

Oracle Financial Services
Behavior Detection
Installation Guide
Release 8.1.2.0.0
September 2023
F82834-01

ORACLE®
Financial Services

OFS Behavior Detection Installation Guide

Copyright © 2015, 2023, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information on third party licenses, click [here](#).

Document Control

Table 1 lists the document control.

Table 1: Revision History

Revision Number	Revision Date	Change Log
3.0	September 2023	The following sections are created/updated: <ul style="list-style-type: none">• Update WebLogic Server• Create Domain in WebLogic Server for Java option entry to disable HTTP2.
2.0	June 2023	The following sections are updated in this iteration: <ul style="list-style-type: none">• In-Place Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0• Cloning Upgrades of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0• OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0• OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0• In-Place Upgrade of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0• Cloning Upgrades of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0• OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0• OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0
1.0	March 2022	The following sections are updated in this release: <ul style="list-style-type: none">• Hardware and Software Requirements• Preparing for Installation• Upgrading OFSBD Application Pack Installation• Configuring FSDF in Different Infodomain (Pack on Pack Installation)• Deploying Analytic Reports and Threshold Analyzer The following section is added in this release: <ul style="list-style-type: none">• How to enable newly licensed App after upgrade to BD 8.1.2.0.0.

Table of Contents

1	Preface	12
1.1	Summary.....	12
1.2	Audience	12
1.2.1	<i>Prerequisites for the Audience</i>	<i>12</i>
1.3	Related Documents.....	12
1.3.1	<i>OFSAAI Related Documents</i>	<i>13</i>
1.3.2	<i>OFS BD Application Related Documents</i>	<i>13</i>
1.4	Conventions	14
1.5	Abbreviations	15
2	About OFSAA and OFSAA Application Packs.....	16
2.1	About OFSAA	16
2.2	Introduction to OFS BD Application	17
2.3	About OFSAA Infrastructure.....	18
2.3.1	<i>Components of OFSAAI</i>	<i>18</i>
2.3.2	<i>OFSAA Infrastructure High Availability</i>	<i>19</i>
2.4	About Data Security Configurations	19
3	Understanding OFS BD Application Pack Installation.....	1
3.1	Installation Overview	1
3.2	Deployment Topology	2
3.3	Hardware and Software Requirements	3
3.3.1	<i>Configurations Supported for Java 8 & 11</i>	<i>3</i>
3.4	Verifying System Environment	5
3.5	Understanding the Installation Mode	5
3.5.1	<i>Installing in Silent Mode</i>	<i>5</i>
4	Preparing for Installation	6
4.1	Installer and Installation Prerequisites.....	6
4.2	Obtaining Software	10
4.3	Performing Common Pre-Installation Tasks.....	10
4.3.1	<i>Identifying the Installation, Download and Metadata Repository</i>	<i>10</i>
4.3.2	<i>Downloading and Copying the OFS BD Application Pack Installer</i>	<i>10</i>

4.3.3	<i>Extracting the Software</i>	11
4.3.4	<i>Setting Up Web Application Server</i>	11
5	Installing OFS BD Application Pack.....	12
5.1	Configuring Wallet	12
5.2	About Schema Creator Utility	12
5.2.1	<i>Configuring Schema Creator Utility for RDBMS</i>	13
5.2.2	<i>Configuring Schema Creator Utility for HDFS Schema</i>	13
5.2.3	<i>Selecting Execution Modes in Schema Creator Utility</i>	14
5.2.4	<i>Selecting Execution Options in Schema Creator Utility</i>	15
5.3	Configuring and Executing Schema Creator Utility	15
5.3.1	<i>Prerequisites</i>	15
5.3.2	<i>Configuring Schema Creator Utility</i>	15
5.3.3	<i>Executing the Schema Creator Utility</i>	16
5.3.4	<i>Verifying the Schema Creator Log Files</i>	26
5.4	Installing the OFS BD Application Pack	26
5.4.1	<i>Installing in Silent Mode</i>	26
5.4.2	<i>Enabling Newly Licensed App for Standalone OFS BD 8.1.2.0.0</i>	36
5.5	Verifying Installation.....	36
6	Upgrading the OFS BD Applications Pack	37
6.1	Upgrading from OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0	37
6.1.1	<i>Standalone Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0</i>	37
6.1.2	<i>In-Place Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0</i>	38
6.1.3	<i>Cloning Upgrades of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0</i>	44
6.1.4	<i>Pack on Pack Inplace Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0</i>	51
6.1.5	<i>Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0</i>	59
6.2	Upgrading from OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0	66
6.2.1	<i>Standalone Upgrade of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0</i>	66
6.2.2	<i>Cloning Upgrades of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0</i>	74
6.2.3	<i>Pack on Pack Inplace Upgrade from OFS BD 8.1.1.1.0, OFS ECM 8.1.1.1.0 and OFS CRR 8.1.1.1.0 to OFS BD</i>	

8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0	80
6.2.4 Pack on Pack Cloning Upgrade from OFS BD 8.1.1.1.0, OFS ECM 8.1.1.1.0 OFS CRR 8.1.1.1.0 to OFS BD	
8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0	88
6.3 How to Enable Newly Licensed App after Upgrade to BD 8.1.2.0.0.....	96
7 Post Installation Configuration	97
7.1 Creating and Deploying the Applications Pack Web Archive	98
7.1.1 OFSBD Application Pack Deployment	98
7.1.2 Scenario Wizard Configuration and Deployment	98
7.1.3 Services Configuration and Deployment	101
7.2 KYC Onboarding Services Deployment.....	103
7.2.1 Updating User ID and Passwords for KYC Onboarding Services in PMF	105
7.3 Installing Scenario Manager	106
7.3.1 Verifying the Pre-installation Requirements	106
7.3.2 Installing the Scenario Manager on Workstation	109
7.4 Copying KEYTAB and KRB5 Files in OFSAAI.....	111
7.5 Deploying Analytic Reports and Threshold Analyzer.....	111
7.5.1 Installing Oracle Analytic Server (OAS) 5.9	112
7.5.2 Installing ORACLE ANALYTIC SERVER (OAS) 5.9 Windows Administration Client	112
7.5.3 Disabling the Cache Feature in Oracle Analytic Server (OAS) 5.9	113
7.5.4 Change Default Repository Password	114
7.5.5 Configuring ORACLE ANALYTIC SERVER (OAS) 5.9 Connection Pool	114
7.5.6 Deploying OFS FCCM Report Analytics	115
7.5.7 Configuring TreeMap Graph	117
7.5.8 Disable Single Sign On	117
7.5.9 Enabling Table Authentication feature in OAS 5.9	117
7.6 Post Installation Steps.....	118
7.7 Accessing Reports through OFS BD Application.....	118
7.8 Installing RAOR Service.....	118
7.9 Creating RAOR.ear/ RAOR.war	119
7.10 Deploying RAOR.ear in WebLogic	120
7.11 Installing RAOR.ear in WebLogic using WebLogic Administrator Console	121

7.12	Deploying RAOR.ear in WebSphere	124
7.13	Deploying RAOR.war in Tomcat.....	131
7.14	Configuring Resource Reference.....	132
7.15	Configuring Web Application Server.....	133
7.16	Configurations for Java 8	133
7.17	Enabling Unlimited Cryptographic Policy for Java	133
7.18	Configurations for Oracle 19c Database.....	134
7.19	Configuring FSDF	135
7.19.1	Configuring CSA Staging Tables	135
7.19.2	Configuring FSDF in Different Infodomain (Pack on Pack Installation)	135
7.20	Configurations for ECM Integration (Applicable only for Promote to Case Action in KYC	138
7.20.1	ECM and BD Installed in Different Databases	138
7.20.2	ECM and BD Installed in the Same Database	139
8	Post Deployment Configuration.....	141
8.1	Creating Application Users.....	141
8.2	Mapping Application User(s) to User Group	141
8.3	Performing Administrative activities for OFS BD	142
8.4	Performing Configurations for OFS BD.....	143
8.5	Setting OFS BD UI as Home Page of OFSAAI for a Particular User	143
8.6	Modifying Additional Configuration Files.....	143
8.7	Changing ICC Batch Ownership	144
9	Appendix A: Configure the Web Server	145
9.1	Configuring Web Server.....	145
9.2	Configuring Web Application Servers.....	145
9.2.1	Configure WebSphere Application Server for Application Deployment	146
9.2.2	Configuring WebSphere before Application Deployments	146
9.2.3	Create a New Profile in WebSphere	147
9.2.4	Manage IBM WebSphere SDK Java Technology Edition Versions	147
9.2.5	Manage Applications in WebSphere	148
9.2.6	Configure Websphere Application Server to Initialize Filters before Initializing Load-On-Startup Servlets and Allowing Empty Servlets Maps	149

9.2.7	Configure WebSphere Application Server Persistence to JPA Specification 2.0	150
9.2.8	Configure Websphere Application Server to Use a Load Balance or Proxy Server	150
9.2.9	Delete WebSphere Profiles	151
9.2.10	Configuring WebSphere Shared Library to Support Jersey 2x and Jackson 2.9x Libraries	151
9.2.11	Configure WebSphere HTTPS	152
9.2.12	Configure WebSphere Memory Settings	152
9.2.13	Configure WebSphere for REST Services Authorization	152
9.2.14	Configuring Application Security in WebSphere	152
9.3	Configure WebLogic for Application Deployment	152
9.3.1	Update WebLogic Server	153
9.3.2	Create Domain in WebLogic Server	153
9.3.3	Delete Domain in WebLogic	159
9.3.4	Configure WebLogic Memory Settings	160
9.3.5	Configuring WebLogic for REST Services Authorization	160
9.4	Configure Apache Tomcat Server for Application Deployment	160
9.4.1	Tomcat User Administration	161
9.4.2	Configuring Tomcat to use JAVA 64 bit Executables	161
9.4.3	Configure Servlet Port	162
9.4.4 Configure SSL Port	162
9.4.5	Configure Apache Tomcat Memory Settings	162
9.4.6	Configuring Axis API	163
9.4.7	Configure Tomcat for User Group Authorization and Data Mapping	163
9.4.8	Uninstall WAR Files in Tomcat	163
10	Appendix B: Configure Resource Reference in Web Servers.....	164
10.1	Configure Resource Reference in WebSphere Application Server	164
10.1.1	Create a JDBC Provider	164
10.1.2	Create Data Source	166
10.1.3	Create J2C Authentication Details	169
10.1.4	Define JDBC Connection Pooling	171
10.2	Configure Resource Reference in WebLogic Application Server	171
10.2.1	Create Data Source	172

10.2.2	Create GridLink Data Source	176
10.2.3	Configure Multi-data Sources	177
10.2.4	Configure Advanced Settings for Data Source	180
10.2.5	Configure JDBC Connection Pooling	180
10.2.6	Create Workmanager	181
10.3	Configure Resource Reference in Tomcat Application Server	182
10.3.1	Create Data Source	182
10.3.2	Define JDBC Connection Pooling	183
10.3.3	Configure ClassLoader for Apache Tomcat	184
11	Appendix C: Configure Work Manager in Web Application Servers.....	185
11.1	Configure Work Manager in WebSphere Application Server	185
11.1.1	Create Work Manager	185
11.1.2	Map Work Manager to OFSAA WebSphere Instance	187
11.2	Configure Work Manager in WebLogic Application Server	191
12	Appendix D: Creating and Deploying EAR/WAR File	194
12.1	Creating EAR/WAR File.....	194
12.2	Deploying EAR/WAR File.....	195
12.2.1	Deploying EAR/WAR Files on WebSphere	195
12.2.2	Start the Application	202
12.2.3	Deploying EAR/WAR files for WebLogic	202
12.2.4	Deploying Tomcat WAR Files on Tomcat	208
13	Appendix E: Starting/Stopping Infrastructure Services.....	211
13.1	Starting Infrastructure Services.....	211
13.2	Starting Web Application Servers	212
13.3	Stopping Infrastructure Services	212
13.4	Cleaning up the environment.....	212
14	Appendix F: Accessing OFSAA Application.....	214
15	Appendix G: Cloning OFSAA Instance.....	215
16	Appendix H: OFSAA Landing Page.....	216
16.1	OFSAA Landing Page.....	216
16.1.1	Applications Tab	216

16.1.2	<i>Sandbox Tab</i>	216
16.1.3	<i>Object Administration Tab</i>	216
16.1.4	<i>System Configuration and Identity Management Tab</i>	217
16.2	Enabling Product within Applications Pack	217
17	Appendix I: Additional Configuration	220
17.1	Configuring FTP/SFTP	220
17.1.1	<i>Adding FTP/SFTP Configuration for File Transfer</i>	220
17.1.2	<i>Setting Up SFTP Private Key</i>	221
17.2	Configuring Infrastructure Server Memory	221
17.3	Configuring Internet Explorer Settings	222
17.4	Retrieving Patch Information	224
17.5	Setting OLAP Data Server Configuration	225
17.6	Changing IP/Hostname, Ports, Deployed Paths of the OFSAA Instance	225
17.7	Executing OFSAAI Setup Information Fetching Tool	225
17.8	Executing Encryption Changer	225
17.9	Setting Infrastructure LDAP Configuration	225
17.10	Enabling Parallel Execution of DML Statements	225
17.11	Configure Message Details in Forms Designer	226
17.12	Clearing Application Cache	227
17.13	Configuring Password Changes	227
17.13.1	<i>Modifying OFSAA Infrastructure Config Schema password</i>	227
17.13.2	<i>Modifying OFSAA Infrastructure Atomic Schema Password</i>	227
17.13.3	<i>Configuring Internal Service (Document Upload/Download)</i>	228
18	Appendix J: OFSAA Infrastructure Installation	229
19	Appendix K: Grants for Atomic/Config Schema	230
19.1	Configuring Grants for Atomic Schema	230
19.2	Configuring Grants for Config Schema	230
19.3	Configuring Grants for Config Schema Entities for Atomic Users	231
20	Appendix L: Configuring Application Pack XML Files	232
20.1	Configuring OFS_BD_PACK.xml File	232
20.2	Configuring OFS_BD_SCHEMA_IN.xml File	233

21	Appendix M: Configuring OFSAAI_InstallConfig.xml File	244
22	Appendix N: Migrating for Excel Upload Functionality	249
22.1	Prerequisites.....	249
22.2	Migrating Excel Upload.....	249
23	Appendix O: JDBC Jar Files	251
24	Appendix P: Upgrading an Existing OFSAA 8.0.x JAVA 7 Instance to Java 8.....	252
24.1	Prerequisites.....	252
24.2	Upgrading OFSAA 8.0.x Java 7 Instance to Java 8.....	252
24.3	Configuring Web Application Server.....	252
24.3.1	Upgrading Oracle WebLogic Server	253
24.3.2	Upgrading Apache Tomcat Server	253
24.4	Configuring User .profile Settings	254
24.5	Configuring OFSAA for New Web Application Server Installation.....	254
25	Appendix Q: Removing OFSAA.....	255
25.1	Uninstalling OFSAA Infrastructure	255
25.2	Uninstalling EAR Files in WebSphere.....	256
25.3	Uninstalling EAR Files in WebLogic.....	256
25.4	Uninstalling WAR Files in Tomcat.....	257
26	Appendix R: Configuring TDE and Data Redaction in OFSAA	259
26.1	Transparent Data Encryption (TDE).....	259
26.1.1	Configuring TDE During Behavior Detection Installation Using Full Installer	259
26.1.2	Configuring TDE in Case of Upgrade	266
26.2	Data Redaction.....	267
26.2.1	Enabling Data Redaction in case of Upgrade	267
27	Appendix S: Tunable Database Parameters	269
28	Appendix T: FAQs and Error Dictionary.....	274
28.1	Frequently Asked Questions.....	274
28.1.1	OFSAAI FAQs	274
28.1.2	Applications Pack 8.1.2.0.0 FAQs	290
28.1.3	Forms Framework FAQs	294
28.2	Error Dictionary	296

28.2.1	<i>Accessing Error Dictionary</i>	296
28.2.2	<i>Error Code Dictionary</i>	296
29	Appendix U : OFS BD Version Compatibility List	299
30	OFSA Support Contact Details	300
31	Send Us Your Comments.....	301

1 Preface

This section provides supporting information for the Oracle Financial Services Behavior Detection Application Pack (OFS BD) Installation Guide.

Topics:

- [Summary](#)
- [Audience](#)
- [Related Documents](#)
- [Conventions](#)
- [Abbreviations](#)

1.1 Summary

You can find the latest copy of this document in [OHC Library](#) which includes all the recent additions/revisions (if any) done to date. Before you begin the installation, ensure that you have access to the Oracle Support Services Portal with the required login credentials to quickly notify us of any issues at any stage. You can obtain the login credentials by contacting [Oracle Support Services](#).

1.2 Audience

This guide is intended for administrators and implementation consultants who are responsible for installing and maintaining the Application Pack components.

1.2.1 Prerequisites for the Audience

The following are the prerequisites for the administrators installing Oracle Financial Services Behavior Detection Application (OFS BD) Pack. This document assumes that you have experience in installing Enterprise components and basic knowledge about the following:

- OFS BD pack components
- Oracle Financial Services Analytical Application (OFSAA) Architecture
- UNIX Commands
- Database Concepts
- Web Server/Web Application Server

1.3 Related Documents

This section identifies additional documents related to Oracle Financial Services Behavior Detection (OFS BD).

Topics:

- [OFSAAI Related Documents](#)
- [OFS BD Application Related Documents](#)

1.3.1 OFSAAI Related Documents

The following documents are available in [OHC](#).

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

1.3.2 OFS BD Application Related Documents

The following documents are available in [OHC](#):

- Oracle Financial Services Behavior Detection Administration Guide
- Oracle Financial Services Scenario Manager User Guide
- Oracle Financial Services Behavior Detection Configuration Guide
- Oracle Financial Services Know Your Customer Administration Guide
- Oracle Financial Services Foreign Account Tax Compliance Act Administration and Configuration Guide
- Oracle Financial Services Currency Transaction Reporting Administration Guide
- Oracle Financial Services Scenario Wizard Configuration Guide
- Oracle Financial Services Know Your Customer Risk Assessment Guide
- Oracle Financial Services Administration Tools User Guide
- Oracle Financial Services Administration Guide
- Oracle Financial Services Alert Management User Guide
- Oracle Financial Services Common Reporting Standard User Guide
- Oracle Financial Services Common Reporting Standard Administration Configuration Guide
- Oracle Financial Services Behavior Detection Release Notes

The following documents are available in My Oracle Support (MOS). You must have SSO credentials to access MOS.

- Oracle Financial Services Analytical Applications Infrastructure Security Guide
- Oracle Financial Services Common Reporting Standard Data Model Reference Guide
- Oracle Financial Services Know Your Customer Data Model Reference Guide
- Financial Services Data Model Reference Guide Volume 1: Business Data
- Financial Services Data Model Reference Guide Volume 2: Oracle Financial Services Data
- Financial Services Data Model Reference Guide Volume 3: Case Management Data
- Data Interface Specification
- Oracle Financial Services Anti-Money Laundering Technical Scenario Description
- Oracle Financial Services Fraud Technical Scenario Description

1.4 Conventions

Table 1 lists the conventions used in this document

Table 1: Convention Used in this Guide

Conventions	Meaning
<i>Italics</i>	<ul style="list-style-type: none">Names of books as referencesEmphasisSubstitute input values
Bold	<ul style="list-style-type: none">Menu names, field names, options, button namesCommands typed at a promptUser input
Monospace	<ul style="list-style-type: none">Directories and subdirectoriesFile names and extensionsProcess namesCode sample, including keywords and variables within the text and as separate paragraphs, and user-defined program elements within the text
Hyperlink	<ul style="list-style-type: none">Hyperlink type indicates links to the external websites and internal document links to sections
Asterisk (*)	<ul style="list-style-type: none">Mandatory fields in User Interface
<Variable>	<ul style="list-style-type: none">Substitute input value

1.5 Abbreviations

Table 2 lists the abbreviations used in this guide.

Table 2: Abbreviations used in this guide

Abbreviation	Meaning
BD	Behavior Detection
FSDf	Financial Services Data Foundation
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
J2C	J2EE Connector
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
LHS	Left Hand Side
MOS	My Oracle Support
OFsAA	Oracle Financial Services Analytical Application
OFsAAI	Oracle Financial Services Analytical Application Infrastructure
OLAP	On-Line Analytical Processing
OS	Operating System
SFTP	Secure File Transfer Protocol
URL	Uniform Resource Locator
WAR	Web Archive
XML	Extensible Markup Language

2 About OFSAA and OFSAA Application Packs

This chapter provides details about the Oracle Financial Services Analytical Application (OFSAA) and its Application Packs.

Topics:

- [About OFSAA](#)
- [Introduction to OFS BD Application](#)
- [About OFSAA Infrastructure](#)
- [About Data Security Configurations](#)

2.1 About 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.

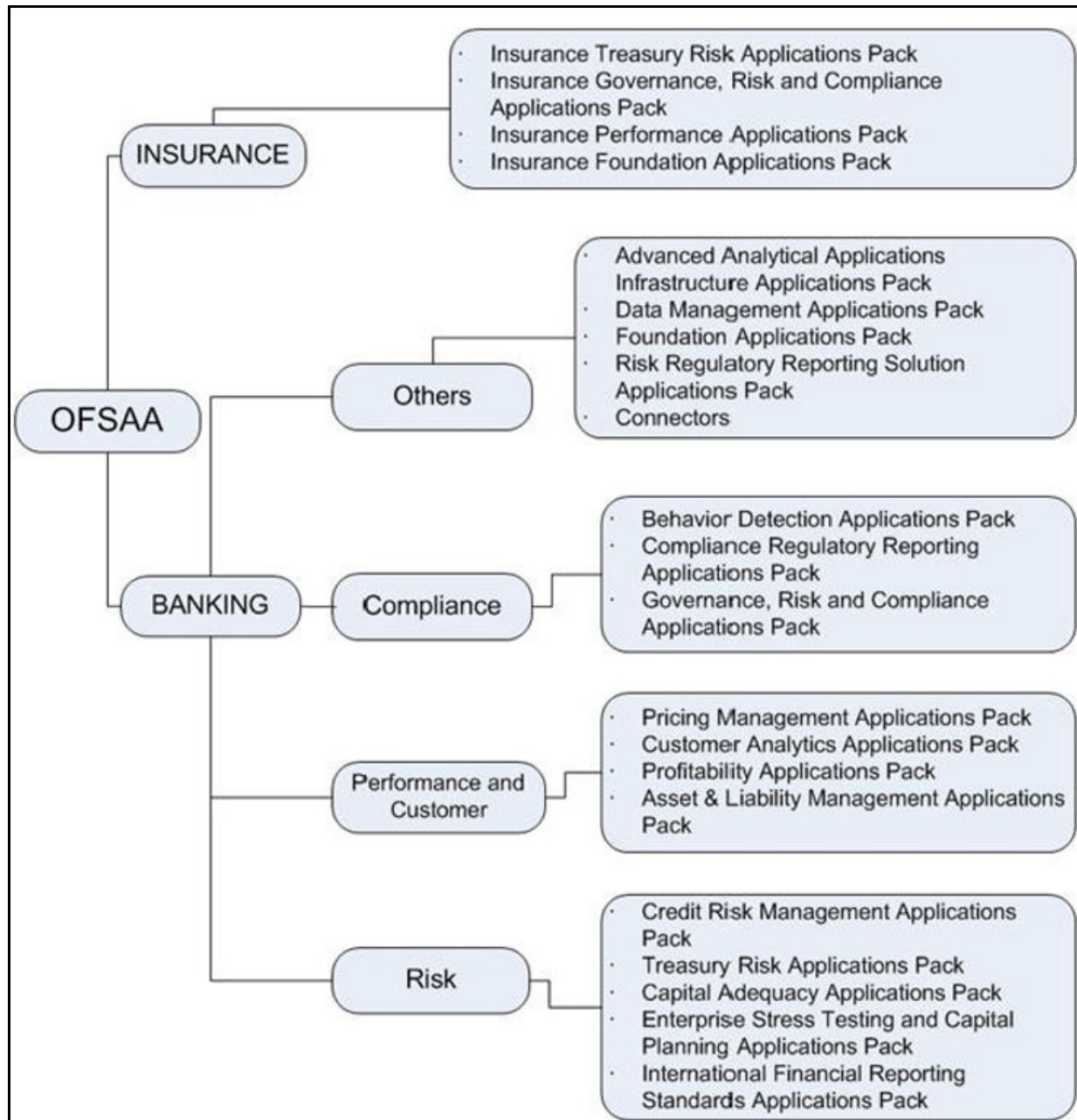
OFSAA uses industry-leading analytical methods, shared data model, and applications architecture to enable integrated risk management, performance management, customer insight, and compliance management. OFSAA actively incorporates risk into decision-making, enables to achieve a consistent view of performance,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

With the help of OFSAA, the financial services organizations can achieve, management excellence with a lower total cost of ownership, due to our integrated, architecture, combining performance and risk applications into a single, seamlessly integrated framework.

OFSAA delivers a comprehensive and integrated suite of financial services analytical applications for both the banking and insurance domain.

Figure 1 depicts the various Applications Packs that are available across the OFSAA Banking and Insurance domains:

Figure 1: OFSAA Applications Packs



2.2 Introduction to OFS BD Application

The OFS BD Application Pack includes the following applications:

- Oracle Financial Services Analytical Applications Infrastructure (OFS AAI)
- Oracle Financial Services Anti-Money Laundering Enterprise Edition (OFS AML)
- Oracle Financial Services Fraud Enterprise Edition
- Oracle Financial Services Know Your Customer (OFS KYC)

- Oracle Financial Services Currency Transaction Reporting (OFS CTR)

NOTE

For AML and Fraud alerts, the Event Correlation module in Enterprise Case Management (ECM) must be used to correlate events from the FCCM Behavior Detection engine or those ingested from external applications. AM can be used as read-only for viewing historical alerts but it is not to be used for investigating alerts, taking action on alerts, editing alerts and/or promoting alerts to a case. The manual Promote to Case functionality is no longer supported. Customers are to use ECM for reviewing and investigating alerts. A restricted use license of ECM is provided with the BDF license, which replicates the functionality available in AM to the best that is currently available within ECM. Implementations must use event correlation to move Alerts from BDF into ECM and then use alert correlation/promote to a case where all levels of investigation can occur. If this updated process is not clear to your implementation team, it is advised that you contact Oracle Partner Network or Oracle Consulting to be trained.

2.3 About OFSAA Infrastructure

Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) powers the Oracle Financial Services Analytical Applications family of products to perform the processing, categorizing, selection, and manipulation of data and information required 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.

Topics:

- [Components of OFSAAI](#)
- [OFSAA Infrastructure High Availability](#)

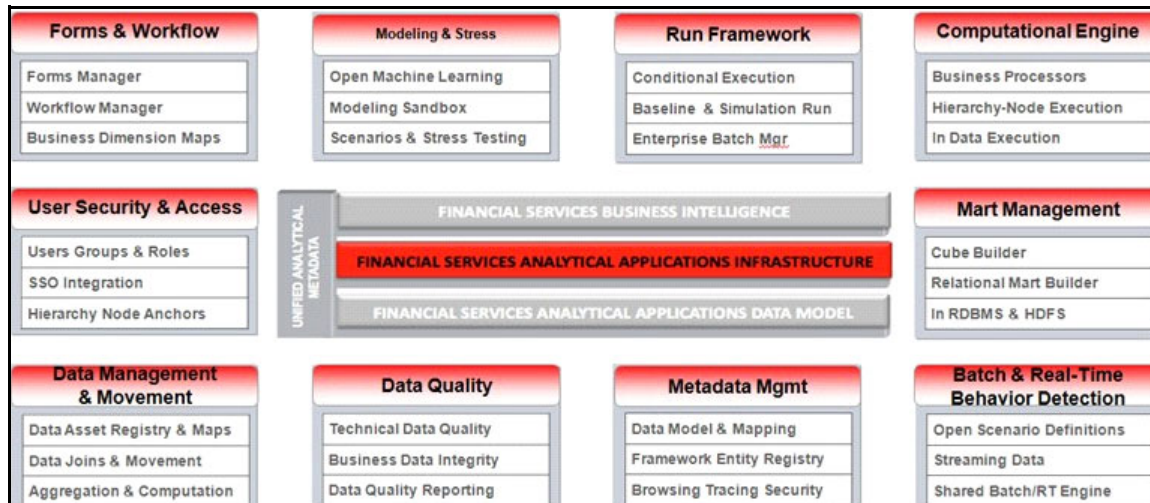
2.3.1 Components of OFSAAI

The OFSAA Infrastructure includes frameworks that operate 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 as 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 [Figure 2](#) depicts the various frameworks and capabilities that make up the OFSAA Infrastructure:

Figure 2: Components of OFSAAI



2.3.2 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 is supported in this release.

This release supports the Active-Passive model of implementation for OFSAAI components.

For more information, see [Oracle Financial Services Analytical Applications Configuration for High Availability- Best Practices Guide](#).

2.4 About Data Security Configurations

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 (MFA)
- Transparent Data Encryption (TDE)
- Data Redaction
- Key Management
- HTTPS
- Logging

For more details on the features in the previous list, see [OFS Analytical Applications Infrastructure Administration Guide](#).

3 Understanding OFS BD Application Pack Installation

Topics:

- [Installation Overview](#)
- [Deployment Topology](#)
- [Hardware and Software Requirements](#)
- [Verifying System Environment](#)
- [Understanding the Installation Mode](#)

3.1 Installation Overview

This release (8.1.2.0.0) of the OFS BD Applications Pack bundles the upgrade patch set along with the base installer. Users/Administrators who wish to install a new OFS BD Applications Pack 8.1.2.0.0 instance or upgrade an existing OFS BD Applications Pack 8.0.x instance to 8.1.2.0.0 must download this installer.

Figure 3 shows the order of procedures required to follow to install a new OFS BD Applications Pack 8.1.2.0.0 instance.

To upgrade an existing OFS BD Applications Pack 8.0.x.x.x instance to 8.1.2.0.0 release, see [Upgrading the OFS BD Applications Pack](#).

Figure 3: Installation Overview

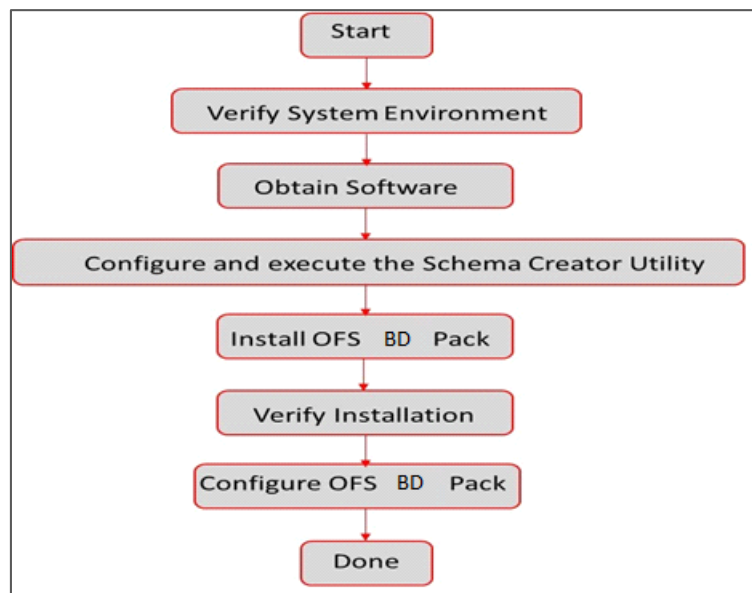


Figure 3 provides additional information and links to specific documentation for each task in the flowchart.

Table 3 shows the OFS BD Application Pack Installation Tasks and Descriptions.

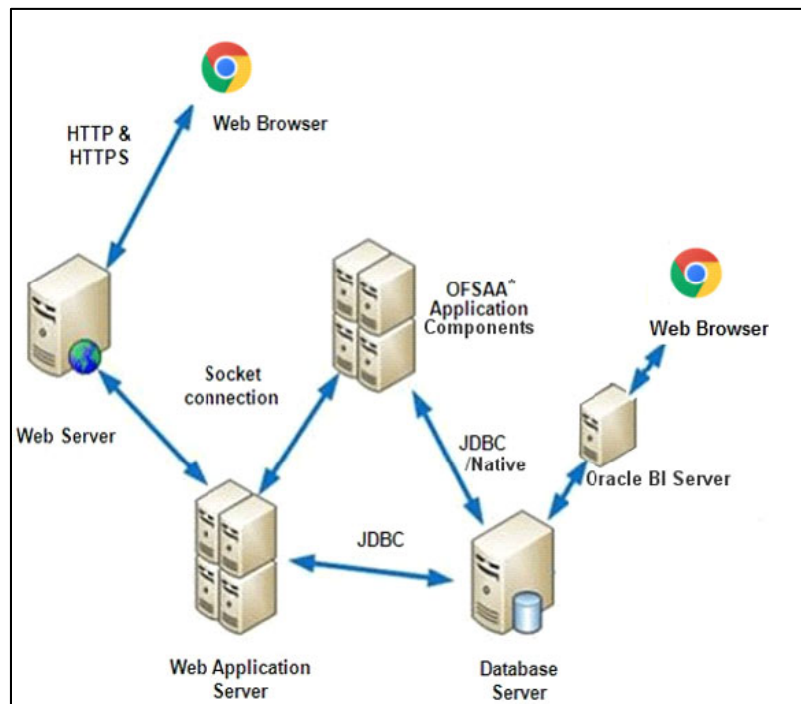
Table 3: OFS BD Application Pack Installation Tasks and Descriptions

Tasks	Details and Documentation
Verify Systems Environment	To verify that your system meets the minimum necessary requirements for installing and hosting the OFS BD Application Pack, see Verifying System Environment .
Obtain the software	To access and download the OFS BD Application Pack, see Obtaining Software .
Configure and Execute the Schema Creator Utility	To create the database schema, see Configuring and Executing Schema Creator Utility .
Install OFS BD Pack	To install the OFS BD Application Pack, see Installing OFS BD Application Pack .
Configure OFS BD Pack after installation	To configure the OFS BD Application Pack post installation, see Post Installation Configuration .

3.2 Deployment Topology

Figure 4 shows the logical architecture implemented for OFS BD Application Pack.

Figure 4: Deployment Topology



3.3 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 OFS BD Application Pack has been qualified.

NOTE

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

The following tables show the minimum hardware and software requirements for installing OFS BD Application Pack.

3.3.1 Configurations Supported for Java 8 & 11

For more information, see [Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix](#).

Table 4 shows the supported configurations for Java 8 & 11.

Table 4: Configurations Supported for Java 8 & 11

Operating System	
Oracle Linux / Red Hat Enterprise Linux (x86-64)	Oracle Linux Server release 7 update level 6+ - 64 bit Oracle Linux Server release 8 - 64 bit Note: Same version of RHEL is supported
Oracle Solaris (SPARC)	11.3+ - 64 bit
Shell	KORN Shell (KSH)
Note: If the operating system is RHEL, install the package lsb_release with one of the following commands by logging in as root user: <pre>yum install redhat-lsb-core</pre> <pre>yum install redhat-lsb</pre>	
Java Runtime Environment	
Oracle Java Runtime Environment (JRE) 1.8.x - 64 bit Oracle JDK Standard Edition 11.0.x	
Oracle Database Server and Client	
Oracle Database Server Client 19.3+ Oracle Database Server Enterprise Edition 19.3+ - 64 bit RAC/ Non-RAC with/ without partitioning option	
OLAP	
Oracle Hyperion Essbase 11.1.2.4+	
Web server/ Web application server	

Table 4: Configurations Supported for Java 8 & 11

Oracle Linux / Red Hat Enterprise Linux/ IBM Solaris	<ul style="list-style-type: none"> • Oracle HTTP Server 11.1.1.9+ / Apache HTTP Server 2.4.x/ IBM HTTP Server 9.0.0.x. • Oracle WebLogic Server 12.2.x and 14.1.x - 64 bit • IBM WebSphere Application Server 9.0.0.x with bundled IBM Java Runtime - 64 bit • Apache Tomcat v9.0.45+ - 64 bit
<p>Note: OFSAA Infrastructure web component deployment on Oracle WebLogic Server with Oracle JRockit is not supported. For deployment on Oracle WebLogic Server (64 bit) with Java 8/Java 11, download from My Oracle Support. Apache Tomcat Support is only for batch applications. For more information, see Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix.</p>	
Desktop Requirements	
Operating System	Windows 10
Browser	<ul style="list-style-type: none"> • Chrome Version 90.0.4430.212 • Firefox Version 78.10.1esr • Microsoft Edge Version 90.0.818.62 <p>Turn off Pop-up blocker settings. For more information, see Configuring Internet Explorer Settings.</p>
Office Tools	<ul style="list-style-type: none"> • MS Office 2013/2016 • Adobe Acrobat Reader 8 or above
Screen Resolution	Minimum screen resolution & Scaling must be "1366 * 768 with 100% scaling.
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.
<p>Note: Configuration of Directory services software for OFSAAI installation is optional. For more information on configuration, see Setting Infrastructure LDAP Configuration. Open LDAP must be installed on MS Windows Server machine.</p>	

[Table 5](#) provides the recommended software combinations for OFS BD Applications Pack deployment and Recommended Software Combinations.

Table 5: Recommended Software Combinations

Operating System	Database	Web Application Server	Web Server
Oracle Linux 7.x and above	Oracle Database	Oracle WebLogic Server /Apache Tomcat Server	Oracle HTTP Server/ Apache HTTP Server

Table 5: Recommended Software Combinations

Operating System	Database	Web Application Server	Web Server
Oracle Solaris 11.2 and above	Oracle Database	Oracle WebLogic Server /Apache Tomcat Server	Oracle HTTP Server/ Apache HTTP Server

3.4 Verifying System Environment

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

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* in the [Related Documents](#) section.

3.5 Understanding the Installation Mode

Installing in Silent Mode is available for the OFS BD Application Pack.

3.5.1 Installing in Silent Mode

This mode mandates updating the installation configuration files with required details and performs installation in a *Silent* non-user interactive format.

NOTE

Graphical User Interface (GUI) mode of installation is not supported for this release.

To verify the type of installation, you must know this mode mandates updating the installation configuration files with required details and performs installation in a *Silent* non-user interactive format.

4 Preparing for Installation

This chapter provides necessary information to review before installing the Oracle Financial Services Behavior Detection (OFS BD) Application Pack v8.1.2.0.0.

Topics:

- [Installer and Installation Prerequisites](#)
- [Obtaining Software](#)
- [Performing Common Pre-Installation Tasks](#)

4.1 Installer and Installation Prerequisites

[Table 6](#) provides the list of prerequisites required before beginning the installation for OFS BD application. If requirements are not met, the Environment Check utility will notify you.

Table 6: Prerequisite Information

Category	Sub_Category	Expected Value
Environment Settings	User Permission	<p>User to have 755 permission on the directory identified for installation (FIC_HOME).</p> <p>Note:</p> <p>User to have 755 permission on the .profile file.</p> <p>Provide BDF_HOME in .profile pointing to Installation Directory (FIC_HOME)</p>
	Java Settings	<ul style="list-style-type: none"> • The path in the .profile file must be set to include the Java Runtime Environment absolute path. The path must include Java version 8 based on the configuration. • Set the Java tool options in the .profile file for all JDK 11.0.20 and later updates. <p>For example:</p> <pre>JAVA_TOOL_OPTIONS="Djdk.util.zip.disableZip64ExtraFieldValidation=true" export JAVA_TOOL_OPTIONS</pre> <p>Note:</p> <p>Ensure that the absolute path to JRE/bin is set at the beginning of PATH variable.</p> <p>For example, PATH=/usr/java/jre1.7/bin:\$ORACLE_HOME/bin:\$PATH</p> <p>Ensure that no SYMBOLIC links to JAVA installation are not set in the PATH variable</p>
	Enable unlimited cryptographic policy for Java	<p>For more information, see the section Enabling Unlimited Cryptographic Policy in OFS Analytical Applications Infrastructure Administration Guide.</p>

Table 6: Prerequisite Information

Category	Sub_Category	Expected Value
	Oracle Database Settings	<p>Oracle Database Server</p> <p>TNS_ADMIN must be set in .profile file pointing to appropriate tnsnames.ora file.</p> <p>Enable Transparent Data Encryption (TDE) and/ or Data Redaction**</p> <p>Note:</p> <p>For more information, see Appendix R: Configuring TDE and Data Redaction in OFSAA.</p> <p>OFSAAProcessing Server</p> <p>Set ORACLE_HOME in .profile file pointing to appropriate Oracle DB Client installation.</p> <p>PATH in .profile file must be set to include appropriate \$ORACLE_HOME/bin path.</p> <p>Entry (with SID/ SERVICE NAME) must be added in the tnsnames.ora file on the OFSAA server.</p>

Table 6: Prerequisite Information

Category	Sub_Category	Expected Value
OS/File System Settings	OS Level Settings	<p>You must set your locale to UTF-8 locale (LANG, NLS_LANG to be set in.profile). Specifying a locale depends on your data and the operating system installed on your system.</p> <p>For example,</p> <p>For Linux OS: export LANG=en_US.utf8</p> <p>You can determine the locale on your system using the locale -a command</p> <p>export,</p> <p>NLS_LANG=AMERICAN_AMERICA.AL32UTF8</p>
	File Descriptor Settings	Greater than 15000
	Total Number of Process Settings	Greater than 4096
	tmp space	Prior to installation, ensure that sufficient free temp space (minimum 1 GB free) is available in /tmp directory of unix server hosting OFSBD.
	Port Settings	Default port numbers to be enabled on the system are 6500, 6501, 6505, 6507, 6509, 6510, 6666, 9999, and 10101.
	Staging Area/ Metadata Repository	<p>A directory to hold the application metadata artifacts and additionally act as staging area. The directory must exist on the same system as the OFSAA Infrastructure (can be configured on different mount). However, the owner of the installation directory mentioned above must have RWX (read, write, and execute) permissions on this folder.</p> <p>Set 775 permission on this folder.</p> <p>Note:</p> <p>This directory is also referred as FTPSHARE folder.</p>
	Installation Directory	<p>A directory where the product files will be installed.</p> <p>Assign User permission to 755 on the installation directory.</p>
	Temporary Directory	<p>Default temporary directory where installation files are stored for a short period of time to support faster installation.</p> <ul style="list-style-type: none"> For installation on UNIX OS, your UNIX administrator must give you the required read-write permissions for the /tmp directory and disable the NOEXEC option Configure adequate space on the /tmp directory. It is recommended that you allocate more than 10 GB of space. <p>Note:</p> <p>If NOEXEC is enabled, the extraction of files by the installer into the /tmp directory is prevented and the binaries will not execute in the directory, which will fail the installation.</p>
	Download Directory	<p>A directory where the product installer file will be downloaded/ copied.</p> <p>Ensure user permission is set to 755 on the Download directory.</p>
	OS Locale	<ul style="list-style-type: none"> Linux: en_US.utf8 Solaris: en_US. Preparing for Installation 3-15 UTF-8
		<p>OFS BEHAVIOR DETECTION INSTALLATION GUIDE 8</p> <ul style="list-style-type: none"> To check the locale installed, execute the following command:

Table 6: Prerequisite Information

Category	Sub_Category	Expected Value
Database Settings	Database Instance Settings	<ul style="list-style-type: none"> NLS_CHARACTERSET to be AL32UTF8 NLS_LENGTH_SEMANTICS to be BYTE AVAILABLE OPEN CURSORS limit to be greater than 4096 <p>For an Oracle Database installation, set your Oracle NLS_LANG environment variable to an appropriate UTF-8 character set.</p> <p>For example, setenv NLS_LANG AMERICAN_ AMERICA.AL32UTF8</p> <p>Note:</p> <p>For more information on other database tunable parameters required for OFS BD, see Appendix S: Tunable Database Parameters.</p> <p>Ensure that the OLAP_USER role is available in the database.</p>
Web Application Server	WebSphere/ WebLogic/ Tomcat	<p>Web application server must be installed and profile/domain created.</p> <p>You are prompted to enter the WebSphere Profile path, WebLogic Domain path, or Tomcat Deployment path during OFSAI installation.</p> <p>Note:</p> <p>For more information about WebSphere Profile and WebLogic Domain creation, see Appendix A: Configure the Web Server.</p>
Web Server	Apache HTTP Server/ Oracle HTTP Server/ IBM HTTP Server.	<p>This is an optional requirement. HTTP Server Installation to be available. You are prompted to enter the Web server IP/Hostname and Port details during installation.</p> <p>Note:</p> <p>For more information on Web server installatio, see Appendix A: Configure the Web Server.</p>
Operating System	Solaris 11	<p>Upgrade to Oracle Solaris 11.3 with SRU09 or higher. See Updating to Oracle® Solaris 11.3 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.</p>
Backup Tables	Table Names	<p>Before starting the installation and post installation, ensure there are no Backup tables created manually with table names suffixed with _BKP or _TEMP.</p> <p>Note:</p> <p>Table names with _BKP and _TEMP that are created outside the application will cause installation/patch application to fail.</p>

NOTE

You cannot install the OFS FSDF application on an existing OFS BD installation, within the same infodom/schema.

4.2 Obtaining Software

The 8.1.2.0.0 release of OFS BD Applications Pack can be downloaded from [My Oracle Support](#). You must have a valid Oracle account to download the software.

4.3 Performing Common Pre-Installation Tasks

The common pre-installation activities that you must carry out before installing the OFS BD Application Pack are:

- [Identifying the Installation, Download and Metadata Repository](#)
- [Downloading and Copying the OFS BD Application Pack Installer](#)
- [Extracting the Software](#)
- [Setting Up Web Application Server](#)

4.3.1 Identifying the Installation, Download and Metadata Repository

To install OFSAA Application packs, create the following directories:

- **OFS BD Download Directory (Optional)** - Create a download directory and copy the OFS BD Application Pack Installer File (archive). This is the directory where the downloaded installer/patches can be copied. However, it's not mandatory to create this directory.
- **OFS BD Installation Directory** - Create an installation directory and copy the installation files. Perform the installation from this directory. Set the variable `FIC_HOME` variable in the `.profile` file to point to the OFS BD Installation Directory. However, it's not mandatory to create this directory.
- **OFS BD Staging/Metadata Directory (Mandatory)** - Create a Staging/Metadata Directory to copy data loading files, save data extracts and so on. Additionally, this directory also maintains the OFSAA metadata artifacts. This directory is also referred to as `FTP SHARE`.

NOTE

- It is not mandatory to create these directories.
- Assign 755 user permission to the Installation and Download Directory.
- Assign 755 user permission to the Staging Directory.

4.3.2 Downloading and Copying the OFS BD Application Pack Installer

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

1. The 8.1.2.0.0 release of OFS BD Applications Pack can be downloaded from [My Oracle Support](#). You must have a valid Oracle account to download the software.
2. Enter the Oracle Financial Services Behavior Detection in the search box to search.
3. Download the installer archive into the download Directory (in Binary mode) in the setup identified for Oracle Financial Services Behavior Detection 8.1.2.0.0.

4.3.3 Extracting the Software

NOTE You must be logged in to the UNIX operating system as a non-root user.

To extract the software, follow these steps:

1. Download the unzip utility (OS specific) `unzip_<os>.Z` and copy it in Binary mode to the directory that is included in your PATH variable. If you already have the unzip utility to extract the contents of the downloaded archive, skip this step.
2. Uncompress the unzip installer file with the following command:

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

NOTE If you encounter an error message when the package is not installed, contact your UNIX administrator.

3. Assign EXECUTE permission to the file with the command:

```
chmod 751 unzip_<OS>
```

For example, `chmod 751 unzip_sparc`

4. Extract the contents of the OFS BD Application Pack 8.1.2.0.0 installer archive file in the download directory with the following command:

```
unzip OFS_BD_PACK.zip
```

NOTE Do not rename the Application Pack installer folder name on extraction from the archive.

5. Navigate to the download directory and assign execute permission to the installer directory with the following command:

```
chmod -R 755 OFS_BD_PACK
```

4.3.4 Setting Up Web Application Server

For setting up the environment based on your selected Web application server, see [Configure Resource Reference in WebLogic Application Server](#).

5 Installing OFS BD Application Pack

This chapter describes the steps to be followed to install the OFS BD Application pack depending on the offline and online modes of installation.

Release 8.1.2.0.0 of the Oracle Financial Services Behavior Detection (BD) application is not fully backward compatible with earlier versions of FCCM. You must upgrade all of your FCCM applications from the existing 8.0.x versions to the 8.1.2.0.0 version and cannot choose to upgrade only selective application packs to 8.1.2.0.0.

NOTE

- If you are installing an Application Pack on an environment, where another Applications Pack is already installed, you may sometimes get a warning message such as Object Already Exists. This message can be ignored.
- Before you start the installation, you must first do the domain creation. For more information, see Creating Domain in WebLogic Server.
- See [Appendix U : OFS BD Version Compatibility List](#) for details on OFS BD Version compatibility with OFSAAI, FSDF, and OFS ECM.

Topics:

- [Configuring Wallet](#)
- [About Schema Creator Utility](#)
- [Configuring and Executing Schema Creator Utility](#)
- [Installing the OFS BD Application Pack](#)
- [Verifying Installation](#)

5.1 Configuring Wallet

For information on Installation and Configuration of Wallet in Non-TCPs and TCPs modes, see, [Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Guide](#).

5.2 About Schema Creator Utility

Creating database users/schemas is one of the primary steps in the complete OFS BD installation. This release of OFSAA provides a utility to quickly get started with the OFSAA 8.1.2.0.0. Installation by allowing easier and faster creation of database User(s)/ Schema(s), assign the necessary GRANT(s), and so on. Additionally, it also creates the required entities in the schemas and so on.

The schema creator utility must be configured and executed before installation of any OFSAA Application Pack.

Topics:

- [Configuring Schema Creator Utility for RDBMS](#)
- [Configuring Schema Creator Utility for HDFS Schema](#)
- [Selecting Execution Modes in Schema Creator Utility](#)
- [Selecting Execution Options in Schema Creator Utility](#)

5.2.1 Configuring Schema Creator Utility for RDBMS

The Pack specific schema details need to be filled in the OFS_BD_SCHEMA_IN.xml file (path is OFS_BD_PACK/schema_creator/conf/OFS_BD_SCHEMA_IN.xml) before executing the Schema Creator Utility. For more information on the xml file, see [Configuring OFS_BD_SCHEMA_IN.xml File](#).

NOTE On successful execution of the utility, the entered passwords in the OFS_BD_SCHEMA_IN.xml file are nullified.

The types of schemas that can be configured are:

- **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 There can be multiple ATOMIC schemas per OFSAA Instance.

5.2.2 Configuring Schema Creator Utility for HDFS Schema

NOTE On successful execution of the utility, the entered passwords in the OFS_BD_SCHEMA_IN.xml file are nullified.

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 METADOM 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.

5.2.3 Selecting Execution Modes in Schema Creator Utility

Schema creator utility supports the following modes of execution:

- **Online Mode:** In this mode, the utility connects to the database and executes the Data Definition Language (DDL) for User, Entities, and GRANTS.

NOTE

To execute the utility in Online mode, you need to connect as `<User> AS SYSDBA`.

- **Offline Mode:** In this mode, the utility generates an SQL script with all the required DDLs for User, Entities and GRANTS. This script must be executed by the DBA on the appropriate database identified for OFSAA usage.

NOTE

For running the SQL script generated in offline mode, the script must reside in the same directory where the *SQLScripts* directory is available.

1. Connect as any database user.
2. Reconfigure the `OFS_BD_SCHEMA_IN.xml` (as the case may be) file and execute the utility. For more information on reconfiguring these files, see [Configuring OFS_BD_SCHEMA_IN.xml File](#).
3. To execute the utility in Offline mode, you must connect as a user with the following GRANTS (alternatively, you can also connect as a user with SYSDBA privileges):
 - SELECT ON DBA_ROLES
 - SELECT ON DBA_USERS
 - SELECT ON DBA_DIRECTORIES
 - SELECT ON DBA_TABLESPACES
 - CREATE SESSION
4. If there are any errors during the SQL script execution, reconfigure the `OFS_BD_SCHEMA_IN.xml` and execute the utility. This regenerates the scripts with corrected information. For more information, see [Configuring OFS_BD_SCHEMA_IN.xml File](#).
5. Do not modify the `OFS_BD_SCHEMA_OUT.XML` file generated after the execution of this utility
6. Do not keep any backup files of xml's in the download directory.
7. Current offline installation throws an error while running the SQL in schema.

5.2.4 Selecting Execution Options in Schema Creator Utility

Depending on the option selected to run the OFSAA Applications Pack installer, you must select the appropriate schema creator utility execution option. To run the OFSAA Applications Pack installer in Silent mode, it is mandatory to execute the schema creator utility with -s option.

5.3 Configuring and Executing Schema Creator Utility

Topics:

- [Prerequisites](#)
- [Configuring Schema Creator Utility](#)
- [Executing the Schema Creator Utility](#)
- [Verifying the Schema Creator Log Files](#)

NOTE

If you intend to use the Oracle OLAP feature, execute the following grant on all ATOMIC schema(s):

```
grant olap_user to &database_username.
```

5.3.1 Prerequisites

The prerequisites you must have before configuring the Schema Creator Utility are:

- Oracle User ID/Password with SYSDBA privileges
- JDBC Connection URL for RAC/Non RAC database
- HOSTNAME/IP of the server on which OFSAA is being installed.
- TNSNames.ora must have an entry for the database planning to install the Database objects.
- For enabling Transparent Data Encryption (TDE) in your OFSAA instance during installation, perform the steps explained in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

5.3.2 Configuring Schema Creator Utility

This section explains the steps to configure the Schema Creator Utility.

NOTE

Do not change the extracted media pack folder name.

To configure the Schema Creator Utility, follow these steps:

1. Log in to the system as a non-root user.
2. Navigate to the path: `OFS_BD_PACK/schema_creator/conf` directory.
3. Edit the `OFS_BD_SCHEMA_IN.xml` file in a text editor.
4. Configure the elements as described in [Configuring OFS_BD_SCHEMA_IN.xml File](#).

5. Save the OFS_BD_SCHEMA_IN.xml file.

NOTE

On successful execution of the utility, the entered passwords in the OFS_BD_SCHEMA_IN.xml file are nullified.

While editing the OFS_BD_SCHEMA_IN.xml, ensure only the values/tag attributes mentioned in must be modified, and none of other tags must be modified.

Do not modify the following list of attributes:

- APP_PACK_ID
- ROLE.NAME
- DIRECTORY. ID
- DIRECTORY.NAME
- SCHEMA. APP_ID
- SCHEMA. DEFAULTTABLESPACE
- SCHEMA.TYPE
- TABLESPACE.NAME

5.3.3 Executing the Schema Creator Utility

You can execute the schema creator utility in Online mode or Offline mode.

Topics:

- [Executing the Schema Creator Utility in Online Mode](#)
- [Executing the Schema Creator Utility in Offline Mode](#)
- [Executing the Schema Creator Utility with -s Option](#)
- [Executing the Schema Creator Utility while Installing Subsequent Applications Pack](#)

5.3.3.1 Executing the Schema Creator Utility in Online Mode

In Online mode, the Schema Creator Utility creates all the Schemas, Schema Objects, Tablespaces, Grants, and Roles in the database during the execution process.

To execute the Schema Creator Utility in Online mode, follow these steps:

1. Log in to the system as non-root user.
2. Navigate to the path: OFS_BD_PACK/schema_creator/bin/
3. Execute the osc.sh file using the command: `./osc.sh`.

The 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).

4. Enter Y/ y to proceed with the script generation.
5. Enter the DB Username with SYSDBA Privileges. For example: SYS as SYSDBA.
6. Enter the User Password.

Figure 5: Schema Creation Online Mode 1

```
Parsing file: /scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/schema_creator/../conf/OFS_ECM_PACK.xml
Checking: app: OFS_AAI schema_name: E81_CONF813 schema_type: CONFIG
Checking: app: OFS_IPE schema_name: E81_ATOM813 schema_type: ATOMIC
Checking: app: OFS_NGECM schema_name: E81_ATOM813 schema_type: ATOMIC
You have chosen to install this Application Pack on "e81_atom813" ATOMIC schema. Do you want to proceed? (Y/N)
Y
You have chosen to install this Application Pack on INFODOM "813ecminfo". Do you want to proceed? (Y/N)
Y
=====
Executing TableSpace Scripts started...
Skipping the creation of tablespace COMM_DATA_TBSP
Skipping the creation of tablespace DATA_CM_TBSP
Skipping the creation of tablespace DATA_CONF_TBSP
Skipping the creation of tablespace IDX_CM_TBSP
=====
Creating Schemas started...
CONFIG User e81_conf813 successfully created on Default TableSpace : DATA_CONF_TBSP on Temp TableSpace : TEMP
Grants creation scripts execution started...
Grants creation scripts execution completed...
Connection jdbc:oracle:thin:@whf000xx.in.oracle.com:1521:Ti3019L64
Successfully connected to User - e81_conf813 URL - jdbc:oracle:thin:@whf000xx.in.oracle.com:1521:Ti3019L64
Scripts execution for CONFIG schema started ...
Scripts execution for CONFIG schema completed ...
User e81_conf813 details updated into the dbmaster table
User e81_conf813 details updated into the I18NMASTER table
User e81_conf813 details updated into the aai_db_detail table
User e81_conf813 details updated into the aai_db_auth_alias table
Skipping the creation of AAAI/IPE app.
User e81_atom813 details updated into the dbmaster table
User e81_atom813 details updated into the I18NMASTER table
User e81_atom813 details updated into the aai_db_detail table
User e81_atom813 details updated into the aai_db_auth_alias table
User e81_atom813 is successfully created on Default TableSpace : DATA_CM_TBSP on Temp TableSpace : TEMP
Executing specific IPE table create
Execution of specific IPE table creation completed
Creating Schemas completed ...
=====
Roles creation scripts execution started ...
Roles creation scripts execution completed ...
the value of redaction flag in atomic schema isfalse
=====
Grants creation scripts execution started...
Grants creation scripts execution completed...
=====
```

Figure 6: Schema Creation Online Mode 2

```
=====
Executing TableSpace Scripts started...
Skipping the creation of tablespace DATA_FATCA_TBSP
Skipping the creation of tablespace IDX_KDD_TBSP
Skipping the creation of tablespace DATA_MANTAS_TBSP
Skipping the creation of tablespace DATA_MINER_TBSP
Skipping the creation of tablespace IDX_MKT1_TBSP
Skipping the creation of tablespace IDX_MKT2_TBSP
Skipping the creation of tablespace DATA_CONF_TBSP
Skipping the creation of tablespace DATA_CTR_TBSP
Skipping the creation of tablespace DATA_FSDF1_TBSP
Skipping the creation of tablespace IDX_CTR_TBSP
Skipping the creation of tablespace IDX_MINER_TBSP
Skipping the creation of tablespace IDX_BUS3_TBSP
Skipping the creation of tablespace DATA_CM_TBSP
Skipping the creation of tablespace IDX_BUS1_TBSP
Skipping the creation of tablespace IDX_FATCA_TBSP
Skipping the creation of tablespace IDX_BUS4_TBSP
Skipping the creation of tablespace IDX_BUS5_TBSP
Skipping the creation of tablespace IDX_BUS2_TBSP
Skipping the creation of tablespace IDX_MKT4_TBSP
Skipping the creation of tablespace IDX_CM_TBSP
Skipping the creation of tablespace IDX_MKT3_TBSP
Skipping the creation of tablespace DATA_AM_TBSP
Skipping the creation of tablespace DATA_BUS6_TBSP
Skipping the creation of tablespace DATA_MKT3_TBSP
Skipping the creation of tablespace DATA_KYC_TBSP
Skipping the creation of tablespace IDX_KYC_TBSP
Skipping the creation of tablespace DATA_OB_TBSP
Skipping the creation of tablespace DATA_MKT1_TBSP
Skipping the creation of tablespace IDX_OB_TBSP
Skipping the creation of tablespace IDX_BUS8_TBSP
Skipping the creation of tablespace DATA_MKT2_TBSP
Skipping the creation of tablespace DATA_MKT4_TBSP
Skipping the creation of tablespace IDX_AM_TBSP
Skipping the creation of tablespace IDX_MANTAS_TBSP
Skipping the creation of tablespace IDX_BUS6_TBSP
Skipping the creation of tablespace IDX_BUS7_TBSP
Skipping the creation of tablespace DATA_BUS4_TBSP
Skipping the creation of tablespace DATA_BUS8_TBSP
Skipping the creation of tablespace DATA_KDD_TBSP
Skipping the creation of tablespace DATA_BUS5_TBSP
Skipping the creation of tablespace DATA_BUS7_TBSP
Skipping the creation of tablespace DATA_BUS1_TBSP
Skipping the creation of tablespace DATA_BUS2_TBSP
Skipping the creation of tablespace DATA_BUS3_TBSP
Skipping the creation of tablespace IDX_FSDF1_TBSP
=====
Creating Schemas started...
CONFIG User tst_conf successfully created on Default TableSpace : DATA_CONF_TBSP on Temp TableSpace : TEMP
Grants creation scripts execution started...
Grants creation scripts execution completed...
Successfully connected to User - tst_conf URL - jdbc:oracle:thin:@ofss222754.in.oracle.com:1521:T112014L64
Scripts execution for CONFIG schema started ...
Scripts execution for CONFIG schema completed ...
User tst_conf details updated into the dbmaster table
User tst_conf details updated into the I18NMASTER table
```

Figure 7: Schema Creation - Online Mode

```
User tst_fccm details updated into the aai_db_detail table
User tst_fccm details updated into the aai_db_auth_alias table
User tst_fccm is successfully created on Default TableSpace : DATA_MANTAS_TBSP on Temp TableSpace : T
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
Skipping the creation of AAAI/IPE app.
User tst_fccm already exists in dbmaster table.
User tst_fccm already exists in dbmaster table.
Creating Schemas completed ...

=====
Roles creation scripts execution started ...
Parsing ROLE tags...
Roles creation scripts execution completed ...

=====
Directory creation scripts execution started ...
Directory creation scripts execution completed ...

=====
Grants creation scripts execution started...
Grants creation scripts execution completed...

=====
                          Schemas Creation Completed

=====
Schema Creator executed Successfully.Please proceed with the installation.
```

\$ █

NOTE

- On successful execution of Schema Creator utility, the console displays the following status messages:
- Schema Creator executed successfully. Please proceed with the installation.
- See log file in OFS_BD_PACK/schema_creator/logs directory for execution status. If there are any errors, contact Oracle Support Services.
- Schema Creator executed successfully. Please proceed with the installation.
- Do not clean up the OFS_BD_SCHEMA_OUTPUT.XML file generated in the folder OFS_BD_PACK/schema_creator, as it would be required in future patch installations and upgrades.

5.3.3.2 Executing the Schema Creator Utility in Offline Mode

In Offline Mode, the Schema Creator Utility creates an output in the SQL file format. This script must be executed manually by logging as database user with SYSDBA privileges. The SQL file contains the creation of Schemas, Schema Objects, and Roles.

5.3.3.2.1 Prerequisites

To execute the utility in Offline mode, you must connect a database user with the following GRANTS (Alternatively, you can also connect as a user with SYSDBA privileges):

- SELECT ON DBA_ROLES
- SELECT ON DBA_USERS
- SELECT ON DBA_DIRECTORIES
- SELECT ON DBA_TABLESPACES
- CREATE SESSION

NOTE

Explicit GRANTS to the user are required. GRANTS assigned through Roles are not supported.

To execute the schema creator utility in Offline mode, follow these steps:

1. Log in to the system as a non-root user.
2. Navigate to the *OFS_BD_PACK/schema_creator/bin* directory.
3. Execute the *osc.sh* file using the command: `./osc.sh -o -s`
4. Enter Y /y to generate the script.

The following message is displayed: You have chosen OFFLINE mode. Triggering the utility in OFFLINE mode will generate the script. Do you wish to proceed? (Y/y or N/n).

5. Enter the DB Username with SELECT privileges.
6. Enter the User Password.

Figure 8: Schema Creation - Offline Mode 1

```
$ ./osc.sh -o
/scratch/ofsaapp/BDGI805/BDGI805
=====
You have chosen OFFLINE mode
=====
Triggering the utility in OFFLINE mode will generate the script. Do you wish to proceed? (Y/N):
Y
=====
Java Validation Started ...
Java found in : /usr/java/jdk1.8.0_45/bin
JAVA Version found : 1.8.0_45
JAVA Bit Version found : 64-bit
Java Validation Completed. Status : SUCCESS
=====
DB specific Validation Started ...
Enter the DB User Name with the following privileges:
1. CREATE SESSION
2. SELECT on DBA_ROLES
3. SELECT on DBA_USERS
4. SELECT on DBA_DIRECTORIES
5. SELECT on DBA_TABLESPACES
Enter the User Name:
sys as sysdba
Enter the User Password:
Oracle Client version : 12.1. Status : SUCCESS
Oracle Server version Current value : 12.2.0.1.0. Status : SUCCESS
DB specific Validation Completed. Status : SUCCESS
=====
Generating Schema Creation Scripts Started
=====
Checking OFSAA installation...
OFSAA installation not found.
Validating the dat file OFS_BD_CFG.dat started...
Successfully validated OFS_BD_CFG.dat file
Validating the input XML file.../scratch/ofsaapp/schema/OFS_BD_PACK/schema_creator/conf/OFS_BD_SCHEMA_IN.xml
Input XML file validated successfully.
=====
Validating Connection URL ...jdbc:oracle:thin:@ofss222754.in.oracle.com:1521:T112014L64
Successfully connected to User - sys as sysdba URL - jdbc:oracle:thin:@ofss222754.in.oracle.com:1521:T112014L64
Connection URL successfully validated...
localhost name - whf00ark IPAddress - 10.184.152.10
Parsing TABLESPACE tags...
Parsing DIRECTORY tags...
You have chosen to install this Application Pack on "tat_fccm" ATOMIC schema. Do you want to proceed? (Y/N)
Y
=====
```

Figure 9: Schema Creation - Offline Mode 2

```
Generating Schema creation scripts started...  
CONFIG User tat_conf creation script generated successfully on Default TableSpace : DATA_CONF_TBSP on Temp TableSpac  
Generation of grants creation scripts started...  
Generation of grants creation scripts completed...  
Scripts Generation for CONFIG schema started ...  
Scripts Generation for CONFIG schema completed ...  
User tat_conf details updated into the dbmaster table  
User tat_conf details updated into the I18NMASTER table  
User tat_conf details updated into the aai_db_detail table  
User tat_conf details updated into the aai_db_auth_alias table  
User tat_focm details updated into the dbmaster table  
User tat_focm details updated into the I18NMASTER table  
User tat_focm details updated into the aai_db_detail table  
User tat_focm details updated into the aai_db_auth_alias table  
User tat_focm creation script generated successfully on Default TableSpace : DATA_MANTAS_TBSP on Temp TableSpace : T  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
Skipping the creation of AAAI/IPE app.  
User tat_focm creation is skipping as the user is already created.  
User tat_focm creation is skipping as the user is already created.  
Generating Schema creation scripts completed...  
=====  
Generating Roles creation Scripts started...  
Parsing ROLE tags...  
Generating Roles creation Scripts completed...  
=====  
Generating Directory creation Scripts started...  
Generating Directory 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/ofsaapp/schema/OFS_BD_PACK/schema_creator/sysdba_outpu
```

The console runs the initial validation checks and displays the following message: You have chosen to install this Applications Pack on <Name of the Atomic Schema>ATOMIC schema. Do you want to proceed? (Y/N).

7. Enter Y/y to start the script generation. The following message is displayed. You have chosen to install this Applications Pack on <Name of the Infodomain>. Do you want to proceed? (Y/N)).

NOTE

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

Success. Execute OFS_BD_PACK/schema_creator/sysdba_output_scripts.sql before proceeding with the installation.

Ignore ORA-01430 and ORA-06512 console errors.

8. Navigate to the *OFS_BD_PACK/schema_creator* directory.
9. Login to SQLPLUS with a user having SYSDBA Privileges.
10. Connect to the Oracle DB Server on which the OFS BD Application Pack installation is to be performed and execute the *sysdba_output_scripts.sql* file using the following command:

```
SQL>@sysdba output scripts.sql
```


Figure 10: Schema Creator - Offline Mode 3

```
$ sqlplus sys/(< > as sysdba

SQL*Plus: Release 12.1.0.2.0 Production on Fri Oct 20 11:43:33 2017

Copyright (c) 1982, 2014, Oracle. All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

SQL> @sysdba_output_scripts.sql

Warning: Package Body created with compilation errors.

Warning: Procedure created with compilation errors.

Disconnected from Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
$ █
```

Alternatively, you can copy the sysdba_output_scripts.sql file and SQLScripts directory to a remote server and execute sysdba_output_scripts.sql file.

NOTE

See the *log sysdba_output_scripts.log* file for execution status. If there are any errors, contact [My Oracle Support](#). SQL Scripts folder and SQL file must reside in the same folder.

Once the above file gets executed, a warning is displayed as shown in the above screen.

11. Run the following scripts in config schema:
 - a. Navigate to the <OFS_BD_PACK>/schema_creator/SQLScripts/oracle folder.
 - b. Connect to the config schema through sqlplus.
 - c. Execute the @compile_objects.sql command.

- d. Commit the change.

NOTE

1. Post Schema creation, *OFS_IPE* tag appears as below in *OFS_BD_SCHEMA_OUTPUT.xml*:

```
<SCHEMA>
<APP_ID>OFS_IPE</APP_ID>
<USERNAME>qa_atm875</USERNAME>
<PASSWORD/>
<TYPE>PRODUCTION</TYPE>
<DEFTABSPACE>##OFS_AML_DATA_MANTS_TBSP##</
DEFTABSPACE>
<INFODOM>p16k21CPfkHkgv6MFb4u0A==</INFODOM>
</SCHEMA>
```
2. You have to manually update the PASSWORD (PASSWORD can be copied from the other App IDs (Encrypted Passwords will not change for App IDs)). Post update *OFS_IPE* tag appears as below:

```
<SCHEMA>
<APP_ID>OFS_IPE</APP_ID>
<USERNAME>qa_atm875</USERNAME>
<PASSWORD/>q1m04rJt6a/yT+magFXisQ==</PASSWORD>
<TYPE>PRODUCTION</TYPE>
<DEFTABSPACE>##OFS_AML_DATA_MANTS_TBSP##</
DEFTABSPACE>
<INFODOM>p16k21CPfkHkgv6MFb4u0A==</INFODOM>
</SCHEMA>
```

5.3.3.3 Executing the Schema Creator Utility with -s Option

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

To execute the utility with -s option, follow these steps:

1. Edit the file `OFS_BD_PACK/schema_creator/conf/OFS_BD_SCHEMA_IN.xml` in text editor.

NOTE

The infodom name and schema name must be same for all these APP_IDS:

- OFS_KYC
- OFS_AAIB
- OFS_CTR
- OFS_FSDF
- OFS_FATCA
- OFS_FRAUD
- OFS_AML
- OFS_TC
- OFS_ECTC
- OFS_PTA
- OFS_TB
- OFS_BC
- OFS_IPE
- OFS_FRAUD_EE
- OFS_CRSR

2. Execute the utility with -s option. For example `./osc.sh -s`

Figure 11: Schema Creator with -s option 1

```

$ ./osc.sh -s
profile Executed
/scratch/ofsaaweb/ECM813/ECM813
=====
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 : /scratch/jre1.8.0_261/bin
JAVA Version found : 1.8.0_261
JAVA Bit Version found : 64-bit
Java Validation Completed. Status : SUCCESS
=====
DATABASENAME = Ti3019L64
DB specific Validation Started ...
Enter the DB User Name With SYSDBA Privileges:
sys as sysdba
Enter the User Password:
user name is sys
Oracle Client version : 19.0.0.0.0. Status : SUCCESS
Oracle Server version Current value : 19.0.0.0.0. Status : SUCCESS
DB specific Validation Completed. Status : SUCCESS
=====
Schema Creation Started
=====
Checking OFSAA installation...
OFSAA installation not found.
Validating the dat file OFS ECM CFG.dat started...
The path is:/scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/schema_creator/conf
Successfully validated OFS ECM CFG.dat file
Validating the input XML file.../scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/schema_creator/conf/OFS_ECM_SCHEMA_IN.xml
Input XML file validated successfully.
=====
Validating Connection URL ...jdbc:oracle:thin:@whf000xx.in.oracle.com:1521:Ti3019L64
Connection jdbc:oracle:thin:@whf000xx.in.oracle.com:1521:Ti3019L64
Successfully connected to User - sys as sysdba URL - jdbc:oracle:thin:@whf000xx.in.oracle.com:1521:Ti3019L64
Connection URL successfully validated...
localhost name - whf000xx IPAddress - 10.40.160.50
LINE 18 ROW 1 not there in schema
IS_HYBRID not there in schema
Parsing TABLESPACE tags...
Parsing file: /scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/schema_creator/.../conf/OFS_ECM_PACK.xml

```


Figure 12: Schema Creator with -s option 2

```
Creating Schemas started...  
CONFIG User tt_conf successfully created on Default TableSpace : DATA_CONF_TBSP on Temp TableSpace : TEMP  
Grants creation scripts execution started...  
Grants creation scripts execution completed...  
Successfully connected to User - tt_conf URL - jdbc:oracle:thin:@ofss222754.in.oracle.com:1521:Til2014L64  
Scripts execution for CONFIG schema started ...  
Scripts execution for CONFIG schema completed ...  
User tt_conf details updated into the dbmaster table  
User tt_conf details updated into the I18NMASTER table  
User tt_conf details updated into the aai_db_detail table  
User tt_conf details updated into the aai_db_auth_alias table  
User tt_fccm details updated into the dbmaster table  
User tt_fccm details updated into the I18NMASTER table  
User tt_fccm details updated into the aai_db_detail table  
User tt_fccm details updated into the aai_db_auth_alias table  
User tt_fccm is successfully created on Default TableSpace : DATA_MANTAS_TBSP on Temp TableSpace : TEMP  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
Skipping the creation of AAAI/IPF app.  
User tt_fccm already exists in dbmaster table.  
User tt_fccm already exists in dbmaster table.  
Creating Schemas completed ...  
  
=====  
Roles creation scripts execution started ...  
Parsing ROLE tags...  
Roles creation scripts execution completed ...  
  
=====  
Directory creation scripts execution started ...  
Directory creation scripts execution completed ...  
  
=====  
Grants creation scripts execution started...  
Grants creation scripts execution completed...  
  
=====  
Schemas Creation Completed  
  
=====  
Schema Creator executed Successfully.Please proceed with the installation.
```

NOTE	To execute the utility in OFFLINE mode with Silent option, type <code>./osc.sh -o -s</code>
-------------	--

5.3.3.4 Executing the Schema Creator Utility while Installing Subsequent Applications Pack

While executing the schema creator utility for subsequent Applications 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 Install OFS BD Applications Pack on a separate information domain.

To execute the schema creator utility while installing OFS BD Pack over an existing Application Pack, follow the step:

- Perform the steps 1 to 5 from the [Executing the Schema Creator Utility](#) section.

NOTE

On successful execution of Schema Creator utility, the console displays the following status message:

Success. Please proceed with the installation.

See the log sysdba_output_scripts.log for execution status, if executed in offline mode.

If there are any errors, contact [My Oracle Support](#).

5.3.4 Verifying the Schema Creator Log Files

You can verify the log files for any errors faced during the schema creation process in the following location: *OFS_BD_PACK/schema_creator/logs*.

5.4 Installing the OFS BD Application Pack

This section provides instructions to install the OFS BD Application Pack in silent mode.

Topics:

- [Installing in Silent Mode](#)
- [Enabling Newly Licensed App for Standalone OFS BD 8.1.2.0.0](#)

5.4.1 Installing in Silent Mode

In the Silent Mode Installation, you must configure the product XML files and follow instructions in the command prompt.

Topics:

- [Configuring OFSAAI_InstallConfig.xml](#)
- [Configuring default.properties Parameters](#)
- [Running the installer in Silent Mode \(Update the note\)](#)
- [Completing the installation in Silent Mode](#)

5.4.1.1 Configuring OFSAAI_InstallConfig.xml

Follow these instructions to configure OFSAAI_InstallConfig.xml file:

1. Log in to the system as non-root user.
2. Identify a directory for installation and set the same in the user .profile file as the following:
FIC_HOME=< OFSAA Installation Directory > export FIC_HOME.
3. Execute the user .profile.
4. Configure the OFSAAI_InstallConfig.xml as mentioned in [Appendix M: Configuring OFSAAI_InstallConfig.xml File](#). Set the Interaction Variable parameter values manually as mentioned in the table. If a value is not applicable, enter NA and ensure that the value is not entered as NULL.

5. Navigate to the file: `OFS_BD_PACK/conf/OFS_BD_PACK.xml` and select the applications to be enabled. For more information see, [Configuring OFS_BD_SCHEMA_IN.xml File](#).

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

5.4.1.2 Configuring default.properties Parameters

NOTE

From BD 8.1.1.0.0 onwards, default.properties replaced from InstallConfig.xml.

To configure the default.properties file, follow these steps:

1. Navigate to the file: `OFS_BD_PACK/OFS_AML/conf/default.properties`.
2. Enter the details mentioned in the tags (`<!-- Start: User input required for silent installer. -->` and `<!-- End: User input required for silent installer. -->`) as mentioned in [Table 7](#).

Table 7: default.properties parameters

Placeholder Name	Significance and Expected Value	Mandatory
<code>##OFS_AML_BASE_COUNTRY##</code>	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: <code>base_country=US</code> <code>base_country=US</code>	Yes
<code>##OFS_AML_DEFAULT_JURISDICTION##</code>	Jurisdiction to assign the derived entities and derived addresses. For example: <code>default_jurisdiction=AMEA</code>	Yes
<code>##OFS_AML_SMTP_HOST##</code>	Hostname of the e-mail gateway to be used by the application for e-mail notifications. For example: <code>smtp_host=mailhost.domain.com</code> <code>smtp_host=mailhost.domain.com</code>	Yes
<code>##OFS_AML_PARTITION_DATE_FORMAT##</code>	Format of the date used in specifying partition dates. Allowed values are DD-MON-YYYY/DD-MM-YYYY	Yes
<code>##OFS_AML_DATADUMPDT_MINUS_0##</code>	Enter the date of the business day for which the data to be loaded. It must be in dd/mm/yyyy format. For Example: 10/12/2015	Yes
<code>##OFS_AML_ENDTHISWEEK_MINUS_00#</code>	Enter the date of the Saturday of the next business week with respect to the date for which the data is loaded. It must be in dd/mm/yyyy format. For Example: 19/12/2015	Yes
<code>##OFS_AML_STARTNEXTMNTH_MINUS_00##</code>	Enter the first business day of the next month with respect to the data load date. It must be in dd/mm/yyyy format. For Example:01/01/2016	Yes

Table 7: default.properties parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##OFS_AML_WEB_SERVICE_USER##	User name to access the web services. Enter "" if no user name is required.	No
##OFS_AML_WEB_SERVICE_PASSWORD##	Password to access the web services. Enter "" if no password is required.	No
##OFS_AML_NLS_LENGTH_SEMANTICS##	##OFS_AML_NLS_LENGTH_SEMANTICS##NLS_LENGTH_SEMANTICS database variable for executing the DDL scripts. Applicable values are CHAR/BYTE. Note: Recommendation to go with CHAR.	Yes
##OFS_AML_CONFIGURE_OBIEE##	Mention flag as '1' to configure OBIEE URL. Otherwise mention as '0'.	Yes
##OFS_AML_OBIEE_URL##	In case ##OFS_AML_CONFIGURE_OBIEE_URL## mentioned as '1'. Provide the URL in the pattern. NOTE: Fully Qualified host name have to be provided.	Yes This parameter is mandatory if the value of ##OFS_AML_CONFIGURE_OBIEE## parameter is set to 1.
##OFS_AML_SW_RMIPORT##	Placeholder to provide scenario wizard RMI port.	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter TRUE to enable big Data or FALSE to not enable Big Data.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.

Table 7: default.properties parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL##	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No
<p>Note: KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> Initiate Onboarding Service (InitiateOnboardingService.war) Table To JSON Service (TabletoJSONService.war) JSON To Table Service (JSONToTablePersistenceUtility.war) Common Gateway Service (CommonGatewayService.war) Generate Case Input Service (GenerateCaseInputService.war) Create JSON Service (createJSONService.war) <p>The above .war files are available in the FIC_HOME path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The below parameters are applicable for KYC Onboarding:</p> <p>Note: The WEB_SERVER_PORT value must be taken from the OFSAAI_InstallConfig.xml file. Also, based on the value of HTTPS_ENABLE in OFSAAI_InstallConfig.xml, the PROTOCOL will be https for value 1 and http for value 0.</p>		
##ECMSOURCE##	This is the Case Management (ECM) source. If ECM is not installed, then you must provide the DB link name.	Mandatory only if KYC onboarding is used.
##ECMLOADTYPE##	This is the Case Management load type. If ECM is on a different database, then you must provide the value as 'DBLINK'.	Mandatory only if KYC onboarding is used.

Table 7: default.properties parameters

Placeholder Name	Significance and Expected Value	Mandatory
##CSSOURCE##	This is the Customer Screening (CS) source. If CS is not installed, then you must provide the DB link name.	Mandatory only if KYC onboarding is used.
##CSLOADTYPE##	This is the Customer Screening (CS) load type. If CS is on a different database, then you must provide the value as 'DBLINK'.	Mandatory only if KYC onboarding is used.
##CRRSOURCE##	This is the Compliance Regulatory Reporting (CRR) source. If CRR is not installed, then you must provide the DB link name.	Mandatory only if KYC onboarding is used.
##CRRLOADTYPE##	This is the Compliance Regulatory Reporting load type. If CRR is on a different database, then you must provide the value as 'DBLINK'.	Mandatory only if KYC onboarding is used.
##OBDATASRCNAME##	Parameter value must be updated with the INFODOM parameter. This is the name of the datasource pointing to the atomic schema. This value is taken from OFS_BD_SCHEMA_IN.xml.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATEWAY_DS##	Parameter value must be updated with the INFODOM parameter. This is the name of the datasource pointing to the atomic schema. This value is taken from OFS_BD_SCHEMA_IN.xml.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATEWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.

Table 7: default.properties parameters

Placeholder Name	Significance and Expected Value	Mandatory
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	<p>This is the URL of the ECM application till the context name. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT/CONTEXT_NAME>.</p> <p>If you install only the BD application, then you must update the##ECM_APP_URL## parameter with the URL of the running and deployed ECM setup of the same version. If you do a pack on pack installation, the##ECM_APP_URL## parameter can be updated with the same URL used for the ##AAI_AUTH_URL## parameter.</p>	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.

Table 7: default.properties parameters

Placeholder Name	Significance and Expected Value	Mandatory
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR application till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL://HOSTNAME:WEB_SERVER_PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL://HOSTNAME:PORT/CONTEXT_NAME>/questionnaire_api/questionnaires/resume/<INFODOM>/en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.

- In order to use the golden data for demonstrations and trainings, you must provide the following partition dates before the installation:
 - DATADUMPDT_MINUS_0##10/12/2015

- ENDTHISWEEK_MINUS_00##19/12/2015
- STARTNEXTTMNTH_MINUS_00##01/01/2016

NOTE AML is mandatory for KYC.

5.4.1.3 Running the installer in Silent Mode (Update the note)

To install the OFSAA Infrastructure in Silent mode, follow these steps:

1. Navigate to the *OFS_BD_PACK/bin* folder.
2. Execute the command in the console: `./setup.sh SILENT`.

5.4.1.4 Completing the installation in Silent Mode

On launching the installer in silent mode, the environment check utility is executed. Enter the required information to execute the utility as explained:

NOTE The above table item is asked if environment check utility is executed in the standalone mode.

Figure 13: SILENT Mode

```
$ ./setup.sh SILENT
profile Executed
/scratch/ofsaaweb/ECM813/ECM813
Current OS Type ---- Linux
FIC_HOME : /scratch/ofsaaweb/ECM813/ECM813
Environment check utility started...
=====
Java Validation Started ...
  Java found in : /scratch/jre1.8.0_261/bin
  org ver =1.8,11.0
  REQUIRED_VERSION =108,1100
  orgVersion =1.8.0_261
  ORG_JAVA =1.8
  VERSION =108
  ORG_REQUIRED_VERSION = 1.8
  JCE IS true
  JAVA Version found : 1.8.0_261
  JAVA Bit Version found : 64-bit
Java Validation Completed. Status : SUCCESS
=====
Environment Variables Validation Started ...
  ORACLE_HOME : /scratch/oraofss/app/product/19.0.0/client_1
  TNS_ADMIN : /scratch/ofsaapp
Environment Variables Validation Completed. Status : SUCCESS
=====
OS specific Validation Started ...
  Checking en_US.utf8 locale. Status : SUCCESS
  Unix shell found : /bin/ksh. Status : SUCCESS
  Total file descriptors : 65536. Status : SUCCESS
  Total number of process : 4096. Status : SUCCESS
  OS version : 7. Status : SUCCESS
OS specific Validation Completed. Status : SUCCESS
=====
DB specific Validation Started ...
  Oracle Client version : 19.0.0.0.0. Status : SUCCESS
  client version 19.0
  Successfully connected to schema e81_atom813. Status : SUCCESS
  CREATE SESSION has been granted to user. Status : SUCCESS
  CREATE PROCEDURE has been granted to user. Status : SUCCESS
  CREATE VIEW has been granted to user. Status : SUCCESS
  CREATE TRIGGER has been granted to user. Status : SUCCESS
  CREATE MATERIALIZED VIEW has been granted to user. Status : SUCCESS
  CREATE TABLE has been granted to user. Status : SUCCESS
  CREATE SEQUENCE has been granted to user. Status : SUCCESS
```

NOTE

- Enter the Infrastructure FTP/SFTP password value, when prompted at the command prompt to access Product Staging/Metadata repository directory in the application server.
- Enter always, when prompted to add host key fingerprint.

The OFSAAI License Agreement is displayed as shown in [Figure 14](#) :

Figure 14: OFSAAI License Agreement Page

```
/scratch/ofsaaweb/ECM813/ECM813
inside checkappstatus-app OFS_NGECEM /scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/bin
all value /scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/bin
In app value
[AppPreCheck] Checking for app installation OFS_NGECEM
[AppPreCheck] app OFS_NGECEM is ENABLED
=====
Start of Environment Checks
=====
/scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/OFS_NGECEM/conf
File log4j.xml not found. Using default logging settings
=====
-----Validating JAVA Version-----
Current JAVA Version is: 1.8.0_261
Required JAVA Version is: 1.8
JAVA Version validation status: SUCCESS
=====
-----Checking OS-----
OS Type: LINUX
OS Supported: TRUE
Current OS Version:7.7
Supported OS Version:7.1
OS Version Validation Status: SUCCESS
=====
-----Checking Disk Space-----
Available Disk Space is :165605
Required Disk Space is :700 MB
Validation for category DISK SPACE. STATUS : SUCCESS
=====
-----Checking Temp Space-----
Available Temp Space is 25794 MB
Required Temp Space is 700 MB
Validation for category TEMP SPACE. STATUS : SUCCESS
=====
-----Checking RAM-----
Available RAM in MB 19395
Required RAM in MB 700 MB
Validation for category RAM. STATUS : SUCCESS
=====
End of Environment Checks
=====
continuing precheck for next app
```

1. Enter Y/y to accept the License Agreement.

NOTE

SYSADMN and SYSAUTH are the two default OFSAAI administrative users created.

Figure 15: OFSAAI License Agreement Page - Launching Installer

```

Launching installer...
Preparing SILENT Mode Installation...

=====
OFSAAIInfrastructure                               (created with InstallAnywhere)
=====

-----
Installing...
-----

[=====|=====|=====|=====]
[-----|-----|-----|-----]

Installation Complete.
THE OS VERSION IS: 7
THE CLIENT VERSION IS: 19
Copying done for BE files....
profile Executed
/scratch/ofsaaweb/ECM813/ECM813
heapsize == 8192
/scratch/ofsaaweb/ECM813/installer/OFS_ECM_PACK/bin
profile Executed
/scratch/ofsaaweb/ECM813/ECM813
checking version
VersionToBeApplied: 8.1.1.0.0
Fresh installation
Y

*****
Welcome to OFS ECM PACK Installation
*****
Starting OFSAA Service...
OFSAA Service - OK
Preparing to install...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...

```

Figure 16: OFSAAI License Agreement Page - Execution Completed

```

Execution completed for PMF update Pipeline
profile Executed
/scratch/ofsaaweb/ECM813/ECM813
executing "ant"
Buildfile: /scratch/ofsaaweb/ECM813/ECM813/ficweb/build.xml

createwar:
[war] Building war: /scratch/ofsaaweb/ECM813/ECM813/ficweb/ECM813.war
createear:
[ear] Building ear: /scratch/ofsaaweb/ECM813/ECM813/ficweb/ECM813.ear

BUILD SUCCESSFUL
Total time: 58 seconds
Shutdown of OFSAAI services started...
nohup: appending output to 'nohup.out'
Shutdown of OFSAAI services done.
OFSAA App Layer Services start-up check started...
Starting startofsaai.sh service...
OFSAA Service - OK
Starting icc service...
icc service - OK
Shutting down icc service...
Shutting down OFSAA service...
OFSAAI App Layer Services check Status: SUCCESSFUL.
OFSAAI DB Layer Services check started...
profile Executed
/scratch/ofsaaweb/ECM813/ECM813
Calling agentshutdown.sh to check and kill, if any of the server is running...
MESSAGE Server service is not running.
AM service is not running.
ROUTER service is not running.
Starting ROUTER Service
ROUTER service started in background mode.
Starting AM Service
AM service started in background mode.
Starting MESSAGE SERVER Service
MESSAGE SERVER service started in background mode.
Stop MESSAGE Server service with Process ID : 27956
Stop AM service with Process ID : 27938
Stop ROUTER service with Process ID : 27926
OFSAAI DB Layer File Services check Status: SUCCESSFUL.
Installation completed...
$

```

NOTE

- The installation process continues on the console. Do not close the console until the installation process is complete.
- Execute .profile from user home directory after the installation is completed.

2. Perform the steps mentioned in [Verifying Installation](#).
3. For enabling TDE, see the *Configuring TDE in Case of Upgrade* section in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

4. For enabling Data Redaction, see *Enabling Data Redaction in Case of Upgrade* section in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

5.4.2 Enabling Newly Licensed App for Standalone OFS BD 8.1.2.0.0

To Enable/Install New App from *OFS_BD_PACK* once the BD812 installation is done.

1. Navigate to the *<OFS_BD_PACK>/conf* folder. Enable the newly licensed app in the *OFS_BD_PACK.xml* file by setting ENABLE flag to YES. For more information, see [Configuring OFS_BD_PACK.xml File](#).

For example: `<APP_ID PREREQ="OFS_AAI" ENABLE="YES">OFS_KYC</APP_ID>`

2. Navigate to the *<OFS_BD_PACK>/bin* folder and trigger the `setup.sh`.

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has newly licensed and Enter NO in the remaining applications.

5.5 Verifying Installation

Verify the following logs files for more information:

- See the `Pack_install.log` file in the folder: */OFS_BD_PACK/logs*
- See the *OFSAAI822018_XX_XX_XX_XX_XX.log* file under */OFS_BD_PACK/OFS_AAI/logs*

NOTE

.log file number (OFSAAI822018_XX_XX_XX_XX_XX) changes every installation.

- See the `BD_log` files located in the folder: */OFS_BD_PACK/<Appid>/logs* for OFS BD Applications Pack Installation log file. (Example: *OFS_AML*, *OFS_KYC*).

NOTE

- If there are any errors, do not proceed with further installation and contact Oracle Support Services.
- If logs are clean the mandatory AAI patch **33738222** has to be applied.

- Once BD installation is completed, check if `jersey-client-2.30.jar` and `jersey-client.jar` are available in the path *\$FIC_HOME/ficweb/webroot/WEB-INF/lib*. If both these Jars are available, follow these steps to remove the older version.
 - Navigate to *\$FIC_HOME/ficweb/webroot/WEB-INF/lib*
 - Delete *Jar jersey-client.jar*
 - Regenerate the EAR/WAR file and redeploy.

6 Upgrading the OFS BD Applications Pack

Topics:

- [Upgrading from OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0](#)
- [Upgrading from OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0](#)
- [How to Enable Newly Licensed App after Upgrade to BD 8.1.2.0.0](#)

NOTE

- Before you run the upgrade, perform a backup of the \$FIC_HOME, and ftpshare directories and the Atomic and Config schemas.
- Take a backup of CSA tables.

6.1 Upgrading from OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0

Topics:

- [Standalone Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0](#)
- [In-Place Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0](#)
- [Cloning Upgrades of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0](#)
- [Pack on Pack Inplace Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0](#)
- [Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0](#)

6.1.1 Standalone Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0

Perform the Standalone Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0 via, **In-Place Upgrade** and **Cloning Upgrade**.

NOTE

- Ensure to take the backup of File System (FIC_HOME and FTPSHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that you end all the batches before you start the upgrade process.
- For enabling the unlimited Cryptographic Policy for Java, see [Enabling Unlimited Cryptographic Policy for Java](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing Inplace upgrade.

6.1.2 In-Place Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0

Perform the In-Place upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0.

Prerequisites: For Inplace Upgrade, a minimum patch set level is required for performing OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0.

For more information, see [Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix](#).

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF, see [Configuring FSDF in Different Infodom \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- When truncating, ignore ORA errors for table not found.
- The minimum BD patch level must be **bug 33767866**.

3. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the **bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0**.
4. Navigate to OFS_BD_PACK and grant execute (755) permission for all executables \$ chmod 755 *.
5. Navigate to installer/OFS_BD_PACK/ conf and update OFS_BD_PACK.xml. Select applications to enable. For more information, see [Configuring OFS_BD_PACK.xml File](#).

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

6. Modify PatchConfig.xml parameters under OFS_BD_PACK/OFS_AML/conf/ PatchConfig.xml with appropriate values as described in [Table 8](#).

Table 8: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)

Table 8: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL#	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No

Table 8: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> Initiate Onboarding Service (InitiateOnboardingService.war) Table To JSON Service (TableToJSONService.war) JSON To Table Service (JSONToTablePersistenceUtility.war) Common Gateway Service (CommonGatewayService.war) Generate Case Input Service (GenerateCaseInputService.war) Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATEWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATEWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.

Table 8: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.

Table 8: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , the URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>/questionnaire_api/questionnaires/resume/<INFODOM>/en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

7. Navigate to the OFS_BD_PACK/bin folder and execute setup.sh file using the following command: `./setup.sh SILENT`.
8. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
9. After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.

10. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

3. After Upgrade Run below scripts manually as a post upgrade steps:
\$FIC_HOME/database/db_tools/bin
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfgDuring installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW
FORCE AS OBJECT (
This issue is to be fixed in release 8.1.2.1 ML.
4. Load the below scenarios manually using the sm_load utility available in the below path:
\$FIC_HOME/database/db_tools/bin
For details on running the sm_load utility, see *Loading Scenario Metadata* section in [OFS BD Administration Guide 8.1.2.0.0](#).
List of scenarios to be loaded:
 - ML-CIBPreviousAverageActivity.116000083.xml
 - ML-CashTransPossibleCTR.116000037.xml
 - ML-DepWDSameAmts.118860020.xml
 - ML-LargeReportableTrans.116000099.xml
 - ML-RapidMvmtFundsAllActivity.116000079.xml
 - ML-StructuringAvoidReportThreshold.116000046.xml
 - ML-StructuringAvoidReportThreshold.116000062.xml

6.1.2.1 Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0

To enable newly licensed App after upgrade to BD 8.1.2.0.0 follow these steps:

1. Place the OFS_BD_SCHEMA_OUTPUT.xml file from previous installer to the current BD812 installer path <OFS_BD_PACK>/schema_creator.
2. Copy the content of default.properties_bkp file from <OFS_BD_PACK>/OFS_AML/conf path to the app specific folder which is newly enabled.
For example: If you are enabling OFS_KYC for the first time, copy the content to default.properties file in <OFS_BD_PACK>/OFS_KYC/conf path.
3. In the app specific default.properties file, enter the details mentioned in the tags (<!-- Start: User input required for silent installer.
--> and <!-- End: User input required for silent installer. -->).
4. Replace the below parameter values in default.properties file with the values available in the previous installer file path <OFS_BD_PACK>/OFS_AML/conf/default.properties

- FCCM_USER=##OFS_AML_ATOMIC_USER##
 - FCCM_PASSWORD=##OFS_AML_ATOMIC_PW##
 - FCCMINFODOM=##OFS_AML_INFODOM_NAME##
 - FCCM_DBNAME=##OFS_AML_INFDBNAME##
 - FCCMINFODOM_DESCRIPTION=##OFS_AML_INFODOM_DESC##
5. Go to <OFS_BD_PACK>/conf folder. Enable the newly licensed app in the OFS_BD_PACK.xml file by setting ENABLE flag to YES. For more information, see [Configuring OFS_BD_PACK.xml File](#).

For example: <APP_ID PREREQ="OFS_AAI" ENABLE="YES">OFS_KYC</APP_ID>

NOTE Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

6. Go to <OFS_BD_PACK>/bin folder and trigger the setup.sh.

NOTE Please make sure there are no leading/trailing spaces in the <JDBC_URL> inside OFS_BD_SCHEMA_OUTPUT.xml file.

6.1.3 Cloning Upgrades of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0

Perform the Cloning Upgrade of OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0.

- NOTE**
- Ensure to take the backup of File System (FIC_HOME and FTPSHARE), Atomic schema, and Config schema before performing the upgrade.
 - Ensure that you end all the batches before you start the upgrade process.
 - For enabling the unlimited Cryptographic Policy for Java, see [Enabling Unlimited Cryptographic Policy for Java](#).
 - ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing cloning upgrade.

Prerequisites

- Perform Cloning as per the Cloning procedure. For more information, see [OFS Analytical Applications Infrastructure Cloning Reference Guide](#).

- Preparing hardware and software requirements. For more information, see [Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix](#) for

NOTENOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF, see *Configuring FSDF in Different Infodm (Pack on Pack Installation)* before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the **STG tables** (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767866.

- Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0.
- Navigate to OFS_BD_PACK and grant execute (755) permission for all executables \$ chmod 755 *.
- Navigate to installer/OFS_BD_PACK/ conf and update OFS_BD_PACK.xml. Select applications to enable. For more information, see [Configuring OFS_BD_PACK.xml File](#).

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

- Modify PatchConfig.xml parameters under OFS_BD_PACK/OFS_AML/conf/ PatchConfig.xml with appropriate values as follows:

Table 9: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes

Table 9: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL##	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No

Table 9: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> • Initiate Onboarding Service (InitiateOnboardingService.war) • Table To JSON Service (TableToJSONService.war) • JSON To Table Service (JSONToTablePersistenceUtility.war) • Common Gateway Service (CommonGatewayService.war) • Generate Case Input Service (GenerateCaseInputService.war) • Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATEWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATEWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.

Table 9: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.

Table 9: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME> /questionnaire_api/questionnaires/resume/<INFODOM>/en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

5. Navigate to the OFS_BD_PACK/bin folder and execute setup.sh file using the command: \$./ setup.sh SILENT.
6. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
7. After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.

8. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.

\$FIC_HOME/database/db_tools/bin

- ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
- ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfg

During installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:

```
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW FORCE
AS OBJECT (
```

This issue is to be fixed in release 8.1.2.1 ML.

2. To enable newly licensed app from OFSA BD pack, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).
3. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin.

List of scenarios to be loaded:

- ML-CIBPreviousAverageActivity.116000083.xml
- ML-CashTransPossibleCTR.116000037.xml
- ML-DepWDSameAmts.118860020.xml
- ML-LargeReportableTrans.116000099.xml
- ML-RapidMvmtFundsAllActivity.116000079.xml
- ML-StructuringAvoidReportThreshold.116000046.xml
- ML-StructuringAvoidReportThreshold.116000062.xml

6.1.4 Pack on Pack Inplace Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0

Performing Pack on Pack Inplace Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0.

NOTE

- Ensure to take the backup of File System (FIC_HOME and FTPSHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that the dispatcher is not running. If the dispatcher is running, stop and then start the upgrading process.
- Ensure that you end all the batches before you start the upgrade process.
- Ensure that you run the END_MANTAS_BATCH before starting the upgrade.
- For enabling the unlimited Cryptographic Policy for Java, see the section [Enabling Unlimited Cryptographic Policy for Java](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing Inplace upgrade.
- If the OFS Sanctions 8.0.8.0.0 is installed, then follow below steps:
 - create table KDD_BUS_DMN_SANC as (select * from KDD_BUS_DMN);
 - UPDATE KDD_BUS_DMN SET TF_BUS_DMN_NM=NULL; commit

Topics:

- [Pack on Pack Upgrade Sequence](#)
- [OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0](#)
- [OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0](#)
- [OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0](#)

6.1.4.1 Pack on Pack Upgrade Sequence

Use the following pack upgrade sequence:

- OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0
- OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0
- OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0

6.1.4.2 OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0

Follow these steps for OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0.

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF, see [Configuring FSDF in Different Infodomain \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767866.

1. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0.

Refer to the following instructions to download, extract, install, and configure this release:

2. To download and copy the OFS BD Applications Pack v8.1.2.0.0 archive file, see [Downloading and Copying the OFS BD Application Pack Installer](#).
3. Login to the OFSAA Server with user credentials used to install OFSAA.
4. Shut down all the OFSAAI Services. For more information, see the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
5. Execute the following command: `chmod -R 755 $FIC_HOME`.
6. If you have Unzip utility, skip to the next step. Download the Unzip utility (OS specific) and copy it in Binary mode to the directory that is included in your PATH variable, typically \$HOME path or directory in which you have copied the 8.1.2.0.0 installer.
7. Uncompress the unzip installer file using the command: `uncompress unzip_<os>.Z`.

NOTE

In case you notice an error message, contact your UNIX administrator if the package is not installed.

8. Extract the contents of the Oracle Financial Services Behavior Detection Applications Pack 8.1.2.0.0 installer archive file using the command: `unzip_<os> <name of the file to be unzipped>`.
9. Assign EXECUTE permission to the archive file OFS_BD_PACK as in the following sample command: `chmod -R 750 OFS_BD_PACK`.

10. Navigate to `installer/OFS_BD_PACK/OFS_AML/conf` and update `patchconfig.xml` and grant permission to the `.sh` files as described in [Table 10](#).

Table 10: Update patchconfig.xml

Placeholder Name	Significance and Expected Value	Mandatory
<code>##OFS_AML_SW_RMIPORT##</code>	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
<code>##OFS_AML_SAVE_METADATA#</code>	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
<code>##EXECUTE_PRE_AND_POST_SCRIPTS##</code>	This flag indicates if certain scripts need to be executed just before and just after the data model upload. Applicable value is 1.	Yes (Value = 0)
<code>##SCHEMA_OUT_XML_PATH##</code>	This attribute refers to the path, which needs to be pointed to <code>OFS_BD_SCHEMA_OUTPUT.xml</code> , which was generated at the time of installation. For example, <code>/scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml</code>	Yes
<code>##OFS_FCCM_LOADER_ROLE##</code>	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in <code>OFS_BD_SCHEMA_OUTPUT.xml</code> and is generated at the time of 8.1.1.0.0 Installation.	Yes
<code>##OFS_AML_ANALYST_DATA_SOURCE##</code>	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
<code>##OFS_AML_MINER_DATA_SOURCE##</code>	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
<code>##BASE_COUNTRY##</code>	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: <code>base_country=US</code> <code>base_country=US</code>	Yes
<code>##DEFAULT_JURISDICTION##</code>	Jurisdiction to assign the derived entities and derived addresses. For example: <code>default_jurisdiction=AMEA</code>	Yes
<code>##TNS_ADMIN##</code>	This attribute refers to the path where <code>TNSNAMES.ORA</code> is placed. For example, <code>/scratch/ofsaapp</code>	Yes
<code>##BIG_DATA_ENABLE##</code>	Placeholder to enable Big Data. Enter FALSE.	Yes

Table 10: Update patchconfig.xml

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL# #	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> • Initiate Onboarding Service (InitiateOnboardingService.war) • Table To JSON Service (TabletoJSONService.war) • JSON To Table Service (JSONToTablePersistenceUtility.war) • Common Gateway Service (CommonGatewayService.war) • Generate Case Input Service (GenerateCaseInputService.war) • Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATEWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATEWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.

Table 10: Update patchconfig.xml

Placeholder Name	Significance and Expected Value	Mandatory
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.

Table 10: Update patchconfig.xml

Placeholder Name	Significance and Expected Value	Mandatory
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/ CONTEXT_NAME> /questionnaire_api/questionnaires/resume/ <INFODOM>/ en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_ RESP_URL##.
##OFS_COMM_DATA_ TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_ COMM_DATA_ TBSP##.

11. Navigate to OFS_BD_PACK/bin and execute the command: `./setup.sh SILENT`.
12. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
13. After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.

14. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.

\$FIC_HOME/database/db_tools/bin

- ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
- ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfg

During installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:

```
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW  
FORCE AS OBJECT (
```

This issue is to be fixed in release 8.1.2.1 ML.

2. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin

List of scenarios to be loaded

- ML-CIBPreviousAverageActivity.116000083.xml
- ML-CashTransPossibleCTR.116000037.xml
- ML-DepWDSameAmts.118860020.xml
- ML-LargeReportableTrans.116000099.xml
- ML-RapidMvmtFundsAllActivity.116000079.xml
- ML-StructuringAvoidReportThreshold.116000046.xml
- ML-StructuringAvoidReportThreshold.116000062.xml

15. Verify if the release is applied successfully by checking the log file generated in the installation folder. You can ignore ORA-00001, ORA-00955, ORA-02260, and ORA-01430 errors in the log file. In case of any other errors, contact Oracle Support.

NOTE

- The DMT migration utility is executed during BD installation to migrate the DMT metadata (PLC/Data Source/Data Mapping/Data File Mapping) to be persisted in tables instead of XML. You may be required to re-run the DMT migration utility in some scenarios. To identify whether to run the utility, how to run, and how to handle migration issues, see OFSAA DMT Metadata Migration Guide.
- Ignore the below fatal error in the putty console while upgrading
Summary will be written to: ../log/
DMTMigrationUtilityReport.log
Detailed logs can be found in: ../log/
DMTMigrationUtility.log
FIC_HOME:/scratch/ofsaadb/BDECM811OCT/
[Fatal Error] ETLLoader.properties:2:1: Premature end of file.

16. For more information on securing your OFSAA Infrastructure, see the Security Guide in [OHC Library](#).
17. Add umask 0027 in the .profile of the UNIX account, which manages the WEB server to ensure restricted access permissions.
18. Restart all the OFSAAI services. For more information, see the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
19. 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 [Appendix D: Creating and Deploying EAR/WAR File](#).
20. Deploy the RPD and Catalog ORACLE ANALYTIC SERVER (OAS) 5.9 files available under \$FIC_HOME/ORACLE ANALYTIC SERVER (OAS) 5.9 folder.
21. For enabling TDE in case of a new installation, see the *Configuring TDE in case of Upgrade* section in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).
22. For enabling Data Redaction in case of a new installation, see the *Enabling Data Redaction in case of Upgrade* section in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

NOTE

To enable newly licensed app from OFSA BD Pack, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).

6.1.4.3 OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0

See the [OFS ECM Installation Guide 8.1.2.0.0](#) for Pack on Pack Inplace Upgrade steps from OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0.

6.1.4.4 OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0

See the [OFS CRR Installation Guide 8.1.2.0.0](#) for Pack on Pack Inplace Upgrade steps from OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0.

6.1.5 Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0

Performing Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0.0, OFS ECM 8.1.1.0.0 and OFS CRR 8.1.1.0.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0.

Prerequisites

- Perform Cloning as per the Cloning procedure. For more information, see [OFS Analytical Applications Infrastructure Cloning Reference Guide](#).
- See the [Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix](#) for preparing hardware and software requirements.

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- Ensure to take the backup of File System (FIC_HOME/FTP SHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that the dispatcher is not running. If the dispatcher is running, stop and then start the upgrading process.
- Ensure that you end all the batches before you start the upgrade process.
- Ensure that you run the END_MANTAS_BATCH before starting the upgrade. For enabling the unlimited Cryptographic Policy for Java, see [Enabling Unlimited Cryptographic Policy for Java](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing cloning upgrade.
- If the OFS Sanctions 8.0.8.0.0 is installed, then follow below steps:
 - create table KDD_BUS_DMN_SANC as (select * from KDD_BUS_DMN);
 - UPDATE KDD_BUS_DMN SET TF_BUS_DMN_NM=NULL; commit

Topics:

- [Pack on Pack Upgrade Sequence](#)
- [OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0](#)
- [OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0](#)
- [OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0](#)

6.1.5.1 Pack on Pack Upgrade Sequence

Use the following pack upgrade sequence:

- OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0
- OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0
- OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0

6.1.5.2 OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0

Follow these steps for OFS BD 8.1.1.0.0 to OFS BD 8.1.2.0.0:

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF, see [Configuring FSDF in Different Infodomain \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767866.

1. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0.
2. Login to the OFSAA Server with user credentials used to install OFSAA.
3. Shut down all the OFSAAI Services. For more information, see the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
4. Execute the command: `chmod -R 755 $FIC_HOME.`
5. If you have Unzip utility, skip to the next step. Download the Unzip utility (OS specific) and copy it in Binary mode to the directory that is included in your PATH variable, typically \$HOME path or directory in which you have copied the 8.1.1.0.0 installer.
6. Uncompress the unzip installer file using the command: `uncompress unzip_<os>.Z`

NOTE

In case you notice an error message “uncompress: not found [No such file or directory]” contact your UNIX administrator if the package is not installed.

7. Extract the contents of the Oracle Financial Services Behavior Detection Applications Pack 8.1.2.0.0 installer archive file using the command: `unzip_<os> <name of the file to be unzipped>`

Assign EXECUTE permission to the archive file OFS_BD_PACK as in the command: `chmod -R 755 OFS_BD_PACK.`

8. Update patchconfig.xml and grant permission to the .sh files as described in [Table 11](#):

Table 11: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.

Table 11: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL# #	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> Initiate Onboarding Service (InitiateOnboardingService.war) Table To JSON Service (TabletoJSONService.war) JSON To Table Service (JSONToTablePersistenceUtility.war) Common Gateway Service (CommonGatewayService.war) Generate Case Input Service (GenerateCaseInputService.war) Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.

Table 11: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.

Table 11: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME> /questionnaire_api/questionnaires/resume/<INFODOM>/ en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

9. Navigate to OFS_BD_PACK/bin and execute the command: `./setup.sh SILENT`.
10. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
11. After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.
12. If the release is applied successfully, check the log file generated by verifying in the installation folder. Ignore ORA-00001, ORA-00955, ORA-02260, and ORA-01430 errors in the log file. In case of any other errors, contact [My Oracle Support](#).

NOTE

- The DMT migration utility is executed during BD installation to migrate the DMT metadata (PLC/Data Source/Data Mapping/Data File Mapping) to be persisted in tables instead of XML. You may be required to re-run the DMT migration utility in some scenarios. To identify whether to run the utility, how to run, and how to handle migration issues, see OFSAA DMT Metadata Migration Guide.
- Ignore the below fatal error in the putty console while upgrading
Summary will be written to: ../log/DMTMigrationUtilityReport.log
Detailed logs can be found in: ../log/DMTMigrationUtility.log
FIC_HOME:/scratch/ofsaadb/BDECM811OCT/
[Fatal Error] ETLLoader.properties:2:1: Premature end of file.

13. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.
\$FIC_HOME/database/db_tools/bin
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfgDuring installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW
FORCE AS OBJECT (
This issue is to be fixed in release 8.1.2.1 ML.
2. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin.
List of scenarios to be loaded:
 - ML-CIBPreviousAverageActivity.116000083.xml
 - ML-CashTransPossibleCTR.116000037.xml
 - ML-DepWDSameAmts.118860020.xml
 - ML-LargeReportableTrans.116000099.xml
 - ML-RapidMvmtFundsAllActivity.116000079.xml
 - ML-StructuringAvoidReportThreshold.116000046.xml
 - ML-StructuringAvoidReportThreshold.116000062.xml

14. For more information on securing your OFSAA Infrastructure, see the Security Guide in [OHC Library](#).
15. Add umask 0027 in the .profile of the UNIX account, which manages the WEB server to ensure restricted access permissions.
16. Restart all the OFSAAI services. For more information, see the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
17. 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 [Appendix E: Starting/Stopping Infrastructure Services](#).
18. Deploy the RPD and Catalog ORACLE ANALYTIC SERVER (OAS) 5.9 files available under \$FIC_HOME/ORACLE ANALYTIC SERVER (OAS) 5.9 folder.
19. For enabling TDE in case of a new installation, see the *Configuring TDE in case of Upgrade* section in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).
20. For enabling Data Redaction in case of a new installation, see the *Enabling Data Redaction in case of Upgrade* section in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

NOTE

To enable newly licensed app from OFSA BD Pack, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).

6.1.5.3 OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0

See [OFS ECM Installation Guide 8.1.2.0.0](#) for Pack on Pack Cloning Upgrade steps from OFS ECM 8.1.1.0.0 to OFS ECM 8.1.2.0.0.

6.1.5.4 OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0

See [OFS CRR Installation Guide 8.1.2.0.0](#) for Pack on Pack cloning Upgrade steps from OFS CRR 8.1.1.0.0 to OFS CRR 8.1.2.0.0.

6.2 Upgrading from OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0

Topics:

- [Standalone Upgrade of OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0](#)
- [Cloning Upgrades of OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0](#)
- [Pack on Pack Inplace Upgrade from OFS BD 8.1.1.0, OFS ECM 8.1.1.0 and OFS CRR 8.1.1.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0.](#)
- [Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0, OFS ECM 8.1.1.0 OFS CRR 8.1.1.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0](#)

6.2.1 Standalone Upgrade of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0

Perform the Standalone Upgrade of OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0 via **In-Place Upgrade** and **Cloning Upgrade**.

NOTE

- Ensure to take the backup of File System (FIC_HOME and FTPSHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that you end all the batches before you start the upgrade process.
- For enabling the unlimited Cryptographic Policy for Java, see [Enabling Unlimited Cryptographic Policy for Java](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing Inplace upgrade.
- If CTR is not enabled in 8.1.1.0.0, 8.1.1.1.0 patch is applied. The below error can be ignored if it is observed.

Query:

```
insert into CSSMS_ROLE_FUNCTION_MAP  
(V_ROLE_CODE, V_FUNCTION_CODE)  
values ('CTRADMN', 'AMPASENCYT')
```

Error: ORA-02291: integrity constraint
(AK7_811CONF.FK_CSSMS_ROLE_FUNCTION_MAP_2)
violated - parent key not found.

6.2.1.1 In-Place Upgrade of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0

Perform the In-Place Upgrade of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0:

Prerequisites: For Inplace Upgrade, a minimum patch set level is required for performing OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0. See [Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix](#).

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF, see [Configuring FSDF in Different Infodom \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767914.

1. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0.
2. Navigate to OFS_BD_PACK and grant execute (755) permission for all executables \$ chmod 755 *.
3. Navigate to installer/OFS_BD_PACK/ conf and update OFS_BD_PACK.xml . Select the applications to enable. For more information, see [Configuring FSDF in Different Infodom \(Pack on Pack Installation\)](#).

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

4. Modify PatchConfig.xml parameters under OFS_BD_PACK/OFS_AML/conf/ PatchConfig.xml with appropriate values as described in [Table 12](#) .

Table 12: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes

Table 12: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL# #	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No

Table 12: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> Initiate Onboarding Service (InitiateOnboardingService.war) Table To JSON Service (TabletoJSONService.war) JSON To Table Service (JSONToTablePersistenceUtility.war) Common Gateway Service (CommonGatewayService.war) Generate Case Input Service (GenerateCaseInputService.war) Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATEWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATEWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.

Table 12: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.

Table 12: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME> /questionnaire_api/questionnaires/resume/<INFODOM>/en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

5. Navigate to the OFS_BD_PACK/bin folder and execute setup.sh file using the command: \$./ setup.sh SILENT.
6. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
7. After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.

8. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.
\$FIC_HOME/database/db_tools/bin
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfgDuring installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW
FORCE AS OBJECT (
This issue is to be fixed in release 8.1.2.1 ML.
2. To enable newly licensed app from OFSA BD Pack, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).
3. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin
List of scenarios to be loaded:
 - ML-CIBPreviousAverageActivity.116000083.xml
 - ML-CashTransPossibleCTR.116000037.xml
 - ML-DepWDSameAmts.118860020.xml
 - ML-LargeReportableTrans.116000099.xml
 - ML-RapidMvmtFundsAllActivity.116000079.xml
 - ML-StructuringAvoidReportThreshold.116000046.xml
 - ML-StructuringAvoidReportThreshold.116000062.xml

6.2.2 Cloning Upgrades of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0

Perform Cloning Upgrades of OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0:

NOTE

- Ensure to take the backup of File System (FIC_HOME and FTPSHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that you end all the batches before you start the upgrade process.
- For enabling the unlimited Cryptographic Policy for Java, see [Enabling Unlimited Cryptographic Policy for Java](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing cloning upgrade.
- If CTR is not enabled in 8.1.1.0.0, 8.1.1.1.0 patch is applied. The below error can be ignored if it is observed.

Query:

```
insert into CSSMS_ROLE_FUNCTION_MAP  
(V_ROLE_CODE, V_FUNCTION_CODE)  
values ('CTRADMN', 'AMPASENCYT')
```

Error: ORA-02291: integrity constraint
(AK7_811CONF.FK_CSSMS_ROLE_FUNCTION_MAP_2) violated -
parent key not found.

Prerequisites:

- Perform Cloning as per the Cloning procedure. For more information, see [OFS Analytical Applications Infrastructure Cloning Reference Guide](#).
- See the [Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix](#) for preparing hardware and software requirements.

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF, see [Configuring FSDF in Different Infodomain \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767914.

1. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0.
2. Navigate to OFS_BD_PACK and grant execute (755) permission for all executables \$ chmod 755 *.
3. Navigate to installer/OFS_BD_PACK/ conf and update OFS_BD_PACK.xml . Select the applications to enable. For more information, see [Configuring FSDF in Different Infodomain \(Pack on Pack Installation\)](#).

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

4. Modify PatchConfig.xml parameters under OFS_BD_PACK/OFS_AML/conf/ PatchConfig.xml with appropriate values as described in [Table 13](#)

Table 13: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)

Table 13: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.

Table 13: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##FSDF_UPLOAD_MODEL# #	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> • Initiate Onboarding Service (InitiateOnboardingService.war) • Table To JSON Service (TabletoJSONService.war) • JSON To Table Service (JSONToTablePersistenceUtility.war) • Common Gateway Service (CommonGatewayService.war) • Generate Case Input Service (GenerateCaseInputService.war) • Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATEWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATEWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.

Table 13: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME> /questionnaire_api/questionnaires/resume/ <INFODOM>/ en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.

Table 13: Modify PatchConfig.xml parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

5. Navigate to the OFS_BD_PACK/bin folder and execute the setup.sh file using the command: `$./setup.sh SILENT`.
6. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
7. After the installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.
8. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.
\$FIC_HOME/database/db_tools/bin
 - `./run_dbbuilder_utility.sh $FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg`
 - `./run_dbbuilder_utility.sh $FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfg`

During installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW
FORCE AS OBJECT (

This issue is to be fixed in release 8.1.2.1 ML.
2. To enable newly licensed app from OFSA BD Pack, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).
3. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin
List of scenarios to be loaded:
 - ML-CIBPreviousAverageActivity.116000083.xml
 - ML-CashTransPossibleCTR.116000037.xml
 - ML-DepWDSameAmts.118860020.xml
 - ML-LargeReportableTrans.116000099.xml
 - ML-RapidMvmtFundsAllActivity.116000079.xml
 - ML-StructuringAvoidReportThreshold.116000046.xml
 - ML-StructuringAvoidReportThreshold.116000062.xml

6.2.3 Pack on Pack Inplace Upgrade from OFS BD 8.1.1.1.0, OFS ECM 8.1.1.1.0 and OFS CRR 8.1.1.1.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0.

Topics:

- [Pack on Pack Upgrade Sequence](#)
- [OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0](#)
- [OFS ECM 8.1.1.1.0 to OFS ECM 8.1.2.0.0](#)
- [OFS CRR 8.1.1.1.0 to OFS CRR 8.1.2.0.0](#)

Performing Pack on Pack Inplace Upgrade from OFS BD 8.1.1.1.0, OFS ECM 8.1.1.1.0 and OFS CRR 8.1.1.1.0 to OFS BD 8.1.2.0.0, OFS ECM 8.1.2.0.0 and OFS CRR 8.1.2.0.0.

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- Ensure to take the backup of File System (FIC_HOME/FTP SHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that the dispatcher is not running. If the dispatcher is running, stop and then start the upgrading process.
- Ensure that you end all the batches before you start the upgrade process.
- Ensure that you run the END_MANTAS_BATCH before starting the upgrade. For enabling the unlimited Cryptographic Policy for Java, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing Inplace upgrade.
- If CTR is not enabled in 8.1.1.0.0, 8.1.1.1.0 patch is applied. The below error can be ignored if it is observed.

Query:

```
insert into CSSMS_ROLE_FUNCTION_MAP  
(V_ROLE_CODE, V_FUNCTION_CODE)  
values ('CTRADMN', 'AMPASENCYT')
```

Error: ORA-02291: integrity constraint
(AK7_811CONF.FK_CSSMS_ROLE_FUNCTION_MAP_2)
violated - parent key not found.

- If the OFS Sanctions 8.0.8.0.0 is installed, then follow below steps:
 - create table KDD_BUS_DMN_SANC as (select * from KDD_BUS_DMN);
 - UPDATE KDD_BUS_DMN SET TF_BUS_DMN_NM=NULL; commit

6.2.3.1 Pack on Pack Upgrade Sequence

Use the following pack upgrade sequence:

- OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0
- OFS ECM 8.1.1.1.0 to OFS ECM 8.1.2.0.0
- OFS CRR 8.1.1.1.0 to OFS CRR 8.1.2.0.0

6.2.3.2 OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0

Follow these steps to upgrade from OFS BD 8.1.1.1.0 to OFS BD 8.1.2.0.0.:

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF. See [Configuring FSDF in Different Infodomain \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767914.

1. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0.
2. Login to the OFSAA Server with user credentials used to install OFSAA.
3. Shut down all the OFSAAI Services. For more information, see the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
4. Execute the command: `chmod -R 755 $FIC_HOME`.
5. If you have Unzip utility, skip to the next step. Download the Unzip utility (OS specific) and copy it in Binary mode to the directory that is included in your PATH variable, typically \$HOME path or directory in which you have copied the 8.1.2.0.0 installer.
6. Uncompress the unzip installer file using the command: `uncompress unzip_<os>.Z`

NOTE

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

7. Extract the contents of the Oracle Financial Services Behavior Detection Applications Pack 8.1.2.0.0 installer archive file using the command: `unzip_<os> <name of the file to be unzipped>`.

Assign EXECUTE permission to the archive file OFS_BD_PACK as in the sample command:
`chmod -R 755 OFS_BD_PACK.`

8. Update patchconfig.xml and grant permission to the .sh files as described in [Table 14](#).

Table 14: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.

Table 14: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL# #	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> Initiate Onboarding Service (InitiateOnboardingService.war) Table To JSON Service (TabletoJSONService.war) JSON To Table Service (JSONToTablePersistenceUtility.war) Common Gateway Service (CommonGatewayService.war) Generate Case Input Service (GenerateCaseInputService.war) Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.

Table 14: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.

Table 14: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME> /questionnaire_api/questionnaires/resume/<INFODOM>/en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

9. Navigate to OFS_BD_PACK/bin and execute the command: `./setup.sh SILENT`.
10. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
11. After the patch installation is successful, execute the `BD_Duplicate_Jar_Removal.sh` script from \$FIC_HOME.

12. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.
\$FIC_HOME/database/db_tools/bin
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
 - ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfgDuring installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW
FORCE AS OBJECT (
This issue is to be fixed in release 8.1.2.1 ML.
2. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin
List of scenarios to be loaded:
 - ML-CIBPreviousAverageActivity.116000083.xml
 - ML-CashTransPossibleCTR.116000037.xml
 - ML-DepWDSameAmts.118860020.xml
 - ML-LargeReportableTrans.116000099.xml
 - ML-RapidMvmtFundsAllActivity.116000079.xml
 - ML-StructuringAvoidReportThreshold.116000046.xml
 - ML-StructuringAvoidReportThreshold.116000062.xml

13. Verify if the release is applied successfully by checking the log file generated in the installation folder. You can ignore ORA-00001, ORA-00955, ORA-02260, and ORA-01430 errors in the log file. In case of any other errors, contact Oracle Support.

NOTE

- The DMT migration utility is executed during BD installation to migrate the DMT metadata (PLC/Data Source/Data Mapping/Data File Mapping) to be persisted in tables instead of XML. You may be required to re-run the DMT migration utility in some scenarios. To identify whether to run the utility, how to run, and how to handle migration issues, see OFSAA DMT Metadata Migration Guide.
- Ignore the below fatal error in the putty console while upgrading and summary will be written to:
../log/DMTMigrationUtilityReport.log
Detailed logs can be found in: ../log/
DMTMigrationUtility.log
FIC_HOME:/scratch/ofsaadb/BDECM811OCT/
[Fatal Error] ETLLoader.properties:2:1: Premature end of file.

14. For more information on securing your OFSAA Infrastructure, see the *Security Guide* in [OHC Library](#).
15. Add umask 0027 in the .profile of the UNIX account, which manages the WEB server to ensure restricted access permissions.
16. Restart all the OFSAAI services. For more information, See the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
17. 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 [Appendix D: Creating and Deploying EAR/WAR File](#).
18. Deploy the RPD and Catalog ORACLE ANALYTIC SERVER (OAS) 5.9 files available under \$FIC_HOME/ORACLE ANALYTIC SERVER (OAS) 5.9 folder.
19. For enabling TDE in case of a new installation, see *Configuring TDE in case of Upgrade* in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).
20. For enabling Data Redaction in case of a new installation, see *Enabling Data Redaction and in case of Upgrade* in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

NOTE

To enable newly licensed app from OFSA BD Pack, see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).

6.2.3.3 OFS ECM 8.1.1.1.0 to OFS ECM 8.1.2.0.0

See [OFS ECM Installation Guide 8.1.2.0.0](#) for Pack on Pack Inplace Upgrade steps from OFS ECM 8.1.1.0 to OFS ECM 8.1.2.0.0.

6.2.3.4 OFS CRR 8.1.1.1.0 to OFS CRR 8.1.2.0.0

See [OFS CRR Installation Guide 8.1.2.0.0](#) for Pack on Pack Inplace Upgrade steps from OFS CRR 8.1.1.0 to OFS CRR 8.1.2.0.0.

6.2.4 Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0, OFS ECM 8.1.1.0 OFS CRR 8.1.1.0 to OFS BD 8.1.2.0, OFS ECM 8.1.2.0 and OFS CRR 8.1.2.0

Performing Pack on Pack Cloning Upgrade from OFS BD 8.1.1.0, OFS ECM 8.1.1.0 and OFS CRR 8.1.1.0 to OFS BD 8.1.2.0, OFS ECM 8.1.2.0 and OFS CRR 8.1.2.0.

Prerequisites

- Perform Cloning as per the Cloning procedure. For more information see, [OFS Analytical Applications Infrastructure Cloning Reference Guide](#).
- See the [Oracle Financial Services Analytical Applications 8.1.2.0 Technology Matrix](#) for preparing hardware and software requirements.

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- Ensure to take the backup of File System (FIC_HOME and FTPSHARE), Atomic schema, and Config schema before performing the upgrade.
- Ensure that the dispatcher is not running. If the dispatcher is running, stop and then start the upgrading process.
- Ensure that you end all the batches before you start the upgrade process.
- Ensure that you run the END_MANTAS_BATCH before starting the upgrade. For enabling the unlimited Cryptographic Policy for Java, see [Enabling Unlimited Cryptographic Policy for Java](#).
- ORACLE_HOME AND JAVA_HOME have to be updated under FIC_HOME SUB DIRECTORIES while performing cloning upgrade.
- If CTR is not enabled in 8.1.1.0, 8.1.1.0 patch is applied. The below error can be ignored if it is observed.

Query:

```
insert into CSSMS_ROLE_FUNCTION_MAP
(V_ROLE_CODE, V_FUNCTION_CODE)
values ('CTRADMN', 'AMPASENCYT')
```

Error: ORA-02291: integrity constraint (AK7_811CONF.FK_CSSMS_ROLE_FUNCTION_MAP_2) violated - parent key not found.

- If the OFS Sanctions 8.0.8.0 is installed, then follow these steps:
 - ```
create table KDD_BUS_DMN_SANC as (select
* from KDD_BUS_DMN);
```
  - ```
UPDATE KDD_BUS_DMN SET
TF_BUS_DMN_NM=NULL; commit
```


Topics:

- [Pack on Pack Upgrade Sequence](#)
- [OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0](#)
- [OFS ECM 8.1.1.0 to OFS ECM 8.1.2.0.0](#)
- [OFS CRR 8.1.1.0 to OFS CRR 8.1.2.0.0](#)

6.2.4.1 Pack on Pack Upgrade Sequence

Use the following pack upgrade sequence:

- OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0
- OFS ECM 8.1.1.0 to OFS ECM 8.1.2.0.0
- OFS CRR 8.1.1.0 to OFS CRR 8.1.2.0.0

6.2.4.2 OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0

Follow these steps for OFS BD 8.1.1.0 to OFS BD 8.1.2.0.0.

NOTE

- The archive files are different for every operating system like Solaris Sparc and RHEL/Oracle Linux.
- If user has different schema for FSDF. See [Configuring FSDF in Different Infodomain \(Pack on Pack Installation\)](#) before upgrading.
- Before upgrade take backup of all STG tables. Use the list of the [STG tables](#) (BD FSDF_OIDF Merged 81210 Staging Tables) and create SQL truncate script for truncating STG tables from BD atomic schema.
- The minimum BD patch level must be bug 33767914.

1. Download and unzip the OFS BD 8.1.2.0.0 Installer from [My Oracle Support](#) by using the bug 33940349 - OFS BD APPLICATION PACK - 8.1.2.0.0. Login to the OFSAA Server with user credentials used to install OFSAA.
2. Shut down all the OFSAAI Services. For more information, see *Start/Stop Infrastructure Services* in [Appendix E: Starting/Stopping Infrastructure Services](#).
3. Execute the command: `chmod -R 755 $FIC_HOME`.
4. If you have Unzip utility, skip to the next step. Download the Unzip utility (OS specific) and copy it in Binary mode to the directory that is included in your PATH variable, typically \$HOME path or directory in which you have copied the 8.1.1.0.0 installer.
5. Uncompress the unzip installer file using the command: `uncompress unzip_<os>.Z`.

NOTE

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

6. Extract the contents of the Oracle Financial Services Behavior Detection Applications Pack 8.1.2.0.0 installer archive file using the command: `unzip_<os> <name of the file to be unzipped>`.

7. Assign EXECUTE permission to the archive file OFS_BD_PACK as in the sample command:
`chmod -R 755 OFS_BD_PACK.`
8. Update patchconfig.xml and grant permission to the .sh files as described in [Table 15](#).

Table 15: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SW_RMIPORT##	The Scenario Wizard uses this attribute. It must consist of a proper port number and not be used by any other application. For example, 7623 or 8204.	Yes
##OFS_AML_SAVE_METADATA#	The installer to decide whether to execute hierarchy Resave uses this attribute. The applicable value is ALL.	Yes
##EXECUTE_PRE_AND_POST_SCRIPTS##	This flag indicates if certain scripts need to be executed just before and just after the data model upload Applicable value is 1.	Yes (Value = 0)
##SCHEMA_OUT_XML_PATH##	This attribute refers to the path, which needs to be pointed to OFS_BD_SCHEMA_OUTPUT.xml, which was generated at the time of installation. For example, /scratch/ofsaapp/Installer/OFS_BD_PACK/schema_creator/OFS_BD_SCHEMA_OUTPUT.xml	Yes
##OFS_FCCM_LOADER_ROLE##	This attribute role is used when OFS BD 8.0.1.0.0/8.0.4.0.0 is installed. The value will be available in OFS_BD_SCHEMA_OUTPUT.xml and is generated at the time of 8.1.1.0.0 Installation.	Yes
##OFS_AML_ANALYST_DATA_SOURCE##	Name of the Analyst Data source used for Admin Tools Configurations. For example: Create a data source with name ANALYST	Yes
##OFS_AML_MINER_DATA_SOURCE##	Name of the Miner Data source used for Admin Tools Configurations For example: Create a data source with name MINER	Yes
##BASE_COUNTRY##	ISO country code to use during data ingestion to record Institution-derived geography risk on parties on transactions that are internal to the OFSBD client. For example: base_country=US base_country=US	Yes
##DEFAULT_JURISDICTION##	Jurisdiction to assign the derived entities and derived addresses. For example: default_jurisdiction=AMEA	Yes
##TNS_ADMIN##	This attribute refers to the path where TNSNAMES.ORA is placed. For example, /scratch/ofsaapp	Yes
##BIG_DATA_ENABLE##	Placeholder to enable Big Data. Enter FALSE.	Yes
##OFS_AML_SQOOP_WORKING_DIR##	Placeholder to provide SQOOP working directory for AML	Mandatory only if big data is enabled.

Table 15: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##OFS_AML_SSH_AUTH_ALIAS##	Placeholder to provide SSH authorization alias for AML	Mandatory only if big data is enabled.
##OFS_AML_SSH_HOST_NAME##	Placeholder to provide SSH host name for AML.	Mandatory only if big data is enabled.
##OFS_AML_SSH_PORT##	Placeholder to provide SSH port name for AML.	Mandatory only if big data is enabled.
##FSDF_UPLOAD_MODEL# #	This flag indicates whether the FSDF data model has to be executed or not. If the user wants to upload FSDF data model, the user must enter the value as 1 or enter the value as 0.	No
<p>Note:</p> <p>KYC Onboarding requires additional deployments of the following:</p> <ul style="list-style-type: none"> Initiate Onboarding Service (InitiateOnboardingService.war) Table To JSON Service (TabletoJSONService.war) JSON To Table Service (JSONToTablePersistenceUtility.war) Common Gateway Service (CommonGatewayService.war) Generate Case Input Service (GenerateCaseInputService.war) Create JSON Service (createJSONService.war) <p>The above .war files are available in the <code>FIC_HOME</code> path post-installation. For information on deploying the .war files, see Post Installation Configuration. These deployments are in addition to the Application Pack deployment, that is, OFSBD, Watch list Service deployment and RAOR deployments which are mandatory for KYC onboarding.</p> <p>For information on the services, see Know Your Customer Service Guide.</p> <p>The following parameters are applicable for KYC Onboarding:</p>		
##OBDATASRCNAME# #	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be OBDATASRCNAME.
##COMN_GATWAY_DS##	This is the name of the datasource pointing to the atomic schema.	Mandatory only if KYC onboarding is used. If not, value must be COMN_GATWAY_DS.
##AAI_AUTH_URL##	This is the URL of the BD application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be AAI_URL.

Table 15: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##TABLE_TO_JSON_PROTOCOL_SERVER_PORT##	This is the URL of Table To JSON Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be T2J_URL.
##JSON_TO_TABLE_PROTOCOL_SERVER_PORT##	This is the URL of JSON To Table Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be J2T_URL.
##OB_PROTOCOL_SERVER_PORT##	This is the URL of Initiate onboarding service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OB_URL.
##ECM_APP_URL##	This is the URL of the ECM application till the context name. For example, <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.	Mandatory only if KYC onboarding is used. If not, value must be ECM_CASE_URL.
##CASE_INPUT_PROTOCOL_SERVER_PORT##	This is the URL of the Generate Case Input Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be GCI_URL.
##COMMON_GATEWAY_PROTOCOL_SERVER_PORT##	This is the URL of the Common Gateway Service till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CMNGTWYURL.
##SCORING_PROTOCOL_SERVER_PORT##	This is the URL of the RAOR Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be SCORING_URL.
##OFSS_WLS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Watch list application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be OFSS_WLS_URL.
##CS_PROTOCOL_SERVER_PORT##	This is the URL of the OFS Customer Screening Application till the port number. For example, <PROTOCOL:/HOSTNAME:PORT>.	Mandatory only if KYC onboarding is used. If not, value must be CS_URL.
##COMM_LOG_PATH##	This is the path of the KYC onboarding log file. For example, /scratch/ofsaapp/KYC808DEV/apache-tomcat-8.0.47/logs.	Mandatory only if KYC onboarding is used.

Table 15: PatchConfig.xml Parameters

Placeholder Name	Significance and Expected Value	Mandatory
##QTNR_RESP_URL##	This is the URL of the OFS KYC onboarding service , The URL is <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME> /questionnaire_api/questionnaires/resume/<INFODOM>/en_US?appCode=OFS_KYC.	Mandatory only if KYC onboarding is used. If not, value must be ##QTNR_RESP_URL##.
##OFS_COMM_DATA_TBSP##	This is the table space for the common gateway. The value is COMM_DATA_TBSP.	Mandatory only if KYC onboarding is used. If not, value must be ##OFS_COMM_DATA_TBSP##.

9. Navigate to OFS_BD_PACK/bin and Execute the following command: `./setup.sh SILENT`.
10. After Installation is successful, apply AAI patch by downloading the bug 33738222 from [My Oracle Support](#).
11. After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.

12. Entry (DBNAME of Atomic Schema) must be added in the tnsnames.ora file on the OFSAA server.

NOTE

1. After Upgrade Run below scripts manually as a post upgrade steps.

\$FIC_HOME/database/db_tools/bin

- ./run_dbbuilder_utility.sh \$FIC_HOME/database/ mantas_schema/delta/oracle/8.0/mantas8.1.2.0.0_delta.cfg
- ./run_dbbuilder_utility.sh \$FIC_HOME/database/ bus_mkt_schema/delta/oracle/8.0/delta_plat8.1.2.0.0.cfg

During installation, the PR_8.1.2.0.0_33645879.miner.sql script can fail with error code ORA-02303. This issue can be resolved by adding keyword FORCE to following string:

```
CREATE OR REPLACE TYPE DEPWD_SAMT_EN_ROW  
FORCE AS OBJECT (
```

This issue is to be fixed in release 8.1.2.1 ML.

2. Load the below scenarios manually using the sm_load utility available at: \$FIC_HOME/database/db_tools/bin

List of scenarios to be loaded:

- ML-CIBPreviousAverageActivity.116000083.xml
- ML-CashTransPossibleCTR.116000037.xml
- ML-DepWDSameAmts.118860020.xml
- ML-LargeReportableTrans.116000099.xml
- ML-RapidMvmtFundsAllActivity.116000079.xml
- ML-StructuringAvoidReportThreshold.116000046.xml
- ML-StructuringAvoidReportThreshold.116000062.xml
- ML-RoutingMultiLocations.118860012.xml (Before loading and executing the scenario, add it to the scnro.cfg file)

13. Verify if the release is applied successfully by checking the log file generated in the installation folder. You can ignore ORA-00001, ORA-00955, ORA-02260, and ORA-01430 errors in the log file. In case of any other errors, contact Oracle Support.

NOTE

- The DMT migration utility is executed during BD installation to migrate the DMT metadata (PLC/Data Source/Data Mapping/Data File Mapping) to be persisted in tables instead of XML. You may be required to re-run the DMT migration utility in some scenarios. To identify whether to run the utility, how to run, and how to handle migration issues, see OFSAA DMT Metadata Migration Guide.
- Ignore the below fatal error in the putty console while upgrading
Summary will be written to: ../log/
DMTMigrationUtilityReport.log
Detailed logs can be found in: ../log/
DMTMigrationUtility.log
FIC_HOME:/scratch/ofsaadb/BDECM811OCT/
[Fatal Error] ETLLoader.properties:2:1: Premature end of file.

14. For more information on securing your OFSAA Infrastructure, see the *Security Guide* in [OHC Library](#).
15. Add umask 0027 in the .profile of the UNIX account, which manages the WEB server to ensure restricted access permissions.
16. Restart all the OFSAAI services. For more information, see *Start/Stop Infrastructure Services* in [Appendix E: Starting/Stopping Infrastructure Services](#).
17. 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 [Appendix D: Creating and Deploying EAR/WAR File](#).
18. Deploy the RPD and Catalog ORACLE ANALYTIC SERVER (OAS) 5.9 files available under \$FIC_HOME/ORACLE ANALYTIC SERVER (OAS) 5.9 folder.
19. For enabling TDE in case of a new installation, see *Configuring TDE in case of Upgrade* in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).
20. For enabling Data Redaction in case of a new installation, see *Enabling Data Redaction in case of Upgrade* in [Appendix R: Configuring TDE and Data Redaction in OFSAA](#).

NOTE

To enable newly licensed app from OFS BD Pack , see [Enabling Newly Licensed App after Upgrade to BD 8.1.2.0.0](#).

6.2.4.3 OFS ECM 8.1.1.1.0 to OFS ECM 8.1.2.0.0

See [OFS ECM Installation Guide 8.1.2.0.0](#) for Pack on Pack Cloning Upgrade steps from OFS ECM 8.1.1.1.0 to OFS ECM 8.1.2.0.0.

6.2.4.4 OFS CRR 8.1.1.1.0 to OFS CRR 8.1.2.0.0

See [OFS CRR Installation Guide 8.1.2.0.0](#) for Pack on Pack Cloning Upgrade steps from OFS CRR 8.1.1.1.0 to OFS CRR 8.1.2.0.0.

6.3 How to Enable Newly Licensed App after Upgrade to BD 8.1.2.0.0

To enable newly licensed App after upgrade to BD 8.1.2.0.0 follow these steps:

1. Place the OFS_BD_SCHEMA_OUTPUT.xml file from previous installer to the current BD812 installer path <OFS_BD_PACK>/schema_creator.
2. Copy the content of default.properties_bkp file from <OFS_BD_PACK>/OFS_AML/conf path to the app specific folder which is newly enabled.
Example: - > If you are enabling OFS_KYC for the first time, copy the content to default.properties file in <OFS_BD_PACK>/OFS_KYC/conf path.
3. In the app specific default.properties file, enter the details mentioned in the tags (<!-- Start: User input required for silent installer.
--> and <!-- End: User input required for silent installer. -->).
4. Replace the below parameter values in default.properties file with the values available in the previous installer file path <OFS_BD_PACK>/OFS_AML/conf/default.properties
 - FCCM_USER=##OFS_AML_ATOMIC_USER##
 - FCCM_PASSWORD=##OFS_AML_ATOMIC_PW##
 - FCCMINFODOM=##OFS_AML_INFODOM_NAME##
 - FCCM_DBNAME=##OFS_AML_INFDBNAME##
 - FCCMINFODOM_DESCRIPTION=##OFS_AML_INFODOM_DESC##
5. Go to <OFS_BD_PACK>/conf folder. Enable the newly licensed app in the [Configuring OFS_BD_PACK.xml File](#) file by setting ENABLE flag to "YES".
Example:-> <APP_ID PREREQ="OFS_AAI" ENABLE="YES">OFS_KYC</APP_ID>

NOTE

Enter **YES** in **ENABLE** tag to enable applications which has been installed and Enter NO in the remaining applications.

6. Go to <OFS_BD_PACK>/bin folder and trigger the setup.sh.

NOTE

Please make sure there are no leading/trailing spaces in the <JDBC_URL> inside OFS_BD_SCHEMA_OUTPUT.xml file.

7

Post Installation Configuration

On successful installation of the Oracle Financial Services Behavior Detection Application Pack, see the following post installation topics.

Topics:

- [Creating and Deploying the Applications Pack Web Archive](#)
- [KYC Onboarding Services Deployment](#)
- [Installing Scenario Manager](#)
- [Copying KEYTAB and KRB5 Files in OFSAAI](#)
- [Deploying Analytic Reports and Threshold Analyzer](#)
- [Post Installation Steps](#)
- [Accessing Reports through OFS BD Application](#)
- [Installing RAOR Service](#)
- [Creating RAOR.ear/ RAOR.war](#)
- [Deploying RAOR.ear in WebLogic](#)
- [Installing RAOR.ear in WebLogic using WebLogic Administrator Console](#)
- [Deploying RAOR.ear in WebSphere](#)
- [Deploying RAOR.war in Tomcat](#)
- [Configuring Resource Reference](#)
- [Configuring Web Application Server](#)
- [Configurations for Java 8](#)
- [Enabling Unlimited Cryptographic Policy for Java](#)
- [Configurations for Oracle 19c Database](#)
- [Configuring FSDF](#)
- [Configurations for ECM Integration \(Applicable only for Promote to Case Action in KYC](#)

NOTE

- Ensure to clear the application cache prior to the deployment of Applications Pack Web Archive. This is applicable to all Web servers (WebSphere, WebLogic, and Tomcat). For more information, see [Clearing Application Cache](#).
- OFS BD 81210 ML is a mandatory patch to be applied. For more information, see [OFSBD installation Guide 8.1.2.1.0](#).

7.1 Creating and Deploying the Applications Pack Web Archive

NOTE Remove the existing Admin Tools deployment (which is integrated with OFS BD pack), if you are upgrading from v8.0.2.0.0 or lower versions.

Topics:

- [OFSBD Application Pack Deployment](#)
- [Scenario Wizard Configuration and Deployment](#)
- [Services Configuration and Deployment](#)

7.1.1 OFSBD Application Pack Deployment

To create and deploy the Applications Pack web archive, follow these steps:

1. Navigate to the \$FIC_WEB_HOME directory.
2. Execute the command: `./ant.sh`.
3. This will trigger the creation of EAR/WAR file - <contextname>.<extn>. Here <contextname> is the context name given during installation.

NOTE Creating ear/war files are done by the installer automatically. If the files are not created, user can execute these steps.

4. On completion of the EAR/WAR files creation, the "BUILD SUCCESSFUL" and "Time Taken" message is displayed and you are returned to the prompt.
5. The EAR/WAR file - <contextname>.<extn> - is created under "\$FIC_WEB_HOME" directory.

NOTE This process overwrites any existing version of EAR/WAR file in the path. If the web application server is Apache Tomcat, the file created would be <contextname>.war.

6. Deploy the generated EAR/WAR file on to the web application server. For more information, see [Deploying EAR/WAR File](#).

7.1.2 Scenario Wizard Configuration and Deployment

The Scenario Wizard Configuration and Deployment must be performed if the following applications are installed.:

NOTE

- Deployment is required only if you use Scenario Wizard.
- Since the Scenario Wizard is a developer tool, it will not work in a Load Balance environment, and does not need to be deployed in a production environment.

- AML
- FR

- Trade Compliance
- Broker Compliance
- Fraud-EE
- ECTC
- TB

To configure and deploy Scenario Wizard, follow these steps:

1. Navigate to `$FIC_HOME/ficweb/SCENARIO_WIZARD`.
2. Update the `install.properties` file for the below parameter, if those parameter values are not mentioned in the file.

NOTE

In case of the wallet setup, the automated configured value `smlite.db.url=jdbc:oracle:thin:@CONFIG` in `install.properties` file need to be manually changed to JDBC URL value (`jdbc:oracle:thin:@Hostname:port:SID/Service Name`).

```
smlite.db.host=##HOSTNAME##  
smlite.db.port=##PORT##  
smlite.db.sid=##SID##  
smlite.db.url=##URL##
```

```
ws.app.rmiport= ##RMI_PORT##
```

#Provide the deployment Path for Scenario Wizard

```
ws.sw.deploy.path=##DEPLOYED_PATH## /SMLiteWeb
```

3. Execute `./install.sh`. When prompted for password, enter the KDD MNR Schema password.
4. Deploy the `<context-name>.war` file (for example, `SMLiteWeb.war`) available at `$FIC_HOME/ficweb/SCENARIO_WIZARD` as an application on your Web application server. While deploying war file, keep context name as `SMLiteWeb`.

NOTE

Only one instance of Scenario Wizard will run on one Application server at a time. While launching the Scenario Wizard if you find any exception pop-up saying `java.rmi.bind` exception or `java.rmi.unknownhost` exception, follow these steps:

1. Stop the `SMLiteWeb.war`
2. Navigate to `<deployed area>SMLiteWeb\WEB-INF\classes\conf\mantas_cfg\install.cfg`.
3. In `install.cfg`, change the token to some other port, which is not occupied.
4. Define `rmiPort`. By default keep it 1099 `rmiPort=1099`
5. Restart the server.

5. Log Details:
 - a. Log file name- `smlite.log`.
 - b. Log path - Navigate to `<deployed area>SMLiteWeb\WEB-INF\classes\logs\smlite.log`.
6. To customize the Log path/log file name, follow these steps:
 - a. Go to `<deployed area>\SMLiteWeb\WEB-INF\classes\log4j.properties` file.

- b. Change the value of the property `log4j.appender.file.File="Your log file path"`.
- c. Restart the `SMLiteWeb.war` file.

To configure and deploy Scenario Wizard on Weblogic:

1. Navigate to the `domain/bin` folder.
2. Add the following two lines into file `setDomainEnv.sh`.
 - `FIC_HOME = "##DEPLOYED_AREA##/ SMLiteWeb.`
 - `export FIC_HOME.`

To configure and deploy Scenario Wizard on WebSphere, follow these steps:

1. Ensure that port 1099 is free and available.
2. Create a folder named `SMLiteWeb.ear` in the deploy path.
3. In the `Install.properties` file, under the `ws.sw.deploy.path` enter:

```
##Deployment_path##/SMLiteWeb.ear/SMLiteWeb.war. For example: /scratch/  
IBM/WebSphere/AppServer/profiles/BECS8124WS/installedApps/ofss-mum  
-889-Node3-Cell108/SMLiteWeb.ear/SMLiteWeb.war
```
4. Generate the `SMLiteWeb.war` file and place this file in the `SMLiteWeb.ear` directory in the deploy path.
5. Navigate to Servers à Server Types à WebSphere Application servers à Choose your server.
6. Navigate to your chosen server à Server Infrastructure à Java and Process Management à Class Loader.
7. Add new class loader and select *Classes loaded with local class loader first (parent last)*.
8. Navigate to your chosen server à Server Infrastructure à Java and Process Management à Process Definition à Environment Entries.
9. Add `FIC_HOME` as Name and `##Deployment_path##/SMLiteWeb.ear/SMLiteWeb.war` as value.
10. Navigate to Applications → Application Types → WebSphere Enterprise Applications → Install and choose the `SMLiteWeb.war` from specified path.
11. During installation, for Map context roots for web modules choose the values as `/SMLiteWeb`.
12. Navigate to Applications à Application Types à WebSphere Enterprise Applications à SMLiteWeb.
13. Click on SMLiteWeb à References à shared Library References à choose application SMLiteWeb.
14. Add the share libraries by going into Reference shared Libraries à move the available libraries to selected (For example: JERSEY2X).
15. Navigate to Applications à Application Types à WebSphere Enterprise Applications à SMLiteWeb.
16. Click on SMLiteWeb à References à shared Library References à choose Module Apache-Axis.
17. Add the share libraries by going into Reference shared Libraries à move the available libraries to selected (For example: JERSEY2X).
18. Start the application. If the application is not accessible, stop and start the application again from the websphere console.

19. If the Scenario Wizard is not accessible, restart the web and app server and start the application.

NOTE

See [Post Deployment Configuration](#) for more details.

For Front-end access, the following settings must be changed on the client side for the Scenario Wizard to work on Windows XP/Windows 7.

1. Navigate to Java Control Panel.
2. Under the General tab ensure the following two settings:
 - Navigate to Network Settings and change the Network Proxy Settings to Direct Connection.
 - Navigate to Settings under Temporary Internet Files and Follow these steps:
 - Check the option to keep temporary files on my computer.
 - For Scenario wizard, in WebSphere, the Java version must be the same in App and Web Server.

20. Click Delete Files to clear the Java cache.

21. To configure Scenario Wizard on Tomcat 8 and above before deploying the warfile, follow these steps:

- a. Remove the following text from context.xml at <deployed area>/conf/:
AbandonedOnBorrow="true"
- b. AbandonedOnMaintenance="true" AbandonedTimeout="60" logAbandoned="true"/>
- c. Replace with the text: maxTotal="100" maxIdle="30" maxWaitMillis="10000"/>
- d. All resources have been moved to Context.xml from server.xml.
- e. Change the following text:

```
<Context path =  
  
/admin_tools" docBase="<deployed_area>/webapps admin_tools" debug="0"  
reloadable="true" crossContext="true">  
  
to <Context>
```

7.1.3 Services Configuration and Deployment

You must configure and deploy Services if the following applications are installed:

- AML
- FR
- Trader Compliance
- Broker Compliance
- ECTC
- Fraud-EE
- TB

- KYC

NOTE JDK is required for creation of Watchlist WAR and can be removed once services deployment is successful.

7.1.3.1 Watchlist Service Deployment

To configure and deploy Services, follow these steps:

1. Create the WAR file by changing to the FIC_HOME/ingestion_manager/scripts directory and executing createWatchListWAR.sh. This will create the mantas.war file which contains the watch list service.
2. Deploy the mantas.war file to the web application server. Any context path can be used, but the KYC application expects it to be at /mantas. The full path leading to the exploded WAR file will be referred to as <Service Deployed Directory> below.
3. Modify the following file: <Service Deployed Directory>/WEB-INF/fuzzy_match/mantas_cfg/install.cfg and change the path in the fuzzy_name.B.stopword_file and fuzzy_name.P.stopword_file properties from: <FIC_HOME>/ingestion_manager to: <Service Deployed Directory>/WEB-INF
4. Modify the following file: <Service Deployed
5. Directory>/WEB-INF/config/install.cfg and change the Creating and Deploying the Applications Pack Web Archive Post Installation Configuration path in the log.message.library,log.categories.file.path, and log4j.config.file properties as specified in step 3.

For WebLogic:

Copy the following contents into setDomainEnv.sh located under \$WL_HOME/user_projects/domains/<user_domain>/bin/setDomainEnv.sh after replacing the place holders - <WATCHLIST_DEPLOYED_AREA> and <ORACLE_HOME>:

```
FIC_HOME=<WATCHLIST_DEPLOYED_AREA> ORACLE_HOME=<ORACLE_HOME>
export FIC_HOME export ORACLE_HOME
KDD_PRODUCT_HOME=${FIC_HOME}/WEB-INF/fuzzy_match export KDD_PRODUCT_HOME
JAVA_LIB_HOME=${KDD_PRODUCT_HOME}/lib/kddcore.jar:${KDD_PRODUCT_HOME}/
lib/log4j-1.2.12.jar
export JAVA_LIB_HOME
LD_LIBRARY_PATH=${KDD_PRODUCT_HOME}/lib:${ORACLE_HOME}/
lib:${LD_LIBRARY_PATH}
export LD_LIBRARY_PATH
```

For Tomcat:

Create file setenv.sh under <TOMCAT_INSTALLED_AREA>/bin/ and copy the following contents after replacing the place holders - <WATCHLIST_DEPLOYED_AREA> and <ORACLE_HOME>:

```
FIC_HOME=<WATCHLIST_DEPLOYED_AREA> ORACLE_HOME=<ORACLE_HOME>
export FIC_HOME export ORACLE_HOME
KDD_PRODUCT_HOME=${FIC_HOME}/WEB-INF/fuzzy_match export KDD_PRODUCT_HOME
JAVA_LIB_HOME=${KDD_PRODUCT_HOME}/lib/kddcore.jar:${KDD_PRODUCT_HOME}/
lib/log4j-1.2.12.jar
```

```
export JAVA_LIB_HOME
LD_LIBRARY_PATH=${KDD_PRODUCT_HOME}/lib:${ORACLE_HOME}/
lib:${LD_LIBRARY_PATH}
export LD_LIBRARY_PATH
```

For WebSphere:

Copy the following contents into the .profile file (Create a .profile file if it is not already existing) of the user after replacing the place holders - <WATCHLIST_DEPLOYED_AREA> and <ORACLE_HOME>:

```
FIC_HOME=<WATCHLIST_DEPLOYED_AREA> ORACLE_HOME=<ORACLE_HOME>
export FIC_HOME export ORACLE_HOME
KDD_PRODUCT_HOME=${FIC_HOME}/WEB-INF/fuzzy_match export KDD_PRODUCT_HOME
JAVA_LIB_HOME=${KDD_PRODUCT_HOME}/lib/kddcore.jar:${KDD_PRODUCT_HOME}/
lib/log4j-1.2.12.jar
export JAVA_LIB_HOME
LD_LIBRARY_PATH=${KDD_PRODUCT_HOME}/lib:${ORACLE_HOME}/
lib:${LD_LIBRARY_PATH}
export LD_LIBRARY_PATH
```

- Restart the web application server.

NOTE

Update the proper LD_LIBRARY_PATH based on your OS:

- **For Linux:**

```
export LD_LIBRARY_PATH=$KDD_PRODUCT_HOME/
lib:${ORACLE_HOME}/lib:${LD_LIBRARY_PATH}
```

- **For Solaris SPARC:**

```
export LD_LIBRARY_PATH=/usr/lib/
lwp:${KDD_PRODUCT_HOME}/lib:${ORACLE_HOME}/
lib:/usr/ucblib/sparcv9:/scratch/JAVA_7/
jdk1.7.0_75/jre/lib/sparcv9/server:/
scratch/JAVA_7/jdk1.7.0_75/jre/lib/
sparcv9:/scratch/JAVA_7/jdk1.7.0_75/jre/
lib/sparcv9/native_threads:/usr/local/lib/
sparcv9:/scratch/JAVA_7/jdk1.7.0_75/jre/
lib:${LD_LIBRARY_PATH}
```

7.2 KYC Onboarding Services Deployment

The following WARs need to be deployed if KYC Onboarding is Installed:

- Initiate Onboarding Service (InitiateOnboardingService.war)
- Table To JSON Service (TabletoJSONService.war)
- JSON To Table Service (JSONToTablePersistenceUtility.war)
- Common Gateway Service (CommonGatewayService.war)
- Generate Case Input Service (GenerateCaseInputService.war)

- Create JSON Service (createJSONService.war)

For Tomcat and WebLogic:

1. Navigate to \$FIC_HOME/Onboarding.
2. Deploy the following files to the web application server.
 - a. InitiateOnboardingService.war.
 - b. TabletoJSONService.war.
 - c. JSONToTablePersistenceUtility.war.
 - d. GenerateCaseInputService.war.
3. Navigate to \$FIC_HOME/CommonGateway.
4. Deploy the following files to the web application server.
 - a. CommonGatewayService.war.
 - b. createJSONService.war.

For Websphere:

From [Table 16](#) , remove all jar files mentioned in the Jar Names column from all paths mentioned in the From Path column:

Table 16: Jar Files to Remove and Corresponding Path Names

Jar Files	Path Names
hk2-api-2.5.0-b30.jar	\$FIC_HOME/Onboarding/InitiateOnboardingService/WEB-INF/lib
hk2-locator-2.5.0-b30.jar	\$FIC_HOME/Onboarding/JSONToTablePersistenceUtility/WEB-INF/lib
hk2-utils-2.5.0-b30.jar	\$FIC_HOME/Onboarding/GenerateCaseInputService/WEB-INF/lib
jackson-annotations-2.4.3.jar	\$FIC_HOME/CommonGateway/TabletoJSONService/WEB-INF/lib
jackson-core-2.4.3.jar file	\$FIC_HOME/CommonGateway/TabletoJSONService/WEB-INF/lib
jackson-databind-2.4.3.jar	
javax.inject-2.5.0-b30.jar	
jersey-client.jar	
jersey-common.jar	
jersey-container-servlet-core.jar	
jersey-guava-2.25.jar	
jersey-server.jar	
validation-api-1.1.0.Final.jar	

After removing the jar files, follow these steps:

1. Execute the ant.sh from \$FIC_HOME/Onboarding to re-create the following war files:
 - a. InitiateOnboardingService.war
 - b. TabletoJSONService.war
 - c. JSONToTablePersistenceUtility.war
 - d. GenerateCaselInputService.war
2. Execute the ant.sh from \$FIC_HOME/CommonGateway to re-create the following war files:
 - a. CommonGatewayService.war
 - b. createJSONService.war
3. Navigate to \$FIC_HOME/Onboarding.
4. Deploy the following files to the web application server:
 - a. InitiateOnboardingService.war
The context name for the war file must be InitiateOnboardingService.
 - b. TabletoJSONService.war
The context name for the war file must be TabletoJSONService.
 - c. JSONToTablePersistenceUtility.war
The context name for the war file must be JSONToTablePersistenceUtility.
 - d. GenerateCaselInputService.war
The context name for the war file must be GenerateCaselInputService.
5. Navigate to \$FIC_HOME/CommonGateway.
6. Deploy the following files to the web application server:
 - a. CommonGatewayService.war
The context name for the war file must be CommonGatewayService.
 - b. createJSONService.war
The context name for the war file must be createJSONService.

7.2.1 Updating User ID and Passwords for KYC Onboarding Services in PMF

KYC Onboarding uses the Process Modelling Framework (PMF) to orchestrate the onboarding workflow. PMF is configured to invoke the services/APIs for the KYC Onboarding.

The service URLs are pre-populated during the installation process, and the content is read from the InstallConfig.xml file.

NOTE

If the deployment URL is not mentioned during the installation process or the deployment URL has changed after installation, you must update the URL through the Process Modeller UI in PMF.

To update the user names and passwords, follow these steps:

1. Navigate to FIC_HOME/ficdb/bin and open the UpdateKYCOBUserPassCodes.sh file in edit mode.

2. Update the dburl value. This must point to the OFS BD database. Format of dburl is as follows:
jdbc:oracle:thin:@<Server>:<port>:<SID>
3. Save and close the file.
4. Execute the UpdateKYCOBUserPassCodes.sh file.
5. Select option 1 if you are using OFS Customer Screening for Watchlist and do the following:
 - a. Enter the OFS Customer Screening Watch list service user name and password.
 - b. Enter the OFS BD Config Schema user name and password.
This will save the user name and password for the OFS customer Screening Watch list service.
6. Select option 2 for all KYC Onboarding services and do the following:
 - a. Enter the KYC Administrator user name and password.
 - b. Enter the OFS BD Config Schema user name and password.
This will save the user name and password for all KYC Onboarding services.
7. Select option 3 for the OFS ECM Real-time Case Create Service:
 - a. Enter the ECM Administrator user name and password.
 - b. Enter the OFS BD Config Schema user name and password.
This will save the user name and password for OFS ECM Real-time Case Create Service.

7.3 Installing Scenario Manager

This section provides the general steps to install the OFS BD Scenario Manager software, along with a reference to the specific section and page where the tasks are explained.

Installing the Scenario Manager involves the following procedures:

- [Verifying the Pre-installation Requirements](#)
- [Installing the Scenario Manager on Workstation](#)

7.3.1 Verifying the Pre-installation Requirements

Before you install the OFSBD Scenario Manager on the Windows workstation, verify the following information:

- [Verifying Prerequisite Third-Party Software Installation](#)
- [Verifying Values for the Scenario Manager Installation Program](#)

NOTE

Install and configure the OFS BD application completely before you install the Scenario Manager software.

7.3.1.1 Verifying Prerequisite Third-Party Software Installation

Before installing the OFS BD Scenario Manager, verify that the third-party software defined in [Table 17](#) is installed and configured on the workstation.

OFS BD application supports the third-party software identified in [Table 17](#)

Table 17: Prerequisite Third-Party Software Products for the Scenario Manager Workstation

Component	Product	Version	Vendor
Operating System	Windows 7 and above		Microsoft
Java (32-bit)	JRE, Standard Edition with HotSpot	1.8 and above	Sun

7.3.1.2 Verifying Values for the Scenario Manager Installation Program

To prepare for the OFS BD Scenario Manager installation program's requests for information, use the pre-installation checklist in [Table 18](#) to verify the database connection information, provide the user and owner names to the Scenario Manager Installation Program.

Table 18: Scenario Manager Pre-installation Checklist

Item	Description	Example Value	Your Value
OFS BD Installation Directory	Directory on the workstation where you want to install the Scenario Manager.	C:\Oracle Scenario Manager	Microsoft
Database Client	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 Database Client & Server - Enterprise Edition 19.3+	N/A	N/A
Service Name/ SID	Service Name/ SID for the instance. This is often the same as the database name.	ORA_PROD	Sun
KDD Schema Database Owner	KDD Schema Database owner's name.	Value for kdd_schema_owner	
Alert Management Schema Database Owner Name	Mantas Schema Database owner's name.	Value for mantas_schema_owner	
Database server name	Name of the server that the database resides on.	prod_server	
KDD Miner User Name	KDD Miner user's name.	Value for tools_user	
Operating System	Windows 7 and above		Microsoft
Java (32-bit)	JRE, Standard Edition with HotSpot	1.8 and above	Sun

Table 19: Scenario Manager Pre-installation Checklist

Item	Description	Example Value	Your Value
JRE Home	Directory name of your JRE 1.7 server installation	C:\apps\jre1.7	
Maximum Java Virtual Machine Memory	UsageMaximum amount of Java Virtual Machine (JVM) memory available for the Scenario Manager.	64	
Program Group Name	Name of the Windows Program Group where you want to install the Scenario Manager.	Financial Crime and Compliance Management Scenario Manager	

Table 19: Scenario Manager Pre-installation Checklist

Item	Description	Example Value	Your Value
JAVA_TOOL_OPTIONS	System environmental variable need to add a new param.	Dos.name=Windows 7	

NOTE

Any path that includes spaces must be entered with double quotes.

For example, C:\Program Files\JRE 1.8.

7.3.2 Installing the Scenario Manager on Workstation

The OFS BD Scenario Manager Installation program installs the Scenario Manager using a series of screens that prompt you for the information relevant to local installation and interface with the other subsystems of the OFS BD application.

NOTE

You can cancel the installation from any screen in the installation program. For more information, see Cancelling the Scenario Manager Installation Program.

To start the OFS BD Scenario Manager installation, follow these steps:

1. Copy the ScenarioManager.exe file from OFS_BD_PACK/OFS_BD/bin to the windows machine.
2. Scenario Manager install with Java version jre1.8.0_60 and above generates the error "Windows Error 2 Occurred While Loading the Java VM". Follow the below steps to address this error
 - a. Open the Command prompt and navigate to the location of the installer
CD C:\Users\YourUsername\Downloads.
 - b. Once in the location of the Installer, execute the command: `ScenarioManager.exe -i GUI LAX_VM "C:\Program Files (x86)\Java\jre1.8.0_291\bin\java.exe"`.

NOTE

The JRE file (jre1.8.0_291) referred to above must be the version available in the local setup.

3. Enter the Oracle database connection string for Oracle Mantas. In most cases, this is the same as the Oracle database instance. For example: jdbc:oracle:thin:@hostname:port ID:service name/Service ID.
4. For the Oracle Mantas database, enter the atomic schema as username for the following
 - a. KDD schema database owner
 - b. FIRM schema database owner
 - c. KDD miner
5. When prompted for Java Runtime Environment Home, click on Next.
6. Make below changes in kddstart.bat at

```
C:\opt\Oracle_Mantas_Platform\behavior_detection\toolkit\bin\kddstart.bat
```

Changes to be made in kddstart.bat are listed below:

```
Set 'set KDD_HOME=C:\opt\Oracle_Mantas_Platform\behavior_detection'  
Set 'set JAVA_HOME="C:\Program Files (x86)\Java\jre1.8.0_291"'
```

NOTE The JRE file (jre1.8.0_291) referred to above must be the version available in the local setup.

```
Set 'SET ORACLE_JAR=%LIBDIR%\ojdbc7.jar'.
```

NOTE

- Set the latest ojdbc.jar file value in ORACLE_JAR. ojdbc6.jar is unable to connect with 19c.
- If the Scenario Manager tool does not have the latest jar files, copy the required .jar files from ##FIC_HOME/ficweb/WEB_INF/lib ## and place them at <INSTALLED_DIRECTORY>\Oracle_Mantas_Platform\behavior_detection\toolkit\lib\.

7. Make below changes in install.cfg at

```
C:\opt\Oracle_Mantas_Platform\behavior_detection\toolkit\mantas_cfg\install.cfg
```

Changes to be made in install.cfg are listed below

Enter the Correct jdbc details. For example:

```
'com.mantas.toolkit.database.url=jdbc:oracle:thin:@whf00qjy.in.oracle.com:1521:Ti41012L74'
```

```
Set 'mantas.jvm.maximum.size=256' or 'mantas.jvm.maximum.size=1000'
```

8. Copy and paste 2 files(common.dtd and pattern.dtd) from
"C:\Oracle_Mantas_Platform\behavior_detection\toolkit\xml" to
"C:\Oracle_Mantas_Platform\behavior_detection\toolkit\bin"
9. Launch Scenario manager

```
C:\opt\Oracle_Mantas_Platform\behavior_detection\toolkit\bin\kddstart.bat'
```

NOTE

If the Command window does not come up when 'kddstart.bat' is clicked, then follow the below steps. This could happen due to an issue with the DB connection.

1. Check 'set JAVA_HOME="C:\Program Files (x86)\Java\jre1.8.0_291"' in kddstart.bat file and confirm that the provided path exists in the local.
 2. Check that the Schema name is correct in the install.cfg.
 3. In install.cfg, the JDBC url must have separator as ":" or "/". If the "kddstart.bat" does not work with ":" as a separator then change the separator to "/".
- For example:
'com.mantas.toolkit.database.url=jdbc:oracle:thin:@whf00qjy.in.oracle.com:1521/Ti41O12L74'
or
'com.mantas.toolkit.database.url=jdbc:oracle:thin:@whf00qjy.in.oracle.com:1521:Ti41O12L74'.

7.4 Copying KEYTAB and KRB5 Files in OFSAAI

A Keytab is a file containing pairs of Kerberos principals and encrypted keys (these are derived from the Kerberos password). The krb5.conf file contains Kerberos configuration information, including the locations of KDCs and admin servers for the Kerberos realms of interest, defaults for the current realm and for Kerberos applications, and mappings of hostnames onto Kerberos realms.

Generate the application EAR/WAR file and redeploy the application onto your configured web application server.

Restart the Web Application Server and the OFSAAI Application Server. For more information, see [Appendix E: Starting/Stopping Infrastructure Services](#).

7.5 Deploying Analytic Reports and Threshold Analyzer

This section explains how to deploy Analytics on Oracle Business Intelligence Enterprise Edition (OAS 5.9) and integrate Analytic Reports and Threshold Analyzer in the OFSBD UI.

Topics:

- [Installing Oracle Analytic Server \(OAS\) 5.9](#)
- [Installing ORACLE ANALYTIC SERVER \(OAS\) 5.9 Windows Administration Client](#)
- [Disabling the Cache Feature in Oracle Analytic Server \(OAS\) 5.9](#)
- [Change Default Repository Password](#)
- [Configuring ORACLE ANALYTIC SERVER \(OAS\) 5.9 Connection Pool](#)
- [Deploying OFS FCCM Report Analytics](#)

- [Configuring TreeMap Graph](#)
- [Deploying OFS FCCM Report Analytics](#)
- [Configuring TreeMap Graph](#)
- [Disable Single Sign On](#)
- [Enabling Table Authentication feature in OAS 5.9](#)

7.5.1 Installing Oracle Analytic Server (OAS) 5.9

To install the ORACLE ANALYTIC SERVER (OAS) 5.9, download the software from [ORACLE ANALYTIC SERVER \(OAS\) 5.9 Server](#). After installation, get the Enterprise Manager URL, Username, Password, and ORACLE ANALYTIC SERVER (OAS) 5.9 installed directory from the system administrator.

NOTE

- You must map BI Admin Reporter Role with atomic schema INFODOM.
- BI Admin Reporter Role has to be mapped to any group (for example, CASESUPERVISOR in case of Pack on Pack) that you need to provide.

7.5.2 Installing ORACLE ANALYTIC SERVER (OAS) 5.9 Windows Administration Client

Download and Install OAS client tool for 5.9.

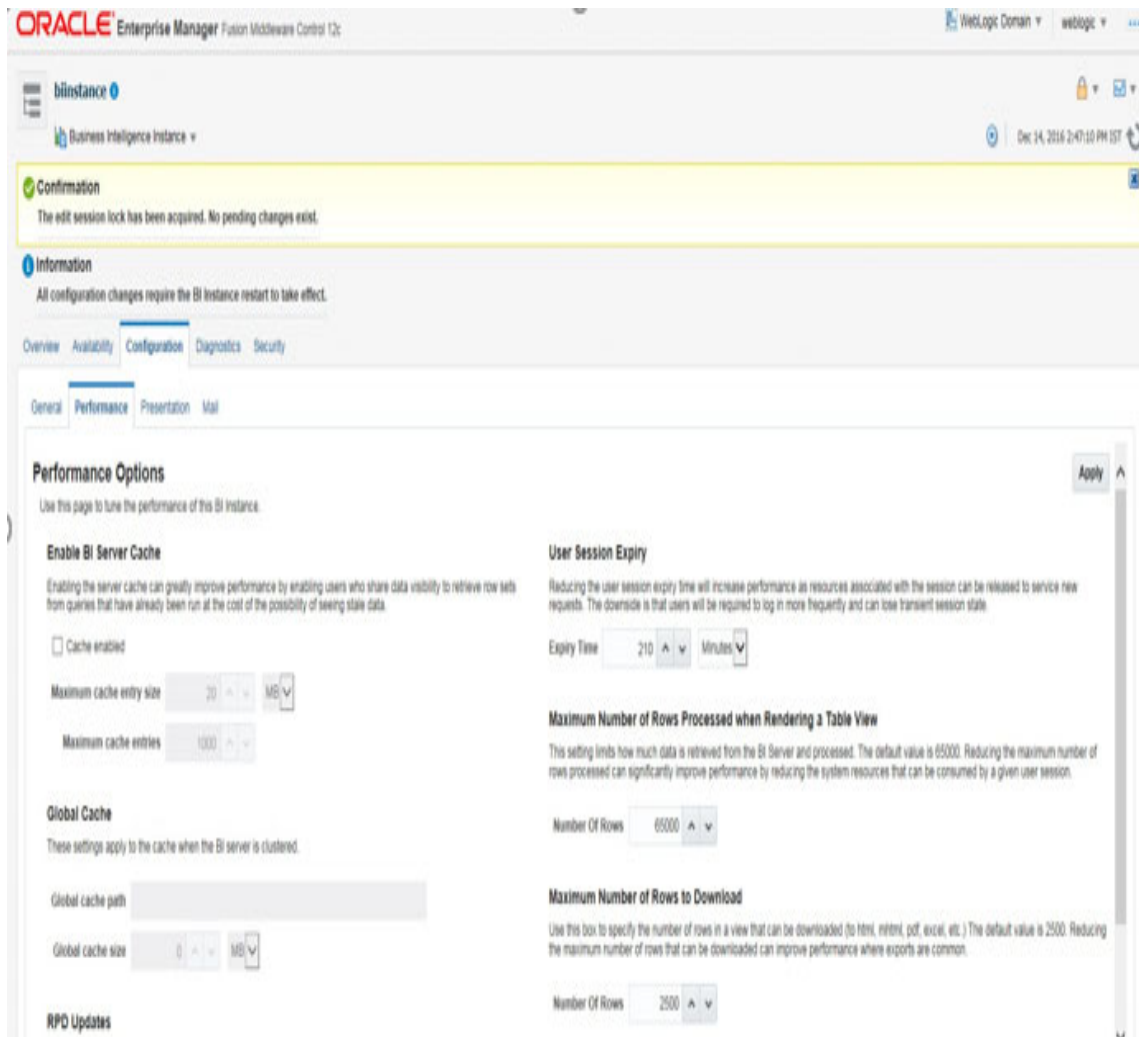
7.5.3 Disabling the Cache Feature in Oracle Analytic Server (OAS) 5.9

ORACLE ANALYTIC SERVER (OAS) 5.9:

Log in to the Enterprise Manager and perform the following steps:

1. Click the Target Navigation icon.
2. Expand the Business Intelligence section and then click biinstance.
3. Click the Configuration tab.
4. Click the Lock icon and then click Lock & Edit to enable the Cache Enabled check box.
5. Under the Performance tab, in the Enable Bi Server Cache section, de-select the Cache Enabled check box and make the required changes.
6. Click the Lock icon and click Release Configuration to save the Cache Enabled changes.

Figure 17: Disabling the Cache Feature in Oracle Analytic Server (OAS) 5.9



7.5.4 Change Default Repository Password

ORACLE ANALYTIC SERVER (OAS) 5.9

Copy FCCM81.rpd from \$FIC_HOME/OBIEE/Repository to the Windows machine where the OAS Windows administration client is installed.

To change the default password for the repository follow these steps:

1. Open the Repository using the OAS Windows administration client from Windows machine. From the File menu, select Open and click Offline. Browse to the Repository on Windows machine. The Oracle BI Administration Tool - FCCM81.rpd windows is displayed.
2. Enter default Repository password: FCCM\$810

To change the default password, follow these steps:

1. From the File menu, choose Change Password.
2. Enter the new password and click OK.

7.5.5 Configuring ORACLE ANALYTIC SERVER (OAS) 5.9 Connection Pool

ORACLE ANALYTIC SERVER (OAS) 5.9:

To configure the Connection Pool of the repository, follow these steps:

1. Open the same Repository (as in the previous step) on the Windows machine. The Oracle BI Administration Tool - FCCM81.rpd window is displayed.
2. Expand the FCCM folder in the Physical section.
3. Double-click on the Connection Pool to open the Connection Pool Properties window.
4. Enter the following in the Data Source Name text box of the Connection Pool Properties window after modifying <Database Server Host Name> and <Database Name> Data Source Name = (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<Database Server HostName>)(PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=<Database Name>)))
5. Enter the Atomic Schema user in the User name text box.
6. Enter the Atomic Schema user password in the Password text box.
7. Click OK.
8. Expand the folder and test connection for any one table name by Right Click > view data.
9. Perform similar changes in the Connection Pools for all remaining folders in the Physical Layer by providing the following schema details for all Connection Pools:
 - KYC Analytics >Atomic Schema

NOTE

Initial block and connection pool: both must point towards the atomic schema.

- UIC_73 > CaseMng connection pool ->Atomic SchemaUIC_73 > Security connection pool->Atomic Schema
- TA > Atomic Schema
- CTRBI-> Atomic Schema

- ORCL->Atomic Schema
 - FCCM > Atomic Schema
10. Select Save option from the File menu. The following message is displayed: Do you want to check global consistency?
 11. Click Yes. The following message is displayed: Consistency check did not find any errors, warning or best practices violations.
 12. Click OK.

7.5.6 Deploying OFS FCCM Report Analytics

ORACLE ANALYTIC SERVER (OAS) 5.9:

To deploy Analytic Reports, follow these steps:

1. Login to System Settings using the below URL:
<http://<oas server name>:<oas analytics port number>/analytics/systemsettings/>
(Example link for reference: <http://testserver:9502/analytics/systemsettings/>)
2. Search for Evaluate in the search box.
3. Select Level 2 from the Evaluate Support Level drop-down .
4. Search for HTML in the search box.
5. Enable Allow HTML Content.
6. Click **Restart** .
7. Update the instanceconfig.xml file available in <Oracle Analytic Server (OAS) 5.9_home>/user_projects/domains/bi/config/fmwconfig/biconfig/OBIPS location as detailed here.
8. Replace the following script:

```
<Security>

This Configuration setting is managed by Oracle Enterprise Manager
Fusion
Middleware Control-->

<ClientSessionExpireMinutes>210</ClientSessionExpireMinutes>

</Security>
```

With the following:

```
<Security>

<!--This Configuration setting is managed by Oracle Enterprise Manager
Fusion
Middleware Control-->

<ClientSessionExpireMinutes>210</ClientSessionExpireMinutes>

<InIFrameRenderingMode>allow</InIFrameRenderingMode>

</Security>
```

9. Deploy BAR(CATALOG)
 - a. Navigate to \$FIC_HOME/OBIEE/catalog.

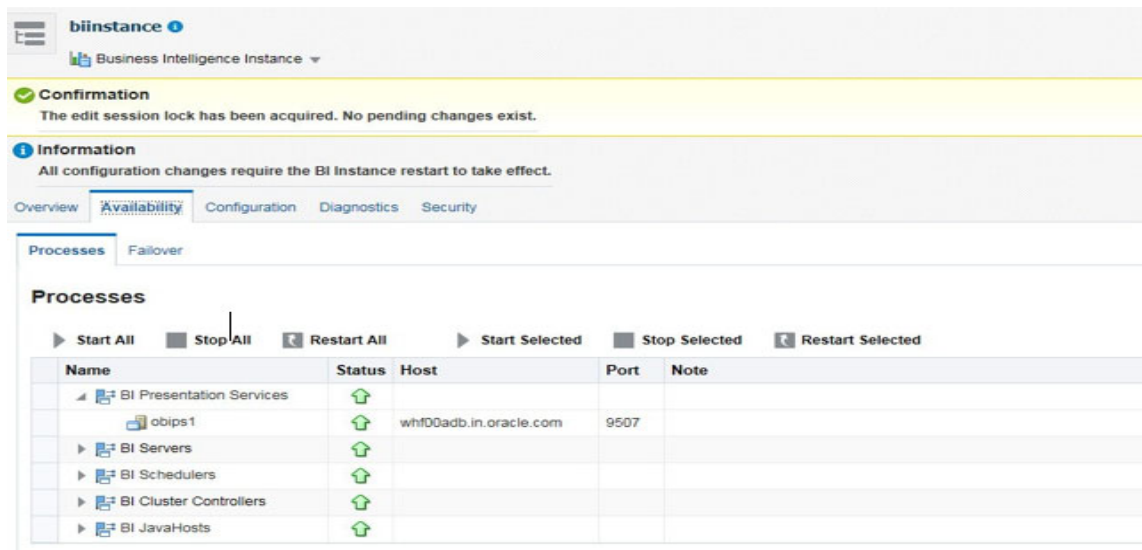
- b. Copy FCCM_ANALYTICS.bar to the working location of OAS server.
 - c. Copy FCCM81.rpd into the working location of OAS server.
 - d. Go to, <OAS 5.9 Home directory>/Oracle_Home/user_projects/domains/bi/bitools/bin path.
 - e. Execute the command:


```
./importarchive.sh ssi <working location>/FCCM_ANALYTICS.bar
encryptionpassword='<pwd>'
```

Note: pwd is the same as RPD (Repository) password.
10. Deploy FCCM81.rpd
- a. Navigate to the working directory and execute the following script:


```
<Oracle Analytic Server (OAS) 5.9_home>/user_projects/domains/bi/
bitools/bin/datamodel.sh uploadrpd -I FCCM81.rpd -SI ssi -U <user> -P
<password>
```
 - b. Restart Oracle Analytic Server (OAS) 5.9 from Enterprise Manager by following these steps: (see [Figure 18](#))
 - c. Click the Target Navigation icon.
 - d. Expand the Business Intelligence section and then click biinstance.
 - e. Click the Availability tab.
 - f. Click Stop All.
 - g. Click Start All.

Figure 18: Restarting Oracle Analytic Server (OAS) 5.9



7.5.7 Configuring TreeMap Graph

This section describes how configure TreeMap graph.

To configure the TreeMap Graph, follow these steps:

1. Login to Oracle Analytic Server (OAS) 5.9.
2. Navigate to ORACLE ANALYTIC SERVER (OAS) 5.9 Home.

NOTE	ORACLE ANALYTIC SERVER (OAS) 5.9 Home is the ORACLE ANALYTIC SERVER (OAS) 5.9 installed path.
-------------	---

3. Execute the command: `cd <Oracle Analytic Server (OAS) 5.9_home>.`
4. Execute the command to find the available treemap-canvas.js: `find -name treemap-canvas.js.`
5. Four different files, all named treemap-canvas.js are displayed.
6. Back up these four files.
7. Edit window.top.console to console in these four files and save.

7.5.8 Disable Single Sign On

This section describes how to disable Single Sign On.

Execute the following to disable Single Sign On:

```
<Oracle Analytic Server (OAS) 5.9_Home>/oracle_common/common/bin/wlst.sh  
disableBISingleSignOn('<Oracle Analytic Server (OAS) 5.9_Home>/user_projects/  
domains/bi').
```

7.5.9 Enabling Table Authentication feature in OAS 5.9

This section describes how to enable the Table Authentication feature in OAS 5.9.

To enable Table authentication, follow these steps:

1. Go to the following location and open or create the .properties file.
`<DOMAIN_HOME(OAS Server Domain home)>
/config/fmwconfig/biconfig/OBIPS/incubation.properties` (if the file does not exist, create it)
2. Add/update the `oracle.bips.auth.nextGenAuth=false` line in the file.
3. Restart the OBIPS process(es).

For example: .

- `<DOMAIN_HOME>/bitools/bin/stop.sh -i obips1`
- `<DOMAIN_HOME>/bitools/bin/start.sh -i obips1.`

7.6 Post Installation Steps

This section describes the post installation steps.

After installing the OAS 5.9, follow these steps:

1. Log in as OFS BD Admin User with valid username and password. The OFS BD Home page is displayed.
2. Click FCCM and then click the Administration Menu and select the Manage Parameters and click Manage Common Parameters.
3. Choose Parameter Category as Used for Design and Parameter Name as OBIEE.
4. Set Attribute 2 Value = <PROTOCOL>://<OAS 5.9_SERVER_NAME>:<PORT>.

NOTE

Fully Qualified host name have to be provided.

<PROTOCOL> is the web page access PROTOCOL (http or https) and <OAS 5.9_SERVER_NAME> is the FQN (fully qualified name)/ host name of the server, where OAS 5.9 is installed.

- <PORT> is the PORT number used in OAS 5.9 installation. It may change based on the OAS 5.9 version. Enter the correct PORT number if it is not 9704.
- Placeholder variables are mentioned between angle brackets. Update the placeholders with actual value.
- If there are any errors, do not proceed with further installation and contact Oracle Support Services.
- After Installation is successful, apply the bug no. 33738222
- After the patch installation is successful, execute BD_Duplicate_Jar_Removal.sh script from \$FIC_HOME.

5. Verify Attribute 4 Value. It must be the OFS BD application URL. If the same OFS BD application is deployed on different machines, then modify the OFS BD Application URL in Attribute 4 Value appropriately.

7.7 Accessing Reports through OFS BD Application

For more information on Accessing Reports, see [Oracle Financial Services FCCM Analytics User Guide](#).

7.8 Installing RAOR Service

NOTE

This is applicable only for KYC. Oracle financial Services Inline Processing Engine (IPE), ILP service deployment is not mandatory for KYC.

To install the RAOR service, follow these steps:

1. Creating RAOR.ear/ RAOR.war
2. Deploying RAOR.ear in WebLogic
3. Deploying RAOR.ear in WebSphere

4. Deploying RAOR.war in Tomcat

NOTE

For information on IPE, configurations, such as JMS connection factory and JMS queue, see [OFS Inline Processing Engine Configuration Guide](#). These configurations are mandatory for RAOR.

To Import IPE KYC Assessments, navigate to \$FIC_HOME/ficapp/common/FICServer/bin and execute the following command after replacing ##NAME_OF_THE_ASSESSMENT## and ##FCCMINFODOM##.

```
./RTIImport.sh $FIC_HOME/IPE/ KYC/##NAME_OF_THE_ASSESSMENT## ##FCCMINFODOM##  
OFS_KYC false.
```

For example:

```
./RTIImport.sh /scratch/ofsaabie/AAA1_80/BD812ADB/BD812ADB/IPE/KYC/  
OFS_KYC_RTExport_ModelBasedAssessment.xml FCCMINFO OFS_KYC false
```

NOTE

Import all the assessments available under the \$FIC_HOME/IPE/ KYC path.

7.9 Creating RAOR.ear/ RAOR.war

It is mandatory to have the RAOR.ear in the same profile or domain where the <contextname>.ear file of the OFS BD Application is deployed.

Figure 19: Creating RAOR.ear/ RAOR.war



```
/scratch/ofsaabie/AAA1_80/realtime_processing>ls  
ant.sh application.xml build.xml ILP.ear ILP.war ipesampleapp WebContent  
/scratch/ofsaabie/AAA1_80/realtime_processing>./ant.sh  
executing "ant"  
Buildfile: build.xml  
  
createwar:  
  
createear:  
  
BUILD SUCCESSFUL  
Total time: 0 seconds  
/scratch/ofsaabie/AAA1_80/realtime_processing>
```

To create RAOR.ear/ RAOR.war, follow these steps:

1. Navigate to < OFSAA Installation Directory >/raor_processing
2. Execute the command:./ant.sh.
3. On successful execution, the RAOR.ear and RAOR.war files are generated under the <OFSAA Installation Directory >/raor_processing/ folder.

7.10 Deploying RAOR.ear in WebLogic

This section defines how to deploy RAOR.ear in WebLogic.

NOTE

It is mandatory to have RAOR.ear in the same domain where <contextname>.ear of the OFS BD Application is deployed.

IF RAOR ILP and TFLT are deployed, then change the following values in the web.xml file of each individual service:

- For ILP, change rti.server.web.root to rtiPE.server.web.root.
- For RAOR, change rti.server.web.root to rtiRAOR.server.web.root.
- For TFLT, change rti.server.web.root to rtiTFLT.server.web.root.

To deploy RAOR.ear in WebLogic, follow these steps:

1. Start the WebLogic server.
2. Create an RAOR.ear folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications

Copy <FIC_HOME>/raor_processing/RAOR.ear to <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RAOR.ear/
3. Explode the RAOR.ear file by executing the command: `jar -xvf RAOR.ear`.
4. Delete the RAOR.ear and RAOR.war files.
5. Create an RAOR.war folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RAOR.ear
6. Copy <FIC_HOME>/raor_processing/RAOR.war to <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RAOR.ear/RAOR.war
7. Explode the RAOR.war file by executing the command: `jar -xvf RAOR.war`.
8. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DomainName>/applications/RAOR.ear/RAOR.war/WEB-INF path, make the following changes in the log4j.xml file:
 - Change the debug value to True as shown below:
`<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/" debug="True">`
 - Change the level value to Debug as shown below:
`<logger name="org.springframework">`
`<level value="DEBUG"/>`
`</logger>`
`<logger name="com.ofs.aai">`
`<level value="DEBUG"/>`
`</logger>`
9. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain Name>/applications/RAOR.ear/RAOR.war/conf path, provide a working watch list URL in the WatchList.wsdl file.

For example: <PROTOCOL://HOSTNAME:PORT/mantas/services/WatchListService

10. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain Name>/applications/RAOR.ear/RAOR.war/conf/ext path, update the raor.auth.role property in the spring-raor.properties file with the required role name. For example, KYCADMIN.

This step is required in order to authorize a role name for RAOR. You must also map this role to the user who is hitting the RAOR service. For example, KYCADMIN1.

11. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain Name>/applications/RAOR.ear/RAOR.war/conf path, update the aai.auth.url property in the install.properties file with the AAI authentication URL. For example, aai.auth.url=<PROTOCOL://HOSTNAME:PORT/CONTEXT_NAME/rest-api/idm/service/login. aai.auth.url=http://<Server>:<port>/<context>/rest-api/idm/service/login

For example: http://testserver:8031/OFSAAI/rest-api/idm/service/login

12. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain Name>config path, update config.xml with the below entry under <security-configuration>:

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

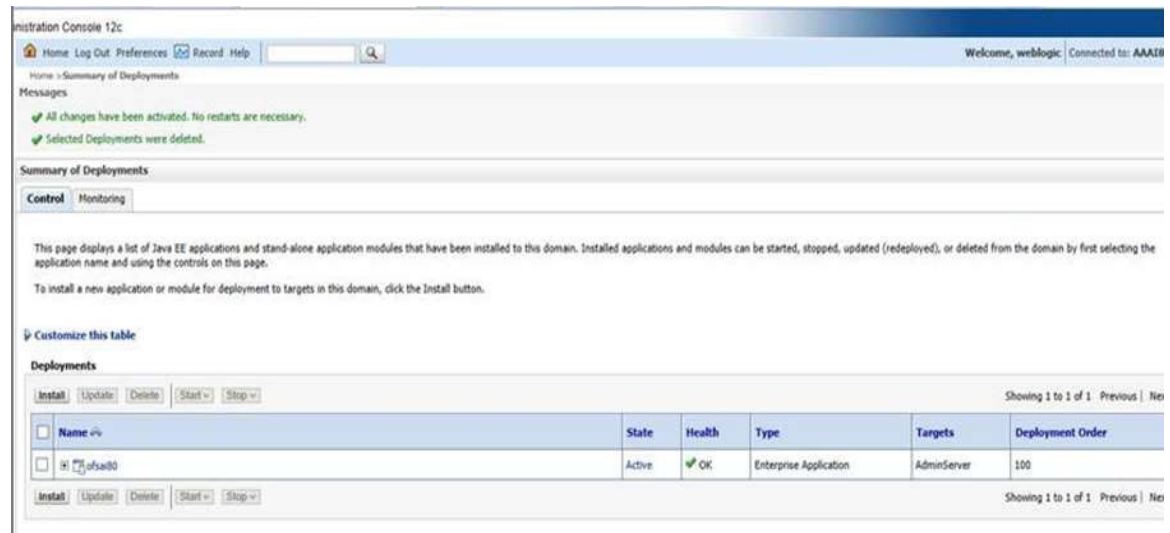
7.11 Installing RAOR.ear in WebLogic using WebLogic Administrator Console

This section describes how to install RAOR.war in WebLogic using WebLogic Administrator console.

To install RAOR.war in WebLogic using WebLogic Administrator console, follow these steps:

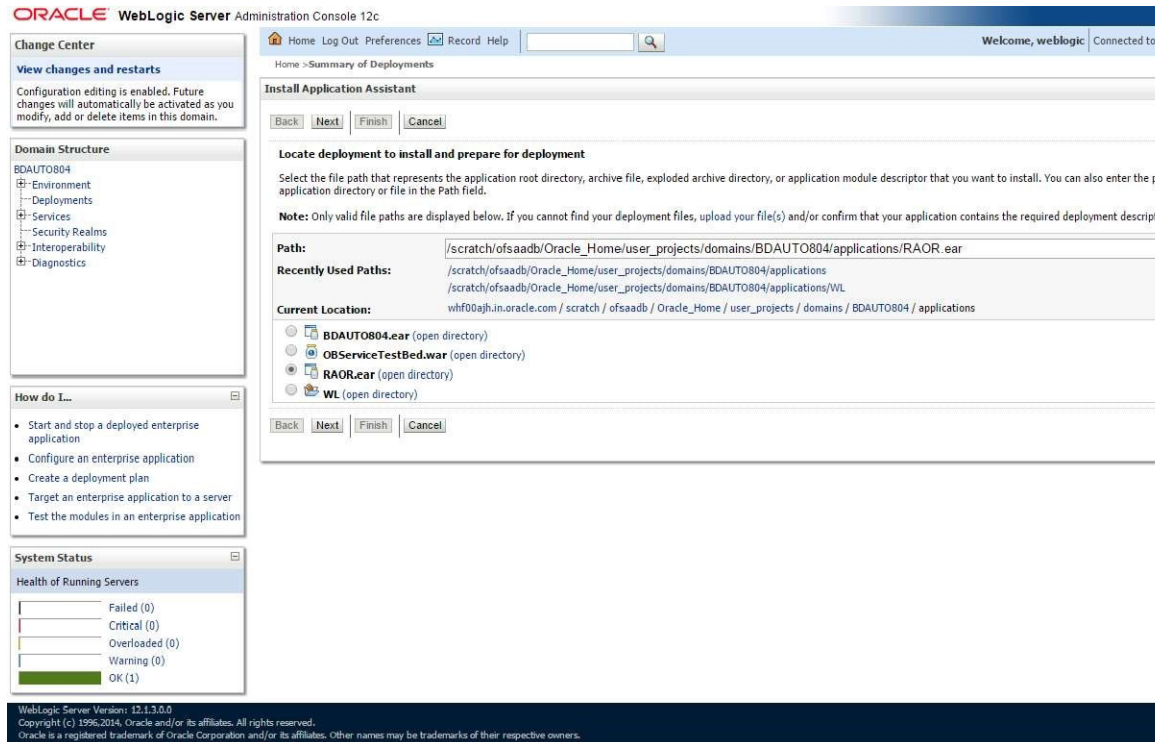
1. Navigate to the path "<WebLogic Installation directory>/user_projects/domains/<domain name>/bin" in the machine in which WebLogic is installed.
2. Start WebLogic by executing the command: ./startWebLogic.sh -d64 file
3. Open the URL in the browser window: http://<ipaddress>:<admin server port>/console. (https if SSL is enabled). The Sign in window of the WebLogic Server Administration Console is displayed.
4. Login with the Administrator Username and Password. The Summary of Deployment page is displayed.

Figure 20: Summary of Deployment



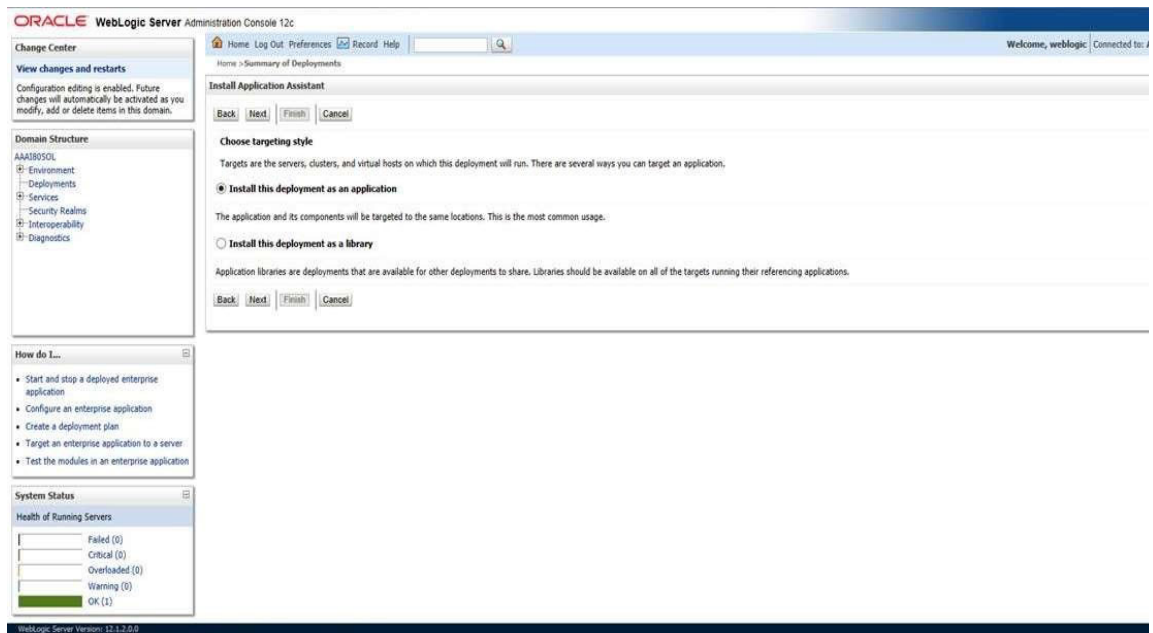
- Click Install. The Install Application Assistance page is displayed.

Figure 21: Install Application Assistance Window



- Select RAOR.ear and click Next. The Install Application Assistance page is displayed with the Choose targeting style section.

Figure 22: Install Application Assistance with choose Target Style



- By default, the Install this deployment as an application option in the Choose targeting style section is selected. Click Next. The Install Application Assistance page is displayed with the Optional Settings section.

Figure 23: Install Application Assistance page with Optional Settings

The screenshot shows the 'WebLogic Server Administration Console 12c' interface. The left sidebar contains navigation links like 'Change Center', 'Domain Structure', 'How do I...', and 'System Status'. The main content area is titled 'Home > Summary of Deployments' and 'Install Application Assistant'. It includes buttons for 'Back', 'Next', 'Finish', and 'Cancel'. The 'Optional Settings' section is active, showing options for 'General' (deployment name 'ILP'), 'Security' (selected: 'DD Only: Use only roles and policies that are defined in the deployment descriptors'), and 'Source Accessibility' (selected: 'Use the defaults defined by the deployment's targets'). A 'Location' field is set to '/scratch/oracle/Oracle/Middleware/Oracle_Home/user_'. A note at the bottom states: 'Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.'

- Retain the default selections and click Next. The Install Application Assistance page is displayed with the Review your choices and click Finish section.

Figure 24: Install Application Assistance page with Review your choices and click Finish section

The screenshot shows the 'Install Application Assistant' page at the 'Review your choices and click Finish' step. It includes buttons for 'Back', 'Next', 'Finish', and 'Cancel'. The 'Additional configuration' section has the option 'No, I will review the configuration later.' selected. The 'Summary' section displays the deployment details: 'Deployment: /scratch/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/AAA1805QL/applications/ILP.ear', 'Name: ILP', 'Staging Mode: Use the defaults defined by the chosen targets', 'Plan Staging Mode: Use the same accessibility as the application', and 'Security Model: DDOnly: Use only roles and policies that are defined in the deployment descriptors.' Below this is a 'Target Summary' table:

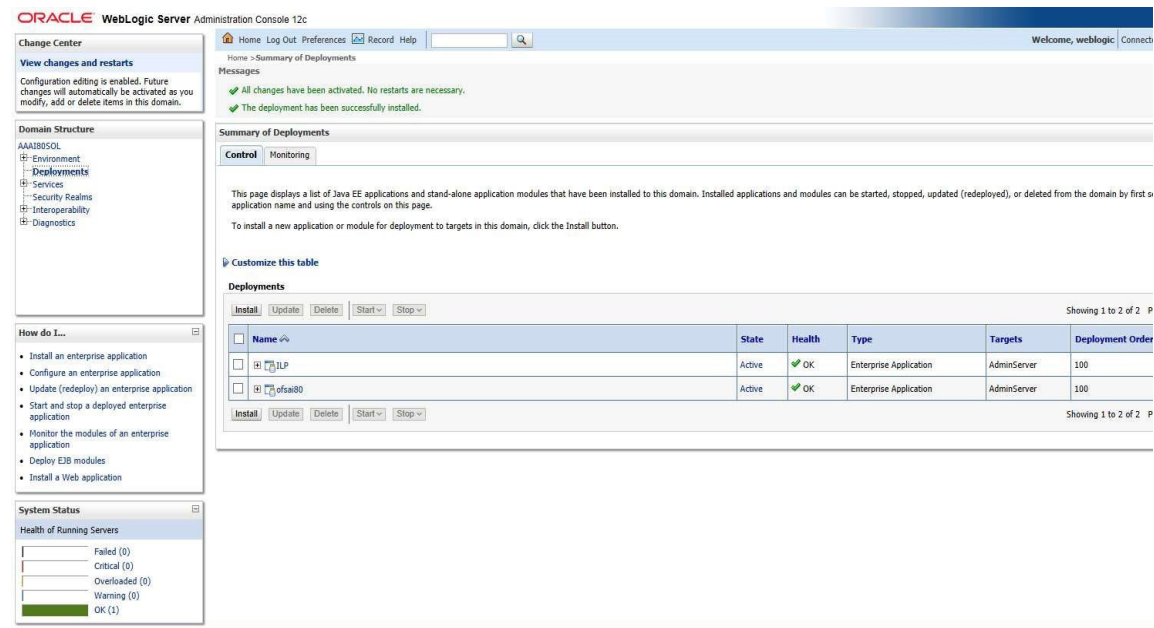
Components	Targets
ILP.ear	AdminServer

Buttons for 'Back', 'Next', 'Finish', and 'Cancel' are at the bottom.

- Select *No, I will review the configuration later* in the Additional Configuration section and click Finish.

The ILP is added in the Name section of the Summary of Deployment page.

Figure 25: Summary of Deployment page with ILP



10. Restart all OFS AAAI servers. For more information, see [Appendix E: Starting/Stopping Infrastructure Services](#).

7.12 Deploying RAOR.ear in WebSphere

This section describes how to deploy the RAOR.ear file in WebSphere.

To deploy RAOR.ear in WebSphere, follow these steps:

NOTE

- It is mandatory to have RAOR.ear in the same domain where <contextname>.ear of the OFS BD Application is deployed.
- Delete all the Jersey related jars in the WEB-INF/lib folder
- Comment the below line from \$FIC_HOME/raor_processing/WebContent/conf/application-env.properties file.
linespring.profiles.active=JMS,JMSApplicationCache,JMSGateway,JMSFeedBackGateway

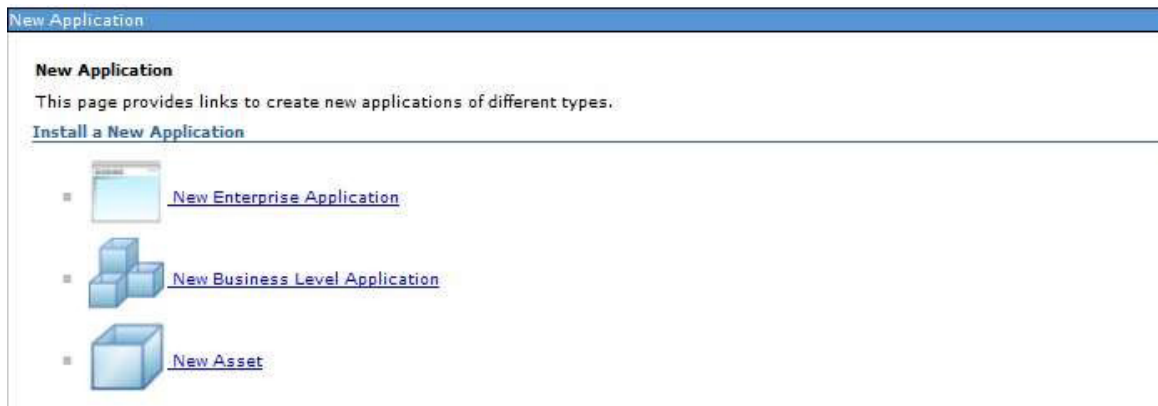
- Start the WebSphere Profile by navigating to the path "<WebSphere_Installation_Directory>/IBM/WebSphere/AppServer/profiles/<Profile_Name>/bin/" then execute the command: `./startServer.sh server1`.
- Open the following URL in the browser: <http://<ipaddress>:<Administrative Console Port>/ibm/console>. (use https protocol if SSL is enabled). The login screen is displayed.

Figure 26: WebSphere Login Window



3. Enter the user credentials which has administrator rights and click Log In.
4. From the LHS menu, select Applications and click New Application. The New Application window is displayed.

Figure 27: New Application



5. Click New Enterprise Application. The Preparing for the application installation window is displayed.

Figure 28: Preparing for the Application Installation

Preparing for the application installation

Specify the EAR, WAR, JAR, or SAR module to upload and install.

Path to the new application

☒ Local file system

Full path

Choose File No file chosen

☐ Remote file system

Full path

/scratch/IBM/RAOR.ear Browse...

Next Cancel

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

Figure 29: Installation Options

Preparing for the application installation

How do you want to install the application?

☒ Fast Path - Prompt only when additional information is required.

☐ Detailed - Show all installation options and parameters.

☒ Choose to generate default bindings and mappings

Previous Next Cancel

7. Select the Fast Path option and click Next. The Install New Application window is displayed.

Figure 30: Install New Application

Specify options for installing enterprise applications and modules.

→ Step 1: Select installation options

Step 2 Map modules to servers

Step 3 Map virtual hosts for Web modules

Step 4 Summary

Select installation options

Specify the various options that are available for your application.

☐ Precompile JavaServer Pages files

Directory to install application

☒ Distribute application

☐ Use Binary Configuration

Application name

RAOR

☒ Create MBeans for resources

☐ Override class reloading settings for Web and EJB modules

Reload interval in seconds

☐ Deploy Web services

Validate Input off/warn/fail

warn

☐ Process embedded configuration

File Permission

Allow all files to be read but not written to

Allow executables to execute

Allow HTML and image files to be read by everyone

.*\,dll=755#.*\,so=755#.*\,a=755#.*\,sl=755

Application Build ID

Unknown

☐ Allow dispatching includes to remote resources

☐ Allow servicing includes from remote resources

Business level application name

Create New BLA

Asynchronous Request Dispatch Type

Disabled

☐ Allow EJB reference targets to resolve automatically

☐ Deploy client modules

Client deployment mode

Isolated

☐ Validate schema

Next

Cancel

8. Enter the required information and click Next. The Map Modules to Servers window is displayed.

Figure 31: Map Modules to Servers

Install New Application

Specify options for installing enterprise applications and modules.

Step 1 Select installation options

→ Step 2: Map modules to servers

Step 3 Map virtual hosts for Web modules

Step 4 Summary

Map modules to servers

Specify targets such as application servers or clusters of application servers where you want to install the modules that are contained in your application. Modules can be installed on the same application server or dispersed among several application servers. Also, specify the Web servers as targets that serve as routers for requests to this application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated, based on the applications that are routed through.

Clusters and servers:

WebSphere:cell=whf00avgNode06Cell,node=whf00avgNode06,server=server1

Apply

☒

☐

Select	Module	URI	Server
<input checked="" type="checkbox"/>	Inline Processing	RAOR.war;WEB-INF/web.xml	WebSphere:cell=whf00avgNode06Cell,node=whf00avgNode06,server=server1

Previous

Next

Cancel

9. Select the Inline Processing check box and click Next. The Map Virtual hosts for Web modules page is displayed.

Figure 32: Map Virtual hosts for Web modules page

The screenshot shows the 'Map virtual hosts for Web modules' page in the 'Install New Application' wizard. The left sidebar contains four steps: 'Step 1 Select installation options', 'Step 2 Map modules to servers', 'Step 3: Map virtual hosts for Web modules' (which is highlighted with a yellow arrow), and 'Step 4 Summary'. The main content area is titled 'Map virtual hosts for Web modules' and includes the instruction: 'Specify the virtual host for the Web modules that are contained in your application. You can install Web modules on the same virtual host or disperse them among several hosts.' Below this is a checkbox labeled 'Apply Multiple Mappings'. A table below the checkbox has two columns: 'Web module' and 'Virtual host'. The 'Web module' column has a checkbox and the text 'Inline Processing'. The 'Virtual host' column has a dropdown menu showing 'default_host'. At the bottom of the page are three buttons: 'Previous', 'Next', and 'Cancel'.

Select	Web module	Virtual host
<input checked="" type="checkbox"/>	Inline Processing	default_host ▼

10. Select the Inline Processing check box and click Next. The Metadata for modules page is displayed.

Figure 33: Summary page

Install New Application
?

Specify options for installing enterprise applications and modules.

Step 1 Select installation options
Step 2 Map modules to servers
Step 3 Map virtual hosts for Web modules
→ **Step 4: Summary**

Summary

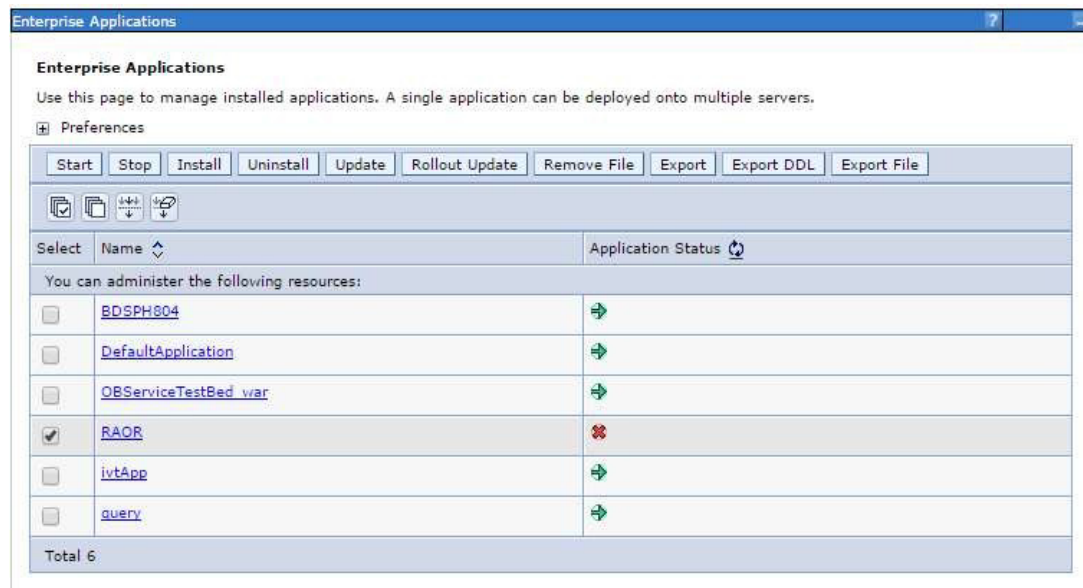
Summary of installation options

Options	Values
Precompile JavaServer Pages files	No
Directory to install application	
Distribute application	Yes
Use Binary Configuration	No
Application name	RAOR
Create MBeans for resources	Yes
Override class reloading settings for Web and EJB modules	No
Reload interval in seconds	
Deploy Web services	No
Validate Input off/warn/fail	warn
Process embedded configuration	No
File Permission	.*\,dll=755#.*\,so=755#.*\,a=755#.*\,sl=755
Application Build ID	Unknown
Allow dispatching includes to remote resources	No
Allow servicing includes from remote resources	No
Business level application name	
Asynchronous Request Dispatch Type	Disabled
Allow EJB reference targets to resolve automatically	No
Deploy client modules	No
Client deployment mode	Isolated
Validate schema	No
Cell/Node/Server	Click here

Previous
Finish
Cancel

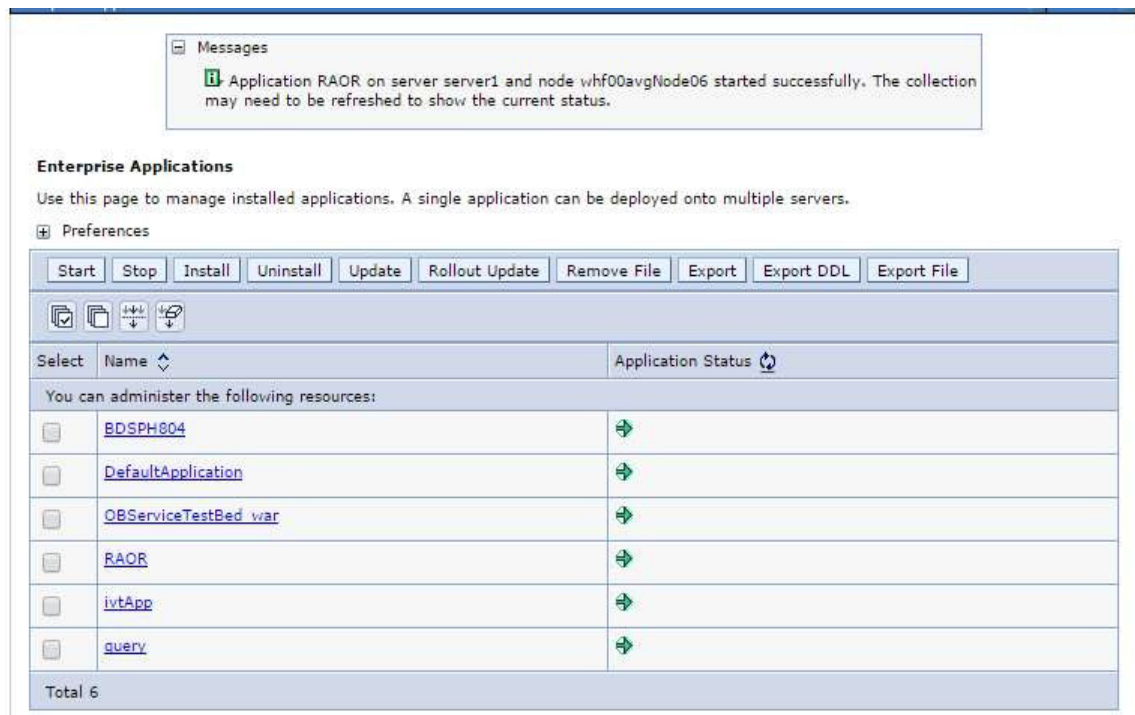
11. Select the Metadata-complete attribute check box and click Next. The Summary page is displayed.
12. Click Finish. On successful installation, a message is displayed.
13. Click Save and save the master file configuration. The details are displayed in the Master File Configuration page.

Figure 34: Master File Configuration page



14. Select RAOR and click Start. The Enterprise Application page is displayed with confirmation message.

Figure 35: Enterprise Application page with Confirmation message



15. If RTFRAUD is deployed, rename StatsManager to StatsManager1 and LogConfig to LogConfig1 in the deployed area/RAOR.ear/RAOR.war/conf/applicationContext-jmx.xml file.

```
<entry key="realtime:name=StatsManager1" value-ref="statMgrBean" />
```

```
<entry key="realtime:name=LogConfig1" value-ref="logRuntimeConfigBean" />
```

16. Restart all OFS AAAI servers. For more information, see [Appendix E: Starting/Stopping Infrastructure Services](#).

7.13 Deploying RAOR.war in Tomcat

This section describes how to deploy the RAOR.war file in Tomcat.

To deploy RAOR.war in Tomcat, follow these steps:

1. Create datasource for RAOR context in Tomcat by editing server.xml in `<TOMCAT_ HOME_DIR>/conf` directory.

Update database details as shown in the following sample:

NOTE Context name must be the directory name under webapps.

```
<Context path="/RAOR"
docBase="/scratch/ofsaaapp/apache-tomcat-8.0.32/webapps/RAOR"
debug="0" reloadable="false" crossContext="true"><Loader
delegate="true"/>
<Resource auth="Container"
name="jdbc/FICMASTER"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver"
username="act_obiconf"
password="password"
url="jdbc:oracle:thin:@whf00agr:1521/DEVUT08SPRINT"
maxTotal="100"
maxIdle="30"
maxWaitMillis="10000"
removeAbandoned="true" removeAbandonedTimeout="60"
logAbandoned="true"/>
<Resource auth="Container"
name="jdbc/<infodom name>". For example,
OFSAAAIINFO
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver"
username="act_obiatm"
password="password"
url="jdbc:oracle:thin:@whf00agr:1521/DEVUT08SPRINT" maxTotal="100"
maxIdle="30"
maxWaitMillis="10000"
removeAbandoned="true"
```

```

removeAbandonedTimeout="60"
logAbandoned="true"/>
<Resource auth="Container"
name="jdbc/<infodom name>CNF". For example,
OFSAAAIINFOCNF
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver"
username="act_obiatm" password="password"
url="jdbc:oracle:thin:@whf00aqr:1521/DEVUT08SPRINT" maxTotal="100"
maxIdle="30"
maxWaitMillis="10000" removeAbandoned="true"
removeAbandonedTimeout="60" logAbandoned="true"/>
</Context>

```

2. Copy RAOR.war file to \$TOMCAT_HOME/webapps directory.
3. Grant 755 (rwxr-xr-x) permissions to the RAOR.war file.
4. Start Tomcat server.
5. Update install.properties file in \$TOMCAT_HOME/webapps/RAOR/conf directory as follows:
 - sql.config.datasource.jndi.name=java:comp/env/jdbc/FICMASTER
 - sql.atomic.datasource.jndi.name=java:comp/env/jdbc/OFSAAAIINF
 - sql.metadom.datasource.jndi.name=java:comp/env/jdbc/OFSAAAIIN FOCNF

NOTE Name must match the Resource Name defined in server.xml.

6. Update application-env.properties file in \$TOMCAT_HOME/webapps/RAOR/conf directory as follows:

```

comment the
#spring.profiles.active=JMS, JMSApplicationCache, JMSGateway, JMSFeedBackG
ateway tag

remove all content after equal to (=) in the spring.profiles.active tag

```
7. Copy jms-api-1.1-rev-1.jar and javax.ws.rs-api-2.0-m02.jar to \$TOMCAT_HOME/webapps/RAOR/WEB-INF/lib directory.
8. Restart all app and web servers.

7.14 Configuring Resource Reference

This section describes the details for configuring the resource reference in WebSphere, WebLogic, and Tomcat Application Servers. For more information, see *Configuring Resource Reference* in [Appendix B: Configure Resource Reference in Web Servers](#).

7.15 Configuring Web Application Server

This section describes the details to configure the different web application servers for OFSAA Infrastructure deployment namely, IBM WebSphere, Oracle WebLogic, and Apache Tomcat Servers.

For more information, see [Configuring Web Application Servers](#).

NOTE

If you are installing CRR 8.1.1.0.0 for the Tomcat 9.x version and performing Pack on Pack installation of BD, ECM, and CRR (goAML STR) see the *Post Installation and Configuring Web Application Server* sections in the [OFS CRR Installation Guide](#).

7.16 Configurations for Java 8

This section describes the Java 8 configurations.

To extract and apply the patch, follow these steps:

1. If the Oracle Database version is 12c, copy ojdbc7.jar from \$ORACLE_HOME/jdbc/lib to the following locations:
 - \$FIC_HOME/utility/OFSAAGenerateRepository/lib/
 - \$FIC_HOME/realtime_processing/WebContent/WEB-INF/lib/
 - \$FIC_HOME/ficdb/lib/
 - \$FIC_HOME/ficapp/icc/lib/
 - \$FIC_HOME/ficapp/common/FICServer/lib/
 - \$FIC_HOME/FMStandalone/FormsManager/WEB-INF/lib/
 - \$FIC_HOME/ficweb/webroot/WEB-INF/lib/

NOTE

If ojdbc6.jar is already available in any of the aforementioned folders, you need to remove it.

2. If the Oracle Database version is 11g, copy ojdbc6.jar from \$ORACLE_HOME/jdbc/lib to the following locations:
 - \$FIC_HOME/utility/OFSAAGenerateRepository/lib/
 - \$FIC_HOME/realtime_processing/WebContent/WEB-INF/lib/
 - \$FIC_HOME/ficdb/lib/
 - \$FIC_HOME/ficapp/icc/lib/
 - \$FIC_HOME/ficapp/common/FICServer/lib/
 - \$FIC_HOME/FMStandalone/FormsManager/WEB-INF/lib/
 - \$FIC_HOME/ficweb/webroot/WEB-INF/lib/

7.17 Enabling Unlimited Cryptographic Policy for Java

Enabling unlimited cryptographic policy for Java enables you to use AES-256 keys for encryption. The JCE Policy JAR files, for the current Java versions required for OFSAA and also for later versions, see [Java Bug Database](#).

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

- Download the JCE Policy related JARs local_policy.jar and US_export_policy.jar.
- Download Oracle Java from [here](#).
- Download BM Java from [here](#).
- Copy (or replace) the downloaded JCE Policy related JARs local_policy.jar and US_export_policy.jar into the /jre/lib/security directory of Java installation directory used for OFSAI and the Web Application Servers.

7.18 Configurations for Oracle 19c Database

This section describes the configurations for Oracle 19c database.

Perform the following to create symbolic link inside the <ORACLE_HOME>/lib directory:

1. Replace all the instances of ojdbc6.jar with ojdbc8.jar in the following files:
 - <FIC_HOME>/bdf/scripts/env.sh
 - <FIC_HOME>/ingestion_manager/scripts/deployWatchList.sh
 - <FIC_HOME>/ingestion_manager/scripts/build.xml
 - <FIC_HOME>/ingestion_manager/scripts/env.sh
 - <FIC_HOME>/ficweb/MANIFEST.MF
 - <FIC_HOME>/ficweb/webroot/solution/bdf/scripts/env.sh
 - <FIC_HOME>/ficweb/webroot/TestScenario_SRC/FicDB/bin/updateTestRunids.sh
 - <FIC_HOME>/ficweb/webroot/TestScenario_SRC/FicDB/bin/pgxLA.sh
 - <FIC_HOME>/database/db_tools/bin/db_env.sh
 - <FIC_HOME>/database/db_tools/bin/db_env.sh
 - <FIC_HOME>/ficdb/bin/IPE_FCCM.sh
 - <FIC_HOME>/ficdb/bin/AccountOpenDoc.sh
 - <FIC_HOME>/ficdb/bin/updateTestRunids.sh
 - <FIC_HOME>/ficdb/bin/pgxLA.sh
 - <FIC_HOME>/ficdb/bin/IDV.sh
 - <FIC_HOME>/ficdb/bin/FCCDATAMOVEMENT.sh
 - <FIC_HOME>/ficdb/bin/PTC_Auto_Case_Assignment.sh
 - <FIC_OME>/ficdb/bin/NNS.sh
 - <FIC_HOME>/ficdb/bin/Case_Assignment.sh
 - <FIC_HOME>/ficdb/bin/BD_populate_common_processing_from_ipe.sh

7.19 Configuring FSDF

This section describes the configurations for Financial Services Data Foundation (FSDF).

Topics:

- [Configuring CSA Staging Tables](#)
- [Configuring FSDF in Different Infodom \(Pack on Pack Installation\)](#)

NOTE Release 8.1.2.0.0 uses the BD-AM slice of Oracle FSDF 8.1.2.1.0.

7.19.1 Configuring CSA Staging Tables

If BD and CSA tables are in same schema, run the following SQL file in Atomic schema available in the path <download_dir>/OFS_BD_PACK/OFS_AML:

FSDFAlterTimezone.sql

7.19.2 Configuring FSDF in Different Infodom (Pack on Pack Installation)

Topics:

- [Upgrade installation from BD 8.1.X.X.X to BD 8.1.2.0.0](#)
- [Standalone OFSBD 8.1.2.0.0 Installation](#)

7.19.2.1 Upgrade installation from BD 8.1.X.X.X to BD 8.1.2.0.0

If BD and FSDF/OIDF are in different Infodom, follow these steps:

1. Run the upgrade installer with FSDF_UPLOAD_MODEL= 0 in PatchConfig.xml
OFS_BD_PACK/OFS_AML/conf
2. Execute the following SQL files in FSDF Atomic schema, available in the path /OFS_BD_PACK/OFS_AML.

FSDFAlterTimezone.sql

NOTE Drop all the staging tables in the BD atomic schema using the below [SQL files](#)

drop_script - BD FSDF 81210 Staging Tables - FCCM 812 Release.sql

drop_script - BD OIDF 81210 Staging Tables - FCCM 812 Release.sql

See [STG tables](#) for list of staging tables of BD-AM slice of Oracle FSDF 8.1.2.1.0.

3. Run the following script in BD Atomic schema, after replacing placeholder ##FSDF_USER## with FSDF Atomic user name in - *INGESTUSERSYNONYMFORFSDFSTGSCHEMAOWNER.sql*.
4. Run the following script in FSDF Atomic schema, after replacing placeholder ##FCCM_USER## with BD Atomic user name in - *FsdfStgSchemaOwnergrant.sql*.

If BD and FSDF are in different Infodoms and client doesn't have different OIDF infodom, follow these steps:

1. Run the upgrade installer with `FSDF_UPLOAD_MODEL= 0` in `PatchConfig.xml`
`OFS_BD_PACK/OFS_AML/conf`
2. Execute the following SQL files in FSDF Atomic schema, available in the path `/OFS_BD_PACK/OFS_AML`.
`FSDFAlterTimezone.sql`

NOTE Drop only FSDF staging tables in the BD atomic schema using the below SQL file attached
`drop_script - BD FSDF 81210 Staging Tables - FCCM 812 Release.sql`

3. Run the following script in BD Atomic schema, after replacing placeholder `##FSDF_USER##` with FSDF Atomic user name in - `INGESTUSERSYNONYMFORFSDFSTGSCHEMAOWNER.sql`.

NOTE Ignore the ORA errors for the OI DF tables:

```
(STG_INS_POLICY_FEATURE_MAP,
STG_LIFE_INS_CONTRACTS,
STG_LIFE_INS_POLICY_TXNS,
STG_PARTY_INS_POLICY_ROLE_MAP,
STG_INS_SELLER_LICENSE)
```

4. Run the following script in FSDF Atomic schema, after replacing placeholder `##FCCM_USER##` with BD Atomic user name in - `FsdfStgSchemaOwnergrant.sql`.

NOTE Ignore the ORA errors for the OI DF tables:

```
STG_INS_POLICY_FEATURE_MAP,
STG_LIFE_INS_CONTRACTS,
STG_LIFE_INS_POLICY_TXNS,
STG_PARTY_INS_POLICY_ROLE_MAP,
STG_INS_SELLER_LICENSE)
```

7.19.2.2 Standalone OFSBD 8.1.2.0.0 Installation

If BD and FSDF/OI DF are in different Infodoms, follow these steps:

1. Run the BD812 installer with `FSDF_UPLOAD_MODEL= 0` in `default.properties`
`OFS_BD_PACK/OFS_AML/conf/default.properties`.
2. Execute the following SQL files in FSDF Atomic schema, available in the path `/OFS_BD_PACK/OFS_AML`.
`FSDFAlterTimezone.sql`

NOTE Dropping the staging tables is not required.

3. Run the following script in BD Atomic schema, after replacing placeholder `##FSDF_USER##` with FSDF Atomic user name in - `INGESTUSERSYNONYMFORFSDFSTGSCHEMAOWNER.sql`.
4. Run the following script in FSDF Atomic schema, after replacing placeholder `##FCCM_USER##` with BD Atomic user name in - `FsdfStgSchemaOwnergrant.sql`.

If BD and FSDF are in different Infodoms and client doesn't have different OI DF infodomain, follow these steps:

1. Run the BD812 installer with `FSDF_UPLOAD_MODEL= 1` in `default.properties`
`OFS_BD_PACK/OFS_AML/conf/default.properties`
2. Execute the following SQL files in FSDF Atomic schema, available in the path `/OFS_BD_PACK/OFS_AML`.
`FSDFAlterTimezone.sql`

NOTE Drop only FSDF staging tables in the BD atomic schema using the below SQL file attached

`drop_script - BD FSDF 81210 Staging Tables - FCCM 812 Release.sql`

3. Run the following script in BD Atomic schema, after replacing placeholder `##FSDF_USER##` with FSDF Atomic user name in `- INGESTUSERSYNONYMFORFSDFSTGSCHEMAOWNER.sql`.

NOTE Ignore the ORA errors for the OI DF tables:

```
(STG_INS_POLICY_FEATURE_MAP,
STG_LIFE_INS_CONTRACTS,
STG_LIFE_INS_POLICY_TXNS,
STG_PARTY_INS_POLICY_ROLE_MAP,
STG_INS_SELLER_LICENSE)
```

4. Run the following script in FSDF Atomic schema, after replacing placeholder `##FCCM_USER##` with BD Atomic user name in the below SQL:

- `FsdfStgSchemaOwnergrant.sql`

NOTE • Ignore the ORA errors for the OI DF tables:

```
(STG_INS_POLICY_FEATURE_MAP,
STG_LIFE_INS_CONTRACTS,
STG_LIFE_INS_POLICY_TXNS,
STG_PARTY_INS_POLICY_ROLE_MAP,
STG_INS_SELLER_LICENSE)
```

- In case on pack on pack installation, the `FSI_PARTY_RIGHT_TO_FORGET` table must be manually created. To do this, run the following code:

```
create table FSI_PARTY_RIGHT_TO_FORGET (
FIC_MIS_DATEDATE not null,
V_PARTY_IDVARCHAR2(20 CHAR) not null,
V_PARTY_FORGET_REASON VARCHAR2(100 CHAR)
not null
);
```

7.20 Configurations for ECM Integration (Applicable only for Promote to Case Action in KYC)

Perform the following procedure to integrate Enterprise Case Management (ECM) with OFS BD application. The process varies when OFS ECM and OFS BD are installed in different databases and OFS ECM and OFS BD are installed within the same database.

NOTE

If you are performing pack on pack installation of OFS ECM v8.0.7.0.0 on existing OFS BD v8.0.7.0.0, the following columns with provided values are generated in the KDD_PRCNG_BATCH_CONTROL table. For further Batch Execution and Ingestion, these columns must be truncated.

- *PRCSNG_BATCH_ID* - -1
- *DATA_DUMP_DT* - 11/16/2017 3:16:07 PM
- *PRCSNG_BATCH_NM* - ECM
- *EOD_PRCNG_BATCH_FL* - Y

Topics:

- [ECM and BD Installed in Different Databases](#)
- [ECM and BD Installed in the Same Database](#)

7.20.1 ECM and BD Installed in Different Databases

If the ECM and BD are installed in different databases, follow these steps:

1. Replace placeholders with corresponding values and execute the following SQL query. This has to be executed by the AM sys user, who has SYSDBA role:

```
Create public database link AMDBLINK connect to <ECM_ATOMIC_USER>
IDENTIFIED BY <ECM_ATOMIC_PWD> using '<CM_TNS_ENTRY>'
```

 - *<ECM_ATOMIC_USER>* - This variable must be replaced with ECM atomic schema User ID.
 - *<ECM_ATOMIC_PWD>* - This variable must be replaced with ECM atomic User Password.
 - *<CM_TNS_ENTRY>* - This variable must be replaced with the ECM Database TNS Entry.
2. Update the file *install.cfg* available in the location *<FIC_HOME>/database/db_tools/mantas_cfg* with the correct values for the following variables:
 - *casemng.schema.owner* - ECM Atomic schema user
 - *caseschema.schema.owner* - ECM Atomic schema user
 - *extract.schema.case* - ECM Atomic schema user
 - *load.schema.case* - ECM Atomic schema user
3. Update the file *db_variables.cfg* available in the location *<FIC_HOME>/database/db_tools/mantas_cfg* with the correct values for the following variables:
 - *case_schema_owner* - ECM Atomic schema user
 - *AMINFODOM* - Alert Management Infodom name.
4. Add the path of the SQL files in the *DB_LINK.cfg* and *DB_LINK_CASE.cfg* files. The path for *DB_LINK.cfg* file is *installer/OFS_BD_PACK/OFS_BD/BDPostScripts/differentDB*. If not, an error is displayed.

For example, in the .cfg file one of the SQL files is called `TABLE_SYNONYM_DBLINK.sql`, so in front of this file user has to mention the path of the SQL file. So the value in the .cfg file will be as follows:

```
/scratch/ofsaapp/BE85E87/installer/OFS_BD_PACK/OFS_
BD/BDPPostScripts/differentDB/TABLE_SYNONYM_DBLINK.sql
```

5. Execute the following commands using the DB builder utility.

- a. Navigate to the differentDB folder mentioned above.
- b. Run the following command to execute the .cfg file using the db builder utility:

```
../../../../../../../../<FIC_HOME>/database/db_tools/bin/
run_dbbuilder_utility.sh /installer/OFS_BD_PACK/OFS_BD/BDPPostScripts/
differentDB/DB_LINK.cfg

../../../../../../../../ indicates that you need to go back to the <FIC_HOME>
path from the differentDB folder.
```

6. To run the DBLink_CASE.cfg file, modify the `utils.database.urlName=` parameter name in the `install.cfg` file with the ECM JDBC URL.
7. In the `utils.database.urlName=` parameter, replace the existing JDBC URL with the Enterprise Case Management (ECM) JDBC URL and execute.

```
../../../../../../../../<FIC_HOME>/database/db_tools/bin/ run_dbbuilder_
utility.sh /installer/OFS_BD_PACK/OFS_BD/BDPPostScripts/differentDB/
DB_LINK_CASE.cfg
```

NOTE

If After you execute the above command, replace the ECM JDBC URL with the Alert Management (AM) JDBC URL.

7.20.2 ECM and BD Installed in the Same Database

If the ECM and BD are installed in the same database, follow these steps:

1. Update the file `install.cfg` available in the location `<FIC_HOME>/database/db_tools/mantas_cfg` with the correct values for the following variables:
 - `casemng.schema.owner` - ECM Atomic schema user
 - `caseschema.schema.owner` - ECM Atomic schema user
 - `extract.schema.case` - ECM Atomic schema user
 - `load.schema.case` - ECM Atomic schema user
2. Update the file `db_variables.cfg` available in the location `<FIC_HOME>/database/db_tools/mantas_cfg` with the correct values for the following variables:
 - `case_schema_owner` - ECM Atomic schema user
 - `AM_INFODOM` - Alert Management Infodomain name.
3. Add the path of the SQL files in the `SAME_DB.cfg` file. The path for `SAME_DB.cfg` file is `<download_dir>/OFS_BD_PACK/OFS_AML/BDPPostScripts/sameDB`. If not, an error is displayed.

For example, in the .cfg file one of the SQL files is called `TABLE_SYNONYM.sql`, so in front of this file you must mention the path of the SQL file. So the value in the .cfg file will be as follows:

```
<download_dir>/OFS_BD_PACK/OFS_AML/BDPostScripts/sameDB/  
TABLE_SYNONYM.sql
```

4. Execute the following commands using the DB builder utility:

- a. Navigate to the sameDB folder mentioned above.
- b. Run the following command to execute the .cfg file using the db builder utility:

```
../../../../../../../../<FIC_HOME>/database/db_tools/bin/  
run_dbbuilder_utility.sh /installer/OFS_BD_PACK/OFS_BD/BDPostScripts/  
sameDB/SAME_DB.cfg
```

../../../../../../../../ indicates that you need to go back to the <FIC_HOME>
path from the sameDB folder.

8 Post Deployment Configuration

This section provides detailed information about the Post Deployment Configurations. Lists the various configurations to be completed before you use the OFSAA Applications.

Topics:

- [Creating Application Users](#)
- [Mapping Application User\(s\) to User Group](#)
- [Performing Administrative activities for OFS BD](#)
- [Performing Configurations for OFS BD](#)
- [Setting OFS BD UI as Home Page of OFSAAI for a Particular User](#)
- [Modifying Additional Configuration Files](#)
- [Changing ICC Batch Ownership](#)

8.1 Creating Application Users

NOTE

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

For more information, see the *User Creation* section in [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

8.2 Mapping Application User(s) to User Group

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

User Groups seeded with the OFS BD Application Pack are listed in [Table 20](#).

Table 20: Seeded User Groups

Name	Description
Modeler Group	User mapped to this group have access to all the menu items for Enterprise modeling, but do not have authorization rights for sandbox population, model deployment and modeling technique authorization.
Modeling Administrator Group	User mapped to this group have access to all the menu items for Enterprise modeling and authorization rights for sandbox population, model deployment and modeling technique authorization.
Inline Processing Admin Group	User mapped to this group have access to all the menu items and actions for Inline Processing module.
Business Administrator	User mapped to this group have access to all the menu items and actions for advanced operations of metadata objects.
Business Authorizer	User mapped to this group have access to all the menu items and actions for authorization of changes to metadata objects.

Table 20: Seeded User Groups

Name	Description
Business Owner	User mapped to this group have access to all the menu items and actions to read and write metadata objects
Business User	User mapped to this group have access to all the menu items and actions to access and read metadata objects.
Identity Administrator	User mapped to this group have access to all the menu items to manage User entitlements, User Group Entitlements and Access Management configurations.
Identity Authorizer	User mapped to this group have access to all the menu items to authorize User entitlements, User Group Entitlements and Access Management configurations.
System Administrator	User mapped to this group have access to all menu items to manage the setup configurations.
Object Administrator	User mapped to this group have access to all menu items to manage object migration and metadata traceability using metadata browser.
Guest Group	User mapped to this group have access to certain menu items with view only access privileges.

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.

NOTE

In case the User Groups related to OFS BD are not mapped, ensure that you map it accordingly in OAS 5.9 catalog for Statement View report.

In order to view the MIS reports in BD Standalone, map the Case Analyst2 User Group in the Application.

For more information, see Mapping/Unmapping Users section from the [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

8.3 Performing Administrative activities for OFS BD

Access the OFS BD UI as BDAP Administrator and perform all the steps given in the following sections of the [BD Administration Guide](#).

- About Configuring Access Control Metadata
- Mapping Users To Access Control Metadata
- About Scenario Manager Login Accounts
- About Changing Passwords for System Accounts
- About Configuring File Type Extensions
- About Configuring File Size
- About Configuring Status To User Role Table

NOTE

Once Security Attributes mapping is completed for the BDAP Administrator user, restart OFSAAI and Web Application servers before accessing the Admin Tools application.

8.4 Performing Configurations for OFS BD

Access the OFS BD UI as BDAP Administrator and perform all the steps given in the following sections of [BD Configuration Guide](#).

- Configuring the Base Time Zone
- Configuring the Default Currency Code
- Configuring E-mail
- Configuring XML Export
- Configuring Case Correlation Owner
- Configuring Default Case Owner

8.5 Setting OFS BD UI as Home Page of OFSAAI for a Particular User

To set OFS BD UI as home page of OFSAAI, follow these steps:

1. Log in as an BD Administrator/Supervisor user.
2. Navigate to Home page.
3. Click on logged in user name in the right top corner.
4. Click Preferences and a new page is displayed.
5. Select Behavior Detection as your default page and click Save.

8.6 Modifying Additional Configuration Files

You can modify the following additional configuration files (although it is not a requirement that you modify them to run the system).

NOTE

This step is optional.

DataIngest.properties: This file (located in the ingestion_manager/config subdirectory) contains the variable values you specified in the silent properties file, including information about database configuration values, and schema specifications. For more information on configuring this file, see [Oracle Financial Services Behavior Detection Applications Pack Administration and Configuration Guide](#).

DataIngest.xml: This file (located in the /<OFS BD Installed Directory>/ingestion_manager/config subdirectory) contains the configuration settings required to configure each Ingestion Management runtime component. For example, setting up and configuring the number of threads used by each component. For more information on configuring this file, see [Oracle Financial Services Behavior Detection Applications Pack Administration and Configuration Guide](#).

8.7 **Changing ICC Batch Ownership**

This section is not applicable for OFS BD Applications Pack.

9 Appendix A: Configure the Web Server

Topics:

- [Configuring Web Server](#)
- [Configuring Web Application Servers](#)
- [Configure WebLogic for Application Deployment](#)
- [Configure Apache Tomcat Server for Application Deployment](#)

9.1 Configuring Web Server

This step assumes the installation of a web server exists as per the prerequisites.

Refer to the product-specific installation guide to install and configure the web server. If an installation already exists, skip, and proceed to the next step..

NOTE

- Make a note of the IP Address/ Hostname and Port of the web application server. This information is required during the installation process (required if the 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 the OFSAA Secure Configuration Guide/Security Guide mentioned in the [Related Documents](#) section for additional information on securely configuring your web server.

9.2 Configuring Web Application Servers

This step assumes an installation of a web application server exists as per the prerequisites. To configure the Web application server for OFSAA Deployment see the following sections.

Topics:

- [Configure WebSphere Application Server for Application Deployment](#)
- [Configuring WebSphere before Application Deployments](#)
- [Create a New Profile in WebSphere](#)
- [Manage IBM WebSphere SDK Java Technology Edition Versions](#)
- [Manage Applications in WebSphere](#)
- [Configure Websphere Application Server to Initialize Filters before Initializing Load-On-Startup Servlets and Allowing Empty Servlets Maps](#)
- [Configure WebSphere Application Server Persistence to JPA Specification 2.0](#)
- [Configure Websphere Application Server to Use a Load Balance or Proxy Server](#)
- [Delete WebSphere Profiles](#)
- [Configuring WebSphere Shared Library to Support Jersey 2x and Jackson 2.9x Libraries](#)

- [Configure WebSphere HTTPS](#)
- [Configure WebSphere Memory Settings](#)
- [Configure WebSphere for REST Services Authorization](#)
- [Configuring Application Security in WebSphere](#)

NOTE

For upgrade from OFS BD 8.0.2.0.0 to OFS BD 8.1.2.0.0 perform the following:

- Remove the persistence.xml from ficweb/webroot/WEB-INF/classes/META-INF/ , regenerate the .ear and war files and re-deploy the application
- Remove the AM folder if available from /ficweb/AM(example /ficweb/AM/AM). Then regenerate EAR/WAR files and deploy.nd.

9.2.1 Configure WebSphere Application Server for Application Deployment

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

9.2.2 Configuring WebSphere before Application Deployments

Before deployment, ensure that you Follow these steps to configure PMF for websphere:

1. Navigate to web.xml file in the <FIC_HOME>/ficweb/webroot/WEB-INF path.
2. Add com.ofs.aai.rest.v1.impl.WSService;com.ofs.aai.rest.v1.service.wf.P MFService as shown:

```
<param-value>com.ofs.aai.rest.v1</param-value>
</init-param>
<init-param>
<param-name>jersey.config.server.provider.classnames</param-name>
<param-value>com.ofs.aai.rest.v1.service.impl.UserService;com.ofs.a
ai.rest.v1.service.impl.FunctionService;com.ofs.aai.rest.v1.service
.impl.GroupService;com.ofs.aai.rest.v1.service.impl.RoleService;com
.ofs.aai.rest.v1.service.impl.Infodom;
com.ofs.aai.rest.v1.report.impl.l18nService;com.ofs.aai.rest.v1.rep
ort.impl.ActionService;com.ofs.aai.rest.v1.report.impl.AuditTrailSe
rvice;com.ofs.aai.rest.v1.report.impl.ReportService;
com.ofs.aai.rest.v1.impl.DBDetailServices;com.ofs.aai.rest.v1.impl.
LogService;com.ofs.aai.rest.v1.impl.Services;com.ofs.aai.rest.v1.im
pl.WSService;com.ofs.aai.rest.v1.service.wf.PMFService
</param-value>
```

3. Delete the .ear and .war files from <FIC_HOME>/ficweb.

4. Execute the `ant.sh` file to recreate the `.ear` and `.war` files.

9.2.3 Create a New Profile in WebSphere

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

Use the following command to create a profile without admin security through the command line:

```
"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, refer to the WebSphere `manageprofiles` command.

9.2.4 Manage IBM WebSphere SDK Java Technology Edition Versions

By default, WebSphere Application Server V8.5.5.X uses 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.

Follow these steps to check the java version and set it to 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.
6. Click Java SDKs link from the Server Infrastructure section to view the list of Java SDKs.
7. Select 8.0_64.
8. Click Make Default and save to master repository.
9. Restart the WebSphere Application Server to apply the changes to the IBM application profile.

9.2.5 Manage Applications in WebSphere

To manage the installed applications in WebSphere, follow these steps:

1. Open the administrator console using the following URL:

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

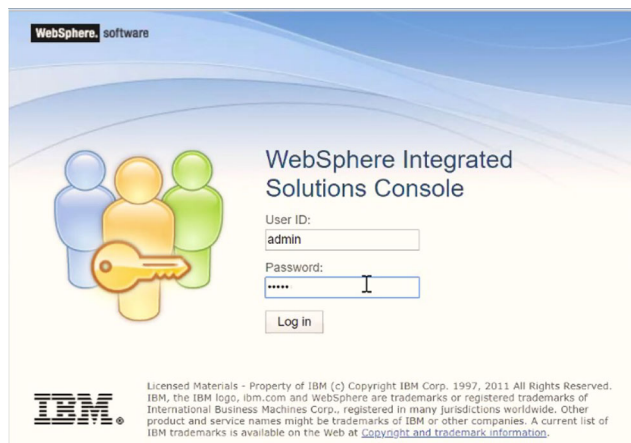
For example: `http://10.111.222.333:9003/ibm/console` (`https` if SSL is enabled.)

NOTE

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

The Integrated Solutions Console Login window is displayed.

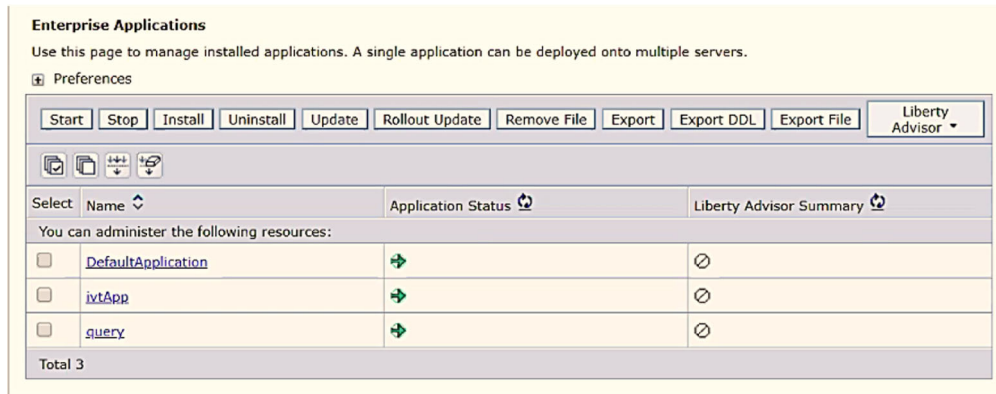
Figure 36: Integrated Solutions Console Login



2. Log in with the **User ID** provided with admin rights.

- From the LHS menu, expand the **Applications > Application Type> WebSphere Enterprise Applications** to display the Enterprise Applications window.

Figure 37: Enterprise Applications



This Enterprise Applications window helps you to:

- Install new application
- Uninstall existing applications
- Start or Stop the installed applications

9.2.6 Configure Websphere Application Server to Initialize Filters before Initializing Load-On-Startup Servlets and Allowing Empty Servlets Maps

The custom configuration information in this section initializes the filters before initializing loadonstartup servlets and allows empty servlet maps when you start an application.

NOTE

This is a mandatory configuration for OFSAA with WebSphere for both fresh and upgrade installation.

To configure custom properties for filters, follow these steps

- 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`.
- Log in with your administrator user ID and password.
- From the left menu, click Servers to expand the menu.
- Click Server Types to expand the menu further and then click WebSphere Enterprise Application Servers to view the Application servers window.
- On the Application servers window, click the required Application Server link.
- Click Web Container Settings and then Custom Properties to view the Custom Properties window.
- Click New and enter the following properties:
 - `com.ibm.ws.webcontainer.initFilterBeforeInitServlet` to true
 - `com.ibm.ws.webcontainer.invokeFilterInitAtStartup` to true
 - `com.ibm.ws.webcontainer.emptyServletMappings` to true.

8. Click OK and then click Save on the Console to save the customized configurations.
9. Restart the WebSphere Application Server to apply the changes.

9.2.7 **Configure WebSphere Application Server Persistence to JPA Specification 2.0**

The persistence configuration information in this section sets JPA 2.0 specification in WebSphere over the default JPA 2.1 specification.

NOTE This is a mandatory configuration for OFSAA with WebSphere for both fresh and upgrade installation.

To set the JPA 2.0 as the default persistence provider, follow these steps:

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. Log in with your administrator user ID and password.
3. From the LHS menu, click Servers to expand 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 the Application servers window, click the required Application Server link.
6. Click Container Services and then click Default Java Persistence API settings to display the Configuration window.
7. From the JPA Specification drop-down, select 2.0 to change the default JPA Specification from 2.1 to 2.0.
8. Click OK and then click Save on the Console to save the customized configurations.
9. Restart the WebSphere Application Server to apply the changes.

9.2.8 **Configure Websphere Application Server to Use a Load Balance or Proxy Server**

The configuration prevents the process server from redirecting to an internal port when using a load balancer or proxy server.

The following steps describe the configuration:

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. Log in 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 the Application servers window, click the required Application Server link. For example, `server1`.
6. Click Web Container Settings and then Custom Properties to view the Custom Properties window.

7. Click New and enter the following properties:
 - a. `com.ibm.ws.webcontainer.extractHostHeaderPort: true`
 - b. `Trusthostheaderport: true`
8. Click OK and then click Save on the Console to save the customized configurations.
9. Restart the WebSphere Application Server to apply the changes.

9.2.9 Delete WebSphere Profiles

This section describes how to delete WebSphere profiles.

To delete a WebSphere profile, follow these steps:

1. Select the checkbox 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 the profile directory.
For example: `<WebSphere_Installation_Directory>/AppServer/profiles/
<profile_name>.`
6. Execute the command: `manageprofiles.sh -validateAndUpdateRegistry.`

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

This section describes how to set up WebSphere shared library to support jersey 2x and Jackson 2.9x libraries.

To set up WebSphere shared library to support jersey 2x and Jackson 2.9x libraries, follow these steps:

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 the following details:
 - 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>/ficweb/webroot/externallib/WEBINF/lib/` directory after creation of the EAR file. Another format of representation of the Path is `<ofsaa_deployed_area_location>/externallib/WEBINF/lib/`.
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.
6. From the Shared Library Mapping window, move the required shared libraries from Available to 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. Navigate to the WebSphere admin console in Servers > WebSphere Application Servers > yourServerName.
 - b. In the Server Infrastructure section, go to Java and Process Management > Process definition > Java Virtual Machine > Custom properties.
 - c. Add the following property:
 - d. `com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine=true`
10. Restart the application.

9.2.11 Configure WebSphere HTTPS

To configure an HTTPS Transport on WebSphere, follow these steps:

1. Create a profile using the Profile Creation Wizard in WebSphere.

NOTE

Record the https port specified during this process and use it as a servlet port or web server port during OFSAAI installation.

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

9.2.12 Configure WebSphere Memory Settings

To configure the WebSphere Memory Settings, follow these steps:

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

9.2.13 Configure WebSphere for REST Services Authorization

For more information, see [OFS Analytical Applications Infrastructure Administration Guide](#).

9.2.14 Configuring Application Security in WebSphere

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

9.3 Configure 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 the WebLogic Application Server.

NOTE

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

Following configuration is required only if OFS Big Data Processing is licensed and enabled in your OFSAA instance and OFSAA is deployed on Oracle WebLogic Server version 12.2.x:

The jersey-server-1.9.jar file must be copied to <HIVE_LIB_PATH> path.

Topics:

- [Update WebLogic Server](#)
- [Create Domain in WebLogic Server](#)
- [Delete Domain in WebLogic](#)
- [Configure WebLogic Memory Settings](#)
- [Configuring WebLogic for REST Services Authorization](#)

9.3.1 Update WebLogic Server

Before proceeding with the domain creation, download and install the latest WLS PSU for 14.1.1 from [My Oracle Support](#).

After applying this patch, set the java option flag `-Dweblogic.http.disablehttp2=true` before starting servers.

For more information, see *Configure WebLogic for Application Deployment* in [AAI installation Guide](#).

9.3.2 Create Domain in WebLogic Server

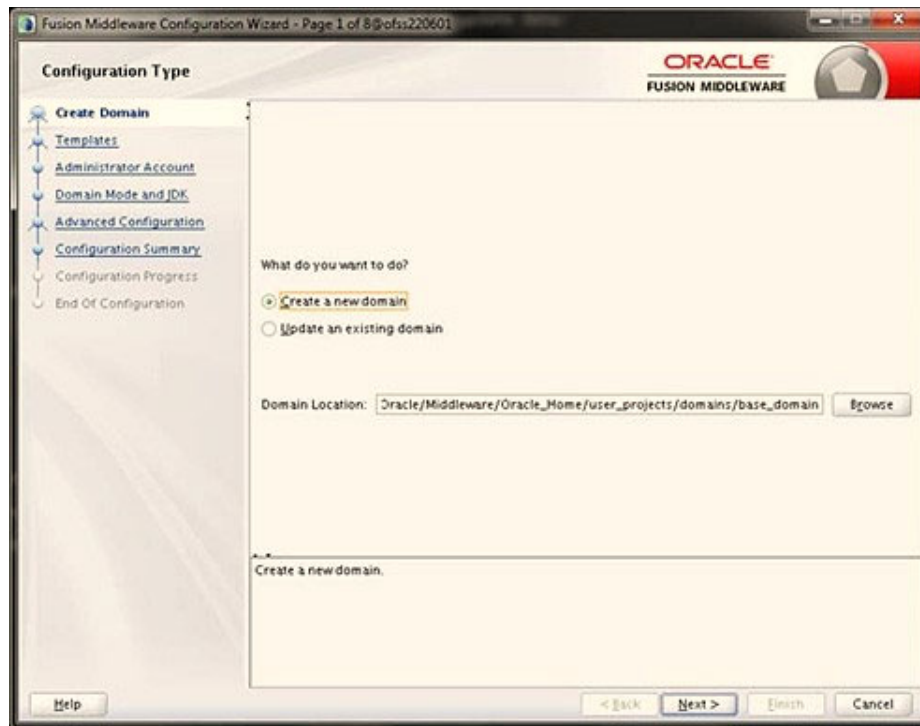
To create a new domain using Configuration Wizard in WebLogic, follow these steps:

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

```
./config.sh
```

The Welcome window of the Configuration Wizard is displayed.

Figure 38: Configuration Type



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

Figure 39: Templates



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

Figure 40: Administrator Account

The screenshot shows the 'Administrator Account' configuration window. On the left is a navigation pane with steps: Create Domain, Templates, Administrator Account (selected), Domain Mode and JDK, Advanced Configuration, Configuration Summary, Configuration Progress, and End Of Configuration. The main area has three input fields: 'Name' (containing 'weblogic'), 'Password', and 'Confirm Password'. Below these fields is a note: 'User name may not contain commas, tabs, or any of the following characters: <>#[]{}()'. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

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

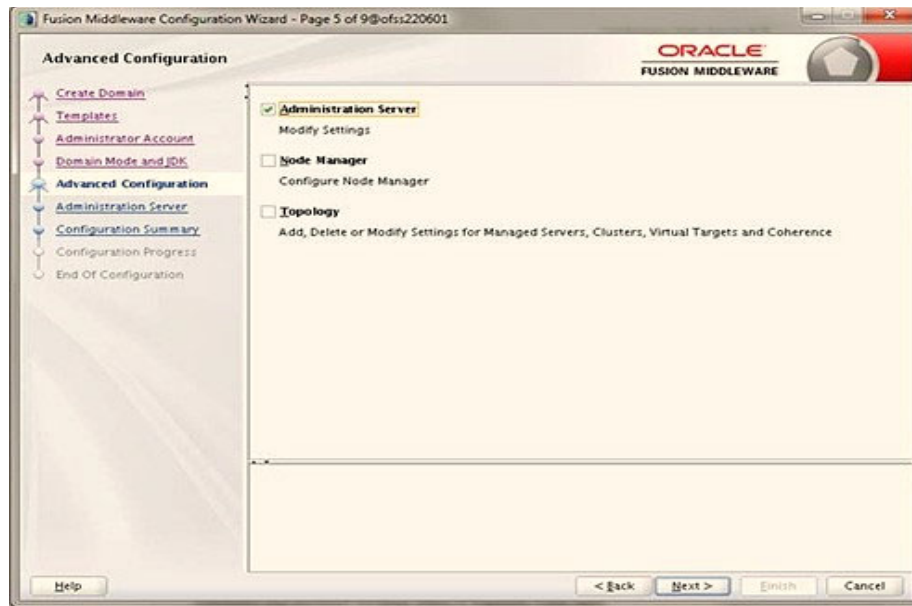
Figure 41: Domain Mode and JDK

The screenshot shows the 'Domain Mode and JDK' configuration window. The left navigation pane is the same as in Figure 40, with 'Domain Mode and JDK' selected. The main area has two sections. The 'Domain Mode' section has two radio buttons: 'Development' (selected) and 'Production'. Below 'Development' is the text: 'Utilize boot properties for username and password, and poll for applications to deploy.' Below 'Production' is the text: 'Require the entry of a username and password, and do not poll for applications to deploy.' The 'JDK' section has two radio buttons: 'Oracle HotSpot 1.8.0_45 /usr/java/jdk1.8.0_45' (selected) and 'Other JDK Location:'. There is a text input field for the 'Other JDK Location' and a 'Browse' button next to it. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

5. Select from the following options:
 - In the Domain Mode section, select the required mode (Development or Production).

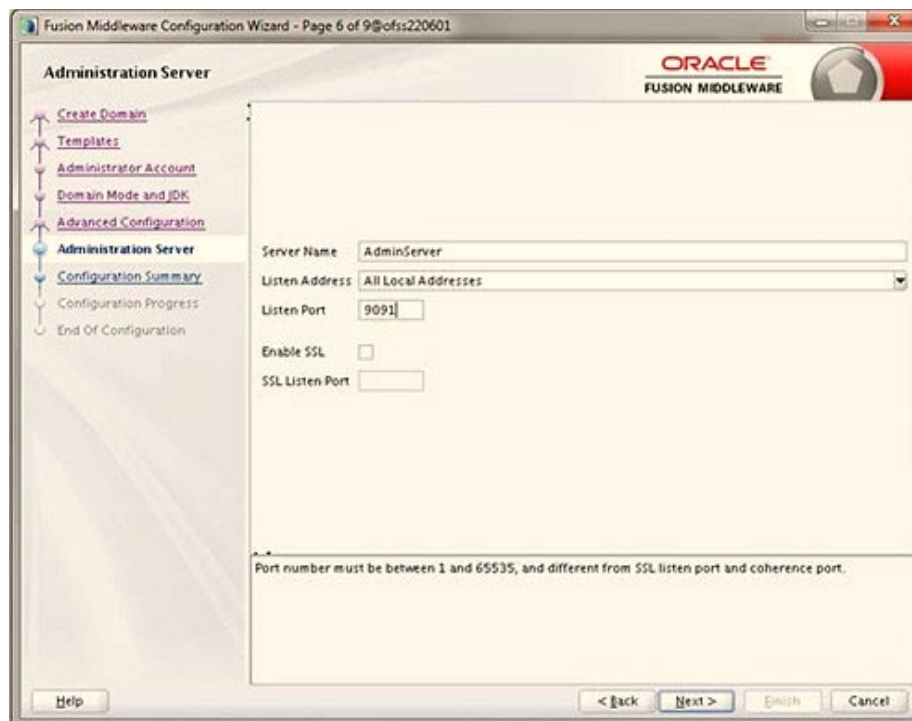
- In the JDK section, select the required option. If you select **Other JDK Location**, click **Browse**, navigate to the JDK location, and select. Click **Next** to display the Advanced Configuration window.

Figure 42: Advanced Configuration



6. Select the **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.

Figure 43: Administration Server

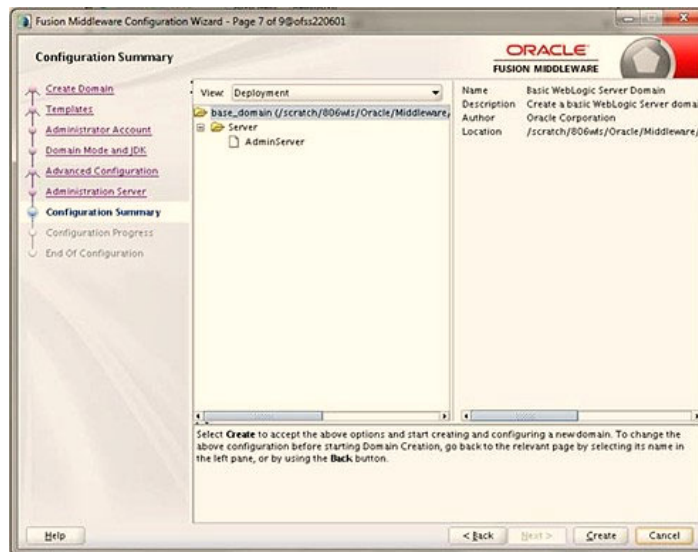


7. Enter Administration Server details such as the **Server Name**, **Listen address**, **Listen Port**, **Enable SSL** (for secure login using https, select this check box), and **SSL Listen Port**. Click **Next** to display the Configuration Summary window.

NOTE

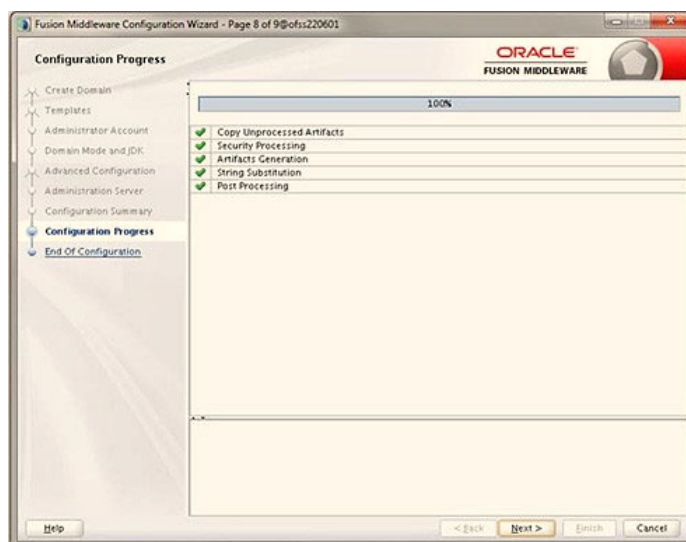
Make a note of the Listen Port or SSL Listen Port value (for example: 7007) since the same has to be re-entered in the Servlet port field during Infrastructure installation.

Figure 44: Configuration Summary



8. Verify the configuration details of the WebLogic domain and click **Create** to display the Configuration Progress window with the status indication of the domain creation process.

Figure 45: Creating Domain



9. Click **Next** when 100% of the activity is complete. The End of Configuration window is displayed.

Figure 46: End of Configuration



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

NOTE

- Record the HTTPS port specified during this process and use it as a 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.

11. Add a java option entry `-DUseSunHttpHandler=true` in the `WLS_HOME/bin/"setDomainEnv.sh"` file (Required only if a self-signed certificate is used).
12. Add a Java option entry `-Dweblogic.http.disablehttp2=true` in the `WLS_HOME/bin/"setDomainEnv.sh"` file , to ensure that the HTTP2 is disabled and only HTTP 1.1 is used as a protocol.

9.3.3 Delete Domain in WebLogic

To delete a domain in WebLogic, follow these steps:

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.

9.3.4 Configure WebLogic Memory Settings

To configure the WebLogic Memory Settings, follow these steps:

1. Change the memory setting for Java Heap to `-Xms512m -Xmx3072m` in the `setDomainEnv.sh` file, which resides in the `<DOMAIN_HOME>/bin` directory and the `CommEnv.sh` file which resides in the `common/bin` directory.
2. 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"
```

9.3.5 Configuring WebLogic for REST Services Authorization

To enable REST API authorization by OFSAA in WebLogic, follow these steps:

1. Open the `config.xml` file located in the domain where OFSAA is deployed - `<domain_home>/config/config.xml`.
2. Add the the security-configuration tag: `<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>`.

9.4 Configure Apache Tomcat Server for Application Deployment

This section is applicable only when the Web application server type is Tomcat.

Topics:

- [Tomcat User Administration](#)
- [Configuring Tomcat to use JAVA 64 bit Executables](#)
- [Configure Servlet Port](#)
- [Configure SSL Port](#)
- [Configure Apache Tomcat Memory Settings](#)
- [Configuring Axis API](#)
- [Configure Tomcat for User Group Authorization and Data Mapping](#)
- [Uninstall WAR Files in Tomcat](#)

9.4.1 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 follows:

NOTE

This file contains an XML `<user>` for each user that will display the username and password used by the admin to log in 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 username/password combinations as shown in the preceding example.
2. Use the same username/password to which the manager role is assigned to access the Tomcat Application Manager.

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

9.4.2 Configuring Tomcat to use JAVA 64 bit Executables

To configure Tomcat to use JAVA 64 bit, follow these steps:

1. Navigate to the `$CATALINA_HOME/bin` folder.
2. Edit the `setclasspath.sh` file as follows:

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
```

3. 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
```

9.4.3 Configure Servlet Port

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

If you must use a different port number, you must first configure the port in the `server.xml` file in the `conf` directory of the Tomcat Installation directory. To configure the Servlet Port, follow these steps:

1. Navigate to `$CATALINA_HOME/conf`. Open `server.xml` and locate the tag: "Define a non-SSL HTTP/1.1 Connector on port 8080 "

Against this tag, a parameter is specified '`Connector port = "8080"`'. Edit this value to the new port number that was used during the Infrastructure installation process.

2. Save your changes in the `server.xml` file.

NOTE

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

9.4.4 Configure SSL Port

If you must 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 the

`<Tomcat_installation_directory>/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"/>
```

NOTENOTE

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

For more information related to SSL Configuration on Tomcat, see [Apache Tomcat](#).

9.4.5 Configure Apache Tomcat Memory Settings

To configure the Apache Tomcat Memory Settings, follow these steps:

1. Locate the `catalina.sh` file that resides in the `<CATALINA_HOME>/bin` directory.
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`. For 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

9.4.6 Configuring Axis API

To configure the Axis API, follow these steps:

1. Copy the *jaxrpc.jar* from the *<OFSAA Installation Directory>/axis-1_4/webapps/axis/WEB-INF/lib* folder.
2. Place the copied file in the *<Tomcat Installation Directory>/lib* folder.
3. Restart the Tomcat Server.

9.4.7 Configure Tomcat for User Group Authorization and Data Mapping

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

1. Navigate to the *\$CATALINA_HOME/conf* directory and open the *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.

9.4.8 Uninstall WAR Files in Tomcat

To uninstall WAR files in Tomcat, see [Uninstalling WAR Files in Tomcat](#).

10 Appendix B: Configure Resource Reference in Web Servers

Topics:

- [Configure Resource Reference in WebSphere Application Server](#)
- [Configure Resource Reference in WebLogic Application Server](#)
- [Configure Resource Reference in Tomcat Application Server](#)

10.1 Configure Resource Reference in WebSphere Application Server

This section is applicable only when the Web application server type is WebSphere.

Topics:

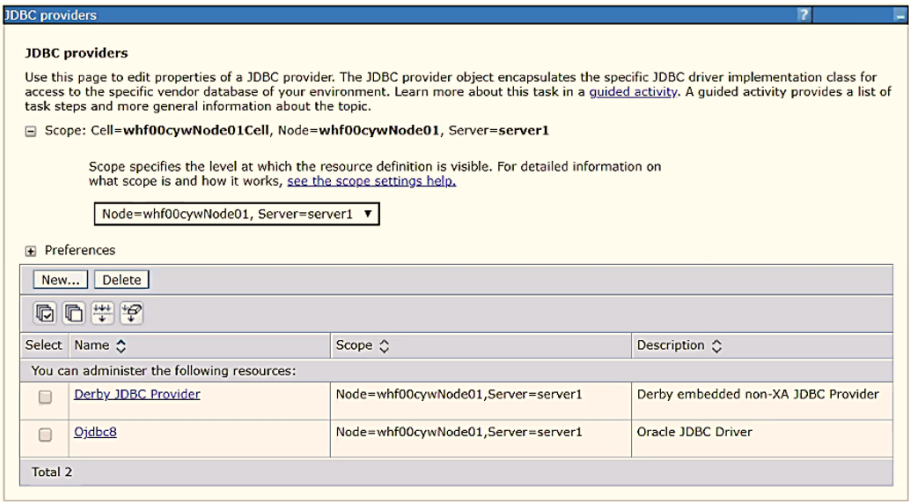
- [Create a JDBC Provider](#)
- [Create Data Source](#)
- [Create J2C Authentication Details](#)
- [Define JDBC Connection Pooling](#)

10.1.1 Create a JDBC Provider

To create the JDBC Provider in WebSphere Application Server, follow these steps:

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. Log in with the user ID with administrative privileges.
3. Expand the **Resources** option in the LHS menu and click **JDBC > JDBC Providers** to display the JDBC Providers window.

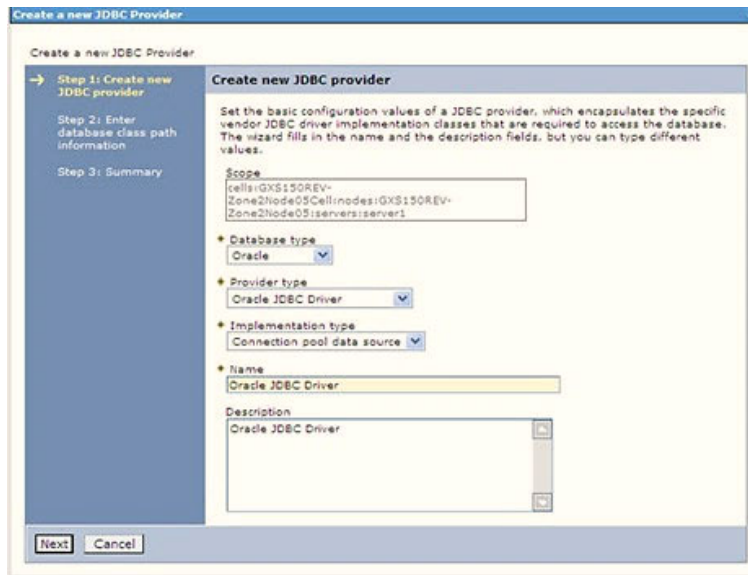
Figure 47: JDBC Providers



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

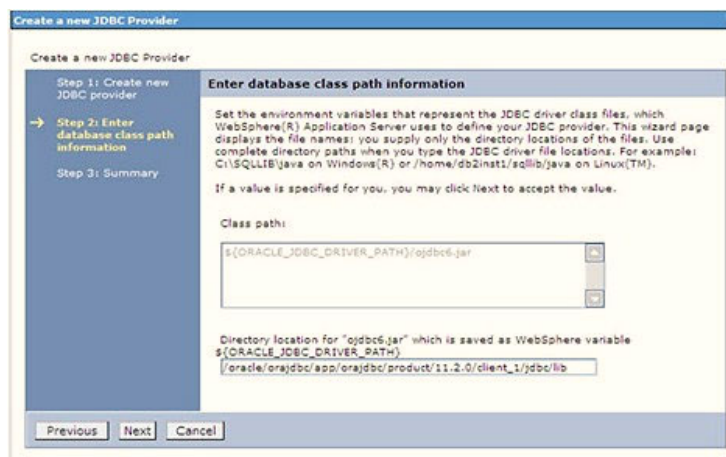
- Click **New** to add the new JDBC Provider under the Preferences section. The Create new JDBC Provider window is displayed.

Figure 48: Create a new JDBC Provider



- 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.
- Click **Next**.

Figure 49: Enter database class path information



- Specify the directory location for the ojdbc<version>.jar file. Do not use the trailing slash file separators.
- The Oracle JDBC driver can be downloaded from the following Oracle Download site:

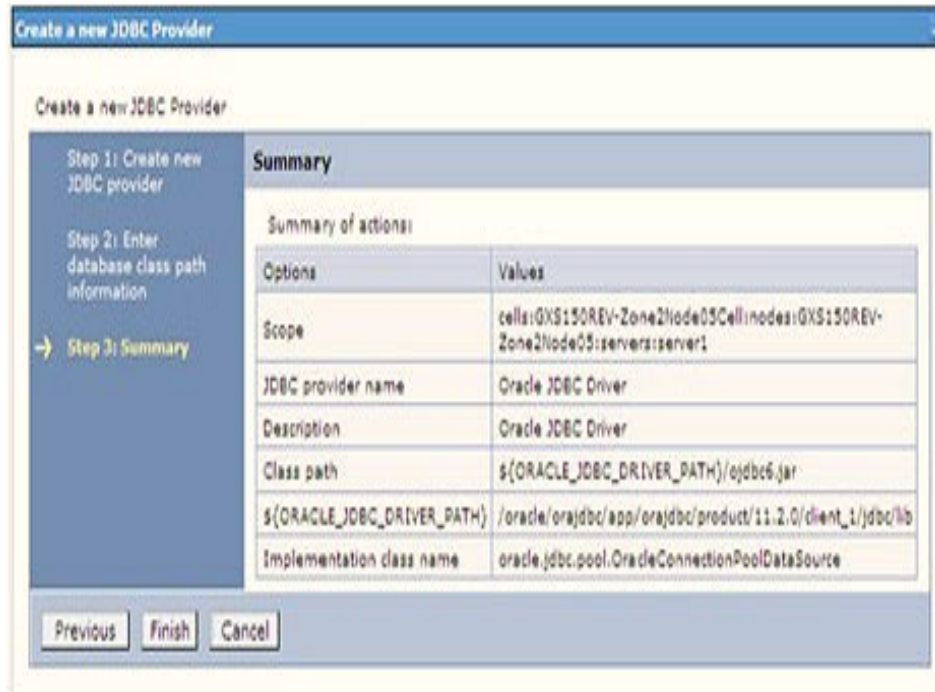
- Oracle Database 18cg Release 3 JDBC Drivers
- Oracle Database 19c Release 3 JDBC Drivers

After downloading, you must copy the file in the required directory on the server.

NOTE See [Hardware and Software Requirements](#) to identify the correct `ojdbc<version>.jar` file version to be copied.

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

Figure 50: Summary



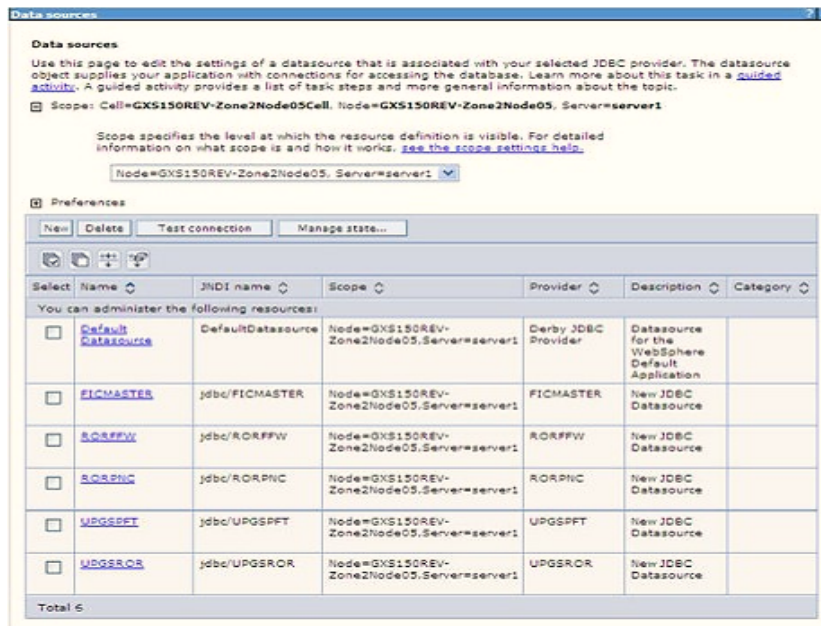
11. Verify the details and click **Finish** to create the JDBC Provider.
12. The options to **Save** and **Review** are displayed. Click **Save**.

10.1.2 Create Data Source

The following steps apply to both config and atomic data source creation. To create the data source, follow these steps:

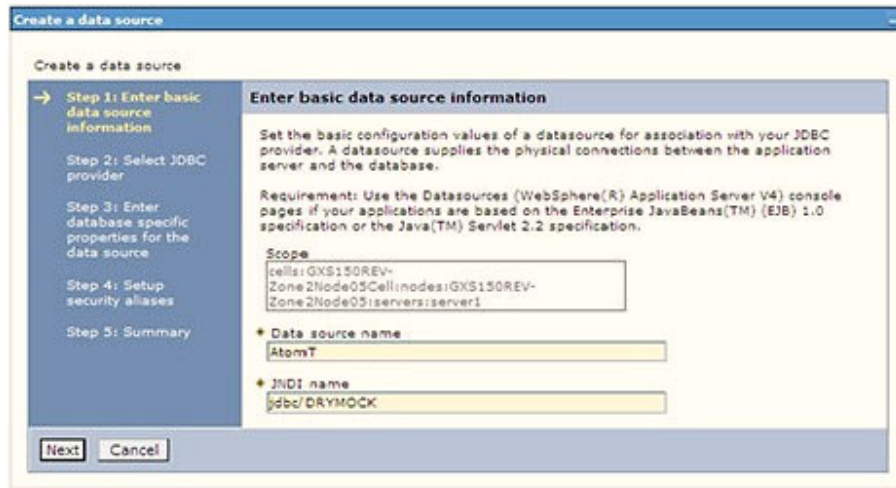
1. Open the following URL in the browser window: `http://<ipaddress>:<administrative console port>/ibm/console` (https if SSL is enabled). The Login window is displayed.
2. Log in with the user ID with administrative privileges.
3. Expand the **Resources** option in the LHS menu and click **JDBC > Data sources** to display the Data sources window.

Figure 51: Data Sources



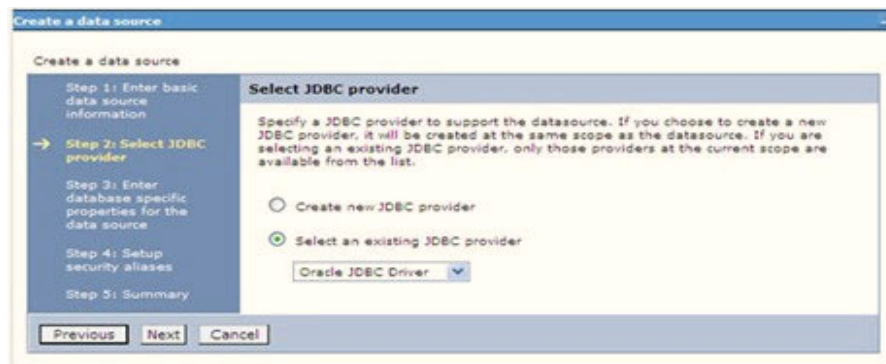
4. Select the **Scope** from the drop-down list. The scope specifies the level at which the resource definition is visible.
5. Click **New** to display the Create a Data Source window.

Figure 52: Create Data Source



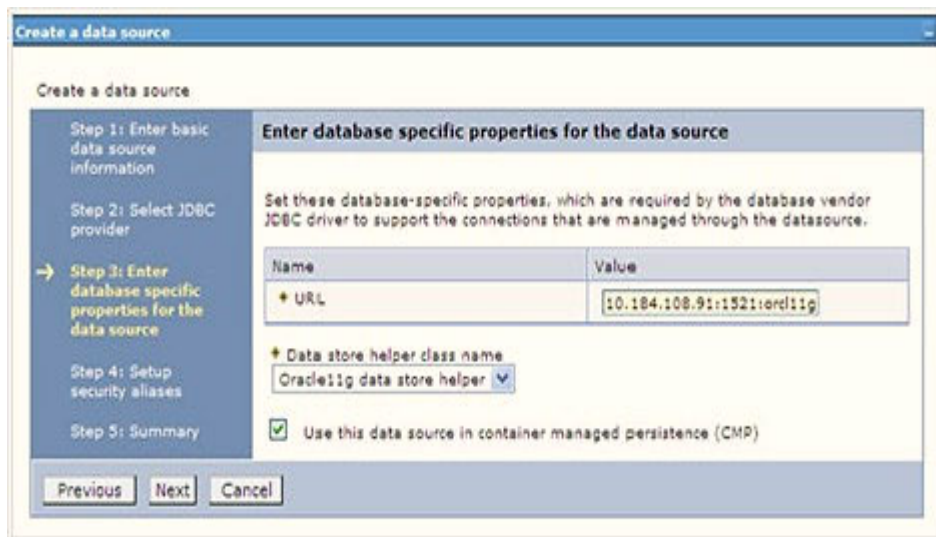
6. Specify the **Data source name** and **JNDI name** for the new "Data Source".
7. The **JNDI name** and **Data source name** are case sensitive and ensure that JNDI name is the same as the "Information Domain" name.
8. Click **Next** to display the Select JDBC provider window.

Figure 53: Select JDBC provider



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

Figure 54: Enter database specific properties



10. Specify the database connection URL.
For example: `jdbc:oracle:thin:@<DB_SERVER_IP>:<DB_SERVER_PORT>:<SID>`
11. Select **Data Store Helper Class Name** from the drop-down list and ensure that the **Use this data source in container managed persistence (CMP)** check box is selected.

NOTE For RAC configuration, provide the RAC URL specified during installation.

Example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=10.11.12.13)(port=1521))(ADDRESS=(PRO
TOCOL=TCP)(HOST=10.11.12.14)(PORT=1521))(LOAD_
BALANCE=no)(FAILOVER=yes))(CONNECT_DATA=(SERVICE_NAME=pqadb)))
```

12. Click **Next**.

Figure 55: Setup security parameters

Create a data source

Step 1: Enter basic data source information
Step 2: Select JDBC provider
Step 3: Enter database specific properties for the data source
→ Step 4: Setup security aliases
Step 5: Summary

Setup security aliases

Select the authentication values for this resource.

Component-managed authentication alias
(none)

Mapping-configuration alias
(none)

Container-managed authentication alias
(none)

Note: You can create a new J2C authentication alias by accessing one of the following links. Clicking on a link will cancel the wizard and your current wizard selections will be lost.

[Global J2C authentication alias](#)
[Security domain](#)

Previous Next Cancel

13. 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**.

Figure 56: Summary

Create a data source

Step 1: Enter basic data source information
Step 2: Select JDBC provider
Step 3: Enter database specific properties for the data source
Step 4: Setup security aliases
→ Step 5: Summary

Summary

Summary of actions:

Options	Values
Scope	cells:GX5150REV-Zone2Node03Cell:nodes:GX5150REV-Zone2Node03:servers:server1
Data source name	AtomT
JNDI name	jdbc/DRYMOCK
Select an existing JDBC provider	Oracle JDBC Driver
Implementation class name	oracle.jdbc.pool.OracleConnectionPoolDataSource
URL	jdbc:oracle:thin:@10.184.108.91:1521:ord11gr2
Data store helper class name	com.ibm.websphere.rsadapter.Oracle10gDataStoreHelper
Use this data source in container managed persistence (CMP)	true
Component-managed authentication alias	(none)
Mapping-configuration alias	(none)
Container-managed authentication alias	(none)

Previous Finish Cancel

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

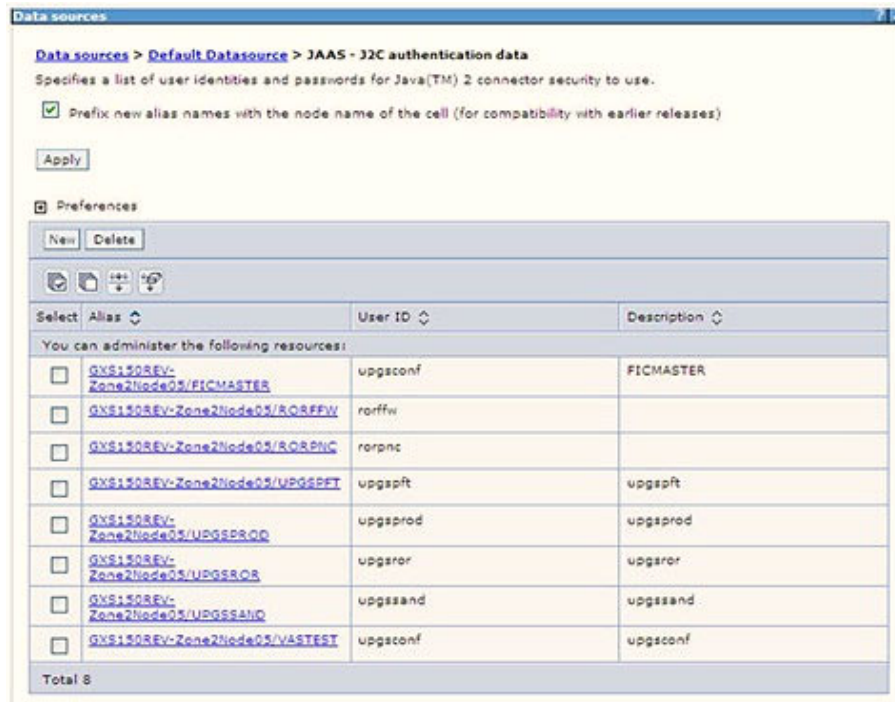
14. You must create another Data source by following the same procedure with jdbc/FICMASTER as JNDI name pointing to the "configuration schema" of Infrastructure.

10.1.3 Create J2C Authentication Details

The following steps apply to create both config and atomic J2C Authentication. To create J2C Authentication details, follow these steps:

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

Figure 57: JAASJ2C authentication data



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

Figure 58: JAASJ2C authentication data New



3. Enter the **Alias**, **User ID**, **Password**, and **Description**. Verify that the 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 the Atomic database user ID and password information for the Atomic schema data source that you created earlier.

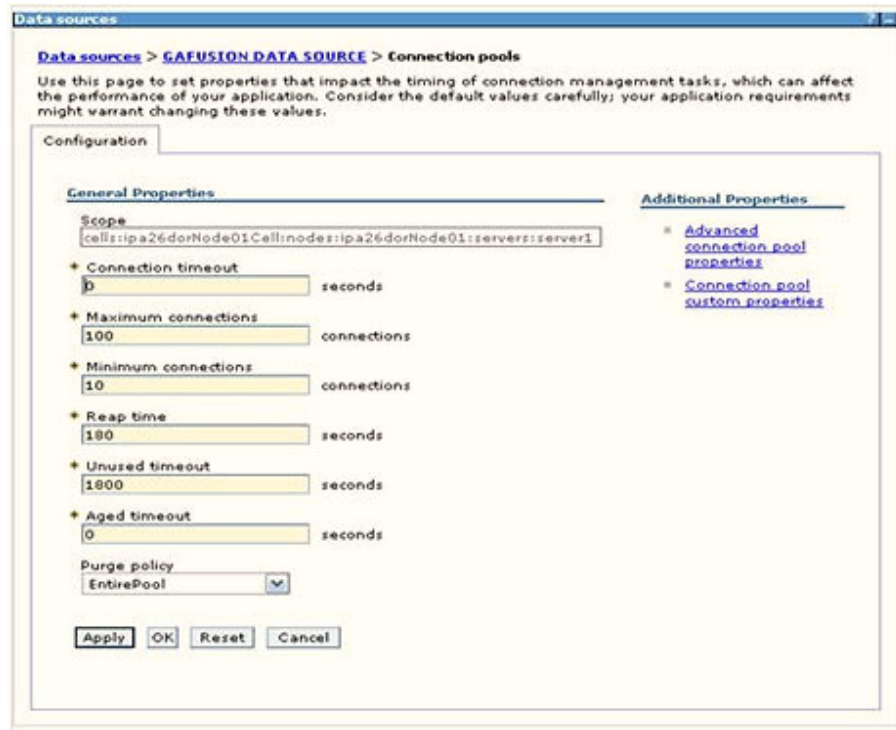
4. Click **Apply** and save the details.

10.1.4 Define 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 window.
2. Click the newly created Data Source \$DATA_SOURCE\$ and navigate to the path Data sources > GAFUSION DATA_SOURCE > Connection pools.

Figure 59: Connection pools



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

You can also define **Reap time**, **Unused timeout**, and **Aged timeout** as required.

10.2 Configure Resource Reference in WebLogic Application Server

Topics:

- [Create Data Source](#)
- [Create GridLink Data Source](#)
- [Configure Multi-data Sources](#)
- [Configure Advanced Settings for Data Source](#)

- [Configure JDBC Connection Pooling](#)
- [Create Workmanager](#)

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

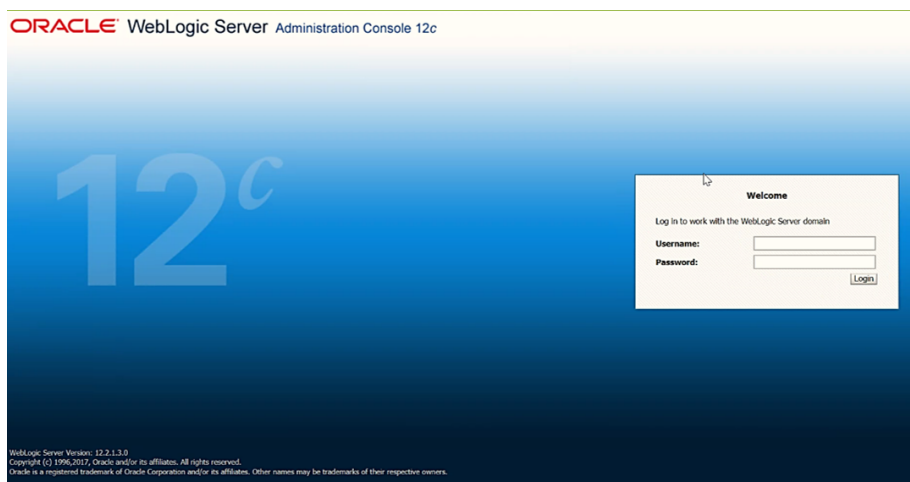
- For a non-RAC Database instance, a Generic Data Source must be created. See [Create Data Source](#).
- For a RAC Database instance, a Gridlink Data Source must be created. See [Create GridLink Data Source](#).
- When Load Balancing/Fail over is required, a Multi Data Source must be created. See [Configure Multi Data Sources](#).

10.2.1 Create Data Source

The following steps apply to both config and atomic data source creation:

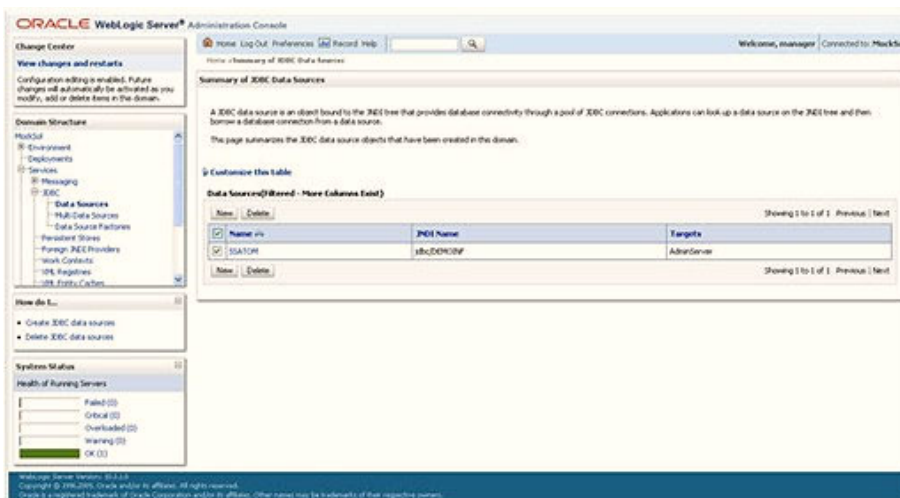
1. Open the following URL in the browser window:
`http://<ipaddress>:<administrative console port>/console`. (https, if SSL is enabled). The Welcome window is displayed.
2. Log in with the Administrator **Username** and **Password**.

Figure 60: Welcome



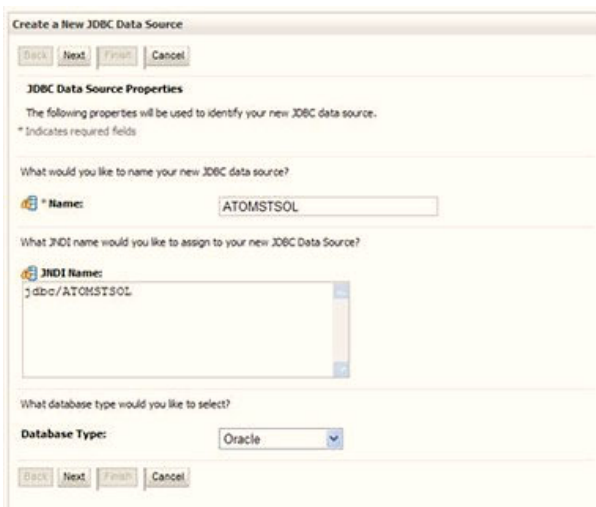
3. From the LHS menu (Domain Structure), click **Services > Data Sources** to display the Summary of JDBC Data Sources window.

Figure 61: Summary of JDBC Data Sources



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

Figure 62: Create a New JDBC Data Source



You can also select **GridLink Data Source** or **Multi Data Source** while creating a Data Source. For more information, see [Create Data Source](#) or [Configure Multi-data Sources](#).

Figure 63: JDBC Data Source Properties



5. Enter JDBC data source Name, JNDI Name, and select the Database Type from the drop-down list.
6. Ensure the following:
 - The JNDI Name field must be in the format jdbc/informationdomain
 - The same steps must 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 the web.xml file of OFSAAI Application.
 - Required "Database Type" and "Database Driver" must be selected.Data sources must be created for atomic and atomiccnf schemas following the same steps.
7. Click **Next**.

Figure 64: Transaction Options

The screenshot shows the 'Create a New JDBC Data Source' wizard, specifically the 'Transaction Options' page. The page has a title bar 'Create a New JDBC Data Source' and navigation buttons 'Back', 'Next', 'Finish', and 'Cancel'. The main content area is titled 'Transaction Options' and contains the following text: 'You have selected non-XA JDBC driver to create database connection in your new data source. Does this data source support global transactions? If yes, please choose the transaction protocol for this data source.' There are four radio button options: 'Supports Global Transactions' (which is selected), 'Logging Last Resource', 'Emulate Two-Phase Commit', and 'One-Phase Commit'. Each option has a brief description. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

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

Figure 65: Database Name

The screenshot shows the 'Create a New JDBC Data Source' wizard, specifically the 'Connection Properties' page. The page has a title bar 'Create a New JDBC Data Source' and navigation buttons 'Back', 'Next', 'Finish', and 'Cancel'. The main content area is titled 'Connection Properties' and contains the following text: 'Define Connection Properties. What is the name of the database you would like to connect to?'. There are five text input fields: 'Database Name' (containing 'fsgbu'), 'Host Name' (containing '10.184.74.80'), 'Port' (containing '1521'), 'Database User Name' (containing 'ssatom'), and 'Password' (containing '*****'). There is also a 'Confirm Password' field with '*****'. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

9. Select the **Supports Global Transactions** check box and the **One-Phase Commit** option.
10. Click **Next** to display the Connection Properties window.

Figure 66: Database Details

The screenshot shows the 'Create a New JDBC Data Source' window with the 'Test Database Connection' tab selected. The window contains several sections for configuring the database connection:

- Test Database Connection:** A section with instructions to test the database availability and connection properties.
- Driver Class Name:** A text field containing 'oracle.jdbc.OracleDriver'.
- URL:** A text field containing 'jdbc:oracle:thin:@10.104.1.104:1521:xe'.
- Database User Name:** A text field containing 'ssatom'.
- Password:** A password field with masked characters.
- Confirm Password:** A password field with masked characters.
- Properties:** A list box containing 'user=ssatom'.
- System Properties:** A list box.
- Test Table Name:** A text field containing 'SQL SELECT 1 FROM DUAL'.

Navigation buttons at the top and bottom include 'Test Configuration', 'Back', 'Next', 'Finish', and 'Cancel'.

11. Enter the required details such as the **Database Name, Host Name, Port, Oracle User Name, Password, and Confirm Password.**
12. Click **Next** to display the Test Database Connection window.

Figure 67: Select Targets

The screenshot shows the 'Create a New JDBC Data Source' window with the 'Select Targets' tab selected. The window contains a section for selecting targets to deploy the new JDBC data source:

- Select Targets:** A section with instructions to select one or more targets to deploy the new JDBC data source.
- Servers:** A list box containing 'AdminServer' with a checked checkbox.

Navigation buttons at the bottom include 'Back', 'Next', 'Finish', and 'Cancel'.

13. Verify the details and click **Test Configuration** and test the configuration settings. A confirmation message is displayed stating "Connection test succeeded."

14. 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" specified for a data source with "FICMASTER" as "JNDI" name must be the Oracle user ID created for the "configuration schema".

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

Figure 68: Data Source

Create a New JDBC GridLink Data Source

Back Next Finish Cancel

JDBC GridLink Data Source Properties

The following properties will be used to identify your new JDBC GridLink data source.
* Indicates required fields

What would you like to name your new JDBC GridLink data source?

Name: xyz

What JNDI name would you like to assign to your new JDBC GridLink data source?

JNDI Name: jdbc/xyz

What database type would you like to select?

Database Type: Oracle

Is this XA driver?

☐ XA Driver

Back Next Finish Cancel

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

10.2.2 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.

Figure 69: GridLink Data Source

Create a New JDBC GridLink Data Source

Back Next Finish Cancel

Connection Properties

Define Connection Properties.

Enter Complete JDBC URL for GridLink database.

Complete JDBC URL:

What database account user name do you want to use to create database connections?

Database User Name:

What is the database account password to use to create database connections?

Password:

Confirm Password:

Back Next Finish Cancel

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

Ensure that the JNDI Name field is specified in the format *jdbc/infodomainname* and the XA Driver check box is not selected. Click Next.

Figure 70: JNDI Name

The screenshot shows a wizard window titled "Create a New JDBC GridLink Data Source". It has navigation buttons at the top: "Back", "Next", "Finish", and "Cancel". The main section is titled "JDBC GridLink Data Source Properties" and includes a note: "The following properties will be used to identify your new JDBC GridLink data source. * Indicates required fields".

The first question is "What would you like to name your new JDBC GridLink data source?". The "Name:" field is required and contains the text "xyz".

The second question is "What JNDI name would you like to assign to your new JDBC GridLink data source?". The "JNDI Name:" field is required and contains the text "jdbc/xyz".

The third question is "What database type would you like to select?". The "Database Type:" dropdown is set to "Oracle".

The fourth question is "Is this XA driver?". The "XA Driver" checkbox is unchecked.

At the bottom, there are navigation buttons: "Back", "Next", "Finish", and "Cancel".

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

10.2.3 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 a 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.

To configure multi-data sources, follow these steps:

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. Log in with the user ID with administrative privileges.
3. In the LHS menu (Domain Structure), select **Services > JDBC > Multi Data Sources** to display the Summary of JDBC Multi Data Sources window.

Figure 71: Multi Data Sources

Summary of JDBC 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.

Use this page to create or view multi data sources in your domain.

Customize this table

Multi Data Sources(Filtered - More Columns Exist)

NewCreate

Showing 1 to 2 of 2 PreviousNext

<input type="checkbox"/>	Name ↕	JNDI Name	Algorithm Type	Targets
<input type="checkbox"/>	RUSTONDS	jdbcRUSTONRHEL	Load-Balancing	AdminServer
<input type="checkbox"/>	RORDS	jdbcRORRHELQT	Load-Balancing	AdminServer

NewDelete

Showing 1 to 2 of 2 PreviousNext

4. Click **New** to display the New JDBC Multi Data Source window.

Figure 72: Configure Multi Data Source

Create a New JDBC Multi Data Source

BackNextFinishCancel

Configure the Multi Data Source

The following properties will be used to identify your new JDBC multi data source.

What would you like to name your new JDBC multi data source?

Name: JDBC Multi Data Source-0

What JNDI name would you like to assign to your new JDBC multi data source?

JNDI Name: jdbc/infodomaine

What algorithm type for this JDBC Multi Data Source would you like to select?

Algorithm Type: Load-Balancing

BackNextFinishCancel

NOTE Ensure that the Data Sources which must be added to the new JDBC Multi Data Source are 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 must be specified in the format jdbc/infodomainname.
- The JNDI Name of the Data Sources that is added to the new JDBC Multi data source must be different from the JNDI name specified during Multi Data Source.
- The same steps must be followed to create a mandatory data source pointing to the "configuration schema" of infrastructure with jdbc/FICMASTER as JNDI name for Data Source.
- The JNDI Name provided in the multi-data source must be the same name that is mentioned in the `web.xml` file of OFSAAI Application.
- You can select the **Algorithm Type** as **Load-Balancing**.

Figure 73: Select Targets



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

Figure 74: Select Data Source Type



7. Select the type of data source to add to the new JDBC Multi Data Source. Click **Next**.

Figure 75: Add Data Sources



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.

10.2.4 Configure Advanced Settings for Data Source

To configure the advanced setting for the data source, follow these steps:

1. Click the new Data Source from the Summary of JDBC Data Sources window to display the Settings for <Data Source Name> window.
2. Select the Connection Pooling tab given under Configuration.
3. Navigate to the Advanced option at the bottom of the window, and check the Test Connection of Reserve check box (enables WebLogic Server to test a connection before giving it to a client).

To verify if the data source is valid, select "Data Source Name". For example, FICMASTER.

4. Select the server and click Test Data Source. A message is displayed indicating that the test was successful.

After the "Data Source" is created successfully, the following messages are displayed: All changes are activated. No restart is necessary.

Settings updated successfully. If not, follow these same steps to recreate the data source.

10.2.5 Configure JDBC Connection Pooling

To define the JDBC connection pooling, ensure that you have created the **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 following values:
 - **Initial Capacity:** 10
 - **Maximum Capacity:** 100
 - **Capacity Increment:** 1
 - **Statement Cache Type:** LRU
 - **Statement Cache Size:** 10
3. Click **Save**.

10.2.6 Create Workmanager

A Workmanager is used to re-trigger failed messages.

To create a Workmanager, follow these steps:

- The **Name** field must have the value `wm/WorkManager-TFLT`
- The **Type** field must have the value `Work Manager`.
- The **Targets** field must have the value `AdminServer`
- The **Scope** field must have the value `Global`
- The **Stuck Thread Action** field must have the value `Ignore stuck threads` Click **Save**.

Figure 76: WorkManager Screen 1

Settings for wm/WorkManager-TFLT

Configuration Targets Notes

Save

Use this page to define the request classes and constraints for the selected Work Manager.

Name:

wm/WorkManager-TFLT

The user-specified name of this MBean instance. More Info...

Scope:

Global

The scope in which this Work Manager is created. More Info...

Request Class:

(None configured) New

A request class associated with this Work Manager. This may be a FairShareRequestClass, ResponseTimeRequestClass, or a ContextRequestClass. More Info...

Minimum Threads Constraint:

(None configured) New

The minimum number of threads allocated to resolve deadlocks. More Info...

Maximum Threads Constraint:

(None configured) New

The maximum number of concurrent threads that can be allocated to execute requests. More Info...

Capacity Constraint:

(None configured) New

The total number of requests that can be queued or executing before WebLogic Server begins rejecting requests. More Info...

Stuck Thread Action:

Ignore stuck threads

Specify how stuck threads should be detected, and what action to take should they occur. More Info...

Max Stuck Thread Time:

0

Time after which a executing thread is declared as stuck. More Info...

Stuck Thread Count:

0

Number of stuck threads after which the WorkManager is shutdown. More Info...

☒ Resume When Unstuck

Whether to resume work manager once the stuck threads were cleared. More Info...

Save

Figure 77: Workmanager Screen 2

Summary of Work Managers

Save

A Work Manager defines a set of request classes and thread constraints that manage work performed by WebLogic Server instances. This page displays the Work Managers, request classes and thread constraints defined for this domain. Work Managers are defined at the domain and partition level. You can also define application-level and module-level Work Managers.

Partition Fair Share:

50

A desired percentage of thread usage by a partition compared to the thread usage by all partitions. It is recommended that the sum of this value for all the partitions running in a WLS domain add up to 100, but it is not strictly enforced. When they do not add up to 100, WLS assigns thread-usage times to different partitions based on their relative values. This attribute is for use in the global domain only. Use the PartitionWorkManager MBean for specifying partition fair share values for partitions. More Info...

Save

Customize this table

Work Managers, Request Classes and Constraints

New Clone Delete

Showing 1 to 1 of 1 Previous Next

Name	Type	Targets	Scope	Domain Partitions
wm/WorkManager-TFLT	Work Manager	AdminServer	Global	

New Clone Delete

Showing 1 to 1 of 1 Previous Next

10.3 Configure Resource Reference in Tomcat Application Server

This section is applicable only when the Web application server type is Tomcat.

Topics:

- [Create Data Source](#)
- [Define JDBC Connection Pooling](#)
- [Configure ClassLoader for Apache Tomcat](#)

Copy the Oracle JDBC driver file, `ojdbc<version>.jar` from `<Oracle Home>/jdbc/lib` and place it in `<Tomcat Home>/lib`.

See [Hardware and Software Requirements](#) to identify the correct `ojdbc<version>.jar` file version to be copied.

10.3.1 Create Data Source

To create a "data source" for Infrastructure application, navigate to `<Tomcat Home>/conf` directory and edit the following block of text by replacing the actual values in the `server.xml` file.

NOTE

The User-IDs for configuration/ atomic schemas have the prefix of setup info depending on the value set for `PREFIX_SCHEMA_NAME` in the `<<APP Pack>>_SCHEMA_IN.XML` file of the Schema Creator Utility.

For example: If the value set for `PREFIX_SCHEMA_NAME` is `DEV` and the schema name is mentioned as `ofsaconf`, then the actual schema created in the database is `DEV_ofsaconf`.

```
<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>

NOTE

- The <Resource> tag must be repeated for each Information Domain created.
- After the configuration, the "WAR" file must be created and deployed in Tomcat.

10.3.2 Define JDBC Connection Pooling

To define the JDBC connection pooling, follow these steps:

1. Copy the \$ORACLE_HOME/jdbc/lib/ojdbc<version>.jar file to the path \$TOMCAT_DIRECTORY/lib/ directory.

See [Hardware and Software Requirements](#) to identify the correct ojdbc<version>.jar file version to be copied.

2. Edit the server.xml file available under the \$TOMCAT_DIRECTORY/conf/ directory with the following changes, which is 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"

maxTotal="300" maxIdle="30" maxWaitMillis="10000"
removeAbandonedOnBorrow="true" removeAbandonedTimeout="60"
logAbandoned="true"/>

</Context>
```

NOTE

- \$APP_DEPLOYED_PATH\$ must be replaced by the OFSAAI application deployed path.
 - \$INFODOM_NAME\$ must be replaced by Infodom Name.
 - \$ATOMICSCHEMA_USERNAME\$ must be replaced by an Atomic schema database user name.
 - \$ATOMICSCHEMA_PASSWORD\$ must be replaced by an Atomic schema database password.
 - \$JDBC_CONNECTION_URL must be replaced by JDBC connection string jdbc:Oracle:thin:<IP>:<PORT>:<SID>.
- For example,:

```
jdbc:oracle:thin 192.168.0.1:1521:soluint
```

The User-IDs for configuration/ atomic schemas have the prefix of setupinfo depending on the value set for PREFIX_SCHEMA_NAME in the <<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 is mentioned as ofsaconf, then the actual schema created in the database is DEV_ofsaconf.

10.3.3 Configure ClassLoader for Apache Tomcat

To configure the ClassLoader for Apache Tomcat, follow the step:

1. Edit the `server.xml` file available in `$TOMCAT_HOME/conf/` directory.

Add the tag `<Loader delegate="true" />` within the `<Context>` tag, above before the `<Resource>` tag. This is applicable only when the web application server is Apache Tomcat 8.

11 Appendix C: Configure Work Manager in Web Application Servers

The process Modelling framework requires creating a Work Manager and mapping it to the OFSAA instance. This configuration is required for WebSphere and WebLogic Web application server types.

Topics:

- [Configure Work Manager in WebSphere Application Server](#)
- [Configure Work Manager in WebLogic Application Server](#)

11.1 Configure Work Manager in WebSphere Application Server

Topics:

- [Create Work Manager](#)
- [Map Work Manager to OFSAA WebSphere Instance](#)

11.1.1 Create Work Manager

To create the Work Manager, follow these steps:

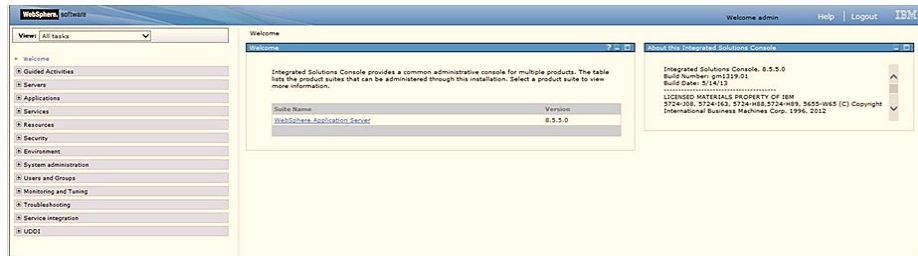
1. Open the WebSphere admin console in the browser window: <http://<ipaddress>:<administrative console port>/ibm/console>. (https if SSL is enabled). The Login window is displayed.

Figure 78: WebSphere Login page



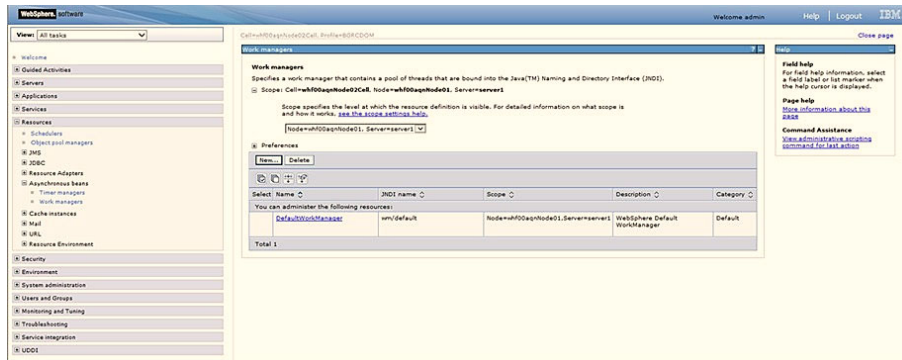
2. Log in with the user ID with administrative privileges.

Figure 79: Home page



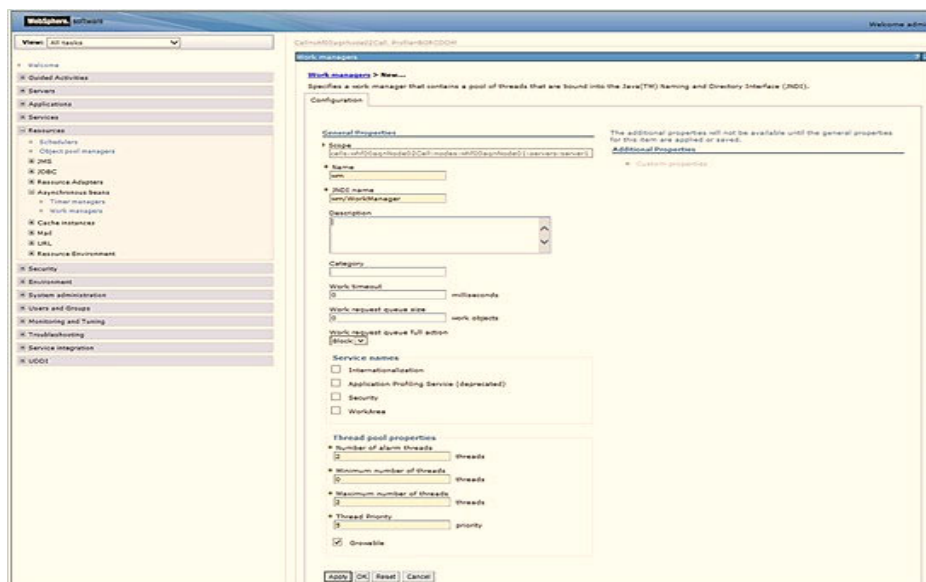
- From the LHS menu, expand **Resources > Asynchronous beans** and select **Work Managers**.

Figure 80: Work Managers



- Select the required Scope from the drop-down list.
For example, Node=whf00aqnNode01, Server=server1.
- Click **New** in the **Preferences** section.

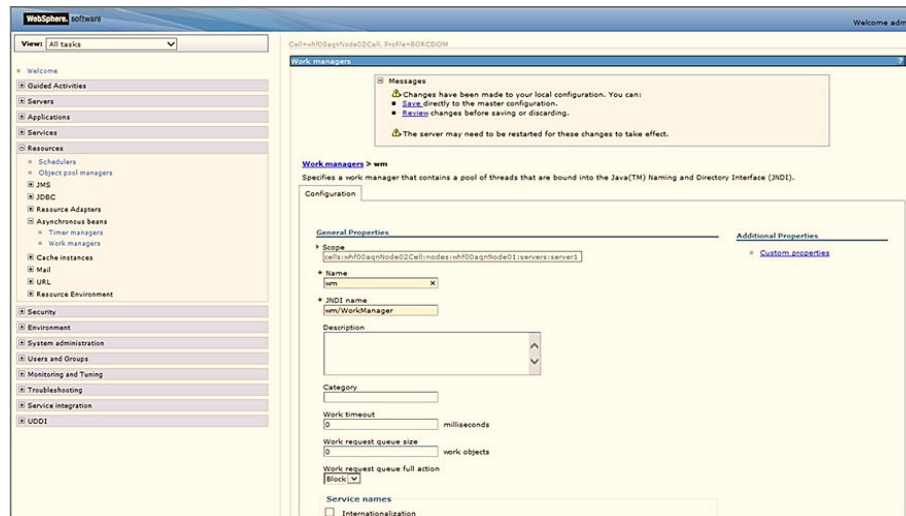
Figure 81: New Work Managers



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

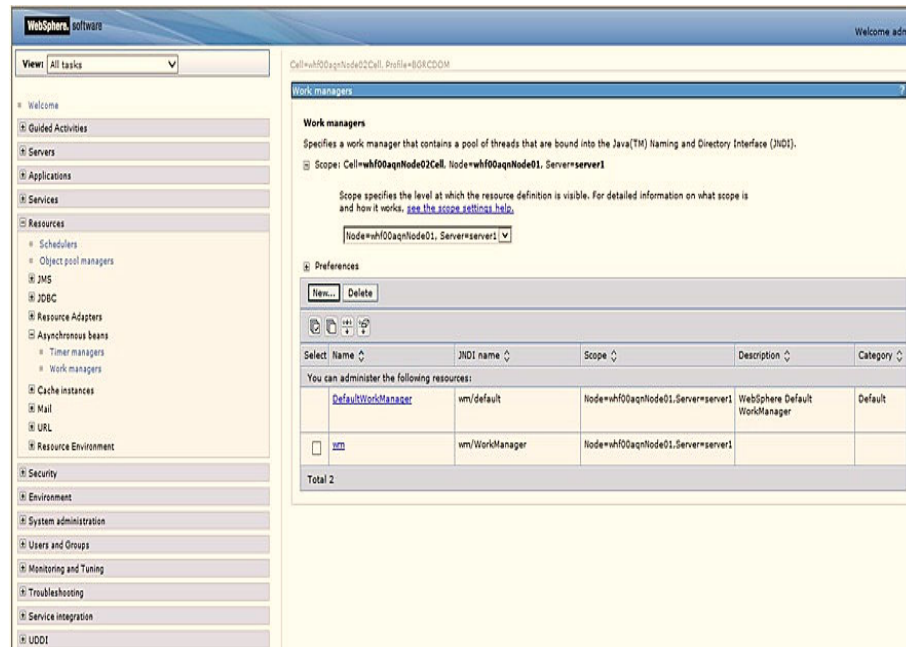
8. Click **Apply**.

Figure 82: Configure Work Managers



9. Click **Save**.

Figure 83: Work Managers Preferences



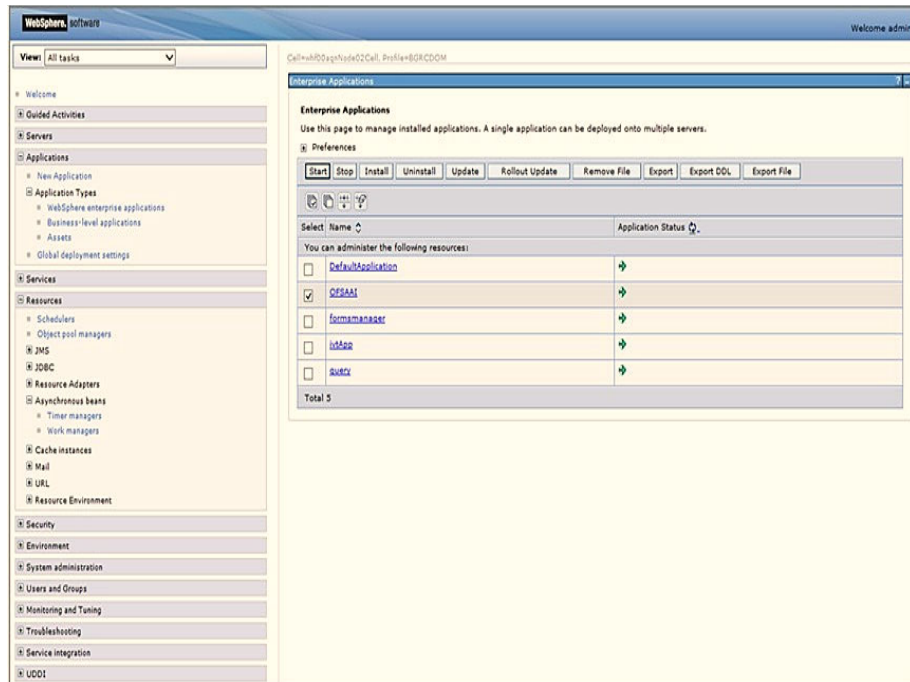
After creating the work manager, you must map it to an OFSAA instance.

11.1.2 Map Work Manager to OFSAA WebSphere Instance

To map the Work Manager to an OFSAA WebSphere Instance, follow these steps:

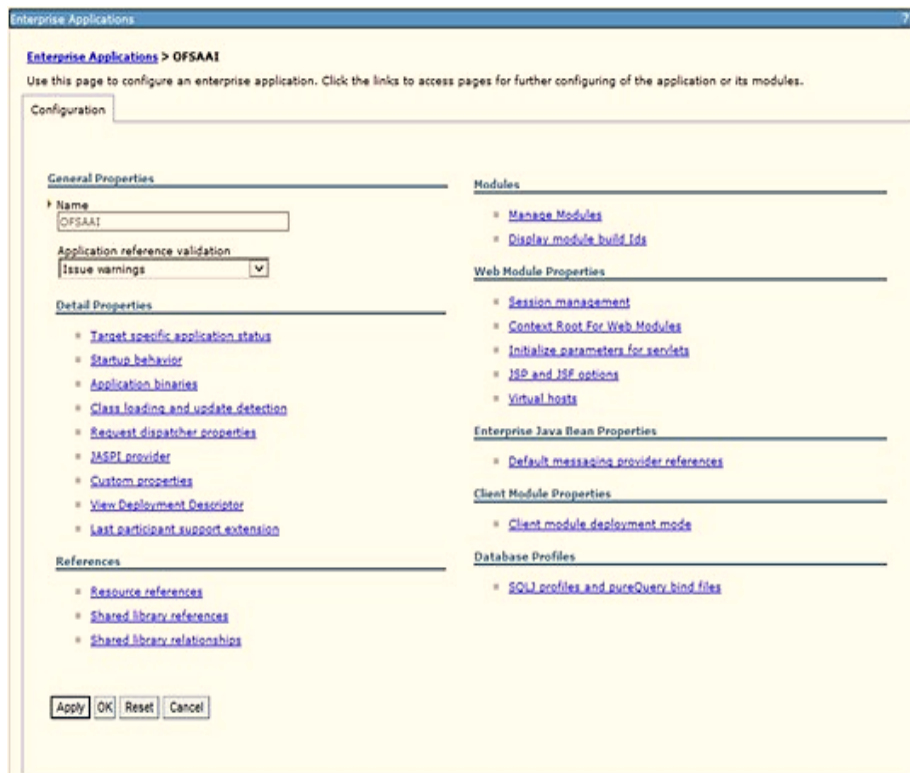
1. From the LHS menu, expand **Applications > Application Types** and click WebSphere enterprise applications.

Figure 84: Enterprise Applications



2. Click the OFSAAI instance hyperlink.

Figure 85: OFSAAI



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

Figure 86: Resource References

The screenshot shows the 'Enterprise Applications' console with the path 'Enterprise Applications > OFSAAI > Resource references'. It displays two resource reference sections: 'commonj.work.WorkManager' and 'javax.sql.DataSource'.

commonj.work.WorkManager

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name
<input checked="" type="checkbox"/>	OFSAAI Web Application		OFSAAI.nar.WEB-INF/web.xml	wm/WorkManager	wm/default <input type="button" value="Browse..."/>

javax.sql.DataSource

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name	Login configuration
<input type="checkbox"/>	OFSAAI Web Application		OFSAAI.nar.WEB-INF/web.xml	jdbc/FICMASTER	jdbc/FICMASTER <input type="button" value="Browse..."/>	Resource authorization: Container Authentication method: None
<input type="checkbox"/>	OFSAAI Web Application		OFSAAI.nar.WEB-INF/web.xml	jdbc/OFSBGRINFO	jdbc/OFSBGRINFO <input type="button" value="Browse..."/>	Resource authorization: Container Authentication method: None

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

Figure 87: Available Resources

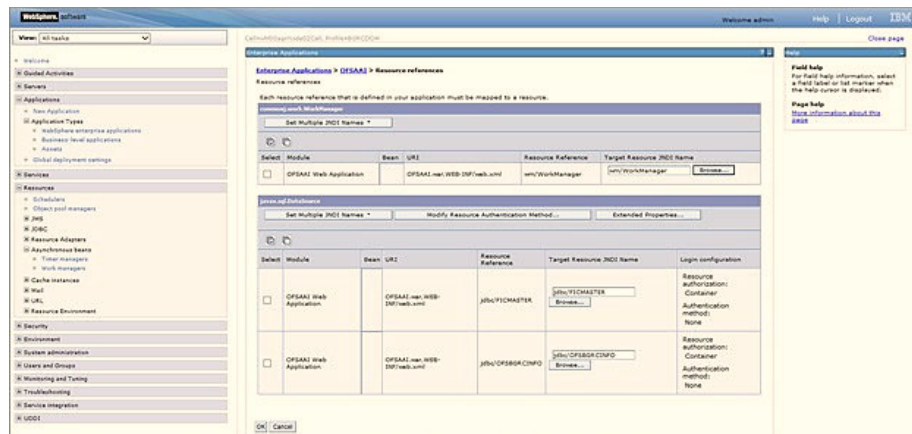
The screenshot shows the 'Enterprise Applications' console with the path 'Enterprise Applications > OFSAAI > Resource references > Available resources'. It displays a table of available resources.

Select	Name	JNDI name	Scope	Description
<input type="radio"/>	AsyncRequestDispatcherWorkManager	wm/ard	Node=whf00agnNode01	
<input type="radio"/>	DefaultWorkManager	wm/default	Node=whf00agnNode01.Server=server1	WebSphere Default WorkManager
<input checked="" type="radio"/>	wm	wm/WorkManager	Node=whf00agnNode01.Server=server1	

Total 3

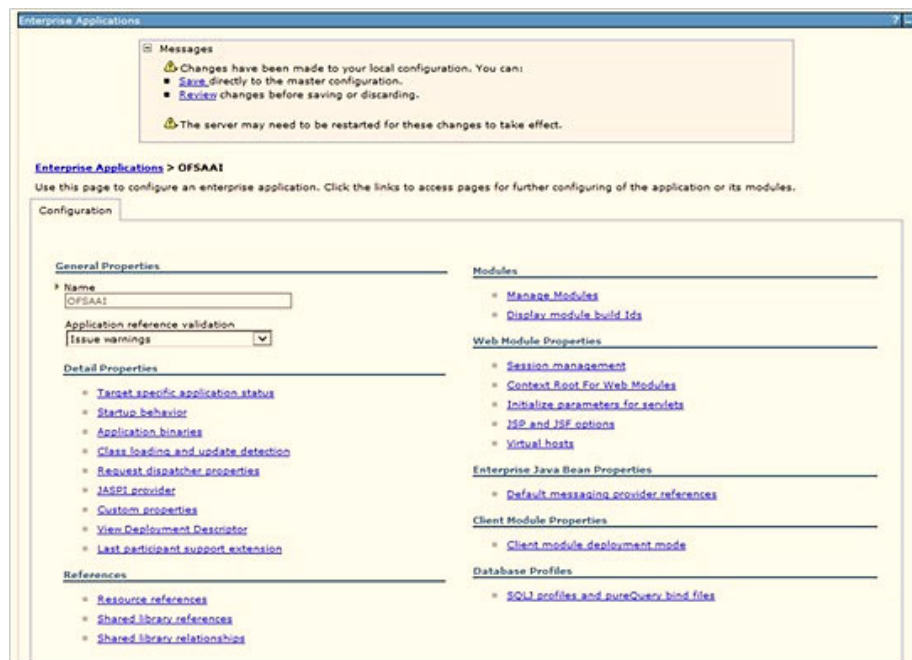
- Select the newly created Work Manager ('wm') and click **Apply**.

Figure 88: Select Work Manager



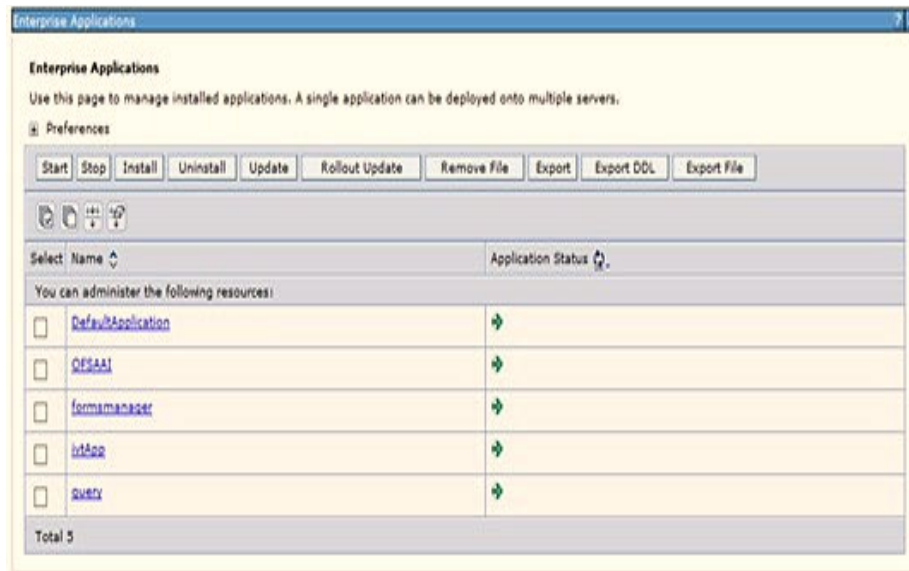
6. Select the Work Manager ('wm/WorkManager') and click **OK**.

Figure 89: OFSAAI Configuration



7. Click **Save**.

Figure 90: Enterprise Applications Preferences

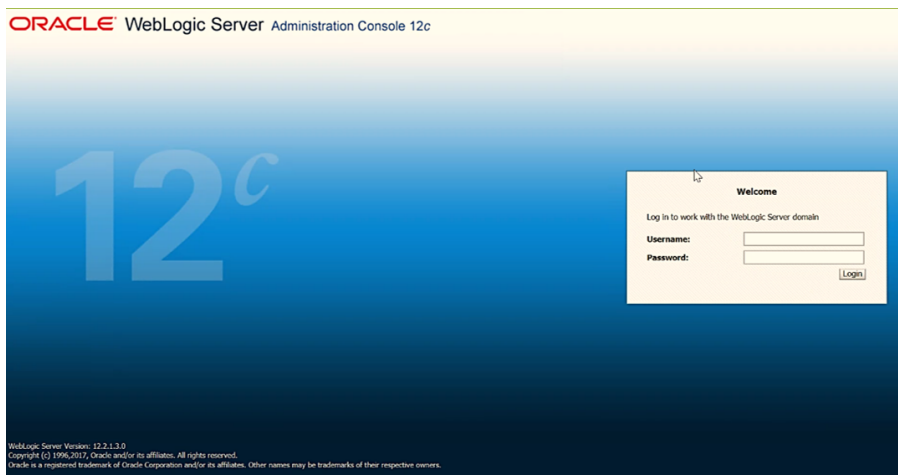


11.2 Configure Work Manager in WebLogic Application Server

To create the Work Manager in WebLogic application server, follow these steps:

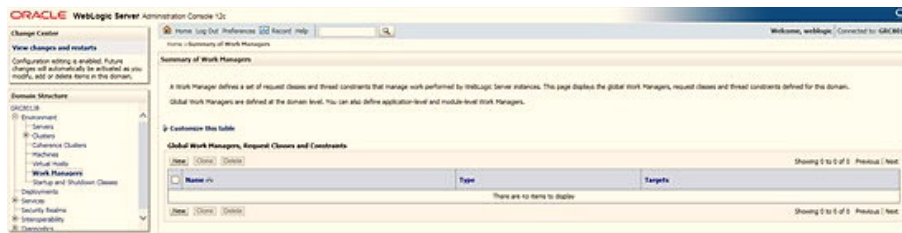
1. Open the WebLogic admin console in the browser window: `http://<ipaddress>:<administrative console port>/console`. (https if SSL is enabled). The Welcome window is displayed.

Figure 91: WebLogic Login page



2. Log in with the user ID with administrative privileges.
3. From the **Domain Structure** menu in the LHS, expand Environment and select **Work Managers** to display the Summary of Work Managers window.

Figure 92: Work Manager



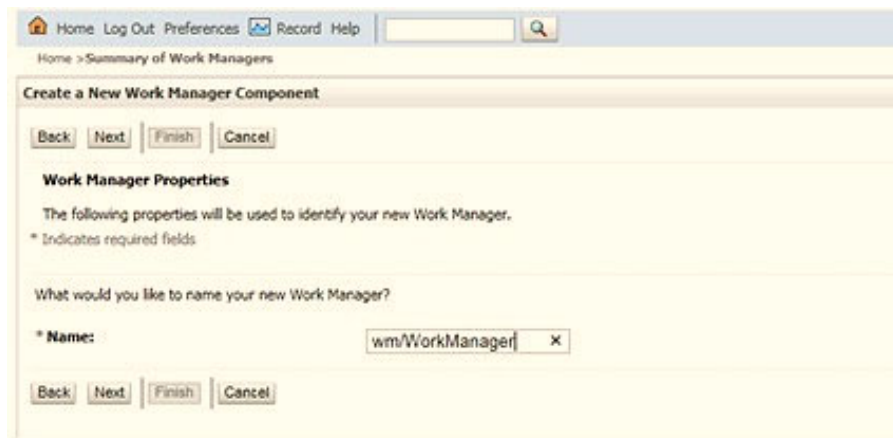
4. Click **New** to create a new Work Manager component.

Figure 93: New Work Manager



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

Figure 94: Work Manager



6. Enter the Name as 'wm/WorkManager' and click **Next**.

Figure 95: Select Deployment Targets

Create a New Work Manager Component

Back Next Finish Cancel

Select deployment targets

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

Available targets :

Servers
<input checked="" type="checkbox"/> AdminServer

Back Next Finish Cancel

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

Figure 96: Summary of Work Managers

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: GACR03J8

Summary of Work Managers

Messages

- All changes have been activated. No restarts are necessary.
- Work Manager created successfully

Summary of Work Managers

A Work Manager defines a set of request classes and thread constraints that manage work performed by WebLogic Server instances. This page displays the global Work Managers, request classes and thread constraints defined for this domain. Global Work Managers are defined at the domain level. You can also define application-level and module-level Work Managers.

Customize this table

Name	Type	Targets
<input type="checkbox"/> wsm/WorkManager	Work Manager	AdminServer

Showing 1 to 1 of 1 Previous Next

12 Appendix D: Creating and Deploying EAR/WAR File

Topics:

- Creating EAR/WAR File
- Deploying EAR/WAR File

12.1 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, a message is displayed with timestamp and you will be returned to the prompt.

Figure 97: Creating EAR/ WAR File

```
/scratch/ofsaaweb>cd /scratch/ofsaaweb/OFS80/ficweb
/scratch/ofsaaweb/OFS80/ficweb>
/scratch/ofsaaweb/OFS80/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/OFS80/ficweb>./ant.sh
executing "ant"
Buildfile: build.xml

createwar:
[war] Building war: /scratch/ofsaaweb/OFS80/ficweb/AAI80.war

createear:
[ear] Building ear: /scratch/ofsaaweb/OFS80/ficweb/AAI80.ear

BUILD SUCCESSFUL
Total time: 2 minutes 8 seconds
/scratch/ofsaaweb/OFS80/ficweb>
```

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` is created.
- If a heap space error occurs when the War file is generated, execute the following command in Putty.

```
export ANT_OPTS=-Xmx1024m
```

12.2 Deploying EAR/WAR File

Topics:

- [Deploying EAR/WAR Files on WebSphere](#)
- [Start the Application](#)
- [Deploying EAR/WAR files for WebLogic](#)
- [Deploying Tomcat WAR Files on Tomcat](#)

NOTE

- Remove the existing Admin Tools deployment (which is integrated with OFS BD pack).
- Ensure to clear the application cache prior to the deployment of Applications Pack Web Archive. This is applicable to all Web servers (WebSphere, WebLogic, and Tomcat). For more information, see Clearing Application Cache section.

12.2.1 Deploying EAR/WAR Files on WebSphere

To deploy Infrastructure application in WebSphere, follow these steps:

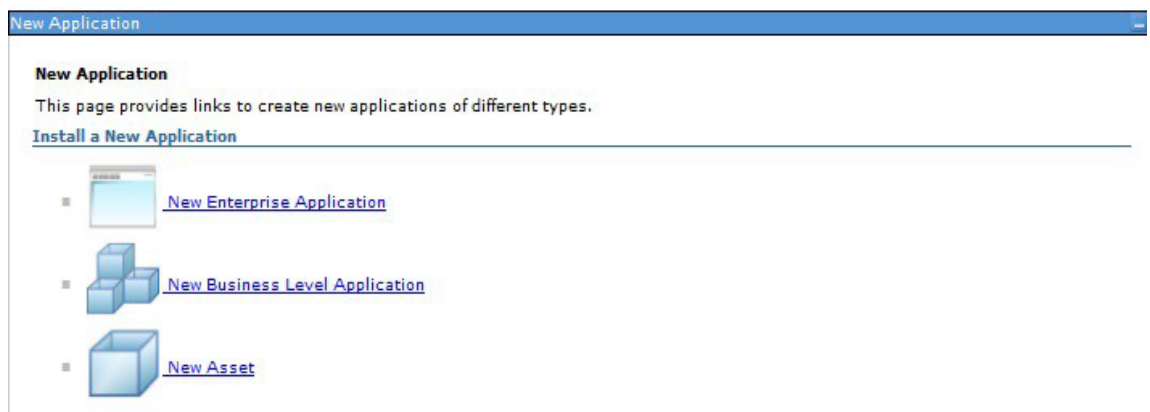
1. Start WebSphere Profile by navigating to the path `/<WebSphere_Installation_Directory>/IBM/WebSphere/AppServer/profiles/<Profile_Name>/bin/` and execute the command: `./startServer.sh server1`.
2. Open the following URL in the browser: <http://<ipaddress>:<Administrative Console Port>/ibm/console>. (https if SSL is enabled). The login screen is displayed.

Figure 98: Login Window



3. Log in with the user ID with administrative privileges.
4. From the LHS menu, select Applications and click New Application. The New Application window is displayed.

Figure 99: New Application



5. Click New Enterprise Application. The Preparing for the application installation window is displayed

Figure 100: Preparing for the application installation

The screenshot shows a window titled "Enterprise Applications" with a sub-header "Preparing for the application installation". Below the header, it says "Specify the EAR, WAR, JAR, or SAR module to upload and install." There are two radio button options: "Local file system" and "Remote file system". The "Remote file system" option is selected. Under "Local file system", there is a text field labeled "Full path" and a "Browse..." button. Under "Remote file system", there is a text field labeled "Full path" containing the path "/scratch/oracle/was855/profiles/TEST80AAI/AAI80" and a "Browse..." button. At the bottom, there are "Next" and "Cancel" buttons.

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

Figure 101: Installation Options

The screenshot shows the same "Preparing for the application installation" dialog box. Below the "Full path" field, there is a section titled "How do you want to install the application?" with two radio button options: "Fast Path - Prompt only when additional information is required." and "Detailed - Show all installation options and parameters." The "Fast Path" option is selected. Below this, there is a checkbox labeled "Choose to generate default bindings and mappings" which is checked. At the bottom, there are "Previous", "Next", and "Cancel" buttons.

7. Select the Fast Path option and click Next. The Install New Application window is displayed.

Figure 102: Install New Application

Install New Application

Specify options for installing enterprise applications and modules.

→ Step 1: Select installation options

Step 2 Map modules to servers

Step 3 Summary

Select installation options

Specify the various options that are available for your application.

☐ Precompile JavaServer Pages files

Directory to install application

☒ Distribute application

☐ Use Binary Configuration

☐ Deploy enterprise beans

Application name

AAI80

☒ Create MBeans for resources

☐ Override class reloading settings for Web and EJB modules

Reload interval in seconds

☐ Deploy Web services

Validate Input off/warn/fail

warn ▼

☐ Process embedded configuration

File Permission

Allow all files to be read but not written to
 Allow executables to execute
 Allow HTML and image files to be read by everyone

.*\dll=755#.*\so=755#.*\a=755#.*\s|=755

Application Build ID

Unknown

☐ Allow dispatching includes to remote resources

☐ Allow servicing includes from remote resources

Business level application name

Create New BLA ▼

Asynchronous Request Dispatch Type

Disabled ▼

☐ Allow EJB reference targets to resolve automatically

☐ Deploy client modules

Client deployment mode

Isolated ▼

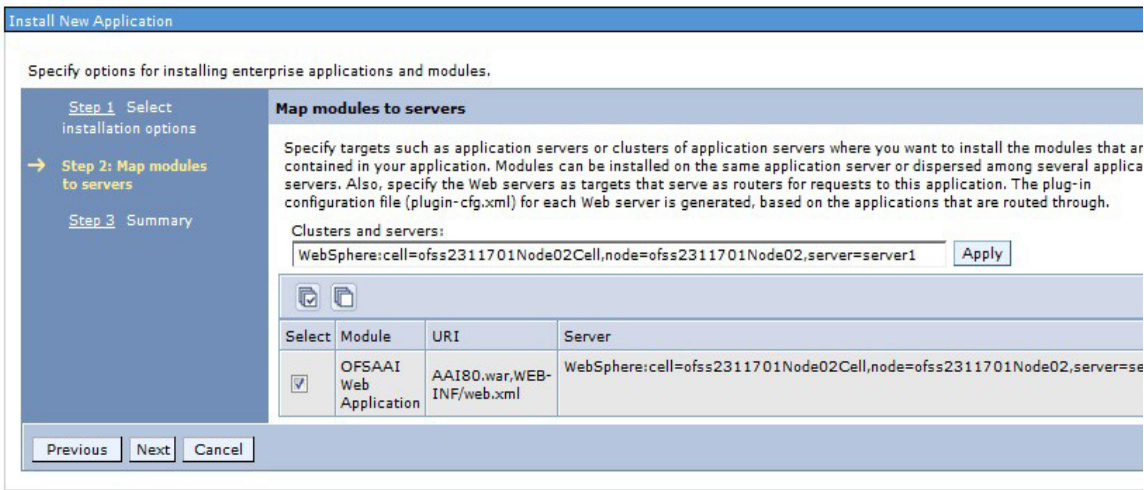
☐ Validate schema

Next

Cancel

- Enter the required information and click Next. The Map Modules to Servers window is displayed.

Figure 103: Map Modules to Servers



9. Select the Web Application and click Next. The Map Resource References to Resources window is displayed.

Figure 104: Map Resource References to Resources

Specify options for installing enterprise applications and modules.

[Step 1: Select installation options](#)

[Step 2: Map modules to servers](#)

→ [Step 3: Map resource references to resources](#)

★ [Step 4: Map virtual hosts for Web modules](#)

[Step 5: Summary](#)

Map resource references to resources

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

commonj.work.WorkManager

Set Multiple JNDI Names ▾

☒ ☐

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name
<input type="checkbox"/>	OFSAAI Web Application		BD801Q.war,WEB-INF/web.xml	wm/WorkManager	<input type="text" value="Browse..."/>

java.sql.DataSource

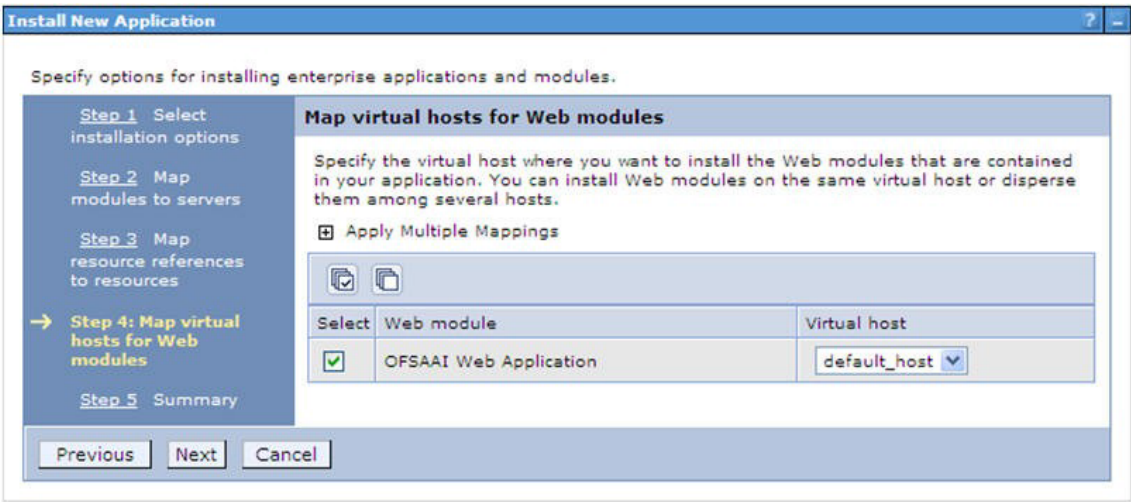
Set Multiple JNDI Names ▾ Modify Resource Authentication Method... Extended Properties...

☒ ☐

Select	Module	Bean	URI	Resource Reference	Target Resource JNDI Name	Login configuration
<input type="checkbox"/>	OFSAAI Web Application		BD801Q.war,WEB-INF/web.xml	jdbc/FICMASTER	<input type="text" value="Browse..."/>	Resource authorization: Container Authentication method: None
<input type="checkbox"/>	OFSAAI Web Application		BD801Q.war,WEB-INF/web.xml	jdbc/analyst	<input type="text" value="Browse..."/>	Resource authorization: Container Authentication method: None
<input type="checkbox"/>	OFSAAI Web Application		BD801Q.war,WEB-INF/web.xml	jdbc/miner	<input type="text" value="Browse..."/>	Resource authorization: Container Authentication method: None
<input type="checkbox"/>	OFSAAI Web Application		BD801Q.war,WEB-INF/web.xml	jdbc/BD801QT	<input type="text" value="Browse..."/>	Resource authorization: Container Authentication method: None

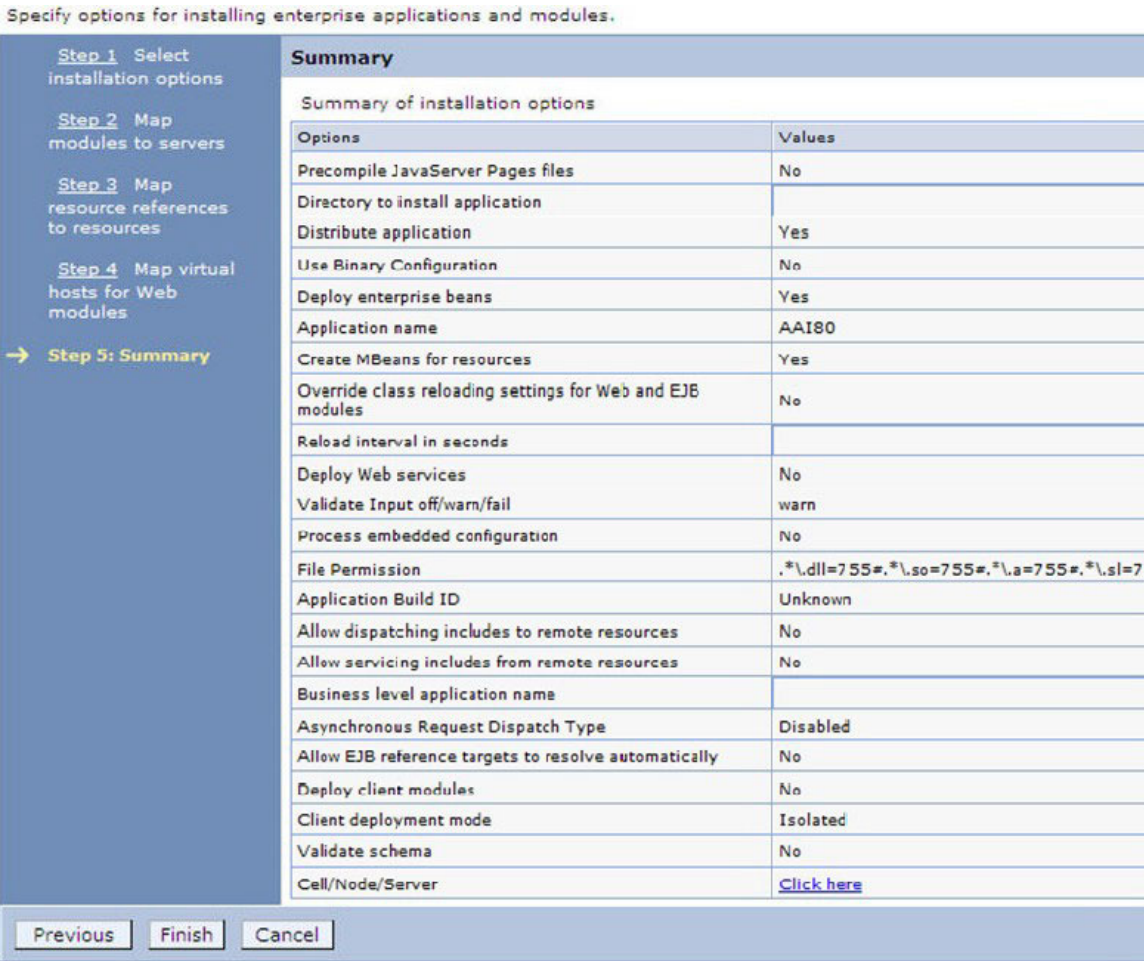
10. Map each resource defined in the application to a resource JNDI name defined earlier.
11. Click Modify Resource Authentication Method and specify the authentication method created earlier.
12. You can specify *config* for FICMASTER resource or *atomic* for atomic resource as the authentication method.
13. Select the OFSAAI Web Application check box and click Next. The Map Virtual hosts for Web Modules window is displayed.

Figure 105: Map Virtual host for Web Modules



14. Select the Web Application check box and click Next. The Summary page is displayed.

Figure 106: Summary



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

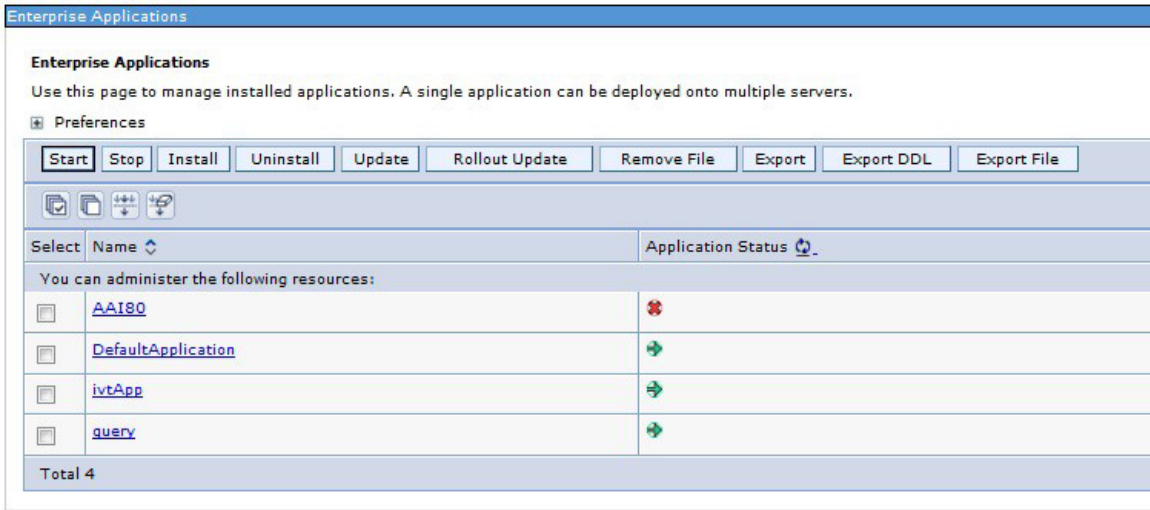
12.2.2

Start the Application

To start the application, follow these steps:

1. Expand Applications > Application Type > WebSphere enterprise applications. The Enterprise Applications window is displayed.

Figure 107: Enterprise Application



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.

12.2.3

Deploying EAR/WAR files for WebLogic

This section describes how to deploy the EAR/WAR files for WebLogic.

To deploy the EAR/WAR files for WebLogic, follow these steps:

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.

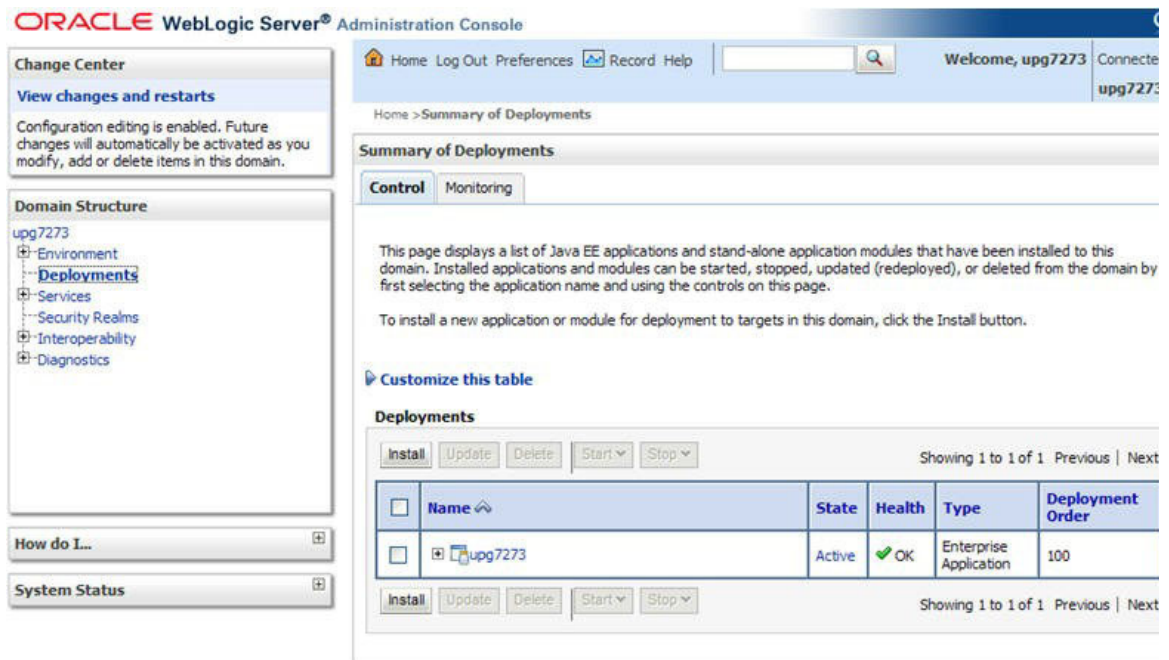
- Open the URL in the browser window: <http://<ipaddress>:<admin server port>/console>. (https if SSL is enabled). The Sign in window of the WebLogic Server Administration Console is displayed.

NOTE

Ensure that you have started Infrastructure Server by executing `./startofsaai.sh` as described in [Starting Infrastructure Services](#).

- Log on to the WebLogic Server by entering the user credentials having privileges to deploy the EAR file.
- From the Domain Structure LHS menu, click Deployments. The Summary of Deployments window is displayed.

Figure 108: Summary of Deployments



- Click Install. The Install Application Assistant window is displayed.
- Select the Exploded EAR directory after browsing to the directory where it is saved and click Next.

12.2.3.1 Explode EAR File

To explode EAR, follow these steps:

- Create the *applications* folder under domain name. For example, `"/Bea/user_projects/domains/<Domain_name>/applications"`.
- Create `<context_name>.ear` folder under the *applications* folder.
- Copy the `<$FIC_WEB_HOME/<context_name>.ear` file to `<WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear`.
- Explode the `<context_name>.ear` file by executing the command: `jar -xvf <context_name>.ear`.
- Delete the `<context>.ear` and `<context>.war` files (recently created) `<WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear`.

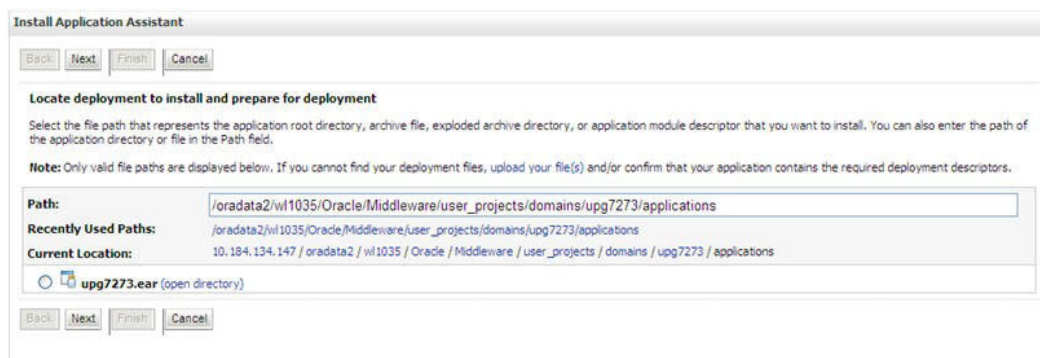
6. Create a directory <context_name>.war under <WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear.
7. Copy <\$FIC_WEB_HOME/<context_name>.war file to <WEBLOGIC_INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_name>.ear/<context_name>.war.
8. Explode the <context_name>.war file by executing the following command to get the directory structure: `jar -xvf <context_name>.war`.

12.2.3.2 Install Application

To install Application, follow these steps:

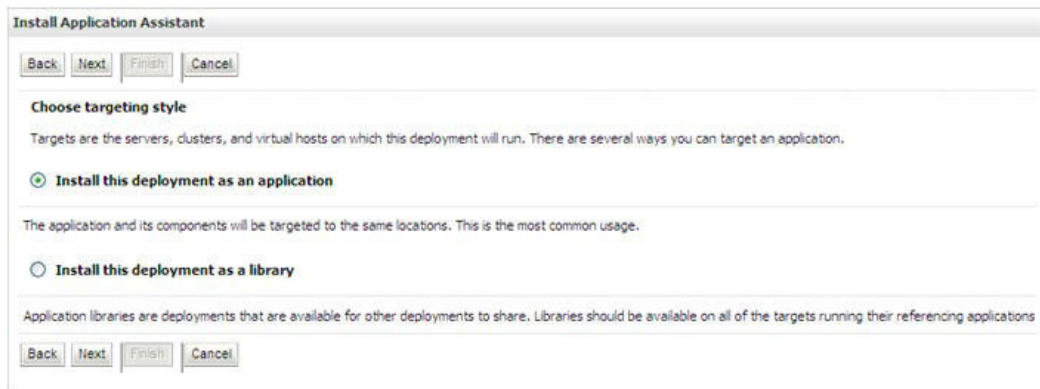
1. Open the Install Application Assistant.

Figure 109: Install Application Assistant



2. Click Next.

Figure 110: Install Application Assistant 1



3. From the Choose targeting style section, select the Install this deployment as an application option and click Next. The Optional Settings window is displayed.

Figure 111: Optional Settings

Install Application Assistant

Back Next Finish Cancel

Optional Settings
You can modify these settings or accept the defaults.

General
What do you want to name this deployment?
Name:

Security
What security model do you want to use with this application?
☒ **DD Only: Use only roles and policies that are defined in the deployment descriptors.**
☐ Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
☐ Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.
☐ Advanced: Use a custom model that you have configured on the realm's configuration page.

Source accessibility
How should the source files be made accessible?
☒ **Use the defaults defined by the deployment's targets.**
 Recommended selection:
☐ Copy this application onto every target for me
 During deployment, the files will be copied automatically to the managed servers to which the application is targeted.
☐ **I will make the deployment accessible from the following location**
 Location:
 Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

Back Next Finish Cancel

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 must be used.
6. Select *I will make the deployment available from the following location* under the Source accessibility section.
7. Click Next to continue. The Deployment Summary window is displayed.

Figure 112: Deployment Summary

Install Application Assistant

Back Next Finish Cancel

Review your choices and click Finish

Click Finish to complete the deployment. This may take a few moments to complete.

Additional configuration

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

☒ Yes, take me to the deployment's configuration screen.

☐ No, I will review the configuration later.

Summary

Deployment: /oradata2/vl1035/Oracle/Middleware/user_projects/domains/upg7273/applications/upg7273.ear

Name: upg72733

Staging mode: Use the defaults defined by the chosen targets

Security Model: DDOnly: Use only roles and policies that are defined in the deployment descriptors.

Target Summary

Components	Targets
upg7273.ear	AdminServer

Back Next Finish Cancel

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

Figure 113: Settings for Deployment Name

Summary of Deployments

Control Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

[Customize this table](#)

Deployments

Install Update Delete Start Stop

Showing 1 to 1 of 1 Previous | Next

Name	State	Health	Type	Deployment Order
upg7273	Active	OK	Enterprise Application	100

Install Update Delete Start Stop

Showing 1 to 1 of 1 Previous | Next

Figure 114: Settings for Deployment Name 1

Settings for upg7273

Overview

Deployment Plan

Configuration

Security

Targets

Control

Testing

Monitoring

Notes

Save

Use this page to view the general configuration of an Enterprise application, such as its name, the physical path to the application files, the associated deployment plan, and so on. The table at the end of the page lists the modules (such as Web applications and EJBs) that are contained in the Enterprise application. Click on the name of the module to view and update its configuration.

Name:

upg7273

The name of this Enterprise Application. [More Info...](#)

Path:

/ oradata2/wl1035/Oracle/Middleware/user_projects/domains/upg7273/applications/upg7273.ear

The path to the source of the deployable unit on the Administration Server. [More Info...](#)

Deployment Plan:

(no plan specified)

The path to the deployment plan document on Administration Server. [More Info...](#)

Staging Mode:

(not specified)

The mode that specifies whether a deployment's files are copied from a source on the Administration Server to the Managed Server's staging area during application preparation. [More Info...](#)

Security Model:

DDOnly

The security model that is used to secure a deployed module. [More Info...](#)

Deployment Order:

100

An integer value that indicates when this unit is deployed, relative to other deployable units on a server, during startup. [More Info...](#)

Deployment Principal Name:

A string value that indicates what principal should be used when deploying the file or archive during startup and shutdown. This principal will be used to set the current subject when calling out into application code for interfaces such as ApplicationLifecycleListener. If no principal name is specified, then the anonymous principal will be used. [More Info...](#)

Save

Modules and Components

Showing 1 to 1 of 1 Previous | Next

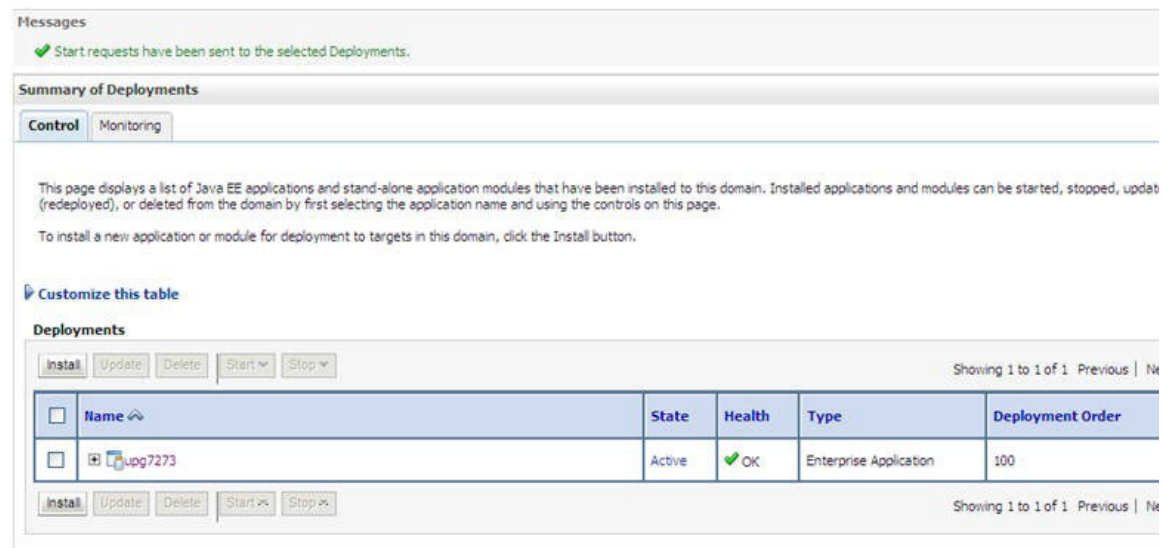
Name	Type
upg7273	Enterprise Application
EJBs	
StatelessCacheBeanBean	EJB
Modules	
upg7273	Web Application
beancache.jar	EJB Module
Web Services	
None to display	

Showing 1 to 1 of 1 Previous | Next

- 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.
- Click Save to update the changes, if any.
- From the LHS menu, click Deployments. The Summary of Deployments window is displayed.
- Select the newly deployed Infrastructure application and click Start > Servicing all requests. Ensure that the Infrastructure server is up and running.

OFS BEHAVIOR DETECTION INSTALLATION GUIDE | 207

Figure 115: Summary of Deployments



The State of the deployed application will be displayed as Active if started successfully.

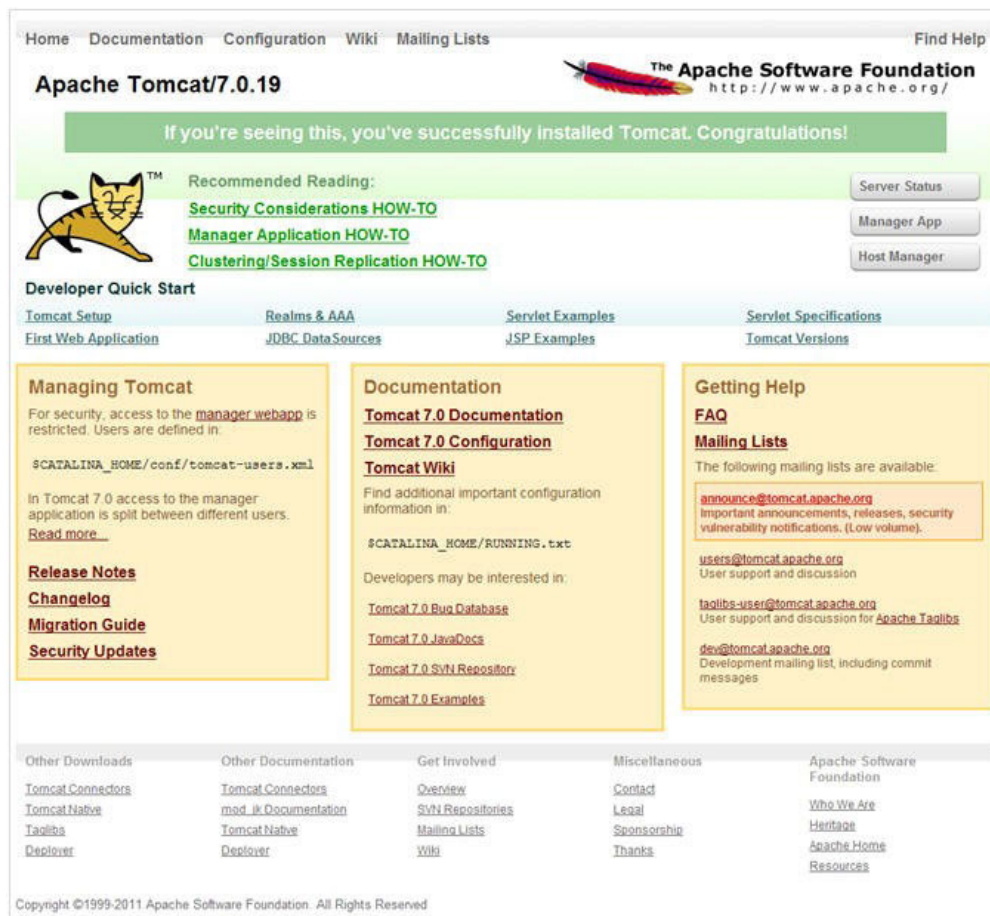
12.2.4 Deploying Tomcat WAR Files on Tomcat

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 these steps to deploy Infrastructure application:

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

Figure 116: Tomcat Home Page



2. Click Manager App. The Connect to dialog box is displayed.
3. Enter the User ID with administrative privileges and click OK. (For user creation in tomcat, see [Tomcat User Administration](#).)
4. The Tomcat Web Application Manager window is displayed with the list of all the applications deployed.

Figure 117: Tomcat Web Application Manager

docs	None specified	Tomcat Documentation	true	0	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ 30 minutes
examples	None specified	Servlet and JSP Examples	true	0	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ 30 minutes
host-manager	None specified	Tomcat Host Manager Application	true	0	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ 30 minutes
manager	None specified	Tomcat Manager Application	true	1	Start <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> <input type="button" value="Expire sessions"/> with idle ≥ 30 minutes

Deploy
Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:

WAR file to deploy
Select WAR file to upload

Diagnostics
Check to see if a web application has caused a memory leak on stop, reload or undeploy
 This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP
Apache Tomcat/7.0.57	1.6.0_45-b06	Sun Microsystems Inc.	Linux	2.6.39-400.211.1.el6uek.x86_64	amd64	ofsa220354.in.oracle.com	10.18

Copyright © 1999-2014, Apache Software Foundation

5. In the Deploy section, enter the Context Path provided during the installation as /<context-name>.
6. 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.
7. On successful application deployment, a confirmation message is displayed. Start the Tomcat server. See [Starting Infrastructure Services](#) for more details.

13 Appendix E: Starting/Stopping Infrastructure Services

This section details about how to start and stop Infrastructure services.

Topics:

- Starting Infrastructure Services
- Starting Web Application Servers
- Stopping Infrastructure Services
- Cleaning up the environment

13.1 Starting Infrastructure Services

Once the installation of Infrastructure is 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 following servers mentioned 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.

To start Infrastructure Services, follow these steps:

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.

2. Start ICC server:

- On the machine in which Infrastructure default Application components have been installed, navigate to `$FIC_HOME/ficapp/icc/bin`.
- Execute the command: `./icccserver.sh.`

NOTE

Only Infrastructure Default Application Server would hold ICC component.

3. Start Back-end Services:

- On the machine on which Infrastructure Database components have been installed, navigate to `$FIC_DB_HOME/bin` 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.

13.2 Starting Web Application Servers

Start the Web application server depending on the type as described in [Table 21](#).

Table 21: Webserver start up options

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

13.3 Stopping Infrastructure Services

To stop Infrastructure services, follow these steps:

1. On the machine in which Infrastructure Application components have been installed, navigate to `$FIC_APP_HOME/common/FICServer/bin` and execute the command: `./stopofsaai.sh`.
2. To stop ICC server, on the machine in which Infrastructure default Application components have been installed, navigate to `$FIC_HOME/ficapp/icc/bin` and execute the command: `./iccserversshutdown.sh`.

NOTE 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` and execute the command: `./agentshutdown.sh`.

13.4 Cleaning up the environment

To clean up the environment, follow these steps:

1. Navigate to `$FIC_HOME`.

2. Execute `./Uninstall.sh`.
3. When prompted, enter OFSAI configuration schema password. This will delete `$FIC_HOME` and drop all the objects from configuration schema.
4. Navigate to ftpshare folder.
5. Delete the infodom folders `$ rm -rf <INFODOM>`.
6. Drop configuration and atomic schemas from the database.

14 Appendix F: Accessing OFSAA Application

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

To access the OFSAA application, follow the step:

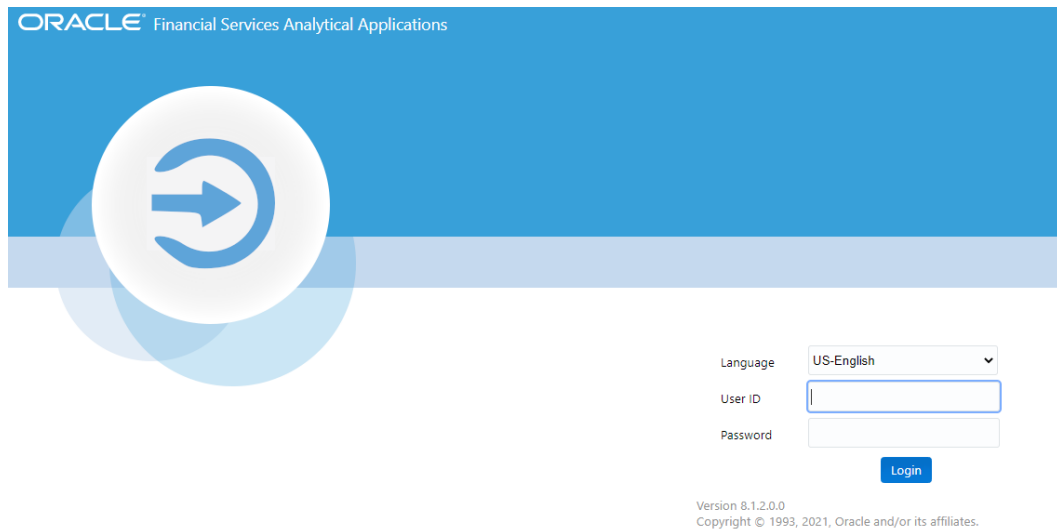
1. From your desktop, open the browser and enter the URL in the following format:

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

For example, <https://111.222.333.444:5555/ofsaa/login.jsp>

The OFSAA login screen is displayed.

Figure 118: OFSAA Login Window



With installation of every OFSAA Applications 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*

2. Login to the application using the SYSADMN User ID. (Note that, there is no "l" 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.

15 **Appendix G: Cloning 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](#).

16 Appendix H: OFSAA Landing Page

Topics:

- [OFSAA Landing Page](#)
- [Enabling Product within Applications Pack](#)

16.1 OFSAA Landing Page

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 on the Landing Page:

- [Applications Tab](#)
- [Sandbox Tab](#)
- [Object Administration Tab](#)
- [System Configuration and Identity Management Tab](#)

16.1.1 Applications Tab

This tab lists the various OFSAA Applications that are installed in the setup.

The <Select Application> drop-down lists the OFSAA Applications based on the user logged in and User Group(s) mapped to OFSAA Application. Selecting an Application from the drop-down refreshes the menus/links.

16.1.2 Sandbox Tab

This tab lists the various OFSAA Sandboxes created in the setup.

The <Select Sandbox> drop-down lists the OFSAA Sandboxes based on the user logged in and User Group(s) mapped to OFSAA Application.

Selecting a Sandbox from the drop-down would refresh the menus/links.

16.1.3 Object Administration Tab

This tab lists the various OFSAA Information Domains created in the setup.

The <Select Information Domain> drop-down lists the OFSAA Information Domains based on the user logged in and User Group(s) mapped to OFSAA Application.

Selecting an Information Domain from the drop-down refreshes the menus/links.

16.1.4 System Configuration and 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/Information Domain dropdown list in this tab.

NOTE

See the [AAI User Guide](#) for more details on how to operate on each tab.

16.2 Enabling Product within Applications Pack

You can also enable a product/application within an Applications Pack post installation at any point of time.

To enable a product through the application UI, follow these steps:

1. Login to the application as SYSADMN user or any user with System Administrator privileges.
2. Navigate to System Configurations & Identity Management tab and expand Financial Services Analytical Applications Infrastructure >> Administration and Configuration >> System Configuration.
3. Click Manage OFSAA Product License(s)

The Manage OFSAA Product License(s) page is displayed as below. This page includes the following sections:

- INSTALLED Applications Packs
- PRODUCTS IN THE Applications Pack

Figure 119: Manage OFSAA Product License(s) Page

Financial Services Analytical Applications Infrastructure > Administration and Configuration > System Configuration > Manage OFSAA Product License(s)

MANAGE OFSAA APPLICATION PACK LICENSE				
» INSTALLED APPLICATION PACKS				
	APPLICATION PACK ID	APPLICATION PACK NAME	DESCRIPTION	INSTALL DATE
<input checked="" type="radio"/>	OFS_AAAI_PACK	Financial Services Advanced Analytics Infrastructure Pack	Applications for Advanced Analytics using Oracle R, Modeling & Stress Testing Framework and Inline Processing Engine	2014-12-02 14:22:33.0
<input type="radio"/>	OFS_CAP_ADO_PACK	Financial Services Capital Adequacy Applications Pack	Applications for Basel Basic, IRB & Analytic, Operational Risk Economic Capital & Analytic and Retail Portfolio Risk Models and Pooling in Banking and Financial Services Domain	2014-12-02 17:59:58.0

» PRODUCTS IN THE APPLICATION PACK				
ENABLE	PRODUCT ID	PRODUCT NAME	DESCRIPTION	ENABLE DATE
<input checked="" type="checkbox"/>	OFS_AAAI	Financial Services Enterprise Modeling	Base Infrastructure for Advanced Analytical Applications	2014-12-02 14:22:33.0
<input checked="" type="checkbox"/>	OFS_IPE	Financial Services Inline Processing Engine	Framework for Inline Processing Engine	

[VIEW LICENSE AGREEMENT](#) [RESET](#)

The following fields described in [Table 22](#) are displayed in the INSTALLED Applications Packs section:

Table 22: Installed Applications Pack - Field Description

Field Name	Description
Applications Pack ID	Displays a unique Applications Pack ID related to the Applications Pack. Select the appropriate Pack id using the radio button. The Products in the Applications Pack will be displayed below in the PRODUCTS IN THE Applications Packs section.
Applications Pack Name	Displays the name of the Applications Pack.
Description	Displays the description of the Applications Pack.
Install Date	Displays the date when the Applications Pack was installed.

The following fields described in [Table 23](#) are displayed in the PRODUCTS IN THE Applications Pack section:

Table 23: Pproducts in the Applications Pack - Field Description

Field Name	Description
Enable	Select the check box to enable a product within an Applications Pack.
Product ID	Displays a unique product id for the product.
Product Name	Displays the name of the Product.
Description	Displays the description of the product.
Enable Date	Displays the date when the product was enabled.

4. Select an Applications Pack by clicking the radio button next to the Applications Pack ID field.
5. Selecting an Applications Pack will display below the products within the Applications Pack.
6. Products which were enabled at the time of installation will have the check box *ENABLE* disabled. You can enable any product within the selected Applications Pack by clicking the *ENABLE* check box against the respective Product ID.
7. Click on RESET button to cancel the operation and refresh the screen.
8. Click VIEW LICENSE AGREEMENT button. The License Agreement section is displayed.
9. Select the option I ACCEPT THE LICENSE AGREEMENT.

10. Click ENABLE. A pop-up message confirmation is displayed showing that the product is enabled for the pack.

NOTE

To use the newly enabled product, you need to map your application users to the appropriate product specific User_Group(s) and subsequently, authorize the actions by logging in as System Authorizer.

- For more information, see the *Mapping/Unmapping Users* section in [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).
- To identify the newly enabled product specific UserGroups/Applications Pack specific User_Groups, see the respective Applications Pack specific Installation and Configuration Guide/User Manual.

17 Appendix I: Additional Configuration

This section gives detailed information about the Additional Configuration regarding OFSAA Installation.

Topics:

- [Configuring FTP/SFTP](#)
- [Configuring Infrastructure Server Memory](#)
- [Configuring Internet Explorer Settings](#)
- [Retrieving Patch Information](#)
- [Setting OLAP Data Server Configuration](#)
- [Changing IP/Hostname, Ports, Deployed Paths of the OFSAA Instance](#)
- [Executing OFSAAI Setup Information Fetching Tool](#)
- [Executing Encryption Changer](#)
- [Setting Infrastructure LDAP Configuration](#)
- [Enabling Parallel Execution of DML Statements](#)
- [Configure Message Details in Forms Designer](#)
- [Clearing Application Cache](#)
- [Configuring Password Changes](#)

17.1 Configuring FTP/SFTP

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

Topics:

- [Adding FTP/SFTP Configuration for File Transfer](#)
- [Setting Up SFTP Private Key](#)

17.1.1 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.

To ensure the OFSAA server recognizes the web application server during file transfers, follow these steps:

1. Log in to the web application server.
2. Type `sftp <user>@<OFSAA Server>`.
3. Specify Yes when prompted for permission.
4. This will add an entry into the *known_hosts* file.

A confirmation message is displayed.

17.1.2 Setting Up SFTP Private Key

NOTE

- To set up SFTP Private Key for Oracle Linux 8.x or Red Hat Enterprise Linux 8.x., see Doc ID [28900101](#).
- For installation, log in to OFSAA Unix user using Putty tool, 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 must be set to `NA`.

To set up SFTP private key, follow these steps:

1. Enter the commands as: `ofsaapp@OFSASERVER:~> ssh-keygen -t rsa` Generating public/private rsa key pair.
2. Enter file in which to save the key (`/home/ofsaapp/.ssh/id_rsa`): Created directory `/home/ofsaapp/.ssh`.
3. 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`
4. Ensure the following permissions exist for the given folders:
 - Permission of `.ssh` must be 700
 - Permission of `.ssh/authorized_keys` must be 640
 - Permission of `.ssh/id_rsa` must be 400
 - Permission of Unix user created must be 755

17.2 Configuring 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 128 MB for heap and 64 MB for stack.

You can configure the Infrastructure Application Memory settings as follows:

1. Locate the `.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

This parameter is modified in 7.3.2 IR and you need to 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"
```

17.3 Configuring Internet Explorer Settings

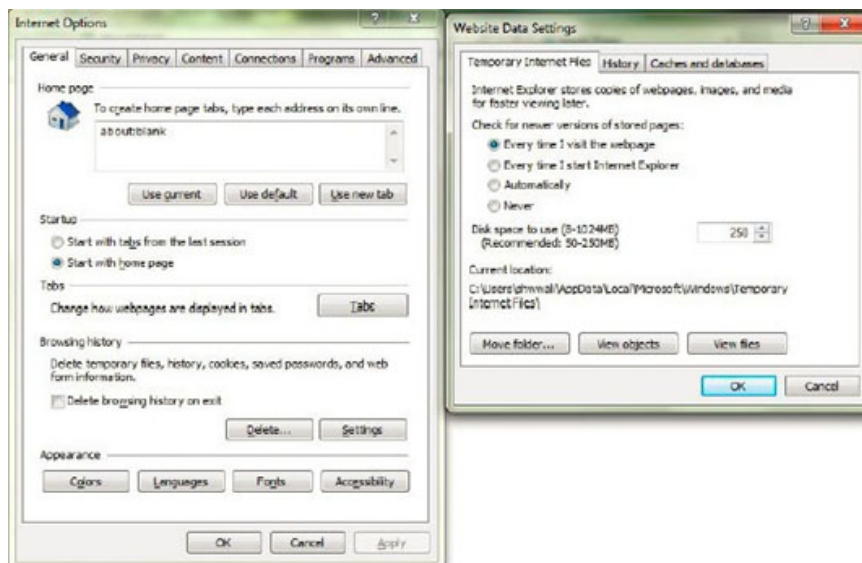
NOTE OFSAAI supports only default zoom setting in Internet Explorer, that is, 100%. Cookies should be enabled.

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

To set up the settings, follow these steps:

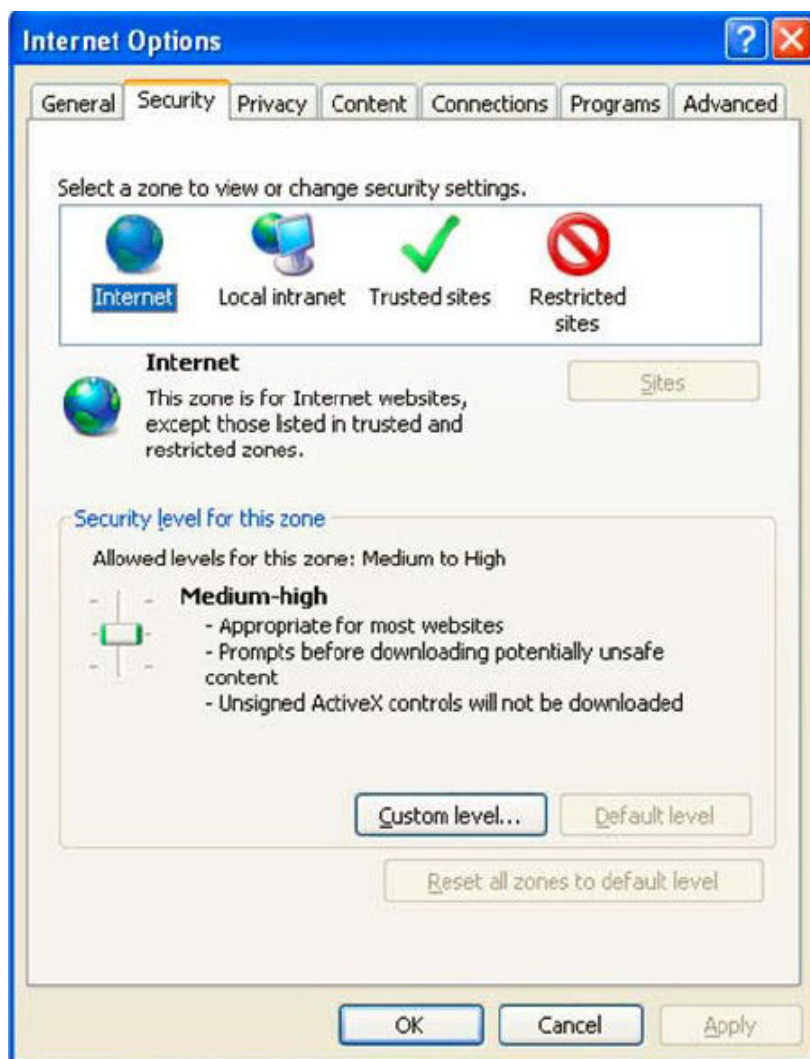
1. Open Internet Explorer. Select Tools > Internet Options. The Internet Options window is displayed.
2. Click Settings. The Settings window is displayed.
3. Select Every time I Visit the webpage and click OK.

Figure 120: Internet Options



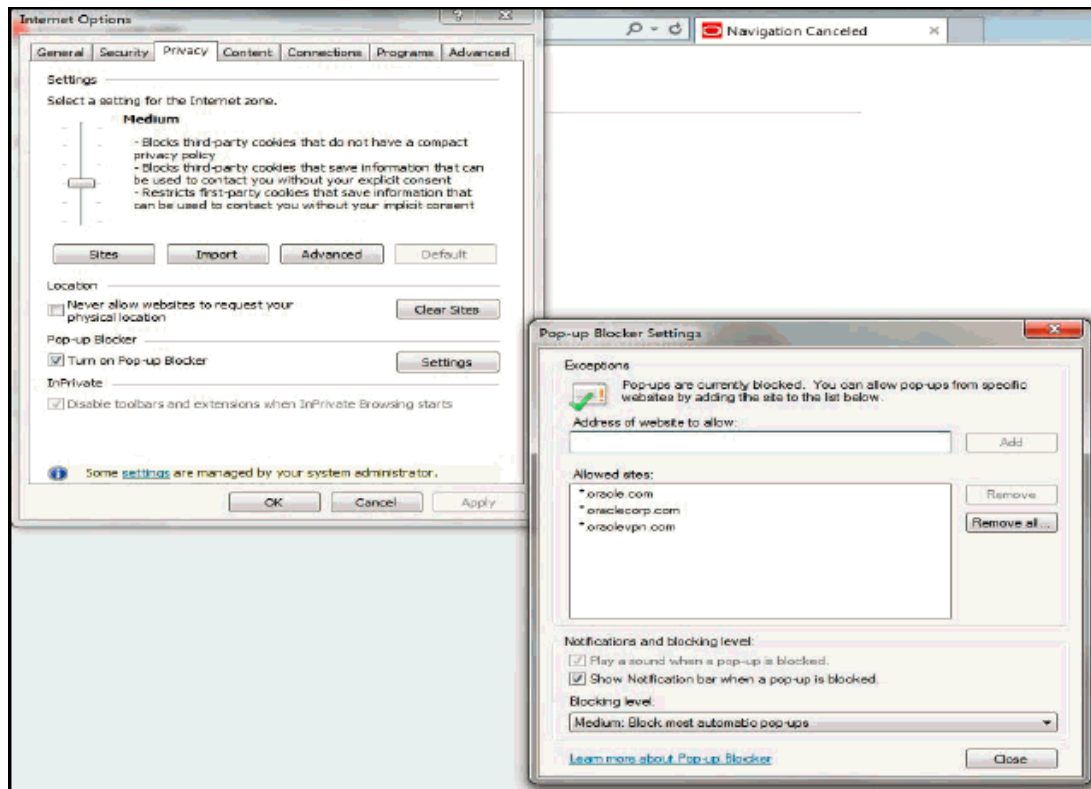
4. In the Internet Options window, select the Security tab and select the Internet option under Select a zone to view or change the security settings.
5. Click Default Level under Security level for this zone.

Figure 121: Internet Options - Security Tab



6. Click Apply to save.
7. Click Internet Explorer > Tools > Compatibility View Settings.
8. Enter the OFSAA setup URL in the Add this website field.
9. Click Add.
10. Ensure the URL is listed under Websites you've added to Compatibility View.
11. In the Internet Options window, select the Privacy tab and select the Turn on Pop-up Blocker option under Pop-up Blocker settings.

Figure 122: Internet Options- Popup Blocker Settings



12. Click Settings. The Pop-up Blocker Settings window is displayed.
13. Enter the URL of the OFSAA Application in the Address of website to allow: field.
14. Click Add. The OFSAA URL is displayed in the Allowed sites section.
15. Click Close.
16. Click OK in the Internet Options window.

17.4 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.
3. Click System Utilities.
4. Click Patch Information.

The page displays the list of patches installed on the OFSAA setup across Applications/Platform.

17.5 Setting 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.

For 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.

17.6 Changing IP/Hostname, Ports, Deployed Paths of the OFSAA Instance

For information on this section, see [OFSAAI Administration Guide](#).

17.7 Executing 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, follow these steps:

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.

17.8 Executing Encryption Changer

For more information on Encryption Changer, see *Key Management* in [OFSAAI Administration Guide](#).

17.9 Setting Infrastructure LDAP Configuration

For more information on LDAP configuration, see [OFSAAI Administration Guide](#).

17.10 Enabling 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 from 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.

17.11 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 as described in [Table 24](#) :

Table 24: NotificationConfig.cfg File

Parameter	Description
SMTP_SERVER_IP	Specify the hostname 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.

17.12 Clearing Application Cache

This is applicable to all Web servers (that is, WebSphere, WebLogic, and Tomcat).

To clear the application cache, follow these steps:

1. Prior to the deployment of Infrastructure or Application Service Packs/One-off patches, clear the cache.
2. Navigate to the following path depending on the WebServer configured and delete the files:
 - a. **Tomcat:** <Tomcat installation folder>/work/Catalina/localhost/<Application name>/org/apache/jsp
 - b. **WebLogic:** <WebLogic installation location>/domains/<Domain name>/servers/<Server name>/tmp/_WL_user/<Application name>/qaelce/jsp_servlet
 - c. **WebSphere:** <WebSphere installation directory>/AppServer/profiles/<Profile name>/temp/<Node name>/server1/<Application name>/<.war file name>

17.13 Configuring Password Changes

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

Topics:

- [Modifying OFSAA Infrastructure Config Schema password](#)
- [Modifying OFSAA Infrastructure Atomic Schema Password](#)
- [Configuring Internal Service \(Document Upload/Download\)](#)

17.13.1 Modifying OFSAA Infrastructure Config Schema password

To change the Config Schema password, follow these 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`.
5. 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.

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

17.13.2 Modifying OFSAA Infrastructure Atomic Schema Password

To change the Atomic Schema password, follow these 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. Select the appropriate connection and edit the password.
4. Navigate to Data Management Tools >Data Sources> Source Designer window. Update the password of the appropriate Source
5. 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).
6. 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).
7. 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).
8. Restart the OFSAI services.

17.13.3 Configuring 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 these configurations:

1. Create the folders download, upload, TempDocument and Temp in the local path of Web application server and provide Read/Write permission.
 - a. To find the exact location, execute the following query in CONFIG schema: `select localpath from web_server_info.`
 - b. 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.
 - a. To find the exact location, execute the query in CONFIG schema: `select ftpdrive from app_server_info.`
 - b. To create folder with Read/Write permission, execute the command: `mkdir -m 777 DocStorage.`

18 **Appendix J: OFSAA Infrastructure Installation**

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

See [My Oracle Support](#) for more information on the latest release.

19 Appendix K: Grants for Atomic/Config Schema

This section mentions about the various grants required for the CONFIG, ATOMIC schemas.

Topics:

- [Configuring Grants for Atomic Schema](#)
- [Configuring Grants for Config Schema](#)
- [Configuring Grants for Config Schema Entities for Atomic Users](#)

19.1 Configuring Grants for Atomic Schema

Atomic Schema creation requires certain grants for object creation. This can be located in \$FIC_HOME/privileges_atomic_user.sql file. The following are the Grants for Atomic Schema:

```
grant create SESSION to &database_username
/
grant create PROCEDURE to &database_username
/
grant create SEQUENCE to &database_username
/
grant create TABLE to &database_username
/
grant create TRIGGER to &database_username
/
grant create VIEW to &database_username
/
grant create MATERIALIZED VIEW to &database_username
/
grant select on SYS.V_$PARAMETER to &database_username
/
grant create SYNONYM to &database_username
/
```

NOTE

If you intend to use Oracle OLAP feature, execute the following grant on all ATOMIC schema(s):

```
grant olap_user to &database_username
```

19.2 Configuring Grants for Config Schema

Config Schema creation requires certain grants for object creation. This can be located in \$FIC_HOME/privileges_config_user.sql file.

The following are the Grants for Config Schema:

```
grant create SESSION to &database_username
/
grant create PROCEDURE to &database_username
/
grant create SEQUENCE to &database_username
/
grant create TABLE to &database_username
/
grant create TRIGGER to &database_username
/
grant create VIEW to &database_username
/
grant create MATERIALIZED VIEW to &database_username
/
grant select on SYS.V_$PARAMETER to &database_username
/
grant create SYNONYM to &database_username
/
```

19.3 **Configuring Grants for Config Schema Entities for Atomic Users**

Atomic Schema creation requires certain grants for config schema object access. This can be located in \$FIC_HOME/config_table_privileges_for_atomic_user.sql file.

20 Appendix L: Configuring Application Pack XML Files

This section explains configuration of the OFS_BD_PACK.xml and OFS_BD_SCHEMA_IN.xml files.

Topics:

- [Configuring OFS_BD_PACK.xml File](#)
- [Configuring OFS_BD_SCHEMA_IN.xml File](#)

20.1 Configuring OFS_BD_PACK.xml File

The OFS_BD_PACK.xml file holds details on the various OFSAA products that are packaged in a particular Applications Pack.

Table 25 provides the details about the various tags/parameters available in the file and the values should be updated. Prior to installing the OFSAA Applications Pack in Silent mode, it is mandatory to update this file.

Table 25: OFS_BD_PACK.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
APP_PACK_ID	Unique Applications Pack Identifier	Y	Unique Seeded Value	DO NOT modify this value.
APP_PACK_NAME	Unique Applications Pack Name	Y	Unique Seeded Value	DO NOT modify this value.
APP_PACK_DESCRIPTION	Unique Applications Pack Description	Y	Unique Seeded Value	DO NOT modify this value.
VERSION	Unique Application Pack 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. 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 Applications Packs, Infrastructure would have this value set to "YES". DO NOT modify this value.

Table 25: OFS_BD_PACK.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
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.
APP_DESCRIPTOR N	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.

20.2 Configuring OFS_BD_SCHEMA_IN.xml File

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

Table 26 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.

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
APP_PACK_ID	Unique Applications Pack Identifier	Y	Unique Seeded Value	DO NOT modify this value.
<IS_TCPS>	Enter if the TCPS configuration is required.	Y	Seeded, with FALSE as the default value.	Modify this to TRUE if you require the installer to uptake the configuration.

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandatory (Y/N)	Default Value/ Permissible Value	Comments
<JDBC_URL>	Enter the JDBC URL Note: You can enter RAC and NON-RAC enabled database connectivity URL.	Y	Example, jdbc:oracle:thin:@<DBSERVER IP/ HOST>:<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	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.
<JDBC_DRIVER>	By default, this driver name is seeded. Note: Do not edit this attribute value.	Y	Example, oracle.jdbc.driver.Oracle Driver	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	

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
<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 E.g. dev_ofsaaconf, uat_ofsaaconf etc.
<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.
<PASSWORD>/ DEFAULT*	Enter the password if you want to set a default password for all schemas. Note: You also need to set APPLYSAMEFORALL 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.	

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandatory (Y/N)	Default Value/ Permissible Value	Comments
<PASSWORD>/ APPLYSAMEFORALL	<p>Enter as Y if you want to apply the password specified in DEFAULT attribute for all the schemas.</p> <p>If you enter as N, you need to provide individual passwords for all schemas</p> <p>Note: In case you have entered Y in APPLYSAMEFORALL Attribute and also have specified individual passwords for all the schemas, then the specified individual passwords will take precedence.</p>	Y	Default - N Permissible - Y or N	<p>If set to N, need to specify PASSWORD value for every SCHEMA.</p> <p>Note: If the DEFAULT attribute is set, setting the attribute value is mandatory.</p>
ROLE/ NAME	Database Role Name attribute used to update place holders.	Y	Unique Seeded value	DO NOT modify this value

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
DIRECTORY/ID	<p>External Directory ID value used to update placeholders.</p> <p>External directory should be created in DB server as shown below:</p> <pre> <DIRECTORIES> <DIRECTORY ID="OFS_ BD_PACK_EXTER NAL_ DIRECTORY_1" NAME="\$OFS_AM L_ SCHEMA_NAME_ DIR\$" VALUE="/users/ fccms/802/ AAI_802/bdf/ inbox" /> </DIRECTORIES> </pre>	Y	Unique Seeded value	DO NOT modify this value.

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandatory (Y/N)	Default Value/ Permissible Value	Comments
<SCHEMA>/ TYPE	<p>The different types of schemas that are supported in this release are ATOMIC, CONFIG, SANDBOX, and ADDON.</p> <p>By default, the schemas types are seeded based on the Applications Pack.</p> <p>Note: Do not edit this attribute value.</p>	Y	<p>ATOMIC/CONFIG/ SANDBOX/ADDON</p> <p>NOTE: SANDBOX AND ADDON Schemas are not applicable for OFS AAAI Applications Pack.</p>	<p>Only One CONFIG schema can exist in the file.</p> <p>This schema identifies as the CONFIGURATION schema that holds the OFSAA setup details and other metadata information.</p> <p>Multiple ATOMIC/ SANDBOX/ ADDON Schemas can exist in the file.</p> <p>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 Applications Pack).</p>

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
<SCHEMA.>/ NAME	<p>By default, the schemas names are seeded based on the Applications Pack. You can edit the schema names if required.</p> <p>Note:</p> <p>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 Applications Pack.</p>	Y	The permissible length is 15 characters and only alphanumeric characters allowed. No special characters allowed except underscore '_'.	<p>SETUPINFO/ NAME</p> <p>Attribute value would be prefixed to the schema name being created.</p> <p>For E.g. if name is set as 'ofsaaatm' and setupinfo as 'uat' then schema, being created would be 'uat_ofsaaatm'.</p> <p>NAME should be same where APP_GRP=1 for all SCHEMA tags (Not applicable for this Applications Pack).</p> <p>NOTE:</p> <p>For example:</p> <pre><Variable name="DATABASE NAME">KYCDB.oracle.co m </Variable></pre> <p>A TNS entry must be made in tnsnames.ora with tnsname same as the value provided for KYC Database Name. If sqlnet.ora file is configured with a value in NAMES.DEFAULT_ DOMAIN then ensure to use the same domain while defining Database Name. It is required for KYC Batch processing.</p> <p>This name should be unique</p> <p>The same above steps to be done for CTR.</p> <p>A restart of web and app servers are necessary whenever any changes are done to config schema</p>

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

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. Takes precedence over DEFAULT attribute value of <PASSWORD> tag.
<SCHEMA>/ APP_ID	By default, the Application ID is seeded based on the Applications 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>/ DEFAULTTABL ESPACE	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>/ TEMPTABLESP ACE	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.

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

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	Infodom Name Associated with each Atomic Schema and ADDON.	Y	Enter the name of the Information Domain to associate this schema. The schema creator utility automatically derives an Information Domain Name based on the Applications Pack if no value is specified for this attribute. Permissible length is 16 characters and only alphanumeric characters allowed. No special characters allowed.	Valid string with up to 11 characters. Mandatory for Silent Installation Mode
<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>

Table 26: OFS_BD_SCHEMA_IN.XML Parameters

Tag Name/ Attribute Name	Description	Mandato ry (Y/N)	Default Value/ Permissible Value	Comments
<TABLESPACES>	Parent tag to hold <TABLESPACE> elements	N	NA	Note: If the Database Admin creates the TABLESPACES, specific entries can be created in the respective tags. 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 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_BD_DATA_CM_TBSP"
VALUE="DATA_CM_TBSP"
DATAFILE="/scratch/oraofss/app/oradata/
Ti26012L64/case_data_01.dbf" SIZE="512M"
AUTOEXTEND="OFF" ENCRYPT="OFF"/>
<TABLESPACE NAME="OFS_BD_IDX_CM_TBSP"
VALUE="IDX_CM_TBSP"
DATAFILE="/scratch/oraofss/app/oradata/
Ti26012L64/case_idx_01.dbf" SIZE="512M"
AUTOEXTEND="OFF" ENCRYPT="OFF" />
<TABLESPACE NAME="OFS_COMM_DATA_TBSP"
VALUE="COMM_DATA_TBSP"
DATAFILE="/scratch/oraofss/app/oradata/
Ti26012L64/comm_data_01.dbf" SIZE="512M"
AUTOEXTEND="OFF" ENCRYPT="OFF"/>
<TABLESPACE NAME="OFS_BD_DATA_CONF_TBSP"
VALUE="DATA_CONF_TBSP"
DATAFILE="/scratch/oraofss/app/oradata/
Ti26012L64/comm_data_01.dbf" SIZE="1024M"
AUTOEXTEND="OFF" ENCRYPT="OFF"/>
</TABLESPACES>
<SCHEMAS>
<SCHEMA TYPE="CONFIG" NAME="ofsaaconf" PASSWORD=""
APP_ID="OFS AAI"
DEFAULTTABLESPACE="##OFS_BD_DATA_CONF_TBSP##"
TEMPTABLESPACE="TEMP" QUOTA="10G"/>
<SCHEMA TYPE="ATOMIC" NAME="ofsaaBD" PASSWORD=""
APP_ID="OFS IPE"
DEFAULTTABLESPACE="##OFS_BD_DATA_CM_TBSP##"
TEMPTABLESPACE="TEMP" QUOTA="10G"
INFODOM="BDINFO"/>
<SCHEMA TYPE="ATOMIC" NAME="ofsaaBD" PASSWORD=""
APP_ID="OFS NGBD"
DEFAULTTABLESPACE="##OFS_BD_DATA_CM_TBSP##"
TEMPTABLESPACE="TEMP" QUOTA="10G"
INFODOM="BDINFO"/>
</SCHEMAS>
```

21

Appendix M: Configuring OFSAI_InstallConfig.xml File

This section gives details about the OFSAI_InstallConfig.xml file.

To configure the OFSAI_InstallConfig.xml file, follow these steps.

1. Navigate to OFS_AAI_PACK/OFS_AAI/conf/directory.
2. Open the file OFSAI_InstallConfig.xml in text editor.
3. Configure the OFSAI_InstallConfig.xml as described in [Table 27](#).
4. You must 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.

Table 27: OFSAA Infrastructure Installation Tasks and Descriptions

Interaction Variable Name	Significance and Expected Value	Mandatory
<Layer name="GENERAL">		
InteractionGroup name="WebServerType"		
WEBAPPSERVERTYPE	Identifies the web application server on which the OFSAA Infrastructure web components would be deployed. The following 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</InteractionVariable>	Yes
InteractionGroup name="OFSAA Infrastructure Server Details"		
DBSERVER_IP	Identifies the hostname 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
InteractionGroup name="Database Details"		
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

Table 27: OFSAA Infrastructure Installation Tasks and Descriptions

Interaction Variable Name	Significance and Expected Value	Mandatory
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 Appendix O: JDBC Jar Files for identifying the correct "ojdbc<version>.jar" version to be copied.	Yes
InteractionGroup name="OLAP Detail"		
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 following 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.		
InteractionGroup name="SFTP Details"		
SFTP_ENABLE	Identifies if the SFTP (Secure File Transfer Protocol) feature is to be enabled. The following numeric value should be set depending on the choice: For SFTP -1. For 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. You can change this selection later by using the OFSAAI administration interface. Set SFTP_ENABLE to -1 to configure ftpshare and weblocal path as local path mounted for OFSAAI server.		
FILE_TRANSFER_PORT	Identifies the port used for the file transfer service. The default value specified is 22 (SFTP). Specify default value as 21 (FTP) if SFTP_ENABLE is 0. Alternatively, this value can be any Port configured by System Administrators to support SFTP/FTP. For example, <InteractionVariable name="FILE_TRANSFER_PORT">21</InteractionVariable>	Yes
InteractionGroup name="Locale Detail"		

Table 27: OFSAA Infrastructure Installation Tasks and Descriptions

Interaction Variable Name	Significance and Expected Value	Mandatory
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
InteractionGroup name="OFSAA Infrastructure Communicating ports" Note: The following ports are used internally by the various OFSAA Infrastructure services. The default values mentioned 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
InteractionGroup name="Web Details" 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.		
HTTPS_ENABLE	Identifies if the UI should be accessed using HTTP or HTTPS scheme. The default value set is 0. The following 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/ Hostname or Web Application Server IP/ Hostname, 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/Hostname. For example, <InteractionVariable name="WEB_SERVER_IP">10.11.12.13</InteractionVariable> or <InteractionVariable name="WEB_SERVER_IP">myweb.server.com</InteractionVariable>	No

Table 27: OFSAA Infrastructure Installation Tasks and Descriptions

Interaction Variable Name	Significance and Expected Value	Mandatory
WEB_SERVER_PORT	<p>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.</p> <p>NOTE:</p> <p>The port value will not be accepted as 80 if HTTPS_ENABLE is 1 and as 443, if HTTPS_ENABLE is 0.</p> <p>For example, <InteractionVariable name="WEB_SERVER_PORT">80</InteractionVariable></p>	No
CONTEXT_NAME	<p>Identifies the web application context name which will be used to built the URL to access the OFSAA applications. The context name can be identified from a URL as follows:</p> <p><scheme>://<host>:<port>/<context-name>/login.jsp</p> <p>Sample URL: https://myweb:443/ofsaadev/login.jsp</p> <p>For example, <InteractionVariable name="CONTEXT_NAME">ofsaadev</InteractionVariable></p>	Yes
WEBAPP_CONTEXT_PATH	<p>Identifies the absolute path of the exploded .ear file on the web application server.</p> <p>For Tomcat, specify the Tomcat directory path till /webapps, such as</p> <p>/oradata6/revwb7/tomcat/webapps/.</p> <p>For WebSphere, enter the WebSphere path as <WebSphere profile directory>/installedApps/ <NodeCellName>. For example,</p> <p>/data2/test//WebSphere/AppServer/profiles/<Profile_Name>/installedApps/aix-imfNode01Cell. Where aix-imf is Host name.</p> <p>For WebLogic, provide the WebLogic home directory path as /<WebLogic home directory path>/bea/wlserver_10.3</p> <p>NOTE:</p> <p>For WebLogic, value specified for this attribute is ignored and value provided against attribute WEBLOGIC_DOMAIN_HOME is considered.</p>	Yes
WEB_LOCAL_PATH	<p>Identifies the absolute path to any directory on the web application server that can hold temporary files being uploadd as part of the applications usage.</p> <p>NOTE:</p> <p>In case of a clustered deployment, ensure this path and directory is same on all the nodes.</p>	Yes
InteractionGroup name="Weblogic Setup Details"		

Table 27: OFSAA Infrastructure Installation Tasks and Descriptions

Interaction Variable Name	Significance and Expected Value	Mandatory
WEBLOGIC_DOMAIN_HOME	Identifies the WebLogic Domain Home. 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)
InteractionGroup name="OFSAI FTP Details"		
OFSAI_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 the following APP_SFTP_USER_ID parameter should have RWX permission on the directory. For example, <InteractionVariable name="APP_FTPSHARE_PATH">">/oradata6/revwb7/ftpshare</InteractionVariable>	Yes
OFSAI_SFTP_USER_ID	Identifies the user who has RWX permissions on the directory identified under the preceding parameter APP_FTPSHARE_PATH.	Yes
OFSAI_SFTP_PRIVATE_KEY	Identifies the SFTP private key for OFSAI. For example, <InteractionVariable name="OFSAI_SFTP_PRIVATE_KEY">/home/ofsaapp/.ssh/id_rsa</InteractionVariable> By default, the value is NA, which indicates password will be prompted for the user <OFSAI_SFTP_USER_ID> for authentication. For more information on generating SFTP Private key, see Setting Up SFTP Private Key .	No
OFSAI_SFTP_PASSPHRASE	Identifies the passphrase for the SFTP private key for OFSAI. For example, <InteractionVariable name="OFSAI_SFTP_PASSPHRASE">enter a pass phrase here</InteractionVariable> By default, the value is NA. If OFSAI_SFTP_PRIVATE_KEY value is given and this is kept as NA, then it is assumed as empty passphrase.	No

22 Appendix N: Migrating for Excel Upload Functionality

This section provides detailed instructions to migrate excel upload functionality.

Topics:

- [Prerequisites](#)
- [Migrating Excel Upload](#)

22.1 Prerequisites

The following are the prerequisites for migration:

- "Data model in ATOMIC schemas should be same on the source and target setups
- "OFS AAI (platform) patch level version should be same on the source and target setups.
- "PL/SQL Developer to connect and query the database.
- "WinSCP to connect and access server file system.

22.2 Migrating Excel Upload

To migrate, follow these steps:

1. Open PL/SQL Developer and log in to the source setup's configuration (CONFIG) schema by entering the appropriate username and password.
2. In a new SQL window query the data of table EXCEL_MAPPING_MASTER.
3. Open a new session in PL/SQL developer and log in to the target setup's configuration (CONFIG) schema by entering the appropriate username and password.
4. Insert the records from Step 1 above in to this table.
5. In V_INFODOM column of EXCEL_MAPPING_MASTER table update the infodom name with the target infodom name.

NOTE

If all the mappings can work out of the single target Infodom, update same Infodom value across all rows. If only few mappings will work out of the target infodom, update the infodom value for selective records. Kindly note, excel upload mappings will work only if the target infodom has same data model entities as used in the mappings defined on source setup.

6. Update V_CREATED_BY column with the name of any user present in the target setup that has appropriate roles to perform Excel Upload tasks.

NOTE

It is mandatory to update values for V_INFODOM and V_CREATED_BY columns.

7. Open WinSCP and login a new session by entering the host name, port number, user name and password to access the source setup.
8. Navigate to the folder referred as FTPSHARE.

9. Copy the excel-entity mapping xml file(s) which are located in this folder according to their folder structure on to your desktop. For example: /ftpshare
/STAGE/ExcelUpload/\$SOURCE_INFODOM_NAME/\$EXCEL_FILE_NAME.xml

NOTE	Actual file name of Excel Sheet is mentioned in the V_EXCEL_NAME column of EXCEL_MAPPING_MASTER table.
-------------	--

10. Copy the excel templates (.xls/ .xlsx) file(s) which are located in this folder according to their folder structure on to your desktop. For example:
/ftpshare/STAGE/ExcelUpload/TEMPLATE/*.xls or *.xlsx

NOTE	Ignore this step if files are not present at the location.
-------------	--

11. Login a new session in WinSCP by entering the host name, port number, user name and password to access the target setup.
12. Copy the xml file(s) from Step 3 to the below location in the target setup. For example:
/ftpshare/STAGE/ExcelUpload/\$TARGET_INFODOM_NAME/\$EXCEL_FILE_NAME.xml

NOTE	\$TARGET_INFODOM_NAME must be target setup infodomain in which you have upload the appropriate data model and the name should be same as the V_INFODOM column value updated in EXCEL_MAPPING_MASTER table.
-------------	--

13. Copy the xls/ xlsx file(s) from Step 3 to the below location in target setup. For example:
/ftpshare/STAGE/ExcelUpload/TEMPLATE/*.xls or *.xlsx

NOTE	Ignore this step if files are not available at the location.
-------------	--

23 Appendix O: JDBC Jar Files

The `ojdbc<version>.jar` file must be copied based on the Oracle Database version and the supported Java (JRE/ JDK) versions. See [Table 28](#) for details.

Table 28: JDBC Jar files version details

Oracle Database Version	JDK/JRE Version Supported	JDBC Jar files specific to the release
19c	<ul style="list-style-type: none">• JDK 8• JRE 8• JDK11	Ojdbc8.jar

24 Appendix P: Upgrading an Existing OFSAA 8.0.x JAVA 7 Instance to Java 8

This section describes the configurations required to upgrade an existing OFSAA 8.0.x Java 7 instance to Java 8.

Topics:

- [Prerequisites](#)
- [Upgrading OFSAA 8.0.x Java 7 Instance to Java 8](#)
- [Configuring Web Application Server](#)
- [Configuring User .profile Settings](#)
- [Configuring OFSAA for New Web Application Server Installation](#)

24.1 Prerequisites

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

- Java 8 must 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 [My Oracle Support](#) for the same.

24.2 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 [Configurations for Java 8](#). For a newly installed Web application server, see [Configuring OFSAA for New Web Application Server Installation](#).
3. Restart the OFSAA services. For more information, see the *Start/Stop Infrastructure Services* section in [Appendix E: Starting/Stopping Infrastructure Services](#).
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 [Appendix D: Creating and Deploying EAR/WAR File](#).

24.3 Configuring Web Application Server

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

Topics:

- [Upgrading Oracle WebLogic Server](#)
- [Upgrading Apache Tomcat Server](#)

24.3.1 Upgrading Oracle WebLogic Server

To upgrade the existing WebLogic server instance to Java 8, follow these steps:

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 wish 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 [Appendix B: Configure Resource Reference in Web Servers](#).

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.

24.3.2 Upgrading Apache Tomcat Server

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 [Appendix B: Configure Resource Reference in Web Servers](#).

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.

24.4 Configuring User .profile Settings

To configure the user.profile settings, follow these steps:

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/jre 1.8.0_45/jre JAVA_BIN=/usr/java/jre 1.8.0_45/jre/bin
LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:/usr/java/jre 1.8.0_45/jre/lib/amd64/server.

24.5 Configuring OFSAA 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.

To configure OFSAA for new web application server installation, 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

25 Appendix Q: Removing OFSAA

Topics:

- Uninstalling OFSAA Infrastructure
- Uninstalling EAR Files in WebSphere
- Uninstalling EAR Files in WebLogic
- Uninstalling WAR Files in Tomcat

25.1 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, follow these steps:

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 [Figure 123](#).

Figure 123: Uninstalling OFSAA Infrastructure

```
/scratch/ofsaadb/OFSAAI>./Uninstall.sh
Uninstallation Started [time : Tue Jun 10 14:20:27 IST 2014 ]
*****
*** Driver loaded with Driver oracle.jdbc.driver.OracleDriver

Please enter Configuration schema Password :
Connected to Config Schema
Cleaning config schema ....
config schema cleaned ...
Cleaning up Infrastructure Home Dir !
Please wait ..
Uninstallation Completed ! Thank You [time : Tue Jun 10 14:21:59 IST 2014 ]
*****
/scratch/ofsaadb/OFSAAI>
```

NOTE

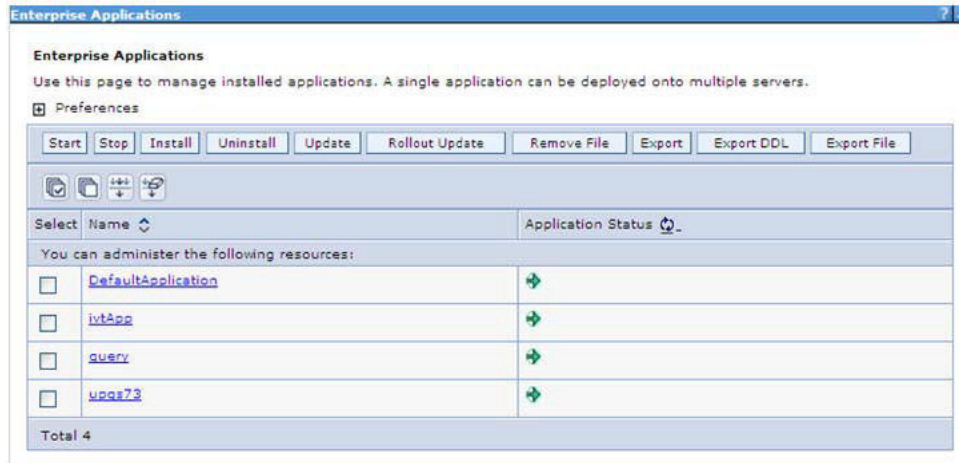
- Uninstallation does not remove the Infrastructure application from the Web application server. This has to be done manually.
- The entries in the .profile file will have to be removed manually.
- The files/ folders under the file system staging area (ftpshare) have to be deleted manually.
- All the Database objects from Atomic Schemas have to be dropped manually.

25.2 Uninstalling EAR Files in WebSphere

To uninstall the EAR files, follow these steps:

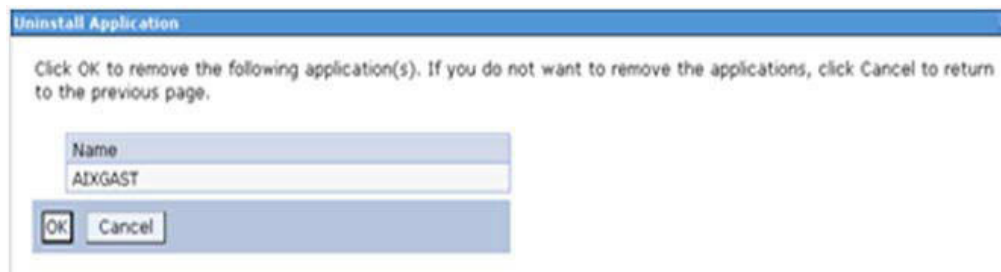
1. Open the URL in the browser window: <http://<ipaddress>:<Administrative Console Port>/ibm/console> (https if SSL is enabled). The Login window is displayed.
2. Log in with the user ID with administrative privileges.
3. Expand Applications > Application Types > WebSphere enterprise applications from the LHS. The Enterprise Applications window is displayed with all the deployed applications.

Figure 124: Enterprise Applications



4. Select the check box adjacent to the application to be uninstalled and click Stop.
5. Click Uninstall. The Uninstall Application window is displayed.

Figure 125: Uninstall Application



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

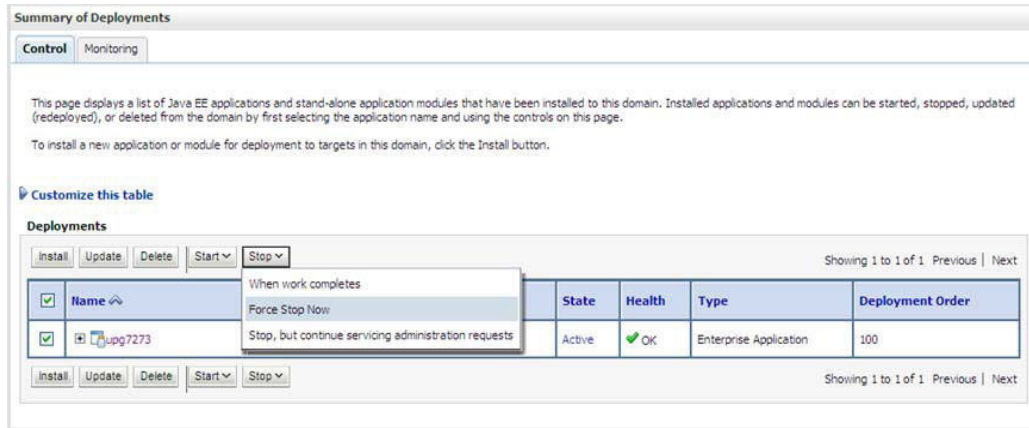
25.3 Uninstalling EAR Files in WebLogic

On the machine that hosts WebLogic, follow these 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.

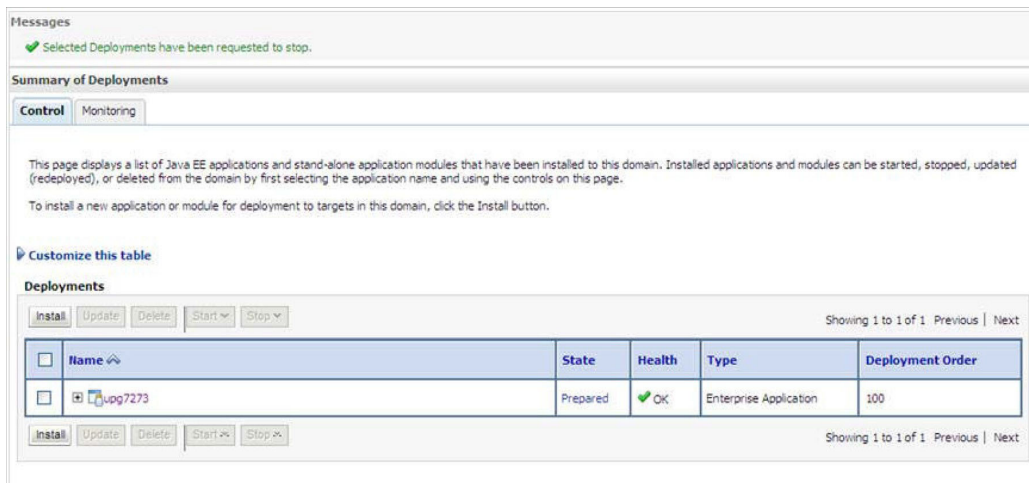
- From the Domain Structure LHS menu, click Deployments. The Summary of Deployments screen is displayed.

Figure 126: Summary of Deployments



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

Figure 127: Summary of Deployments- Messages



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

25.4 Uninstalling WAR Files in Tomcat

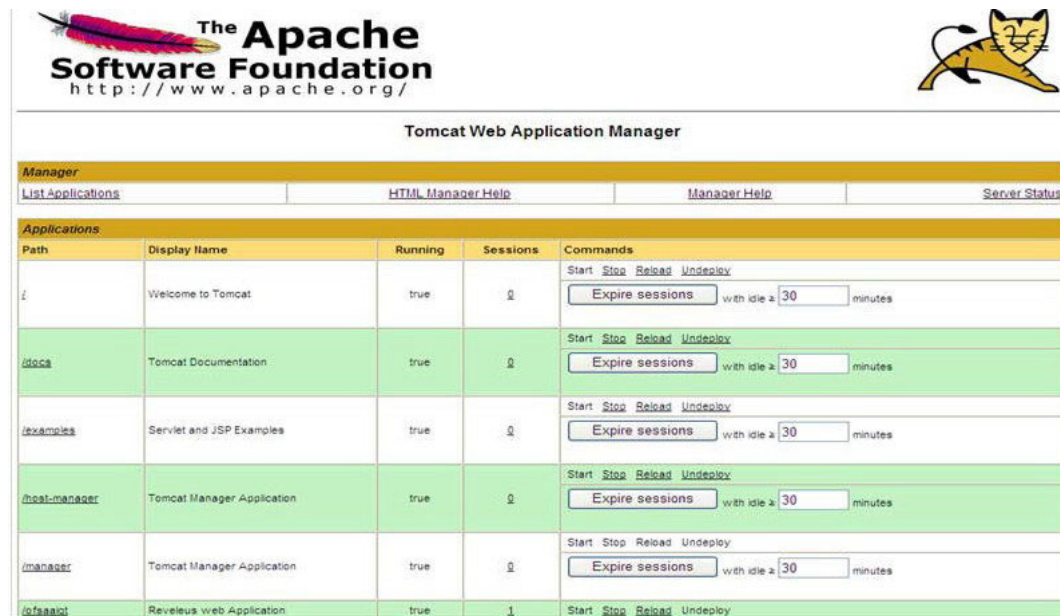
On the machine that hosts Tomcat, follow these steps to uninstall any previously deployed application:

- 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>
-->
```

2. 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 command `./shutdown.sh`.
 - d. Start the tomcat services using the command `./startup.sh`.
3. Open the URL in a browser window: <http://<IP address>:<Tomcat server port>>. (https if SSL is enabled). The Tomcat home window is displayed.
4. Click the Manager App. The Connect to window is displayed.
5. 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.

Figure 128: Tomcat Web Application Manager



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

26 Appendix R: Configuring TDE and Data Redaction in OFSAA

Two features comprise Oracle Advanced Security: Transparent Data Encryption and Oracle Data Redaction.

This section details about the configurations required in case you want to enable TDE or Data Redaction in OFSAA applications.

Topics:

- [Transparent Data Encryption \(TDE\)](#)
- [Data Redaction](#)

26.1 Transparent Data Encryption (TDE)

Transparent Data Encryption (TDE) enables you to encrypt sensitive data, such as Personally Identifiable Information (PII), that you store in tables and tablespaces. After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data. To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a Keystore. For more details on TDE, see the [Database Advanced Security Guide](#). TDE tablespace encryption enables you to encrypt all of the data stored in a tablespace. To control the encryption, you use a Keystore and TDE master encryption key. Oracle Database supports both software keystores and hardware, or

HSM-based, keystores. A software keystore is a container for the TDE master encryption key, and it resides in the software file system.

26.1.1 Configuring TDE During Behavior Detection Installation Using Full Installer

This section provides information on how to enable TDE (Transparent Data Encryption) in the database.

Topics:

- [Configuring a Software Keystore and Encrypted Tablespace Creation](#)
- [Running the Schema Creator Utility With Encryption](#)
- [Testing the Encryption](#)

26.1.1.1 Configuring a Software Keystore and Encrypted Tablespace Creation

A software keystore is a container for the TDE master encryption key, and it resides in the software file system. You must define a location for the key in the sqlnet.ora file so that the database locates the keystore (one per database) by checking the keystore location in the sqlnet.ora file. After defining the location, create the keystore and open it. Set the TDE master key after opening it and then encrypt the data.

To find whether a wallet is already existing, check the following entries:

1. The location specified by the ENCRYPTION_WALLET_LOCATION parameter in the sqlnet.ora file.
2. The location specified by the WALLET_LOCATION parameter in the sqlnet.ora file.

3. Encrypted tablespaces can share the default database wallet. However, Oracle recommends that you use a separate wallet for transparent data encryption functionality by specifying the `ENCRYPTION_WALLET_LOCATION` parameter in the `sqlnet.ora` file.

NOTE You should have proper privileges to perform the following actions.

To configure the software keystore, follow these steps:

1. **Step 1: Set the Software keystore location in the `sqlnet.ora` file**

The first step is to designate a location for software keystore in the `sqlnet.ora` file. The Oracle Database will check the `sqlnet.ora` file for the directory location of the keystore to determine whether it is a software keystore or a hardware module security (HSM) keystore.

NOTE Ensure that the directory location which you want to set for software keystore exists beforehand. Preferably, this directory must be empty.

In a multitenant environment, the keystore location is set for the entire multitenant container database (CDB), not for individual pluggable databases (PDBs).

By default, the `sqlnet.ora` file is located in the `ORACLE_HOME/network/admin` directory or in the location set by the `TNS_ADMIN` environment variable. Ensure that you have properly set the `TNS_ADMIN` environment variable to point to the correct `sqlnet.ora` file.

To create a software keystore on a regular file system, use the following format when you edit the `sqlnet.ora` file:

```
ENCRYPTION_WALLET_LOCATION= (SOURCE=
(METHOD=FILE) (METHOD_DATA=
(DIRECTORY=<<path to keystore>>)))
```

Examples:

For regular file system in which the database name is `orclb`: `ENCRYPTION_WALLET_LOCATION= (SOURCE= (METHOD=FILE) (METHOD_DATA= (DIRECTORY=/etc/ORACLE/WALLETS/orcl)))`

When multiple databases share the `sqlnet.ora` file:

```
ENCRYPTION_WALLET_LOCATION= (SOURCE=
(METHOD=FILE) (METHOD_DATA=
(DIRECTORY=/etc/ORACLE/WALLETS/orcl)))
```

When Oracle Automatic Storage Management (ASM) is configured:

```
ENCRYPTION_WALLET_LOCATION= (SOURCE=
(METHOD=FILE) (METHOD_DATA=
(DIRECTORY=+disk1/mydb/wallet)))
```

For ASM Diskgroup:

```
ENCRYPTION_WALLET_LOCATION= (SOURCE=
```

(METHOD=FILE) (METHOD_DATA=
(DIRECTORY=+ASM_file_path_of_the_diskgroup)))

2. Step 2: Create the Software Keystore

There are three different types of Software Keystores:

- Password-based Software Keystores
- Auto-login Software Keystores
- Local Auto-login Software Keystores

a. Follow these steps to create a software keystore:

- i. Login as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
- ii. Use the following command to create password-based software keystore:

```
CONN sys/password@serviceid AS SYSDBA
```

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE 'keystore_location' IDENTIFIED  
BY software_keystore_password;
```

keystore_location is the path of the keystore directory you want to create

software_keystore_password is the password of the keystore that you want to create.

For example, to create the keystore in the /etc/ORACLE/WALLETS/orcl directory:

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/etc/ORACLE/WALLETS/  
orcl'
```

```
IDENTIFIED BY password;
```

After you run this statement, the ewallet.p12 file, which is the keystore, appears in the keystore location.

Alternatively, you can create an Auto-Login or Local-Login Keystore to avoid opening the Keystore manually every time. Use the following command:

```
ADMINISTER KEY MANAGEMENT CREATE [LOCAL] AUTO_LOGIN KEYSTORE FROM  
KEYSTORE 'keystore_location' IDENTIFIED BY keystore_password;
```

LOCAL enables you to create a local auto-login software keystore. Otherwise, omit this clause if you want the keystore to be accessible by other computers.

After you run this statement, the cwallet.sso file appears in the keystore location.

NOTE

It is important to remember the master key password (<keystore_password>) used during creation of the keystore. There are no ways to retrieve the password if forgotten.

3. Step 3: Open the Software Keystore

Depending on the type of keystore you create, you must manually open the keystore before you can use it.

You do not need to manually open auto-login or local auto-login software keystores. These keystore are automatically opened when it is required, that is, when an encryption operation must access the key. If necessary, you can explicitly close any of these types of keystores. You can check the status of whether a keystore is open, closed, open but with no master key, or open

but with an unknown master key by querying the STATUS column of the V\$ENCRYPTION_WALLET view.

NOTE After you open a keystore, it remains open until you manually close it. Each time you restart a database instance, you must manually open the password keystore to re-enable encryption and decryption operations.

Follow these steps to open the software wallet:

Login as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.

Use the following command to open password-based software keystore:

```
CONN sys/password@serviceid AS SYSDBA
```

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY software_
keystore_password [CONTAINER = ALL | CURRENT];
```

software_keystore_password is the same password that you used to create the keystore in *Step 2: Create the Software Keystore*.

CONTAINER is for use in a multitenant environment. Enter ALL to set the keystore in all of the PDBs in this CDB, or CURRENT for the current PDB.

NOTE In a CDB, open the Keystore in the ROOT (CDB\$ROOT) container and in all the associated PDBs, where TDE is enabled.
You do not need to manually open auto-login or local auto-login software Keystores.

4. Step 4: Set the Software TDE Master Encryption Key

Once the keystore is open, you can set a TDE master encryption key for it. The TDE master encryption key is stored in the keystore. This key protects the TDE table keys and tablespace encryption keys. By default, the TDE master encryption key is a key that Transparent Data Encryption (TDE) generates.

In a multitenant environment, you can create and manage the TDE master encryption key from either the root or the PDB.

Ensure that the database OPEN_MODE is set as READ WRITE. To find the status for a non-multitenant environment, query the OPEN_MODE column of the V\$DATABASE dynamic view. If you are using a multitenant environment, then query the V\$PDBS view. (If you cannot access these views, then connect as SYSDBA and try the query again. In order to connect as SYSKM for this type of query, you must create a password file for it. See Oracle Database Administrator's Guide for more information.)

Follow these steps to set the encryption key:

- a. Login as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
- b. Use the following command to set the encryption key:

```
CONN sys/password@serviceid AS SYSDBA
```

```
ADMINISTER KEY MANAGEMENT SET KEY [USING TAG 'tag'] IDENTIFIED BY
password [WITH BACKUP [USING 'backup_identifier']] [CONTAINER = ALL |
CURRENT];
```

- tag is the associated attributes and information that you define. Enclose this setting in single quotation marks (' ').
- password is the mandatory keystore password that you created when you created the keystore in "Step 2: Create the Software Keystore".
- WITH BACKUP creates a backup of the keystore. You must use this option for password-based keystores. Optionally, you can use the USING clause to add a brief description of the backup. Enclose this description in single quotation marks (' '). This identifier is appended to the named keystore file (for example, ewallet_time_stamp_emp_key_backup.p12, with emp_key_backup being the backup identifier). Follow the file naming conventions that your operating system uses.
- CONTAINER is for use in a multitenant environment. Enter ALL to set the key in all of the PDBs in this CDB, or CURRENT for the current PDB.

For example,

```
ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY password WITH BACKUP
USING 'emp_key_backup';
```

5. Step 5: Encrypting your Data

After completing the keystore configuration, encrypt the data. You can encrypt individual columns in a table or entire tablespaces. OFSAA recommends encrypting entire tablespaces and the description in this section covers encrypting entire tablespaces.

Note the following restrictions on using Transparent Data Encryption when you encrypt a tablespace:

- Transparent Data Encryption (TDE) tablespace encryption encrypts or decrypts data during read and write operations, as compared to TDE column encryption, which encrypts and decrypts data at the SQL layer. This means that most restrictions that apply to TDE column encryption, such as data type restrictions and index type restrictions, do not apply to TDE tablespace encryption.
- To perform import and export operations, use Oracle Data Pump. Encrypting data involves the following steps:
 - Setting the COMPATIBLE initialization parameter for tablespace encryption.
 - Setting the tablespace TDE master encryption key.
 - Creating the Encrypted Tablespace.

Step 1: Setting the COMPATIBLE initialization parameter for tablespace encryption

Prerequisite- You must set the COMPATIBLE initialization parameter for the database to 11.2.0.0 or later. Once you set this parameter to 11.2.0.0, the change is irreversible.

Follow these steps to set the COMPATIBLE initialization parameter:

1. Log into the database instance. In a multitenant environment, log into the PDB.
2. Check the current setting of the COMPATIBLE parameter as described in [Table 29](#).

Table 29: Show Parameter Compatible

Name	Type	Value
Compatible	String	12.0.0.0
noncdbcompatible	Boolean	False

3. If you want to change the COMPATIBLE parameter, follow these steps:
 - a. Locate the initialization parameter file for the database instance.
 UNIX systems: This file is in the ORACLE_HOME/dbs directory and is named initORACLE_SID.ora (for example, initmydb.ora).
 - b. In SQL*Plus, connect as a user who has the SYSDBA administrative privilege, and then shut down the database.
 For example:

```
CONNECT /AS SYSDBA SHUTDOWN
```
 - c. Edit the initialization parameter file to use the correct COMPATIBLE setting.
 For example:

```
COMPATIBLE = 12.2.0.0
```
 - d. In SQL*Plus, ensure that you are connected as a user who has the SYSDBA administrative privilege, and then start the database.
 For example:

```
CONNECT /AS SYSDBA STARTUP
```
 - e. If tablespace encryption is in use, then open the keystore at the database mount. The keystore must be open before you can access data in an encrypted tablespace.

```
STARTUP MOUNT;
```

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY password; ALTER DATABASE OPEN;
```

Step 2: Setting the tablespace TDE master encryption key

Make sure that you have configured the TDE master encryption key as shown in Step 4: Setting the software TDE master encryption key.

Step 3: Creating the Encrypted Tablespace

After you have set the COMPATIBLE initialization parameter, you are ready to create the encrypted tablespace.

Follow the instruction given in Running the Schema Creator Utility with Encryption section for configuring the schema creator file to create tablespaces.

If you are enabling TDE in case of upgrade or you did not enable it during installation and want to enable at a later point of time, for more information, see on manually [Creating Encrypted Tablespaces](#).

26.1.1.2 Running the Schema Creator Utility With Encryption

This section is applicable only if you want to enable TDE during installation.

Run the schema creator utility by including the encrypt=on option in the Tablespace tag in the

<<APP PACK>>_SCHEMA_IN.xml file. You have to perform this procedure manually as it is not a part of the <<APP PACK>>_SCHEMA_IN.xml.TEMPLATE originally.

Following is an example for OFS_AAAI_PACK_SCHEMA_IN.xml

```
<APPPACKSCHEMA>
<APP_PACK_ID>OFS_AAAI_PACK</APP_PACK_ID>
<JDBC_URL>jdbc:oracle:thin:@<DB_Server_IP>:1521:<DB_NAME></JDBC_URL>
<JDBC_DRIVER>oracle.jdbc.driver.OracleDriver</JDBC_DRIVER>
<HOST><OFSAA_Server_IP/HOST Name></HOST>
<SETUPINFO NAME="<PREFIX_NAME>" PREFIX_SCHEMA_NAME="Y"/>
<PASSWORD APPLYSAMEFORALL="Y" DEFAULT="<PASSWORD>" />
<TABLESPACES>
<TABLESPACE NAME="OFS_AAI_TBSP" VALUE="TS_USERS1" DATAFILE="<ABSOLUTE PATH to
TABLESPACE>/<TABLESPACE_DATA_FILE_NAME>.dbf" SIZE="500M" AUTOEXTEND="OFF"
ENCRYPT="ON" />
</TABLESPACES>
<SCHEMAS>
<SCHEMA TYPE="CONFIG" NAME="ofsaaconf" PASSWORD="" APP_ID="OFS_AAI"
DEFAULTTABLESPACE="##OFS_AAI_TBSP##" TEMPTABLESPACE="TEMP"
QUOTA="unlimited"/>
<SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_AAAI"
DEFAULTTABLESPACE="##OFS_AAI_TBSP##" TEMPTABLESPACE="TEMP" QUOTA="unlimited"
INFODOM="OFSAAAIINFO"/>
<SCHEMA TYPE="ATOMIC" NAME="ofsaaatm" PASSWORD="" APP_ID="OFS_IPE"
DEFAULTTABLESPACE="##OFS_AAI_TBSP##" TEMPTABLESPACE="TEMP" QUOTA="unlimited"
INFODOM="OFSAAAIINFO"/>
</SCHEMAS>
</APPPACKSCHEMA>
```

26.1.1.3 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;
```

indicates whether the TABLESPACE is encrypted or not in the ENCRYPTED column.

Table 30: Testing the Encryption

TABLESPACE_NAME	ENCRYPTED
SYSTEM	No
SYS_AUX	No
UNDOTBS1	No

Table 30: Testing the Encryption

TABLESPACE_NAME	ENCRYPTED
TEMP	No
USERS	No
ENCRYPTED_TS	Yes
6 rows selected.	

The above example indicates TABLESPACE ENCRYPTED_TS is created with Encryption ON.

26.1.2 Configuring TDE in Case of Upgrade

This section details about the configurations required in case you want to enable TDE in OFSAA applications after upgrade to OFSAA 8.1.2.0.0 version from a previous version. Additionally, these configurations are required in case you did not enable TDE during 8.1.2.0.0 installation and want to enable at a later point of time.

Configuring TDE in case of upgrade, follow these steps:

1. Create a new PDB (12c)/ instance (11g) on same or different Database Server for TDE. For more information, see [Configuring a Software Keystore and Encrypted Tablespace Creation](#).
2. Shutdown the OFSAAI Services.
3. Export all Configuration, Atomic and Sandbox Schemas as per the applications installed in your OFSAA instance.

For example:

```
expdp SYSTEM/oracle@OFSAA12C2DB DIRECTORY=data_pump_dir
DUMPFILE=ofsaaconf_ofsaaatm_%U.dmp filesize=2G SCHEMAS=ofsaaconf,ofsaaatm
LOGFILE=ofsaaconf_ofsaaatm_exp.log.
```

NOTE

The above command will create data dumps as files of 2GB size each (multiples). Any other commands/tools as appropriate may be used to archive the schemas.

4. Import all schemas that are exported using the above command, into the new DB instance. For example:

```
impdp SYSTEM/oracle@OFSAA12nDB DIRECTORY=data_pump_dir
DUMPFILE=ofsaaconf_ofsaaatm_%U.dmp SCHEMAS=ofsaaconf,ofsaaatm
LOGFILE=ofsaaconf_ofsaaatm_imp.log
```

NOTE

Restoring the exported dumps creates Configuration and Atomic Schema(s) with the same user credentials as that of the source, along with the existing grants.

If schemas are restored using a tool/ mechanism other than as mentioned in the Step 1 and 2, retain the user credentials of Configuration and Atomic Schemas same as in the Source environment, along with the Schema grants.

5. Provide select grants on sys.V_\$parameter to view Configuration and Atomic Schemas of Target Environment database.

For example:

Login as sys user:

```
SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaacnf;
```

Grant succeeded

```
SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaatm;
```

Grant succeeded

6. Update .profile for ORACLE_SID environment variable with new ORACLE_SID.
7. Update JDBC URL by executing Port Changer utility. For details on how to execute Port Changer utility, see [Changing IP/Hostname, Ports, Deployed Paths of the OFSAA Instance](#).
8. Navigate to the \$FIC_WEB_HOME directory and execute the following command to trigger the creation of EAR/WAR file: `./ant.sh`.
9. The EAR/WAR file - <contextname>.ear/.war - is created in \$FIC_WEB_HOME directory. On completion of EAR/WAR file creation, a message indicating that build is successful is displayed.
10. Edit the existing Connection Pool settings to point to new JDBC URL and verify connections.
11. Clear the webserver cache and redeploy the application onto your configured web application server.
12. Restart the OFSAA Services. For more information, refer to the Start/Stop Infrastructure Services section in [Oracle Financial Services Advanced Analytical Applications Infrastructure Application Pack Installation and Configuration Guide](#).

26.2 Data Redaction

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

26.2.1 Enabling Data Redaction in case of Upgrade

This section details about the configurations required in case you want to enable Data Redaction in OFSAA applications after upgrade to OFSAA 8.1.2.0.0 version from a previous version. Additionally, these configurations are required in case you did not enable TDE during BD Application Pack 8.1.2.0.0 installation and want to enable at a later point of time.

Follow these steps:

1. Login as SYSDBA into the database.
2. Execute the file `$FIC_HOME/utility/data_security/scripts/create_data_sec_roles.sql` only once per database (PDB in case of 12c).
3. Execute the following sql statement to find out the list of atomic users from the table:

```
select v_schema_name from aai_db_detail where V_DB_NAME <> 'CONFIG' AND  
V_DB_TYPE = 'ORACLE'
```

4. Execute the file `$FIC_HOME/utility/data_security/scripts/grant_data_sec_roles.sql` for all atomic users found in the previous step.
5. From the Configuration window in the System Configuration module, select the Allow Data Redaction checkbox.
6. Run the Data Redaction utility. For more details on how to run the utility, see the *Data Redaction* section in [OFS Analytical Applications Infrastructure Administration Guide](#).

27 Appendix S: Tunable Database Parameters

This appendix contains the Tunable Database Parameters.

NOTE

Review the Oracle recommended guidelines in setting the `SGA_TARGET`, `SGA_MAX_SIZE` and `PGA_AGGREGATE_TARGET` parameters. The values for these memory parameters can vary significantly based on database server specifications and estimated data volume. For values of `PGA_AGGREGATE_TARGET` parameter Oracle recommends that they be kept at a minimum of 1024 MB.

Table 31 describes the Database Tunable Parameters.

Table 31: Database Tunable Parameters

Tunable Database Parameters		Parameter Values			
Category	Parameter Name	Type	Default	Oracle Recommended	Oracle Recommended for Exadata
Parameters affecting database creation (not tunable through the init.ora file)	CHARACTER SET	string	AL32UTF8	AL32UTF8	AL32UTF8
	NLS_LENGTH_	string	byte	byte	byte
	NLS_SORT	binary	binary	binary	binary
	MAXDATAFILES	integer	254		
	MASXINSTANCES	integer	1		
	MAXLOGFILES	integer	32		
	MAXLOGHISTORY	integer	24794		
	MAXLOGMEMBER	integer	2	4	4
	S				
	REDO LOG SIZE	integer	10M	3G	16G

Table 31: (Continued) Database Tunable Parameters

Tunable Database Parameters		Parameter Values			
Parameters affecting I/O operation	DB_BLOCK_SIZE	integer	2048	8192	8192
	DB_FILE_MULTIBLOCK_READ_COUNT	integer	The default value corresponds to the maximum I/O size that can be efficiently performed and is platform-dependent.	32	32
	DB_FILES	integer	200		
	DISK_ASYNC_IO	boolean	TRUE		
	TAPE_ASYNC_IO	boolean	TRUE		
	DB_WRITER_PROCESSES	integer	1	4	4

Table 31: (Continued) Database Tunable Parameters

Tunable Database Parameters		Parameter Values			
Parameters affecting resource consumption and parallel operations	FAST_START_PARALLEL_ROLLBACK	string	LOW	HIGH	HIGH
	LOG_BUFFER	integer	7M	10000000	10000000
	LOG_CHECKPOINT_INTERVAL	integer	0	10000	10000
	LOG_CHECKPOINT_TIMEOUT	integer	0	0	0
	OPEN_CURSORS	integer	50	4096	4096
	PARALLEL_EXECUTION_MESSAGE_SIZE	integer	2148	16384	16384
	PARALLEL_MAX_SERVERS	integer	10 * No of CPUs	Set if you are configuring DOP manually at site and PARALLEL_DEGREE_POLICY is set to MANUAL.	Do not set or change
	PARALLEL_MIN_SERVERS	integer	0	Set if you are configuring DOP manually at site and PARALLEL_DEGREE_POLICY is set to MANUAL.	Do not set or change
	PROCESSES	integer	150	600	600
	LARGE_POOL_SIZE	integer	0	512M	

Table 31: (Continued)Database Tunable Parameters

Tunable Database Parameters		Parameter Values			
	PARALLEL_MIN_PERCENT	integer	0	Set if you are configuring DOP manually at site and PARALLEL_DEGREE_POLICY is set to MANUAL.	Do not set or change
	PARALLEL_THREADS_PER_CPU	integer	2		
Additional needed parameters	OPTIMIZER_MODE	string	ALL_ROWS	ALL_ROWS	ALL_ROWS
	COMPATIBLE	string		11.2.0 (for Oracle 11gR2)	11.2.0 .3.0(if using Oracle 11.2.0.3.0) otherwise 11.2.0.2.0
	GLOBAL_NAMES	string	FALSE	TRUE	TRUE
	PRE_PAGE_SGA	string	FALSE	TRUE	TRUE
	UNDO_MANAGEMENT	string	AUTO	AUTO	AUTO
	UNDO_TABLESPACE	string		Set as Per Site Values	Set as Per Site Values
	UNDO_RETENTION	integer	900	10800	18000
	TIMED_STATISTICS	boolean	TRUE	TRUE	TRUE
	OPTIMIZER_INDEX_CACHING	integer	0		
	OPTIMIZER_INDEX_COST_ADJ	integer	100	30	
	QUERY_REWRITE_ENABLED	string	TRUE	FALSE	FALSE

Table 31: (Continued)Database Tunable Parameters

Tunable Database Parameters		Parameter Values			
	STAR_TRANSFORMATION_ENABLED	string	FALSE	FALSE	FALSE

28 Appendix T: FAQs and Error Dictionary

This section of the document consists of resolution to the frequently asked questions and error codes noticed during OFSAAI installation.

Topics:

- [Frequently Asked Questions](#)
- [Error Dictionary](#)
- [Error Code Dictionary](#)

OFSAAI installer performs all the pre-requisite validation check during installation. Any errors encountered in the process is displayed with an appropriate Error Code. You can see the Error Dictionary to find the exact cause and resolution to rectify the error.

28.1 Frequently Asked Questions

You can see the Frequently Asked Questions which has been developed with the interest to help you resolve some of the OFSAAI Installation and configuration issues. This intends to share the knowledge of problem resolution to a few of the known issues. This is not an official support document and just attempts to share the knowledge of problem resolution to a few of the known issues.

Topics:

- [OFSAAI FAQs](#)
- [Applications Pack 8.1.2.0.0 FAQs](#)
- [Forms Framework FAQs](#)

28.1.1 OFSAAI FAQs

1. What are the different components that get installed during OFSAAI?

The different components of OFSAAI are illustrated in [Figure 2](#).

2. What are the different modes of OFSAAI installation?

OFSAAI can be installed in Silent mode.

3. Can the OFSAA Infrastructure components be installed on multi-tier?

No. OFSAA Infrastructure components (ficapp, ficweb, ficdb) cannot be installed on multi-tier. By default, they will be installed on single-tier. However, OFSAA Infrastructure can be deployed within the n-Tier architecture where the Database, Web server and Web application server is installed on separate tiers.

4. Is JDK (Java Development Kit) required during installation of OFSAA? Can it be uninstalled after OFSAA installation?

JDK is not required during installation of OFSAA and only a run time is needed for details. See [Hardware and Software Requirements](#), Java Runtime Environment section.

5. Is JRE required during installation of OFSAA? Can it be uninstalled after OFSAAI installation?

Only JRE (Java Runtime Environment) is required during installation of OFSAA and cannot be uninstalled as the JRE is used by the OFSAA system to work.

6. How do I know what is the Operating system, webserver and other software versions that OFSAA supports?

See [OFSAA Technology Stack Matrices](#).

7. What are the different files required to install OFSAAI?

The following files are required:

- setup.sh
- envCheck.sh
- preinstallcheck.sh
- VerInfo.txt
- OFSAAInfrastructure.bin
- validatedXMLinputs.jar
- MyResources_en_US.properties
- log4j.xml
- OFSAAI_PostInstallConfig.xml
- OFSAAI_InstallConfig.xml
- privileges_config_user.sql
- privileges_atomic_user.sql
- XML_Utility.jar

8. What should I do if I get the following error message during installation, "Execute Permission denied"?

Check whether all the files provided for OFSAAI installation has execute permissions.

To give execute permissions,

Navigate to the path OFSAAI_80000 and execute the command: `chmod 755 .`

"Graphical installers are not.."

If error resembles "Graphical installers are not supported by the VM. The console mode will be used instead..." then check whether any of the X-windows software has been installed.

Example: Hummingbird Exceed is started and configured to Graphical mode installation.

NOTE	Type 'xclock' from prompt and this should display clock in graphical mode.
-------------	--

"No Java virtual machine could be..."

If the error message reads "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program", then

- Check whether "java path" is set in PATH variable. See [Table 6](#) for Prerequisite Information.
- Check whether sufficient temporary space is available.
- Ensure that the movement of OFSAAI Installer text files to the target system is done in the Text mode so that setup.sh file does not contain control line feed characters (^M).

9. What should I do if I get the following error message during installation, "OracleDriver Files Not Found, Please Choose the Right Path To Continue"?

Check whether the provided path for Oracle Driver files is correct and whether the user has permissions to access the files.

10. **What should I do if I get the following error message during installation, "User must have CREATE TABLE, CREATE VIEW, CREATE TRIGGER, CREATE INDEX, CREATE SEQUENCE, CREATE PROCEDURE" even though the oracle schema user created has the mentioned privileges?**

OFSAAI installer validates the database details provided during installation, so ensure:

- Whether the oracle schema user has the required set of privileges for successful installation.
- Whether the oracle schema user has been created with quota privileges on tablespace to create database objects.
- See [Table 6](#) for Prerequisite Information.

11. **Installation of OFSAAI was completed successfully! What next?**

Post the successful completion of OFSAAI installation, you must perform the Post Installation steps. See [Post Installation Configuration](#).

12. **What is to be done when OFSAAI Installation is unsuccessful?**

OFSAAI installer generates log file OFSAAIInfrastructure_Install.log in the Infrastructure Installation Directory. There is also another log file created in the path configured in Log4j.xml. The logs of any of these reported, Warnings/Non Fatal Errors/Fatal Errors/Exceptions should be brought to the notice of the OFSAAI Customer Support. It is recommended not to proceed, until the reported problems are adequately addressed.

13. **How do I completely uninstall OFSAAI?**

OFSAAI can be completely uninstalled by performing the steps provided in [Uninstalling OFSAAI Infrastructure](#). Alternately you can see [OFSAAI Installation and Configuration Guide Release 8.1.2.0.0](#).

14. **Can OFSAAI config and atomic schemas be on different databases?**

OFSAAI requires both config and atomic schemas to be present on the same database instance.

15. **How to grant privileges if a new information domain is created?**

If you are creating a new information domain, provide a set of privileges (database permissions) to the new Atomic schema.

- Log into the database as sys and connect as sysdba user..
- Execute the file privileges_config_user.sql available under \$FIC_HOME directory
- Enter the database schema for which you want to grant privileges.

16. **When should I run the MLS utility?**

See the *Multiple Language Support (MLS) Utility* section in [OFS AAI Administration Guide](#).

17. **Does OFSAAI support Oracle Linux versions other than 5.5?**

OFSAAI supports the Oracle Linux versions from 5.5 up to 5.10 and also from 6.0 and above.

18. **What should I do if I get the following error message on the UNIX System terminal while executing ./setup.sh, "Insert New Media. Please insert Disk1 or type its location"?**

- a. Login as root user on the Unix machine where OFSAAI is getting installed.
- b. Navigate to the path /etc/security/.

- c. Edit the file `limits.conf` to add/edit a row for the unix user installing OFSAA: `<Unix User> soft nofile 9216`
- d. After saving the changes, log in as unix user with which OFSAAI is getting installed and execute the command: `ulimit -n`.

The command returns the value 9216.

19. How do I verify if the system environment is ready for OFSAAI installation?

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

See [Verifying System Environment](#) for additional information.

20. How do I know if the installation is completed successfully?

The OFSAA Infrastructure installation performs a post install health check automatically on successful installation of the product. To rerun the post install verification at a later time, follow these steps:

- Navigate to the path `$FIC_HOME` (Product Installation Directory).
- Execute the command: `./piverify.sh`.

21. What should I do if I get the following error message during OFSAAI installation on Solaris 11 system?

"Error: OFSAAI-1108

ORA-00604: error occurred at recursive SQL level 1

ORA-01882: timezone region not found"

Or

"Time zone cannot be set as null or 'localtime' "

This happens if the time zone is not set, that is NULL or it is set as 'localtime'. Set the environment variable TZ to a valid time zone region in the `.profile` file. For example, `TZ=Asia/Calcutta`, export TZ

22. What should I do if there are any exceptions or errors in installation and how to proceed?

Backup the installation logs and share the backup logs with [My Oracle Support](#).

23. What should I do if the installation process is abruptly terminated or aborted?

If the installation is abruptly terminated, then the installation process will be incomplete. To recover from this, follow the below steps:

- a. Drop the DB objects in the config schema created by OFSAAI installation.
- b. Open the `.profile` and remove the entries made by the OFSAAI installation which are made between the comment statements, `#Beginning of entries by OFSAA Infrastructure installation` and `#End of entries by OFSAA Infrastructure installation`.
- c. Delete the OFSAA install directory created by the OFSAAI installer.
- d. Perform the OFSAAI installation again.

24. Does OFSAA support any other web server types, other than the ones stated in tech matrix and installation guide?

No, all the supported softwares and versions are stated in the OFSAA Technology Stack Matrices.

25. What should I do if the database connection from connection pool displays the following error message, "java.sql.SQLRecoverableException: IO Error: Connection reset"?

This happens while running several database intensive tasks in parallel. To correct this error, add the line `securerandom.source=file:/dev/.urandom` in the `java.security` configuration file available in `$JAVA_HOME/jre/lib/security/` path.

NOTE This needs to be configured on all the machines or VMs where the OFSAAI components are installed.

If the issue is not resolved even with the above settings, check the MTU (Maximum Transmission Unit) settings on the linux box. For details on MTU settings and updating them, contact your system Administrator.

26. What should I do when I get syntax errors/file not found error messages while invoking setup.sh file from my install archive?

This could mostly happen:

When installer was not unzipped rightly or corrupted during unzip.

setup.sh file which resides within the install archive was not transferred in ASCII or text mode, which could have corrupted the file.

To correct this, follow the steps:

- a. Copy the installer (in BINARY mode) to the system on which the OFSAA Infrastructure components will be installed.
- b. Unzip the installer using the command: `unzip <OFSAAI_Installer>.zip`.

The corrupted setup.sh file would have introduced certain ^M characters into the file. You can remove ^M characters from the `setup.sh` file by following these steps:

- a. Login to the server where the installer is copied.
- b. Navigate to the directory `OFSAAI_80000`.
- c. Open the setup.sh file in the vi editor using the command: `vi setup.sh`.
- d. Inside vi editor in Esc mode, type: `%s/^M//g`.

NOTE To enter ^M, hold the CTRL key then press V and M in succession.

- e. Save the setup.sh file by typing: `wq!`

27. Does OFSAA support Oracle DB 11g Standard edition?

The OCI client and the jdbc driver does not change depending on whether it is a standard or enterprise edition. So, OFSAAI will work with standard edition as well.

We do not recommend standard edition because it will not scale and does not support partition pack, database security vault, or advanced analytics.

28. What should I do if I get the following error message while executing ./startofsaai.sh file on the UNIX System terminal "/startofsaai.sh: /java: Execute permission denied"?

- a. Ensure JAVA_BIN environment variable path is set on the *unix user* terminal from where the `./startofsaai.sh` file is invoked.
- b. Ensure the .profile where the environment/path settings are made has been executed successfully.

29. What should I do if the OFSAAI Login page does not open and I get the following error message, "Could not retrieve list of locales"?

This could be due to 2 reasons:

- System is unable to resolve the hostname configured.
- Conflict with the ports configured.

To correct them, follow the below steps:

- a. Steps to replace the hostnames with IP address:
 - iii. Stop all the OFSAA services. For more information, see [Appendix E: Starting/Stopping Infrastructure Services](#).
 - iv. Replace all the hostnames with the IP address in all the places mentioned in the document (Where to find port, IP address, HTTPS Configuration for OFSAAI 7.2 Installation (DOC ID 1500479.1)).
 - v. Restart all the OFSAAI services. For more information, see [Appendix E: Starting/Stopping Infrastructure Services](#).
- b. Steps to correct the port number conflicts
 - i. Stop all the OFSAA services.
 - ii. See the port numbers stated in the document (Where to find port, IP address, HTTPS Configuration for OFSAAI 7.2 Installation (DOC ID 1500479.1)) and check on the discrepancy in the port numbers and correct them.
 - iii. Restart all the OFSAAI services.

30. What happens when the OFSAAI Application Server does not proceed even after providing the system password?

Ensure that, the System Password provided when prompted must match with the *Oracle Configuration Password* provided during installation. Also check whether the connection to the *Configuration Schema* can be established through sqlplus.

31. Although the OFSAAI installation has completed successfully, when OFSAAI servers are started, and the application URL is accessed, it gives an error message "the page cannot be found or displayed" or "Could not retrieve list of languages from Server. Please contact the system administrator". What should one do?

Ensure OFSAAI servers have been started and are running successfully. On the server start up parameters options, see [Starting Infrastructure Services](#).

For more details on the issue, see the Revappserver log in \$FIC_APP_HOME/common/FICServer/logs directory or the Web server log files.

32. Is it necessary to provide the specified grants to the Oracle schema user before installation? If yes, can it be revoked after completing the installation?

The *Oracle Schema* user requires the necessary grants specified before, during, and after the installation process. Grants provided must not be revoked as the application makes use of these grants all the time.

33. Can we have distributed OFSAAI Application Server for load balancing?

OFSAAI Application server can be scaled out/distributed across different JVM's (machines) based on the various services and Information Domains, in other words, Load balancing can be achieved with distribution of services.

34. Why do we need Ftpshare on all the layers? Can we have ftpshare on another machine other than the machines where OFSAAI is installed?

Ftpshare is a Metadata Repository directory. All the metadata related files used in Infrastructure are stored in the ftpshare directory. The ftpshare contains folders for each Information Domain, with each Information Domain folders holding Erwin, log, and scripts folder. The transfer of data among the Web, Application, and Database servers in Infrastructure takes place through FTP/SFTP.

You need to configure FTP/SFTP and enable communication between the servers by providing App server's FTP/SFTP credentials to the Web server and DB server users.

Yes, we can have ftpshare on another machine other than the machines where OFSAAI is installed.

35. Is it mandatory to provide the ftp/sftp password?

Yes, OFSAAI needs credentials of the user which has complete permissions on ftpshare directory, and should be able to independently login to the unix server.

36. What are the permissions required for ftpshare and when should I give them?

It is recommended to provide permissions on ftpshare in case of installations done across different machines or VMs (multitier installation).

In case of single tier installation, 770 permissions can be provided if the unix users of OFSAAI and web server belong to the same unix group.

And on any new file that is created in the 'ftpshare' folder of any installation layer must be granted specific/explicit permission.

Port Change utility could be used to have the Port number modified, which are currently being used by the Infrastructure application. For more information, see [Changing IP/Hostname, Ports, Deployed Paths of the OFSAA Instance](#).

37. Are there any in-built system administration users within OFSAAI Application?

The three in-built system administration users are provided to configure and setup OFSAAI.

- SYSADMN
- SYSAUTH
- GUEST

38. Does OFSAAI Application support both FTP and SFTP?

OFSAAI supports both FTP and SFTP configuration.

39. Is it necessary to enable the FTP/SFTP services to use the OFSAAI?

Yes, enabling of FTP/SFTP services and its ports is a pre-requisite step towards using the OFSAAI.

40. OFSAAI Configuration: Unable to save the server details?

- Ensure the input User ID, Password, and Share Name are correct.
- Ensure FTP/SFTP services are enabled.
- Have a test FTP/SFTP connection made and confirm if they are successful.

41. What should I do if I get the following message while creating Information Domain, "Please create a database and then create the information domain"?

Information Domain is mapped to only one Database; and thus before the creation of Information Domain, at least one database details would need to exist.

42. What should I do if I get the following message during startup of backend engine message server, "ConnectToDatabase: FatalError, could not connect to the DB server"?

- Verify whether connection to the "configuration schema" can be established through sqlplus.
- Verify "configuration schema" password is modified post installation.
- Ensure oracle database alias name created for oracle instance and oracle service name are same.
- On a multi tier Installation mode, ensure TNSNAME and SID are the same in both the Application and Database Layers.

43. What should I do if I get the following message during the startup of backend engine message server, "Fatal Error, failed to get user ID from LibSmsConnect"?

Ensure Reveleus.sec file exist under the \$FIC_HOME/conf directory where the Database components are installed.

44. Does OFSAAI Application support LDAP authentication?

OFSAAI supports LDAP configuration and authentication.

45. Does OFSAAI support multiple languages?

Yes, OFSAAI supports multiple languages.

46. Does OFSAAI provide any data back-up features?

OFSAAI does not have built-in back up facility. External Storage Infrastructure is recommended for back-up.

47. What kind of security features does the OFSAAI provide?

OFSAAI provides security at:

- Segment Level - Users can access only the segment they are mapped to.
- Application Level - Users can perform an operation only if mapped to appropriate role and functions.

48. Does OFSAAI have the ability to enforce periodic password change?

OFSAAI provides configurable parameters to define number of days after which the user password would expire and then the user is forced to change the password after expiration period.

49. What is the password policy followed in OFSAAI?

OFSAAI enforces a minimum password length with a combination of Upper and Lower case characters and alpha-numeric strings.

50. Which version of Erwin Data Modeler does OFSAAI support?

OFSAAI framework supports Data Modeler Erwin versions 9.0, 9.2, 9.6, and 9.7 for backward compatibility. However, the data models shipped with version 8.1.2.0.0 of the application packs are compatible with Erwin 9.5, 9.64, and 9.7.

51. Does OFSAAI provide the mechanism to upload Business Data model?

OFSAAI provides two mechanisms for business data model upload:

- Easy to use GUI based Model upload mechanism to upload the Business Data Model through Unified Metadata Manager --> Import Model.
- OFSAAI also provides a model upload utility "upload.sh" for uploading the business data model through the command line parameter by executing this shell script file under the path <FIC_HOME>/ficapp/common/FICServer/bin.

See *Run Model Upload Utility* in [OFS Analytical Applications Infrastructure User Guide](#) for details.

52. How do I apply incremental change to the existing model when the Business Data model undergoes a change?

Modified data model can be upload into the system and OFSAAI has the ability to compare the changes within the data model with respect to the one already present in the system and enables propagation of incremental changes in a consistent manner.

53. What are the different types of uploading a business data Model?

OFSAAI supports uploading of business data model from client desktop and also by picking up the data model from the server location.

54. Can the OFSAAI "Configuration Schema" password be modified post installation?

The OFSAAI *Configuration Schema* password can be modified post installation. OFSAAI application stores the password in the database and few configuration files, thus any changes to the *Configuration Schema* password would necessitate updating in these.

Contact OFSAAI support for more details.

55. Can the OFSAAI "Atomic Schema" password be modified?

The OFSAAI *Atomic Schema* password can be modified. OFSAAI application stores the atomic schema password in the database and few configuration files, thus any change to the atomic schema password would necessitate updating the password.

To change the Atomic Schema password, follow the steps:

- a. Login to OFSAA.
- b. Navigate to System Configuration > Database Details window. Select the appropriate connection, provide the modified password and save.
- c. Navigate to Unified Metadata Manager > Technical Metadata> Data Integrator > Define Sources window. Update the appropriate Source details.

If you are using Apache Tomcat as Web server:

- i. Update the <Context> -> Resource tag details in server.xml file from the
- ii. \$CATALINA_HOME/conf folder. (In case of Tomcat only Atomic <Resource> will exist).
- iii. If you are using WebSphere as Web server:
- iv. Login to the WebSphere Administration Console from the left side menu.
- v. Navigate to Resources > JDBC >Data Sources. A list of data sources will be populated on the right side.
- vi. Select the appropriate Data Source and edit the connection details. (In this case, both Config and Atomic data sources need to be modified).

If you are using WebLogic as Web server:

- i. Login to the WebLogic Administration Console from the left side menu.

- ii. 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.
- iii. Select the appropriate Data Source and edit the connection details. (In this case, both Config and Atomic data sources need to be modified).
- iv. Restart the OFSAAI services.

NOTE

If the modified passwords are not updated, OFSAAI logs displays the message ORA-28000: the account is locked.

56. Does the upload of Business Data model depend on Java Memory?

Business data model upload through OFSAAI depends on the Java memory settings on the client and server machines. Java memory setting varies with the data model size and the available RAM. Contact OFSAAI support for more details.

57. Why do the Business Metadata Management screens (Business Processors screen) in the User Interface, take more time to load than other screens?

The Log file in DynamicServices.xml which resides in \$FIC_HOME/conf is continuously being updated/refreshed to cache metadata. This can be observed when you are starting startofsaai.sh and if any of the log file (Ex: SMSService.log) in DynamicServices.xml is being continuously refreshed for longer time.

By default, the Metadata Log file cache size is set to 1000. If in case the log is being updated beyond this limit, retrospectively the preceding entries are overwritten. For example, the 1001th entry is overwritten by deleting the first entry. This results in the application screen taking a longer time to load.

Increase the cache size limit in DynamicServices.xml located at <FIC_HOME>/conf, depending on the currently logged count for the specific metadata.

- a. Generate the Log report by executing the below query in config schema.

```
select count(1), t.metadata_name, m.dsn_id from metadata_master m,
metadata_type_master t where m.metadata_type = t.metadata_type
group by t.metadata_name, m.dsn_id
```

- b. The above query returns a list of codes with their respective metadata count. You can see the *metadata_type_master* table to identify the metadata name.
- c. View the log report to identify the metadata which is being updated/refreshed beyond the specified cache size limit. Accordingly increase the cache size limit in DynamicServices.xml depending on the currently logged count for the specific metadata.

For example, if the "MEASURE_CACHE_SIZE" is set to 1000 and total measure reported in log is 1022, increase the limit to 2000 (approximately).

- d. Restart Reveleus/OFSAAI servers (Web and APP) and check the issue.

58. What should I do if I get OutOfMemoryError while deploying EAR file in WebSphere application server?

The Java memory needs to be increased in ejbdeploy.sh file which is present under

<WebSphere Install directory>/AppServer/deploytool/itp. For example,

```
$JAVA_CMD \
```

```
-Xbootclasspath/a:$ejbd_bootpath \ Xms256m -Xmx1024m \
```

59. What configurations should I ensure if my data model size is greater than 2GB?

In order to upload data model of size greater than 2GB in OFSAAI Unified Metadata Manager-Import Model, you need to configure the required model size in struts.xml file available in the path \$FIC_WEB_HOME/webroot/WEB-INF/classes.

NOTENOTE The size requirements have to be always specified in bytes.

For example, if you need to configure for model size of 2.5GB, then you can approximately set the max size to 3GB (3221225472 bytes) as indicated below, in order to avoid size constraints during model upload.

```
<constant name="struts.multipart.maxSize" value="3221225472"/>
```

After configuring struts.xml file, 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 [Appendix D: Creating and Deploying EAR/WAR File](#).

60. What should I do if my Hierarchy filter is not reflecting correctly after I make changes to the underlying Hierarchy?

In some cases, the Hierarchy Filters do not save the edits correctly if the underlying Hierarchy has been changed. This can occur in hierarchy maintenance, where you have moved a member to another hierarchy branch, and that member was explicitly selected in the Filter and is now a child of a node which is already selected in the Filter.

See [Support Note](#) for the workaround.

61. Can I install an Applications Pack on an existing Atomic schema/ Information Domain created manually?

No, you cannot install an Applications Pack on existing Atomic schema/Information Domain created manually. Applications Packs can be installed only on Atomic Schemas/Information Domain created using schema creator utility and/ or the Applications Pack installer.

62. What should I do if I get the following exception while trying to view the model outputs in Model Outputs screen, "Exception ->Local Path/STAGE/Output file name (No such file or directory)"?

Ensure you have created a folder "STAGE" under the path mentioned as "Local Path" in the web server details screen. This folder needs to be created under the local path on every node, in case of web application server clustering.

63. What should I do if I get the following exception during OFSAA services startup, "Exception in thread "main" java.lang.UnsatisfiedLinkError: net (Not a directory)"?

Ensure the JRE referred in .profile is not a symbolic link. Correct the path reference to point to a physical JRE installed.

64. What is the optimized memory settings required for "New" model upload?

[Table 32](#) lists the optimized memory settings required for "New" model upload.

Table 32: Optimized Memory Settings for New Model Upload

Model Upload Options	Size of Data Model XML File	X_ARGS_APP ENV Variable in OFSAAI APP Layer
Pick from Server	106 MB	"-Xms1024m -Xmx1024m
	36 MB	"-Xms2048m -Xmx2048m
	815 MB	"-Xms4096m -Xmx4096m
	1243 MB	"-Xms6144m -Xmx6144m
Model Upload Utility	106 MB	"-Xms1024m -Xmx1024m"-Xms2048m -Xmx2048m
	336 MB	"-Xms4096m -Xmx4096m
	815 MB	"-Xms4096m -Xmx4096m
	1243 MB	"-Xms6144m -Xmx6144m
Save New Erwin File In Server	106 MB	"-Xms1024m -Xmx1024m
	336 MB	"-Xms2048m -Xmx2048m
		"-Xms4096m -Xmx4096m
		"-Xms6144m -Xmx6144m

65. I did not enable OFS Inline Processing Engine Application license during the installation. However, I have enabled it post installation, using the Manage OFSAA Product License(s) in the Admin UI. Are there any other additional configurations that I need to do?

Yes. Follow the instructions explained in the [OFS Inline Processing Engine Configuration Guide](#).

66. I get an error when I try to build an Oracle OLAP cube. What should I do?

Execute the below grant on the appropriate ATOMIC schema:

```
grant olap_user to &database_username.
```

67. How do you turn off unused Information Domains (Infodoms) from caching?

Follow these steps to turn off unused infodoms from caching:

- Navigate to \$FIC_HOME/conf in the APP layer of your OFSAAI installation.
- In the DynamicServices.xml file, identify the section for <Service code="20">.
- Modify the value of parameter CACHE_ON_STARTUP to 0 (default is 1).
- Repeat the same in the WEB layer too. 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 [Appendix D: Creating and Deploying EAR/WAR File](#).
- Restart the OFSAAI Services (APP and WEB). For more information, see [Appendix E: Starting/Stopping Infrastructure Services](#).

NOTE

This setting helps cache the Infodom metadata only for the infodoms that get accessed after user login. Infodoms which are not accessed, are not cached.

Sample code is as follows:

```
<SERVICE CODE="20"
CLASS="com.iflex.fic.metadata.services.MetadataServiceProvider"
NAME="BMD" SERVERID="DEFAULT" PATH=" " LOGGERNAME="UMMLOGGER"
LOGGERLEVEL="10">
<PARAMETERS>
<PARAMETER NAME="CACHE_ON_STARTUP" VALUE="0" />
<PARAMETER NAME="BACKUP_XML" VALUE="1" />
<PARAMETER NAME="MAX_BACKUP_XML" VALUE="2" />
<PARAMETER NAME="PC_NONBI_BI_SWITCH" VALUE="2048" />
<PARAMETER NAME="HIERARCHY_NODE_LIMIT" VALUE="2000" />
<PARAMETER NAME="ALIAS_CACHE_SIZE" VALUE="1000" />
<PARAMETER NAME="DATASET_CACHE_SIZE" VALUE="2000" />
<PARAMETER NAME="MEASURE_CACHE_SIZE" VALUE="2000" />
<PARAMETER NAME="HIERARCHY_CACHE_SIZE" VALUE="2000" />
<PARAMETER NAME="DIMENSION_CACHE_SIZE" VALUE="2000" />
<PARAMETER NAME="HIERARCHYATTRIBUTE_CACHE_SIZE" VALUE="1000" />
```

```
<PARAMETER NAME="CUBE_CACHE_SIZE" VALUE="1000" />
<PARAMETER NAME="RDM_CACHE_SIZE" VALUE="1000" />
<PARAMETER NAME="BUSINESSPROCESSOR_CACHE_SIZE" VALUE="2000" />
<PARAMETER NAME="DERIVEDENTITY_CACHE_SIZE" VALUE="1000" />
<PARAMETER NAME="LOG_GET_METADATA" VALUE="false" />
<PARAMETER NAME="METADATA_PARALLEL_CACHING" VALUE="0" />
</PARAMETERS>
</SERVICE>
```

- 68. While creating an Excel Mapping, after specifying the excel worksheet, the target table, and mapping each column in the worksheet to a target table, I click SAVE and nothing happens. But when I click CANCEL, a message pops up informing me that all changes will be discarded", what is to be done?**

Check if the excel mapping creation is done using I.E 8 with JRE 1.4 plug in enabled on machine. If so, upgrade the JRE plug in to 1.7+.

- 69. Can Multiple OFSAA Infrastructure instances share the same config schema?**

No, only one OFSAA environment can be installed using one config schema.

- 70. Can Atomic schema be shared?**

Yes, it can be shared between two OFSAA instances.

- 71. While setting a firewall, which ports should be opened for communication between the Web server (Apache HTTP Server/ Oracle HTTP Server/ IBM HTTP Server) and the Web application server (WebSphere/ WebLogic/ Tomcat) for OFSAAI to operate properly?**

The OFSAA Servlet port which is same as Web server port should be open. Also the web application port should be open.

- 72. Can I modify the NLS_LENGTH_SEMANTICS to BYTE from CHAR for the Database where older versions of OFSAA is Installed?**

Yes, NLS_LENGTH_SEMANTICS can be modified to BYTE from CHAR if you are not intending to use multi language support.

- 73. Can I install already installed application in a different infodomain?**

No, it is not possible to install the same application in two different infodomains.

- 74. How can I configure the OFSAA application for High Availability?**

OFSAA can have active-passive high availability. For more information, see [Configuring OFSAA in Clustered Environment Guide](#).

- 75. During OFSAA installation should I provide web application server's IP /Hostname and port or web server's IP/Hostname and port, if the Apache HTTP Server/ Oracle HTTP Server/ IBM HTTP Server are configured?**

In case the web server is configured, you should enter the Web server IP Address/Hostname and Port details during OFSAA installation. Here the Servlet port should be same as the Web server port.

If Web server is not configured, the Web application server's IP Address/ Hostname and Port is required during the installation process. Here the Servlet port should be same as the Web application Server port.

76. Is "ReveleusAdminConsoleAgent" applicable for OFSAAI 8.0.0.0.0 and higher versions?

No, ReveleusAdminConsoleAgent is not applicable starting OFSAAI 7.3.3.0.0. There is a change in the way agentservers are managed through AGENTSTARTUP.SH & AGENTSHUTDOWN.SH.

77. What should I do when the message server process does not open and I get the following error message, "CI18NProvider::CI18NProvider, Error, unable to connect to the config database"?

This error is displayed due to the following reasons:

- The Config Schema password is already expired.
- If the config schema password is going to expire soon and the message such as "ORA-28002: the password will expire within 6 days" displays while connecting to config schema through sqlplus.
- The Config schema password is Modified.

To resolve the error, re-set the config schema password to the old password. Else, if the config schema password is modified to something else then follow the below steps:

- a. Delete the \$FIC_HOME/conf/Reveleus.SEC file.
- b. Shutdown the OFSAAI App service: cd \$FIC_APP_HOME/common/FICServer/bin ./stopofsaai.sh
- c. Shutdown the OFSAAI App service: cd \$FIC_APP_HOME/common/FICServer/bin ./stopofsaai.sh
- d. Start the Infrastructure Server in foreground directly on the server or through XWindows software using the command: ./startofsaai.sh.
- e. Enter System Password.
- f. Enter the new Config schema password. The service starts and initializes if it is able to successfully connect to the DB and generates the Reveleus.SEC file.
- g. Post successful startup of the service, if required, the Infrastructure server may be shut down and restarted in the background using nohup mode.

78. What is the mechanism of Log File sizing and backup?

OFSAAI Log files created under \$FIC_APP_HOME/common/FICServer/logs &

<OFSAAI_DEPLOYED_AREA>/<CONTEXT.war>/logs is configurable in RevLog4jConfig.xml.

The default size of the log files (MaxFileSize) is set to max 5000kb & number of max backup log files (MaxBackupIndex) retained is set to 5, both of which are configurable. Increasing these parameters to a higher value should depend on the server HW configurations and may reduce the performance.

To configure the Logs file size on OFSAA Application server, follow these steps:

- a. Navigate to \$FIC_HOME/conf where OFSAA is installed.
- b. Edit the following parameters in the file RevLog4jConfig.xml
 - <param name="file" : Enter the path where the Logs are to be generated.
 - <param name="MaxFileSize" : Provide the required file size.
 - <param name="MaxBackupIndex" : Provide the required number of backup files to be created.

Example:


```
<appender name="REVSERAPPENDER" class="org.apache.log4j.RollingFileAppender">
<param name="file" value="$FIC_HOME/ficapp/common/FICServer/logs/RevAppserver.log"/
>

<param name="Append" value="true" />
<param name="MaxFileSize" value="5000kb" />
<param name="MaxBackupIndex" value="5" />
<layout class="org.apache.log4j.PatternLayout">
<param name="ConversionPattern" value="[REVELEUSLOG] %m%n"/>
</layout>
</appender>
```

To configure the Deployed area logs file, follow these steps:

- a. Navigate to <EAR/WAR Deploy area>/conf folder.
- b. Repeat step 2 from the above section.

79. Can we modify the Log file path?

Yes, Log file path is configurable, it can be configured in RevLog4jConfig.xml.default log file path (file) is set by the installer. This can be configured to another path.

80. Can I point the environment with HTTP enabled to HTTPS after installation and vice versa?

For more details, see the *HTTPS* section in the [OFSAAI Administration Guide](#).

81. What should I do if the sliced data model upload takes a long time to complete?

If the metadata cache size is set to a lower value than the actual count of each metadata type (hierarchy, dataset, dimension etc), then it gets into performance degrade issues. We have to increase the cache size for each metadata type according to the count in the environment.

Following are the parameters in DynamicServices.xml to be configured depends on the metadata count in your environment.

```
<PARAMETER NAME="HIERARCHY_NODE_LIMIT" VALUE="2000"/>
<PARAMETER NAME="ALIAS_CACHE_SIZE" VALUE="1000"/>
<PARAMETER NAME="DATASET_CACHE_SIZE" VALUE="2000"/>
<PARAMETER NAME="MEASURE_CACHE_SIZE" VALUE="3000"/>
<PARAMETER NAME="HIERARCHY_CACHE_SIZE" VALUE="2000"/>
<PARAMETER NAME="DIMENSION_CACHE_SIZE" VALUE="2000"/>
<PARAMETER NAME="CUBE_CACHE_SIZE" VALUE="1000"/>
<PARAMETER NAME="BUSINESSPROCESSOR_CACHE_SIZE" VALUE="2000"/>
<PARAMETER NAME="DERIVEDENTITY_CACHE_SIZE" VALUE="1000"/>
```

Metadata count can be derived based on the following queries:

```
select count(1) from metadata_master where metadata_version=0 --- for all metadata select
count(1) from metadata_master where metadata_version=0 and metadata_type=1 --- for
measure
```

```
select count(1) from metadata_master where metadata_version=0 and metadata_
```

- type=2 --- for Dimension
select count(1) from metadata_master where metadata_version=0 and metadata_type=3 --- for HCY
select count(1) from metadata_master where metadata_version=0 and metadata_type=4 --- for DATASET
select count(1) from metadata_master where metadata_version=0 and metadata_type=59 --- for BP's
select count(1) from metadata_master where metadata_version=0 and metadata_type=54 --- for Alias
select count(1) from metadata_master where metadata_version=0 and metadata_type=5 --- for CUBES
select count(1) from metadata_master where metadata_version=0 and metadata_type=856 --- for Derived Entity
82. **For LDAP authentication, which server connects with the LDAP server, the Application server (where OFSAAI is installed), or Web Application server (where EAR is deployed)?**
For LDAP authentication, the Application server (ficapp) connects with the LDAP server.
83. **The LDAP server in the setup listens on secure protocol ldaps (port 636). I have the root certificate of the LDAP server for SSL, and would like to know where to offload this certificate?**
You need to import the certificate into the JDK/JVM used by Reveleus server in ficapp layer.
84. **How to relocate FTPSHARE folder?**
You can run the PortC.jar utility. For more information, see the *Changing IP/Hostname, Ports, Deployed Paths of the OFSAA Instance* section in [OFSAAI Administration Guide](#).
85. **How do we identify the list of ports that are used by/configured in an OFSAA environment?**
Navigate to \$FIC_HOME directory on target.
86. **What should I do if I get the following error message, "Error while fetching open cursor value Status : FAIL"?**
This error occurs while executing envCheck.sh because the user does not have access to V\$parameter. This error does not occur due to sysdba or non sysdba privileges provided they have access/grants to V\$parameter.

28.1.2 Applications Pack 8.1.2.0.0 FAQs

- What is an Applications Pack?**
An Applications Pack is suite of products. For more information, see [About OFSAA Infrastructure](#).
- Can I get a standalone installer for OFSAAI 8.1?**
No. AAI is part of every Applications Pack and installs automatically.
- How does OFSAA 8.1 Applications Pack relate to OFSAA 7.x series?**
8.1 is a new major release consolidating all products from OFSAA product suite.
- Can existing OFSAA 7.x customers upgrade to OFSAA 8.1 Applications Pack?**

- There is no upgrade path available. However, we will have migration kit/path for every product to 8.1 Applications Pack. Further details will be available with Oracle Support Services.
5. **Does OFSAA 8.1 Applications Pack UPGRADE automatically to existing environments?**
No. OFSAA 8.1 Applications Pack has to be installed in an new environment and subsequently migration path / migration kit needs to be run to migrate from 7.x to 8.1. Note that the objects can be migrated only from the previously released version of OFSAA products.
 6. **Where can I download OFSAA 8.1 Applications Pack?**
You can download the OFSAAI 8.1 Applications Pack from [Oracle Software Delivery Cloud \(OSDC\)](#).
 7. **What are the minimum system and software requirements for OFSAA 8.1 Applications Pack?**
See [Hardware and Software Requirements](#).
 8. **Is my environment compatible with OFSAA 8.1 Applications Pack?**
Environment Check utility performs the task. It is part of install and can also be run separately.
 9. **Does the OFSAA 8.1.2.0.0 Applications Pack support all Operating systems?**
OFSAA 8.1.2.0.0 Applications Pack supports the following Operating Systems: LINUX, AIX, SOLARIS. See [Technology Matrix](#) that OFSAA suite products are/will be qualified on.
 10. **How can I install OFSAA 8.1.2.0.0 Applications Pack?**
See [Oracle Financial Services Advanced Analytical Infrastructure Installation And Configuration Guide](#) for the Applications Pack installers.
 11. **Does this installation require any Third party Softwares?**
The See [Oracle Financial Services Advanced Analytical Infrastructure Installation And Configuration Guide](#) lists the third party software that needs to be installed.
 12. **What languages are supported during OFSAA 8.1.2.0.0 Applications Pack installation?**
US English is the supported language supported.
 13. **What mode of installations OFSAA Applications Pack supports?**
OFSAA Applications Packs supports Silent Mode.
 14. **Does OFSAA 8.1.2.0.0 Applications Pack support Multi-tier Installations?**
OFSAA 8.1.2.0.0 supports only single tier installation. For more information, see [OFSAAI FAQs](#).
 15. **Does this Applications Pack validate all Pre-requisites required for this installation i.e., Memory, Disk Space etc.?**
Yes. The pre-requisite checks are done by the respective Applications Pack installer.
 16. **What happens if it aborts during installation of any application with in Applications Pack?**
You must restore the system and retrigger the installation
 17. **Does this Applications Pack 'Roll Back' if any application installation fails due to errors?**
Rollback of installation is not supported.
 18. **Does the Applications Pack install all applications bundled?**
All Applications Pack system files are installed but there is an option to enable the licensed products.
 19. **Can I re-install any of the Applications Packs?**

You can retrigger in case of failure.

20. Does this Applications Pack allow enabling/disabling any of the applications installed?

Yes. You cannot disable once the product is enabled in an environment.

21. I have installed one application in an Applications Pack, can I install any of new application within the Applications Pack later?

No, installation of additional applications is not required. If you wish to add an application later, you can enable the application at that time.

22. How many OFSAA Infrastructures can be installed in a single server?

There is no issue in installing separate OFSAAI installations, each with their own PFT/FTP installations and separate associated database instances and separate Web server installations on the same server as long as adequate memory is allocated for each instance and as long as each OFSAAI installation is installed using a separate UNIX user and profile. Care should be taken if running multiple OFSAAI installations on a single server. Adequate memory will be required for each installation as several OFSAAI processes (model upload, DEFQ services, etc) take significant amounts of memory. So it depends on your server memory.

23. Is it possible to Install OFSAA 8.1 Applications Pack on an existing 'Infodom' where another OFSAA 8.1 application is installed?

Yes. However, the Behavioral Detection Applications Pack and Compliance Regulatory Reporting Applications Pack are the exceptions. They need to be installed in a different INFODOM.

24. Can I select an Infodom in Applications Pack during installation?

Yes. You can select or change the required infodom.

25. Can I install all Applications Packs in a 'Single Infodom'?

Yes. But Behavioral Detection Applications Pack and Compliance Regulatory Reporting Applications Pack are the exceptions. They need to be installed in a different INFODOM.

26. Is it possible to install applications on different Infodom within the Applications Pack? (For example, I want to install LRM & MR in two infodoms)

Applications within Applications Pack have to be installed in the same information domain in the same environment.

27. How many Infodoms can be created over a single OFSAA Infrastructure of 8.1.2.0.0?

You can install only one infodom during installation. But after installation, you can create multiple infodoms.

28. Is the 'Data Model' bundled specific to an Applications Pack or to an individual application?

A merged data model for all applications within the Applications Pack is bundled and upload.

29. Is it possible to install OFS Enterprise Modeling later?

OFS Enterprise Modeling is a separate product and can be enabled as an option later from any Applications Pack that bundles Enterprise Modeling.

30. Does the Applications Pack create sandbox automatically for the required applications?

Yes, Sandbox creation is part of application install process.

31. Are upgrade Kits available for individual applications or the complete Applications Pack?

Maintenance Level (ML) Release / Minor Release upgrades are available across all applications.

32. Can I upgrade AAI only?

Yes, you can upgrade AAI alone.

33. Can I upgrade one application within the Applications Pack? (For example, I want to upgrade LRM in the Treasury Applications Pack, but not MR.)

No, an upgrade is applied to all applications in the Applications Pack.

34. Is it possible to uninstall any Application from the Applications Pack?

No, it is not possible to uninstall any Application from the Applications Pack.

35. Can I uninstall entire Applications Pack?

No, you cannot uninstall the Applications Pack.

36. Is it possible to uninstall only application and retain AAI in the installed environment? No, you cannot uninstall only the application and retain AAI in the installed environment. Does Applications Pack contain all Language Packs supported?

Language Packs need to be installed on 8.1 Applications Packs.

37. Can I install an Applications Pack over another Applications Pack (that is same infodomain or different infodomain)?

Yes, you can install an Applications Pack over another Applications Pack in the same information domain or different information domain. But Behavioral Detection Applications Pack and Compliance Regulatory Reporting Applications Pack, Asset Liability Management Applications Pack and Profitability Applications Pack are the exceptions. They need to be installed in a different INFODOM.

38. Can I use an existing manually created schema as information domain for Applications Pack installation?

No. Schemas required by OFSAA applications have to be created using Schema Creator Utility.

39. Does OFSAA 8.1 support on WebLogic 10.3.6 with Oracle 12c?

Yes, OFSAA 8.1 will support on WebLogic 10.3.6 with Oracle 12c. WebLogic 10.3.6 supports Oracle 12c with some additional configurations. See [Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server](#) for additional configurations.

40. What should I do if I get the following error message while running the schema creator utility, "HostName in input xml is not matching with the local hostname"?

One possible reason could be the machine is configured for zonal partitioning. Ensure all the known IP Addresses of the machine are present in the /etc/hosts file.

41. What are the Java versions supported in OFS AAI Applications Pack version 8.1.2.0.0?

OFS AAI Applications Pack supports Java 1.7.x and 1.8.x.

42. Is OFS AAI Applications Pack version 8.1.2.0.0 supported on Java 8?

Yes. To install this release of the OFS AAI Applications Pack version 8.1.2.0.0 on Java 8. For more information, see specific notes mentioned in the sections:

- [Installer and Installation Prerequisites](#)
- [Configurations Supported for Java 8 & 11](#)
- [Configuring and Executing Schema Creator Utility](#)
- [Installing in Silent Mode](#)

43. What should I do when I get "[ERROR] - Error : APP Setup bin file failed." message during OFS_Application_PACK installation?

This is a generic error message that appears during application installation failure. You should check the installation log files for more information about what failed the installation.

However, if the message is displayed and the log files are not generated, it could be that it is a temp directory issue. The resolution is that your UNIX administrator has to disable the NOEXEC option. The installers extract the installation files into the /tmp directory, and if NOEXEC is enabled, execution of binaries will not happen in the directory and the installation fails. Re-run the installer after the configuration is changed. For more information, see the support note [Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server](#).

44. What should I do if I get the following error message during Scenario Manager installation?

Execute Permission denied

Invocation of this Java application has cause an Invocation Target Exception. this application will now exit (LAX)

ZeroGu6: Windows DLL failed to load

at ZeroGa4.b(DashoA10*..)

at ZeroGa4.b(DashoA10*..)

at com.zerog.ia.installer.LifeCycleManager.b(DashoA10*..)

at com.zerog.ia.installer.LifeCycleManager.a(DashoA10*..)

at com.zerog.ia.installer.Main.main(DashoA10*..)

at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)

at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)

at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)

at java.lang.reflect.Method.invoke(Method.java:606)

at com.zerog.lax.LAX.launch(DashoA10*..)

at com.zerog.lax.LAX.main(DashoA10*..)

Add the below variable in Environment Variables to address this issue.

- Name: JAVA_TOOL_OPTIONS
- Value: "-Dos.name=Windows 7"

28.1.3 Forms Framework FAQs

1. What should I do when I have large volume of data to be exported?

It is recommended to use BIP reports or OAS 5.9 reports if you have to export large volume of data.

2. How do I export the columns added to the grid using Field Chooser option?

Perform Grid Export operation to export the columns added to the grid by Field Chooser option.

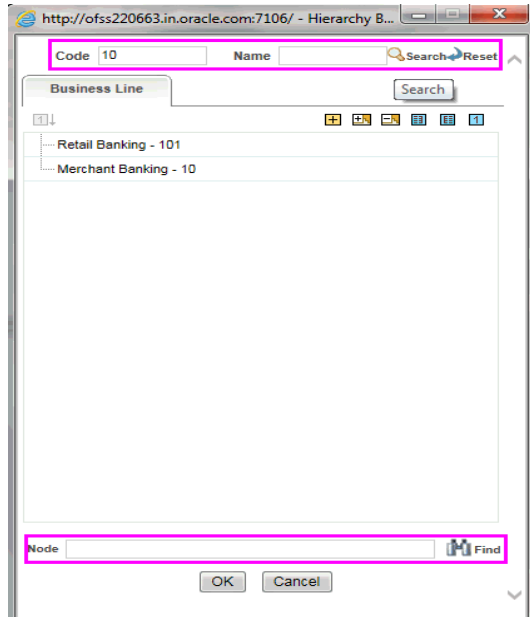
3. 'Expand All/ Collapse All' button is not visible in the Hierarchy Browser window. What should I do?

Expand All/ Collapse All button is enabled only if the number of hierarchy nodes is less than 50. If it is more than that, it is considered as large hierarchy and the data will be fetched dynamically when you expand each node.

4. What is the difference between the two Searches available in the Hierarchy Browser window?

In the new Hierarchy Browser window introduced from 7.3.5.1.0 version, there are 2 search options available as highlighted in:

Figure 129: Search Options



DB Search (Top search container): It will search the required node in database and displays the result as shown below. This search is performed on full hierarchy nodes.

UI search (Below the hierarchy): This search will find the required node in the UI and will show in tree structure.

NOTE

In case hierarchy nodes are more than 50 and if it is a non-custom hierarchy, then the UI search will not show the required node in tree structure, until all the nodes are expanded and loaded manually in the UI.

5. What is a Custom Hierarchy?

Custom hierarchies will be having the parameter configuration customQuery as shown below and the customized query will be taken from the HIERARCHY_FILTER_MASTER table.

Configuration in xml:

```
<CONTROL ID="1003" TYPE="41">
<CONTROLPROPS>
<EXTRAPARAMETERS>
<PARAMETER NAME="customQuery" VALUE="Yes"/>
</EXTRAPARAMETERS>
</CONTROLPROPS>
</CONTROL>
```

For custom hierarchy, all the hierarchy nodes are loaded in UI without any limit.

So, even if the hierarchy nodes are more than 50, the UI search will show the required node in tree structure and ExpandAll and ExpandBranch images will be enabled.

28.2 Error Dictionary

This contents of this section has been created with the interest to help you resolve the installation issues if any. There is a compilation of all the possible errors that might arise during the installation process with the possible cause and the resolution to quickly fix the issue and proceed further with the installation.

Topics:

- [Accessing Error Dictionary](#)
- [Error Code Dictionary](#)

28.2.1 Accessing Error Dictionary

Instead of scrolling through the document to find the error code, you can use the pdf search functionality. In the *Find* dialog available in any of the Adobe Acrobat version that you are using to view the pdf document, follow the below instructions to quickly find the error resolution.

1. With the Installation pdf open, press Ctrl+F or select Edit > Find.
2. The Find dialog is displayed as indicated.
3. Enter the error code that is displayed on screen during Infrastructure installation.
4. Press Enter. The search results are displayed and highlighted as indicated below.

Figure 130: Error Code (Cause & Resolution)

Error code - OFSAAI-1003	
Cause	JAVA_HOME/bin not found in PATH variable.
Resolution	Import <JAVA_HOME>/bin into PATH variable. Example: PATH = \$JAVA_HOME/bin:\$PATH export PATH.

View the details of the issues, its cause, and resolution specific to the error code. Repeat the step to find an answer to any other errors that you notice during installation. If you are not able to resolve the issue even after following the steps provided in resolution, you can contact support.oracle.com along with log files and appropriate screen shots.

28.2.2 Error Code Dictionary

28.2.2.1 Error Code - OFSAAI-1001

Cause: Unix shell is not "korn" shell.

Resolution: Change the shell type to *korn*. Use the `chsh` unix command to change SHELL type.

Shell type can also be changed by specifying shell path for the Unix user in `/etc/passwd` file.

Note: The `chsh` command is not available in Solaris OS.

28.2.2.2 Error Code - OFSAAI-1002

Cause: No proper arguments are available.

Resolution: Provide proper arguments. Invoke `Setup.sh` using Silent mode.

Example: `./Setup.sh SILENT`

28.2.2.3 Error Code - OFSAAI-1004

Cause: File `.profile` is not present in `$HOME`.

Resolution: Create `.profile` in `$HOME`, i.e. in the home directory of user.

28.2.2.4 Error Code - OFSAAI-1005

Cause: File `OFSAAIInfrastructure.bin` is not present in current folder.

Resolution: Copy `OFSAAIInfrastructure.bin` into installation kit directory.

28.2.2.5 Error Code - OFSAAI-1006

Cause: File `CustReg.DAT` is not present in current folder.

Resolution: Copy `CustReg.DAT` into installation kit directory.

28.2.2.6 Error Code - OFSAAI-1007

Cause: File `OFSAAI_InstallConfig.xml` is not present in current folder.

Resolution: Copy `OFSAAI_InstallConfig.xml` into installation kit directory.

28.2.2.7 Error Code - OFSAAI-1008

Cause: File `validateXMLInputs.jar` is not present in current folder.

Resolution: Copy `validateXMLInputs.jar` into installation kit directory.

28.2.2.8 Error Code - OFSAAI-1009

Cause: File `log4j.xml` is not present in current folder.

Resolution: Copy `log4j.xml` into installation kit directory.

28.2.2.9 Error Code - OFSAAI-1010

Cause: Unknown error occurred.

Resolution: Make sure to provide proper argument (Silent) to the `Setup.sh` file.

28.2.2.10 Error Code - OFSAAI-1011

Cause: XML validation failed.

Resolution: Check `InfrastructurePreValidations.Log` for more details.

28.2.2.11 Error Code - OFSAAI-1012

Cause: Property file with locale name does not exist.

Resolution: Copy `MyResources_en_US.properties` to the setup kit directory and keep `en_US` in `LOCALE` tag of `OFSAAI_InstallConfig.xml`.

28.2.2.12 Error Code - OFSAAI-1013

Cause: File `OFSAAI_InstallConfig.xml/OFSAAI_PostInstallConfig.xml` not found.

Resolution: Copy OFSAAI_InstallConfig.xml/OFSAAI_PostInstallConfig.xml to the setup kit directory.

28.2.2.13 Error Code - OFSAAI-1014

Cause: XML node value is blank.

Resolution: Make sure all node values except SMTPSERVER, PROXYHOST, PROXYPORT, PROXYUSERNAME, PROXYPASSWORD, NONPROXYHOST, or RAC_URL are not blank.

28.2.2.14 Error Code - OFSAAI-1015

Cause: XML is not well formed.

Resolution: Execute the command `dos2unix OFSAAI_InstallConfig.xml` to convert plain text file from DOS/MAC format to UNIX format.

OR

Make sure that OFSAAI_InstallConfig.xml is valid. Try to open the file through Internet Explorer for a quick way to check validity. If it is not getting opened, create new OFSAAI_InstallConfig.xml using the XML_ Utility.jar.

28.2.2.15 Error Code - OFSAAI-1016

Cause: User installation directory contain blank spaces.

Resolution: Provide an installation path that does not contain spaces. Check the tag USER_INSTALL_DIR in OFSAAI_InstallConfig.xml file. This path must not contain any spaces.

28.2.2.16 Error Code - OFSAAI-1017

Cause: User installation directory is invalid.

Resolution: Provide a valid installation path. Check if you are able to create the directory mentioned in USER_INSTALL_DIR tag value of OFSAAI_InstallConfig.xml file.

28.2.2.17 Java Console Error Messege - java.io.IOException: invalid SHA1 signature file

Cause: While accessing the Scenario Wizard JNLP file the error message is displayed.

Resolution:

To fix the issue, follow these steps:

1. Navigate to path: `deployedArea/SMLiteWeb/lib` and `deployedArea/SMLiteWeb/WEB-INF/lib`.
2. Run the following command to remove files from both the *orabpel.jar* files:

```
zip -d orabpel.jar 'META-INF/SUN_MICR.SF' 'META-INF/SUN_MICR.RSA'
```
3. Restart the server and re-launch the Scenario Wizard JNLP file.

29 Appendix U : OFS BD Version Compatibility List

Table 33 shows the OFS BD Version Compatibility List.

Table 33: OFS BD Version Compatibility List

OFS BD Version	OFSAAI Version	FSDf Version	OFS ECM Version
8.1.2	8.1.2	8.1.2.1 (includes all changes in FSDf 81201)	8.1.2
8.1.1.1	8.1.1.2	8.1.2.0.1	8.1.1.1
8.1.1	8.1.1	8.0.8	8.1.1
8081	8.0.8.6	8.0.8	8.0.8.x
8.0.8	8.0.8 to 8.0.8.6	8.0.8	8.0.8
8072	8.0.7.8	8.0.7	8.0.7.x
8071	8.0.7.4 to 8.0.7.8	8.0.7	8.0.7.x
8.0.7	8.0.7 to 8.0.7.8	8.0.7	8.0.7

OFSAA Support Contact Details

Raise a Service Request (SR) in [My Oracle Support \(MOS\)](#) for queries related to OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.

