Oracle® Financial Services

Analytical Applications Infrastructure

Installation and Configuration Guide

Release 8.1.2.0.0
G37707-01
July 2025

Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Guide, Release 8.1.2.0.0

G37707-01

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

Contents

11 Configure Resource Reference in Web Servers

12 Configure Work Manager in Web Application Servers

13 Additional Configurations for Application Packs

14 Additional Information

15 Remove OFSAA Infrastructure

16 Frequently Asked Questions (FAQs) and Error Dictionary

Index

Revision History

This log lists significant documentation updates:

Revision Date	Details
November 2023	Updated Java tool options to be included in the .profile file for all versions JDK 11.0.20 and above updates (36018169).
October 2023	Updated the tables that are granted privileges after installing OFSAA automatically (35813418).
August 2023	• Updated the FIC_SERVLET_PORT information details in AAI_SETUP_PROPS . For more information, refer EAR/WAR File - Build Once and Deploy Across Multiple OFSAA Instances (35751177). • Added steps to Update Weblogic server to 14.1.1 and include required Java option entry to disable HTTP2.
March 2023	• Replaced/deleted references to include Apache big data in the relevant sections • Updated prerequisite for FICserver in How to Run the Generate JSON Utility • Updated the list of files to be HTTPS enabled in Frequently Asked Questions (33841737) test • Updated Schema name format details in Configure the OFS__SCHEMA_IN.xml File (34835911)
January 2023	Added Solution for Errors generated while installing one-off patch on TCPS environment (34976170) - FAQ - 83
November 2022	• Updated Configure the excludeURLList.cfg File with correct instructions (Doc 34252585) • Updated steps for Deploy the EAR/WAR Files for WebLogic to include steps to activate services after deployment.
April 2022	Updated the Configure Operating System and File System Settings (Doc 33679099).
February 2022	Updated the Configure Password Changes (Doc 33858601).
December 2021	• Updated the Copy Jars to the OFSAA Installation Directory (32391102). • Updated the document for 33663417 Mandatory Patch instructions (Doc 33668822). • Updated the document for Installer Patch Download Number (Doc 33666242).

License Information

Oracle and third-party license details for installing and configuring OFSAA.

Third-party software tools - OFSAA Licensing Information User Manual Release 8.1.2.0.0.

OFSAA Product Licenses after installation of Application Packs - Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

Preface

Topics:

- xref to the Audience topic
- Documentation Accessibility
- xref to the Related Resources topic
- xref to the Conventions topic

<*book title*> describes how to <text>.

1

What’s New in Release 8.1.2.0.0

OFSAAI Installation and Configuration Guide bundles the following new features in version 8.1.2.0.0.

New features in the OFSAAAI Application Pack Release 8.1.2.0.0

Feature	Description
Common Library Upgrade	The following commonly used libraries are upgraded in OFSAA for the 8.1.2.0.0 Release: • ant 1.10.11 • Batik 1.14 • guava 2.29.0 • spring-xml-3.0.10.RELEASE.jar • spring-ws-core-3.0.10.RELEASE.jar • spring-ws-security-3.0.10.RELEASE.jar • xmlsec 2.2.3

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

2
Introduction

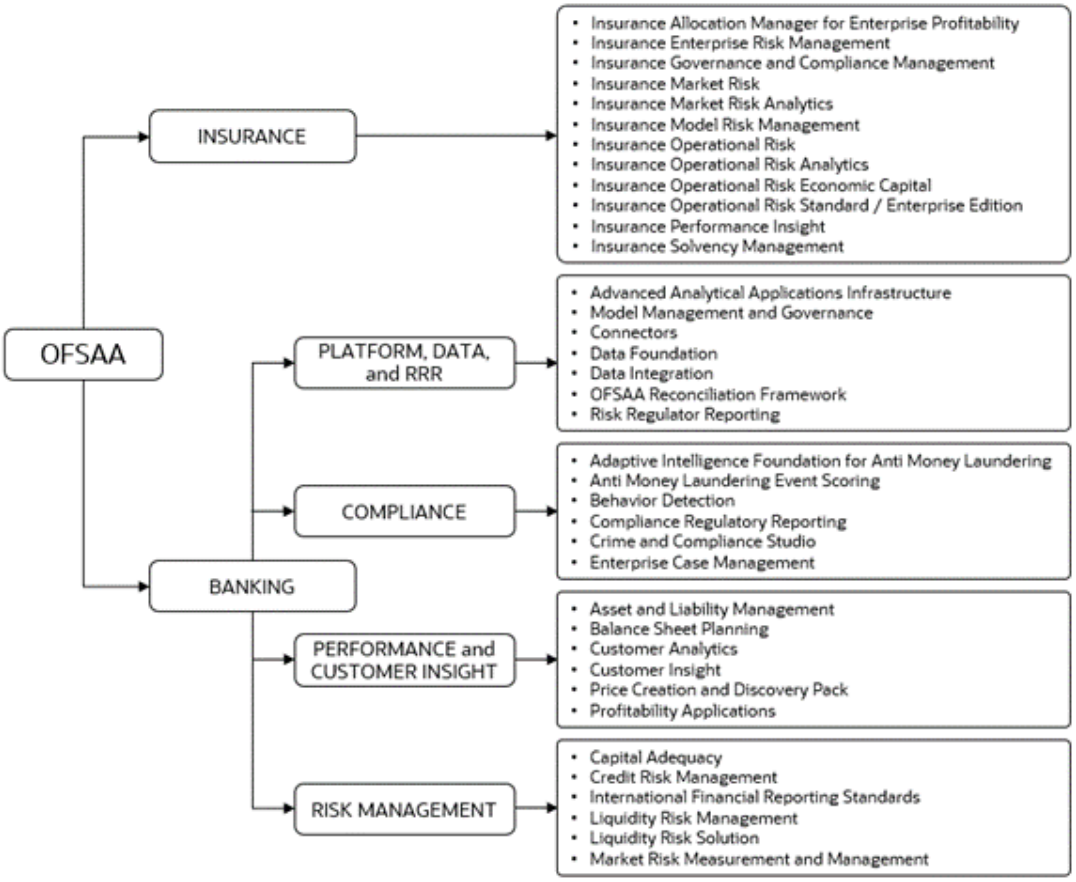
In today's turbulent markets, financial institutions require a better understanding of their risk-return, while strengthening competitive advantage and enhancing long-term customer value. Oracle Financial Services Analytical Applications (OFSAA) enable financial institutions to measure and meet risk-adjusted 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 models, 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, promote a transparent risk management culture, and provide pervasive intelligence.

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

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

Figure 2-1 Application Packs of OFSAA



Oracle Financial Services Analytical Applications Infrastructure (OFSAAI)

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.

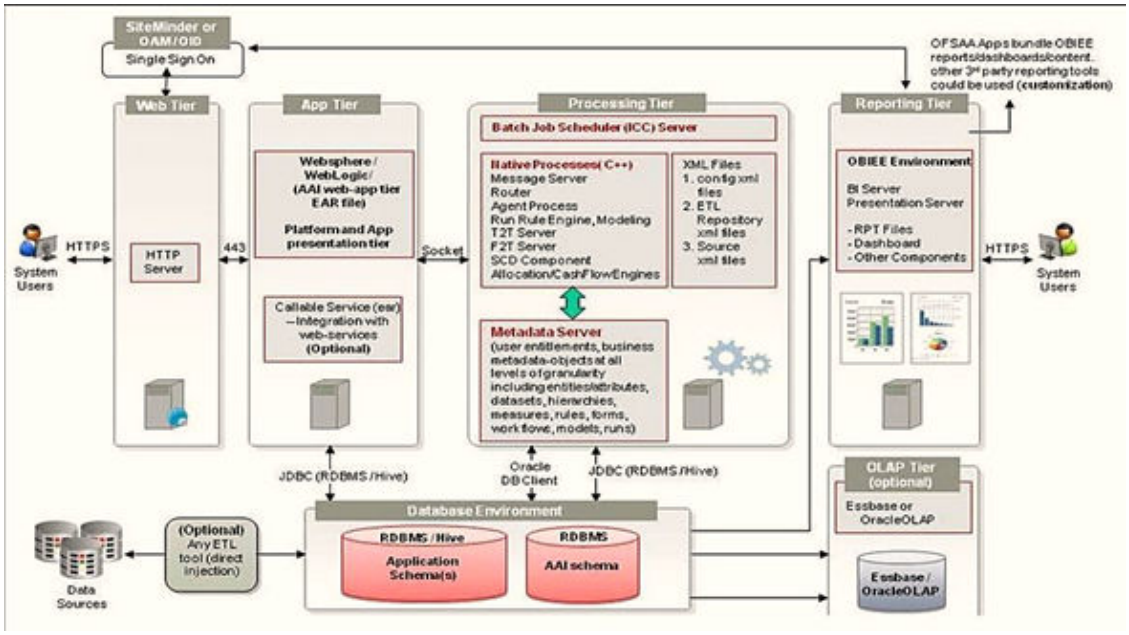
Components of OFSAAI

The OFSAA Infrastructure includes frameworks that operate on and with the Oracle Financial Services Analytical Applications Data Model and forms 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, while the UI and presentation logic runs on the other. The UI and presentation layer is deployed on any of the supported J2EE Servers.

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

Figure 2-2 Components of OFSAAI



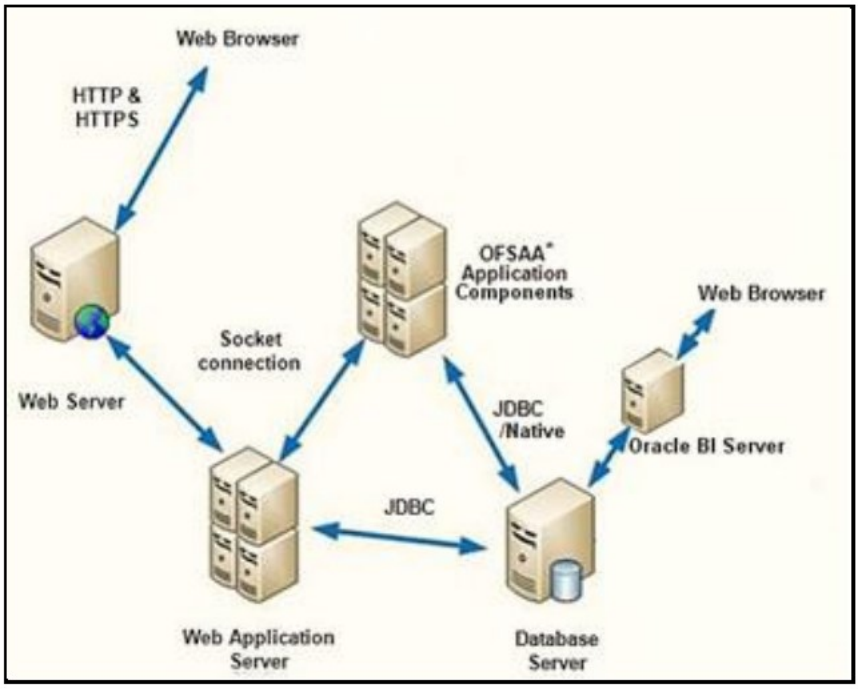
OFSAA Infrastructure High Availability

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

This release supports 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.

Deployment Topology

Figure 2-3 The logical architecture implemented for OFSAAAI Application Pack



About Oracle Financial Services Advanced Analytical Applications Infrastructure (OFSAAAI) Application Pack

Oracle Financial Services Advanced Analytical Applications Infrastructure (OFSAAAI) Application Pack provides integrated stress testing and modeling capabilities that you can readily apply across multiple risk areas enabling institutions to devise appropriate enterprise-wide and holistic risk and economic capital strategies.

OFSAAAI enables you to comply with regulatory requirements on stress testing, enables advanced customer and portfolio analytics, utilize multiple industry-standard techniques, test and model with complete data integrity.

OFSAAAI Application Pack includes the following applications:

Financial Services Analytical Applications Infrastructure

This application 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.

Financial Services Enterprise Modeling

This application helps banking institutions to identify the business opportunities and to measure the risk prevailing in the competitive market to safeguard the regulatory and economic capital of banks.

Financial Services Big Data Processing

This option introduces, into the OFSAA platform (OFSAAI), the capability to run analytics on data stored in Hadoop Distributed File System (HDFS).

With the Big Data Processing (BDP) add-on option, all core data management frameworks within OFSAA such as Data Management Framework (T2T/ F2T), Data Quality Framework, and Rules framework are enhanced to operate on both Oracle RDBMS data sources as well as Apache Hive data sources. An OFSAA Run definition can contain tasks that transform data held in the Hive. OFSAA applications that use these platform frameworks for expressing application logic automatically gain the ability to manage data held in the Hive. The OFSAA platform leverages HiveQL and Map Reduce to process data directly in the Hadoop cluster without having to stage data in a relational database.

Financial Services Inline Processing Engine

This application provides real-time monitoring, detection and interdiction of single and complex fraud events across multiple channels and lines of business.

About Oracle Financial Services Analytical Applications Infrastructure Extension Pack

The Oracle Financial Services Analytical Applications Infrastructure Extension (OFS AAIE) Pack adds a set of new advanced features for 8.1.2.0.0 Release across OFSAA applications. You can install this pack on an OFSAA instance having one or more OFSAA application packs.

The OFS AAIE Pack includes the following advanced features and functionalities:

- Distributed Processing Capabilities
- Analytic Pipeline and Process models
- Attribution Analysis
- Content Management Interoperability Services

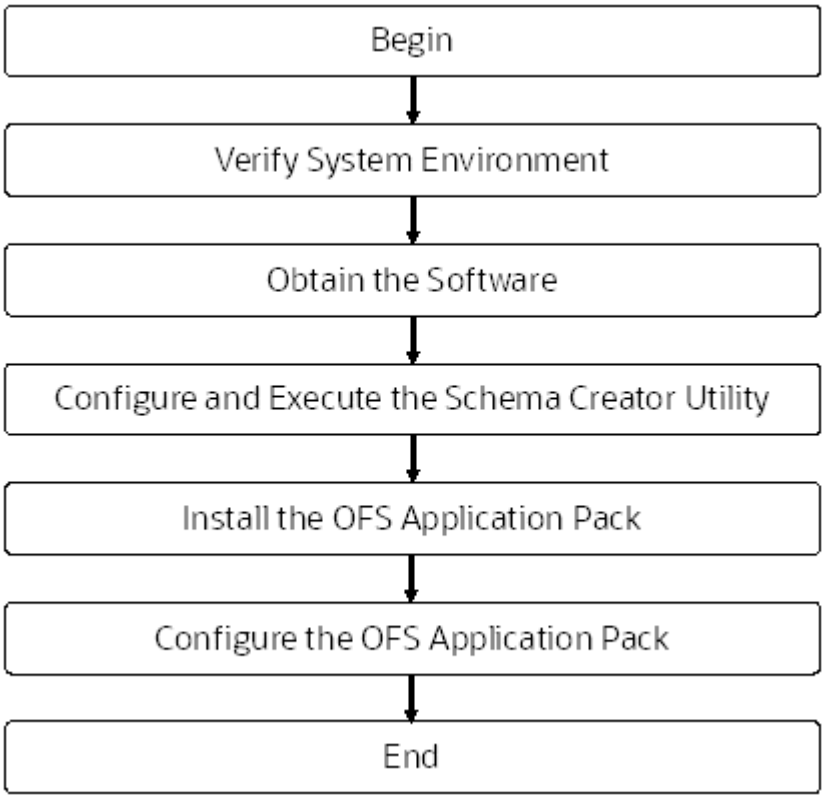
> **Note:**
>
> The pack is enabled by procurement of an additional license. For more information, see the OFS AA IE Release Notes and Installation Guide.

Installation Overview

Release 8.1.2.0.0 of OFSAA Application Packs support the fresh installation.

The following illustration shows the sequence of steps you need to follow to perform the installation.

Figure 2-4 Installation Flow of OFSAA Application Packs



3
Installation and Upgrade Scenarios

OFSAAI Release 8.1.2.0.0 supports various installation and upgrade scenarios. Refer to the following table for a high-level overview of the possible scenarios.

Table 3-1 Release 8.1.2.0.0 Installation and Upgrade Scenarios

Scenario	Installation and Upgrade Instructions
New Installation Installing Release 8.1.2.0.0 application pack for the first time (new installation).	1. Prepare for the Installation. 2. Execute the Schema Creator Utility. 3. Install the OFSAAI Application Pack.
Upgrade Installation Upgrade an already installed application pack from v8.1.1.0.0 or later Example: You are using release v8.1.1.1.0 and now want to upgrade to Release 8.1.2.0.0.	1. Run the Environment Check Utility tool and ensure that the hardware and software requirements are installed as per the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix. 2. Prepare for Upgrade. 3. Download the installer. 4. Extract the software. 5. Trigger the installation.
Upgrade OFS AAAI from Linux 7 to Linux 8 If your OFS AAAI instance is on Linux 7 Operating System and you want to install OFS AAAI on Linux 8.	1. Clone your existing environment to the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix. 2. Run the upgrade installer in the cloned environment.
Upgrade from OFS AAAI Release v8.0.x on AIX or Solaris x86 Operating System	Release v8.1.2.0.0 of OFS AAAI is not certified for IBM AIX and Oracle Solaris x86 Operating Systems. If you are currently running OFSAA v8.0.x on AIX or Solaris x86 Operating Systems and plan to upgrade to Release v8.1.2.0.0, then you must migrate from AIX or Solaris x86 to Oracle Linux or Oracle Solaris SPARC. For more information, refer to Certification and Migration Information for Operating Systems on OFSAA v8.1.0.0.0 (Doc ID 2700084.1).

4
Installation Checklist

Checklist to validate OFSAA Installation

For seamless OFSAA installation, refer to the following checklist:

Table 4-1 Installation Checklist

	Sl. No.	Activity
Pre-installation Steps	1	Install all the prerequisite *hardware and software* as per the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix.
	2	Verify the System Environment using the Environment Check Utility.
	3	Configure the Database Instance settings.
	4	Install and configure the web application server.
	5	Configure the HTTP settings on the web server.
	6	(Optional) Install and configure for Big Data/Hive.
	7	Create the Installation, Download, and Metadata Repository Directories: • Installation directory • Temporary directory • Staging Area/Metadata Repository • Download directory
	8	Configure the following Operating System and File System settings: • File Descriptor • Total number of processes • Port(s) • .profile file permissions • Add FTP/SFTP configuration for file transfer (to access staging area and metadata directory)

Table 4-1 (Cont.) Installation Checklist

	Sl. No.	Activity
	9	Update the following Environment Settings as required for the installation in the .profile file: Java Settings • Oracle Database Server and Client Settings • Add TNS entries in the TNSNAMES.ORA file • Oracle Essbase Settings • Time Zone Settings
	10	(Optional) Install and configure Oracle R/ Oracle R Enterprise.
	11	Download the installer kit.
Installation Steps	12	Extract the installer kit.
	13	Configure the OFS_<App pack>_PACK.xml file.
	14	Configure the OFS_<App pack>_SCHEMA_IN.xml file.
	15	(Optional) Configure the <App pack>_SCHEMA_BIGDATA_IN.xml file.
	16	Execute the Schema Creator Utility in Online, Offline, or TCPS modes and verify the log file.
	17	Configure the OFSAAI_InstallConfig.xml file.
	18	Trigger the application installation.
Post-Installation Steps	19	Verify the installation logs.
	20	Verify that all patches are successfully installed.
	21	Backup the OFS_<PACK>_SCHEMA_IN .xml and OFS_<PACK>_SCHEMA_OUTPUT.xml files.
	22	Stop the OFSAA Infrastructure services.
	23	Create and deploy EAR or WAR files.
	24	Assign Grants for schemas.
	25	Start the OFSAA Infrastructure services.
	26	Access the OFSAA Application.
	27	Configure the excludeURLList.cfg file.
	28	(Optional) Configure Big Data Processing.
	29	Create Application Users.

Table 4-1 (Cont.) Installation Checklist

	Sl. No.	Activity
	30	Map Application User(s) to User Groups.
	31	Add TNS entries in the TNSNAMES.ORA file.
	32	Set TDE and Data Redaction in OFSAAI.
	33	Implement Data Protection in OFSAAI.
Additional Configuration	34	Configure the web server.
	35	Configure Resource Reference in web servers.
	36	Configure Work Manager in web application servers.
	37	Add FTP/SFTP Configuration for File Transfer.
	38	Configure Infrastructure Server Memory.
	39	Retrieve Patch Information.
	40	Change IP/Hostname, Ports, Deployed Paths of the OFSAA Instance.
	41	Set Infrastructure LDAP Configuration.
	42	Configure OFSAAI Web Services.
	43	Configure Message Details in Forms Designer.
	44	Configure Password Changes.
	45	Configure Java Virtual Machine.
	46	Configure Internal Service.

5

Hardware and Software Requirements

Hardware and software requirements for OFSAA 8.1.2.0.0.

See the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix for the hardware and software required.

Table 5-1 Recommended Software Combination

Operating System	Database	Web Application Server	Web Server
Oracle Linux	Oracle Database	Oracle WebLogic Server/ Oracle WebSphere Application Server/ Apache Tomcat Server	Oracle HTTP Server/ Apache HTTP Server
Oracle Solaris SPARC	Oracle Database	Oracle WebLogic Server/ Apache Tomcat Server	Oracle HTTP Server/ Apache HTTP Server

> **Note:**
>
> Oracle Applications are developed and tested on Oracle Linux, which is optimized for performance, stability, and security.

License Information

For details on the third-party software tools used, see the link below.

OFSAA Licensing Information User Manual Release 8.1.2.0.0.

For information about OFSAA Product Licenses after installation of Application Packs, see the **View OFSAA Product Licenses After Installation of Application Pack** section in the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

Verify System Environment

Use the Pre-Install check utility to verify the system environment before installing OFSAA.

Use the Pre-Install Check utility bundled with the Install Kit archive file, to verify if your system meets the minimum requirements for OFSAA installation. You can also download this utility from My Oracle Support. For more information about using this utility, refer to Oracle Financial Services Analytical Applications Infrastructure Environment Check Utility Guide.

Though the system environment verification is an integral and automated part of the installation, we recommend to run this utility before beginning the installation as part of your organization's **Installation Readiness Verification Process**.

6
Pre-installation Tasks

List of pre-installation tasks to be completed before installing OFSAA.

1. Install all the prerequisite hardware and software as per the OFS Analytical Applications 8.1.2.0.0 Technology Matrix.
2. Verify the system environment using the **Environment Check Utility**.
3. Configure the database instance settings.
4. Install and configure the Web application server.
5. Configure the HTTP settings on the Web server.
6. (Optional) Install and configure for Big Data/Hive.
7. Create the installation, download, and metadata repository directories.
8. Configure the OS file system settings in the `.profile` file.
9. Configure the environment settings in the `.profile` file.
10. Install Oracle R distribution and Oracle R Enterprise (ORE).
11. Download the OFSAAAI Applications Pack installer and mandatory patches.
12. Download the OFSAAAI Applications Pack installer and mandatory patches.
13. Download the OFSSTA Application Pack installer and mandatory patches.
14. Install the Linux libraries.
15. Install MySQL version 8.0.3.2
16. Install JDK version 17
17. Install Phython version 3.8 or greater
18. Create the following databases:
    ```
    CREATE DATABASE openmetadata_db; CREATE DATABASE airflow_db CHARACTER SET
    utf8mb4 COLLATE utf8mb4_unicode_ci; CREATE USER 'openmetadata_user'@'%'
    IDENTIFIED BY 'openmetadata_password'; CREATE USER 'airflow_user'@'%'
    IDENTIFIED BY 'airflow_pass'; CREATE USER 'airflow_user'@'localhost'
    IDENTIFIED BY 'airflow_pass'; GRANT ALL PRIVILEGES ON openmetadata_db.* TO
    'openmetadata_user'@'%' WITH GRANT OPTION; GRANT ALL PRIVILEGES ON
    airflow_db.* TO 'airflow_user'@'%' WITH GRANT OPTION; GRANT ALL PRIVILEGES ON
    airflow_db.* TO 'airflow_user'@'localhost' WITH GRANT OPTION; commit;
    ```
19. Update the environment variables file (set_env.env) with the locations of the variables:
    ```
    OMD_INS_DIR=/scratch/openmetadata-ins-dir LOCAL_REPO_DIR=/scratch/
    openmetadata-ins-dir/local_repo AIRFLOW_HOME=/scratch/openmetadata-ins-dir/
    airflow PYTHON_INS_DIR=/scratch/openmetadata-ins-dir/python39
    HTTP_PROXY_URL=http://www-proxy-adcq7.us.oracle.com:80 HTTPS_PROXY_URL=http://
    www-proxy-adcq7.us.oracle.com:80
    ```
20. Extract the installation software.

Configure Oracle Database Instance Settings

Oracle Database Instance Settings.

Configure the following database instance settings:

- `NLS_CHARACTERSET` to `AL32UTF8`
- `NLS_LENGTH_SEMANTICS` to `BYTE`
- `OPEN CURSORS` limit to greater than 1000

Configure Web Server Settings

The Web server settings.

(Optional). If you have installed an HTTP Server, then configure the appropriate HTTP server settings:

Table 6-1 Web Server Settings

Description	Example Value
Apache HTTP Server/ Oracle HTTP Server/ IBM HTTP Server	Configure the HTTP Server and note down the IP/ Hostname and Port details as you will be prompted to enter these details during installation. For more information, refer to Configure the Web server.

Configure Big Data Settings

Configure Big Data settings.

Perform this task, if you intend to install OFSAA Big Data Processing.

Install Big Data components from Apache. For version information, see the Hardware and Software Requirements.

Create Installation, Download, and Metadata Repository Directories

Create directories for installation, download, and metadata repository.

- **OFSAA Download Directory (Optional)**: Create a download directory and copy the OFSAA Application Pack Installer File (archive) and downloaded installer/patches to this directory. Assign `755` permission to this directory.
- **Temporary Directory**: Create a default temporary directory to store the installation files for a short time to support faster installation. Allocate more than 10 GB of space, for the /tmp directory. Assign `755` permission to this directory with `NOEXEC` option disabled.

> **Note:**
>
> If `NOEXEC` option is enabled, the installer cannot extract the files to the /tmp directory and the binaries will not execute in the directory. Hence. the installation will not be successful.

- **OFSAA Installation Directory (Mandatory)**: Create an installation directory, to install the product binaries. Set the variable `FIC_HOME` in the `.profile` file to point to the OFSAA Installation Directory. Assign `755` user permission to the installation directory.
- **OFSAA Staging/Metadata Directory (Mandatory)**: Create a staging directory to hold the application metadata artifacts and act as the staging area for the flat files. This directory is also referred to as **FTPSHARE**. You can also use this directory to copy data files and save data extracts.
  Create the staging directory on the system where OFSAA is installed. You can also configure this directory on a different mount or under a different user profile. The owner of the installation directory must have `RWX (775)` permissions to this directory.

> **Note:**
>
> Ensure the OFSAA staging directory is not set to the same path as the OFSAA installation directory and is not a subdirectory inside the OFSAA installation directory.

Configure the OS File System Settings and Environment Settings in the .profile File

A `.profile` file is a start-up file for a UNIX user and contains various parameters for Environment settings, OS, and File System settings.

Create the `.profile` file in the home directory of the logged-in user, if it is not already present. The user must have `755` permission on the file to execute it.

To set the parameters for the `.profile` file, log in as a non-root user, and configure the environment settings.

> **Note:**
>
> Ensure that you modify only the parameters mentioned in the following categories:

- Configure Operating System and File System Settings
- Configure the Environment Settings

Configure Operating System and File System Settings in the .profile File

Configure the Operating System and file system settings.

Table 6-2 Configure Operating System and File System settings

Parameter	Configuration Action
Installation Directory	In the `.profile` file, set the variable `FIC_HOME` to point to the OFSAA Installation Directory.
File Descriptor Settings	To change the number of file descriptors, log in as a root user in the `sysctl.conf` file and edit the following: 1. Edit the following entry in the `/etc/sysctl.conf` file: `fs.file-max` = <value>, where <value> is greater than 15000. **Note:** This value is the minimum value required to proceed with the installation. For other modules, this value may depend on the available resources and the number of processes executed in parallel. 2. Run the command to save the changes: `# /sbin/ sysctl -p`
Total Number of Process Settings	In the `sysctl.conf` file, set the value to greater than 15000. This value is the minimum value required to proceed with the installation. For other modules, this value may depend on the available resources and the number of processes executed in parallel.
Port Settings	Enable the following default port numbers on the system: **6500**, **6501**, **6505**, **6507**, **6509**, **6510**, **6666**, **9999**, and **10101**.

Configure the Environment Settings

Configure the Environment settings.

The `.profile` file consists of various parameters for Environment Settings.

To set the parameters for the `.profile` file, log in as a non-root user, and configure the following environment settings:

- Java Settings
- Oracle Database Server and Client Settings
- TNS entries in the `TNSNAMES.ORA` file for Non-TCPS and TCPS
- Oracle Wallet Settings for Installation in TCPS Mode
- Oracle Essbase Settings
- Time Zone Settings

Java Settings

Configure the Java settings.

Description	Example

In the `.profile` file, set PATH to include the Java Runtime Environment (JRE) absolute path. Ensure that SYMBOLIC links to JAVA installation are not set in the PATH variable.	For example:
	`PATH=/usr/java/jre1.8.0_221/bin:$ORACLE_HOME/bin:$PATH`
	`export PATH`
	Note:
	OFSAA does not support OpenJDK and JRE.

In the `.profile` file, set PATH to include the Java Runtime Environment bin path.	`JAVA_BIN=/scratch/<<version>>/jre/bin`
	For example:
	`PATH=/usr/java/jre1.8.0_221/bin:$ORACLE_HOME/bin:$PATH`

In the `.profile` file, set the Java tool options for all versions JDK 11.0.20 and above updates	`JAVA_TOOL_OPTIONS=" -Djdk.util.zip.disableZip64ExtraFieldValidation=true"` `export JAVA_TOOL_OPTIONS`
Enable unlimited cryptographic policy for Java.	For more information, refer to Enabling Unlimited Cryptographic Policy in the OFS Analytical Applications Infrastructure Administration Guide.

Oracle Database Server and Client Settings

Configure the Oracle Database Server and Client settings.

Table 6-3 Oracle Database Server and Client Settings

Description	Example
In the `.profile` file, set `TNS_ADMIN` pointing to the appropriate `tnsnames.ora` file.	`TNS_ADMIN=$HOME/tnsnames.ora`
In the `.profile` file, set `ORACLE_HOME` pointing to the appropriate Oracle Client installation.	`ORACLE_HOME=/scratch/oraofss/app_client18c/product/18.0.0/client_1`
In the `.profile` file, set PATH to include the appropriate `$ORACLE_HOME/bin` path.	`PATH=$JAVA_HOME/bin:$ORACLE_HOME/bin`

Add TNS entries in the TNSNAMES.ORA File

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

To add the TNS name for the entries:

1. Log in to the application using System Administrator privileges.
2. Navigate to **System Configuration & Identity Management** tab.
3. Click **Administration** and **Configuration**, select **System Configuration**, and click **Database Details**.
4. Expand **Name** to get the list of TNS entry names.

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

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

TNS entries in the TNSNAMES.ORA file for Non-TCPS and TCPS

Configure the TNS entries in the `TNSNAMES.ORA` file for Non-TCPS and TCPS.

TNS entries in the TNSNAMES.ORA file for Non-TCPS mode

- Add an entry (with SID/ SERVICE NAME) is added in the `tnsnames.ora` file on the OFSAA server.

```
<SID NAME> =
(DESCRIPTION =
  (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = <HOST_NAME/IP ADDRESS>)(PORT =
<PORT_NUMBER>))
)
(CONNECT_DATA =
  (SERVICE_NAME = <SID_NAME>))
)
<ATOMICSCHEMANAME> =
(DESCRIPTION =
  (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = <HOST_NAME/IP ADDRESS>)(PORT =
<PORT_NUMBER>))
)
(CONNECT_DATA =
  (SERVICE_NAME = <SID NAME>)
))
```

Example

```
<SID_NAME> =
(DESCRIPTION =
  (ADDRESS_LIST =
  (ADDRESS =
  (PROTOCOL = TCP)(HOST = <HOST_NAME/IP ADDRESS>.in.oracle.com)(PORT =
1521))
)
(CONNECT_DATA =
  (SERVICE_NAME = <SID_NAME>))
)
<ATOMIC_SCHEMA_NAME> =
(DESCRIPTION =
  (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = <HOST_NAME/IP ADDRESS>.in.oracle.com)
```

```
(PORT = 1521))
)
(CONNECT_DATA =
  (SERVICE_NAME = <SID_NAME>)
))
```

> **Note:**
>
> The ATOMIC SCHEMA NAME must be the same as defined in the `OFS_<App Pack>_SCHEMA_IN.xml` file, which also includes prefix without underscore. For example, `DEVOFSAAATM`.

TNS entries in the TNSNAMES.ORA file for TCPS mode

- Add an entry (with SID/ SERVICE NAME) is added in the `tnsnames.ora` file on the OFSAA server.

```
 <SID_NAME> =
(DESCRIPTION =
  (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCPS)(HOST = <HOST_NAME/IP ADDRESS>)(PORT =
<PORT_NUMBER>))
)
(CONNECT_DATA =
  (SERVICE_NAME = <SID NAME>)
(security=(ssl_server_cert_dn=CN=<HOST_NAME>))
))
<ATOMICSCHEMANAME> =
(DESCRIPTION =
  (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCPS)(HOST = <HOST NAME/IP ADDRESS>)(PORT =
<PORT_NUMBER>))
)
(CONNECT_DATA =
  (SERVICE_NAME = <SID NAME>)
  (security=(ssl_server_cert_dn=CN=<HOST_NAME>))
))
```

Example

```
 <SID_NAME> =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS)(HOST = .in.oracle.com)(PORT = 1521))
)
(CONNECT_DATA =
(SERVICE_NAME = <SID NAME>)
(security=(ssl_server_cert_dn=CN=<HOST_NAME>))  )  )
<ATOMICSCHEMANAME> =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS)(HOST = <HOST_NAME/IP ADDRESS>.in.oracle.com)
(PORT = 1521))
```

```
)
(CONNECT_DATA =
(SERVICE_NAME = <SID NAME>)
(security=(ssl_server_cert_dn=CN=<HOST_NAME>)) )  )
```

> **Note:**
>
> The ATOMIC SCHEMA NAME must be the same as defined in the `OFS_<App Pack>_SCHEMA_IN.xml` file, which also includes prefix without underscore. For example, DEVOFSAAATM.

- Add an entry (with `WALLET_HOME` and wallet parameters) in the `sqlnet.ora` file on the OFSAA server must be same as Oracle database server running with TCPS.

```
<SID NAME> =
 (DESCRIPTION =
 (ADDRESS_LIST =
 (ADDRESS = (PROTOCOL = TCPS)(HOST = <HOST NAME/IP ADDRESS>)(PORT = <PORT
NUMBER>))
 )
 (CONNECT_DATA =
 (SERVICE_NAME = <SID NAME>)
(security=(ssl_server_cert_dn=CN=<HOST NAME>))
 )
 )
<ATOMICSCHEMANAME> =
 (DESCRIPTION =
 (ADDRESS_LIST =
 (ADDRESS = (PROTOCOL = TCPS)(HOST = <HOST NAME>)(PORT = <PORT
NUMBER>))
 )
 (CONNECT_DATA =
 (SERVICE_NAME = <SID NAME>)
(security=(ssl_server_cert_dn=CN=<HOST NAME>)) )
 )
```

Example

```
NAMES.DIRECTORY_PATH=(TNSNAMES, EZCONNECT)
WALLET_LOCATION =
(SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY = )))
SQLNET.WALLET_OVERRIDE = TRUE
SSL_CLIENT_AUTHENTICATION = FALSE
SQLNET.AUTHENTICATION_SERVICES = (TCPS,NTS,BEQ)
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA)
```

> **Note:**
>
> The ATOMIC SCHEMA NAME must be the same as defined in the `OFS_<App Pack>_SCHEMA_IN.xml` file, which also includes prefix without underscore. For example, DEVOFSAAATM.

Oracle Wallet Settings for Installation in TCPS Mode

Configure the Oracle Wallet for installation in TCPS mode.

To run the installer in the TCPS mode, configure the following parameters for Oracle Wallet in the `.profile` file.

```
OFS_ORA_WAL_ENABLED=TRUE
export OFS_ORA_WAL_ENABLED
WALLET_HOME=<PATH_TO_THE_DIRECTORY_WHERE WALLET RELATED FILES EXIST>
export WALLET_HOME
```

> **Note:**
>
> - To install in TCPS mode, ensure that Oracle Wallet includes Config and Atomic Schema credentials, along with required certificates.
> - If you do not configure this variable, the system defaults to `OFS_ORA_WAL_ENABLED=FALSE`.
> - For information on creating and managing Oracle Wallet, refer to:
>   - SSL Connection to Oracle DB using JDBC, TLSv1.2, JKS or Oracle Wallets
>   - WebLogic JDBC Use of Oracle Wallet for SSL

Oracle Essbase Settings

Configure the Oracle Essbase settings.

To use Oracle Hyperion Essbase OLAP features, configure the following parameters in the `.profile` file:

- `ARBORPATH` to point to an appropriate Oracle Essbase Client installation:
  `PATH=$PATH:$ARBORPATH/bin`
- `ESSBASEPATH` to point to an appropriate Oracle Essbase Client installation:

  ```
  ESSBASEPATH=/scratch/essps3/Oracle/MiddlewareHome/EP
  MSystem11R1/common/EssbaseRTC-64/11.1.2.0
  export ESSBASEPATH
  ```

- `HYPERION_HOME` to point to an appropriate Oracle Essbase Client installation:

```
HYPERION_HOME=/scratch/essps3/Oracle/MiddlewareHome/
EPMSystem11R1/common/EssbaseRTC-64/11.1.2.0
export HYPERION_HOME
```

Time Zone Settings

Configure the time zone settings in the `.profile` file.

Configure the `Time Zone` parameter in the `.profile` file to indicate the time zone of your region/location. For example, `TZ=Asia/Calcutta`.

Install Oracle R distribution and Oracle R Enterprise (ORE)

Install the Oracle R distribution (ORD) and Oracle R Enterprise (ORE).

> **Note:**
>
> (Optional). Required only if you intend to use Oracle R scripting in Oracle Financial Services Enterprise Modeling.

Install Oracle R Distribution and Oracle R Enterprise (server components) on the Oracle Database server. Refer to Oracle R Enterprise Installation and Administration Guide for Linux and Solaris.

For supported versions of ORD and ORE, refer to the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix.

> **Note:**
>
> If you are using ORE 1.4.1 with Oracle Financial Services Enterprise Modeling,configure the session time zone in the `R_HOME/etc/ Rprofile.site` file on the database server. Here, `R_HOME` is the home directory of the R instance where ORE server packages are installed. You can also set the session time zone in scripts registered in OFS EM using the `Sys.env(TZ=<time zone>)` R function.

Download the OFSAAAI Applications Pack Installer and Mandatory Patches

Download the OFSAAAI Applications Pack Installer and the mandatory patches.

To download the OFSAAAI Applications Pack Installer Release 8.1.2.0.0:

1. Log in to My Oracle Support and search for **32791983** in **Patches & Updates**.
2. Download the installer archive and copy it (in Binary mode) to the download directory in the OFSAAAI installation setup.

> **Note:**
>
> Select the required archive files for either Solaris SPARC or Linux based on the OFSAAAI operating system.

3. Log in to My Oracle Support, search for the **33663417** mandatory patch in **Patches & Updates** and download it.

> **Note:**
>
> Oracle issued Security Alert CVE-2021-44228 on December 10, 2021, in response to the disclosure of a new vulnerability affecting Apache Log4J prior to version 2.15. Applying the **33663417** mandatory patch resolves the issue. For details, refer to the My Oracle Support Doc ID 2827801.1.
>
> Reapply the **33663417** mandatory patch whenever you install or upgrade the application, or apply an incremental patch.

Extract the Software

Extract the installation software.

Ensure you are logged in to the UNIX operating system as non-root user to extract the software.

To extract the software:

1. Download the unzip utility (OS-specific) `unzip_<os>.zip` and copy it in Binary mode to the directory included in your PATH variable.

   If you already have an unzip utility to extract the contents of the downloaded archive, skip this step. Uncompress the unzip installer file:

   ```
   uncompress unzip_<os>.zip
   ```

   > **Note:**
   >
   > If you encounter the error `uncompress: not found [No such file or directory]`, contact your UNIX administrator.

2. Assign execute (`751`) to the file: `chmod 751 unzip_<OS>`

   For example: `chmod 751 unzip_sparc`

3. Extract the contents of the Application Pack Release 8.1.2.0.0 installer archive file in the download directory:

   ```
   unzip OFS_AAAI_PACK.zipUnzip <name of the file to be unzipped>.zip
   ```

4. Navigate to the download directory and assign execute permission to the installer directory:

   ```
   chmod -R 750 OFS_AAAI_Packchmod -R 755 OFS_LRS_PACK
   ```

> **Note:**
>
> For Solaris OS, download, extract and apply the one-off patch 31509494 from My Oracle Support. See the Readme packaged with the patch for further instructions on how to install the patch.

5. Give execute permission to the archive file. Navigate to the path where the directory OFS_LRS_PACK exists and execute the command:`chmod -R 755 OFS_LRS_PACK`
6. Execute the user .profile file.
7. Navigate to the /OFS_LRS_PACK/schema_creator/conf directory and modify the OFS_LRS_SCHEMA_IN.xml file by providing the existing values to the parameters JDBC_URL, JDBC_DRIVER, Host, Setupinfo name, schema names (config and atomic), password, default tablespace, Infodom, Quota as per the previous version.
8. Navigate to the /OFS_LRS_PACK/schema_creator/bin directory and execute the osc.sh file using the following command: `./osc.sh -s`

> **Note:**
>
> Steps 7 and 8 are required to generate the OFS_LRS_SCHEMA_OUTPUT.xml file.

After assigning the required permissions, proceed with the Installation Tasks.

7

Installation Tasks

List of installation tasks for installing the OFSAA application pack.

Installation Tasks

1. Configure the OFS_<App pack>_PACK.xml File .
2. Configure the OFS_<App pack>_SCHEMA_IN.xml File .
3. (Optional) Configure the <App pack>_SCHEMA_BIGDATA_IN.xml File .
4. Execute the Schema Creator Utility in Online, Offline, or TCPS modes and verify the log file.
5. Configure the `OFS_<App pack>_InstallConfig.xml` file.
6. Trigger the application installation.

Configure the OFS_<App pack>_PACK.xml file

The XML file contains details about the various products bundled together in the OFS <App pack>.

To configure the `OFS_<App pack>_PACK.xml` file:

1. Navigate to the `OFS_<APP PACK>/conf` directory and configure the `OFS_<APP PACK>.xml` file in a text editor as mentioned in the table below.
2. Save the file.

Figure 7-1 Sample OFS_LRS_PACK.xml File

```
<APP>
    <APP_ID PREREQ="OFS_AAAI" ENABLE="YES">OFS_LRM_LCR</APP_ID>
    <APP_NAME>Financial Services Liquidity Risk Measurement and Management</APP_NAME>
    <APP_DESCRIPTION>Core application for Liquidity Risk Solutions LCR</APP_DESCRIPTION>
    <VERSION>8.1.2.0.0</VERSION>
    <OPTIONS>
        <OPTION ID="OFS_LRM_LCR_EBA" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_EBA</OPTION>
        <OPTION ID="OFS_LRM_LCR_USFED" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_USFED</OPTION>
        <OPTION ID="OFS_LRM_LCR_BOT" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_BOT</OPTION>
        <OPTION ID="OFS_LRM_LCR_RBI" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_RBI</OPTION>
        <OPTION ID="OFS_LRM_LCR_BNM" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_BNM</OPTION>
        <OPTION ID="OFS_LRM_LCR_MAS" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_MAS</OPTION>
        <OPTION ID="OFS_LRM_LCR_HKMA" PREREQ="OFS_LRM_LCR" ENABLE="YES">OFS_LRM_LCR_HKMA</OPTION>
    </OPTIONS>
</APP>
<APP>
    <APP_ID PREREQ="OFS_AAAI" ENABLE="YES">OFS_LRM_DIC</APP_ID>
    <APP_NAME>Financial Services Deposit Insurance Calculations for Liquidity Risk Solutions Pack</APP_NAME>
    <APP_DESCRIPTION>Core application for Liquidity Risk Solutions Insurance</APP_DESCRIPTION>
    <VERSION>8.1.2.0.0</VERSION>
    <OPTIONS>
        <OPTION ID="OFS_LRM_DIC_USFED" PREREQ="OFS_LRM_DIC" ENABLE="YES">OFS_LRM_DIC_USFED</OPTION>
        <OPTION ID="OFS_LRM_DIC_BNM" PREREQ="OFS_LRM_DIC" ENABLE="YES">OFS_LRM_DIC_BNM</OPTION>
        <OPTION ID="OFS_LRM_DIC_MAS" PREREQ="OFS_LRM_DIC" ENABLE="YES">OFS_LRM_DIC_MAS</OPTION>
        <OPTION ID="OFS_LRM_DIC_HKMA" PREREQ="OFS_LRM_DIC" ENABLE="YES">OFS_LRM_DIC_HKMA</OPTION>
    </OPTIONS>
</APP>
</APP_PACK_CONFIG>
```

Table 7-1 `OFS_<APP PACK>.xml` File Parameters

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Comments
APP_PACK_ID	Unique Application Pack Identifier	Y	Unique Seeded Value. Do not modify this value.
IS_OPT_INSTALL VALUE="TRUE"	Unique Application Entry	Y	Unique Seeded Value. Do not modify this value.
APP_PACK_NAME	Unique Application Pack Name	Y	Unique Seeded Value. Do not modify this value.
APP_PACK_DESCRIPTION	Unique Application Pack Description	Y	Unique Seeded Value. Do not modify this value.
VERSION	Unique release version	Y	Unique Seeded Value. Do not modify this value.
APP	Unique Application Entries	Y	Unique Seeded Value. Do not modify this value.
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, OFSAAAI is the prerequisite set. For all other applications, the default Application ID is set to none. You can set it for the applications you want to install. Do not modify this value.
APP_ID/ DEF_SEL_FLAG	Default Selected Flag	Y	In all application packs, Infrastructure requires this value to be set to "YES". Do not modify this value.

Table 7-1 (Cont.) `OFS_<APP PACK>.xml` File Parameters

Tag Name/ Attribute Name	Description	Mandatory (Y/ N)	Comments
APP_ID/ ENABLE	Enable Application/ Product	Y	• Default YES for Infrastructure • NO for Others Set this attribute-value to YES against every APP_ID which is licensed and must be enabled for use. Note: The Application/ Product cannot be disabled once enabled. Only applications/ products which are enabled are installed. In order to enable other licensed applications/ products, you must reinstall by setting the flag as Y for the App_ID. However, in case of a reinstallation, to enable the other applications/ products, skip the execution of the schema creation utility if it does not involve creation of additional sandboxes.
APP_NAME	Unique Application/ Product Name	Y	Unique Seeded Value. Do not modify this value.
APP_DESCRIPTION	Unique Application/ Product Name	Y	Unique Seeded Value. Do not modify this value.
VERSION	Unique release version	Y	Unique Seeded Value. Do not modify this value.

Configure the Schema Creator Utility

Configure and execute the schema creator utility before installing the application pack.

Creating database users/schemas (RDBMS) is one of the primary steps in the comprehensive OFSAAAI installation process. The Schema Creator utility enables you to quickly get started with the installation by creating Database User(s)/ Schema(s) (RDBMS), assigning the necessary GRANT(s), and creating the required entities in the schemas.

Prerequisites for configuring the Schema Creator utility

- Oracle User ID/Password with SYSDBA privileges
- JDBC Connection URL for RAC/Non RAC database

- The HOSTNAME/IP of the server on which OFSAA is getting installed.

For HIVE installation, you must also have the following:

- HIVE connection credentials (For example: Kerberos connection properties).
- Hostname/IP of the HIVE Server installation

Configure the Schema Creator Utility for RDBMS Installation

Configure the `OFS_<APP PACK>_SCHEMA_IN.xml` file for RDBMS.

Add the Pack specific schema details for the following schema, present in the `OFS_<App Pack>_SCHEMA_IN.xml` file.

- **CONFIG**: This schema holds the entities and other objects required for OFSAA setup configuration information. 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. There can be multiple ATOMIC schemas per OFSAA Instance.

Configure the `OFS_<App Pack>_SCHEMA_IN.xml` File

This section describes how to create database schemas, objects within schemas, and assigning appropriate grants.
Specify the database schemas required for the installation in the `OFS_<APP PACK>_SCHEMA_IN.xml` file. Update the values of the various tags and parameters available in this file before executing the schema creator utility.

This file must be configured only if the database is RDBMS.

To configure the `<APP PACK>_SCHEMA_IN.xml` file:

1. Log in to the system as a non-root user.
2. Navigate to the `<APP PACK>/schema_creator/conf` directory and configure the `<APP PACK>_SCHEMA_IN.xml` file based on the following parameters.

Figure 7-2 Sample OFS_LRS_SCHEMA_IN.xml File

3. Save the file.

> **Note:**
>
> On successful execution of the utility, the passwords entered in the OFS_LRS_SCHEMA_IN.xml file are nullified.

Table 7-2 `OFS_<APP PACK>_SCHEMA_IN.xml` File Parameters

Tag / Attribute Name	Details	Default Value/ Permissible Value
<APP_PACK_ID>	Seeded unique ID for the OFSSAA Application Pack. Do not modify this value.	Seeded
<IS_TCPS>	Enter if the TCPS configuration is required. Modify this to `TRUE` if you require the installer to uptake the configuration.	Seeded, with `FALSE` as the default value.

Table 7-2 (Cont.) OFS_<APP PACK>_SCHEMA_IN.xml File Parameters

Tag / Attribute Name	Details	Default Value/ Permissible Value
<JDBC_URL>	Enter the JDBC URL. You can enter the following JDBC URL types: **a.** RAC/ NON-RAC enabled database connectivity URL. **b.** TCPS RAC/ NON-RAC enabled database connectivity URL provided the <IS_TCPS> tag value is TRUE. **c.** Wallet-enabled JDBC URL. Ensure to add an entry (with SID/ SERVICE NAME) in the tnsnames.ora file on the OFSAA server. The entry must match with the SID/ SERVICE NAME used in the JDBC URL. Ensure that you have configured: **a.** The correct Oracle Wallet with the credentials for stored Sys, Config, and Atomic Users. **b.** The JDBC URL as: jdbc:oracle:thin:/@ For more information on how to configure Oracle Wallets for OFSAA Installation and Data Sources, refer to the OFS Analytical Applications Infrastructure Administration Guide.	**Example 1**: jdbc:oracle:thin:@< DBSERVER IP/ HOST/ IP>:<PORT>:<SID> **Example 2**: jdbc:oracle:thin:@//[HOS T] [:PORT]/ SERVICE **Example 3**: jdbc:oracle:thin:@(DESCRI PTION=(ADDRESS_ LIST=(ADDRESS=(PROT OCOL=TCP)(HOST=[HO ST])(port=[PORT]))(ADD RESS=(PROTOCOL=TCP) (HOST=[HOST])(PORT=[PORT])) (LOAD_ BALANCE=yes)(FAILOV ER=yes))(CONNECT_ DATA=(SERVICE_ NAME=[SERVICE]))) **Example 4**: jdbc:oracle:thin:@//dbhos t.server.com:1521/service 1 **Example 5**: jdbc:oracle:thin:@//dbsho st.server.com:1521/scan-1 **Example 6**: jdbc:oracle:thin:@(DESCRI PTION=(ADDRESS_ LIST=(ADDRESS=(PROT OCOL=TCP) (HOST=dbhost1.server.com) (port=1521)) (ADDRESS=(PROTOCOL=TCP)(H OST=dbhost2.s erver.com) (PORT=1521))(LOAD_BALANCE=yes) (FAILOV ER=yes))(CONNECT_ DATA=(SERVICE_NAME=service1)))

Table 7-2 (Cont.) OFS_<APP PACK>_SCHEMA_IN.xml File Parameters

Tag / Attribute Name	Details	Default Value/ Permissible Value
		Example 7: <JDBC_URL>jdbc:oracle:thin:@(DESCRIPTIO N = (ADDRESS = (PROTOCOL =TCPS)(HOST = dbhost.server.com)(PORT = 2484)) (CONNECT_DATA =(SERVER = DEDICATED) (SERVICE_NAME=SERVICEID)) (security=(ssl_server_cert_dn=CN=dbhost))) **Example 8**: jdbc:oracle:thin:/@
<JDBC_DRIVER>	This driver's name is seeded by default. Only JDBC Thin Driver is supported. Do not modify this value.	**Example**: oracle.jdbc.driver.OracleDriver
<HOST>	Enter the Host name/ IP Address of the system on which you are installing the OFSAA components.	Host Name/ IP Address
<SETUPINFO>/PREFIX_SCHEMA_NAME	(Optional). Identifies whether the value specified in <SETUPINFO>/NAME attribute must be prefixed to the schema name. The default value is YES.	YES or NO
<SETUPINFO>/NAME	Enter the acronym for the type of implementation. This information is displayed in the OFSAA Home Page. On executing the schema creator utility, this value is prefixed with each schema name. For example: dev_ofsaaconf, uat_ofsaatm. This name appears in the OFSAA Landing Page as Connected To: xxxx.	Accepts strings with a minimum length of two and a maximum of four. Example: DEV, SIT, PROD
<PASSWORD>/DEFAULT*	(Optional). Enter the password if you want to set a default password for all schemas. You also must set the APPLYSAMEFORALL attribute as Y to apply the default password for all the schemas. On successful execution of the utility, the entered password in the OFS_<APP PACK>_SCHEMA_IN.xml file is cleared.	The maximum length allowed is 30 characters. Special characters are not allowed.

Table 7-2 (Cont.) OFS_<APP PACK>_SCHEMA_IN.xml File Parameters

Tag / Attribute Name	Details	Default Value/ Permissible Value
<PASSWORD>/ APPLYSAMEFORALL	If 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. Setting this attribute value is mandatory if the DEFAULT attribute is set.	Default N Permissible: Y or N Enter Y if you want to apply the password specified in the DEFAULT attribute for all the schemas. If you enter as N, you must provide individual passwords for all schemas.
<SCHEMA>/ TYPE	The different types of schemas that are supported in this release are ATOMIC, CONFIG, SANDBOX, and ADDON. By default, the schemas types are seeded based on the Application Pack. Only One CONFIG schema can exist in the file. Do not edit this attribute value. This schema identifies as the CONFIGURATION schema that holds the OFSAA setup detains and other Metadata information. Multiple ATOMIC/ SANDBOX/ADDON schemas can exist in the file.	ATOMIC/CONFIG/SANDBOX/ADDON SANDBOX and ADDON schemas do not apply to OFSAAI.
<SCHEMA>/ NAME	The schemas' names are seeded based on the Application Pack by default. You can edit the schema names if required. The Schema Name will have a prefix of the SETUPINFO/NAME attribute. SCHEMA NAME must be the same for all the ATOMIC Schemas of the applications within an Application Pack. SETUPOINFO/NAME attribute value is prefixed to the schema name being created. For example, if a name is set as ofsaatm and setupinfo as uat, then schema being created is uat_ofsaatm. NAME must be the same where APP_GRP=1 for all SCHEMA tags (Not applicable for this Application Pack).	The permissible length is 15 characters and only alphanumeric characters are allowed. No special characters allowed except underscore '_'.
<SCHEMA>/ PASSWORD	(Optional). Enter the password of the schema to be created. If this attribute is left blank, then the password specified in the <PASSWORD>/ DEFAULT attribute is applied as the Schema Password. It is mandatory to enter the password if you have set the <PASSWORD>/ APPLYSAMEFORALL attribute as N.	The maximum length allowed is 30 characters. Special characters are not allowed.

Table 7-2 (Cont.) OFS_<APP PACK>_SCHEMA_IN.xml File Parameters

Tag / Attribute Name	Details	Default Value/ Permissible Value
<SCHEMA>/ APP_ID	The Application ID is seeded based on the Application Pack by default. Identifies the Application/ Product for which the schema is being created. Do not edit this attribute value.	Unique Seeded Value
<SCHEMA>/ DEFAULTTABLESPACE	(Optional). Enter the available default tablespace for DB User. If this attribute is left blank, then USERS is set as the default tablespace. Modify this value to associate any valid tablespace with the schema.	Default USERS Permissible Any existing valid tablespace name.
<SCHEMA>/ TEMPTABLESPACE	(Optional). Enter the available temporary tablespace for DB User. If this attribute is left bank, TEMP is set as the default tablespace. Modify this value to associate any valid tablespace with the schema.	Default TEMP Permissible Any existing valid temporary tablespace name.
<SCHEMA>/ QUOTA	Enter the quota to be set on the DEFAULTTABLESPACE attribute for the schema/ user. By default, the quota size is set to 500M. Minimum: 500M or Unlimited on default Tablespace. Modify this value to grant the specified quota on the mentioned tablespace to the user.	**Example**: 600M/ m 20G/ g UNLIMITED/ unlimited
<SCHEMA>/ INFODOM	(Optional). Enter the name of the Information Domain to associate this schema. The schema creator utility automatically derives an Information Domain Name based on the Application Pack if no value is specified for this attribute.	Permissible length is 16 characters and only alphanumeric characters are allowed. No special characters are allowed.
<ADV_SEC_OPTIONS>/	(Optional). Parent tag to hold Advance Security Options. Uncomment the tag and edit if you want to add security options. For example, TDE and Data Redact. For details, see the example in the comments for the <TABLESPACE>/ENCRYPT tag.	
<ADV_SEC_OPTIONS>/ TDE	(Optional). Tag to enable/disable TDE. Ensure this tag is not commented if you have uncommented <ADV_SEC_OPTIONS>	The default is FALSE. To enable TDE, set this to TRUE.
<ADV_SEC_OPTIONS>/ DATA_REDACT	(Optional). Tag to enable/disable the Data Redaction feature. Ensure this tag is not commented if you have uncommented <ADV_SEC_OPTIONS>	The default is FALSE. To enable DATA_REDACT, set this to TRUE

Table 7-2 (Cont.) OFS_<APP PACK>_SCHEMA_IN.xml File Parameters

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

Table 7-2 (Cont.) OFS_<APP PACK>_SCHEMA_IN.xml File Parameters

Tag / Attribute Name	Details	Default Value/ Permissible Value

<TABLESPACE> / ENCRYPT	Specifies if the tablespace(s) must be encrypted using TDE.
	Set to ON to ensure that the tablespaces when created are encrypted using TDE.
	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 is shown with encryption ON.
	
	`<ADV_SEC_OPTIONS>`
	`<OPTION NAME="TDE"`
	`VALUE="FALSE"/>`
	`<OPTION NAME="DATA_REDACT"`
	`VALUE="FALSE" />`
	`</ADV_SEC_OPTIONS>`
	`<TABLESPACES>`
	`<TABLESPACE`
	`NAME="OFS_AAI_TBSP_1"`
	`VALUE="TS_USERS1" DATAFILE="/`
	`scratch/ora19c/app/oracle/orada`
	`ta/OFSPQA19cDB/ts_users1.dbf"`
	`SIZE="500M" AUTOEXTEND="ON"`
	`ENCRYPT="ON" />`
	`<TABLESPACE`
	`NAME="OFS_AAI_TBSP_2"`
	`VALUE="TS_USERS2" DATAFILE="/`
	`scratch/ora19c/app/oracle/orada`
	`ta/OFSPQA19cDB/ts_users2.dbf"`
	`SIZE="500M" AUTOEXTEND="ON"`
	`ENCRYPT="ON" />`
	`</TABLESPACES>`
	
	`<SCHEMAS>`
	`<SCHEMA TYPE="CONFIG"`
	`NAME="ofsaaconf" PASSWORD=""`
	`APP_ID="OFS_AAI"`
	`DEFAULTTABLESPACE="##OFS_AAI_TB`
	`SP_1##" TEMPTABLESPACE="TEMP"`
	`QUOTA="unlimited"/>`
	`<SCHEMA TYPE="ATOMIC"`
	`NAME="ofsaaatm" PASSWORD=""`
	`APP_ID="OFS_AAAI"`
	`DEFAULTTABLESPACE="##OFS_AAI_TB`
	`SP_2##" TEMPTABLESPACE="TEMP"`
	`QUOTA="unlimited"`
	`INFODOM="OFSAAAIINFO"/>`
	`</SCHEMAS>`
		ON or OFF

Configure the Schema Creator Utility for HDFS Schema

Configure the `<APP Pack>_SCHEMA_BIGDATA_IN.xml` file for HDFS installation.

Add the pack specific schema details for the following schema, present in the `<APP Pack>_SCHEMA_BIGDATA_IN.xml` file.

- **CONFIG**: This schema holds the entities and other objects required for OFSAA setup configuration information. 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. There can be multiple DATADOM schemas per OFSAA Instance. This schema is created only in RDBMS. It has only platform entities that hold the metadata details. However, it does not hold the data model entities.
- **DATADOM**: This schema holds data model entities. One DATADOM schema is attached to one Information Domain. There can be multiple DATADOM schemas per OFSAA Instance.

Configure the <APP Pack>_SCHEMA_BIGDATA_IN.xml file

The primary steps in OFSAA Applications installation involve creating HIVE schemas and objects within the schemas.

The `<APP PACK>_SCHEMA_BIGDATA_IN.xml` file contains details of the various application schemas. Update the values of the various tags and parameters available in this file before executing the schema creator utility.

This file must be configured only if the installation is for HDFS. This file is not required to be configured for an RDBMS ONLY target installation.

Table 7-3 <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<APP_PACK_ ID>	Seeded unique ID for the OFSAA Application Pack DO NOT modify this value.	Seeded
<IS_TCPS>	Enter if the TCPS configuration is required. Modify this to `TRUE` if you require the installer to uptake the configuration.	Seeded, with `FALSE` as the default value.

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<JDBC_URL>	Enter the JDBC URL You can enter RAC/ NON-RAC enabled database connectivity URL.	**Example 1**: jdbc:oracle:thin:@<HOST/ IP>:<PORT>:<SID> **Example 2**: jdbc:oracle:thin:@//[HOS T][:PORT]/ SERVICE For an HDFS ONLY target installation, this URL must be of the RDBMS instance that hosts the Application's METADOM. **Example 3**: jdbc:oracle:thin:@(DESCRI PTION=(ADDRESS_ LIST=(ADDRESS=(PROT OCOL=TCP)(HOST=[HO ST])(port=[PORT]))(ADD RESS=(PROTOCOL=TCP) (HOST=[HOST])(PORT=[PORT]))(LOAD_ BALANCE=yes)(FAILOV ER=yes))(CONNECT_ DATA=(SERVICE_ NAME=[SERVICE]))) **Example 4**: jdbc:oracle:thin:@// dbhos t.server.com:1521/service 1 **Example 5**: jdbc:oracle:thin:@//dbsho st.server.com:1521/scan-1 **Example 6**: jdbc:oracle:thin:@(DESCRI PTION=(ADDRESS_ LIST=(ADDRESS=(PROT OCOL=TCP)(HOST=dbhost 1.server.co m)(port=1521))(ADDRESS=(PROTOCOL=TCP) (HOST=dbhost2 .s erver.com)(PORT=1521))(LOAD_ BALANCE=yes)(FAILOV ER=yes))(CONNECT_

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
		DATA=(SERVICE_ NAME=service1)))
<JDBC_ DRIVER>	By default, this driver's name is seeded. Only JDBC Thin Driver is supported. DO NOT modify this value.	**Example**: oracle.jdbc.driver.OracleDriver
<HOST>	Enter the Hostname/ IP Address of the system on which you are installing the OFSAA components.	Host Name/ IP Address
<SETUPINFO>/ PREFIX_ SCHEMA_ NAME	(Optional). Identifies if the value specified in <SETUPINFO>/NAME attribute must be prefixed to the schema name. The default value is YES.	YES or NO
<SETUPINFO>/ NAME	Enter the acronym for the type of implementation. This information is displayed in the OFSAA Home Page. This name appears in the OFSAA Landing Page as Connected To: xxxx On executing the schema creator utility, this value is prefixed with each schema name. **For example**: dev_ ofsaaconf, uat_ofsaaatm.	Accepts strings with a minimum length of two and a maximum of four. **Example**: DEV, SIT, PROD
<PASSWORD>/ DEFAULT*	(Optional). Enter the password if you want to set a default password for all schemas. You also must set the APPLYSAMEFORALL attribute as Y to apply the default password for all the schemas. Applies only to the RDBMS type METADOM schema(s).	The maximum length allowed is 30 characters. Special characters are not allowed.
<PASSWORD>/ APPLYSAMEFORALL	Enter as Y if you want to apply the password specified in the DEFAULT attribute for all the schemas. If you enter as N, you must provide individual passwords for all schemas. If you have entered Y in the APPLYSAMEFORALL attribute and also have specified individual passwords for all the schemas, then the specified individual passwords will take precedence. Setting this attribute value is mandatory If the DEFAULT attribute is set. Applies only to the RDBMS type METADOM schema(s).	Default N Permissible Y or N

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<SCHEMAS>/ TYPE=RDBMS	Identifies the RDBMS schema details. In an HDFS ONLY target installation, the Application's METADOM (that hosts the metadata) for an application is stored in RDBMS schema and the data model entities of the application are stored in the DATADOM (which are on Hive).	Default names for schemas within the pack are derived in absence of any value specified.
<SCHEMA>/ TYPE	The different types of schemas that are supported in this release are ATOMIC, CONFIG, SANDBOX, and ADDON. By default, the schemas types are seeded based on the Application Pack. Do not edit this attribute value. Only One CONFIG schema can exist in the file. This schema identifies as the CONFIGURATION schema that holds the OFSAA setup details and other metadata information. Multiple ATOMIC/ SANDBOX/ ADDON schemas can exist in the file. ATOMIC schema refers to the METADOM within the Information Domain schema. SANDBOX schema refers to the SANDBOX schema. ADDON schema refers to another miscellaneous schema (not applicable for this Application Pack).	ATOMIC/CONFIG/SANDBOX/ADDON The SANDBOX AND ADDON schemas do not apply to the OFSAAAI Application Pack.
<SCHEMA>/ NAME	By default, the schema's names are seeded based on the Application Pack. You can edit the schema names if required. The Schema Name will have a prefix of the `SETUPINFO/ NAME` attribute. `SCHEMA NAME` must be the same for all the ATOMIC Schemas of applications within an Application Pack. **For example**, if the name is set as `ofsaaatm` and setupinfo as `uat`, then the schema being created would be `uat_ofsaaatm`. `NAME` must be the same where `APP_GRP=1` for all SCHEMA tags (Not applicable for this Application Pack).	The permissible length is 15 characters and only alphanumeric characters allowed. No special characters allowed except underscore '_'.
<SCHEMA>/ PASSWORD	(Optional). Enter the password of the schema to be created. If this attribute is left blank, then the password specified in the `<PASSWORD>/DEFAULT` attribute is applied as the Schema Password. It is mandatory to enter the password if you have set the `<PASSWORD>/ APPLYSAMEFORALL` attribute as N.	The maximum length allowed is 30 characters. Special characters are not allowed.

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<SCHEMA>/ APP_ID	By default, the Application ID is seeded based on the Application Pack. Identifies the Application/ Product for which the schema is being created. Do not edit this attribute value.	Unique Seeded Value
<SCHEMA>/ DEFAULT TABLESPACE	(Optional). Enter the available default tablespace for DB User. If this attribute is left blank, then `USERS` is set as the default tablespace. Modify this value to associate any valid tablespace with the schema.	Default USERS Permissible Any existing valid tablespace name.
<SCHEMA>/ TEMPTABLESPACE	(Optional). Enter the available temporary tablespace for the DB User. If this attribute is left blank, then TEMP is set as the default tablespace. Modify this value to associate any valid tablespace with the schema.	Default TEMP Permissible Any existing valid temporary tablespace name.

<SCHEMA>/ QUOTA	(Optional). 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.
	Modify this value to grant the specified quota on the mentioned tablespace to the user.
		Example, `600M/m`
		`20G/g`
		`UNLIMITED/unlimited`

<SCHEMA>/ INFODOM	(Optional). Enter the name of the Information Domain to associate this schema. The schema creator utility automatically derives an Information Domain Name based on the Application Pack if no value is specified for this attribute.	Permissible length is 16 characters and only alphanumeric characters allowed. No special characters allowed.
<SCHEMAS>/ TYPE=HDFS	Type of schemas being created. Refers to the DATADOM of the Application Pack being installed.	
<HIVE_SERVER_HOST>	IP/HostName of the server where HIVE is installed.	
<HIVE_LIB_PATH>	The directory path where the HIVE related drivers/jar files are copied. Manually copy the jars mentioned in the Copy_Jars_to_OFSAA_Installation_Folder and Copy_KEYTAB_and_KRB5_Files_in_OFSAAI sections. Select the appropriate versions of the files.	

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<SCHEMA>/NAME	By default, the schema names are seeded based on the Application Pack. You can edit the schema names if required. The Schema Name will have a prefix of the `SETUPINFO/ NAME` attribute. The Schema Name must not be the same as the Schema Name specified for the ATOMIC Schema Type.	The permissible length is 20 characters and only alphanumeric characters allowed.
<SCHEMA>/TYPE	Identifies the type of schema where the data model entities reside. DO NOT modify this value.	By default, the `TYPE` attribute in this tag is set to `DATADOM`.
<SCHEMA>/DB TYPE	Identifies the type of driver to be used for the connection. In upcoming releases, the type value can be HIVE/ IMPALA, etc.	By default, the only supported type is HIVE in this release.
<SCHEMA>/ <PROPERTY>/ COMMENT	(Optional). COMMENTS for the HIVE schema.	
<SCHEMA>/ <PROPERTY>/ LOCATION	(Optional). You can optionally specify a location for the table data.	
<CONNECTION_PROPERTIES>/ <PROPERTY>/ JDBC_DRIVER	HIVE JDBC driver details. The default HiveServer 2 driver name.	`com.cloudera.hive.j dbc4.HS2Driver`
<CONNECTION_PROPERTIES>/ <PROPERTY>/ JDBC_URL	Enter the HIVE JDBC URL. Specify the Hive JDBC URL to connect to the Hive Server. **For example**, `jdbc:hive2://ofss-****:10000/default;principal=hive/ofssxxx@xxx.COM`	Valid Hive JDBC URL to be specified.

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<CONNECTION_PROPERTIES>/<PROPERTY>/AUTH_TYPE	Authentication Type. Only "Kerberos with keytab" based authentication supported in this release.	Permissible values: `KERBEROS_WITH_KEYTAB`
<CONNECTION_PROPERTIES>/<PROPERTY>/AUTH_ALIAS	Alias name for authentication credentials. An Alias name mapping to a principal and password combination specified in the following tags.	
<CONNECTION_PROPERTIES>/<PROPERTY>/PRINCIPAL	Authentication principal name Principal name used in authentication to connect to the Hive Server. **For example**: `hive/ofss-xxx@xxx.COM`	
<CONNECTION_PROPERTIES>/<PROPERTY>/PASSWORD	Authentication password Password used in authentication to connect to the Hive Server.	
<CONNECTION_PROPERTIES>/<PROPERTY>/KRB_GSS_JAAS_FILE_NAME	A keytab file containing pairs of Kerberos principals and an encrypted copy of that principal's key. This file must be copied to the location specified in `<HIVE_LIB_PATH>`.	

Table 7-3 (Cont.) <APP Pack>_SCHEMA_BIGDATA_IN.xml File Parameters

Tag Name/ Attribute Name	Details	Default Value/ Permissible Value
<CONNECTION_PROPERTIES>/<PROPERTY>/KRB_REALM_FILE_NAME	REALM configuration file. This file must be copied to the location specified in <HIVE_LIB_PATH>.	

Execute the Schema Creator Utility

Execute the schema creator utility in offline mode, online mode, TCPS mode, or while installing the applications pack.

Based on the selected option for running the OFSAA Application Pack installer, select the appropriate execution option for the schema creator utility from the following alternatives:

- Execute the Schema Creator Utility in Offline Mode
- Execute the Schema Creator Utility in Online Mode
- Execute the Schema Creator Utility in TCPS Mode
- Execute the Schema Creator Utility while Installing Subsequent Applications Pack

After creating the schema, proceed to Configure the OFSAAI_InstallConfig.xml File.

> **Note:**
>
> If upgrading in an Application-on-Application scenario, you must provide the same schema details you provided earlier.

Execute the Schema Creator Utility in Offline Mode

Execute the Schema Creator utility in the offline mode.

In the Offline mode, the schema creator utility generates an SQL script with all the required DDLs for Users, Objects, and Grants. This script must be executed by the DBA on the appropriate database identified for OFSAA usage. If you do not have the SYSDBA privileges, you can execute the Schema Creator Utility in Offline mode and generate the script file that contains the Schemas, Objects, and Grants information. Subsequently, an SYSDBA user can execute the script file manually. To run the OFSAA Application Pack installer in Silent mode, it is mandatory to execute the schema creator utility with `-s` option.

To execute the utility in Offline mode, you must be 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 users are required. Grants assigned through Roles are not supported.

To execute the schema creator utility in the offline mode:

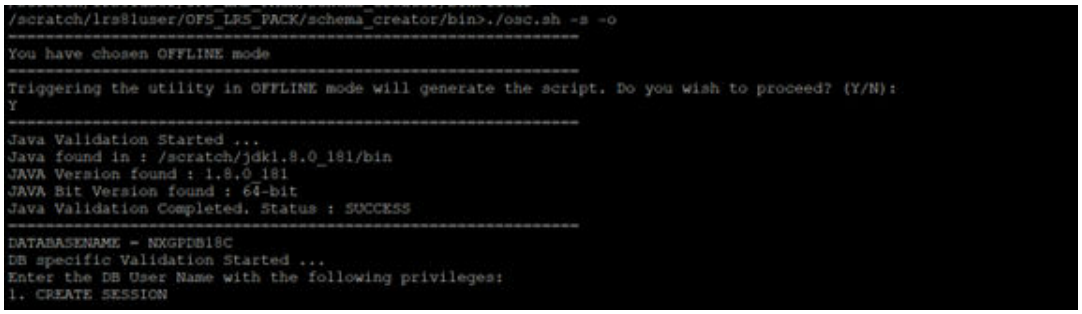
1. Log in to the system as a non-root user.
2. Navigate to the path: `OFS_<APP_PACK>_PACK/schema_creator/bin`
3. Execute the `osc.sh` file using the command: `./osc.sh -s -o`

   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).
   ```

4. Enter **Y** to proceed.
5. Enter the **DB Username** with **SELECT** privileges.
6. Enter the **User Password**.

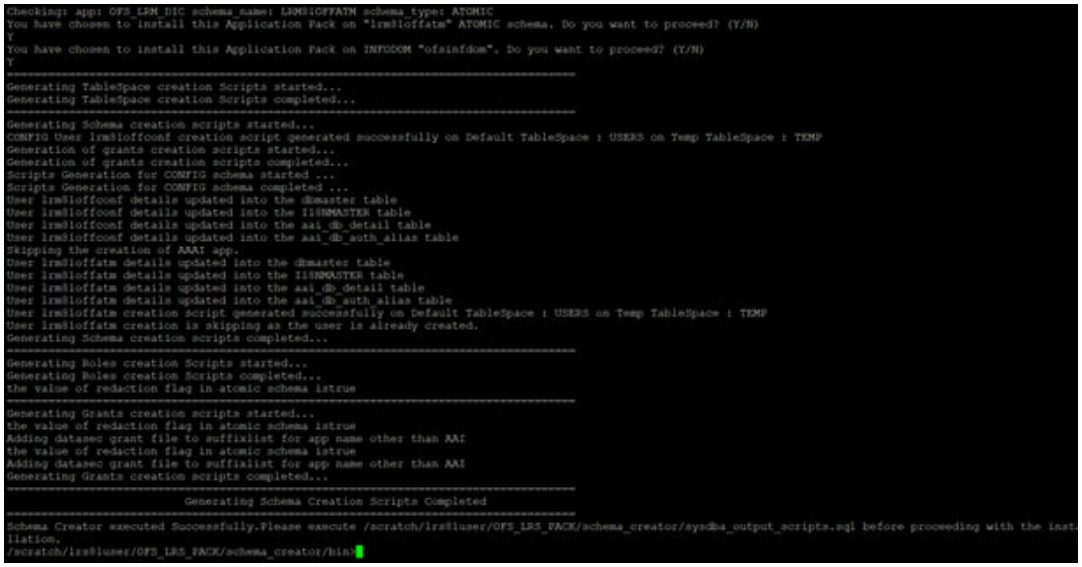
Figure 7-3 Schema Creation in Offline Mode



7. The console runs the initial validation checks and displays the following message:

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

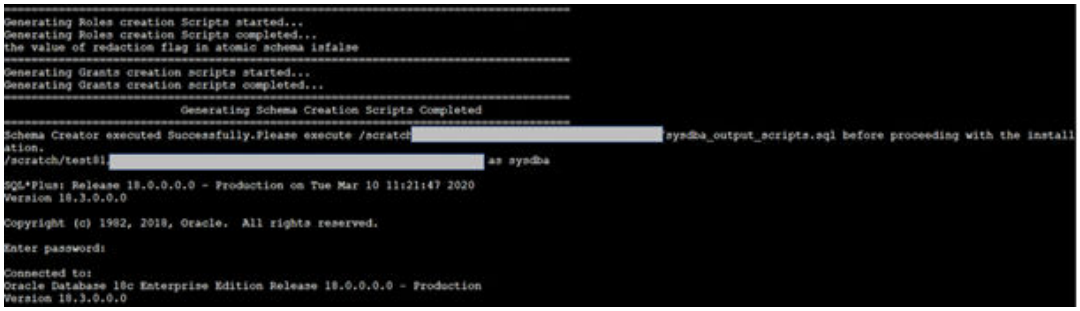
Figure 7-4 Schema Creation in Offline Mode Script Generation



8. Enter Y to start the script generation. The following message is displayed:

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

Figure 7-5 Schema Creation in Offline Mode Successful



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

`Schema Creator executed successfully. Please execute scratch/ofsaaapp/OFS_LRS_PACK/schema_creator/sysdba_output_scripts.sql before proceeding with the installation.`

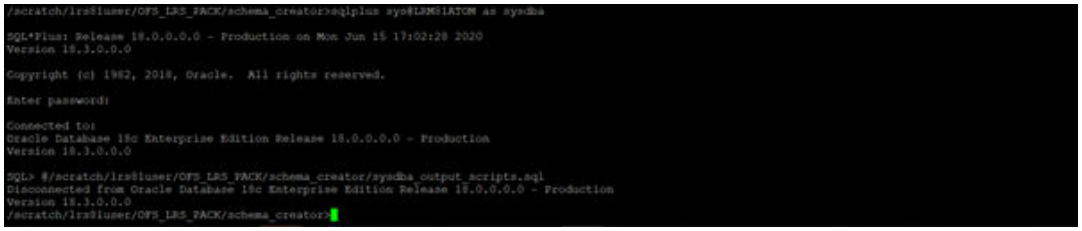
Additionally, if you have configured the `<<APP PACK>>_SCHEMA_BIGDATA_ IN.xml` file, a file called `hive_output_scripts.hql` is also created in the `/scratch/ofsaaapp/OFS_AAAI_PACK/schema_creator` directory.

> **Note:**
>
> If there are any errors during the SQL script execution, reconfigure the `<PACK>_SCHEMA_IN.xml` and/or `<APP_PACK>_SCHEMA_ BIGDATA_IN.xml` files and repeat steps in this procedure to execute the utility. This regenerates the scripts with the correct information.

> **Note:**
>
> If there are any errors during the SQL script execution, reconfigure the `OFS_LRS_SCHEMA_IN.xml`, and repeat steps in this procedure to execute the utility. This regenerates the scripts with the correct information.

9. Navigate to the `OFS_AAAI_PACK/schema_creator` `OFS_LRS_PACK/schema_creator` directory.
10. Log in to `SQLPLUS` as a user having SYSDBA Privileges.

Figure 7-6 Schema Creation in Offline Mode – Execute sysdba_output_scripts.sql



11. Execute the sysdba_output_scripts.sql file using the following command:

    `SQL>@sysdba_output_scripts.sql`
    Alternatively, you can copy the sysdba_output_scripts.sql file and SQLScripts directory to a remote server and execute the sysdba_output_scripts.sql file, after providing appropriate execute permissions.
12. Make a TNS entry for the new users created. For details, see #unique_57.

> **Note:**
>
> See the sysdba_output_scripts.log file for execution status. If there are any errors, contact My Oracle Support. If there are no errors in the execution, the log file is empty.

The result of this task is that the `<PACK> _SCHEMA_OUT.XML` file is generated. Do not modify this file.

As a result of this task the `OFS_LRS_SCHEMA_OUTPUT.XML` file is generated. Do not modify this file.

After creating the schema, proceed to Configure the OFSAAI_InstallConfig.xml File section.

Execute the Schema Creator Utility in Online Mode

Execute the Schema Creator utility in the online mode.

In online mode, the utility connects to the database and executes the DDLs for Users, Objects, and Grants. If you have SYSDBA privileges you can execute the Schema Creator Utility in Online mode and thereby create the Users, Objects, and Grants during the execution process. To execute the utility in the Online mode, you must connect as "<User> AS SYSDBA".
If you want to run the OFSAA Application Pack Installer in Online mode, it is mandatory to execute the schema creator utility with -s option.

To execute the utility with -s option in online mode:

1. Edit the file `OFS_AAAI_PACK/schema_creator/conf/OFS_<APP PACK>_SCHEMA_IN.xml` in a text editor. See Configure OFS_<App Pack>_SCHEMA_IN.xml for values to modify in the XML file.
2. Execute the utility with -s option. For Example: `./osc.sh -s`

Figure 7-7 Schema Creation in Online Mode

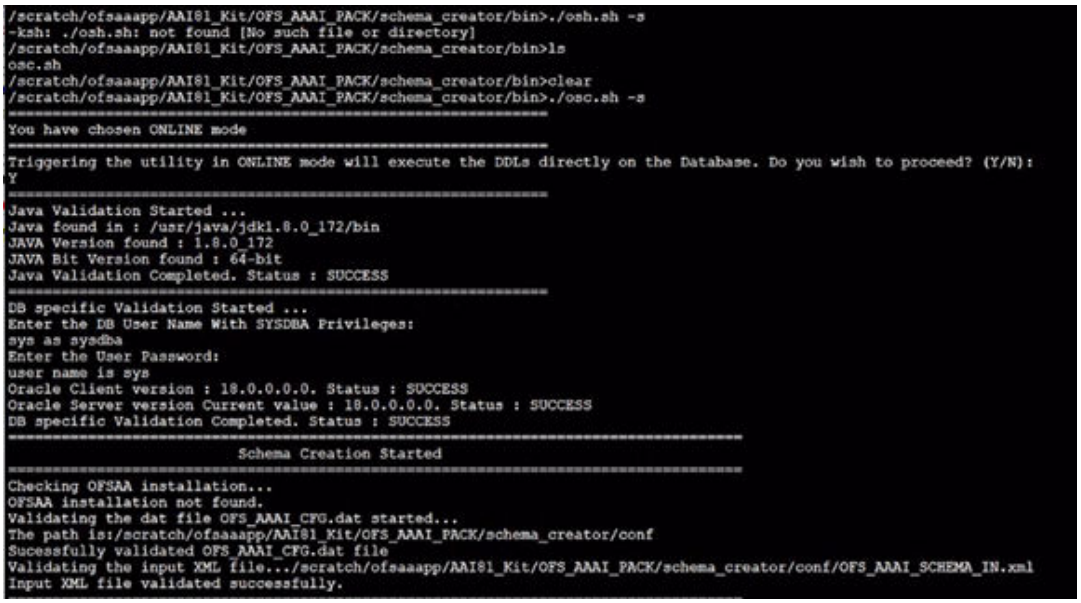
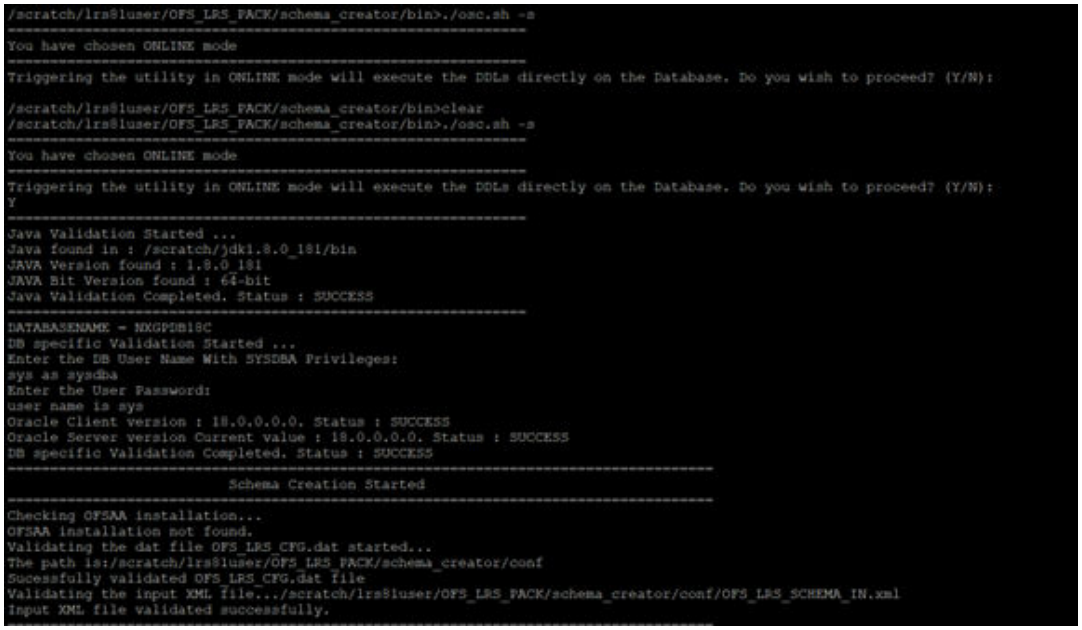


Figure 7-8 Schema Creation in Online Mode

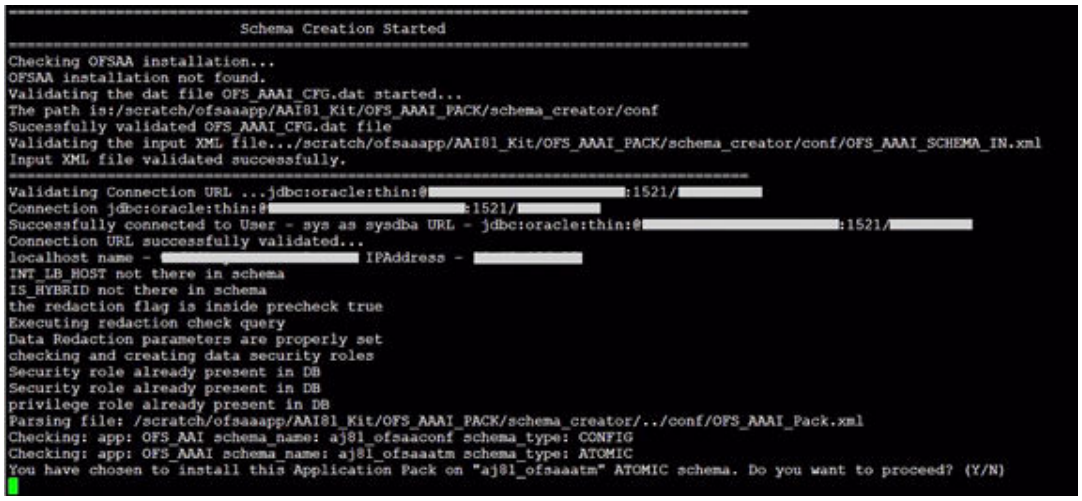


3. The following message is displayed:

   `You have chosen ONLINE mode. Triggering the utility in ONLINE mode will execute the DDLs directly on the Database. Do you wish to proceed? (Y/y or N/n).`

4. Enter `Y` to proceed.

Figure 7-9 Schema Creation in Online Mode – DDL Execution

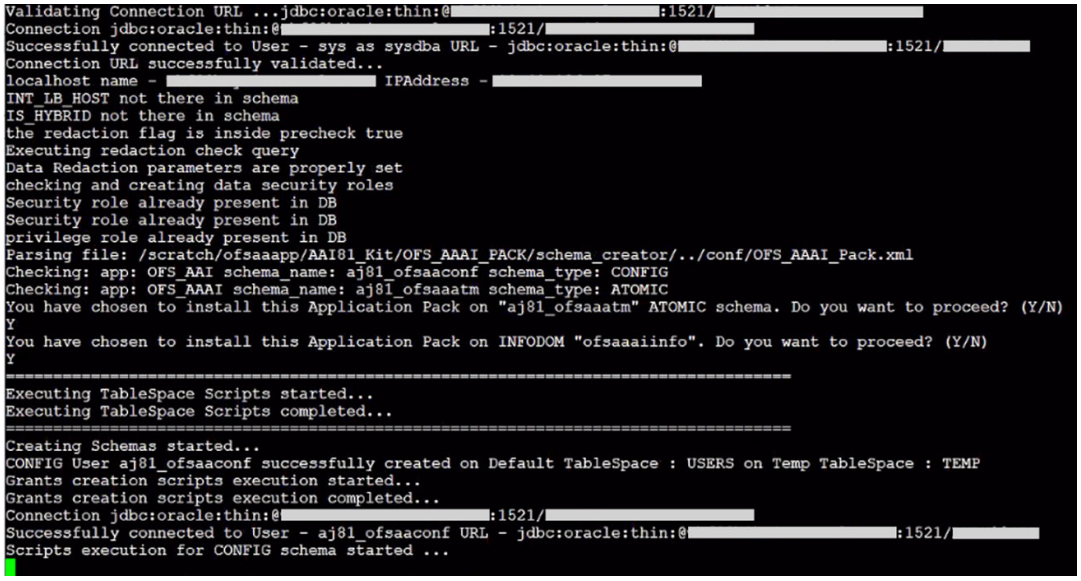


5. The following message is displayed:

   `You have chosen to install this application pack on INFODOM "<INFODOM_NAME>". Do you wish to proceed? (Y/y or N/n).`

6. Enter `Y` to proceed.

Figure 7-10 Schema Creation in Online Mode – Infodom Confirmation



7. After Schema creation is successful, proceed to configure the OFSAAI_InstallConfig.xml file.

Figure 7-11 Schema Creation in Online Mode –Successful

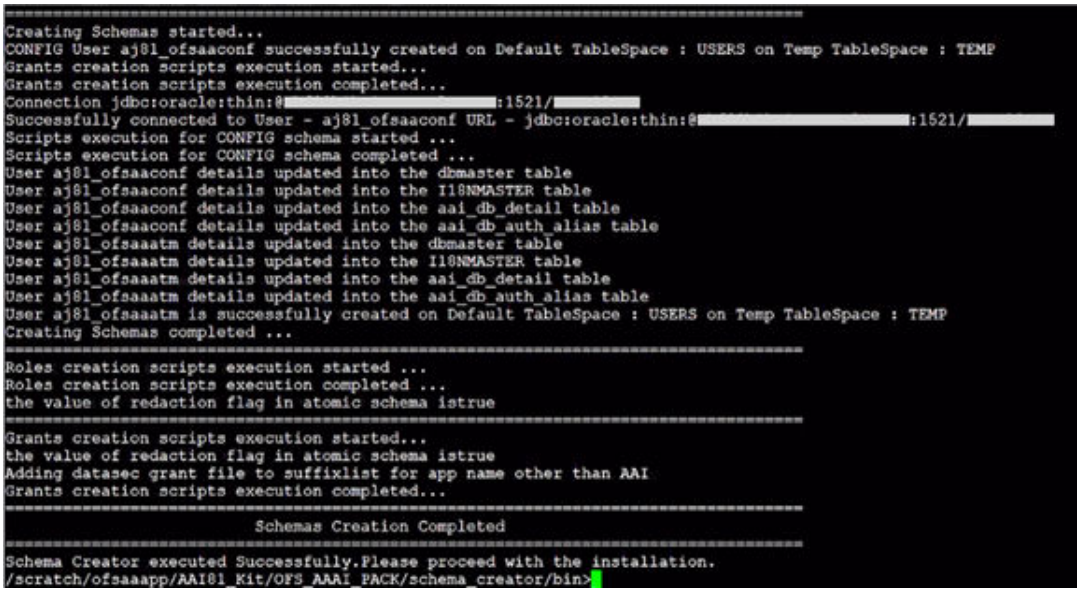
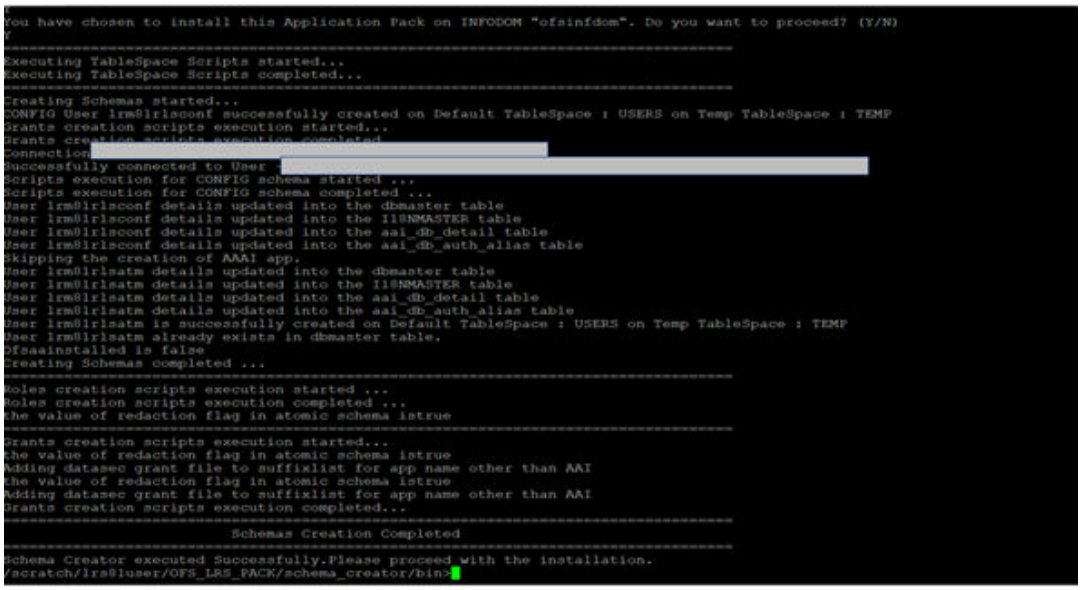


Figure 7-12 Schema Creation in Online Mode –Successful



As a result of this task the OFS_<APP_PACK>_SCHEMA_OUTPUT.XML file is generated. Do not modify this file.

Configure the OFSAAI_InstallConfig.xml File

Set up the `OFSAAI_InstallConfig.xml` file according to the desired configuration.

To configure the `OFS_InstallConfig.xml` file:

1. Navigate to the `OFS_<APP_PACK>_PACK/OFS_<APP_PACK>/conf/` directory.
2. Open the `OFS<APP_PACK>_InstallConfig.xml` file and configure it as described in the table below.

   You must manually set the **InteractionVariable** parameter values as mentioned in the table. If a value is not applicable, enter NA. Ensure that the value is not entered as NULL.

Table 7-4 OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable 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 are deployed. Set the following numeric value depending on the type of web application server: • Apache Tomcat = 1 • IBM WebSphere Application Server = 2 • Oracle WebLogic Server = 3 For example, `<InteractionVariablename="WEBAPPSERVERTYPE">3 </InteractionVari able>`	Yes

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable Name	Significance and Expected Value	Mandatory
InteractionGroup name="OFSAA Infrastructure Server Details"		
DBSERVER_IP	Identifies the host name or IP address of the system on which the Database Engine is hosted. **Note:** For RAC Database, the value must 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 must be exactly the same as it is mentioned in `JDBC_URL`. For example, `<InteractionVariable name="ORACLE_SID/SERVICE_NAME">ofsaser</ InteractionVariable>`	Yes
ABS_DRIVER_PATH	Identifies the directory where the JDBC driver (`ojdbc<version>.jar`) exists. This is typically the `$ORACLE_HOME/jdbc/lib` directory. For example, `<InteractionVariable name="ABS_DRIVER_ PATH">">/oradata6/revwb7/ oracle </InteractionVariable>` **Note:** See Hardware and Software Requirements to identify the correct `ojdbc<version>.jar` file version to be copied.	Yes
InteractionGroup name="OLAP Detail		

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable Name	Significance and Expected Value	Mandatory
OLAP_SERVER_IMPLEMENTATION	Identifies whether the OFSAA Infrastructure OLAP component must be configured. It depends on whether you intend to use the OLAP feature. The following numeric value must be set depending on the choice: • YES: 1 • NO: 0 **Note:** If the value for `OLAP_SERVER_IMPLEMENTATION` is set to 1, the installer checks if the following environment variables are set in the `.profile` file: • ARBORPATH • HYPERION_HOME • ESSBASEPATH	No
InteractionGroup name="SFTP Details"		
SFTP_ENABLE	Identifies if the SFTP (Secure File Transfer Protocol) feature is to be enabled. The following numeric value must be set depending on the choice: • SFTP: 1 • FTP: 0 **Note:** The default value for `SFTP_ENABLE` is **1**, which signifies that SFTP is used. Oracle recommends using SFTP instead of FTP because SFTP is more secure. However, you can ignore this recommendation and use FTP by setting `SFTP_ENABLE` to **0**. You can change this selection later from the OFSAAI administration interface. Set `SFTP_ENABLE` to **-1** to configure ftpshare and weblocal path as a local path mounted for the OFSAAI server.	Yes
FILE_TRANSFER_PORT	Identifies the port used for the file transfer service. The default value specified is **22** (SFTP). Specify the value as **21** or any other PORT value if the value for `SFTP_ENABLE` is **0**. For example, `<InteractionVariable name="FILE_TRANSFER_ PORT">21</ InteractionVariable>`	Yes
InteractionGroup name="Locale Detail"		
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

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable Name	Significance and Expected Value	Mandatory
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, ensure that the port value is in the range 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 the value for `HTTPS_ENABLE` is set to **1**, ensure that you have a valid certificate available from a trusted CA and it is configured on your web application server.		
HTTPS_ENABLE	Identifies whether the UI must be accessed using HTTP or HTTPS scheme. The default value is set to 0. The numeric value must be set depending on the following options: • YES: 1 • NO: 0 For example, `<InteractionVariable name="HTTPS_ENABLE">0</InteractionVariable>`	Yes
WEB_SERVER_IP	Identifies the HTTP Server IP/ Host name or Web application server IP/ Host name, to be used to access the UI. This IP is typically the HTTP Server IP. If a separate HTTP Server is not available, then the value must be Web application server IP/Host name. For example, `<InteractionVariable name="WEB_SERVER_ IP">10.11.12.13</InteractionVariable>` or `<InteractionVariable name="WEB_SERVER_IP">myweb.server.com</InteractionVariable>`	No
WEB_SERVER_PORT	Identifies the Web Server Port, which is typically 80 for non SSL and 443 for SSL. If a separate HTTP Server exists, the port value must be the value configured for the Web Server. **Warning**: The installer will not accept the port value as: • 80, if the HTTPS_ENABLE variable is 1 • 443, if the HTTPS_ENABLE variable is 0 For example, `<InteractionVariable name="WEB_SERVER_PORT">80</InteractionVariable>`	No

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable Name	Significance and Expected Value	Mandatory
CONTEXT_NAME	Identifies the web application context name which is used to build the URL to access the OFSAA application. You can identify the context name from the following URL format: `<scheme>://<host>:<port>/<context-name>/login.jsp` Example: `https://myweb:443/ofsaadev/login.jsp` For example, `<InteractionVariable name="CONTEXT_NAME">ofsaadev</InteractionVariable>`	Yes
WEBAPP_CONTEXT_PATH	Identifies the absolute path of the exploded EAR file on the web application server. • For Tomcat, specify the Tomcat directory path till /webapps. For example, `/oradata6/ revwb7/tomcat/webapps/`. • For WebSphere, specify the WebSphere path as `<WebSphere profile directory>/installedApps/<NodeCellName>`. For example, `/data2/test//WebSphere/AppServer/profiles/<Profile_Name>/installedApps/aiximfNode01Cell`, where aix-imf is the Host name. • For WebLogic, specify the WebLogic home directory path. For example, `/<WebLogic home directory path>/bea/wlserver_10.3` **Note:** For WebLogic, the value specified for this attribute is ignored and the value provided against the attribute `WEBLOGIC_DOMAIN_HOME` is considered.	Yes
WEB_LOCAL_PATH	Identifies the absolute path to any directory on the web application server that can hold temporary files, which are uploaded as part of the usage of the application. Set this in the FTPSHARE location. **Note:** During a clustered deployment, ensure that this path and the directory are the same on all the nodes.	Yes
InteractionGroup name="Weblogic Setup Details"		

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable 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 WEBAPPSERVER TYPE is set as 3 (WebLogic)
InteractionGroup name="OFSAAI FTP Details"		
OFSAAI_FTPSHARE_PATH	Identifies the absolute path of the directory that is identified as the file system stage area. **Note:** The directory must exist on the same system on which the OFSAA Infrastructure is being installed (can be on a separate mount). The user mentioned in the APP_SFTP_USER_ID parameter in the following example must have RWX permission on the directory. For example, `<InteractionVariable name="APP_FTPSHARE_PATH">">/oradata6/ revwb7/ftpsh are</ InteractionVariable>`	Yes
OFSAAI_SFTP_USER_ID	Identifies the user who has RWX permissions on the directory identified for the parameter `APP_FTPSHARE_PATH`.	Yes
OFSAAI_SFTP_PRIVATE_KEY	Identifies the SFTP private key for OFSAAI. For example, `<InteractionVariable name="OFSAAI_SFTP_PRIVATE_KEY">/home/ ofsaapp/.ssh /id_rsa</InteractionVariable>` By default, the value is **NA**, which indicates that, for authentication, you are prompted to enter the password for the user <OFSAAI_SFTP_USER_ ID>. For more information on how to generate an SFTP Private key, refer to Set Up SFTP Private Key.	No

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable Name	Significance and Expected Value	Mandatory
OFSAAI_SFTP_PASSPHRASE	Identifies the passphrase for the SFTP private key for OFSAAI. For example, `InteractionVariable name="OFSAAI_SFTP_PASSPHRASE">enter a pass phrase here</InteractionVariable>` By default, the value is **NA**. If the `OFSAAI_SFTP_PRIVATE_KEY` value is given and the `OFSAAI_SFTP_PASSPHRASE` value is **NA**, then the passphrase is identified as empty.	No
InteractionGroup name="Hive Details" The default value set for the interaction variables under this group is NA.		
Note: The following values are required only for Hive Configuration.		
HIVE_SERVER_PORT	Identifies the port used for the file transfer service. The default value is 22 (SFTP). To use this port for FTP, set this value to **21**. For example, `<InteractionVariable name="HIVE_SERVER_PORT">22</InteractionVariable>`	Yes
HIVE_SERVER_FTPDRIVE	Identifies the absolute path to the directory identified as file system stage area of the HIVE server. For example, `<InteractionVariable name="HIVE_SERVER_FTPDRIVE">/scratch/ofsaa/ftpshare</InteractionVariable>`	Yes
HIVE_SERVER_FTP_USERID	Identifies the user who has RWX permissions on the directory identified under the parameter `HIVE_SERVER_FTPDRIVE`. For example, `<InteractionVariable name="HIVE_SERVER_FTP_USERID">ofsaa</InteractionVariable>`	Yes
HIVE_SERVER_FTP_PROTOCOL	If the `HIVE_SERVER_PORT` is **21**, then set the value to **FTP**. If not, set it to **SFTP**. For example, `<InteractionVariable name="HIVE_SERVER_FTP_PROTOCOL">SFTP</InteractionVariable>`	Yes

Table 7-4 (Cont.) OFSAA Infrastructure Installation Tasks and Descriptions

InteractionVariable Name	Significance and Expected Value	Mandatory
HIVE_SFTP_PRIVATE_KEY	Identifies the SFTP private key for the HIVE server. For example, `<InteractionVariable name="HIVE_SFTP_PRIVATE_ KEY">/scratch/testuser/.ssh/id_rsa</InteractionVariable>` By default, the value is **NA**, which indicates that, for authentication, you are prompted to enter the password for the user `<HIVE_SERVER_FTP_USERID>`.	
HIVE_SFTP_PASSPHRASE	Identifies the passphrase for the SFTP private key for HIVE. For example, `<InteractionVariable name="HIVE_SFTP_ PASSPHRASE">NA</InteractionVariable>` By default, the value is **NA**. If the `HIVE_SFTP_PRIVATE_KEY` value is **NA**, then the passphrase is identified as empty.	

Configure SFTP Private Key

Generate the SFTP private key.

Ensure the following permissions exist for the given directories:

- `.ssh`: `700`
- `.ssh/authorized_keys`: `640`
- `.ssh/id_rsa`: `400`
- UNIX user: `755`

To generate a private key:

1. Log in to OFSAA UNIX user using the Putty tool.
2. Enter the following commands:

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

Set the passphrase, if required. Otherwise, set the `OFSAAI_SFTP_PASSPHRASE` tag to NA.

Install the OFSAAI Application Pack

Install the OFSAAI application pack.

Before installing the OFSAAI application pack, configure and execute the following files:

1. OS File System Settings and Environment Settings in the `.profile` file
2. `OFS_<App pack>_PACK.xml`
3. `OFS_<App Pack>_SCHEMA_IN.xml`
4. `<APP Pack>_SCHEMA_BIGDATA_IN.xml`
5. `OFSAAI_InstallConfig.xml` (Do not configure this file if an installation of OFSAAI 8.1 already exists.)
6. Schema Creator Utility

To install the OFS Application Pack:

1. Log in to the system as a non-root user.
2. Identify a directory for installation and update the user `.profile` file as:

   ```
   FIC_HOME=<OFSAA Installation Directory>
   export FIC_HOME
   ```

3. Execute the user `.profile` file.
4. Navigate to the `OFS_AAAI_PACK` `OFS_LRS_PACK`directory.
5. Rename the `OFS_AAAI_PACK/schema_creator/conf/OFS_AAAI_SCHEMA_IN.xml.Template` file to `OFS_AAAI_PACK/schema_creator/conf/OFS_AAAI_SCHEMA_IN.xml`.

   If the installation is for Big Data, then rename the `OFS_AAAI_ PACK/ schema_creator/conf/OFS_AAAI_SCHEMA_BIGDATA_IN.xml.Template` file to `OFS_AAAI_PACK/schema_creator/conf/OFS_AAAI_SCHEMA_BIGDATA_IN.xml`.

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

6. Navigate to the path `OFS_LRS_PACK/conf/OFS_LRS_PACK.xml`, and enter `YES` in the enable tag for OFS_AAI and OFS_AAAI.
7. To execute the application pack installer in silent mode, enter the command: `./setup.sh SILENT`.

   The `Silent.template` file is available in the path `OFS_LRS_PACK/appsLibConfig/conf`. The `Silent.template` file is populated with default values. Ensure to modify the template in the directory. Create a copy of this file and rename it as `Silent.props`.

8. The installer proceeds with pre-installation checks.

Figure 7-13 Silent Mode of Installation

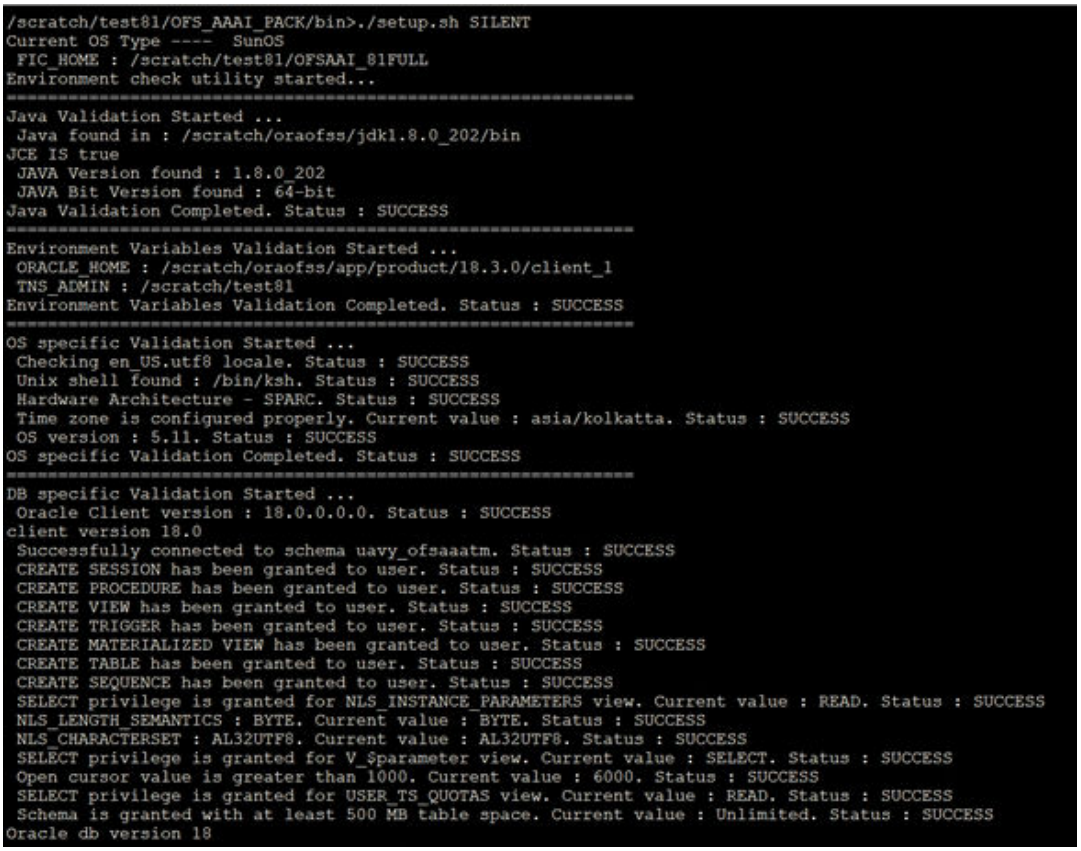
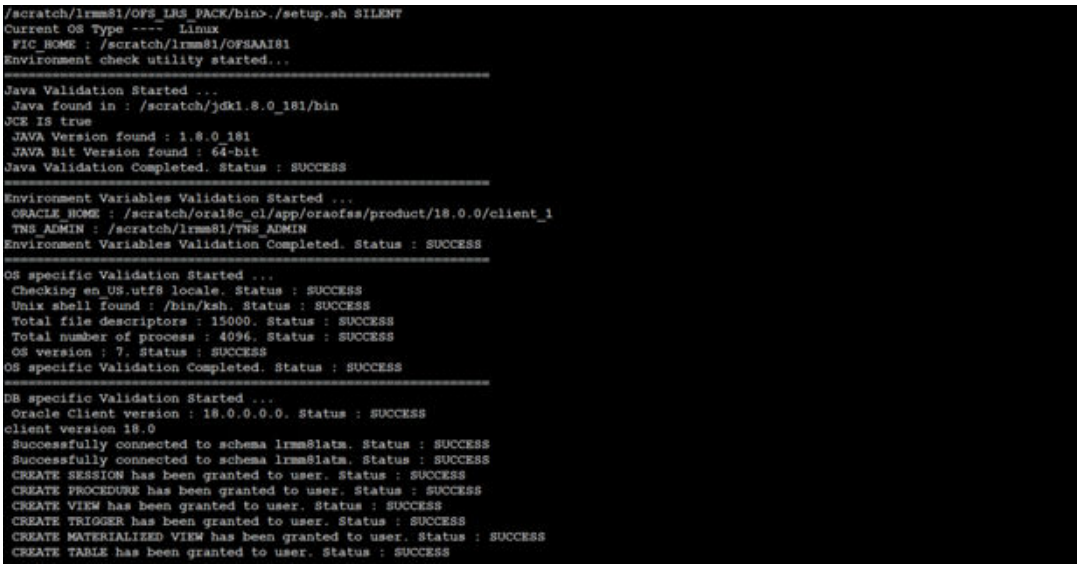


Figure 7-14 Silent Mode of Installation



9. Installation is achieved through the properties file (`Silent.props`) that must be updated with proper values, before attempting to install using silent mode. Edit the parameters in the Silent.props file and specify the parameters as per the requirements.

> **Note:**
>
> The default values for LCR and DIC are the same. If you modify the values, you must have the same values for LCR and DIC parameters.

The following table lists all the properties that must be specified:

Table 7-5 Parameters for the Silent.props File

Property Name	Description of Property	Permissible values	Comments
LOG_MODE	Specify Log Mode.	1 = Debug Mode [Password will be printed in the log file] 0 = General Mode [Passwords will not be printed in the log file]	The default value is 0.
APPFTP_LOG_PATH	Specify the Infodom Maintenance log path (to be created) for the new Infodom. Ignore if you are doing the installation on an existing information domain.	User Input	
DBFTP_LOG_PATH	Specify the Infodom Maintenance log path (to be created) for the new Infodom. Ignore if you are doing the installation on an existing information domain.	User Input	
UPLOAD_MODEL	Specify whether you want to perform Model Upload.	0 = If you have already performed Model Upload and want to skip the model upload process. 1 = If you want to perform Model Upload.	The default value is 1.
MODEL_TYPE	Specify whether you want to use the released datamodel or customized datamodel for the model upload process.	0 = If you want to upload the released datamodel. 1 = If you want to upload the customized datamodel.	The default value is 0.

Table 7-5 (Cont.) Parameters for the Silent.props File

Property Name	Description of Property	Permissible values	Comments
DATAMODEL DM_DIRECTORY	Specify the path (DM_DIRECTORY) and file (DATAMODEL) name for the customized datamodel. Mandatory only if you want to upload the customized datamodel, that is, you have specified MODEL_TYPE=1.	User Input	
OFS_LRM_LCR_SEGMENT_1_CODE	Specify OFS_LRM_LCR Segment Code.	LRSSEGMNT	The default value is LRSSEGMNT.
OFS_LRM_LCR_ETL_APPSRC_TYPE	Specify if you want to create a new ETL App or Src pair or use an existing one.	0 = If you want to create a new ETL App or Src pair. 1 = If you want to use an existing pair.	The default value is 0.
OFS_LRM_LCR_ETL_SRC_1_DESC	ETL OFS_LRM_LCR source description.	Describe the ETL Src. Mandatory if you want to create new ETL Src if you have specified ETL_APPSRC_TYPE=0.	The default value is LRS Source.
OFS_LRM_LCR_ETL_SRC_2_DESC	ETL Staging source description.	Describe the ETL Src. Mandatory if you want to create new ETL Src if you have specified ETL_APPSRC_TYPE=0.	The default value is Staging Source.
OFS_LRM_LCR_ETL_SRC_1_NAME	ETL OFS_LRM_LCR source name.	User Input	The default value is LRSSRC. Specify the ETL Source Name into ETL Area Definitions to be deployed.
OFS_LRM_LCR_ETL_SRC_2_NAME	ETL Staging source name.	User Input	The default value is STGSRC. Specify the ETL Source Name into ETL Area Definitions to be deployed.
OFS_LRM_DIC_SEGMENT_1_CODE	Specify OFS_LRM_DIC Segment Code.	User Input	The default value is LRSSEGMNT.

Table 7-5 (Cont.) Parameters for the Silent.props File

Property Name	Description of Property	Permissible values	Comments
OFS_LRM_DIC_ETL_APPSRC_TYPE	Specify if you want to create a new ETL App or Src pair or use an existing one.	Specify if you want to create a new ETL App or Src pair or use an existing one. 0 = If you want to create a new ETL App or Src pair. 1 = If you want to use an existing pair.	The default value is 0.
OFS_LRM_DIC_ETL_SRC_1_DESC	ETL OFS_LRM_DIC source description.	Describe the ETL Src. Mandatory if you want to create new ETL Src if you have specified ETL_APPSRC_TYPE= 0.	The default value is LRS Source.
OFS_LRM_DIC_ETL_SRC_2_DESC	ETL Staging source description.	Describe the ETL Src. Mandatory if you want to create new ETL Src if you have specified ETL_APPSRC_TYPE= 0.	The default value is Staging Source.
OFS_LRM_DIC_ETL_SRC_1_NAME	ETL OFS_LRM_DIC source name.	Specify the ETL Source Name into ETL Area Definitions to be deployed.	The default value is Staging LRSSRC.
OFS_LRM_DIC_ETL_SRC_2_NAME	ETL Staging source name.	Specify the ETL Source Name into ETL Area Definitions to be deployed.	The default value is Staging STGSRC.

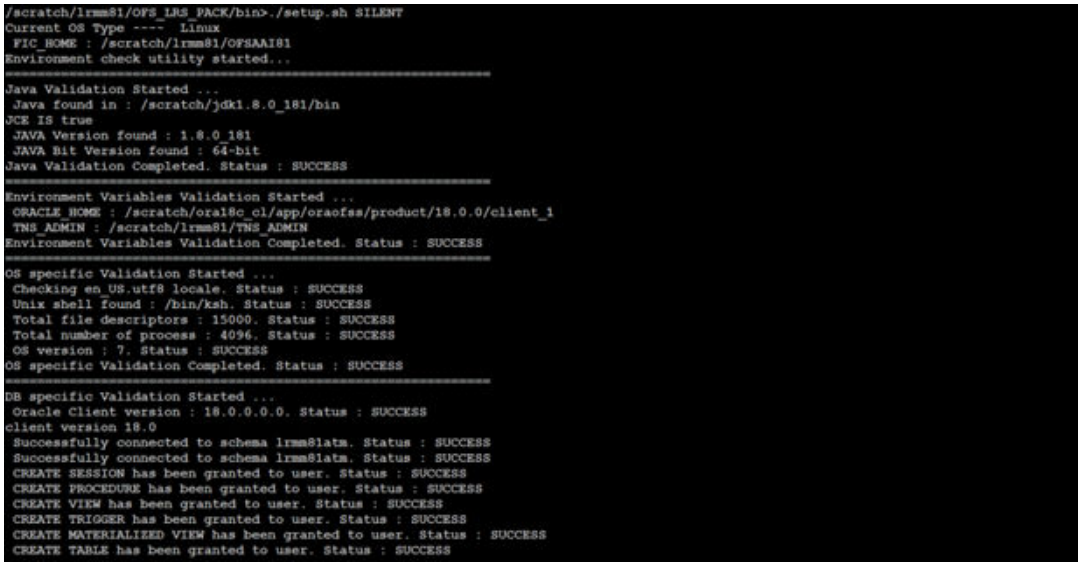
> **Note:**
>
> Do not install new packs in the same segment if the preinstalled applications use the Run Management functionality of OFSAAI.

10. Enter the following command in the console to execute the application pack installer with the Silent option.

    ```
    ./setup.sh SILENT
    ```

11. The installer proceeds with Pre-Installation Checks.

Figure 7-15 Silent Mode of Installation

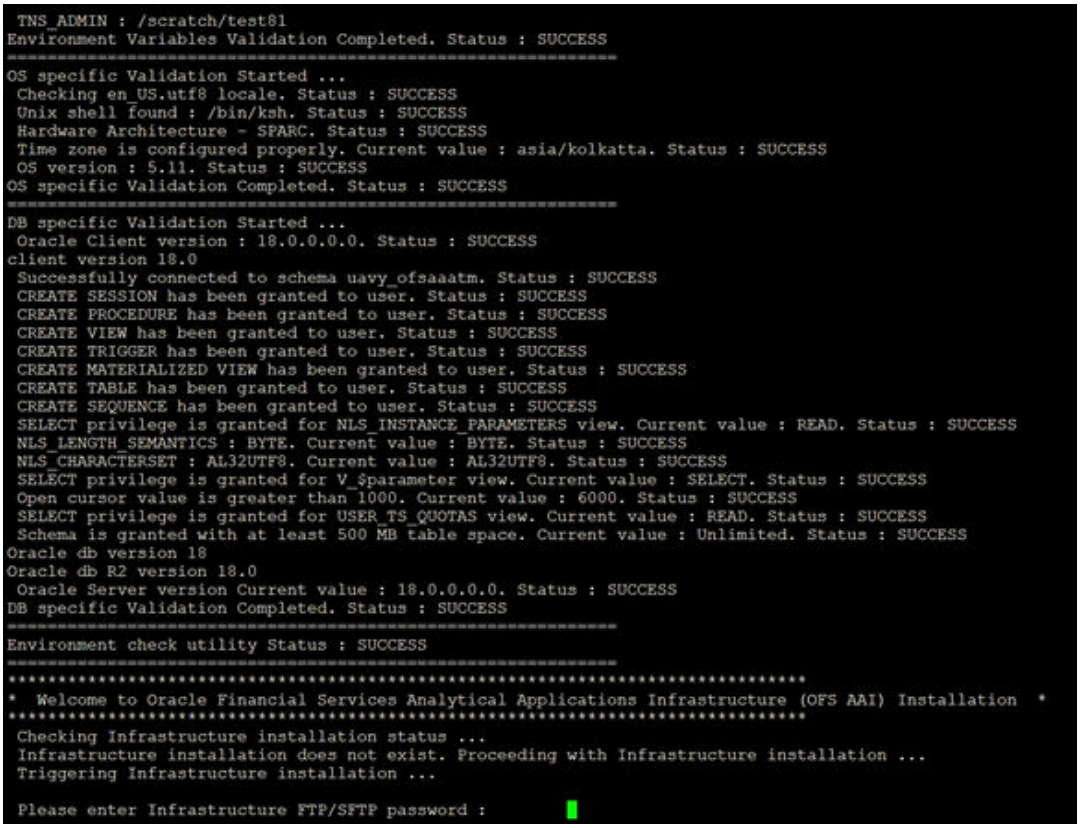


12. Enter the OFSAA Processing Tier FTP/SFTP password value and proceed, when prompted in the command prompt.

Table 7-6 Console Prompt: Enter the OFSAA Processing Tier FTP/SFTP Password

Console Prompts	User Inputs
Please enter OFSAA Processing Tier FTP or SFTP password	Enter the password to access the processing tier in the application server. **Note:** If the prompt reads as follows, enter the username and password for accessing the product Staging or Metadata Repository FTPSHARE: • Kerberos username [user] • Kerberos password for user

Figure 7-16 OFSAA Processing Tier FTP/SFTP Password Prompt



13. The process displays the OFSAA License. Enter **Y** and proceed.

Figure 7-17 Accept the OFSAA License Agreement

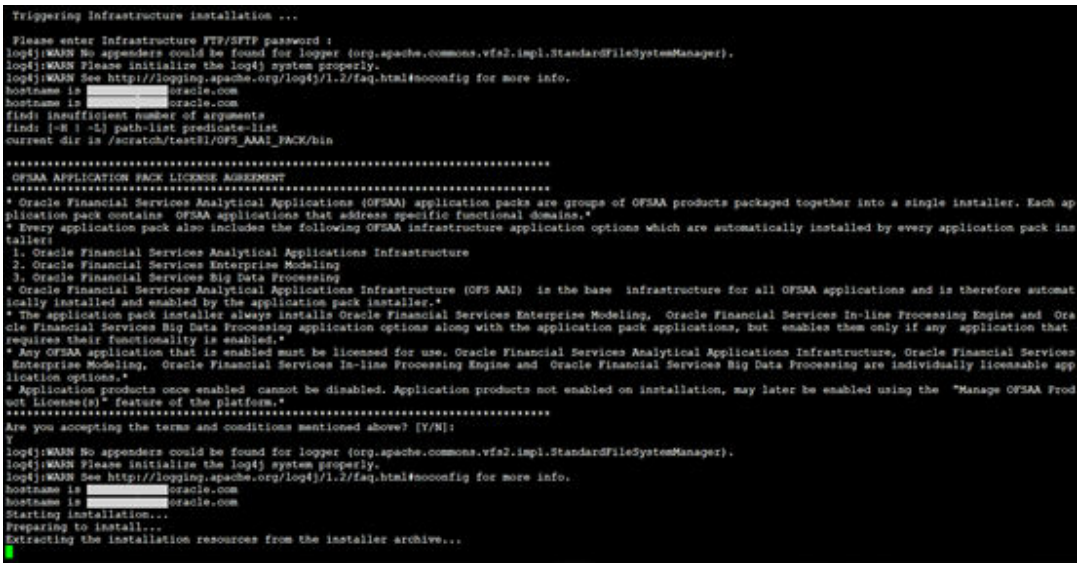


Figure 7-18 Accept the OFSAA License Agreement

14. The installer installs the OFS application.

Figure 7-19 OFS AAAI Silent Mode Installation

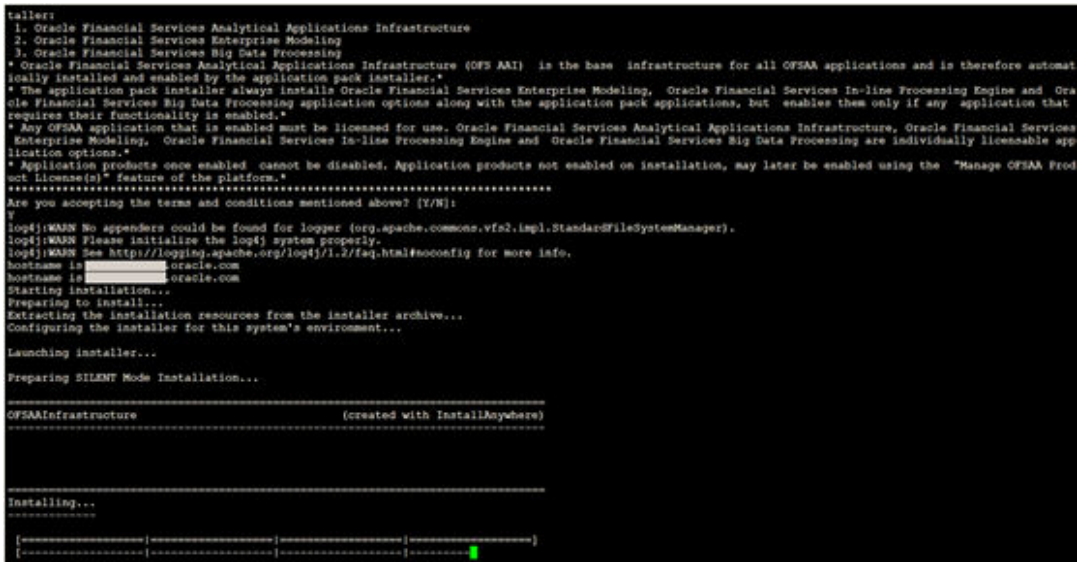
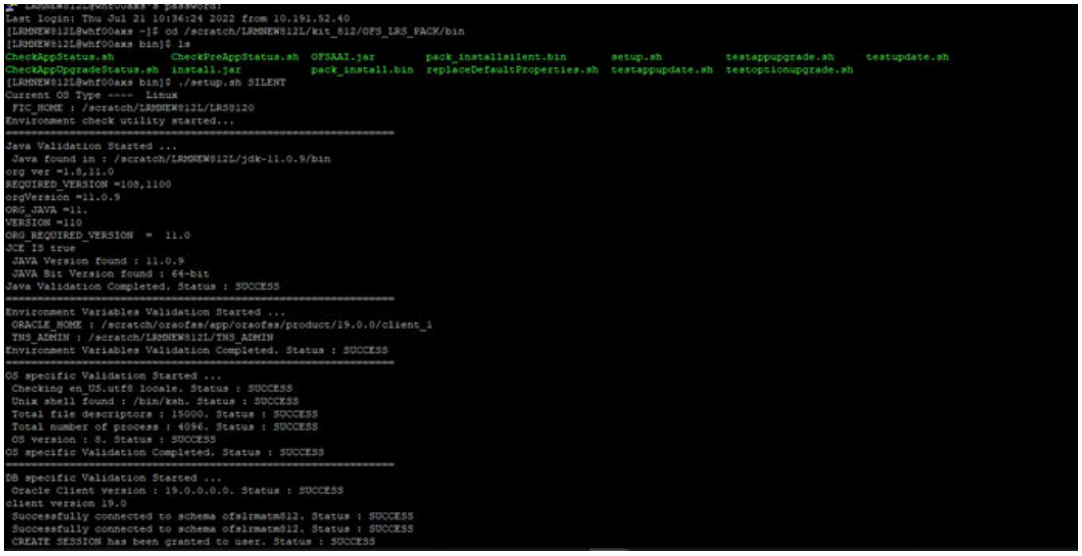


Figure 7-20 LRS Silent Mode Installation



After the platform is installed, the OFS LRS installation begins.

Data Model Upload may take several hours to complete. You can check the installation logs in the location: `OFS_AAAI_PACK/OFS_AAI/logs`
After successful App pack installation, the WAR file is generated, and all the servers are verified and the installation complete message is displayed.

15. A post-install check is performed automatically after the successful installation of the product.

Figure 7-21 Installation Complete

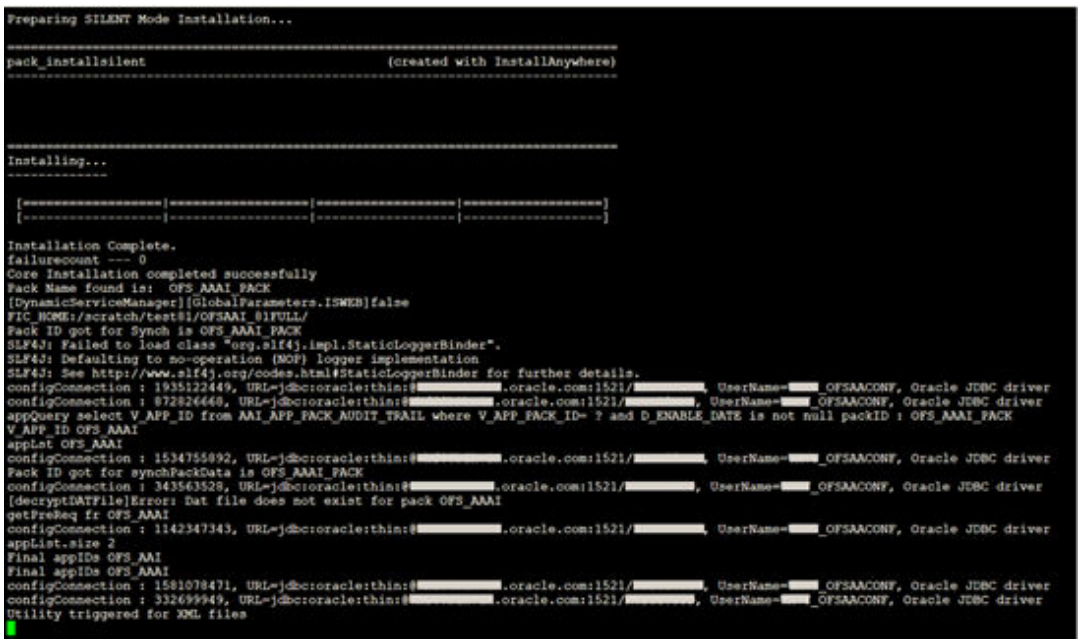
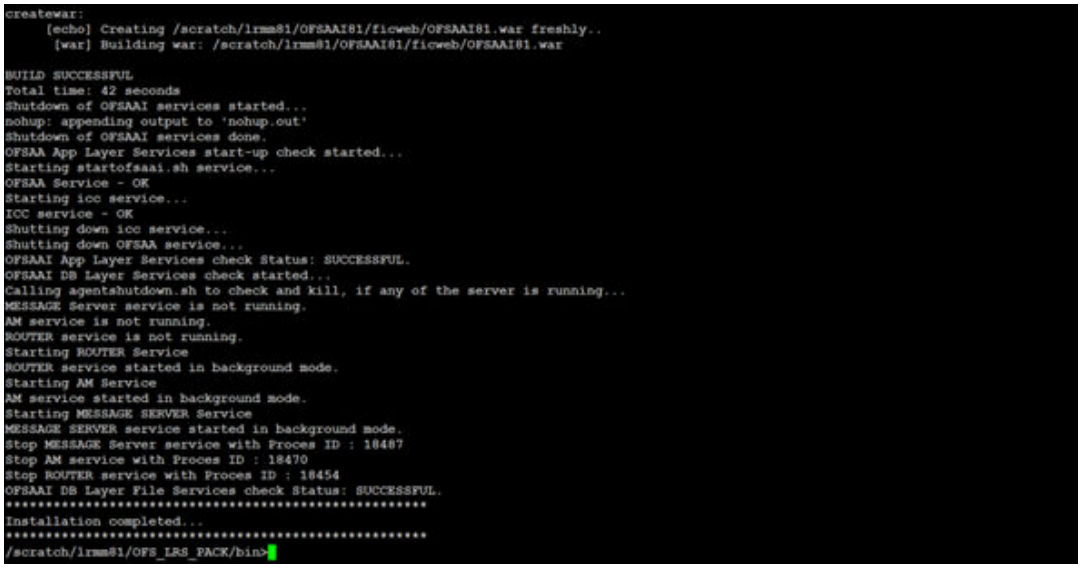


Figure 7-22 Silent Mode Installation Complete



Congratulations! Your installation is complete.

> **Note:**
>
> Ensure that the OFS_LRS_PACK installer directory with its contents is preserved, for enabling additional products in the future.

Verify Log Files and TNS Entries

After installing OFSAAAI 8.1.2.0.0, verify the log files and TNS entries.

Log Files

- Infrastructure installation log files in the `OFS_AAAI_PACK/OFS_AAI/logs/ directory`.
- `OFSAAInfrastucture_Install.log` file in the `$FIC_HOME` directory.

TNS Entries

Expand **Name** to get the list of TNS entry names. Alternatively, you can connect to the CONFIG schema and execute the query: `select dbname from db_master where dbname !='CONFIG'`

8
Post-installation Tasks

List of post-installation tasks for the OFSAA application pack.

> **Note:**
>
> In an integrated environment:
>
> - When ALM is to be installed after LRS, to resolve the screen loading issues in the Holiday Calendar, Time Buckets, Business Assumption and Run Management windows, execute the following SQL statement after LRS installation and before ALM installation.
>
>   ```
>   UPDATE rev_app_user_preferences a
>   SET a.sys_id_num = FSI_OBJECT_DEN_SEQ_NUM.nextval
>   WHERE a.appid IN ('OFS_LRM_LCR','OFS_LRM_DIC');
>   ```
>
> - If more than one OFSAA Application exists in the same environment, then the output of one OFSAA application can be consumed by another OFSAA application. If OFS Capital Adequacy Application Pack (OFS CAP or BASEL) or OFS Liquidity Risk Solution Application Pack (OFS LRS) is not installed in the same environment as the OFSDF Application Pack, then execute the Integration Utility to enable the Integration process provided in the OFSDF Application Pack v8.1.2.0.0 release. See the **Enable Integration T2Ts** section in the Oracle Financial Services Data Foundation Application Pack Installation and Configuration Guide for more details.

1. Verify that all patches are successfully installed.
2. Backup the OFS_<PACK>_SCHEMA_IN .xml and OFS_<PACK>_SCHEMA_OUTPUT.xml files.
3. Backup the OFS_<PACK>_SCHEMA_IN .xml, OFS_<PACK>_SCHEMA_OUTPUT.xml and Silent.props files.
4. Stop the OFSAA Infrastructure services.
5. Configure Referrer Header Validation
6. Create and deploy EAR or WAR files.
7. EAR/WAR File - Build Once and Deploy Across Multiple OFSAA Instances.
8. Assign Grants for schemas.
9. Start Infrastructure Services.
10. Access the OFSAA Application.
11. Configure the `excludeURLList.cfg` file.
12. Configure Oracle R Distribution and Oracle R Enterprise (ORE)
13. (Optional) Configure Big Data Processing.

14. (Optional)Enable Financial Services Enterprise Modeling on Another Application Pack
15. OBIEE Configuration – Deploy OFS LRS Analytics.
16. Logging as System Administrator.
17. Create Application Users.
18. Map Application User(s) to User Groups.
19. Change the ICC batch ownership.
20. Add TNS entries in the TNSNAMES.ORA file.
21. Update OBIEE URL.
22. Configure Data Source.
23. Set TDE and Data Redaction in LRS in OFSAAI.
24. Implement Data Protection in OFSAA.
25. Configure the web server.
26. Configure Resource Reference in web servers.
27. Configure Work Manager in web application servers.
28. Configure Tomcat.
29. Add FTP/SFTP Configuration for File Transfer.
30. Configure Infrastructure Server Memory.
31. Retrieve Patch Information.
32. Change IP/Hostname, Ports, Deployed Paths of the OFSAA Instance.
33. Set Infrastructure LDAP Configuration.
34. Configure OFSAAI Web Services.
35. Configure Message Details in Forms Designer.
36. Configure Password Changes.
37. Configure Java Virtual Machine.
38. Configure Internal Service.
39. LRS Pack User Group Names

Install OFSAA Infrastructure Patches

Install all the available patches for OFSAAA 8.1.2.0.0.

Install all the patches for Oracle Financial Services Advanced Analytical Applications 8.1.2.0.0 available on My Oracle Support.

Install all the patches for Oracle Financial Services Liquidity Risk Solution Applications 8.1.2.0.0 available on My Oracle Support.

To download and install all the available patches:

1. Log in to My Oracle Support
2. In the **Patches & Updates** tab, click **Product or Family (Advanced)**.
3. Type the product name (**Oracle Financial Services Advanced Analytical Applications**) and select the **Release** number.

For this release, select **Oracle Financial Services Advanced Analytical Applications 8.1.2.0.0**.

4. Type the product name (**Oracle Financial Services Liquidity Risk Solution Applications**) and select the **Release** number.
5. Click **Search** to view the available patches.

   Apply the Mandatory one-off patch **34336823**.
6. Install all the patches, based on the instructions provided in the patch readme file.

After the installation of OFSAAAI 8.1.2.0.0, apply the mandatory patch **33663417**.

> **Note:**
>
> On the 10th of December 2021, Oracle released Security Alert CVE-2021-44228 in response to the disclosure of a new vulnerability affecting Apache Log4J before version 2.15. The application of the 33663417 Mandatory Patch fixes the issue. For details, see the My Oracle Support Doc ID 2827801.1. Ensure that you reapply the **33663417** Mandatory Patch whenever you install or upgrade the application, or apply an incremental patch.

Backup the OFS_<PACK>_SCHEMA_IN.xml and OFS_<PACK>_SCHEMA_OUTPUT.xml Files

Backup the `OFS_<PACK>_SCHEMA_IN.xml` and `OFS_<PACK>_SCHEMA_OUTPUT.xml` files.

Create backups of the `OFS_<PACK>_SCHEMA_IN.xml` and `OFS_<PACK>_SCHEMA_OUTPUT.xml` files to use later for upgrading existing applications or installing new ones.

File directories:

- `OFS_<PACK>_SCHEMA_IN.xml`: `<OFS_AAAI_PACK>/schema_creator/conf`
- `OFS_<PACK>_SCHEMA_OUTPUT.xml`: `<OFS_AAAI_PACK>/schema_creator/`

Stop the Infrastructure Services

To stop Infrastructure services, follow these steps:

1. On the machine where the Infrastructure Application components are installed, navigate to the $FIC_APP_HOME/common/FICServer/bin directory, and execute the following command:
   `./stopofsaai.sh`
2. To stop the ICC server on the machine where the Infrastructure Default Application components are installed, navigate to the $FIC_HOME/ficapp/icc/bin directory, and execute the following command:
   `./iccservershutdown.sh`

> **Note:**
>
> Only the Infrastructure Default Application Server will hold the ICC component.

3. To stop the Back-end server on the machine where the Infrastructure database components are installed, navigate to the $FIC_DB_HOME/bin directory, and execute the following command:
`./agentshutdown.sh`

Configure Referrer Header Validation

Set up Referrer Header validation.

Referrer Header validation protects against CSRF attacks by allowing validated host URLs.

To configure Referrer Header validation:

- Navigate to the `web.xml` file in the `$FIC_HOME/ficweb/webroot/WEB-INF/` directory, and add the following tag:

```
<filter>
<filter-name>FilterServlet</filter-name>
<filter-class>com.iflex.fic.filters.FilterServlet</filter-class>
<init-param>
  <param-name>AllowHosts</param-name>
  <param-value><URL1>/ <URL2>/</param-value>
</init-param>
</filter>
```

Note:

1. Ensure there is a single space between <URL1> and <URL2>. Adding the URLs without a space between them or adding two or more spaces between them results in errors, and confirm that <URL> concludes with a forward slash (/).
2. If you choose to set **Referrer-Policy no-referrer**, disregard the above steps to configure Referrer Header validation and proceed with the following:
   a. Open the `web.xml` file in the `$FIC_HOME/ficweb/webroot/WEB-INF/` directory. The **REFERRER_POLICY_FLAG** is set to **TRUE** by default in the `web.xml` file:

```
<context-param>
<param-name>REFERRER_POLICY_FLAG</param-name>
<param-value>TRUE</param-value>
</context-param>
```

   b. Modify the referrer policy in the `web.xml` file to **FALSE**.

Create and Deploy the EAR/WAR Files

EAR/WAR files are used for deploying the OFSAAI application to a production server.

Refer to the following topics, to create and deploy EAR/WAR files

- Create the EAR/WAR File
- Explode the EAR File

- Deploy the EAR/WAR File

Build EAR/WAR File Once and Deploy Across Multiple OFSAA Instances

OFSAA 8.1.2.0.0 now supports a single archive deployment model. You can build the EAR/WAR file once and deploy it across multiple OFSAA instances on the same release.

Prerequisites:

1. The web server type must be the same across all OFSAA instances.
2. The information domain must be the same across all OFSAA instances.

Feature Highlights

1. The path of the deployed area log files is in the `AAI_SETUP_PROPS` database table in the Config Schema.
2. The following parameters are moved from the `FICWEB.cfg` file to the `AAI_SETUP_PROPS` table with tier as WEB. The file is removed and the respective parameters are set in the servlet context.
   - `FIC_SERVLET_PORT`
   - `ICC_SERVER_PORT`
   - `CSS_LOGGER_PATH`
3. The following values for the AAI servlet config parameters in the `web.xml` file are moved to the `AAI_SETUP_PROPS` table:
   - `FIC_WEBPROTOCOL`
   - `FIC_PHYSICAL_HOME_LOC`
   - `FIC_WEBSERVER_PORT`
   - `FIC_HOME`
   - `FIC_WEBSERVER_IP`
4. OFSAA environment details used to establish communication between the web and app layer now moved from the `LookupServices.xml` and `DynamicServices.xml` file to the following database tables:
   - `aai_dyn_svcs_params`
   - `aai_dyn_svcs_servers`
   - `aai_lkp_svcs_servers`

> **Note:**
>
> This change to the configuration XML files is done only at the web layer deployment location.

Create the EAR/WAR File

Create the EAR/WAR files.

The EAR/WAR files are automatically generated during the new installation. To create EAR/WAR files after installation or upgrade, refer to the following topics.

- Non-TCPS Installed Setup
- TCPS Installed Setup

Non-TCPS Installed Setup

Create the EAR/WAR file in a non-TCPS installed setup.

To create the EAR/WAR file in a non-TCPS installed setup:

1. Navigate to the `$FIC_WEB_HOME` directory on the OFSAA Installed server.
2. Execute `./ant.sh` to trigger the creation of the EAR/WAR file.

   The EAR/WAR (`<contextname>.ear/ .war`) is created.

   The `BUILD SUCCESSFUL` and `Time taken` message is displayed.

Figure 8-1 Creating EAR/ WAR File

> **Note:**
>
> - The `<contextname>` refers to the name assigned during installation. This process overwrites any existing version of the EAR file in the specified path.
> - For OFSAA configured on Tomcat installation,`<contextname>.war` file is created.
> - Ignore ANT warning(s) for the `tools.jar` file while executing the `./ant.sh` command.

TCPS Installed Setup

Create the EAR/WAR file in a TCPS installed setup.

To create the EAR/WAR file in a TCPS installed setup:

1. Navigate to the `$FIC_WEB_HOME/webroot/WEB-INF/lib` directory on the OFSAA installed server and delete the `ojdbc7.jar` file if it exists in the directory.
2. Navigate to the `$FIC_HOME/utility/AppPckMastSynch/bin` directory and execute the `App Pack Mast Sync` utility by running the `AppPckMastSynch.sh` command.
3. Navigate to the `$FIC_WEB_HOME` directory and execute the `./ant.sh` command to trigger the creation of the EAR/WAR file.
4. The EAR/WAR (`<contextname>.ear/ .war`) is created.

The BUILD SUCCESSFUL and Time taken message is displayed.

Figure 8-2 Creating EAR/ WAR File

Note:

- The <contextname> refers to the name assigned during installation. This process overwrites any existing version of the EAR file in the specified path.
- For OFSAA configured on Tomcat installation, <contextname>.war file is created.
- Ignore ANT warning(s) for the tools.jar file while executing the ./ant.sh command.

Explode the EAR File

Explode the EAR file.

To explode the EAR file:

1. Create the applications directory under the domain name directory.

   For example, /Bea/user_ projects/domains/ <Domain _name>/applications.
2. Create the <context_name>.ear directory under the applications directory.
3. Copy the <$FIC_WEB_HOME/<context_name>.ear file to the <WEBLOGIC_INSTALL_ DIR>/Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_ name>.ear directory.
4. Explode the <context_name>.ear file by executing: jar -xvf <context_name>.ear.
5. Delete the <context>.ear and <context>.war files located in <WEBLOGIC_ INSTALL_DIR>/Bea/user_projects/domains/<DOMAIN_ NAME>/applications/ <context_name>.ear
6. Create a directory <context_name>.war under the <WEBLOGIC_INSTALL_ DIR>/Bea/user_projects/domains/<DOMAIN_ NAME>/applications/<context>.ear./<context>.war directory.
7. Copy the <$FIC_WEB_HOME/<context_name>.war file to <WEBLOGIC_INSTALL_ DIR>/ Bea/user_projects/domains/<DOMAIN_NAME>/applications/<context_ name>.ear/ <context_name>.war directory.
8. Execute jar -xvf <context_name>.war command to explode the <context_name>.war file, to get the directory structure:

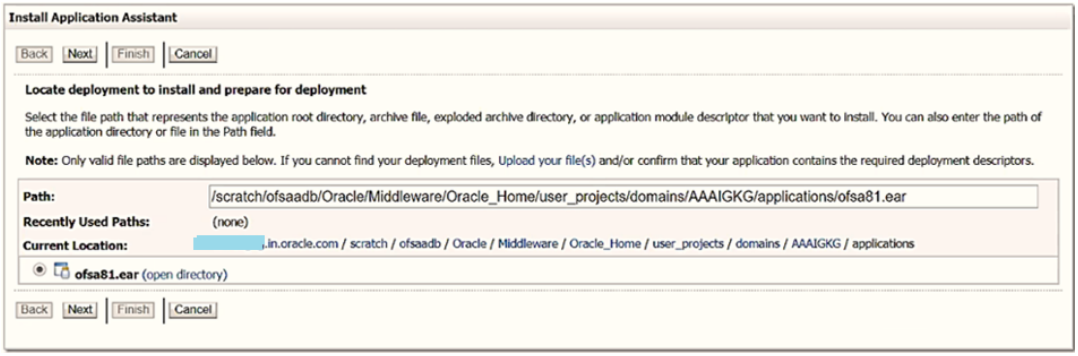
Install Application

Install the OFSAA application using <??>.

To install the application:

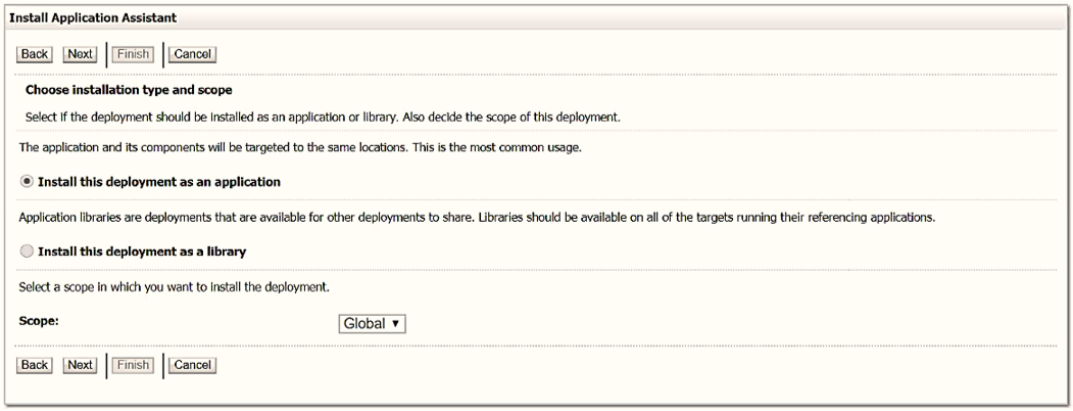
1. Select **Install Application Assistant** from the **Navigation Tree** to display the **<what ??>** window.

Figure 8-3 Install Application Assistant



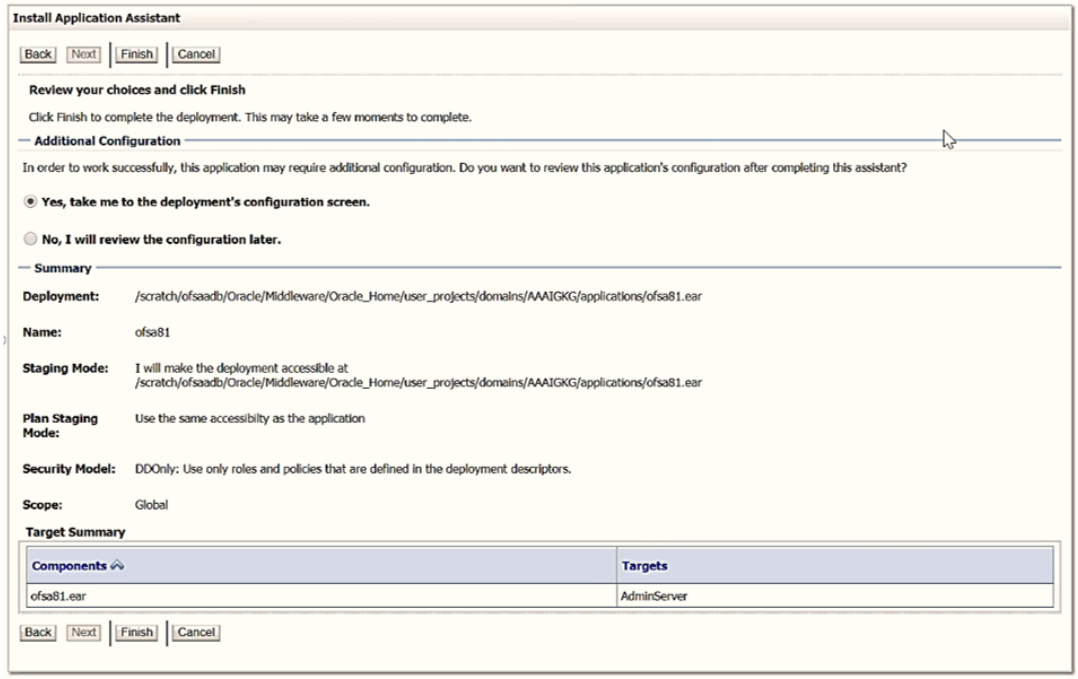
2. Click **Next**, to choose the **installation type and scope**.

Figure 8-4 Install Application Assistant



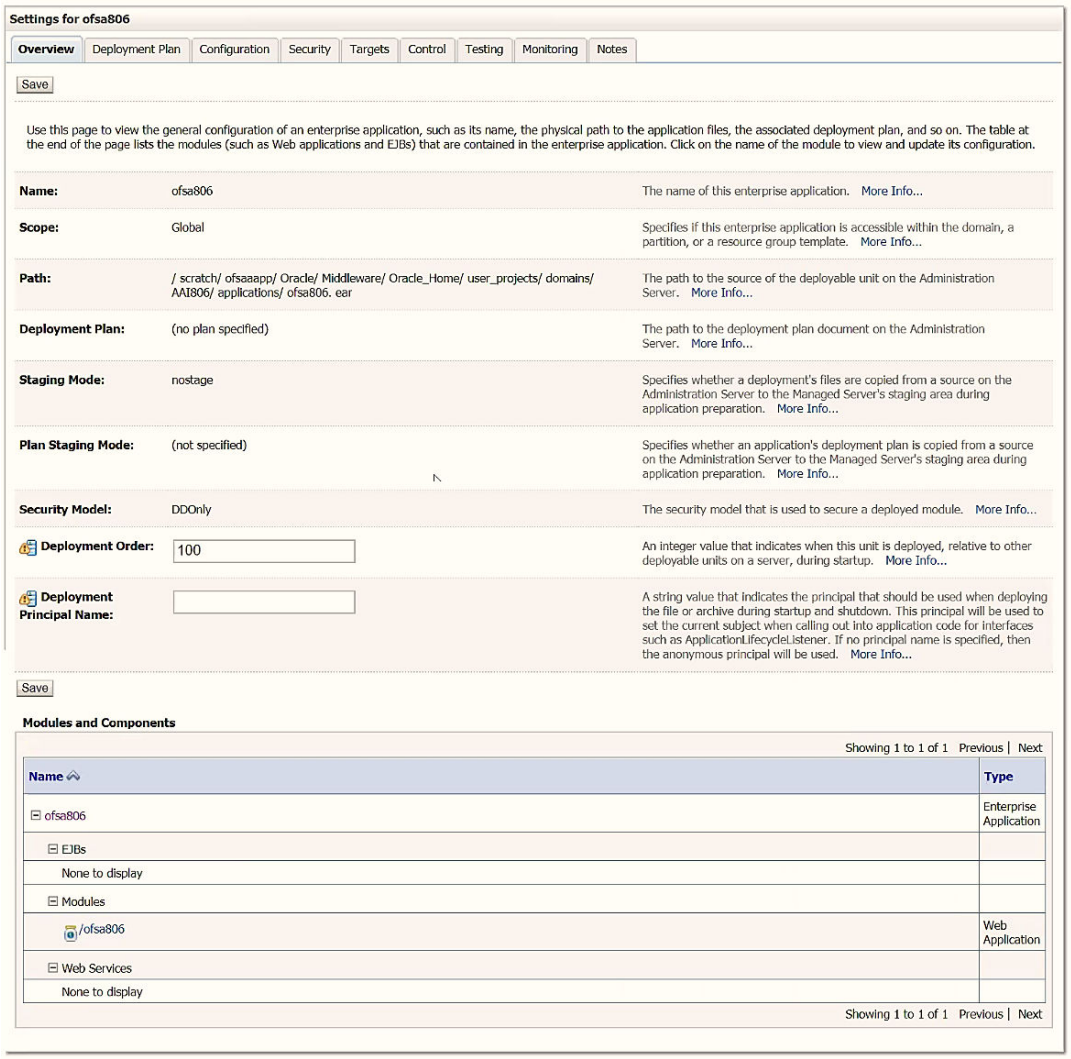
3. Click Next, to access the **Choose targeting style** tab.
4. Select **Install this deployment as an application**, and click **Next** to edit the following details in the **Optional Settings**.
   - **Name** - Deployment name
   - **Security Model** - Select the **DD Only: Use only roles and policies that are defined in the deployment descriptors** option.
   - Source Accessibility - Select **I will make the deployment available from the following location** under the **Source Accessibility** section.
5. Click **Next** to view the **Deployment Summary** window.

Figure 8-5 Deployment Summary



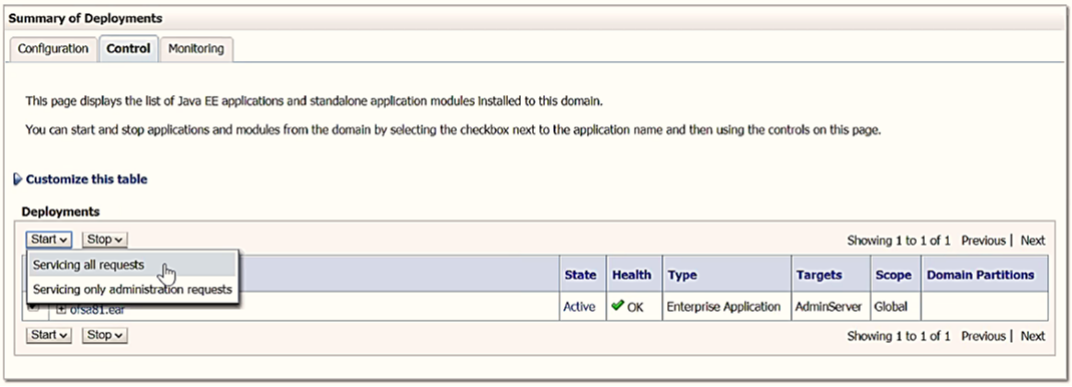
6. Select **Yes** to view the deployment configuration screen.
7. Click **Finish** to display the Settings for <Deployment Name> window.

Figure 8-6 Settings for Deployment Name



8. 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.
9. Click **Save** to update the changes.
10. From the navigation tree, click **Deployments** to display the **Summary of Deployments** window.

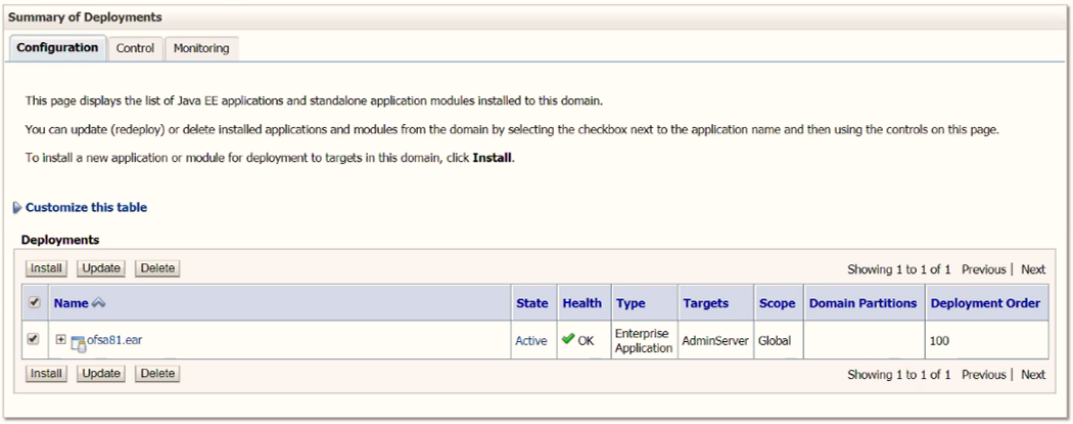
Figure 8-7 Summary of Deployments



11. Select the newly deployed Infrastructure application.
12. Click **Start** and then select **Servicing all requests**.

> **Note:**
>
> Verify that the Infrastructure server is up and running. For more information, see Start the Infrastructure Services.

Figure 8-8 Summary of Deployments



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

Deploy the EAR/WAR File

Deploying the EAR/EAR file.

> **Note:**
>
> Clear the application cache before deploying the Applications Pack Web archive. This applies to all Web Servers (WebSphere, WebLogic, and Tomcat).

To deploy EAR/WAR files after installation or upgrade, refer to the following topics.

- Clear Application Cache
- Deploy the EAR/WAR Files on WebSphere
- Deploy the EAR/WAR Files on WebLogic
- Deploy the WAR File on Tomcat

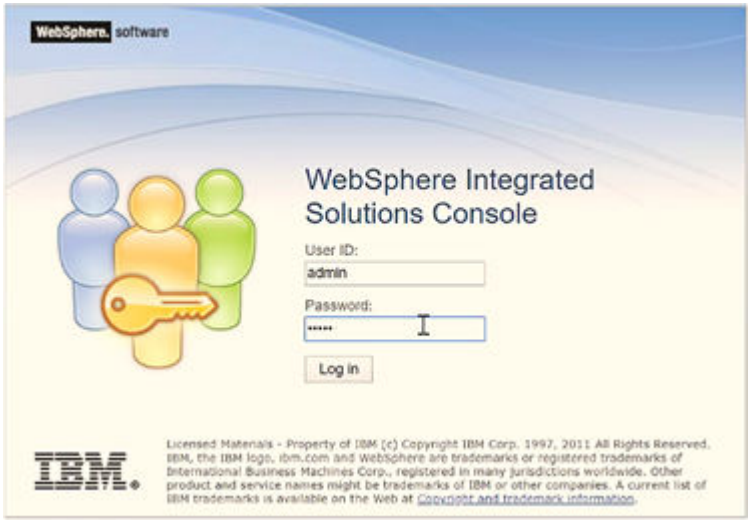
Deploy the EAR/WAR Files on WebSphere

Deploying the EAR/WAR files on WebSphere.

To deploy the Infrastructure application in WebSphere:

1. Navigate to the `/<Websphere_Installation_ Directory>/ IBM/WebSphere/AppServer/ profiles/<Profile_Name>/bin/` directory
2. Start the WebSphere profile by executing: `./startServer.sh server1`.
3. Open the URL `http://<ipaddress>:<Administrative Console Port>/ibm/console` (https, if SSL is enabled) in a browser to access the **Login** window.

Figure 8-9 WebSphere Login Window

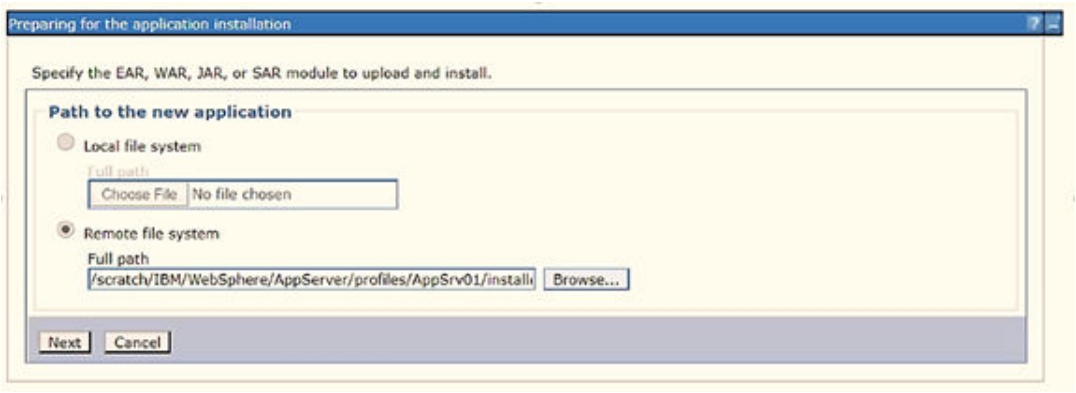


4. Enter the user credentials with administrator rights and click **Log in**.
5. From the navigation, select **Applications**, and then select **New Application** to access the **New Application** window.

Figure 8-10 New Application

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

Figure 8-11 Preparing for the application installation

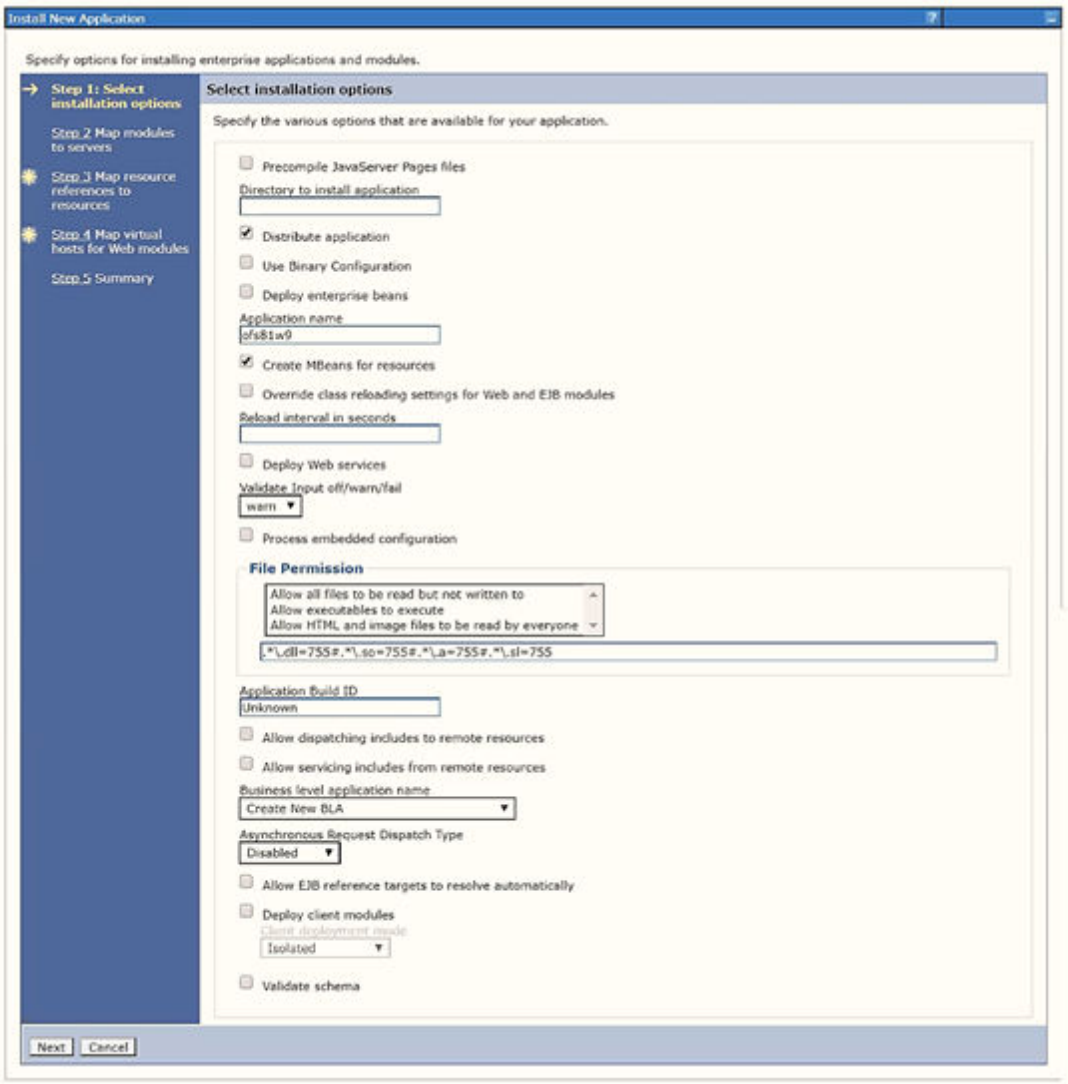


7. Select the **Remote File System** and click **Browse**.
8. Select the EAR file (generated for OFSAAI) to upload and install. Click **Next**.

Figure 8-12 Installation Options

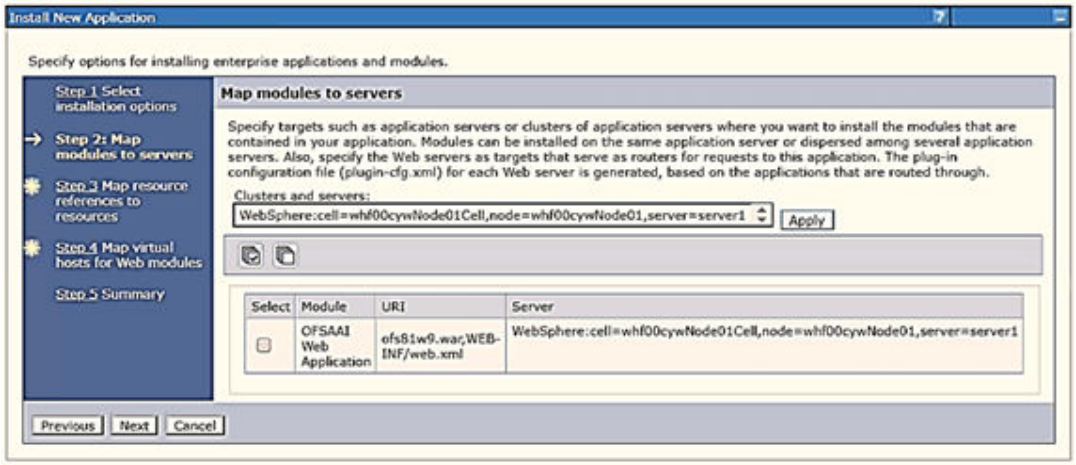
9. Select the **Fast Path** option and click **Next** to display the **Install New Application** window.

Figure 8-13 Install New Application



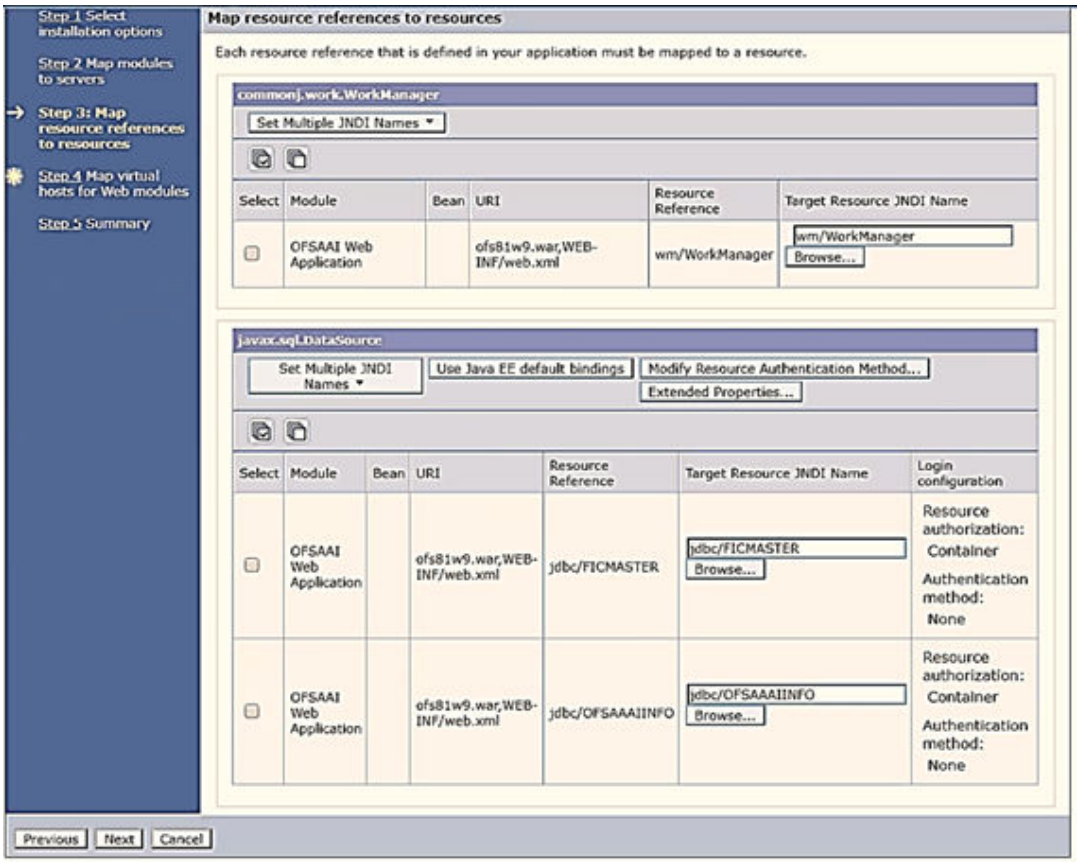
10. Enter the required information and click **Next** to display the **Map Modules to the Servers** window.

Figure 8-14 Map Modules to Servers



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

Figure 8-15 Map Resource References to Resources

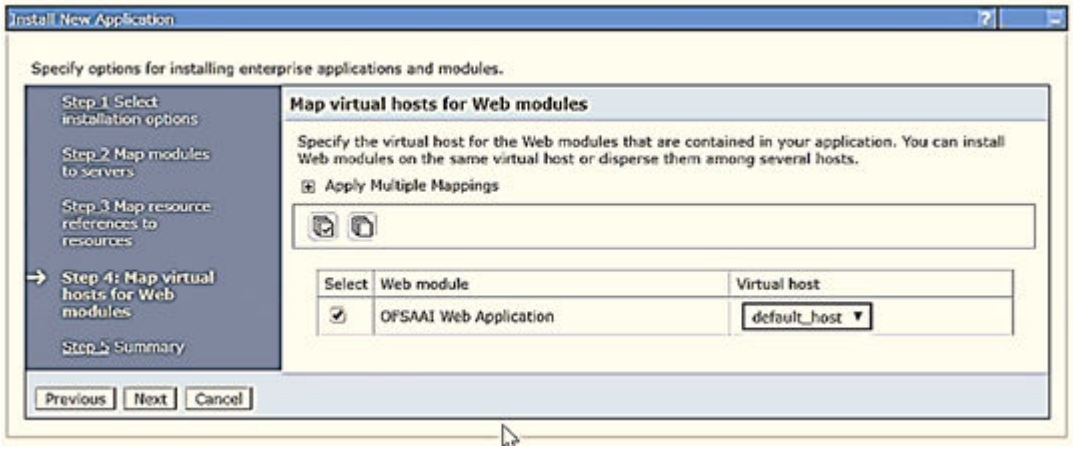


12. Map each resource defined in the application to a resource JNDI name defined earlier.
13. Click **Modify Resource Authentication Method** and specify the authentication method created earlier.

> **Note:**
>
> Specify "config" for `FICMASTER` resource or "atomic" for the atomic resource as the authentication method.

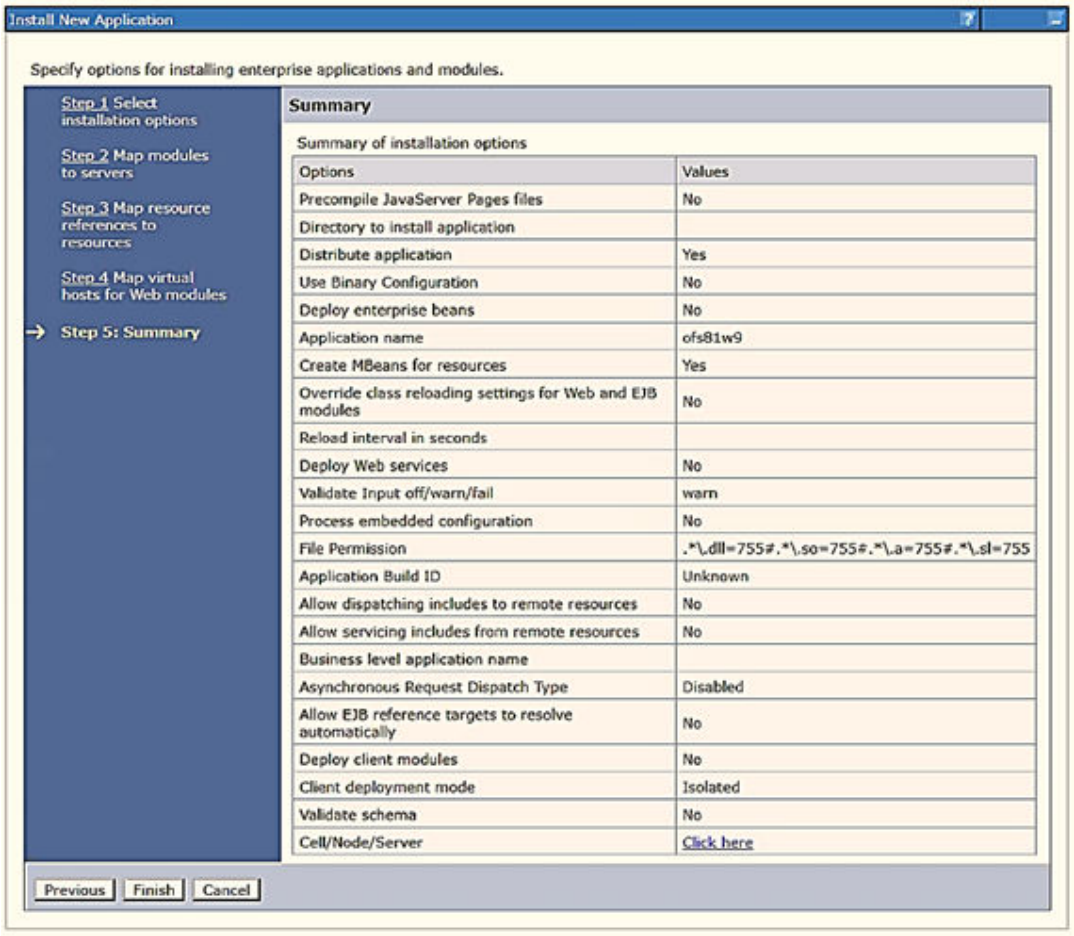
14. Select **OFSAAI Web Application** and click **Next** to display the **Map Virtual hosts for Web Modules** window.

Figure 8-16 Map Virtual host for Web Modules



15. Select **OFSAAI Web Application** and click **Next** to display the **Summary** window.

Figure 8-17 Summary



16. Click **Finish** to deploy the Infrastructure Application on WebSphere.
17. Click **Save** to save the master file configuration.

    The details are displayed in the **Master File Configuration** window.

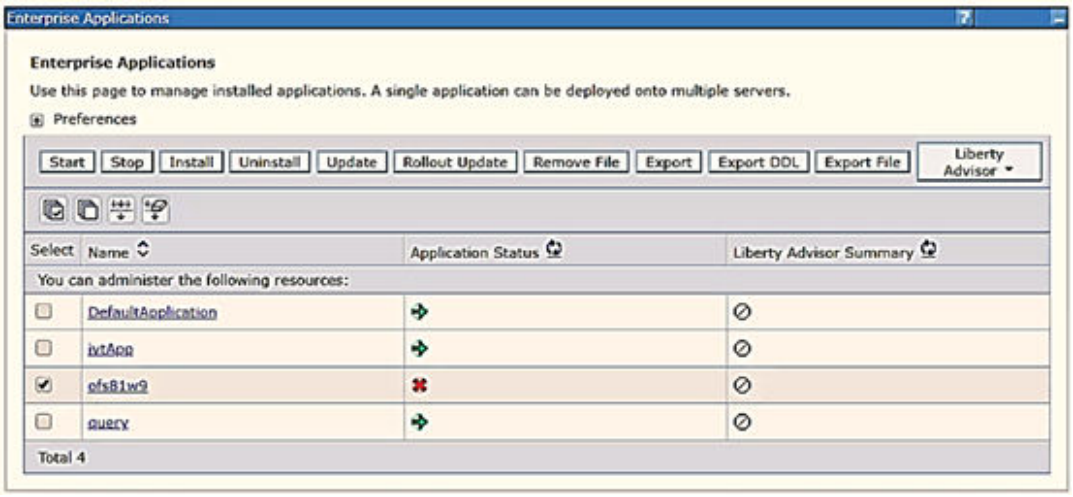
Start the Application

Initiate the installed application.

To start the application:

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

Figure 8-18 Enterprise Applications Window



2. Select the installed application and click **Start**.

> **Note:**
>
> - <profile name>: Name assigned during the WebSphere profile creation.
> - <cell name>: Cell name assigned during profile creation.
> - <contextname>: Context name assigned during installation.

Deploy the EAR/WAR Files for WebLogic

Deploy the EAR/WAR files for WebLogic.

To deploy the OFSAAI EAR (ofaai and tflt) files:

1. Navigate to the <WebLogic Installation directory>/user_ projects/domains/<domain name>/bin directory in the machine in which WebLogic is installed.

   (Optional) <Enter a step example.>

2. Start WebLogic by executing the command:

   ```
   ./startWebLogic.sh
   ```

3. Open the following URL in a browser window:

   ```
   http://<ipaddress>:<admin server port>/ console (https, if SSL is enabled).
   ```

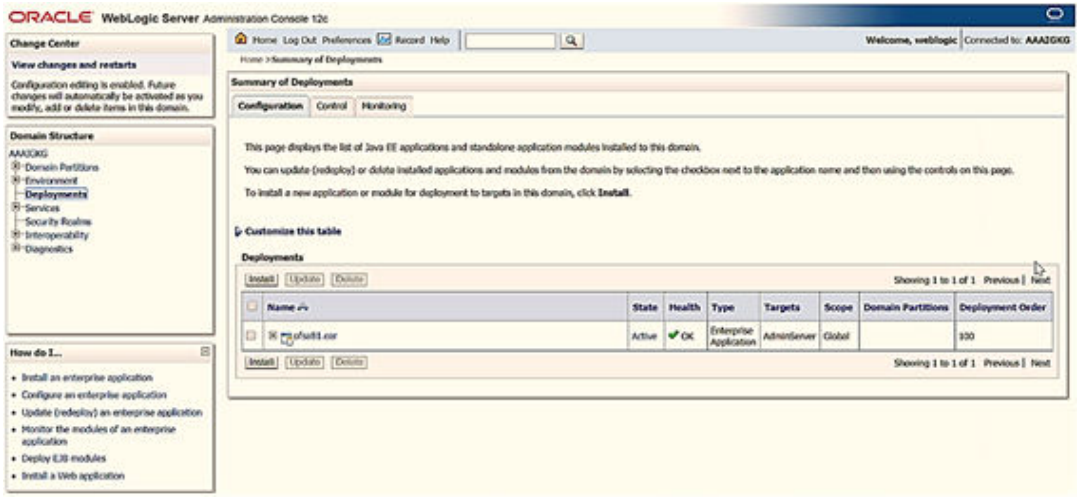
   The Login window of the WebLogic Server Administration Console is displayed.

> **Note:**
>
> Ensure that you have started the Infrastructure Server by executing "./ startofsaai.sh" as mentioned in the Start the Infrastructure Services section.

4. Log in to the WebLogic Server by entering the user credentials with privileges to deploy the EAR file.

5. From the Domain Structure navigation tree, click **Deployments** to display the **Summary of Deployments** window.

Figure 8-19 Summary of Deployments



6. Click **Install** to display the Install Application Assistant window.
7. Navigate to the location where the Exploded EAR directory exists and select it.
8. Click **Next**.

   After the installation is complete, proceed with the following steps to enable your deployment.
9. Go to **Summary of Deployments**, click **Control** tab
10. Select Deployment and click "**Servicing all requests**"

    This will enable the Deployment and set it to **ACTIVE** status from **PREPARED** status.

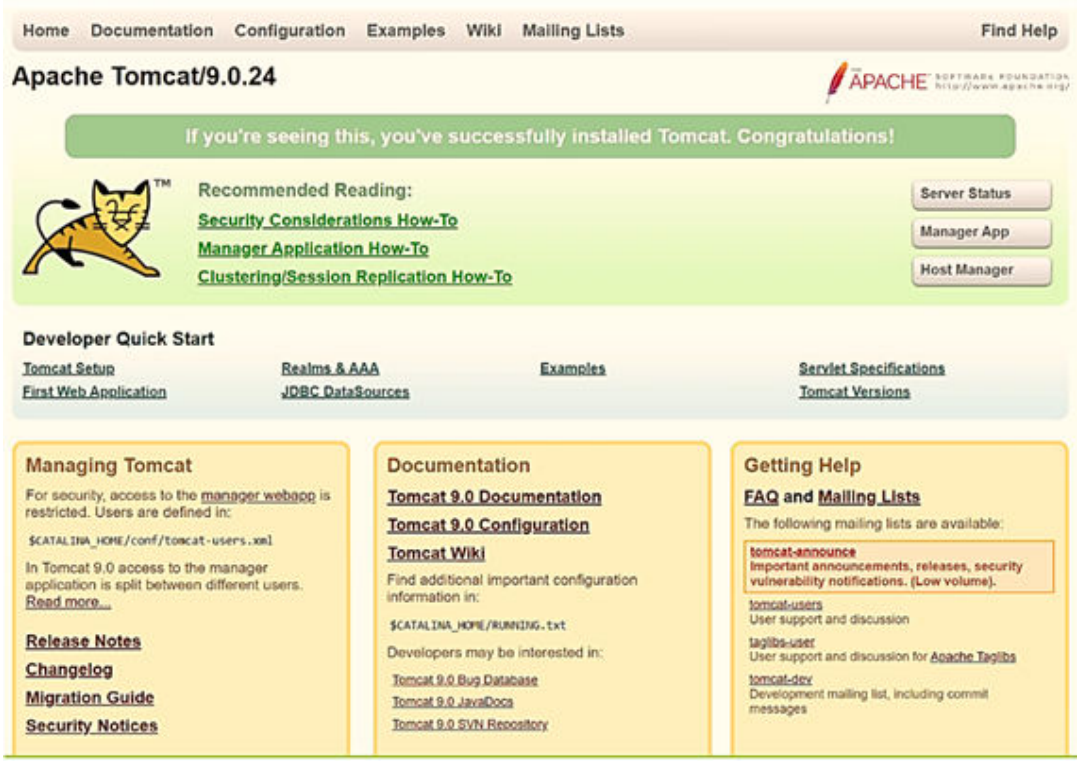
Deploy WAR Files on Tomcat

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

To deploy Infrastructure application on the machine that hosts Tomcat:

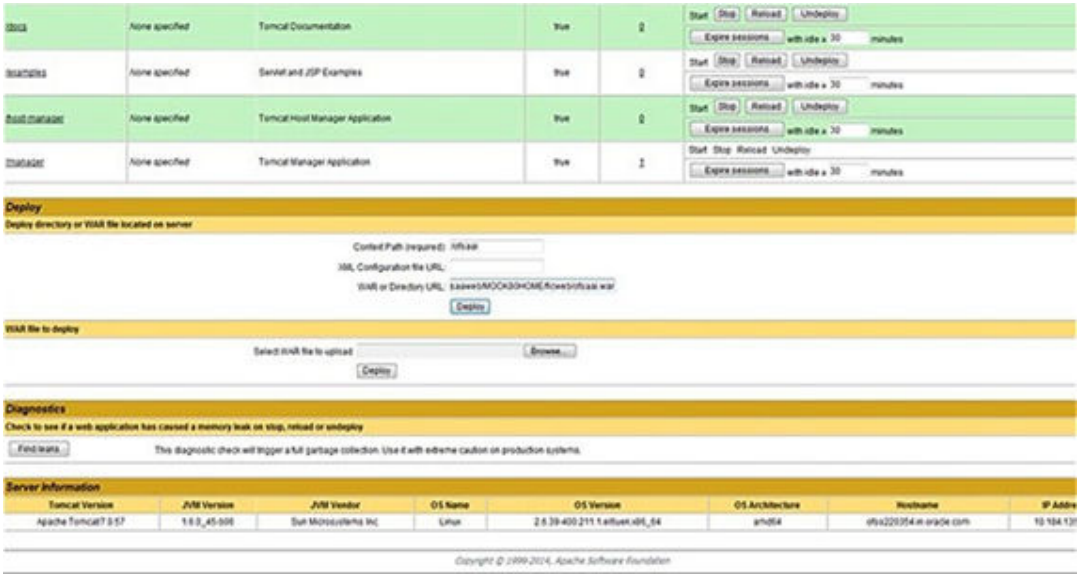
1. Copy the `<context-name>.war` file from `$FIC_WEB_HOME/<context-name.war>` directory to the `<Tomcat Installation Directory>/webapps/`directory.

Figure 8-20 Tomcat Home window



2. Click Manager App to display the Connect to dialog box.
3. Enter the User ID and Password with admin rights and click **OK**. The Tomcat Web Application Manager window is displayed with the list of all the applications deployed. (For user creation in Tomcat, see Tomcat User Administration.)

Figure 8-21 Tomcat Web Application Manager



4. In the Deploy section, enter the Context Path provided during the installation as "/<context-name>".

5. Enter the path where the `<context-name>.war` file resides (by default `$FIC_WEB_HOME/<context-name.war>`) in WAR or Directory URL and click Deploy. On successful application deployment, a confirmation message is displayed.
6. Start the Tomcat server. For more information, see Start the Infrastructure Services.

EAR/WAR File - Build Once and Deploy Across Multiple OFSAA Instances

OFSAA 8.1.2.0.0 supports a single archive deployment model. You can build the EAR/WAR file once and deploy it across multiple OFSAA instances on the same release version.

Prerequisites:

1. The web server type must be the same across all OFSAA instances.
2. The information domain must be the same across all OFSAA instances.

Feature Updates

1. The path of the deployed area log files is in the `AAI_SETUP_PROPS` database table in the Config Schema.
2. The following parameters are moved from the `FICWEB.cfg` file to the `AAI_SETUP_PROPS` table with tier as WEB. The file is removed and the respective parameters are set in the servlet context.
   - `FIC_SERVLET_PORT`reconfigured as `FIC_WEBSERVER_PORT`
   - `ICC_SERVER_PORT`
   - `CSS_LOGGER_PATH`
3. The following values for the AAI servlet configuration parameters in `web.xml` file is moved to the `AAI_SETUP_PROPS` table:
   - `FIC_WEBPROTOCOL`
   - `FIC_PHYSICAL_HOME_LOC`
   - `FIC_WEBSERVER_PORT`
   - `FIC_HOME`
   - `FIC_WEBSERVER_IP`
4. OFSAA environment details used to establish communication between the Web and application layer now moved from the `LookupServices.xml` and `DynamicServices.xml` file to the following database tables:
   - `aai_dyn_svcs_params`
   - `aai_dyn_svcs_servers`
   - `aai_lkp_svcs_servers`

> **Note:**
>
> This change to the configuration XML files is done only at the Web layer deployment location.

Assign Grants for Schemas

This section discusses the various grants required for the Atomic and Sandbox schemas.

Assign Grants for Atomic Schema

Atomic Schema creation requires certain grants for object creation present in the `$FIC_HOME/privileges_atomic_user.sql` file.

To assign grants for the Atomic Schema, execute the following script in the SQL Plus console:

```
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
/
```

Assign Grants for Config Schema

Config Schema creation requires certain grants for object creation present in the $FIC_HOME/privileges_config_user.sql file.

To assign grants for the Config Schema, execute the following script in the SQL Plus console:

```
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 olap_user to &database_username
/
grant select on SYS.V_$PARAMETER to &database_username
/
```

```
grant create SYNONYM to &database_username
/
```

Assign Grants for Config Schema Entities for Atomic Users

Atomic Schema creation requires certain grants for config schema object access present in the $FIC_HOME/config_table_privileges_for_atomic_user.sql file. To assign grants for the Config Schema entities for Atomic Users, execute the following script in the SQL Plus console:

```
grant select on CSSMS_USR_PROFILE to &database_username
/
grant select on CSSMS_ROLE_MAST to &database_username
/
grant select on CSSMS_GROUP_MAST to &database_username
/
grant select on CSSMS_FUNCTION_MAST to &database_username
/
grant select on CSSMS_USR_GROUP_MAP to &database_username
/
grant select on CSSMS_USR_GROUP_DSN_SEG_MAP to &database_username
/
grant select on CSSMS_ROLE_FUNCTION_MAP to &database_username
/
grant select on CSSMS_GROUP_ROLE_MAP to &database_username
/
grant select on CSSMS_SEGMENT_MAST to &database_username
/
grant select on CSSMS_USR_DSN_SEG_MAP to &database_username
/
grant select on CSSMS_USR_ROLE_MAP to &database_username
/
grant select on CSSMS_METADATA_SEGMENT_MAP to &database_username
/
grant select on BATCH_RUN to &database_username
/
grant select on PR2_FILTERS to &database_username
/
grant select on PR2_TASK_FILTER to &database_username
/
grant select on PR2_TASK_FILTER_DETAIL to &database_username
/
grant select on ST_STRESS_MASTER to &database_username
/
grant select on ST_SCENARIO_MASTER to &database_username
/
grant select on ST_SHOCK_MASTER to &database_username
/
grant select on BATCH_MASTER to &database_username
/
grant select on ICC_MESSAGELOG to &database_username
/
grant select on PR2_MASTER to &database_username
/
grant select on PR2_RUN_REQUEST to &database_username
/
grant select on MF_MODEL_SCRIPT_MASTER to &database_username
```

```
/
grant select on MF_INPUT_VALUES to &database_username
/
grant select on MF_MODEL_OUTPUT_VALUES to &database_username
/
grant select on DB_MASTER to &database_username
/
grant select on DSNMASTER to &database_username
/
grant select on pr2_rule_map to &database_username
/
grant delete on pr2_rule_map_pr to &database_username
/
grant insert on pr2_rule_map_pr to &database_username
/
grant update on pr2_rule_map_pr to &database_username
/
grant select on pr2_rule_map_pr to &database_username
/
grant delete on pr2_rule_map_pr_tmp to &database_username
/
grant insert on pr2_rule_map_pr_tmp to &database_username
/
grant update on pr2_rule_map_pr_tmp to &database_username
/
grant select on pr2_rule_map_pr_tmp to &database_username
/
grant select on pr2_rule_map_exclude to &database_username
/
grant delete on pr2_rule_map_exclude_pr to &database_username
/
grant insert on pr2_rule_map_exclude_pr to &database_username
/
grant update on pr2_rule_map_exclude_pr to &database_username
/
grant select on pr2_rule_map_exclude_pr to &database_username
/
grant delete on pr2_rule_map_exclude_pr_tmp to &database_username
/
grant insert on pr2_rule_map_exclude_pr_tmp to &database_username
/
grant update on pr2_rule_map_exclude_pr_tmp to &database_username
/
grant select on pr2_rule_map_exclude_pr_tmp to &database_username
/
grant select on pr2_run_object to &database_username
/
grant select on pr2_run_object_member to &database_username
/
grant select on pr2_run_map to &database_username
/
grant select on pr2_run_execution_b to &database_username
/
grant select on pr2_run_execution_filter to &database_username
/
grant select on pr2_firerun_filter to &database_username
```

```
/
grant select on pr2_filters to &database_username
/
grant select on configuration to &database_username
/
grant select on batch_parameter to &database_username
/
grant select on component_master to &database_username
/
grant select on MDB_OBJECT_TYPE_ATT_LAYOUT to &database_username
/
grant select on REV_OBJECT_ATTRIBUTE_DTL to &database_username
/
grant select on FORMS_LOCALE_MASTER to &database_username
/
grant select on mdb_object_dependencies to &database_username
/
grant select on mdb_execution_details to &database_username
/
grant select on REV_STAT_DATA to &database_username
/
grant select on REV_OBJECT_REPOSITORY_B to &database_username
/
grant select on REV_OBJECT_REPOSITORY_TL to &database_username
/
grant select on REV_OBJECT_ATTRIBUTE_DTL_MLS to &database_username
/
grant select on REV_OBJECT_APPLICATION_MAP to &database_username
/
grant select on MDB_OBJ_EXPR_DETAILS to &database_username
/
grant select on MDB_EXECUTION_DETAILS to &database_username
/
grant select on REV_OBJECT_TYPES_CD to &database_username
/
grant select on REV_OBJECT_TYPES_MLS to &database_username
/
grant select on REV_APPLICATIONS_CD to &database_username
/
grant select on REV_APPLICATIONS_MLS to &database_username
/
grant select on METADATA_BROWSER_LOCALE to &database_username
/
grant select on MDB_STAT_DATA to &database_username
/
grant select on MDB_OBJECT_TYPE_LAYOUT to &database_username
/
grant select on ofsa_md_id_ref to &database_username
/
grant select on MDB_ETL_MAPPING to &database_username
/
grant select on setupinfo to &database_username
/
grant select on LOCALEREPOSITORY to &database_username
/
grant select on MF_MODEL_MASTER to &database_username
```

```
/
grant select on MF_SANDBOX_MASTER to &database_username
/
grant select on MF_VARIABLE_MASTER to &database_username
/
grant select on MF_TECHNIQUE_MASTER to &database_username
/
grant select on MDB_RULE_SOURCE_HEADER to &database_username
/
grant select on MDB_RULE_TARGET_HEADER to &database_username
/
grant select on MDB_RULE_TARGET_MEMBER_HEADER to &database_username
/
grant select on MDB_RULE_GRID_DATA to &database_username
/
grant select on MDB_MODEL_MAPPING to &database_username
/
grant delete on AAI_MAP_MAPPER to &database_username
/
grant insert on AAI_MAP_MAPPER to &database_username
/
grant update on AAI_MAP_MAPPER to &database_username
/
grant select on AAI_MAP_MAPPER to &database_username
/
grant select on RTI_UI_EXCLUDE_PDM_LISTto &database_username
/
grant select on RTI_VIR_PHY_TBL_NAMEto &database_username
/
grant select on infodom_patches to &database_username
/
```

Start the Web Application Servers

Start the required Web application Servers, to run the infrastructure services.

Start WebSphere Profile

Navigate to the `[Webshpere_Installation_Directory] /AppServer/<profiles>/<profile name>/bin` directory, and execute `./startServer.sh server1`.

Start WebLogic Domain

Navigate to the `<WebLogic Installation Directory>/user_ projects/domains/<domain name>/bin` directory, and execute `startWebLogic.sh -d64`.

> **Note:**
>
> If WebLogic is already running, access the WebLogic Admin Console. Stop and start the application `<context name>.ear` file.

Start Tomcat Application

Navigate to the `<Tomcat_Install_ Directory>/bin` directory, and execute `./catalina.sh run`.

Accessing the OFSAA Application

To access OFSAA application:

1. Open a browser and enter the URL in the following format, to view the OFSAA Login window.

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

   For example, `https://192.0.2.2/ofsaa/login.jsp`

   By default, two seeded profiles are configured:

   - SYSADMN System Administrator
   - SYSAUTH System Authorizer

   The SYSADMN and SYSAUTH users are configured with a default password, which you will require to login for the first time. See the MOS Doc ID 2691681.1 for the password.

2. Log in to the application using the **SYSADMN** as the user ID and the default password. After the first login, you are prompted to change the password.

> **Note:**
>
> The password change is required only for a new installation scenario and not for upgrade scenarios.

On successful login, the OFSAA Landing screen is displayed.

Figure 8-22 OFSAA Landing screen

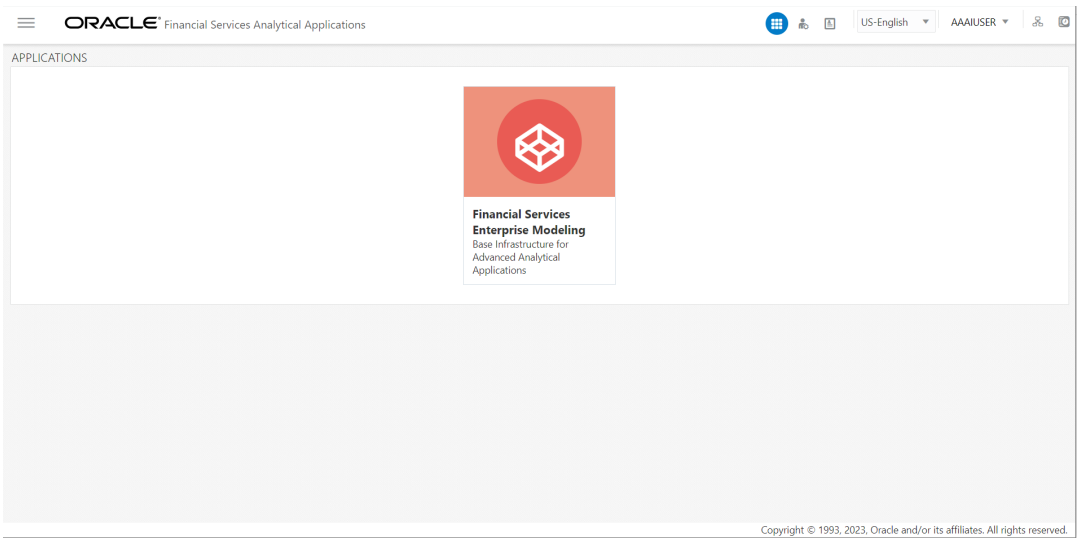
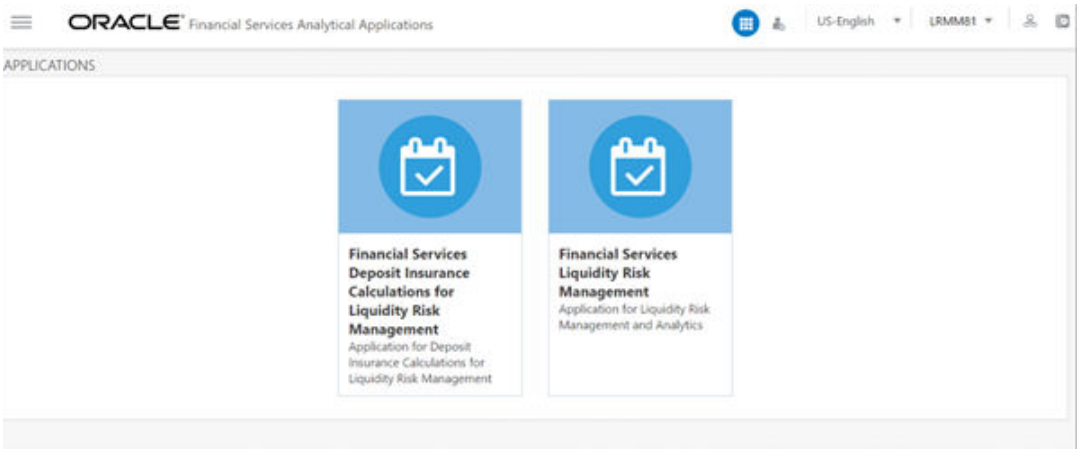


Figure 8-23 OFSAA Landing screen



The available applications are displayed as tiles. Click an application tile to launch that particular application. To customize the landing page click the **Username** and go to **Preferences**. For more information about components of OFSAA landing page, refer OFSAA User guide.

Create Application Users

Create the application users in the OFSAA setup before use. For more information, see the User Administrator section in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

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

Map Application User(s) to User Group

Starting the OFSAA 8.1 release, with the installation of every OFSAA Application Pack, pre-configured application user groups are seeded. These user groups are unique to every OFSAA Application Pack and have application roles pre-configured.

User Groups seeded with the OFSAAAI Application Pack are listed in the Seeded User Groups Table

Table 8-1 Seeded User Groups

Name	Description
Modeler Group	A user mapped to this group has access to all the menu items for Enterprise modeling but does not have authorization rights for sandbox population, model deployment, and modeling technique authorization.

Table 8-1 (Cont.) Seeded User Groups

Name	Description
Modeling Administrator Group	A user mapped to this group has access to all the menu items for Enterprise modeling and has authorization rights for the sandbox population, model deployment, and modeling technique authorization.
Business Administrator	A user mapped to this group has access to all the menu items and actions for the advanced operations of metadata objects.
Business Authorizer	A user mapped to this group has access to all the menu items and actions for authorization of changes to metadata objects.
Business Owner	A user mapped to this group has access to all the menu items and actions for read and write of metadata objects
Business User	A user mapped to this group has access to all the menu items and actions for access and read of metadata objects.
Identity Administrator	A user mapped to this group has access to all the menu items for managing User entitlements, User Group Entitlements, and Access Management configurations.
Identity Authorizer	A user mapped to this group has access to all the menu items for authorizing User entitlements, User Group Entitlements, and Access Management configurations.
System Administrator	A user mapped to this group has access to all menu items for managing the setup configurations.
Object Administrator	A user mapped to this group has access to all menu items for managing object migration and metadata traceability using the metadata browser.
Guest Group	A user mapped to this group has access to certain menu items with 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.

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

Configure Transparent Data Encryption (TDE) and Data Redaction in OFSAA

Two features comprise of Oracle Advanced Security: Transparent Data Encryption and Oracle Data Redaction.

This section details the configurations required in case you want to enable TDE or Data Redaction in OFSAA applications.

- Prerequisites
- Transparent Data Encryption (TDE)

- Data Redaction

Prerequisites

Ensure the required Oracle Database Server versions are installed:

- Oracle Database Server Enterprise Edition 18c Release 3 - 64 bit RAC/Non-RAC with/ without partitioning option, Advanced Security Option.
- Oracle Database Server Enterprise Edition 19c Release 3 - 64 bit RAC/Non-RAC with/ without partitioning option, Advanced Security Option.

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.

To configure TDE for OFSAA, follow these steps:

1. Create a new PDB (19c)/ instance (18c) on the same or different Database Server for TDE. For more information, see Configure 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@OFSA19c2DB 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@OFSA12nDB 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 Steps 1 and 2, retain the user credentials of Configuration and Atomic Schemas the 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:

   ```
   Log in as sys user:
   SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaaconf;
   Grant succeeded
   SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaaatm;
   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, Protocol of the OFSAA Instance* section under *Generic Configurations* chapter in OFS Analytical Applications Infrastructure Administration Guide.
8. Navigate to the `$FIC_WEB_HOME` directory and execute the following command to trigger the creation of the EAR/WAR file:

   ```
   ./ant.sh
   ```

9. The EAR/WAR file - `<contextname>.ear/.war` - is created in the `$FIC_WEB_HOME` directory.
10. On completion of the EAR/WAR file creation, the message "BUILD SUCCESSFUL" is displayed.
11. Edit the existing Connection Pool settings to point to the new JDBC URL and verify connections.
12. Clear the webserver cache and redeploy the application onto your configured web application server.
13. Restart the OFSAA Services. For more information, see Start the Infrastructure Services.

Configure 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.

   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 must have the required privileges to perform the following actions.

To configure the software keystore, follow the instructions in the following sections:

- Set the Software Keystore Location in the sqlnet.ora File
- Create the Software Keystore
- Open the Software Keystore
- Set the Software TDE Master Encryption Key
- Encrypting your Data
- Test the Encryption

Set the Software Keystore Location in the sqlnet.ora File

The first step is to designate a location for the 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 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 a 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)))
  ```

Create the Software Keystore

There are three types of Software Keystores:

- Password-based Software Keystores
- Auto-login Software Keystores
- Local Auto-login Software Keystores

Perform the following steps to create a software keystore:

1. Log in as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. 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 the creation of the keystore. There are no ways to retrieve the password if forgotten.

Open the Software Keystore

Depending on the type of keystore you create, you must manually open the keystore before you can use it.

You must not manually open auto-login or local auto-login software keystores. These keystores 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.

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.

Perform the following steps to open the software wallet:

1. Log in as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. 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 must not manually open auto-login or local auto-login software Keystores.

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. 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.)

Perform the following steps to set the encryption key:

1. Log in as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. 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 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
BACKUPUSING 'emp_key_backup';
```

Encrypt 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:

- Set the COMPATIBLE Initialization Parameter for Tablespace Encryption
- Set the Tablespace TDE Master Encryption Key
- Create the Encrypted Tablespace

Set the COMPATIBLE Initialization Parameter for Tablespace Encryption

Prerequisite: You must set the COMPATIBLE initialization parameter for the database to 12.2.0.0 or later. Once you set this parameter to 12.2.0.0, the change is irreversible.

To set the COMPATIBLE initialization parameter, follow these steps:

1. Log in to the database instance. In a multitenant environment, log into the PDB.
2. Check the current setting of the `COMPATIBLE` parameter.
   For example:

```
SHOW PARAMETER COMPATIBLE
NAME                 TYPE             VALUE
------------------        -----------        -------------------
compatible             string         12.0.0.0
noncdbcompatible         BOOLEAN         FALSE
```

3. If you want to change the COMPATIBLE parameter, perform the following steps:
   - 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`).
   - 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
```

   - Edit the initialization parameter file to use the correct COMPATIBLE setting.
     For example:

```
COMPATIBLE = 12.2.0.0
```

   - 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
```

- 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;
```

Set the Tablespace TDE Master Encryption Key

Make sure that you have configured the TDE master encryption key as shown in the Set the Software TDE Master Encryption Key .

Create the Encrypted Tablespace

After you have set the COMPATIBLE initialization parameter, you are ready to create the encrypted tablespace.

Test the Encryption

Test the encryption by checking if a tablespace is encrypted or not. Execute the following query to check:

```
SELECT tablespace_name, encrypted FROM dba_tablespaces;
```

The following result is displayed, which indicates whether the TABLESPACE is encrypted or not in the ENCRYPTED column.

Table 8-2 Testing the Encryption

TABLESPACE_NAME	ENCRYPTED
SYSTEM	NO
SYSAUX	NO
UNDOTBS1	NO
TEMP	NO
USERS	NO
ENCRYPTED_TS	YES

The above example indicates TABLESPACE `ENCRYPTED_TS` is created with Encryption ON.

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 before display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed into a pattern that does not contain any identifiable information.

To enable Data Redaction, perform the following steps:

1. Log in as SYSDBA into the database.

2. Execute the `$FIC_HOME/utility/data_security/scripts/create_data_sec_ roles.sql` file only once per database (PDB in case of 18c/19c).
3. Execute the following SQL statement to find out the list of atomic users from the table: select v_schema_name from aai_db_detail where V_DB_NAME <> 'CONFIG' AND V_DB_TYPE = 'ORACLE'
4. Execute the `$FIC_HOME/utility/data_security/scripts/grant_data_sec_roles.sql` file 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 enabling Data Redaction, see the *Data Redaction* section in the *Data Security and Data Privacy* topic in the OFS Analytical Applications Infrastructure Administration Guide.

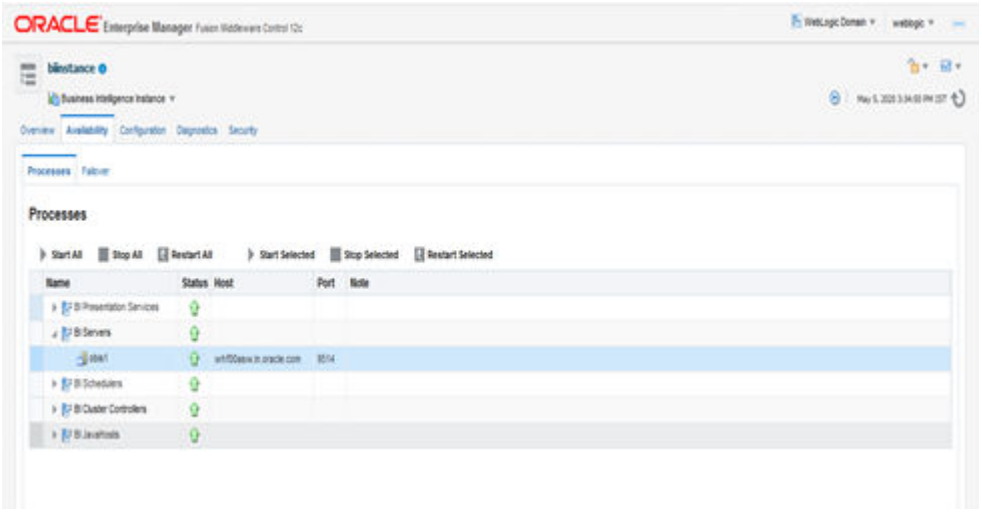
OBIEE Configuration – Deploy OFS LRS Analytics

The OFS LRM Analytics application release 8.1.2.0.0 is based upon a dedicated reporting mart built from the new Fusion Financial Services Data Model. OFS LRM Analytics 8.1.2.0.0 leverages several components of Oracle Business Intelligence Enterprise Edition (OBIEE) or Oracle Analytics Server (OAS) technology including Dashboards and Answers. It also includes various Dashboards and Reports for the user to carry out various Liquidity Gap based analytics.
To configure the OFS LRM Analytics:

1. Make sure Oracle Business Intelligence 12.2.1.4.0 or OAS 5.5.0 installation is completed and available. See the Installing and Configuring Oracle Business Intelligence section or the Installing and Configuring Oracle Analytics Server section for more details.
2. Configure the ODBC data source to connect to the Oracle BI Server:
   a. Navigate to **Control Panel**, select **Administrative Tools**, and then select **Data Sources (ODBC)**.
   b. Select the **System DSN** tab and click **Add**.
   c. Select a driver-specific to **Oracle BI Server 2.2.1.4.0** or **OAS 5.5** and click **Finish**.
   d. Enter the **Name** and **Server** details (specify the Hostname or IP Address of the BI Server) and click **Next**.
   e. Enter the Oracle BI Server login ID and password (Enter the User Name and Password created at the time of OBIEE or OAS installation). Update the port with the port number available for the BI Server in the **Availability** tab of Business Intelligence in the Enterprise Manager.

      For example: In the following figure, the port number is 9514.

Figure 8-24 Update Port Number in the BI Server



f. Click **Next**.

g. Navigate to the RPD and Catalog folders available in the following directories. Copy the RPD and required Catalog files (as per the license agreement) in the server where the BI client tools are installed:

- `$FIC_HOME/OFS_LRM_DASHBOARDS/12.2.1.4.0/datamodel` directory containing the `Liquidity_Risk_Management_Pack.rpd` file in the data model directory.
- `Liquidity_Risk_Management_Pack.catalog`, `Bank of Thailand.catalog`, `BNM.catalog`, `Deposit Insurance.catalog`, `HKMA.catalog`, `RBI.catalog`, and `USFED.catalog` files in the `$FIC_HOME/OFS_LRM_DASHBOARDS/12.2.1.4.0/content/catalog` directory.

h. Click **Finish**.

3. Modify the connection pool and set the properties.

a. Open the OBI Administration tool.

b. Select **Start**, select **Programs**, select **Oracle Business Intelligence**, and then select the **BI Administration**.

c. Select **File**, select **Open**, select **Offline**, and then select the `Liquidity_Risk_Management_Pack.rpd` file.

d. In the Open dialog box, select and open the `Liquidity_Risk_Management_Pack.rpd` file.

e. Enter the Repository password. See the MOS Doc ID: 2691681.1 for the password

f. In the **Physical** layer, double-click the **Connect Pool**: LRMBI to open its properties.

g. In the **General** tab, edit and check the following entries:

i. **Call Interface**: (OCI 10g/11g).

ii. **Data source name**: `<TNS Entry connecting to OFSAA atomic schema>`
For example: `(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<Database IP address>)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=<Database Name>)))`

iii. **User name**: <enter atomic db user name>.

iv. **Password**: <enter atomic db user password>.

v. Confirm the password and click **OK** to close the window.

vi. Similarly, configure the connection pools for *LRMBITRANS* and *LRMBI_INIT_BLOCK* and *LRMBI*.

- Check **Global Consistency**, that is, press *Ctrl+k*.
- Double-click on the warning (if you are using OAS).
- Click **Reset to defaults** and click **OK**.
- Click **Save**.

h. Click **Yes** for the Global Consistency Message. No warnings should be generated at this stage.

i. Close the RPD file (close the file and exit).

4. Log in to the OFS LRM Analytics application using the URL: `http://<ipaddress>:<port>/analytics` (replace the port number based on your setup).

5. Follow these steps to configure the BI publisher Data Source:

a. Log in to the OFS LRM Analytics application

b. Navigate to **Administration**, select **BI Publisher**, and then select **Manage BI Publisher**.

c. Click **JDBC Connection** from Data Sources.

d. Click **Add Data Source**.

e. Enter the Data Source name as **LRM**.

f. Add Database details in the Connection string, that is the hostname (IP address), port number, and SID.

g. Enter the username (schema name) and password.

h. Click **Test Connection**.

i. Ensure that the connection successfully established. Click **Apply**.

6. Follow these steps to implement the Writeback feature:

a. Add the tag `<LightWriteback>true</LightWriteback>` in between `<ServerInstance></ServerInstance>` in the `instanceconfig.xml` file.

For example:

```
<ServerInstance>
<LightWriteback>true</LightWriteback>
</ServerInstance>
```

b. Copy the writeback.xml file available in the `$FIC_HOME/OFS_LRM_DASHBOARDS/12.2.1.4.0/content/msgdb/ directory` to the following OBIEE server directories. If the `customMessages` directory is not present, create the directory manually.

Path1: `<BI Domain Home>/bidata/components/OBIPS/custommessages`

For example: `/scratch/oraobiee/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/bidata/components/OBIPS/custommessages`

Path2: `<BI Domain Home>/bidata/service_instances/ssi/metadata/content/msgdb/l_en/customMessages`

For example:

```
/scratch/oraobiee/Oracle/Middleware/Oracle_Home/user_projects/domains/bi/
bidata/service_instances/ssi/metadata/content/msgdb/l_en/customMessages
```

c. Restart the **BI Services**.

d. Login to **OBIEE Analytics** and navigate to the **Administration** section on the right top corner.

e. Click **Manage Privileges** and scroll down to **Writeback**.

f. Grant **Writeback to Database** privilege to Authenticated User and BI Administrator roles.

7. Perform the following OBIEE presentation server configuration steps:

a. Navigate to the `<<Oracle BI Instance Home>/config/fmwconfig/biconfig/OBIPS` directory.

b. Edit the `instanceconfig.xml` file.

c. Insert the following code within the XML tag <Views> </Views>.

- ```
  <Charts>
  <MaxVisibleColumns>50000</MaxVisibleColumns>
  <MaxVisiblePages>25000</MaxVisiblePages>
  <MaxVisibleRows>10000000</MaxVisibleRows>
  <MaxVisibleSections>50000</MaxVisibleSections>
  <JavaHostReadLimitInKB>10240</JavaHostReadLimitInKB>
  </Charts>
  ```

- ```
  <Table>
  <DefaultRowsDisplayedInDelivery>75</DefaultRowsDisplayedInDelivery>
  <DefaultRowsDisplayedInDownload>6500</
  DefaultRowsDisplayedInDownload>
  <MaxCells>4000000</MaxCells>
  <MaxVisibleRows>140000</MaxVisibleRows>
  </Table>
  <Narrative><MaxRecords>500000</MaxRecords>
  <DefaultRowsDisplayed>25</DefaultRowsDisplayed>
  </Narrative>
  ```

d. Save the file and restart the BI services.

> **Note:**
>
> Take a backup of the `instanceconfig.xml` file before making any changes.

9
Upgrade

Upgrading the application pack from Release 8.1.1.0.0 or later to Release 8.1.2.0.0.

To upgrade the application pack to Release 8.1.2.0.0:

- Run the Environment Check Utility tool and ensure that the hardware and software requirements are installed in accordance with the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix.
- Trigger the installation.

> **Note:**
>
> If you want to upgrade from Release v8.0.x of OFS AAAI on AIX or Solaris x86 Operating System, skip the other upgrade topics in this guide and see the instructions in the Migration Guide.

Prepare for Upgrade

Prerequisites for installing/upgrading any application packs to Release 8.1.2.0.0.

Before you plan to install/upgrade any of your application packs to Release 8.1.2.0.0, ensure that all the application packs in your current OFSAA instance are available in the Release 8.1.2.0.0 version. Contact My Oracle Support or more information about the release version details.

> **Note:**
>
> The minimum supported version is 8.0.6.1.0. If you are upgrading from a release before v8.0.6.1.0, then first upgrade to v8.0.6.1.0 or later. After this step, you can upgrade to v8.1.2.0.0 or later.

> **Note:**
>
> - Ensure to revert any customized data model changes done without performing data model upload before upgrading.
> - If you have defined any custom run purpose, ensure to take a backup of the tables FSI_LRM_LOOKUP_TL and FSI_LRM_PROCESS_PURPOSE_MAP, before you run the upgrade.

1. Backup the following environment files from their respective directories:
   - The Database

- The following environment files from the `<OFS_AAAI_PACK>/schema_creator/conf directory`:
  - `OFS_<App pack>.xml`
  - `OFS_<PACK>_SCHEMA_IN.xml`
  - `OFSAAI_InstallConfig.xml`

2. See the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix for the hardware and software required to upgrade to OFS AAAI Release 8.1.2.0.0.
3. Enable unlimited cryptographic policy for Java. For more information, see the Enabling Unlimited Cryptographic Policy section in the OFS Analytical Applications Infrastructure Administration Guide.
4. Clone your environment. For more information, see the OFSAA Cloning Reference Guide.
5. Execute the following SQL query on the Atomic Schema:

```
update rev_tables_b set version=0 where version is null;
commit;
```

Download the OFSAAAI Applications Pack Installer and Mandatory Patches

To download the OFSAAAI Applications Pack Installer Release 8.1.2.0.0:

1. Log in to My Oracle Support and search for 32791983 in the Patches & Updates Tab.
2. Download the installer archive and copy (in Binary mode) to the download directory that exists in the OFSAAAI installation setup.

> **Note:**
>
> Select the required archive files for either Solaris SPARC or Linux based on the operating system of your OFSAAAI.

3. Log in to My Oracle Support, search for the 33663417 Mandatory Patch in the Patches & Updates Tab and download it.

> **Note:**
>
> On the 10th of December 2021, Oracle released Security Alert CVE-2021-44228 in response to the disclosure of a new vulnerability affecting Apache Log4J before version 2.15. The application of the **33663417** Mandatory Patch fixes the issue.
>
> For details, see the My Oracle Support Doc ID 2827801.1.
>
> Ensure that you reapply the **33663417** Mandatory Patch whenever you install or upgrade the application, or apply an incremental patch.

Extract the Software

Extract the installation software.

Ensure you are logged in to the UNIX operating system as non-root user to extract the software.

To extract the software:

1. Download the unzip utility (OS-specific) `unzip_<os>.zip` and copy it in Binary mode to the directory included in your PATH variable.

   If you already have an unzip utility to extract the contents of the downloaded archive, skip this step. Uncompress the unzip installer file:

   ```
   uncompress unzip_<os>.zip
   ```

   > **Note:**
   >
   > If you encounter the error `uncompress: not found [No such file or directory]`, contact your UNIX administrator.

2. Assign execute (`751`) to the file: `chmod 751 unzip_<OS>`

   For example: `chmod 751 unzip_sparc`

3. Extract the contents of the Application Pack Release 8.1.2.0.0 installer archive file in the download directory:

   ```
   unzip OFS_AAAI_PACK.zipUnzip <name of the file to be unzipped>.zip
   ```

4. Navigate to the download directory and assign execute permission to the installer directory:

   ```
   chmod -R 750 OFS_AAAI_Packchmod -R 755 OFS_LRS_PACK
   ```

   > **Note:**
   >
   > For Solaris OS, download, extract and apply the one-off patch 31509494 from My Oracle Support. See the Readme packaged with the patch for further instructions on how to install the patch.

5. Give execute permission to the archive file. Navigate to the path where the directory OFS_LRS_PACK exists and execute the command:`chmod -R 755 OFS_LRS_PACK`
6. Execute the user .profile file.
7. Navigate to the /OFS_LRS_PACK/schema_creator/conf directory and modify the OFS_LRS_SCHEMA_IN.xml file by providing the existing values to the parameters JDBC_URL, JDBC_DRIVER, Host, Setupinfo name, schema names (config and atomic), password, default tablespace, Infodom, Quota as per the previous version.
8. Navigate to the /OFS_LRS_PACK/schema_creator/bin directory and execute the osc.sh file using the following command: `./osc.sh -s`

> **Note:**
>
> Steps 7 and 8 are required to generate the OFS_LRS_SCHEMA_OUTPUT.xml file.

After assigning the required permissions, proceed with the Installation Tasks.

Trigger the Upgrade Installation

Trigger the upgrade installation.

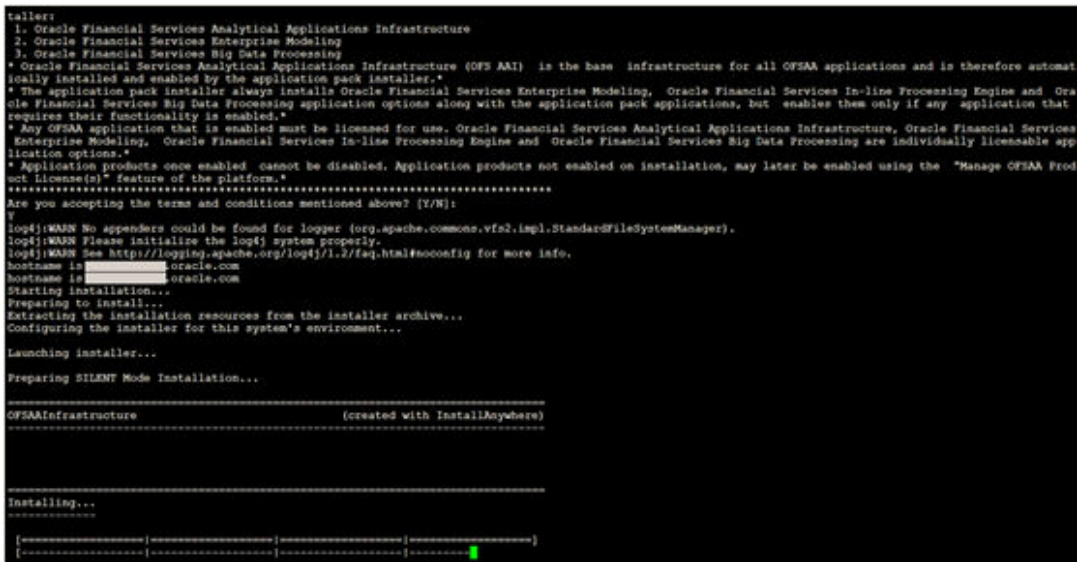
To trigger the installation:

1. Navigate to `OFS_APP_PACK/bin` and enter the following command in the console to execute the application pack installer with the Silent option.

   ```
   ./setup.sh SILENT
   ```

2. The installer proceeds with the pre-installation checks and starts the upgrade installation process.
3. The OFS application installation begins.

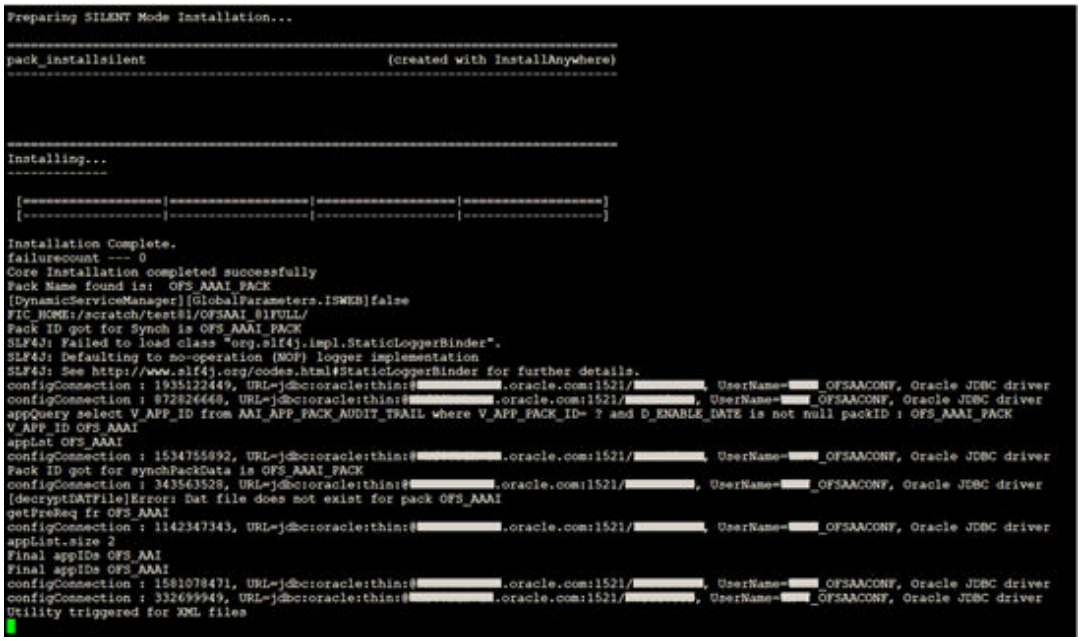
Figure 9-1 OFS AAAI Silent Mode Installation



Data Model Upload may take several hours to complete. You can check the installation logs in the following location: OFS_AAAI/OFS_AAAI/logs

4. The OFSAA Infrastructure installation performs a post-install check automatically on the successful installation of the product.

Figure 9-2 Silent Mode Installation In Progress



5. The OFS LRS installation or upgrade begins. After the installation is complete, an Installation Successful message is displayed.

Congratulations! Your installation is complete.

Verify the Log File Information

After installing the OFSAAI upgrade, verify the log files.

See the following logs paths for more information:

- See the `Pack_Install.log` file in the `OFS_AAI/logs/` directory for installation status and errors.
- Verify if the release is applied successfully by checking the log file generated in the locations mentioned in section #unique_154.
- Verify the OFSAAI log files from the OFS_LRS_PACK/OFS_AAAI_PACK/logs directory.
- Verify the Model Upload log file available in the ftpshare/<INFODOM>/logs directory.
- Verify if the Data Model is uploaded successfully by checking the log file generated as per the directory or path mentioned in the Silent.props file.
- Ignore the error codes **ORA-00001**, **ORA-00955**, **ORA-01430**, and **ORA-02292** in the log file. For any other error, contact My Oracle Support.
  - You can ignore the `ORA-00001` error in the log file available in the path `OFS_LRS_PACK/schema_creator/logs`.

> **Note:**
>
> – Ignore all the warnings in the installation log. For any issues contact My Oracle Support.
>
> – After upgrading any OFSAA Application or OFSAA Application Pack to the 8.1.2.0.0 version, if the invalid identifier error occurs with the error code `ORA-00904` for the `update-description-msg-oth.sql` seeded script file, ignore the error.

- Verify if the Data Model is uploaded successfully by checking the log file generated as per the directory or path mentioned in the Silent.props file.

Post Installation Steps

After removing the OFSAAI Application pack, proceed with the following post-installation tasks.

For completing the post installation steps, refer to Post Installation Tasks.

Upgrade OFS AAAI from Linux 7 to Linux 8

Upgrading the OFS AAAI from Linux 7 to Linux 8.

If your OFS AAAI instance is on Linux 7 Operating System and you want to install OFS AAAI on Linux 8.

To upgrade the OFS AAAI environment from Linux 7 to Linux 8, follow these steps:

1. Clone your existing environment to the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix.
2. Run the upgrade installer in the cloned environment.
3. For detailed steps, see the sections 8.2 to 8.6.

10

Configure Web Servers

Configure Weblogic, Websphere or Apache Tomcat for Application deployment during OFSAA installation.

> **Note:**
>
> - To enable a sticky session/affinity session configuration on the web server, see the respective product-specific Configuration Guide for more details. Also, enable the sticky session/ affinity session configuration at the Load Balancer level if you have configured a Load Balancer in front of the Web server.
> - Note down the IP Address/ Hostname and Port of the Web application server. This information is required during the installation, 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 Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix for the hardware and software required.

To manage the security configurations of your Web server, refer to OFSAAI Security Guide.

Configure WebSphere Application Server

Follow these instructions to configure and deploy the application server.

Configure WebLogic Server

Follow these instructions to configure and deploy the application server.

Configure Tomcat Server

Follow these instructions to configure and deploy the application.Configure Apache Tomcat Server for Application Deployment

Configure Infrastructure Server Memory

Configure the memory settings for Infrastructure Application Server, Tomcat, WebSphere, and WebLogic, for customizing memory settings and garbage collector settings depending on the available hardware configuration.

These memory settings are the bare minimum and have 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 the stack.

To configure the Infrastructure Application Memory settings:

- Locate the `.profile` file and edit `X_ARGS` field for customizing memory settings and garbage collector settings based on the hardware configuration.

  The default value is `X_ARGS="-Xms200m" X_ARGS=" "$X_ARGS" $DELIM -Xmx2048m"`

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

  For Run and Rule executions, the recommended values are:

```
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"
```

Configure WebSphere for Application Deployment

Deploy multiple OFSAA applications on different profiles of a stand-alone WebSphere application server.

A profile is the set of files that define the runtime environment. At least one profile must exist to run the WebSphere Application Server.To create multiple WebSphere Profiles in a stand-alone server, using the command line utility:

- 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
- Configure WebSphere Application Server Persistence to JPA Specification 2.0
- Configure WebSphere Application Server to Use a Load Balancer or Proxy Server
- Delete WebSphere Profiles
- Configure WebSphere HTTPS
- Configure WebSphere Memory Settings
- Configure WebSphere for Rest Services Authorization

Create New Profile in WebSphere

A profile is the set of files used to define the run-time environment.

Create a new profile in WebSphere through the command line using the `manageprofiles.sh` present in the `<WebSphere Install directory>/AppServer/bin` directory.

To create a profile without admin security:

```
"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
```

To create a profile with admin security :

```
"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 <baseport>` which specifies the starting port number to generate and assign all ports for the profile.

Set Java Version

Configure the Java version.

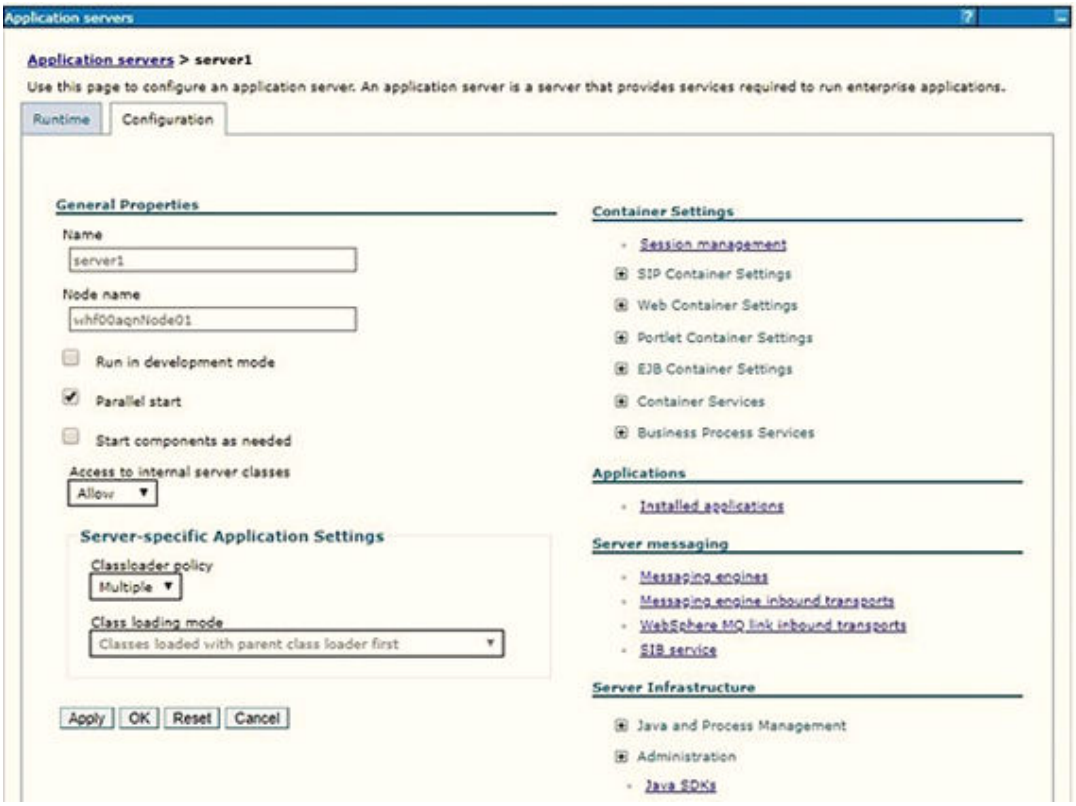
To set the Java version to JAVA 8.X SDK:

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. 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 in the following figure:

Figure 10-1 Application Server Java SDKs



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

Figure 10-2 Application Server List of Java SDKs

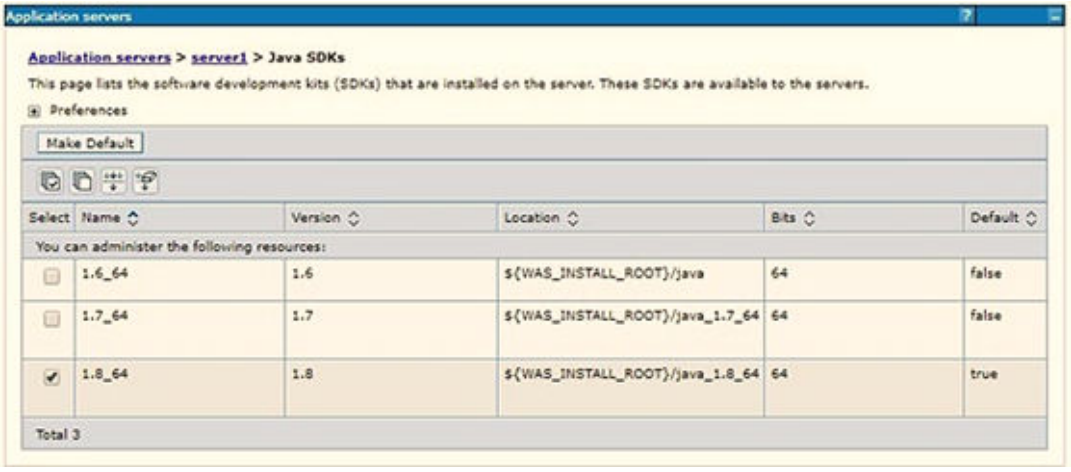
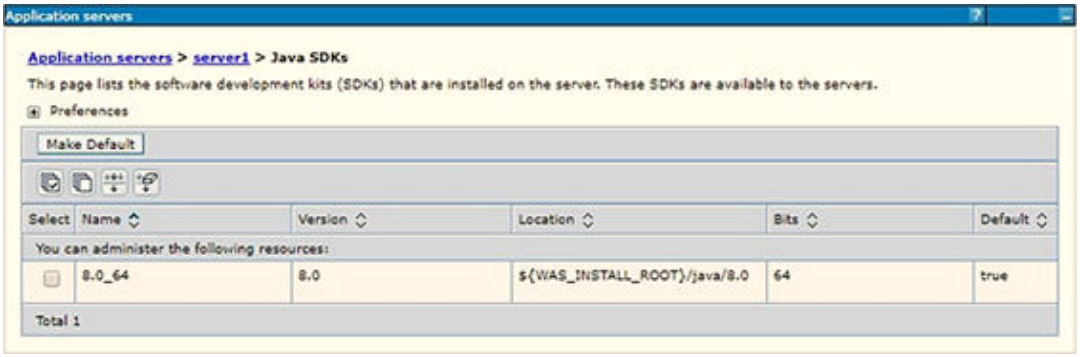


Figure 10-3 Application Server List of Java SDKs



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.

Manage Installed Applications

Manage the installed applications in WebSphere.

To manage the installed applications in WebSphere:

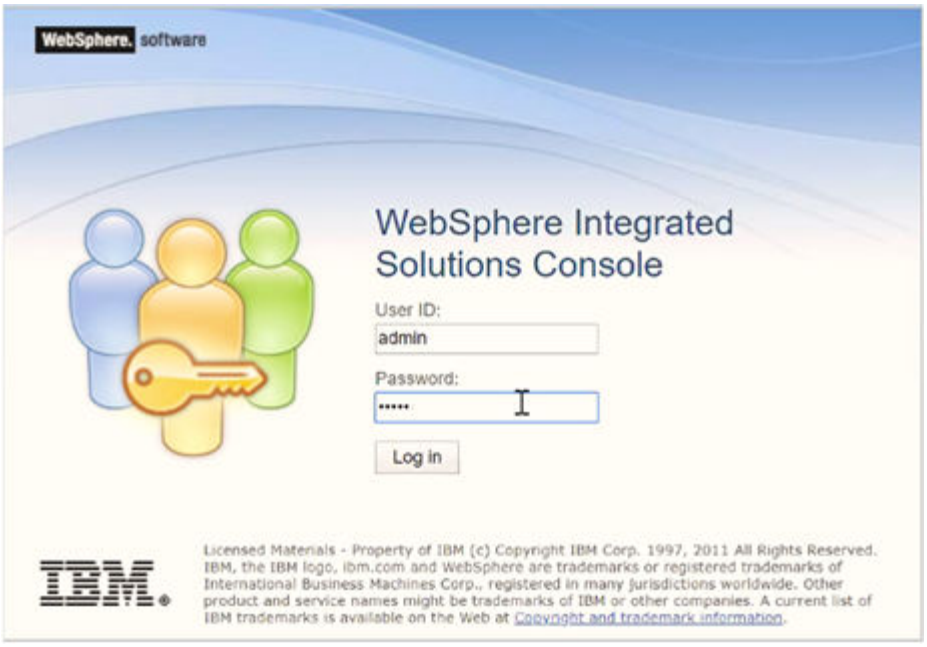
1. Open the administrator console using the URL `http://<ipaddress>:<Administrative Console Port>/ibm/console`.

   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.

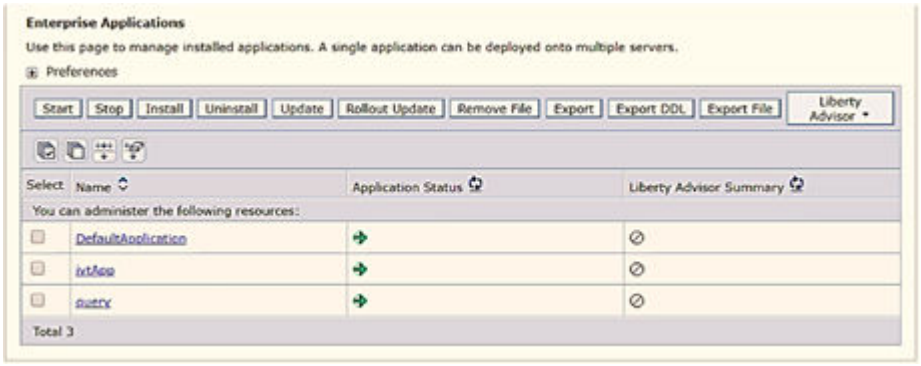
   The Integrated Solutions Console Login window is displayed.

Figure 10-4 Integrated Solutions Console Login



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

Figure 10-5 Enterprise Applications



This Enterprise Applications window enables you to:

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

Initialize Filters

Configure WebSphere Application server to Initialize Filters before initializing Load-On-Startup Servlets and allowing empty servlets maps.

This is a mandatory configuration for OFSAA with WebSphere for both fresh installations and upgrades.

To configure the custom properties for filters:

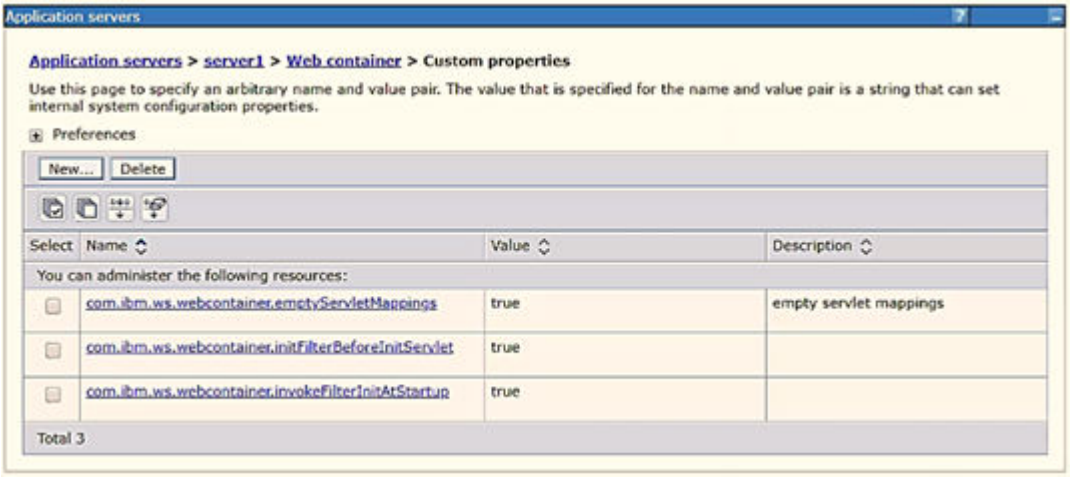
1. Enter the WebSphere URL in the format `http://HOST_NAME:PORT_ NUMBER/ibm/console` (use https if SSL is enabled.).

   For example, `http://192.168.1.0:9000/ibm/console`.

2. Log in with your administrator user ID and password.
3. From the left 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 **Web Container Settings** and then **Custom Properties** to view the **Custom Properties** window.

   Web Container Initialize Filters Before Servlet

Figure 10-6 Web Container Initialize Filters Before Servlet



7. 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.

Server Persistence

Configure WebSphere Application server persistence to JPA specification 2.0.

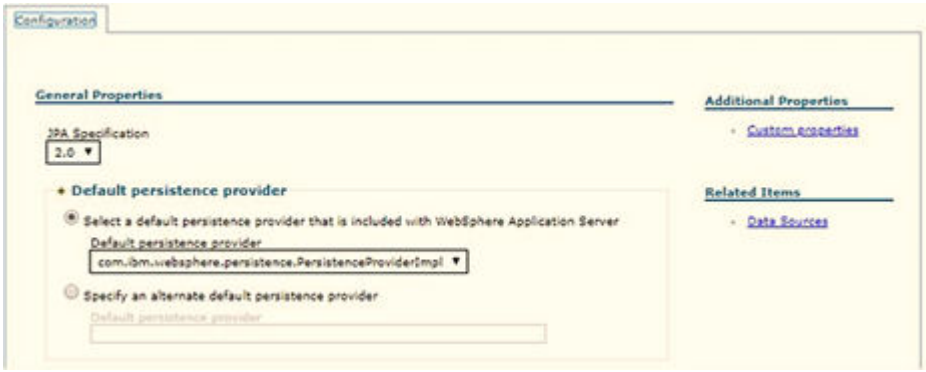
This is a mandatory configuration for OFSAA with WebSphere for both fresh installation and upgrades.

To set the JPA 2.0 as the default persistence provider:

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:

Figure 10-7 Default Java Persistence Settings JPA Specification 2.0



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.

Prevent Process Server Redirection

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

To configure the WebSphere Application server to use a load balancer or proxy server:

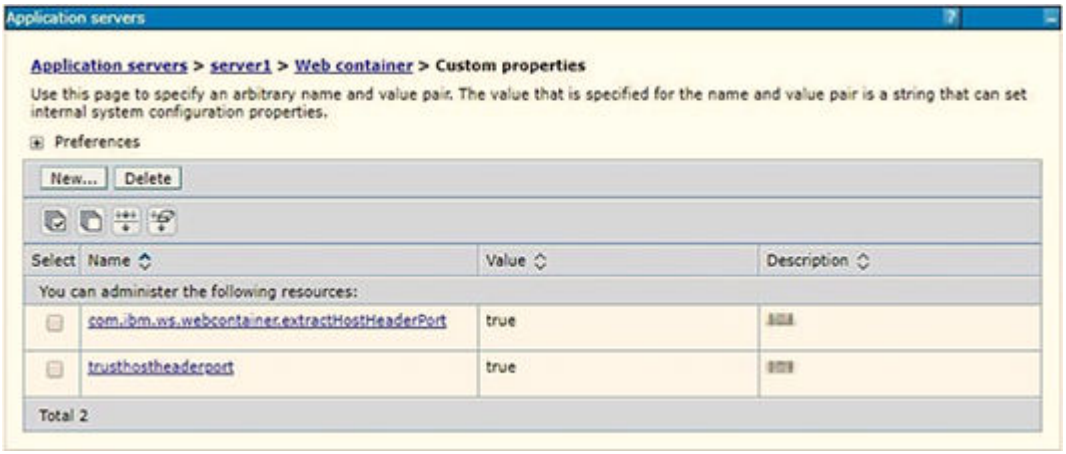
1. Enter the WebSphere URL in the format `http://HOST_NAME:PORT_NUMBER/ibm/console` (use https if SSL is enabled.).

   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.

Figure 10-8 Application Servers Load Balancer Proxy Server



7. Click **New** and enter the following properties:
   - `com.ibm.ws.webcontainer.extractHostHeaderPort: true`
   - `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.

Enable Sticky Session/Affinity Session

Enable the sticky session/affinity session configuration.

Enable the sticky session/ affinity session configuration at the Load Balancer level if you have configured a Load Balancer in front of the web server. See the respective product-specific Configuration Guide to enable a sticky session/affinity session configuration.

Configure 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.

Configure 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

Authorize REST Services

For more information, see the OFS Analytical Applications Infrastructure Administration Guide.

Configure Application Security

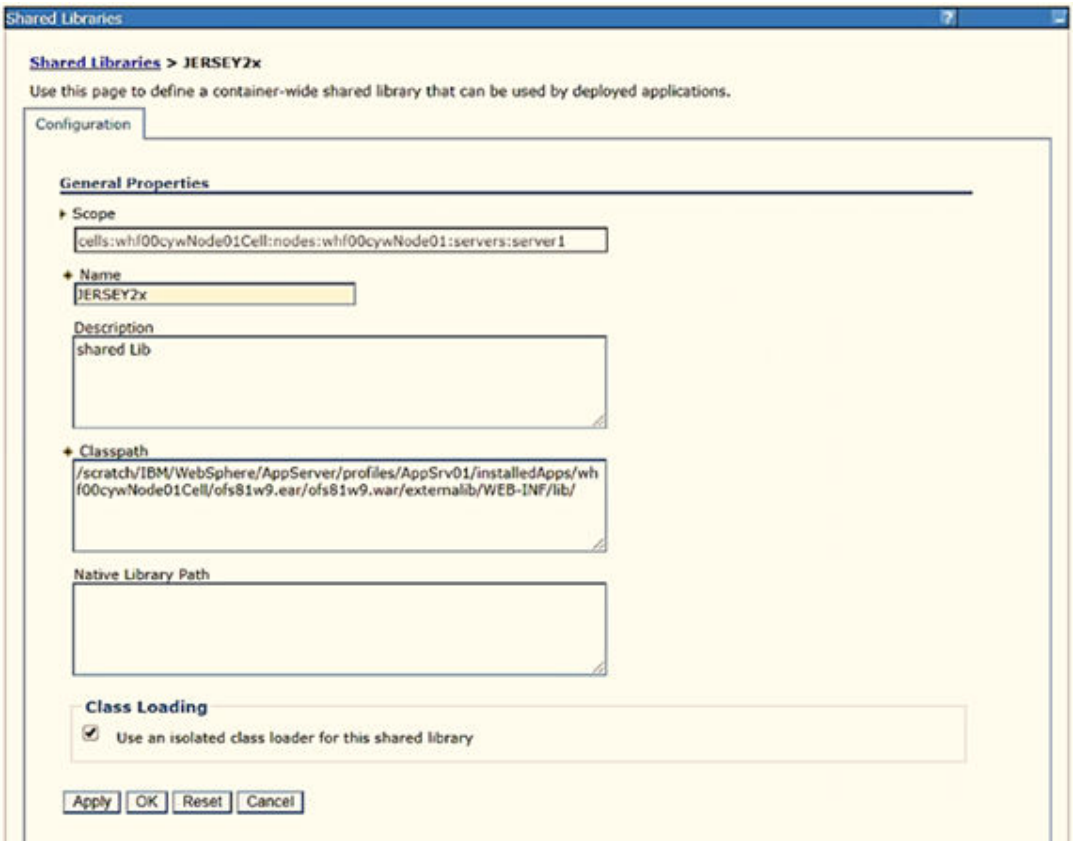
This is a mandatory security procedure for WebSphere to restrict the unauthorized access of configuration files in directories. For detailed information, see the Oracle Financial Services Analytical Applications Infrastructure Security Guide.

Configure Shared Library

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

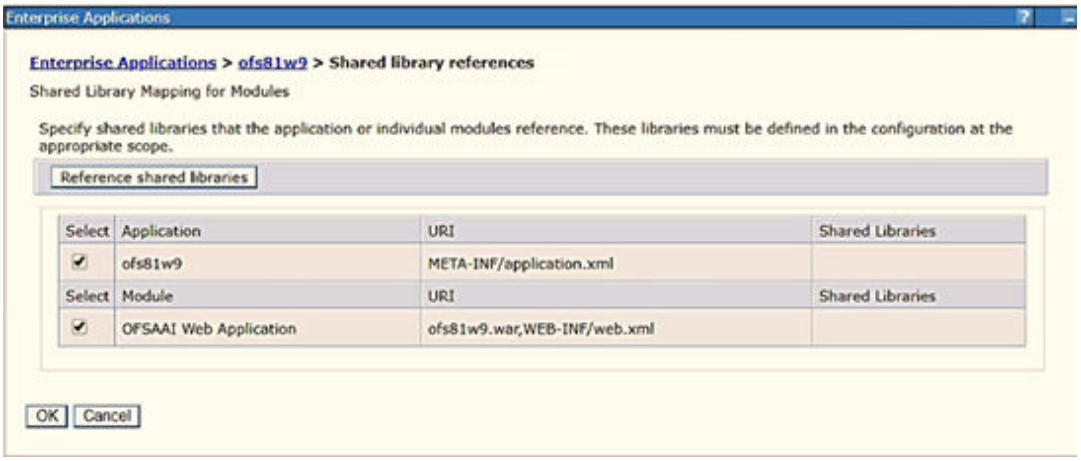
1. Click **Environment** from the menu on the left to expand and view the list. Click **Shared Libraries** to open the Shared Libraries window.

Figure 10-9 WebSphere Shared Libraries



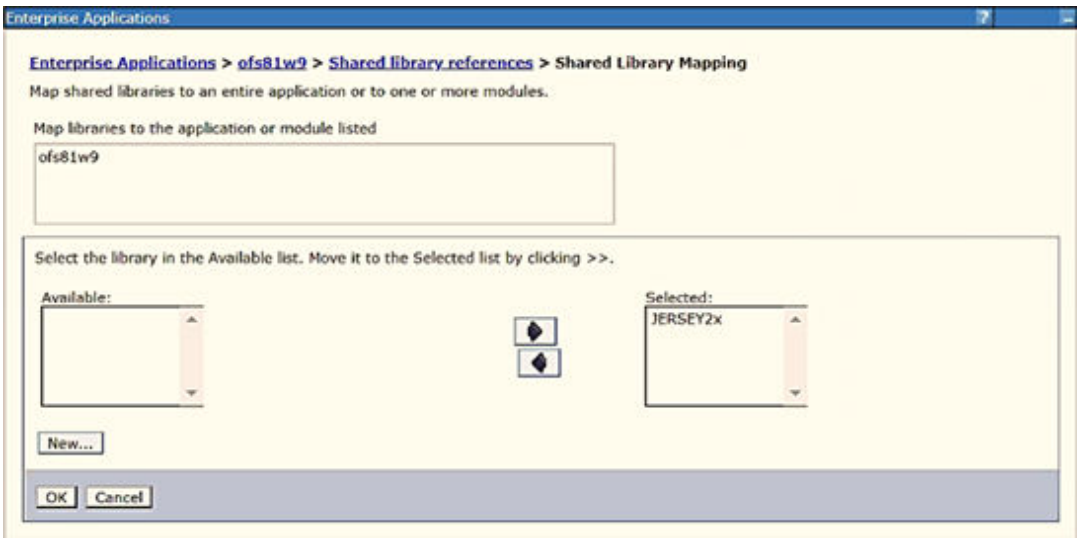
2. Enter the following details:
   a. **Name**: Enter a uniquely identifiable name.
   b. **Description**: Enter a valid description.
   c. **Classpath**: Enter the absolute path where the JARs related to Jersey 2.x and Jackson 2.9x are copied. These jars are available in the `<OFSAA_HOME>/ficweb/webroot/externallib/WEBINF/lib/` 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. In the following figure, ofsa is selected.

Figure 10-10 WebSphere Shared Library References



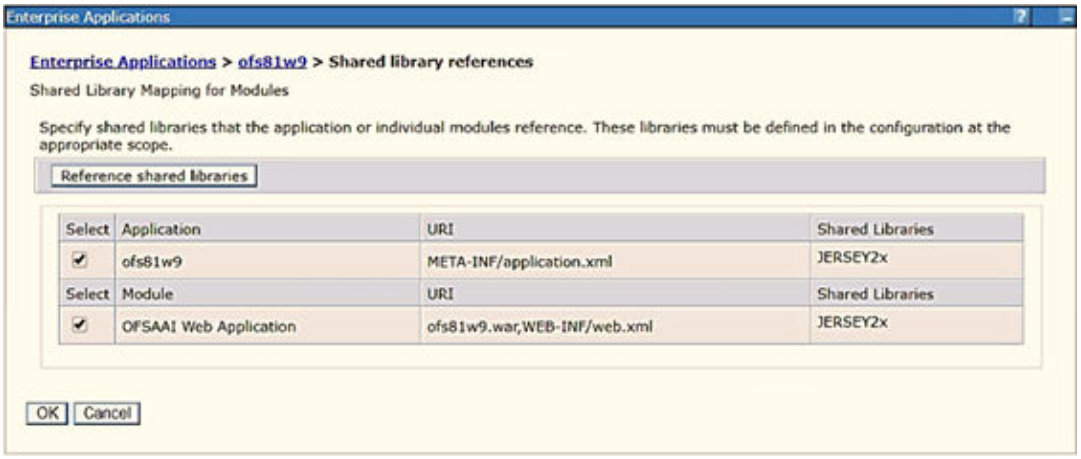
6. From the Shared Library Mapping window, move the required shared libraries from **Available** to **Selected**. In the following figure, JERSEY2x is selected.

Figure 10-11 WebSphere Shared Libraries Mapping Selection



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

Figure 10-12 WebSphere Shared Libraries Select Next Application



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:

      ```
      com.ibm.websphere.jaxrs.server.DisableIBMJAXRSEngine=true
      ```

10. Restart the application.

Configure IBM WebSphere Application Server

Resource Reference for WebSphere

Create a JDBC Provider

Create a JDBC Provider in WebSphere Application Server.

To create the JDBC Provider in WebSphere Application Server:

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

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

2. Log in with the user ID that has admin rights.
3. Expand the **Resources** option in the LHS menu and click **JDBC > JDBC Providers** to access the **JDBC Providers** window.
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 add the new JDBC Provider under the Preferences section. The **Create new JDBC Provider** window is displayed.
6. Enter the following details:
   a. **Database Type**: Oracle
   b. **Provider Type**: Oracle JDBC Driver

c. **Implementation Type**: Connection pool data source

d. **Name**: The required display name for the resource.

e. **Description**: The optional description for the resource.

7. Click **Next**.
8. 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.

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

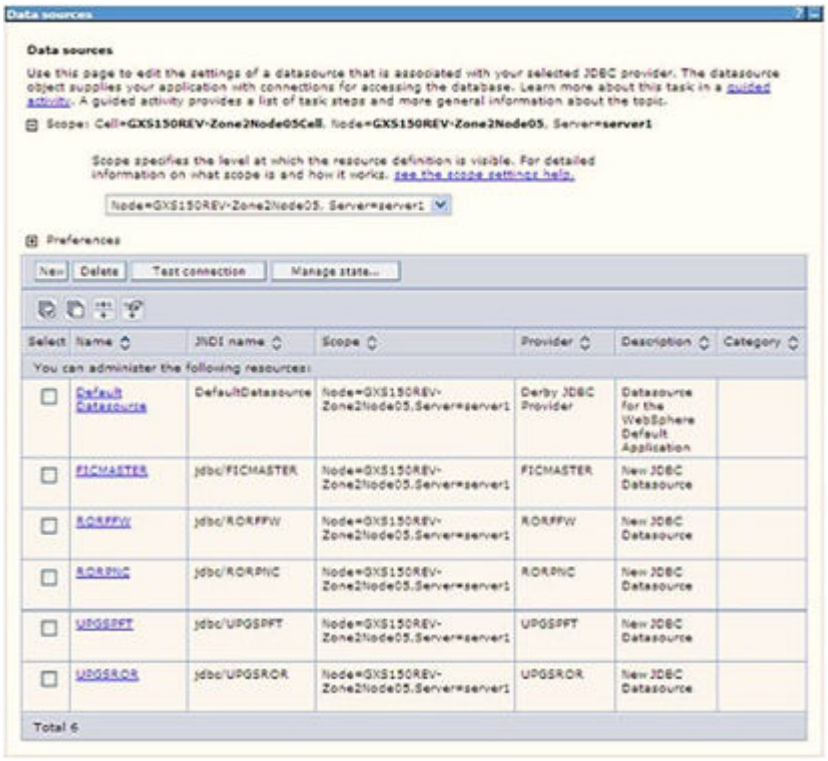
Create Data Source

Create a data source. This process is applicable to both config and atomic data source creation.

To create the data source:

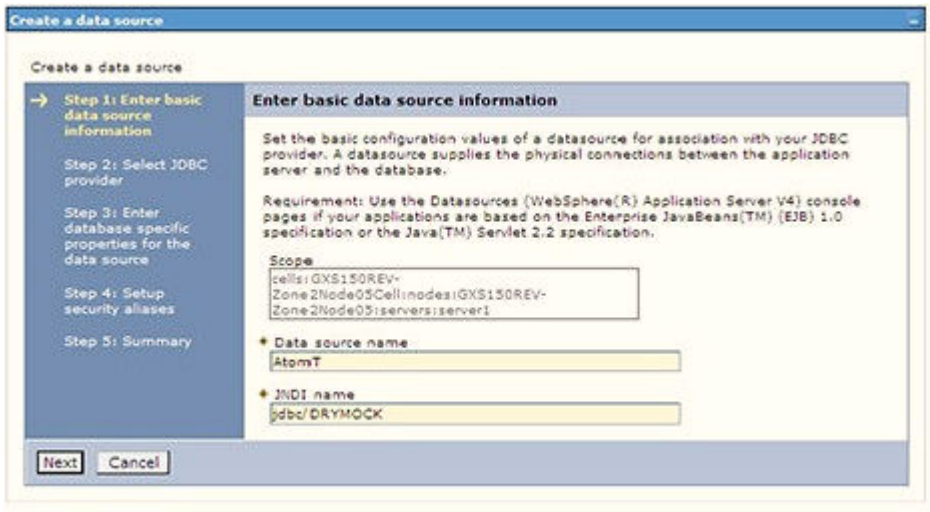
1. Open the following URL in the browser window: `http://<ipaddress>:<administrative console port>/ibm/console` (https if SSL is enabled). The Login window is displayed.
2. Log in with the user ID that has admin rights.
3. Expand the **Resources** option in the LHS menu and click **JDBC > Data sources** to display the Data sources window.

Figure 10-13 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 10-14 Create Data Source

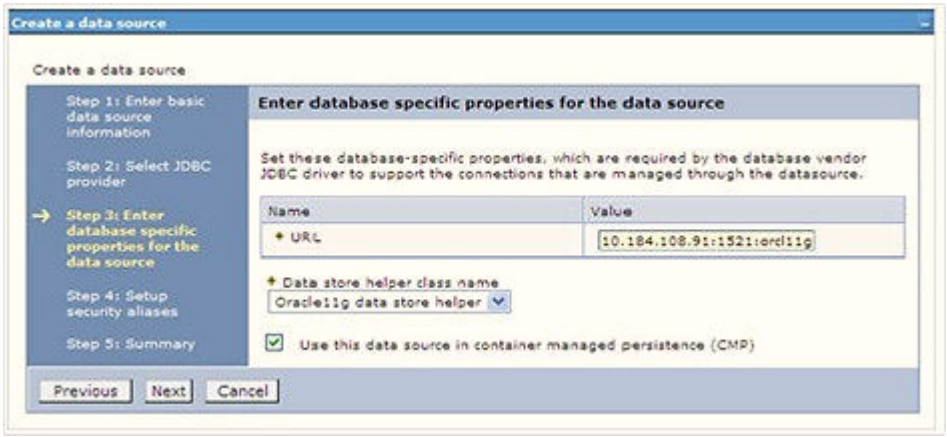


6. Specify the **Data source name** and **JNDI name** for the new "Data Source".
7. The **JNDI name** and **Data source name** are case sensitive and ensure that JNDI name is the same as the "Information Domain" name.
8. Click **Next** to display the Select JDBC provider window.

Figure 10-15 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 10-16 Enter database specific properties



10. Specify the database connection URL.

    For example: `jdbc:oracle:thin:@<DB_SEREVER_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.

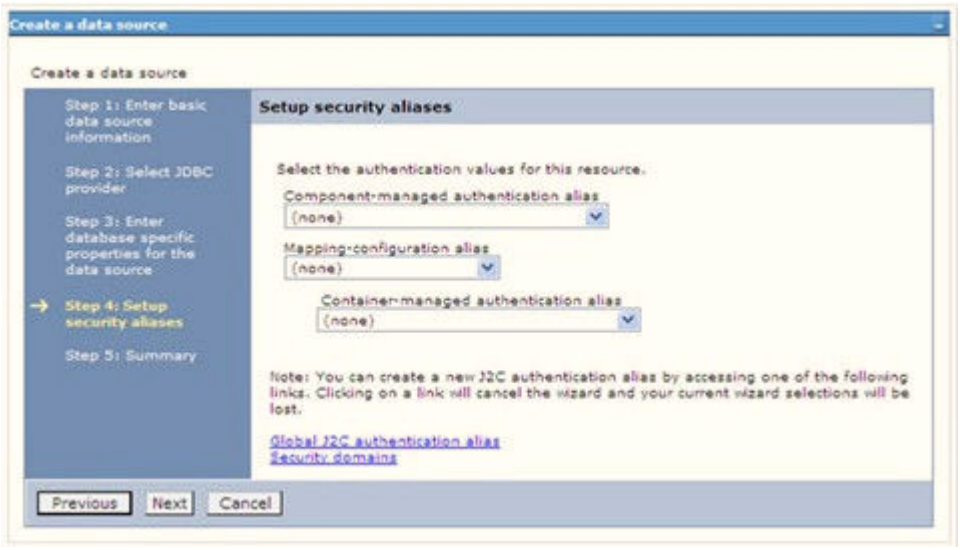
> **Note:**
>
> For RAC configuration, provide the RAC URL specified during installation.

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)))
```

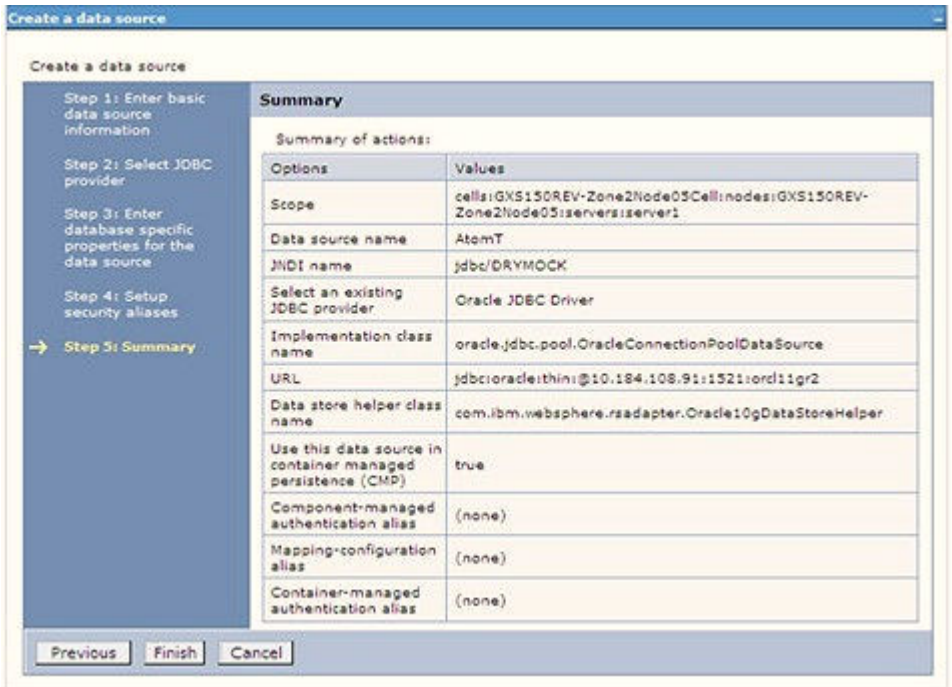
12. Click **Next**.

Figure 10-17 Enter Database specific properties



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 10-18 Summary



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.

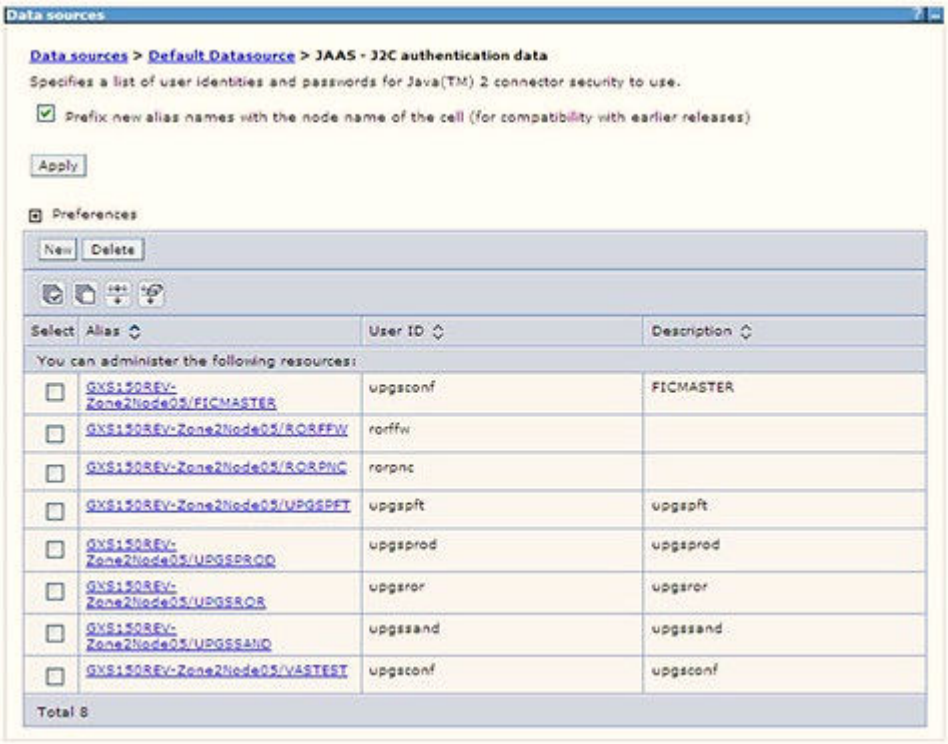
Create J2C Authentication Details

Set up J2C authentication details. These steps are for creating both config and atomic J2C authentication.

To create J2C Authentication details:

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

Figure 10-19 JAASJ2C authentication data



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

Figure 10-20 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.

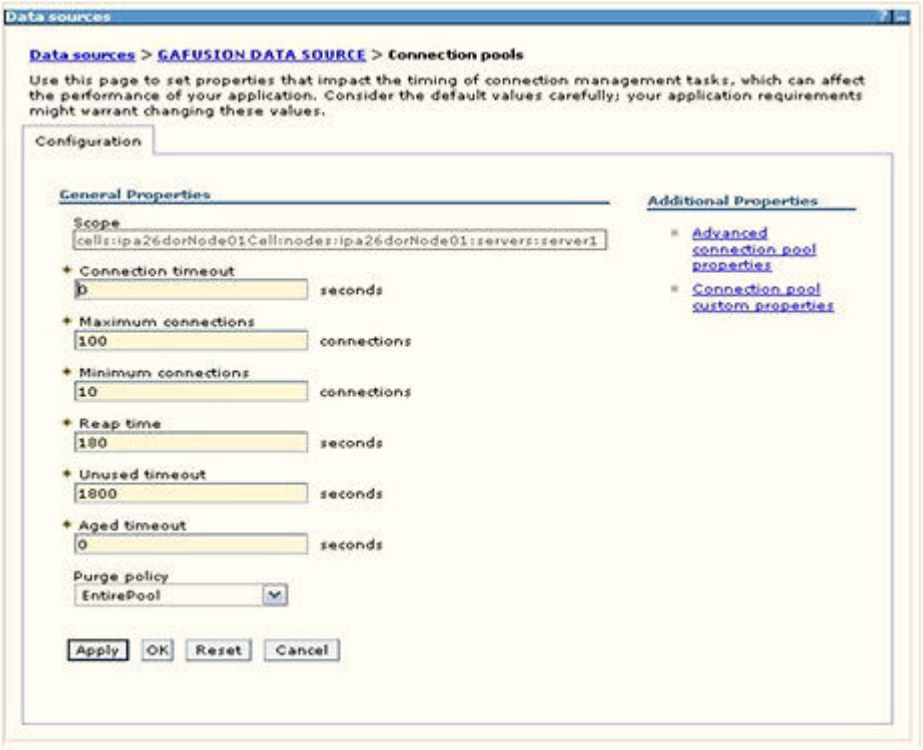
Define JDBC Connection Pooling

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

To define JDBC Connection Pooling:

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 10-21 Connection Pools



3. Set the following values:
   a. **Connection timeout**: 0
   b. **Maximum connections**: 100
   c. **Minimum connections**: 10

   You can also define **Reap time**, **Unused timeout**, and **Aged timeout** as required.

Work Manager for WebSphere

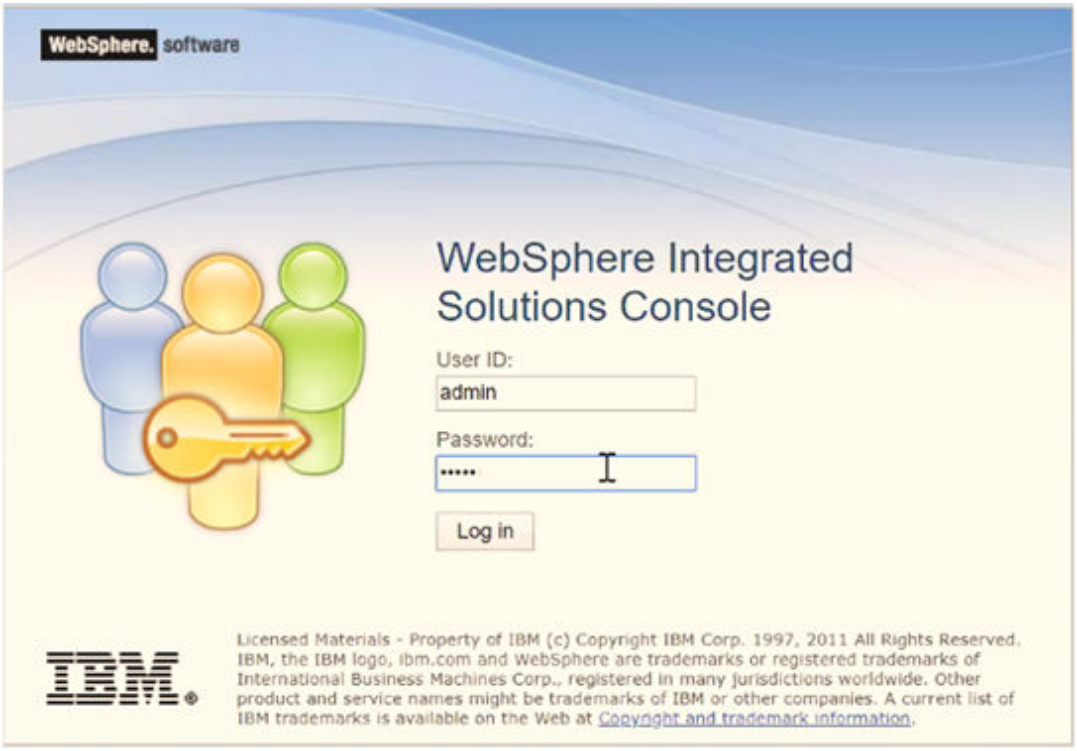
Create Work Manager

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 10-22 WebSphere Login page

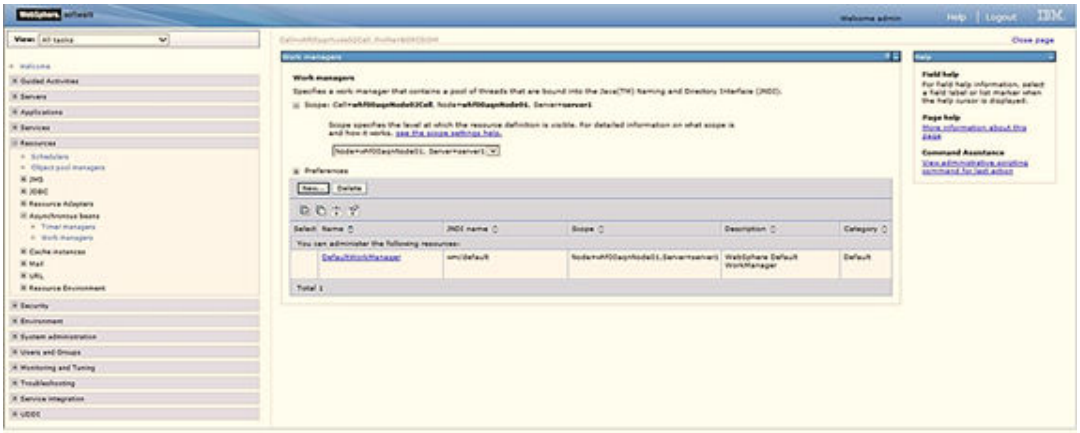


2. Log in with the user ID which has admin rights.

Figure 10-23 Home page

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

Figure 10-24 Work Managers

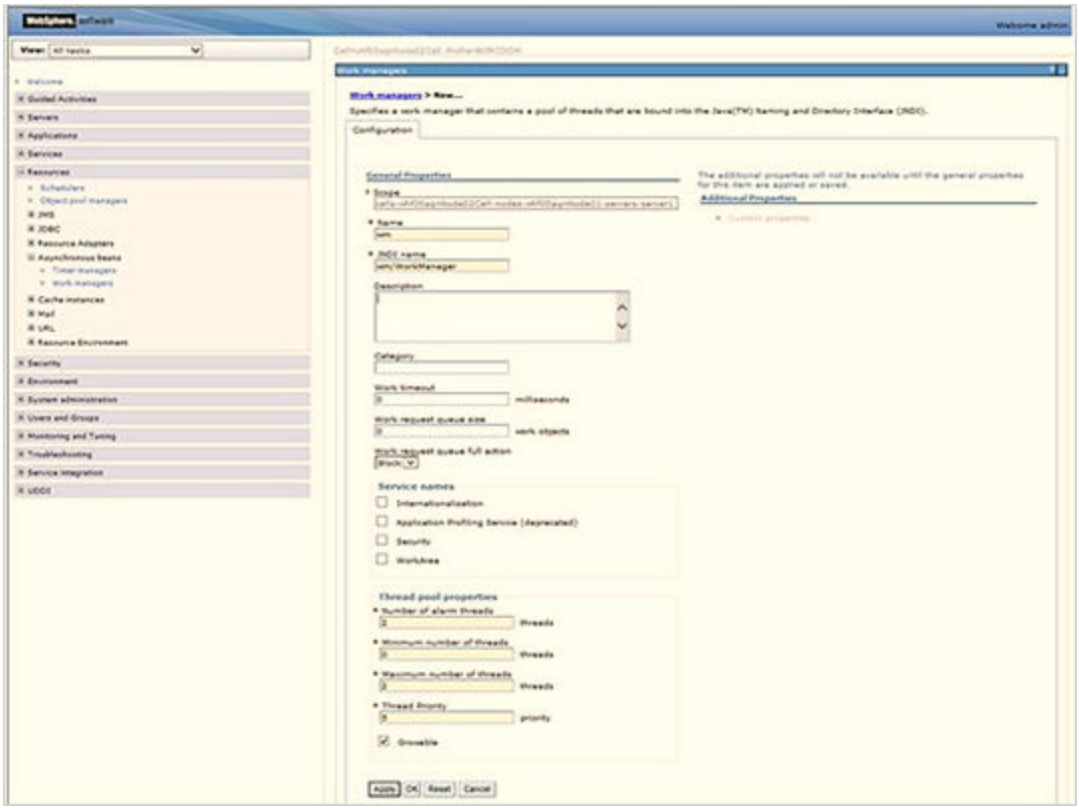


4. Select the required Scope from the drop-down list.

   For example, Node=whf00aqnNode01, Server=server1.

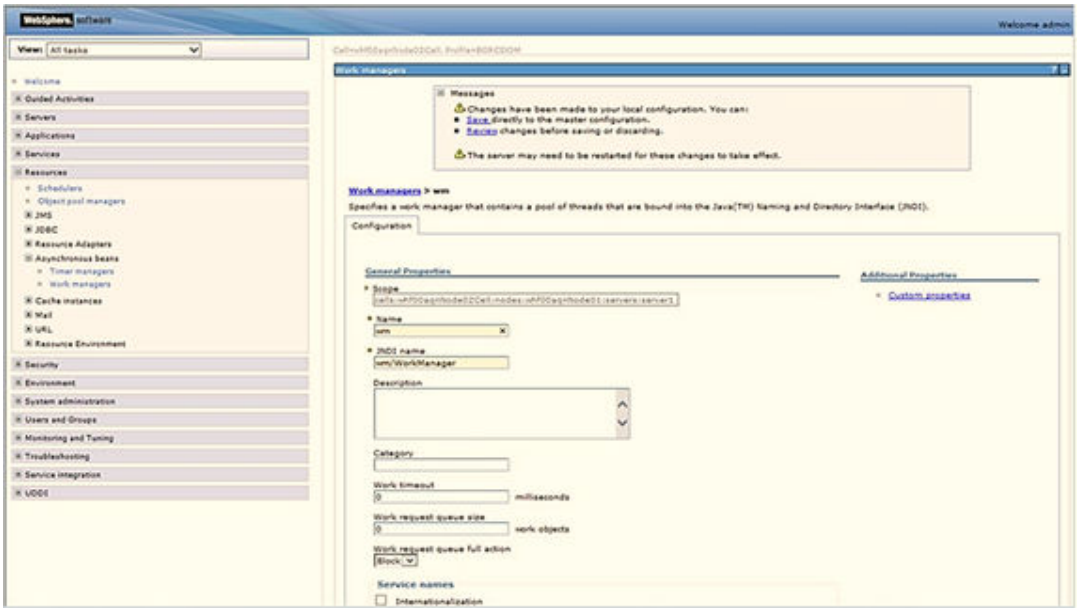
5. Click **New** in the **Preferences** section.

Figure 10-25 New Work Managers



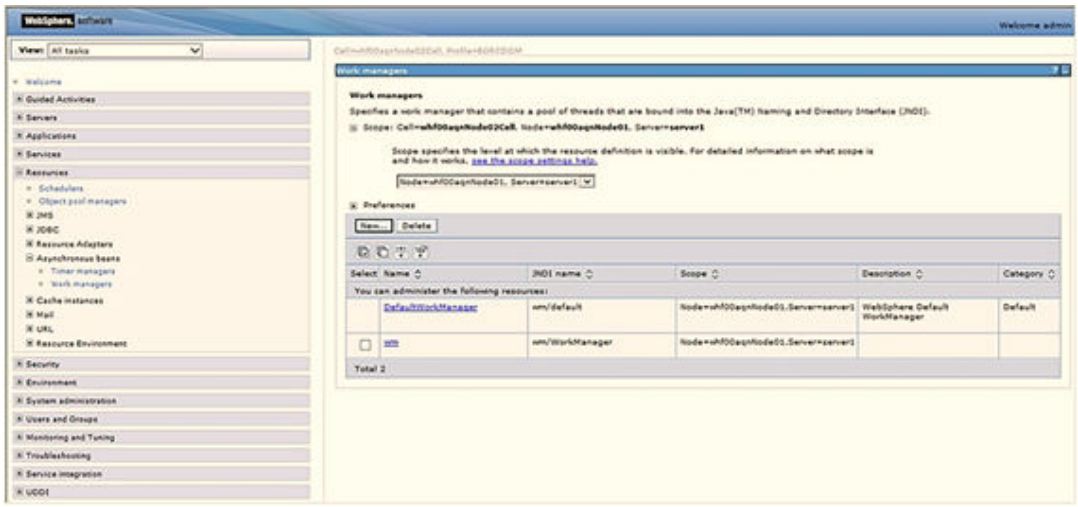
6. Enter the **Name** as 'wm' and JNDI name as 'wm/WorkManager ' in the respective fields.
7. Enter the **Thread pool properties**.
8. Click **Apply**.

Figure 10-26 Configure Work Managers



9. Click **Save**.

Figure 10-27 Work Managers Preferences



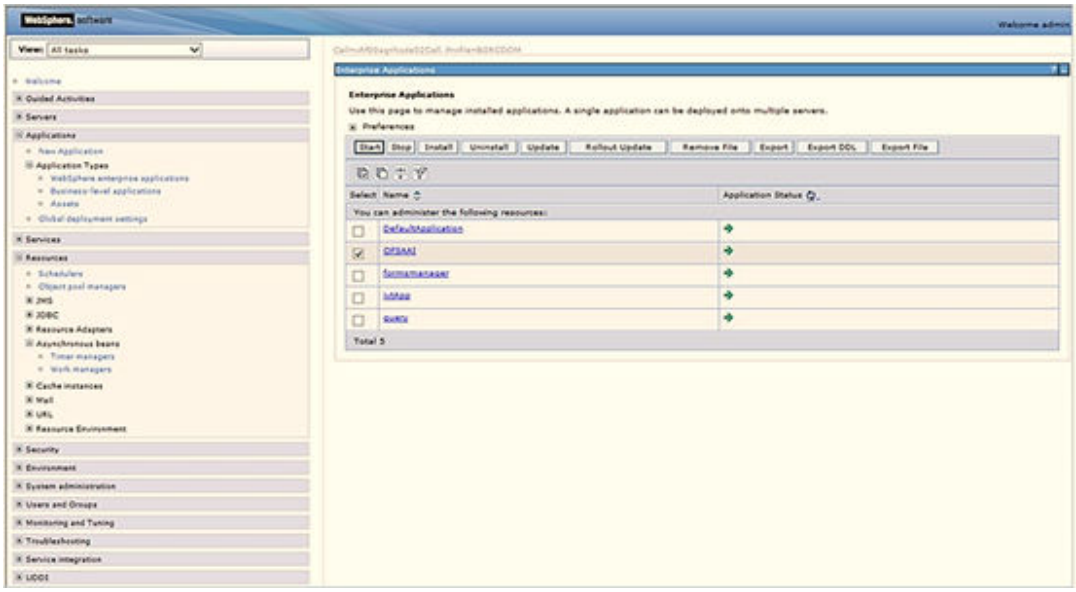
After creating the work manager, you must map it to an OFSAA instance.

Map Work Manager to OFSAA WebSphere Instance

To map the Work Manager to an OFSAA WebSphere Instance, follow these steps:

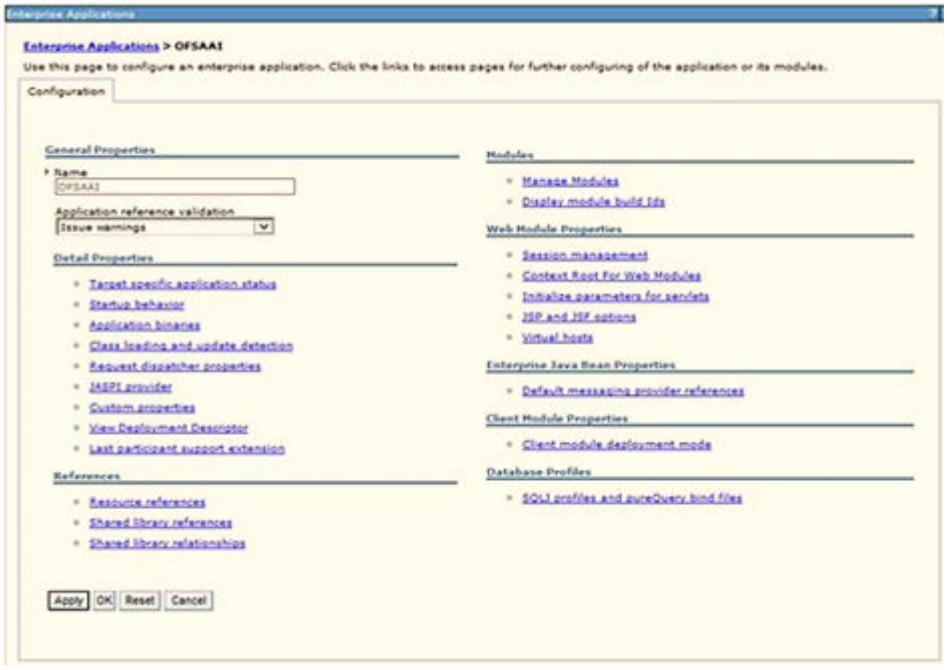
1. From the LHS menu, expand **Applications > Application Types** and click **WebSphere enterprise applications**.

Figure 10-28 Enterprise Applications



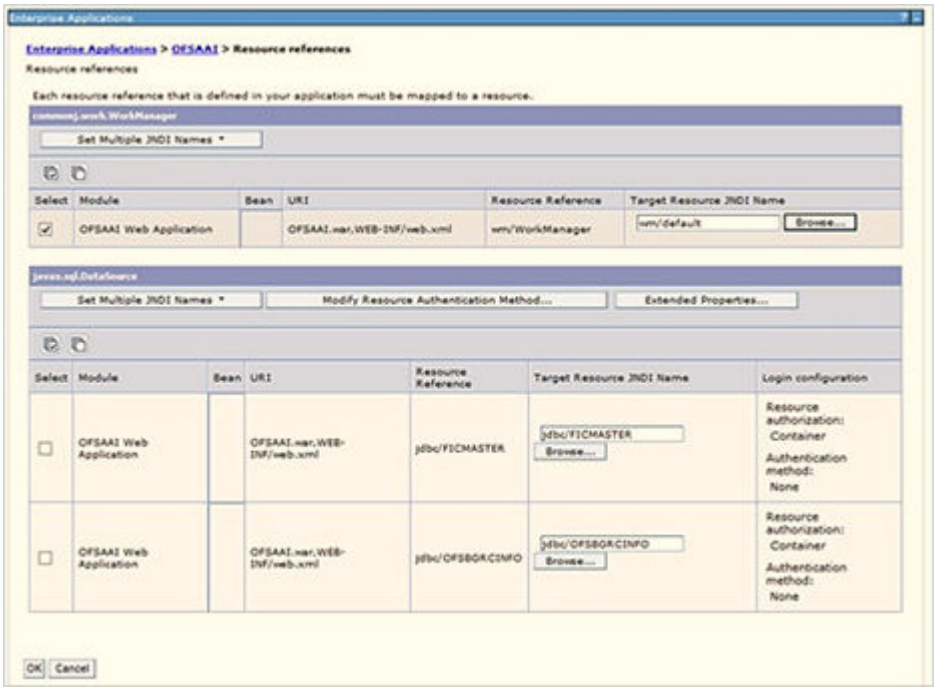
2. Click OFSAAI instance hyperlink.

Figure 10-29 OFSAAI



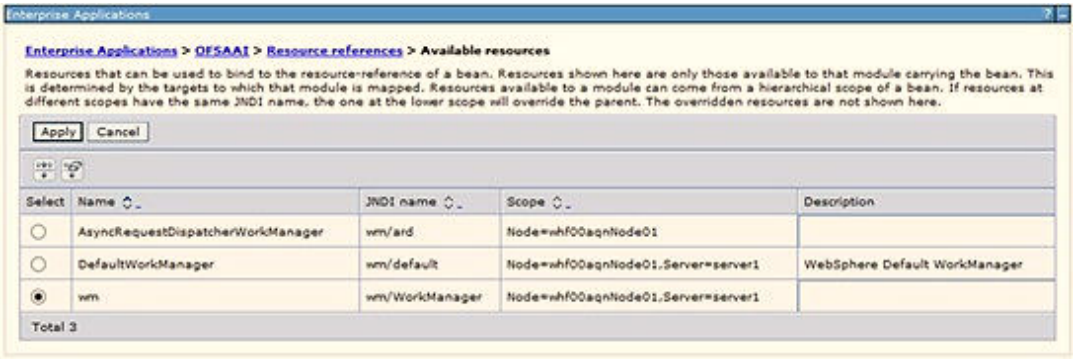
3. Click the **Resource references** link under the **References** section.

Figure 10-30 Resource References



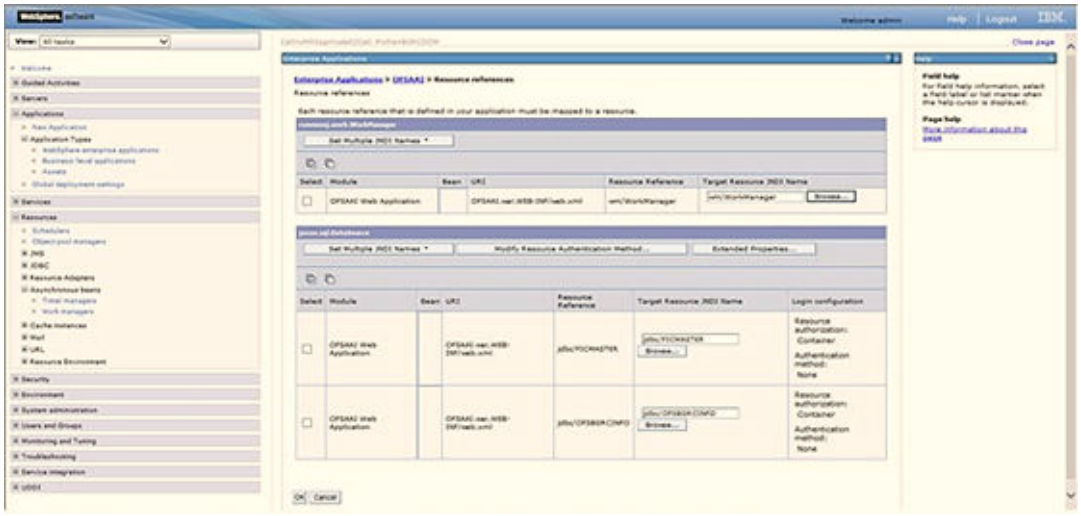
4. Click **Browse** corresponding to the Work Manager Resource Reference. The available resources are displayed.

Figure 10-31 Available Resources



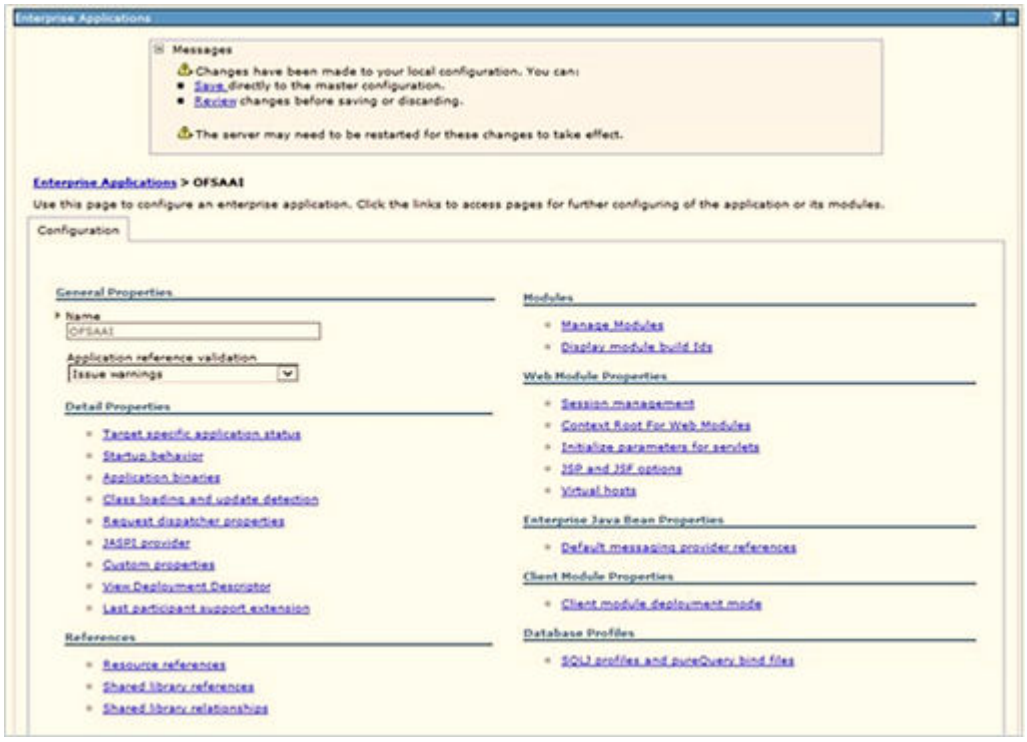
5. Select the newly created Work Manager ('wm') and click **Apply**.

Figure 10-32 Select Work Manager



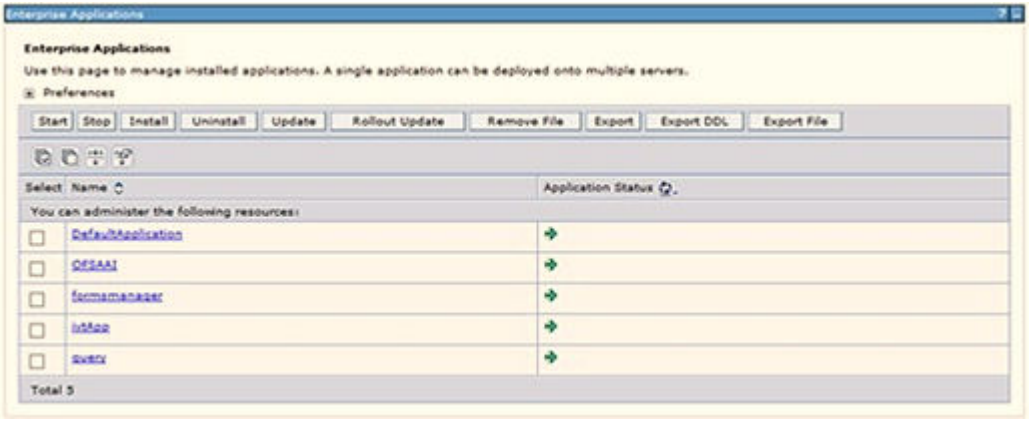
6. Select the Work Manager ('wm/WorkManager') and click **OK**.

Figure 10-33 OFSAAI Configuration



7. Click **Save**.

Figure 10-34 Enterprise Applications Preferences



Managing WebSphere

Delete WebSphere Profiles

To delete a WebSphere profile, follow these steps:

1. Select the check box adjacent to the required application and click **Stop**.
2. **Stop** the WebSphere profile to be deleted.
3. Navigate to WebSphere directory:

   `<WebSphere_Installation_Directory>/AppServer/bin/`
4. Execute the command:

   `manageprofiles.sh -delete -profileName <profile_name>`
5. Delete the profile directory.

   Example: `<WebSphere_Installation_ Directory>/AppServer/profiles/<profile_name>`
6. Execute the command:

   `manageprofiles.sh -validateAndUpdateRegistry`

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.

This section covers the following topics:

- Create Domain in WebLogic Server
- Delete Domain in WebLogic
- Configure WebLogic Memory Settings

Update Weblogic Server

Update the Weblogic server with required patches.

Before proceeding with the domain creation, download and install the one-off Patch 32077936 or the latest WLS PSU for 14.1.1 from My Oracle Support (Doc ID 2806740.2).

After applying this patch, set the java option flag `-Dweblogic.http.disablehttp2=true` before starting servers.

Create Domain in WebLogic Server

Create a new domain using Configuration Wizard in WebLogic.

To create a new domain using Configuration wizard:

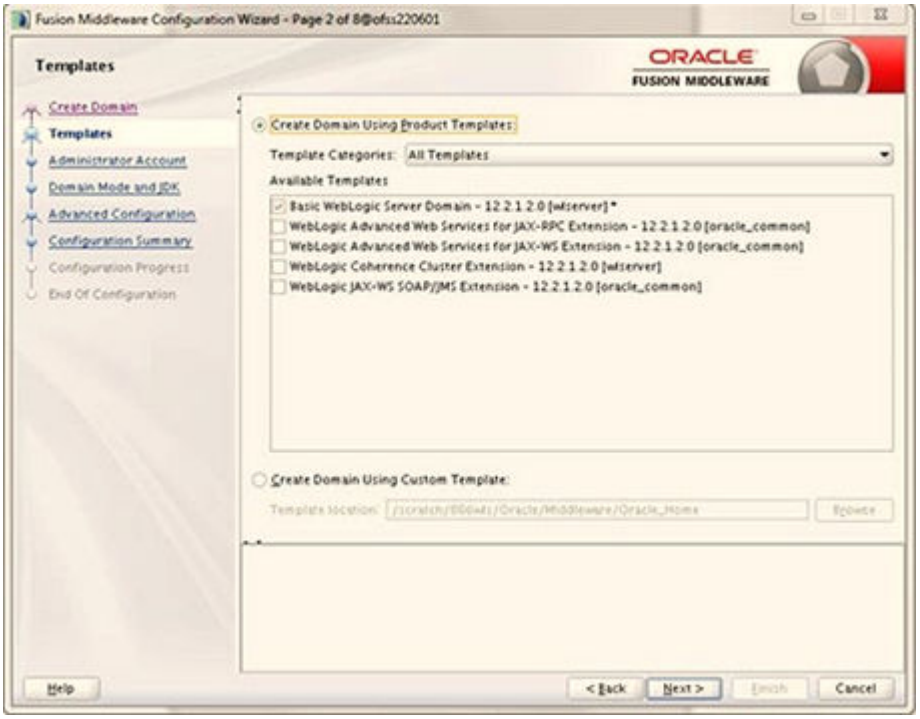
1. Navigate to the directory `<WLS_HOME>/wlserver/common/bin` and execute the following command, to access the **Welcome** screen.

   ```
   ./config.sh
   ```

Figure 10-35 Configuration Type

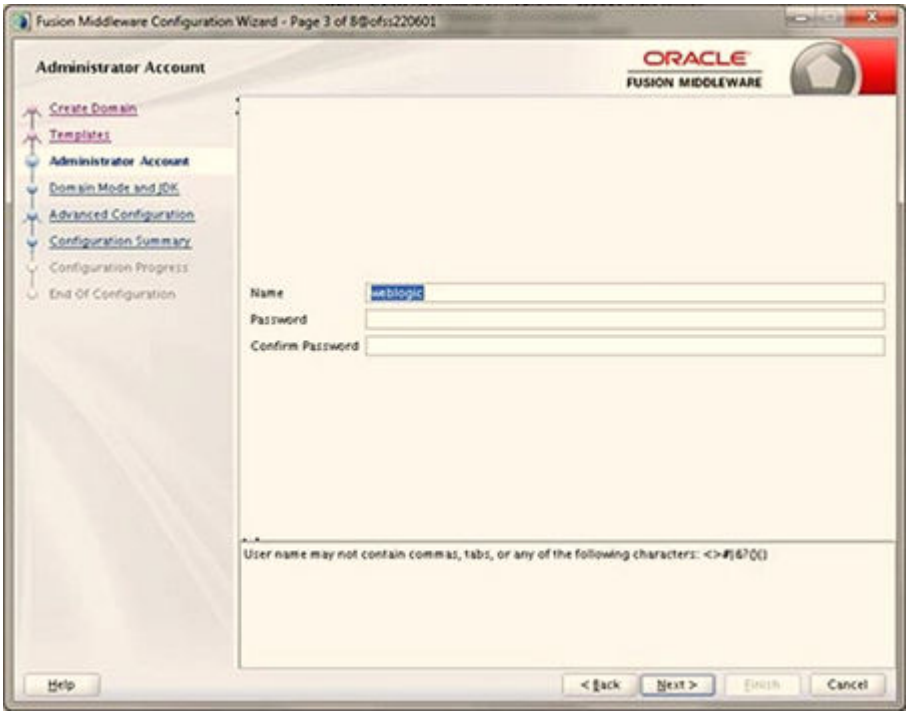
2. Select **Create a new domain** and click **Next** to access the **Templates** screen.

Figure 10-36 Templates



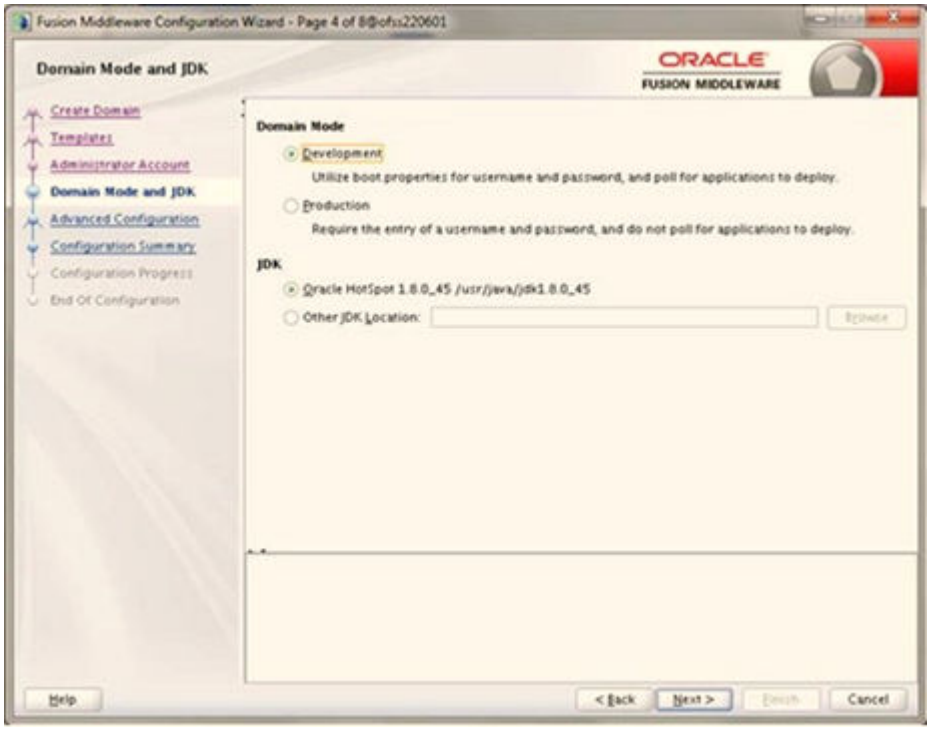
3. Select **Create Domain Using Product Templates** and click **Next** to view the **Administrator Account** screen.

Figure 10-37 Administrator Account



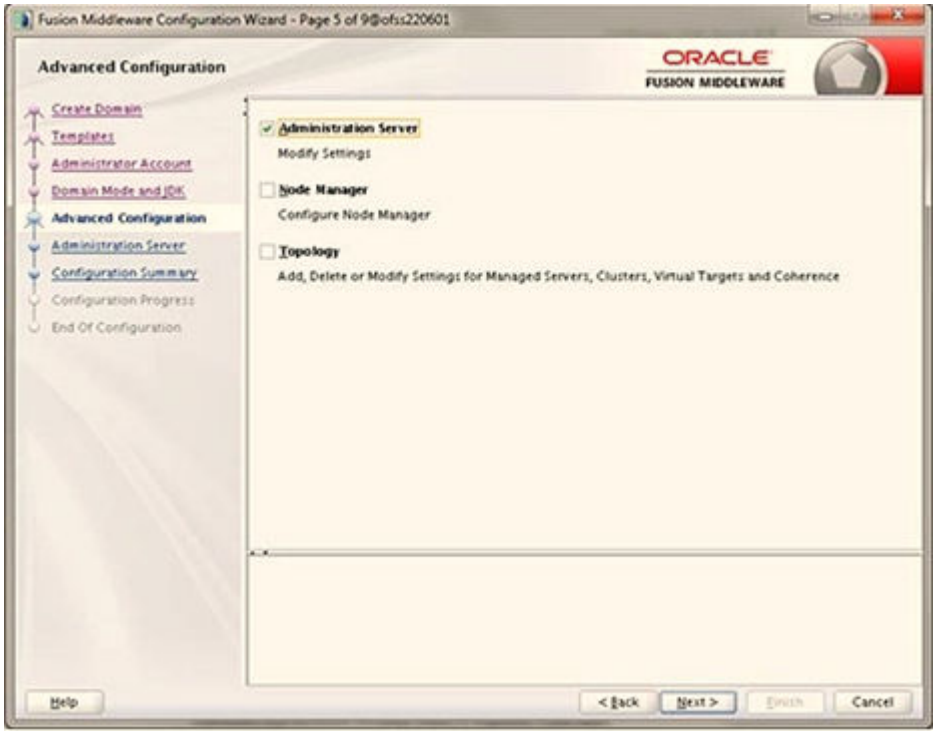
4. Enter the user name to be assigned to the administrator, the password, and confirm the password. Click **Next** to access the **Domain Mode and JDK** screen.

Figure 10-38 Domain Mode and JDK



5. Select the Domain mode and JDK location :
   a. **Domain Mode** - select the required mode (Development or Production).
   b. **JDK** - select the required option. If you select **Other JDK Location**, click **Browse** and navigate to the specific directory and select it. Click **Next** to display the Advanced Configuration window.

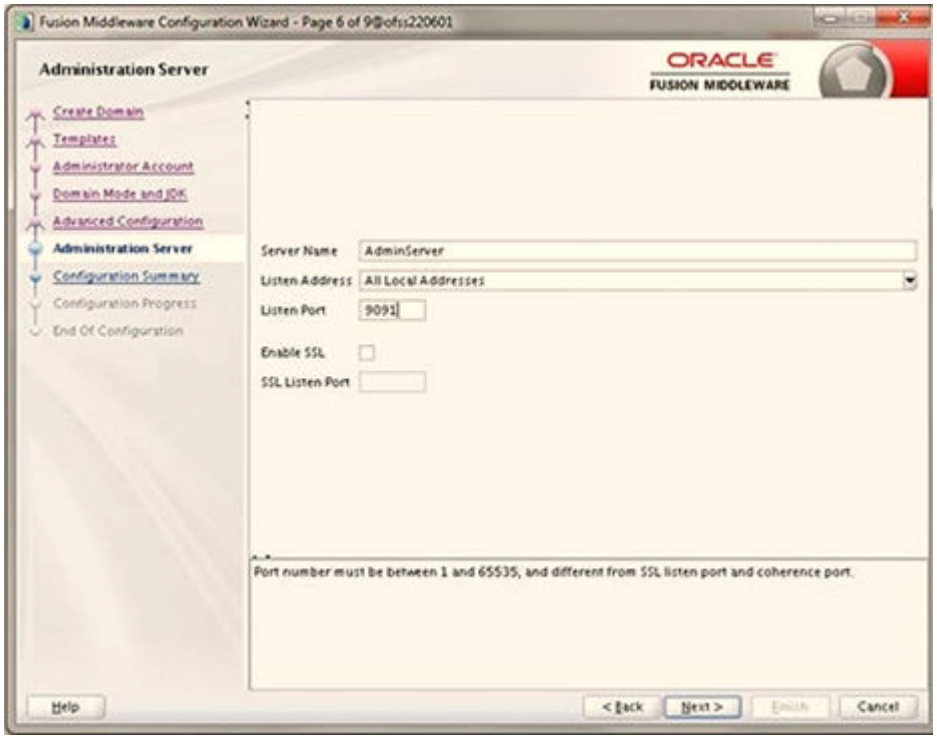
Figure 10-39 Advanced Configuration



6. Select the **Administration Server** and Click **Next** to access the **Administration Server** screen.

   A WebLogic Server domain must have an Administration Server. You can also select **Manages Servers, Clusters and Machines**, and **RDBMS Security Store** if required.

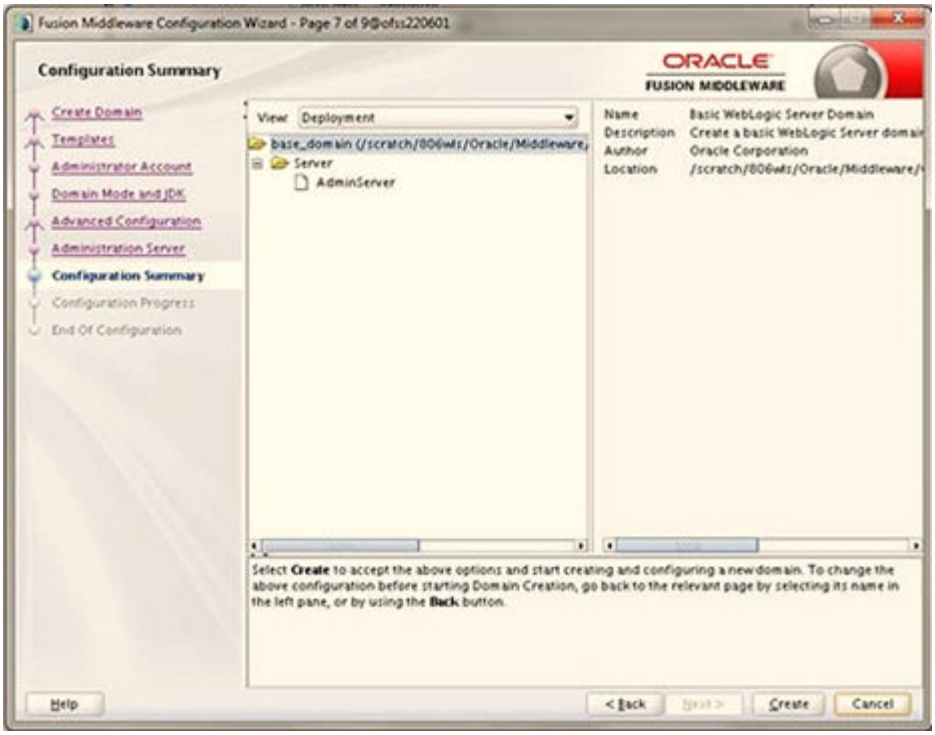
Figure 10-40 Administration Server



7. Enter the following Administration Server details (and click **Next** to access the **Configuration Summary** screen.
   - **Server Name**
   - **Listen address**
   - **Listen Port**
   - **Enable SSL** - Enable this option for secure login using https
   - **SSL Listen Port**

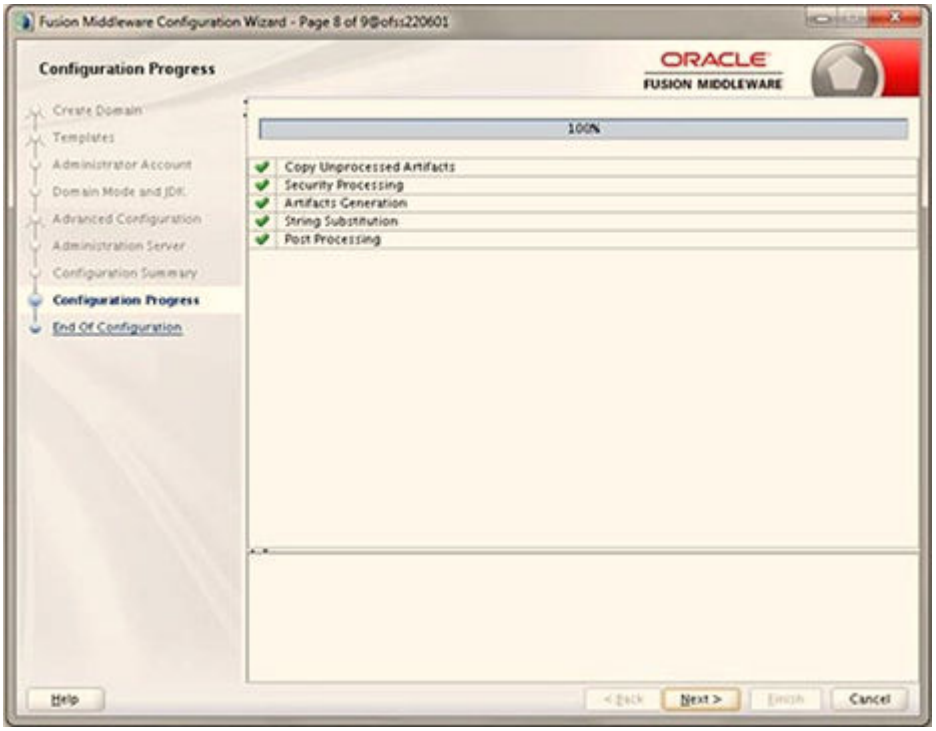
> **Note:**
>
> Make a note of the Listen Port or SSL Listen Port value (for example: 7007) since the same has to be re-entered in the Servlet port field during Infrastructure installation.

Figure 10-41 Configuration Summary



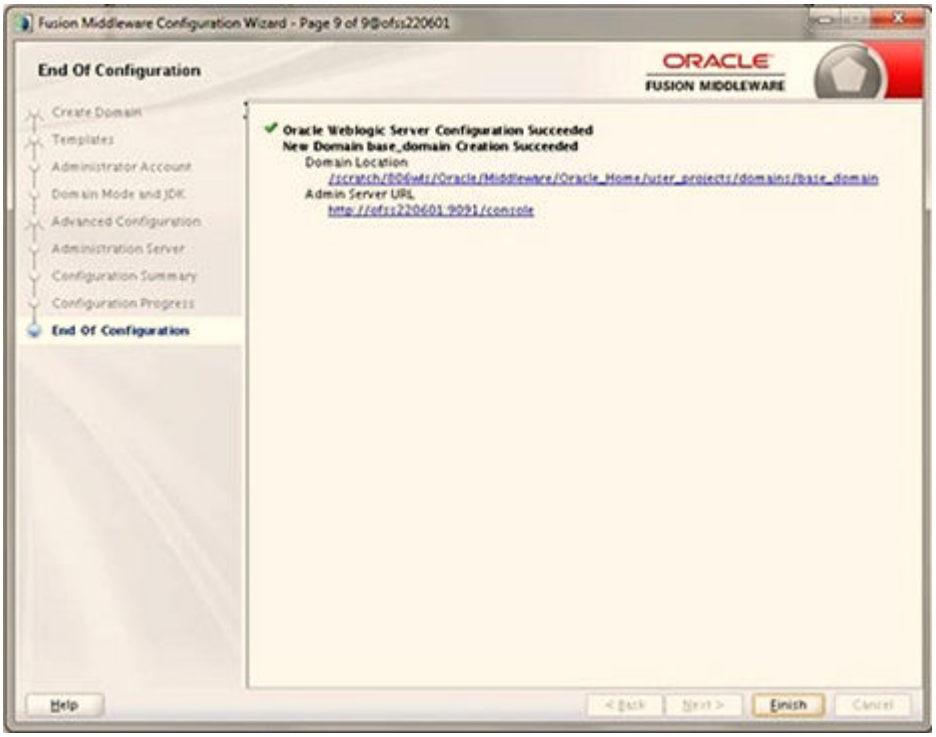
8. Verify the WebLogic domain configuration details and click **Create** to view the **Configuration Progress**.

Figure 10-42 Creating Domain



9. Click **Next**, after the configuration is completed successfully, to access the **End of Configuration** screen.

Figure 10-43 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.

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.

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"
   ```

Resource Reference for WebLogic

Configure Resource Reference in WebLogic Application Server

Set up Resource Reference in WebLogicApplication Server.

This section applies only when the Web application server type is WebLogic. This section includes the following 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.
- For a RAC Database instance, a Gridlink Data Source must be created.
- When Load Balancing/Fail over is required, a Multi Data Source must be created.

Create Data Source

Create a data source. This process is applicable to both config and atomic data source creation.

To create a data source:

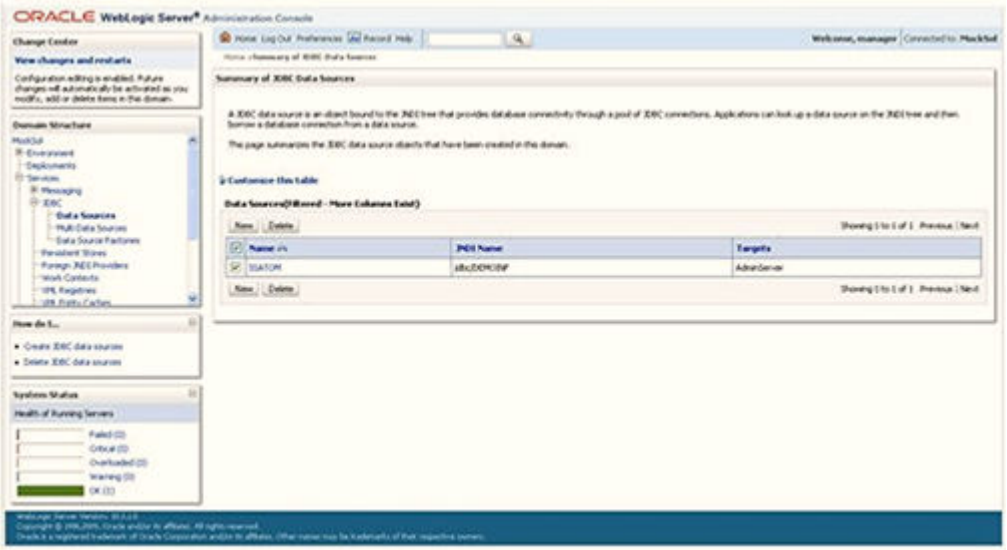
1. Open the following URL in the browser window:

   `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 10-44 Welcome

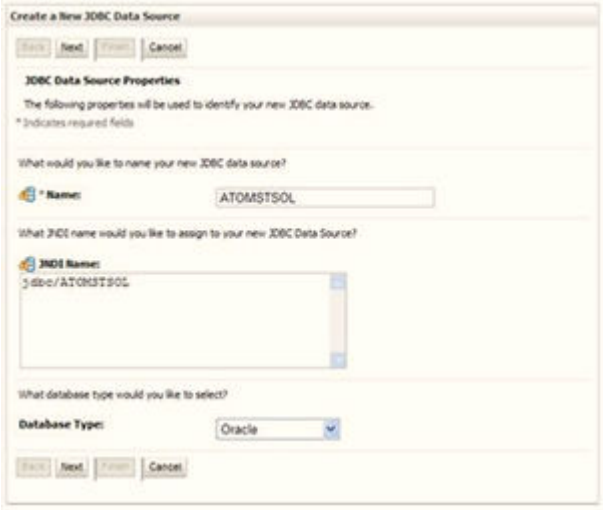
3. From the LHS menu (Domain Structure), click **Services** > **Data Sources** to display the Summary of **JDBC Data Sources** window.

Figure 10-45 Summary of JDBC Data Sources



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

Figure 10-46 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 GridLink Data Source or Configure Multi Data Sources.

5. In the **Create a New JDBC Data Source** window, enter JDBC data source **Name**, **JNDI Name**, and select the **Database Type** from the drop-down list, and then click **Next** to access the **JDBC Data Source Properties** window.

> **Note:**
>
> Ensure the following:
>
> a. The **JNDI Name** field must be in the format `jdbc/informationdomain`
>
> b. 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**.
>
> c. **JNDI Name** is the same as mentioned in the `web.xml` file of OFSAAI Application.
>
> d. Required **Database Type** and **Database Driver** must be selected.

> **Note:**
>
> Data sources must be created for atomic and atomiccnf schemas following the same steps.

6. In the **JDBC Data Source Properties** window, 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** to access **Transaction Options**.

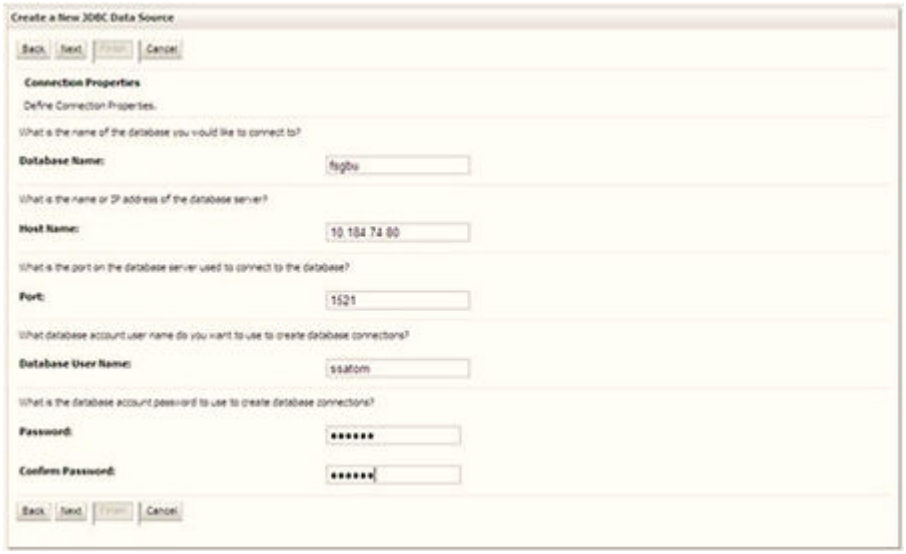
Figure 10-47 JDBC Data Source Properties

7. Select the **Supports Global Transactions** check box and the **One-Phase Commit** option.

Figure 10-48 Transaction Options

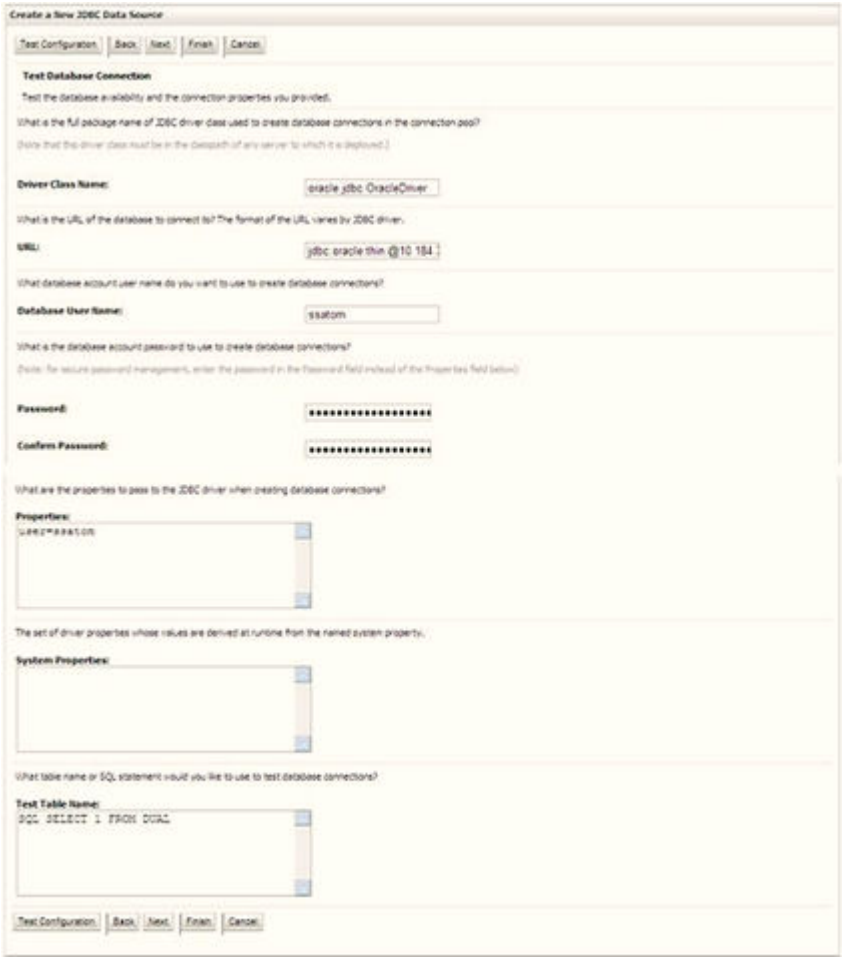
8. Click **Next** to access the **Connection Properties** window. Enter the required details such as the **Database Name**, **Host Name**, **Port**, **Oracle User Name**, **Password**, and **Confirm Password**.

Figure 10-49 Database Name



9. Click **Next** to display the **Test Database Connection** window. Verify the details and click **Test Configuration** and test the configuration settings.

Figure 10-50 Database Details



A confirmation message is displayed stating Connection test succeeded.

10. After testing the configuration, click **Next** to access the **Select Targets** window, and then select the target(s) to deploy the new JDBC Data Source.

Figure 10-51 Select Targets

11. Select the **AdminServer** option and 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.

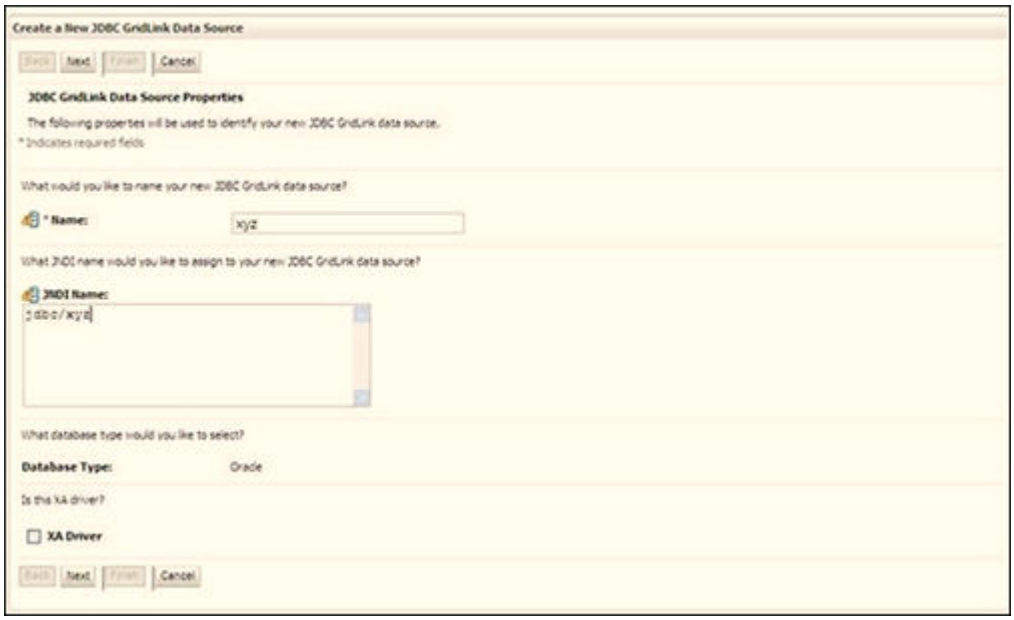
Create GridLink Data Source

To create a new GridLink Data Source:

1. From the **Summary of JDBC Data Sources**, click **New** and select **GridLink Data Source** to access the **Create a New JDBC GridLink Data Source** window.
2. Enter the Data Source **Name** and **JNDI Name**.

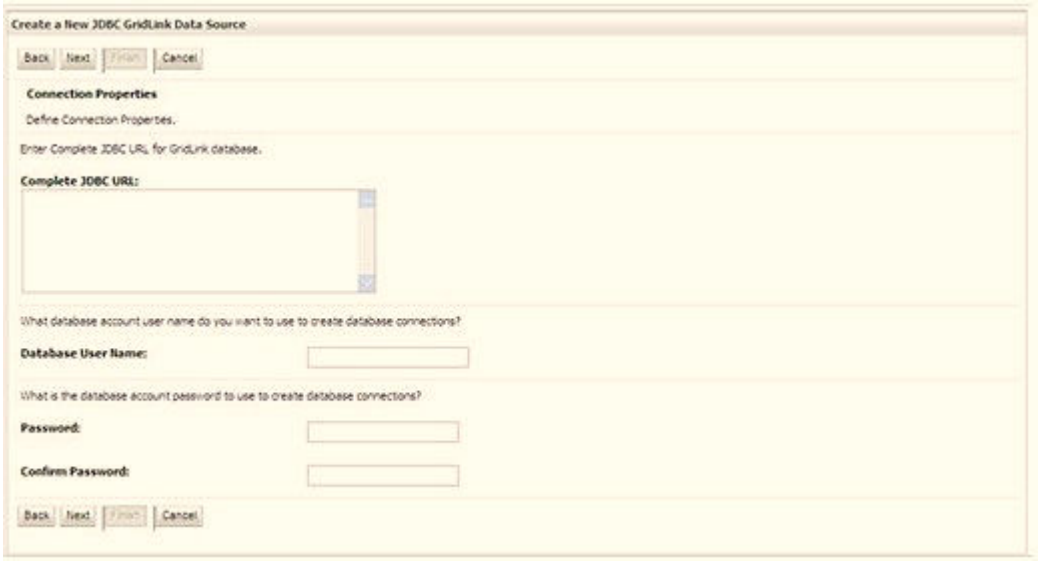
   Ensure that the **JNDI Name** field is specified in the format `jdbc/infodomname` and the **XA Driver** check box is not selected. Click **Next**.

Figure 10-52 JNDI Name



3. Specify **Complete JDBC URL**, **Database User Name**, and **Password**. Click **Finish**.

Figure 10-53 GridLink Data Source



The created **Data Source** is displayed in the list of Data Sources.

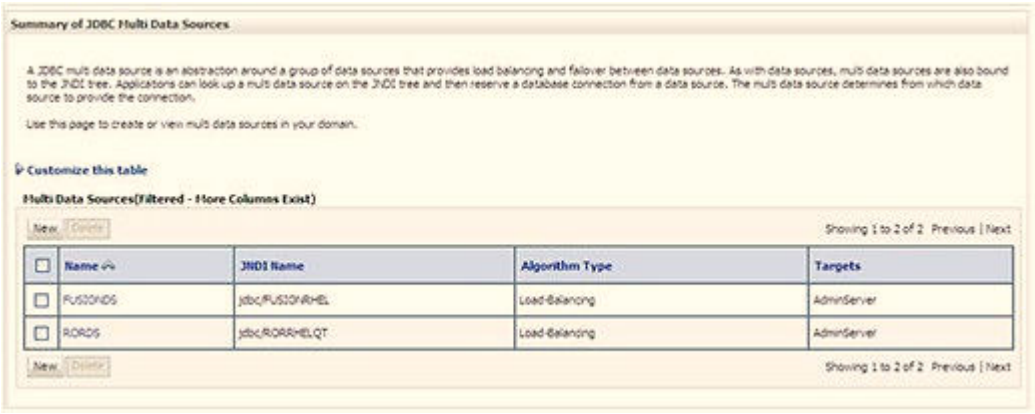
Configure Multi-data Sources

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

When the database used is Oracle RAC (Real Application Clusters), which allows Oracle Database to run across a set of clustered servers, then 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.

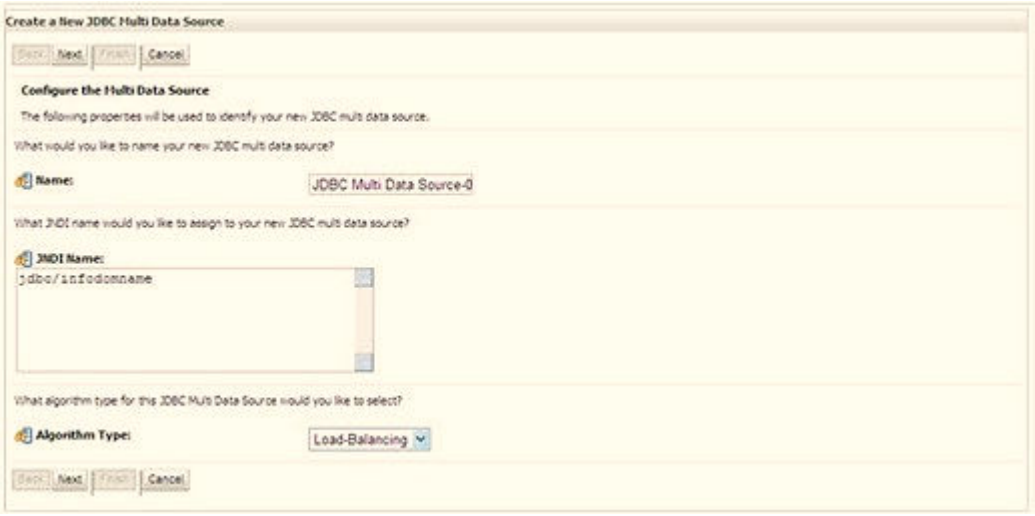
1. Open the WebLogic Admin Console in the browser window: http://<ipaddress>:<administrative console port>/console. (https if SSL is enabled). The Login window is displayed.
2. Login with the **User ID** that has admin rights.
3. In the LHS menu (Domain Structure), select **Services > JDBC > Multi Data Sources** to display the Summary of JDBC Multi Data Sources window.

Figure 10-54 Multi Data Sources



4. Click **New** to display the New JDBC **Multi Data Source** window.

Figure 10-55 Configure Multi Data Source



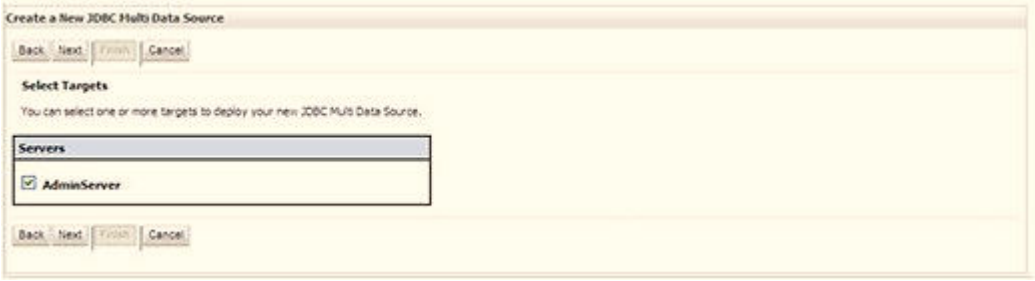
Ensure that the Data Sources which must be added to the new JDBC Multi Data Source are created.

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/ infodomname.
- 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 10-56 Select Targets

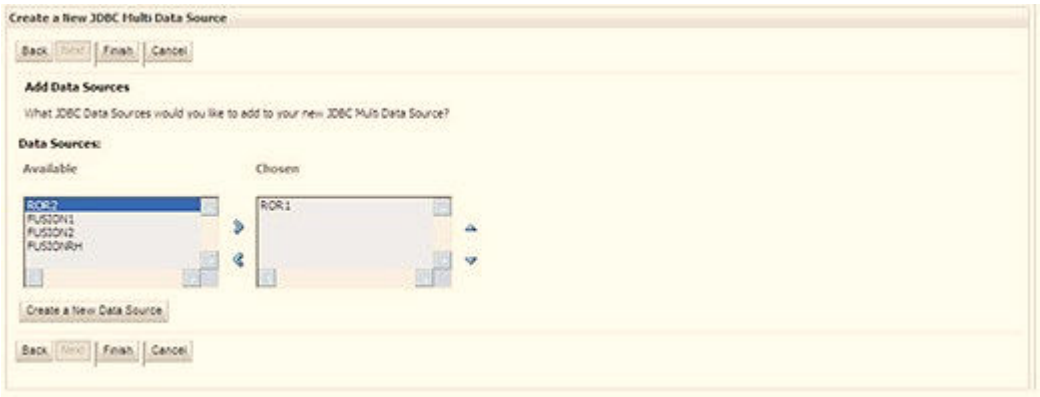


6. Select the **AdminServer** check box and click **Next**.

Figure 10-57 Select Data Source Type

7. Select the type of data source to add to the new JDBC Multi Data Source. Click **Next**.

Figure 10-58 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.

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.

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:
   a. **Initial Capacity**: 10
   b. **Maximum Capacity**: 100
   c. **Capacity Increment**: 1
   d. **Statement Cache Type**: LRU

e. **Statement Cache Size**: 10

3. Click **Save**.

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 10-59 WorkManager Screen 1

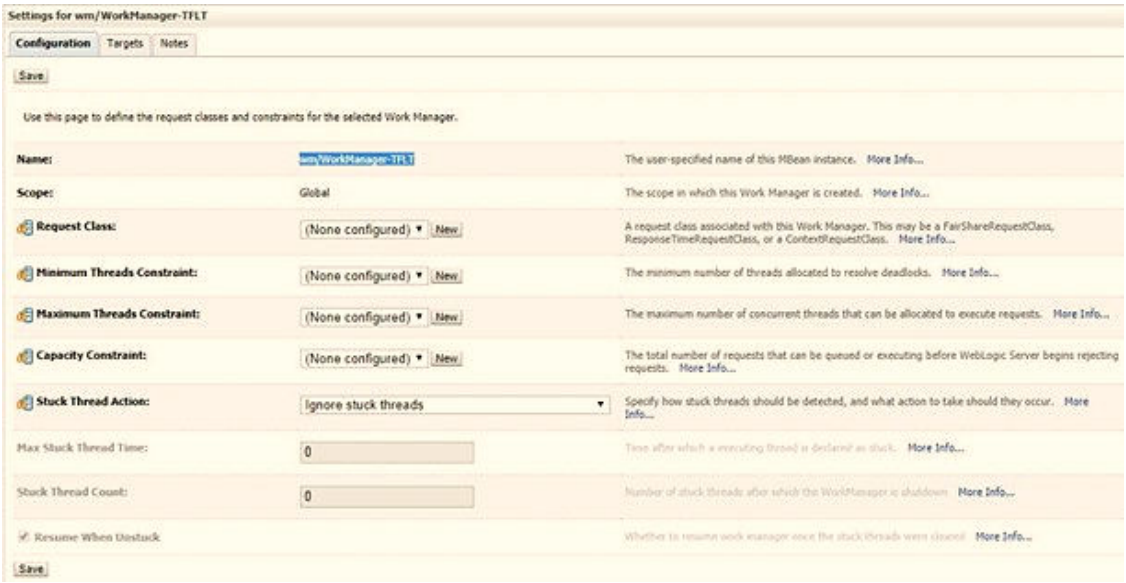


Figure 10-60 Workmanager Screen 2

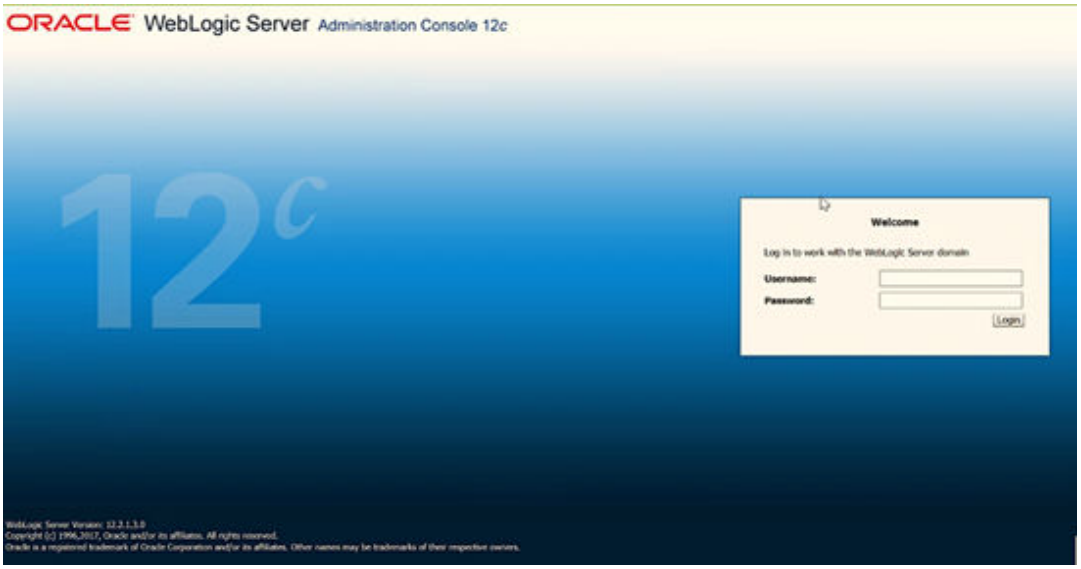
Work Manager for WebLogic

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 10-61 WebLogic Login page

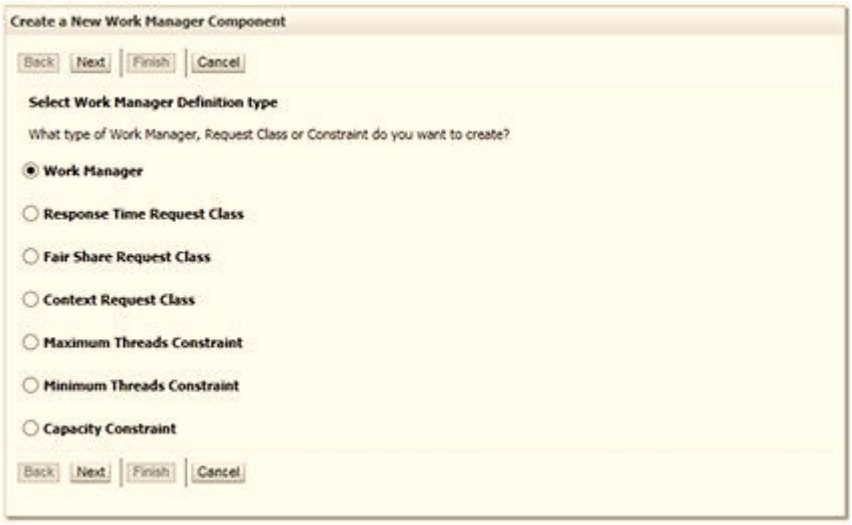


2. Log in with the user ID that has admin rights.
3. From the **Domain Structure** menu in the LHS, expand Environment and select **Work Managers** to display the Summary of Work Managers window.

Figure 10-62 Work Manager

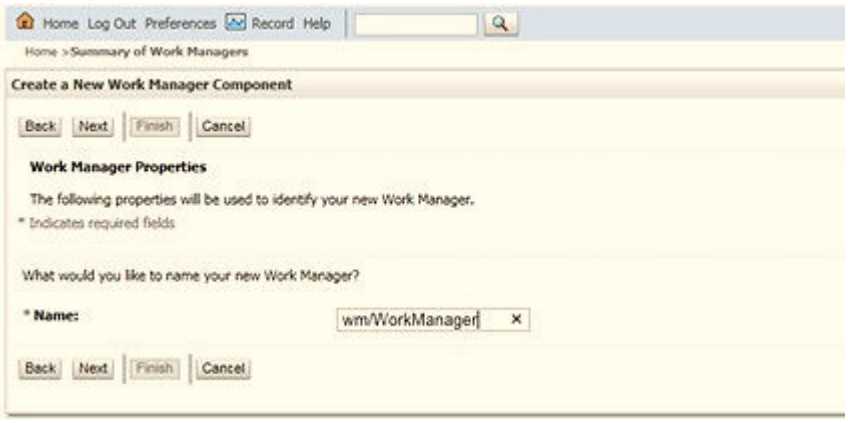
4. Click **New** to create a new Work Manager component.

Figure 10-63 New Work Manager



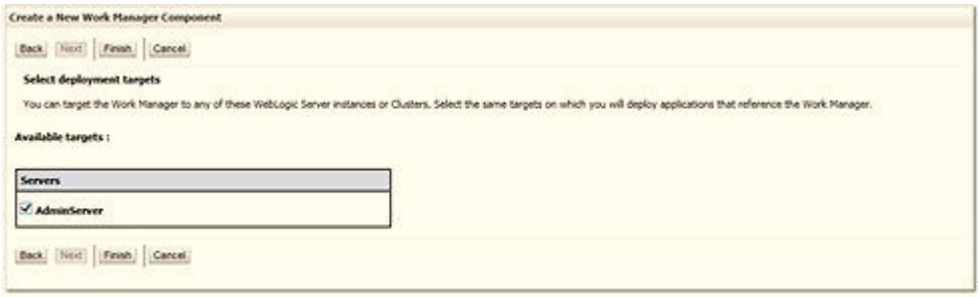
5. Select the Work Manager and click **Next**.

Figure 10-64 Work Manager



6. Enter the Name as 'wm/WorkManager' and click **Next**.

Figure 10-65 Select Deployment Targets



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

Figure 10-66 Summary of Work Managers

Configure Tomcat for Application Deployment

Configure Apache Tomcat Server for Application Deployment

This section is applicable only when the Web application server type is Tomcat. This section includes the following topics:

- Tomcat User Administration
- Configure Servlet Port
- Configure SSL Port
- Configure Apache Tomcat Memory Settings
- Configure Tomcat for User Group Authorization
- Uninstall WAR Files in Tomcat

Tomcat User Administration

Manage Tomcat users.

The Tomcat administration and manager application does not provide a default login. Edit the `$CATALINA_HOME/conf/tomcat-users.xml` file. 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" />`

- Add the manager role to any one of the existing username/password combinations as shown in the preceding example.
- 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.

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.

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"
```

> **Note:**
>
> - 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 http://tomcat.apache.org/.

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
```

Configuring Tomcat for User Group AuthorizationConfiguring Tomcat for User Group Authorization, Data Mapping, and Disabling WADL for the Web Service

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. To disable the WADL for the Web Service, navigate to the following snippet in the web.xml file.

```
<servlet>
<servlet-name>CommonRESTServlet</servlet-name>
<servlet-class>org.glassfish.jersey.servlet.ServletContainer</servlet-
class>
<init-param>
<param-name>javax.ws.rs.Application</param-name>
<param-value>com.ofs.fsapps.commonapps.util.ApplicationResourceConfig</
param-value>
</init-param>
<load-on-startup>1</load-on-startup>
</servlet>
```

4. Add the following snippet before the <load-on-startup>1</load-on-startup> attribute.

```
<init-param>
<param-name>jersey.config.server.wadl.disableWadl</param-name>
<param-value>true</param-value>
</init-param>
```

5. Save and close the file.

Uninstall WAR Files in Tomcat

To remove the OFSAAI setup completely, unistall the WAR files in Tomcat server.

To uninstall the WAR files in Tomcat, refer to Uninstall WAR Files in Tomcat.

Resource Reference for Tomcat

Configure Resource Reference in Tomcat Application Server

This section is applicable only when the Web application server type is Tomcat and includes the following 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.

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 ofsaaconf, then the actual schema created in the database is DEV_ofsaaconf.

```
<Context path ="/<context name>" docBase="<Tomcat Installation
Directory>/webapps/<context name>" debug="0" reloadable="true"
crossContext="true"><Resource auth="Container" name="jdbc/FICMASTER"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver" username="<user id for the
configuration schema>" password="<password for the above user id>"
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100" maxIdle="30" maxWait="10000"/><Resource auth="Container"
name="jdbc/< INFORMATION DOMAIN NAME >"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver" username="<user id for the
atomic schema>" password="<password for the above user id>"
```

```
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100" maxIdle="30" maxWait="10000"/>
</Context>
```

> **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.

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 present 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 ofsaaconf, then the actual schema created in the database is DEV_ofsaaconf.

Configure ClassLoader for Apache Tomcat

To configure the ClassLoader for Apache Tomcat, follow these steps:

1. Edit the `server.xml` file available in `$TOMCAT_HOME/conf/` directory.
2. 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.

Add FTP/SFTP Configuration for File Transfer

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

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

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

   Are you sure you want to continue connecting (Yes/No)?

   This will add an entry into the "known_hosts" file.
4. A confirmation message is displayed:

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

11

Configure Resource Reference in Web Servers

Configure the resource reference in web servers.

A resource reference facilitates application access to a resource, like a data source or URL, by using a logical name instead of the actual name within the environment. Configuring resource reference in web servers includes the following activities.

Topics:

Configure Resource Reference in WebSphere Application Server

Set up 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 a JDBC Provider in WebSphere Application Server.

To create the JDBC Provider in WebSphere Application Server:

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

   `http://<ipaddress>:<administrative console port>/ibm/console` (https, if SSL is enabled). The Login window is displayed.
2. Log in with the user ID that has admin rights.
3. Expand the **Resources** option in the LHS menu and click **JDBC > JDBC Providers** to access the **JDBC Providers** window.
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 add the new JDBC Provider under the Preferences section. The **Create new JDBC Provider** window is displayed.
6. Enter the following details:

a. **Database Type**: Oracle
b. **Provider Type**: Oracle JDBC Driver
c. **Implementation Type**: Connection pool data source
d. **Name**: The required display name for the resource.
e. **Description**: The optional description for the resource.

7. Click **Next**.
8. 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.

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

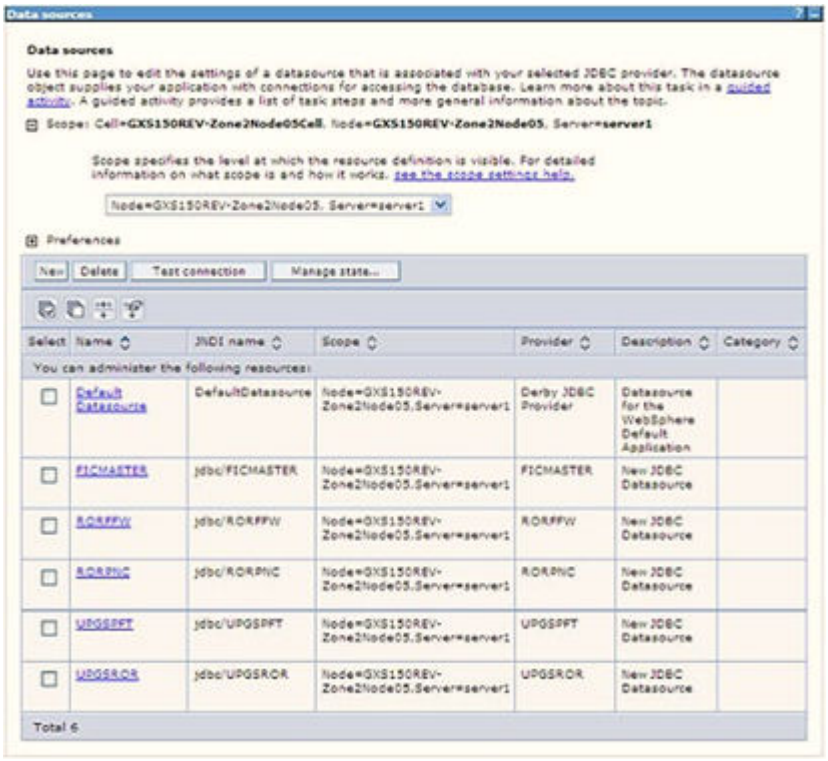
Create Data Source

Create a data source. This process is applicable to both config and atomic data source creation.

To create the data source:

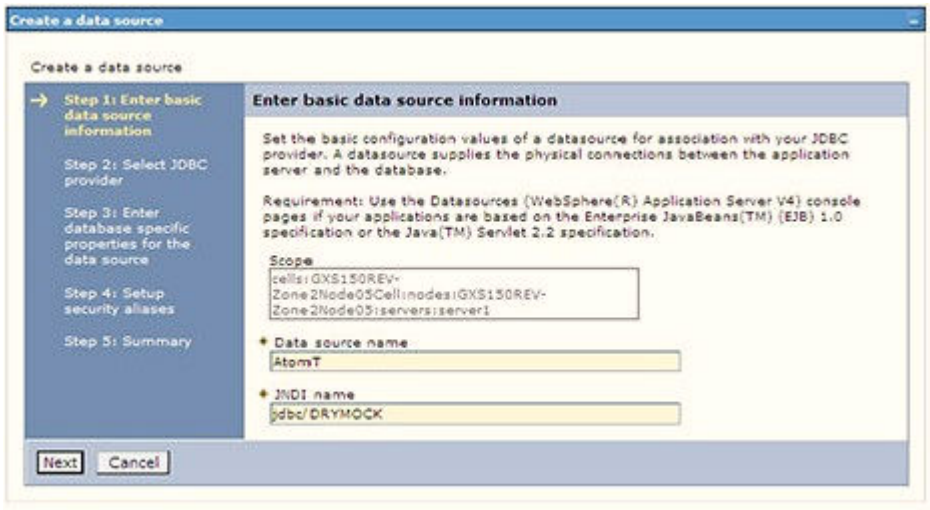
1. Open the following URL in the browser window: `http://<ipaddress>:<administrative console port>/ibm/console` (https if SSL is enabled). The Login window is displayed.
2. Log in with the user ID that has admin rights.
3. Expand the **Resources** option in the LHS menu and click **JDBC > Data sources** to display the Data sources window.

Figure 11-1 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 11-2 Create Data Source

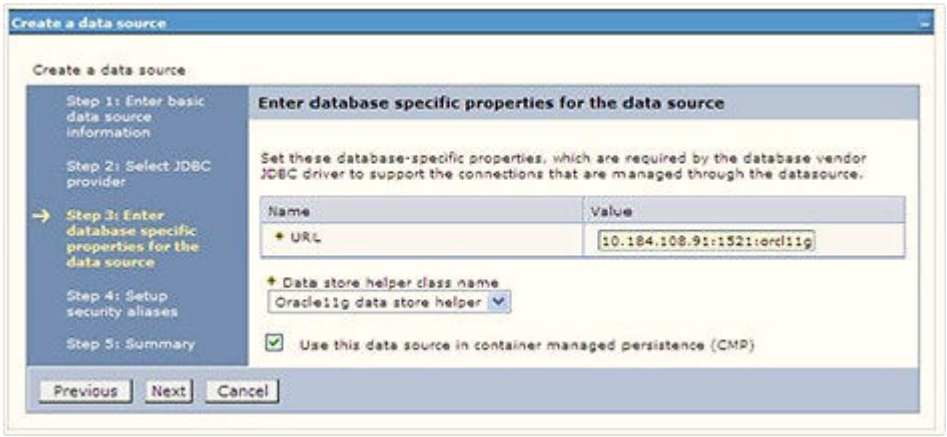


6. Specify the **Data source name** and **JNDI name** for the new "Data Source".
7. The **JNDI name** and **Data source name** are case sensitive and ensure that JNDI name is the same as the "Information Domain" name.
8. Click **Next** to display the Select JDBC provider window.

Figure 11-3 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 11-4 Enter database specific properties



10. Specify the database connection URL.

    For example: `jdbc:oracle:thin:@<DB_SEREVER_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.

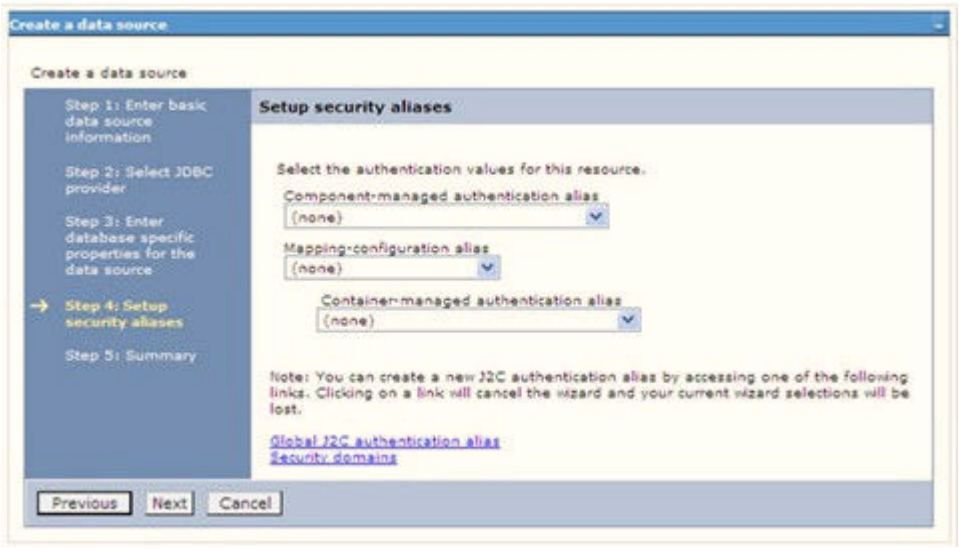
> **Note:**
>
> For RAC configuration, provide the RAC URL specified during installation.

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)))
```

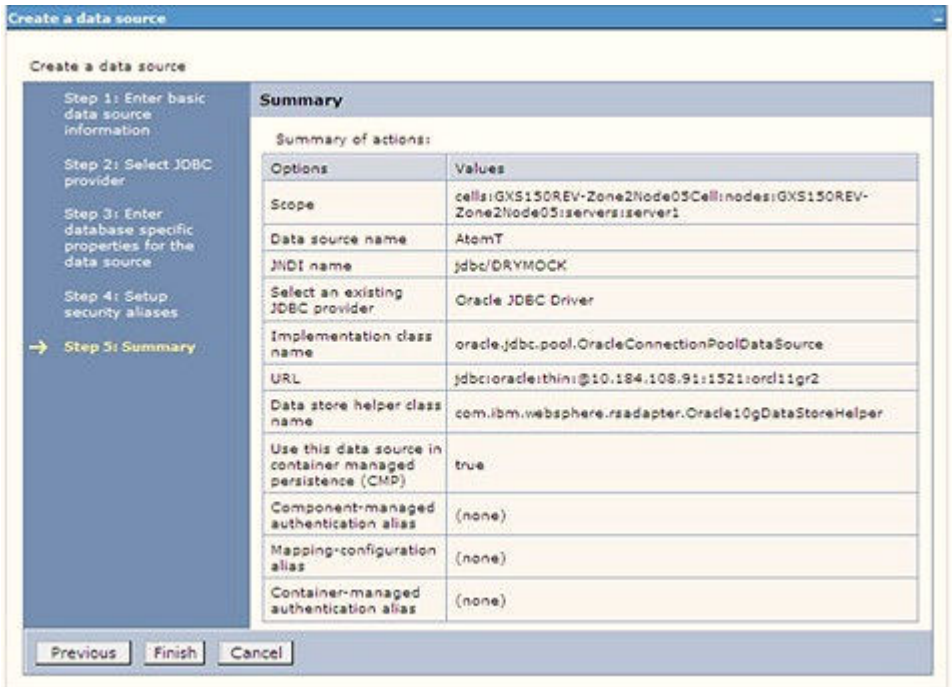
12. Click **Next**.

Figure 11-5 Enter Database specific properties



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 11-6 Summary



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.

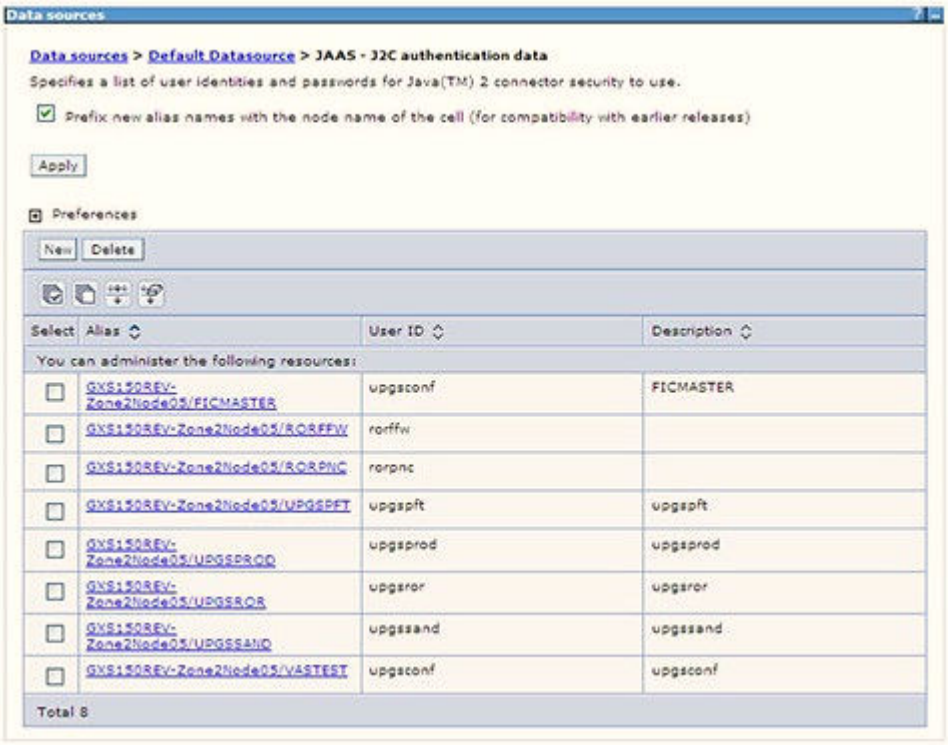
Create J2C Authentication Details

Set up J2C authentication details. These steps are for creating both config and atomic J2C authentication.

To create J2C Authentication details:

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

Figure 11-7 JAASJ2C authentication data



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

Figure 11-8 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.

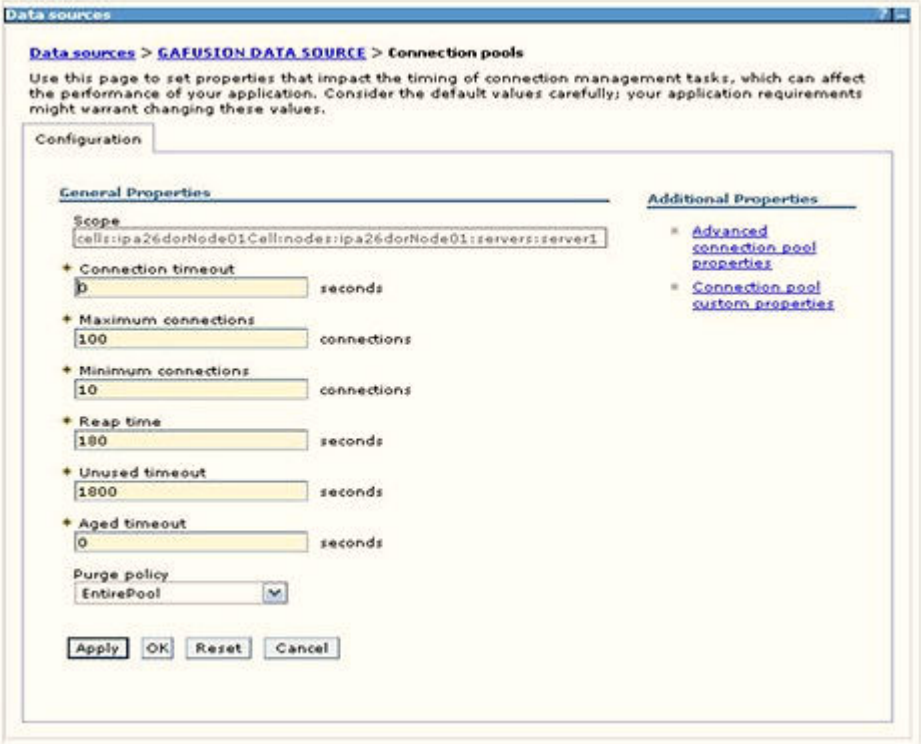
Define JDBC Connection Pooling

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

To define JDBC Connection Pooling:

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 11-9 Connection Pools



3. Set the following values:
   a. **Connection timeout**: 0
   b. **Maximum connections**: 100
   c. **Minimum connections**: 10

   You can also define **Reap time**, **Unused timeout**, and **Aged timeout** as required.

Configure Resource Reference in WebLogic Application Server

Set up Resource Reference in WebLogicApplication Server.

This section applies only when the Web application server type is WebLogic. This section includes the following 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.
- For a RAC Database instance, a Gridlink Data Source must be created.
- When Load Balancing/Fail over is required, a Multi Data Source must be created.

Create Data Source

Create a data source. This process is applicable to both config and atomic data source creation.

To create a data source:

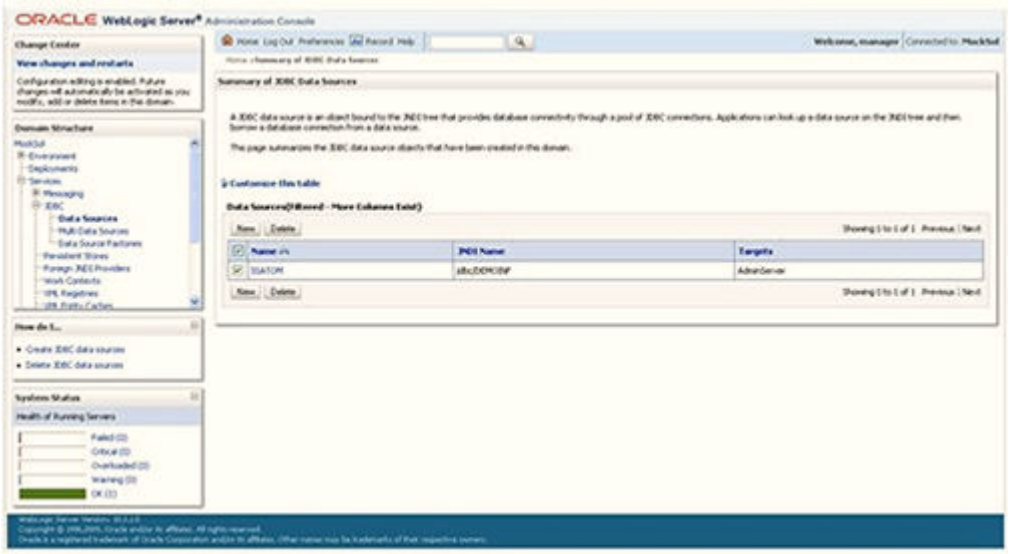
1. Open the following URL in the browser window:

   `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 11-10 Welcome

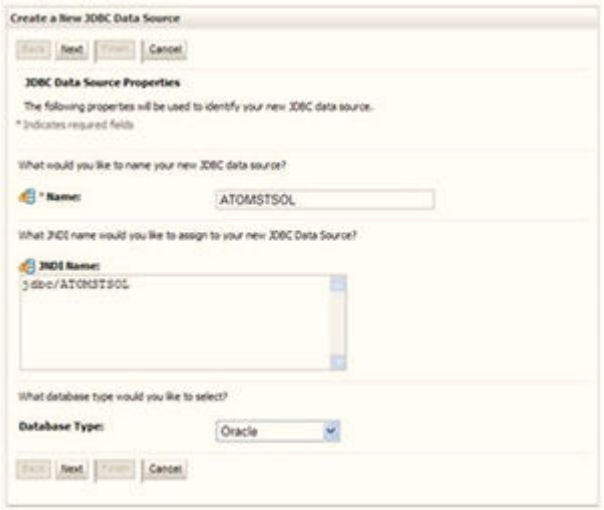
3. From the LHS menu (Domain Structure), click **Services** > **Data Sources** to display the Summary of **JDBC Data Sources** window.

Figure 11-11 Summary of JDBC Data Sources



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

Figure 11-12 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 GridLink Data Source or Configure Multi Data Sources.

5. In the **Create a New JDBC Data Source** window, enter JDBC data source **Name**, **JNDI Name**, and select the **Database Type** from the drop-down list, and then click **Next** to access the **JDBC Data Source Properties** window.

> **Note:**
>
> Ensure the following:
>
> a. The **JNDI Name** field must be in the format `jdbc/informationdomain`
>
> b. 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**.
>
> c. **JNDI Name** is the same as mentioned in the `web.xml` file of OFSAAI Application.
>
> d. Required **Database Type** and **Database Driver** must be selected.

> **Note:**
>
> Data sources must be created for atomic and atomiccnf schemas following the same steps.

6. In the **JDBC Data Source Properties** window, 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** to access **Transaction Options**.

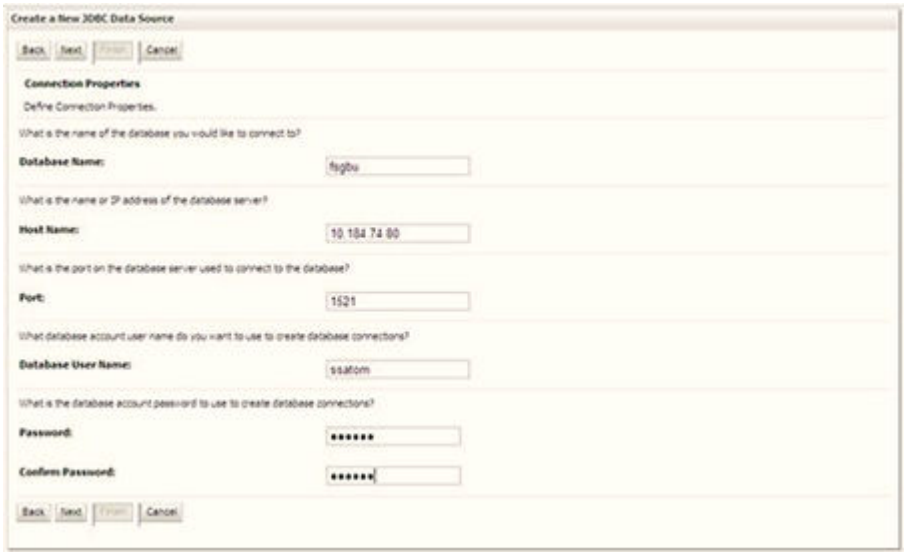
Figure 11-13 JDBC Data Source Properties

7. Select the **Supports Global Transactions** check box and the **One-Phase Commit** option.

Figure 11-14 Transaction Options

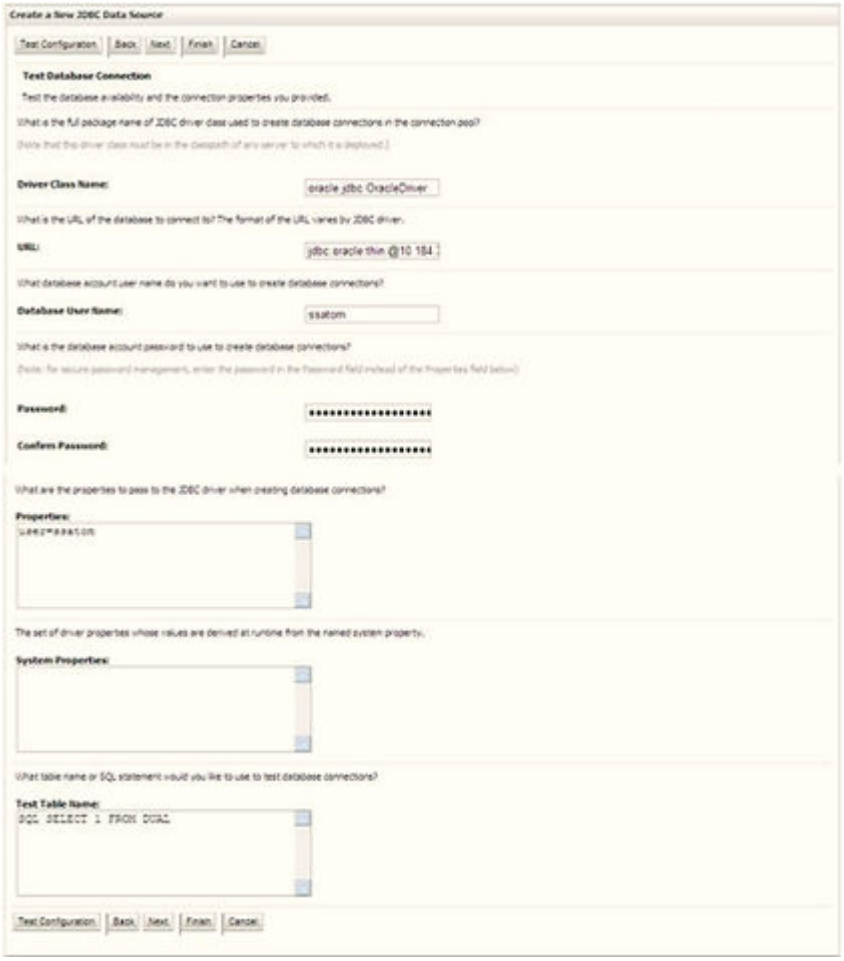
8. Click **Next** to access the **Connection Properties** window. Enter the required details such as the **Database Name**, **Host Name**, **Port**, **Oracle User Name**, **Password**, and **Confirm Password**.

Figure 11-15 Database Name



9. Click **Next** to display the **Test Database Connection** window. Verify the details and click **Test Configuration** and test the configuration settings.

Figure 11-16 Database Details



A confirmation message is displayed stating Connection test succeeded.

10. After testing the configuration, click **Next** to access the **Select Targets** window, and then select the target(s) to deploy the new JDBC Data Source.

Figure 11-17 Select Targets

11. Select the **AdminServer** option and 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.

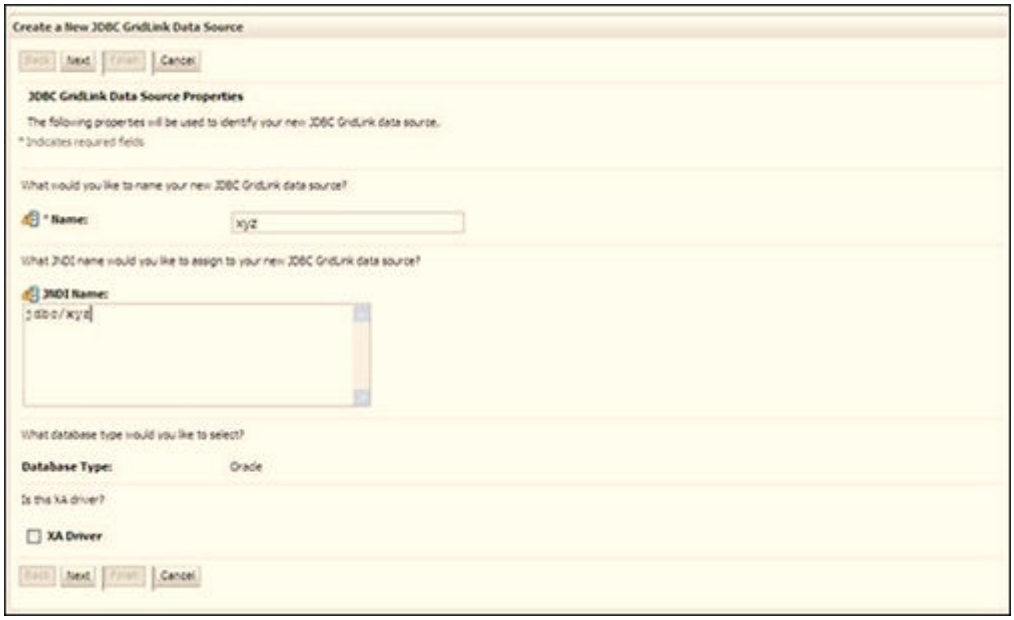
Create GridLink Data Source

To create a new GridLink Data Source:

1. From the **Summary of JDBC Data Sources**, click **New** and select **GridLink Data Source** to access the **Create a New JDBC GridLink Data Source** window.
2. Enter the Data Source **Name** and **JNDI Name**.

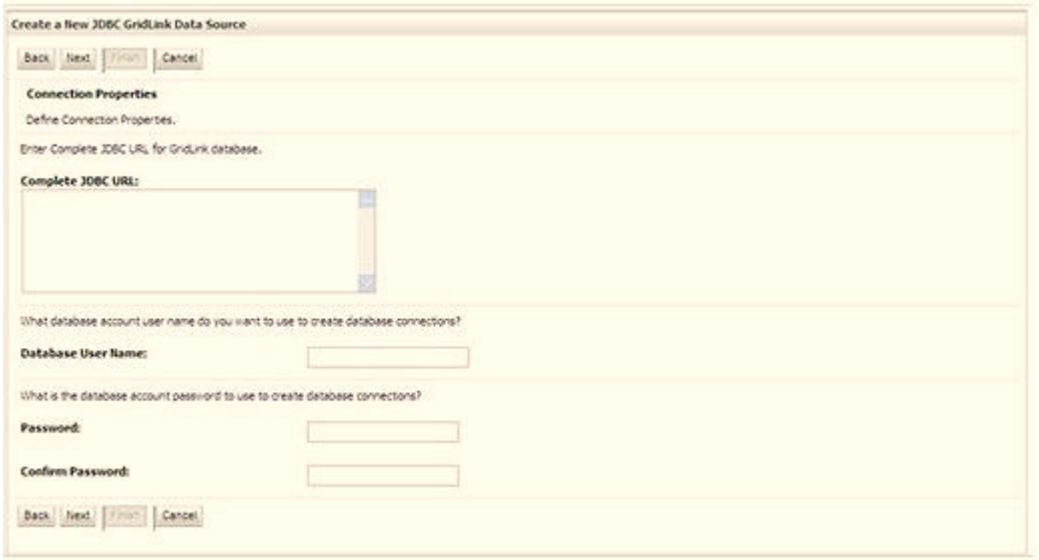
   Ensure that the **JNDI Name** field is specified in the format `jdbc/infodomname` and the **XA Driver** check box is not selected. Click **Next**.

Figure 11-18 JNDI Name



3. Specify **Complete JDBC URL**, **Database User Name**, and **Password**. Click **Finish**.

Figure 11-19 GridLink Data Source



The created **Data Source** is displayed in the list of Data Sources.

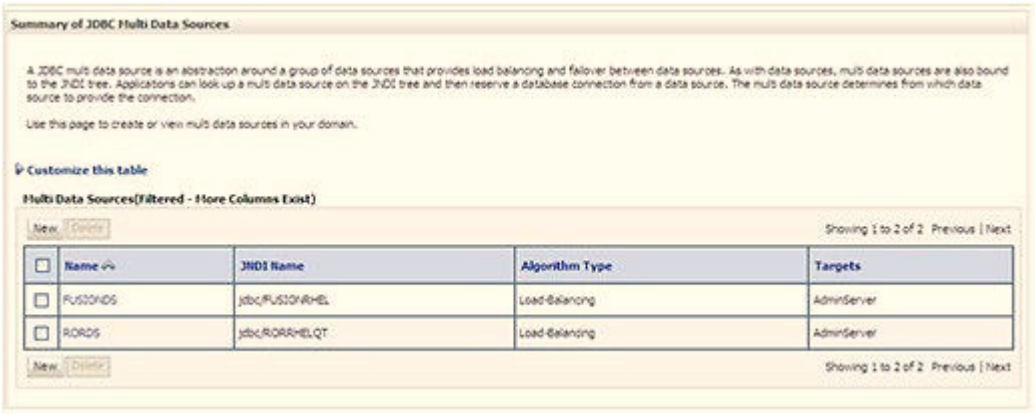
Configure Multi-data Sources

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

When the database used is Oracle RAC (Real Application Clusters), which allows Oracle Database to run across a set of clustered servers, then 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.

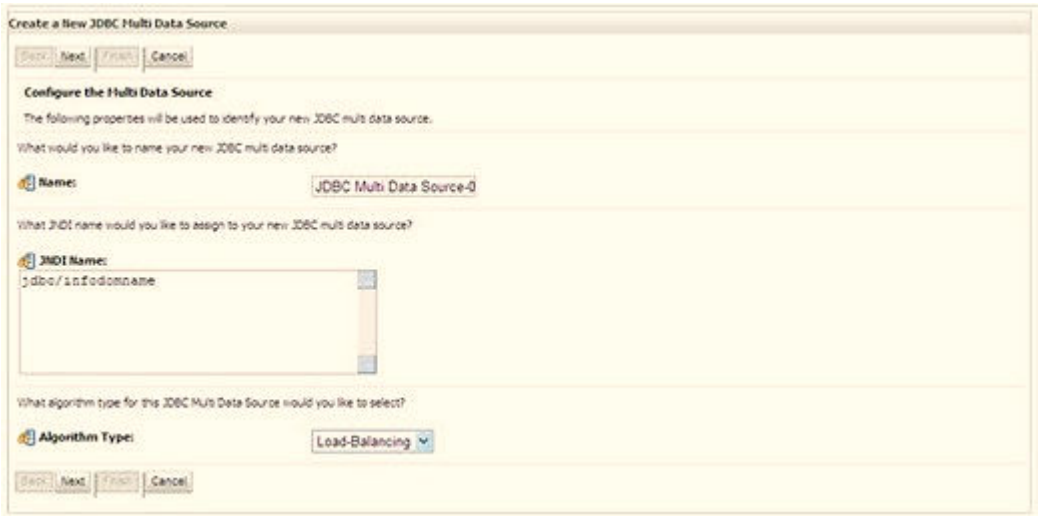
1. Open the WebLogic Admin Console in the browser window: http://<ipaddress>:<administrative console port>/console. (https if SSL is enabled). The Login window is displayed.
2. Login with the **User ID** that has admin rights.
3. In the LHS menu (Domain Structure), select **Services > JDBC > Multi Data Sources** to display the Summary of JDBC Multi Data Sources window.

Figure 11-20 Multi Data Sources



4. Click **New** to display the New JDBC **Multi Data Source** window.

Figure 11-21 Configure Multi Data Source



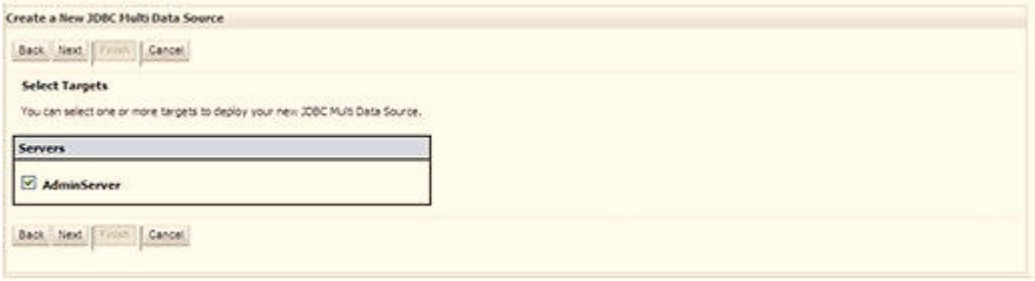
Ensure that the Data Sources which must be added to the new JDBC Multi Data Source are created.

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/ infodomname.
- 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 11-22 Select Targets

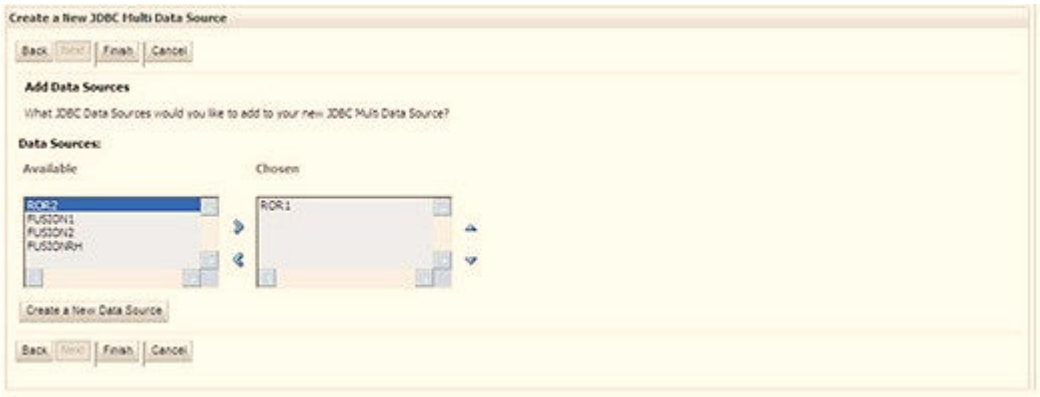


6. Select the **AdminServer** check box and click **Next**.

Figure 11-23 Select Data Source Type

7. Select the type of data source to add to the new JDBC Multi Data Source. Click **Next**.

Figure 11-24 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.

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.

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:
   a. **Initial Capacity**: 10
   b. **Maximum Capacity**: 100
   c. **Capacity Increment**: 1
   d. **Statement Cache Type**: LRU

e. **Statement Cache Size**: 10

3. Click **Save**.

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 11-25 WorkManager Screen 1

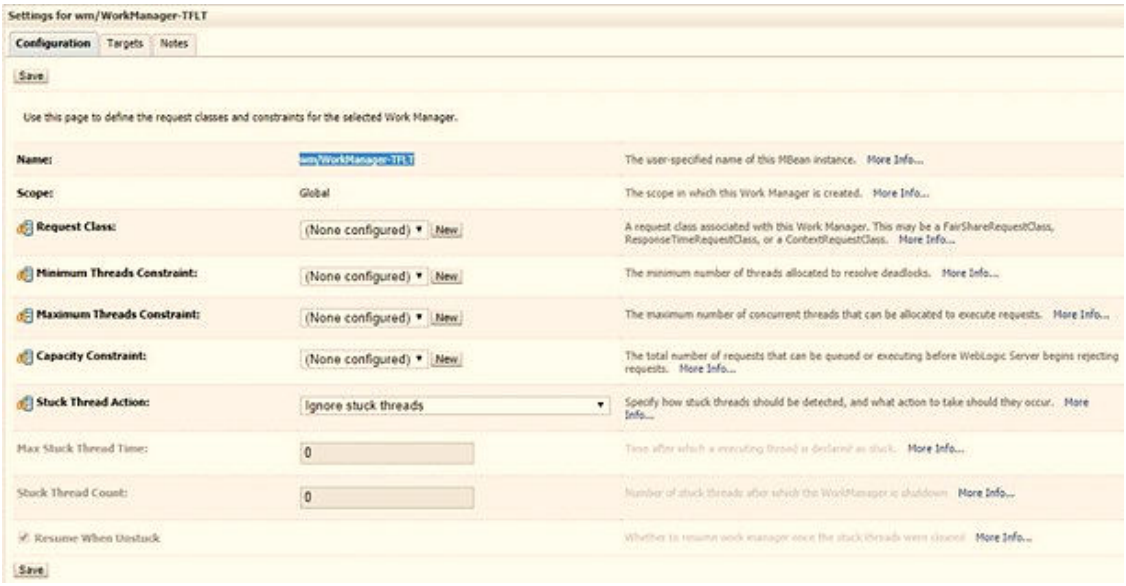
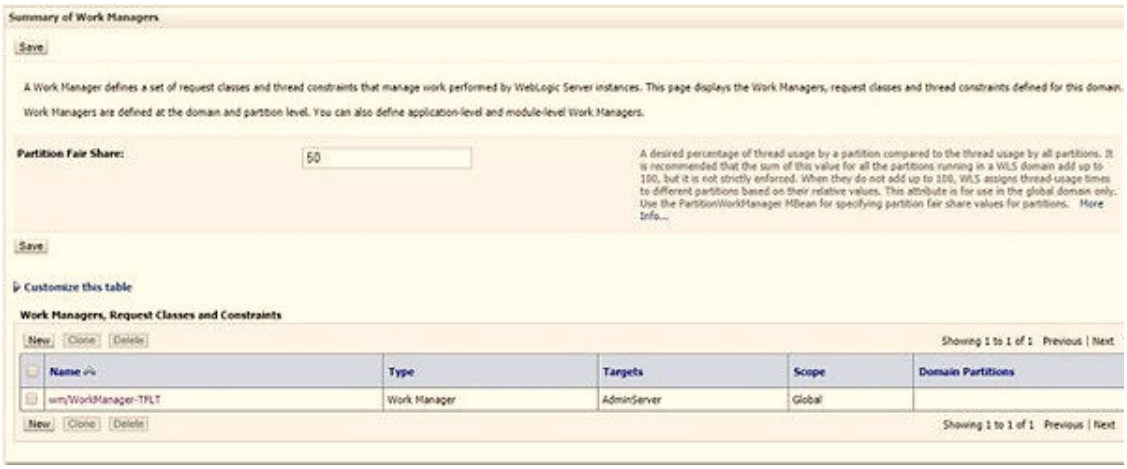


Figure 11-26 Workmanager Screen 2



Configure Resource Reference in Tomcat Application Server

This section is applicable only when the Web application server type is Tomcat and includes the following 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.

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 ofsaaconf, then the actual schema created in the database is DEV_ofsaaconf.

```
<Context path ="/<context name>" docBase="<Tomcat Installation
Directory>/webapps/<context name>" debug="0" reloadable="true"
crossContext="true"><Resource auth="Container" name="jdbc/FICMASTER"
```

```
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver" username="<user id for the
configuration schema>" password="<password for the above user id>"
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100" maxIdle="30" maxWait="10000"/><Resource auth="Container"
name="jdbc/< INFORMATION DOMAIN NAME >"
type="javax.sql.DataSource"
driverClassName="oracle.jdbc.driver.OracleDriver" username="<user id for the
atomic schema>" password="<password for the above user id>"
url="jdbc:oracle:thin:@<DB engine IP address>:<DB Port>:<SID>"
maxActive="100" maxIdle="30" maxWait="10000"/>
</Context>
```

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.

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 present 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 ofsaaconf, then the actual schema created in the database is DEV_ofsaaconf.

Configure ClassLoader for Apache Tomcat

To configure the ClassLoader for Apache Tomcat, follow these steps:

1. Edit the `server.xml` file available in `$TOMCAT_HOME/conf/` directory.
2. 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.

12

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

Topics:

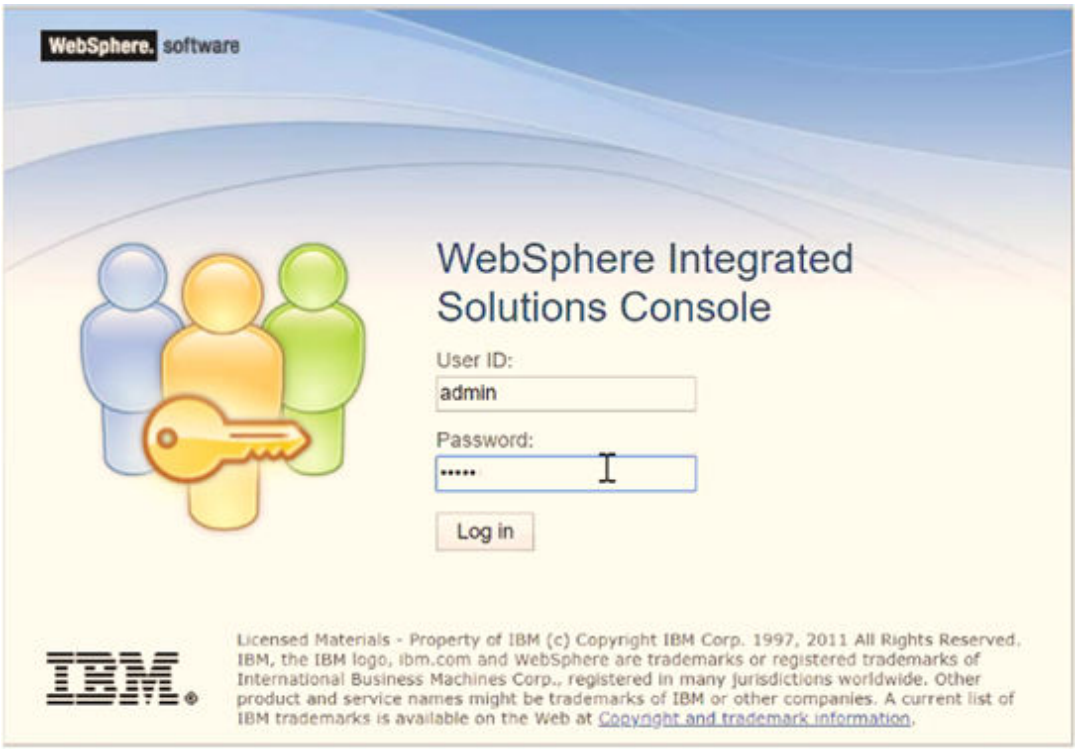
Create Work Manager

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 12-1 WebSphere Login page

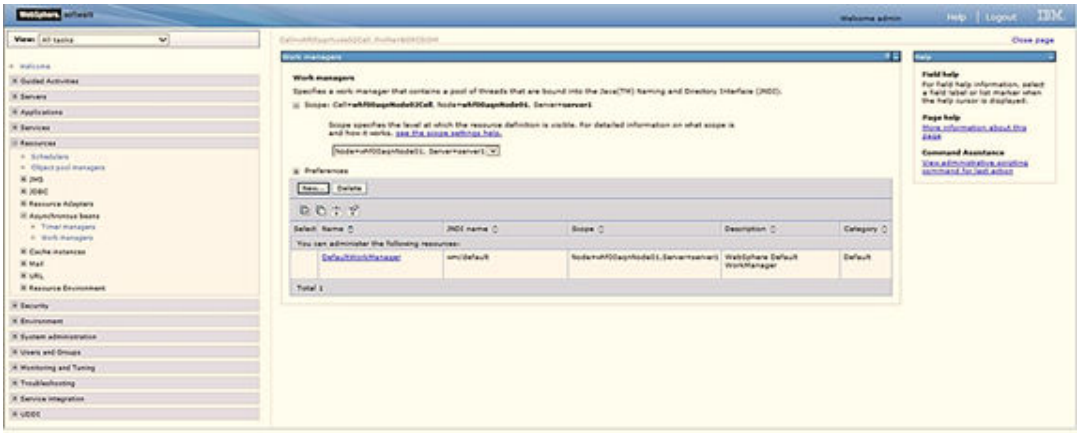


2. Log in with the user ID which has admin rights.

Figure 12-2 Home page

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

Figure 12-3 Work Managers

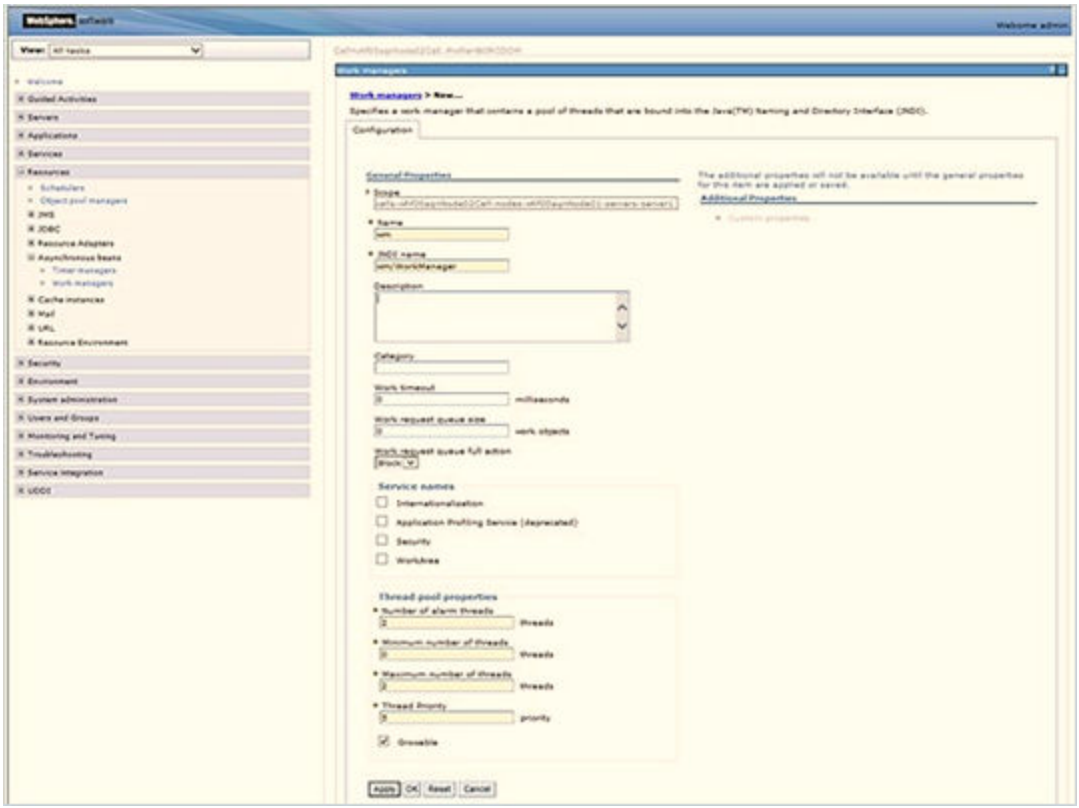


4. Select the required Scope from the drop-down list.

   For example, Node=whf00aqnNode01, Server=server1.

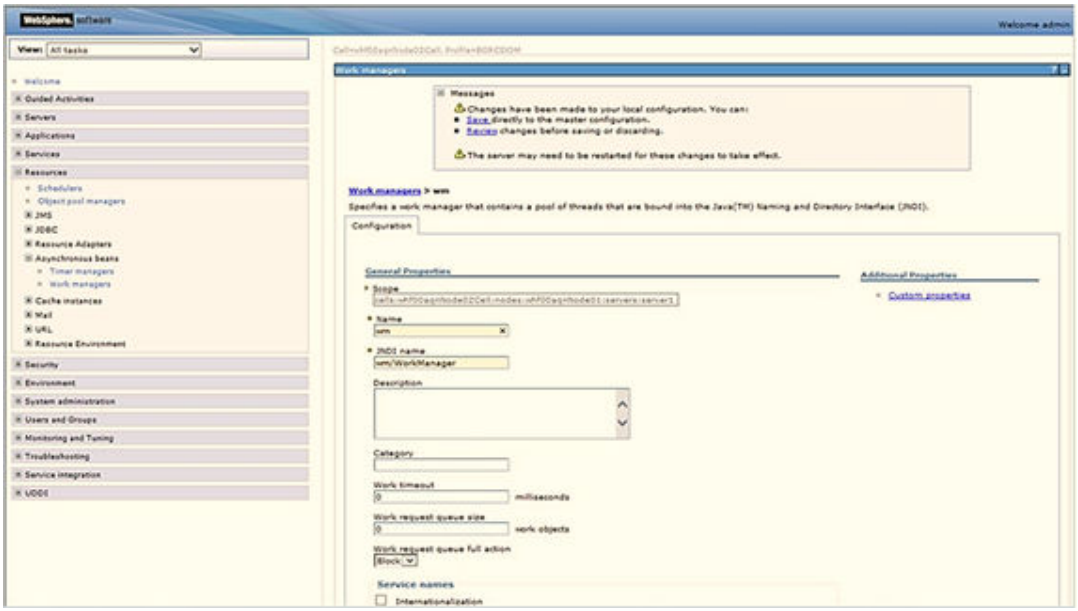
5. Click **New** in the **Preferences** section.

Figure 12-4 New Work Managers



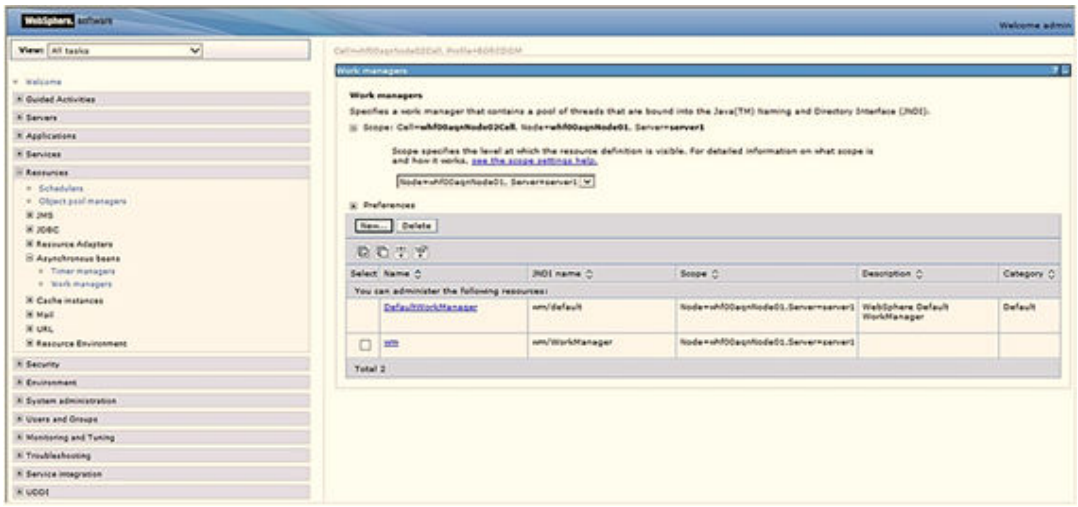
6. Enter the **Name** as 'wm' and JNDI name as 'wm/WorkManager ' in the respective fields.
7. Enter the **Thread pool properties**.
8. Click **Apply**.

Figure 12-5 Configure Work Managers



9. Click **Save**.

Figure 12-6 Work Managers Preferences



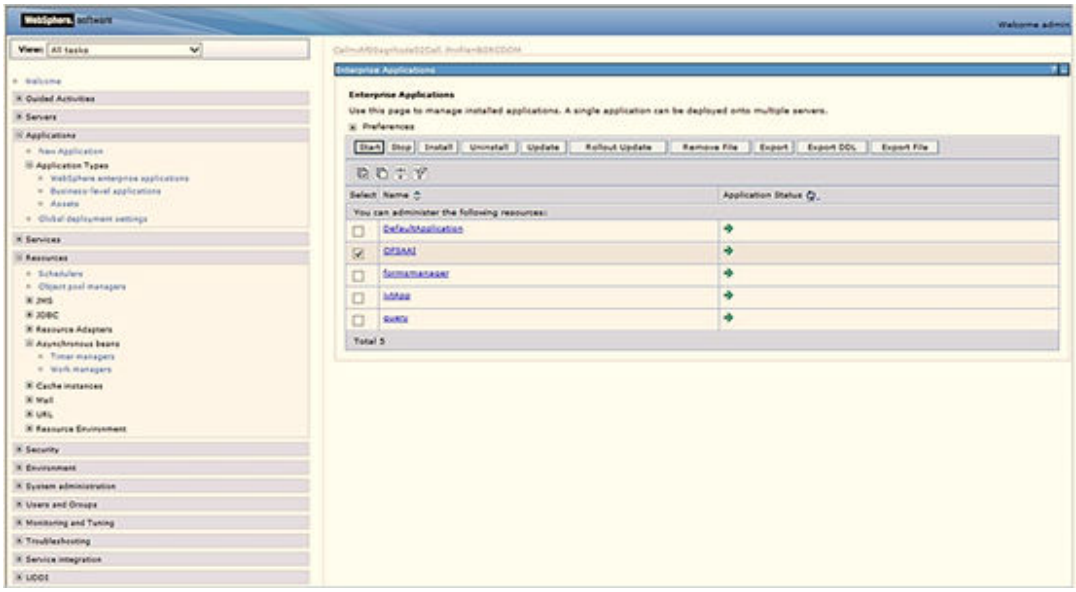
After creating the work manager, you must map it to an OFSAA instance.

Map Work Manager to OFSAA WebSphere Instance

To map the Work Manager to an OFSAA WebSphere Instance, follow these steps:

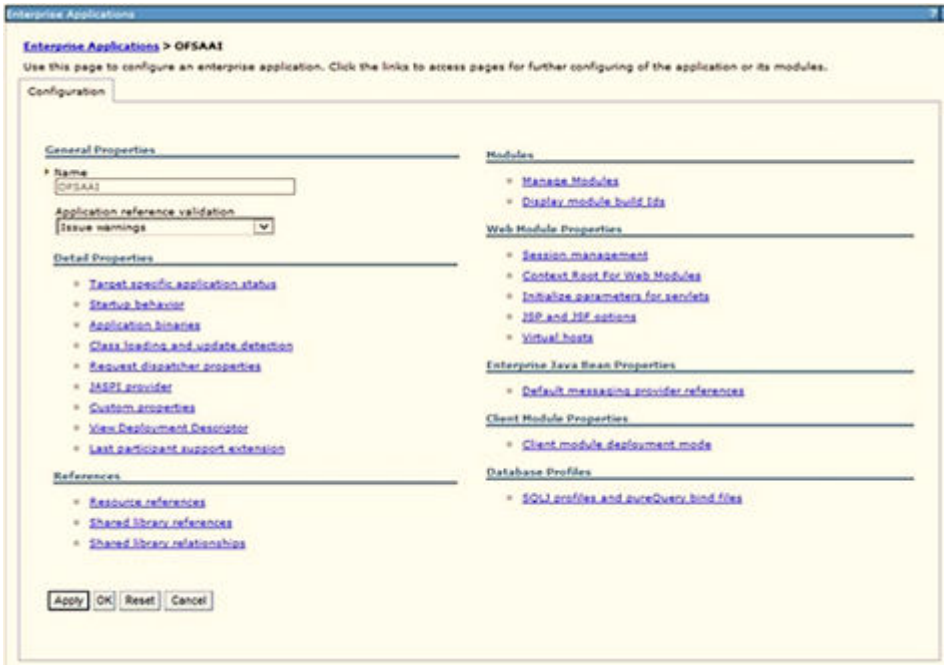
1. From the LHS menu, expand **Applications > Application Types** and click **WebSphere enterprise applications**.

Figure 12-7 Enterprise Applications



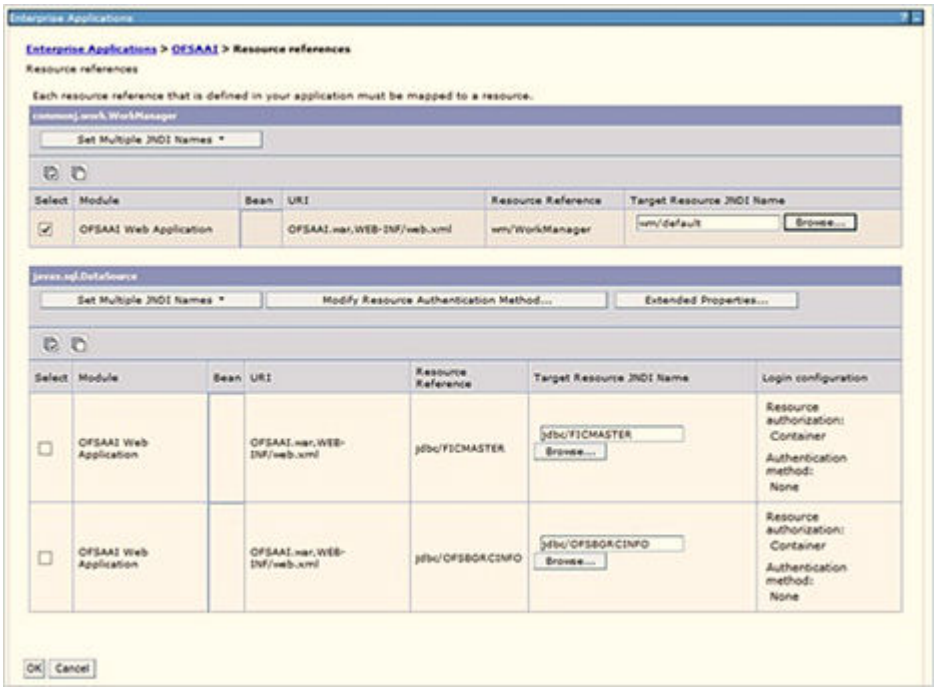
2. Click OFSAAI instance hyperlink.

Figure 12-8 OFSAAI



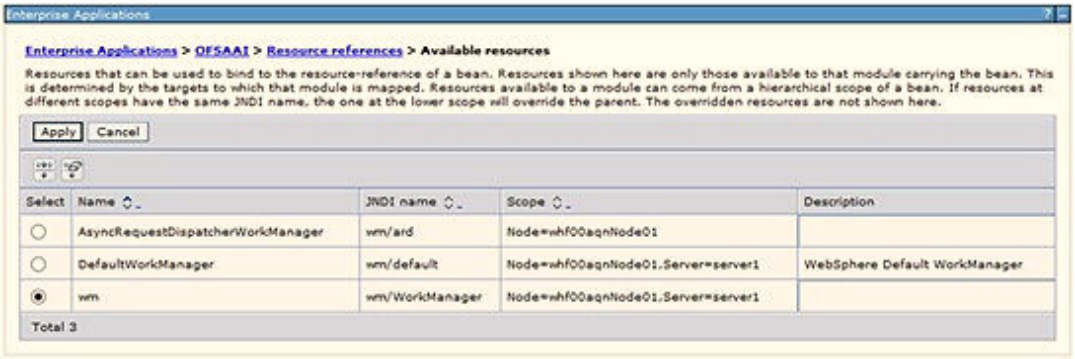
3. Click the **Resource references** link under the **References** section.

Figure 12-9 Resource References



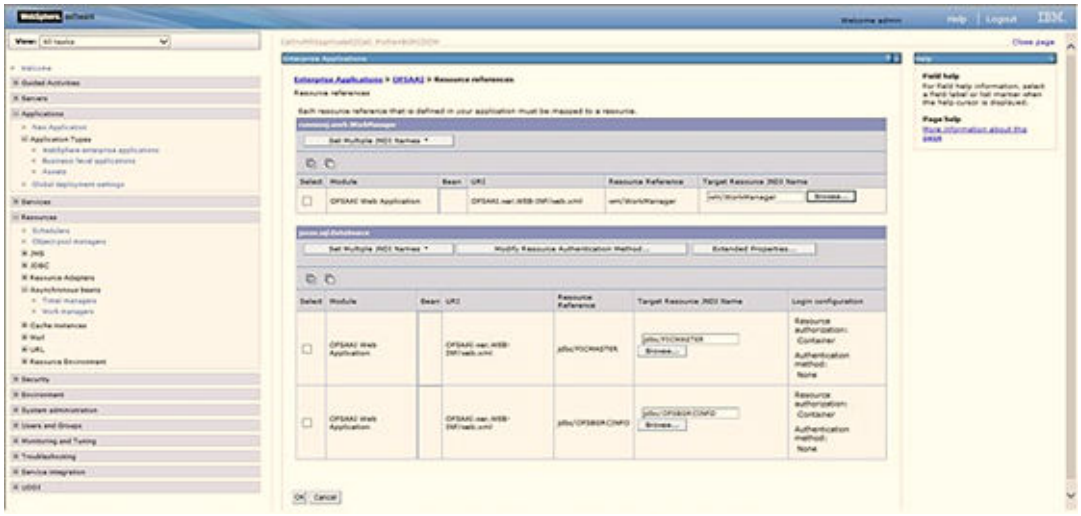
4. Click **Browse** corresponding to the Work Manager Resource Reference. The available resources are displayed.

Figure 12-10 Available Resources



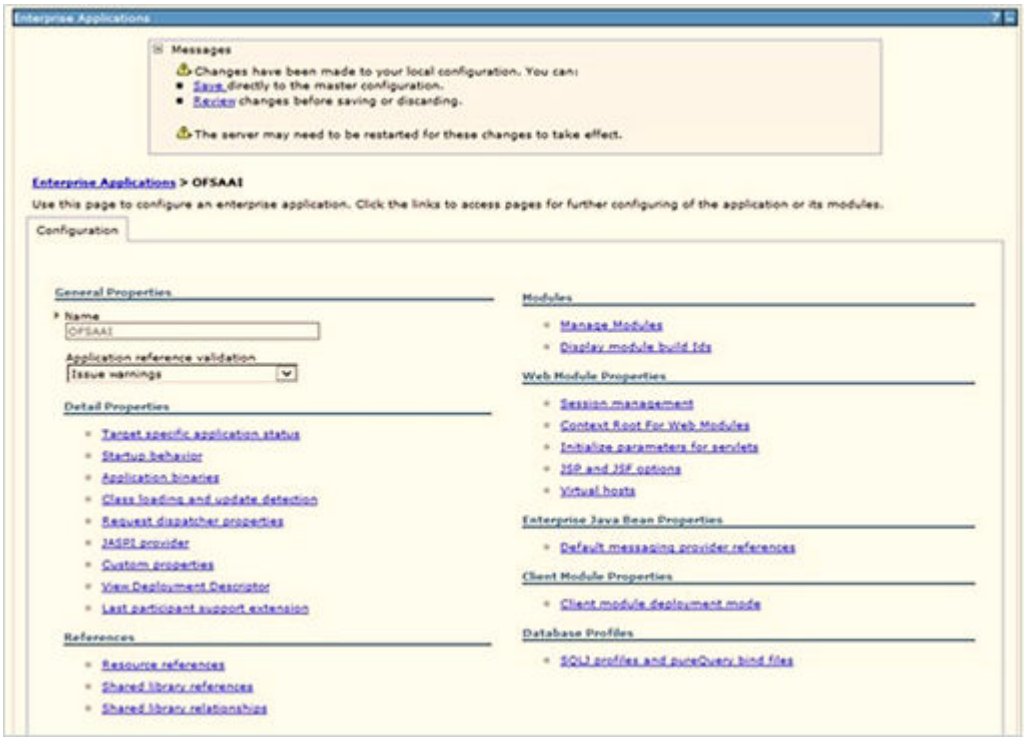
5. Select the newly created Work Manager ('wm') and click **Apply**.

Figure 12-11 Select Work Manager



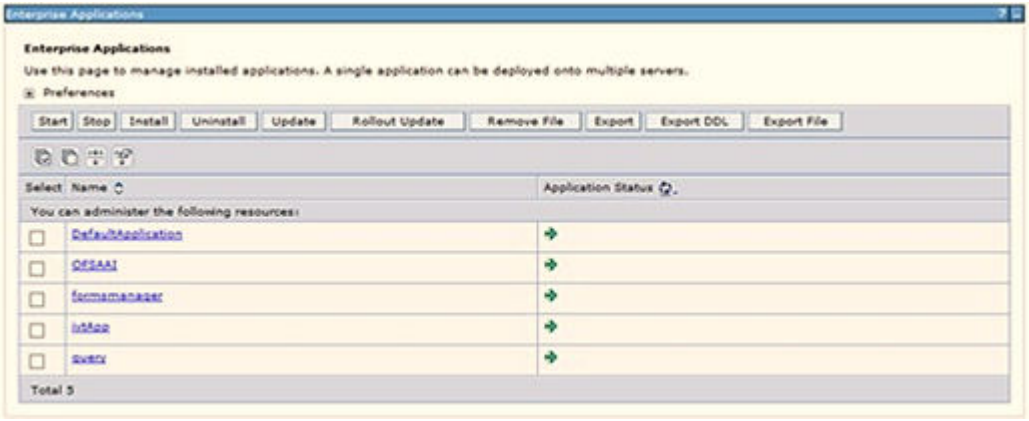
6. Select the Work Manager ('wm/WorkManager') and click **OK**.

Figure 12-12 OFSAAI Configuration



7. Click **Save**.

Figure 12-13 Enterprise Applications Preferences

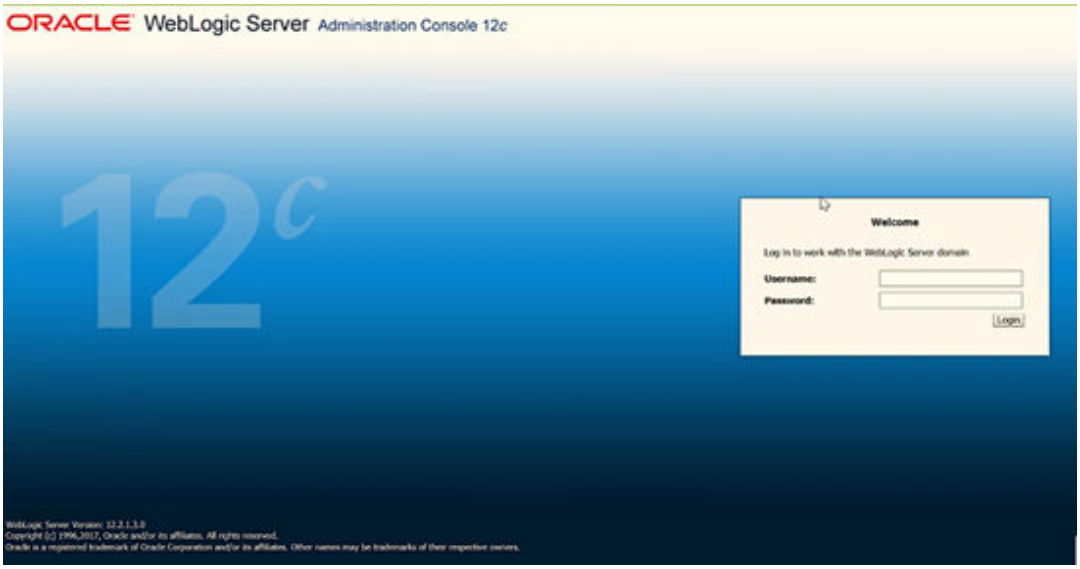


Configure Work Manager in WebLogic Application Server

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 12-14 WebLogic Login page

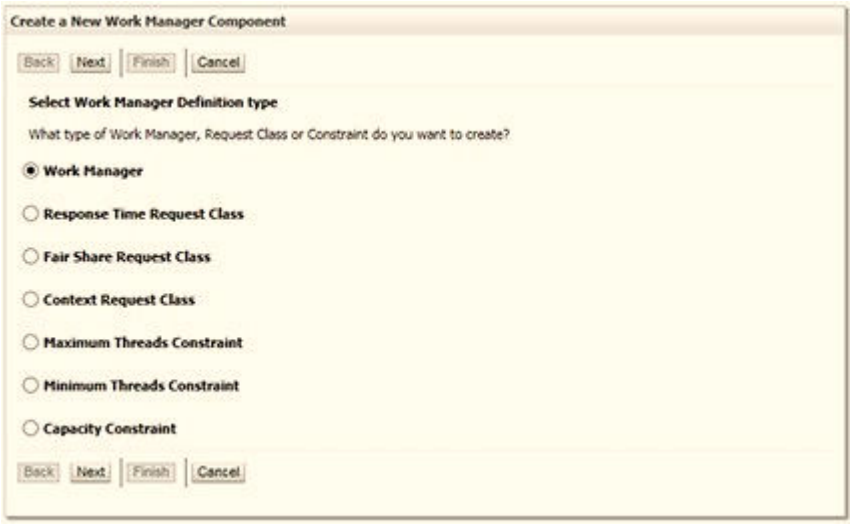


2. Log in with the user ID that has admin rights.
3. From the **Domain Structure** menu in the LHS, expand Environment and select **Work Managers** to display the Summary of Work Managers window.

Figure 12-15 Work Manager

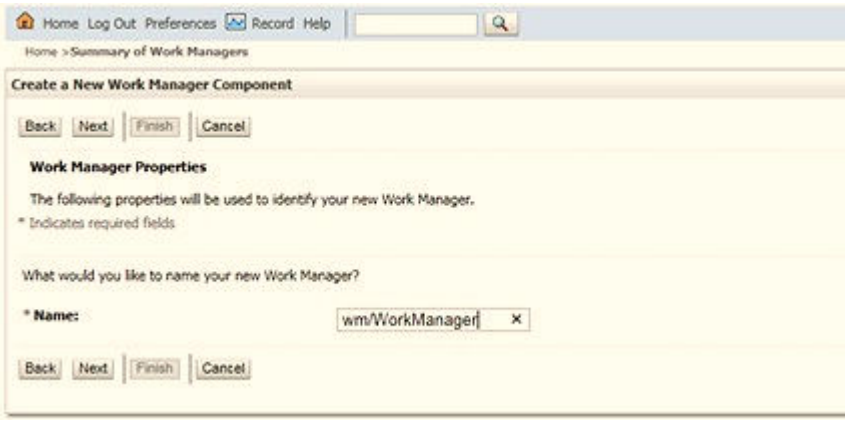
4. Click **New** to create a new Work Manager component.

Figure 12-16 New Work Manager



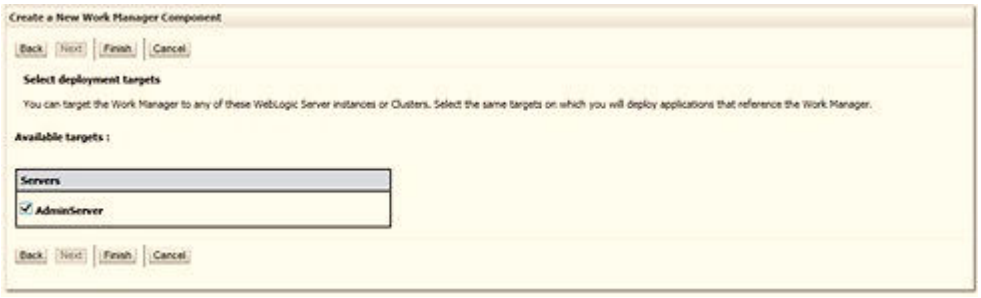
5. Select the Work Manager and click **Next**.

Figure 12-17 Work Manager



6. Enter the Name as 'wm/WorkManager' and click **Next**.

Figure 12-18 Select Deployment Targets



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

Figure 12-19 Summary of Work Managers

13

Additional Configurations for Application Packs

This section provides information for additional configurations required for the OFSAA application packs.

Topics:

Configurations for Enterprise Modeling

This section is applicable only if OFS Enterprise Modeling is licensed and enabled in your OFSAA instance. See the OFS Analytical Applications Infrastructure Administration Guide for information on additional configurations.

Perform the following configurations before you start using Enterprise Modeling framework:

1. Install the OFSAAAI Runner package in the database server to execute ORE models. This is a mandatory step and you can find the Runner package in the `$FIC_ HOME/ficdb/lib` directory. For more information, refer to the section Install OFSAAAI Runner Package.
2. Configure ORE 1.5 to load the Cairo library in Oracle Linux/RHEL 7 by creating a symbolic link from libtiff.so.3 to libtiff.so.5 for the ORE executions to succeed. Follow the steps given below to create a symbolic link:
   a. Log in as root and change directory to `/usr/lib64`.
   b. Execute the following command:
   ```
   ln -s libtiff.so.5 libtiff.so.3
   ```

   > **Note:**
   >
   > Contact My Oracle Support if you require further assistance on ORE 1.5

   c. Execute Variable Migration Utility to migrate the variables defined in previous versions to 8.1.2.0.0 version. For more details, see the Variable Migration utility section in OFS Analytical Applications Infrastructure Administration Guide.

Sandbox Resave Utility

A utility is provided to regenerate the CONSTRAINTS.XML as per the changes done as part of Update Constraints utility. The constraint XML is required for the sandbox data population which will store the foreign key names of all the tables.

The XML files to be regenerated are:

```
ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/CONSTRAINTS.xml
```

```
ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/<TABLE_NAME>.xml
```

Prerequisites

Update Constraints utility must be run successfully on all the sandbox and production Infodoms.

How to Run the Utility

To run the utility:

1. Navigate to the `$FIC_HOME/utility/sandboxutil/bin` directory and grant RWX (755) permissions for all executables (`.sh` files).
2. Execute the utility using the following command:

   ```
   ./updatesandbox.sh
   ```

3. Verify logs from the `$FIC_HOME/utility/sandboxutil/logs/Update.log` directory.
4. If the process is successful, verify the following references for new constraint names:

   ```
   ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/CONSTRAINTS.xml
   ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox/<TABLE_NAME>.xml
   ```

5. In case of failure, refer the utility's log and restore the backups for the file system.
6. Execute the utility for the failed infodoms one by one using the following command:

   `$FIC_HOME/utility/sandboxutil/bin/updatesandbox.sh $INFODOM`.

> **Note:**
>
> The utility does the backup of `ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox` directory as `ftpshare/<SANDBOXINFODOM>/erwin/scripts/sandbox_bkp`, but restore is not done. Restore must be done manually in case of any failure. The backup directory will be created in the app ftpshare area. In case of any failure, the backup has to be replaced in the database ftpshare area also. For queries, contact My Oracle Support.

Model Resave Utility

If you upgrade OFSAAI to 8.1.2.0.0 from an older version, you have to resave all ORE based models. To resave, you have to use the utility `modelresave.sh`, which is available in the directory `$FIC_DB_HOME/bin`.

> **Note:**
>
> You cannot trigger the model resave utility if the RQADMIN role is not granted to Configuration Schema. For more information on granting the role, refer to the section Configure Oracle R distribution and Oracle R Enterprise (ORE).

To run the utility from the console:

1. Navigate to the `$FIC_DB_HOME/bin` directory and grant RWX (755) permissions for all executables (.sh files).

2. Execute the utility using the following command:
   `./modelresave.sh`

   This will resave all the available ORE models.

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

   For example, `./modelresave.sh <infodom>`

> **Note:**
>
> You can find the logs in `$FIC_DB_HOME/log/migration.log`
>
> .

Enable Financial Services Enterprise Modeling on Another Application Pack

To enable Enabling Financial Services Enterprise Modeling on another Application Pack, follow these steps:

1. Download the OFSAAAI Applications Pack Installer
2. Extract the Software
3. Configure OFS_<App pack>_PACK.xml File
4. Enable the option as YES for the App ID OFS_AAAI as shown in the following illustration:

Figure 13-1 Enable Financial Services Enterprise Modeling

5. Install the OFSAAI Application Pack

Configure Process Modeling Framework

Configure the excludeURLList.cfg File

To configure the `excludeURLList.cfg` file, follow these steps:

1. Go to `$FIC_WEB_HOME/webroot/conf`.
2. Create a backup of the file `excludeURLList.cfg`.
3. Edit the following details in `excludeURLList.cfg` file:

   ```
   [SQLIA]./dataIntegrator/ to [ALL]./dataIntegrator/
   [SQLIA]./ETLExtractionServlet to [ALL]./ETLExtractionServlet
   ```

4. Go to `$FIC_WEB_HOME`.
5. Backup the existing ear/war files.
6. Delete `<app>.ear` and `<app>.war` files.
7. Re-create the ear/war files by running `ant.sh`.
8. Use the new ear/war files and re-deploy them.
9. Re-start the OFSAA environment.

Configure Oracle R Distribution and Oracle R Enterprise (ORE)

Configure Oracle R Distribution and Oracle R Enterprise only if OFS Enterprise Modeling is licensed and enabled in your OFSAA instance.

1. Install OFSAAIRunner Package. For more information, see Install OFS_AAAI_Runner_Package. If you have already installed the OFSAAIRunner package (as part of a previous installation), uninstall it. (For more information, see Uninstall_OFSAAI_Runner_Package, and reinstall the latest available OFSAAIRunner package.
2. Log in to the database with dba privileges and provide the RQADMIN privilege to Configuration Schema by executing the command: `GRANT RQADMIN TO <config_schema>;`
3. Log in to the database with dba privileges and provide the following privileges to Atomic Schema:
   CREATE UNLIMITED TABLESPACE privilege by executing the command:

   ```
   GRANT CREATE UNLIMITED TABLESPACE TO <atomic_schema>;
   ```

   CREATE MINING MODEL privilege (to execute the Data Mining models) by executing the command:

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

Installing OFSAAAI/OFSAAI Runner Package

Oracle R and ORE must be installed on the Oracle Database server before installing the OFSAAIRunner package.

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

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

OFSAAIRunner package (`OFSAAIRunner_1.0.0.tar.gz`) is available in the `$FIC_DB_ HOME/lib` directory.

To install OFSAAI Runner package:

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

   ```
   ORE CMD INSTALL OFSAAIRunner_1.0.0.tar.gz
   ```

6. Successful installation is indicated in the installation log as:

   ```
   * DONE (OFSAAIRunner)
   Making packages.html ... done
   ```

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

7. Navigate to the directory `$ORACLE_HOME/R/library` and check whether OFSAAIRunner package is listed thereby executing the command:

   `>library(OFSAAIRunner)>OFSAAIRunner::` and press TAB twice.

   This lists out all the functions.

Uninstall OFSAAI Runner Package

Perform the following instructions to uninstall the OFSAAIRunner package:

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

   ```
   #ORE
   >remove.packages("OFSAAIRunner")
   ```

3. To save the workspace image, enter the command:

   ```
   >q()
   ```

4. Enter y when prompted to save the workspace image. Save workspace image? `[y/n/c]:` `y`

5. Navigate to the directory `$ORACLE_HOME/R/library` and verify the package is not listed thereby executing the command:

   `ls -l`

Configure ORE Execution

To configure ORE execution, add a TNS entry in the `tnsnames.ora` file. This is the value set for `ORACLE_SID` in the database server.

For the RAC database, repeat the above step in all the machines.

Configure Tomcat

Configure the `web.xml`file.

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

To configure the `web.xml` file:

1. Navigate to `tomcat/conf` directory.
2. In the `web.xml` file, set the mapped file parameter to `False` in the servlet tag mentioned with `<servlet-name>jsp</servlet-name>. <init-param> <param-name>mappedfile</ param-name> <param-value>false</param-value> </init-param>`.

Configure Big Data Processing

This section is not applicable if you have enabled Financial Services Big Data Processing during the installation of OFSAAI 8.1.2.0.0 full installer. Follow instructions in this section if you intend to enable Big Data Processing.

Topics:

Copy Jars to the OFSAA Installation Directory

1. Download the supported Cloudera HIVE JDBC Connectors and copy the following Jars to the location `$FIC_HOME/ext/lib` and `$FIC_WEB_ HOME/webroot/WEB-INF/lib`. For the latest supported versions, see OFSAA Technology Matrix 8.1.2.0.0.
   - `hive_service.jar`
   - `hive_metastore.jar`
   - `HiveJDBC4.jar`
   - `zookeeper-3.4.6.jar`
   - `TCLIServiceClient.jar`

> **Note:**
>
> If the Hive JDBC version is 2.5.x, then copy the log4j-1.2.17.jar File to the $FIC_WEB_HOME/webroot/WEB-INF/lib and $FIC_HOME/ext/lib Directory locations.

2. Copy the following Jars <Cloudera Installation Directory>/jars directory based on the CDH version to the location `$FIC_HOME/ext/lib` and `$FIC_WEB_HOME/webroot/WEB-INF/lib`:

CDH v5.13.0:

```
commons-collections-3.2.2.jar
commons-configuration-1.7.jar
commons-io-2.4.jar
commons-logging-1.2.jar
hadoop-auth-2.6.0-cdh5.13.0.jar
hadoop-common-2.6.0-cdh5.13.0.jar
hadoop-core-2.6.0-mr1-cdh5.13.0.jar
hive-exec-1.1.0-cdh5.13.0.jar
httpclient-4.3.jar
httpcore-4.3.jar
libfb303-0.9.3.jar
libthrift-0.9.3.jar
slf4j-api-1.7.5.jar
slf4j-log4j12-1.7.5.jar
```

CDH v6.3.0:

```
commons-collections-3.2.2.jar
commons-configuration2-2.1.1.jar
commons-io-2.6.jar
commons-logging-1.2.jar
hadoop-auth-3.0.0-cdh6.3.0.jar
hadoop-common-3.0.0-cdh6.3.0.jar
hive-exec-2.1.1-cdh6.3.0.jar
httpclient-4.5.3.jar
httpcore-4.4.6.jar
libfb303-0.9.3.jar
libthrift-0.9.3.jar
slf4j-api-1.7.25.jar
slf4j-log4j12-1.7.25.jar
stax2-api-3.1.4.jar
woodstox-core-5.0.3.jar
```

Copy 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 Kerberos applications, and mappings of hostnames onto Kerberos realms.

If the Authentication is configured as KERBEROS_WITH_KEYTAB for the Hive database, then you must use the Keytab file to login to Kerberos. The Keytab and Kerberos files must be copied to `$FIC_HOME/conf` and `$FIC_WEB_ HOME/webroot/conf` of the OFSAAAI installation directory.

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

Restart the Web application server and the OFSAAAI Application Server. For more information, see the Start the Infrastructure Services section.

Enable Big Data

To enable Big Data option, follow these steps:

1. Download the OFSAAAI Applications Pack Installer
2. Extract the Software
3. Configure OFS_<App pack>_PACK.xml File
4. Enable the option as YES for the App ID OFS_AAIB as shown in the following illustration:

Figure 13-2 Enable Big Data

5. Install the OFSAAI Application Pack

Configure Transparent Data Encryption (TDE) and Data Redaction in OFSAA

This section details the configurations required in case you want to enable Transparent Data Encryption (TDE) or Data Redaction in OFSAA applications.

Prerequisites

Ensure the required Oracle Database Server versions are installed:

- Oracle Database Server Enterprise Edition 18c Release 3 - 64 bit RAC/Non-RAC with/ without partitioning option, Advanced Security Option.
- Oracle Database Server Enterprise Edition 19c Release 3 - 64 bit RAC/Non-RAC with/ without partitioning option, Advanced Security Option.

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.

To configure TDE for OFSAA, follow these steps:

1. Create a new PDB (19c)/ instance (18c) on the same or different Database Server for TDE. For more information, see Configure 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@OFSA19c2DB 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@OFSA12nDB 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 Steps 1 and 2, retain the user credentials of Configuration and Atomic Schemas the 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:

   ```
   Log in as sys user:
   SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaaconf;
   Grant succeeded
   SQL> GRANT SELECT ON SYS.V_$PARAMETER TO ofsaaatm;
   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, Protocol of the OFSAA Instance* section under *Generic Configurations* chapter in OFS Analytical Applications Infrastructure Administration Guide.
8. Navigate to the `$FIC_WEB_HOME` directory and execute the following command to trigger the creation of the EAR/WAR file:

   ```
   ./ant.sh
   ```

9. The EAR/WAR file - `<contextname>.ear/.war` - is created in the `$FIC_WEB_HOME` directory.
10. On completion of the EAR/WAR file creation, the message "BUILD SUCCESSFUL" is displayed.
11. Edit the existing Connection Pool settings to point to the new JDBC URL and verify connections.
12. Clear the webserver cache and redeploy the application onto your configured web application server.
13. Restart the OFSAA Services. For more information, see Start the Infrastructure Services.

Configure 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.

   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 must have the required privileges to perform the following actions.

To configure the software keystore, follow the instructions in the following sections:

- Set the Software Keystore Location in the sqlnet.ora File
- Create the Software Keystore
- Open the Software Keystore
- Set the Software TDE Master Encryption Key
- Encrypting your Data
- Test the Encryption

Set the Software Keystore Location in the sqlnet.ora File

The first step is to designate a location for the 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 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 a 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)))
```

Create the Software Keystore

There are three types of Software Keystores:

- Password-based Software Keystores
- Auto-login Software Keystores
- Local Auto-login Software Keystores

Perform the following steps to create a software keystore:

1. Log in as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. 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 the creation of the keystore. There are no ways to retrieve the password if forgotten.

Open the Software Keystore

Depending on the type of keystore you create, you must manually open the keystore before you can use it.

You must not manually open auto-login or local auto-login software keystores. These keystores 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.

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.

Perform the following steps to open the software wallet:

1. Log in as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. 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 must not manually open auto-login or local auto-login software Keystores.

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. 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.)

Perform the following steps to set the encryption key:

1. Log in as sysdba or user with ADMINISTER KEY MANAGEMENT or SYSKM privilege.
2. 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 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
BACKUPUSING 'emp_key_backup';
```

Encrypt 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:

- Set the COMPATIBLE Initialization Parameter for Tablespace Encryption
- Set the Tablespace TDE Master Encryption Key
- Create the Encrypted Tablespace

Set the COMPATIBLE Initialization Parameter for Tablespace Encryption

Prerequisite: You must set the COMPATIBLE initialization parameter for the database to 12.2.0.0 or later. Once you set this parameter to 12.2.0.0, the change is irreversible.

To set the COMPATIBLE initialization parameter, follow these steps:

1. Log in to the database instance. In a multitenant environment, log into the PDB.
2. Check the current setting of the `COMPATIBLE` parameter.
   For example:

```
SHOW PARAMETER COMPATIBLE
NAME                 TYPE            VALUE
------------------        -----------        -------------------
compatible             string        12.0.0.0
noncdbcompatible         BOOLEAN         FALSE
```

3. If you want to change the COMPATIBLE parameter, perform the following steps:
   - 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`).
   - 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
```

   - Edit the initialization parameter file to use the correct COMPATIBLE setting.
     For example:

```
COMPATIBLE = 12.2.0.0
```

   - 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
```

- 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;
```

Set the Tablespace TDE Master Encryption Key

Make sure that you have configured the TDE master encryption key as shown in the Set the Software TDE Master Encryption Key .

Create the Encrypted Tablespace

After you have set the COMPATIBLE initialization parameter, you are ready to create the encrypted tablespace.

Test the Encryption

Test the encryption by checking if a tablespace is encrypted or not. Execute the following query to check:

```
SELECT tablespace_name, encrypted FROM dba_tablespaces;
```

The following result is displayed, which indicates whether the TABLESPACE is encrypted or not in the ENCRYPTED column.

Table 13-1 Testing the Encryption

TABLESPACE_NAME	ENCRYPTED
SYSTEM	NO
SYSAUX	NO
UNDOTBS1	NO
TEMP	NO
USERS	NO
ENCRYPTED_TS	YES

The above example indicates TABLESPACE `ENCRYPTED_TS` is created with Encryption ON.

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 before display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed into a pattern that does not contain any identifiable information.

To enable Data Redaction, perform the following steps:

1. Log in as SYSDBA into the database.

2. Execute the `$FIC_HOME/utility/data_security/scripts/create_data_sec_ roles.sql` file only once per database (PDB in case of 18c/19c).
3. Execute the following SQL statement to find out the list of atomic users from the table: select v_schema_name from aai_db_detail where V_DB_NAME <> 'CONFIG' AND V_DB_TYPE = 'ORACLE'
4. Execute the `$FIC_HOME/utility/data_security/scripts/grant_data_sec_roles.sql` file 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 enabling Data Redaction, see the *Data Redaction* section in the *Data Security and Data Privacy* topic in the OFS Analytical Applications Infrastructure Administration Guide.

Generate JSON Utility

The JSON Utility reads the Object Registration tables and generates entity-wise JSONs that are registered into the **AAI_DMM_METADATA** table.

From the OFS AAI v8.1.2.0.0 release, the model upload processing is done through the JSON format.

> **Note:**
>
> The JSON utility is triggered as part of the OFSAA Application upgrade installation.
>
> The generation of JSONs is done automatically during an upgrade installation. Run this utility only in the event of a failure to generate the JSONs during an upgrade installation.

For information on how it is used in the application, see the Model Upload Using JSON section in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

How to Run the Generate JSON Utility

Refer for steps to run the Generate JSON Utility.

To run the Generate JSON Utility:

Before running the JSON utility, ensure that the FICServer is up and running.

1. Navigate to the `$FIC_HOME/utility/GenerateJSON/bin/` directory and grant `RWX (755)` permissions to all the executable `.sh` files.
2. Execute the utility for each of the failed information domains as follows:

   `$FIC_HOME/utility/GenerateJSON/bin/generatejson.sh <$INFODOM_NAME>`, where the Infodom name is the name of the failed information domain.
3. After executing the utility for all information domains successfully, verify the following references for the JSON files:
   a. All the entity JSONs are generated in the **ftpshare/<INFODOM>/json/fipjson** directory.

b. The **AAI_DMM_METADATA** table must be registered with all the generated JSON.

c. The **V_FLAG_VALUE** parameter in the **AAI_DMM_UTIL_UPDATE_JSON** table in the Config Schema is updated to **Y** for the selected Infodom.

> **Note:**
>
> a. If the Utility fails to generate, check the Utility's log and identify the cause of the failure. Resolve the issues and run the Utility again.
>
> b. If the Utility fails to generate because the Table Version is empty and the Entities were created (Tables created through Batches) outside the Model, update the Version to 0 and re-run the utility.
>
> c. If the JSON Utility fails to generate because of the inconsistent constraints present in the existing environment, run the Update Constraints Utility and make the constraints consistent before running the JSON Utility again. Refer toExecute the Update Constraints Utility for more details.
>
> For any queries, contact Oracle Support Services.

Execute the Update Constraints Utility

Execute the Update Constraints Utility to make the constraints consistent before running the JSON Utility again after it fails.

> **Note:**
>
> This Utility applies only in an Upgrade Scenario.

To execute the Update Constraints Utility, follow these steps:

1. Update the **aai_mu_util_update_cons.v_flag_value** to **N** for the Problematic Infodom in the Config Schema.
2. Drop the following Tables (if they exist) from the Atomic Schema. These Tables were created previously by the Update Constraints Utility.
   - `rev_tab_constraints_u`
   - `rev_tab_ref_constraints_u`
   - `rev_tab_constraint_columns_u`
3. Create a backup of the existing `db.xml` file.
4. Insert a dummy record into the **aai_table_uid_map** Table with **n_table_id** as **maxvalue + 1**.
5. Create a backup of the **aai_table_uid_map** Table and truncate the data except for the dummy record.
6. Execute execute `.sh` for the specific Infodom as follows:

```
cd $FIC_HOME/utility/UpdateConstraints/bin
./execute.sh <infodom_name>
```

7. Verify the log files generated in the `$FIC_HOME/utility/UpdateConstraints/logs` directory.

14

Additional Information

Additional tasks are required to perform miscellaneous task like file transfer, accessing patch information, configuring File OLAP details, Java virtual machine and password.

Retrieve Patch Information

View the list of patches installed on the OFSAA setup.

To identify the list of patches installed on your OFSAA setup:

1. Log in to the OFSAA application as a user with Object AdminAdvanced Role.
2. Navigate to **Object Administration** tab, expand **Utilities**, and click **Patch Information** to view the list of patches installed on the OFSAA setup across Applications/Platforms.

Set 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 must 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 the shutdown of the 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 based on the load the system is subjected to, before restarting the Data Services subsystem.

Change IP/ Hostname, Ports, Deployed Paths of the OFSAAInstance

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

Set Infrastructure LDAP Configuration

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

Configure OFSAAI Web Services

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

Topics:

Configure DynamicWSConfig.xml File

Configure the `DynamicWSConfig.xml` template file.

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

The variable <WebServer> denotes any one of the application servers, that is, WebSphere, WebLogic, or Tomcat.

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

The `DynamicWSConfig.xml` template file is in the `<WebServer Deployment Path>/EXEWebService.ear/EXEWebService.war/conf` directory.

This template is as follows:

```
<XML>
<WEBSERVICES>
<WEBSERVICE CODE="$CODE"
ENDPOINT="$ENDPOINT" TARGETNAMESPACE="$TARGETNAMESPACE"
XMLNS_XSD="$XMLNS_XSD" ENCODINGSTYLE="$ENCODINGSTYLE"
SERVICENAME="$SERVICENAME" PORTTYPENAME="$PORTTYPENAME"
SESSION_MAINTAIN_PROPERTY="$SESSION_MAINTAIN_PROPERTY" USERNAME="$USERNAME"
PASSWORD="$PASSWORD" STYLE="$WEBSERVICESTYLE"
STUBIMPLEMENTATION="$STUBIMPLEMENTATION">
<OPERATION CODE="$CODE" NAME="$NAME" SOAPACTION="$SOAPACTION" STYLE="$STYLE"
PACKAGENAME="$PACKAGENAME">
<INPUT ORDER="$ORDER" PARAMNAME="$PARAMNAME" ARGTYPE="$ARGTYPE"
CLASSNAME="$CLASSNAME"/>
<OUTPUT PARAMNAME="$PARAMNAME" RETURNTYPE="$RETURNTYPE"
CLASSNAME="$CLASSNAME"/>
</OPERATION>
</WEBSERVICE>
```

```
</WEBSERVICES>
</XML>
```

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

Attributes of WEBSERVICE tag

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

Attributes of OPERATION tag

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

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

Attributes of the INPUT tag

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

Attributes of OUTPUT tag

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

Adding web.xml Entries

This step is optional and required only for Tomcat web application server.

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

> **Note:**
>
> In case of Java 7 when WebLogic is used as web application server, replace following line of `<OFSAAI Installation Directory>/EXEWebService/Weblogic/ROOT/WEB-INF/web.xml` file
>
> ```
> <?xml version='1.0' encoding='UTF-8'?>
> <web-app id="WebApp_ID" version="3.0" xmlns="http://
> java.sun.com/xml/ns/javaee"
> xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
> xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://
> java.sun.com/xml/ns/javaee/web-app_3_0.xsd" metadata-
> complete="true">
> ```
>
> with `<?xml version='1.0' encoding='UTF-8'?> <web-app xmlns="http://java.sun.com/xml/ns/j2ee" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">`

Configure WSConfig File

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

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

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

Configure Proxy Settings

Replace the following <param-value> text in the web.xml file with appropriate values.

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

```
<context-param>
<description>http Proxy Host</description>
<param-name>http.proxyHost</param-name>
<param-value>$PROXYHOST$</param-value>

<!-- Specify the IP address or hostname of the http proxy server-->
</context-param>
<context-param>
<description>http Proxy Port</description>
<param-name>http.proxyPort</param-name>
<param-value>$PROXYPORT$</param-value>

<!--Port Number for the Proxy Server-->
</context-param>
<context-param>
<description>http proxy UserName</description>
<param-name>http.proxyUserName</param-name>
<param-value>$PROXYUSERNAME$</param-value>

<!-- User ID To get authenticated by proxy server-->
</context-param>
<context-param>
<description>http proxy Password</description>
<param-name>http.proxyPassword</param-name>
<param-value>$PROXYPASSWORD$</param-value>

<!-- User Password To get authenticated by proxy server-->
</context-param>
<context-param>
<description>http non-ProxyHosts</description>
<param-name>http.nonProxyHosts</param-name>
<param-value>$NONPROXYHOST$</param-value>
```

```
<!--Hosts for which the proxy settings should get by-passed (Note: Separate
them by "|" symbol) -->
</context-param>
```

Configure OFSAAI Home Entry

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

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

```
<context-param>
<description>OFSAAI Web Home</description>
<param-name>FIC_HOME</param-name>
<param-value>$FIC_HOME$</param-value>

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

Deploy OFSAAI Web Services

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

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

   ```
   ./ant.sh
   ```

   This will trigger the EAR/WAR file creation, which is required for the deployment.
3. Deploy the generated EXEWebService.EAR/EXEWebService.WAR file into the WebServer.

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

Enable Parallel Execution of DML statements

A configuration file, OracleDB.conf is introduced to accommodate any configurable parameter related to operations on the Oracle database. If you do not want to set a parameter to a specific value, then the respective parameter entry can be removed/commented off form the OracleDB.conf file that resides in the path `$FIC_ DB_HOME/conf`.

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

clause of the ALTER SESSION statement. The default mode of a session is DISABLE PARALLEL DML. If CNF_DEGREE_OF_PARALLELISM is not set, then the default degree, as decided by Oracle will be used.

Configure Message Details in Forms Designer

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

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

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

Table 14-1 `NotificationConfig.cfg` File Attributes

Parameter	Description
SMTP_SERVER_IP	Specify the hostname or IP address of the 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 the SMTP server requires the client to be authenticated, otherwise set to 'false'.
SMTP_USERNAME	Username required for logging into the SMTP server, if authentication is not required use a dummy value.
SMTP_PASSWORD	Password required for logging into the SMTP server. If authentication is not required, use false value.
SMTP_MAILID	If the Messages must go from a Particular ID that ID must be added. The exchange server forces you to set a valid ID that is there in the exchange server. (Based on Security settings)

Configure Password Changes

This section explains about how to modify the OFSAA Infrastructure Config Schema and Atomic Schema passwords for non Wallet-based and Wallet-based setups.

Topics:

Modify OFSAA Infrastructure Config Schema Password in a Non Wallet-Based Setup

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

1. Shutdown the OFSAAI App service:

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

2. Change the Config Schema User Password in the database.
3. Delete the `$FIC_HOME/conf/Reveleus.SEC` file.
4. Navigate to the `$FIC_HOME/utility/updateatomicpwd/bin` Directory and execute the Utility as shown in the following:

   Syntax:

   ```
   ./rotateAtomicDBPwd.sh <CONFIG/ATOMICALIASNAME> <DB_USER> <DB_PASS>
   ```

   For example,

   ```
   ./rotateAtomicDBPwd.sh CONFIG acte_ofsaaconf password123
   ```

   The execution of the Utility generates the `Reveleus.SEC` File in the `$FIC_HOME/conf/` Directory and a new Encrypted Schema Password is reflected in the **DB_MASTER** and **AAI_DB_AUTH_ALIAS** Tables in the row which displays the Config Schema.

   > **Note:**
   >
   > If you do not delete the existing `Reveleus.SEC` File, then a backup of the file is saved with the `Reveleus.SEC_cfgbkp` name before generating the new `Reveleus.SEC` File.

5. Restart the Infrastructure Server.
6. If you are using Apache Tomcat as the Web server, update the <Context> -> Resource tag details in the `Server.xml` file from the `$CATALINA_HOME/conf` directory. For Tomcat, both Config Schema (FICMASTER resource) and Atomic Schema (<INFODOM_NAME> resource) exist.

   If you are using WebSphere as a Web Server:

   a. Log in to the WebSphere Administration Console, from the left side menu.
   b. Navigate to Resources >JDBC >Data Sources. A list of data sources are 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 must be modified).

   If you are using WebLogic as a Web Server:

   a. Log in 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 are 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 must be modified).

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

Modify OFSAA Infrastructure Atomic Schema Password in a Non Wallet-Based Setup

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

1. Change the Atomic schema User Password in the database.
2. Log in to the application from the browser using the SYSADMN account or any user id, which has a System Administrator role mapped.
3. Navigate to System Configuration > Database Details window. Modify the password as explained in the following steps:
   a. From the Database Master window, select the connection whose password you want to modify and click the button from the toolbar.
   b. Click the button corresponding to the Alias Name. The Alias Details window is displayed.
   c. Modify the password in the Auth String field.

   Alternatively, the steps 1, 2, and 3 can be done using the rotateAtomicDBPwd.sh Utility with the Servers down.
4. Shutdown the OFSAAI App service:

   ```
   cd $FIC_APP_HOME/common/FICServer/bin
   ./stopofsaai.sh
   ```
5. Change the Atomic Schema User Password in the database.
6. Navigate to the $FIC_HOME/utility/updateatomicpwd/bin Directory and execute the Utility as shown in the following:

   ```
   ./rotateAtomicDBPwd.sh <CONFIG/ATOMICALIASNAME> <DB_USER> <DB_PASS>
   ```

   For example,

   ```
   ./rotateAtomicDBPwd.sh acteofsaaatm acte_ofsaaatm password123
   ```

   A new Encrypted Schema Password is reflected in the **DB_MASTER** and **AAI_DB_AUTH_ALIAS** Tables in the row which displays the Atomic Schema.

   > **Note:**
   >
   > ATOMICALIASNAME value is a TNS alias for Atomic Schema and must not contain underscores.
   >
   > For example, if the Atomic Schema Name is PROD_OFSAAATM, then the value for ATOMICALIASNAME must be entered as PRODOFSAAATM.

After you have completed either of the methods mentioned above, proceed with the following steps:

1. Restart the Infrastructure Server.
2. If you are using Apache Tomcat as the Web server, update the <Context> -> Resource tag details in the `Server.xml` file from the `$CATALINA_HOME/conf` directory. For Tomcat, both Config Schema (FICMASTER resource) and Atomic Schema (<INFODOM_NAME> resource) exist.
   If you are using WebSphere as Web server:

a. Log in to the WebSphere Administration Console, from the left side menu.

b. Navigate to Resources >JDBC >Data Sources. A list of data sources are 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 must be modified).

If you are using WebLogic as Web server:

a. Log in 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 are 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 must be modified).

3. Restart the OFSAAI services.

Modify the OFSAA Infrastructure Config Schema Password in a Wallet-Based Setup

To change the Config Schema Password in a Wallet-Based setup, follow these steps:

1. Shutdown all the OFSAAI Services and Web Servers.
2. Change the Config Schema User Password in the Database.
3. Log in as a UNIX user with the permission to modify the Oracle Wallet.
4. Execute the following command to configure Config Schema credentials.

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -modifyCredential -nologo CONFIG
<CONFIG_DATABASE_USERNAME> <CONFIG_DATABASE_NEWPASSWORD>
```

5. Enter the password to store the credentials in the Wallet when prompted.
6. Start all the OFSAAI Services excluding Web Servers.
7. If you use Apache Tomcat, WebSphere, or WebLogic as the Web Server, update the associated Wallet Directory with the new Config Schema User Password.
8. Start the associated Web Servers.

Modify the OFSAA Infrastructure Atomic Schema Password in a Wallet-Based Setup

To change the Atomic Schema Password in a Wallet-Based setup, follow these steps:

1. Shutdown all the OFSAAI Services and Web Servers.
2. Change the Atomic Schema User Password in the Database.
3. Log in as a UNIX user with the permission to modify the Oracle Wallet.
4. Execute the following command to configure the Atomic Schema credentials.

```
$ORACLE_HOME/bin/mkstore -wrl <WALLET_HOME> -modifyCredential -nologo
<ATOMICALIASNAME> <ATOMIC_DATABASE_USERNAME> <ATOMIC_DATABASE_NEWPASSWORD>
```

> **Note:**
>
> ATOMICALIASNAME value is a TNS alias for Atomic Schema and must not contain underscores. For example, if the Atomic Schema Name is PROD_OFSAAATM, then the value for ATOMICALIASNAME must be entered as PRODOFSAAATM.

5. Enter the password to store the credentials in the Wallet when prompted.
6. Start all the OFSAAI Services excluding Web Servers.
7. If you use Apache Tomcat, WebSphere, or WebLogic as the Web Server, update the associated Wallet directory with the new Atomic Schema User Password.
8. Start the associated Web Servers.

Configure Java Virtual Machine

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

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

Configure Internal Service (Document Upload/ Download)

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

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

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

1. Create the directories download, upload, TempDocument, and Temp in the local path of the Web application server and provide Read/Write permission.
   - To find the exact location, execute the following query in the CONFIG schema:
     `select localpath from web_server_info`
   - To create directories with Read/Write permission, execute the command:
     `mkdir -m 777 download upload TempDocument Temp`
2. Create DocStorage directory in the FTPSHARE location of APP tier and provide Read/ Write permission.
   - To find the exact location, execute the query in the CONFIG schema:
     `select ftpdrive from app_server_info`
   - To create a directory with Read/Write permission, execute the command:
     `mkdir -m 777 DocStorage`

By default, the parameter DOCUMENT_SERVICE_TYPE_EXTERNAL value is set to FALSE in the Configuration table in CONFIG schema and hence the application “ExeWebService” will not be used. It is recommended that the value be set to FALSE and use the Internal service for

document upload/ downloads. If you intend to continue using the External ExeWebService, set the value to TRUE.

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

Update the OFSAA 8.1.2.x Java 8 Instance to Java 11

This section explains the configurations required to update an existing OFSAA 8.1.2.x Java 8 instance to Java 11.

Topics:

Prerequisites

The following prerequisites must be matched before you can update the OFSAA 8.1.2.x Java 8 instance to Java 11:

- Java 11 must be installed on the OFSAA server and Web Application Server.
- OFS AAI Release 8.1.2.0.0. must be the minimum version installed.

Update the OFSAA 8.1.2.x Java 8 Instance to Java 11

To update the OFSAA 8.1.2.x Java 8 instance to Java 11, follow these steps:

1. Configure the OFSAA instance to Java 11. See Apply OFSAA Generic Configurations.
2. Configure Web Application Server to Java 11. See Configure the Web Application Server.

> **Note:**
>
> For a newly installed Web Application Server, see Configure OFSAA for the New Web Application Server Installation.

3. Generate the application EAR/WAR file and redeploy the application on your configured Web Application Server.

   For more information on generating and deploying EAR/WAR files, see Create and Deploy the EAR/WAR Files.
4. Restart the OFSAA services. See Start the Infrastructure Services.

Apply OFSAA Generic Configurations

This section consists of the following topics:

- Configure User '.profile' Settings
- Configure Java 11 (Java Virtual Machine)

Configure User '.profile' Settings

Perform the following configurations:

1. Log in to the OFSAA server as a non-root user.

   (Optional) <Enter a step example.>

2. Edit the user .profile. Update the value for the PATH variable from JRE 1.8 to JDK 11.

   For example,

   ```
   PATH=/usr/java/ jdk-11.0.11
   JAVA_BIN=/usr/java/ jdk-11.0.11/bin
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/java/jdk-11.0.11/lib/server
   ```

Configure the Web Application Server

This section describes the changes that are to be made in the Web Application Server. The following are the options to configure Web Application Server Configurations:

- Update the existing Web Application Server installation to Java 11
- Install a new instance of the Web Application Server with Java 11

This section consists of the following topics:

- Upgrade Java 8 to Java 11 for Oracle WebLogic Server 14.1.1.0
- Upgrade Java 8 to Java 11 for Apache Tomcat Server

Upgrade Java 8 to Java 11 for Oracle WebLogic Server 14.1.1.0

To upgrade Java 8 to Java 11 for WebLogic Server 14.1.1.0, follow these steps:

1. Navigate to the `<WLS_HOME>/Middleware/Oracle_Home/user_projects/domains/<domain>/bin` directory.

   Update `SUN_JAVA_HOME`, `DEFAULT_SUN_JAVA_HOME`, `JAVA_HOME` in the `setDomainEnv.sh` file to point to the new Java path.

   For example,

   ```
   SUN_JAVA_HOME="/usr/java/jdk-11.0.11"
   DEFAULT_SUN_JAVA_HOME="/usr/java/jdk-11.0.11"
   JAVA_HOME="/usr/java/jdk-11.0.11"
   ```

2. 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:

a. Install Oracle WebLogic Server 14.1.1.0 and later on Java 11.

b. Perform the configurations for the newly installed WebLogic server.

For more information, see Configure Resource Reference in WebLogic Application Server.

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

Upgrade Java 8 to Java 11 for Apache Tomcat Server

To upgrade Java 8 to Java 11 for Apache Tomcat Server, follow these steps:

1. Log in to the Apache Tomcat Server as a non-root user.
2. Update the value for JAVA_HOME from JRE 1.8 to JRE 1.11 in the user `.profile`. For Example,

   ```
   JAVA_HOME=/usr/java/ jdk-11.0.11
   ```

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:

   a. Install Apache Tomcat Server 9.0.x with Java 11.

   b. Perform the configurations for the newly installed Tomcat server.

   For more information, see Configure Resource Reference in Tomcat Application Server.

> **Note:**
>
> - Update the Connector Port in `/apache-tomcat-9.0.24/conf/server.xml` file to that of the existing Tomcat instance.
> - Note down the new deployment path to perform OFSAA Configurations.

Configure OFSAA for the New Web Application Server Installation

The configuration in this section is required only if you have freshly installed Oracle WebLogic 14.1.1.0 and later, or Apache Tomcat Server 9.0.x.

To configure, follow these steps:

1. Modify the following parameters in the Configuration Table present in the Config Schema with the new Domain Path if the webserver is WebLogic or with the new deployment path if the webserver is Tomcat:
   - DeFiHome
   - REV_IMG_PATH

- EMBEDDED_JSP_JS_PATH

2. Modify the following parameters in the AAI_SETUP_PROPS Table present in the Config Schema with the new Domain Path if the webserver is WebLogic or with the new deployment path if the webserver is Tomcat:
   - FIC_PHYSICAL_HOME_LOC
   - FIC_HOME
   - CSS_LOGGER_PATH
   - LOG_HOME_PATH

Migrate Excel Upload Functionality

This section provides detailed instructions to migrate excel upload functionality.

Topics:

Prerequisites

The following are the prerequisites for migration.

- The data model in ATOMIC schemas must be the same on the source and target setups.
- OFSAAI (platform) patch level version must be the same on the source and target setups.
- PL/SQL Developer to connect and query the database.
- WinSCP to connect and access the server file system.

Migrate Excel Upload

To migrate, follow these steps:

1. Open PL/SQL Developer and logon 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 the PL/SQL developer and logon to the target setup's configuration (CONFIG) schema by entering the appropriate username and password.
4. Insert the records from Step 1 into this table.
5. In the V_INFODOM column of the 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 the same Infodom value across all rows. If only a few mappings will work out of the target infodom, update the infodom value for selective records. Excel upload mappings will work only if the target infodom has the same data model entities as used in the mappings defined on the source setup.

6. Update the 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 log in a new session by entering the host name, port number, user name, and password to access the source setup.
8. Navigate to the directory referred to as FTPSHARE.
9. Copy the `excel-entity mapping xml` file(s) which are located in this directory according to their directory structure on to your desktop.

   For example: `/ftpshare/STAGE/ExcelUpload/$SOURCE_INFODOM_NAME/$EXCEL_FILE_NAME.xml`

> **Note:**
>
> The actual file name of the Excel Sheet is mentioned in the V_EXCEL_ NAME column of the EXCEL_MAPPING_MASTER table.

10. Copy the excel templates (.xls/ .xlsx) file(s) which are located in this directory according to their directory structure on to your desktop. For example:

    `/ftpshare/STAGE/ExcelUpload/TEMPLATE/*.xls` or `*.xlsx`

> **Note:**
>
> xls/.xlsx files must be copied to the path as per the local path given in your webserverinfo table of config schema. Ignore this step if files are not present at the location.

11. Log into 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 following 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 infodom in which you have uploaded the appropriate data model and the name must be the 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 following location in target setup.

    For example: `/ftpshare/STAGE/ExcelUpload/TEMPLATE/*.xls` or `*.xlsx`.

> **Note:**
>
> Ignore this step if files are not present at the location.

15

Remove OFSAA Infrastructure

Refer to the following topics, to remove the OFSAAI installation from a setup.

- Uninstall the OFSAA Infrastructure
- Uninstall the EAR Files, from WebSphere, WebLogic, and Tomcat application server
- Clean Up the Environment

Uninstall the OFSAA Infrastructure

To uninstall the OFSAA Infrastructure, follow these steps:

Before you start the uninstallation process, ensure that no open connections exist to the OFSAA Infrastructure Config and Atomic Schemas and Stop the Infrastructure Services.

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

   ```
   ./Uninstall.sh
   ```

3. Enter the password for the OFSAAI Configuration Schema when prompted:

Figure 15-1 OFSAAI Configuration Schema Prompt

Uninstall the EAR/WAR Files

This topic covers the instructions to uninstall the EAR/WAR files from the web application servers.

- Uninstall the EAR Files associated with a deployed application, from a WebSphere application server
- Uninstall the EAR Files in WebLogic associated with a deployed application, from a WebLogic server
- Uninstall the WAR Files in Tomcat associated with a deployed application, from a Tomcat server.

Uninstall the EAR Files in WebSphere

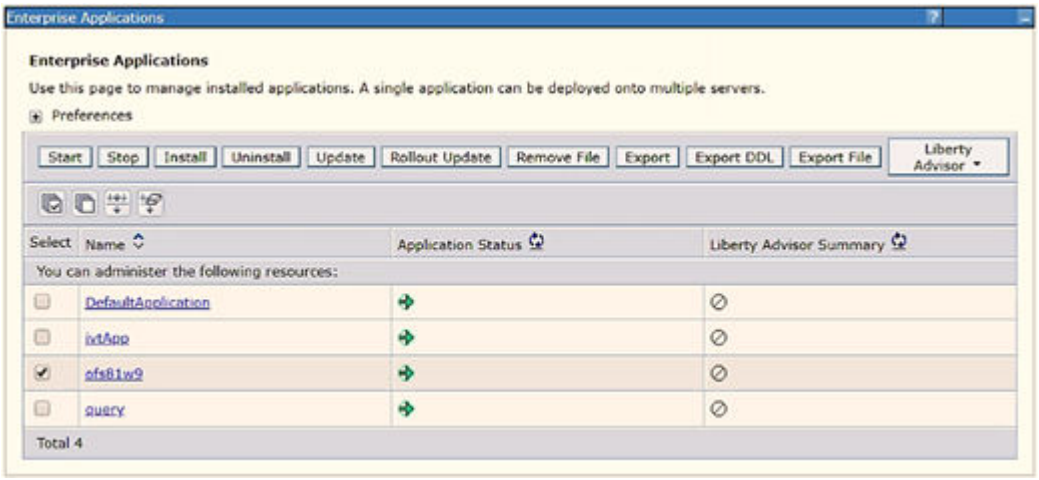
To uninstall a previously deployed application from a WebSphere application server, follow these steps:

1. Open the URL in a browser window: `http://<ipaddress>:<Administrative Console Port>/ibm/console` (https if SSL is enabled).

   The login window for the WebSphere Application Server Administration Console is displayed.

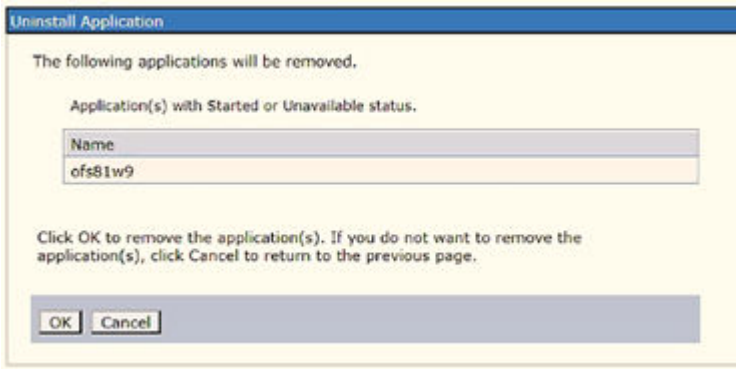
2. Log in with the user ID that has admin rights.
3. From the Navigation Tree, select **Applications**, select **Application Types**, and then select **WebSphere enterprise applications**. The Enterprise Applications window with all the previously deployed applications is displayed.

Figure 15-2 Enterprise Applications Window - Previously Deployed Applications



4. Select the check box adjacent to the application that you want to uninstall and click Stop.
5. Click **Uninstall** to display the Uninstall Application window.

Figure 15-3 Uninstall Application window



6. Click **OK** to confirm.

7. Click **Save** to save the master file configuration.

Uninstall the EAR Files in WebLogic

To uninstall a previously deployed application from the WebLogic application server, follow these steps:

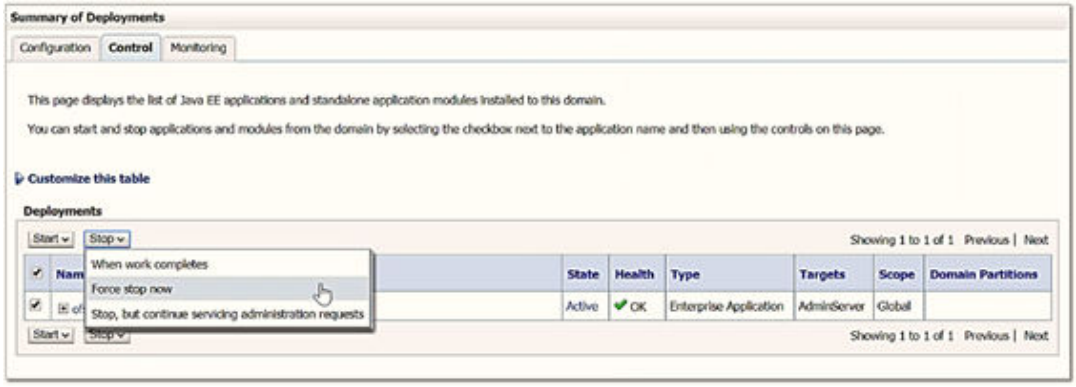
1. Open the URL in a browser window:

   ```
   http://<ipaddress>:<admin server port>/console (https if SSL is enabled).
   ```

   The login window of the *WebLogic Server Administration Console* is displayed.

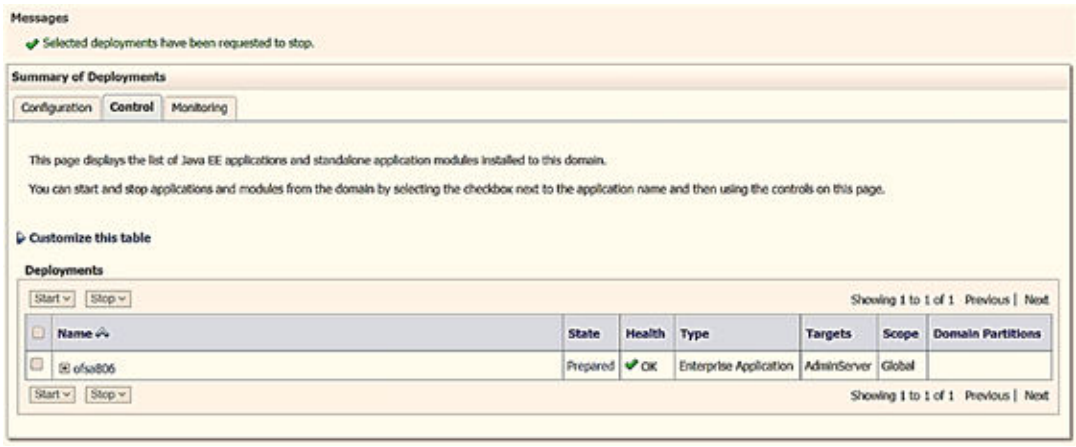
2. Log in with the WebLogic user credentials having administrator privileges.
3. From the Navigation Tree for Domain Structure, select **Deployments** to display the Summary of Deployments window.

Figure 15-4 Summary of Deployments Window



4. Select the check box adjacent to the application that you want to uninstall, click Stop, and then select Force Stop Now.
5. Click **Yes** in the confirmation dialog to stop the selected deployment.

Figure 15-5 Stop the Selected Deployment



6. Select the check box adjacent to the application and click Delete to delete the selected deployment.

7. Click **Yes** in the confirmation dialog to remove the selected deployment from the domain configuration.

Uninstall the WAR Files in Tomcat

To uninstall a previously deployed application from Tomcat server, follow these steps:

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

```
<!--
<Context path ="/pr2test" docBase="/home/perfuser/tomcat7.0.19/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:@<HOST_NAME>:1521:PERFTEST"
maxTotal="100"
maxIdle="30" maxWaitMillis="10000"/></Context>
-->
```

2. To restart the Tomcat service, follow these steps:
   a. Log in to the "UNIX server" through a terminal emulator.
   b. Navigate to the `$catalina_home/bin` directory.
   c. Stop the Tomcat services using the following command:

      `./shutdown.sh`

   d. Start the Tomcat services using the following command:

      `./startup.sh`

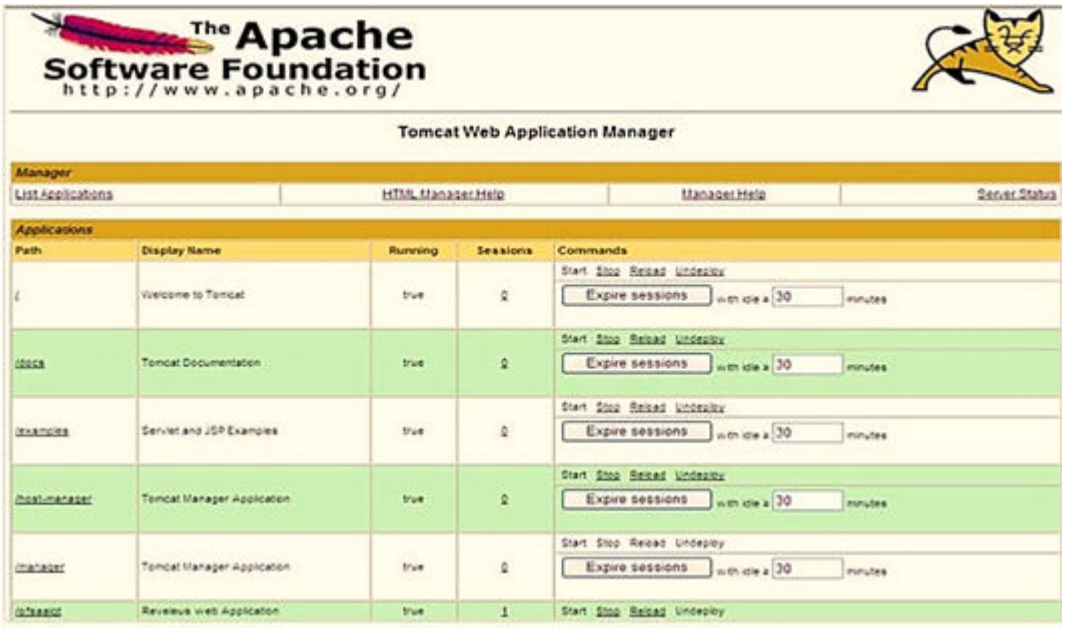
3. Open the URL in a browser window:

   `http://<IP address>:<Tomcat server port>` (https if SSL is enabled)

   The **Tomcat home** window is displayed.

4. Click Manager App to display the Connect to window.
5. Log in 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 15-6 Tomcat Web Application Manager Window



6. Click the Undeploy link corresponding to the deployed Infrastructure application. A confirmation message is displayed.

Clean Up the Environment

To clean up the Infrastructure environment, follow these steps:

1. Uninstallation does not remove the Infrastructure application from the Web application server. Manually remove the Infrastructure application.
2. Remove the entries in the `.profile` file.
3. Navigate to the ftpshare directory and delete the infodom files and directories under the file system staging area (ftp share) by executing the following command:

   ```
   $ rm -rf <INFODOM>
   ```

4. Drop config and atomic schemas from the database. Drop all the database objects from the Atomic Schemas manually.

16

Frequently Asked Questions (FAQs) and Error Dictionary

This section consists of resolution to the frequently asked questions and error codes noticed during OFSAAI installation.

- Frequently Asked Questions
- Error Dictionary

Frequently Asked Questions

You can refer to the Frequently Asked Questions which is 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.

Frequently Asked Questions

1. What are the different components that get installed during OFSAAI?
   The different components of OFSAAI are illustrated in Components of OFSAAI.
2. What are the different modes of OFSAAI installation?
   OFSAAI can be installed only 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 are installed on a 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 the JDK (Java Development Kit) required during the installation of OFSAA? Can it be uninstalled after the OFSAA installation?
   JDK is not required during the installation of OFSAA and only a run-time is needed. For details, see Hardware and Software Requirements.

   Only JRE (Java Runtime Environment) is required during the installation of OFSAA and cannot be uninstalled as the JRE is used by the OFSAA system to work.
5. How do I know what are the Operating system, web servers, and other software versions that OFSAA supports?
   See the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix.
6. 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_InstallConfig.xml
- privileges_config_user.sql
- privileges_atomic_user.sql

7. What should I do if I get `Execute Permission denied?` error message during installation?
   Check whether all the files provided for OFSAAI installation has execute permissions.

   To give execute permissions, navigate to the directory path where the Installation files are extracted and execute the following command:

   ```
   chmod -R 755 OFS_AAAI_PACK
   ```

8. What should I do if I get `No Java virtual machine could be found from your PATH environment variable.` error message?
   Install a VM before running this program, then
   - Check whether the "java path" is set in the PATH variable. See the Hardware and Software Requirements section in this document.
   - 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 the `setup.sh` file does not contain control line feed characters (^M).

9. What should I do if I get "`Oracle Driver Files Not Found, Please Choose the Right Path To Continue`" error message during installation?
   Check whether the provided path for Oracle Driver files is correct and whether the user has permission to access the files.

10. The installation of OFSAAI was completed successfully! What next?
    Post the successful completion of the OFSAAI installation, one has to perform the Post Installation steps. See Post-installation.

11. What is to be done when OFSAAI Installation is unsuccessful?
    OFSAAI installer generates the log file `OFSAAInfrastructure_Install.log` in the Infrastructure Installation Directory. There are also other log files created in the directories:
    - `< directory path where the Installation files are extracted >/OFS_AAAI_PACK/logs`
    - `< directory path where the Installation files are extracted >/OFS_AAAI_PACK/OFS_AAI/logs`

    If the logs of any of these reported Warnings, Non Fatal Errors, Fatal Errors, or Exceptions, they must be brought to the notice of the OFSAAI My Oracle Support. It is recommended not to proceed until the reported problems are adequately addressed.

12. How do I completely uninstall OFSAAI?
    OFSAAI can be completely uninstalled by performing the steps provided in the Uninstall OFSAA Infrastructure section in this guide.

13. Can OFSAAI config and atomic schemas be on different databases?

OFSAAI requires both config and atomic schema to be present on the same database instance.

14. How do I 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.
    a. Log into the database as sys and connect as sysdba user.
    b. Execute the `privileges_atomic_user.sql` file available under the `$FIC_HOME` directory.
    c. Enter the database schema for which you want to grant privileges.
15. When should I run the MLS utility?
    See the Multiple Language Support (MLS) Utility section in the OFS Analytical Applications Infrastructure Administration Guide.
16. 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. Log in 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 15000`
    d. After saving the changes, log in as UNIX user with which OFSAAI is getting installed and execute the command:
       `ulimit -n`
    e. The command must return the value 15000.
17. 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 My Oracle Support.

    See Verifying System Environment section for additional information.
18. How do I know if the installation is completed successfully?
    The OFSAA Infrastructure installation performs a post-install health check automatically on the successful installation of the product.
19. What should I do if there are any exceptions or errors in installation and how to proceed?
    a. See the Verify the Log File Information section for log file information.
    b. Backup the installation logs.
    c. Share the backup logs with My Oracle Support.
20. 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

21. What should I do if the installation process is abruptly terminated or aborted?
If the installation process is abruptly terminated, then the installation is incomplete. To recover from this, follow these steps:
    a. Drop the DB objects in the config and atomic schemas 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 and FTP Share directories created by the OFSAAI installer.
    d. Perform the OFSAAI installation again. See Pre-installation
22. Does OFSAA support any other web server types, other than the ones stated in the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix and Installation Guide?
No, all the supported software and versions are stated in the Oracle Financial Services Analytical Applications 8.1.2.0.0 Technology Matrix
23. What should I do if the database connection from the 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 must be configured on all the machines or VMs where the OFSAAI components are installed.

    If the issue is not resolved even with the preceding settings, check the MTU(Maximum Transmission Unit) settings on the Linux box. For details on MTU settings and updating them, contact your system administrator.
24. What should I do when I get syntax errors/file not found error messages while invoking `setup.sh` file from my install archive?
This can mostly happen due to the following reasons:
    - When the installer is not extracted correctly or corrupted during the unzip utility process.
    - setup.sh file which resides within the install archive is not transferred in ASCII or text mode, which can corrupt 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. Log in to the server where the installer is copied.

b. Navigate to the directory `< directory path where the Installation files are extracted >/OFS_AAAI_PACK/bin`.

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!`

25. 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`"?

- Ensure the `JAVA_BIN` environment variable path is set on the "`UNIX user`" terminal from where the `startofsaai.sh` file is invoked.
- Ensure that the `.profile` file, where the environment/ path settings are made, is executed successfully.

26. What should I do if the OFSAAI Application Server does not proceed even after providing the system password?
Ensure that, the System Password provided when prompted during installation is correct. Also, check whether the connection to the "`configuration schema`" can be established through sqlplus.

27. 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 the list of languages from Server. Please contact the system administrator`". What should one do?
Ensure OFSAAI servers are started and are running successfully. For details on startup parameter options, see Start the Infrastructure Services section.

    For more details on the issue, refer to the logs under `$FIC_HOME /logs` directory.

28. 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 never be revoked as the application makes use of these grants all the time.

29. Can we have a 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 the distribution of services.

30. Why do we need FTPSHARE on all the layers? Can we have ftpshare on another server other than the server 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 directories for each Information Domain, with each Information Domain directories holding Erwin, log, and scripts directory. The transfer of data among the Web, Application, and Database servers in Infrastructure takes place through FTP/SFTP.

    You must 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, you can have FTPSHARE as a common local storage mount point which can be mounted where OFSAAI is installed.

31. Is it mandatory to provide the FTP/SFTP password?
Yes, OFSAAI needs credentials of the user who has complete permissions on the FTPSHARE directory, and the user must be able to independently log in to the UNIX server.

    For more information, see the Configure OFSAAI_InstallConfig.xml File section.

32. 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 (multi tier installation).

    In the case of a single-tier installation, 770 permissions can be provided if the UNIX users of OFSAAI and web servers belong to the same UNIX group.

    Additionally, any new file that is created in the FTPSHARE directory of any installation layer must be granted specific/explicit permission.

33. How to modify the port number currently being used by the Infrastructure application?
Port Changer utility can be used to have the Port number modified, which is currently being used by the Infrastructure application. For more information, refer to the Change IP/ Hostname, Ports, Deployed Paths of the OFSAA Instance section in the OFS Analytical Applications Infrastructure Administration User Guide.

34. Are there any in-built system administration users within OFSAAI Application?
The two in-built system administration users are provided to configure and setup OFSAAI.

    - SYSADMN
    - SYSAUTH

35. Does OFSAAI Application support both FTP and SFTP?
OFSAAI supports both FTP and SFTP configuration.

36. 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.

37. 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.

38. 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 must exist.

39. What should I do if I get the following message during the startup of the backend engine message server, "`ConnectToDatabase: FatalError, could not connect to the DB server`"?

    - Verify whether a connection to the Configuration Schema can be established through SQL*PLUS.
    - Verify the Configuration Schema password is modified post-installation.
    - Ensure Oracle Database Alias Name created for Oracle Instance and Oracle Service Name are the same.

40. What should I do if I get the following message during the startup of the backend engine message server, "`Fatal Error, failed to get the user ID from LibSmsConnect`"?
Ensure the `Reveleus.SEC` file exists under the `$FIC_HOME/conf` directory where the Database components are installed.
41. Does OFSAAI Application support LDAP authentication?
OFSAAI supports LDAP configuration and authentication.
42. Does OFSAAI support multiple languages?
Yes, OFSAAI supports multiple languages.
43. Does OFSAAI provide any data back-up features?
OFSAAI does not have a built-in backup facility. External Storage Infrastructure is recommended for back-up.
44. What kind of security features does the OFSAAI provide?
See the Security Guide for more information.
45. Does OFSAAI have the ability to enforce periodic password change?
OFSAAI provides configurable parameters to define the number of days after which the user password must expire and then the user is forced to change the password after the expiration period.
46. What is the password policy followed in OFSAAI?
OFSAAI enforces a minimum password length with a combination of Upper and Lower case characters and alphanumeric strings.
47. Which version of Erwin Data Modeller does OFSAAI support?
See the Hardware and Software Requirements section for more information.
48. 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 Data Model Management -->Data Model Maintenance --> 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`.

    For more details, see the Model Upload Utility section of the OFS Analytical Applications Infrastructure User Guide.
49. How do I apply the incremental change to the existing model when the Business Data model changes?
The modified data model can be uploaded into the system and OFSAAI can compare the changes within the data model concerning the one already present in the system and enables propagation of incremental changes in a consistent manner.
50. What are the different types of uploading a business data Model?
OFSAAI supports uploading of the business data model from client desktop and also by picking up the data model from the server location.
51. 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 will require updating in those files. For more information, see Modify OFSAAInfrastructure Config Schema Password.
52. 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 will require updating those files.

To change the Atomic Schema password, follow the steps:

a. Log in to OFSAA.

b. Navigate to System Configuration > Database Details window. Select the appropriate connection, provide the modified password, and save.

c. Based on the Web Server installed, follow the steps:

- If you are using Apache as Web server:
  - Update the <Context> -> Resource tag details in the `server.xml` file from the `$CATALINA_HOME/conf` directory. (In case of Tomcat only Atomic <Resource> will exist).
- If you are using WebSphere as Web server:
  - Log in to the WebSphere Administration Console from the left side menu.
  - Navigate to Resources >JDBC > Data Sources. A list of data sources are populated on the right side.
  - Select the appropriate Data Source and edit the connection details. (In this case, both Config and Atomic data sources must be modified).
- If you are using WebLogic as Web server:
  - Log in to the WebLogic Administration Console from the left side menu.
  - Under Domain Structure list box, expand the appropriate Domain and navigate to Services > JDBC >Data Sources. A list of data sources are populated on the right side.
  - Select the appropriate Data Source and edit the connection details. (In this case, both Config and Atomic data sources must be modified).

d. Restart the OFSAAI services

> **Note:**
>
> If the modified passwords are not updated, OFSAAI logs display the message ORA-28000: the account is locked.

53. Does the upload of the 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 My Oracle Support for more details.

54. Why do the Business Metadata Management screens (Business Processors screen) in User Interface take more time to load than other screens?
The Log file in `DynamicServices.xml` which resides in the `$FIC_HOME/conf` directory is continuously being updated/refreshed to cache metadata. This can be observed when you are starting startofsaai.sh and if any of the log files (For example, SMSService.log) in DynamicServices.xml is being continuously refreshed for a longer time.

    By default, the Metadata Logfile 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 1001st entry is overwritten by deleting the first entry. This results in the application window 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 following query in the 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 preceding query returns a list of codes with their respective metadata count. You can refer to 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 the total measure reported in the log is 1022, increase the limit to 2000 (approximately).

d. Restart Reveleus/OFSAAI servers (Web and APP) and check the issue.

55. What should I do if I get OutOfMemoryError while deploying the EAR file in the WebSphere application server?
The Java memory must be increased in the `ejbdeploy.sh` file which is present under `<WebSphere Install directory>/AppServer/deploytool/itp`. For example,

```
$JAVA_CMD \
-Xbootclasspath/a:$ejbd_bootpath \ Xms256m -Xmx1024m \
```

56. What is the default memory setting configured by the installer?
During OFSAAI installation, the X_ARGS_APP parameter in the `.profile` file is set as given:

```
X_ARGS_APP="-Xms200m -Xmx8g -XX:+UseAdaptiveSizePolicy -
XX:MaxPermSize=1024M -XX:+UseParallelOldGC -XX:+DisableExplicitGC
```

During the application installation, if 10 times the data model size (data model size*10) is greater than the default Xmx value of 8g (8GB), the installer automatically updates the Xmx value to 10 times the data model size.

57. What configurations should I ensure if my data model size is greater than 2GB?
Ensure the Xmx value in the X_ARGS_APP parameter in the `.profile` file is set as 10 times the data model size.

For example, if it is 2GB, set it as:

```
X_ARGS_APP="-Xms200m -Xmx20g -XX:+UseAdaptiveSizePolicy -
XX:MaxPermSize=1024M -XX:+UseParallelOldGC -XX:+DisableExplicitGC
```

Then execute the `.profile` file.

58. 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 is changed. This can occur in hierarchy maintenance, where you have moved a member to another hierarchy branch, and that member is explicitly selected in the Filter and is now a child of a node that is already selected in the Filter.

59. Can I install an Application Pack on an existing Atomic schema/ Information Domain created manually?

No, you cannot install an Application Pack on existing Atomic schema/Information Domain created manually. Application Packs can be installed only on Atomic Schemas/Information Domain created using schema creator utility and/ or the Application Pack installer.

60. 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 directory "STAGE" under the path mentioned as "Local Path" in the web server details window. This directory must be created under the local path on every node, in case of web application server clustering.

61. 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.

62. 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).
- Update the same details in the table Aai_Dyn_Svcs_Params of Config Schema for the parameter CACHE_ON_STARTUP. Set the value as 0 and commit the change.
- Restart the OFSAAI Services (APP and WEB). For more information, refer to the Start the Infrastructure Services section.

> **Note:**
>
> This setting helps cache the Infodom metadata only for the infodoms that are accessed after the 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>
```

63. 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 version of the browser and JRE Plugin are as mentioned in the Hardware and Software Requirements section of this manual. If not, use the qualified versions as mentioned.

64. Can multiple OFSAA Infrastructure instances share the same Config Schema?
No, only one OFSAA environment can be installed using one Config Schema.

65. Can Atomic Schema be shared?
Yes, it can be shared between two OFSAA instances.

    While setting a firewall, which ports must 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 the same as the Web server port must be open. Also, the web application port must be open.

66. Can I install an already installed application in a different infodom?
No, it is not possible to install the same application in two different infodoms.

67. How can I configure the OFSAA application for High Availability?
OFSAA can have active-passive high availability. For more details, refer Configuration for High Availability- Best Practices Guide.

68. During OFSAA installation should I provide a 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 must enter the Web Server IP Address/ Hostname and Port details during OFSAA installation. Here the Servlet port must be the same as the Web Server port.

    If Web Server is not configured, the Web application server's IP Address/ Hostname and Port are required during the installation process. Here the Servlet port must be the same as the Web application server port.

69. Is "ReveleusAdminConsoleAgent" applicable for OFSAAI 8.1.2.0.0 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 and agentshutdown.sh.

70. 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 like "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 these 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. Start the Infrastructure Server in foreground directly on the server or through XWindows software using the command: ./startofsaai.sh

d. Enter System Password.

e. Enter the new Config schema password. The service starts and initializes if it can successfully connect to the DB and generates the Reveleus.SEC file.

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

71. What is the mechanism of log file sizing, changing the log file path, and creating backups of the log files?
OFSAAI Log files created under `$FIC_APP_HOME/common/FICServer/logs` and `<OFSAAI_DEPLOYED_AREA>/<CONTEXT.war>/logs` is configurable in `RevLog4jConfig.xml`.

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

To configure the Logs file size on the OFSAA Application server, follow these steps:

a. Navigate to `$FIC_HOME/conf` where OFSAA is installed.

b. Edit the following parameters in the RevLog4jConfig.xml file:

- param name="fileName" : Enter the path where the Logs are to be generated.
- param name="size" : Provide the required file size.
- param name="max" : Provide the required number of backup files to be created.

Example:

```
<RollingFile name="REVSERVERAPPENDER"
fileName="<Path_exists>/logs/RevAppserver.log"
 filePattern="<Path_exists>/logs/RevAppserver-%i.log" >
 <PatternLayout>
 <Pattern> [%d{dd-MM-yy HH:mm:ss,SSS zzz aa}{GMT}] [%-
5level] [APP] [REVELEUS] %m%n</Pattern>
 </PatternLayout>
 <Policies>
 <SizeBasedTriggeringPolicy size="5000 KB" />
 </Policies>
 <DefaultRolloverStrategy max="5"> <!-- number of backup
files -->
 </DefaultRolloverStrategy>
 </RollingFile>
```

c. Navigate to `$FIC_HOME/ficweb/webroot/conf` and configure the deployed area logs. Edit the following parameters in the `RevLog4jConfig.xml` file:

- param name="file": Do not change this value.
- param name="MaxFileSize" : Provide the required file size.

- param name="MaxBackupIndex" : Provide the required number of backup files to be created.

Example:

```
<RollingFile name="REVSERVERAPPENDER"
fileName="${sys:LOG_HOME}/logs/RevAppserver.log"
 filePattern="${sys:LOG_HOME}/logs/RevAppserver-%i.log" >
 <PatternLayout>
 <Pattern> [%d{dd-MM-yy HH:mm:ss,SSS zzz aa}{GMT}] [%-
5level] [WEB] [REVELEUS] %m%n</Pattern>
 </PatternLayout>
 <Policies>
 <SizeBasedTriggeringPolicy size="5000 KB" />
 </Policies>
 <DefaultRolloverStrategy max="5"> <!-- number of backup
files -->
 </DefaultRolloverStrategy>
 </RollingFile>
```

To configure the deployed area log file path, modify the value in the LOG_HOME_PATH parameter in the aai_setup_props table.

72. Can I point the environment with HTTP enabled to HTTPS after installation and vice versa?
Follow these steps:

a. Create SSL related certificates and import to respective servers.

b. Enable SSL on a desired Port (example 9443) on your existing and already deployed web application servers.

c. Replace the protocol as https and new ssl port (FIC_SERVLET_PORT) configured and in all the URLs specified on the following files:

```
- $FIC_HOME/ficapp/common/FICServer/conf/FICWeb.cfg
- $FIC_HOME/ficapp/icc/conf/WSMREService.properties
- $FIC_HOME/ficdb/conf/MDBPublishExecution.properties
- $FIC_HOME/ficdb/conf/ObjAppMap.properties
- $FIC_HOME/utility/Migration/conf/WSMigration.properties
- $FIC_HOME/utility/WSExecution/conf/WSExecution.properties
```

d. Replace XML attribute/Node values as specified on the following files:

```
- $FIC_HOME/ficweb/webroot/WEB-INF/web.xml
- FIC_WEBSERVER_PORT=9443
- FIC_WEBPROTOCOL=https
- $FIC_HOME/conf/LookUpServices.xml and $FIC_
HOME/ficweb/webroot/conf/LookUpServices.xml
- PORT="9443" PROTOCOL="https:"
```

e. Log in to Config Schema and execute the following SQL command to replace protocol and SSL port.

- `SQL> update configuration cn set cn.paramvalue='9443' where cn.paramname='SERVLET_ENGINE_PORT';`

- `SQL> update configuration cn set cn.paramvalue=replace(cn.paramvalue,'http:','https:') where cn.paramname='FormsManagerCacheReload';`
- `SQL> update web_server_info ws set ws.servletport='9443',ws.servletprotocol='https';`

f. Create EAR/WAR file and Re-Deploy.

73. What should I do if my HIVE connection fails with the following exception: java.sql.SQLException: [Cloudera][HiveJDBCDriver](500164) Error initialized or created transport for authentication:

[Cloudera][HiveJDBCDriver](500168) Unable to connect to server: GSS initiate failed.

com.ibm.security.krb5.KrbException, status code: 37

message: PROCESS_TGS at com.ibm.security.krb5.KrbTgsRep.<init>(KrbTgsRep.java:20)

This happens if there is clock skew between the client and the KDC server. To resolve this, there are two solutions:

Solution 1:

Synchronize the clocks between the servers. For more information, refer http://docs.oracle.com/cd/E19253-01/816-4557/setup-192/index.html

Solution 2:

- Set clock skew parameter on the server side (KDC) krb5.conf file and replace the same file in the HIVE_LIBRARY_PATH directory. Parameter value must be decided based on the time difference between the two machines.
- Get the epoch time on the two servers by firing “date +%s” on the command line.
- Clock skew param value must be chosen as a value sufficiently larger than the difference of the preceding two calculated values.
- Set “clock skew = <value>” in the /etc/krb5.conf on the KDC server.
- Restart Kerberos services.

74. What should I do if my schema creator log has the following exception:

```
Failed to detect a valid hadoop home directory java.io.IOException:
HADOOP_HOME or hadoop.home.dir are not set. at
org.apache.hadoop.util.Shell.checkHadoopHome(Shell.java:302)
at org.apache.hadoop.util.Shell.<clinit>(Shell.java:327) at
org.apache.hadoop.util.StringUtils.<clinit>(StringUtils.java:79) at
org.apache.hadoop.security.Groups.parseStaticMapping(Groups.java:130)
at org.apache.hadoop.security.Groups.<init>(Groups.java:94) at
org.apache.hadoop.security.Groups.<init>(Groups.java:74) at
org.apache.hadoop.security.Groups.getUserToGroupsMappingService(Groups.
java:30 3) at
org.apache.hadoop.security.UserGroupInformation.initialize(UserGroupInf
ormation.ja va:283) at
org.apache.hadoop.security.UserGroupInformation.setConfiguration(UserGr
oupInfor mation.java:311) at HdfsDbUtil.connect(HdfsDbUtil.java:162) at
SchemaParserUtil.validateHiveConnection(SchemaParserUtil.java:1359) at
SchemaParserUtil.checkAllPreChecks(SchemaParserUtil.java:1011) at
Main.execute(Main.java:317) at Main.main(Main.java:145) This occurs
when HADOOP_HOME environment variable is not set.
```

You can ignore this exception since we do not mandate to install HIVE where OFSAA is installed.

75. 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
    ```

76. 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.

77. 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 must import the certificate into the JDK/JVM used by Reveleus server in ficapp layer.

78. How to relocate FTPSHARE directory, change IP HOST name, and deployed area in OFSAA?
You can run the `PortC.jar` utility. For more details, refer Change IP/ Hostname, Ports, Deployed Paths of the OFSAA Instance section in the OFS Analytical Applications Infrastructure Administration Guide.

79. How do we identify the list of ports that are used by/configured in an OFSAA environment?
    - Navigate to `$FIC_HOME` directory on Target.
    - Refer to the `PortsDef.log` file.
80. What should I do if I get the following error message, "Error while fetching open cursor value Status : FAIL"?
    This error occurs while executing `envCheck.sh` because the user does not have access to the V$parameter. This error does not occur due to sysdba or non sysdba privileges provided they have access/grants to the V$parameter.
81. What should I do when an entity containing many attributes (>100 columns) is selected as a Source entity and the Data Mapping (T2T definition) save operation takes longer than expected with the hourglass in the UI continuously rotating?
    a. Locate the webserver deployed area webroot/conf/excludeURLList.cfg file.
    b. Modify the following entries:
    ```
    [SQLIA]./dataIntegrator/ to [ALL]./dataIntegrator/

    [SQLIA]./ETLExtractionServlet to

    [ALL]./ETLExtractionServlet
    ```
    c. Save the changes and restart the webserver.
    d. Resave the definition.
82. What should I do if I get the following error message when I try to start the OLAP server:

    ```
    ./olapdataserver: error while loading shared libraries: libessapinu.so:
    cannot open shared object file: No such file or directory FATAL ERROR
    :- OLAP DATA SERVER start up failed.
    ```

    This error occurs when the OLAP component is not configured and the OLAP feature in OFSAA is not used. However, this error can be ignored.
83. What should I do if I get the error "FATAL ERROR-Problem with OFSAA Service" during the OFS_AAAI_PACK installation?
    Increase the sleep counter (default value is 80) to a higher value in the following section of the `OFS_AAAI_PACK/OFSAAIUpdate.sh` file:

    ```
    if [ $count -eq 0 ]multitier; then sleep 80;
    count=` grep -i "FICServer Initialization Complete"
    $FIC_HOME/ficapp/common/FICServer/bin/nohup.out|wc -l ` fi
    if [[ $count -gt 0 ]] ; then echo OFSAA Service - OK
    else
    fi
    echo FATAL ERROR-Problem with OFSAA Service exit 1
    ```

Application Pack 8.1.2.0.0 FAQs

1. **What is an Application pack?**
   An Application Pack is a suite of products. For more information, refer to Introduction.
2. **Can I get a standalone installer for OFSAAI 8.1?**
   No. AAI is part of every application pack and installs automatically.
3. **Where can I download OFSAA 8.1.2.0.0 Application Pack?**

You can download the OFSAAI 8.1.2.0.0 Application Pack from Oracle Software Delivery Cloud (OSDC).

4. **What are the minimum system and software requirements for the OFSAA 8.1 Application Pack?**
   Refer to Hardware and Software Requirements for more information.
5. **Is my environment compatible with OFSAA 8.1.2.0.0 Application Pack?**
   Environment Check utility performs the task. It is part of the install and can also be run separately.
6. **Does the OFSAA 8.1.2.0.0 Application Pack support all Operating systems?**
   Refer to the Hardware and Software Requirements section.
7. **How can I install the OFSAA 8.1.2.0.0 Application Pack?**
   Refer to Oracle Financial Services Advanced Analytical Infrastructure Installation And Configuration Guide.
8. **Does this installation require any Third-party Softwares?**
   For details on the third-party software tools used, see the OFSAA Licensing Information User Manual Release 8.1.2.0.0 available in the OHC Documentation Library.
9. **What languages are supported during the OFSAA 8.1.2.0.0 Application Pack installation?**
   US English is the language supported.
10. **What mode of installations OFSAA Application Pack supports? [that is., Silent, GUI]**
    OFSAA Application Packs support only Silent Mode.
11. **Does OFSAA 8.1.2.0.0 Application Pack support multi-tier Installations?**
    OFSAA 8.1.2.0.0 supports only a single-tier installation. For more information refer to the OFS AAI FAQssection.
12. **Does this Application Pack validate all prerequisites required for this installation like Memory, Disk Space, and so on?**
    Yes. The prerequisite checks are done by the respective application pack installer.
13. **What happens if it aborts during the installation of any application/products within an Application pack?**
    You must restore the system and retrigger the installation
14. **Does this Application pack 'Roll Back' if any application installation fails due to errors?**
    The rollback of installation is not supported.
15. **Does the Application pack install all applications bundled?**
    Only Application pack system which are enabled are installed. In order to enable other licensed Applications, you need to reinstall by making the flag as Y. See the Table 15: OFS_<APP PACK>.xml File Parameters, APP_ID/ ENABLE attribute for information on how to enable. However, in case of reinstallation to enable the other Applications, execution of the schema creation utility must be skipped if it does not include any additional sandboxes to be created.
16. **Can I re-install any of the Application Packs?**
    You can retrigger in case of failure.
17. **Does this Application pack allow enabling/disabling any of the applications installed?**
    Yes, you can enable but you cannot disable once the product is enabled in an environment.
18. **I have installed one application in an Application pack, can I install any of the new applications within the Application pack later?**

Yes, the installation of additional applications is done by setting the flag as Y. See the Table 15: OFS_<APP PACK>.xml File Parameters, APP_ID/ ENABLE attribute for information on how to enable. However, in case of a reinstallation, to enable the other Applications, skip the execution of the schema creation utility if it does not include any additional sandboxes to be created.

19. **How many OFSAA Infrastructures can be installed in a single server?**
    There are 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 must be taken when running multiple OFSAAI installations on a single server. Adequate memory is required for each installation as several OFSAAI processes (model upload, DEFQ services, etc) take significant amounts of memory. So it depends on your server's memory.
20. **Is it possible to install OFSAA 8.1.2.0.0 Application pack on an existing 'Infodom' where another OFSAA 8.1.2.0.0 application is installed?**
    Yes. However, the Behavioral Detection Application Pack and Compliance Regulatory Reporting Application pack are the exceptions. They must be installed in a different Infodom.
21. **Can I select an Infodom for the Application pack during installation?**
    Yes. You can select or change the required infodom.
22. **Can I install all Application Packs in a 'Single Infodom'?**
    Yes. But, the Behavioral Detection Application Pack and Compliance Regulatory Reporting Application Pack are the exceptions. They must be installed in a different Infodom.
23. **Is it possible to install applications on different Infodom within the Application pack? (For example, I want to install LRM and MR in two infodoms)**
    Applications within the application pack have to be installed in the same information domain in the same environment.
24. **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.
25. **Is the 'Data Model' bundled specifically to an Application pack or an individual application?**
    A merged data model for all applications within the application pack is bundled and uploaded.
26. **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 application pack that bundles Enterprise Modeling. For more information, see Enable Financial Services Enterprise Modeling on Another Application Pack.
27. **Does the Application pack create a sandbox automatically for the required applications?**
    Yes, Sandbox creation is part of the application install process.
28. **Are upgrade Kits available for individual applications or the complete Application Pack?**
    Maintenance Level (ML) Release / Minor Release upgrades are available across all applications.
29. **Can I upgrade AAI only?**
    Yes, you can upgrade AAI alone.
30. **Can I upgrade one application within the Application Pack? (For example, I want to upgrade LRM in the Treasury Application pack, but not MR.)**

No, an upgrade is applied to all applications in the application pack.

31. **Is it possible to uninstall any Application from the Application pack?**
No, it is not possible to uninstall any Application from the Application Pack.

32. **Can I uninstall the entire Application Pack?**
No, you cannot uninstall the Application Pack.

33. **Is it possible to uninstall only the application and retain AAI in the installed environment?**
No, you cannot uninstall only the application and retain AAI in the installed environment.

34. **Does Application Pack contain all Language Packs supported?**
Language Packs must be installed on the application packs.

35. **Can I install an Application Pack over another Application Pack (that is the same infodom or different infodom)?**
Yes, you can install an Application Pack over another Application Pack in the same information domain or different information domain. But Behavioral Detection Application Pack and Compliance Regulatory Reporting Application Pack, Asset Liability Management Application Pack, and Profitability Application Pack are the exceptions. They must be installed in a different Infodom.

36. **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 can be the machine is configured for zonal partitioning. Ensure all the known IP Addresses of the machine are present in the /etc/hosts file.

37. **What are the Java versions supported in OFSAAAI Application Pack version 8.1.2.0.0?**
See the Hardware and Software Requirements section.

38. **Is OFSAAAI Application Pack version 8.1.2.0.0 supported on Java 9 and Java 11?**
For information about supported Java versions, see the Hardware and Software Requirements section.

39. **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 must 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, this can be 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, the execution of binaries will not happen in the directory and the installation fails. Re-run the installer after the configuration is changed. For detailed information, see the support note at https://support.oracle.com/epmos/faces/DocumentDisplay?id=2340045.1.

Error Dictionary

The contents of this section are 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.

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 refer to the Error Dictionary to find the exact cause and resolution to rectify the error.

This section includes the following topics:

Access the 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 these instructions to quickly find the error resolution:

1. With the Installation pdf open, press **Ctrl+F** or select **Edit > Find**. The Find dialog is displayed as indicated.
2. Enter the error code that is displayed on the screen during Infrastructure installation.
3. Press **Enter**. The search results are displayed and highlighted.
4. 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 the resolution, you can contact support.oracle.com along with log files and appropriate screenshots.

Error Code Dictionary

Table 16-1 Error Code Dictionary

Error Code	Cause	Resolution
OFSAAI-1001	UNIX shell is not "korn" shell.	Change the shell type to "korn". Use the chsh UNIX command to change the SHELL type. Shell type can also be changed by specifying the shell path for the UNIX user in the /etc/passwd file. Note: The chsh command is not available in Solaris OS.
OFSAAI-1002	No proper arguments are available	Provide proper arguments. Invoke the Setup.sh file using `SILENT`. Example: `./Setup.sh SILENT`
OFSAAI-1004	File `.profile` is not present in $HOME.	Create the `.profile` file in the `$HOME` directory, that is, in the home directory of the user.
OFSAAI-1005	`OFSAAInfrastructure.bin` file is not present in the current directory.	Copy the OFSAAInfrastructure.bin file into the installation kit directory.
OFSAAI-1006	`CustReg.DAT` file is not present in the current directory.	Copy the `CustReg.DAT` file into the installation kit directory.
OFSAAI-1007	`OFSAAI_InstallConfig.xml` file is not present in the current directory.	Copy the `OFSAAI_InstallConfig.xml` file into the installation kit directory.
OFSAAI-1008	`validateXMLInputs.jar` file is not present in the current directory.	Copy the `validateXMLInputs.jar` file into the installation kit directory.
OFSAAI-1009	`log4j.xml` file is not present in the current directory.	Copy the `log4j.xml` file into the installation kit directory.
OFSAAI-1010	An unknown error occurred.	Make sure to provide a proper argument (SILENT) to the Setup.sh file.

Table 16-1 (Cont.) Error Code Dictionary

Error Code	Cause	Resolution
OFSAAI-1011	XML validation failed.	Check the `InfrastructurePreValidations.Log` file for more details.
OFSAAI-1012	Property file with locale name does not exist.	Copy the `MyResources_en_US.properties` file to the setup kit directory and keep en_US in the LOCALE tag of the `OFSAAI_InstallConfig.xml` file.
OFSAAI-1013	`OFSAAI_InstallConfig.xml/ OFSAAI_PostInstallConfig.xml` file not found.	Copy the `OFSAAI_InstallConfig.xml/ OFSAAI_PostInstallConfig.xml` file to the setup kit directory.
OFSAAI-1014	XML node value is blank.	Make sure all node values except SMTPSERVER, PROXYHOST, PROXYPORT, PROXYUSERNAME, PROXYPASSWORD, NONPROXYHOST, or RAC_URL are not blank.
OFSAAI-1015	XML is not well-formed.	Execute the command dos2unix `OFSAAI_InstallConfig.xml` file to convert a plain text file from DOS/MAC format to UNIX format. OR Ensure that the `OFSAAI_InstallConfig.xml` file is valid. Try to open the file through a web browser for a quick way to check validity. If it is not getting opened, create a new `OFSAAI_InstallConfig.xml` file using the `XML_Utility.jar` file.
OFSAAI-1016	The user installation directory contains blank spaces.	Provide an installation path that does not contain spaces. Check the tag `USER_INSTALL_DIR` in the `OFSAAI_InstallConfig.xml` file. This path must not contain any spaces.
OFSAAI-1017	The user installation directory is invalid.	Provide a valid installation path. Check if you can create the directory mentioned in the `USER_INSTALL_DIR` tag value of the `OFSAAI_InstallConfig.xml` file. See the My Oracle Support reference document for a workaround on this issue: https://mosemp.us.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=192791484383909&id=2412630.1&_afrWindowMode=0&_adf.ctrl-state=u2t2m1rei_4.

Glossary

Index