11
    1.1.1 Data Movement from RDBMS Source to HDFS Target (T2H) ......................... 11
    1.1.2 Data Movement from HDFS Source to RDBMS Target (H2T) ......................... 12
    1.1.3 Data Movement from File to HDFS Target (F2H) ........................................... 12
    1.1.4 Data Movement of WebLog Source to HDFS Target (L2H) ......................... 13
  1.2 Oracle® Loader for Hadoop (OLH) Configuration ................................................ 16
    1.2.1 Prerequisite .................................................................................................. 16
    1.2.2 Steps for Configuring OLH .......................................................................... 16
    1.2.3 Limitations .................................................................................................. 18
  1.3 Sqoop Configuration ............................................................................................ 19
    1.3.1 Prerequisites ............................................................................................... 19
    1.3.2 Steps for Configuring Sqoop ....................................................................... 19
  1.4 SCD Execution on Hive Information Domain ....................................................... 22
    1.4.1 Constraints .................................................................................................. 22
    1.4.2 Assumptions: ............................................................................................... 22
  1.5 Heterogeneous Support for SCD to RDBMS ......................................................... 23
    1.5.1 Assumptions ............................................................................................... 23

2 DIMENSION MANAGEMENT MODULE CONFIGURATIONS ..................................... 24
  2.1 Configurations to use Alphanumeric and Numeric Codes for Dimension Members .... 24
    2.1.1 Configure Alphanumeric Dimensions ......................................................... 25
    2.1.2 Configure Numeric Dimensions ................................................................. 25
    2.1.3 Configure Alphanumeric Code in Simple Dimension Tables ...................... 27
    2.1.4 Create Index on Code Column ..................................................................... 27
  2.2 General Configurations for Dimension Management Module .............................. 27

3 RULE RUN FRAMEWORK CONFIGURATIONS .......................................................... 31
# Table of Contents

3.1 Performance Optimization Setting for RRF Module .......................................................... 31
  Behavior of Execution Modes .............................................................................................. 33
  Use ROWID ...................................................................................................................... 33
  Use PARTITION ............................................................................................................... 34
  Hints/ Scripts .................................................................................................................. 34

3.2 Component Registration in RRF ......................................................................................... 34
  3.2.1 Component Detailed Implementation Class .............................................................. 34
  3.2.2 Deployment ............................................................................................................ 38
  3.2.3 Entry to PR2_COMPONENT_MASTER Table ............................................................. 39
  3.2.4 Sample Code ......................................................................................................... 40

3.3 Configure Forms XML to Execute Server Side Rule .......................................................... 40

4 OPERATIONS ....................................................................................................................... 41
  4.1 Distributed Activation Manager (AM) Based Processing .............................................. 41
    4.1.1 Setting Up of Secondary AM Server .................................................................. 41
    4.1.2 Configuring OFSAA Instance through Load Balancer to Distribute Batch Tasks on Multiple AM Nodes .................................................................................. 43
    4.1.3 Executing Batches on Multiple AM Nodes ......................................................... 44

5 UNIFIED ANALYTICAL METADATA CONFIGURATIONS ................................................. 45
  5.1 Hierarchy Node Internationalization .............................................................................. 45
    5.1.1 Scope ................................................................................................................... 45
    5.1.2 Prerequisites ........................................................................................................ 45
    5.1.3 Multi Language Support (MLS) Table ................................................................ 46
    5.1.4 Node Generation Process .................................................................................... 50
    5.1.5 Configure Mapper for Multiple Locales ............................................................... 50
    5.1.6 Update Nodes in Existing Regular BI and PC Hierarchies .................................. 51
    5.1.7 Limitations .......................................................................................................... 51

  5.2 Data Element Filters Classification ............................................................................... 51
    5.2.1 Limitations .......................................................................................................... 52

  5.3 Configuring Essbase Connectivity Check ....................................................................... 53
    5.3.1 Settings in .profile ............................................................................................. 53
    5.3.2 Checking the Connection .................................................................................... 53

6 ENTERPRISE MODELING FRAMEWORK CONFIGURATIONS ......................................... 54
  6.1 Configuration of Oracle R distribution and Oracle R enterprise (ORE) .......................... 54
  6.2 Configurations for OFSAAI Remote Invocation of Scripted Models Using Standard R Distributions ................................................................. 54
    6.2.1 Prerequisite ........................................................................................................ 54
    6.2.2 Configurations .................................................................................................... 56
6.2.3 Structure of the gss-jasa.conf File ................................................................. 57
6.3 Configurations for Open-R with HDFS .............................................................. 58
6.3.1 Prerequisites ................................................................................................. 58
6.3.2 Installing OFSAAIRunnerHDFS Package ...................................................... 58
6.3.3 Additional Configurations for ORAAH Executions ........................................ 59
6.4 Support for Scripts which work on HDFS Files Directly ...................................... 59
6.5 User Configurable Execution Implementation .................................................. 60
6.6 Configuration for Parallel Execution of Models ................................................ 60
6.7 Configurations for ORE Execution ...................................................................... 60
6.8 Variable Migration Utility ................................................................................ 60
6.9 Model Execution Venue Migration Utility ........................................................ 61
6.10 Data Redaction Grants to Sandbox Schema ..................................................... 61

7 PROCESS MODELING FRAMEWORK CONFIGURATIONS ....................................... 63
7.1 SMTP Server Configurations ............................................................................ 63
7.2 Work Manager Configurations ......................................................................... 64
7.2.1 Creating Work Manager in WebSphere Application Server ........................ 64
7.2.2 Mapping Work Manager to OFSAA WebSphere Instance ............................ 67
7.2.3 Creating Work Manager in WebLogic Application Server ........................... 71
7.3 Configuring Attributes for Attribute Expression and Advanced Attribute Expression Application Rule ............................................................... 73
7.3.1 Attribute Types ............................................................................................ 74
7.4 Enabling Proxy for REST Service Application Rule .......................................... 74

8 INLINE PROCESSING ENGINE CONFIGURATIONS ............................................... 75

9 DOCUMENT MANAGEMENT CONFIGURATIONS .................................................. 76
9.1 Content Management Integration ..................................................................... 76

10 FLEXIBLE KBD CONFIGURATIONS .................................................................. 77

11 QUESTIONNAIRE SETUP AND CONFIGURATION DETAILS .......................... 79
11.1 Launching Questionnaire Menu ...................................................................... 79
11.2 Mapping Roles to Access Questionnaire ....................................................... 79
11.3 Configuring Components, Dimensions, and Static Options ............................ 81
11.3.1 Configuring Components for Questionnaire ............................................. 81
11.3.2 Configuring Dimensions for Questionnaire ............................................. 81
11.3.3 Configuring Static Options for Questionnaire .......................................... 81
11.4 Registering and Invoking your Application's Customized Workflow ............... 81
## Table of Contents

### 12 Data Security and Data Privacy

12.1 Multi-Factor Authentication .................................................. 83  
12.1.1 Prerequisites ........................................................................ 83  
12.1.2 Configuring OTP through Email using OAM Adaptive Authentication Service .................................................. 83  
12.2 Transparent Data Encryption (TDE) ............................................. 93  
12.3 Data Redaction ........................................................................ 94  
12.3.1 Prerequisites ........................................................................ 94  
12.3.2 Input for Data Redaction ....................................................... 94  
12.3.3 Data Redaction utility ............................................................ 95  
12.3.4 Creating Batch for Executing Data Redaction Utility ............... 97  
12.3.5 Logs .................................................................................... 97  
12.3.6 Disabling Data Redaction ....................................................... 98  
12.4 Data File Encryption ................................................................. 98  
12.5 Key Management ...................................................................... 98  
12.5.1 Executing EncryptC Utility .................................................... 99  
12.6 HTTPS Protocol ...................................................................... 100  
12.7 Logging .................................................................................. 101  
12.7.1 Purging of Logs .................................................................. 101  
12.7.2 Log File Format ................................................................. 102

### 13 Generic Configurations

13.1 OFSAA Global Performance Optimization .................................. 103  
13.2 Query Performance Optimization ............................................ 104  
13.3 Multiple Language Support (MLS) Utility ................................ 105  
13.3.1 AAIpif.sh Utility ................................................................. 107  
13.4 Transferring Batch Ownership .................................................. 108  
13.5 Database Password Reset/ Change .......................................... 109  
13.6 Changing IP/ Hostname, Ports, Deployed paths, Protocol of the OFSAA Instance .................................................. 110  
13.6.1 Running Port Changer Utility .............................................. 110  
13.7 Using X-Frame-Options to Embed OFSAA Content on your Site .................................................. 111  
13.7.1 Knowing the Prerequisites .................................................... 111  
13.7.2 Enabling or Disabling X-Frame-Options in the web.xml File .................................................. 111  
13.8 Setting Access-Control-Allow-Origin Header ............................ 112  
13.9 Configuration for Tomcat .......................................................... 113  
13.10 Configuring WebLogic ............................................................. 114  
13.10.1 Configuring WebLogic for REST Services Authorization .......... 114
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.11</td>
<td>Configuring WebSphere</td>
<td>114</td>
</tr>
<tr>
<td>13.11.1</td>
<td>Configuring WebSphere for REST Services Authorization</td>
<td>114</td>
</tr>
<tr>
<td>13.12</td>
<td>SSO Authentication (SAML) Configuration</td>
<td>115</td>
</tr>
<tr>
<td>13.13</td>
<td>Public Key Authentication</td>
<td>117</td>
</tr>
<tr>
<td>13.13.1</td>
<td>Prerequisite</td>
<td>117</td>
</tr>
<tr>
<td>13.13.2</td>
<td>Setting Up Public Key Authentication on Client Server</td>
<td>117</td>
</tr>
<tr>
<td>13.13.3</td>
<td>Other SSH Software</td>
<td>118</td>
</tr>
<tr>
<td>13.13.4</td>
<td>Configurations Required in OFSAA Setup</td>
<td>119</td>
</tr>
<tr>
<td>13.14</td>
<td>Enable and Disable Users</td>
<td>120</td>
</tr>
<tr>
<td>13.14.1</td>
<td>Prerequisites</td>
<td>120</td>
</tr>
<tr>
<td>13.14.2</td>
<td>Enabling or Disabling Users with System Administrator and System Authorizer Roles</td>
<td>121</td>
</tr>
<tr>
<td>13.15</td>
<td>Password Reset</td>
<td>121</td>
</tr>
<tr>
<td>13.15.1</td>
<td>Prerequisites</td>
<td>121</td>
</tr>
<tr>
<td>13.15.2</td>
<td>Resetting a User Password</td>
<td>122</td>
</tr>
<tr>
<td>13.16</td>
<td>Configuring OFSAA OIM Connector</td>
<td>123</td>
</tr>
<tr>
<td>13.16.1</td>
<td>Knowing the Prerequisites</td>
<td>123</td>
</tr>
<tr>
<td>13.16.2</td>
<td>Configuring the Connector</td>
<td>123</td>
</tr>
<tr>
<td>13.16.3</td>
<td>Configuring Entitlements</td>
<td>129</td>
</tr>
<tr>
<td>13.17</td>
<td>Using REST APIs for User Management from Third-Party IDMs</td>
<td>135</td>
</tr>
<tr>
<td>13.17.1</td>
<td>Knowing the Prerequisites</td>
<td>135</td>
</tr>
<tr>
<td>13.17.2</td>
<td>Understanding REST API Specifications</td>
<td>136</td>
</tr>
<tr>
<td>13.18</td>
<td>Configuring the Logout URL for OBIEE in OFSAA</td>
<td>138</td>
</tr>
<tr>
<td>13.19</td>
<td>Enabling Deep Linking in OFSAA</td>
<td>139</td>
</tr>
<tr>
<td>13.20</td>
<td>Enabling Unlimited Cryptographic Policy for Java</td>
<td>141</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Conventions</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>

Abbreviations

The following table lists the abbreviations used in this document:

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>Advanced Interactive eXecutive</td>
</tr>
<tr>
<td>CDH</td>
<td>Cloudera Distribution Including Apache Hadoop</td>
</tr>
<tr>
<td>EPM</td>
<td>Enterprise Performance Management</td>
</tr>
<tr>
<td>F2H</td>
<td>HDFS File/Flat File to HDFS target</td>
</tr>
<tr>
<td>HDFS</td>
<td>Hadoop Distributed File System</td>
</tr>
<tr>
<td>H2T</td>
<td>HDFS-Hive source to RDBMS target mapping</td>
</tr>
<tr>
<td>H2H</td>
<td>HDFS-Hive source to HDFS target</td>
</tr>
<tr>
<td>H2F</td>
<td>HDFS-Hive source to Flat File target</td>
</tr>
<tr>
<td>JCE</td>
<td>Java Cryptography Extension</td>
</tr>
<tr>
<td>KBD</td>
<td>Key Business Dimensions</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>OEL</td>
<td>Oracle Enterprise Linux</td>
</tr>
<tr>
<td>OFSAAI</td>
<td>Oracle Financial Services Analytical Applications Infrastructure</td>
</tr>
<tr>
<td>OLH</td>
<td>Oracle Loader for Hadoop</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Relational Database Management System</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>RRF</td>
<td>Run Rule Framework</td>
</tr>
<tr>
<td>SCD</td>
<td>Slowly Changing Dimension</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>TDE</td>
<td>Transparent Data Encryption</td>
</tr>
<tr>
<td>T2H</td>
<td>RDBMS source to HDFS-Hive target</td>
</tr>
<tr>
<td>UDP</td>
<td>User Defined Properties</td>
</tr>
<tr>
<td>UMM</td>
<td>Unified Metadata Manager</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
</tbody>
</table>
1 Data Management Tools (DMT) Module Configurations

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

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

1.1 Data Mapping Configurations

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

- RDBMS source to HDFS-Hive target (T2H)
- HDFS Source to RDBMS Target (H2T)
- File source to HDFS-Hive target (F2H)
- HDFS/Local-WebLog Source to HDFS Target (L2H)

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

1.1.1.1 Default Implementation

Step 1: Configuring Properties

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

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

Step 2: Copy the required Jars

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

- htrace-core-3.0.4.jar
- commons-cli-1.2.jar
- hadoop-hdfs-2.6.0-cdh5.4.4.jar
NOTE: Version of Jars depends on the CDH Version and the Drivers used. From CDH 5.8.4 version onwards, htrace-core4-4.0.1-incubating.jar has to be copied.

1.1.2 Sqoop Implementation

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

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

1.1.2.1 Default Implementation

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

1.1.2.2 OLH (Oracle Loader for Hadoop) Implementation

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

1.1.2.3 Sqoop Implementation

1. From DMT Configurations window, set H2T Mode as Sqoop.
2. Sqoop should have been installed and configured in your system. For more information on how to use Sqoop for T2H, see Sqoop Configuration.

1.1.3 Data Movement from File to HDFS Target (F2H)

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

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

Step 1: Configuring Properties

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

For more information, see the DMT Configurations section in the OFS Analytical Applications Infrastructure User Guide.
2. From the Register Cluster tab in the DMT Configurations window, register a cluster with Target Information domain name as the Cluster Name for the following scenarios:
   - If Flat File is local and Is Hive Local is set as No.
   - If Flat File is Remote and Is Hive Local is set as Yes

Step 2: Copy the required Jars

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

- htrace-core-3.0.4.jar
- commons-cli-1.2.jar
- hadoop-hdfs-2.6.0-cdh5.4.4.jar

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

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

1.1.4.1 Prerequisites

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

1.1.4.2 Configurations

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

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

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

2. Copy the required Third Party Jars from the 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-2.6.0-cdh5.4.4.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-mrl-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.

3. Copy core-site.xml, hdfs-site.xml, mapred-site.xml, hive-site.xml, and yarn-site.xml from the Hadoop Cluster to the location mentioned in the **Configuration File Path** field in the Cluster Configurations window and <deployed location>/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.

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.

1.1.4.3 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.

<table>
<thead>
<tr>
<th>V_LOG_TYPE</th>
<th>V_LOG_COLUMNS</th>
<th>V_LOG_COL_DATATYPE</th>
<th>V_LOG_REGEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Sample</td>
<td>IP,Identity,User,Time,URL,Status,Size,Referer,Agent,Bytes</td>
<td>string,string,string,string,string,string,string,string,string,string,string,string,string,string,string</td>
<td>([^ ]<em>) ([^ ]</em>) ([^ ]<em>) ([^ ]</em>) ([0-9]<em>) ([0-9]</em>) ([^ ]<em>) ([^ ]</em>) ([^ ]<em>) ([0-9]</em>) ([0-9]<em>) ([^ ]</em>) ([0-9]<em>) ([0-9]</em>) ([0-9]*)</td>
</tr>
<tr>
<td>Microsoft-IIS Sample</td>
<td>IP,User,Date,Time,Service,ServerName,ServerIP,TimeTaken,ClientBytesSent,ServerBytesSent,ServiceStatus,WindowsStatus,RequestType,TargetOperation,Parameters</td>
<td>string,string,string,string,string,string,string,string,string,string,string,string,string,string,string,string</td>
<td>DELIMITED~,</td>
</tr>
</tbody>
</table>

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 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.

1.2.1 Prerequisite

- CDH 5.2.1 and above (with up to Apache Hive 1.2.1) 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 3.9.0 should have been installed on the OFSAAI VM.

1.2.2 Steps for Configuring OLH

Step 1: Installing OLH in the OFSAAI VM

1. Unzip the OLH Package downloaded from the Oracle site in the VM where OFSAAI is installed.
   Location: Inside the Home Directory of the user where OFSAAI is installed.

2. Set OLH_HOME environment variable in the .profile.
   OLH_HOME contains the directories such as bin, examples, jlib and lib.

Step 2: Configuring the Property

1. Set the following property in the jdbcOutput.xml file, which is present in the location $FIC_DB_HOME/conf/:
   <property>
     <name>oracle.hadoop.loader.connection.defaultExecuteBatch</name>
     <value>100</value>
   </property>

2. From the DMT Configurations window, set H2T Mode as OLH.

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

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

Step 3: Copy Configuration xmls from Hadoop Cluster

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

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

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

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

1. Copy commons-httpclient-3.1.jar from the CDH installation libraries into the $OLH_HOME/jlib folder.

2. If OFSAA is using Apache driver, perform the following:
   - 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:
     a) 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)
     b) Copy the entire property to FIC_DB_HOME/conf/dtextInput.xml

3. If OFSAA 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.

### 1.2.3 Limitations

- OLH can read data from a Single Source Table (ANSI joins are not supported) and load it into a single target RDBMS table.
- OLH 2.3.1 is built against HIVE 0.10. It works well with HIVE 0.12 too; however, Data Type DATE (that is supported in HIVE 12) is not supported by OLH.
- 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.

1.3 **Sqoop Configuration**

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

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.

1.3.1 **Prerequisites**

• CDH4.7 or CDH 5.2.1 should have been installed.
• 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.

1.3.2 **Steps for Configuring Sqoop**

1.3.2.1 **Sqoop 1 Cluster Mode**

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

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

1.3.2.2 **Sqoop 1 Client Mode**

Step 1: Configuring the Properties
1. From the *DMT Configurations* window, set **Sqoop Mode** as **Client**.

2. Specify the path of the HDFS working directory for Sqoop related operations in the **Sqoop Working Directory** field.

3. From the *Register Cluster* tab in the *DMT Configurations* window, register a cluster with Target Information domain name as the **Cluster Name** in case of T2H or register a cluster with Source Information domain name as the **Cluster Name** in case of H2T.

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

**Step 2: Copy Third Party Jars**

Copy the following Third Party Jars from the 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-mrl-cdh4.7.0.jar
- libfb303-0.9.0.jar
- librthrift-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 the Configuration File Path given in the Cluster Configurations window of the registered cluster. 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.

**1.3.2.3 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.
1.4 SCD Execution on Hive Information Domain

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

1.4.1 Constraints

1. Default Columns with Surrogate Key (SK) as 0 and -1 will be inserted into destination (DIM) table, only if data is present in the table DIM_SCD_SEEDED.

2. PRTY_LOOKUP_REQD_FLG should always be set to 'N'.

3. The data type of SK column in destination (DIM) table should always be INT/BIGINT and it will be generated using the following logic:

   \[ \text{MAX_SKEY} + \text{row_number(n)} \text{ where (n) is rowid.} \]

4. Query to fetch Maximum SKEY value will give performance improvement, if indexing is done on DIM table.

5. Stage Column where Column Type = ‘ED’ should be updated with Date in Hive Format – ‘yyyy-mm-dd’.

   Apart from this only ‘dd-Mon-yyyy’ format is supported to keep the current seeding intact. Final data in Date column will always be inserted in ‘yyyy-mm-dd’ format.

6. Columns which are not part of STG and DIM mapping will be passed as ” (empty strings).

7. Columns with column type STRING/VARCHAR/CHAR will be inserted as empty strings and all other column types will be inserted as NULL.

8. Stage table should not contain duplicate records for the same MISDATE.

9. Two or more SCDs executing in parallel should not update the same Dimension table. In such cases, ensure the processing is sequential. Similar limitation is applicable for the option Map Ref No: =-1.

1.4.2 Assumptions:

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

2. Since Hive does not have PK functionality, you should map an ID Column as PK, on the basis of which STG and DIM tables will be matched for TYPE1 and TYPE2.

3. SK column in destination (DIM) table will always be of data type INT/BIGINT.

4. DIM_SCD_SEEDED table will be created automatically. You need to insert data manually as mentioned in the following table:
1.5 Heterogeneous Support for SCD to RDBMS

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

1.5.1 Assumptions

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

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

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

For example:

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

Relevant entry should be present in `AAI_DB_DETAIL` table corresponding to `<TARGET RDBMS SERVER>` and `<TARGET RDBMS NAME>`. 
2 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:

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

   ```sql
   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:

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

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

  ```sql
  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:**
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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Code</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td># Member Deletion</td>
<td>MEMBER_DEL-$INFODOM$-</td>
<td>MEMBER_DEL-ORAFUSION-1=Y</td>
</tr>
<tr>
<td>Configuration - VALUE- Y/N</td>
<td>$$DIMENSION_ID$=$VALUE$</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Code</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td># Attribute Default Date Format - DB_DATE_FORMAT:DD-MON-YYYY</td>
<td>ATTR_DEF_DATE_FORMAT-$INFODOM$=$$DB_DATE_FORMAT$</td>
<td>ATTR_DEF_DATE_FORMAT-ORAFUSION=DD/MON/YYYY</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Code</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td># Members Reverse population - VALUE- Y/N</td>
<td>MEMBER_REVERSE_POP-$INFODOM$-$DIMENSION_ID$=$VALUE$</td>
<td>MEMBER_REVERSE_POP-ORAFUSION-1=Y</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Code</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Hierarchy Reverse population - VALUE- Y/N</td>
<td>HIERARCHY_REVERSE_POP-$INFODOM$-$DIMENSION_ID$=$VALUE$</td>
<td>HIERARCHY_REVERSE_POP-ORAFUSION-1=Y</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Code</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Hierarchy Maximum level allowed for the hierarchy in particular Information Domain - VALUE - Integer number</td>
<td>MAX_DEPTH-$INFODOM$=$VALUE$</td>
<td>MAXDEPTH-FUSION=15</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Code</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Tree node limit for the hierarchy - Values is Integer number</td>
<td>TREE_NODE_LIMIT=$VALUE$</td>
<td>TREE_NODE_LIMIT=30</td>
</tr>
</tbody>
</table>
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

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:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_OBJ_CODE</td>
<td>Rule/Process/Run Code</td>
<td>Rule(PR2_RULE_B.V_RULE_NAME)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process(PR2_PROCESS_B.V_PROCESS_NAME)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run (PR2_RUN_B.V_RUN_NAME)</td>
</tr>
<tr>
<td>V_INFODOM_CODE</td>
<td>Infodom Code</td>
<td>Infodom</td>
</tr>
<tr>
<td>V_OBJ_TYPE</td>
<td>Rule/Process/Run Type</td>
<td>Rule(RL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process(PT)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run (RN)</td>
</tr>
<tr>
<td>V_EXECUTION_MODE</td>
<td>Type of query used while executing.</td>
<td>MERGE- Merge statement will be used SELECT- Select Insert will be used PARTITION- Partition swap will be used</td>
</tr>
<tr>
<td>F_USE_PARTITION</td>
<td>If partition is used as a filter</td>
<td>Y/N</td>
</tr>
<tr>
<td>F_USE_ROWID</td>
<td>If ROWID is used other than primary key in MERGE. This is used only for MERGE query execution.</td>
<td>Y/N</td>
</tr>
<tr>
<td>V_MERGE_HINT</td>
<td>Used for MERGE or INSERT hint.</td>
<td></td>
</tr>
<tr>
<td>V_SELECT_HINT</td>
<td>Used for SELECT hint</td>
<td></td>
</tr>
<tr>
<td>V_PRE_SCRIPT</td>
<td>Used for alter statements executed before rule execution</td>
<td></td>
</tr>
<tr>
<td>V_POST_SCRIPT</td>
<td>Used for alter statements executed after rule execution.</td>
<td></td>
</tr>
</tbody>
</table>
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 Rule2). 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 OFSAAI Object Registration, then the partition columns will be added as a filter to all the type of rule queries (MERGE/SELECT/PARTITION); 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 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 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.

### 3.2.1.2 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.

### 3.2.1.3 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, levellmg properties for that sub-level and the Vector<TaskDefinition> contains all the data needed for using the component in a process or run.

3.2.1.4 getCompDescMap

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

The Input Parameters are:

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

Return is:

- Map<String, String>

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

### 3.2.1.5 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. All the parameter in this map has to be put in correct order. This LinkedHashMap will be returned back to the calling method.

3.2.1.6 **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.

3.2.2 **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 folder.
3. Rebuild and redeploy the application.
3.2.3 **Entry to PR2_COMPONENT_MASTER Table**

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

An entry contains the following fields.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Description</th>
<th>Null</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_PR2_COMPONENT_ID</td>
<td>VARCHAR2(30)</td>
<td>Represents component type in a Process or Run.</td>
<td>N</td>
</tr>
<tr>
<td>V_PR2_COMPONENT_PARENT_ID</td>
<td>VARCHAR2(30)</td>
<td>Indicates parentage which refers to V_PR2_COMPONENT_ID.</td>
<td>Y</td>
</tr>
<tr>
<td>V_COMPONENT_ID</td>
<td>VARCHAR2(30)</td>
<td>Existing ICC Component Id.</td>
<td>Y</td>
</tr>
<tr>
<td>V_PR2_COMPONENT_CLASS</td>
<td>VARCHAR2(100)</td>
<td>Fully qualified class path of the implementation class for this component.</td>
<td>N</td>
</tr>
<tr>
<td>V_TREE_IMAGE</td>
<td>VARCHAR2(100)</td>
<td>Name with relative path (with respect to web context) of the image which will be displayed in the component tree.</td>
<td>N</td>
</tr>
<tr>
<td>N_TREE_ORDER</td>
<td>NUMBER(9)</td>
<td>Display order of the component in the tree. The order is done upon the peers.</td>
<td>N</td>
</tr>
<tr>
<td>V_SEEDED_BY</td>
<td>VARCHAR2(8)</td>
<td>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.</td>
<td>Y</td>
</tr>
<tr>
<td>V_CREATED_BY</td>
<td>VARCHAR2(30)</td>
<td>Stores the creator username.</td>
<td>N</td>
</tr>
<tr>
<td>D_CREATED_DATE</td>
<td>TIMESTAMP(6)</td>
<td>Stores created date and time.</td>
<td>N</td>
</tr>
</tbody>
</table>
### Column Name

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Type</th>
<th>Description</th>
<th>Null</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_LAST_MODIFIED_BY</td>
<td>VARCHAR2(30)</td>
<td>Stores the modifier username.</td>
<td>Y</td>
</tr>
<tr>
<td>D_LAST_MODIFIED_DATE</td>
<td>TIMESTAMP(6)</td>
<td>Stores modified date and time.</td>
<td>Y</td>
</tr>
</tbody>
</table>

Example:

```sql
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')
```

### 3.2.4 Sample Code

The [COMPONETSAMPLE.txt](#) file contains the sample code of a created component.

### 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:

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

With

```xml
<RULESET ID="110" TYPE="FIRERUN">
```
4 Operations

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

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.

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 OFSAA 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:

```sql
INSERT INTO ficsysmaster
WEBIPADDRESS,APPIPADDRESS,ETLAPPHOME,NOOFCPUS,VMEMORY,PMEMORY,
CACHE,NOOFTHREADS,IOTRANSFER,MAXTRANSERSEC,DISKSDBSTRIPING,DISKSFILESTRIPPING,MAXFILESIZE,MAXFTPFILESIZE,MAXFILENAMELEN,OSDATABLOCKSIZE,DATASETTYPE,STAGEPATH,DBFTPSHARE,WEBFTPSHARE,WEBFTPUSERID,WEBFTPPASSWD
SELECT WEBIPADDRESS,APPIPADDRESS,'<NEWAMIPADDRESS>',ETLAPPHOME,NOOFCPUS,VMEMORY,PMEMORY,CACHE,NOOFTHREADS,IOTRANSFER,MAXTRANSERSEC,DISKSDBSTRIPING,DISKSFILESTRIPPING,MAXFILESIZE,MAXFTPFILESIZE,MAXFILENAMELEN,OSDATABLOCKSIZE,DATASETTYPE,STAGEPATH,DBFTPSHARE,WEBFTPSHARE,WEBFTPUSERID,WEBFTPPASSWD
```

Oracle Financial Services Software Confidential - Restricted
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:
   c) 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/ofssausr`, you can setup the secondary OFSAA instance as well under `/scratch/ofssausr` 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.

d) 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


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.

**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.
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 'DIMENSION' 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.
This tables hold locale specific information about various object sub types present in OFSAAI and information on the subtypes of ‘DIMENSION’ 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:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Primary Key</th>
<th>Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>N_CUST_INCOME_BAND_CODE</td>
<td>PK</td>
<td>Number(5,0)</td>
</tr>
<tr>
<td>FIC_MIS_DATE</td>
<td></td>
<td>Date</td>
</tr>
<tr>
<td>V_CUST_INCOME_SHORT_DESC</td>
<td></td>
<td>Varchar2(80)</td>
</tr>
<tr>
<td>V_INCOME_DESC</td>
<td></td>
<td>Varchar2(80)</td>
</tr>
<tr>
<td>N_D_INCOME_UPPER_VALUE</td>
<td></td>
<td>Number(22,3)</td>
</tr>
<tr>
<td>N_D_INCOME_LOWER_VALUE</td>
<td></td>
<td>Number(22,3)</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Primary Key</th>
<th>Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>N_INCOME_BAND_CODE</td>
<td>PK</td>
<td>Number(5,0)</td>
</tr>
<tr>
<td>LOCALE_CD</td>
<td></td>
<td>Varchar2(10)</td>
</tr>
<tr>
<td>V_CUST_INCOME_SHORT_DESC</td>
<td></td>
<td>Varchar2(80)</td>
</tr>
</tbody>
</table>

The following figure represents the Income Hierarchy definition:
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 DIMENSION. Information about the table such as the MLS table meant for the Dimension, the hierarchy table, the attribute table, and so on will be maintained in this table.

- **AAI_DIM_META_COLUMN**

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

- **AAI_DIM_META_JOIN**

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

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

<table>
<thead>
<tr>
<th>N_CUST_BAND_CODE</th>
<th>V_INCOME_DESC</th>
<th>LOCALE_CD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AAA</td>
<td>en_US</td>
</tr>
<tr>
<td>2</td>
<td>BBB</td>
<td>en_US</td>
</tr>
<tr>
<td>1</td>
<td>CCC</td>
<td>zh_CN</td>
</tr>
<tr>
<td>2</td>
<td>DDD</td>
<td>zh_CN</td>
</tr>
</tbody>
</table>

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 window to Define Data Element Filters on any tables and columns. Based on the Classification, the appropriate Classification type option has to be selected in the Data Element Selection window to list the tables.
Note the following:

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

  By Default, the classification codes 20, 200, 210, 310, 370, 50, 300, and 500 will have the `CLASSIFICATION_FLG` set to “1”.

- The `REV_TABLE_CLASSIFICATION_TL` table will have an entry `TABLE_CLASSIFICATION_CD = "1000"`, `TABLE_DESCRIPTION = "UnClassified"` to identify UnClassified Tables (that is, tables which are not classified in the ERwin through UDP).

- The category “All” option will select all the tables available in the infodom, irrespective of whether table is classified or not.

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

### 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.
5.3 Configuring Essbase Connectivity Check

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

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

5.3.1 Settings in .profile

Perform the following settings in the .profile file:

1. Open .profile file from $HOME directory of primary OFSAA server.
2. Set ARBORPATH to EPMSYSTEM11R1/common/EssbaseRTC-64/11.1.2.0 path.
3. Set ESSBASEPATH to EPMSYSTEM11R1/common/EssbaseRTC-64/11.1.2.0 path.
4. Set export ESSLANG=English_UnitedStates.Latin1@Binary.
5. Save and close the file.

5.3.2 Checking the Connection

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

1. Login to the OFSAA Server.
2. Navigate to $HYPERION_HOME/products/Essbase/EssbaseServer/bin directory.
3. Execute command ./ESSCMD.
4. Enter ::::[0]-> login.
5. Enter the following details for the Login:
   a. Host Node >ESSBASE_SERVER_HOST_NAME>
   b. User >ADMINISTRATOR_USER_NAME>
   c. Password >PASSWORD>
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
- Variable Migration Utility
- Model Execution Venue 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

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 OFSAAI 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. Install the following packages along with R (R version 3.0.1):
   - rJava - version 0.9-8
The packages are available to download from https://cran.r-project.org/.

2. To execute R scripted models, ensure that the Rserve related jar files such as REngine.jar and RserveEngine.jar are copied into the $FIC_DB_HOME/lib folder.

3. Install the OFSAAIRunnerOpenR R Package in the remote box where Rserve is running. For more information, see Installing OFSAAIRunnerOpenR R Package.

### 6.2.1.1 Installing OFSAAIRunnerOpenR R Package

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

Perform the following instructions to install OFSAAIRunnerOpenR R Package:

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

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

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

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

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

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

   ```
   ls -l
   ```
### 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](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 `ojdbc<version>.jar` file to the lib directory in the remote file path configured. The version of `ojdbc<version>.jar` file is based on the Java version.
     
     **Limitation:** For OFSAA release 8.0.6.0.0, copy the `ojdbc6.jar` file to the lib directory.

   - 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 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

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

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

- CDH (Version: OFSAA qualified CDH version)

For more information on installation and configuration of ORAAH, see ORAAH Installation Guide.

- Cairo - The package is available to download from https://cran.r-project.org/. Download and transfer it to Rserve box. Install the package using the following command:

  R CMD INSTALL Cairo_Package_Name
  Or
  install.packages("Cairo", dependencies = T) #using R session

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

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

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

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 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.

6.8 **Variable Migration Utility**

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

The following are the steps to run the migration utility:

1. Navigate to `$FIC_HOME/utility/variable/bin` directory.
2. Execute `variableresaveutil.sh` (UNIX).
   ```bash
   ./variableresaveutil.sh
   ```
   This command will migrate all available variables from all Infodoms, which are in the `ftpshare/<infodom>/erwin/variable/` directory.
3. Provide the following parameter if you want to migrate variables that are present in a particular information domain:
6.9 Model Execution Venue Migration Utility

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

Following are the steps to run the utility:

1. Navigate to $FIC_HOME/utility/modelutil/bin directory.
2. Execute ExecutionConfig.sh (UNIX).
   ```shell
   ./ExecutionConfig.sh
   ```
   This command migrates all available ModelingFramework.xml target entries to table.
3. Check the status, and errors if any, in the MF_xml_migration.log file available in the $FIC_HOME/utility/modelutil/log folder.

6.10 Data Redaction Grants to Sandbox Schema

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

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

1. Login with System Database Administrator (SYSDBA) rights to the database where the Sandbox schema is created.
2. Give the following Grants:
   ```sql
   grant execute on DBMS_REDACT to &atomicUser
   ```
/
Create role OFS_SEC_DATA
/
grant OFS_SEC_DATA to &atomicUser
/
create role OFS_NOSEC_DATA
/
grant EXEMPT REDACTION POLICY to OFS_NOSEC_DATA
/
grant OFS_NOSEC_DATA to &atomicUser
/
alter user &atomicUser default role none
/
7 Process Modeling Framework Configurations

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.

<table>
<thead>
<tr>
<th>V_USER_ID</th>
<th>N_EMAIL_NOTIF_REQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER1</td>
<td>1</td>
</tr>
<tr>
<td>USER2</td>
<td>2</td>
</tr>
</tbody>
</table>

- 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.

<table>
<thead>
<tr>
<th>V_USR_ID</th>
<th>V_EMAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER1</td>
<td><a href="mailto:user1@oracle.com">user1@oracle.com</a></td>
</tr>
<tr>
<td>USER2</td>
<td><a href="mailto:user2@oracle.com">user2@oracle.com</a></td>
</tr>
</tbody>
</table>

4. Add the following entries in the AAI_WF_EMAIL_TEMPLATE table:
   - V_MAIL_FROM: Email id from which the mail is sent
   - V_MAIL_MESSAGE: Email message template
   - V_MAIL_SUBJECT: Subject of the mail
   - V_APP_PACKAGE_ID: Application package ID
   - V_MAIL_TYPE: Email type such as task or bulk task.
   - N_TEMPLATE_ID: A unique Email Template ID
   - V_TEMPLATE_NAME: Email Template name

5. Set the V_EMAIL_REQUIRED value to Y in AAI_WF_APP_PACKAGE_B (for app level setting), AAI_WF_APP_REGISTRATION (for entity type level setting) and AAI_WF_ACTIVITY_TASK_B (for task level setting) tables.

7.2 Work Manager Configurations

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

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

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

4. Select the required Scope from the drop-down list.
For example, Node=whf00aqnNode01, Server=server1.

5. Click New in the Preferences section.

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.
9. Click Save.

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.
2. Click OFSAI instance hyperlink.

3. Click **Resource references** link under **References** section.
4. Click **Browse** corresponding to the Work Manager Resource Reference. The available resources are displayed.

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

7. Click **Save**.
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.

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.

4. Click New to create a new work manager component.
5. Select **Work Manager** and click **Next**.

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

7. Click **Next**.

8. Select the required deployment target and click **Finish**.
7.3 Configuring Attributes for Attribute Expression and Advanced 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:

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

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

<table>
<thead>
<tr>
<th>Attribute Type ID</th>
<th>Attribute Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Static</td>
</tr>
<tr>
<td>1002</td>
<td>Query</td>
</tr>
<tr>
<td>1003</td>
<td>JavaAPI</td>
</tr>
</tbody>
</table>

- **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 REST Service Application Rule

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

Add the following entries in the `AAI_WF_GLOBAL_SETTINGS` table:

<table>
<thead>
<tr>
<th>V_PARAM_NAME</th>
<th>V_PARAM_VALUE</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROXY_SERVER_IP</td>
<td>For example, <a href="http://www.proxy.myserver.com">www.proxy.myserver.com</a></td>
<td>Provide the IP address of the Proxy server.</td>
</tr>
<tr>
<td>PROXY_SERVER_PORT</td>
<td>For example, 80</td>
<td>Provide the port number of the Proxy server.</td>
</tr>
</tbody>
</table>
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 Document Management Configurations

9.1 Content Management Integration

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

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 “OFSAINFO”, rename the file to OFSAINFO_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.
10 Flexible KBD Configurations

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:

<table>
<thead>
<tr>
<th>Sequence name</th>
<th>Table name</th>
<th>Column name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLEXKBD_CTRL_LOC_SEQ</td>
<td>flexkbd_ctrl_loc</td>
<td>CONTROL_ID</td>
</tr>
<tr>
<td>FLEXKBD_DIM_INFO_SEQ</td>
<td>flexkbd_dim_info</td>
<td>KBDID</td>
</tr>
<tr>
<td>FLEXKBD_PREF_MASTER_SEQ</td>
<td>flexkbd_pref_master</td>
<td>PREF_ID</td>
</tr>
</tbody>
</table>
11 Questionnaire Setup and Configuration Details

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

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

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

11.1 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.

11.2 Mapping Roles to Access Questionnaire

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

1. Login to OFSAA with your system administrator credentials.
2. Click from the header to display the administration tools in a Tiles menu.
3. Click Identity Management to view the Security Management menu in a separate window.
4. Click User Administrator to expand the list further.
5. Click **User Group Role Map** to display the **User Group Role Map** window.

6. Map users to User or Approver roles.
   
   c) Users of applications mapped to groups can access the Questionnaire menu by mapping the groups to following roles:

<table>
<thead>
<tr>
<th>Number</th>
<th>Role Codes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>QTNRADMNRL</td>
<td>ABC Questionnaire Administrator</td>
</tr>
<tr>
<td>2</td>
<td>QUESTMATRL</td>
<td>ABC Questionnaire Maintenance</td>
</tr>
<tr>
<td>3</td>
<td>QTNRCONFRL</td>
<td>Questionnaire Configuration Execute</td>
</tr>
</tbody>
</table>

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

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

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

**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.
11.3 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.

11.3.1 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.

11.3.2 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.

11.3.3 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.

11.4 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 SAPP_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_TYPE 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.
12 Data Security and Data Privacy

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

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

12.1 Multi-Factor Authentication

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

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

12.1.1 Prerequisites

The following list mentions the prerequisites required for this configuration:

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

12.1.2 Configuring OTP through Email using OAM Adaptive Authentication Service

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

12.1.2.1 Enabling Adaptive Authentication Service

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

NOTE: The Adaptive Authentication Service has to be licensed separately to use the two-factor authentication feature.
To enable the Adaptive Authentication Service, perform the following steps:

1. Login in to OAM Admin Console and click Configuration tab.
3. Click Enable Service against Adaptive Authentication Service.

12.1.2.2 Configuring Adaptive Authentication Plugin

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

1. Login to OAM Admin Console and click Application Security tab.
2. Click **Authentication Plug-ins** under **Plug-ins** tile. The **Plug-ins** window is displayed.

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

5. Configure OTP through Email by updating the following *Configuration Parameters*:
   
a) **SFATypes** - Types of Second Factor Authentication methods. To send OTP through Email, add Email to the list. Add Email if you are not using other SFA types.
b) **Email Enabled** - Set this attribute to **true** to send OTP through Email.
c) **IdentityStoreRef** - Enter the user Identity store where your user details are stored and user is authenticated in First-level authentication.

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

d) **UMSAvailable** - Set the value to **true**
e) **UmsClientUrl** - Enter the value for **UmsClientUrl**. Adaptive Authentication Service uses Oracle SOA User Messaging Services to send the Email notification.
f) **EmailField** – Enter the value for Email Address attribute in the User Identity Store. The Adaptive Authentication plugin fetches the value for this field to send the email notification.
g) **PinLength** – Specify the length of the OTP pin sent through Email.
h) **PinChars** – Specify the characters to generate the OTP. If you want only digits in the OTP, enter only "0123456789".
i) **EmailMsgSubject** – Email Subject for the OTP notification.
j) **EmailMsgFrom** – From email address in the email notification.
k) **EmailMsgFromName** – From name in the email notification
6. Click **Save**.

**12.1.2.3 Configuring AdaptiveAuthenticationModule**

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

1. Navigate to **Application Security > Plug-ins > Authentication Modules**.
2. Search for **AdaptiveAuthenticationModule**.
3. Click **AdaptiveAuthenticationModule**.
4. Click **Steps** tab and validate the configuration details entered. Update any Email related parameter if it is missing.
5. Validate **IdentityStoreRef, UmsAvailable, UmsClientUrl, EmailField, Email Enabled** and so on. Update the values if required.

**12.1.2.4 Configuring Credentials for UMS**

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

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

1. Login to OAM EM console.
2. Expand **Weblogic Domain** and then right click on `<Domain_Name>` and navigate to **Security > Credentials**.
3. From the Credentials window, click OAM_CONFIG and then click Create Key. The Edit Key window is displayed.

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

5. Click OK to save.

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

1. Navigate to <MiddleWare_HOME>/common/bin.

2. Execute the following command:
   ./wlst.sh

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

12.1.2.5 Protecting the Resource with AdaptiveAuthenticationScheme

The adaptiveAuthentication Scheme is used for two-factor authentication.

To configure, perform the following steps:

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

2. From the Application Security tab and click Access Manager > Authentication Schemes.

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

5. Verify the details and click **Apply**.
12.1.2.6 Enabling Two-Factor Authentication to a Protected Resource

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

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

2. Click Access Manager > Application Domains.

3. From the Resources tab, search for your SSO added Resource Type.

4. Select Authentication Policies tab and then click Protected Resource Policy.
5. Click **Advanced Rules** tab.

6. From the *Post-Authentication* tab in the created Authentication Policy, click **Add**.

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

**12.1.2.7 Accessing the UI**

To access the UI, perform the following steps:

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

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

   For example:

   \[http://<SERVER_HOME>:7777/<CONTEXT>/login.jsp\]

2. Login with User Name and Password. After successful OIM login, the application prompts for Second Factor Authentication through OTP.
3. Select the method to receive the OTP from the options: SMS or Email.

4. Enter the OTP which you received through SMS or Email.

5. Click Login. The OFSAI Landing Screen is displayed.

12.2 Transparent Data Encryption (TDE)

OFSAI is enhanced to support Transparent Data Encryption (TDE) feature of Oracle Advanced Security option. Transparent Data Encryption (TDE) enables you to encrypt sensitive data, such as Personally Identifiable Information (PII), that you store in tables and tablespaces. After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data. To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a Keystore.

In case you did not enable TDE or Data Redaction during OFSAI 8.0.6.0.0 installation and want to enable at a later point of time, see Enabling Transparent Data Encryption (TDE) and Data Redaction section in OFSAI Application Pack Installation and Configuration Guide 8.0.6.0.0.
12.3 Data Redaction

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

12.3.1 Prerequisites

1. Ensure the required Oracle Database Server versions are installed:
   - Oracle Database Server Enterprise Edition 11g Release 2 (11.2.0.4.0 +) - 64 bit RAC/Non-RAC with/without partitioning option, Advanced Security Option
   - Oracle Database Server Enterprise Edition 12c Release 1 (12.1.0.1.0 +) - 64 bit RAC/Non-RAC with/without partitioning option, Advanced Security Option

2. Ensure the required patches are applied for your respective Oracle DB versions:
   - For Oracle DB Serve 11.2.0.4, the patch 22205607 should have been applied.
   - For Oracle DB Server 12.1.0.1 and 12.1.0.2, the patches 27010930 and 22205607 should have been applied.

3. You should have done all configurations mentioned in "Enabling Data Redaction" section in OFS AAAI Application Pack Installation and Configuration Guide 8.0.6.0.0. In case of applications installed using Full Installers, see the respective sections for enabling Data Redaction in your application Installation Guides.

4. User should have DATASECURITYADMIN User Role mapped to his user group.

5. From the Configuration window in the System Configuration module, select the Allow Data Redaction checkbox. For more information, see Configuration section in the OFS Analytical Applications Infrastructure User Guide.

12.3.2 Input for Data Redaction

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

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAI_DRF_FUNCTION_MASTER</td>
<td>This table holds the Redaction function definitions. Generic Functions can be email, card number, phone number etc.</td>
</tr>
<tr>
<td>AAI_DRF_FUNCTION_COLUMN_MAP</td>
<td>This table holds the Redaction Function-Column mappings. The columns will be redacted according to the Function mapping.</td>
</tr>
</tbody>
</table>
AAI_DRF_TABLE_ACCESS_CD_MAP | This table holds the mapping of tables having columns marked for redaction to the Access codes. These access codes are SMS function codes and are expected to be mapped to the role DATASECURITY. The policy expression would be created based on this role and would be evaluated in order to access unredacted data.

12.3.3 Data Redaction utility

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

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

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

- User ID- OFSAA user who is the batch owner

Note the following:

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

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

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

```
Alter user <<atomic schema user>> default role RQADMIN
```
12.3.3.1 Executing Data Redaction Utility with False Flag

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

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

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

12.3.3.2 Executing Data Redaction utility with TRUE flag

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

1. From the Configuration window of System Configuration module, enter the absolute path where the encryption key is stored in the Encryption Key Path field. If this is not provided, default key will be used which is available in $fic_home/conf folder.
2. From the Batch Maintenance window, search for Batch ID as "##INFODOM##_DATA_REDACTION".
3. Select the Batch.
4. Select the task from the Task Details pane and click Edit.
5. In the Executable field in the Dynamic Parameters List, specify as
   dataredaction.sh,true,<<ofsaa user id>>.
6. Click Save.
7. From the Batch Execution window, search for Batch ID as <>>.
8. Select the Batch and click Execute Batch.
9. Navigate to FTPshare/DataRedaction folder. You can find 2 folders called Scripts and Postscripts inside DataRedaction folder.
10. Decrypt “create scripts” in the FTPshare/DataRedaction/scripts folder using
    dmtfileencryption.sh with the following arguments:
    
    
    
    ./dmtfileencryption.sh decrypt_file <INPUTFILE> <OUTPUTFILE> <KEYFILE>
    
    • <INPUTFILE>- Provide the absolute path of the input file. Since all “create scripts” in the scripts folder need to be decrypted, you can provide the folder path, that is, FTPshare/DataRedaction/scripts.
    • <OUTPUTFILE>- Provide the absolute path of the input file.
• `<KEYFILE>`- Provide the absolute path of key file with key file name. This should be same as that is provided in the Configuration window. If nothing was provided in the Configuration window, specify the default key path as `$fic_home/conf/ofssaa8xkey.ext`.

For more details, see Command Line Utility for DMT File Encryption section in OFS Analytical Applications Infrastructure User Guide.

11. Execute the decrypted "create scripts" in the Atomic Schema.

12. Execute scripts in the FTPshare/DataRedaction/postscripts folder for populating required OFSAA metadata.

The identified table data will be redacted.

### 12.3.4 Creating Batch for Executing Data Redaction Utility

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

Following are the steps required to create a Batch

1. From the Batch Maintenance window, click Add button in the Batch Name tool bar. The Add Batch Definition window is displayed.

2. Enter Batch Name and Batch Description.

3. Click Save. The newly added Batch will be listed in the Batch Maintenance window.

4. Select the Batch and click Add from the Task Details tool bar. The Add Task Definition window is displayed.

5. Enter Task Description and select Component as RUN EXECUTABLE from the drop-down list.

6. In the Executable field in the Dynamic Parameters List, specify as dataredaction.sh,false/true,<<ofsaa user id>>.

7. See Adding Task Details section in the Operations Chapter in the OFS Analytical Applications Infrastructure User Guide for details on other fields.

### 12.3.5 Logs

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

For disabling data redaction, perform the following steps:

1. From the Configuration window in the System Configuration module, de-select the Allow Data Redaction checkbox.

2. Run the Data Redaction utility. For details on running the Data Redaction utility, see Data Redaction utility section.

12.4 Data File Encryption

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

To configure File encryption:

1. From the DMT Configurations window under File Encryption grid, enter the following details:

   a) Select Yes from the Encryption at Rest drop-down list.
   b) Enter the Key File Name and Key File Path of the key that is used to encrypt or decrypt the Data File. You can use File Encryption utility to generate key in AES 256 bit format. For details, see Command Line Utility for File Encryption section in OFS Analytical Applications Infrastructure User Guide 8.0.6.0.0.

2. For F2T or F2H, encrypt your Data File using File Encryption utility and place the Key used for encryption in the Key File Path given in the DMT Configurations window. Then place the encrypted Data File in /ftpshare/<INFODOM>/dmt/source/<SOURCE_NAME>/data/<MIS_DATE>/.

3. For T2F or H2F, the output Data file will be encrypted. Use the File Encryption utility to decrypt the data file.

For details on how to execute File Encryption Utility, see Command Line Utility for File Encryption section in OFS Analytical Applications Infrastructure User Guide 8.0.6.0.0.

12.5 Key Management

The OFSAA Configuration Schema (CONFIG) is the repository to store passwords for users and application database schemas centrally. These values are AES 128 bit encrypted using an encryption key uniquely generated for each OFSAA instance during the installation process.

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

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

This section details about the EncryptC Utility, which is used to:
- Generate keystore from AESCryptkey.ext key.
- Retrieve AESCryptkey.ext if it is deleted using the keystore.
- Generate new AESCryptKey.ext and update the keystore.

### 12.5.1 Executing EncryptC Utility

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

#### 12.5.1.1 Knowing the Prerequisites

- Ensure that the Keystore.properties file is present in the $FIC_HOME/conf directory.
- Enter the keystore path where you want to generate AESkeystore.ks.
  
  For example,
  
  keystorepath=/scratch/ofsaaweb/OFSAAI_806

- Ensure that EncryptC utility is present in the $FIC_HOME/utility/EncryptC directory.

#### 12.5.1.2 Generating Keystore

Generate keystore using the following procedure:

1. Navigate to the $FIC_HOME/utility/EncryptC/bin directory.
2. Execute the command:
   
   ```
   ./EncryptC.sh -genkeystore
   ```
3. Expected output and actions required are listed:
   
   a) A prompt appears to enter the keystore path if the path is not mentioned in keystore.properties.
   
   b) A prompt appears to enter keystore password and keypassword. If the keypassword is not given, then the system picks the keystorepassword as the keypassword.

   c) Keystore path is read from KeyStore.properties file and name of keystore is AESKeyStore.ks. So this generates keystore at specified location.

#### 12.5.1.3 Retrieving AESCryptKey.ext

Retrieve AESCryptKey.ext using the following procedure:

1. Navigate to the $FIC_HOME/utility/EncryptC/bin directory.
2. Execute the command:
   
   ```
   ./EncryptC.sh -retrieve
   ```
3. Expected output and actions required are listed:
   a) A prompt appears to confirm whether you want to retrieve the AESCryptKey.ext file or not.
   b) If you select Yes, then a prompt appears to enter keystore password and key password.
   c) After you enter the passwords, AESCryptKey.ext is retrieved to all locations where it was originally present.

12.5.1.4 Generating new AESCryptKey.ext and updating the keystore

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

1. Navigate to $FIC_HOME/utility/EncryptC/bin directory.
2. Execute the command:
   
   ```sh
   ./EncryptC.sh -genkey
   ```
3. Expected output and actions required are listed:
   a) The system checks whether keystore exists or not. If it does not, then it prompts for generating keystore using the -genkeystore option.
   b) The system rotates the existing AESCryptKey.ext and generates a new AESCryptKey.ext key.
   c) Then it updates the keystore with the new key.

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

12.6 HTTPS Protocol

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

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

1. Create SSL related certificates and import to respective servers.
2. Enable SSL on a desired Port (example 9443) on your existing and already deployed web application servers.
3. Execute PortC Utility to change the Servlet port to hold new SSL port and Servlet Protocol from http to https. For details, see Changing IP/Hostname, Ports, Deployed paths, Protocol of the OFSAA Instance.
4. When SSL/TLS is configured on Java 7, navigate to $FIC_HOME/utility/Migration/bin path and modify the ObjectMigration.sh file as given:
$JAVA_BIN/java $X_ARGS_OBJMIG -Dhttps.protocols=TLSv1.2 -classpath $_CLASSPATH $MAIN_JAVA_CLASS $MIGRATION_HOME> $LOG_FILE

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

12.7 Logging

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

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

12.7.1 Purging of Logs

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

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

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

To configure the Logs file size, follow these steps:

1. Navigate to `$FIC_HOME/conf` folder or `<DeployedLocation>/<context.war>/<context>/` and locate `RevLog4jConfig.xml` file.

2. Configure the logger related attributes in the `RevLog4jConfig.xml` file. This file will have Appenders for each log files.

Sample Appender for UMM log file is shown:

```xml
<RollingFile name="UMMAPPENDER"
fileName="/scratch/ofsaaweb/weblogic/user_projects/domains/cdb/applications/cdb.ear/cdb.war/logs/UMMService.log"
filePattern="/scratch/ofsaaweb/weblogic/user_projects/domains/cdb/applications/cdb.ear/cdb.war/logs/UMMService-%i.log" />
```
3. To change the log file size, modify the value set for `SizeBasedTriggeringPolicy size`.

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

### 12.7.2 Log File Format

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

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

Sample:

```
[25-04-18 10:08:41,066 GMT AM] [INFO ] [WEB] [UMM] [UMMUSER] [BUSINESSMETADATA] Inside createImplicitObjectsForAllInfodom
[25-04-18 10:08:41,069 GMT AM] [INFO ] [WEB] [UMM] [UMMUSER] [BUSINESSMETADATA] Call createImplicitObjectsForMapper for infodom = TESTCHEF
[25-04-18 10:08:42,142 GMT AM] [DEBUG] [WEB] [UMM] [UMMUSER] [BUSINESSMETADATA] Source created successfully for infodom TESTCHEF
[25-04-18 10:08:42,142 GMT AM] [INFO ] [WEB] [UMM] [UMMUSER] [BUSINESSMETADATA] Start - code added to create user group hierarchy for this infodom
[25-04-18 10:08:42,142 GMT AM] [INFO ] [WEB] [UMM] [UMMUSER] [BUSINESSMETADATA] Inside createUserGroupHierarchyForInfodom
```
13 **Generic Configurations**

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

- OFSAA Global Performance Optimization
- 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
- Using X-Frame-Options to Embed OFSAA Content on your Site
- Setting Access-Control-Allow-Origin Header
- Configuration for Tomcat
- Configuring WebLogic
- Configuring WebSphere
- 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 IDM
- Configuring the Logout URL for OBIEE in OFSAA
- Enabling Deep Linking in OFSAA
- Enabling Unlimited Cryptographic Policy

### 13.1 OFSAA Global Performance Optimization

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

The columns and the values to be given in the `AAI_GLOBAL_EXEC_OPTIMIZATION` table are indicated as follows:
<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_INFODOM_CODE</td>
<td>Information Domain code</td>
<td>ALL or specific information domain code.</td>
</tr>
<tr>
<td>V_DB_TYPE</td>
<td>Database type of the Information Domain</td>
<td>ORACLE or HIVE</td>
</tr>
<tr>
<td>V_OBJ_TYPE_CODE</td>
<td>Object type for which you want to apply execution</td>
<td>For example, Rule (RL).</td>
</tr>
<tr>
<td></td>
<td>optimization.</td>
<td>This is referred from AAI_OBJ_TYPE_SUBTYPE_MAP.V_OBJ_TYPE_CODE.</td>
</tr>
<tr>
<td>V_OBJ_SUBTYPE_CODE</td>
<td>Object sub type for which you want to apply execution</td>
<td>For example, for Rule (RL) Object type, TYPE2 and TYPE3 are subtype</td>
</tr>
<tr>
<td></td>
<td>optimization.</td>
<td>codes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is referred from AAI_OBJ_TYPE_SUBTYPE_MAP.V_OBJ_SUBTYPE_CODE.</td>
</tr>
<tr>
<td>V_EXEC_OPTIM_PARAM_NAME</td>
<td>Name of the parameter using which optimization is done.</td>
<td>This is referred from AAI_EXEC_OPTIM_PARAM_B.V_EXEC_OPTIM_PARAM_NAME.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Currently supported parameters are POSTSCRIPT, PRESCRIPT, MERGE,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HINT and SELECT.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V_EXEC_OPTIM_PARAM_VALUE</td>
<td>Value for the optimization parameter mentioned in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>V_EXEC_OPTIM_PARAM_NAME column.</td>
<td></td>
</tr>
</tbody>
</table>

### 13.2 Query Performance Optimization

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

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNF_PARALLEL_DEGREE_POLICY</td>
<td>Sets the parallel degree policy. Possible values – MANUAL, LIMITED, or AUTO. Query fired on the database - ALTER SESSION SET PARALLEL_DEGREE_POLICY=&lt;&lt;CNF_PARALLEL_DEGREE_POLICY&gt;&gt;</td>
</tr>
<tr>
<td>CNF_PARALLEL_QUERY</td>
<td>Sets parallelism for queries. Possible values – DISABLE, ENABLE, or FORCE. Query fired on the database - ALTER SESSION &lt;&lt;CNF_PARALLEL_QUERY&gt;&gt; PARALLEL QUERY</td>
</tr>
<tr>
<td>CNF_PARALLEL_DML</td>
<td>Sets parallelism for DML operations. Possible values – DISABLE, ENABLE, or FORCE. Query fired on the database - ALTER SESSION &lt;&lt;CNF_PARALLEL_QUERY&gt;&gt; PARALLEL DML</td>
</tr>
<tr>
<td>CNF_DEGREE_OF_PARALLELISM</td>
<td>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 &lt;&lt;CNF_PARALLEL_QUERY&gt;&gt; PARALLEL QUERY PARALLEL &lt;&lt;CNF_DEGREE_OF_PARALLELISM&gt;&gt; ALTER SESSION &lt;&lt;CNF_PARALLEL_QUERY&gt;&gt; PARALLEL DML PARALLEL &lt;&lt;CNF_DEGREE_OF_PARALLELISM&gt;&gt;</td>
</tr>
</tbody>
</table>

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

### 13.3 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.
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 Spanish.

Command:

./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:
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.

### 13.3.1 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_ofsaaai.sh MIG
./MLS_ofsaaai.sh MLS
./MLS_ofsaaai.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/.

13.4 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;

### 13.5 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, see the **Configuring Resource Reference** sections in Appendix B in **OFS AAI Application Pack Installation and Configuration Guide** available in **OHC Documentation Library**.

**13.6 Changing IP/ Hostname, Ports, Deployed paths, Protocol of the OFSAA Instance**

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

**Prerequisite**

- 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**

1. Navigate to `$FIC_HOME/utility/PortC/bin` folder on **Target**.

2. Run the `PortC.sh` utility using command:

   ```bash
   ./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.

### 13.7 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.

#### 13.7.1 Knowing the Prerequisites

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

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

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

#### 13.7.2 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:

```xml
<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:

```xml
<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>
```

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.

### 13.8 Setting Access-Control-Allow-Origin Header

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

**NOTE:** The configuration described in this section is applicable to release 8.0.6.1.0 and later.

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

1. Open the `web.xml` file in an editor.

2. Search for the following tag:

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

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

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

<init-param>
<param-name>AllowOrigin</param-name>
<param-value>https://example.com/</param-value>
</init-param>

4. Replace https://example.com/ with the URL of your site. This allows requesting code from the origin.

13.9 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>
13.10 Configuring WebLogic

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

13.10.1 Configuring WebLogic for REST Services Authorization

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

1. Open the config.xml file located in the domain where OFSAA is deployed, that is, <domain_home>/config/config.xml.

2. Add the following in the security-configuration tag:

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

13.11 Configuring WebSphere

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

13.11.1 Configuring WebSphere for REST Services Authorization

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

1. Log on to WebSphere console with the User ID provided with the admin rights.

2. Expand Security menu in the LHS and click Global security > Web and SIP security > General settings.

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

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

### 13.12 SSO Authentication (SAML) Configuration

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: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 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 USERNAME 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.
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.

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:

```bash
$ 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. Login to OFSAA with your system administrator credentials.
2. Click  from the header to display the administration tools in a Tiles menu.
3. Click **System Configuration** to view the menu.
4. Click **Configure Application Server** from the menu to view the **Application Server Details** window.
5. In the **Application Server Details** window, click **Modify**.

6. Select **Authentication Type** as **Publickey Auth**.
7. Click **Save**.
8. A confirmation message is displayed to inform that you need to provide the PKI details in the **Web Server Details** window. Click **OK**.
9. Click **Hamburger Icon** to view the Navigation list.
10. Click **Configure Web Server** from the Application Navigation Drawer. The **Web Server Details** window is displayed.
If you have selected Authentication Type as Public Key Auth in the Application Server Details window, the PKA Details check box gets automatically selected and the PKI Details pane is displayed.

11. Click Modify.

12. Enter Private Key Path and Passphrase which you created during Step 1 (Generate a public/private key pair on your webserver).

13. Click Save.

### 13.14 Enable and Disable Users

The users with System Administrator (sysadm) 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 sysadm 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:

13.15 Password Reset

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:

   ![Password reset successful output](image)

   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:
13.16 Configuring OFSAA OIM Connector

OFSAA OIM Connector is used for provisioning users in the Oracle Financial Services Analytical Applications (OFSAA) from Oracle Identity Manager (OIM). For information on OIM, see http://www.oracle.com/technetwork/middleware/idmgmt/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:

- You must have the user credentials with which you installed IDM Suite.
- 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/utility folder.
   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.identityconnectors.ofs-1.0.0.jar
```

**NOTE:** ctxFactory value is `weblogic.jndi.WLInitialContextFactory` for WebLogic and `com.ibm.websphere.naming.WsnInitialContextFactory` for WebSphere.

7. Navigate to the `${OIM_ORACLE_HOME}/server/plugin_utility` directory and set the following values in the `ant.properties` file:

- `wls.home=<Path to WebLogic Server Dir>`  
  For example, `/u01/oracle/products/fmw/10.3.6/wlserver_10.3`

- `oim.home=<OIM Home Path>`  
  For example, `/u01/oracle/products/fmw/10.3.6/Oracle_IDM/server`

- `login.config=<Login Configuration File Home Path>`  
  For example, `${oim.home}/config/authwl.conf`

- `mw.home=<Middleware Home Path>`  
  For example, `/u01/oracle/products/fmw/10.3.6`

8. Execute the following command from the `${OIM_ORACLE_HOME}/connectors/OFSConnector/` directory and upload the schedule task in OIM:

```
sh deploySchTask.sh -username << Xellerate admin username>> -password << admin password>> -serverURL <<oim_server_url>> -id <<OFSAA_ID>>
```

9. Upload the OFSAA Connector metadata to OIM by executing the following command from the `${OIM_ORACLE_HOME}/connectors/OFSConnector/` directory:

```
sh ImportMetadata.sh <xellerate admin username> <admin password> <oim_server_url> OFS-ConnectorConfig_<OIM_VERSION>.xml <OFSAA_ID> <OFS_USER> <OFS_PASSWD> <OFS_URL>
```

**NOTE:** For SSO, `<OFS_USER>` is a valid OIM user. If the setup is non-SSO, then `<OFS_USER>` is SYSADMN.

Based on the OIM version 11.1.2.2 or 11.1.2.3, select the appropriate version of the files to upload.
If the file upload from the shell script is successful, the following message is printed:

File imported successfully: OFS-ConnectorConfig_11.1.2.2.xml

10. For other OFSAA environments such as DEV, UAT and PROD, use the following command to create IT Resource and Access Policy:

   sh ImportMetadata.sh <xellerate admin username> <admin password> <oim_server_url> OFS-ITResource_<OIM_VERSION>.xml <OFSAA_ID> <OFS_USER> <OFS_PASSWD> <OFS_URL>

   **Note:**
   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.

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.

**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:

```bash
wls:/offline>
connect('<user_id>','<password>','t3://<IDM_HOST>:<ADMIN_PORT>')
```

d) Import the OAM Policies using the following:

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

![Authentication Policies](image)

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

![Basic Authentication Policy](image)

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

![Advanced Rules](image)

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)

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 Policies window.
3. Search for server access policy in the window and click the server access policy name to view the Access Policy Information window.

4. By default, All Users role is mapped to the server access policy. To create and map Roles to provision specific users, see https://docs.oracle.com/cd/E40329_01/user.1112/e27151/role_mangmnt.htm#OMUSG3006.
5. Click System Management to view the window and click the Scheduler tab to view the Scheduler window.
6. Enter OFS* in Search Scheduled Jobs and click to view the OFSAA group jobs.
7. Click OFS {OFSAA_ID} Group Search Reconciliation to view the OFS {OFSAA_ID} Group Search Reconciliation window.
8. Select from **Schedule Type**, the frequency at which you want to run the job. Select one from the following options:

   a) **Periodic** - Select this option if you want to run the job at a specific time and on a recurring basis. Enter an integer value in the Run every field in the Job Periodic Settings section and select one of the following values:
      - mins
      - hrs
      - days

   b) **Cron** - Select this option if you want to run the job at a particular interval and on a recurring basis. For example, you can create a job that runs at 8:00 A.M. every Monday through Friday, or at 1:30 A.M. every last Friday of the month. Specify the recurrence of the job in the Cron Settings section. Select any of the following values in the Recurring Interval field:
      - Daily
      - Weekly
      - Monthly on given dates
      - Monthly on given weekdays
      - Yearly

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

   c) **Single** - Select this option if you want to run the job only once at a specific start date and time.

   d) **No pre-defined schedule** – Select this option if you do not want to create a schedule that triggers the job automatically. To trigger the job, click **Save and Run Now**.

10. Click **OFS {OFSAAI_ID} Lookup Search Reconciliation** to view the **OFS {OFSAAI_ID} Lookup Search Reconciliation** window.

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

12. Run **OFS {OFSAAI_ID} Lookup Search Reconciliation** and check for successful execution of the run.

13. Click **OFS {OFSAAI_ID} User Group Reconciliation** to view the **OFS {OFSAAI_ID} User Group Reconciliation** window. Reconcile existing user-group mapping from OFSAA to OIM based on the User Filter field on this window.

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

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

16. Run **OFS {OFSAAI_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.

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

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

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.
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.

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

Following is the procedure to approve an entitlement request:

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.

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

**NOTE:** Prefix `http://<Webserverip>:<servletport>/<context>` to the values in the URL column. For example, `/rest/idm/service/create/user` should be `http://<Webserverip>:<servletport>/<context>/rest/idm/service/create/user`.

The following table provides details for the REST APIs:

<table>
<thead>
<tr>
<th>Number</th>
<th>Requirement</th>
<th>URL</th>
<th>Method Type</th>
<th>Request</th>
<th>Sample Request JSON</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create user</td>
<td>/rest/idm/service/create/user</td>
<td>POST</td>
<td>JSON</td>
<td>{ &quot;attributes&quot;: { &quot;user_id&quot;: &quot;user_id&quot;, &quot;user_name&quot;: &quot;user_name&quot;, &quot;user_password&quot;: &quot;password&quot;, &quot;user_start_date&quot;: &quot;start_date&quot;, &quot;user_end_date&quot;: &quot;End_date&quot;, &quot;user_is_authorized&quot;: true/false, &quot;user_is_enabled&quot;: true/false, &quot;user_logon_holiday&quot;: true/false } }</td>
<td>All FIELDS are mandatory. Date format is mm/dd/yyyy. If <code>user_is_authorized</code> is set to true, then user is authorized during creation.</td>
</tr>
<tr>
<td>Number</td>
<td>Requirement</td>
<td>URL</td>
<td>Method</td>
<td>Request Type</td>
<td>Sample Request JSON</td>
<td>Comments</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------</td>
<td>------------------------------------------</td>
<td>--------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>2</td>
<td>Update user</td>
<td>/rest/idm/service/update/user</td>
<td>POST</td>
<td>JSON</td>
<td>{</td>
<td>All FIELDS are mandatory. Date format is mm/dd/yyyy. If user_is_authorized is set to true, then user is authorized during creation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;attributes&quot;: {</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_id&quot;: &quot;user_id&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_name&quot;: &quot;user_name&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_password&quot;: &quot;password&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_start_date&quot;: &quot;start_date&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_end_date&quot;: &quot;End_date&quot;,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_is_authorized&quot;: true(/false),</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_is_enabled&quot;: true(/false),</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;user_logon_holiday&quot;: true(/false)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Delete User</td>
<td>/rest/idm/service/delete/user</td>
<td>POST</td>
<td>TEXT</td>
<td>USERID</td>
<td>User ID is mandatory.</td>
</tr>
<tr>
<td>4</td>
<td>Authorize User</td>
<td>/rest/idm/service/authorize/user</td>
<td>POST</td>
<td>TEXT</td>
<td>USERID</td>
<td>User ID is mandatory.</td>
</tr>
<tr>
<td>5</td>
<td>Reinstate user</td>
<td>/rest/idm/service/reinstate/user</td>
<td>POST</td>
<td>TEXT</td>
<td>USERID</td>
<td>User ID is mandatory.</td>
</tr>
<tr>
<td>Number</td>
<td>Requirement</td>
<td>URL</td>
<td>Method Type</td>
<td>Request Type</td>
<td>Sample Request JSON</td>
<td>Comments</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-----</td>
<td>-------------</td>
<td>--------------</td>
<td>---------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 6      | Map user to group | /rest/idm/service/map/group members | POST | JSON | {  
  "user_id": "user_id",  
  "group": [  
    {  
      "group_id": "group_id",  
      "group_name": "groupname"  
    },  
    ...  
  ]  
} | Mapping of user id to groups. |
| 7      | Unmap user from group | /rest/idm/service/unmap/groupmembers | POST | JSON | {  
  "user_id": "user_id",  
  "group": [  
    {  
      "group_id": "group_id",  
      "group_name": "groupname"  
    },  
    ...  
  ]  
} | Unmapping of user ids from groups.  
Note: This requirement is applicable for release 8.0.6.1.0 and later versions. |

### 13.18 Configuring the Logout URL for OBIEE in OFSAA

Logging out from OFSAA does not logout a user from Oracle Business Intelligence Enterprise Edition (OBIEE) if the OBIEE Logout URL is not configured in OFSAA.

Perform the following configuration in OFSAA to enable logging out of OBIEE when you logout of OFSAA:

1. Log in to the OFSAA database with CONFIG user credentials:
2. In the database, update the configuration table by running the script in the following format:

```
update configuration set paramvalue = '<OBIEE_LOGOUT_URL>' where paramname = 'OBIEE_LOGOUT_URL_VAL';
/
update configuration set paramvalue = '<IS_CROSSDOMAIN>' where paramname = 'OBIEE_CROSS_DOMAIN_VAL';
```

Replace `<OBIEE_LOGOUT_URL>` with the OBIEE logout URL.

For example,

```
update configuration set paramvalue = 'http://obieehost:port/analytics/saw.dll?Logoff' where paramname = 'OBIEE_LOGOUT_URL_VAL';
```

and

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

For example,

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

### 13.19 Enabling Deep Linking in OFSAA

When a user logs into OFSAA, by default, the application opens the default landing page or the preferred landing page. However, it is possible to open a specific page (show requested resource URL) other than the default or preferred landing page by using Deep Linking in a SSO-enabled setup.

To enable deep linking, perform the following procedure:

1. Login to the **OAM Administrator Console**.
2. From the **Launch Pad**, click **Application Domains** from the **Access Manager** widget. The **Application Domain** window is displayed.
3. Search for the required application domain for which you want to switch the authentication scheme and click **Name** from the search results to display the details for the application domain.

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

5. Click **Protected Resource Policy** from the list to view the details for the policy.

6. Click **LDAPScheme** from Authentication Scheme.

7. Click **Responses** tab and click **Add** button.

8. To configure deep linking in your OFSAAI, set **res_url** header in response to send Requested resource URL path. In the popup, select **Header** for **Type**. Enter **res_url** for **Name**, and enter **$request.res_url** for **Value**. Click **OK**.

9. Click **Apply** to save.

For reference information on the preceding instructions, see the following link for OAM:

Enabling unlimited cryptographic policy for Java enables you to use AES-256 keys for encryption. The JCE Policy JAR files, for the current Java versions required for OFSAAI and also for later versions, are available in the following link:


For Java versions, where unlimited cryptographic policy is not enabled by default, perform the following steps to enable:

1. Download the JCE Policy related JARs `local_policy.jar` and `US_export_policy.jar`.
2. Copy (or replace) the downloaded JCE Policy related JARs `local_policy.jar` and `US_export_policy.jar` into the `/jre/lib/security` directory of Java installation directory used for OFSAAI and the Web Application Servers.