ORACLE®

FINANCIAL SERVICES

Customer Analytics Application Pack

Release: 8.0.6.0.0

Installation and Configuration Guide

December, 2021

Primary Author: Raghavacharyulu NCB

Other Author: Parag Ray, Prashant Sharma

Contents

PREFACE

This Preface provides supporting information for the Oracle Financial Services Customer Analytics Application Pack Installation Guide and includes the following topics:

- Summary
- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

Oracle Financial Services Customer Analytical Applications Pack Installation and Configuration Guide is intended for administrators, and implementation consultants who are responsible for installing and maintaining the application pack components.

Prerequisites for the Audience

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

The following are the expected preparations from the administrator before starting the actual installation:

- Oracle Financial Services Customer Analytical Applications pack components
- OFSAA Architecture
- UNIX Commands
- Database Concepts
- Web Server/ Web Application Server

Recommended Environment

Infrastructure application has been tested with Microsoft Internet Explorer™ browser. For best viewing of Infrastructure pages, set the screen resolution to a minimum resolution of 1024 x 768 pixels.

Related Documents

For more information, refer the Oracle Financial Services Customer Analytical Applications Pack 8.0.6.0.0 documents available in Oracle Help Center OHC.

Conventions

The following text conventions are used in this guide:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, folder paths, or placeholder variables for which you supply particular values.
`monospace`	monospace indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
`Filenames`	filenames indicate the file names within a pragraph.
Hyperlink	Hyperlinks indicate the cross-references, external document links, and external website links.

Abbreviations

Abbreviation	Meaning
AIX	Advanced Interactive eXecutive
BDP	Big Data Processing
DBA	Database Administrator
DDL	Data Definition Language
DEFQ	Data Entry Forms and Queries
DML	Data Manipulation Language
EAR	Enterprise Archive
EJB	Enterprise JavaBean
ERM	Enterprise Resource Management
Abbreviation	Meaning
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HTTPS	Hypertext Transfer Protocol Secure
J2C	J2EE Connector

Abbreviation	Meaning
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JDK	Java Development Kit
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
LHS	Left Hand Side
MOS	My Oracle Support
OFSAAI	Oracle Financial Services Analytical Application Infrastructure
OHC	Oracle Help Center
OLAP	On-Line Analytical Processing
OLH	Oracle Loader for Hadoop
ORAAH	Oracle R Advanced Analytics for Hadoop
OS	Operating System
RAM	Random Access Memory
RDBMS	Relational Database Management System
SFTP	Secure File Transfer Protocol
SID	System Identifier
SSL	Secure Sockets Layer
TDE	Transparent Data Encryption
TNS	Transparent Network Substrate
URL	Uniform Resource Locator
VM	Virtual Machine
WAR	Web Archive
XML	Extensible Markup Language

CHAPTER 1 – ABOUT OFSAA AND OFSAA APPLICATION PACKS

This chapter includes the following topics:

About Oracle Financial Services Analytical Applications (OFSAA)

In today's turbulent markets, financial institutions require a better understanding of their risk-return, while strengthening competitive advantage and enhancing long-term customer value. Oracle Financial Services Analytical Applications (OFSAA) enable financial institutions to measure and meet risk adjusted performance objectives, cultivate a risk management culture through transparency, lower the costs of compliance and regulation, and improve insight into customer behavior.

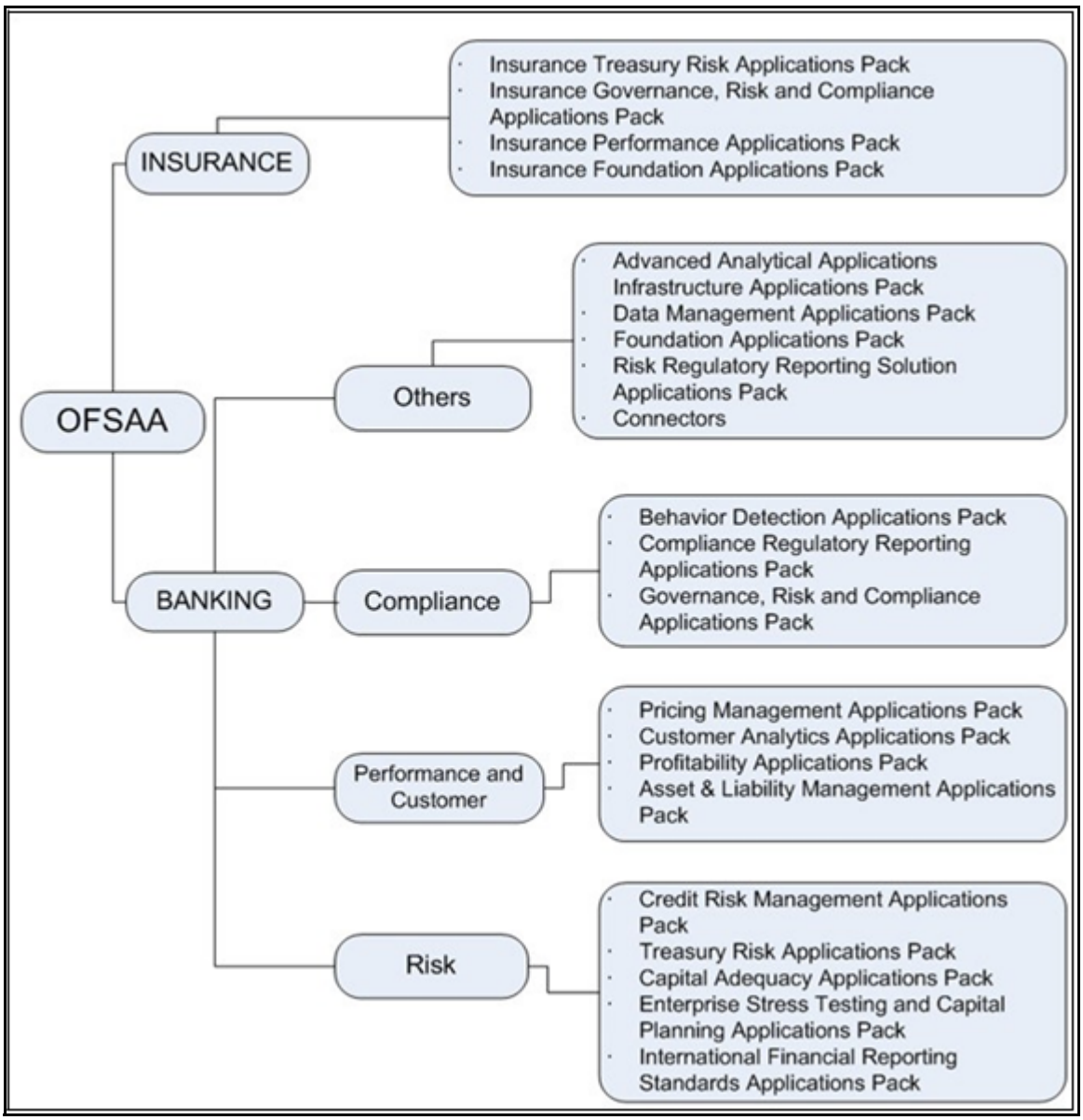
OFSAA uses industry-leading analytical methods, shared data model and applications architecture to enable integrated risk management, performance management, customer insight, and compliance management. OFSAA actively incorporates risk into decision making, enables to achieve a consistent view of performance, promotes a transparent risk management culture, and provides pervasive intelligence.

Oracle Financial Services Analytical Applications delivers a comprehensive, integrated suite of financial services analytical applications for both banking and insurance domain.

About Oracle Financial Services Analytical Applications (OFSAA) Packs

OFSAA applications are packaged, and released as Application Packs starting from 8.0 release. An Application Pack is a group of OFSAA products packaged together in a single installer and addresses specific functional area via its products that are grouped together. Packaging applications in a group ensures simplified installation, maintenance, development and integration in an integrated deployment.

The following figure depicts the various application packs that are available across the OFSAA Banking and Insurance domains:



Introduction to Oracle Financial Services Customer Analytics (OFS CA) Application

OFS CA Application is a complete end-to-end web-based Business Intelligence solution for Customer Analytics. It provides tools for data integration and includes customizable, pre-built dashboards and reports, a reporting data model, and user friendly functional subject areas for ad-hoc reporting. It enables you to actively plan, manage, and track marketing investments with pre-built reports, dashboards, and underlying data structures.

About Oracle Financial Services Analytical Applications Infrastructure (OFS AAI)

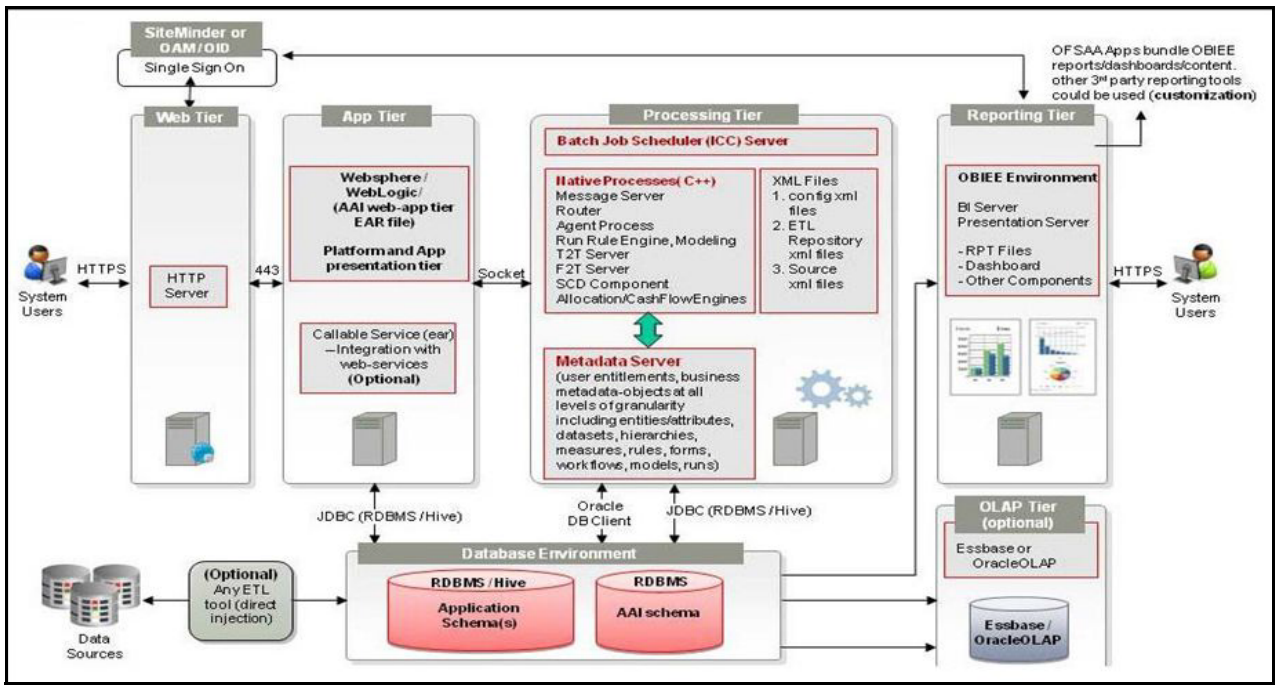
Oracle Financial Services Analytical Applications Infrastructure (OFS AAI) powers the Oracle Financial Services Analytical Applications family of products to perform the processing, categorizing, selection and manipulation of data and information needed to analyze, understand and report on specific performance, risk, compliance and customer insight issues by providing a strong foundation for the entire family of Oracle Financial Services Analytical Applications across the domains of Risk, Performance, Compliance and Customer Insight.

Components of OFSAAI

The OFSAA Infrastructure is comprised of a set of frameworks that operates on and with the Oracle Financial Services Analytical Applications Data Model and form the array of components within the Infrastructure.

The OFSAA Infrastructure components/ frameworks are installed in two layers; primarily the Metadata server and Infrastructure services run on one layer, and the UI and presentation logic runs on the other. The UI and presentation layer is deployed on any of the supported J2EE Servers.

The following figure depicts the various frameworks and capabilities that make up the OFSAA Infrastructure:



OFSAA Infrastructure High Availability

The current release of the OFSAA Infrastructure supports only "Single Instance" installation for the Infrastructure components. However, the High Availability (HA) for the Database Server and/ or the Web Application Server clustering and deployment are supported in this release.

This release supports Active-Passive model of implementation for OFSAAI components. For more information, see Oracle Financial Services Analytical Applications Configuration for High Availability- Best Practices Guide.

About Data Security Configuration

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
- Key Management
- HTTPS
- Logging

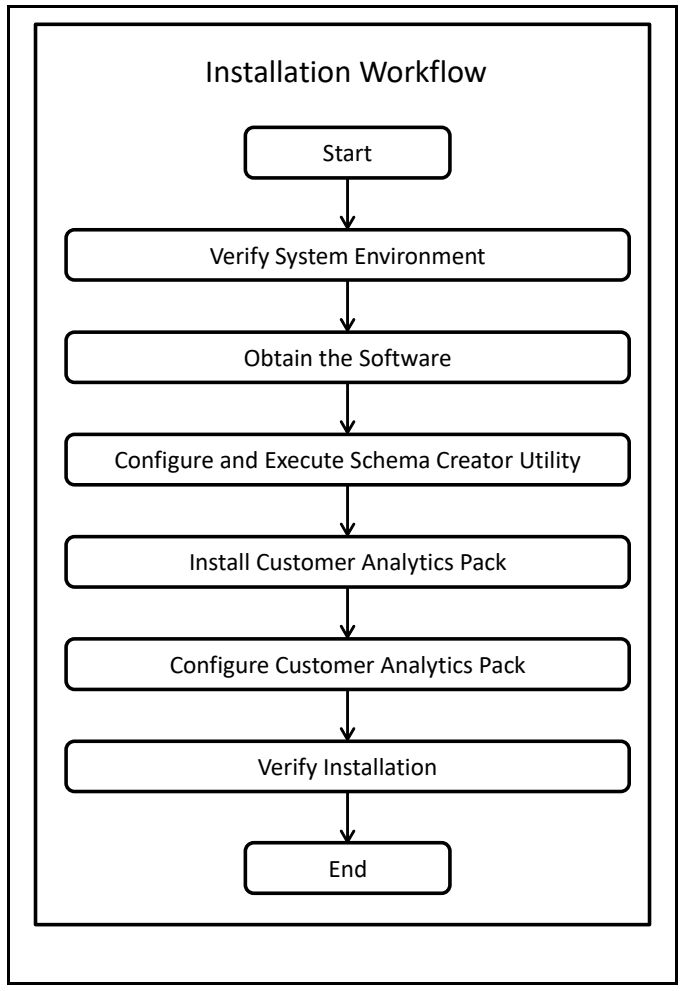
For more details on the features in the previous list, see the relevant topics in this guide and the Data Security and Data Privacy section in the OFSAAI Administration Guide.

CHAPTER 2 – UNDERSTANDING OFS CUSTOMER ANALYTICS APPLICATION PACK INSTALLATIONS

This chapter includes the following topics:

Installation Overview

This section gives an overview of the OFS CA Pack Installation. The following figure shows the order of procedures you will need to follow:

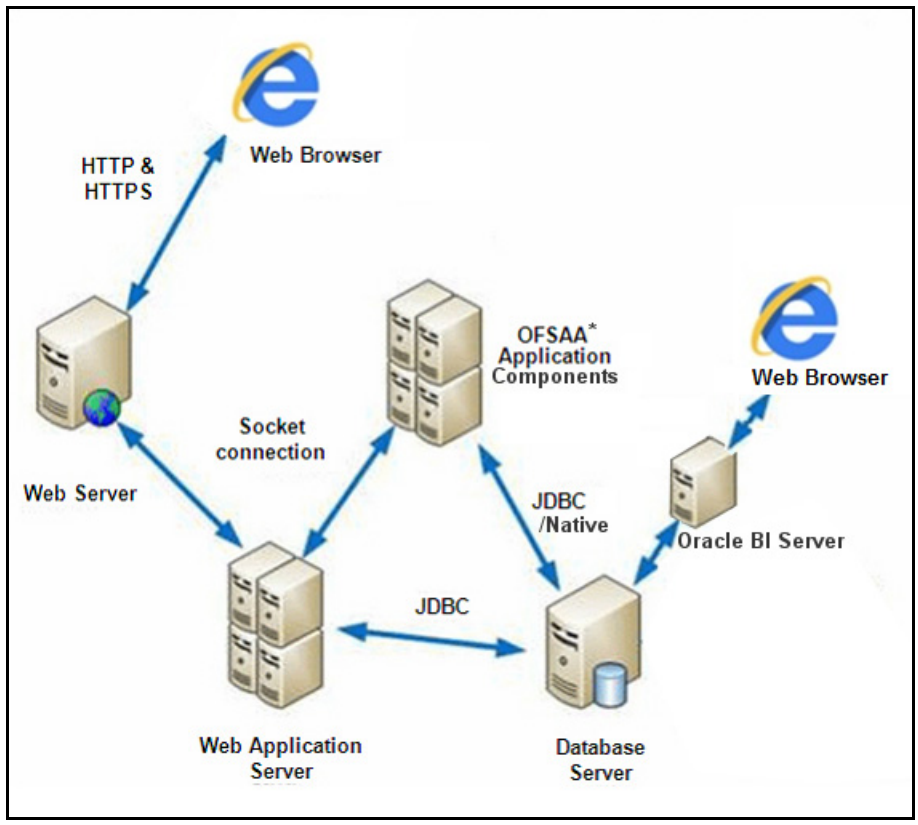


The following table describes the tasks and their descriptions:

Tasks	Details and Documentation
Verify Systems Environment	To verify that your system meets the minimum necessary requirements for installing and hosting the OFS CA Application Pack, see Verifying the System Environment.
Obtain the software	To access and download the OFS CA Application Pack, see Obtaining the Software.
Configure and Execute the Schema Creator Utility	For instructions on creating the database schemas, see Executing the Schema Creator Utility.
Install OFS CA Application Pack	For instructions on Installing OFS CA Application Pack, see Installing the OFS CA Application Pack.
Configure OFS CA Setup	See Post Installation Configuration.

Deployment Topology

The following figure depicts the typical deployment topology implemented for OFSAA Applications:



Hardware and Software Requirements

This section describes the various Operating Systems, Database, Web Server, and Web Application Server versions, and other variant details on which this release of the Oracle Financial Services Customer Analytics Application Pack has been qualified.

OFS CA Application Pack installation can be performed on both Virtual and Physical servers.

Configurations Supported for Java 7

The following table shows the minimum hardware and software requirements for installing OFS Customer Analytics Application Pack (for Java 7):

Requirement	Sub-Category	Value
Operating System	Oracle Linux / Red Hat Enterprise Linux (x86-64)	■ Red Hat Enterprise Linux or Oracle Linux Server release 6 update 6 to latest update version ■ Red Hat Enterprise Linux or Oracle Linux Server release 7 update 1 to latest update version
	Oracle Solaris (SPARC)/ Solaris x86	■ Oracle Solaris v5.10 Update 11 and above - 64 bit ■ Oracle Solaris v5.11 update 3 and above - 64 bit
	IBM AIX (PowerPC)	■ AIX 6.1 (TL 09 and above) - 64 bit ■ AIX 7.1 (TL 03 and above) - 64 bit
	Shell	KORN Shell (KSH)
	Note: ■ If the OS is IBM AIX 6.1 and the file size limit for the AIX user on the target server is too small, configure the size parameter setting for "Large File Support". Follow these steps: Change the file size limit for the user that initiates the transfer on the AIX system. To change the file size limit for a particular user, add or edit the fsize attribute for the user in the /etc/security/limits file on the AIX system. Change the file size limit to unlimited (fsize = -1) or to a size equal to the size of the file being transferred. This may require an restart of the AIX server to pick up the new configuration. For more information, see IBM Support. ■ If the operating system is RHEL, install the package **lsb_release** using one of the following commands by logging in as root user: ❍ `yum install redhat-lsb-core` ❍ `yum install redhat-lsb` ■ To install this release on Oracle Solaris OS, refer to the following list for version specific information: ❍ **Solaris 11** - Upgrade to Oracle Solaris 11.3 with SRU09 or higher. See https://docs.oracle.com/cd/E60778_01/html/E60743/gouaw.html#scrolltoc to upgrade to SRU09 if you have a lower SRU version. Additionally, install the required runtime libraries. For more information, see Installing Only the Runtime Libraries on Oracle Solaris 11. ❍ **Solaris 10** - Install the required OS patches. For more information, see Installing the Required Oracle Solaris 10 Patches. Additionally, install the required runtime libraries. For more information, see Installing Only the Runtime Libraries on Oracle Solaris 10. **Note:** In an OFSAA instance where multiple OFSAA application packs have been installed/deployed, it is mandatory to upgrade all OFSAA application packs to 8.0.4.0.0 release. You should start the upgrade of OFS AAAI<<your pack name>>pack, only after confirming that all of the application packs in your OFSAA instance are available for upgrade to 8.0.4.0.0 version. For information on availability of the required OFSAA Application Packs, see 2246606.1.	

<table>
<tr><th>Requirement</th><th>Sub-Category</th><th>Value</th></tr>
<tr><td rowspan="2">Java Runtime Environment</td><td>Oracle Linux / Red Hat Enterprise Linux</td><td>■ Oracle Java Runtime Environment (JRE) 1.7.x - 64 bit</td></tr>
<tr><td>IBM AIX</td><td>IBM AIX Runtime, Java Technology JRE 1.7.x - 64 bit</td></tr>
<tr><td>Oracle Database Server and Client</td><td colspan="2">■ Oracle Database Server Enterprise Edition 11g Release 2 (11.2.0.3.0 +) - 64 bit RAC/ Non-RAC with partitioning option
■ Oracle Database Server Enterprise Edition 11g Release 2 (11.2.0.4.0 +) - 64 bit RAC/Non-RAC with partitioning option, Advanced Security Option**
■ Oracle Database Server Enterprise Edition 12c Release 1 (12.1.0.1.0 +) - 64 bit RAC/ Non-RAC with partitioning option, Advanced Security Option**
■ Oracle Database Server Enterprise Edition 12C Release 2 (12.2.0.1.0 +) - 64 bit RAC/Non-RAC with partitioning option, Advanced Security Option**
Note: ** See the "Additional Notes" section in the 806 Tech Matrix for details.
■ Oracle Client 11g Release 2 (11.2.0.3.0+) - 64 bit
■ Oracle Client 12c Release 1 (12.1.0.1.0+) - 64 bit
■ Oracle 11g Release 2 (11.2.0.3+) JDBC driver (Oracle thin driver)
■ Oracle 12C Release 1 (12.1.0.1+) JDBC driver (Oracle thin driver)
■ Oracle R Distribution (ORD) version 3.2.0/3.3.0 (Optional)
■ Oracle R Enterprise (Server) version 1.5 with ORD 3.2.0 and version 1.5.1 with ORD 3.3.0 (Optional).
Note: Ensure that the following patches are applied:
❍ For Oracle DB Server 12.1.0.1 and 12.1.0.2, download the patches 27010930 and 22205607 from My Oracle Support and apply them.
❍ For Oracle DB Server 11.2.0.4, download the patch 22205607 from My Oracle Support and apply.</td></tr>
<tr><td></td><td colspan="2">ORAAH Technical Description</td></tr>
<tr><td></td><td colspan="2">
<table>
<tr><th>No.</th><th>Oracle R Enterprise</th><th>Oracle R Advanced Analytics for Hadoop</th><th>Open Source R or Oracle R Distribution</th><th>Oracle Database Enterprise Edition</th></tr>
<tr><td>1</td><td>1.5.1</td><td>2.7.1</td><td>3.3.0</td><td>11.2.0.4,
12.1.0.1,
12.1.0.2,
12.2.0.1</td></tr>
<tr><td>2</td><td>1.5.0</td><td>2.5.1,
2.6.0,
2.7.0</td><td>3.2.0</td><td>11.2.0.4,
12.1.0.1,
12.1.0.2</td></tr>
</table>
</td></tr>
</table>

Requirement	Sub-Category	Value
OLAP	Oracle Hyperion Essbase	■ V 11.1.2.1+ (Server and Client) with Oracle 11g Database ■ V 11.1.2.3+ (Server and Client) with Oracle 12c Database
	Note: Oracle Hyperion Essbase is required only if you are using the OLAP feature of OFSAAI.	
Web Server/ Web Application Server	Oracle Linux / Red Hat Enterprise Linux / IBM AIX Oracle Solaris	Oracle HTTP Server 11.1.1.1/ Apache HTTP Server 2.2.x/ IBM HTTP Server ■ Oracle Weblogic Server 12.1.3+ with jersey 2.25 ■ Oracle WebLogic Server 12.2.x (64 bit) ■ IBM WebSphere Application Server 8.5.5.9+ (Full Profile) with IBM Java Runtime - 64 bit ■ Apache Tomcat version 8.0.21+ up to version 8.0.38 (64 bit) **Note:** OFS Inline Processing Engine does not support Tomcat Web Application Server.
	Note: OFSAA Infrastructure web component deployment on Oracle WebLogic Server with Oracle JRockit is not supported.	
Big Data	Cloudera Distribution Hadoop 5.3.3	■ CDH Version 5.3.3 ■ Hadoop-2.5.0+cdh5.3.3+844 ■ Hive-0.13.1+cdh5.3.3+350 ■ Sqoop1 V 1.4.5+cdh5.3.3+67 ■ Sqoop2 V 1.99.4+cdh5.3.3+23 ■ Oracle Loader For Hadoop (OLH) V 3.2
	Cloudera Distribution Hadoop 5.4.4	■ CDH Version -5.4 ■ Hadoop-2.6.0+cdh5.4.4+597 ■ Hive V 1.1.0+cdh5.4.4+152 ■ Sqoop1 V 1.4.5+cdh5.4.4+101 ■ Sqoop2 V 1.99.5+cdh5.4.4+36
	Cloudera Distribution Hadoop 5.8.4	■ CDH Version -5.8.4 ■ Hadoop-2.6.0+cdh5.8.4+1801 ■ Hive-1.1.0+cdh5.8.4+723 ■ Sqoop-1.4.6+cdh5.8.4+100 ■ Sqoop2-1.99.5+cdh5.8.4+42
	Cloudera Hive Connectors	Hive JDBC Connectors V 2.5.15 and V 2.5.18
	Oracle R Advanced Analytics for Hadoop	Oracle R Advanced Analytics for Hadoop (ORAAH) 2.6.0/ 2.7.0.
	Hadoop Security Protocol	■ Kerberos R release 1.6.1 ■ Sentry-1.4.0

Requirement	Sub-Category	Value
Desktop Requirements	Operating System	Windows 7/8/10
	Browser	■ Microsoft Internet Explorer Browser 11.x ■ Chrome 57.x ■ FireFox 52.x **Note:** Turn off Pop-up blocker settings. For more information, see Internet Explorer Settings.
	Office Tools	■ MS Office 2007/ 2010/ 2013/ 2016 ■ Adobe Acrobat Reader 10 and 11
	Screen Resolution	1024*768 or 1280*1024
Other Software	Directory Services	OFSAAI is qualified on both OPEN LDAP 2.2.29+ and Oracle Internet Directory v 11.1.1.3.0. However, it can be integrated with other directory services software such as MS Active Directory.
	Note: Configuration of Directory services software for OFSAAI installation is optional. For more information on configuration, see LDAP Configuration section in OFSAAI Administration Guide. Open LDAP needs to be installed on MS Windows Server machine only.	
AAI	One-off patch	Download the consolidated one-off patch for bug number **27938294** from http://support.oracle.com.

Configurations Supported for Java 8

The following table shows the minimum hardware and software requirements for installing OFS Customer Analytics Application Pack (for Java 8):

Requirement	Sub-Category	Value
Operating System	Oracle Linux / Red Hat Enterprise Linux (x86-64)	■ Red Hat Enterprise Linux or Oracle Linux Server release 6 update 6 to latest update version ■ Red Hat Enterprise Linux or Oracle Linux Server release 7 update 1 to latest update version
	Oracle Solaris (SPARC)/ Solaris x86	■ Oracle Solaris v5.10 Update 11 and above - 64 bit ■ Oracle Solaris v5.11 update 3 and above - 64 bit
	IBM AIX (PowerPC)	■ AIX 6.1 (TL 09 and above) - 64 bit ■ AIX 7.1 (TL 03 and above) - 64 bit
	Shell	KORN Shell (KSH)
	Note: ■ If the OS is IBM AIX 6.1 and the file size limit for the AIX user on the target server is too small, configure the size parameter setting for "Large File Support". Follow these steps: Change the file size limit for the user that initiates the transfer on the AIX system. To change the file size limit for a particular user, add or edit the fsize attribute for the user in the /etc/security/limits file on the AIX system. Change the file size limit to unlimited (fsize = -1) or to a size equal to the size of the file being transferred. This may require an restart of the AIX server to pick up the new configuration. For more information, see IBM Support. ■ If the operating system is RHEL, install the package **lsb_release** using one of the following commands by logging in as root user: ❍ `yum install redhat-lsb-core` ❍ `yum install redhat-lsb` ■ To install this release on Oracle Solaris OS, refer to the following list for version specific information: ❍ **Solaris 11** - Upgrade to Oracle Solaris 11.3 with SRU09 or higher. See https://docs.oracle.com/cd/E60778_01/html/E60743/gouaw.html#scrolltoc to upgrade to SRU09 if you have a lower SRU version. Additionally, install the required runtime libraries. For more information, see Installing Only the Runtime Libraries on Oracle Solaris 11. ❍ **Solaris 10** - Install the required OS patches. For more information, see Installing the Required Oracle Solaris 10 Patches. Additionally, install the required runtime libraries. For more information, see Installing Only the Runtime Libraries on Oracle Solaris 10. **Note:** In an OFSAA instance where multiple OFSAA application packs have been installed/deployed, it is mandatory to upgrade all OFSAA application packs to 8.0.4.0.0 release. You should start the upgrade of OFS AAAI<<your pack name>>pack, only after confirming that all of the application packs in your OFSAA instance are available for upgrade to 8.0.4.0.0 version. For information on availability of the required OFSAA Application Packs, see 2246606.1.	

<table>
<tr><th>Requirement</th><th>Sub-Category</th><th>Value</th></tr>
<tr><td rowspan="2">Java Runtime Environment</td><td>Oracle Linux / Red Hat Enterprise Linux//IBM AIX
Oracle Solaris</td><td>■ Oracle Java Runtime Environment (JRE) 1.7.x - 64 bit
■ Oracle Java Runtime Environment (JRE) 1.8.x - 64 bit</td></tr>
<tr><td>IBM AIX</td><td>IBM AIX Runtime, Java Technology JRE 1.8.x - 64 bit</td></tr>
<tr><td rowspan="4">Oracle Database Server and Client</td><td colspan="2">■ Oracle Database Server Enterprise Edition 11g Release 2 (11.2.0.3.0 +) - 64 bit RAC/ Non-RAC with partitioning option
■ Oracle Database Server Enterprise Edition 11g Release 2 (11.2.0.4.0 +) - 64 bit RAC/Non-RAC with partitioning option, Advanced Security Option**
■ Oracle Database Server Enterprise Edition 12c Release 1 (12.1.0.1.0 +) - 64 bit RAC/ Non-RAC with partitioning option, Advanced Security Option**
Note: See the "Additional Notes" section in the 806 Tech Matrix for details.
■ Oracle Client 11g Release 2 (11.2.0.3.0+) - 64 bit
■ Oracle Client 12c Release 1 (12.1.0.1.0+) - 64 bit
■ Oracle 11g Release 2 (11.2.0.3+) JDBC driver (Oracle thin driver)
■ Oracle 12C Release 1 (12.1.0.1+) JDBC driver (Oracle thin driver)
■ Oracle R Distribution (ORD) version 3.2.0/3.3.0 (Optional)
■ Oracle R Enterprise (Server) version 1.5 with ORD 3.2.0 and version 1.5.1 with ORD 3.3.0 (Optional).</td></tr>
<tr><td colspan="2">Note:
Ensure that the following patches are applied:
■ Oracle Server 12c, v12.1.0.1 - 17082699
■ Oracle Server 12c, v12.1.0.2 - 19392604, 19649591
■ For Oracle DB Server 12.1.0.1 and 12.1.0.2, download the patches 27010930 and 22205607 from My Oracle Support and apply them.
■ For Oracle DB Server 11.2.0.4, download the patch 22205607 from My Oracle Support and apply.
Also for latest information, see http://support.oracle.com, 12.1.0.2 Bundle Patches for Engineered Systems and DB In-Memory - List of Fixes in each Bundle (Doc ID 1937782.1).</td></tr>
<tr><td colspan="2">ORAAH Technical Description</td></tr>
<tr><td colspan="2"><table>
<tr><th>No.</th><th>Oracle R Enterprise</th><th>Oracle R Advanced Analytics for Hadoop</th><th>Open Source R or Oracle R Distribution</th><th>Oracle Database Enterprise Edition</th></tr>
<tr><td>1</td><td>1.5.1</td><td>2.7.1</td><td>3.3.0</td><td>11.2.0.4,
12.1.0.1,
12.1.0.2,
12.2.0.1,
12.1.0.2</td></tr>
</table></td></tr>
</table>

Requirement	Sub-Category	Value
OLAP	Oracle Hyperion Essbase	■ V 11.1.2.1+ (Server and Client) with Oracle 11g Database ■ V 11.1.2.3+ (Server and Client) with Oracle 12c Database
	Note: Oracle Hyperion Essbase is required only if you are using the OLAP feature of OFSAAI.	
Web Server/ Web Application Server	Oracle Linux / Red Hat Enterprise Linux / IBM AIX Oracle Solaris	Oracle HTTP Server 11.1.1.1/ Apache HTTP Server 2.2.x/ IBM HTTP Server ■ Oracle Weblogic Server 12.1.3+ with jersey 2.25 ■ Oracle WebLogic Server 12.2.x - (64 bit) ■ IBM WebSphere Application Server 8.5.5.9+ (Full Profile) with IBM Java Runtime - 64 bit ■ Apache Tomcat version 8.0.21+ up to version 8.0.38 - 64 bit **Note:** OFS Inline Processing Engine does not support Tomcat Web Application Server.
	Note: OFSAA Infrastructure web component deployment on Oracle WebLogic Server with Oracle JRockit is not supported. For deployment on Oracle WebLogic Server 12.1.3+ (64 bit) with Java 8, download and install patch 18729264 from http://support.oracle.com.	

Requirement	Sub-Category	Value
Big Data	Cloudera Distribution Hadoop 5.3.3	■ CDH Version 5.3.3 ■ Hadoop-2.5.0+cdh5.3.3+844 ■ Hive-0.13.1+cdh5.3.3+350 ■ Sqoop1 V 1.4.5+cdh5.3.3+67 ■ Sqoop2 V 1.99.4+cdh5.3.3+23 ■ Oracle Loader For Hadoop (OLH) V 3.2
	Cloudera Distribution Hadoop -5.4.4	■ CDH Version -5.4 ■ Hadoop-2.6.0+cdh5.4.4+597 ■ Hive V 1.1.0+cdh5.4.4+152 ■ Sqoop1 V 1.4.5+cdh5.4.4+101 ■ Sqoop2 V 1.99.5+cdh5.4.4+36
	Cloudera Distribution Hadoop 5.8.4	■ CDH Version -5.8.4 ■ Hadoop-2.6.0+cdh5.8.4+1801 ■ Hive-1.1.0+cdh5.8.4+723 ■ Sqoop-1.4.6+cdh5.8.4+100 ■ Sqoop2-1.99.5+cdh5.8.4+42
	Cloudera Hive Connectors	Hive JDBC Connectors V 2.5.15 and V 2.5.18
	Oracle R Advanced Analytics for Hadoop	Oracle R Advanced Analytics for Hadoop (ORAAH) 2.6.0/ 2.7.0.
	Hadoop Security Protocol	■ Kerberos R release 1.6.1 ■ Sentry-1.4.0
Desktop Requirements	Operating System	MS Windows 7/8/10
	Browser	■ Microsoft Internet Explorer Browser 11.x ■ Chrome 57.x ■ FireFox 52.x **Note:** Turn off Pop-up blocker settings. For more information, see Internet Explorer Settings.
	Office Tools	■ MS Office 2007/ 2010/ 2013/ 2016 ■ Adobe Acrobat Reader 10 and 11
	Screen Resolution	1024*768 or 1280*1024

Requirement	Sub-Category	Value
Other Software	Directory Services	OFSAAI is qualified on both OPEN LDAP 2.2.29+ and Oracle Internet Directory v 11.1.1.3.0. However, it can be integrated with other directory services software like MS Active Directory.
	Note: Configuration of Directory services software for OFSAAI installation is optional. For more information on configuration, see LDAP Configuration section in OFSAAI Administration Guide. Open LDAP needs to be installed on MS Windows Server machine only.	
AAI	One-off patch	Download the consolidated one-off patch for bug number **27938294** from http://support.oracle.com.

Note: To upgrade an existing OFSAA 8.0.x Java 7 instance to Java 8, see Upgrading an Existing OFSAA 8.0.x Java 7 Instance to Java 8.

Recommended Software Combinations

OFS Customer Analytics Application Pack recommends the following software combinations for deployment:

Operating System	Database	Web Application Server	Web Server
Oracle Linux 5.3 up to 5.10/ 6.0 and above	Oracle Database	Oracle WebLogic Server/ Apache Tomcat Server	Oracle HTTP Server/ Apache HTTP Server
Oracle Solaris 5.10/ 5.11	Oracle Database	Oracle WebLogic Server/ Apache Tomcat Server	Oracle HTTP Server/ Apache HTTP Server
IBM AIX 6.1	Oracle Database	IBM WebSphere Application Server/ Apache Tomcat Server	IBM HTTP Server/ Apache HTTP Server

Verifying the System Environment

To verify if your system environment meets the minimum requirements for the installation, a Pre-Install Check utility (Environment Check) is available within the Install Kit archive file. This utility can also be obtained separately by contacting Oracle Support.

Though the system environment verification is an integral and automated part of the installation of this software product, Oracle strongly recommends running this utility prior to beginning the installation as part of your organization's "Installation Readiness Verification Process".

Note: For more details on download and usage of this utility, see *Oracle Financial Services Analytical Applications Infrastructure Environment Check Utility Guide* given in the Related Documents section.

Understanding Installation Modes

OFA CA application pack can be installed in Hybrid and Standard modes.

Standard Installation: This is used for RDBMS Only installation using the standard template.

Hybrid Installation: Hybrid installation files are used for HADOOP additional capability. The hybrid files are provided as template which needs to be changed to proper extension by removing 'template'. After changing file name, the values need to be provided as mentioned in the section 1.3.1.

CHAPTER 3 – PREPARING FOR INSTALLATION

This chapter provides necessary information to review before installing the OFS CA Pack v8.0.6.0.0.

This chapter includes the following topics:

Installer and Installation Prerequisites

The following table mentions the list of prerequisites required before beginning the installation for OFS CA Application Pack. The Installer/ Environment Check utility notifies you if any requirements are not met.

Requirement	Sub-Category	Expected Value
Environment Settings	Java Settings	PATH in .profile to be set to include the Java Runtime Environment absolute path. The path should include Java version (Java 7 or Java 8) based on the configuration. **Note:** Ensure the absolute path to JRE/bin is set at the beginning of PATH variable. For example, PATH=/usr/java/jre1.6/bin:$ORACLE_HOME/bin:$PATH Ensure no SYMBOLIC links to JAVA installation is being set in the PATH variable.
	Oracle Database Settings	**Oracle Database Server** ■ TNS_ADMIN must be set in .profile file pointing to appropriate tnsnames.ora file. ■ Enable Transparent Data Encryption (TDE) and/ or Data Redaction** **Note:** For more information, see TDE, Data Redaction and the Corresponding Settings in OFSAA.
		OFSAA Processing Server ■ ORACLE_HOME must be set in .profile file pointing to appropriate Oracle Client installation. ■ PATH in .profile must be set to include appropriate $ORACLE_HOME/bin path. ■ Ensure that an entry (with SID/ SERVICE NAME) is added in the tnsnames.ora file.
	Oracle Essbase Settings	ARBORPATH, ESSBASEPATH, HYPERION_HOME to be set in the .profile pointing to an appropriate Oracle Essbase Client installation. **Note:** These settings are required only if you want to use Oracle Hyperion Essbase OLAP features.

Requirement	Sub-Category	Expected Value
OS/ File System Settings	File Descriptor Settings	Greater than 15000 **Note:** The value specified here is the minimum value to be set for the Installation process to go forward. For other modules, this value may depend on the available resources and the number of processes executed in parallel.
	Total Number of Process Settings	Greater than 4096 **Note:** The value specified here is the minimum value to be set for the Installation process to go forward. For other modules, this value may depend on the available resources and the number of processes executed in parallel.
	Port Settings	Default port numbers to be enabled on the system are 6500, 6501, 6505, 6507, 6509, 6510, 6666, 9999, and 10101.
	.profile permissions	User to have 755 permission on the .profile file.
	Installation Directory	A directory where the product files will be installed/ copied. Assign 755 permission on this directory. This directory needs to be set as FIC_HOME.
	Staging Area/ Metadata Repository	A directory to hold the application Metadata artifacts and additionally act as staging area for flat files. The directory should exist on the same system as the OFSAA Installation. This directory can be configured on different mount or under a different user profile. Assign 775 permission on this directory. **Note:** This directory is also referred to as FTPSHARE folder.
	Download Directory	A directory where the product installer files will be downloaded/ copied. Set 755 permission on this directory.
	OS Locale	■ Linux: en_US.utf8 ■ AIX: EN_US.UTF-8 ■ Solaris: en_US.UTF-8 To check the locale installed, execute the following command: `locale -a | grep -i 'en_US.utf'`
Database Settings	Database Instance Settings	NLS_CHARACTERSET to be AL32UTF8 NLS_LENGTH_SEMANTICS to be BYTE OPEN CURSORS limit to be greater than 1000

Requirement	Sub-Category	Expected Value
Web Application Server	WebSphere/ WebLogic/ Tomcat	Web Application Server should be installed and profile /domain created. You will be prompted to enter the WebSphere Profile path or WebLogic Domain path or Tomcat Deployment path during OFSAAI installation. **Note:** See Configuring Web Server for WebSphere Profile Creation and WebLogic Domain Creation.
Web Server	Apache HTTP Server/ Oracle HTTP Server/ IBM HTTP Server	This is an optional requirement. HTTP Server Installation to be present. You will be required to enter the Web Server IP/ Hostname and Port details during installation. Note: See Configuring Web Server for Web Server configuration.
Big Data	Cloudera CDH and Cloudera JDBC Connectors	This is an optional requirement and required if Oracle Financial Services - Big Data Processing license is enabled. For more information, see Installing Cloudera CDH.
Others	Oracle R/ Oracle R Enterprise	This is an optional requirement. For more details, see Configuration for Oracle R Distribution and Oracle R Enterprise (ORE).

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

Login to Configuration Schema and execute the following SQL statements:

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

Note: Ensure that the tablespace(s) used for the database user(s) is set to AUTOEXTEND ON.

Prerequisites for Hybrid Installation

It is required to copy the Hive related files. To copy the files:

1. Create a directory */scratch/<user>/clientconf/* with 775 permission.
2. Copy the Hive jars, conf file, and keytab files into the above directory.
3. The following is required only if you are installing OFS CA pack in Hybrid mode of installation. You need to do this after you have performed the prerequisites for standard installation.

a. Create a folder in *User_Home* and copy the Hadoop jars, Kerberos files and client config of Hadoop into the newly created folder and *clientconf/lib* folder.

The files for CDH 5.3.1 are as shown below. Note that the version number is different for each CDH. Ensure that the user permission is set to 755 on this folder.

Note: The following list is a sample and may vary from Hadoop release to release.

- avro-1.7.6-cdh5.3.1.jar
- commons-cli-1.2.jar
- commons-collections-3.2.1.jar
- commons-configuration-1.6.jar
- commons-httpclient-3.1.jar
- commons-io-2.4.jar
- commons-logging-1.1.3.jar
- core-site.xml
- guava-11.0.2.jar
- hadoop-auth-2.5.0-cdh5.3.1.jar
- hadoop-common-2.5.0-cdh5.3.1.jar
- hadoop-core-2.5.0-mr1-cdh5.3.1.jar
- hadoop-core.jar
- hadoop-hdfs-2.5.0-cdh5.3.1.jar
- hdfs-site.xml
- hive-exec-0.13.1-cdh5.3.1.jar
- hive-exec.jar
- hive-jdbc-0.13.1-cdh5.3.1.jar
- HiveJDBC4.jar
- hive-jdbc.jar
- hive-metastore-0.13.1-cdh5.3.1.jar
- hive_metastore.jar
- hive-service-0.13.1-cdh5.3.1.jar
- hive_service.jar
- hive-site.xml
- htrace-core-3.0.4
- httpclient-4.2.5.jar
- httpcore-4.2.5.jar
- jackson-core-asl-1.8.8.jar
- jackson-mapper-asl-1.8.8.jar
- krb5.conf

- libfb303-0.9.0.jar
- libthrift-0.9.0-cdh5-2.jar
- libthrift-0.9.0.jar
- log4j-1.2.14.jar
- mapred-site.xml
- ofsaa.keytab
- protobuf-java-2.5.0.jar
- ql.jar
- servlet-api.jar
- slf4j-api-1.7.5.jar
- TCLIServiceClient.jar
- yarn-site.xml
- zookeeper-3.4.6.jar

b. Copy realm, Kerberos and CDH client config files to *$TOMCAT_HOME/webapps/<context>/conf* folder.

c. Copy ofsaa-hive-udf.jar to */scratch/hive* in hive server.

d. Also, carry out the following other configuration:

i. Remove OFS_CA_SCHEMA_IN.xml in */schema_creator/conf/* folder.

ii. Rename OFS_CA_SCHEMA_BIGDATA_IN.XML.HYBRID.template to FS_CA_SCHEMA_BIGDATA_IN.xml.

iii. Update OFS_CA_SCHEMA_BIGDATA_IN.xml accordingly for hybrid installation.

iv. Remove OFS_CA_CFG.dat file present in /schema_creator/conf/ folder.

v. Rename OFS_CA_CFG.DAT.HYBRID.template to OFS_CA_CFG.dat.

vi. Remove default.properties in */OFS_CA/conf/* folder.

vii. Rename default.properties.HYBRID.template to default.properties.

viii. Remove Silent.template in */OFS_CA/conf/* folder.

ix. Rename Silent.template.HYBRID.template to Silent.props.

x. Remove OFS_CA_PACK.xml in *<installation folder>/conf/* folder.

xi. Rename OFS_CA_PACK.XML.HYBRID.template to OFS_CA_PACK.xml.

xii. Update OFSAAI_InstallConfig.xml file.

Obtaining the Software

This release of OFS CA Application Pack v8.0.6.0.0 is available for download in My Oracle Support (https://support.oracle.com) as Patch **28391701**. You need to have a valid Oracle account in order to download the software.

Common Installation Tasks

The following are the common pre-installation activities that you need to carry out before installing the OFS CA Application Pack.

This section includes the following topics:

- Identifying the Installation, Download and Metadata Repository Directories
- Downloading and Copying the OFS CA Application Pack Installer
- Setting up the Web Server/ Web Application Server
- Installation of Oracle R Distribution

Identifying the Installation, Download and Metadata Repository Directories

For installing any OFSAA Application Pack, the below folders/ directories required to be created.

- **OFSAA Download Directory (Optional)**: Create a download directory and copy the OFSAA Application Pack Installer File (Archive). This is the directory where the downloaded installer/ patches can be copied.
- **OFSAA Installation Directory (Mandatory)**: Create an installation directory. This is the directory where the installer installs or copies the product files. FIC_HOME variable to be set in the .profile file to point to the OFSAA Installation Directory.
- **OFSAA Staging/ Metadata Repository Directory (Mandatory)**: Create a Staging/ Metadata Repository Directory. This is the directory where you should copy data loading files, save data extracts and so on. Additionally, this folder also maintains the OFSAA Metadata artifacts. This is commonly referred as "FTPSHARE". This directory must be created on the same host as the OFSAA Installation Directory mentioned in the previous point in this list.

Note: Ensure that the user permission is set to 755 on the Installation and Download Directory and the user permission is set to 777 on the Staging Directory.

Downloading and Copying the OFS CA Application Pack Installer

To download and copy the OFS CA Application Pack Installer, follow these steps:

- This release of OFS CA Application Pack v8.0.6.0.0 is available for download in MOS as Patch **28391701**. You need to have a valid Oracle account in order to download the software.
- Copy the downloaded installer archive to the Download Directory (in Binary Mode) on the setup identified for OFSAA installation.
- Log in to My Oracle Support, search for the 33663417 Mandatory Patch in the Patches & Updates Tab and download it.
- **ATTENTION**: On the 10th of December 2021, Oracle released Security Alert CVE-2021-44228 in response to the disclosure of a new vulnerability affecting Apache Log4J prior to version 2.15. The application of the 33663417 Mandatory Patch fixes the issue.

  For details, see the My Oracle Support Doc ID 2827801.1.

Setting up the Web Server/ Web Application Server

For more information to set up the environment based on your selected Web Server/ Web Application Server, see Configuring Web Server and Configuring Web Application Server.

Installation of Oracle R Distribution

This is an optional step and required only if you intend to use Oracle R scripting in the Oracle Financial Services Enterprise Modeling Application or if the OFSAA Application that you have licensed uses this feature. For information on applications that use this feature, see the Tech Matrix.

The following is the instruction to install ORD and ORE:

Install Oracle R Distribution and Oracle R Enterprise (Server Components) on the Oracle Database server. See Oracle® R Enterprise Installation and Administration Guide for Windows, Linux, Solaris and AIX - Release 1.5 at Oracle R Enterprise Documentation Library and Release 1.5.1 at Oracle R Enterprise Documentation Library.

No.	Oracle R Enterprise	Oracle R Advanced Analytics for Hadoop	Open source R or Oracle R Distribution	Oracle Database Enterprise Edition
1	1.5.1	2.7.1	3.3.0	11.2.0.4, 12.1.0.1, 12.1.0.2, 12.2.0.1
2	1.5.0	2.5.1, 2.6.0, 2.7.0	3.2.0	11.2.0.4, 12.1.0.1, 12.1.0.2

Note: If you use ORE 1.5 or ORE 1.5.1, for Oracle Financial Services Enterprise Modeling, you must set the session time zone in *'R_HOME/etc/Rprofile.site*' file on the database server, where R_HOME is the home directory of the R instance on which ORE server packages are installed. Alternatively, you can set session time zone in scripts registered within OFS EM by using the 'Sys.env(TZ=<time zone>)' R function.

Installing Cloudera CDH

This is an optional step and required only if you intend to install OFSAA Big Data Processing. Follow these steps:

1. Install CDH v5.3.3, 5.4.4 or v5.8.4. For more information, see Cloudera 5.3.x Documentation, Cloudera 5.4.x Documentation or Cloudera 5.8.x Documentation.

CHAPTER 4 – INSTALLING OFS CA APPLICATION PACK

This chapter describes the steps to be followed to install the OFS CA Application pack.

Note: Release 8.0.6.0.0 of OFS CA Application pack is not fully backward compatible with earlier versions of OFSAA applications. You can either upgrade all of your applications from existing 8.0.x versions to 8.0.6.0.0 version or choose to upgrade only selective application packs to v8.0.6.0.0. In the case of the latter, you must also apply the mentioned compatibility patches for the required application packs, so that the remaining application-packs can continue to be at their pre-8.0.6.0.0 versions.

This chapter includes the following topics:

About Schema Creator Utility

Creating database users/ schemas (RDBMS/ HIVE) is one of the primary steps in the complete OFSAA installation process. The Schema Creator utility facilitates you to quickly get started with the OFSAA 8.0 installation by allowing easier and faster creation of database User(s)/ Schema(s) (RDBMS/ HIVE), assigning the necessary GRANT(s), creating the required entities in the schemas, and so on.

The schema creator utility should be configured and executed mandatorily every time prior to installation of any OFSAA Application Pack.

This section includes the following topics:

Configuring Schema Creator Utility for RDBMS Installation

OFS CA Application Pack specific schema details need to be filled in the `OFS_CA_SCHEMA_IN.xml` file before executing the Schema Creator Utility. For more information on the xml file, see Configuring OFS_CA_SCHEMA_IN.xml.

The following are the types of schemas that can be configured in the OFSAA:

- **CONFIG**: This schema holds the entities and other objects required for OFSAA setup configuration information.

  Note: There can be only one CONFIG schema per OFSAA instance.

- **ATOMIC**: This schema holds the data model entities. One ATOMIC schema is attached to one Information Domain.

  Note: For some application packs, there can be multiple ATOMIC schemas per OFSAA Instance, but the OFS Customer Analytics Pack supports only one atomic schema per OFSAA instance.

- **SANDBOX**: Denotes the schema that contains the data for all Sandbox executions. One SANDBOX schema is attached to one Sandbox Information Domain.

  Note: This Schema type is not applicable for OFS Customer Analytics Application Pack. There can be multiple SANDBOX schemas per OFSAA Instance and a Sandbox Information Domain can have only one SANDBOX schema.

- **ADDON**: Denotes any additional schema used by the OFSAA Applications.

  Note: This Schema type is not applicable for OFS Customer Analytics Application Pack.

Configuring Schema Creator Utility for Hybrid Installation

In case the installation is being performed for Big Data, the pack specific schema details need to be filled in the `OFS_CA_SCHEMA_BIGDATA_IN.xml` file, before executing the utility. For more information on the xml file, see Configuring OFS_CA_SCHEMA_BIGDATA_IN.XML file.

The following are the types of schemas that can be configured:

- **CONFIG**: This schema holds the entities and other objects required for OFSAA setup configuration information.

  Note: There can be only one CONFIG schema per OFSAA instance. This schema is created only in RDBMS.

- **METADOM**: This schema holds the data model entities. One METADOM schema is attached to one Information Domain.

  Note: There can be multiple DATADOM schemas per OFSAA Instance. This schema is created only in RDBMS. It has only platform entities that hold the metadata details. However, it does not hold the data model entities.

- **DATADOM**: This schema holds data model entities. One DATADOM schema is attached to one Information Domain.

  Note: There can be multiple DATADOM schemas per OFSAA Instance. Each Datadom has a Metadom. However, the names of the Datadom and Metadom name cannot be the same.

Selecting Execution Options in Schema Creator Utility

Depending on the option you choose to run the OFSAA Application Pack Installer, you need to choose the schema creator utility execution option. To run the OFSAA Application Pack installer in SILENT mode, it is mandatory to execute the schema creator utility with -s option.

Configuring and Executing the Schema Creator Utility

This section includes the following topics:

Prerequisites

The following prerequisites must be ensured before configuring the Schema Creator Utility:

- You must have the Oracle User ID/Password with SYSDBA privileges.
- You must have the JDBC Connection URL for RAC/Non RAC database.
- The HOSTNAME/IP of the server on which OFSAA is getting installed.
- For enabling Transparent Data Encryption (TDE) in your OFSAA instance during installation, perform the steps explained in TDE, Data Redaction and the Corresponding Settings in OFSAA.
- It is recommended to set the `PGA_AGGREGATE_LIMIT` database-parameter value sufficiently, when Oracle 12c is installed
- You must add a TNS entry before the installation.
- For HIVE installation, the prerequisites you must have before configuring the Schema Creator Utility are:
  - HIVE connection credentials (For example: Kerberos connection properties).
  - Hostname/IP of the HIVE Server installation

Note: The TNS Entry for an atomic schema should be without any special character, i.e '_'. If the atomic schema name is like 'DEV_ATOM', the TNS name should be like 'DEVATOM'.

Configuring the Schema Creator Utility

To configure the Schema Creator Utility, follow these steps:

1. Log in to the system as non-root user.
2. Navigate to the following path: *OFS_CA_PACK/schema_creator/conf*.
3. Edit the OFS_CA_SCHEMA_IN.xml file in a text editor.
4. Configure the elements as described in the following files:
   - **For Standard Installation**: Configuring OFS_CA_SCHEMA_IN.xml
   - **For Hybird Installation**: Configuring OFS_CA_SCHEMA_BIGDATA_IN.XML.
5. Save the OFS_CA_SCHEMA_IN.xml and OFS_CA_SCHEMA_BIGDATA_IN.xml files.

Note: On successful execution of the utility, the entered passwords in the OFS_CA_SCHEMA_IN.xml and OFS_CA_SCHEMA_BIGDATA_IN.xml files are nullified.

Executing the Schema Creator Utility

This section includes the following topics:

- Executing the Schema Creator Utility with -s option
- Executing the Schema Creator Utility for Subsequent Application Pack
- Verifying the Log File

Executing the Schema Creator Utility with -s option

If you want to run the OFSAA Application Pack Installer in SILENT mode, it is mandatory to execute the schema creator utility with -s option.

1. Log in to the system as non-root user.
2. Edit the file *OFS_CA_PACK/schema_creator/conf/*OFS_CA_SCHEMA_IN.xml in text editor.
3. Set the value for attribute "INFODOM" of <SCHEMA> tag(s) to specify a specific Information Domain name. By default, the value is empty and the utility derives the Information Domain name. If the attribute value is set, the utility/ installer configures the Information Domain against this <SCHEMA>.
4. Navigate to the following folder path: *OFS_CA_PACK/schema_creator/bin/*.
5. Execute the utility with -s option.

   For Example: `./osc.sh -s`

   The following message is displayed: *You have chosen ONLINE mode. Triggering the utility in ONLINE mode will execute the DDLs directly on the Database. Do you wish to proceed? (Y/y or N/n).*

6. Enter Y/y to proceed.

```
$ ./osc.sh -S
============================================================
You have chosen ONLINE mode
============================================================
Triggering the utility in ONLINE mode will execute the DDLs directly on the Database. Do you wish to proceed? (Y/N):
y
============================================================
Java Validation Started ...
Java found in : /usr/java/jdk1.7.0_72/bin
JAVA Version found : 1.7.0_72
JAVA Bit Version found : 64-bit
Java Validation Completed. Status : SUCCESS
============================================================
DB specific Validation Started ...
Enter the DB User Name With SYSDBA Privileges:
sys as sysdba
Enter the User Password:
Oracle Client version : 12.1.0.2.0. Status : SUCCESS
Oracle Server version Current value : 12.2.0.1.0. Status : SUCCESS
DB specific Validation Completed. Status : SUCCESS
============================================================
================================================================================
                        Schema Creation Started
================================================================================
Checking OFSAA installation...
OFSAA installation not found.
Validating the dat file OFS_CA_CFG.dat started...
The path is:/scratch/806RCAMock/806/OFS_CA_PACK/schema_creator/conf
Sucessfully validated OFS_CA_CFG.dat file
Validating the input XML file.../scratch/806RCAMock/806/OFS_CA_PACK/schema_creator/conf/OFS_CA_SCHEMA_BIGDATA_IN.xml
Input XML file validated successfully.
================================================================================
Validating Connection URL ...jdbc:oracle:thin:@ofss220618.in.oracle.com:1521/CIPMDB
Successfully connected to User - sys as sysdba URL - jdbc:oracle:thin:@ofss220618.in.oracle.com:1521/CIPMDB
Connection URL successfully validated...
localhost name - whf00azi IPAddress - 10.184.156.203
IS_HYBRID not there in schema
ADV_SEC_TAG not there in schema
Parsing TABLESPACE tags...
Parsing DATADOM...
Validating the DATADOM connection
principal: hdfs@DEV.ORACLE.COM - useProxy: false - proxyUserId:
```

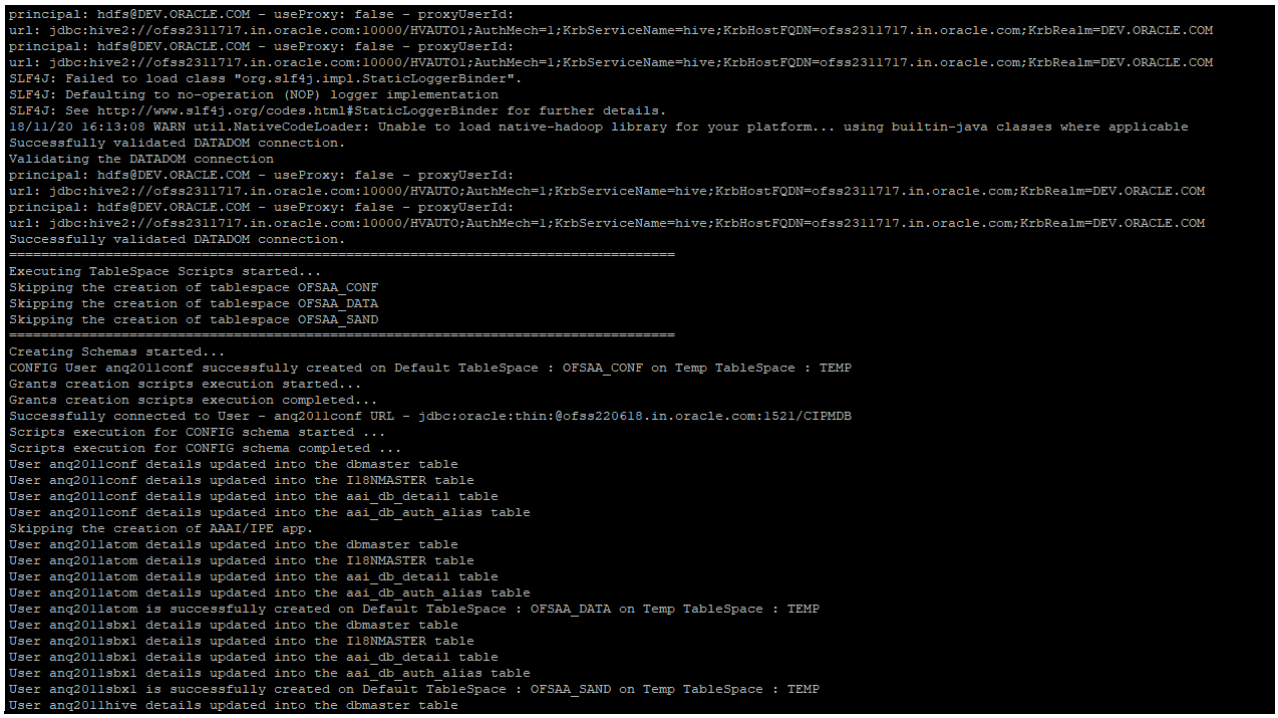
7. Enter the DB Username with SYSDBA Privileges.

   For example: SYS as SYSDBA.

8. Enter the User Password.
   - The console runs the initial validation checks and then displays the following message:

     You have chosen to install this Application Pack on <Name of the Atomic Schema > ATOMIC schema. Do you want to proceed? (Y/N).

You have chosen to install this Application Pack on <Name of the Infodom>. Do you want to proceed? (Y/N).



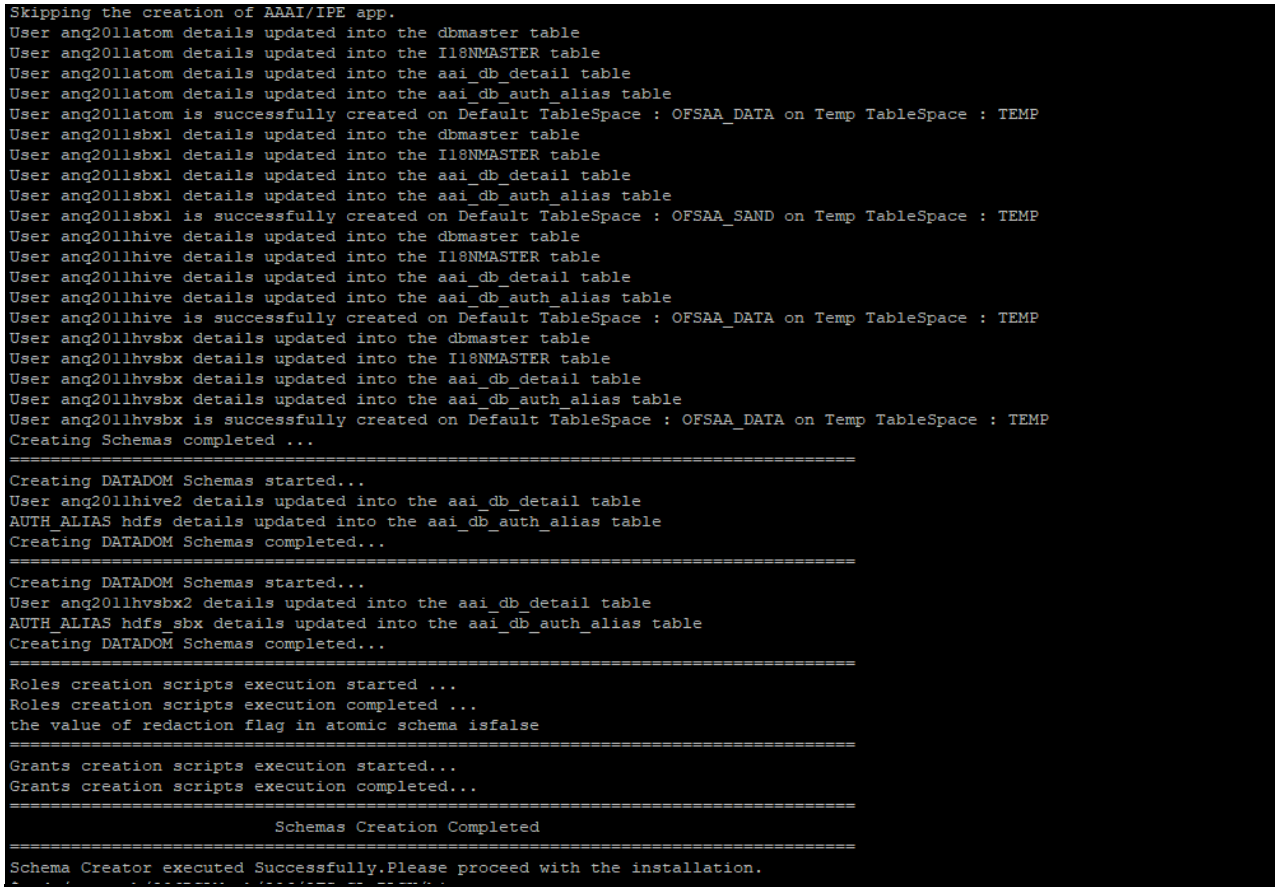
9. Enter Y/y to start the schema creation.

Or

Enter N/n if you want to quit executing the schema creation.

On successful execution of schema creator utility, the console displays the following status message:

Schema Creator executed successfully. Please proceed with the installation.



See log file in *OFS_CA_PACK/schema_creator/logs* folder for execution status. If there are any errors, contact Oracle Support.

Note: If the utility is executed without the -s option, it is mandatory to launch the OFSAA Application Pack Installer in GUI mode.

To execute the utility in OFFLINE mode with SILENT option, enter following command:

```
/osc.sh -o -s
```

Executing the Schema Creator Utility for Subsequent Application Pack

While executing the schema creator utility for subsequent Application Pack, you can choose to install the pack either on the same Information Domain/Atomic Schema or on a new Information Domain/Atomic Schema. You can execute the Schema Creator Utility either in Online or Offline Mode.

Note: OFS CA Application Pack can be installed on any Information Domain/ Atomic schema where any OFS Application Packs are installed other than OFS Behavior Detection Application Pack or OFS Compliance Regulatory Reporting Application Pack.

To execute the schema creator utility while installing OFS CA Application Pack over an existing Application Pack, follow these steps:

1. Repeat the steps 1 to 9 from the Executing the Schema Creator Utility section.

   Note: Ensure to use the same config schema user name as the previous Application Pack.

2. The utility identifies the Application Packs that are already installed on the current OFSAA setup and displays the following on console:
   - Atomic schema of the Existing Application Pack
   - Information Domain Name of the Existing Pack, and the
   - List of Installed Application Packs Execute the ./osc.sh file.

```
Validating Connection URL ...jdbc:oracle:thin:@ofss220623:1521:MEDIADB
Successfully connected to User - sys as sysdba URL - jdbc:oracle:thin:@ofss220623:1521:MEDIADB
Connection URL successfully validated...
The following Application Packs are already installed in this OFSAA setup:


dev_atm1-           INFOTR-             "OFS_TR_PACK"


You have selected to install this Application Pack on "dev_atm3" ATOMIC schema. To proceed enter (Y/y). To change the selection, enter (N/n).
n
Choose the ATOMIC schema from the below list on which you wish to install this Application Pack:


1. dev_atm1-           INFOTR-             "OFS_TR_PACK"
2. dev_atm3


Enter the option number:2
================================================================================
Generating TableSpace creation Scripts started...
Generating TableSpace creation Scripts completed...
================================================================================
Generating Schema creation scripts started...
Skipping the creation of CONFIG user dev_conf1 as OFSAAI is already installed on dev_conf1
User dev_atm3 details updated into the dbmaster table
User dev_atm3 creation script generated successfully on Default TableSpace : USERS on Temp TableSpace : TEMP
User dev_atm3 creation is skipping as the user is already created.
Generating Schema creation scripts completed...
================================================================================
Generating Roles creation Scripts started...
Generating Roles creation Scripts completed...
================================================================================
Generating Grants creation scripts started...
Generating Grants creation scripts completed...
================================================================================
                        Generating Schema Creation Scripts Completed
================================================================================
Schema Creator executed Successfully.Please execute /scratch/ofsaadb/OFS_AAAI_PACK/schema_creator/sysdba_output_scripts.sql before proceeding with the installation.
$
```

3. Select the Atomic User, on which you want to install the Application Pack.

   On successful execution or schema creator utility, the following message is displayed:

   Schemas Creation Completed.

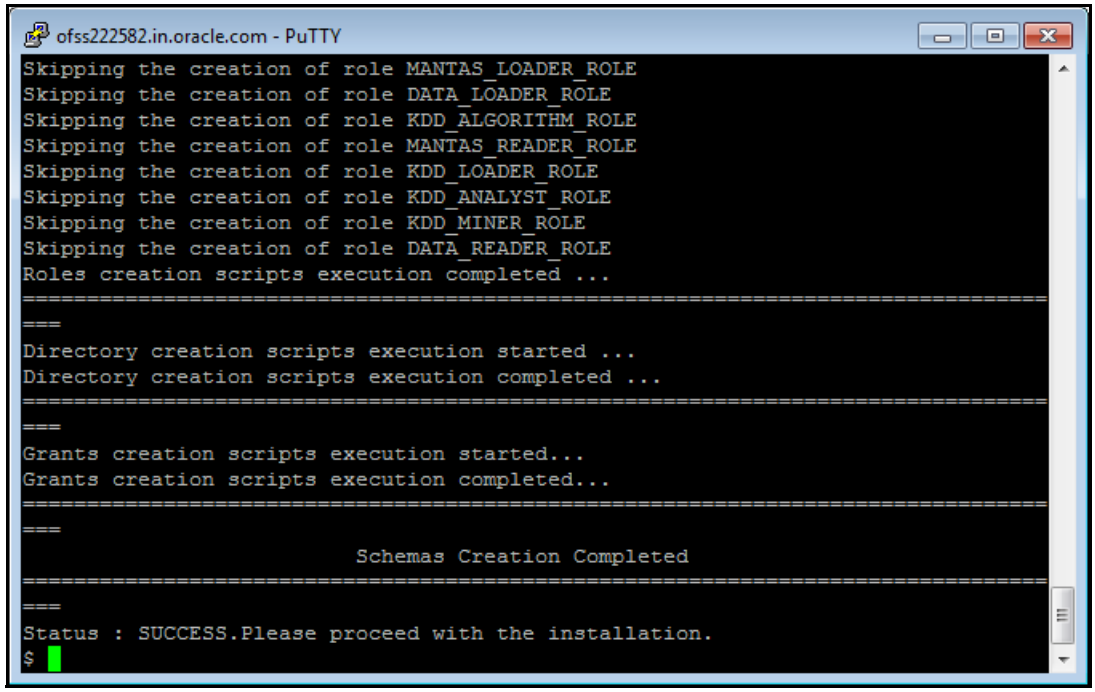
See the log file in *OFS_CA_PACK/schema_creator/logs* folder for execution status.

See the log sysdba_output_scripts.log file for execution status, if executed in offline mode. This log would be empty if there are no errors in the execution.

If there are any errors, contact Oracle Support.

Verifying the Log File

If schema creation is successful, the console would display an appropriate message.



If the schema creation runs into errors, see the log files:

<<OFSCA Installer folder>>/<<OFS_CA_PACK>>/schema_creator/logs/ and <<OFS_CA>>_OSC_<timestamp>.log for further details.

You may contact Oracle support anytime for assistance.

Installing the OFS CA Application Pack

OFA CA application pack can be installed in Hybrid and Standard modes.

Standard Installation: This is used for RDBMS Only installation using the standard template.

Hybrid Installation: Hybrid installation files are used for HADOOP additional capability. The hybrid files are provided as template which needs to be changed to proper extension by removing 'template'. After changing file name, the values need to be provided as mentioned in the following table.

The following table gives the list of different files to be used for both Standard and Hybrid installation methods:

Type of File	Standard Installation	Hybrid Installation
Schema creator configuration	■ OFS_CA_CFG.dat ■ OFS_CA_SCHEMA_IN.xml	■ OFS_CA_CFG.DAT.HYBRID.template ■ OFS_CA_SCHEMA_BIGDATA_IN.XML.HYBRID.template
Pack Installer Configuration files under OFS_CA	■ Silent.template ■ default.properties.template	■ Silent.template.HYBRID.template ■ default.properties.HYBRID.template
Pack Installer Configuration files under OFS_CA_PACK	■ OFS_CA_PACK.XML.template	■ OFS_CA_PACK.XML.HYBRID.template

Follow the instructions in this section to install the OFS CA Application Pack depending on the mode of installation.

Installing OFS CA Pack

Refer to the following instructions to download, extract, install, and configure this Interim Release.

1. Ensure that `SYS.DBMS_DATA_MINING` privilege is available to the atomic schema if not already provided. This is to run statistical models through Modelling Framework.
2. Login to https://support.oracle.com/ and search for **28391701** under the **Patches & Updates** tab.
3. Download the OFS Customer Analytics Application Pack v8.0.6.0.0 archive file and copy it to your OFSAA server in Binary mode.

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

4. Log in to the system as non-root user.
5. Assign WRITE permission to the files/ folders such as commonscripts, EXEWebService, ficapp, ficweb, and ficdb in the *$FIC_HOME* folder by executing the command:

   ```
   chmod -R 755 $FIC_HOME
   ```

6. Execute the user .profile.

7. If you have Unzip utility, skip to the next step. Download the Unzip utility (OS specific) unzip_<os>.Z from the location https://updates.oracle.com/unzips/unzips.html and copy it in Binary mode to the directory that is included in your PATH variable, typically *$HOME* path or directory in which you have copied the 8.0.6.0.0 release.
   - Uncompress the unzip installer file using the command:

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

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

   - Give EXECUTE permission to the file using the command:

     ```
     chmod 755 OFS_CA_80600_<OperatingSystem>.zip
     ```

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

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

   Note: The above "-a" option is mandatory to unzip the archive file. For example: unzip_aix -a OFS_CA_80600_<OperatingSystem>.zip

9. Pre-Installation XML/ File Populations:

   Before Proceeding to installation, we need to populate following files with pre-defined values.

   - `OFSAAI_InstallConfig.xml` (Location: *OFS_CA_PACK/OFS_AAI/conf*). For more information, see Configuring OFSAAI_InstallConfig.xml File section.

     Note: If value for HTTPS_ENABLE is set to 1, ensure you have a valid certificate available from a trusted CA and the same is configured on your web application server.

   - `SILENT.props` File. (Location: *OFS_CA_PACK/OFS_CA/conf*)

     Note: The file name will be `SILENT.template` in case of the standard installer and it has to be renamed as `SILENT.props`.

     The file name will be `Silent.template.HYBRID.template` in case of the hybrid installer and it has to be renamed as `SILENT.props`.

Do not install the new applications in the same segment if the pre-installed applications use run management.

Property Name	Description of Property	Permissible Values	Comments
UPLOAD_MODEL	whether you want to perform Model Upload	0 = No 1 = yes	Mandatory
MODEL_TYPE	Released data model or Customized data model	0 = released 1 = customized	# Mandatory only in the case of uploading the data model
DATAMODEL	the path for the customized data model	Not Applicable	# Mandatory only in the case of uploading the customized data model # Option selected for MODEL_TYPE=1
DM_DIRECTORY	the file name for the customized data model	Not Applicable	# Mandatory only in the case of uploading the customized data model # Option selected for MODEL_TYPE=1

To access the respective Business Intelligence Analytics Application, update the OBIEE URL in the `silent.props` file in *<INSTALLER_HOME>/OFS_CA/conf/* as given the following example:

```
# Specify the Host Name of the OBIEE Server

OBI_HOST=<<hostname>>

# Specify the Port Number of the OBIEE Server

OBI_PORT=<<port>>

# Specify the Context Name of the OBIEE Server

OBI_CONTEXT=<<context name>>

OBI_PROTOCOL=<<protocol like http>>
```

10. For Hybrid installation, refer to the section Prerequisites for Hybrid Installation for updating the `silent.props` file.
11. The `OFS_CA_PACK.xml` file holds details on the various products that are packaged together in CA Application Pack.

    This section details the various tags/ parameters available in the file and the values that need to be updated. Prior to installing the CA Application Pack, it is mandatory to update this file. For more information, see Configuring OFS_CA_PACK.xml.
12. Navigate to the folder path: *OFS_CA_Pack/bin/*.
13. Execute the `setup.sh` file using the following command:

    ```
    ./setup.sh SILENT
    ```
14. Restart servers.
15. Install the following AAI maintenance level patches. Refer to the Readme available with the patch for further instructions on installing the patch.:

- **28033370**
- **28622102**

16. Perform steps mentioned in the Post Installation Configuration section.
17. For enabling Transparent Data Encryption (TDE), see TDE, Data Redaction and the Corresponding Settings in OFSAA.
18. For enabling Data Redaction, see Data Redaction section under Data Security and Data Privacy chapter in OFS Analytical Applications Infrastructure Administration Guide 8.0.6.0.0.
19. For information on Data Protection Implementation, see Data Protection Implementation in OFSAA.

Verifying the Log File

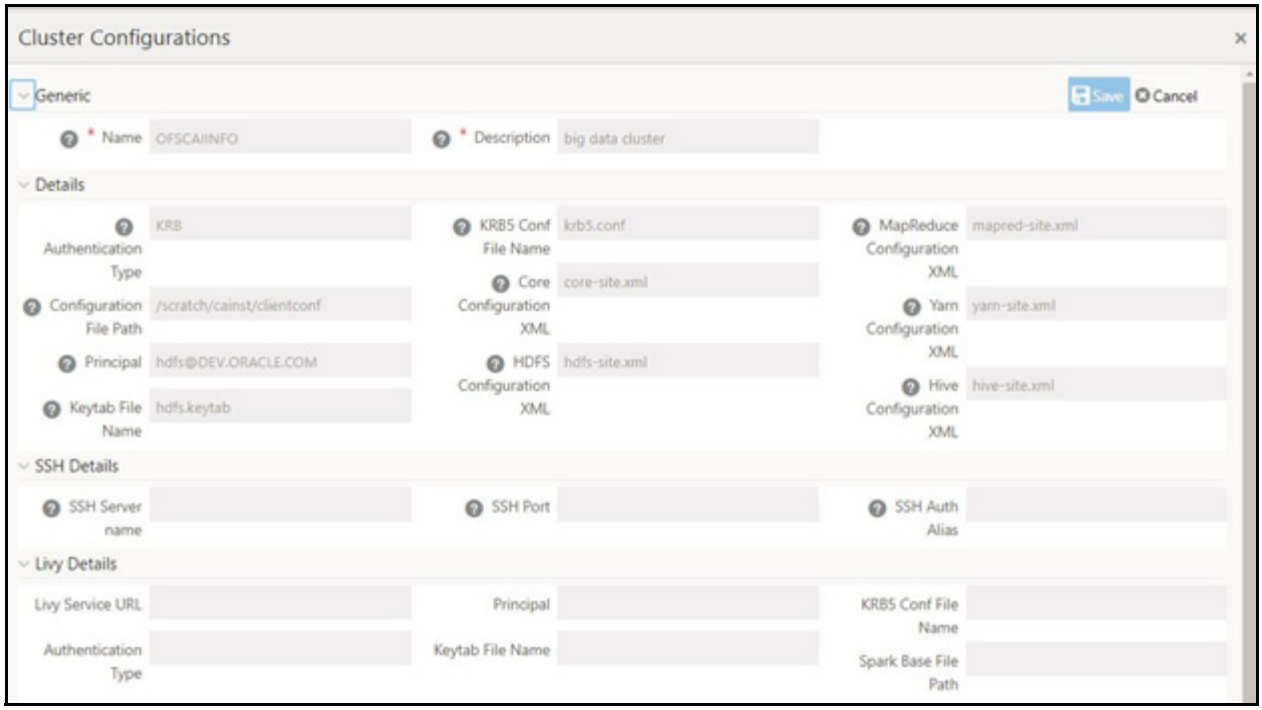
See the following logs files for more information:

- See the `OFS_CA_installation.log` located at *`OFS_CA_PACK/OFS_CA/logs`* folder for OFS CA Application Pack installation log file.
- See the `Pack_Install.log` located at *`OFS_CA_PACK/logs/`* folder for OFS CA Application Pack installation log file.
- See the log file(s) located at *`OFS_CA_PACK/OFS_AAI/logs/`* folder for Infrastructure installation log.
- See the `OFSAAInfrastucture_Install.log` located at *`$FIC_HOME`* folder for Infrastructure installation log.

Registering Clusters

Use the following procedure to register the clusters:

1. Select Big Data Application (Financial Services Retail Customer analytics on big data).
2. Select Data management framework, data management tools and then DMT configuration.
3. Click **Register Cluster**.
4. In Cluster Click **Add**, create cluster as shown in the below image and **Save**.



Known Issues

1. When installing multiple packs on a single environment, that is, OFS Pack on OFS Customer Analytics Pack or OFS Customer Analytics Pack on OFS Pack, the installation log of the latter pack will have the following SQL script error:

   Error:ORA-00904: "N_PROJ_DATE_SKEY": invalid identifier

   This is an error due to redundancy of a script when installing two packs on the same setup. This error will have no bearing on the functionality of the applications and needs to be ignored.

CHAPTER 5 – POST INSTALLATION CONFIGURATION

After successfully installing the Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack, follow the post installation steps mentioned below.

This chapter includes the following topics:

Note: Ensure that to clear the application cache prior to the deployment of Application Pack Web Archive. This is applicable to all Web Servers (WebSphere, WebLogic, Tomcat). For more information, See Clearing Application Cache section.

Configure Resource Reference

Configure the resource reference in the Web Application Server configured for OFSAA Applications. See Configuring Resource Reference in Web Application Servers for details on configuring the resource reference in WebSphere, WebLogic, and Tomcat Application Servers.

Start/Stop OFSAA Infrastructure Services

Start the OFSAA Infrastructure Services prior to deployment or accessing the OFSAA Applications.

This chapter details on how to start and stop OFSAA Infrastructure services. This section includes the following sub-sections:

- Starting Infrastructure Services
- Starting Web Application Servers

Starting Infrastructure Services

Once the installation of Infrastructure has been completed successfully and the post-installation steps are completed, the servers must be started. Log on to each machine and run the .profile file. All servers mentioned must be started from the same shell encoding. The servers mentioned below are dependent on each other. It is mandatory to maintain the order in which the servers are started. Allow each of the servers to initialize completely before starting the next server.

1. On the machine in which Infrastructure Application components have been installed, navigate to *$FIC_APP_HOME/common/FICServer/bin* and execute the following command to start the Infrastructure Server.

   ```
   ./startofsaai.sh
   ```

   Note: You can also start the Infrastructure Server by executing the command "nohup ./ startofsaai.sh &". Starting the process using "nohup" and "&" will return the command prompt without having to wait till the process completes. However, this command cannot be used when you are starting the server for the first time or starting after changing user password in the configuration database schema.You can also start the Infrastructure Server by executing the command "nohup ./ startofsaai.sh &". Starting the process using "nohup" and "&" will return the command prompt without having to wait till the process completes. However, this command cannot be used when you are starting the server after changing user password in the Configuration database schema.

2. Start ICC server:
   - On the machine in which Infrastructure default Application components have been installed, navigate to *$FIC_HOME/ficapp/icc/bin* folder.
   - Execute the command:

     ```
     ./iccserver.sh
     ```

     Note: Only Infrastructure Default Application Server would hold ICC component.

3. Stopping Infrastructure Services:
   - On the machine on which Infrastructure Database components have been installed, navigate to *$FIC_DB_HOME/bin* folder and execute the command to start "Agent server":

     ```
     ./agentstartup.sh
     ```

   Or

- Start Back-end services using the command:

  ```
  nohup ./agentstartup.sh &
  ```

  Note: This agent internally starts the Router, Message Server, OLAP data server and AM services.

Starting Web Application Servers

Start the Web Application Server depending on the type from the following table.

Start up Option	Description
Starting WebSphere profile	On the machine in which Web sphere is installed, navigate to [Webshpere_Install_Directory] /AppServer/<profiles>/<profile name>/bin and execute the command: `./startServer.sh server1`
Starting WebLogic Domain	On the machine in which WebLogic is installed navigate to <WebLogic Installation directory>/user_projects/domains/<domain name>/bin and execute the command: startWebLogic.sh -d64 **Note:** If WebLogic is already running, access the WebLogic Admin Console. Stop and start the application <context name>.ear.
Starting Tomcat Application	On the machine in which Tomcat is installed, navigate to <Tomcat_Install_ Directory>/bin and execute the command: `./catalina.sh run`

Stopping Infrastructure Services

To stop Infrastructure services:

1. On the machine in which Infrastructure Application components have been installed, navigate to *$FIC_APP_HOME/common/FICServer/bin* folder and execute the command:

   ```
   ./stopofsaai.sh
   ```

2. To stop ICC server, on the machine in which Infrastructure default Application components have been installed, navigate to *$FIC_HOME/ficapp/icc/bin* folder and execute the command:

   ```
   ./iccservershutdown.sh
   ```

   Only Infrastructure Default Application Server would hold ICC component.

3. To stop Back-end server, on the machine in which Infrastructure database components have been installed, navigate to *$FIC_DB_HOME/bin* folder and execute the command:

   ```
   ./agentshutdown.sh
   ```

Add TNS entries in TNSNAMES.ORA file

Add TNS entries in the `tnsnames.ora` file, for every schema created for the Application Pack:

To find the tnsname for the entries, follow these steps:

1. Login to the application using System Administrator privileges.
2. Navigate to System Configuration & Identity Management tab.
3. Click Administration and Configuration >> System Configuration >> Database Details.
4. Expand the drop-down list for Name to get the list of TNS entry names.

Alternatively, you can connect to the CONFIG schema and execute the below query:

```
select dbname from db_master where dbname !='CONFIG'
```

Configuring Web Server

This section includes the following topics:

- Configuring Web Server
- Configuring Web Application Server

Configuring Web Server

This step assumes an installation of a Web Server exists as per the prerequisites.

Refer the product specific Installation Guide/ Configuration Guide to install/ configure the Web Server. If an installation already exists, skip and proceed to the next step.

Note: Make a note of the IP Address/ Host-name and Port of the web server. This information is required during the installation process.

See Oracle Financial Services Analytical Applications Infrastructure Security Guide for additional information on securely configuring your Web Server.

Ensure to enable sticky session/ affinity session configuration on the web server. See the respective product specific Configuration Guide for more details. Additionally, you also need to enable the sticky session/ affinity session configuration at Load Balancer level if you have configured a Load Balancer in front of the web server(s).

Configuring Web Application Server

This step assumes an installation of a web application server exists as per the prerequisites. To configure the Web Application Server for OFSAA Deployment refer the sections below.

This section includes the following topics:

- Configuring WebSphere Application Server for Application Deployment
- Configuring WebLogic for Application Deployment
- Configuring Apache Tomcat Server for Application Deployment

---

Note: Make a note of the IP Address/ Host-name and Port of the web application server. This information is required during the installation process (required if Web Server is not configured).

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

See Oracle Financial Services Analytical Applications Infrastructure Security Guide for additional information on securely configuring your Web Server.

Configuring WebSphere Application Server for Application Deployment

You can deploy multiple OFSAA applications on different profiles of a WebSphere application server. To create multiple WebSphere "Profiles" in a stand-alone server, use the command line option as explained below. A profile is the set of files that define the runtime environment. At least one profile must exist to run WebSphere Application Server.

This section includes the following topics:

- Creating a New Profile in WebSphere
- Managing IBM WebSphere SDK Java Technology Edition Versions
- Managing Applications in WebSphere
- Deleting WebSphere Profiles
- Configuring WebSphere Shared Library to Support Jersey 2x and Jackson 2.9x Libraries
- WebSphere HTTPS Configuration
- WebSphere Memory Settings
- Configuring WebSphere for REST Services Authorization
- Configuring Application Security in WebSphere

Creating a New Profile in WebSphere

The Profile is created in WebSphere through command line using the manageprofiles.sh which resides in <WebSphere Install directory>/AppServer/bin folder.

The command to create a profile without admin security through command line is as follows:

```
"manageprofiles.sh -create -profileName <profile> -profilePath <profile_path> -
templatePath <template_path> -nodeName <node_name> -cellName <cell_name> -hostName
<host_name>"
```

Example:

```
$usr/home>./manageprofiles.sh -create -profileName mockaix -profilePath/websphere/
webs64/Appserver/profiles/mockaix -templatePath/websphere/webs64/Appserver/
profileTemplates/default -nodeName ipa020dorNode04 - cellName ipa020dorNode04Cell -
hostName ipa020dor
```

The command to create a profile with admin security through command line is as follows:

```
"manageprofiles.sh -create -profileName <profile> -profilePath <profile_path> -
templatePath <template_path> -nodeName <node_name> -cellName <cell_name> -hostName
<host_name> -enableAdminSecurity true -adminUserName <Admin User Name> -adminPassword <
Admin User Password> -samplespassword <sample User Password>"
```

Example:

```
$usr/home>./manageprofiles.sh -create -profileName mockaix -profilePath/websphere/
webs64/Appserver/profiles/mockaix -templatePath/websphere/webs64/Appserver/
profileTemplates/default -nodeName ipa020dorNode04 -cellName ipa020dorNode04Cell -
hostName ipa020dor -enableAdminSecurity true -adminUserName ofsaai -adminPassword ofsaai
-samplespassword ofsaai"
```

Note: While using the manageprofiles.sh command to create a New Profile in WebSphere, you can also use "-validatePorts" to validate if the specified ports are not reserved or in use. Additionally, you can specify new ports with "-startingPort <base port>" which specifies the starting port number to generate and assign all ports for the profile. For more information on using these ports, see WebSphere manageprofiles command.

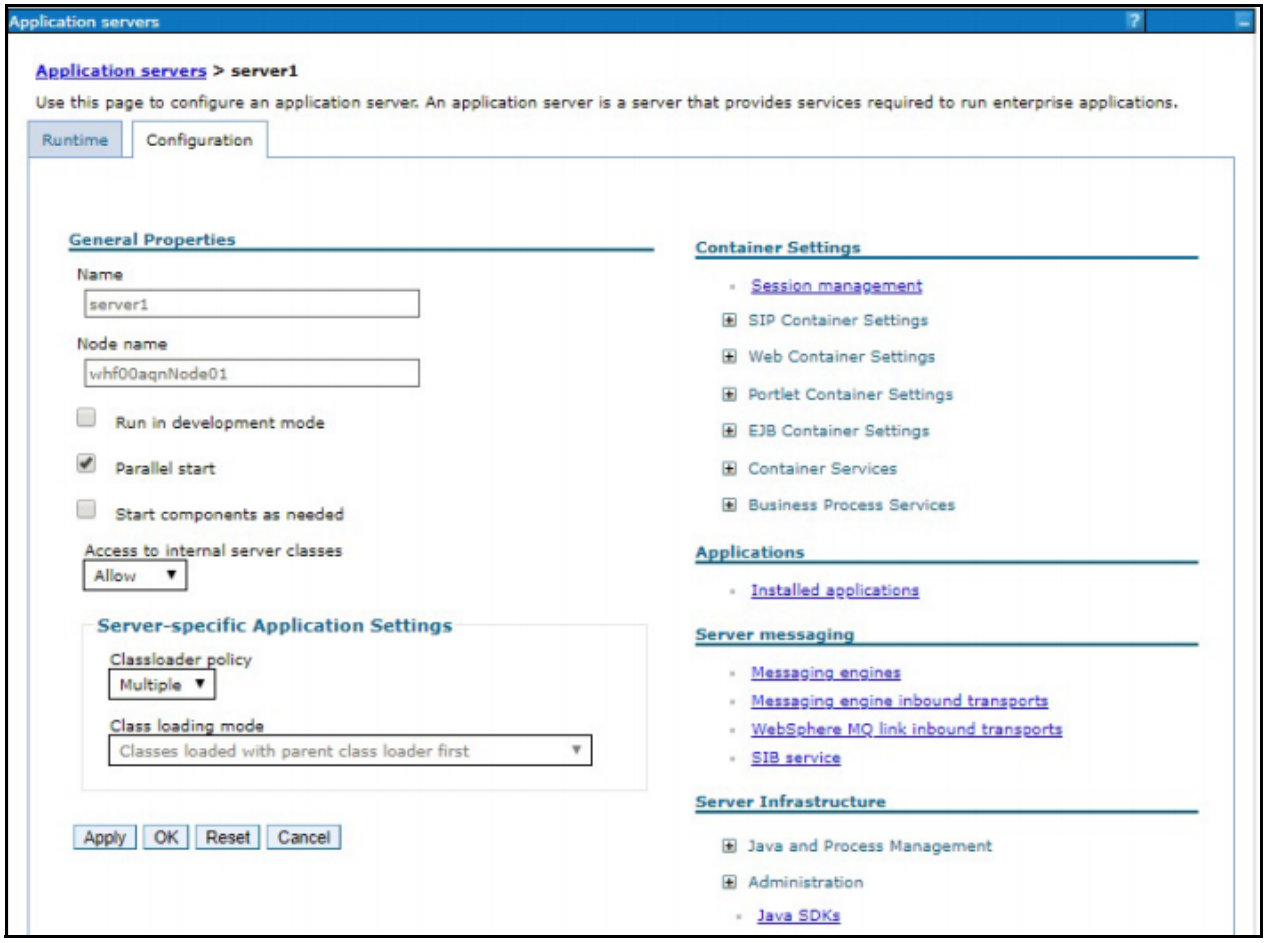
Managing IBM WebSphere SDK Java Technology Edition Versions

By default, WebSphere Application Server V8.5.5.X uses the Java 6.0 SDK. You must upgrade to Java 7.X SDK or JAVA 8.X SDK.

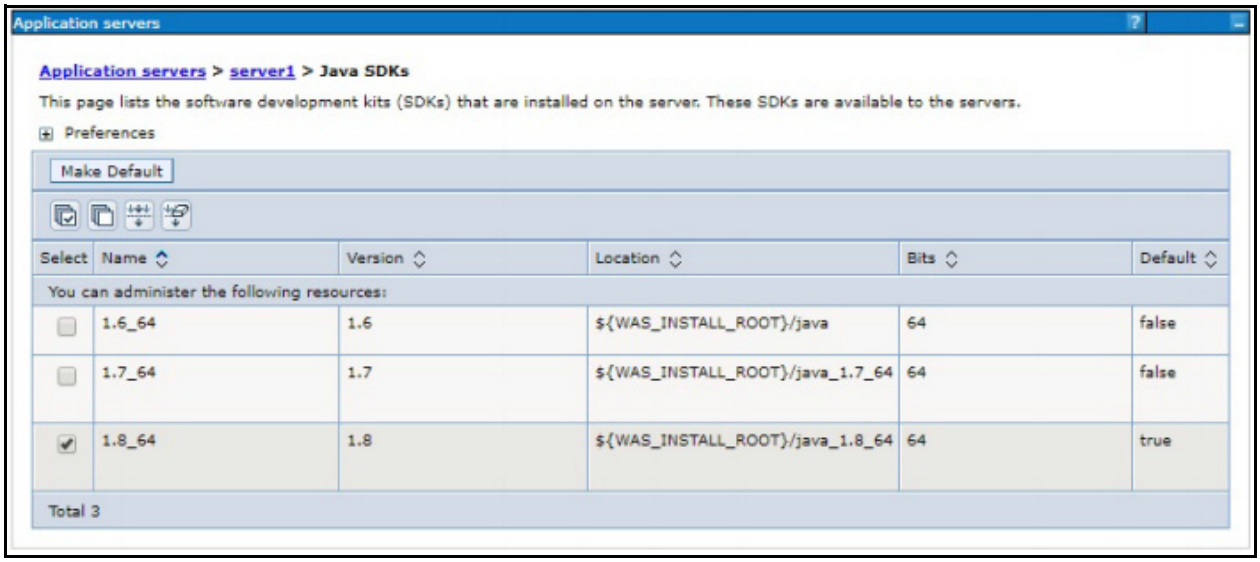
Prerequisites: Install the IBM WebSphere SDK Java Technology Edition Versions 1.7.X_64 or 1.8.X_64.

Perform the following steps to upgrade to Java 7.X SDK or JAVA 8.X SDK:

1. Enter the WebSphere URL in the format http://HOST_NAME:PORT_NUMBER/ibm/console (use https if SSL is enabled.). For example, http://192.168.1.0:9000/ibm/console.
2. Login with your administrator user ID and password.
3. From the LHS menu, click **Servers** to expand and view the menu.
4. Click **Server Types** to expand the menu further and then click **WebSphere Enterprise Application Servers** to view the Application servers window.
5. On Application servers window, click the required Application Server link. For example, server1 in the following illustration:



6. Click **Java SDKs** link from Server Infrastructure to view the list of Java SDKs.



7. Select either **1.7_64** or **1.8_64** based on the JVM version with which you plan to install OFSAA or have installed with.
8. Click **Make Default** button and save to master repository.
9. Restart the WebSphere Application Server to apply the changes to the IBM application profile.

Managing Applications in WebSphere

To manage the installed applications in WebSphere, do the following:

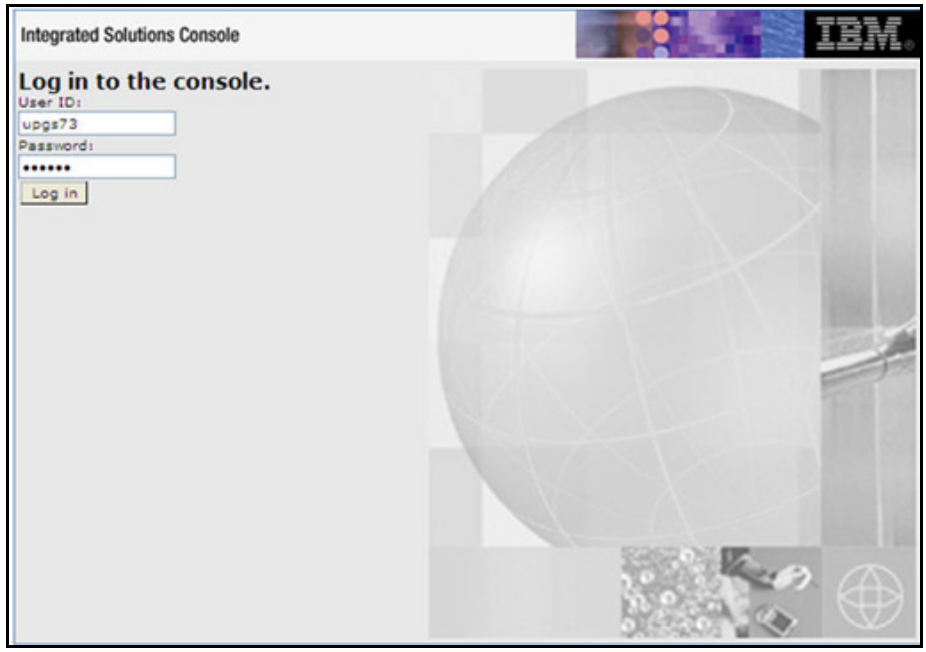
1. Open the administrator console using the following URL:

   `http://<ipaddress>:<Administrative Console Port>/ibm/console`

   Example: `http://10.111.222.333:9003/ibm/console` (https if SSL is enabled)

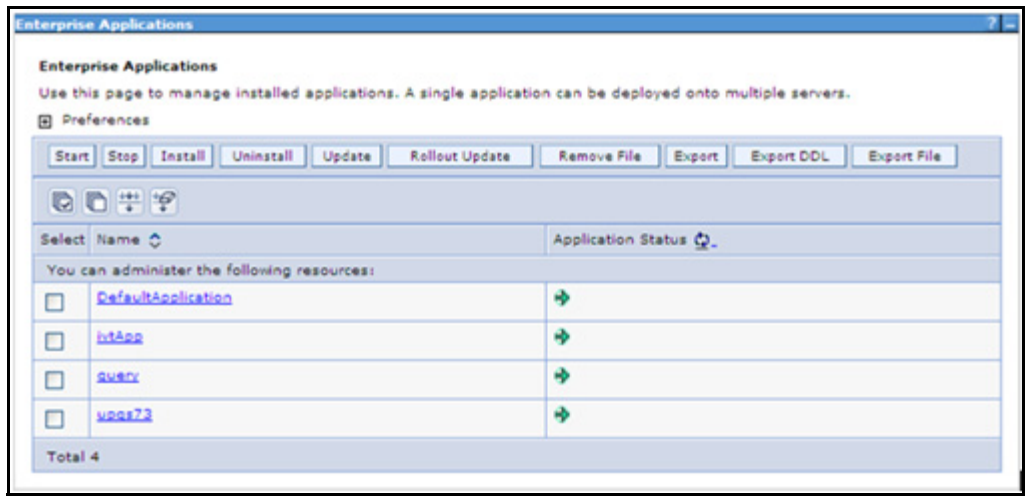
   Note: Administrative Console Port value is available in serverindex.xml file within *`<WebSphere Profile Directory>/config/cells/<Node Cell>/nodes/<Node Name>`* directory.

   The Integrated Solutions Console Login window is displayed.



2. Log on with the **User ID** provided with the admin rights.
3. From the LHS menu, expand the **Applications > Application Type> WebSphere Enterprise Applications**.

The Enterprise Applications screen is displayed.



4. This Enterprise Applications screen helps you to:

- Install new application
- Un-install existing applications
- Start or Stop the installed applications

Deleting WebSphere Profiles

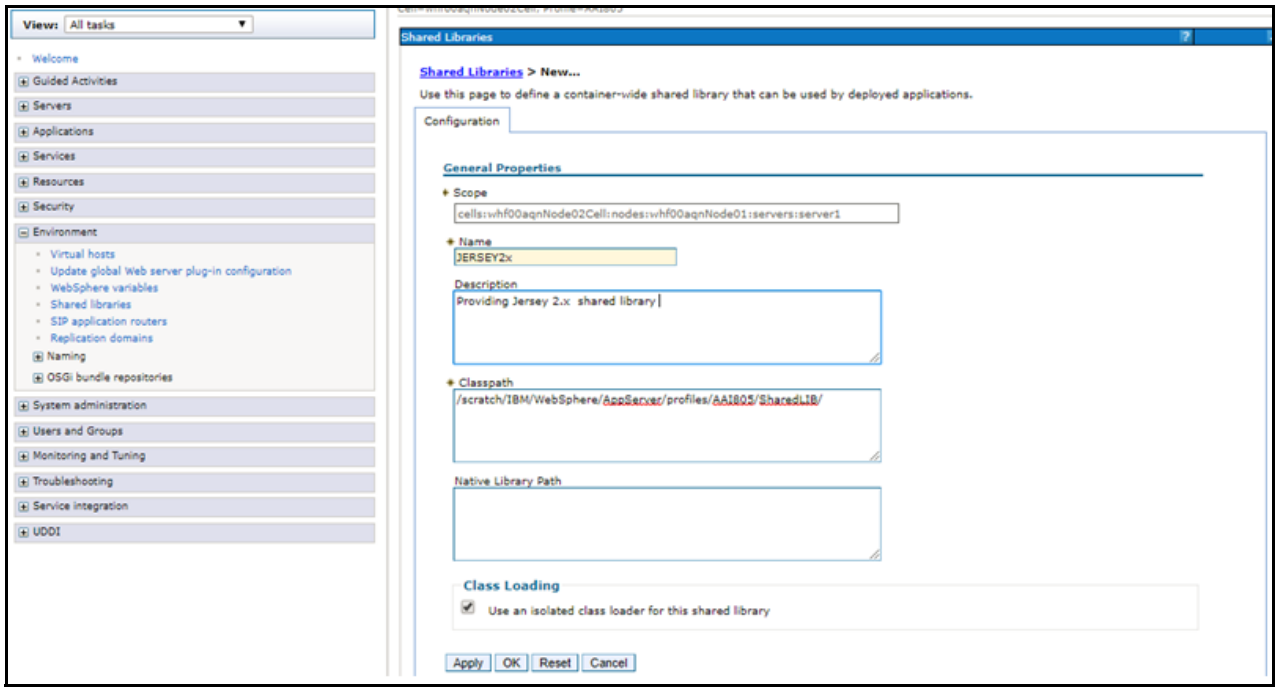
To delete a WebSphere profile, do the following:

1. Select the check box adjacent to the required application and click Stop.
2. Stop the WebSphere profile to be deleted.
3. Navigate to WebSphere directory:
   <WebSphere_Installation_Directory>/AppServer/bin/
4. Execute the command:
   `manageprofiles.sh -delete -profileName <profile_name>`
5. Delete profile folder.
   Example: *<WebSphere_Installation_Directory>/AppServer/profiles/<profile_name>*
6. Execute the command:
   `manageprofiles.sh -validateAndUpdateRegistry`

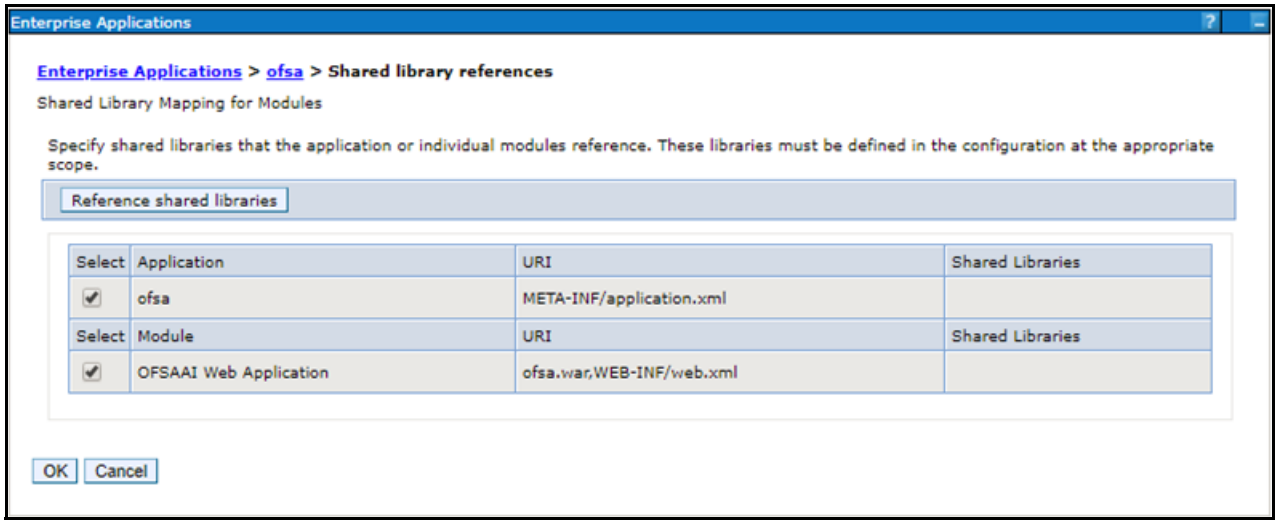
Configuring WebSphere Shared Library to Support Jersey 2x and Jackson 2.9x Libraries

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

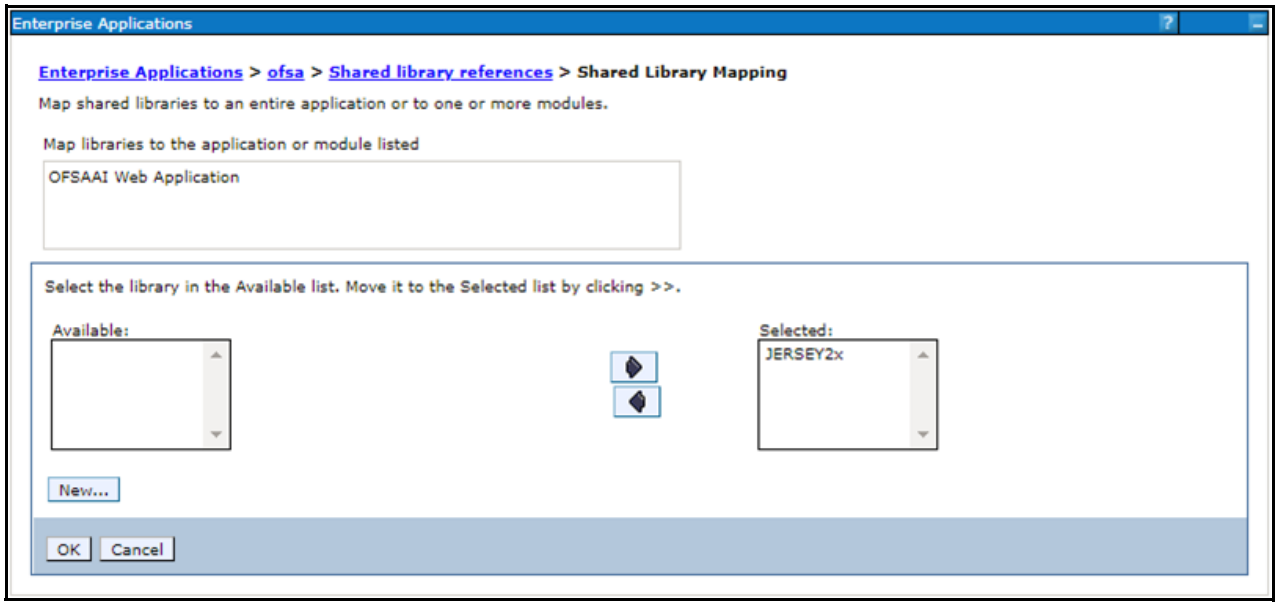
1. Click **Environment** from the menu on the left to expand and view the list. Click **Shared Libraries** to open the Shared Libraries window.



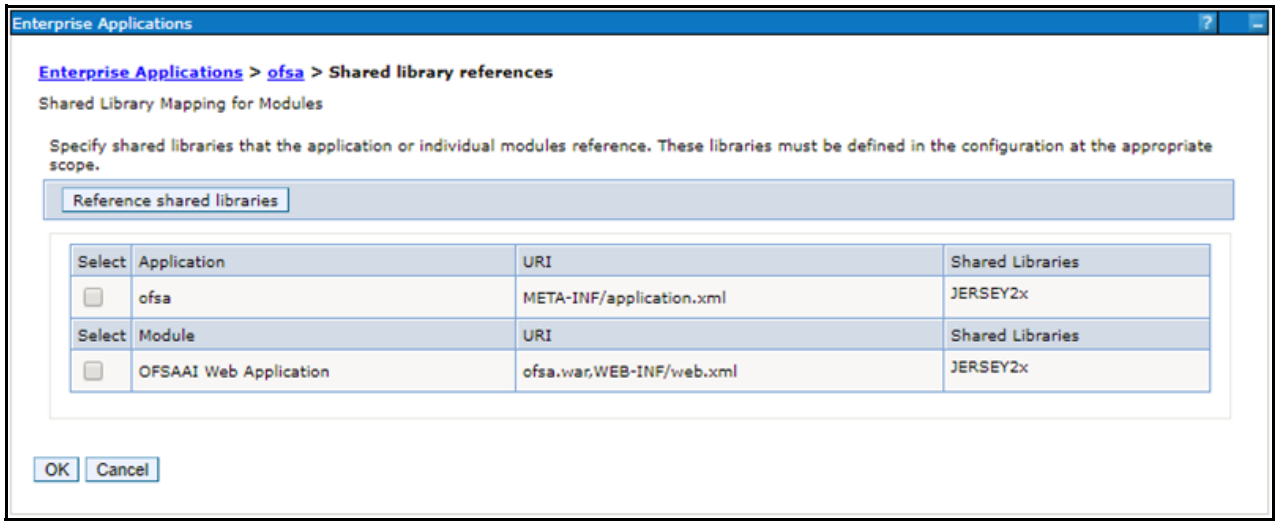
2. Enter details as shown in the following:
   a. **Name**: Enter a unique identifiable name.
   b. **Description**: Enter a valid description.
   c. **Classpath**: Enter the absolute path where the JARs related to Jersey 2.x and Jackson 2.9x are copied. These jars are available in the <OFSAA_HOME>/utility/externallib/WEB-INF/lib directory after creation of the EAR file.
3. Select **Use an isolated class loader for this library**.
4. Click **OK** to save to master configuration.
5. Select the application or module and map the shared libraries. Click **OK**. In the following illustration, ofsa is selected.



6. From the Shared Library Mapping window, move the required shared libraries from **Available** to **Selected**. In the following illustration, JERSEY2x is selected.



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



9. Disable the built-in JAX-RS via JVM property.
   a. Go to WebSphere admin console in **Servers > WebSphere Application Servers > yourServerName**.
   b. In **Server Infrastructure** section, go to **Java and Process Management > Process definition > Java Virtual Machine > Custom properties**.
   c. Add the following property:

      `com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine=true`
10. Restart the application.

WebSphere HTTPS Configuration

Following are the steps for configuring an HTTPS Transport on WebSphere:

1. Create a profile using the Profile Creation Wizard in WebSphere.
2. Note down the https port specified during this process and use the same as servlet port or web server port during OFSAAI installation.

   To enable https configuration on Infrastructure, assign value 1 to "`HTTPS_ENABLE`" in `OFSAAI_InstallConfig.xml` for SILENT mode OFSAAI installation.

WebSphere Memory Settings

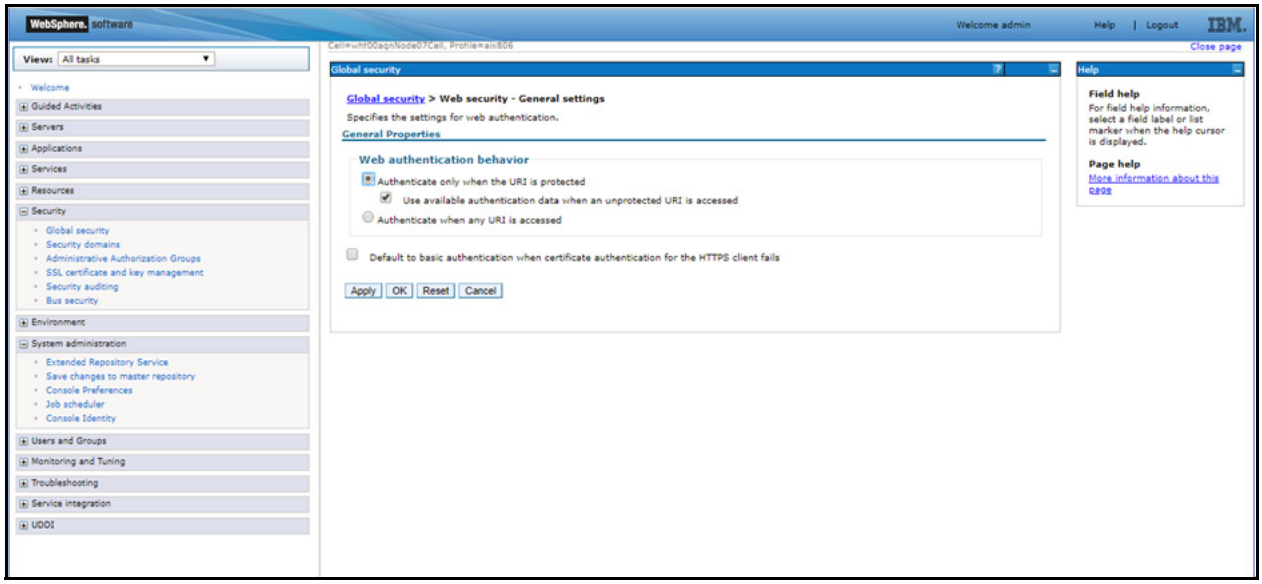
To configure the WebSphere Memory Settings:

1. Navigate to Websphere applications server > Application servers > server1 > Process definition > Java Virtual Machine.
2. Change the memory setting for Java Heap:
   - Initial heap size = 512
   - Maximum heap size = 3072

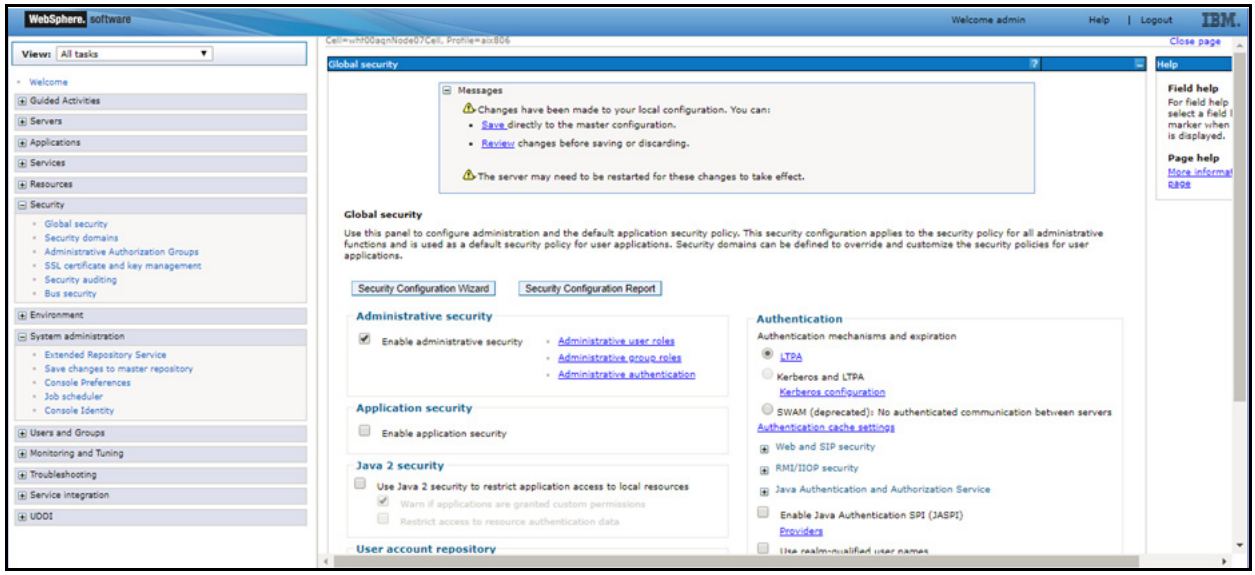
Configuring WebSphere for REST Services Authorization

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 check box.
4. Click OK.



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

Configuring Application Security in WebSphere

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

Configuring WebLogic for Application Deployment

You can deploy multiple Infrastructure applications on different domains of a stand-alone WebLogic application server. To create multiple WebLogic "Domains" in a stand-alone server you can use the Domain Creation wizard. A domain is the set of files that define the runtime environment. At least one domain must exist to run WebLogic Application Server.

Note: For deployment on Oracle WebLogic Server 12.1.3+ (64 bit) with Java 8, download and install patch 18729264 from My Oracle Support.

This section includes the following topics:

- Creating Domain in WebLogic Server
- Delete Domain in WebLogic
- WebLogic Memory Settings
- Configuring WebLogic for REST Services Authorization

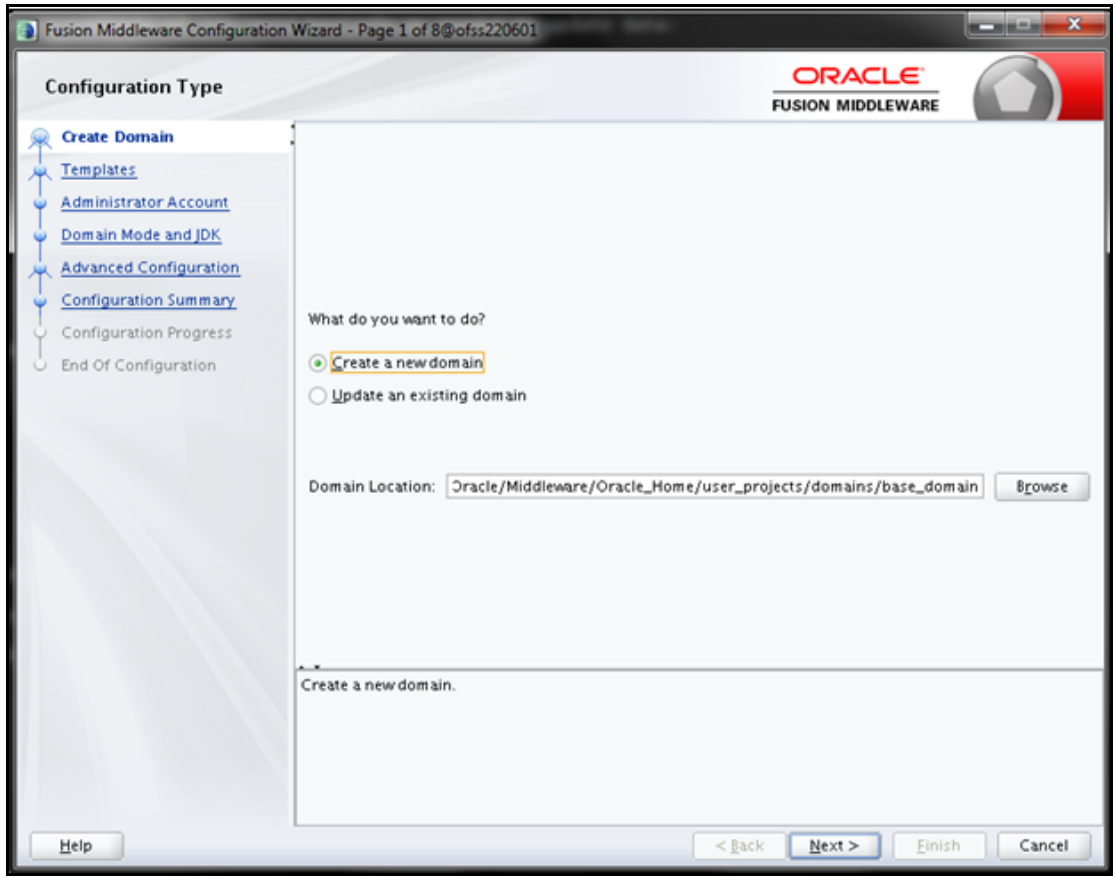
Creating Domain in WebLogic Server

To create a new domain using Configuration Wizard in WebLogic, do the following:

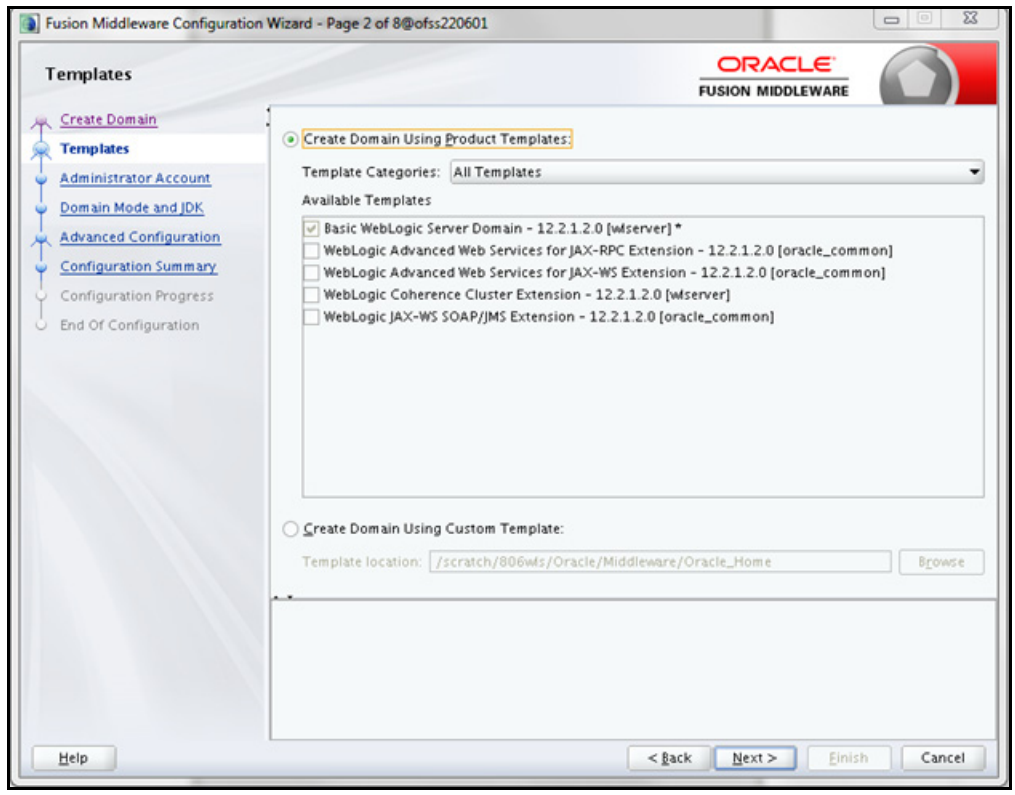
1. Navigate to the directory <WLS_HOME>/wlserver/common/bin and execute the command:

   ```
   ./config.sh
   ```

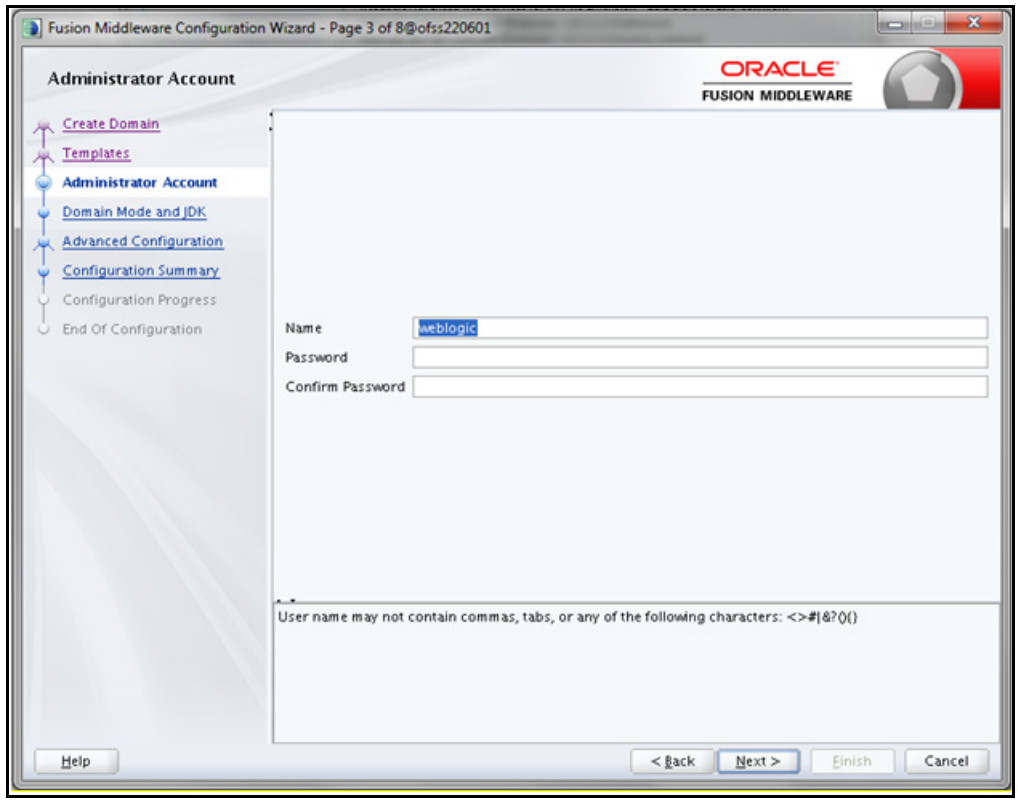
The Configuration Type window of the Configuration Wizard is displayed.



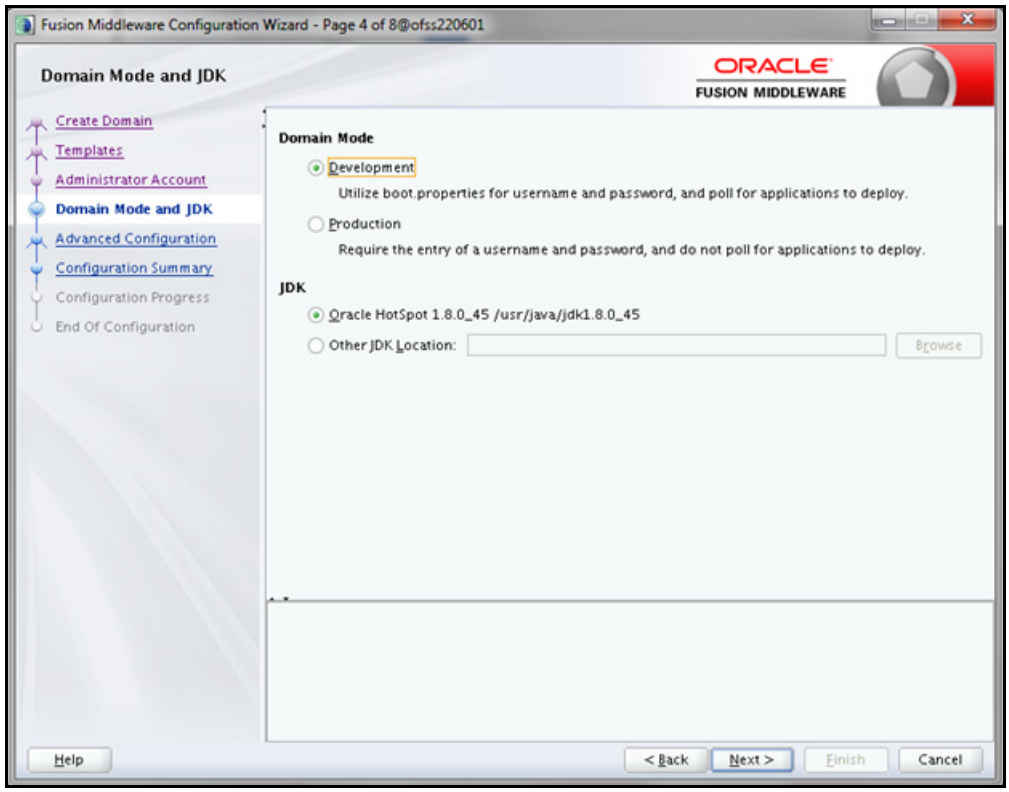
2. Select **Create a new domain** option and click **Next** to display the **Templates** window.



3. Select the **Create Domain Using Product Templates** option and click **Next** to display the **Administrator Account** window.

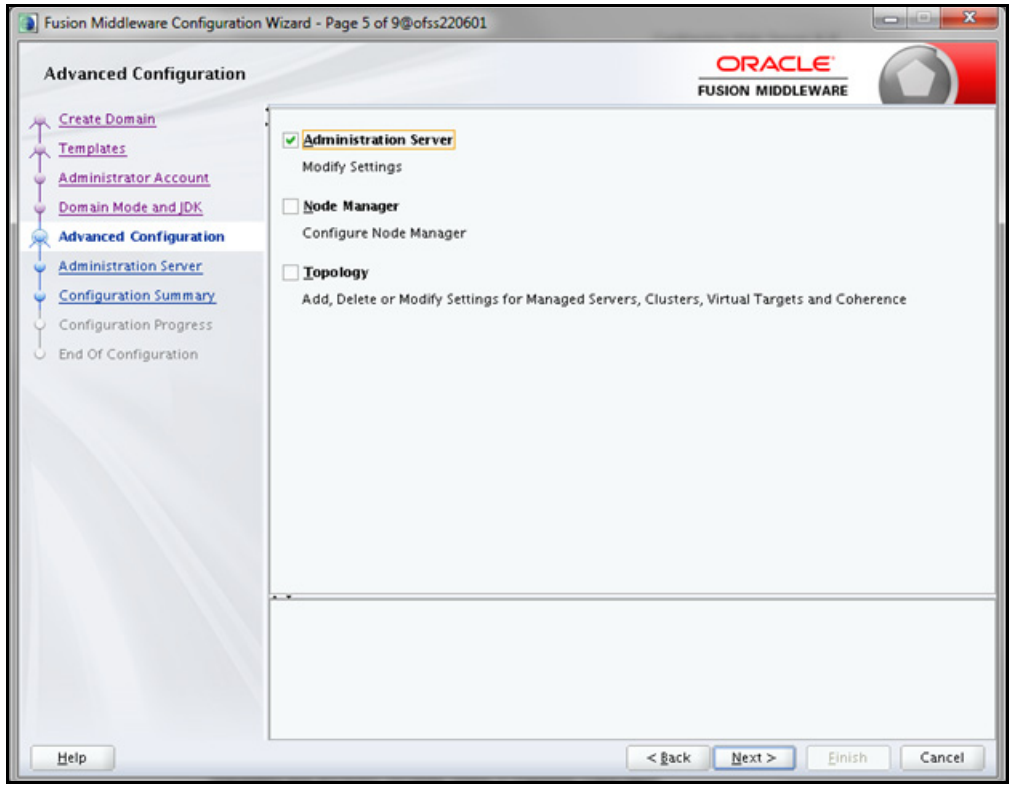


4. Enter the user name to be assigned to the administrator, the password and confirm the password. Click **Next** to display **Domain Mode and JDK** window is displayed.

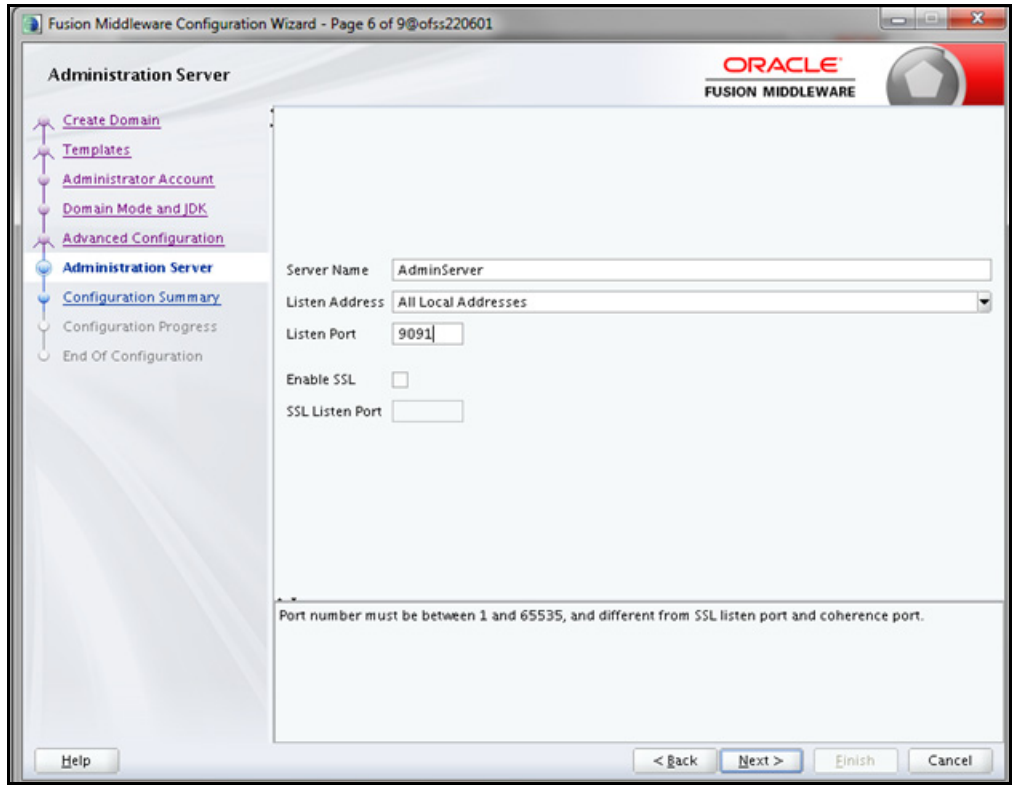


5. Select from the following options:
   - In the **Domain Mode** section, select the required mode (Development or Production).
   - In the **JDK** section, select the required option. If you select **Other JDK Location**, click **Browse**, navigate to the JDK location, and select.

Click **Next** to display the **Advanced Configuration** window.



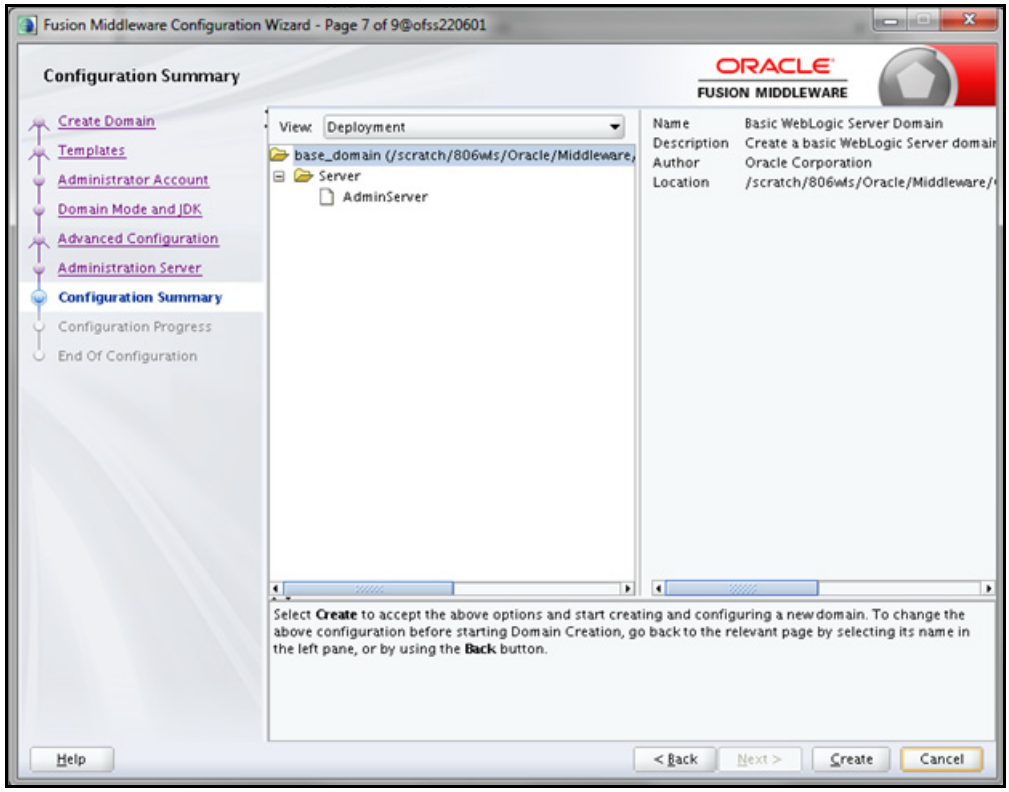
6. Select **Administration Server**. A WebLogic Server domain must have an Administration Server. You can also select **Manages Servers**, **Clusters and Machines** and **RDBMS Security Store**, if required. Click **Next** to display the **Administration Server** window.



7. Enter Administration Server details such as the **Server Name**, **Listen address**, **Listen Port**, **Enable SSL** (for secure login using https, select this check box), and SSL listen port.

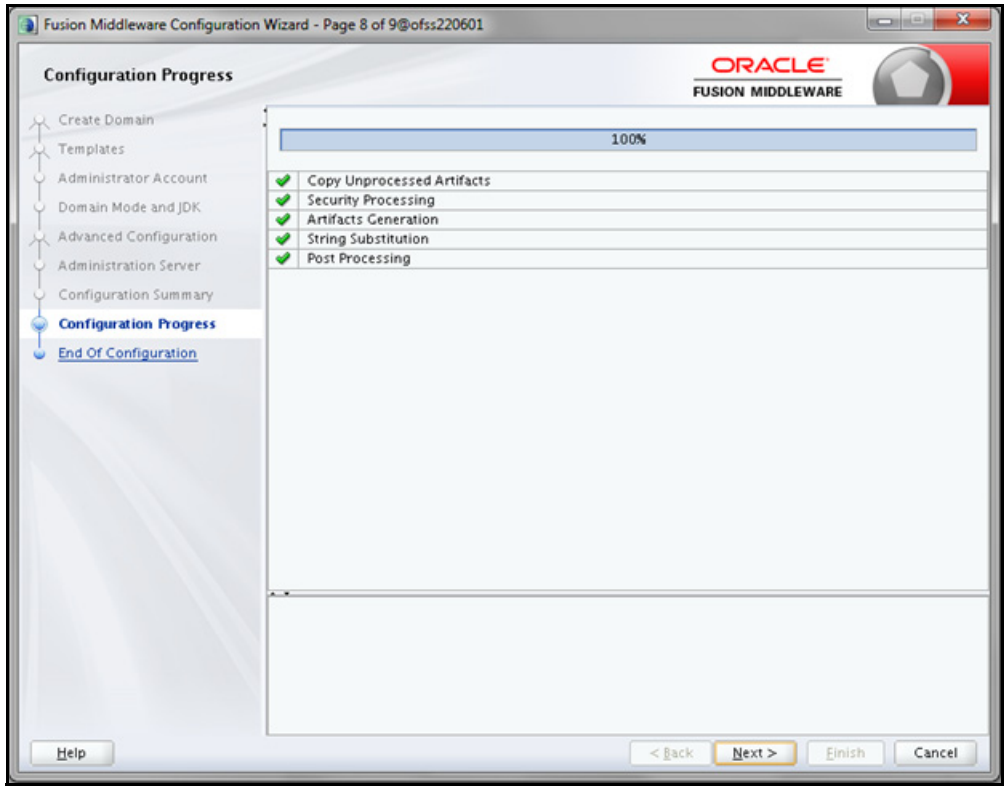
   Click **Next** to display the **Configuration Summary** window.

Note: Make a note of the Listen Port or SSL Listen Port value (for example: 7007), since the same has to be re-entered in the Servlet port field during Infrastructure installation.



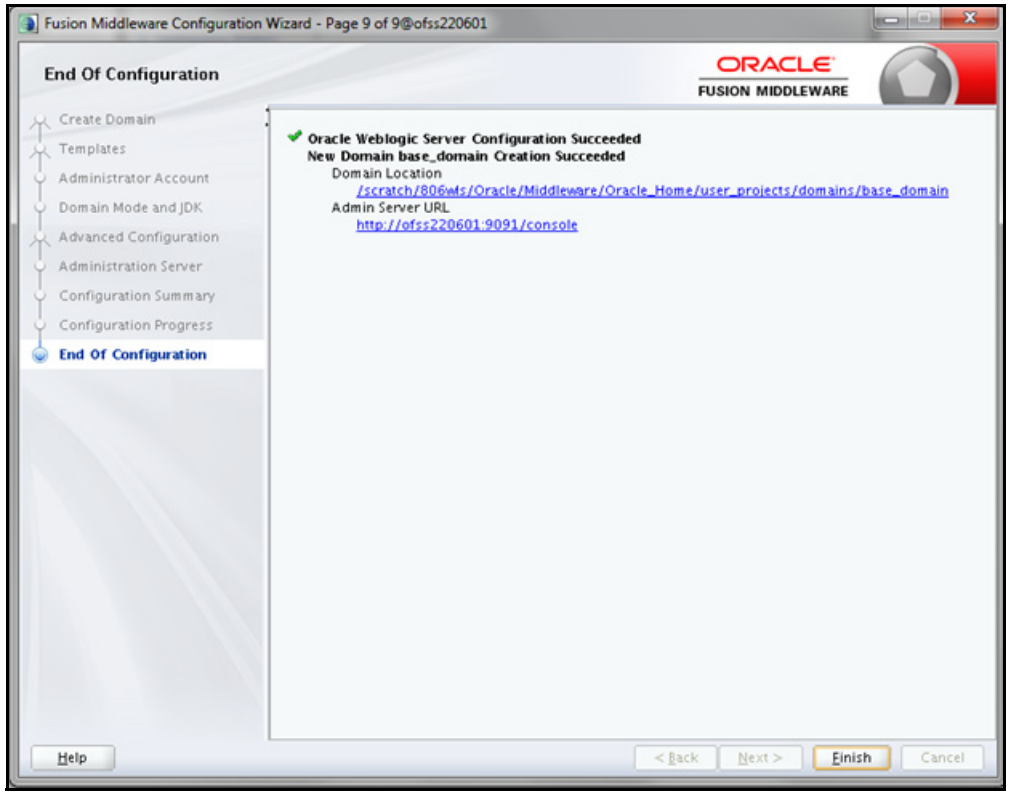
8. Verify the configuration details of the WebLogic domain and click **Create**.

The **Configuration Progress** window is displayed with the status indication of the domain creation process.



9. Click **Next** when 100% of the activity is complete.

The **End of Configuration** window is displayed



10. Click **Finish**. The domain server is created enabling the deployment of multiple Infrastructure applications on a single WebLogic.

Note: Note down the HTTPS port specified during this process and use the same as servlet port or web server port during OFSAAI Installation.

To enable https configuration on Infrastructure, assign value 1 to "`HTTPS_ENABLE`" in `OFSAAI_InstallConfig.xml` for silent mode OFSAAI installation

---

Add a java option entry `-DUseSunHttpHandler=true` in *`WLS_HOME/bin/`* `"setDomainEnv.sh"` file (Required only if self signed certificate is used).

Delete Domain in WebLogic

1. Navigate to the following directory:

   `<WebLogic Installation directory>/user_projects/domains/<domain name>/bin`
2. Execute stopWebLogic.sh to stop the Weblogic domain.
3. Delete the Weblogic domain.

WebLogic Memory Settings

To configure the WebLogic Memory Settings:

1. Change the memory setting for Java Heap to `-Xms512m -Xmx3072m` in `setDomainEnv.sh` file, which resides in the folder *<DOMAIN_HOME>/bin* and in `CommEnv.sh` file which resides in the folder *common/bin*.

   Edit this file for customizing memory settings and garbage collector settings depending on the available hardware configuration.

   Example 1:

   ```
   if [ "${JAVA_VENDOR}" = "Sun" ] ; then
   WLS_MEM_ARGS_64BIT="-Xms512m -Xmx1024m"
   export WLS_MEM_ARGS_64BIT
   WLS_MEM_ARGS_32BIT="-Xms512m -Xmx1024m"
   export WLS_MEM_ARGS_32BIT
   else
   WLS_MEM_ARGS_64BIT="-Xms512m -Xmx1024m"
   export WLS_MEM_ARGS_64BIT
   WLS_MEM_ARGS_32BIT="-Xms512m -Xmx1024m"
   export WLS_MEM_ARGS_32BIT
   ```

- Example 2:

  ```
  JAVA_VM=
  MEM_ARGS="-Xms256m -Xmx1024m"
  ```

Configuring WebLogic for REST Services Authorization

To enable REST API authorization by OFSAA in WebLogic, 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>
   ```

Configuring Apache Tomcat Server for Application Deployment

This section is applicable only when the Web Application Server type is Tomcat.

This section includes the following topics:

Tomcat User Administration

The Tomcat administration and manager application does not provide a default login. You are required to edit *"$CATALINA_HOME/conf/tomcat-users.xml"* as instructed below.

This file contains an XML tag <user> for each individual user, which will display the user name and password used by admin to log on to Tomcat, and the role names to which the admin user is associated with. For example, <user name="admin" password="admin" roles="standard-manager " />

1. Add the manager role to any one of the existing user name/ password combination as shown in the example above.
2. Use the same user-name/ password to which the manager role has been assigned to access the Tomcat Application Manager.
3. If the Tomcat server is already running, it requires a re-start after the above configuration is done.

Configure Tomcat to use JAVA 64 bit Executables

1. Navigate to the "$CATALINA_HOME/bin" folder.
2. Edit the setclasspath.sh as explained below:
3. Replace the following block of text:

```
# Set standard commands for invoking Java.
_RUNJAVA="$JRE_HOME"/bin/java
if [ "$os400" != "true" ]; then
_RUNJDB="$JAVA_HOME"/bin/jdb
```

With:

```
# Set standard commands for invoking Java.
_RUNJAVA="$JAVA_BIN"/java
if [ "$os400" != "true" ]; then
_RUNJDB="$JAVA_BIN"/jdb
```

4. If the Tomcat server is already running, it requires a re-start after the above configuration is done.

Note: In case tomcat is installed under different Unix profile, set JAVA_BIN environment variable in .profile to include the Java Runtime Environment absolute path.

For example:

```
export JAVA_BIN /usr/java6_64/jre/bin
export JAVA_BIN = /usr/java6_64/jre/bin//sparcv9
```
for Solaris Sparc.

Configure Servlet Port

The default servlet port configured for the Tomcat installation is 8080. Ignore this section if you need to use the default port.

If you need to use a different port number, you must first configure the port in the "server.xml" in the "conf" directory of Tomcat Installation directory. The following steps guide you through the configuration process:

1. Navigate to *$CATALINA_HOME/conf*. Open `server.xml` and locate the tag:
   `"Define a non-SSL HTTP/1.1 Connector on port 8080 "`
2. Against this tag, a parameter is specified 'Connector port = "8080" '. Edit this value to the new port number that will be used during the installation process.
3. Save your changes in `server.xml`.

Note: Make a note of the servlet port configured. This information is required during the installation of OFSAA Application Pack.

SSL Port Configuration

If you need to configure and access your OFSAA setup for HTTPS access, ensure that the following connect tag under "`Define a SSL HTTP/1/1 Connector on port 8443`" in "*<Tomcat_installation_folder>/conf/*`server.xml`" file is uncommented for SSL Configuration. (By default, it is commented).

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
```

Note: Make a note of the servlet port configured. This information would be required during the installation of OFSAA Application Pack. To enable https configuration on Infrastructure, assign value 1 to "`HTTPS_ENABLE`" in `OFSAAI_InstallConfig.xml` for SILENT mode OFSAAI installation.

For example, see the following connector tag for https configuration:

```
<Connector port="8091" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" secure="true"
    clientAuth="false"
    maxHttpHeaderSize="8192"
    minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" scheme="https"
    sslProtocol="SSL"
    keystorefile=".keystore" keystorepass="changeit"
    truststorefile=".keystore" truststorepass="changeit"
```

For more information related to SSL Configuration on Tomcat, see http://tomcat.apache.org/.

Apache Tomcat Memory Settings

To configure the Apache Tomcat Memory Settings:

1. Locate the file catalina.sh which resides in the folder *<CATALINA_HOME>/bin*.
2. Edit this file for customizing the memory settings and garbage collector settings depending on the available hardware configuration.
3. Add the memory setting for Java Heap to `-Xms512m -Xmx1024m`.

   Example:

```
if [ -z "$LOGGING_MANAGER" ]; then
JAVA_OPTS="$JAVA_OPTS -Xms512m -Xmx1024m
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager"
else
JAVA_OPTS="$JAVA_OPTS -Xms512m -Xmx1024m $LOGGING_MANAGER"
Fi
```

Configuring Tomcat for User Group Authorization and Data Mapping

Users with system authorization roles can access User Group Authorization. However, to make it available on Tomcat web server, you have to perform the following configuration steps:

1. Navigate to the *$CATALINA_HOME/conf* folder and open web.xml file.
2. Enter the following in the `web.xml` file.

```
<init-param>
    <param-name>mappedfile</param-name>
    <param-value>false</param-value>
</init-param>
```

3. Save and close the file.

Uninstalling WAR Files in Tomcat

To uninstall WAR files in tomcat, see Uninstalling WAR Files in Tomcat.

Configuration for Axis API

This step is optional and required only if the web application server used in Apache Tomcat. If you use any other web application server, skip and proceed to next step.

Copy the `jaxrpc.jar` from the *<OFSAA Installation Directory>/axis-1_4/webapps/axis/WEB-INF/lib* and place it in under *<Tomcat Installation Directory>/lib* and restart the Tomcat Server.

Additional Configurations 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>
   ```

Configuring Work Manager in Web Application Servers

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

This section covers the following topics:

- Configuring Work Manager in WebSphere Application Server
- Configuring Work Manager in WebLogic Application Server

Configuring Work Manager in WebSphere Application Server

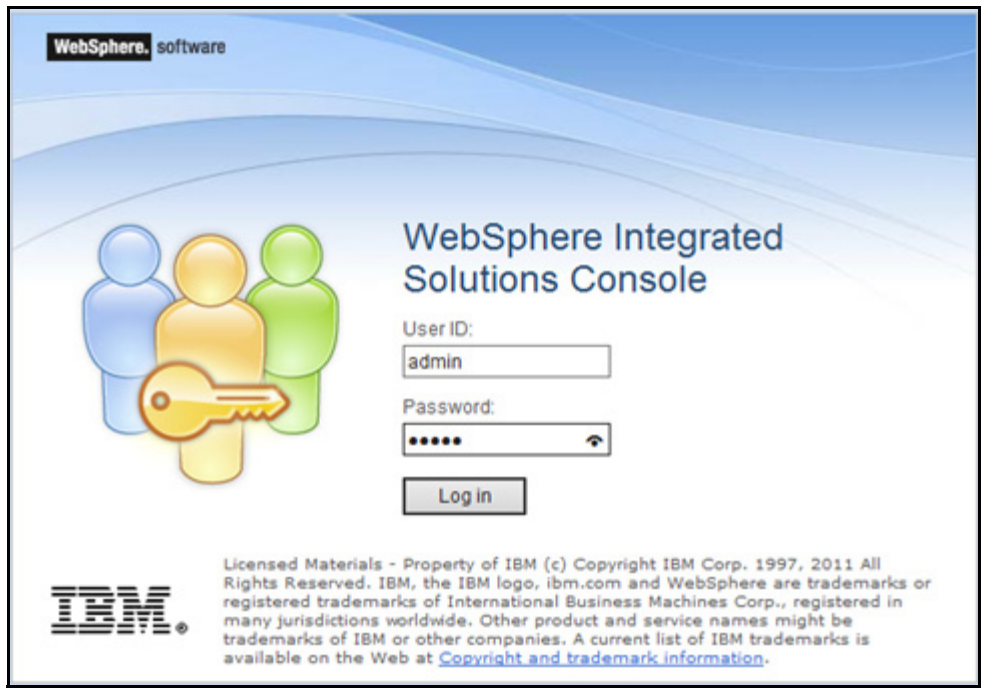
This section is applicable only when the Web Application Server type is WebSphere.

This section covers the following topics:

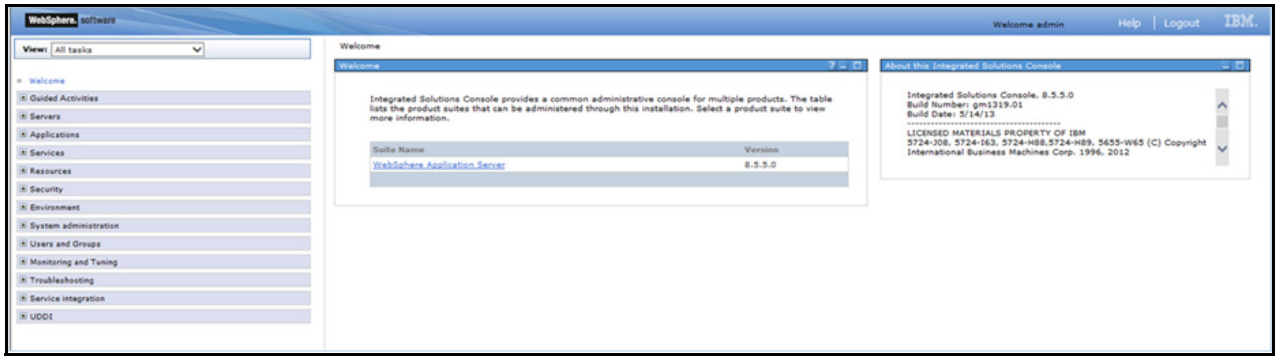
- Creating Work Manager
- Mapping Work Manager to OFSAA WebSphere Instance

Creating Work Manager

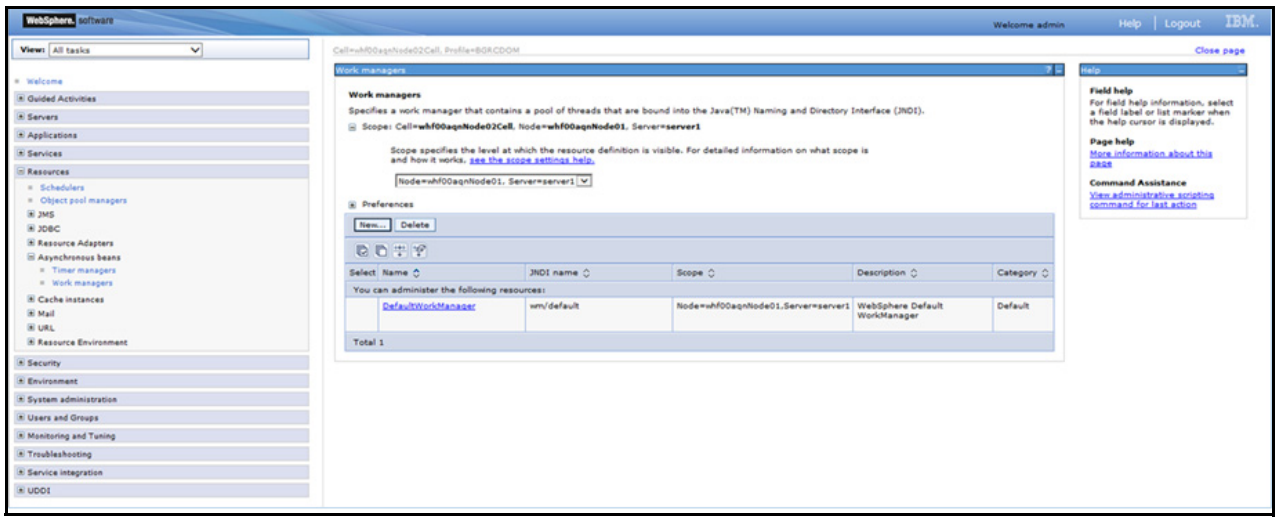
1. Open the WebSphere admin console in the browser window: http://<ipaddress>:<administrative console port>/ibm/console. (https if SSL is enabled). The Login window is displayed.



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



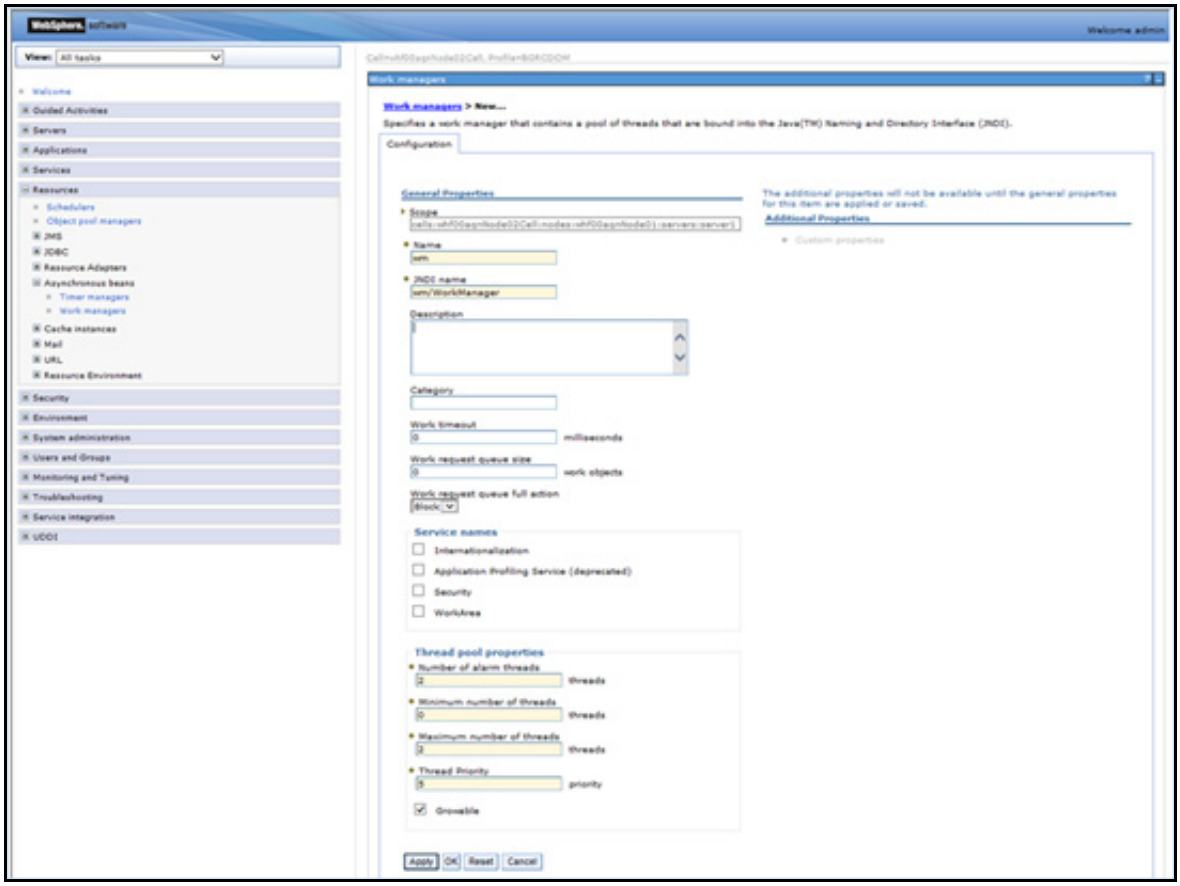
3. From the LHS menu, expand **Resources > Asynchronous beans** and select **Work Managers**.



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

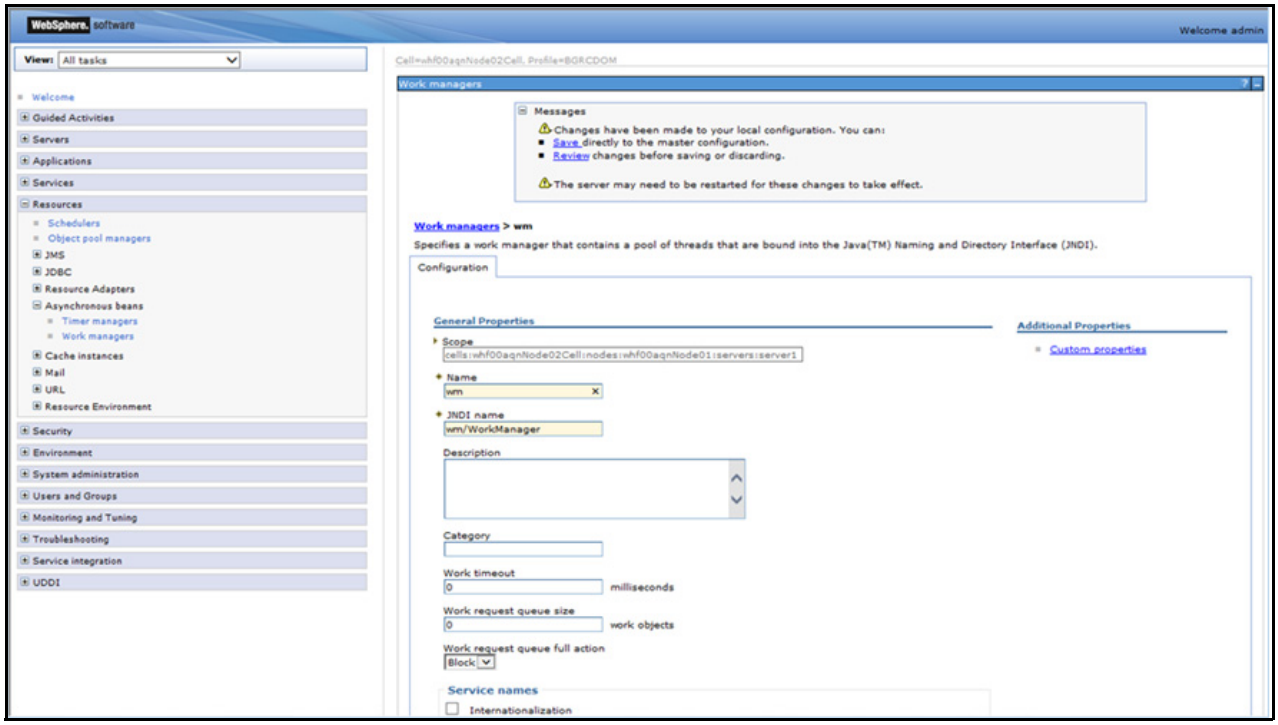
   For example, Node=whf00aqnNode01, Server=server1.

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

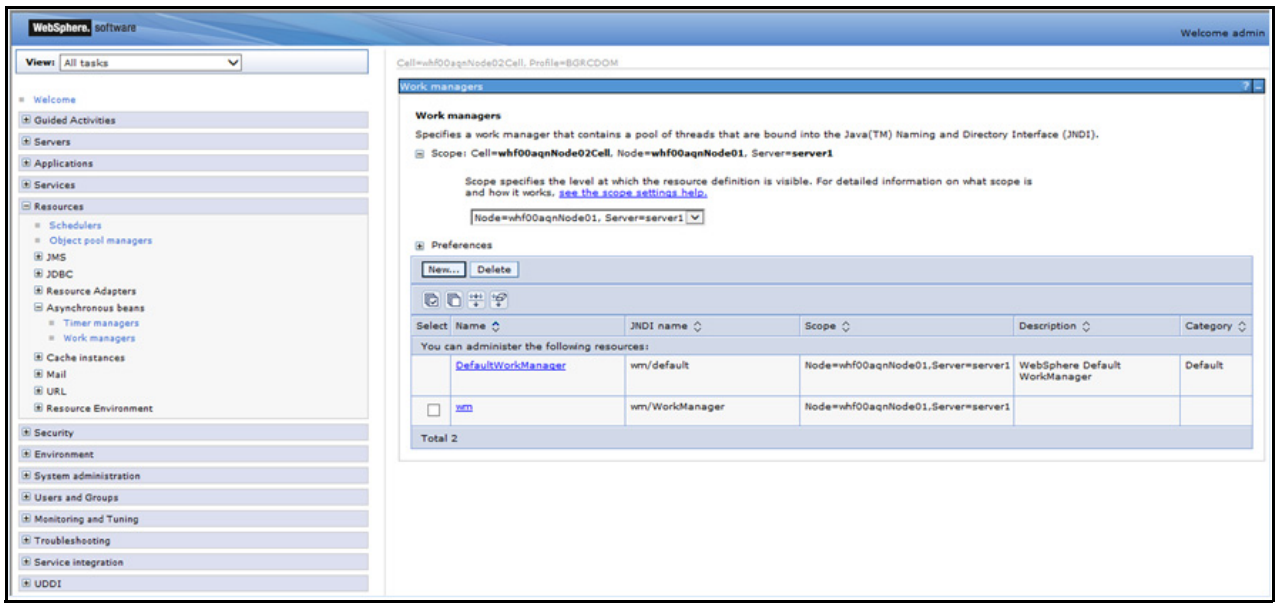


6. Enter the **Name** as 'wm' and **JNDI** name as 'wm/WorkManager ' in the respective fields.
7. Enter the **Thread pool properties**.

8. Click **Apply**.



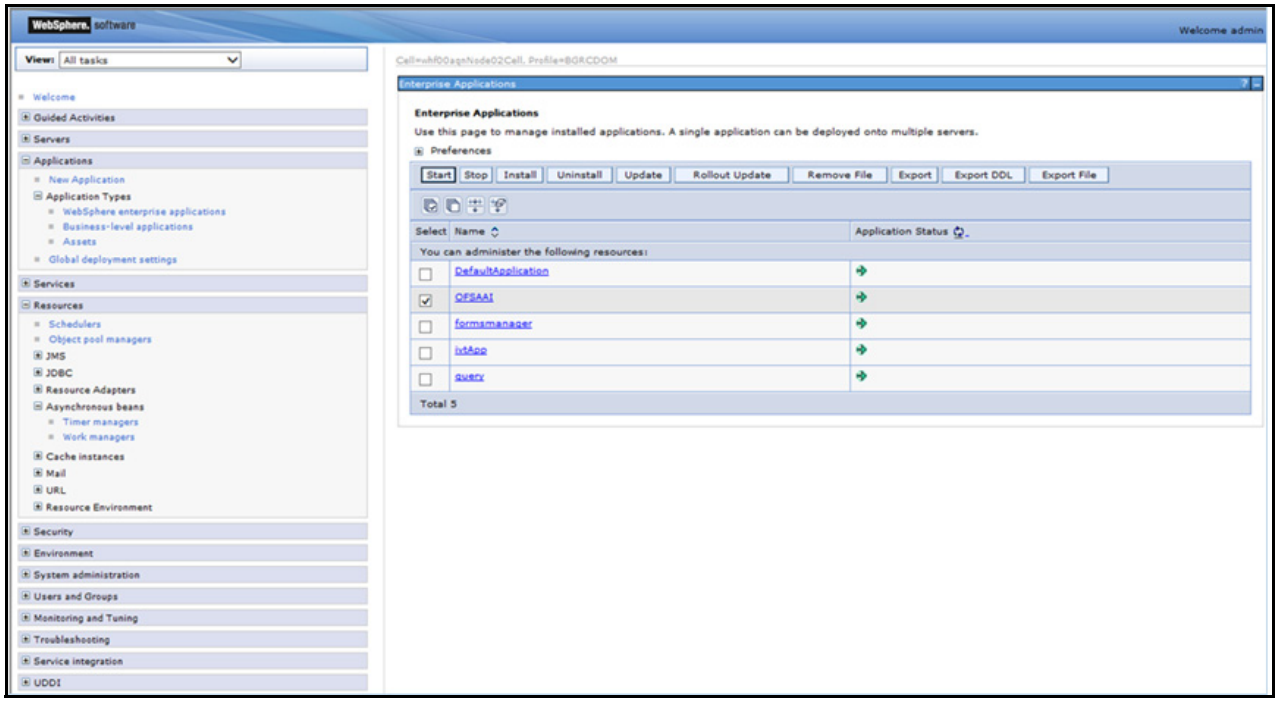
9. Click **Save**.



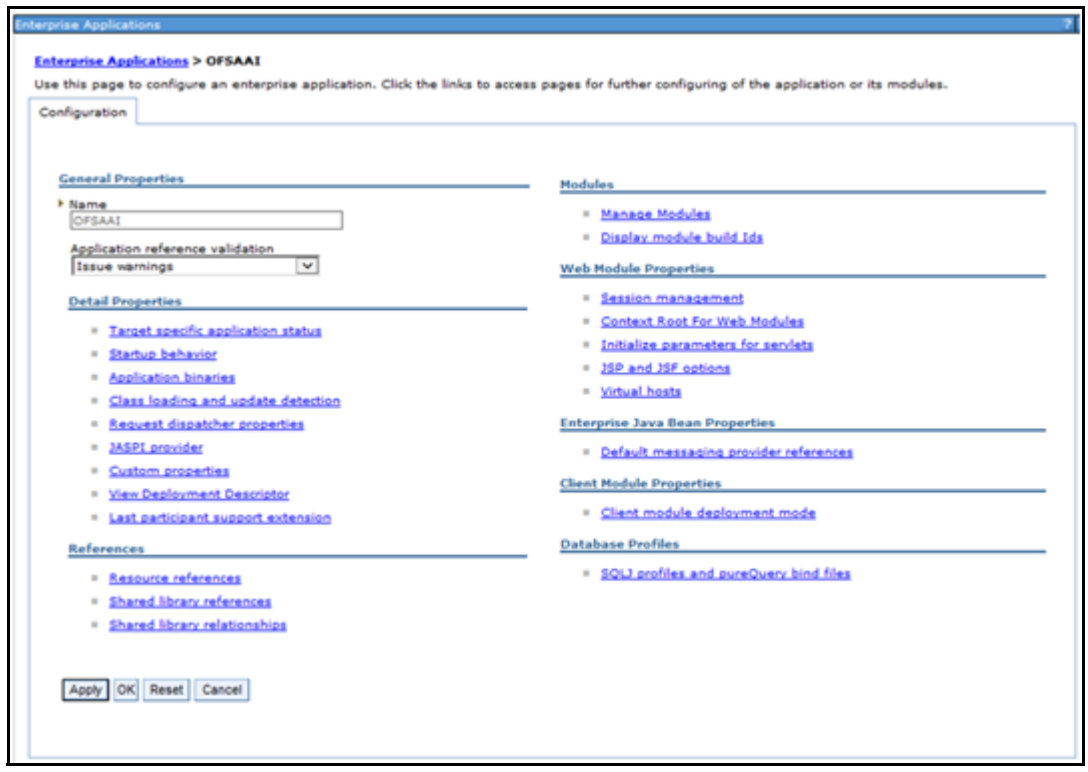
After creating work manager successfully, you have to map it to OFSAA instance.

Mapping Work Manager to OFSAA WebSphere Instance

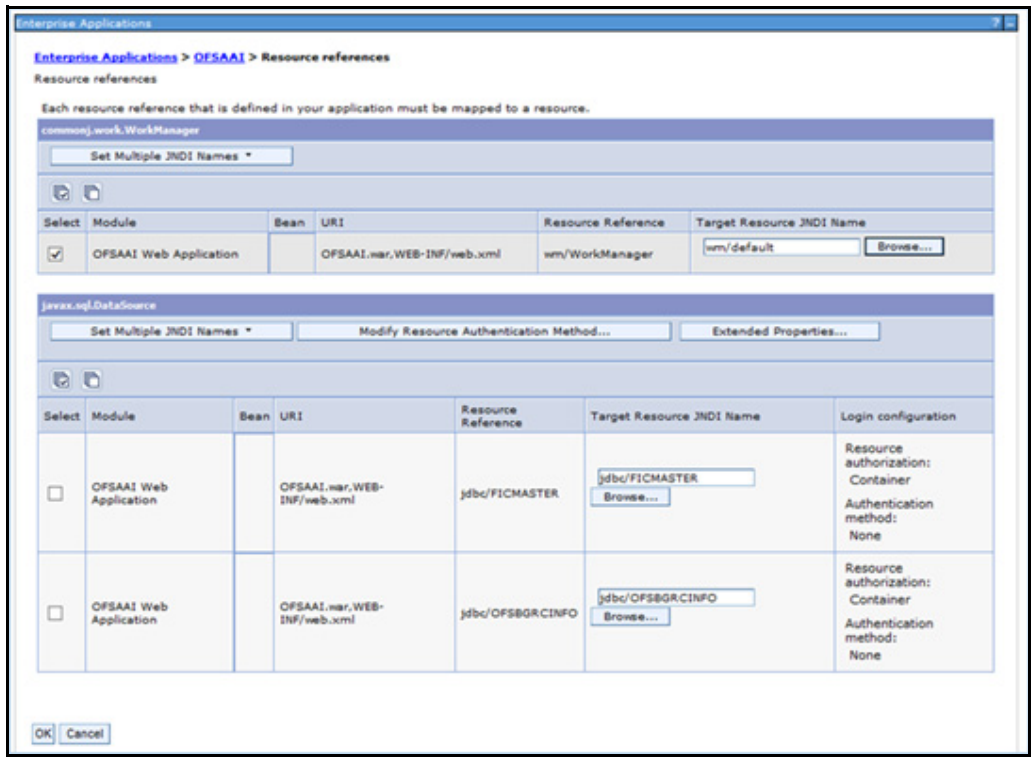
1. From the LHS menu, expand **Applications > Application Types** and select **WebSphere enterprise applications**.



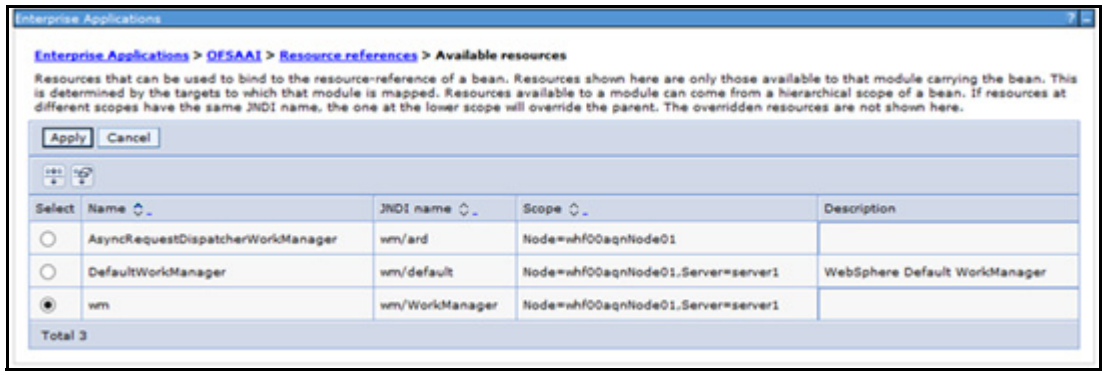
2. Click OFSAAI instance hyperlink.



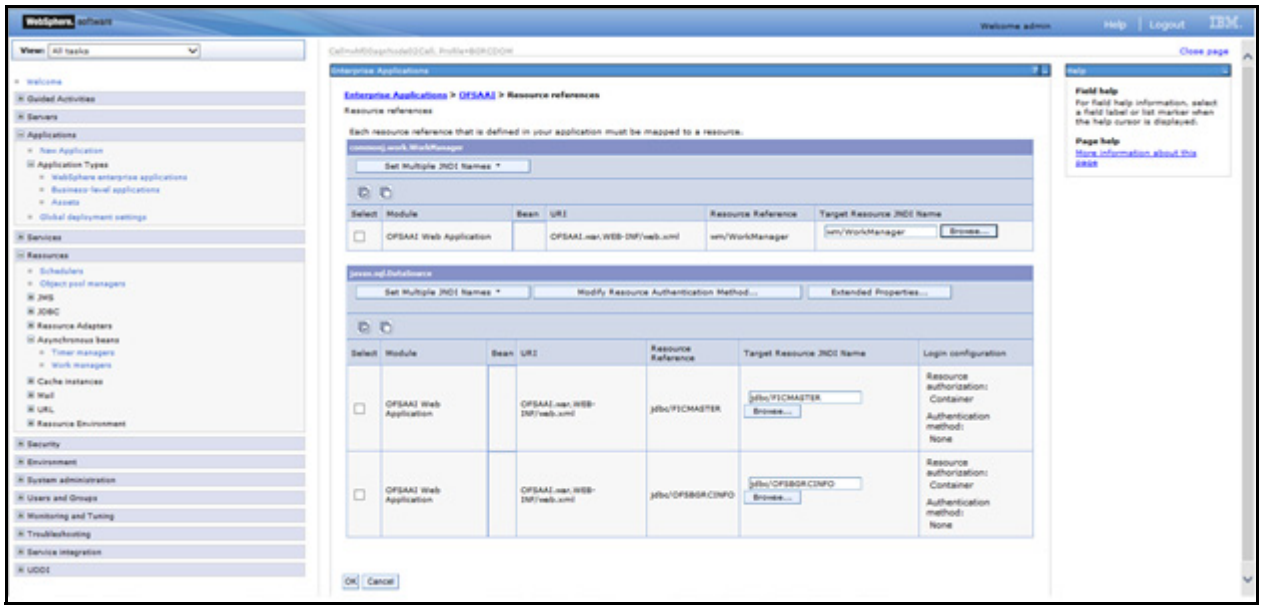
3. Click **Resource references** link under References section.



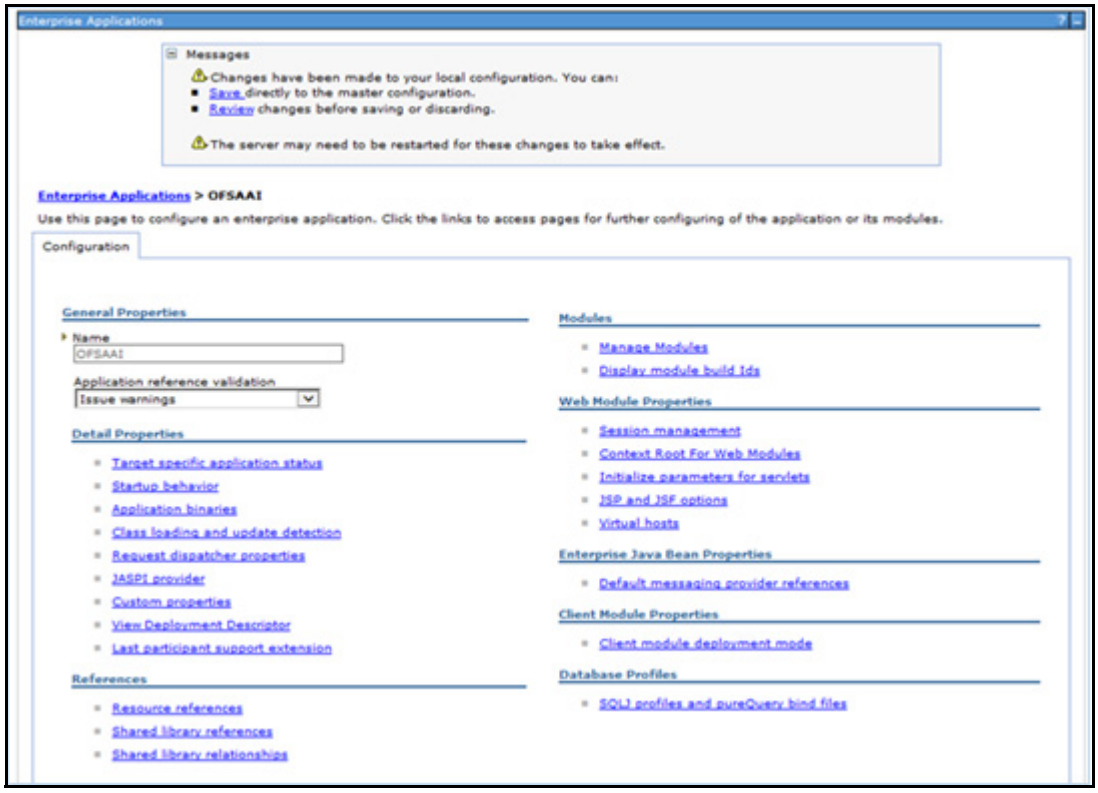
4. Click **Browse** corresponding to the Work Manager Resource Reference. The available resources are displayed.



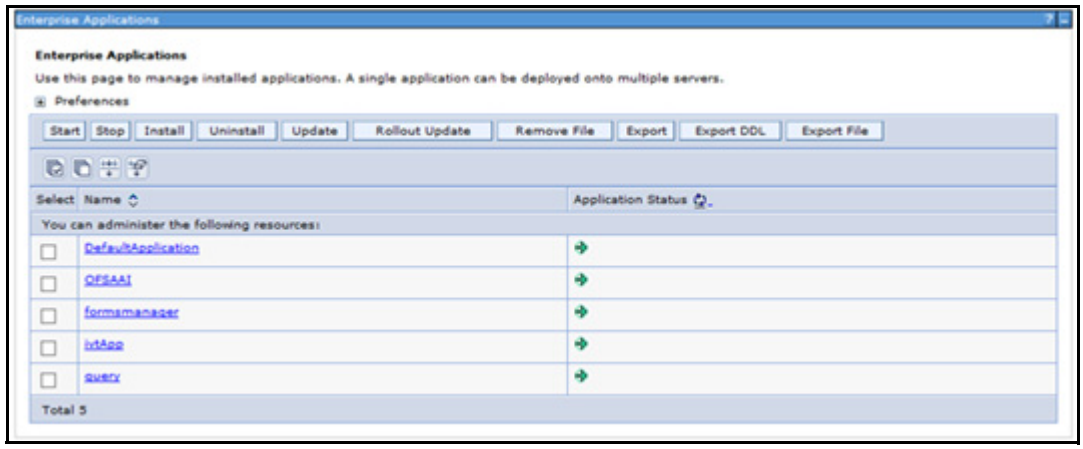
5. Select the newly created Work Manager ('wm') and click Apply.



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



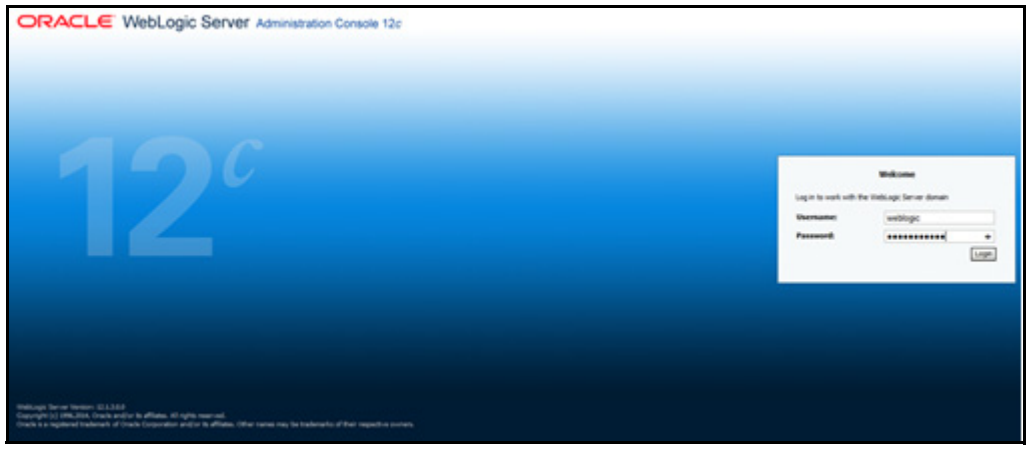
7. Click Save.



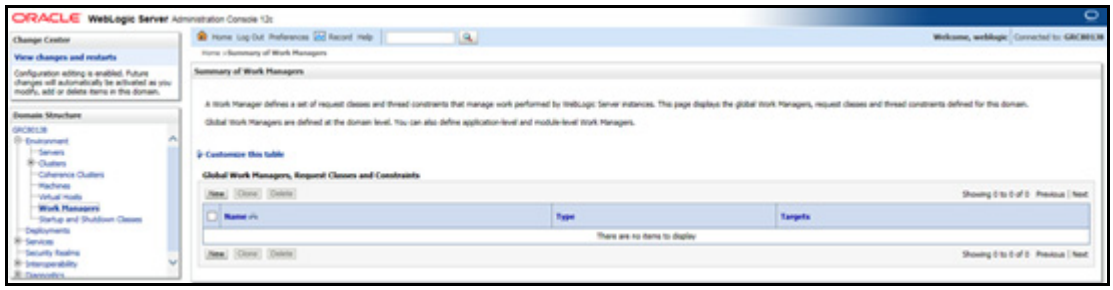
Configuring Work Manager in WebLogic Application Server

This section is applicable only when the Web Application Server type is WebLogic.

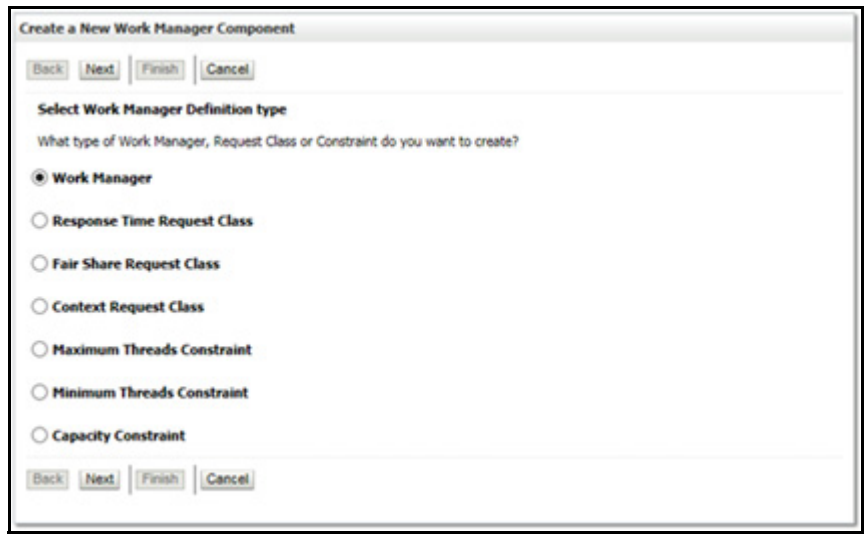
1. Open the WebLogic admin console in the browser window: http://<ipaddress>:<administrative console port>/console. (https if SSL is enabled). The Welcome window is displayed.



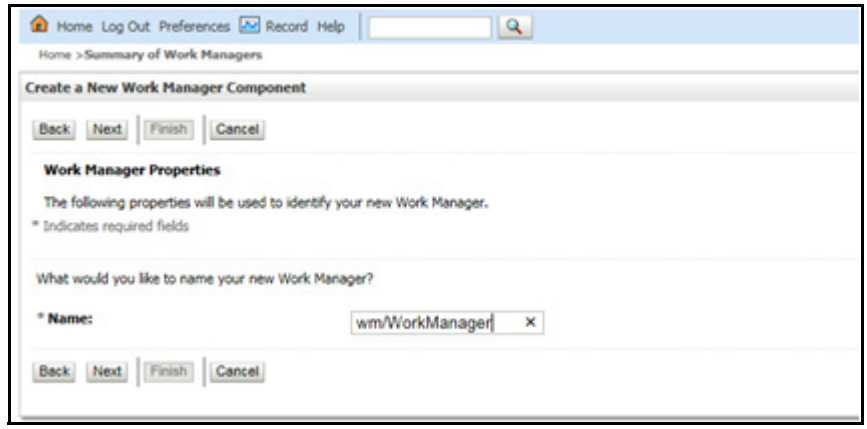
2. Login with the user id that has admin rights.
3. From the Domain Structure menu in the LHS, expand **Environment** and select **Work Managers**. The Summary of Work Managers window is displayed.



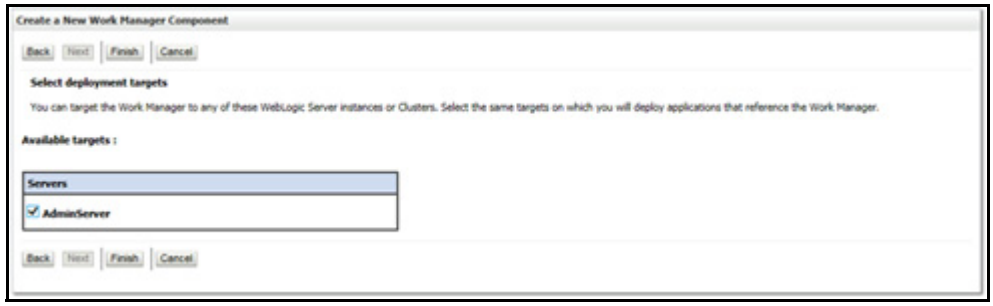
4. Click **New** to create a new work manager component.



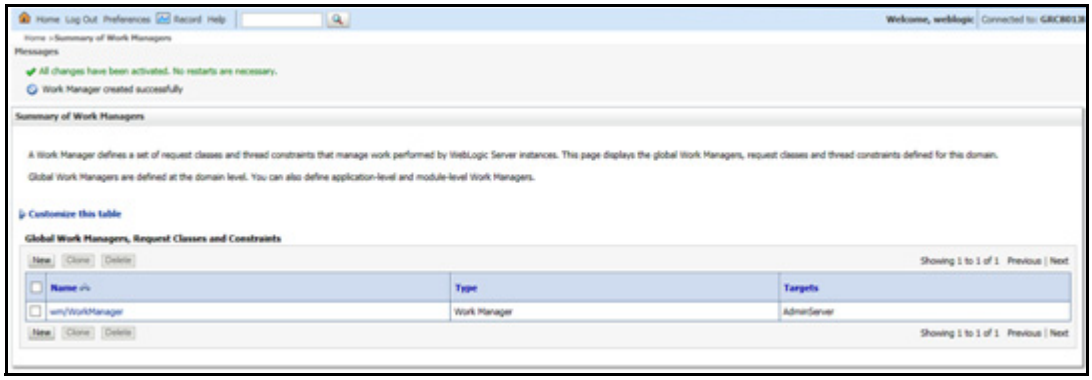
5. Select **Work Manager** and click **Next**.



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



8. Select the required deployment target and click Finish.



Creating and Deploying EAR/WAR File

This section includes the following topics:

Creating EAR/WAR File

To create EAR/WAR File, follow these steps:

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

```
/scratch/ofsaaweb>cd /scratch/ofsaaweb/OFSA80/ficweb
/scratch/ofsaaweb/OFSA80/ficweb>
/scratch/ofsaaweb/OFSA80/ficweb>ls
ant.sh                      ficwebChecksum.sh
apache-ant-1.7.1            ficweb_InstalledChecksum.txt
application.xml             lib
build.xml                   MANIFEST.MF
conf                        mycertificates
ficweb_Build_CheckSum.txt   OFSALMINFO_FusionMenu.xml
ficwebCheckSum.log          unix
ficwebChecksum.properties   webroot
/scratch/ofsaaweb/OFSA80/ficweb>./ant.sh
executing "ant"
Buildfile: build.xml

createwar:
      [war] Building war: /scratch/ofsaaweb/OFSA80/ficweb/AAI80.war

createear:
      [ear] Building ear: /scratch/ofsaaweb/OFSA80/ficweb/AAI80.ear

BUILD SUCCESSFUL
Total time: 2 minutes 8 seconds
/scratch/ofsaaweb/OFSA80/ficweb>
```

4. The EAR/ WAR file - <contextname>.ear/ .war - is created.

Note: The <contextname> is the name given during installation.
This process overwrites any existing version of EAR file that exists in the path.
In case of OFSAA configured on Tomcat installation, `<contextname>.war` will be created.

Deploying EAR/WAR File

This section includes the following topics:

- Deploying EAR/WAR Files on WebSphere
- Deploying EAR / WAR File on WebLogic
- Deploying WAR Files on Tomcat

Note: Ensure to clear the application cache prior to the deployment of Application Pack Web Archive. This is applicable to all Web Servers (WebSphere, WebLogic, and Tomcat). For more information, see Clearing Application Cache section.

Deploying EAR/WAR Files on WebSphere

To deploy WebSphere EAR/WAR File, follow these steps:

1. Start WebSphere Profile by navigating to the path *"/<Websphere_Installation_Directory>/IBM/WebSphere/AppServer/profiles/<Profile_Name>/bin/"* and execute the command:

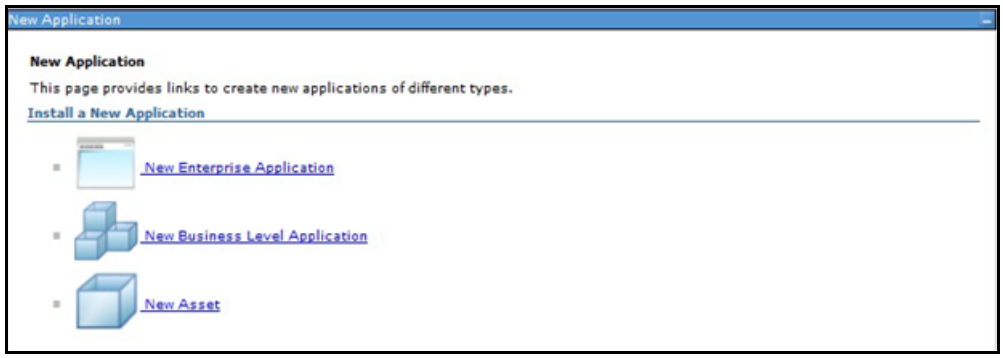
   `./startServer.sh server1`

2. Open the WebSphere admin console in the browser window:

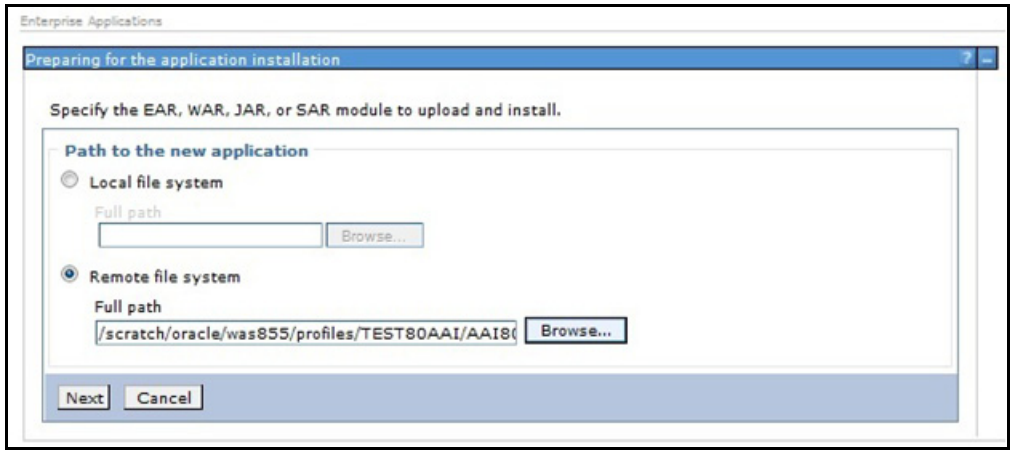
   `http://<ipaddress>:<administrative console port>/ibm/console`. (https if SSL is enabled). The Login window is displayed.

3. Enter the user credentials with admin privileges and click **Log In**.

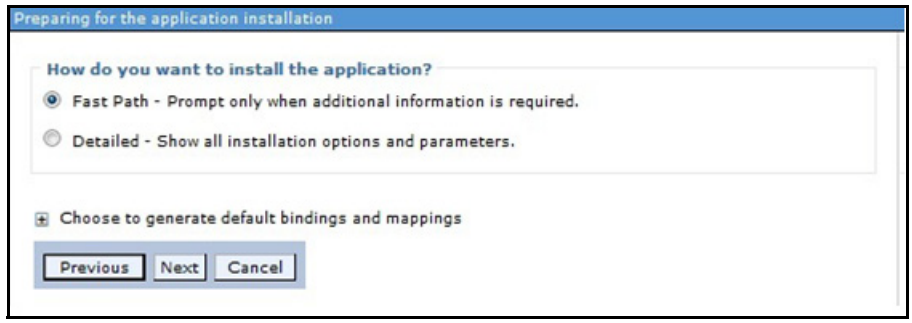
4. From the LHS menu, select **Applications** and click **New Application** to display the **New Application** window.



5. Click **New Enterprise Application** to display the **Preparing for the application installation** window.

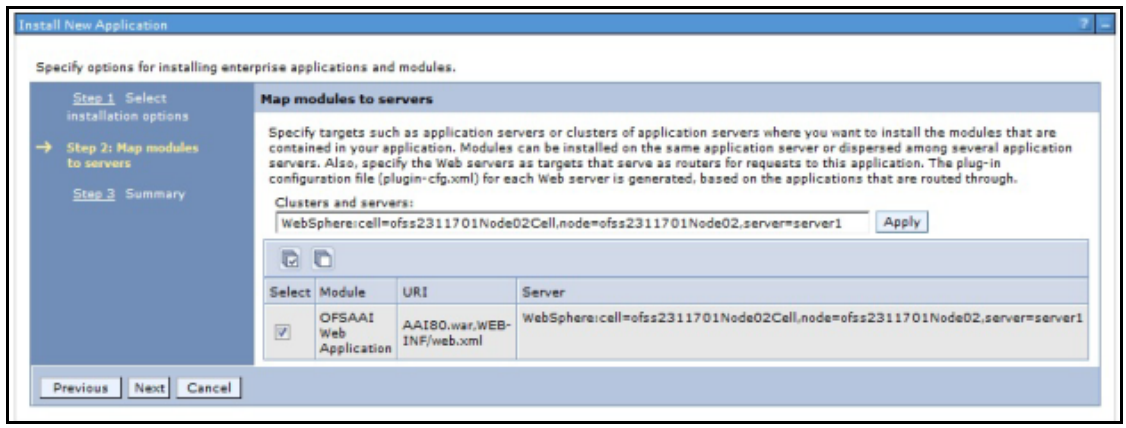


6. Select **Remote File System** and click **Browse**. Select the EAR file generated for OFSAA to upload and install. Click **Next**.

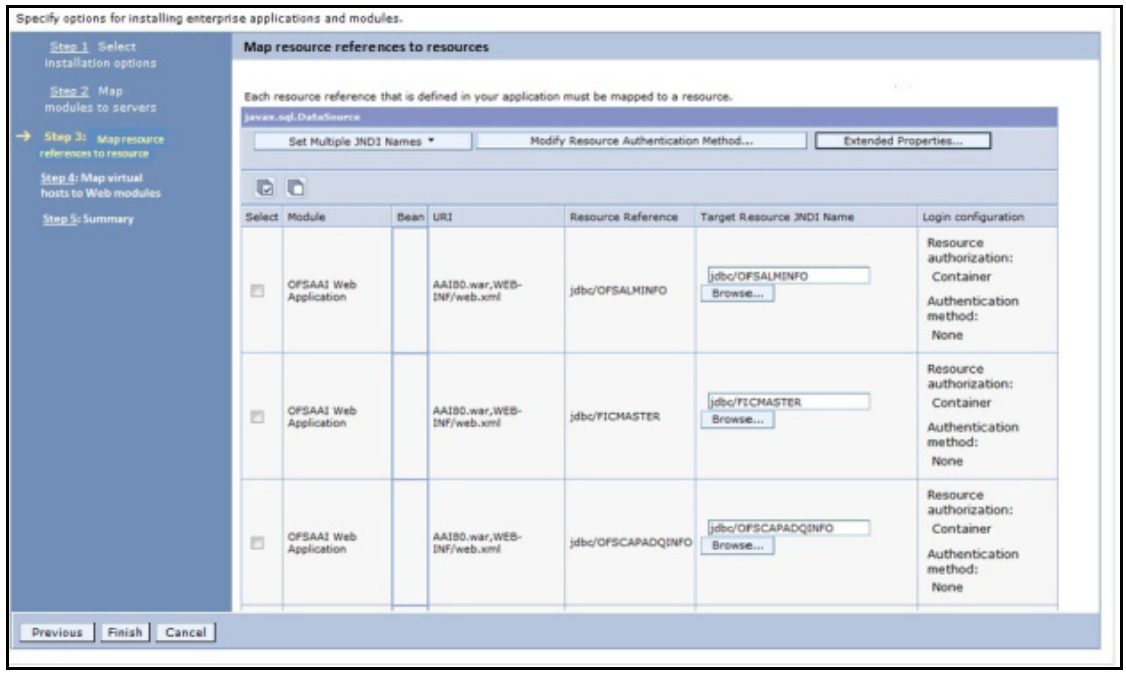


7. Select the **Fast Path** option and click **Next** to display the **Install New Application** window.

8. Enter the required information and click **Next** to display the **Map Modules to Servers** window.



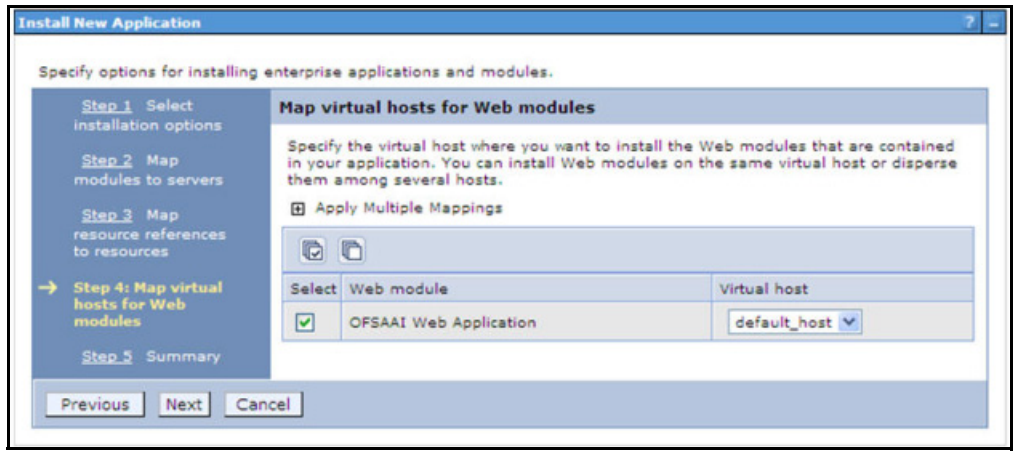
9. Select the **Web Application** and click **Next** to display the **Map Resource References to Resources** window.



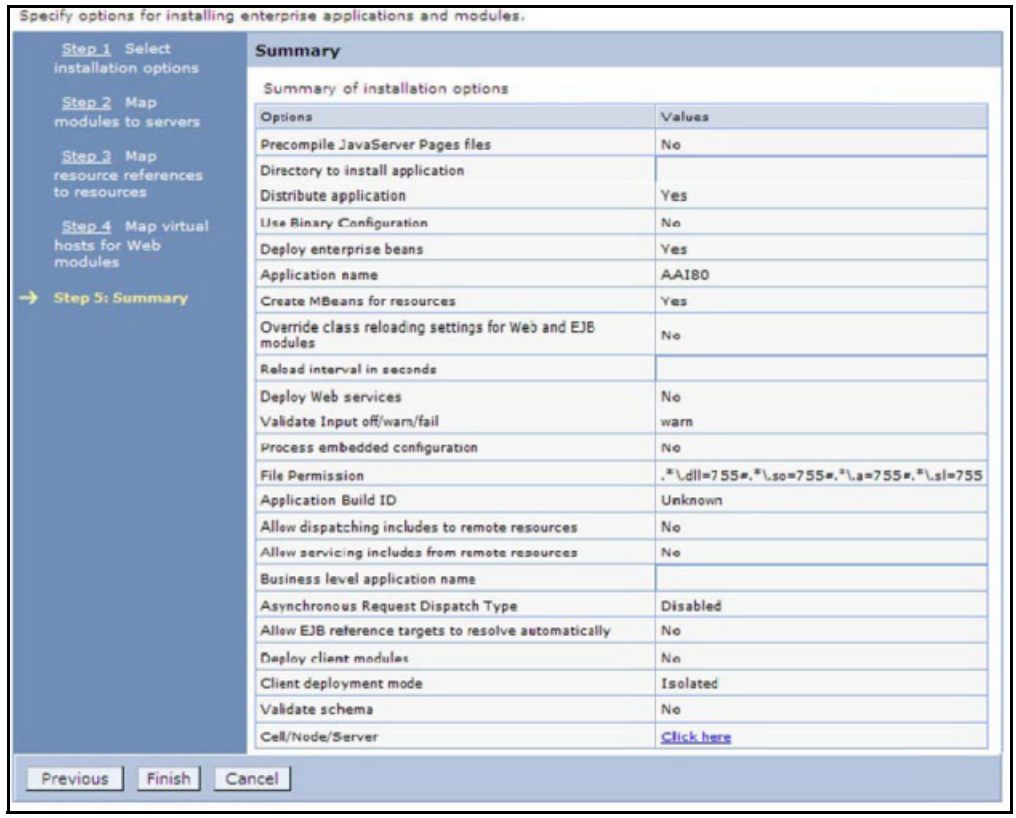
10. Map each resource defined in the application to a resource JNDI name defined earlier.
11. Click **Modify Resource Authentication Method** and specify the authentication method created earlier.

    You can specify "config" for FICMASTER resource or "atomic" for atomic resource as the authentication method.

12. Select the **OFSAAI Web Application** check box and click **Next** to display the **Map Virtual hosts for Web Modules** window.



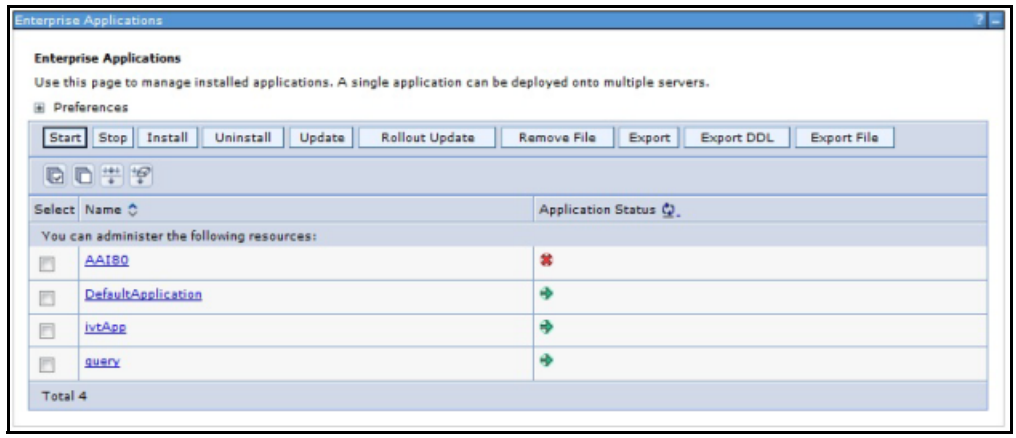
13. Select the **Web Application** check box and click **Next** to display the **Summary** page.



14. Click **Finish** and deploy the Infrastructure Application on WebSphere.
15. On successful installation, a message is displayed. Click **Save** and save the master file configuration. The details are displayed in the Master File Configuration window.

To start the application:

1. Expand **Applications > Application Type > WebSphere enterprise applications** to display the **Enterprise Applications** window.



2. Select the installed application and click Start.

Note: **<profile name>** is the profile name given while creating the WebSphere profile.
<cell name> is the cell name given during profile creation.
<contextname> is the context name given during installation.

Deploying EAR / WAR File on WebLogic

Following are the steps for deploying Infrastructure application that would be created during installation:

1. Navigate to the path <WebLogic Installation directory>/user_projects/domains/<domain name>/bin in the machine in which WebLogic is installed.
2. Start WebLogic by executing the command:

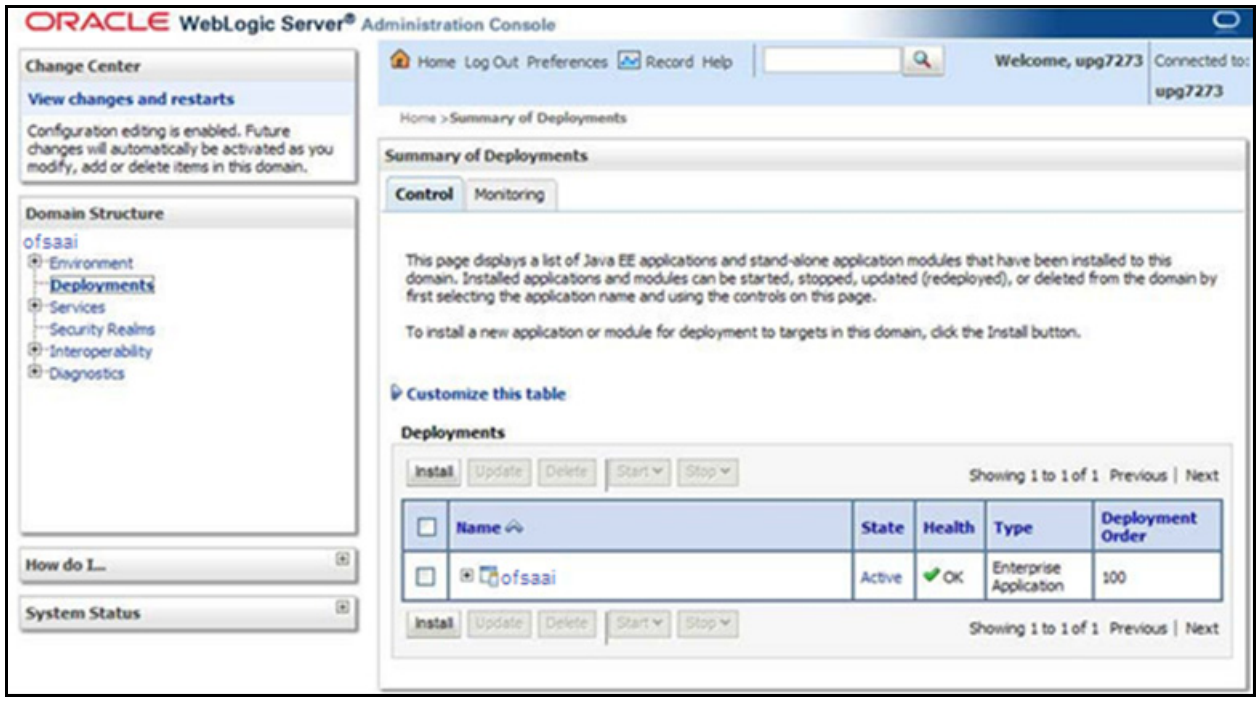
   `./startWebLogic.sh -d64 file`
3. Open the URL in the browser window: `http://<ipaddress>:<admin server port>/console`. (https if SSL is enabled). The Sign in window of the WebLogic Server Administration Console is displayed.

   Note: Ensure that you have started Infrastructure Server by executing "./reveleusstartup.sh" as mentioned in Start Infrastructure section.

   ---

4. Log on to the WebLogic Server by entering the user credentials having privileges to deploy the EAR file.

5. From the **Domain Structure** LHS menu, click **Deployments** to display the **Summary of Deployments** window.



6. Click **Install** to display the **Install Application Assistant** window.
7. Select the Exploded EAR directory after browsing to the directory where it is saved and click **Next**.

Explode EAR File

To explode EAR, follow the below steps:

1. Create the "applications" folder under domain name. For example:

   /Bea/user_projects/domains/ <Domain _name>/applications.

2. Create *<context_name>.ear* folder under "applications" folder.
3. Copy the *<$FIC_WEB_HOME/<context_name>.ear* file to *<WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear*
4. Explode the <context_name>.ear file by executing the command:

   `jar -xvf <context_name>.ear`

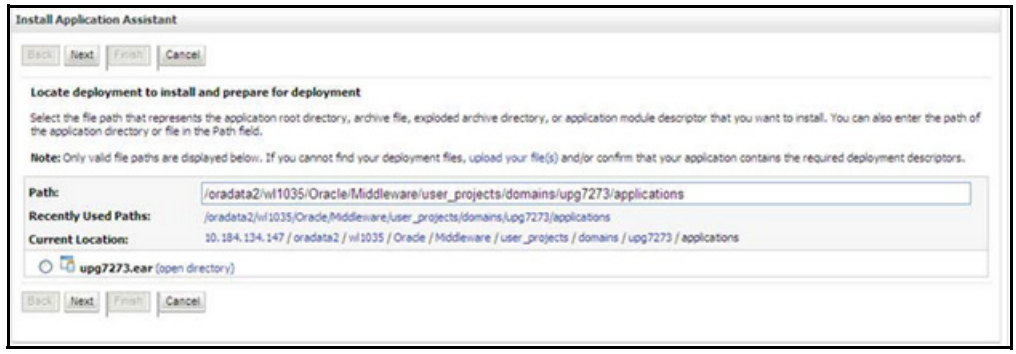
5. Delete the `<context>.ear` and `<context>.war` files (recently created) *<WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear*
6. Create a directory `<context_name>.war` under *<WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear*
7. Copy *<$FIC_WEB_HOME/<context_name>.war* file to *<WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear/<context_name>.war*
8. Explode the `<context_name>.war` file by executing the following command to get the directory structure:

   `jar -xvf <context_name>.war`

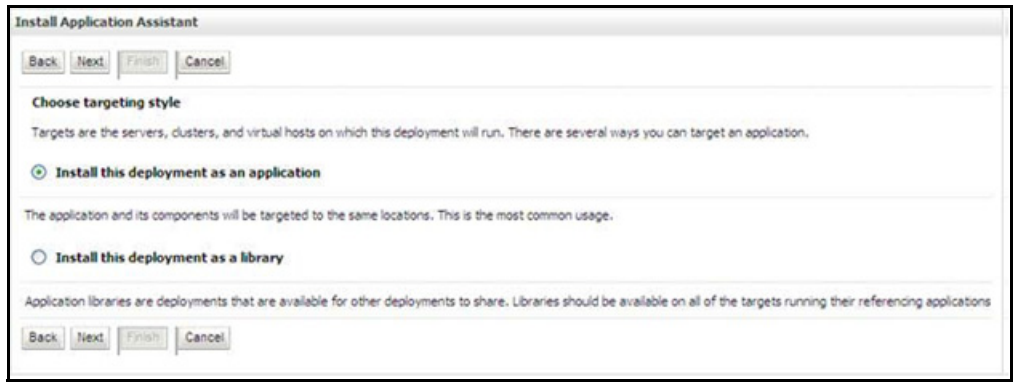
Install Application

To install the Application:

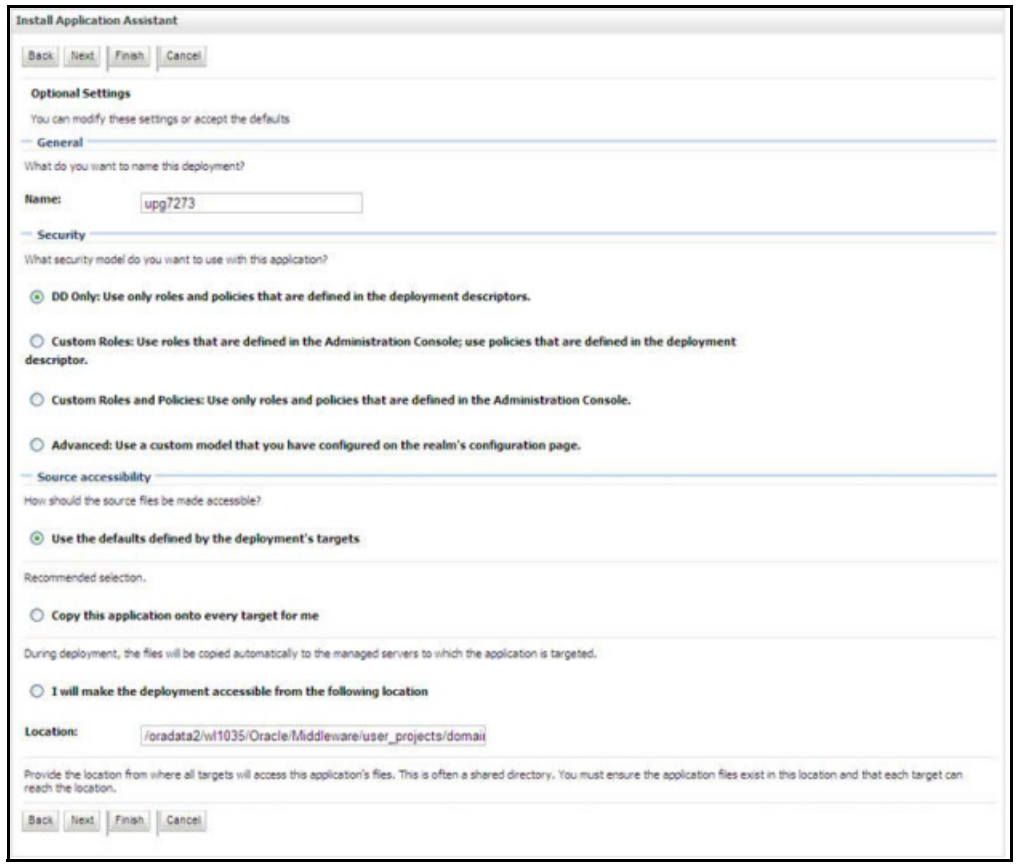
1. Open the Install Application Assistant.



2. Click **Next**.

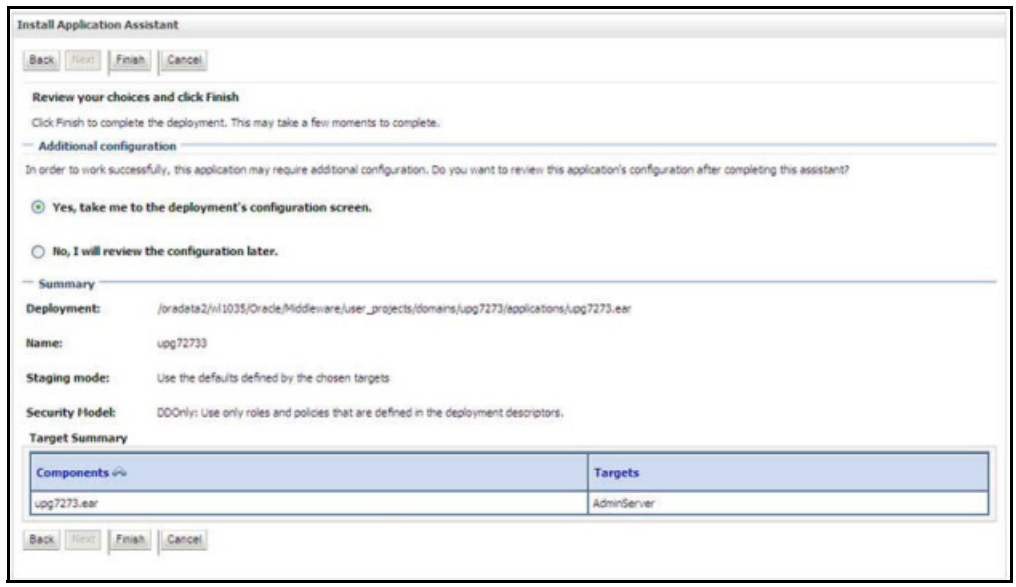


3. From the Choose targeting style section, select the **Install this deployment as an application** option and click **Next** to display the **Optional Settings** window.

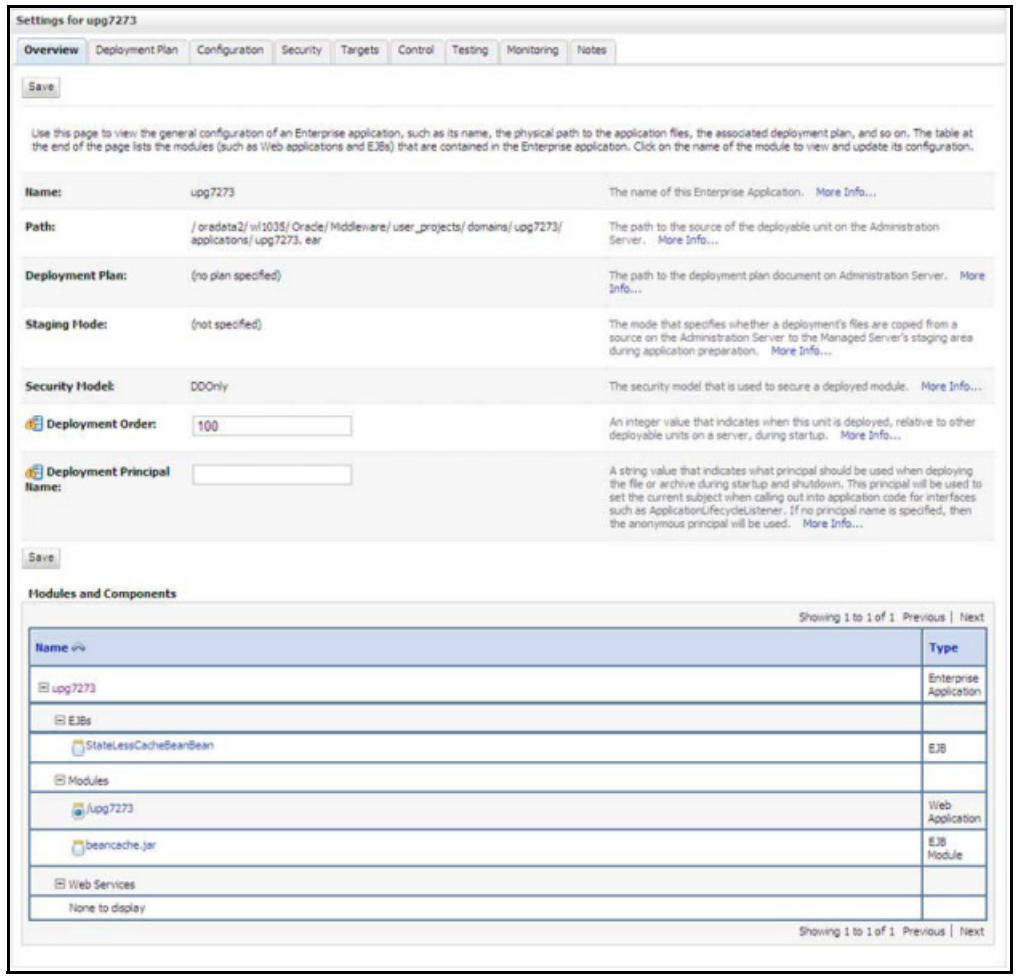


4. Enter a **Name** for the deployment if required.
5. Under the Security section, select the **DD only** option to specify that only roles and policies that are defined in the deployment descriptors should be used.
6. Select the **I will make the deployment available from the following location** option under the Source accessibility section.

7. Click **Next** to continue and display the **Deployment Summary** window.

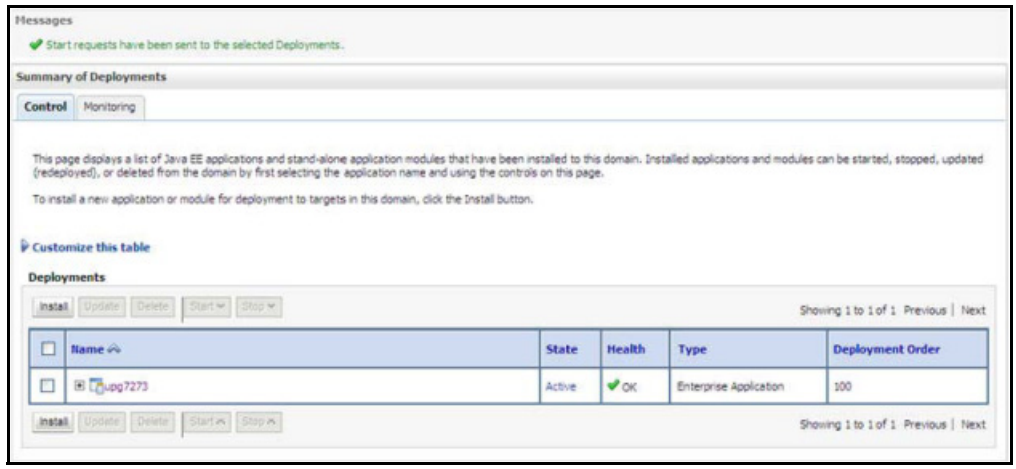


8. Select the option **Yes, take me to the deployment's configuration screen** option and click **Finish** to display the **Settings for <Deployment Name>** window.



9. Review the general configuration details of the deployment. You can also update the configuration of the deployment in this window. In the Overview tab you can view the complete deployment configuration.
10. Click **Save** to update the changes, if any.
11. From the LHS menu, click **Deployments** to display the **Summary of Deployments** window.

12. Select the newly deployed Infrastructure application and click **Start > Servicing all requests**. Ensure that the Infrastructure server is up and running.



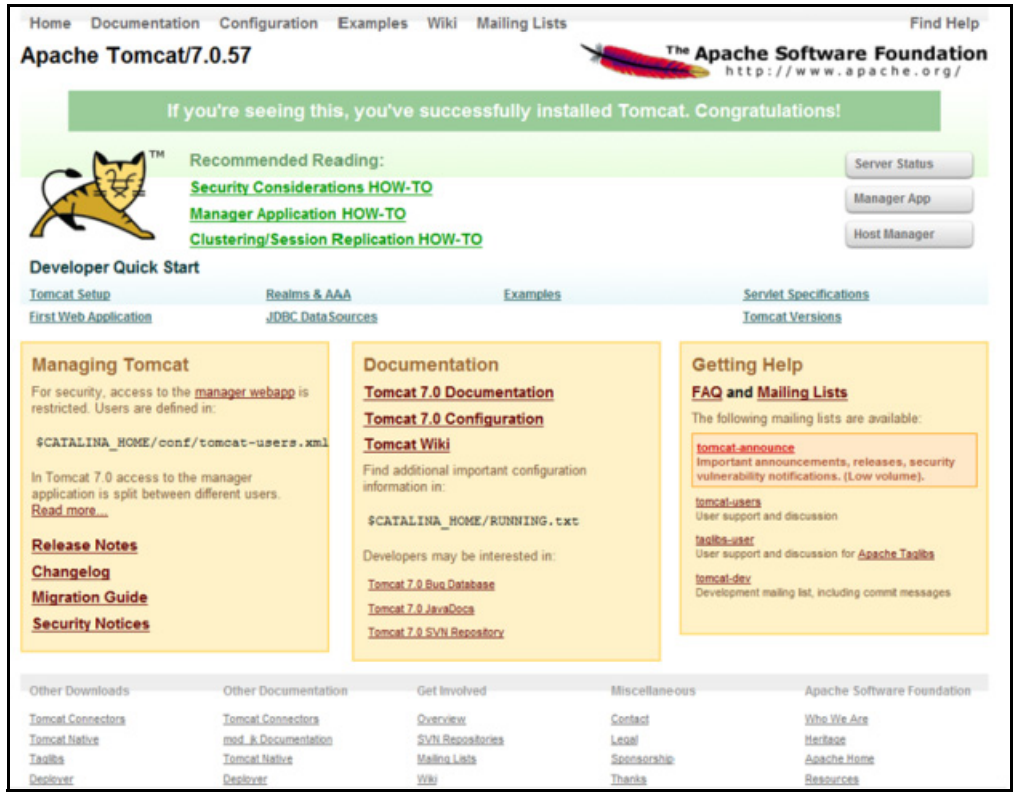
13. The **State** of the deployed application is displayed as **Active** if started successfully.

Deploying WAR Files on Tomcat

Before deploying the WAR files, ensure that the previously deployed applications of Infrastructure are uninstalled. See Uninstalling Previously Deployed WAR Files in Tomcat for the procedure to uninstall the previously deployed Infrastructure war files.

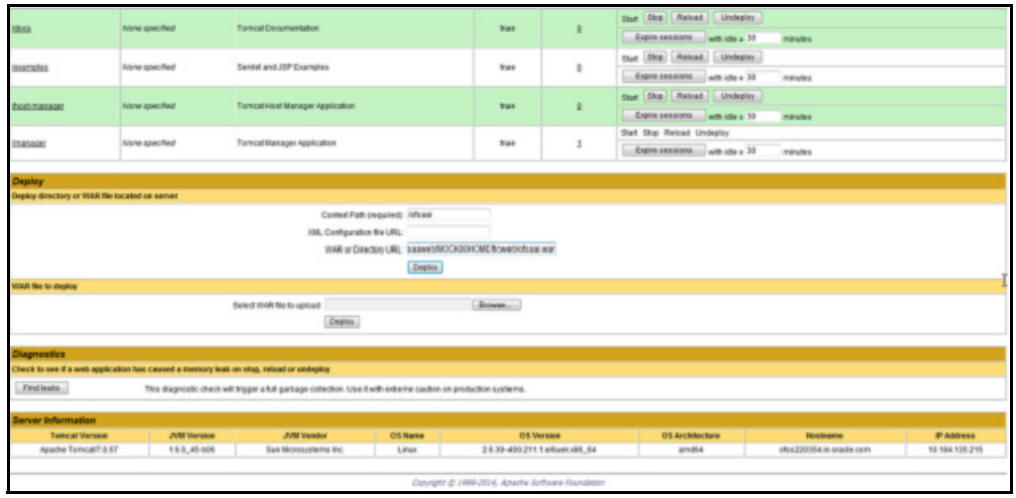
On the machine that hosts Tomcat, follow the below steps outlined to deploy Infrastructure application:

1. Copy the `<context-name>.war` from *`$FIC_WEB_HOME/<context-name.war>`* to *`<Tomcat Installation Directory>/webapps/`* directory.



2. Click **Manager App**. The Connect to dialog box is displayed.

3. Enter the User Id and Password that has admin rights and click OK. (For user creation in tomcat, see Tomcat User Administration. The **Tomcat Web Application Manager** window is displayed with the list of all the applications deployed.



4. In the Deploy section, enter the Context Path provided during the installation as "/<context-name>".
5. Enter the path where the <context-name>.war file resides (by default "*$FIC_WEB_HOME/*<context-name.war>") in the WAR or Directory URL field and click Deploy.
6. On successful application deployment, a confirmation message is displayed. Start the Tomcat server. For more information, see Starting Infrastructure Services.

Accessing the OFSAA Application

This section gives details about the steps to be performed to access OFSAA Application.

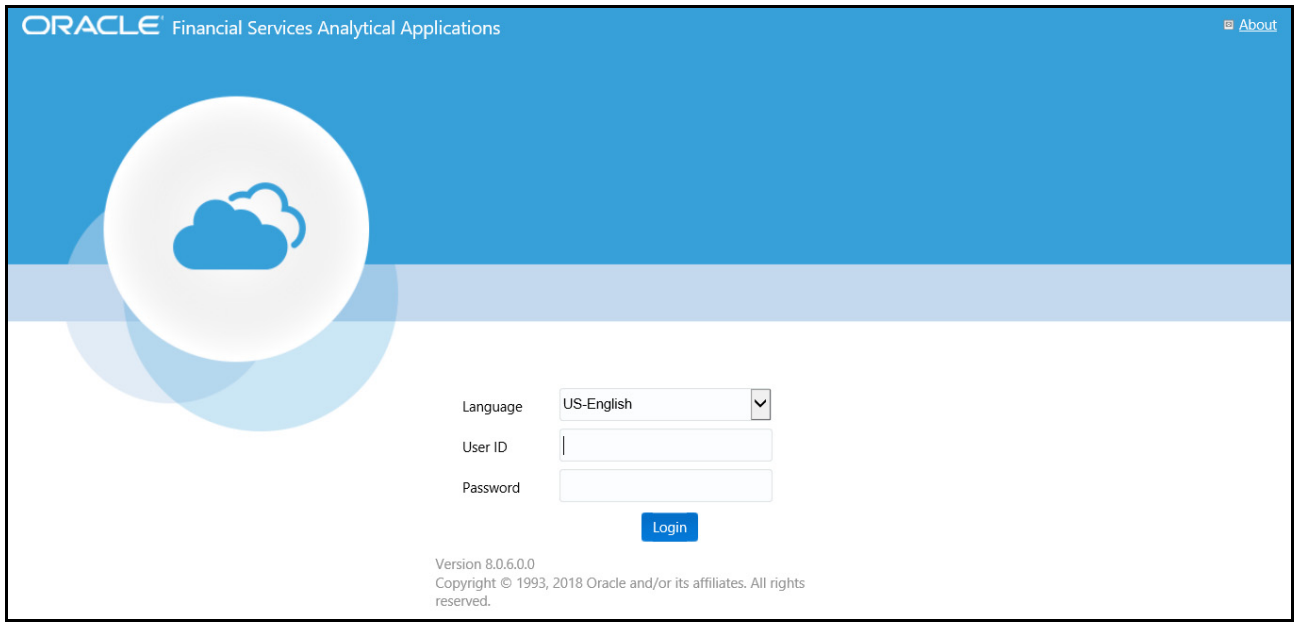
To access the OFSAA application:

1. From a your desktop, open the browser and enter the URL in below format:

   `<scheme>://<IP address/ hostname>:<port>/<context-name>/login.jsp`

   For example: `https://111.222.333.444:5555/ofsaa/login.jsp`

   The OFSAA login window is displayed as below:



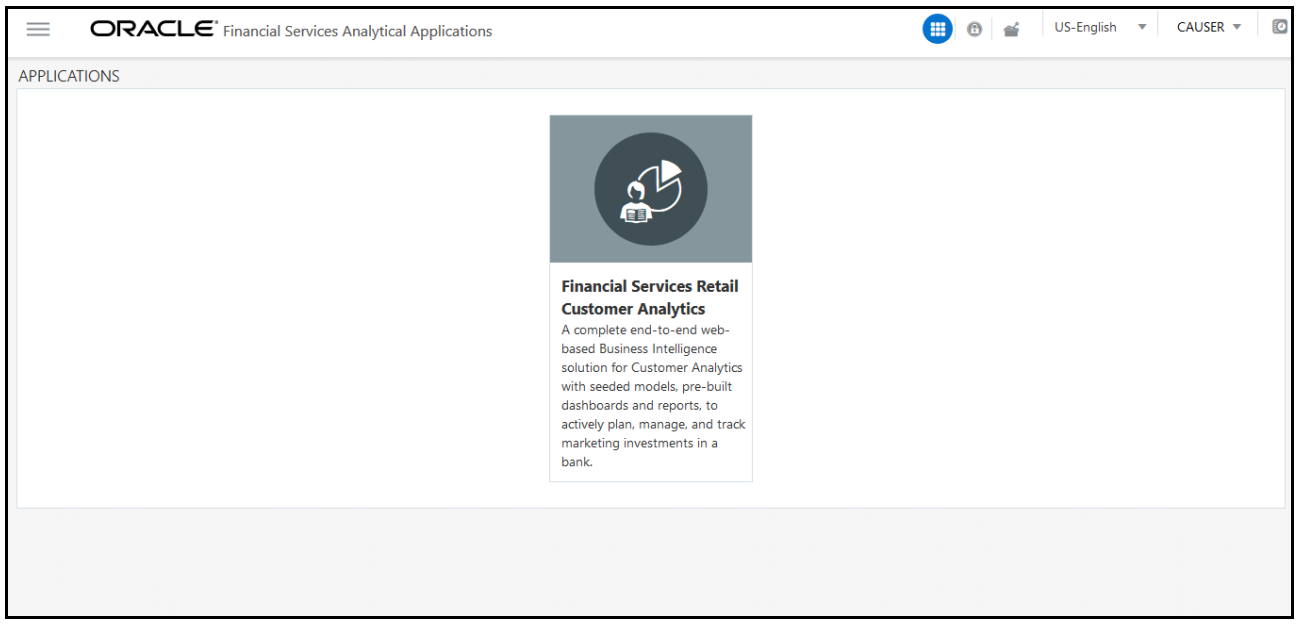
2. With installation of every OFSAA Application Pack, there are two seeded user profiles configured in the system:
   - SYSADMN - System Administrator
   - SYSAUTH - System Authorizer

   Note: For SYSADMN and SYSAUTH, the default password is password0.

3. Login to the application using the "SYSADMN" User ID. (Note that, there is no "I" in the SYSADMN login USER ID). Enter the password that was provided during installation. On the first login, you will be prompted to change the password.

OFSAA Landing Page for CA Administrator

On successful authentication, the OFSAA Landing Page is displayed. This is a common landing page for all users until a preferred application landing page is set by the user in his preferences.



The landing page includes multiple tabs and each tab has specific links to OFSAA Infrastructure and/or Application modules. The tabs and links are displayed based on the OFSAA Application accessed and the access roles mapped to the logged in user.

Each tab contains LHS Menu and RHS Menu. The LHS Menu holds link(s) to modules in a tree structure. The RHS Menu holds link(s) to modules in a navigational panel format.

The following tabs are available in the Landing Page:

- Applications tab
- Object Administration tab
- System Configuration & Identity Management tab

Applications tab

This tab lists the various OFSAA Applications that are installed in the OFSAA setup. The Select Application drop-down list displays the OFSAA Applications, based on the logged in user and mapped OFSAA Application User Group(s). Links to related modules within Applications and Infrastructure are grouped appropriately to maintain a unified experience.

Object Administration tab

This tab lists the various OFSAA Information Domains created in the OFSAA setup. The Select Information Domain drop-down list displays the OFSAA Information Domains based on the logged in user and mapped OFSAA Application User Group(s). Links to modules that enable object traceability and migration of objects are grouped in this tab.

System Configuration & Identity Management tab

This tab lists the OFSAA Infrastructure System Configuration and Identity Management modules. These modules work across Applications/ Information Domains and hence there are no Application and Information Domain drop-down lists in this tab. Links to modules that allow the maintenance of setup installation and identity management tasks are grouped together in this tab.

Note: The navigation path differs from Application to Application. That is, based on the selected Application, the navigation varies.

For more details on how to operate on each tab, see OFSAAI User Guide available in OHC.

RCA and PFT Pack-on-Pack Installation

If you are installing OFS PFT Pack Release v.8.0.7.0.0 on OFA RCA Release v.8.0.6.0.0, then the following tables should be dropped after backup. After that, re-sync the date from the backup of PFT after installation:

- DIM_ORG_UNIT_ATTR
- DIM_ORG_UNIT_B
- DIM_ORG_UNIT_TL
- DIM_GENERAL_LEDGER_HIER
- DIM_COMMON_COA_ATTR
- FSI_ACCOUNT_TYPE_CD
- DIM_GENERAL_LEDGER_TL
- DIM_GENERAL_LEDGER_ATTR
- DIM_GENERAL_LEDGER_B
- DIM_COMMON_COA_B
- DIM_COMMON_COA_TL
- DIM_PRODUCTS_B
- DIM_PRODUCTS_TL
- DIM_PRODUCTS_ATTR

User Group Mapping

Application specific User Group mappings:

- **RCA**:
  - Application Administrator
  - Application Analyst
  - Application Auditor
  - Big Data Administrator
  - Big Data BI Analyst
  - Big Data Data Analyst

Additionally, the following user groups are introduced for GDPR compliance:

- **Data Controller**: This group has the privileges to maintain the PII list and Redaction policies against them. This group also has the privilege to ensure the Right to be Forgotten.
- **Data Security Group**: This group has the privileges to see the PII in un-redacted manner when the reports are accessed through OBIEE.

Create and Deploy the Application Pack Web Archive

On successful installation of the OFSAA Application Pack, the web archive file is automatically generated. However, you need to deploy the generated web archive file on the Web Application Server.

For identifying the location of the generated web archive file and for generating and deploying the web archive file at any time later, see Creating EAR/WAR File and Deploying EAR/WAR File sections.

Note: See the Oracle Financial Services Forms Manager User Guide for instructions on Creating and Deploying the Forms Manager Web Archive.

Patching Your OFS CA Pack Installation

Oracle strongly recommends installing the latest available patch set so as to be up to date with the various releases of the OFSAA Infrastructure product.

See http://support.oracle.com for more information on latest releases.

Excel Upload Mapping and Template

To migrate, follow these steps:

1. Copy the ExcelUpload directory present in $FICHOME/CIRCA/ExcelUpload.
2. Change the name of directory named as infodom in ExcelUpload to respective infodom name.
3. Copy the ExcelUpload directory to ftpshare/STAGE directory.
4. Create STAGE directory in <TOMCAT_HOME>.
5. Copy the ExcelUpload directory to STAGE directory in <TOMCAT_HOME>.

CHAPTER 6 – RPD/ CATALOG DEPLOYMENT FOR OBIEE 11G

This chapter includes the following topics:

Deploying Customer Analytics Pack Dashboards and Analytics

This section covers the following topics:

Installing OBIEE Server

To install Oracle Business Intelligence Enterprise Edition (OBIEE) server, see the Oracle Fusion Middle ware Installation Guide for Oracle Business Intelligence11g Release 1 (11.1.1.9.5). After installing Oracle Business Intelligence Enterprise Edition (OBIEE) server, get the Enterprise Manager URL, username, password, and OBIEE installed directory from the System Administrator.

Note: From the OFS CA Release 8.0.3.0.0 onwards, the OBIEE version 11.1.1.7.1 will not have support and enhancements. All the existing reports work same as the previous versions, but the new developments will not function in 11.1.1.7.1 version of OBIEE.

Installing OBIEE Windows Administration Client

To install OBIEE repository administration client for Windows machine, see the Oracle® Fusion Middle ware Installation Guide for Oracle Business Intelligence11g Release 1 (11.1.1.9.0).

Deploying Customer Analytics Pack Report Analytics

To deploy Analytic Reports, follow these steps:

1. Copy `CIRCA.rpd` and `CIRCA.catalog` files from *`$FIC_HOME/CIRCA/OBIEE/11.1.1.x.x/`* of Web layer to windows machine where the OBIEE windows administration client is installed and deploy. For the more information on deployment, refer to your OBIEE 11g documentation.
2. Open the `CIRCA.rpd` file online with default password as **Admin123**.
3. Configure the Connection Pool details according to the atomic schema.
4. Click **File** menu and then click **Save**.
5. Click **Yes** on the pop-up message Do you want to check global consistency?
6. Click **OK**, on the pop-up message Consistency check didn't find any errors, warning or best practices violations.

Note: Warnings on consistency check can be ignored.

HTML5 Compliance of OBIEE Reports in IE11

Perform the following steps in order to verify the HTML5 compliance of OBIEE reports in IE11:

1. Remove the compatibility settings for analytics.
2. Change the instanceconfig.xml file to make all the chart views to be shown in HTML5 by default.

   You can find the instanceconfig.xml file in the following location:

   OBIEE_HOME/instances/instance1/config/OracleBIPresentationServicesComponent/coreapplication_obips1

   ```
   <Charts>
   <DefaultWebImageType>html5</DefaultWebImageType>
   </Charts>
   ```
3. Enable Mapviewer and D3 reports (to ensure that these reports show up as is).
4. Verify all the BI reports by removing the default chart view setting (to ensure that these reports show up as usual irrespective of HTML5 or flash web Image formats).

Details on OBIEE11.1.9.5

In a browser that does not support the html5 format, the image renders in the flash format instead (which is also interactive).

CHAPTER 7 – RPD/ CATALOG DEPLOYMENT FOR OBIEE12C

This chapter includes the following topics:

Deploying Pack Dashboards and Analytics

This section covers the following tooics:

Installing OBIEE Server

To install Oracle Business Intelligence Enterprise Edition (OBIEE) server, see the Oracle Fusion Middle ware Installation Guide for Oracle Business Intelligence Release 12.2.1.3.0. After installing Oracle Business Intelligence Enterprise Edition (OBIEE) server, get the Enterprise Manager URL, username, password, and OBIEE installed directory from the System Administrator.

Note: From the OFS CA Release 8.0.6.0.0 onwards, the OBIEE version 12.2.1.2.0 will not have support and enhancements. All the existing reports work same as the previous versions, but the new developments will not function in 12.2.1.2.0 version of OBIEE.

Once the OBIEE server is installed, it should be upgraded to the version as mentioned in the Environment section.

Installing OBIEE Windows Administration Client

To install OBIEE repository administration client for Windows machine, see the Oracle® Fusion Middle ware Installation Guide for Oracle Business Intelligence Release 12.2.1.3.0.

Deploying Customer Analytics Application Pack Report Analytics

To deploy Customer Analytics Application Pack Analytic Reports, follow these steps:

1. Copy `CIRCA.rpd` and `CIRCA.catalog` files from *`$FIC_HOME/CIRCA/OBIEE/12.2.1.3.0/`* of Web layer to windows machine where the OBIEE windows administration client is installed and deploy. For the more information on deployment, refer to your OBIEE 12c documentation.
2. Open the `CIRCA.rpd` file online with default password as **Admin123**.
3. Configure the Connection Pool details according to the atomic schema.
4. Click **File** menu and then click **Save**.
5. Click **Yes** on the pop-up message Do you want to check global consistency?
6. Click **OK**, on the pop-up message Consistency check didn't find any errors, warning or best practices violations.

Note: Warnings on consistency check can be ignored.

Post Installation Changes

Do the following changes in the `instanceconfig.xml` file as post installation changes:

1. Backup and edit the `instanceconfig.xml` file located at:

   `$ORACLE_HOME/user_projects/domains/bi/config/fmwconfig/biconfig/OBIPS`

Tag to be changed	Changes

`<Views>`	`<Views>`
	`<Charts>`
	`<DefaultWebImageType>flash</DefaultWebImageType>`
	`</Charts>`
	`</Views>`

<Security>	`<Security>`
	`<CheckUrlFreshness>false</CheckUrlFreshness>`
	`<EnableSavingContentWithHTML>true</EnableSavingContentWithHTML>`
	`</Security>`

2. Save and exit the file.
3. To make Marketing Triggers to work, copy the *`mktgjob`* folder from *`$FIC_HOME/CIRCA/OBIEE/12.2.1.3.0`* folder and replace it in your server where OBIEE is installed as given below:

   `$ORACLE_HOME/user_projects/domains/bi/bidata/service_instances/ssi/metadata/content/catalog/root/system`
4. Restart the presentation server for the changes to take effect.

APPENDIX A - INSTALLATION OF R AND ORACLE R ENTERPRISE (ORE)

This is an optional step and required only if you intend to use Term Structure Parameter Estimation functionality under Rate Management - Interest Rates, for computing term structure parameters. Both Funds Transfer Pricing and Asset Liability Management applications require term structure parameters for all monte carlo engine based calculations (OAS, VaR and EaR).

Following are the prerequisites:

- Install R and Oracle R Enterprise Server on the Oracle Database server. See
- https://docs.oracle.com/cd/E57012_01/doc.141/e57007.pdf
- ORE version supported - Oracle R Enterprise (Server) version 1.4.1

Dependencies

R code of the application requires dependent packages to be installed before the Reporting Line Forecast batch is executed. Usage of the predictive model requires installation of packages - tseries, lattice, and R Oracle. Verify that lattice and R Oracle are compatible with each other.

Package installation instructions can be found at:

http://cran.r-project.org/doc/manuals/r-release/R-admin.html#Installing-packages

Configuration for Oracle R Enterprise

Grant the `RQADMIN` role to atomic schema.

You can grant the `rqadmin` role in SQL*Plus by logging in to the database with DBA privileges and provide the following privilege to Atomic Schema:

`RQADMIN` by executing the command:

```
GRANT RQADMIN TO < atomic_schema>;
```

Configuration for Oracle R Distribution and Oracle R Enterprise (ORE)

This is an optional step. Skip and proceed with the next steps if OFS Enterprise Modeling Application with R scripting is not enabled during installation.

1. Install OFSAAIRunner Package. For more information, see Installing OFS AAAI Runner Package. If you have already installed OFSAAIRunner package (as part of a previous installation), uninstall it (For more information, see Uninstalling OFS AAAI Runner Package section), and reinstall the latest available OFSAAIRunner package.
2. Log in to the database with dba privileges and provide the following privilege to Configuration Schema:

- RQADMIN by executing the command:

  ```
  GRANT RQADMIN TO <config_schema>;
  ```

3. Log in to the database with dba privileges and provide the following privileges to Atomic Schema:
   - CREATE MINING MODEL privilege (to execute the Data Mining models) by executing the command:

     ```
     GRANT CREATE MINING MODEL TO <atomic_schema>;
     ```

Installing OFS AAAI Runner Package

OFSAAIRunner is an R package built by the OFS Enterprise Modeling Application. It is a prerequisite for executing models developed using R scripts. This package helps in:

- Initializing inputs
- Mapping framework variables to R objects
- Configuring possible outputs of the script
- Storing results back to the Database

OFSAAIRunner package (`OFSAAIRunner_1.0.0.tar.gz`) is available under *`$FIC_DB_HOME/lib`*.

Prerequisite

Oracle R & ORE should be installed on the Oracle Database server before installing OFSAAIRunner package.

Use the following procedure to install OFSAAIRunner package:

1. Log in to the OFSAA Server. Navigate to the folder *`$FIC_DB_HOME/lib`*.
2. Copy the file `OFSAAIRunner_1.0.0.tar.gz` in Binary mode to the Oracle Database Server.
3. Log in to the Oracle Database Server with the user using which Oracle Database Server installation is done.
4. Navigate to the directory where the file `OFSAAIRunner_1.0.0.tar.gz` is copied.
5. Install the package by executing the command:

   ```
   ORE CMD INSTALL OFSAAIRunner_1.0.0.tar.gz
   Successful installation is indicated in the installation log as:
   * DONE (OFSAAIRunner)
   Making packages.html ... done
   ```

   Note: The OFSAAIRunner package is installed in *`/usr/lib64/R/library`*.

6. Navigate to the directory *`$ORACLE_HOME/R/library`* and check whether OFSAAIRunner package is listed there by executing the command:

   ```
   ls -l
   ```

Uninstalling OFSAAIRunner Package

Use the following procedure to uninstall the OFSAAIRunner package:

1. Log in to the Oracle Database Server with the same username, using which Oracle Database Server installation is done.
2. Enter ORE in command prompt and execute the command:

   ```
   #ORE
   ```
3. Enter the following command to save workspace image:

   ```
   >remove.packages("OFSAAIRunner")
   ```
4. Enter y when prompted to save the workspace image.

   ```
   q()
   ```
5. Navigate to the directory $ORACLE_HOME/R/library and verify the package is not listed there by executing the command:
6. Save workspace image? [y/n/c]: y

   ```
   ls -l
   ```

Configurations for ORE Execution

Follow this step:

1. Add a TNS entry in tnsnames.ora file with tns name same as that of value set for ORACLE_SID in database server.

Note: For RAC database, follow the aforementioned configuration in all machines.

Configuring 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 directory.
2. Edit `web.xml` file as follows:

   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>
   ```

APPENDIX A - ADDITIONAL CONFIGURATION

The following topics provide detailed module specific post installation configurations.

This appendix includes the following topics:

Configuring FTP/SFTP

This section details about the configurations required for FTP/SFTP.

Adding FTP/SFTP Configuration for File Transfer

In OFSAA, certain modules require transfer of files from the web application server to the OFSAA server over SSH.

Follow these steps to ensure the OFSAA server recognizes the web application server during file transfers.

1. Login to the web application server.
2. Type sftp <user>@<OFSAA Server>
3. Specify Yes when prompted for permission.

   Are you sure you want to continue connecting (Yes/No)?
4. This will add an entry into the "known_hosts" file.
5. A confirmation message is displayed:

   Permanently added <OFSAA Server> RSA) to the list of known hosts.

Setting Up SFTP Private Key

Log in to OFSAA Unix user using Putty tool, where you plan for installation and generate a pair of authentication keys using the `ssh-keygen` command. If required, set passphrase. Otherwise `OFSAAI_SFTP_PASSPHRASE` tag in the `OFSAAI_InstallConfig.xml` file should be set to NA.

To generate private key, enter the commands as shown:

```
ofsaapp@OFSASERVER:~> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ofsaapp/.ssh/id_rsa):
Created directory '/home/ofsaapp/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ofsaapp/.ssh/id_rsa.
Your public key has been saved in /home/ofsaapp/.ssh/id_rsa.pub.
The key fingerprint is:
3e:4f:05:79:3a:9f:96:7c:3b:ad:e9:58:37:bc:37:e4
ofsaapp@OFSASERVER:~> cat /home/ofsaapp/.ssh/id_rsa.pub >> /home/ofsaapp/.ssh/
authorized_keys
```

In case, you are generating SFTP Private key for Hive server, append the content of */home/ofsaapp/.ssh/id_rsa.pub* to Hiveserver authorized_keys file located at *$HOME_DIR_HIVE/.ssh* folder.

Ensure the following permissions exist for the given folders:

- Permission of .ssh should be 700
- Permission of .ssh/authorized_keys should be 640
- Permission of .ssh/id_rsa should be 400
- Permission of Unix user created should be 755

Configure Infrastructure Server Memory

The memory settings for Infrastructure Application Server, Tomcat, WebSphere, and WebLogic can be edited for customizing memory settings and garbage collector settings depending on the available hardware configuration as explained below. These settings are base minimum and has to be incremented considering the deployment metrics into account. The increments are usually handled in multiples of 128mb for heap and 64mb for stack.

Infrastructure Application Server Memory Settings

You can configure the Infrastructure Application Memory settings as follows:

1. Locate .profile file.
2. Edit X_ARGS field in this file for customizing memory settings and garbage collector settings depends on the hardware configuration.

   This has a default value `X_ARGS="-Xms200m"`

   ```
   X_ARGS=" "$X_ARGS" $DELIM -Xmx2048m"
   ```

Note: Modify X_ARGS_APP variable in the .profile file to customize Java Memory Settings for Model Upload based on the Data Model size.

For Run and Rule executions, the following value is recommended:
X_ARGS_RNEXE="-Xms1g -Xmx1g
XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=512M -XX:+UseParallelOldGC -XX:+DisableExplicitGC"

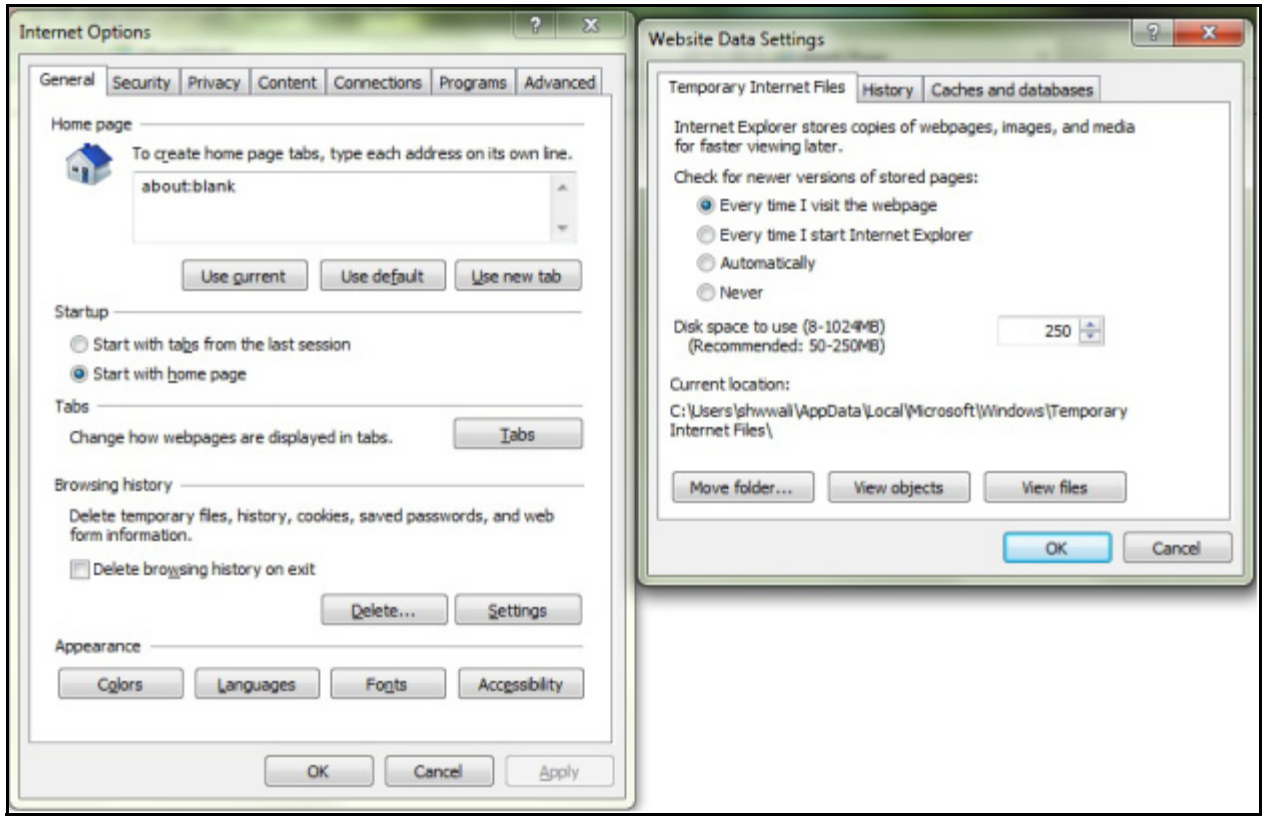
X_ARGS_RLEXE="-Xms1g -Xmx1g -XX:+UseAdaptiveSizePolicy -XX:MaxPermSize=512M
XX:+UseParallelOldGC -XX:+DisableExplicitGC"

Internet Explorer Settings

Note: OFSAAI supports only default zoom setting in Internet Explorer, that is, 100%. Cookies should be enabled.

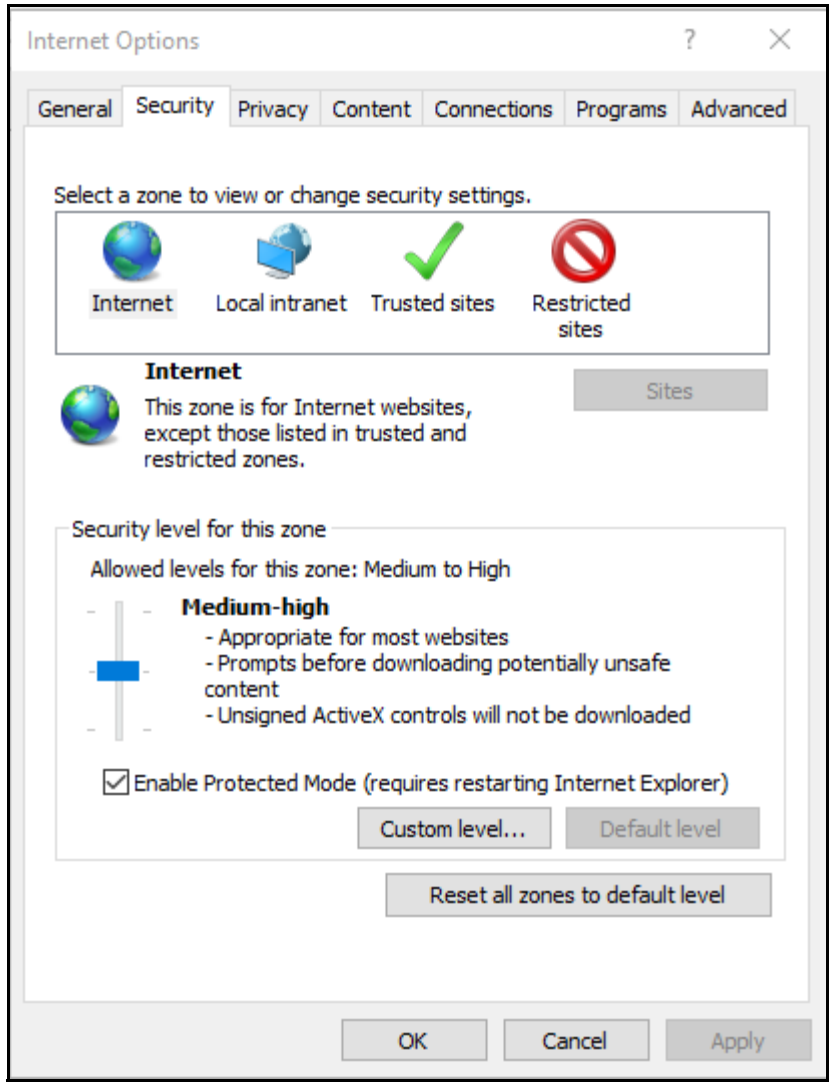
The following browser settings have to be specified at every client machine prior to accessing the Infrastructure application:

1. Open Internet Explorer. Select Tools > Internet Options. The Internet Options window is displayed.
2. Click the Settings button. The Settings window is displayed.
3. Select the option Every time I Visit the webpage and click OK.



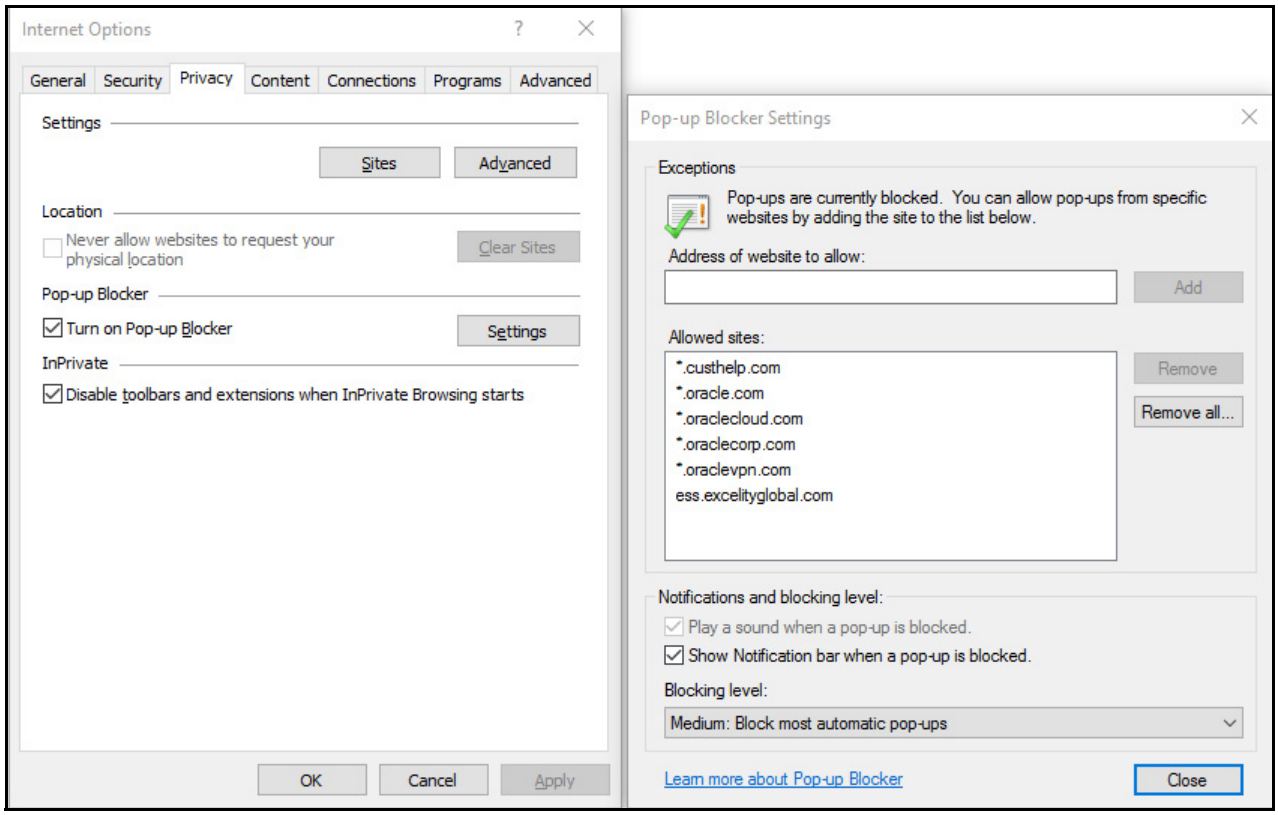
4. In the Internet Options window, select the **Security** tab and select the **Internet option** under **Select a zone to view or change the security** settings.

5. Click **Default Level** under **Security level for this zone**.



6. Click **OK** to save.

7. In the **Internet Options** window, select the **Privacy** tab and select the **Turn on Pop-up Blocker** option under **Pop-up Blocker** settings.



8. Click **Settings**. The Pop-up Blocker Settings window is displayed.
9. Enter the URL of the OFSAA Application in the **Address of Website to Allow:** field.
10. Click **Add**. The OFSAA URL is displayed in the **Allowed Sites** section.
11. Click **Close**.
12. Click **OK** in the Internet Options window.

Retrieving Patch Information

To identify the list of patches installed on your OFSAA setup, follow these steps:

1. Login to the OFSAA application as a user with Object AdminAdvanced Role.
2. Navigate to **Object Administration** tab, expand **Utilities** and click **Patch Information**.
3. The window displays the list of patches installed on the OFSAA setup across Applications/ Platform.

OLAP Data Server Configuration

This section is applicable if you are using the OLAP feature of OFSAAI.

The following parameters must be set to ensure that the system limitations are not exceeded at any stage. The values for these OS parameters should be specified based on the expected load at each implementation site.

Example:

Process Memory Limit

Max Thread Stack Size

Max Number of Threads per Process

- Sort Buffer settings: This must be set at the Essbase application level appropriate to the anticipated load.
- Shutdown and Restart: During shutdown of OFSAAI Server that has an instance of Data Services that is communicating with an OLAP Data Server, it is imperative to ensure that the cleanup of the old instance is completed on the OLAP Data Server before restarting the OFSAAI Server. Pause for a period of time based on the load the system was subjected to, before restarting the Data Services subsystem.

Changing IP/ Host name, Ports, Deployed Paths of the OFSAA Instance

For information on this section, see the OFS Analytical Applications Infrastructure Administration User Guide.

OFSAAI Setup Information Fetching Tool

Executing the SetupInfo.jar file available in the FIC_HOME path will help you retrieve the related information about the OFSAAI Set up such as Operating System Name and version, Database Type and Version, OFSAAI architecture, Log file locations and so on.

To execute `SetupInfo.jar` in console:

1. Navigate to the path *`$FIC_HOME`*.
2. Enter the command:

   ```
   java -jar SetupInfo.jar
   ```

   After execution, the output file location is displayed in the console.

Encryption Changer

This utility helps you to regenerate the new AESCryptKey.ext file and encrypt all the encrypted values of the OFSAAI setup according to the new key.

To execute `EncryptC.jar` in console:

1. Navigate to the path $FIC_HOME.
2. Enter the command:

   ```
   java -jar EncryptC.jar
   ```

3. A confirmation message is displayed after execution.

Once executed, you need to create and deploy the EAR / WAR file depending on the configured Web Application Server. For more information, see Creating EAR/WAR File and Deploying EAR/WAR File sections.

Infrastructure LDAP Configuration

For more information on LDAP configuration, see the OFS Analytical Applications Infrastructure Administration User Guide.

Configure OFSAAI Web Services

Web Services in OFSAAI is meant for exposing a web service to "asynchronously" or "synchronously" execute requested tasks offered by OFSAAI. The configuration steps given below are to be done only if you are using the Web Services feature of OFSAAI.

Configure DynamicWSConfig.xml File

For each third party web service that needs to be accessed using the OFSAAI Web services framework and the operations to be invoked, corresponding entries are to be made in the `DynamicWSConfig.xml` template file.

The variable `<WebServer>` denotes any one of the application server, i.e. WebSphere, WebLogic, or Tomcat.

The `DynamicWSConfig.xml` file will be available in the *`<OFSAAI Installation Directory>/EXEWebService/<WebServer>/ROOT/conf`* directory. This file can be placed in any directory that is accessible by the application and this location must be specified in the web.xml file, as `WSCONFIGFILE` parameter.

The `DynamicWSConfig.xml` template file will be in *`<WebServer Deployment Path>/ EXEWebService.ear/EXEWebService.war/conf`* directory.

This template is given below:

```
<XML>
    <WEBSERVICES>
    <WEBSERVICE CODE="$CODE"
    ENDPOINT="$ENDPOINT" TARGETNAMESPACE="$TARGETNAMESPACE"
    XMLNS_XSD="$XMLNS_XSD" ENCODINGSTYLE="$ENCODINGSTYLE"
    SERVICENAME="$SERVICENAME" PORTTYPENAME="$PORTTYPENAME"
    SESSION_MAINTAIN_PROPERTY="$SESSION_MAINTAIN_PROPERTY"
    USERNAME="$USERNAME"
    PASSWORD="$PASSWORD" STYLE="$WEBSERVICESTYLE"
    STUBIMPLEMENTATION="$STUBIMPLEMENTATION">
    <OPERATION CODE="$CODE"
    NAME="$NAME"
    SOAPACTION="$SOAPACTION"
    STYLE="$STYLE"
```

```
        PACKAGENAME="$PACKAGENAME">
        <INPUT ORDER="$ORDER"
        PARAMNAME="$PARAMNAME"
        ARGTYPE="$ARGTYPE"
        CLASSNAME="$CLASSNAME"/>
        <OUTPUT PARAMNAME="$PARAMNAME"
        RETURNTYPE="$RETURNTYPE"
        CLASSNAME="$CLASSNAME"/>
        </OPERATION>
        </WEBSERVICE>
        </WEBSERVICES>
    </XML>
```

The `DynamicWSConfig.xml` has the placeholders as tabulated below. These have to be updated depending on the web service chosen and the mode of accessing it. For each Web service to be accessed, the entire web service tag in the `DynamicWSConfig.xml` file must be repeated. The placeholders tabulated below should be set in accordance to the parameters published in the third party wsdl files (web-services) to be accessed. The stub class specified must implement the "`com.iflex.Oracle Reveleus.execution.webservice.EXEWebIF`" interface.

Attributes for WEBSERVICE tag

Placeholder	Description
$CODE	Unique number within the xml file and cannot be 999 or 0.
$ENDPOINT	soap: address location in the wsdl: service name tag of the wsdl file.
$TARGETNAMESPACE	The attribute value for the targetNamespace of the wsdl: definitions tag.
$XMLNS_XSD	The attribute value for the xmlns:s of the wsdl:definitions tag.
$ENCODINGSTYLE	The attribute value for the xmlns:soapenc of the wsdl:definitions tag.
$SERVICENAME	Name of the service found under the wsdl:service name tag of the wsdl file.
$PORTTYPENAME	wsdl port type name as mentioned in the wsdl file.
$SESSION_MAINTAIN_PROPERTY	This could be given as "" also.
$USERNAME	User name to access the web services. Enter "" if no user name is required.
$PASSWORD	Password to access the web services. Enter "" if no password is required.
$WEBSERVICESTYLE	This can take either "rpc" in case of DII mode of invoking web services or "stub" in case of static mode. This is a mandatory parameter.
$STUBIMPLEMENTATION	Fully qualified class name (package name.classname).

Attributes for OPERATION tag

Ensure that the "operation tag attributes" are repeated for each of the operation tags.

Placeholder	Description
$CODE	Should be unique within the Web service tag.
$NAME	The name of the Function that is to be called by the wsdl file.
$SOAPACTION	The URL for the Operation to access. This is associated with the Operation tag of the wsdl file.
$STYLE	This can take "rpc" if the web services invoking is in DII mode or "stub" if it is in static mode. This is a mandatory parameter.
$PACKAGENAME	Represents the JAXB package of input object.

Attributes for INPUT tag

Placeholder	Description
$ORDER	The sequential number of the INPUT tag. Should start from 0. This is in line with the input order of the arguments that the API accepts which is called by this operation.
$PARAMNAME	Input parameter name to be called by the wsdl file.
$ARGTYPE	Input Parameter Data Type. If the input argument type is complex object, specify $ARGTYPE as "xmlstring".
$CLASSNAME	Represents class name of input object parameter.

Attributes for OUTPUT tag

Placeholder	Description
$PARAMNAME	Output parameter name to be returned by the web service.
$RETURNTYPE	Output parameter Data Type. If the web service response is a complex object, then specify $RETURNTYPE as "object".
$CLASSNAME	Represents class name of output object parameter.

web.xml Entries

This step is optional and required only if the web application server used is Tomcat. In case of any other application server, skip and proceed with next step.

1. Navigate to *$FIC_HOME/webroot/WEB-INF/* and edit the web.xml file. Set parameter value DOCSERVICEAPP to EXEWebServiceAXIS.
2. Navigate to *<OFSAAI Installation Directory>/EXEWebService/<WebServer>/ROOT/WEB-INF/* and edit the web.xml file as explained below.

Note: In case of Java 7 when WebLogic is used as web application server replace following line of *<OFSAAI Installation Directory>/EXEWebService/Weblogic/ROOT/WEB-INF/web.xml* file that is

```
<?xml version='1.0' encoding='UTF-8'?>
<web-app id="WebApp_ID" version="3.0"
xmlns="http://java.sun.com/xml/ns/javaee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd" metadata-complete="true">
```

with

```
<?xml version='1.0' encoding='UTF-8'?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

Entry for WSConfig File

The WSCONFIG file (DynamicWSConfig.xml) is available in the *<WebServer Deployment Path>/EXEWebService.ear/EXEWebService.war/conf* directory. This file can be placed in any directory that is accessible by the application.

The path where the WSCONFIG file is placed must be specified in place of *$WSCONFIGFILELOCATION$* in the below block of text in web.xml.

```
<context-param>
    <description>WebServices Configuration File</description>
    <param-name>WSCONFIGFILE</param-name>
    <param-value>$WSCONFIGFILELOCATION$</param-value>
    <!--Specify the Location of DynamicWSConFig.xml-->
</context-param>
```

Proxy Settings

Replace the following <param-value> given in bold in the following block of text in web.xml file, with appropriate values.

If no values are required, leave the <param-value> blank.

```
<context-param>
   <description>http Proxy Host</description>
   <param-name>http.proxyHost</param-name>
   <param-value>$PROXYHOST$</param-value>
   <!-- Specify the IP address or hostname of the http proxy server-->
</context-param>
<context-param>
   <description>http Proxy Port</description>
   <param-name>http.proxyPort</param-name>
   <param-value>$PROXYPORT$</param-value>
   <!--Port Number for the Proxy Server-->
</context-param>
<context-param>
   <description>http proxy UserName</description>
   <param-name>http.proxyUserName</param-name>
   <param-value>$PROXYUSERNAME$</param-value>
   <!-- User ID To get authenticated by proxy server-->
</context-param>
<context-param>
   <description>http proxy Password</description>
   <param-name>http.proxyPassword</param-name>
   <param-value>$PROXYPASSWORD$</param-value>
   <!-- User Password To get authenticated by proxy server-->
</context-param>
<context-param>
   <description>http non-ProxyHosts</description>
   <param-name>http.nonProxyHosts</param-name>
   <param-value>$NONPROXYHOST$</param-value>
   <!--Hosts for which the proxy settings should get by-passed (Note: Separate them by
   "|" symbol) -->
</context-param>
```

OFSAAI Home Entry

This entry should point to the Application layer / Web layer of the OFSAAI installation and should be accessible.

Replace `$FIC_HOME$` in the following block of text in `web.xml` with <*WebServer Deployment Path*>/*EXEWebService.ear/EXEWebService.war*.

```
<context-param>
    <description>OFSAAI Web Home</description>
    <param-name>FIC_HOME</param-name>
    <param-value>$FIC_HOME$</param-value>
    <!--OFSAAI Installation Folder-->
</context-param>
<context-param>
    <description>OFSAAI Web Home</description>
    <param-name>FIC_PHYSICAL_HOME</param-name>
    <param-value>$FIC_HOME$</param-value>
    <!--OFSAAI Installation Folder-->
</context-param>
```

DynamicWSConfig.xml

For each third party web service that needs to be accessed using the OFSAAI Web services framework, and the operation to be invoked, make corresponding entries into this file. This file is to be placed in the location that is specified in the web.xml, as `WSCONFIGFILE` parameter.

Deploy OFSAAI Web Services

You can deploy OFSAAI Web Services separately if you had not configured OFSAAI Web Services as part of the installation.

1. Complete the manual configuration of OFSAAI Web Services.
2. Navigate to *<OFSAAI Installation Directory>/EXEWebService/<WebServer>* and execute the command:

   ```
   ./ant.sh
   ```
3. This will trigger the EAR/WAR file creation, which is required for the deployment.
4. Deploy the generated EXEWebService.EAR/EXEWebService.WAR file into the Web Server.

If you have already configured OFSAAI Web Services as part of the installation, deploy the generated EXEWebService.EAR/ EXEWebService.WAR file into the OFSAAI Deployment area in Web Server profile.

Configuration to Enable Parallel Execution of DML Statements

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

As of now, the `OracleDB.conf` file has only one parameter namely `CNF_DEGREE_OF_PARALLELISM`. This parameter indicates the degree of parallelism to be used for a DML operation if parallel DML is explicitly enabled in the session with the `ENABLE PARALLEL DML` clause of the `ALTER SESSION` statement. 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.

Configure Message Details in Forms Designer

You can configure the Message Details in Forms Designer under Data Entry Forms and Queries module by updating the details of mail server in the `"NotificationConfig.cfg"` file which resides in the path *`$FIC_APP_HOME/common/FICServer/conf`*.

Ensure that the "authorized User details" for whom you need to configure the Message details are included in **Administration > Security Management > User Administrator > User Maintenance** window.

Update the following parameters in the `"NotificationConfig.cfg"` file:

Parameter	Description
SMTP_SERVER_IP	Specify the host name or IP address of SMTP Server.
SMTP_DEBUG_MODE	To run SMTP service in Debug mode, set value to 'true', otherwise set value to 'false'.
SMTP_AUTHORIZATION	Set to 'true' if SMTP server requires the client to be authenticated, otherwise set to 'false'.
SMTP_USERNAME	Username required for logging into SMTP server, if authentication is not required use a dummy value.
SMTP_PASSWORD	Password required for logging into SMTP server, if authentication is not required use a dummy value.
SMTP_MAILID	If the Messages has to go from a Particular ID that ID need to be added. Exchange server forces you set a valid ID that is there in the exchange server (Based on Security settings).

Ensure that the authorized User details are included in **Administration > Security Management > User Administrator > User Maintenance** window.

Clearing Application Cache

This is applicable to all Web Servers (i.e. WebSphere, WebLogic, and Tomcat).

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

- **Tomcat**: *<Tomcat installation folder>/work/Catalina/localhost/<Application name>/org/apache/jsp*
- **WebLogic**: *<Weblogic installation location>/domains/<Domain name>/servers/<Server name>/tmp/_WL_user/<Application name>/qaelce/jsp_servlet*
- **WebSphere**: *<Websphere installation directory>/AppServer/profiles/<Profile name>/temp/<Node name>/server1/<Application name>/<.war file name>*

Configuring Password Changes

This section explains about how to modify the OFSAA Infrastructure Config Schema and Atomic Schema passwords.

OFSAA Infrastructure Config Schema Password Modification

To change the Config Schema password, perform the following steps:

1. Change the Config schema User Password in the database.
2. Delete the $FIC_HOME/conf/Reveleus.SEC file.
3. Shutdown the OFSAAI App service:

   ```
   cd $FIC_APP_HOME/common/FICServer/bin
   ./stopofsaai.sh
   ```

4. Start the Infrastructure Server in foreground directly on the server or through X-Windows software using the command:

   ```
   ./startofsaai.sh
   ```

   At the prompt, enter System Password. Enter the "new Config schema" password. The service will start and initialize itself if it is able to successfully connect to the DB.

5. Post successful startup of the service, if required, the Infrastructure server may be shut down and restarted in the background using nohup mode.

OFSAA Infrastructure Atomic Schema Password Modification

To change the Atomic Schema password, perform the following steps:

1. Change the Atomic schema User Password in the database.
2. Login to the application from the browser using SYSADMN account or any user id, which has System Administrator role mapped.
3. Navigate to System Configuration > Database Details window. Modify the password as explained in the following steps:

- From the Database Master window, select the connection whose password you want to modify and click button from the tool bar.
- Click button corresponding to the Alias Name. The Alias Details window is displayed.
- Modify the password in the Auth String field.

4. If you are using Apache Tomcat as Web server, update the <Context> -> Resource tag details in Server.xml file from the $CATALINA_HOME/conf folder. (In case of Tomcat only Atomic <Resource> will exist).
5. If you are using WebSphere as Web server:
   a. Login to the WebSphere Administration Console, from the left side menu.
   b. Navigate to Resources >JDBC >Data Sources. A list of data sources will be populated on the right side.
   c. Select the appropriate Data Source and edit the connection details. (In this case, both Config and Atomic data sources will need to be modified).
6. If you are using WebLogic as Web server:
   a. Login to the WebLogic Administration Console, from the left side menu.
   b. Under Domain Structure list box, expand the appropriate Domain and navigate to Services > JDBC >Data Sources. A list of data sources will be populated on the right side.
   c. Select the appropriate Data Source and edit the connection details. (In this case, both Config and Atomic data sources need to be modified).
7. Restart the OFSAAI services.

Configuring Java Virtual Machine

While running several database intensive tasks in parallel, fetching the database connection from connection pool may face an error. To ensure no such error is encountered, add the line `securerandom.source=file:/dev/./urandom` in the `java.security` configuration file available in *`$JAVA_HOME/jre/lib/security/`* path.

This needs to be configured on all the machines or virtual machines where the OFSAAI database components (ficdb layer) are installed.

Configure Internal Service (Document Upload/ Download)

This step can be ignored if it has already been configured as part of any previous IR/ML installation.

The Document Upload/Download feature has undergone a change and can now be configured to use Internal service for document upload/ download instead of the earlier ExeWebService.

To facilitate Internal service for document upload/ download, perform the following configurations:

1. Create the folders download, upload, TempDocument and Temp in the local path of Web application server and provide Read/Write permission.
   - To find the exact location, execute the following query in CONFIG schema:

     ```
     select localpath from web_server_info
     ```
   - To create folders with Read/Write permission, execute the command:

     ```
     mkdir -m 777 download upload TempDocument Temp
     ```
2. Create DocStorage folder in the FTPSHARE location of APP tier and provide Read/Write permission.

- To find the exact location, execute the query in CONFIG schema:

  ```
  select ftpdrive from app_server_info
  ```

- To create folder with Read/Write permission, execute the command:

  ```
  mkdir -m 775 DocStorage
  ```

By default, the parameter `DOCUMENT_SERVICE_TYPE_EXTERNAL` value is set to `FALSE` in the Configuration table in CONFIG schema and hence the application "ExeWebService" will not be used. It is recommended that the value to be set to `FALSE` and use the Internal service for document upload/ downloads. If you intend to continue using the External ExeWebService, set the value to `TRUE`.

Navigate to *`$FIC_HOME/EXEWebService/<WEBSERVER_TYPE>`* directory of WEB tier and type `./ant.sh`. This triggers the creation of EAR/WAR file `EXEWebService.ear/.war`. The EAR/WAR file `EXEWebService.ear/.war` will be created in *`$FIC_HOME/EXEWebService/<WEBSERVER_TYPE>`* directory of WEB tier. Redeploy the generated EAR/WAR file onto your configured web application server.

APPENDIX A - CLONING OF AN OFSAA INSTANCE

There is a consistent need for a faster and effective approach of replicating an existing OFSAA instance for further project developments, that is, setting up OFSAA instances that are exact copies of the current OFSAA instance. For more information on cloning, see OFSAA Cloning Reference Guide.

APPENDIX A - POST DEPLOYMENT CONFIGURATION

This chapter covers the following topics:

Logging as System Administrator

Post installation, the first login into Infrastructure is possible only for a System Administrator through user id "sysadmn". This ID is created at the time of installation with the password provided during installation. Enter login id "sysadmn" and password that was provided during installation. Click Login.

System Administrator

System Administration refers to a process of managing, configuring, and maintaining confidential data in a multi-user computing environment. System Administration in Security Management involves creating functions, roles, and mapping functions to specific roles. System Administration also involves maintaining segment information, holiday list, and restricted passwords to ensure security within the Infrastructure system.

You can access System Administrator in LHS menu of Security Management. The options available under System Administrator are:

- Function Maintenance
- Role Maintenance
- Segment Maintenance
- Holiday Maintenance
- Restricted Passwords

Function Maintenance

A function in the Infrastructure system defines the privileges to access modules or components and to define or modify Metadata information associated. Function Maintenance allows you to create functions for users to ensure only those functions are executed which are specific to the user's role.

You can access Function Maintenance by expanding **System Administrator** section within the tree structure of LHS menu. The Function Maintenance window displays the function details such as Function Code, Function Name, Description, and the number of Roles Mapped to the function. The Function Maintenance window also facilitates you to view, create, modify, and delete functions within the system.

You can also make use of Search and Pagination options to search for a specific function or view the list of existing functions within the system.

Role Maintenance

A role in the Infrastructure system is a collection of functions defined for a set of users to execute a specific task. You can create roles based on the group of functions to which users are mapped.

You can access Role Maintenance by expanding System Administrator section within the tree structure of LHS menu. The Role Maintenance window displays the role details such as Role Code, Role Name, Role Description, and the number of Users Mapped to the role. The Role Maintenance window also facilitates you to view, create, modify, and delete roles within the system.

You can also make use of Search and Pagination options to search for a specific role or view the list of existing roles within the system.

Segment Maintenance

Segment is used to control access rights on a defined list of objects. It is mapped to an information domain.

Segment Maintenance in the Infrastructure system facilitates you to create segments and assign access rights. You can have different segments for different Information Domains or same segments for different Information Domains.

User scope is controlled by segment/ folder types with which the object is associated.

- Objects contained in a public folder will be displayed irrespective of any user.
- Objects contained in a shared folder will be displayed if user belongs to a user group which is mapped to an access type role with the corresponding folder.
- Objects contained in a private folder will be displayed only to the associated owner.

You can access Segment Maintenance by expanding System Administrator section within the tree structure of LHS menu. The Segment Maintenance window displays a list of available segments with details such Domain, Segment Code, Segment Name, Segment Description, Segment/Folder Type, Owner Code, and the number of Users Mapped to the segment. You can view, create, modify, and delete segments within the Segment Maintenance window.

You can also make use of Search and Pagination options to search for a specific role or view the list of existing roles within the system.

Holiday Maintenance

Note: As part of OFSAAI 7.3.3.0.0 release, this feature will not be available if Authentication is configured to SSO Authentication and SMS Authorization.

Holiday Maintenance facilitates you to create and maintain a schedule of holidays or non-working days within the Infrastructure system. On a holiday, you can provide access to the required users and restrict all others from accessing the system from the User Maintenance window.

You can access Holiday Maintenance by expanding System Administrator section within the tree structure of LHS menu. The Holiday Maintenance window displays a list of holidays in ascending order. In the Holiday Maintenance window you can create and delete holidays.

Restricted Passwords

Note: As part of OFSAAI 7.3.3.0.0 release, this feature will not be available if Authentication Type is selected as SSO Authentication and SMS Authorization from System Configuration> Configuration.

Restricted Passwords facilitates you to add and store a list of passwords using which users are not permitted to access the Infrastructure system.

You can access Restricted Passwords by expanding System Administrator section within the tree structure of LHS menu. The Restricted Passwords window displays a list of restricted passwords and allows you to add and delete passwords from the list.

You can also make use of Search and Pagination options to search for a specific password or view the list of existing passwords within the system. For more information, refer Pagination and Search & Filter.

Note: While searching for any pre-defined restricted password, you have to key in the entire password.

Creating Application Users

Create the application users in the OFSAA setup prior to use.

Note: This step may not be required if you have already setup users in the OFSAA setup.

For more information refer user creation section from the Oracle Financial Services Analytical Applications Infrastructure User Guide.

Mapping Application User(s) to User Group

Starting the OFSAA 8.0 release, with installation of Customer Application Pack, pre-configured application user groups are seeded. These user groups are unique to every OFSAA Application Pack and have application roles pre-configured.

Map the application user(s) to the respective Application User Group(s) and subsequently authorize the entitlements by logging in as SYSAUTH (System Authorizer) user.

For more information on seeded User Groups, refer to User Group Mapping.

Change ICC Batch Ownership

All the seeded Batches in Customer Analytics Applications Pack will be automatically assigned to SYSADMN user during Installation. If one user who wants to see the Batches in Batch Maintenance Menu, He needs to execute the following Queries in Config Schema of the Database.

Syntax:

```
begin
AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP ('fromUser','toUser','infodom');
end;
OR
begin
AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP ('fromuser','touser');
end;
```

Where from User indicates the user who currently owns the batch, to User indicated the user to which the ownership has to be transferred. Infodom is optional parameter, if specified the ownership of batches pertaining to that Infodom will be changed.

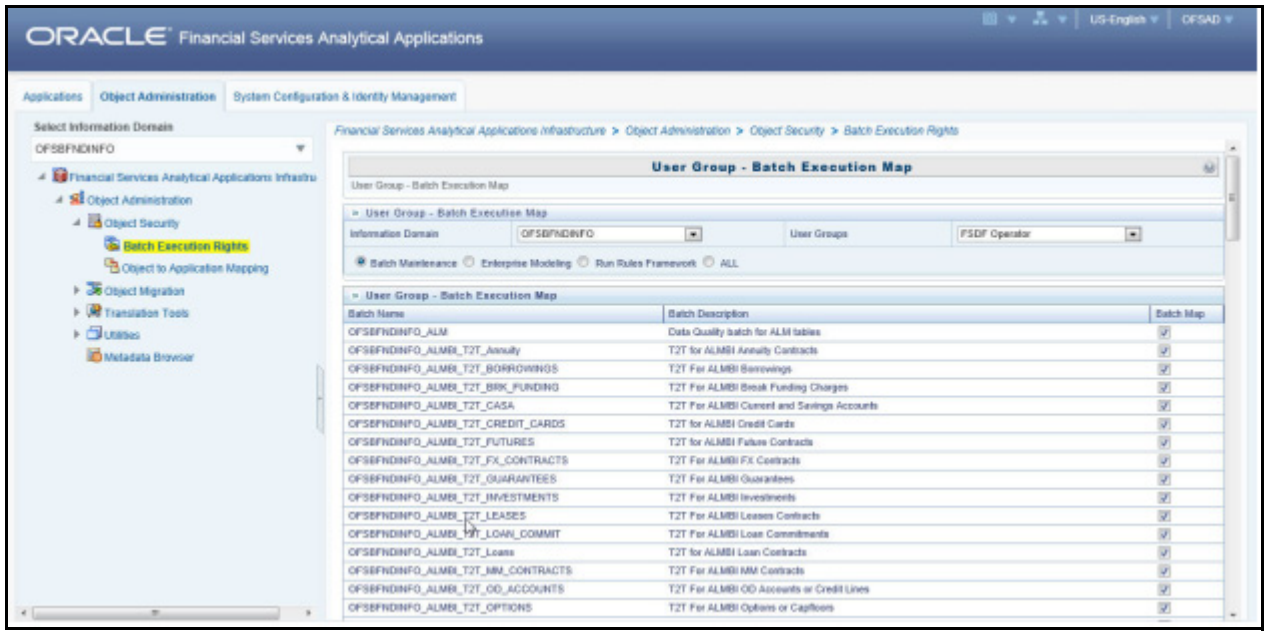
Example:

```
begin
AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP ('SYSADMN','CIRCAOP','OFSCIRCAINFO');
end;
```

Mapping ICC Batch Execution Rights to User

Login as SYSADMN and navigate to **Identity Management > System Administrator > Function-Role Map**. Map the User-Batch Execution Mapping Screen function to RLCIRCAADMIN role.

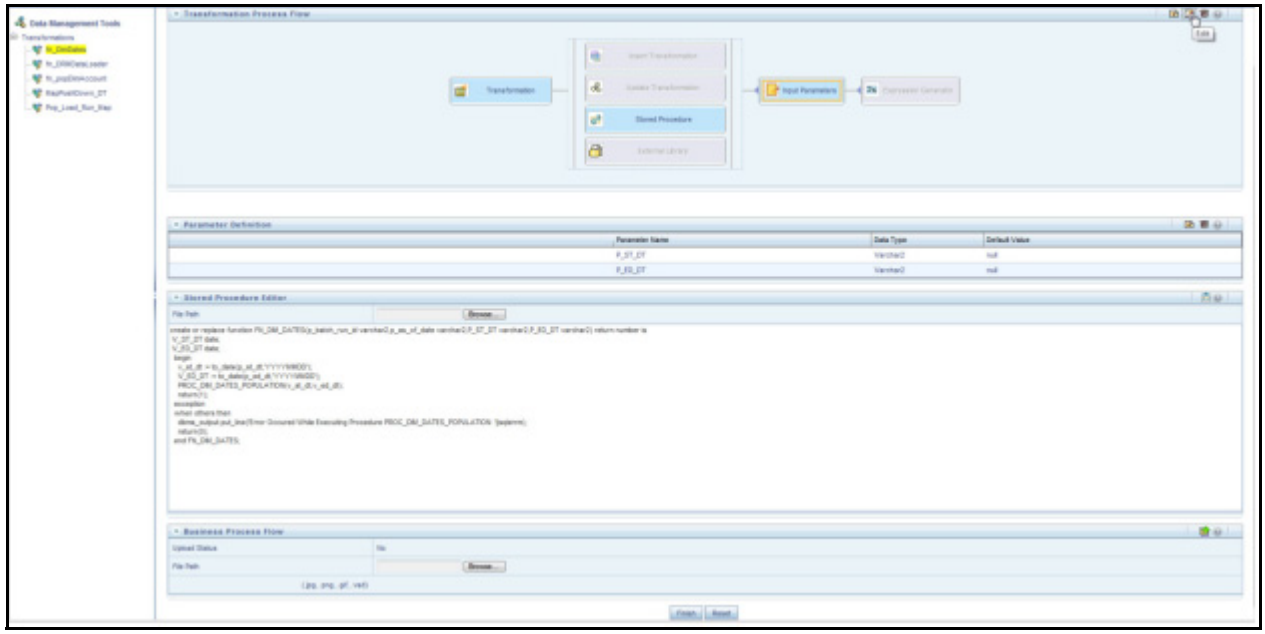
Now any user who is mapped under CA Admin User Group will have the access to the **Batch execution rights** Menu under **Operations** list.



Saving Post- Load Change Transformations

After creating users, Login to Infrastructure as any user who is mapped to CA Admin or CA Analyst group. Navigate to **Data Management Framework >> Post Load Changes**.

A New window will be displayed. Click on Each Transformation from Transformations List & Click on Stored Procedure in the Right Panel, Click on Edit in the Top Right Menu and Click on Finish button in Bottom.



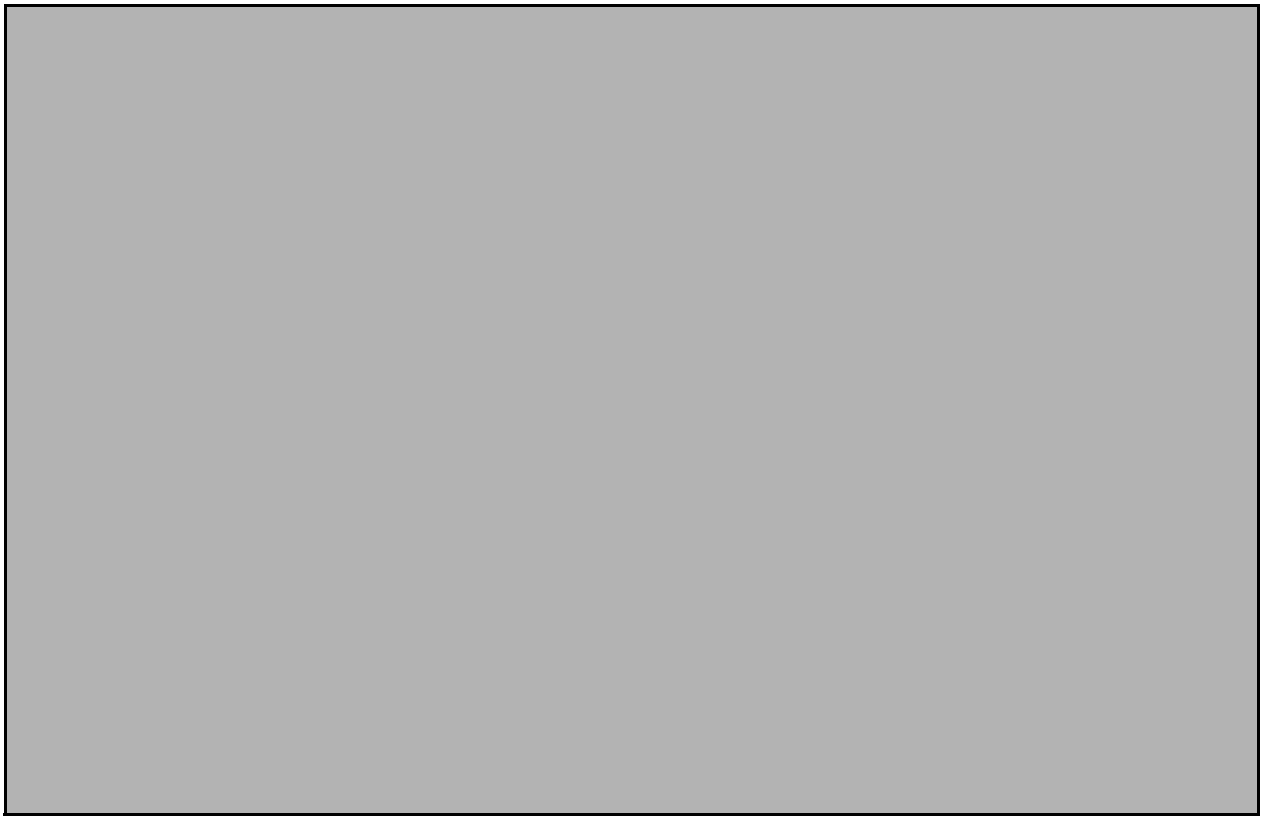
All the Transformation Stored Procedures are required to be edited and saved (Finish Button) once for getting it is available.

Internet Explorer Settings

Note: OFSAAI supports only default zoom setting in Internet Explorer, that is, 100%. Cookies should be enabled.

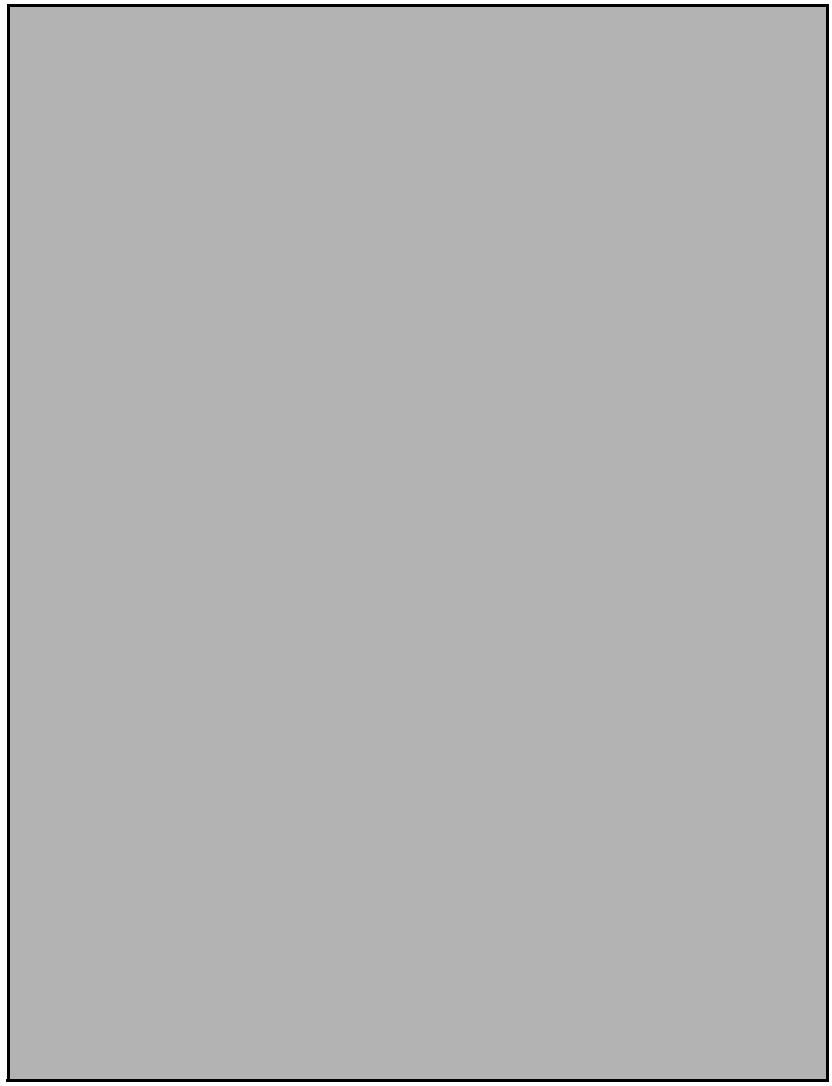
The following browser settings have to be specified at every client machine prior to accessing the Infrastructure application:

1. Open Internet Explorer. Select Tools > Internet Options. The Internet Options window is displayed.
2. Click the Settings button. The Settings window is displayed.
3. Select the option Every time I Visit the webpage and click OK.



4. In the Internet Options window, select the **Security** tab and select the **Internet option** under **Select a zone to view or change the security** settings.

5. Click **Default Level** under **Security level for this zone**.



6. Click **OK** to save.

7. In the **Internet Options** window, select the **Privacy** tab and select the **Turn on Pop-up Blocker** option under **Pop-up Blocker** settings.

8. Click **Settings**. The Pop-up Blocker Settings window is displayed.
9. Enter the URL of the OFSAA Application in the **Address of Website to Allow:** field.
10. Click **Add**. The OFSAA URL is displayed in the **Allowed Sites** section.
11. Click **Close**.
12. Click **OK** in the Internet Options window.

APPENDIX A - REMOVING OFSAA

This chapter includes the following sections:

Uninstalling OFSAA Infrastructure

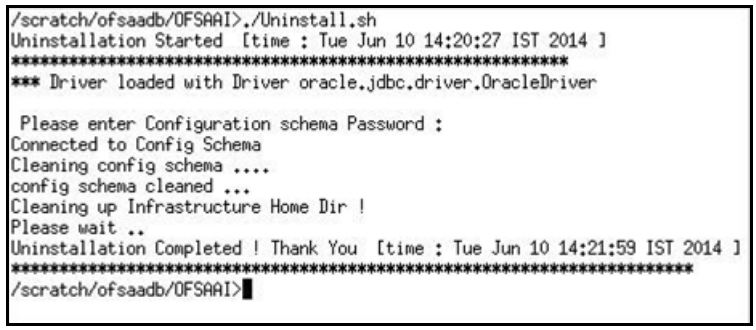
This section will guide you through the necessary steps to uninstall the OFSAA Infrastructure product.

Before you start the uninstallation process, ensure that no open connections exist to the OFSAA Infrastructure Config and Atomic Schemas and Infrastructure services are brought down.

To uninstall OFSAA Infrastructure:

1. Log in to the system as non-root user.
2. Navigate to the $FIC_HOME directory and execute the command:

   ```
   ./Uninstall.sh
   ```
3. Enter the password for OFSAAI Configuration Schema when prompted as shown in the following figure.



Note: Uninstallation does not remove the Infrastructure application from the Web Application Server. This has to be done manually.

The entries in the .profile file will have to be removed manually.

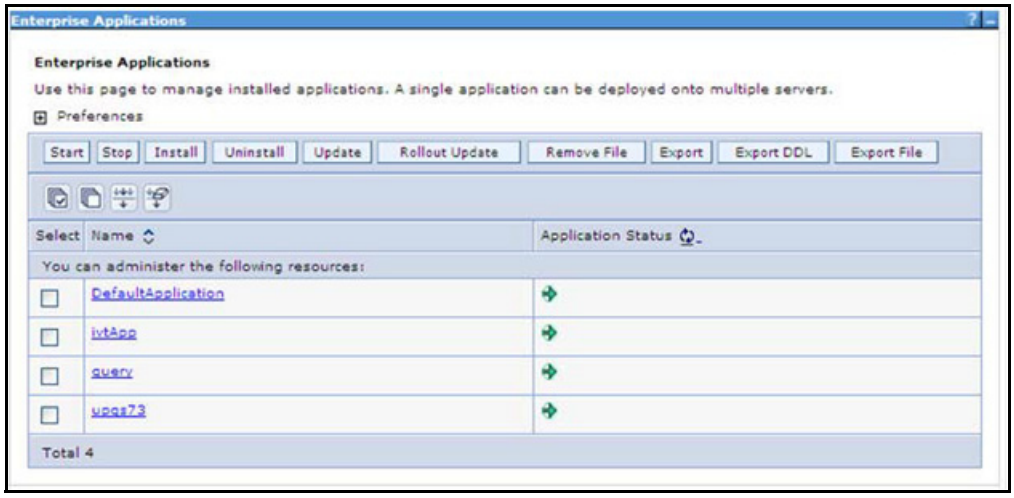
The files/ folders under the file system staging area (ftpshare) have to be deleted manually.

All the Database objects from Atomic Schemas have to be dropped manually.

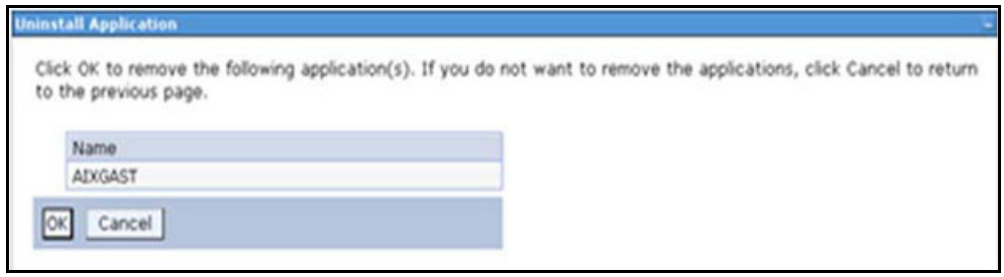
Uninstalling EAR Files in WebSphere

Following are the steps to uninstall any previously deployed application:

1. Open the URL 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. Expand Applications > Application Types > WebSphere enterprise applications from the LHS. The Enterprise Applications window is displayed with all the deployed applications.



4. Select the check box adjacent to the application to be uninstalled and click **Stop**.
5. Click **Uninstall** to display the Uninstall Application window.

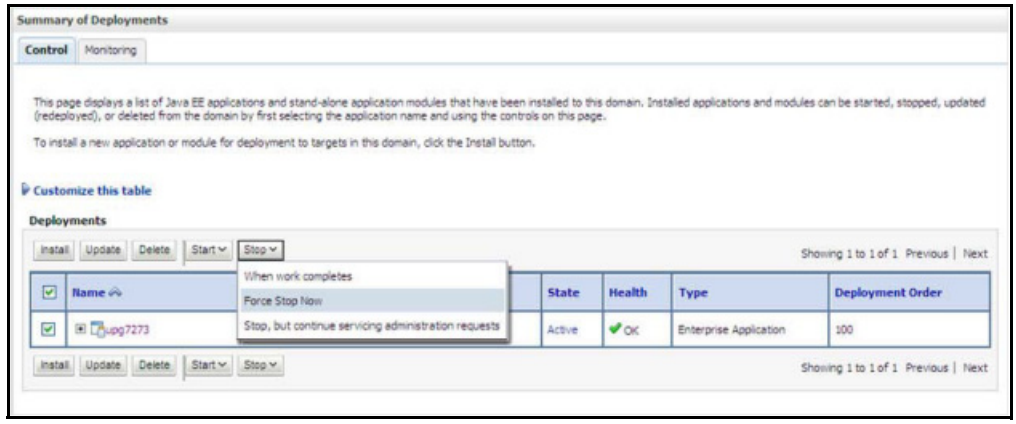


6. Click **OK** to confirm.
7. Click **Save** to save the master file configuration.

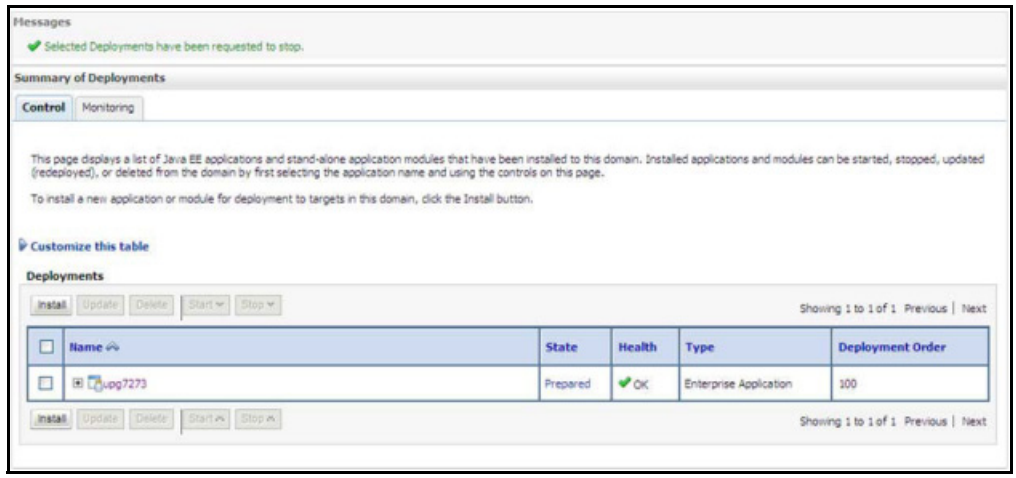
Uninstalling EAR Files in WebLogic

On the machine that hosts WebLogic, perform the following steps to uninstall any previously deployed application:

1. Open the URL in the browser window: http://<ipaddress>:<admin server port>/console (https if SSL is enabled). The Login window of the WebLogic Server Administration Console is displayed.
2. Login with the WebLogic user credentials having administrator privileges.
3. From the Domain Structure LHS menu, click Deployments to display the Summary of Deployments screen.



4. Select the check box adjacent to the application to be uninstalled and click **Stop > Force Stop Now**.
5. Click **Yes** in the confirmation dialog to stop the selected deployment.



6. Select the check box adjacent to the application and click **Delete** to delete the selected deployment.
7. Click **Yes** in the confirmation dialog to remove the selected deployment from the domain configuration.

Uninstalling WAR Files in Tomcat

On the machine that hosts Tomcat, perform the following steps to uninstall any previously deployed application:

1. Comment out Context path section from server.xml file in $CATALINA_HOME/conf directory to avoid conflict during undeploy and re-deploy of the WAR file.

   Place comment <!-- --> in between the context path section. For example:

   ```
   <!--
   <Context path ="/pr2test" docBase="/home/perfuser/tomcat-7.0.19/webapps/pr2test"
   debug="0" reloadable="true" crossContext="true">
   <Resource auth="Container"
   name="jdbc/PR2ATM"
   type="javax.sql.DataSource"
   driverClassName="oracle.jdbc.driver.OracleDriver"
   username="pr2atm"
   password="pr2atm"
   url="jdbc:oracle:thin:@10.184.74.99:1521:PERFTEST"
   maxActive="100"
   maxIdle="30"
   maxWait="10000"/>
   </Context>
   -->
   ```

   Restart the Tomcat service by doing the following:

   a. Login to the "Unix server" through a terminal emulator.
   b. Navigate to *$catalina_home/bin* directory.
   c. Stop the tomcat services using the following command:

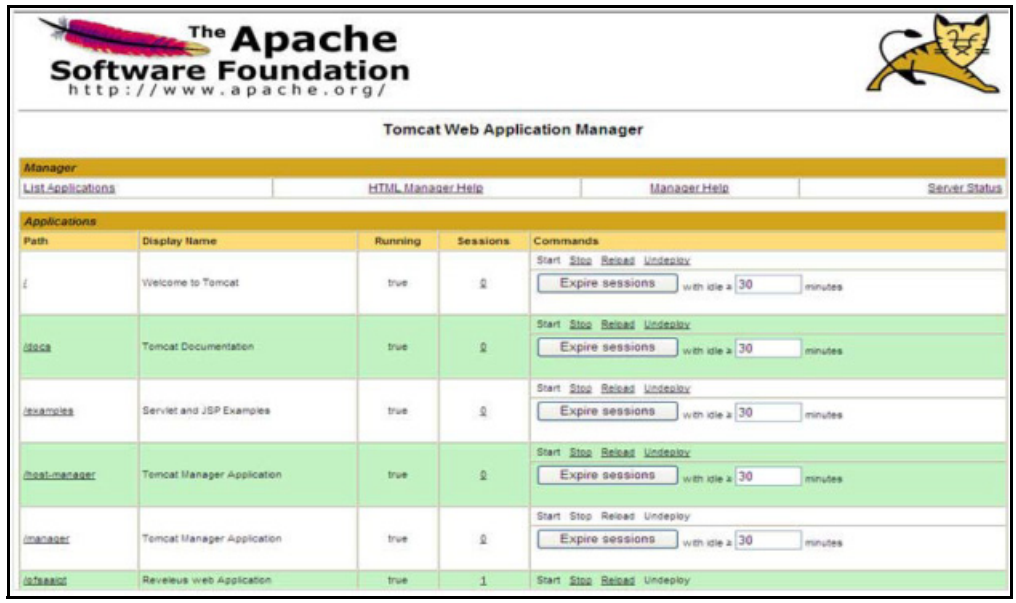
      ```
      ./shutdown.sh
      ```

   d. Start the tomcat services using the following command:

      ```
      ./startup.sh
      ```

2. Open the URL in a browser window: http://<IP address>:<Tomcat server port>. (https if SSL is enabled). The Tomcat home window is displayed.
3. Click the **Manager App**. The Connect to window is displayed.

4. Login with the user credentials having admin rights. The Tomcat Web Application Manager window is displayed with the list of all applications deployed in Tomcat.



5. Click the **Undeploy** link against the deployed Infrastructure application. A confirmation message is displayed on the application /Infrastructure being uninstalled.

APPENDIX A - UPGRADING AN EXISTING OFSAA 8.0.X JAVA 7 INSTANCE TO JAVA 8

This appendix explains the configurations required to upgrade an existing OFSAA 8.0.x Java 7 instance to Java 8. It consists of the following topics:

Prerequisites

The following are the prerequisites for upgrading OFSAA 8.0.x Java 7 instance to Java 8:

- Java 8 should be installed on the OFSAA server and Web Application Server.
- Oracle WebLogic Server should be 12.1.3.0 or above. Download and install patch **18729264** from http://support.oracle.com/.

Note: IBM WebSphere 8.5.x (Full Profile) on Java 8 is not available.

Steps for upgrading OFSAA 8.0.x Java 7 instance to Java 8

To upgrade OFSAA 8.0.x Java 7 instance to Java 8, follow these steps:

1. Configure Web Application Server to Java 8. For more information, see Configuring Web Application Server.
2. Configure the OFSAA instance to Java 8. For more information, see OFSAA Generic Configurations. For a newly installed Web Application Server, see OFSAA Configurations for New Web Application Server Installation.
3. Restart the OFSAA services. For more information, see Start/Stop OFSAA Infrastructure Services section.
4. Generate the application EAR/WAR file and redeploy the application onto your configured web application server. For more information on generating and deploying EAR / WAR file, see Creating EAR/WAR File and Deploying EAR/WAR File sections.

Web Application Server Configurations

This section describes the changes to be made in the Web Application Server. Following are the two options to perform Web Application Server Configurations which are listed as follows:

- Upgrade the existing Web Application Server installation to Java 8
- Install a new instance of the Web Application Server with Java 8

This section consists of the following topics:

Oracle WebLogic Server Updates

Perform the following configurations to upgrade the existing WebLogic server instance to Java 8:

1. Navigate to <WLS_HOME>/Middleware/Oracle_Home/wlserver.
2. Edit the `product.properties` file. Set `JAVA_HOME`, `WLS_JAVA_HOME`, `JAVAHOME` properties to the new Java path and `java.vm.version` to the new Java version. For example:

   ```
   JAVA_HOME=/usr/java/jre1.8.0_45
   WLS_JAVA_HOME=/usr/java/jre1.8.0_45
   JAVAHOME=/usr/java/jre1.8.0_45
   java.vm.version=1.8.0_45
   ```

3. Navigate to *<WLS_HOME>/Middleware/Oracle_Home/user_projects/domains/<domain>/bin*. Update `SUN_JAVA_HOME`, `DEFAULT_JAVA_HOME`, `JAVA_HOME` in the `setDomainEnv.sh` file to point to the new Java path. For example:

   ```
   SUN_JAVA_HOME="/usr/java/jre1.8.0_45"
   DEFAULT_SUN_JAVA_HOME="/usr/java/jre1.8.0_45"
   JAVA_HOME="/usr/java/jre1.8.0_45"
   ```

4. Clear the Application cache. Navigate to the following path and delete the files:

   <Weblogic installation location>/domains/<Domain name>/servers/<Server name>/tmp/_WL_user/<Application name>/qaelce/jsp_servlet

If you want to install a new instance of the Oracle WebLogic Server, follow these steps:

1. Install Oracle WebLogic Server 12.1.3.x on Java 8.
2. Perform the configurations for the newly installed WebLogic server. For more information, see Configure Resource Reference in WebLogic Application Server.

Note: While creating WebLogic Domain, the Listen Port should be set same as that of the existing Domain. Note down the new Domain path to perform OFSAA Configurations.

Apache Tomcat Server Updates

Perform the following configurations to upgrade the existing Apache Tomcat Server from Java 7 to Java 8:

1. Login to the Apache Tomcat Server as a non-root user.
2. Edit the `user.profile`. Update the value for `JAVA_HOME` from JRE 1.7 to JRE 1.8. For Example:
   `JAVA_HOME=/usr/java/jre1.8.0_45`
3. Clear the Application cache. Navigate to the following path and delete the files:
   <Tomcat installation folder>/work/Catalina/localhost/<Application name>/org/apache/jsp

If you wish to install a new instance of the Apache Tomcat Server, follow these steps:

1. Install Apache Tomcat Server 8 with Java 8.
2. Perform the configurations for the newly installed Tomcat server. For more information, see Configure Resource Reference in Tomcat Application Server.

Note: Update the Connector Port in */apache-tomcat-8.0.21/conf/server.xml* file to that of the existing Tomcat instance. Note down the new deployment path to perform OFSAA Configurations.

OFSAA Generic Configurations

User .profile Settings

Perform the following configurations:

1. Login to the OFSAA Server as a non-root user.
2. Edit the user .profile. Update the value for PATH variable from JRE 1.7 to JRE 1.8. For Example,
   ```
   PATH=/usr/java/jre1.8.0_45/jre
   JAVA_BIN=/usr/java/jre1.8.0_45/jre/bin
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/java/jre1.8.0_45/jre/lib/amd64/server
   ```

OFSAA Configurations for New Web Application Server Installation

This configuration is required only if you have freshly installed Oracle WebLogic 12.1.3 or Apache Tomcat Server 8.0. Follow these steps:

1. Modify the following parameters in the Configuration table present in the Config Schema with the new Domain Path in case of WebLogic or with the new deployment path in case of Tomcat:
   - DeFiHome
   - REV_IMG_PATH
   - EMBEDDED_JSP_JS_PATH
2. Login to the OFSAA Server as a non-root user.
3. Navigate to *$FIC_HOME/ficweb/webroot/WEB_INF* and update the following parameters in the web.xml file with the new Domain path in case of WebLogic or with the new deployment path in case of Tomcat:
   - FIC_PHYSICAL_HOME_LOC
   - FIC_HOME
   - ICC_SERVLET_LOG_FILE
4. Navigate to $FIC_HOME/ficweb/webroot/conf and update the Domain path in case of WebLogic or with the new deployment path in case of Tomcat:
   - OFSAALogger.xml
   - MDBLogger.xml
   - RevLog4jConfig.xml
   - RFDLogger.xml
   - ExportLog4jConfig.xml
   - RFDLogger.xml
   - PR2Logger.xml

APPENDIX A - JDBC JAR FILES

The ojdbc<version>.jar file should be copied based on Database and Java version. Refer to the following table for details:

Oracle Database version	JDK/JRE Version supported	JDBC Jar files specific to the release
12.1 or 12cR1	JDK 8, JDK 7 and JDK 8	ojdbc7.jar for JDK 7/JDK 8
11.2 or 11gR2	JDK 7 supported in 11.2.0.3 and 11.2.0.4	ojdbc6.jar for JDK 7

APPENDIX A - CONFIGURING APPLICATION PACK XML FILES

This appendix explains configuration of the application pack specific xml files.

This section includes the following topics:

Configuring OFS_CA_PACK.xml

The `OFS_CA_PACK.xml` file holds details on the various products that are packaged together in OFS CA Application Pack.

This section details the various tags/ parameters available in the file and the values that need to be updated. Prior to installing the CA Application Pack in SILENT mode, it is mandatory to update this file.

Note: If you are installing in the GUI mode, then this file need not be updated.

```
<APP_PACK_CONFIG>
    <APP_PACK_ID>OFS_CA_PACK</APP_PACK_ID>
    <APP_PACK_NAME>Financial Services Customer Analytics Applications Pack</APP_PACK_NAME>
    <APP_PACK_DESCRIPTION>Applications for Customer Analytics for Retail Customers</APP_PACK_DESCRIPTION>
    <VERSION>8.0.6.0.0</VERSION>
    <APP>
        <APP_ID PREREQ="" DEF_SEL_FLG="YES" ENABLE="YES">OFS_AAI</APP_ID>
        <APP_NAME>Financial Services Analytical Applications Infrastructure</APP_NAME>
        <APP_DESCRIPTION>Base Infrastructure for Analytical Applications</APP_DESCRIPTION>
        <VERSION>8.0.6.0.0</VERSION>
    </APP>
    <APP>
        <APP_ID PREREQ="OFS_AAI" ENABLE="YES">OFS_AAAI</APP_ID>
        <APP_NAME>Financial Services Enterprise Modeling</APP_NAME>
        <APP_DESCRIPTION>Financial Services Enterprise Modeling</APP_DESCRIPTION>
        <VERSION>8.0.6.0.0</VERSION>
    </APP>
    <APP>
        <APP_ID PREREQ="OFS_AAAI" ENABLE="YES">OFS_RCA</APP_ID>
        <APP_NAME>Financial Services Retail Customer Analytics</APP_NAME>
        <APP_DESCRIPTION>Application for Retail Customer Analytics</APP_DESCRIPTION>
        <VERSION>8.0.6.0.0</VERSION>
    </APP>
</APP_PACK_CONFIG>
```

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
APP_PACK_ID	Unique Application Pack Identifier	Y	Unique Seeded Value	Do not modify this value.
APP_PACK_NAME	Unique Application Pack Name	Y	Unique Seeded Value	Do not modify this value.
APP_PACK_DESCRIPTION	Unique Application Pack Description	Y	Unique Seeded Value	Do not modify this value.
VERSION	Unique release version	Y	Unique Seeded Value	Do not modify this value.
APP	Unique Application Entries	Y	Unique Seeded Value	Do not remove these tags.
APP_ID	Unique Application Identifier	Y	Unique Seeded Value	Do not modify this value.
APP_ID/ PREREQ	Prerequisite Application/ Product	Y	Unique Seeded Value	For most applications Infrastructure would be the prerequisite set. For certain other applications, an appropriate Application ID would be set. Do not modify this value.
APP_ID/ DEF_SEL_FLAG	Default Selected Flag	Y	Default - YES	In all Application Packs, Infrastructure would have this value set to "YES". Do not modify this value.
APP_ID/ ENABLE	Enable Application/ Product	YES if installing in SILENT mode.	Default - YES for Infrastructure NO for Others Permissible - YES or NO	Set this attribute-value to YES against every APP_ID which is licensed and should be enabled for use. **Note:** Application/ Product once enabled cannot be disabled. However, Application/ Product not enabled during installation can be enabled later through the Administration UI.
APP_NAME	Unique Application/ Product Name	Y	Unique Seeded Value	Do not modify this value.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
APP_DESCRIPTION	Unique Application/ Product Name	Y	Unique Seeded Value	Do not modify this value.
VERSION	Unique release version	Y	Unique Seeded Value	Do not modify this value.

Configuring OFS_CA_SCHEMA_IN.xml

Creating database schemas, objects within schemas and assigning appropriate grants are the primary steps in the installation process of OFSAA Applications. The `OFS_CA_SCHEMA_IN.xml` file contains details on the various application schemas that should be created prior to the Application Pack installation.

Note: This file should be configured only if OFS CA Application Pack installation for **RDBMS ONLY** target.

The following table gives details about the various tags/ parameters available in the file and the values that need to be updated. Prior to executing the schema creator utility, it is mandatory to update this file.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<APP_PACK_ID>	Seeded unique ID for the OFSSAA Application Pack	Y	Seeded	Do not modify this value.
<JDBC_URL>	Enter the JDBC URL. Note: You can enter RAC/ NON-RAC enabled database connectivity URL.	Y	Example: jdbc:oracle:thin:@<DBSERVER IP/HOST/IP>:<PORT>:<SID> or jdbc:oracle:thin:@//[HOST][:PORT]/SERVICE or jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=[HOST])(port=[PORT]))(ADDRESS=(PROTOCOL=TCP)(HOST=[HOST])(PORT=[PORT]))(LOAD_BALANCE=yes)(FAILOVER=yes))(CONNECT_DATA=(SERVICE_NAME=[SERVICE]))) For example: jdbc:oracle:thin:@//dbhost.server.com:1521/service1 or jdbc:oracle:thin:@//dbshost.server.com:1521/scan-1 or jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=dbhost1.server.com)(port=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=dbhost2.server.com)(PORT=1521))(LOAD_ BALANCE=yes)(FAILOVER=yes))(CONNECT_DATA=(SERVICE_NAME=service1)))	Ensure to add an entry (with SID/ SERVICE NAME) in the tnsnames.ora file on the OFSAA server. The entry should match with the SID/ SERVICE NAME used in the JDBC URL.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<JDBC_DRIVER>	By default this driver name is seeded. **Note:** Do not edit this attribute value.	Y	Example: oracle.jdbc.driver.OracleDriver	Only JDBC Thin Driver is supported. Do not modify this value.
<HOST>	Enter the Host name/ IP Address of the system on which you are installing the OFSAA components.	Y	Host Name/ IP Address	
<SETUPINFO>/ PREFIX_SCHEMA_NAME	Identifies if the value specified in <SETUPINFO>/ NAME attribute should be prefixed to the schema name.	N	YES or NO	Default value is YES.
<SETUPINFO>/ NAME	Enter the acronym for the type of implementation. This information will be displayed in the OFSAA Home Page. **Note:** On executing the schema creator utility, this value will be prefixed with each schema name. For example: dev_ofsaaconf, uat_ofsaatm.	Y	Accepts strings with a minimum length of two and maximum of four. Example: DEV, SIT, PROD	This name would appear in the OFSAA Landing Page as "Connected To: xxxx". The schemas being created would get this prefix. For example, dev_ofsaaconf, uat_ofsaaconf, etc.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<PASSWORD>/ DEFAULT*	Enter the password if you want to set a default password for all schemas. **Note:** You also need to set APPLYSAMEFOR ALL attribute as Y to apply the default password for all the schemas.	N	The maximum length allowed is 30 characters. Special characters are not allowed.	
<PASSWORD>/ APPLYSAMEF ORALL	Enter as Y if you want to apply the password specified in DEFAULT attribute for all the schemas. If you enter as N, you need to provide individual passwords for all schemas. **Note:** In case you have entered Y in APPLYSAMEFOR ALL attribute and also have specified individual passwords for all the schemas, then the specified individual passwords will take precedence.	Y	Default - N Permissible - Y	**Note:** Setting this attribute value is mandatory, if DEFAULT attribute is set.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<SCHEMA>/ TYPE	The different types of schemas that are supported in this release are ATOMIC, CONFIG, SANDBOX, and ADDON. By default, the schemas types are seeded based on the Application Pack. **Note:** Do not edit this attribute value.	Y	ATOMIC/CONFIG/SANDBOX/ ADDON **Note:** SANDBOX and ADDON schemas are not applicable for OFS CA Application Pack.	Only One CONFIG schema can exist in the file. This schema identifies as the CONFIGURATION schema that holds the OFSAA setup detains and other Metadata information. Multiple ATOMIC/ SANDBOX/ADDON schemas can exist in the file. ATOMIC schema refers to the Information Domain schema. SANDBOX schema refers to the SANDBOX schema. ADDON schema refers to other miscellaneous schema (not applicable for this Application Pack). **Note:** The CA Pack supports only one Atomic Schema.
<SCHEMA>/ NAME	By default, the schema names are seeded based on the Application Pack. You can edit the schema names if required. **Note:** The Schema Name will have a prefix of the SETUPINFO/ NAME attribute. SCHEMA NAME must be same for all the ATOMIC Schemas of the applications within an Application Pack.	Y	The permissible length is 15 characters and only alphanumeric characters are allowed. No special characters allowed except underscore '_'.	SETUPOINFO/NAME attribute value would be prefixed to the schema name being created. For example, if name is set as 'ofsaatm' and setupinfo as 'uat', then schema being created would be 'uat_ofsaatm'. NAME should be same where APP_GRP=1 for all SCHEMA tags (Not applicable for this Application Pack).

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<SCHEMA>/ PASSWORD	Enter the password of the schema to be created. **Note:** If this attribute is left blank, then the password specified in the <PASSWORD>/ DEFAULT attribute is applied as the Schema Password.	N	The maximum length allowed is 30 characters. Special characters are not allowed.	**Note:** You need to mandatorily enter the password if you have set the <PASSWORD>/ APPLYSAMEFORALL attribute as N.
<SCHEMA>/ APP_ID	By default, the Application ID is seeded based on the Application Pack. **Note:** Do not edit this attribute value.	Y	Unique Seeded Value	Identifies the Application/ Product for which the schema is being created. Do not modify this value.
<SCHEMA>/ DEFAULTTABLESPACE	Enter the available default tablespace for DB User. **Note:** If this attribute is left blank, then USERS is set as the default tablespace.	N	Default - USERS Permissible - Any existing valid tablespace name.	Modify this value to associate any valid tablespace with the schema.
<SCHEMA>/ TEMPTABLESPACE	Enter the available temporary tablespace for DB User. Note: If this attribute is left bank, TEMP is set as the default tablespace.	N	Default - TEMP Permissible - Any existing valid temporary tablespace name.	Modify this value to associate any valid tablespace with the schema.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<SCHEMA>/ QUOTA	Enter the quota to be set on DEFAULTTABLESPACE attribute for the schema/ user. By default, the quota size is set to 500M. Minimum: 500M or Unlimited on default Tablespace.	N	Example: 600M/ m 20G/ g UNLIMITED/ unlimited	Modify this value to grant the specified quota on the mentioned tablespace to the user.
<SCHEMA>/ INFODOM	Enter the name of the Information Domain to associate this schema. The schema creator utility automatically derives an Information Domain Name based on the Application Pack if no value is specified for this attribute.	N	Permissible length is 16 characters and only alphanumeric characters are allowed. No special characters are allowed.	
<ADV_SEC_OPTIONS>/	Parent tag to hold Advance Security Options.	N		Uncomment the tag and edit if you want to add security options. For example, TDE and Data Redact. For details, see the example following the table.
<ADV_SEC_OPTIONS>/TDE	Tag to enable/ disable TDE.	N	Default is FALSE. To enable TDE, set this to TRUE.	Ensure this tag is not commented if you have uncommented <ADV_SEC_OPTIONS>
<ADV_SEC_OPTIONS>/ DATA_REDACT	Tag to enable/ disable Data Redaction feature.	N	Default is FALSE. To enable DATA_REDACT, set this to TRUE	Ensure this tag is not commented if you have uncommented <ADV_SEC_OPTIONS>

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<TABLESPACES>	Parent tag to hold <TABLESPACE> elements	N	NA	Uncomment the tag and edit. ONLY if tablespaces are to be created as part of the installation. For details, see the example following the table. Note: When TDE is TRUE in ADV_SEC_OPTIONS, then it is mandatory for the <TABLESPACES> tag to be present in the xml file.
<TABLESPACE>/ NAME	Logical Name of tablespace to be created.	Y		Name if specified should be referred in the <SCHEMA DEFAULTTABLESPACE= "##NAME##"> attribute. Note the ## syntax.
<TABLESPACE>/ VALUE	Physical Name of the tablespace to be created.	Y	NA	Value if specified will be the actual name of the TABLESPACE.
<TABLESPACE>/ DATAFILE	Specifies the location of the data file on the server	Y	NA	Enter the absolute path of the file to be created.
<TABLESPACE>/ AUTOEXTEND	Specifies if the tablespace should be extensible or have a hard limit	Y	ON or OFF	Set to ON to ensure that the tablespace does not run out of space when full.
<TABLESPACE>/ ENCRYPT	Specifies if the tablespace(s) should be encrypted using TDE.	Y	ON or OFF	Set to ON to ensure that the tablespaces when created are encrypted using TDE.

Note: Encryption of tablespaces requires to enabling Transparent Data Encryption (TDE) on the Database Server.

Example: (The following snippet shows that TDE is enabled and hence the tablespace has been shown with encryption **ON**.)

```
<ADV_SEC_OPTIONS>
    <OPTION NAME="TDE" VALUE="FALSE"/>
    <OPTION NAME="DATA_REDACT" VALUE="FALSE" />
</ADV_SEC_OPTIONS>
<TABLESPACES>
    <TABLESPACE NAME="OFS_AAI_TBSP_1" VALUE="TS_USERS1" DATAFILE="/scratch/ora12c/app/
    oracle/oradata/OFSPQA12CDB/ts_users1.dbf" SIZE="500M" AUTOEXTEND="ON" ENCRYPT="ON" /
    >
    <TABLESPACE NAME="OFS_AAI_TBSP_2" VALUE="TS_USERS2" DATAFILE="/scratch/ora12c/app/
    oracle/oradata/OFSPQA12CDB/ts_users2.dbf" SIZE="500M" AUTOEXTEND="ON" ENCRYPT="ON" /
    >
</TABLESPACES>

<SCHEMAS>
    <SCHEMA TYPE="CONFIG" NAME="ofsaaconf" PASSWORD="" APP_ID="OFS_AAI"
    DEFAULTTABLESPACE="##OFS_AAI_TBSP_1##" TEMPTABLESPACE="TEMP" QUOTA="unlimited"/>
    <SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_AAAI"
    DEFAULTTABLESPACE="##OFS_AAI_TBSP_2##" TEMPTABLESPACE="TEMP" QUOTA="unlimited"
    INFODOM="OFSAAAIINFO"/>
</SCHEMAS>
```

Configuring OFS_CA_SCHEMA_BIGDATA_IN.XML

Creating HIVE schemas, objects within the schemas are the primary steps in the installation process of OFSAA Applications. The `OFS_CA_SCHEMA_ BIGDATA_IN.xml` file contains details on the various application schemas that should be created/ referred prior to the Application Pack installation.

Note: This file should be configured only in case of OFS AAAI Application Pack installation for HDFS ONLY target. This file is not required to be configured for an RDBMS ONLY target installation.

The following table provides details about the various tags/ parameters available in the file and the values that have to be updated.

Prior to executing the schema creator utility, it is mandatory to update this file.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<APP_PACK_ ID>	Seeded unique ID for the OFSAA Application Pack	Y	Seeded	DO NOT modify this value.
<JDBC_URL>	Enter the JDBC URL **Note:** You can enter RAC/ NON-RAC enabled database connectivity URL.	Y	Example, jdbc:oracle:thin:@<HOST/ IP>:<PORT>:<SID> or jdbc:oracle:thin:@//[HOS T][:PORT]/SERVICE or jdbc:oracle:thin:@(DESCRI PTION=(ADDRESS_ LIST=(ADDRESS=(PROT OCOL=TCP)(HOST=[HO ST])(port=[PORT]))(ADD RESS=(PROTOCOL=TCP) (HOST=[HOST])(PORT=[PORT]))(LOAD_ BALANCE=yes)(FAILOV ER=yes))(CONNECT_ DATA=(SERVICE_ NAME=[SERVICE]))) For example, jdbc:oracle:thin:@//dbhos t.server.com:1521/service 1 or jdbc:oracle:thin:@//dbsho st.server.com:1521/scan-1 or jdbc:oracle:thin:@(DESCRI PTION=(ADDRESS_ LIST=(ADDRESS=(PROT OCOL=TCP)(HOST=dbho st1.server.com)(port=1521))(ADDRESS=(PROTOCO L=TCP)(HOST=dbhost2.s erver.com)(PORT=1521))(LOAD_ BALANCE=yes)(FAILOV ER=yes))(CONNECT_ DATA=(SERVICE_ NAME=service1)))	In case of an HDFS ONLY target installation, this URL should be of the RDBMS instance that hosts the Application's METADOM.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<JDBC_ DRIVER>	By default this driver name is seeded. **Note:** Do not edit this attribute value.	Y	Example, oracle.jdbc.driver.OracleD river	Only JDBC Thin Driver is supported. DO NOT modify this value.
<HOST>	Enter the Hostname/ IP Address of the system on which you are installing the OFSAA components.	Y	Host Name/ IP Address	
<SETUPINFO>/ PREFIX_ SCHEMA_ NAME	Identifies if the value specified in <SETUPINFO>/ NAME attribute should be prefixed to the schema name.	N	YES or NO	Default value is YES.
<SETUPINFO>/ NAME	Enter the acronym for the type of implementation. This information will be displayed in the OFSAA Home Page. **Note:** On executing the schema creator utility, this value will be prefixed with each schema name. For example: dev_ ofsaaconf, uat_ofsaaatm.	Y	Accepts strings with a minimum length of two and maximum of four. Example, DEV, SIT, PROD	This name would appear in the OFSAA Landing Page as "Connected To: xxxx" The schemas being created would get this prefix. For example, dev_ ofsaaconf, uat_ofsaaconf etc.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<PASSWORD>/ DEFAULT*	Enter the password if you want to set a default password for all schemas. **Note:** You also need to set APPLYSAMEFOR ALL attribute as Y to apply the default password for all the schemas.	N	The maximum length allowed is 30 characters. Special characters are not allowed.	Applies only to the RDBMS type METADOM schema(s).
<PASSWORD>/ APPLYSAMEF O RALL	Enter as Y if you want to apply the password specified in DEFAULT attribute for all the schemas. If you enter as N, you need to provide individual passwords for all schemas. **Note:** In case you have entered Y in APPLYSAMEFOR ALL attribute and also have specified individual passwords for all the schemas, then the specified individual passwords will take precedence.	Y	Default - N Permissible - Y or N	**Note:** Setting this attribute value is mandatory, If DEFAULT attribute is set. Applies only to the RDBMS type METADOM schema(s).

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<SCHEMAS>/ TYPE=RDBMS	Identifies the RDBMS schema details.	Y	Default names for schemas within the pack would be derived in absence of any value specified.	In an HDFS ONLY target installation, the Application's METADOM (that hosts the metadata) for an application is stored in RDBMS schema and the data model entities of the application are stored in the DATADOM (which would be on Hive).
<SCHEMA>/ TYPE	The different types of schemas that are supported in this release are ATOMIC, CONFIG, SANDBOX, and ADDON. By default, the schemas types are seeded based on the Application Pack. **Note:** Do not edit this attribute value.	Y	ATOMIC/CONFIG/SAN DBOX/ ADDON Note: SANDBOX AND ADDON schemas are not applicable for OFS AAAI Application Pack.	Only One CONFIG schema can exist in the file. This schema identifies as the CONFIGURATION schema that holds the OFSAA setup details and other metadata information. Multiple ATOMIC/ SANDBOX/ ADDON schemas can exist in the file. ATOMIC schema refers to the METADOM within the Information Domain schema. SANDBOX schema refers to the SANDBOX schema. ADDON schema refers to other miscellaneous schema (not applicable for this Application Pack).

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<SCHEMA>/ NAME	By default, the schemas names are seeded based on the Application Pack. You can edit the schema names if required. **Note:** The Schema Name will have a prefix of the SETUPINFO/ NAME attribute. SCHEMA NAME must be same for all the ATOMIC Schemas of applications within an Application Pack.	Y	The permissible length is 15 characters and only alphanumeric characters allowed. No special characters allowed except underscore '_'.	SETUPINFO/ NAME attribute value would be prefixed to the schema name being created. For example, if name is set as 'ofsaaatm' and setupinfo as 'uat' then schema being created would be 'uat_ofsaaatm'. NAME should be same where APP_GRP=1 for all SCHEMA tags (Not applicable for this Application Pack).
<SCHEMA>/ PASSWORD	Enter the password of the schema to be created. **Note:** If this attribute is left blank, then the password specified in the <PASSWORD>/ DEFAULT attribute is applied as the Schema Password.	N	The maximum length allowed is 30 characters. Special characters are not allowed.	**Note:** You need to mandatorily enter the password if you have set the <PASSWORD>/ APPLYSAMEFORALL attribute as N.
<SCHEMA>/ APP_ID	By default, the Application ID is seeded based on the Application Pack. **Note:** Do not edit this attribute value.	Y	Unique Seeded Value	Identifies the Application/ Product for which the schema is being created. DO NOT modify this value.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<SCHEMA>/ DEFAULTTABLESPACE	Enter the available default tablespace for DB User. Note: If this attribute is left blank, then USERS is set as the default tablespace.	N	Default - USERS Permissible - Any existing valid tablespace name.	Modify this value to associate any valid tablespace with the schema.
<SCHEMA>/ TEMPTABLESPACE	Enter the available temporary tablespace for the DB User. **Note:** If this attribute is left blank, then TEMP is set as the default tablespace.	N	Default - TEMP Permissible - Any existing valid temporary tablespace name.	Modify this value to associate any valid tablespace with the schema.
<SCHEMA>/ QUOTA	Enter the quota to be set on DEFAULTTABLESPACE attribute for the schema/ user. By default, the quota size is set to 500M. Minimum: 500M or Unlimited on default Tablespace.	N	Example, 600M/m 20G/g UNLIMITED/unlimited	Modify this value to grant the specified quota on the mentioned tablespace to the user.
<SCHEMA>/ INFODOM	Enter the name of the Information Domain to associate this schema. The schema creator utility automatically derives an Information Domain Name based on the Application Pack if no value is specified for this attribute.	N	Permissible length is 16 characters and only alphanumeric characters allowed. No special characters allowed.	
<SCHEMAS>/ TYPE=HDFS	Type of schemas being created.	Y		Refers to the DATADOM of the Application Pack being installed.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<HIVE_ SERVER_ HOST>	IP/HostName of the server where HIVE is installed	Y		
<HIVE_LIB_ PATH>	Folder path where HIVE related drivers/jar files are copied	Y		Should contain the list of jars mentioned in the section Copying Jars to OFSAA Installation Folder and krb5.conf, keytab files. Manually copy the preceding listed files from CDH distribution to this identified folder.
<SCHEMA>/ NAME	By default, the schemas names are seeded based on the Application Pack. You can edit the schema names if required. Note: The Schema Name will have a prefix of the SETUPINFO/ NAME attribute.	Y	The permissible length is 20 characters and only alphanumeric characters allowed.	Schema Name should not be the same as Schema Name specified for Schema Type ATOMIC.
<SCHEMA>/ TYPE	Identifies the type of schema where the data model entities would reside.	Y	By default, the TYPE attribute in this tag is set to DATADOM.	DO NOT modify this value.
<SCHEMA>/ DB TYPE	Identifies the type of driver to be used for connection.	Y	By default, the only supported type is HIVE in this release.	In the upcoming releases, the type value can be HIVE/ IMPALA etc.
<SCHEMA>/<P ROPERTY>/CO MMENT	COMMENTS for HIVE schema	N		
<SCHEMA>/<P ROPERTY>/LO CATION	You can optionally specify a location for the table data	N		
<CONNECTIO N_ PROPERTIES> /<PROPERTY>/ J DBC_DRIVER	HIVE JDBC driver details	Y	com.cloudera.hive.j dbc4.HS2Driver	The default cloudera HiveServer 2 driver name.

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Default Value/ Permissible Value	Comments
<CONNECTION_ PROPERTIES> /<PROPERTY>/ J DBC_URL	Enter HIVE JDBC URL	Y	Valid Hive JDBC URL to be specified.	Specify the Hive JDBC URL to connect to the Hive Server.
<CONNECTION_ PROPERTIES> /<PROPERTY>/ AUTH_TYPE	Authentication Type	Y	Permissible values: KERBEROS_WITH_ KEYTAB	Only "Kerberos with keytab" based authentication supported in this release.
<CONNECTION_ PROPERTIES> /<PROPERTY>/ AUTH_ALIAS	Alias name for authentication credentials	Y		An Alias name mapping to a principal and password combination specified in the following tags.
<CONNECTION_ PROPERTIES> /<PROPERTY>/ PRINCIPAL	Authentication principal name	Y		Principal name used in authentication to connect to the Hive Server.
<CONNECTION_ PROPERTIES> /<PROPERTY>/ PASSWORD	Authentication password	Y		Password used in authentication to connect to the Hive Server.
<CONNECTION_ PROPERTIES> /<PROPERTY>/ KRB_GSSJAAS _ FILE_NAME	A keytab file containing pairs of Kerberos principals and an encrypted copy of that principal's key.	Y		This file should be copied to the location specified in <HIVE_LIB_PATH>
<CONNECTION_ PROPERTIES> /<PROPERTY>/ KRB_REALM_ FILE_NAME	REALM configuration file	Y		This file should be copied to the location specified in <HIVE_LIB_PATH>

APPENDIX A - CONFIGURING OFSAAI_INSTALLCONFIG.XML FILE

To configure the OFS_InstallConfig.xml file:

1. Navigate to *OFS_CA_PACK/OFS_AAI/conf/* folder.
2. Open the file OFSAAI_InstallConfig.xml in text editor.

   The following screen shot gives a snapshot of Standard Installation.

```
<?xml version="1.0" encoding="UTF-8"?>

<UserInteractions>
        <Layer name="GENERAL">
                <InteractionGroup name="WebServerType" >
                        <InteractionVariable name="WEBAPPSERVERTYPE">1</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OFSAA Infrastructure Server Details">
                        <InteractionVariable name="DBSERVER_IP">10.184.149.54</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="Database Details" >
                        <InteractionVariable name="ORACLE_SID/SERVICE_NAME">FTPDEV</InteractionVariable>
                        <InteractionVariable name="ABS_DRIVER_PATH">/scratch/oracle/app/product/11.2.0.3/client_1/jdbc/lib</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OLAP Detail">
                    <InteractionVariable name="OLAP_SERVER_IMPLEMENTATION">0</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="SFTP Details">
                    <InteractionVariable name="SFTP_ENABLE">1</InteractionVariable>
                        <InteractionVariable name="FILE_TRANSFER_PORT">22</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="Locale Detail">
                    <InteractionVariable name="LOCALE">en_US</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OFSAA Infrastructure Communicating ports" >
                        <InteractionVariable name="JAVAPORT">9999</InteractionVariable>
                        <InteractionVariable name="NATIVEPORT">6666</InteractionVariable>
                        <InteractionVariable name="AGENTPORT">6510</InteractionVariable>
                        <InteractionVariable name="ICCPORT">6507</InteractionVariable>
                        <InteractionVariable name="ICCNATIVEPORT">6509</InteractionVariable>
                        <InteractionVariable name="OLAPPORT">10101</InteractionVariable>
                        <InteractionVariable name="MSGPORT">6501</InteractionVariable>
                        <InteractionVariable name="ROUTERPORT">6500</InteractionVariable>
                        <InteractionVariable name="AMPORT">6505</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="WEB_DETAILS" >
                    <InteractionVariable name="HTTPS_ENABLE">0</InteractionVariable>
                    <InteractionVariable name="WEB_SERVER_IP">10.184.149.241</InteractionVariable>
                        <InteractionVariable name="WEB_SERVER_PORT">8080</InteractionVariable>
                        <InteractionVariable name="CONTEXT_NAME">OFSAAI</InteractionVariable>
                        <InteractionVariable name="WEBAPP_CONTEXT_PATH">/scratch/mediapack/apache-tomcat-7.0.19/webapps</InteractionVariable>
                        <InteractionVariable name="WEB_LOCAL_PATH">/scratch/mediapack/ftpshare</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name=" Weblogic Setup Details" >
                        <InteractionVariable name="WEBLOGIC_DOMAIN_HOME">NA</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OFSAAI FTP Details">
                            <InteractionVariable name="OFSAAI_FTPSHARE_PATH">/scratch/mediapack/ftpshare</InteractionVariable>
                        <InteractionVariable name="OFSAAI_SFTP_USER_ID">mediapack</InteractionVariable>
                </InteractionGroup>
        </Layer>
</UserInteractions>
```

The following screen shots give the snapshot of Hybrid Installation.

```
<?xml version="1.0" encoding="UTF-8"?>

<UserInteractions>
        <Layer name="GENERAL">
                <InteractionGroup name="WebServerType" >
                        <InteractionVariable name="WEBAPPSERVERTYPE">1</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OFSAA Infrastructure Server Details">
                        <InteractionVariable name="DBSERVER_IP">whf00azi</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="Database Details" >
                        <InteractionVariable name="ORACLE_SID/SERVICE_NAME">CIPMDB</InteractionVariable>
                        <InteractionVariable name="ABS_DRIVER_PATH">/scratch/oracle/app/product/12.1.0/client_1/jdbc/lib</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OLAP Detail">
                    <InteractionVariable name="OLAP_SERVER_IMPLEMENTATION">0</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="SFTP Details">
                    <InteractionVariable name="SFTP_ENABLE">1</InteractionVariable>
                        <InteractionVariable name="FILE_TRANSFER_PORT">22</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="Locale Detail">
                   <InteractionVariable name="LOCALE">en_US</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OFSAA Infrastructure Communicating ports" >
                        <InteractionVariable name="JAVAPORT">2830</InteractionVariable>
                        <InteractionVariable name="NATIVEPORT">3304</InteractionVariable>
                        <InteractionVariable name="AGENTPORT">4013</InteractionVariable>
                        <InteractionVariable name="ICCPORT">5593</InteractionVariable>
                        <InteractionVariable name="ICCNATIVEPORT">6302</InteractionVariable>
                        <InteractionVariable name="OLAPPORT">13102</InteractionVariable>
                        <InteractionVariable name="MSGPORT">6812</InteractionVariable>
                        <InteractionVariable name="ROUTERPORT">6909</InteractionVariable>
                        <InteractionVariable name="AMPORT">6310</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="WEB_DETAILS" >
```

```
                        <InteractionVariable name="NATIVEPORT">3304</InteractionVariable>
                        <InteractionVariable name="AGENTPORT">4013</InteractionVariable>
                        <InteractionVariable name="ICCPORT">5593</InteractionVariable>
                        <InteractionVariable name="ICCNATIVEPORT">6302</InteractionVariable>
                        <InteractionVariable name="OLAPPORT">13102</InteractionVariable>
                        <InteractionVariable name="MSGPORT">6812</InteractionVariable>
                        <InteractionVariable name="ROUTERPORT">6909</InteractionVariable>
                        <InteractionVariable name="AMPORT">6310</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="WEB_DETAILS" >
                    <InteractionVariable name="HTTPS_ENABLE">0</InteractionVariable>
                    <InteractionVariable name="WEB_SERVER_IP">whf00azi</InteractionVariable>
                        <InteractionVariable name="WEB_SERVER_PORT">8449</InteractionVariable>
                        <InteractionVariable name="CONTEXT_NAME">ofsa</InteractionVariable>
                        <InteractionVariable name="WEBAPP_CONTEXT_PATH">/scratch/806Mock/apache-tomcat-8.5.32/webapps</InteractionVariable>
                        <InteractionVariable name="WEB_LOCAL_PATH">/scratch/806Mock/apache-tomcat-8.5.32/webapps</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name=" Weblogic Setup Details" >
                        <InteractionVariable name="WEBLOGIC_DOMAIN_HOME">NA</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="OFSAAI FTP Details">
                            <InteractionVariable name="OFSAAI_FTPSHARE_PATH">/scratch/806Mock/ftpshare/</InteractionVariable>
                       <InteractionVariable name="OFSAAI_SFTP_USER_ID">806Mock</InteractionVariable>
                           <InteractionVariable name="OFSAAI_SFTP_PRIVATE_KEY">NA</InteractionVariable>
                           <InteractionVariable name="OFSAAI_SFTP_PASSPHRASE">NA</InteractionVariable>
                </InteractionGroup>
                <InteractionGroup name="HIVE_DETAILS" >
                        <InteractionVariable name="HIVE_SERVER_PORT">22</InteractionVariable>
                        <InteractionVariable name="HIVE_SERVER_FTPDRIVE">/scratch/hive/hiveSftp/</InteractionVariable>
                        <InteractionVariable name="HIVE_SERVER_FTP_USERID">root</InteractionVariable>
                        <InteractionVariable name="HIVE_SERVER_FTP_PROTOCOL">SFTP</InteractionVariable>
                        <InteractionVariable name="HIVE_SFTP_PRIVATE_KEY">NA</InteractionVariable>
                        <InteractionVariable name="HIVE_SFTP_PASSPHRASE">NA</InteractionVariable>
                </InteractionGroup>
        </Layer>
</UserInteractions>
```

3. Configure the OFSAAI_InstallConfig.xml as mentioned in the below table:

You need to manually set the `InteractionVariable` parameter values as mentioned in the table. If a value is not applicable, enter NA and ensure that the value is not entered as NULL.

InteractionVariable Name	Significance and Expected Value	Mandatory
<Layer name="GENERAL">		
WEBAPPSERVERTYPE	Identifies the web application server on which the OFSAA Infrastructure web components would be deployed. The below numeric value should be set depending on the type: Apache Tomcat = 1 IBM WebSphere Application Server = 2 Oracle WebLogic Server = 3 For example, <InteractionVariable name="WEBAPPSERVERTYPE">3</InteractionVari able>	Yes
DBSERVER_IP	Identifies the host name or IP address of the system on which the Database Engine is hosted. Note: For RAC Database, the value should be NA. For example, <InteractionVariable name="DBSERVER_ IP">14.15.16.17</InteractionVariable> or <InteractionVariable name="DBSERVER_ IP">dbhost.server.com</InteractionVariable>	Yes
ORACLE_SID/ SERVICE_NAME	Identifies the Oracle DB Instance SID or SERVICE_NAME Note: The Oracle_SID value should be exactly the same as it is mentioned in JDBC_URL. For example, <InteractionVariable name="ORACLE_SID/ SERVICE_ NAME">ofsaser</InteractionVariable>	Yes
ABS_DRIVER_PATH	Identifies the directory where the JDBC driver (ojdbc<version>.jar) exists. This would typically be the $ORACLE_HOME/jdbc/lib For example, <InteractionVariable name="ABS_DRIVER_ PATH">">/oradata6/revwb7/oracle </InteractionVariable> Note: See JDBC Jar Files for identifying the correct "ojdbc<version>.jar" version to be copied.	Yes
OLAP_SERVER_ IMPLEMENTATION	Identifies if the OFSAA Infrastructure OLAP component needs to be configured depending on whether you intend to use the OLAP feature. The below numeric value should be set depending on the choice: YES - 1 NO - 0	No
Note: If value for OLAP_SERVER_IMPLEMENTATION is set to 1, it checks for following environment variables are set in .profile: ARBORPATH, HYPERION_HOME and ESSBASEPATH.		

InteractionVariable Name	Significance and Expected Value	Mandatory
SFTP_ENABLE	Identifies if the SFTP (Secure File Transfer Protocol) feature is to be enabled. The below numeric value should be set depending on the choice: SFTP - 1 FTP - 0	Yes
Note: The default value for SFTP_ENABLE is 1, which signifies that SFTP will be used. Oracle recommends using SFTP instead of FTP because SFTP is considered more secure. However, a client may choose to ignore this recommendation and to use FTP by setting SFTP_ENABLE to 0. This selection may be changed later by using the OFSAAI administration interface.		
FILE_TRANSFER_PORT	Identifies the port used for the file transfer service. The default value specified is 22 (SFTP). Specify value as 21 or any other PORT value if value for SFTP_ENABLE is 0. For example, <InteractionVariable name="FILE_TRANSFER_PORT">21</InteractionVariable>.	Yes
LOCALE	Identifies the locale information to be used during the installation. This release of the OFSAA Infrastructure supports only US English. For example, <InteractionVariable name="LOCALE">en_US</InteractionVariable>	Yes
Note: The below ports are used internally by the various OFSAA Infrastructure services. The default values mentioned below are set in the installation. If you intend to specify a different value, update the parameter value accordingly and ensure this port value is in the range of 1025 to 65535 and the respective port is enabled.		
JAVAPORT	9999	Yes
NATIVEPORT	6666	Yes
AGENTPORT	6510	Yes
ICCPORT	6507	Yes
ICCNATIVEPORT	6509	Yes
OLAPPORT	10101	Yes
MSGPORT	6501	Yes
ROUTERPORT	6500	Yes
AMPORT	6505	Yes
Note: If value for HTTPS_ENABLE is set to 1, ensure you have a valid certificate available from a trusted CA and the same is configured on your web application server. For more details on configuring your setup for HTTPS.		

InteractionVariable Name	Significance and Expected Value	Mandatory
HTTPS_ENABLE	Identifies if the UI should be accessed using HTTP or HTTPS scheme. The default value set is 0. The below numeric value should be set depending on the choice: YES - 1 NO - 0 For example, <InteractionVariable name="HTTPS_ENABLE">0</ InteractionVariable>	Yes
WEB_SERVER_IP	Identifies the HTTP Server IP/ Host name or Web Application Server IP/ Host name, to be used for accessing the UI. This IP would typically be the HTTP Server IP. If no separate HTTP Server is available, the value should be Web Application Server IP/Host name. For example, <InteractionVariable name="WEB_SERVER_ IP">10.11.12.13</InteractionVariable> or <InteractionVariable name="WEB_SERVER_ IP">myweb.server.com</InteractionVariable>	No
WEB_SERVER_PORT	Identifies the Web Server Port. This would typically be 80 for non SSL and 443 for SSL. If no separate HTTP Server exists, the value should be the port configured for Web Server. Note: The port value will not be accepted as 80 if HTTPS_ENABLE is 1 and as 443, if HTTPS_ENABLE is 0. For example, <InteractionVariable name="WEB_ SERVER_PORT">80</InteractionVariable>	No
CONTEXT_NAME	Identifies the web application context name which will be used to build the URL to access the OFSAA applications. The context name can be identified from a URL as below: <scheme>://<host>:<port>/<context-name>/lo gin.jsp Sample URL: https://myweb:443/ofsaadev/login.jsp For example, <InteractionVariable name="CONTEXT_ NAME">ofsaadev</InteractionVariable>	Yes

InteractionVariable Name	Significance and Expected Value	Mandatory
WEBAPP_CONTEXT_PATH	Identifies the absolute path of the exploded .ear file on the web application server. For Tomcat, specify the Tomcat directory path till /webapps, such as /oradata6/revwb7/tomcat/webapps/. For WebSphere, enter the WebSphere path as <WebSphere profile directory>/installedApps/ <NodeCellName>. For example, /data2/test//WebSphere/AppServer/profiles/ <Profile_ Name>/installedApps/aix-imfNode01Cell. Where aix-imf is Host name. For WebLogic, provide the WebLogic home directory path as /<WebLogic home directory path>/bea/wlserver_10.3 Note: For WebLogic, value specified for this attribute is ignored and value provided against attribute WEBLOGIC_DOMAIN_HOME is considered.	Yes
WEB_LOCAL_PATH	Identifies the absolute path to any directory on the web application server that can hold temporary files being uploaded as part of the applications usage. User can set this in FTPSHARE location to avoid the confusion. Note: In case of a clustered deployment, ensure this path and directory is same on all the nodes.	Yes
WEBLOGIC_DOMAIN_HOME	Identifies the WebLogic Domain Home. Specify the value only if WEBSERVERTYPE is set as 3 (WebLogic). For example, <InteractionVariable name="WEBLOGIC_DOMAIN_ HOME">/home/weblogic/bea/user_ projects/domains/mydomain </InteractionVariable>	Yes. Specify the value only if WEBSERVERTYPE is set as 3 (WebLogic)
OFSAAI_FTPSHARE_PATH	Identifies the absolute path to the directory identified as file system stage area. Note: The directory should exist on the same system on which the OFSAA Infrastructure is being installed (can be on a separate mount). The user mentioned in APP_SFTP_USER_ID parameter below should have RWX permission on the directory. For example, <InteractionVariable name="APP_FTPSHARE_PATH">">/oradata6/revwb7/ftpshare</InteractionVariable>	Yes
OFSAAI_SFTP_USER_ID	Identifies the user who has RWX permissions on the directory identified under parameter APP_FTPSHARE_PATH above.	Yes
HIVE_SERVER_PORT	HIVE SFTP Port. Typically, 22	Yes

InteractionVariable Name	Significance and Expected Value	Mandatory
HIVE_SERVER_FTPDRIVE	HIVE SFTP Folder Structure	Yes
HIVE_SERVER_FTP_USERID	HIVE SFTP User ID	Yes
HIVE_SERVER_FTP_PROTOCOL	HIVE Server File Transfer Protocol. For example. SFTP	Yes

APPENDIX A - CONFIGURING RESOURCE REFERENCE IN WEB APPLICATION SERVERS

This appendix includes the following topics:

Configure Resource Reference in WebSphere Application Server

This section is applicable only when the Web Application Server is WebSphere.

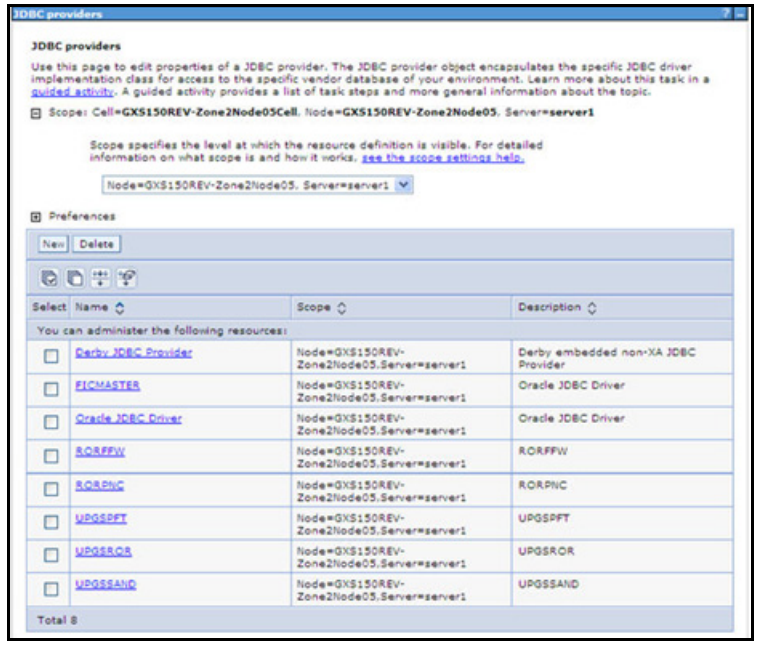
This section includes the following topics:

Create JDBC Provider

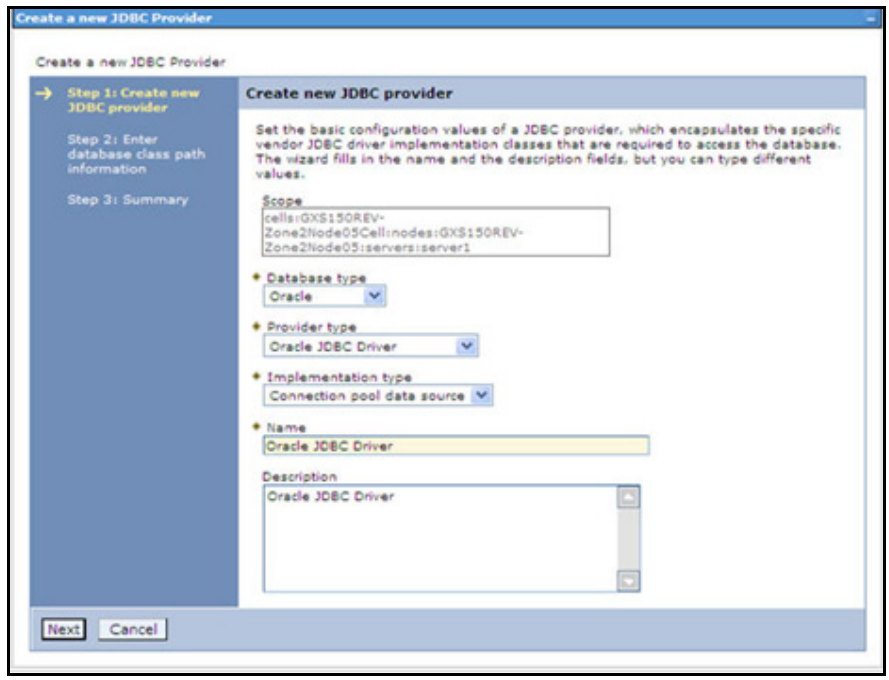
1. Open the WebSphere admin console in the browser window:

   `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.

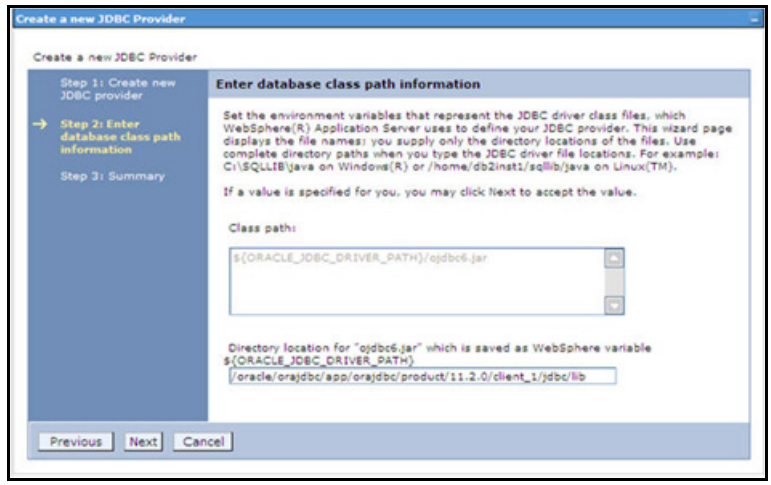
3. Expand the Resources option in the LHS menu and click JDBC > JDBC Providers to display the JDBC Providers window.



4. Select the **Scope** from the drop-down list. Scope specifies the level at which the resource definition is visible.
5. Click **New** to add new JDBC Provider under the Preferences section. The **Create new JDBC provider** window is displayed.



6. Enter the following details:
   - Database Type - Oracle
   - Provider Type- Oracle JDBC Driver
   - Implementation Type- Connection pool data source
   - Name- The required display name for the resource
   - Description - The optional description for the resource
7. Click **Next**.



8. Specify the directory location for "ojdbc<version>.jar" file. Ensure that you do not use the trailing slash file separators.

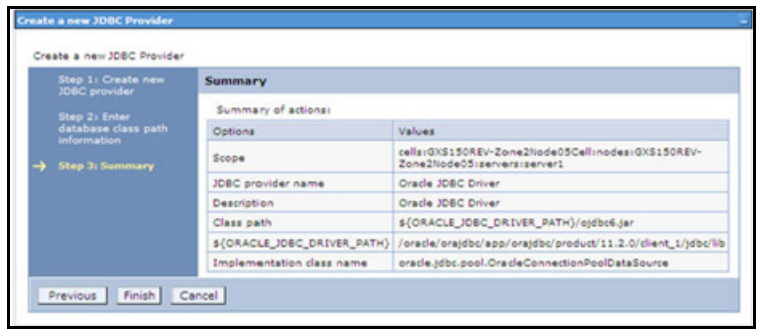
   The Oracle JDBC driver can be downloaded from the following Oracle Download site:
   - Oracle Database 11g Release 2 (11.2.0.4) JDBC Drivers
   - Oracle Database 12c Release 1 (12.1.0.1) JDBC Drivers

   Once downloaded, you need to copy the file in the required folder on the server.

Note: See JDBC Jar Files for identifying the correct ojdbc<version>.jar version to be copied.

After dowloading, you need to place the file in the required folder in your system. While creating the JDBC Provider, ensure that the path to the jar file in the folder is specified in the **Classpath** field in the previous window.

9. Click **Next** to display the **Summary** window.



10. Verify the details and click **Finish** to create the JDBC Provider.
11. The options to **Save** and **Review** are displayed. Click **Save**.

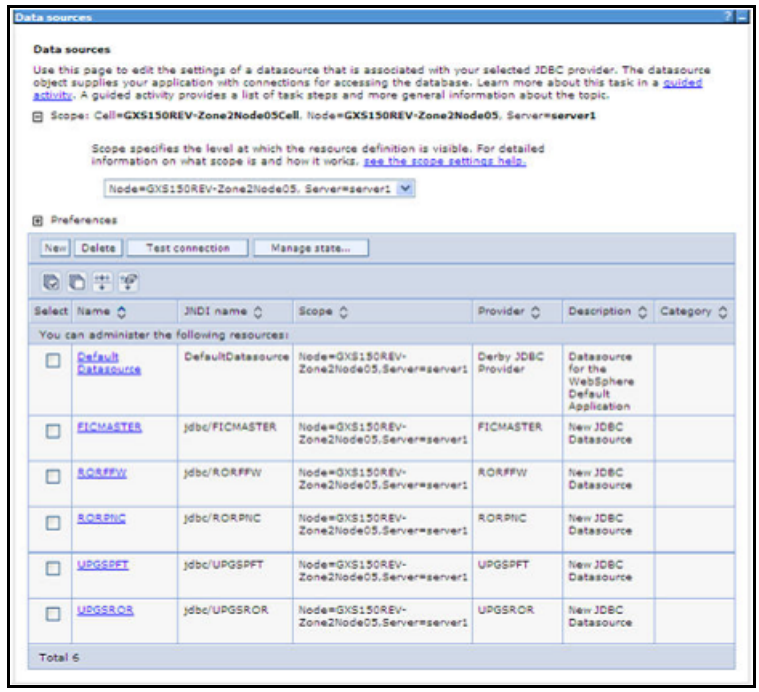
Create Data Source

The steps given below are applicable for both CONFIG and ATOMIC data source creation.

1. Open the WebSphere admin console in the browser window:

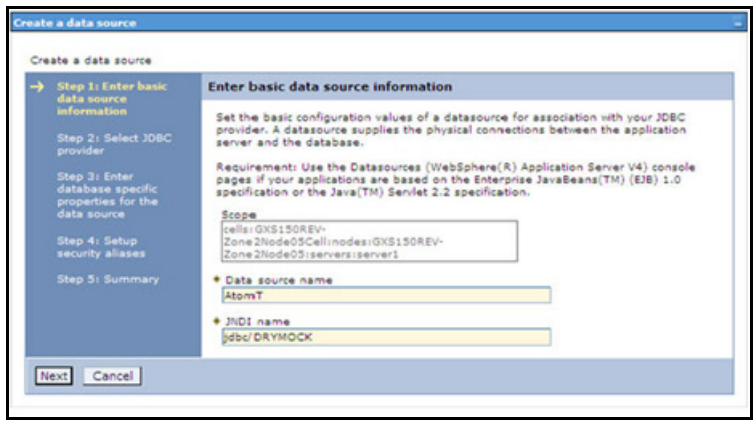
   `http://<ipaddress>:<administrative console port>/ibm/console`. (https if SSL is enabled). The Login window is displayed.

2. Login with the user id that has admin rights.
3. Expand the **Resources** option in the LHS menu and click **JDBC > Data sources** option to display the **Data sources** page.



4. Select the **Scope** from the drop down list. Scope specifies the level at which the resource definition is visible.

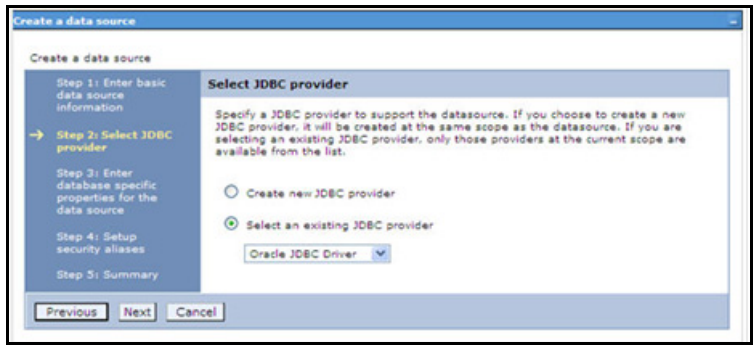
5. Click **New** to display the **Create a Data Source** window.



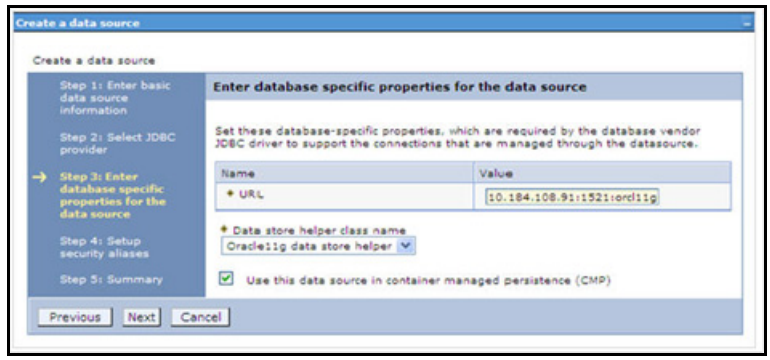
6. Specify the **Data Source name** and **JNDI name** for the new "Data Source".

   The **JNDI** and **Data Source name** are case sensitive. Ensure that JNDI name is same as the "Information Domain" name.

7. Click **Next** to display the **Select JDBC provider** window.



8. Select the option **Select an Existing JDBC Provider** and select the required JDBC provider from the drop-down list. Click **Next**.



9. Specify the database connection URL.

   For Example: `jdbc:oracle:thin:@<DB_SEREVER_IP>:<DB_SERVER_PORT>:<SID>`

10. Select **Data Store Helper Class Name** from the drop-down list and ensure that the checkbox **Use this data source in container managed persistence (CMP)** is selected.

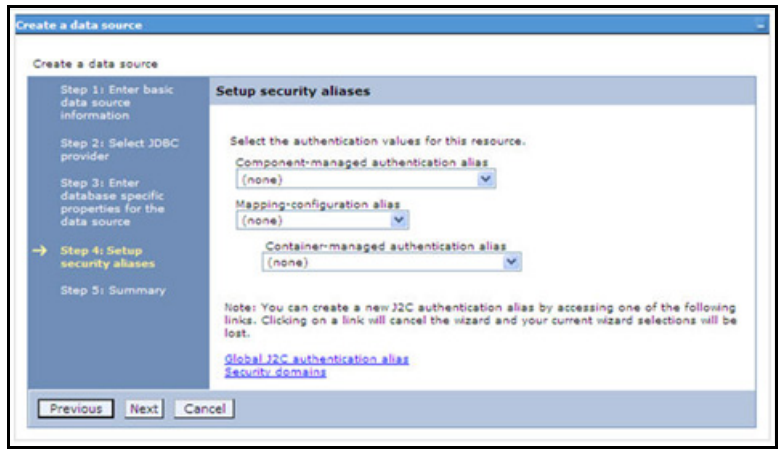
Note: For RAC configuration, provide the RAC URL specified during installation.

For Example:

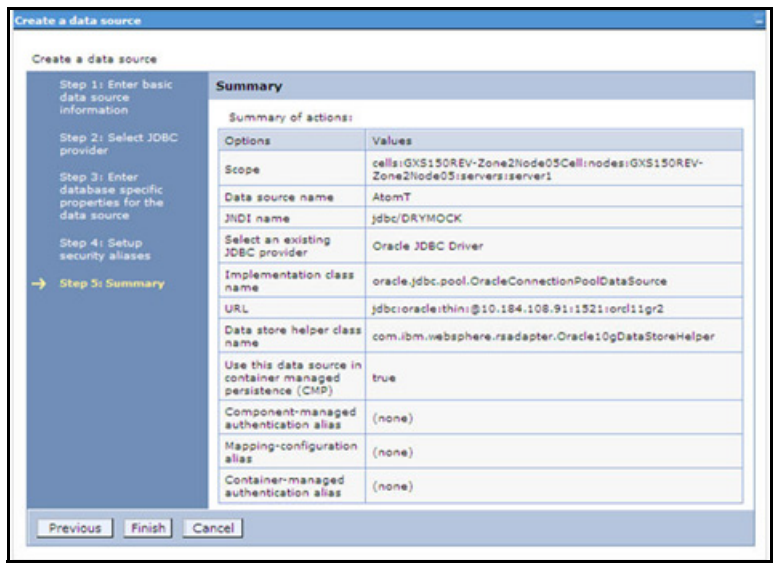
```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=10.11.12.13)
(port=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=10.11.12.14)(PORT=1521))(LOAD_BALANCE=no)(FAI
LOVER=yes))(CONNECT_DATA=(SERVICE_NAME=pqadb)))
```

---

11. Click **Next**.



12. Map the J2C authentication alias, if already created. If not, you can create a new J2C authentication alias by accessing the link given (**Global J2C authentication alias**) or you can continue with the data source creation by clicking Next and then Finish.



You can also create and map J2C authentication alias after creating the data source.

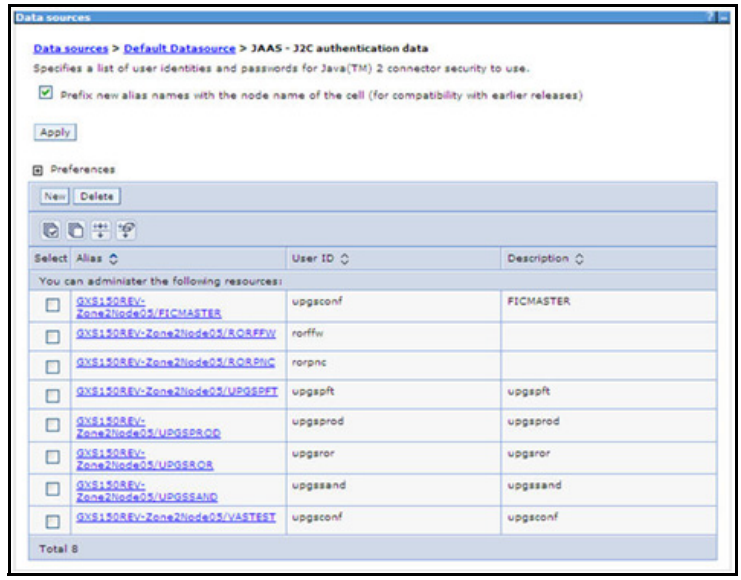
13. You must create another Data source by following the above procedure with jdbc/FICMASTER as JNDI name pointing to the "configuration schema" of Infrastructure.

J2C Authentication Details

The steps given below are applicable for creating both config and atomic J2C Authentication.

To create J2C Authentication details:

1. Select the newly created Data Source and click **JAAS - J2C authentication data** link under **Related Items**.



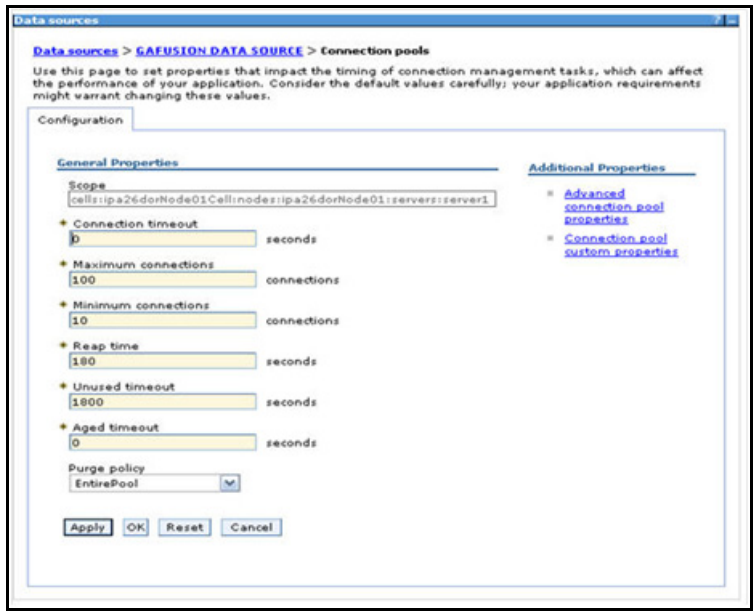
2. Click **New** under the **Preferences** section.

3. Enter the Alias, User ID, Password, and Description. Ensure the following:
   - User ID is the Oracle user ID created for the respective CONFIG and ATOMIC Schema for the "Information Domain".
   - Specify the CONFIG database user ID and password information for the jdbc/FICMASTER data source, and specify the ATOMIC database user ID and password information for the ATOMIC schema data source that you created earlier.
4. Click **Apply** and save the details.

JDBC Connection Pooling

To define the JDBC connection pooling ensure that you have created JDBC Provider and Data source to access the data from the database.

1. Expand the **Resources** option in the LHS menu and click **JDBC > Data sources** option to display the **Data sources** page.
2. Click the newly created Data Source `$DATA_SOURCE$` and navigate to the path **Data sources > $DATA_SOURCE$ > Connection pools**.



3. Set the values for the following:
   - **Connection timeout** to 0 seconds
   - **Maximum connections** to 100 connections
   - **Minimum connections** to 10 connections

   You can also define **Reap Time**, **Unused Timeout**, and **Aged Timeout** as required.

Configure Resource Reference in WebLogic Application Server

This section is applicable only when the Web Application Server is WebLogic.

This section includes the following topics:

- Create Data Source
- Create GridLink Data Source
- Configure Multi Data Sources
- Advanced Settings for Data Source
- JDBC Connection Pooling

In WebLogic, you can create "Data Source" in the following ways:

For a Non RAC Database instance, Generic Data Source has to be created. For more information, see Create Data Source.

For a RAC Database instance, Gridlink Data Source has to be created. For more information, see Create GridLink Data Source.

When Load Balancing/Fail over is required, Multi Data Source has to be created. For more information, see Configure Multi Data Sources.

Create Data Source

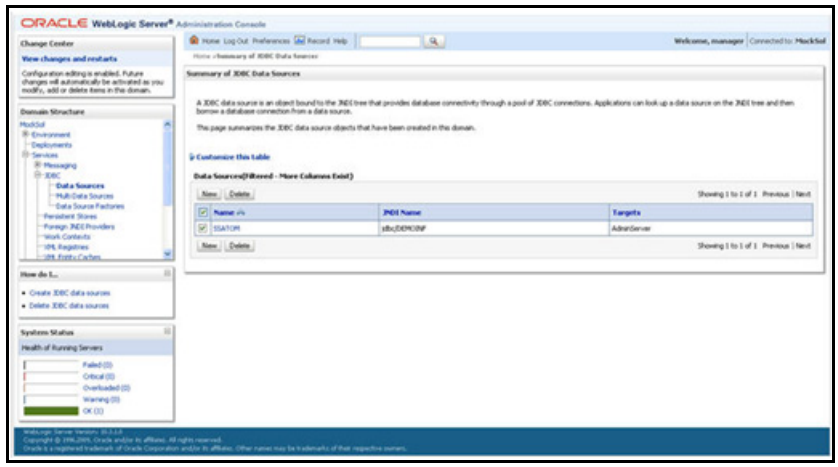
The steps given below are applicable for both config and atomic data source creation.

1. Open the WebLogic admin console in the browser window:

   `http://<ipaddress>:<administrative console port>/console`. (https if SSL is enabled). The Login window is displayed.

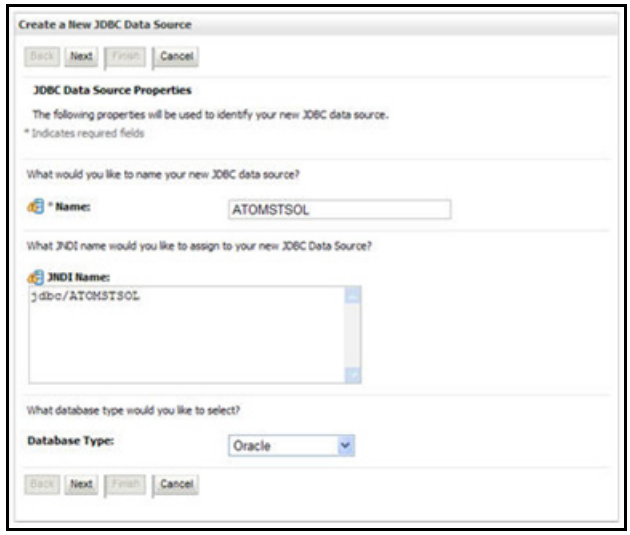
2. Login with the Administrator Username and Password.

3. From the LHS menu (Domain Structure), click **Services > Data Sources** to display the **Summary of JDBC Data Sources** window.



4. Click **New** and select **Generic Data Source** option to display the **Create a New JDBC Data Source** window.

   You can also select **GridLink Data Source** or **Multi Data Source** while creating a Data Source. For more information, see Create GridLink Data Source or Configure Multi Data Sources.



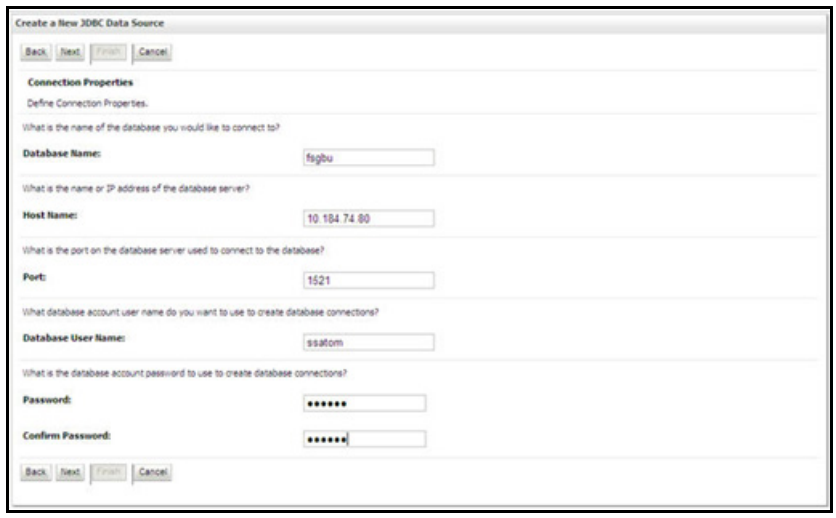
5. Enter JDBC data source **Name**, **JNDI Name**, and select the **Database Type** from the drop-down list. Click **Next**.

   Ensure the following:

   - The JNDI Name field should be in the format "jdbc/informationdomain"
   - Same steps needs to be followed to create a mandatory data source pointing to the "configuration schema" of infrastructure with jdbc/FICMASTER as JNDI name.
   - JNDI Name is the same as mentioned in web.xml file of OFSAAI Application.
   - Required "Database Type" and "Database Driver" should be selected.

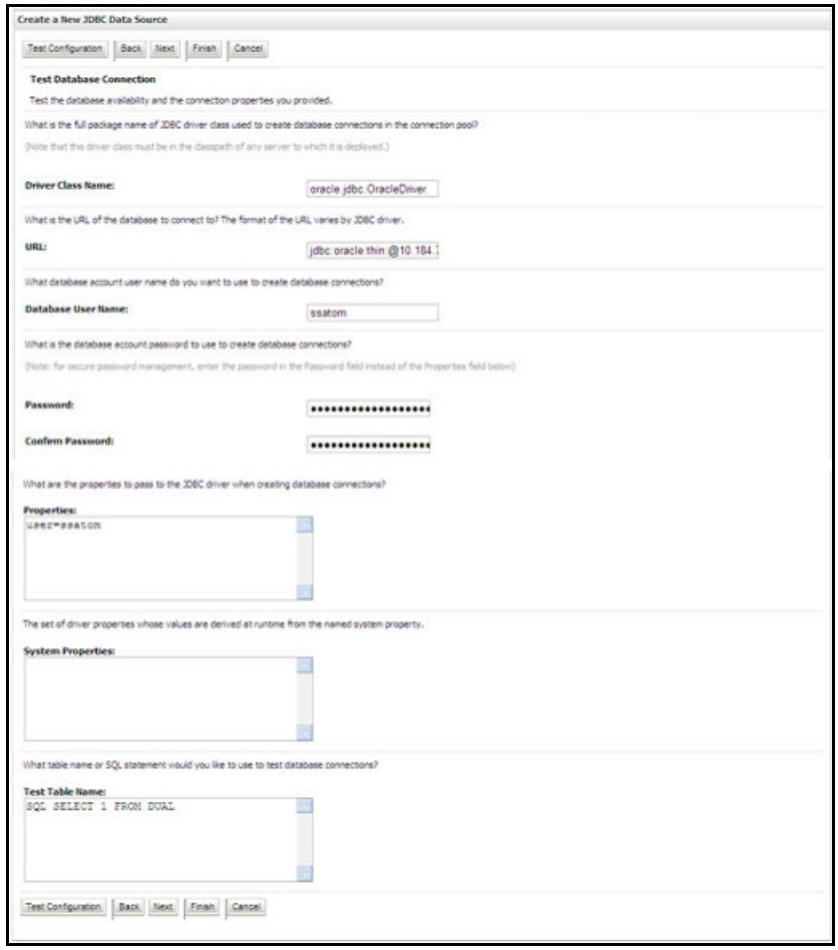
6. Select the **Database Driver** from the drop-down list. You need to select the Database Driver depending on database setup, that is, with or without RAC. Click **Next**.

7. Select the **Supports Global Transactions** checkbox and the **One-Phase Commit** option.
8. Click **Next** to display the **Connection Properties** window.



9. Enter the required details such as the **Database Name**, **Host Name**, **Port**, **Oracle User Name**, and **Password**.

10. Click **Next** to display the **Test Database Connection** window.



11. Verify the details and click **Test Configuration** and test the configuration settings.

A confirmation message is displayed stating "Connection test succeeded."

12. Click **Finish**. The created "Data Source" is displayed in the list of Data Sources.

Note: “User ID" is the Oracle user ID that is created for the respective "Information Domain".

"User ID" to be specified for data source with "FICMASTER" as "JNDI" name should be the Oracle user ID created for the CONFIG schema.

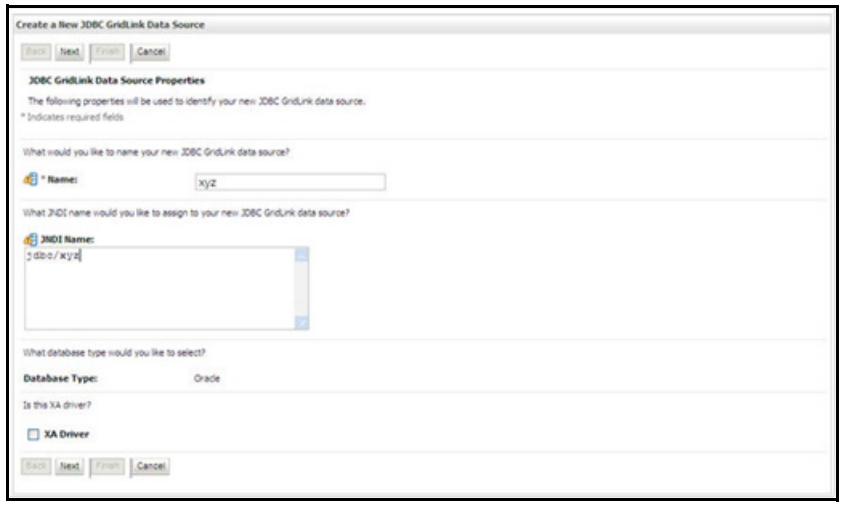
---

13. Select the new **Data Source** and click the **Targets** tab.

14. Select the **AdminServer** option and click **Finish**.

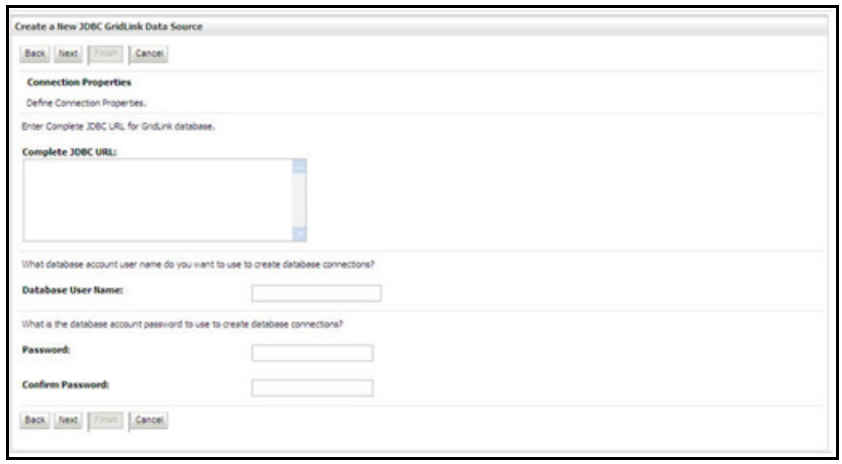
Create GridLink Data Source

If you have selected the option, **New > GridLink Data Source** while creating the "Data Source", you can directly specify the JDBC URL as indicated.



1. Enter Data Source **Name**, and **JNDI Name**.

Ensure that the "JNDI Name" field is specified in the format "jdbc/infodomname" and the **XA Driver** checkbox is not selected. Click **Next**.



2. Specify **Complete JDBC URL**, **Database User Name**, and **Password**. Click **Finish**. The created "Data Source" is displayed in the list of Data Sources.

Configure Multi Data Sources

A JDBC multi data source is an abstraction around a group of data sources that provides load balancing and failover between data sources. As with data sources, multi data sources are also bound to the JNDI tree. Applications can look up a multi data source on the JNDI tree and then reserve a database connection from a data source. The multi data source determines from which data source to provide the connection.

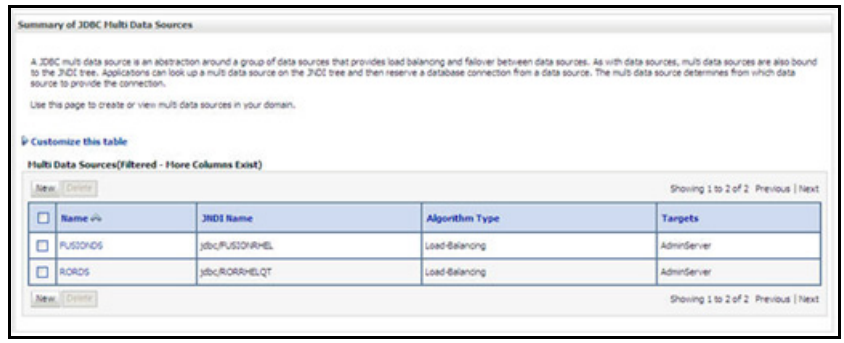
When the database used is Oracle RAC (Real Application Clusters) which allows Oracle Database to run across a set of clustered servers, then group of data sources can be created for instances running on a set of clustered servers and a JDBC multi data source can be created so that applications can look up a multi data source on the JNDI tree to reserve database connection. If a clustered server fails, Oracle continues running on the remaining servers.

1. Open the WebLogic admin console in the browser window:

   `http://<ipaddress>:<administrative console port>/console`. (https if SSL is enabled). The Login window is displayed.

2. Login with the "User ID" that has admin rights.

3. In the LHS menu (Domain Structure), select **Services > JDBC > Multi Data Sources** to display the **Summary of JDBC Multi Data Sources** window.



4. Click New to display the New JDBC Multi Data Source screen.

Note: Ensure that the Data Sources which needs to be added to new JDBC Multi Data Source has been created.

5. Enter the **JDBC Source Name**, **JNDI name**, and select the **Algorithm Type** from the drop-down list. Click **Next**.

Note: The JNDI Name has to be specified in the format jdbc/infodomname.

JNDI Name of the Data Sources that will be added to new JDBC Multi data source should be different from the JNDI name specified during Multi Data Source.

Same steps needs to be followed to create a mandatory data source pointing to the "configuration schema" of infrastructure with jdbc/FICMASTER as JNDI name for Data Source.

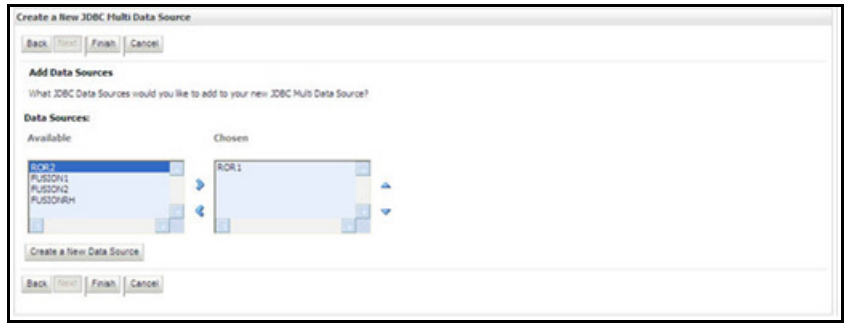
Same steps needs to be followed to create a mandatory data source pointing to the "configuration schema" of infrastructure with jdbc/FICMASTER as JNDI name for Data Source.

JNDI Name provided in multi data source should be the same name that will be mentioned in the web.xml file of OFSAAI Application.

You can select the Algorithm Type as Load-Balancing.

6. Select the **AdminServer** check box and click **Next**.

7. Select the type of data source which will be added to new JDBC Multi Data Source. Click **Next**.

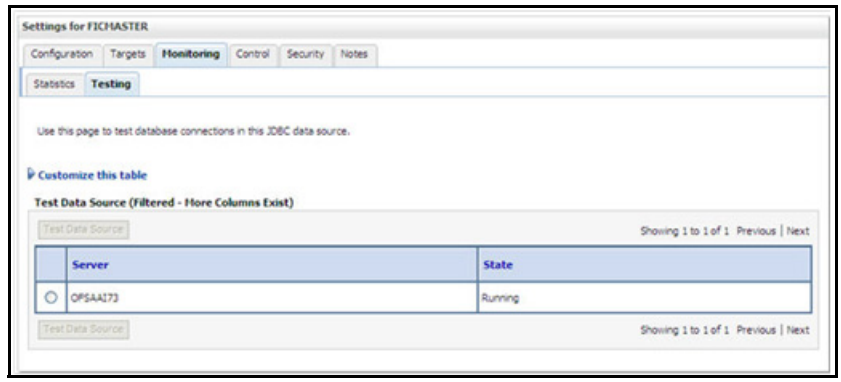


8. Map the required Data Source from the Available Data Sources. Click **Finish**.

   The New JDBC Multi Data Source is created with added data sources.

Advanced Settings for Data Source

1. Click the new Data Source from the **Summary of JDBC Data Sources** window. The **Settings for <Data Source Name>** window is displayed.
2. Select the **Connection Pooling** tab given under **Configuration**.
3. Go to the **Advanced** option at the bottom of the page, and check the **Test Connection of Reserve** checkbox (Enables Weblogic Server to test a connection before giving it to a client).
4. To verify if the data source is valid, select "Data Source name". For example, FICMASTER.



5. Select the server and click **Test Data Source**.

   A message is displayed indicating that the test was successful.
6. Once the "Data Source" is created successfully, the following messages are displayed:
   - All changes have been activated. No restart is necessary.
   - Settings updated successfully.

   If not, follow the steps given above to recreate the data source.

JDBC Connection Pooling

To define the JDBC connection pooling, ensure that you have created JDBC Provider and Data source to access the data from the database.

1. Click the newly created Data Source $DATA_SOURCE$ and navigate to the path Home >Summary of Services: JDBC >Summary of JDBC Data Sources >JDBC Data Source-<INFODDOM_NAME>
2. Set the values for Initial Capacity to 10, Maximum Capacity to 100, Capacity Increment by 1, Statement Cache Type to LRU, and Statement Cache Size to 10.
3. Click **Save**.

Configure Resource Reference in Tomcat Application Server

This section is applicable only when the Web Application Server is Tomcat.

This section includes the following topics:

- Create Data Source
- JDBC Connection Pooling
- Class loader Configuration for Apache Tomcat

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

Note: See JDBC Jar Files for identifying the correct `ojdbc<version>.jar` version to be copied.

Create Data Source

To create "data source" for OFSAA application, navigate to <Tomcat Home>/conf and edit the following block of text by replacing the actual values in server.xml.

Note: The User-IDs for configuration/ atomic schemas have the prefix of setupinfo depending on the value set for `PREFIX_SCHEMA_NAME` in `<<APP Pack>>_SCHEMA_IN.XML` file of Schema Creator Utility.

For example: If the value set for `PREFIX_SCHEMA_NAME` is DEV and the schema name was mentioned as `ofsaaconf`, then the actual schema created in the database would be DEV_ofsaaconf.

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

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

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

JDBC Connection Pooling

To define the JDBC connection pooling, do the following:

1. Copy *$ORACLE_HOME/jdbc/lib/ojdbc<version>.jar* to the path *$TOMCAT_DIRECTORY/lib/*.

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

2. Edit the server.xml present under the path *$TOMCAT_DIRECTORY/conf/* with the below changes, which are required for connection pooling.

```
<Context path="/ $CONTEXTNAME$" docBase=" $APP_DEPLOYED_PATH$ " debug="0"
reloadable="true" crossContext="true">
    <Resource auth="Container"
    name="jdbc/ $INFODOM_NAME$"
    type="javax.sql.DataSource"
    driverClassName="oracle.jdbc.driver.OracleDriver"
    username=" $ATOMICSCHEMA_USERNAME$"
    password="$ATOMICSCHEMA_PASSWORD$"
    url="$JDBC_CONNECTION_URL"
    maxActive="100"
    maxIdle="30"
    maxWait="10000"
    removeAbandoned="true" removeAbandonedTimeout="60"
    logAbandoned="true"/>
</Context>
```

Note the following:

- $APP_DEPLOYED_PATH$ should be replaced by OFSAAI application deployed path.
- $INFODOM_NAME$ should be replaced by Infodom Name.
- $ATOMICSCHEMA_USERNAME$ should be replaced by Atomic schema database user name.
- $ATOMICSCHEMA_PASSWORD$ should be replaced by Atomic schema database password.
- $JDBC_CONNECTION_URL should be replaced by JDBC connection string jdbc:Oracle:thin:<IP>:<PORT>:<SID>. For example, jdbc:oracle:thin 10.80.50.53:1521:soluint
- The User-IDs for configuration/ atomic schemas have the prefix of setupinfo depending on the value set for PREFIX_SCHEMA_NAME in <<APP Pack>>_SCHEMA_IN.XML file of Schema Creator Utility.

  For example: if the value set for PREFIX_SCHEMA_NAME is DEV and the schema name was mentioned as ofsaaconf, then the actual schema created in the database would be DEV_ofsaaconf.

Class loader Configuration for Apache Tomcat

Edit the server.xml available in *$TOMCAT_HOME/conf/* folder.

Add tag <Loader delegate="true" /> within the <Context> tag, above the <Resource> tag. This is applicable only when the web application server is Apache Tomcat 8.

This configuration is required if Apache Tomcat version is 8.

APPENDIX A - TDE, DATA REDACTION AND THE CORRESPONDING SETTINGS IN OFSAA

This section provides information to help enable TDE (Transparent Data Encryption), Data Redaction and its corresponding settings in OFSAA. For more details on TDE and Data Redaction, see the Database Advanced Security Guide.

The following sections provide details to enable TDE in the database and run the schema utility.

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.

Creating a Wallet

The environment setup for tablespace encryption is the same as that for transparent data encryption. Before creating an encrypted tablespace, create a wallet to hold the encryption key. The search order to find the wallet is described in the following list:

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

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

1. Add the following entry into the `sqlnet.ora` file on the server and check if the specified directory is created:

```
ENCRYPTION_WALLET_LOCATION=
    (SOURCE=(METHOD=FILE)(METHOD_DATA=
       (DIRECTORY=/u01/app/oracle/admin/DB11G/WALLET/)))
```

   For RAC-DB or ASM enabled databases, use the following entry:

```
ENCRYPTION_WALLET_LOCATION=
    (SOURCE=
        (METHOD=FILE)
        (METHOD_DATA=
        (DIRECTORY=+DATA/PRODCDB/WALLET)
    )
)
```

2. For ASM Diskgroup, create a relevant directory as defined by `ENCRYPTION_WALLET_LOCATION` using the following instruction:

```
[oracle@server ~]$ echo $ORACLE_SID
+ASM

[oracle@server ~]$ asmcmd
ASMCMD>
ASMCMD> cd +DATA/PRODCDB
ASMCMD> mkdir WALLET
ASMCMD> cd WALLET/
ASMCMD> pwd
+DATA/PRODCDB/WALLET
```

3. Use the following command to create and open the wallet:

```
CONN sys/password@serviceid AS SYSDBA
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "my Password";
```

4. Reopen Wallets after the instance restart and then close it to prevent access to encrypted data using the following command.

```
ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY "my Password";
```

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

Alternatively, you can create an Auto-Login or Local-Login Keystore to avoid opening the Keystore manually every time. To enable the Keystore to open automatically, use the following command:

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

Running the Schema Utility with Encryption

Run the schema creator utility by including the **encrypt=on** option in the Tablespace tag in the Schema in the XML file. You have to perform this procedure manually as it's not a part of the schema template originally.

```
<APPPACKSCHEMA>
    <APP_PACK_ID>OFS_AAAI_PACK</APP_PACK_ID>
    <JDBC_URL>jdbc:oracle:thin:@whf00ajn:1521:OFSPQA12CDB</JDBC_URL>
    <JDBC_DRIVER>oracle.jdbc.driver.OracleDriver</JDBC_DRIVER>
    <HOST><HOST_NAME></HOST>
    <SETUPINFO NAME="t608" PREFIX_SCHEMA_NAME="Y"/>
    <PASSWORD APPLYSAMEFORALL="Y" DEFAULT="<password>"/>
    <TABLESPACES>
        <TABLESPACE NAME="OFS_AAI_TBSP" VALUE="TS_USERS1" DATAFILE="<HOME_DIR>/ora12c/app/
        oracle/oradata/OFSPQA12CDB/ts_users1.dbf" SIZE="500M" AUTOEXTEND="OFF" ENCRYPT="ON"
        />
    </TABLESPACES>
    <SCHEMAS>
        <SCHEMA TYPE="CONFIG" NAME="ofsaaconf" PASSWORD="" APP_ID="OFS_AAI"
        DEFAULTTABLESPACE="TS_USERS1" TEMPTABLESPACE="TEMP" QUOTA="unlimited"/>
        <SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_AAAI"
        DEFAULTTABLESPACE="TS_USERS1" TEMPTABLESPACE="TEMP" QUOTA="unlimited"
        INFODOM="OFSAAAIINFO"/>
        <SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_IPE"
        DEFAULTTABLESPACE="TS_USERS1" TEMPTABLESPACE="TEMP" QUOTA="unlimited"
        INFODOM="OFSAAAIINFO"/>
    </SCHEMAS>
</APPPACKSCHEMA>
```

Testing the Encryption

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

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

The following result is displayed, which indicates whether the TABLESPACE is encrypted (ENCRYPTED TS - YES) or not (ENCRYPTED TS - NO) in the ENC column:

TABLESPACE_NAME	ENC
SYSTEM	NO
SYSAUX	NO
UNDOTBS1	NO
TEMP	NO
USERS	NO
ENCRYPTED_TS	YES

6 rows selected.

APPENDIX A - DATA PROTECTION IMPLEMENTATION IN OFSAA

This chapter includes sections about Data Protection implemented in OFSAA applications and covers the following sections:

Right to be Forgotten

This section covers the following sub-sections:

Introduction to Right to be Forgotten

Right to be Forgotten is the task of removing PII (Personally Identifiable Information) of a Data Subject for the given Party. The financial institution can delete PII for those Data Subjects who have requested this Right to be Forgotten functionality.

The Data Subjects may have made significant financial transactions, and/or financial information may be required for regulatory or compliance reporting. Deleting the complete record that consists of PII may lead to issues in data reconciliation. In OFSAA, the PII data will be replaced with randomized values and therefore, the complete Data Subject record is retained. As a result, financial information is retained; however, the associated Party PII is removed permanently.

Implementation of Right to be Forgotten by OFSAA

To implement Right to be Forgotten:

1. Use the FSI_PARTY_RIGHT_TO_FORGET table to collect the input list of Party IDs for which PII must be removed from the system. The financial institution must source this Party ID list into the FSI_PARTY_RIGHT_TO_FORGET table, and then invoke the batch (<<INFODOM>>_RightToForget) or schedule it.

   Note: For sample query, see Sample Query for the FSI_PARTY_RIGHT_TO_FORGET table.

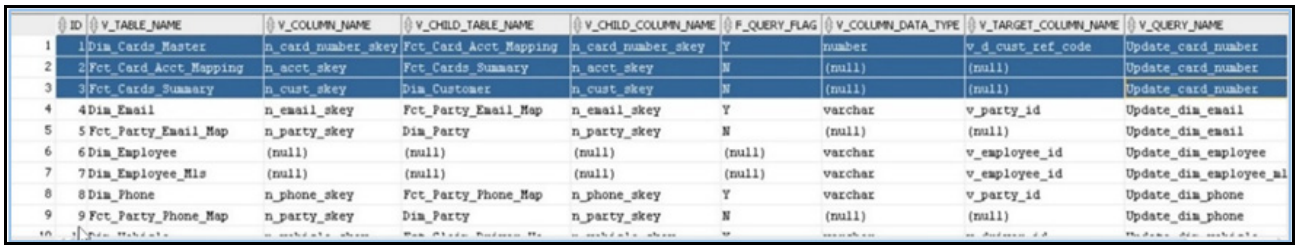
2. Use the AAI table AAI_DRF_FUNCTION_COLUMN_MAP to store the PII attribute list. During the Right to Forget batch execution, AAI_DRF_FUNCTION_COLUMN_MAP table is referred to randomize the PII values. See the Data Redaction section in OFSAAI Administration Guide.

3. Use the AAI table AAI_DRF_QUERY_METADATA to store the query metadata, which is used during the <<INFODOM>>_RightToForget batch execution. This is the query metadata table that can lead to two types of queries:
   a. When the table consists of Party Identifier as an attribute, a simple record is required in the metadata query table.

      For example:

      Select v_party_id from Dim_Party where v_party_id='10'

   b. When the table does not consist of Party Identifier as an attribute, an interrelated set of records are required in the metadata query table AAI_DRF_QUERY_METADATA. Compose these set of records in a systematic way such that, for the selected Party Identifier, the table join procedure can be performed and traversed to reach the required PII attribute.



	ID	V_TABLE_NAME	V_COLUMN_NAME	V_CHILD_TABLE_NAME	V_CHILD_COLUMN_NAME	F_QUERY_FLAG	V_COLUMN_DATA_TYPE	V_TARGET_COLUMN_NAME	V_QUERY_NAME
1	1	Dim_Cards_Master	n_card_number_skey	Fct_Card_Acct_Mapping	n_card_number_skey	Y	number	v_d_cust_ref_code	Update_card_number
2	2	Fct_Card_Acct_Mapping	n_acct_skey	Fct_Cards_Summary	n_acct_skey	N	(null)	(null)	Update_card_number
3	3	Fct_Cards_Summary	n_cust_skey	Dim_Customer	n_cust_skey	N	(null)	(null)	Update_card_number
4	4	Dim_Email	n_email_skey	Fct_Party_Email_Map	n_email_skey	Y	varchar	v_party_id	Update_dim_email
5	5	Fct_Party_Email_Map	n_party_skey	Dim_Party	n_party_skey	N	(null)	(null)	Update_dim_email
6	6	Dim_Employee	(null)	(null)	(null)	(null)	varchar	v_employee_id	Update_dim_employee
7	7	Dim_Employee_Mls	(null)	(null)	(null)	(null)	varchar	v_employee_id	Update_dim_employee_ml
8	8	Dim_Phone	n_phone_skey	Fct_Party_Phone_Map	n_phone_skey	Y	varchar	v_party_id	Update_dim_phone
9	9	Fct_Party_Phone_Map	n_party_skey	Dim_Party	n_party_skey	N	(null)	(null)	Update_dim_phone

Table definition for AAI_DRF_QUERY_METADATA

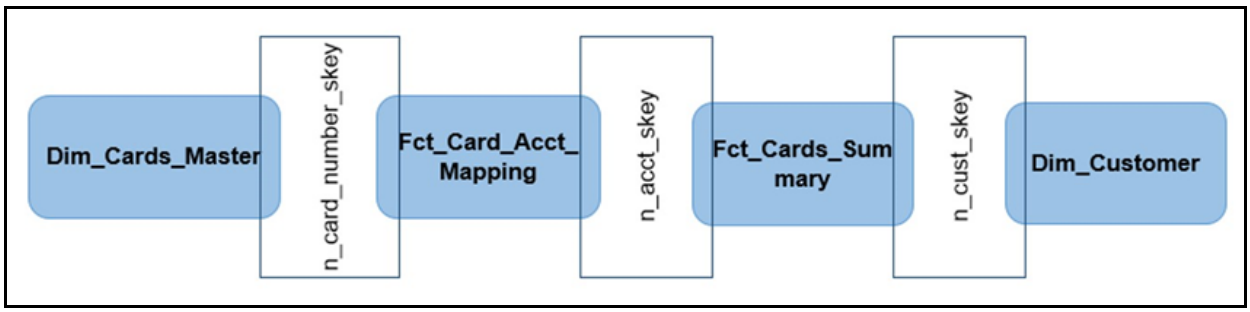
Column Name	Column Type	Description
ID	Number	This is the Primary Key field. You must enter a numerical value.
V_TABLE_NAME	Varchar	This is the source table name.
V_COLUMN_NAME	Varchar	This is the source column name.
V_CHILD_TABLE_NAME	Varchar	This is the table name, which must be linked to the V_TABLE_NAME. If the same table name is repeated with the same column name V_COLUMN_NAME, then the AND condition is formed with V_CHILD_TABLE_NAME. V_CHILD_TABLE_NAME
V_CHILD_COLUMN_NAME	Varchar	This the column name, which must be linked to the V_COLUMN_NAME.
F_QUERY_FLAG	Varchar	Enter Y or N, which is case sensitive. If the value is Y, then you must form a query from V_TABLE_NAME .V_COLUMN_NAME
V_COLUMN_DATA_TYPE	Varchar	Mention the Data Type of the V_COLUMN_NAME. This is required only if F_QUERY_FLAG = Y.

Column Name	Column Type	Description
V_TARGET_COLUMN_NAME	Varchar	Mention the PARTY_ID column name, which is required only if F_QUERY_FLAG = Y.
V_QUERY_NAME	Varchar	Mention the same query for a set of joining tables and columns. The set of tables and columns under join query are grouped together using the same query name.

For example:

Dim_Cards_Master table does not consist of n_cust_skey (n_cust_skey is the required Primary Key for the PII Attribute n_card_number_skey). Therefore, perform the table join procedure similar to the following query:

```
Select Dim_Cards_Master.n_card_number_skey from Dim_Cards_Master Dim_Cards_Master,
Fct_Card_Acct_Mapping Fct_Card_Acct_Mapping,
Fct_Cards_Summary Fct_Cards_Summary, Dim_Customer Dim_Customer where
Dim_Cards_Master.n_card_number_skey=Fct_Card_Acct_Mapping.n_card_number_skey and
Fct_Card_Acct_Mapping.n_acct_skey=Fct_Cards_Summary.n_acct_skey and
Fct_Cards_Summary.n_cust_skey=Dim_Customer.n_cust_skey and v_d_cust_ref_code='GDPR'
```



Where Dim_Customer.n_cust_skey is a Number Datatype.

Note: For more sample queries generated using the query metadata table, see Sample Queries using the AAI_DRF_QUERY_METADATA Metadata Table.

To arrive at the above-mentioned query, follow these steps:

In first figure, the required table Dim_Cards_Master does not consist of Party Identifier. Therefore, perform the table join procedure using the AND condition at the table level.

i. Search for a table, which consists of the Party Identifier field. In this query, we have searched for the table Dim_Customer with unique identifier n_cust_skey field. This table must be joined with the required table Dim_Cards_Master.

ii. However, the tables Dim_Cards_Master and Dim_Customer do not consist of any common column name to perform the table join operation. Therefore, search for one more table Fct_Card_Acct_Mapping. This table (Fct_Card_Acct_Mapping) consists of common column name (n_card_number_skey) between Dim_Cards_Master table and itself.

iii. Join the Fct_Card_Acct_Mapping table, which consists of common column name (n_acct_skey) with another table Fct_Cards_Summary.

iv. Join the Fct_Cards_Summary table, which consists of common column name (n_cust_skey) with the final table Dim_Customer.

v. Now, the Dim_Cards_Master table is joined with the Dim_Customer table.

c. You must arrive at the skey or equivalent column in the table, which consists of the required PII attributes. Then the <<INFODOM>>_RightToForget batch uses this key to filter records (For example: Dim_Cards_Master) and randomize all the PIIs listed in the AAI_DRF_FUNCTION_COLUMN_MAP for that table.

4. Now, PII attributes can be queried and the values are randomized.

Sample Queries using the AAI_DRF_QUERY_METADATA Metadata table

These are the sample queries generated using the AAI_DRF_QUERY_METADATA table:

Example 1:

```
select DIM_MANAGEMENT.n_manager_skey from DIM_MANAGEMENT DIM_MANAGEMENT, FCT_CUSTOMER
FCT_CUSTOMER, DIM_CUSTOMER DIM_CUSTOMER where
DIM_MANAGEMENT.n_manager_skey=FCT_CUSTOMER.n_manager_skey and
FCT_CUSTOMER.n_cust_skey=DIM_CUSTOMER.n_cust_skey and DIM_CUSTOMER.v_d_cust_ref_code
in(?,?)
```

Example 2:

```
select  DIM_EMAIL.n_email_skey from DIM_EMAIL DIM_EMAIL, FCT_PARTY_EMAIL_MAP
FCT_PARTY_EMAIL_MAP, DIM_PARTY DIM_PARTY where
DIM_EMAIL.n_email_skey=FCT_PARTY_EMAIL_MAP.n_email_skey and
FCT_PARTY_EMAIL_MAP.n_party_skey=DIM_PARTY.n_party_skey and DIM_PARTY.v_party_id
in(?,?)
```

Example 3:

```
select  STG_CLAIM_DETAILS.v_claim_id from STG_CLAIM_DETAILS STG_CLAIM_DETAILS,
STG_CLAIM_CLAIMANT STG_CLAIM_CLAIMANT where
STG_CLAIM_DETAILS.v_claim_id=STG_CLAIM_CLAIMANT.v_claim_id and
STG_CLAIM_CLAIMANT.v_cust_ref_code in(?,?)
```

Example 4:

```
select STG_CONTACT_MASTER.v_contact_id from STG_CONTACT_MASTER STG_CONTACT_MASTER,
DIM_CONTACT DIM_CONTACT where STG_CONTACT_MASTER.v_contact_id=DIM_CONTACT.v_contact_id
and DIM_CONTACT.v_customer_id in(?,?)
```

Example 5:

```
select  DIM_CARDS_MASTER.n_card_number_skey from DIM_CARDS_MASTER DIM_CARDS_MASTER,
FCT_CARD_ACCT_MAPPING FCT_CARD_ACCT_MAPPING, FCT_CARDS_SUMMARY FCT_CARDS_SUMMARY where
DIM_CARDS_MASTER.n_card_number_skey=FCT_CARD_ACCT_MAPPING.n_card_number_skey and
FCT_CARD_ACCT_MAPPING. n_acct_skey=FCT_CARDS_SUMMARY.n_acct_skey and
FCT_CARDS_SUMMARY.v_d_cust_ref_code in(?,?)
```

Sample Query for the FSI_PARTY_RIGHT_TO_FORGET table

This is the sample entry for the FSI_PARTY_RIGHT_TO_FORGET table:

```
Insert into FSI_PARTY_RIGHT_TO_FORGET values (SYSDATE, <<PARTY_ID_FROM_Ur_ENV>>,
'Testing Right2Forget');
```

Data Portability

According to the Data Protection guidelines, a scenario may occur with a customer in which a Data Subject requests the financial institution to share the PII of that Data Subject stored in the application. To cater to such a scenario, the customer may use T2F (Table to File) functionality provided by AAI. This T2F functionality enables the customer to query the data warehouse and save the attributes to a file.

Data Portability Scenario

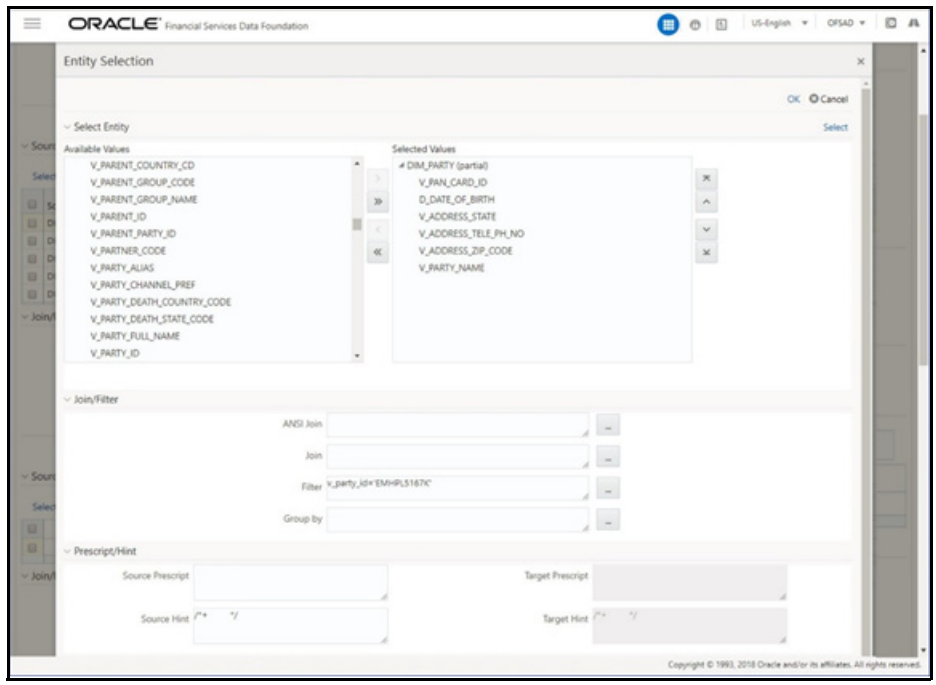
A sample scenario to apply Data Portability:

1. The DIM_PARTY table consists of a set of PIIs for multiple Data Subjects.

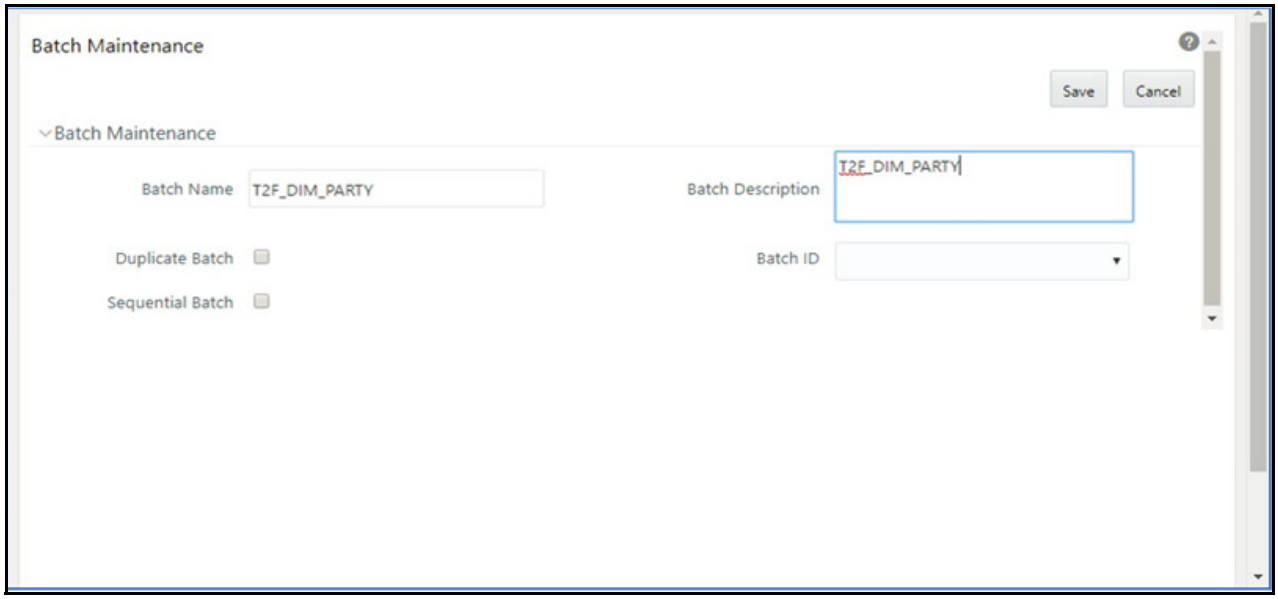
	V_PARTY_NAME	V_PAN_CARD_ID	D_DATE_OF_BIRTH	D_DATE_OF_BIRTH_1	V_ADDRESS_TELE_PH_NO	V_ADDRESS_STATE	V_ADDRESS_STATE_1
1	Aditya Sharma	HSWNJ8291T	09-JAN-93	09-JAN-93	8801283098	Himachal Pradesh	Himachal Pradesh
2	Maria Victor	PCLDS7413N	15-SEP-84	15-SEP-84	9024372784	Karnataka	Karnataka
3	Abdul Mohammed	AHJNS8384F	04-DEC-73	04-DEC-73	9852198762	Orissa	Orissa
4	Vibha Rao	RQSAA7190L	13-MAY-78	13-MAY-78	8962735610	Maharashtra	Maharashtra
5	Sharanya Gupta	EMHPL5167K	29-JAN-90	29-JAN-90	9901838919	Punjab	Punjab

   A Data Subject requests the bank to share a copy of the PII data of that Data Subject stored by the bank. For illustration, the Data Subject with V_PAN_CARD_ID EMHPL5167K is used.

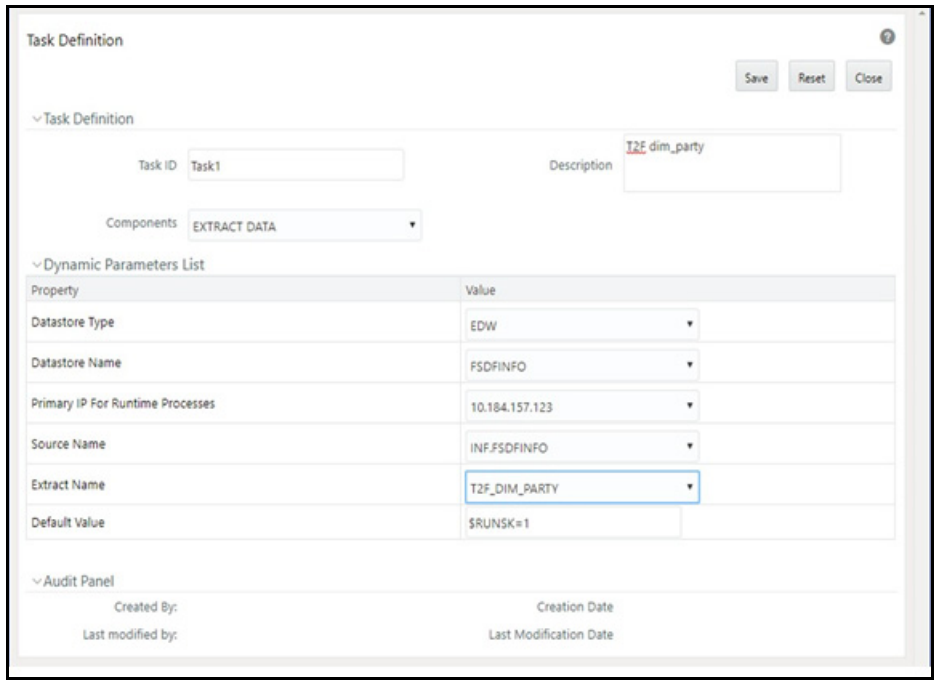
2. To make a file copy of the PII requested by the Data Subject, the User (bank) must perform T2F data mapping. Follow the Data Mapping procedure. See the *Defining Data Mapping to File (T2F, H2F)* section in the *Data Mapping* part in the OFS AAAI Application Pack Minor Release 8.0.6.0.0 User Guide to:
   a. Create a T2F definition for the scenario mentioned in step 1. V_PAN_CARD_ID is the V_PARTY_ID in the DIM_PARTY table.



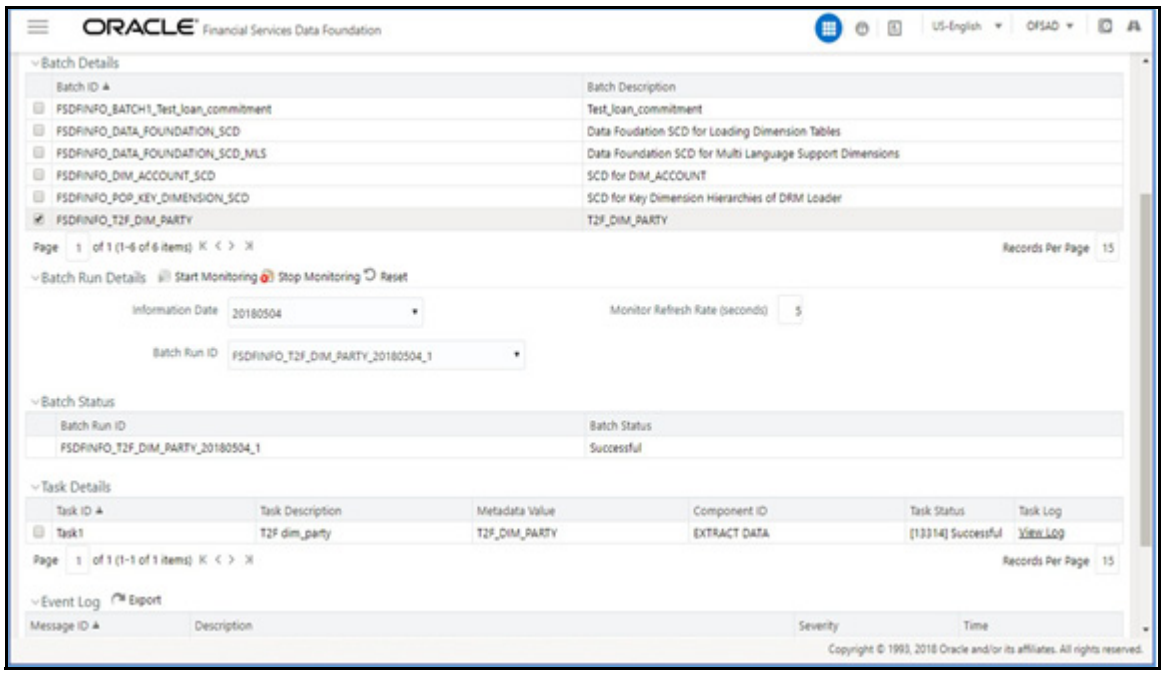
b. Create a Batch to run the T2F.



c. Create a Task for the Batch.



d. Execute the Batch. Verify the progress of batch execution in Batch Monitor.



1. The output file path is:

/scratch/ofsaaapp1/ftpshare/FSDFINFO/dmt/def/<T2F_name>/<Batch_name>/<batch_run_id>/<information_date>/<T2Fname>.dat

For example:

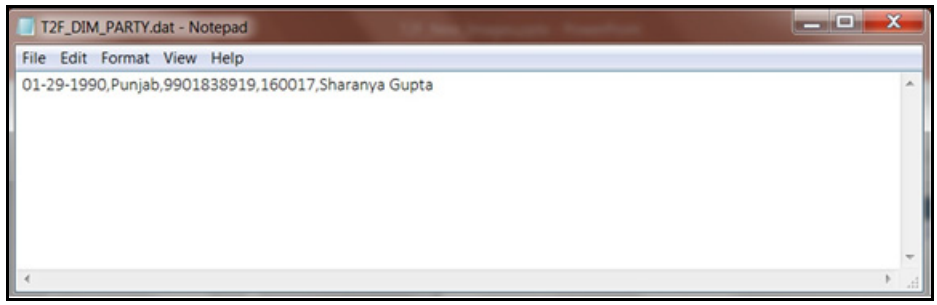
/scratch/ofsaaapp1/ftpshare/FSDFINFO/dmt/def/T2F_DIM_PARTY/FSDFINFO_T2F_DIM_PARTY_20180504_1_Task1/20180504/ T2F_DIM_PARTY.dat

---

Note: This extracted file consists of PII of a Data Subject that must be encrypted. See the Data Mapping section in Data Management Tools chapter in the OFS AAAI Application Pack Minor Release 8.0.6.0.0 User Guide.

---

2. T2F output file with the PII details requested by the Data Subject.



Pseudonymization

Overview of Pseudonymization

Pseudonymization is a process by which PII fields of a record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or one pseudonym for each replaced field. Therefore, Pseudonymization is a method to substitute PII data with a reversible and consistent value. This decreases the linking ability of a data set with the original identity of a data subject and acts as a Data Security mechanism.

The mapping of pseudonyms to those PIIs that are required for lookups, to retrieve the data subject information, must be stored away from the data warehouse in a secure location. This involves highly restricted access controls and security mechanisms that are defined at the customer environment to suit customer data security needs.

Implementation of Pseudonymization

OFSDF data model enables its customers to implement Pseudonymization process such that the PII data is separated from transaction data, and this PII data is referenced only by pseudonym. For a wide range of analytical processes, the access to PII data is not necessary.

1. Customers can employ Pseudonymization and load the Pseudonymized data into OFSDF.
2. When analytical or modeling condition requires the availability of PII data, then care must be taken by the customer to load PII data into those columns that consist of additional data security controls such as Redaction. When the requisite attributes are not part of the seeded PII list, then the customer must:
   - Extend the PII list
   - Verify the completeness of the extensions
   - Verify that Redaction is enabled on the extended PII fields prior to loading sensitive data attributes

To know more about Data Redaction, see OFS Analytical Applications Infrastructure Administration Guide.

Note: It is recommended that the PII values must not be added in the account dimension, party dimension, and customer dimension columns where redaction is not applied. For example, PII values must not be added in the v_account_number, v_party_id, and v_cust_id columns. Instead, they must be loaded in the v_original_account_number, v_orig_party_id and v_orig_cust_ref_code columns respectively, where redaction is applied.

Notice and Consent

Introduction to Notice and Consent

According to the Data Protection guidelines, a clear, legal based and accessible Notice must be provided to the Party regarding the Personally Identifiable Information (PII), which is collected from the Party during the on-boarding process or during any stage of the workflow where PII of the Data Subject is captured.

After providing a Notice, a clear Consent must be obtained from the Party regarding the usage and handling of PII by the financial institutions. This Consent must be given by the Party, and must be presented to them as their choice with the option of withdrawal from providing Consent at any time. After the Party gives their Consent, their PII can be used in the workflow.

Populating Consent Purpose Dimension Party Consent and Fact Party Consent

OFSAA is a back office product, and does not have direct interaction with the end user of the bank. Therefore, Notice, and Consent User Interfaces are not applicable. However, Data Model of Data Foundation is enhanced to hold Notice and Consent information as a download from source systems. The bank may further use this feature for the task of processing or reporting.

Procedure to Populate Consent Purpose Dimension and Fact Party Consent

This section provides information about Consent Purpose Dimension Population and Party Consent Population processes in the Oracle Financial Services Data Foundation application.

Overview of Consent Purpose Dimension Population and Fact Party Consent Population

- **Overview of Consent Purpose Dimension Population**

  In the Consent Purpose Dimension table (DIM_CONSENT_PURPOSE), Consent content is stored. This table can be populated from Stage Consent Purpose Master Entity (STG_CONSENT_PURPOSE_MASTER) using the SCD-468 packaged in FSDF.

- **Overview of Fact Party Consent Population**

  Fact Party Consent is the table where Consent of the Party is stored. Table to Table seeded definitions are provided for loading data into the target table Fact Party Consent (FCT_PARTY_CONSENT):

Source Table Name	Target Table Name	T2T Definition Name
STG_PARTY_CONSENT	FCT_PARTY_CONSENT	T2T_FCT_PARTY_CONSENT

Executing Consent Purpose Dimension Population and Fact Party Consent Population T2T

- **Executing through Batch**
  - From Consent Party Master, Consent Purpose Dimension SCD can be executed by executing task present in the SCD batch FSDFINFO_DATA_FOUNDATION_SCD.
  - Fact Party Consent T2T can be executed by executing task present in the T2T batch FSDF_SOURCED_RUN.

    Follow these steps to execute the batch:

    i. Navigate to the **Batch Execution** screen.

    ii. Select the seeded batch:

    FSDFINFO_DATA_FOUNDATION_SCD for Consent Purpose Dimension

    FSDF_SOURCED_RUN for Fact Party Consent

    where Infodom is the information domain where application is installed.

    iii. Select the AS_OF_DATE for which source customer information is required to be loaded into the table.

    iv. Click **Execute Batch**.

    Monitor the status of the batch in the screen of OFSAAI.
- **Execution of T2T Batch through Run Management**

  T2T_FCT_PARTY_CONSENT is part of Financial Services Data Foundation Sourced Run. The process can be executed through the Seeded Run Financial Services Data Foundation Execution Run.

Note: When executing through Run, the RUNSkey is auto-generated and stamped against each record.

Error Messages

In the log file present in the:

- ftpshare/logs/<Run_Date>/FSDFINFO/RUN EXECUTABLE folder for DIM_CONSENT_PURPOSE
- ftpshare/logs/<Run_Date>/FSDFINFO/LOAD DATA folder for T2T_FCT_PARTY_CONSENT

This is the most common error message:

- **Unique Constraint Violation**: This occurs when attempting re-load or loading existing records for the already executed AS_OF_DATE.

Checking the Execution Status for Fact Party Consent T2T

The status of execution can be monitored using the Batch Monitor screen.

Note: For a more comprehensive coverage of configuration and execution of a batch, see Oracle Financial Services Analytical Applications Infrastructure Release 8.0.6.0.0 User Guide.

The status messages in Batch Monitor are:

- N - Not Started
- O - On Going
- F - Failure
- S - Success

The execution log can be accessed on the application server in the directory *ftpshare/logs/<Run_Date>/FSDFINFO/LOAD DATA*. The file name consists of the Batch Execution ID.

This is the error log table in atomic schema:

- FCT_PARTY_CONSENT$ for T2T_FCT_PARTY_CONSENT

Fact Party Consent T2T

T2T definition can be retrieved as an excel document for reference from the metadata browser of the Unified Metadata Manager (UMM) component of OFSAAI.

Data Archival

Synopsis for Data Archival

The OFSAA data model, along with the active data stores Personally Identifiable Information (PII) of Data Subjects who are no longer actively using the financial services, which is a liability.

Implementation of Data Archival by OFSAA

To implement this invisibility of data at row level, Oracle Database 12c has introduced a new feature called Row Archival.

- The Row Archival feature is simple and effective to use as opposed to the traditional approach, which requires storage and maintenance of historical tables.
- This feature enables to archive records based on a given criteria within the account table. The criteria can be, for example, the Account Close Date of the Data Subject.
- This archived data can be viewed or made hidden by setting a session parameter.

A Criteria for Data Archival

To archive Party records, which are closed for more than seven years:

1. To enable Row Archival on the DIM_PARTY table, run this command:

   ```
   ALTER TABLE DIM_PARTY ROW ARCHIVAL
   ```

2. Run the Row Archival Update statement periodically, to search for the account Party records which are closed for more than seven years. Run this command:

   ```
   UPDATE DIM_PARTY SET ora_archive_state='1' where
   trunc(months_between(SYSDATE, d_closed_date)/12)>7
   ```

   In the above query:

   - `ora_archive_state` is a hidden column which is created after the ROW ARCHIVAL is set on the table.
   - SET `ora_archive_state='1'` archives the records which meets the criteria of seven years of account closure.
   - Hidden rows are available for Select/Update queries only after `ora_archive_state` is disabled.

Viewing Archived Rows

- To make hidden rows visible for a session, run this command:

  ```
  ALTER SESSION SET ROW ARCHIVAL VISIBILITY=ALL;
  ```

- To make the rows invisible, run this command:

  ```
  ALTER SESSION SET ROW ARCHIVAL VISIBILITY=ACTIVE;
  ```

Data Redaction

Overview of Data Redaction in OFSAA

Data Redaction is one of the Data Security features that provides protection of data against unauthorized access and data theft.

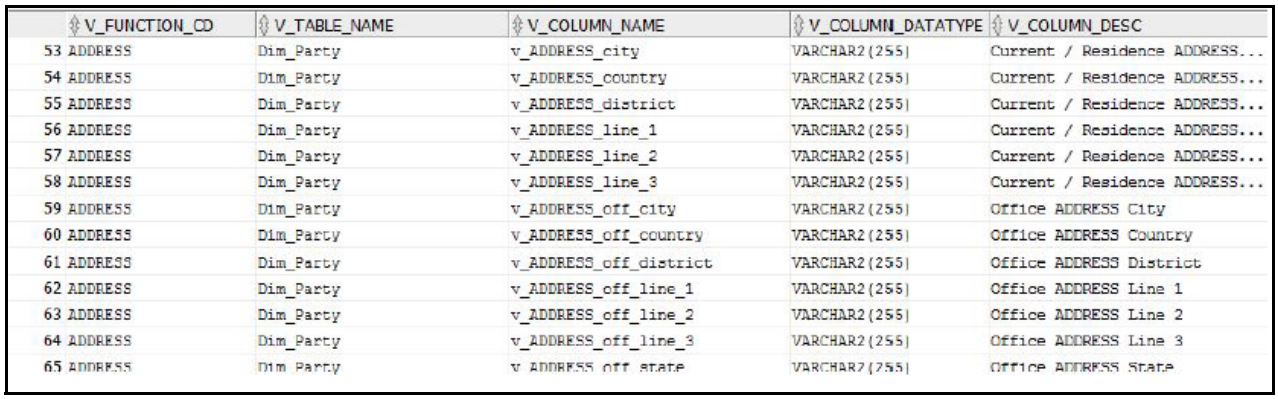
In OFSAA, these tables are seeded as part of Data Redaction:

- AAI_DRF_FUNCTION_MASTER

  This table holds the Redaction function definitions. Generic logical functions can be address, email, card number, phone number etc.

- AAI_DRF_FUNCTION_COLUMN_MAP

This table holds the Redaction Function- Column mappings. The PII columns will be redacted according to the Function mapping.



	V_FUNCTION_CD	V_TABLE_NAME	V_COLUMN_NAME	V_COLUMN_DATATYPE	V_COLUMN_DESC
53	ADDRESS	Dim_Party	v_ADDRESS_city	VARCHAR2(255)	Current / Residence ADDRESS...
54	ADDRESS	Dim_Party	v_ADDRESS_country	VARCHAR2(255)	Current / Residence ADDRESS...
55	ADDRESS	Dim_Party	v_ADDRESS_district	VARCHAR2(255)	Current / Residence ADDRESS...
56	ADDRESS	Dim_Party	v_ADDRESS_line_1	VARCHAR2(255)	Current / Residence ADDRESS...
57	ADDRESS	Dim_Party	v_ADDRESS_line_2	VARCHAR2(255)	Current / Residence ADDRESS...
58	ADDRESS	Dim_Party	v_ADDRESS_line_3	VARCHAR2(255)	Current / Residence ADDRESS...
59	ADDRESS	Dim_Party	v_ADDRESS_off_city	VARCHAR2(255)	Office ADDRESS City
60	ADDRESS	Dim_Party	v_ADDRESS_off_country	VARCHAR2(255)	Office ADDRESS Country
61	ADDRESS	Dim_Party	v_ADDRESS_off_district	VARCHAR2(255)	Office ADDRESS District
62	ADDRESS	Dim_Party	v_ADDRESS_off_line_1	VARCHAR2(255)	Office ADDRESS Line 1
63	ADDRESS	Dim_Party	v_ADDRESS_off_line_2	VARCHAR2(255)	Office ADDRESS Line 2
64	ADDRESS	Dim_Party	v_ADDRESS_off_line_3	VARCHAR2(255)	Office ADDRESS Line 3
65	ADDRESS	Dim_Party	v_ADDRESS_off_state	VARCHAR2(255)	Office ADDRESS State

- 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 will be created based on this role and evaluated to access non-redacted data.

Note: The list of PIIs, on which Data Redaction is applied, is available at My Oracle Support.

Accessing PII Table and PII Datasheet

- AAI_DRF_FUNCTION_COLUMN_MAP is the PII table.
- PII Datasheet list can be accessed from My Oracle Support.

Data Redaction Batch

Execute the Data Redaction seeded Batch `##INFODOM##_DATA_REDACTION` to execute the Data Redaction Utility if it is available as part of application common metadata. If the Batch is not available, you must create a new Batch as mentioned in the *Creating Batch for Executing Data Redaction Utility* section in the OFS Analytical Applications Infrastructure Administration Guide.

The task in the Batch `##INFODOM##_DATA_REDACTION` consists of three parameters:

- `dataredaction.sh`
- true/false
- OFSAA User ID

For more information, see *Data Redaction* section in the OFS Analytical Applications Infrastructure Administration Guide.

Mapping Roles to User Groups for Data Redaction

Data Controller Group is mapped to DATASECURITYADMIN role:

- Group Code: DATACONTROLLER
- Group Name: Data Controller Group
- Group Description: Data Controller Group
- Role code: DATASECURITYADMIN
- Role Name: Data Security Admin
- Role Description: Data security admin role for executing redaction policies

Mapping from individual applications to DATASECURITY role:

- Role code: DATASECURITY
- Role Name: Data Security Viewer
- Role Description: Data Security Viewer role for viewing original (non-redacted) data.
  a. DATASECURITY role must be mapped to those application User Groups which have the privilege to view the data in its originality (un-redacted). Therefore, applications must identify the functions which must be mapped to the DATASECURITY role. These mappings must come as seeded data.
  b. And then, map DATASECURITY role to the respective User groups. This mapping must be done manually from individual applications to the DATASECURITY role.

Data Redaction Batch Execution Sample

- Data before executing Data Redaction Batch:

Row 1	Fields
N_ACCT_SKEY	6
V_ACCOUNT_NUMBER	BC1007
V_ACCOUNT_DESC	data redaction desc
V_ACCOUNT_MANAGER_CODE	drmc1
V_ORIGINAL_ACCOUNT_NUMBER	data redaction original account numb

- Data after executing Data Redaction Batch:

Row 1	Fields
N_ACCT_SKEY	6
V_ACCOUNT_NUMBER	BC1007
V_ACCOUNT_DESC	
V_ACCOUNT_MANAGER_CODE	
V_ORIGINAL_ACCOUNT_NUMBER	